Bundesamt
für Sicherheit in der
Informationstechnik

Bundesministerium
für Wirtschaft
und Energie

Standardisierungsstrategie zur sektorübergreifenden Digitalisierung nach dem Gesetz zur Digitalisierung der Energiewende

Roadmap für die Weiterentwicklung der technischen BSI-Standards in Form von Schutzprofilen und Technischen Richtlinien

Vorwort

Mit dem „Gesetz zur Digitalisierung der Energiewende“ (GDEW) hat der Gesetzgeber einen verbindlichen Rechtsrahmen für die stufenweise Modernisierung des Energienetzes zu einem intelligenten Energienetz („Smart Grid“) gesetzt. Es gibt den Unternehmen die Chance, diesen Rahmen mit Leben zu füllen. Für das Bundesministerium für Wirtschaft und Energie (BMWi) geht es parallel darum, den Rechts- und Standardisierungsrahmen zusammen mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) kontinuierlich fortzuentwickeln. Dazu wurde das mehrjährige Projekt „Digitalisierung der Energiewende: Barometer und Topthemen“ aufgesetzt. Das Digitalisierungs-Monitoring („Barometer“) erscheint erstmals im Januar 2019. Ein gesondertes, in Kürze zu veröffentlichendes Gutachten zum Topthema 2 des Barometer-Projektes („Regulierung, Flexibilisierung, Sektorkopplung“) unterstützt das BSI im energiewirtschaftlichen Dialog mit der Branche zu energiewirtschaftlichen Anwendungsfällen für einen Einsatz des Smart-Meter-Gateways (SMGW) in den Bereichen Smart Grid und Smart Mobility. Insgesamt geht es darum, den Auftrag des GDEW zu erfüllen und das SMGW zur Kommunikationsplattform des intelligenten Energienetzes zu ertüchtigen. Die vorliegende Roadmap stellt hierzu die maßgebliche Arbeitsplanung vor. Umgesetzt wird dies durch zahlreiche Arbeitsgruppen des BSI, unterstützt von den Auftragnehmern des Barometer-Projektes.

Herausforderungen der Energiewende – Stellenwert der Digitalisierung

Die Energiewirtschaft steht vor einem beispiellosen Wandel. Die Energiewende stellt die Herausforderung, hunderttausende dezentraler Stromerzeugungsanlagen sicher und beherrschbar in das Stromnetz und den Strommarkt zu integrieren. Diese Herausforderung ist ohne eine grundlegende Modernisierung und Digitalisierung nicht zu meistern. Die angestrebte Digitalisierung fungiert hier nicht als Selbstzweck, sondern ist zentral für eine funktionierende Netzintegration von Erneuerbaren Energien (EE).

Übersetzt für die Energiewende bedeutet Digitalisierung die Vernetzung aller Akteure der Stromversorgung im Smart Grid. Dazu muss die Digitalisierung genau das leisten, was das Smart Grid energiewirtschaftlich erfordert: Sie muss den Ansprüchen der Verbraucher, Erzeuger, Netzbetreiber, Aggregatoren, Direktvermarkter und Lieferanten genügen. Vor allem muss die Digitalisierung eine sichere Kommunikation ermöglichen. Zentraler Inhalt des GDEW ist daher das intelligente Messsystem (iMSys) mit dem Herzstück SMGW als sicherer Kommunikationsplattform.

Das Smart Grid der Zukunft ist für das Gelingen der Energiewende ein unverzichtbarer Baustein. Hierbei stellen sich insbesondere vier Aufgaben: Die Schaffung einer standardisierten, sicheren Infrastruktur, die Gewährleistung von Datenschutz und Datensicherheit, das Setzen von Investitionsanreizen und schließlich die Gewinnung der Akzeptanz bei Verbraucherinnen und Verbrauchern. All diesen Aufgaben stellt sich das Gesetz zur Digitalisierung der Energiewende.

Kerngedanke des GDEW ist ein Infrastrukturansatz: Die bundesweite Einführung des Smart-Meter-Gateways, welches durch das BSI zertifiziert wird. Dieses fungiert als sichere und standardisierte Kommunikationsplattform, als Infrastruktur mit großer Anwendungsbreite. Schließlich gilt es, zahlreiche Anwendungsfälle aus den Bereichen Netzbetrieb, Strommarkt und Energieeffizienz technisch umsetzbar zu machen. Ein Beispiel sind variable Stromtarife. Auch können Millionen dezentrale Erzeugungsanlagen „sichtbar" (zeitnahe Erkennung des Status und der tatsächlichen Energieerzeugung) gemacht werden. Die Möglichkeit der Einbeziehung der Gas- und Wärmemessung schafft zudem große Potenziale für den Wettbewerb, für die Verbraucher und für die Gebäudemodernisierung. Perspektivisch kann das SMGW darüber hinaus als sichere, standardisierte Infrastruktur für Anwendungsfälle im „Smart Home" dienen (z. B. Gesundheitsdienste oder weitere Mehrwertdienste im Bereich der Gebäudeautomatisierung).

Aufbauend auf der digitalen Infrastruktur ist die Entwicklung konkreter Anwendungen, Produkte und Geschäftsmodelle notwendig. Hierfür hat das BMWi das SINTEG-Programm „Schaufenster intelligente Energie – Digitale Agenda für die Energiewende" gestartet. In fünf großen Modellregionen – sog. „Schaufenstern" – mit über 300 Unternehmen und weiteren Akteuren können landesweit Musterlösungen für die technischen, wirtschaftlichen und regulatorischen Herausforderungen der Digitalisierung des Energiebereichs entwickelt und demonstriert werden. Dabei stehen insbesondere sichere, effiziente und massengeschäftstaugliche Verfahren, innovative Technologien sowie Marktmechanismen für flexible, intelligente Netze und Märkte im Fokus. Ziel ist auch das Sammeln von in der Praxis erprobten Erfahrungen für die zukünftige Weiterentwicklung des Rechtsrahmens.

Stellenwert von Datenschutz und Datensicherheit

Vernetzung und Datenaustausch, wie sie das SMGW ermöglicht, bedürfen eines besonderen Schutzes. Auf der einen Seite sind Daten über den Energieverbrauch datenschutzrechtlich sehr sensibel. Auf der anderen Seite sind Daten über Netzzustand, Erzeugung und Verbrauch systemnotwendig und müssen gegen Angriffe geschützt werden.

Datenschutz und Datensicherheit wurden deshalb bei allen Anstrengungen im Bereich Digitalisierung von Anfang an mitbedacht („Privacy & Security by Design"). Schutzprofile und Technische Richtlinien des BSI für Smart-Meter-Gateways geben der Wirtschaft die benötigten verbindlichen Vorgaben für eine praktische Umsetzung. Im Auftrag des BMWi wurden sie vom BSI gemeinsam mit Branchenvertretern und Datenschützern erarbeitet. Auch enthält das Gesetz abschließende Regelungen zum Datenumgang. Nur so ist sichergestellt, dass jeder Akteur die Daten erlangt, die er für die Erledigung seiner gesetzlichen Aufgaben benötigt – aber eben auch grundsätzlich nur diese.

Standardisierungsauftrag des GDEW

Das GDEW hat Smart Metering neu definiert und ein wichtiges Signal für ein zukunftstaugliches Smart Grid gesetzt, denn die Energiewende braucht mehr als nur „smarte Zähler". Das Gesetz unternimmt einen großen

Schritt in Richtung „neuer Energiewelt“ auf Basis der Eckpfeiler Standardisierung, Datenschutz und Datensicherheit, Investitionssicherheit und Akzeptanz.

Die technischen Mindeststandards für Smart-Meter-Gateways müssen gepflegt und kontinuierlich fortentwickelt werden. Sie müssen dabei mit den Anforderungen der Energiewende Schritt halten, einen Mehrwert für die Verbraucher liefern, spartenübergreifend und im Sinne der Sektorkopplung umgesetzt werden (insb. Wärme und Smart Home), relevante Bereiche wie die Elektromobilität einbeziehen und für zukünftige Bedrohungsszenarien gewappnet sein.

Die technischen Herausforderungen werden dadurch nicht kleiner. Nach einer längeren und anspruchsvollen Entwicklungsphase konnte im Dezember 2018 ein wichtiger Meilenstein für die Digitalisierung der Energiewende erreicht werden.

Mit der ersten erfolgreichen Zertifizierung eines SMGW durch das BSI steht erstmals die Digitalisierungstechnologie für die Energiewende zur Verfügung, die das GDEW als der im September 2016 eingeführte neue Rechtsrahmen verlangt. Das erste zertifizierte SMGW zeigt auch, dass Digitalisierung auch bei hohen Vorgaben an Datenschutz und IT-Sicherheit gelingt. Immer mehr Betreiber engagieren sich aktiv und treiben den Prozess der Digitalisierung so nach vorne. Die in diesem Vorwort beschriebenen Aspekte erfordern eine intensive Koordinierung und Planung. Deshalb veröffentlichen BMWi und BSI nunmehr gemeinsam die vorliegende Roadmap mit dem Titel *„Standardisierungsstrategie zur sektorübergreifenden Digitalisierung nach dem Gesetz zur Digitalisierung der Energiewende“*.

Die Roadmap ist der maßgebliche und stetig fortzuschreibende Arbeitsplan für die Fortentwicklung des Smart-Meter-Gateways hin zur umfassenden Kommunikationspattform für die Energiewende. Gleichzeitig unterstützt die Roadmap die weitere Planung des Rollouts intelligenter Messsysteme durch die verantwortlichen Stakeholder.

Das SMGW, welches Datenschutz, Datensicherheit und Digitalisierung erfolgreich miteinander vereinbart, soll zukünftig als Vorbild für die Entwicklung in weiteren Einsatzbereichen dienen. Für Anwendungsvielfalt müssen Datenschutz und Datensicherheit nicht aufgegeben werden. Im Gegenteil: Informationssicherheit ist die Voraussetzung für eine erfolgreiche Digitalisierung. Nur wenn Staat, Wirtschaft sowie Bürgerinnen und Bürger auf den Schutz ihrer Daten vertrauen können und ihre IT-Systeme gegen zunehmende Bedrohungen ausreichend geschützt sind, wird die digitale Transformation gelingen und deren Potential voll ausgeschöpft werden.

Inhaltsverzeichnis

Abbildungs- und Tabellenverzeichnis

1 IT-Sicherheitsstandards für die Digitalisierung der Energiewende

Leitsätze

- Die Energiewende erfordert die Vernetzung der Akteure in einem Smart Grid. Dafür werden verbindliche Standards für Datenschutz, Datensicherheit und Interoperabilität der Systeme benötigt. Diese Standards sollen die Verlässlichkeit, die Effizienz und den Wettbewerb sichern.
- Das Gesetz zur Digitalisierung der Energiewende (GDEW) gestaltet aktiv die Digitalisierung. Es legt die technischen und rechtlichen Grundlagen und gibt den Startschuss für die Etablierung eines Smart Grid in Deutschland. Kernstück ist das vom BSI entwickelte und durch Schutzprofile und Technische Richtlinien standardisierte Smart-Meter-Gateway (SMGW).
- Aufbauend auf dieser digitalen Infrastruktur ist die Entwicklung konkreter Anwendungen, Produkte und Geschäftsmodelle notwendig. Hierfür hat das BMWi das SINTEG-Programm „Schaufenster intelligente Energie – Digitale Agenda für die Energiewende“ mit fünf großen Modellregionen (sog. „Schaufenstern“) gestartet. Dabei stehen insbesondere sichere, effiziente und massengeschäftstaugliche Verfahren, innovative Technologien sowie Marktmechanismen für flexible, intelligente Netze und Märkte im Fokus.
- Das SMGW wurde für einen Einsatz als sichere, datenschutzkonforme und interoperable Kommunikationsplattform im intelligenten Energienetz konzipiert. Ziel ist, dass es nach und nach die bisher eingesetzten Techniken in allen energiewenderelevanten Anwendungsfällen ersetzen, die nicht diesen Anforderungen genügen.
- Der zukünftige Einsatz der SMGW-Architektur für weitere Bereiche (Sub-Metering, Smart Grid, Smart Mobility, Smart Home/Building und Smart Services) führt zu einer kontinuierlichen Fortentwicklung der BSI-Standards im modularen Ansatz nach dem GDEW.
- Kernanliegen dieser Roadmap ist es deshalb, die Standardisierungsstrategie für die sektorübergreifende Digitalisierung nach dem GDEW aufzuzeigen und einen strukturierten Arbeitsprozess für alle Beteiligten zu ermöglichen.
- Die Roadmap ist der maßgebliche Arbeitsplan für die Fortentwicklung des SMGWs für weitere Einsatzbereiche nach dem GDEW hin zur umfassenden Kommunikationsplattform für die Energiewende und unterstützt gleichzeitig die weitere Planung des Rollouts intelligenter Messsysteme durch die verantwortlichen Stakeholder.

Die mit der rasanten Technologieentwicklung einhergehende Digitalisierung aller gesellschaftlichen Lebensbereiche stellt Staat, Wirtschaft und unsere Gesellschaft vor große Herausforderungen. Die zunehmende Digitalisierung und Vernetzung aller gesellschaftlichen Bereiche führt auf der einen Seite zu Effizienzsteigerungen und Prozessoptimierungen in der Wirtschaft sowie zu mehr Komfort bei den Bürgerinnen und Bürgern, indem Produktkomponenten sowie Systeme untereinander kommunikativ verknüpft werden. Auf der anderen Seite steigt damit das Bedrohungspotential deutlich an, da sich die Anzahl der Angriffspunkte erhöht, die Kommunikationsinfrastrukturen immer komplexer werden und die zu verarbeitenden Datenmengen sich vervielfachen.

Die Wahrscheinlichkeit erfolgreicher Angriffe auf digitalisierte Infrastrukturen wird folglich zunehmend größer. Daher sind nachweislich sichere Produktkomponenten und Systeme im Netz sowie eine sichere Kommunikationsinfrastruktur entscheidend für das Vertrauen der Anwender. Eine erfolgreiche digitale Transformation kann nur mit der frühzeitigen Entwicklung und Bereitstellung von allgemeinverbindlichen Sicherheitsstandards und Maßnahmen zur Sicherung der Vertrauenswürdigkeit digitaler Infrastrukturen gelingen. Elektronische Identitäten und Verschlüsselung spielen hier eine zentrale Rolle für eine sichere und datenschutzkonforme Digitalisierung. Durch Verschlüsselung werden Integrität, Authentizität und Vertraulichkeit der Informationen auf den Kommunikationswegen sichergestellt. Die gegenseitige Authentisierung der elektronischen Identitäten untereinander bildet die Vertrauensbasis digitaler Kommunikationsinfrastrukturen. Hierzu müssen neue Technologien in Deutschland entwickelt und erfolgreich eingeführt werden.

Auch der Erfolg der Energiewende in Deutschland steht in Abhängigkeit zur Etablierung neuer digitaler Informations- und Kommunikationstechnologien. Die mit der Energiewende einhergehende fortschreitende Dezentralisierung der Stromerzeugung macht Anstrengungen erforderlich, die steigende Vielzahl an volatil einspeisenden Erzeugungsanlagen sicher und beherrschbar in das Stromnetz zu integrieren. Unabdingbar hierfür ist die Etablierung eines intelligenten Netzes (Smart Grid), das Energieerzeugung, Weiterleitung, Speicherung und Verbrauch effizient verknüpft und ausbalanciert.

Die Möglichkeit, auf Erzeugungsanlagen und flexible Verbrauchseinrichtungen auf Basis digitaler Vernetzung steuernd eingreifen zu können, erfordert ein hohes Maß an Vorkehrungen zur Gewährleistung von Datenschutz und Datensicherheit.

Für den Aufbau eines energiewendetauglichen Smart Grid sind somit **zwei** Grundvoraussetzungen zu erfüllen:

1. Schaffung einer standardisierten, sicheren Infrastruktur getreu dem Grundsatz „Privacy & Security by Design“;
2. Regelungen zum Umgang mit Daten unter Berücksichtigung von Vorgaben zum Datenschutz, zur Datensicherheit und zur Datensouveränität.

Aufbauend auf dieser digitalen Infrastruktur ist die Entwicklung konkreter Anwendungen, Produkte und Geschäftsmodelle notwendig. Hierfür hat das BMWi das SINTEG-Programm „Schaufenster intelligente Energie – Digitale Agenda für die Energiewende“ gestartet. In fünf großen Modellregionen – sog. „Schaufenstern“ – mit über 300 Unternehmen und weiteren Akteuren werden landesweit Musterlösungen für die technischen, wirtschaftlichen und regulatorischen Herausforderungen der Digitalisierung des Energiebereichs entwickelt und demonstriert. Dabei stehen insbesondere sichere, effiziente und massengeschäftstaugliche Verfahren, innovative Technologien sowie Marktmechanismen für flexible, intelligente Netze und Märkte im Fokus. Ziel ist auch das Sammeln von in der Praxis erprobten Erfahrungen für die zukünftige Weiterentwicklung des Rechtsrahmens.

1.1 Das Gesetz zur Digitalisierung der Energiewende

Das am 2. September 2016 in Kraft getretene Gesetz zur Digitalisierung der Energiewende (GDEW) greift diese Grundvoraussetzungen auf und schafft über Vorgaben für die Standardisierung, den Rollout intelligenter Messsysteme und die Datenkommunikation die Basis für den Aufbau einer modernen digitalen Infrastruktur für die Energiewende.

Abbildung 1 - Smart-Meter-Gateway (Beispielhafte Darstellung)

Im Fokus steht hierbei das Smart-Meter-Gateway (SMGW) als Kommunikationsplattform für energiewirtschaftliche und energiewenderelevante Anwendungsfälle des intelligenten Netzes. Dessen Einführung ist in einem neuen Stammgesetz, dem Messstellenbetriebsgesetz (MsbG) geregelt.

Grundkonzeption des Smart-Meter-Gateways als sichere Kommunikationsplattform

Das SMGW stellt die zentrale Systemlösung der sicheren Mess-, Steuer- und Kommunikationsinfrastruktur des Energiesystems dar. Es sorgt dafür, dass alle Kommunikationsverbindungen verschlüsselt werden und nur bekannten Teilnehmern und Geräten vertraut wird. Wird ein elektronischer Stromzähler (im Rechtsrahmen als „moderne Messeinrichtung“ verankert) an diese Kommunikationsplattform angeschlossen, entsteht ein intelligentes Messsystem. Dieses versorgt das Smart Grid mit allen notwendigen Informationen.

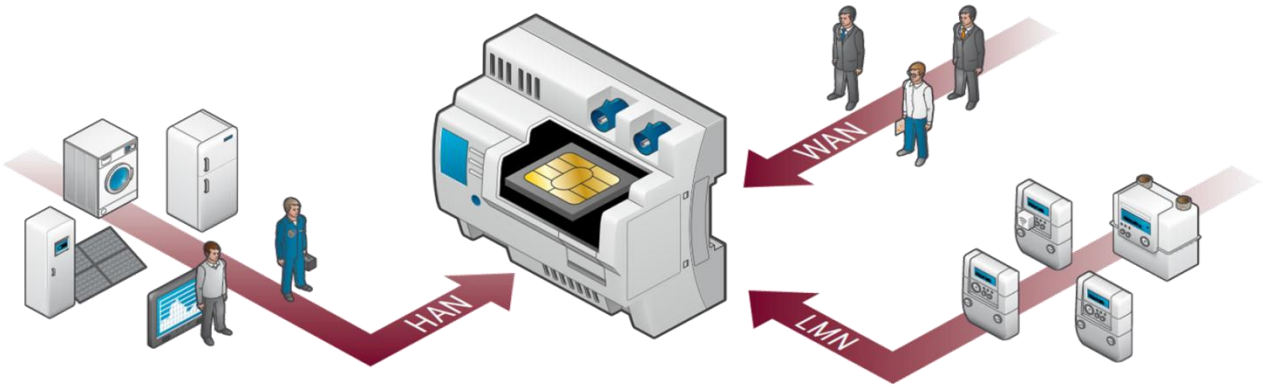

Abbildung 2 - Architektur der SMGW-Kommunikationsplattform

Auf der einen Seite sorgen intelligente Messsysteme für die vom europäischen Rechtsrahmen geforderte Verbrauchstransparenz, die für Energieeffizienzanstrengungen von großer Bedeutung ist. Auf der anderen Seite steht das intelligente Messsystem für die sichere Übermittlung von Mess-, Steuerungs- und Netzführungsdaten sowie Energiemanagement- und Mehrwertdienstdaten. Als Kommunikationsplattform können SMGW die technische Basis nicht nur für die sichere Anbindung verschiedenster Verbraucher und Erzeuger an das Smart Grid sein, sondern auch die technische Basis für ein Last- und Erzeugungsmanagement im Stromverteilernetz bilden. So kann eine einheitliche Plattform geschaffen werden, wie sie für die Netzintegration der Erneuerbaren Energien unabdingbar ist.

Anforderungen an die Sicherheit

Es ist eine große Herausforderung und bedarf einer sorgfältigen Vorbereitung bei der Vernetzung von Millionen von Einheiten mit zahllosen Kommunikationsverbindungen die Sicherheit, den Datenschutz und die Interoperabilität zu gewährleisten. Seit 2011 entwickelt das Bundesamt für Sicherheit in der Informationstechnik (BSI) im Auftrag des Bundesministeriums für Wirtschaft und Energie (BMWi) Anforderungen an SMGW (mit integriertem Sicherheitsmodul), an die Informationssicherheit bei Administration und Betrieb sowie an die vertrauenswürdige Kommunikationsinfrastruktur (Smart Metering - Public Key Infrastruktur, nachfolgend „PKI“). Diese Standards sind auch in den §§ 19-23 des MsbG rechtlich verankert. Auf den Internetseiten des BSI (www.bsi.bund.de) wurden unter dem Oberbegriff „Smart Metering Systems“ bereits entsprechende Schutzprofile (Protection Profile, PP) und Technischen Richtlinien (TR) veröffentlicht. Diese Standards sind die Grundlage für alle aktuellen Entwicklungen der Hersteller und werden in Kapitel 2 genauer erläutert.

Ein Sicherheitsstandard kann nur dann erfolgreich sein, wenn er bereits in der Innovationsphase von Herstellern und Anwendern mitgestaltet wird sowie auf deren breite Akzeptanz stößt. Daher hat das BSI betroffene Verbände aus den Bereichen Telekommunikation, Informationstechnik, Energie, Wohnungswirtschaft und Verbraucherschutz sowie die Datenschutzbeauftragten des Bundes (BfDI) und der Länder, die Bundesnetzagentur (BNetzA) sowie die Physikalisch-Technische Bundesanstalt (PTB) von Anfang an in den entsprechenden Entwicklungsprozess eingebunden.

Zertifizierte Sicherheit und Interoperabilität

Das MsbG regelt in § 24, dass Zertifizierungen für modulare SMGW-Komponenten durchgeführt werden müssen, um den Nachweis der Konformität zu den bereitgestellten Standards zu belegen. Damit wird das Ziel verfolgt, auf Basis einer behördlichen Prüfung Transparenz und Vergleichbarkeit bei der Umsetzung der BSI-Vorgaben durch die Hersteller von SMGW zu schaffen. Die unterschiedlichen Zertifizierungen werden in Kapitel 3 genauer erläutert. Ferner regelt § 25 MsbG auch die Zertifizierung des Smart-Meter-Gateway-Administrators, um einen sicheren Betrieb des SMGW zu gewährleisten. Neben einer Zertifizierung des Smart-Meter-Gateway-Administrators (GWA) durch das BSI kann ein GWA

auch durch eine bei der deutschen nationalen Akkreditierungsstelle (DAkkS) für den Anwendungsbereich des MsbG akkreditierten Zertifizierungsstelle zertifiziert werden.

Das MsbG enthält weiterhin abschließende Vorgaben zum Datenumgang. So wird – getreu dem Grundsatz der Zweckbindung – gewährleistet, dass jeder Akteur aus dem intelligenten Messsystem Daten nur erhält, soweit dies zur Erfüllung seiner Aufgaben erforderlich ist. Dabei erhält jeder Berechtigte die Daten möglichst direkt vom SMGW: Im Zielmodell der Marktkommunikation aus § 60 MsbG (sog. sternförmige Kommunikation) ist es das Gateway, welches selbstständig Daten aufbereitet (inkl. ggf. notwendiger Plausibilisierung und Ersatzwertbildung) und verschlüsselt direkt an alle Akteure versendet. Neben der Berücksichtigung der Datensicherheit und Datensparsamkeit sorgt dies auch dafür, dass der Nutzen aus dem Einsatz intelligenter Messsysteme maximiert wird, da jeder Berechtigte die erforderlichen Daten direkt und nicht über Umwege erhält.

Weitere Einsatzbereiche

Die Grundkonzeption ermöglicht es, das SMGW als sichere Kommunikationsplattform im Smart Grid einzusetzen. Eine stetige Weiterentwicklung des Gateways und seiner Komponenten ist notwendig, um das hohe Sicherheitsniveau aufrecht zu erhalten. Daneben soll das SMGW auch für weitere energiewirtschaftliche und energiewenderelevante Anwendungsfälle eingesetzt werden. Das GDEW sieht deshalb weitere Einsatzbereiche für SMGW vor. Abbildung 3 zeigt einen Überblick über die derzeit adressierten Einsatzbereiche:

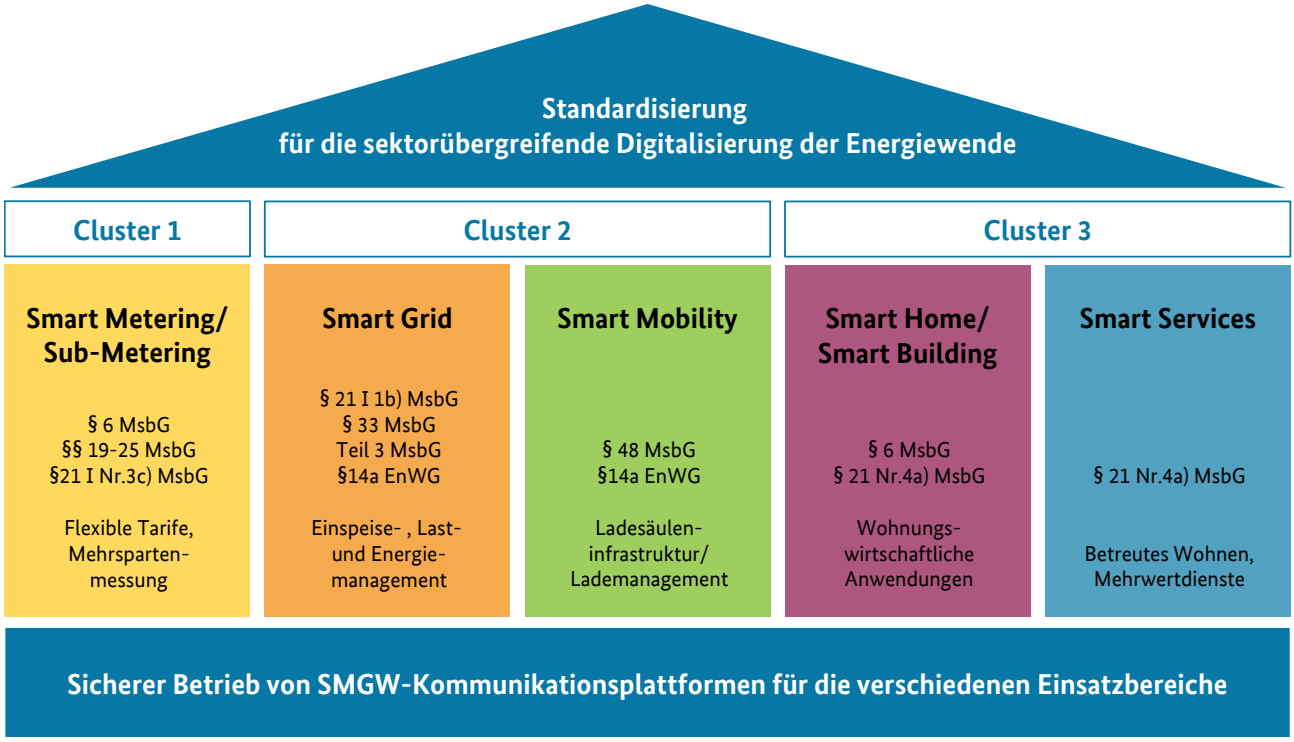

Abbildung 3 – Übersicht der Einsatzbereiche für die Digitalisierung der Energiewende

Für die drei Einsatzbereiche Smart Metering, Smart Grid und Smart Mobility lassen sich auf Basis der gesetzlichen Regelungen (insb. Messstellenbetriebsgesetz) bereits konkrete Anwendungsfälle ableiten. Im Bereich Smart Metering ist die spartenübergreifende Verbrauchsmessung (Strom, Gas, Wasser, Wärme), die dezentrale Tarifierung sowie im Sinne der Energieeffizienzrichtlinie eine sichere, datenschutzkonforme Visualisierung für den Letztverbraucher erfasst. Im Bereich Smart Grid stehen die energiewenderelevanten Anwendungsfälle zur Erhebung und Übermittlung von Netzzustandsdaten, der Ist-Einspeisung sowie die Fernsteuerung von Anlagen (§14a Anlagen, EEG- und KWKG-Anlagen) im Fokus.

Dass Messstellenbetriebsgesetz zeigt auch bereits perspektivisch über § 48 die Ausgestaltung von verbindlichen Mindestanforderungen zur sicheren Integration der Ladesäuleninfrastruktur von Elektromobilen in das intelligente Netz auf. Da noch nicht umfassend abzusehen ist, in welche Richtung sich der technische Fortschritt in der Elektromobilität bewegt, muss die zukünftige Integration der Elektromobilität ganzheitlich betrachtet werden. Daher werden Messsysteme, an denen ausschließlich Messeinrichtungen der Elektromobilität angeschlossen sind, bis zum 31. Dezember 2020 von den Vorschriften des MsbG ausgenommen. Das BSI hat jedoch bereits jetzt die Möglichkeit auch hier entsprechende

Maßnahmen zu treffen, soweit dies zur Abwehr von unverhältnismäßigen Gefahren für Datensicherheit und Datenschutz erforderlich ist.

Die Nutzung der Batterien von Elektromobilen als Stromspeicher und die Erzeugung von Regelenergie, die zum Ausgleich der schwankenden Einspeisung aus Windparks und Solaranlagen gebraucht wird, werden zukünftig eine wichtige Rolle spielen und stehen bezüglich der Anwendungsfälle im engen Zusammenhang mit dem Einsatzbereich Smart Grid. Denn Ladevorgänge von Elektromobilen müssen vorausschauend in Energiemanagementsystemen aufeinander abgestimmt werden, um Netzschwankungen und negative Rückwirkungen in das intelligente Netz zu vermeiden. Die zukünftige Integration des Smart-Meter-Gateways in Ladesäulen ermöglicht ein sicheres und datenschutzkonformes Laden und Abrechnen. Neben Anforderungen an die Ladesäule und an die Gesamtsystemarchitektur sind daher sichere Authentisierungsverfahren, Administration und Betrieb bei Ladepunkten, eine datenschutzkonforme Messwertverarbeitung sowie die Notwendigkeit einer vertrauenswürdigen Kommunikationsinfrastruktur entscheidend.

Für weitere Einsatzbereiche formuliert das Messstellenbetriebsgesetz nach § 21 Abs.1 Nr. 4a lediglich die Anforderung, dass das SMGW „offen“ für mögliche Anwendungen und Mehrwertdienste sein muss. Es handelt sich daher um ein Angebot an die Anbieter aus diesen Bereichen, das SMGW zukünftig als Plattform für ihre Dienstleistungen zu verwenden, um so den Nutzen und die Akzeptanz beim Letztverbraucher weiter zu erhöhen. Konkrete Dienstleistungen sind daher durch den Markt zunächst selbst zu entwickeln. Damit diese Mehrwertdienste (z. B. im Bereich Smart Home abseits von Elektromobilität und Smart Grid Anwendungen) auf dem SMGW aufsetzen können, bietet das SMGW bereits jetzt einen sicheren Kommunikationskanal. Für die Weiterentwicklung der SMGW-Kommunikationsplattform (z. B. um zukünftig benötigte Funktionalitäten) bedarf es daher eines Dialogprozesses, der durch die Arbeitsplanung dieser Roadmap näher beschrieben wird.

Die Grundlagen für die Digitalisierung legt das GDEW über Mindestanforderungen an Funktionsbreite und Ausführung. Die gesetzlichen Anforderungen werden nach und nach vom BSI über detaillierte Standardvorgaben für modulare SMGW-Komponenten ausspezifiziert. Im Anhang befindet sich eine ausführliche Tabelle zu den gesetzlichen Mindestanforderungen an den Funktionsumfang von intelligenten Messsystemen nach dem MsbG. Auch die BNetzA hat Möglichkeiten zur Konkretisierung über Festlegungen. Verkürzt lässt sich sagen: Das GDEW

(insbesondere das MsbG) regelt das „Was“ an gesetzlichen Mindestanforderungen erfüllt werden müssen, welche BSI-Standards hierzu technische Mindestanforderungen vorschreiben und welche BNetzA-Festlegungen orientiert am MsbG, dem EnWG, EEG, KWKG, MessEG getroffen werden können oder müssen.

Mit dem GDEW und der damit verbundenen Einführung intelligenter Messsysteme sowie dem SINTEG-Programm sind wesentliche Maßnahmen ergriffen, um die erheblichen Potenziale der Digitalisierung für das Gelingen der Energiewende zu nutzen und zum Vorreiter in den Bereichen Smart Grid, Smart Meter und Smart Home zu werden. Standardisierte Kommunikationsplattform und „Privacy & Security by Design“- Ansatz können zum Markenzeichen „Made in Germany“ werden und eignen sich als Modell für weitere Bereiche der Digitalisierung. Näheres zu den Weiterentwicklungen der Standards in diesem Sinne enthalten Kapitel 5 und 6.

1.2 Zielsetzung der Roadmap

Dieses Dokument soll Antworten geben auf die Fragen: „Warum, wie und wann entwickelt das BSI Standards für die Digitalisierung der Energiewende?“ Es werden die gesetzlichen und technischen Mindestanforderungen für die SMGW-Kommunikationsplattform erläutert. Zudem werden die technischen Weiterentwicklungsnotwendigkeiten und –Prozesse hin zu einem Sicherheitsstandard für die Energiewende mit folgender Anwendungsbreite beschrieben:

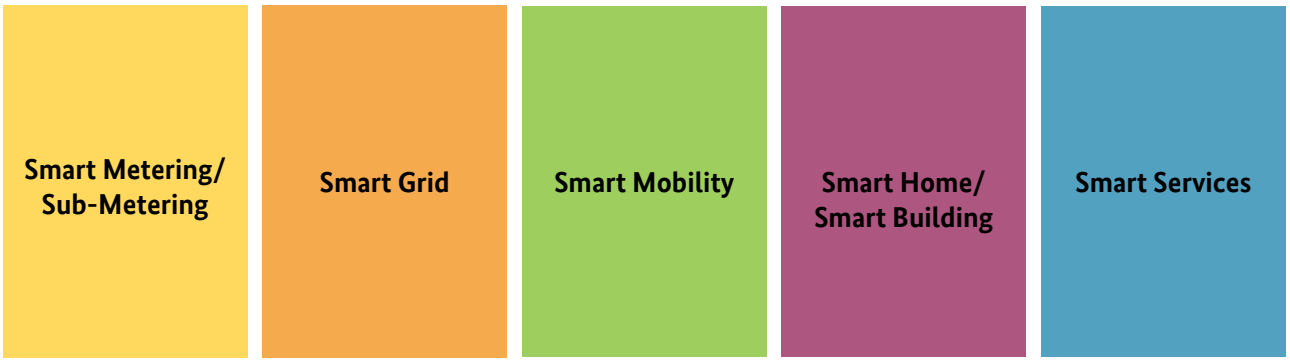

Abbildung 4 – Energiewende relevante Digitalisierungsbereiche nach dem GDEW

Aufsetzend auf den Schutzprofilen und Technischen Richtlinien für das erste SMGW nach Interimsmodell beschreibt dieses Dokument eine Roadmap für die notwendige Weiterentwicklung der BSI-Standards.

Diese Roadmap zeigt für diese und weitere Einsatzbereiche das Prozedere auf, damit das SMGW mit höchsten Ansprüchen an Datenschutz und Datensicherheit schließlich für alle energiewenderelevanten Sachverhalte aus Abbildung 4 zur Verfügung steht.

Indem sie die erforderlichen Arbeitsschritte aufzeigt, vereinfacht und strukturiert die Roadmap den Dialogprozess für die künftigen Arbeiten. Herstellern wie Anwendern soll sie auch dadurch Hilfestellung sein, indem sie den gestuften Rolloutansatz nach dem GDEW erläutert.

Rollout und Weiterentwicklung von Standards werden in einem kontinuierlichen Prozess erfolgen, Abbildung 5 zeigt die wesentlichen Phasen auf, die digitale Infrastruktur standardmäßig nach dem GDEW-Rechtsrahmen durchlaufen muss.

Abbildung 5 - Projektphasen der sektorübergreifenden Digitalisierung der Energiewende

1.3 Aufbau der Roadmap

Dieses Dokument zeigt Aufgaben und Projekte des BSI auf, um den Digitalisierungs- und Standardisierungsauftrag nach dem GDEW zu erfüllen. Diese reichen von der Entwicklung und

Konsolidierung der festgelegten Standards im MsbG für die erste SMGW-Kommunikationsplattform im Einsatzbereich Smart Metering (Kapitel 2) über die Zertifizierungen nach Schutzprofilen und Technischen Richtlinien und den Aufgaben zur Unterstützung der Aufrechterhaltung des sicheren Betriebs der Infrastruktur (Kapitel 3), bis hin zu den Aufgaben zur Einführung und Inbetriebnahme von zertifizierten Produkten (Kapitel 4). Im Anschluss werden die Aufgaben und Projekte zur Analyse und Planung der Weiterentwicklung von BSI-Standards in den verschiedenen Einsatzbereichen dargestellt (Kapitel 5). Dort geht es dann darum, wie und wann die BSI-Standards so weiterentwickelt werden, dass die gesamte Einsatzbreite des SMGW zur Verfügung steht und durch „Zertifikatsnachweise des BSI“ eine geprüfte Sicherheitsleistung auch für erweiterte Einsatzbereiche der SMGW-Kommunikationsplattform und weiterer Komponenten belegt werden kann. Zeitpläne für Digitalisierungs- und Standardisierungsprojekte fassen die Planungen abschließend zusammen (Kapitel 6). Zu Beginn eines jeden Kapitels sind jeweils die Kernaussagen in Leitsätzen hervorgehoben.

2 Schutzprofile und Technische Richtlinien: Schutzkonzept für die Digitalisierung der Energiewende

Leitsätze

- Angesichts der Grundrechts- und Systemrelevanz des Datenaustauschs im Smart Grid hat der Gesetzgeber dem BSI bei der technischen Standardisierung eine zentrale Rolle zugewiesen.
- Die vom GDEW vorgesehenen Schutzprofile und Technischen Richtlinien des BSI verwirklichen ein solches Schutzkonzept. Sie enthalten grundlegende Vorgaben an die Sicherheitsarchitektur genauso wie Detailspezifikationen zur Gewährleistung von Datenschutz, Datensicherheit und Interoperabilität. Zur Aufrechterhaltung des sicheren Betriebs und zur Nutzung des SMGW in weiteren Einsatzbereichen werden Schutzprofile und Technische Richtlinien kontinuierlich weiterentwickelt.
- Bei der Weiterentwicklung wird durch das BSI darauf geachtet, wo technisch möglich und sinnvoll Bewährtes zu überführen, so dass sich bereits frühzeitig Anwendungen und Mehrwertdienste auf bereits vorhandenen Plattformen entwickeln können. Prüfungsmaßstab ist dabei das MsbG. Über einen sicheren Firmware-Update-Prozess werden grundsätzlich Migrationspfade ermöglicht.
- Ein Standard für eine sichere Kommunikationsinfrastruktur kann nur dann Datenschutz und Datensicherheit gewährleisten, wenn er ganzheitlich „Ende zu Ende“ Sicherheit umfasst. Das GDEW bezieht deshalb neben dem SMGW die gesamte Kommunikationskette in das Schutzkonzept mit ein.
- Die Technische Richtlinie TR-03109-1 gibt den jeweils aktuellen „Stand der Technik“ wieder. Mit der Veröffentlichung der TR-03109-1 Version 1.0.1 und der neu hinzugekommenen Anlage VII hat das BSI daher die Technische Richtlinie um ein Interoperabilitätsmodell und funktionale Geräteprofile erweitert.
- Transparenz schafft Vertrauen: Das GDEW stellt deshalb sicher, dass Standards im Dialog mit Branchenvertretern, Behörden, Daten- und Verbraucherschützern vom BSI entwickelt werden. Bei der Weiterentwicklung werden auch die Erfahrungen des SINTEG-Programms einfließen.

Für den Datenaustausch im intelligenten Energienetz hat der Gesetzgeber angesichts der Grundrechts- und Systemrelevanz entschieden, dem BSI bei der technischen Standardisierung des SMGW eine zentrale Rolle zuzuweisen. Es soll Standards entwickeln und Anforderungen für

einen sicheren Betrieb der kritischen Infrastruktur zur Gewährleistung von Datenschutz, Datensicherheit und Interoperabilität aufstellen. Geregelt wird dies in den §§ 19 bis 30 MsbG. Das BSI kann seine Aufgaben bestmöglich erfüllen, wenn es von den Fachleuten der Branchen, von Verbraucher- und Datenschützern genauso wie von Fachbehörden Unterstützung bekommt.

Abbildung 6 zeigt diesen Entwicklung- und Dialogprozess, der charakteristisch sein soll für die Herangehensweise des BSI. Interessenvertreter werden fortwährend eingebunden, ein transparenter Prozess aufgesetzt, an dessen Ende eine Entscheidung über den Standard steht.

Abbildung 6 – Entwicklungs-, Abstimmungs-, Veröffentlichungsprozess für die BSI-Standards

In den folgenden Unterkapiteln werden zunächst die Aufgaben des BSI nach MsbG zur Entwicklung von technischen Vorgaben aufgezeigt und eine kurze Übersicht der bisherigen verankerten BSI-Vorgaben gegeben. Im Anschluss wird der Dialog- und Abstimmungsprozess zur Konsolidierung von Anforderungen an vertrauenswürdige Produkte mit den Fachexperten der Branche aufgezeigt und das Zusammenspiel mit dem Standardisierungsausschuss erläutert. Danach wird auf die Veröffentlichung der Standards und die Festlegung der Nachweispflicht zur Zertifizierung eingegangen.

2.1 Entwicklung der technischen BSI-Vorgaben für die SMGW-Kommunikationsplattform

Wenn vertrauenswürdige, personenbezogene Daten und systemrelevante Netzführungsdaten mithilfe von Systemen wie Zählern ermittelt und über ein Kommunikationsnetz an andere Systeme übertragen werden, so reicht es nicht aus nur punktuell IT-Sicherheit zu realisieren. Um das Vertrauen in die erhobenen Daten zu steigern, eine Ende-zu-Ende gesicherte Datenübertragung zu etablieren und somit die Hürde für Angriffe auf diese Systeme zu erhöhen, ist es wichtig eine ganzheitliche Strategie zur Festlegung von Anforderungen für den Schutz dieser Informationen aufzustellen. Das MsbG verankert deshalb in den §§ 19-23 MsbG eine Regelungssystematik, die es ermöglicht, IT-Sicherheitsstandards zur Gewährleistung von Datenschutz, Datensicherheit und Interoperabilität für die Kommunikation festzulegen. In §§ 19-21 MsbG werden allgemeine energiewirtschaftliche und gesetzliche Mindestanforderungen an intelligente Messsysteme gestellt, die es ermöglichen sollen, den tatsächlichen Energieverbrauch der Letztverbraucher an die Erzeugung aus volatilen Erzeugungsanlagen anzupassen. Sie bieten auch Funktionalitäten, die dazu beitragen können, die Energiebeschaffung in der Weise zu optimieren, dass reale Verbräuche und nicht länger Prognosen die Energiebeschaffung bestimmen. Intelligente Messsysteme können darüber hinaus zur Realisierung von netzdienlichen Prozessen eingesetzt werden, indem sie Netzzustandsinformationen bereitstellen und als eine sichere Plattform für verschiedene Anwendungen aus den Bereichen Energiemanagement, Erzeugungsmanagement und auch weit darüber hinaus dienen.

§ 19 Abs. 2 und 3 des MsbG schließen es aus, dass andere als vom BSI freigegebene Komponenten zur Datenerhebung, -verarbeitung, -speicherung, -prüfung und -übermittlung eingesetzt werden. Den Stand der Technik, den es zu erfüllen gilt, ist durch technische Mindestanforderungen in Form von Schutzprofilen und Technischen Richtlinien geregelt, die unter der Federführung des BSI mit allen beteiligten Interessengruppen erarbeitet und abgestimmt werden. § 19 Absatz 5 MsbG ist insoweit die Übergangsvorschrift, um „stranded investments“ zu vermeiden.

Die folgenden Unterkapitel gehen auf die Ausgestaltung der technischen BSI-Vorgaben für „Privacy & IT-Security by design“ ein, welche zur Umsetzung der gesetzlichen Mindestanforderungen im Einsatzbereich Smart Metering erforderlich sind.

2.1.1 Einsatzbereiche von SMGW-Kommunikationsplattformen

Die energiewirtschaftlichen Anforderungen an Kommunikationsplattformen sind teils höchst unterschiedlich, weisen andererseits aber auch große Gemeinsamkeiten auf. Unterschiedliche Orte, an dem ein Messsystem zum Einsatz kommt, sei es z. B. die Windturbine, die PV-Anlage, der Privathaushalt oder der Industriebetrieb müssen hierbei betrachtet werden. Für unterschiedliche Einsatzbereiche sieht der energiewirtschaftliche Rechtsrahmen zum Teil unterschiedliche bzw. besondere Anforderungen vor (z. B. Anforderungen an die Kommunikationsfähigkeit von EEG-Anlagen im EEG etc.). Das MsbG hat aus den verschiedensten Kommunikationsanforderungen unterschiedlichster Einsatzbereiche gemeinsame Mindestanforderungen destilliert und diese benannt. Schutzprofile und Technische Richtlinien müssen als Standards für die Energiewirtschaft die besonderen Anforderungen der jeweiligen Einsatzbereiche unterstützen und werden deshalb - wo erforderlich – in den Anwendungsfällen nach Einsatzbereichen differenzieren. Mit Hilfe der konkretisierten technischen Anwendungsfälle werden der spezifische Funktionsumfang und zudem die zu erbringende Sicherheitsleistung für SMGWs in der ermittelten operativen Einsatzumgebung bestimmt. § 30 MsbG gibt diese Vorgehensweise vor, indem er verdeutlicht, dass das BSI eine Rolloutfreigabe erst wird erteilen können, wenn in ausreichender Weise intelligente Messsysteme am Markt angeboten werden, „die den am Einsatzbereich orientierten Vorgaben des § 24 Absatz 1 (MsbG) genügen“. Kapitel 4 greift dies auf und enthält weitere Ausführungen zur Marktanalyse des BSI nach § 30 MsbG.

Die SMGW-Architektur soll z. B. neben den modernen Messeinrichtungen auch Erzeugungsanlagen nach dem Erneuerbare-Energien-Gesetz (EEG) und Kraft-Wärme-Koppelungsgesetz (KWKG), Anlagen im Sinne von § 14a des Energiewirtschaftsgesetzes (EnWG) sowie neue Messeinrichtungen für die Sparte Gas, in ein Kommunikationsnetz sicher einbinden können und daneben über die Fähigkeiten verfügen, die das MsbG in den §§ 6, 21-23, 29, 33, 35 und 60 ff. beschreibt. SMGW nach dem GDEW sind auf dieses breite Programm ausgelegt. Einen

detaillierten Überblick über den gesetzlichen Mindestfunktionsumfang von intelligenten Messsystemen nach dem MsbG gibt die im Anhang befindliche Tabelle.

Die Konkretisierung der Anwendungsfälle in den Einsatzbereichen sowie die Ausgestaltung der Standards der zukünftigen SMGW-Architektur wird in Kapitel 5 aufgezeigt. Ziel ist, dass die technischen Standards für die Energiewende alle Einsatzbereiche der Energiewende abdecken.

Dabei sieht das GDEW vor, dass diese Standards als sogenannter Stand der Technik in Schutzprofilen und Technische Richtlinien beschrieben werden. Die folgenden Kapitel geben eine kurze Übersicht über die aktuell verankerten Schutzprofile und Technische Richtlinien.

2.1.2 BSI-Schutzprofile für die SMGW-Kommunikationsplattform

Das BSI entwickelt Prüfstandards in Form von Schutzprofilen unter Beteiligung betroffener Behörden und in Kooperation mit Interessengruppen und Herstellern. Mit Hilfe dieser Standards können informationstechnische Produkte und Systeme geprüft und zertifiziert werden (siehe Kapitel 3). In Schutzprofilen sind generische Mindestsicherheitsanforderungen an eine Produktkategorie festgeschrieben. Sie sind zunächst implementierungsunabhängig, können aber durch die daraus ableitbaren Sicherheitsvorgaben (Security Target) auf einen konkreten Evaluationsgegenstand (Target of Evaluation, ToE) zugeschnitten werden. Anforderungen an die Funktionalität sowie an die Vertrauenswürdigkeit werden in Schutzprofilen zusammengefasst und decken eine bestimmte Menge von Sicherheitszielen vollständig ab.

In einem Schutzprofil sind die allgemeinen Sicherheitseigenschaften sowie die Bedingungen für den sicheren Einsatz des Produktes festgelegt. Dieses Schutzkonzept beschreibt nicht nur den Wert der Daten und deren Verarbeitung, sondern erfasst auch die Annahmen an eine typische Einsatzumgebung.

Der einheitliche Aufbau eines Schutzprofils ist in den Common Criteria (CC) geregelt. Die Common Criteria sind ein internationaler Standard, der allgemeine Kriterien zur Prüfung und Bewertung von Sicherheitseigenschaften von IT-Produkten im Labor bereitstellt. Auf Basis eines Schutzprofils können IT-Produkte evaluiert werden, die nach einer positiven Prüfung ein Zertifikat erhalten und somit nachweislich das Schutzziel erfüllen. Zugleich lässt das

Schutzprofil dem Hersteller Spielraum bei der technischen Ausgestaltung der Sicherheitsanforderungen.

Durch das Verfassen von Schutzprofilen kann das BSI somit Mindeststandards für bestimmte Produktgruppen setzen. Dies hat das BSI bereits initial für den Einsatzbereich Smart Metering umgesetzt. Folgende Abbildung zeigt die im Rechtsrahmen nach § 22 MsbG verankerten Schutzprofile:

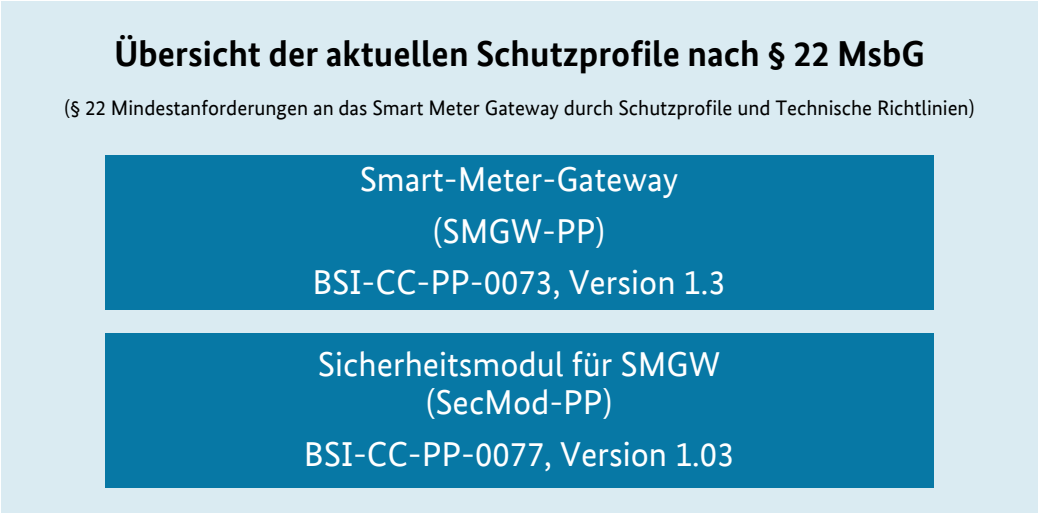

Abbildung 7 - Übersicht der aktuellen Schutzprofile nach MsbG

Dabei beschreiben die Schutzprofile mehrere Sicherheitsziele, die durch das SMGW umgesetzt werden müssen, um den zuvor beschriebenen Bedrohungen in der Einsatzumgebung des Gateways wirksam zu begegnen.

Das SMGW-Schutzprofil BSI-CC-PP-0073 und die ergänzenden Technischen Richtlinien (siehe folgenden Abschnitt) beschreiben das SMGW als vertrauenswürdige, zentrale Kommunikationskomponente mit mehreren Kommunikationsbeziehungen. Die zentralen Punkte des Schutzprofils können aufgrund des Umfangs der Schutzprofil-Anforderungen an dieser Stelle nur zusammengefasst wiedergegeben werden. Die folgende Abbildung 8 zeigt das SMGW in seiner zentralen Kommunikationsrolle:

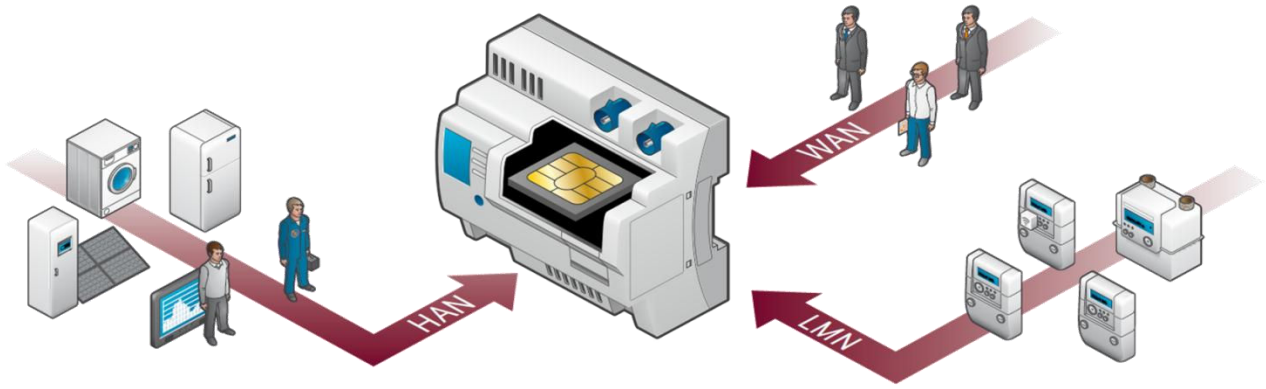

Abbildung 8 - Architektur der SMGW-Kommunikationsplattform

Das SMGW-Schutzprofil stellt hierbei sicherheitstechnische Mindestanforderungen an das SMGW zur Durchsetzung der Separierung der aufgezeigten Netze HAN (Heimnetz), LMN (Lokales Metrologisches Netz) und des WAN (Weitverkehrsnetz). Mit Hilfe von Firewall-Mechanismen wird neben der Separierung der Kommunikationsverbindungen auch der Kommunikationsaufbau durch das SMGW zu externen Marktteilnehmern oder dem SMGW-Administrator (GWA) durchgesetzt. Das Schutzprofil sorgt zudem dafür, dass das SMGW die Kommunikationswege kryptographisch sichert, sodass die Authentizität, die Integrität und die Vertraulichkeit der versendeten Messwerte gewährleistet werden. Des Weiteren erfasst, verarbeitet und speichert das SMGW Messwerte, welche dann mit Hilfe des Sicherheitsmoduls signiert und verschlüsselt zu autorisierten Marktteilnehmern versendet werden. Für die Erfassung von Messdaten und den dabei zu setzenden Zeitstempel muss das SMGW Anforderungen zur regelmäßigen Zeitsynchronisation mit einer vertrauenswürdigen und verlässlichen Zeitquelle erfüllen. Für Erweiterungen im Funktionsumfang und zur Gewährleistung der Sicherheitsleistung hat das SMGW einen sicheren Softwareupdate-Mechanismus bereitzustellen. Authentizität und Integrität des ausgelieferten Updates müssen durch das SMGW überprüft werden. Ferner sind sicherheits-und eichtechnische Ereignisse im Gateway zu protokollieren. Das im Gateway einzusetzende Sicherheitsmodul muss hier die Anforderungen des Schutzprofils BSI-CC-PP-0077 nachweislich erfüllen. Es agiert als kryptographischer Dienstleister und steht dem Gateway als sicherer Schlüsselspeicher zur Verfügung.

Im SMGW-Schutzprofil wird die Vertrauenswürdigkeitsstufe EAL4 (Evaluation Assurance Level 4) für die Prüfung festgelegt. Sie wird mit Vorgaben an den Schutz gegen hohes

Angriffspotenzial (AVA.VAN 5) und Prozeduren zur Fehlerbehebung (ALC.FLR 2) erweitert. Über diese Vertrauenswürdigkeitsanforderungen werden Prüftiefe und Widerstandsfähigkeit gegen Angreifer festgelegt, sodass dem hohen Angriffspotenzial aus dem Weiterverkehrsnetz Rechnung getragen wird.

Im Ergebnis gewährleistet damit das definierte Sicherheitskonzepts des SMGW-Schutzprofils, dass selbst bei unterschiedlicher technischer Umsetzung durch SMGW-Hersteller, einheitliche und vergleichbare Sicherheitsleistungen durch die SMGW-Produkte erbracht werden.

2.1.3 Technische Richtlinien für die SMGW-Kommunikationsplattform

Zur Gewährleistung der Interoperabilität der verschiedenen in einem intelligenten Messsystem vorhandenen Komponenten müssen diese auch rein funktionale Vorgaben erfüllen. Des Weiteren müssen auch die im Schutzprofil getroffenen Sicherheitsanforderungen näher spezifiziert werden. Neben Schutzprofilen entwickelt das BSI daher zusätzlich zu den Schutzprofilen auch Technische Richtlinien (TR). Die Anforderungen für intelligente Messsysteme und deren sicheren Betrieb finden sich in der Technischen Richtlinie BSI TR-03109 wieder.

Die im MsbG verankerten Technischen Richtlinien unterhalb der BSI TR-03109 ergänzen u. a. die Sicherheitsanforderungen des Schutzprofils um funktionale Anforderungen zu Kommunikationsprotokollen, Tarif- und Berechtigungsprofilen sowie kryptographischen Verfahren. SMGW, die eine TR-Zertifizierung auf Basis der technischen Konformitätsprüfung nachweislich bestanden haben, werden sich zukünftig an den Schnittstellen gleich verhalten. Sie können deshalb einheitlich über verschiedene GWA-Systeme angebunden und betrieben werden. Folgende Abbildung zeigt eine Übersicht der aktuellen Technischen Richtlinien nach § 22 MsbG:

Abbildung 9 - Übersicht der aktuellen Technischen Richtlinien nach MsbG

Die Technische Richtlinie BSI TR-03109 ist in mehrere Dokumente untergliedert und widmet sich thematisch neben dem SMGW und dem Sicherheitsmodul auch der Kommunikationsinfrastruktur und dem GWA. Aufgrund des Umfangs und der Komplexität der Vorgaben der Technischen Richtlinien wird hier auf eine vollständige Übersicht der funktionalen Anforderungen verzichtet. Sämtliche Technische Richtlinien sind auf den Internetseiten des BSI verfügbar. Das folgende Kapitel gibt einen Überblick über das Datenschutz- und Datensicherheitskonzept der SMGW-Kommunikationsplattform.

Die Technische Richtlinie TR-03109-1 gibt den jeweils aktuellen „Stand der Technik“ wieder. Mit der Veröffentlichung der TR-03109-1 Version 1.0.1 und der neu hinzugekommenen Anlage VII hat das BSI daher die Technische Richtlinie um ein Interoperabilitätsmodell und funktionale Geräteprofile erweitert. Hier ist bereits ein funktionales Geräteprofil für nach Interimsmodell entwickelte SMGW enthalten. Die Entwicklung der TR 03109-1 v1.1 steht in Abhängigkeit zu den Rahmenbedingungen des Zielmodells der Bundesnetzagentur (u. a. Messwertverarbeitungskonzept). Das BSI strebt eine Veröffentlichung der TR 03109-1 v1.1 für das 4. Quartal 2019 an.

2.1.4 Datenschutz- und Datensicherheitskonzept der SMGW-Kommunikationsplattform

Das MsbG etabliert durch die Verankerung der BSI-Vorgaben ein umfassendes Datenschutz- und Datensicherheitskonzept. Es verlangt den Schutz personenbezogener Daten und fordert hierzu die Umsetzung der IT-Sicherheitsanforderungen aus den Schutzprofilen (SMGW-PP) und der funktionalen bzw. organisatorischen Vorgaben aus den Technischen Richtlinien (TR-03109-1). Das neue Gesetz fordert zusätzlich im Interesse von Datensparsamkeit, Datensouveränität und Effizienz die sternförmige Datenkommunikation (§ 60 MsbG). Das SMGW muss dafür in der Lage sein, jedem Berechtigten Ende-zu-Ende verschlüsselt passgenau die Daten zu schicken, die er berechtigterweise auch bekommen soll. Durch BSI-Vorgaben der TR-03109-1 wird geregelt, dass das SMGW Messwerte erfasst, verarbeitet (inklusive Plausibilisierung und Ersatzwertbildung) und vor Ort im Gateway speichert (Datenhoheit). Dabei werden Messdaten anonymisiert, pseudonymisiert und aggregiert im SMGW aufbereitet (Datensparsamkeit) und sternförmig direkt an berechtigte Stellen verschlüsselt durch das Gateway versendet (Zweckbindung). Die TR-03109-1 beschreibt hierfür konkrete Anwendungsfälle für die Tarifierung und setzt konkrete funktionale Anforderungen an die Messwerterfassung, -verarbeitung und -versendung. Letztverbraucher haben damit volle Transparenz über die im SMGW verarbeiteten Daten und können Kommunikations- und Verarbeitungsschritte nachvollziehen („im Logbuch“). Durch die Dokumentation im Logbuch würde zudem jeder Datenmissbrauch erkennbar und nachweisbar. Dies erleichtert die Durchsetzung von Verbraucherrechten. Die gesicherte, korrekte Verarbeitung der Daten wird durch die Zertifizierung des Gateways beim BSI nachgewiesen. Die hohe Prüftiefe (Evaluation Assurance Level 4) sichert das Vertrauen in die korrekte Implementierung des Datenschutzkonzepts (Kapitel 3).

Bis zu einem Jahresverbrauch von 10.000 Kilowattstunden sieht das Gesetz nach § 60 MsbG standardmäßig nur eine Übermittlung von jährlichen Jahresarbeitswerten an externe 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.

Mit den technischen Standards des BSI wird Datenschutz auf höchstem Niveau umgesetzt; zahlreiche Anforderungen der Datenschutzbeauftragten von Bund und Ländern sind in die Standards eingeflossen. Das MsbG enthält einen detaillierten Katalog für zulässige zweckgebundene Datenkommunikation. Daneben werden Anforderungen der PTB zur Gewährleistung des eichtechnischen Kundenschutzes durch die technischen Anforderungen des BSI durchgesetzt.

2.1.5 Informationssicherheit für Administration und Betrieb von SMGW-Kommunikationsplattformen

Neben den Anforderungen an die vertrauenswürdigen Produktkomponenten der SMGW-Kommunikationsplattform müssen auch BSI-Vorgaben an den Betrieb solcher intelligenten Systeme gestellt werden, um ein einheitliches Sicherheitsniveau für das intelligente Netz zu etablieren. Für den sicheren Betrieb von intelligenten Messsystemen ist nach § 25 Absatz 1 MsbG der Smart-Meter-Gateway–Administrator (GWA) verantwortlich, dies ist nach § 3 Absatz 1 Satz 2 MsbG der Messstellenbetreiber. Das SMGW-Schutzprofil fordert genau diesen vertrauenswürdigen GWA. Um das Vertrauen in seine Handlungen aufzubauen, enthält die TR-03109-6 („Smart-Meter-Gateway Administration“) einheitliche organisatorische und technische Anforderungen sowie Maßnahmen für die Mindestsicherheit beim GWA. Diese Mindest-Maßnahmen sind durch ein Informationssicherheitsmanagementsystem (ISMS) beim GWA konkret auszugestalten und im Rahmen der Zertifizierung nach § 25 Absatz 5 MsbG nachzuweisen (siehe hierzu Kapitel 3).

2.1.6 BSI-Vorgaben zur Teilnahme an der Smart Metering-Infrastruktur

Das Zielbild der rechtlichen Mindestanforderungen des MsbG ist eine Ende-zu-Ende gesicherte Datenübertragung. So legt § 52 Abs. 4 MsbG fest, dass der Austausch von personenbezogenen Daten, Stammdaten und Netzzustandsdaten nur über die Smart Metering PKI gestützte Kommunikation mit den berechtigten Teilnehmern erfolgen muss. Um somit die Schutzziele Vertraulichkeit, Authentizität und Integrität von Informationen zu gewährleisten, sind

Vorgaben an die vertrauenswürdige Kommunikationsinfrastruktur unerlässlich. So wird der ganzheitlichen Strategie des Gesetzes zum Schutz der zu übertragenden Informationen besonders Rechnung getragen.

Die PKI-gestützte Kommunikation des SMGW ermöglicht die gegenseitige Authentisierung der Kommunikationspartner und stellt sicher, dass Daten ausschließlich an registrierte PKI-Teilnehmer gehen. Die Kommunikation erfolgt dabei stets über einen verschlüsselten, integritätsgesicherten Kommunikationskanal. Zudem werden zu sendende Daten vom SMGW zusätzlich auf Inhaltsebene für den Endempfänger verschlüsselt und signiert. Für die gegenseitige Authentisierung der Teilnehmer werden digitale Zertifikate bereitgestellt. Gleiches gilt für die Etablierung eines verschlüsselten, integritätsgesicherten Kommunikationskanals genauso wie für die Verschlüsselung und Signatur von Daten.

Die vertrauenswürdige und sichere WAN-Kommunikation in der Smart Metering Infrastruktur basiert technisch auf der Smart Metering PKI (SM-PKI). Hierzu hat das BSI Vorgaben der TR-03109-4 an die Architektur der SM-PKI entwickelt, mit der die Authentizität der bei dieser Kommunikation eingesetzten öffentlichen Schlüssel der Kommunikationspartner auf WAN-Ebene sichergestellt. Das BSI ist nach § 28 MsbG für den Betrieb der Smart Metering Root Certificate Authority (SM-Root-CA) verantwortlich, welche die Wurzelinstanz (Root) der SM-PKI bildet. Der Wirkbetrieb der Root wird seit dem 1. März 2015 unter der Aufsicht des BSI von einem Zertifizierungsdiensteanbieter durchgeführt.

Für die sichere Kommunikation der Teilnehmer der Smart Metering Infrastruktur werden digitale Zertifikate eingesetzt, welche von unterschiedlichen kommerziellen Anbietern unterhalb der im Auftrag des BSI betriebenen SM-Root-CA ausgestellt werden. Diese kommerziellen Anbieter als SM-Sub-CA stellen eine wettbewerbsorientierte Variante bei gleich hohem Sicherheitsniveau dar.

Eine SM-Test-PKI dient der Entwicklung und Erprobung von Prototypen von SMGW und zugehöriger Infrastrukturkomponenten unter funktionalen Echtbedingungen. Dabei ist das Sicherheitsniveau der SM-Test-PKI niedriger als das der SM-PKI, die für den produktiven Einsatz vorgesehen ist. Ein Übergang aus der SM-Test-PKI in die SM-PKI ist daher nicht möglich.

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 Smart Grid.

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 Smart Grid durch.

2.2 Transparenter Dialog- und Abstimmungsprozess mit Verbänden und Interessengruppen

Wie bereits erläutert hat das BSI von Anfang an sämtliche Stakeholder in die Erstellung und Weiterentwicklung der Schutzprofile und der Technischen Richtlinien eingebunden. Interessierte Verbände, die sich vor dem Hintergrund neuer Anwendungsbereiche an der Weiterentwicklung der BSI-Standards mit technischen Fachexperten beteiligen möchten, können sich gerne an das BSI wenden. Bei der Weiterentwicklung werden im engen Austausch auch die Erfahrungen des SINTEG-Programms einfließen.

2.3 Festlegungen und Bekanntmachungen durch den Standardisierungsausschuss

Standards sind fortlaufend durch das BSI weiterzuentwickeln, um die Anwendungsbreite zu erhöhen, sie zu optimieren und der aktuellen Bedrohungslage anzupassen. Aufgaben und Verfahren dazu müssen institutionalisiert sein. Das MsbG sieht deshalb einen Standardisierungsausschuss vor (vgl. § 27 MsbG). Beschlüsse des Standardisierungsausschusses werden erforderlich, wenn wesentliche Änderungen der Standards und/oder neue Standards anstehen. Der Standardisierungsausschuss ist unter dem Vorsitz des Bundesministeriums für Wirtschaft und Energie aufgestellt, welches auch die Mitglieder für die Dauer von drei Jahren benennt. Folgende ständige Mitglieder des Ausschusses sind gemäß § 27 MsbG für den Ausschuss vorgesehen:

1. Bundesministerium für Wirtschaft und Energie;
2. Bundesamt für Sicherheit in der Informationstechnik;
3. Bundesbeauftragte für den Datenschutz und die Informationsfreiheit;
4. Physikalisch-Technische Bundesanstalt;
5. Bundesnetzagentur;
6. Je ein Vertreter von drei auf Bundesebene bestehenden Gesamtverbänden, deren Belange in dem aktuellen Digitalisierungs- und Standardisierungsvorhaben berührt sind.

Die Anzahl der ständigen Mitglieder für die Punkte 1 bis 5 werden durch das BMWi benannt. Ebenso die konkreten Verbandsvertreter aus Punkt 6 benannt. Zusätzlich kann das BMWi temporäre Mitglieder zu Sitzungen hinzuziehen.

2.3.1 Bekanntmachung der Standards

Die ständigen Mitglieder des Ausschusses setzen die Überwachung der benötigten Standards in gemeinsamen Sitzungen die für die Digitalisierung der Energiewende um. Projekte zur Entwicklung von Standards werden durch das BSI durchgeführt und unter der Federführung des BSI mit den Interessengruppen abgestimmt. Nach erfolgreicher Erstellung werden die Standards durch den Ausschuss bekannt gegeben und veröffentlicht.

2.3.2 Festlegung der Zeitpunkte der Nachweispflichten

Nach erfolgreichem Abschluss der Entwicklung und Veröffentlichung eines Standards ist eine aktualisierte Grundlage für die notwendigen Zertifizierungen nach § 24 MsbG geschaffen. Zusätzlich werden durch den Ausschuss die Zeitpunkte der Nachweispflichten von abgeschlossenen Zertifizierungen für bestimmte Produkt- und Systemkomponenten nach § 27 MsbG festgelegt und bekannt gegeben. Ebenso werden Fristen festgelegt, wie lange ältere Standards noch als Grundlage der Zertifizierung herangezogen werden dürfen und wann der ältere Standard vollständig durch den neuen Standard abgelöst wird.

Weitere Aufgabendefinitionen, Sitzungszeitpunkte und Zusammensetzungen werden durch das Bundesministerium für Wirtschaft und Energie in der ersten Sitzung des Ausschusses

bekannt gegeben. Zudem kann der Standardisierungsausschuss Gremien und Arbeitsgemeinschaften einberufen, um Themen zur Digitalisierung der Energiewende für die Sitzungen des Ausschusses vorzubereiten.

2.4 Weiterentwicklung der IT-Sicherheitsstandards des BSI

Mit dem Ziel, die gesetzlichen Mindestanforderungen für weitere Einsatzbereiche in die technischen Vorgaben des BSI zu integrieren, müssen die Vorgaben der Technischen Richtlinien und der Schutzprofile für die SMGW-Kommunikationsplattform fortentwickelt werden. Dementsprechend sollen im Rahmen zukünftiger Projekte des BSI die gesetzlichen und technischen Mindestanforderungen für die SMGW-Kommunikationsplattform analysiert und die Weiterentwicklungspotentiale hin zu einem IT-Sicherheitsstandard für die Energiewende aufgezeigt werden.

Ebenfalls werden seitens des BMWi parallel Kernfragestellungen zu den verschiedenen Einsatzbereichen durch das Projekt „Digitalisierung der Energiewende: Barometer und Topthemen“ analysiert. Neben diesen Projektergebnissen sind zudem weitere Arbeiten des BMWi zu konkreten Rechtsverordnungen nach GDEW (§ 46 und § 74 MsbG) geplant, welche bei der Weiterentwicklung der BSI-Vorgaben in den kommenden Jahren berücksichtigt werden müssen.

Bei der Fortentwicklung der Schutzprofile und Technischen Richtlinien geht es insbesondere um Anforderungen des zukünftigen Marktkommunikationsmodells. Hier sind u. a. die technischen Vorgaben an die Plausibilisierung und Ersatzwertbildung im SMGW zu nennen. Vorgaben hierfür sind besonders wichtig, da sie die sternförmige Datenkommunikation nach § 60 MsbG umsetzen. Auch geht es um zusätzliche (eichrechtskonforme) Formen zur Visualisierung in einem sog. „Online-Portal“ und um Vorgaben zur sicheren Anbindung von Erzeugungsanlagen und steuerbaren Lasten.

Das BSI wird zudem die kontinuierliche Überwachung und Weiterentwicklung der Sicherheitsstandards für modulare SMGW-Komponenten des Smart Grid und dessen Umsetzung gemäß §§ 26, 27 MsbG gewährleisten (siehe hierzu Kapitel 3.4 und 5).

3 Zertifizierungen und Maßnahmen zur Aufrechterhaltung des sicheren Betriebs

Leitsätze

- Zertifizierungen durch das BSI und durch akkreditierte Zertifizierungsstellen sind wirksame Mechanismen des GDEW, um ein dauerhaft hohes Schutzniveau sicherzustellen.
- Zertifizierungen schaffen Vertrauen, denn sie stellen in einem hoheitlich überwachten Prüfverfahren sicher, dass Gateways hinsichtlich Ihrer Sicherheits- und Interoperabilitätseigenschaften den hohen Standards des BSI aus Schutzprofilen und Technischen Richtlinien entsprechen und Smart-Meter-Gateway-Administratoren über ein angemessenes Informationssicherheitsmanagementsystem verfügen.
- Erlaubt nach dem MsbG ist nur ein Betrieb von SMGW mit gültigen Zertifikaten. Das BSI kann die Gültigkeit der Zertifikate zeitlich befristen, beschränken oder mit Auflagen versehen
- Bei gültigem Zertifikat genießen Hersteller und Anwender von SMGW einen insgesamt 8-jährigen Bestandschutz, sofern die Gültigkeit des Zertifikats durch ein Re-Assessment (Neubewertung) alle zwei Jahre bestätigt wird.
- Meldepflichten für GWA an das BSI schaffen die Basis für eine wirksame Überwachung der Standards und Sofort-Maßnahmen. Je nach Kritikalität des Sicherheitsvorfalls sind ggfs. Maßnahmen durch das BSI erforderlich.

Mit dem Inkrafttreten des GDEW und den darin festgelegten Standards des BSI (siehe hierzu Kapitel 2), ist die Grundlage geschaffen worden, damit Hersteller von SMGW und SMGW-Administratoren entsprechende Zertifizierungen beantragen können.

Da es beim Aufbau und der Nutzung einer intelligenten Mess-, Steuer- und Kommunikationsinfrastruktur nicht zuletzt um die Verwendung einer zentralen Komponente, dem SMGW und dessen Verarbeitung personenbezogener Daten geht, fördern diese Zertifizierungen das Vertrauen in die Sicherheitsleistungen des SMGW und die organisatorischen Fähigkeiten der SMGW-Administratoren. Kurzum: Sie belegen, ob die Anforderungen an Datenschutz, Datensicherheit und Interoperabilität durch Hersteller und Anwender umgesetzt wurden.

Nach Abschluss der Zertifizierungsverfahren folgt die Veröffentlichung der Nachweise in Form von Zertifikatsurkunden und ggfs. von abschließenden Zertifizierungsberichten. Folgende Abbildung fasst vereinfacht die Zertifizierungsphase zusammen:

Abbildung 10 – Zertifizierungsphase auf Basis der BSI-Prüfstandards für § 24 MsbG

Die folgenden Unterkapitel gehen nun näher auf die Zertifizierungen der Produkte und (Management-)Systemen des MsbG näher ein.

3.1 Zertifizierung des SMGW

Zertifizierungen für das SMGW gemäß § 24 MsbG schaffen Vertrauen, denn sie stellen in einem hoheitlichen Prüfverfahren sicher, dass SMGW hinsichtlich Ihrer Sicherheits- und Interoperabilitätseigenschaften den hohen Standards des BSI aus Schutzprofilen und Technischen Richtlinien entsprechen. Der Rechtsrahmen sieht in § 24 MsbG die nationale Zertifizierung des SMGW als zentrale Sicherheitskomponente im Smart Grid durch das BSI vor. Folgende Abbildung gibt einen Überblick der Zertifizierungen in dieser hoch sensiblen Infrastruktur, die nach MsbG durchgeführt werden müssen:

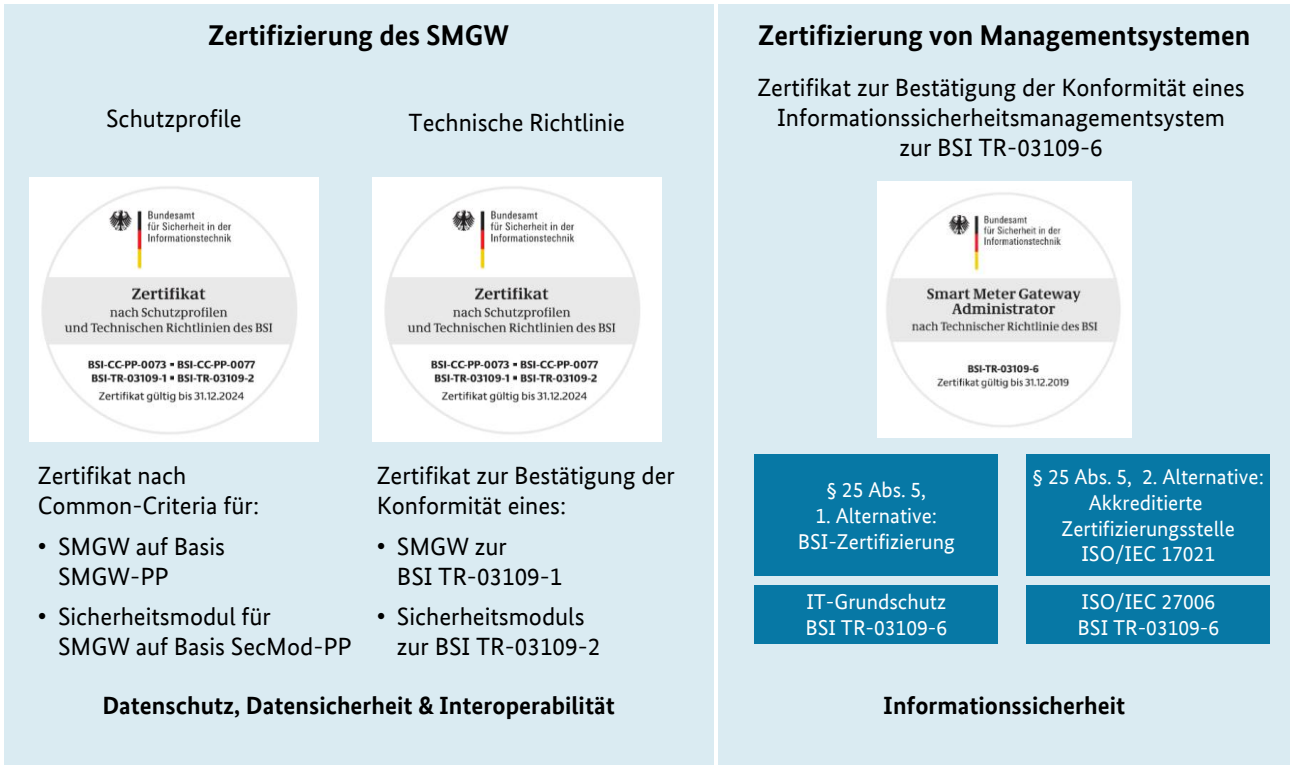

Abbildung 11 - Übersicht der Zertifizierungen für Produkte und Systeme

Im Zuge des Zertifizierungsverfahrens ist eine technische Prüfung (Evaluierung) durch eine vom BSI anerkannte Prüfstelle durchzuführen. Die Prüfung und Zertifizierung wird auf Basis der Common Criteria (CC) und den vom BSI bereitgestellten Schutzprofilen durchgeführt. Sie stellen Prüfanforderungen nicht nur an das IT-Produkt selbst, sondern ebenfalls auch an die Entwicklungs- und Produktionsumgebung des Herstellers. Zusätzlich werden Anforderungen an die vom Hersteller zu erstellende Anwenderdokumentation gestellt. Die Objektivität und die einheitliche Vorgehensweise bei der Evaluierung werden durch die enge Begleitung der Mitarbeiter der hoheitlichen BSI-Zertifizierungsstelle gewährleistet. Am Ende des Verfahrens, nach Abnahme der Prüfergebnisse durch das BSI, erhält der Hersteller ein Zertifikat, welches die erbrachte Vertrauenswürdigkeit und die erfolgreiche Konformität zu den Schutzprofilen belegt.

Zusätzlich zu den PP-Zertifizierungsverfahren nach CC wird durch das BSI die Konformität eines SMGW mit der Technischen Richtlinien TR-03109-1 mit Hilfe einer TR-Zertifizierung nachgewiesen. Um auch hier ein Zertifikat zu erhalten, muss eine Konformitätsprüfung durch eine vom BSI anerkannte Prüfstelle durchgeführt werden. Nach Abnahme des Prüfberichts wird die Konformität durch ein Zertifikat des BSI bestätigt

Der Nachweis ist zur Erfüllung der sicherheitstechnischen Anforderungen im Rahmen des Zertifizierungsverfahrens nach Common Criteria (CC) durch das BSI entscheidend. Die Pflicht zum Einbau eines zertifizierten SMGW wird nach § 30 MsbG jeweils erst dann aktuell, wenn für den konkreten Anwendungsfall die technische Möglichkeit des Einbaus und dessen sicheren Betrieb besteht. Diese Aufgabe, die „Feststellung der technischen Möglichkeit“ zu belegen und bekannt zu machen, wird zukünftig durch das BSI verfolgt. In Kapitel 4 wird auf diese Aufgabe im Zuge des Starts zur Einführung von zertifizierten SMGW näher eingegangen.

Der Zeitpunkt der Nachweispflicht zur Interoperabilität wird durch das BSI noch festgelegt werden und in dem dafür vorgesehenen Verfahren bekannt gemacht. Hersteller von SMGW haben dann das Zertifikat zur Konformität nach der Technischen Richtlinie dem GWA vorzulegen. Grundsätzlich gilt: Systeme müssen die am Einsatzbereich orientierten jeweils gültigen Anforderungen des BSI erfüllen. Systeme, bei denen das nicht der Fall ist, sind innerhalb einer vom BSI festgesetzten Frist z. B. durch ein Update auf den neuesten Stand zu bringen.

3.2 Zertifizierungen für den technischen Betrieb der intelligenten Messsysteme beim Gateway-Administrator

Der Nachweis der Umsetzung der definierten Vorgaben nach BSI TR-03109-6 für den sicheren Betrieb von intelligenten Messsystemen beim Smart-Meter-Gateway-Administrator (GWA) ist erforderlich, um zertifizierte SMGW in der SM-PKI betreiben zu dürfen. Der Nachweis zur Umsetzung kann nach § 25 MsbG entweder durch eine ISO 27001-Zertifizierung auf Basis von IT-Grundschutz (beim BSI) oder alternativ durch eine Zertifizierung gemäß ISO/ IEC 27001 bei einer bei der Deutschen Akkreditierungsstelle (DAkkS) gemäß ISO/IEC 27006 akkreditierten Zertifizierungsstelle erbracht werden. Die Gültigkeit des erteilten Zertifikats beträgt nach ISO/IEC 17021 drei Jahre. Nach Erteilung des Zertifikats erfolgen jährliche Überwachungsaudits durch Personenzertifizierte Auditoren des BSI. Zur Erneuerung der Gültigkeit nach Ablauf der drei Jahre erfolgt eine Re-Zertifizierung.

Nach § 25 Abs. 5 MsbG ist ein GWA verpflichtet, den Auditnachweis zur Erfüllung der Vorgaben dem BSI vorzulegen. So können mögliche Abweichungen bei der Umsetzung von den

Mindestanforderungen durch das BSI frühzeitig analysiert und Handlungsempfehlungen in die Prüfverfahren einfließen.

3.3 Veröffentlichung der Zertifikate und abschließenden Zertifizierungsberichte

Auf den Internetseiten des BSI (www.bsi.bund.de) wurden unter dem Oberbegriff „Smart Metering Systems“ die Schutzprofile und Technischen Richtlinien zum SMGW inklusive Sicherheitsmodul, die Technische Richtlinie zur Administration und Betrieb sowie Vorgaben zur Teilnahme an der Smart Metering PKI veröffentlicht. Nach erfolgreichem Abschluss der Zertifizierungsverfahren werden die Zertifizierungsberichte und Urkunden auf den Internetseiten des BSI veröffentlicht.

3.4 Maßnahmen zur Aufrechterhaltung des sicheren Betriebs der digitalen Infrastruktur

Neben den wirtschaftlichen Rahmenbedingungen für die beteiligten Stakeholder sieht das MsbG auch Regelungen zur Aufrechterhaltung des etablierten Sicherheitsniveaus modularer SMGW-Komponenten vor. Schließlich verändert sich die Bedrohungslage kontinuierlich mit dem technologischen Fortschritt und die Gewährleistung von Informationssicherheit ist ein dauerhafter Prozess. Nach § 26 MsbG muss daher ein kontinuierliches Überwachungs- und Änderungsmanagement der BSI-Vorgaben erfolgen. Ergebnis können geplante Software-Updates auf Basis von weiterentwickelten Standards sein oder BSI Anordnungen für Hersteller und Anwender zum Rollout von Hotfix-Patches. Um für diese Aufgaben gerüstet zu sein, wird das BSI für die Umsetzung dieser Regelungen ein Change-Control-Board (CCB) etablieren.

Abbildung 12 zeigt eine erste Übersicht des Überwachungs- und Änderungsprozesses (Change- und Release-Management) für bestehende BSI-Vorgaben mit Hilfe des Change-Control-Boards auf.

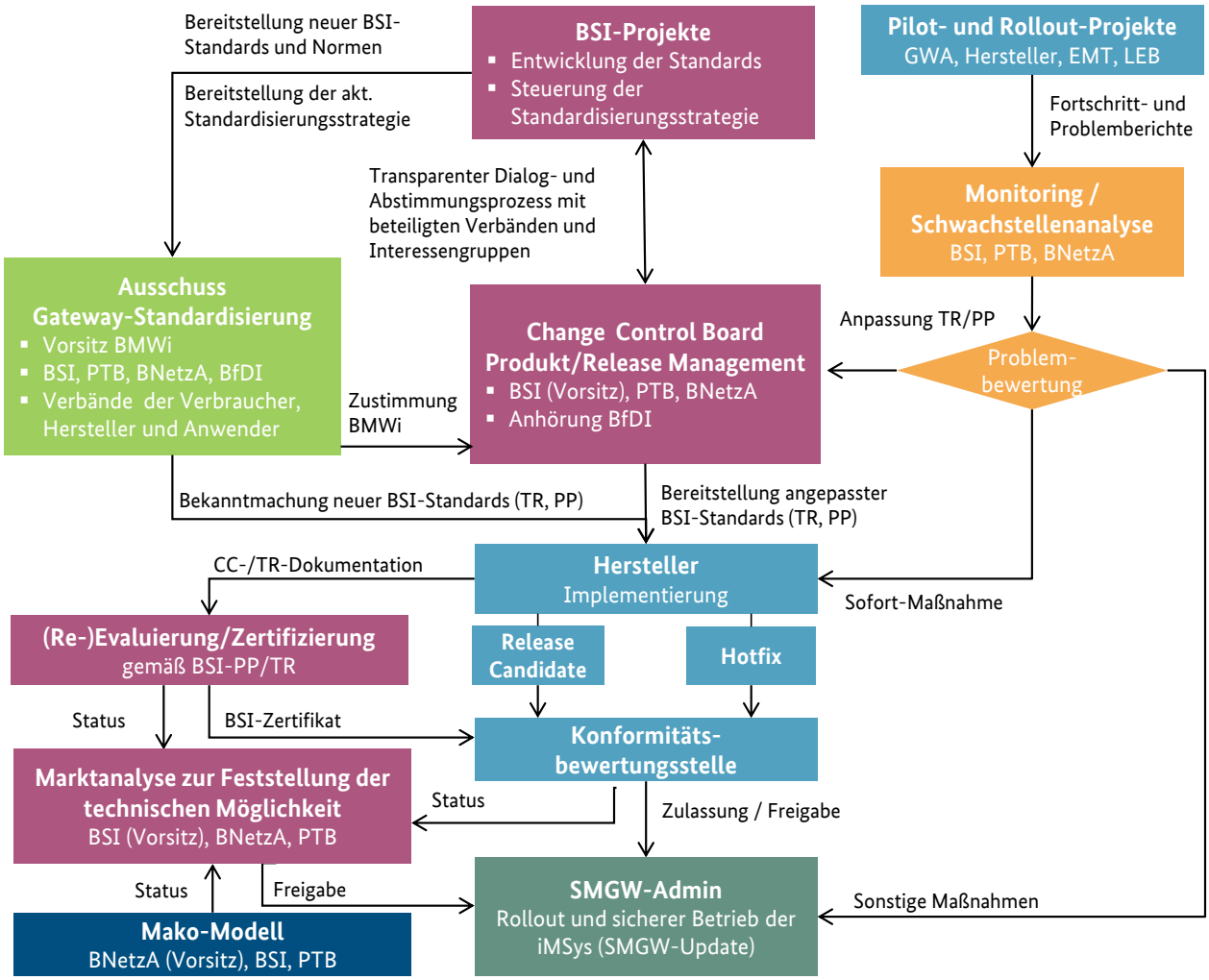

Abbildung 12 - Monitoring und Weiterentwicklung der Vorgaben für modulare SMGW-Komponenten

Die genauen Festlegungen der Überwachungs- und Änderungsprozesse des Change-Control-Boards werden noch durch das BSI weiter ausgestaltet werden.

3.4.1 Bewertung von Fortschritts- und Problem- Meldungen aus dem Test- und Regelbetrieb

Der Rechtsrahmen stellt mit § 25 Abs. 1 MsbG sicher, dass das BSI von Sicherheitsvorfällen und Problemen im Zuge des Rollouts erfährt und wirksame Maßnahmen ergreifen kann. Abbildung 13 illustriert diesen Mechanismus.

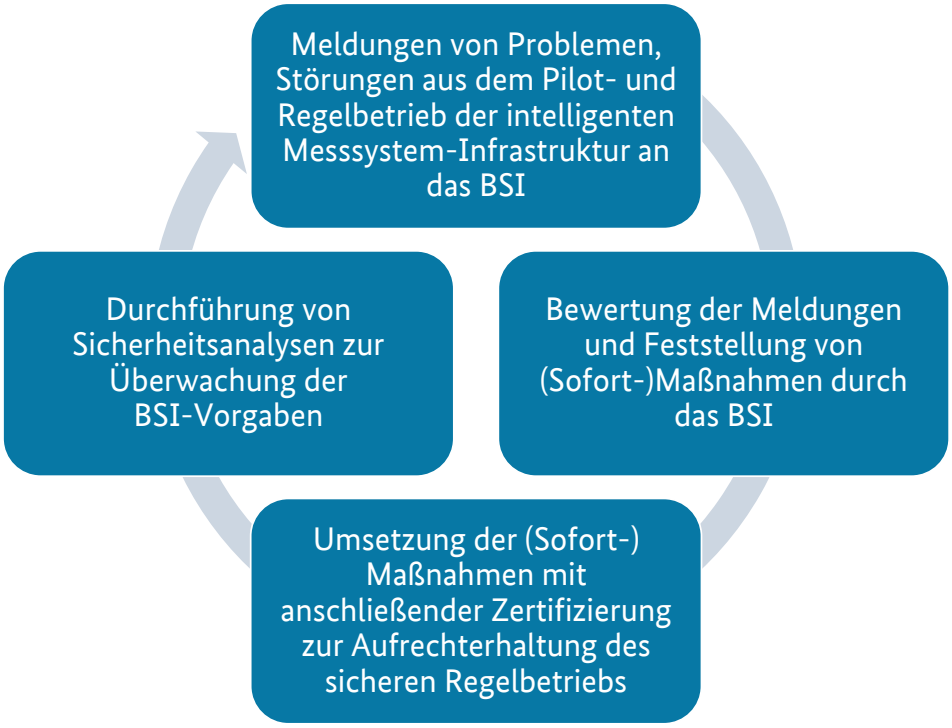

Abbildung 13 – Herleitung von Maßnahmen für den sicheren Betrieb von intelligenten Messsystemen

Das BSI wird Bewertungen dieser Meldungen der beteiligten Unternehmen vornehmen und über ihre Kritikalität entscheiden. Hält das BSI danach kleine Änderungen am veröffentlichten Standard für notwendig, kann es diese selbst vornehmen. Wesentliche Änderungen legt es dem Gateway-Standardisierung-Ausschuss nach § 27 MsbG vor. Je nach Kritikalität der Meldung, sind natürlich auch Sofort-Maßnahmen des BSI (Software-Update oder Hotfix) möglich, die durch Hersteller und Anwender umgesetzt werden müssen.

3.4.2 Zertifizierung zur Aufrechterhaltung des sicheren Regelbetriebs

§ 19 Abs. 3 MsbG regelt, dass Messstellen nur mit SMGW betrieben werden dürfen, die erfolgreich eine BSI-Zertifizierung durchlaufen haben und somit nachweislich den Vorgaben des BSI genügen. Sofern ein Software-Update auszurollen ist, muss dies zunächst zertifiziert werden. Im Falle eines Hotfixes erfolgt die Zertifizierung im Anschluss. § 24 Abs. 2 und 3 MsbG stellt die Verbindung zur BSI-Zertifizierungs-und-Anerkennungsverordnung (BSIZertV) her, wodurch grundsätzlich Zertifikate des BSI zu befristen sind. Weiter können Zertifikate unter dem Vorbehalt des Widerrufs sowie unter Nebenbestimmungen, insbesondere mit Auflagen, erlassen werden. Für den Technologiebereich SMGW hat das BSI die Zertifikatslaufzeit auf einen Gültigkeitszeitraum von 8 Jahren, in Anlehnung an das MessEG, beschränkt und mit der

Auflage verbunden, dass die Geräte alle 2 Jahre einer BSI-Neubewertung (Re-Assessment) unterzogen werden müssen. Durch Fortentwicklung der Angriffstechniken, bei Bekanntwerden neuer Schwachstellen einer Produkttechnologie oder bei Auslaufen der Gültigkeit von kryptografischen Algorithmen und Parametern „altert“ ein bestehendes Zertifikat oder kann sogar seine Gültigkeit verlieren. Zur Verifikation der Gültigkeit eines Zertifikates kann eine BSI-Neubewertung der Angriffsresistenz nach dem aktuellen Stand der Technik beantragt und durchgeführt werden. Auch bei einem Zertifikat, bei dem explizit eine Neubewertung nach einer bestimmten Frist gefordert ist, kann diese Überprüfung durch eine Neubewertung durchgeführt werden.

Das BSI erarbeitet zukünftig eine Richtlinie zur Aufrechterhaltung des einheitlichen Sicherheitsniveaus für den sicheren Betrieb von zertifizierten SMGW.

3.4.3 Überwachung der BSI-Standards durch regelmäßige Sicherheitsanalysen des BSI

Zusätzlich zu den Auswertungen der Meldungen aus dem Regelbetrieb der intelligenten Messsysteme führt das BSI Sicherheitsanalysen nach § 26 MsbG (respektive § 7a BSIG) durch. Auf Basis der Ergebnisse der Sicherheitsanalysen werden auch hier Änderungen an den veröffentlichten BSI-Standards erfolgen bzw. neue BSI-Standards nach § 27 MsbG erstellt.

4 Rolloutansatz des GDEW: Marktanalyse, stufenweise Einführung und Inbetriebnahme intelligenter Messsysteme und weiterer Komponenten

Leitsätze

- Das GDEW setzt den Rahmen für den stufenweisen Einsatz von SMGW als Kommunikationsplattformen im Smart Grid. Die gesetzlichen Einbaufälle umfassen alle energiewenderelevanten Situationen.
- Die Marktanalyse des BSI gibt den Startschuss für den Rollout. Für die Einbaugruppen des § 31 MsbG, für die die technische Möglichkeit nach § 30 MsbG festgestellt wird, kann der Rollout beginnen.
- Das zeigt die entscheidende Bedeutung der Marktanalyse nach § 30 MsbG. Sie fasst das Marktangebot in einer „Rollout-Tauglichkeitsbewertung“ zusammen.
- Das BSI wird ab 2019 jährlich zum 31. Januar die Marktanalyse nach § 30 MsbG veröffentlichen (erstmalig zum 31. Januar 2019). Unterjährige Aktualisierungen erfolgen anlassbezogen.
- Bis zur Einbaupflicht können nach § 19 Absatz 5 MsbG übergangsweise herkömmliche Systeme verwendet werden.

Das GDEW setzt den Rahmen für den stufenweisen Einsatz von SMGW als Kommunikationsplattformen im intelligenten Energienetz. Die gesetzlichen Einbaufälle umfassen dabei alle energiewenderelevanten Situationen: Von PV-Anlagen ab einer installierten Leistung von mindestens 7 kW bis hin zur großen Windturbine, von dem größeren Privathaushalt mit einem Jahresverbrauch über 6.000 kWh bis zum Industriebetrieb, von der steuerbaren Wärmepumpe über das Elektromobil und seiner Ladevorrichtung bis hin zu vom Netzbetreiber ausgewählten Punkten.

Die §§ 29 ff. MsbG regeln, unter welchen Voraussetzungen die zertifizierten Gateways bei Anschlussnutzern und Anlagenbetreibern verpflichtend einzubauen sind. Es wird ein Rollout-Mechanismus festgelegt, der die flächendeckende Durchführung von Digitalisierungsprojekten der Hersteller und Anwender fördert. Die folgende Abbildung zeigt den Rolloutpfad des Gesetzes.

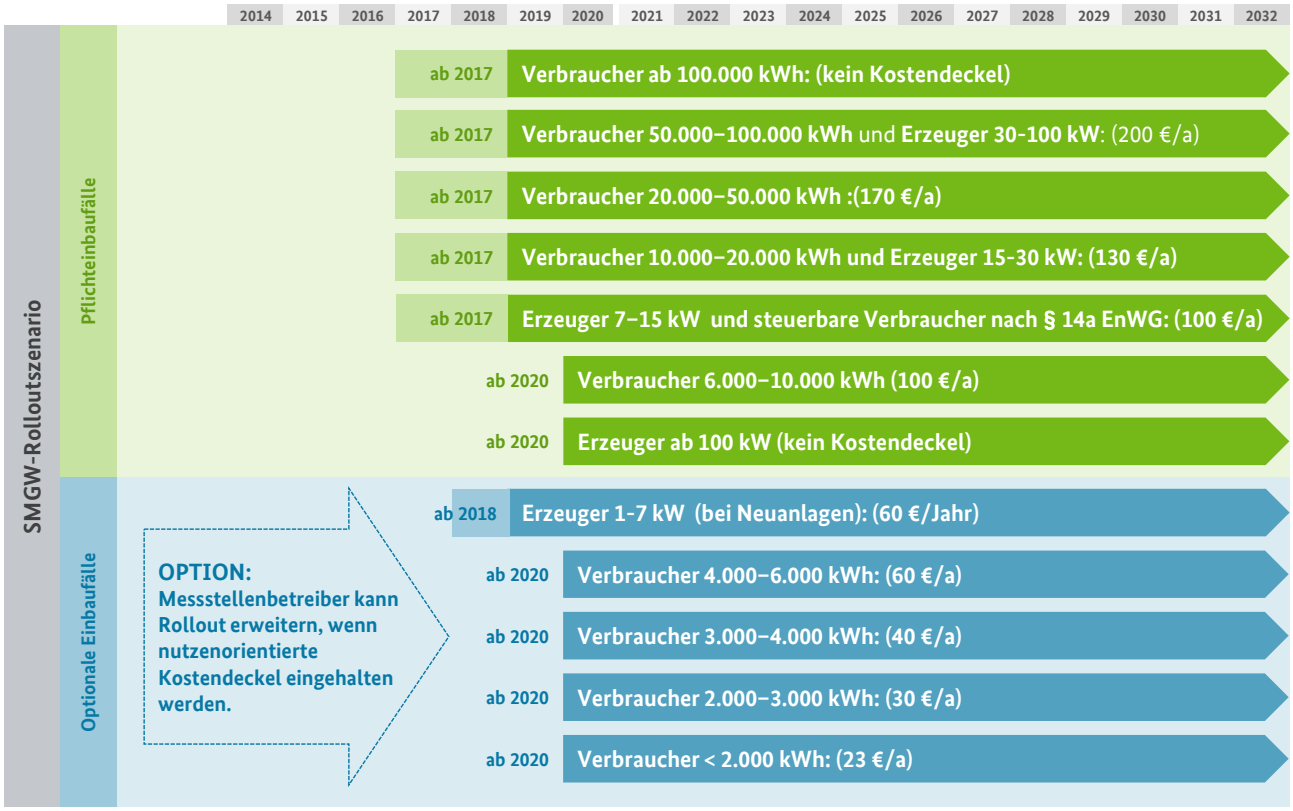

Abbildung 14 - Rolloutszenario nach Einbaugruppen des MsbG

Da ein Einbau nicht vorgenommen werden kann, wenn für den jeweiligen Einsatzbereich die Technik mit der notwendigen Ausstattung noch nicht am Markt verfügbar ist und/oder ein zuverlässiger Betrieb der Technik nicht gewährleistet ist, steht der gesamte abgebildete Rolloutpfad unter der Bedingung der technischen Möglichkeit nach § 30 MsbG.

Hierfür ist folgendes erforderlich:

- Fertigstellung und Bekanntmachung anwendungsfallbezogener Schutzprofile und Technischer Richtlinien durch das BSI;
- Marktverfügbarkeit von zertifizierten SMGW (mindestens drei unterschiedliche Unternehmen) mit den vom MsbG geforderten Fähigkeiten, die der Einsatzbereich verlangt;
- Positive Analyse des BSI und Freigabe für den Rollout.

Es gilt somit der Grundsatz, dass nur BSI-konforme SMGW-Komponenten mit entsprechender Zertifizierung Bestandteil einer Einbauverpflichtung werden können. Hierbei kommt dem BSI die zentrale Rolle zu, die im Folgenden erläutert werden soll.

Abbildung 15 ordnet die Entscheidung nach § 30 MsbG in den Gesamtzusammenhang ein.

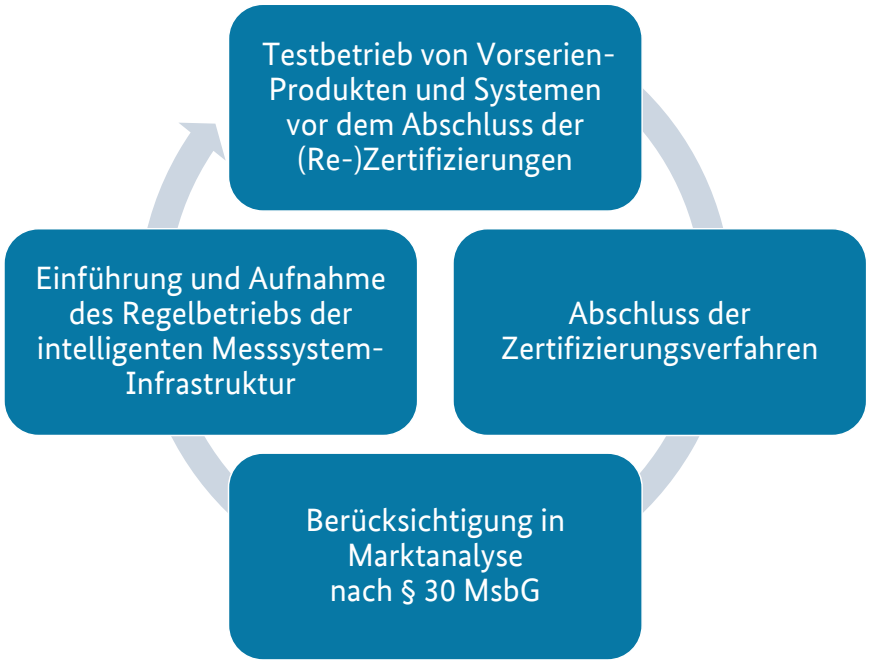

Abbildung 15 – Stufenweise Einführung der intelligenten Messsysteme Infrastruktur

Im Weiteren werden nun in diesem Kapitel die Aufgaben des BSI während der Einführungsphase dargestellt.

4.1 Startschuss für den Rollout: Feststellung der technischen Möglichkeit und Freigabe für den Rollout von intelligenten Messsystemen

Erforderlich für die technische Möglichkeit ist u. a. eine abgeschlossene Zertifizierung von marktreifen SMGW-Geräten nach Vorgaben des SMGW-Schutzprofils für den betrachteten Einsatzbereich. Erst wenn das BSI eine Freigabe erteilt hat, kann die technische Möglichkeit zum Einbau vorliegen und folglich die Einbauverpflichtung für den konkreten Anwendungsbereich greifen, welcher in den Vorgaben des BSI festgelegt wird.

Unterschiedliche Einsatzbereiche (z. B. Industriepark mit gleichzeitiger Erfassung mehrerer Medien, Windturbine mit Funktionalitäten zum Einspeisemanagement und zur Direktvermarktung, PV-Kleinanlage mit Speicherung eines Steuerprofils) bringen unterschiedliche Anforderungen an ein SMGW mit sich. Die unter Beteiligung der relevanten

Interessengruppen weiterzuentwickelnden Schutzprofile und Technischen Richtlinien des BSI werden dies berücksichtigen.

Das BSI kann für die unterschiedlichen Anwendungsfälle unterschiedliche „Startschüsse" setzen. Die Vorgaben für das erste SMGW nach Interimsmodell finden sich in den Schutzprofilen und Technischen Richtlinien, die bereits im Verkündungszeitpunkt im Anhang des MsbG waren. Die weitergehenden Vorgaben für das SMGW nach Zielmodell werden aktuell durch das BSI erarbeitet (siehe Zeitplan in Kapitel 6.1). Folgende Tabelle gibt einen zusammenfassenden Überblick der Zertifizierungsgrundlagen des SMGW:

SMGW	Schutzprofil	Technische Richtlinie
Interimsmodell	BSI-CC-PP-0073 v1.3	BSI TR-03109-1 v1.0.1
Zielmodell	BSI-CC-PP-0073 v2.0 (in Bearbeitung)	BSI TR-03109-1 v1.1 (in Bearbeitung)

Tabelle 1 - Vorgaben für das SMGW

Erst wenn das BSI der Auffassung ist, dass unter Einbeziehung der genannten Akteure für den jeweiligen Anwendungsfall die notwendigen Standards erarbeitet wurden und auch eine hinreichende Verfügbarkeit von zertifizierten Produkten am Markt vorliegt, gibt es die jeweiligen Einbaugruppen nach §31 MsbG frei. Im folgenden Kapitel wird nun auf die Marktanalyse nach § 30 MsbG genauer eingegangen.

4.1.1 Durchführung von Marktanalysen durch das BSI

Der Startschuss für den Rollout und den verpflichtenden Einbau von zertifizierten SMGW-Produkten kann erst dann gegeben werden, wenn die Marktanalyse des BSI nach § 30 MsbG dies hergibt.

Für den Beginn des Rollouts von SMGW ist zunächst der Nachweis der erfolgreichen Zertifizierung des SMGW erforderlich. Im Zuge der Feststellung der technischen Möglichkeit wird das BSI in den Marktanalysen nicht nur auf den Status der Zertifizierungen für die Produktkomponente SMGW selbst eingehen. Abbildung 16 zeigt die Bewertungsbereiche der Marktanalyse zur Feststellung der technischen Möglichkeit unter Berücksichtigung der Einbaugruppen, Einsatzbereiche und Anwendungsfälle. Die Basis für die verschiedenen Bewertungsbereiche stellen die veröffentlichten BSI-Standards in Form von Schutzprofilen und

Technischen Richtlinien dar. Somit wird neben dem Status der Produktzertifizierungen auch die Umsetzung der Vorgaben für den GWA und für die PKI geprüft.

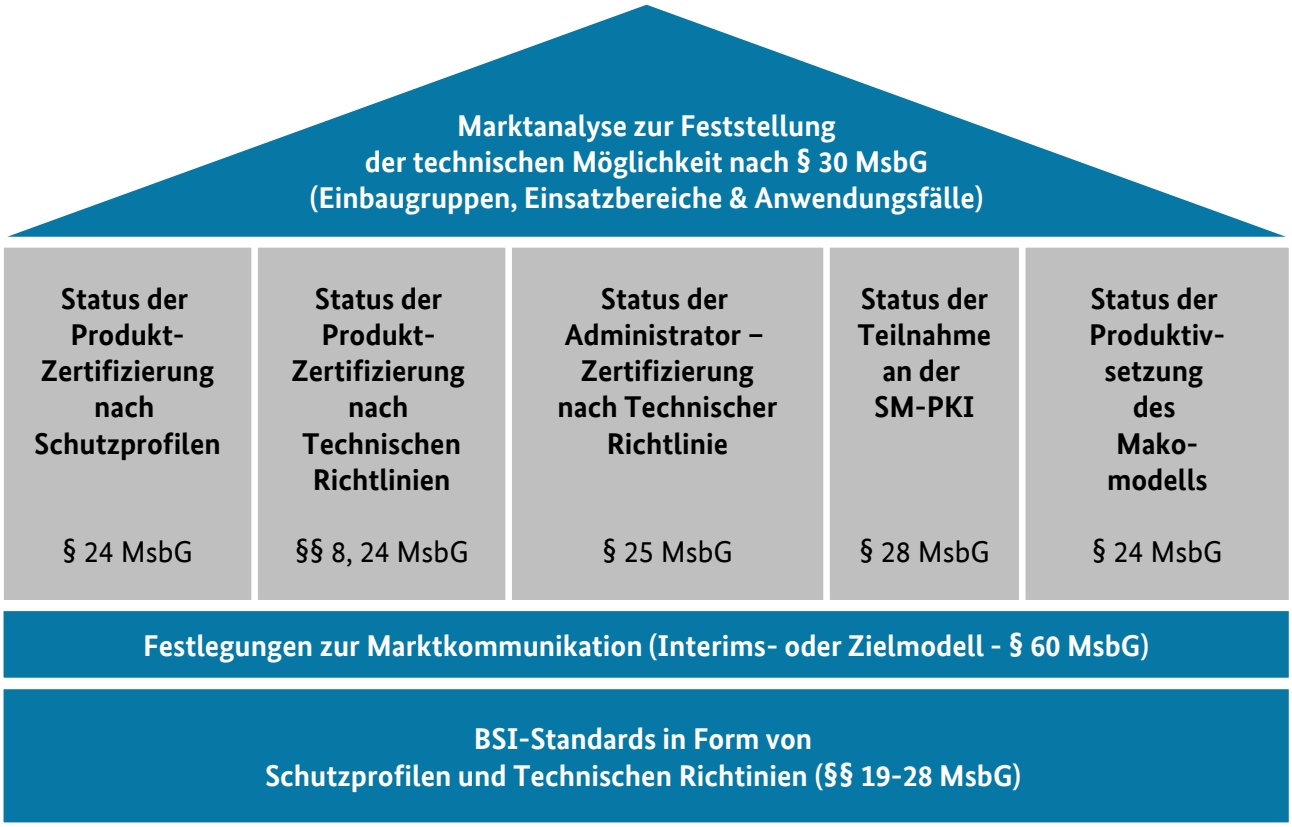

Abbildung 16 – Rollout-Szenario nach Einbaugruppen des Messstellenbetriebsgesetzes

Zusätzlich sind die BNetzA-Festlegungen zur Marktkommunikation für das zugrundeliegende Marktkommunikations-Modell nach § 60 MsbG und ihre Umsetzung im Markt relevant. Dazu haben BNetzA und BSI einen engen Abstimmungsprozess zur Festlegung gemeinsamer Leitplanken etabliert, damit auf der einen Seite das BSI die technischen Spezifikationen und zum anderen die BNetzA die notwendigen Anpassungen der Marktkommunikationsprozesse parallel vorantreiben kann.

Schließlich müssen die erfolgreich abgeschlossenen Produkt-Zertifizierungen in Bezug zum umgesetzten Marktkommunikations-Modell betrachtet werden. Durch das zugrundeliegende umgesetzte Marktkommunikations-Modell wird entschieden, wie die Regelungen in den §§ 49-70 MsbG zur Datenkommunikation in intelligenten Energienetzen zur Geltung kommen müssen.

Unter der Voraussetzung, dass die technische Möglichkeit festgestellt wird, adressiert § 31 MsbG verschiedene Einbaugruppen zu unterschiedlichen Zeitpunkten. Das zeigt die entscheidende

Bedeutung der Marktanalyse. Sie fasst das Marktangebot in einer „Rollout-Tauglichkeitsbewertung“ zusammen. Ausgehend von der betrachteten Einbaugruppe und dem vorgesehenen Einsatzbereich werden in der Analyse aufgezeigte Anwendungsfälle bewertet. Eine Marktanalyse wird demnach alle Anwendungsfälle des Einsatzbereiches identifizieren, die es mit dem zugrundeliegenden Stand der Technik im Sinne des sicheren Betriebs dieser Infrastruktur umzusetzen gilt.

4.1.2 Veröffentlichung der Ergebnisse der Marktanalyse

Nach positivem Ergebnis der Marktanalyse des BSI zur Feststellung der technischen Möglichkeit für die zertifizierten modularen SMGW-Komponenten in dem betrachteten Einsatzbereich erfolgt die Freigabe für den Rollout der zertifizierten SMGW-Komponenten. Nach Freigabe des Rollouts greift die Verpflichtung für den Einbau von intelligenten Messsystemen. Hierzu wird das BSI die Ergebnisse der Marktanalysen zu den betrachteten Einbaugruppen und den betrachteten Einsatzbereichen auf der Internetseite www.bsi.bund.de/SmartMeter veröffentlichen. Die dazu erforderliche Marktanalyse nach § 30 MsbG wird das BSI ab 2019 jährlich am 31. Januar veröffentlichen und anlassbezogen unterjährig aktualisieren.

4.2 Begleitung der Digitalisierungs- und Rollout-Projekte der Hersteller und Anwender

Innerhalb der verschiedenen Bewertungsbereiche können Rollout-Projekte diverse Phasen vom Testbetrieb bis hin zum Regelbetrieb (auch parallel) durchlaufen. Die folgende Abbildung stellt die zu erwartenden Projektphasen der ersten beiden Rollout-Stufen dar. Sie zeigt ebenfalls Schritte für den Rollout der zukünftigen SMGW-Architektur im jeweiligen Marktkommunikationsmodell auf.

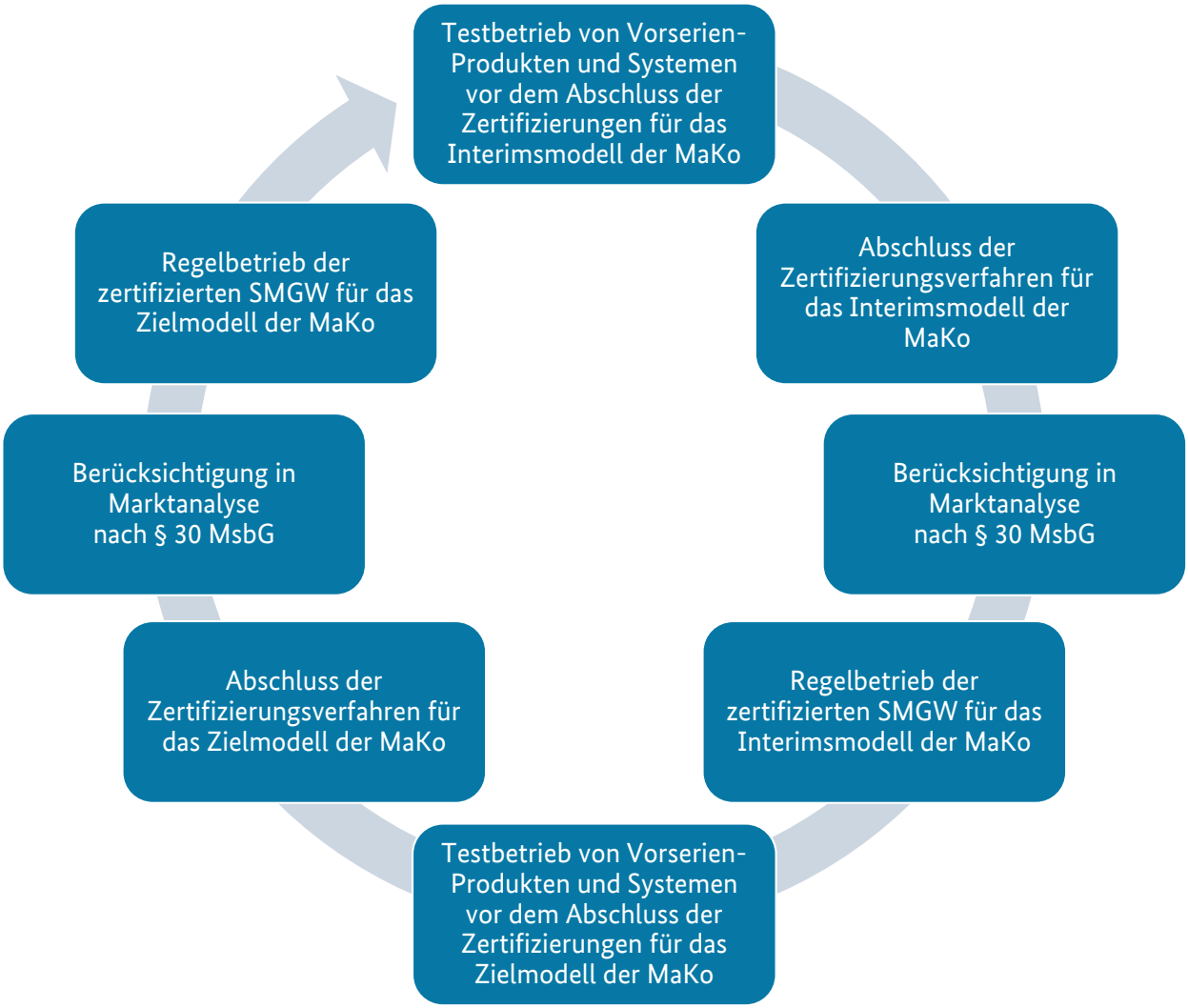

Abbildung 17 – Projektphasen bis zum vollständigen Betrieb der zertifizierten Produkte- und Systeme

Im Folgenden werden die möglichen Phasen bis zum Regelbetrieb kurz zusammengefasst.

4.2.1 Testbetrieb von Vorserienprodukten der intelligenten Messsystem-Infrastruktur

Im Zuge der Rollout-Projektplanung werden Hersteller und Messstellenbetreiber Testphasen bis zum finalen Regelbetrieb planen. In einer ersten Phase werden Tests mit Vorserien-Produkten und Administrations-Systemen durchgeführt. Nach § 19 Abs. 5 MsbG dürfen Messsysteme, die noch nicht nachweislich den BSI-Standards entsprechen, übergangsweise eingebaut werden, wenn keine IT-Sicherheitsbedenken existieren und die Anschlussnutzer dem Einbau zugestimmt haben. Entwicklungsbegleitend bieten sich GWA- und Hersteller-Tests zu aktuellen Funktionsumfängen und Betriebsprozessen an. Anpassungen der eigenen

Betriebsprozesse sowie den Feldtestbetrieb der Vorserien-Produkte in der Test-PKI sind Ziele, die es in dieser Phase zu erreichen gilt. Neben der eigentlichen Produktzertifizierung wird in der Regel parallel auch das Zertifizierungsprojekt für den sicheren technischen Betrieb beim GWA aufgenommen. Nach den eigentlichen Labortests und kleineren Feldtests, die mit einer begrenzten Menge von Vor-Serienprodukten ausgestattet werden, werden die SMGW mit den ersten GWA-Systemen im Backend betrieben. Auch hier wird der Testbetrieb weiterhin mithilfe einer Test-PKI umgesetzt, da Vorserien-Produkte und GWA-Systeme eingesetzt werden, die noch nicht durch das BSI zertifiziert sind und zusätzlich nicht vollständig für eichrechtliche relevante Prozesse zugelassen sind. In dieser Konstellation werden alle Prozesse des gesamten Lebenszyklus der Geräte getestet. Insbesondere für den Rollout von geplanten Software-Updates werden Hersteller und Betreiber entsprechende Teststufen einplanen.

4.2.2 Regelbetrieb des intelligenten Messsystems im Interimsmodell

Das MsbG ermöglicht auch für die Modernisierung der Marktkommunikation ein stufenweises Vorgehen. So kann die BNetzA auf dem Weg zum vollumfänglichen Messstellenbetrieb mit intelligenten Messsystemen im Zielmodell einen Zwischenschritt mit einem Übergangsmodell für die Marktkommunikation einziehen. Mit ihrer Festlegung vom 20. Dezember 2016 hat sie davon Gebrauch gemacht. Abbildung 18 fasst auf einem Blick die Bewertungsbereiche zusammen, die für einen Startschuss für den Rollout von intelligenten Messsystemen zu betrachten sind. Zur Veranschaulichung sind in der Abbildung 18 die Bewertungssäulen gefärbt. Sie können ihre Farbe von „grau“ (siehe Abbildung 16) nach „gelb“ (siehe Abbildung 18) für den Zwischenschritt im Interimsmodell wechseln. Der Farbwechsel nach „grün“ (siehe Abbildung 19) kann erst im Zielmodell erfolgen.

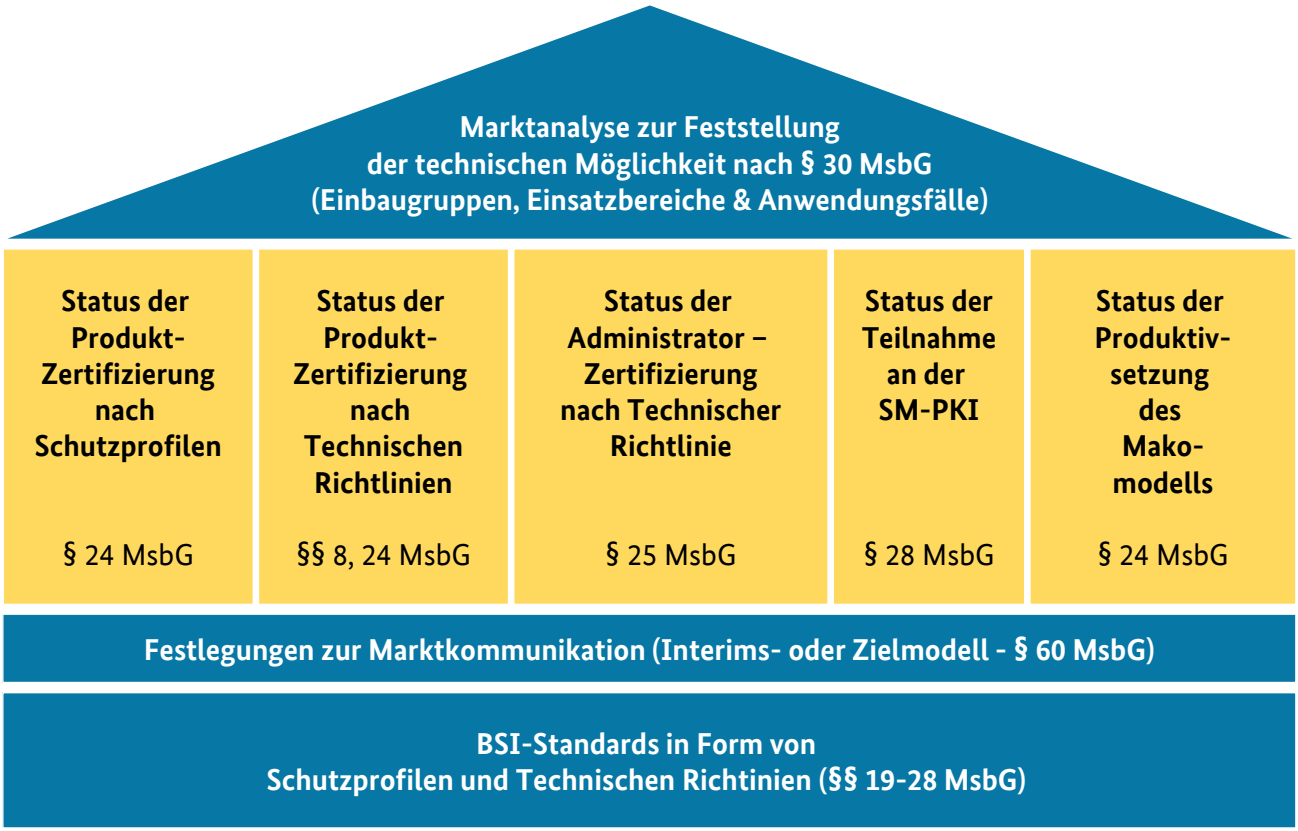

Abbildung 18 –Status der Bewertungen für die Freigabe nach § 30 MsbG für das Interimsmodell

Für die Rollout-Projekte werden zur Einführung von intelligenten Messsystemen neben den nach Eichrecht zugelassenen modernen Messeinrichtungen bereits zertifizierte Serienprodukte von SMGW nach Interimsmodell verfügbar sein. Das Interimsmodell der BNetzA nach § 60 MsbG gibt hier die Prozesse der Marktkommunikation vor. Zertifizierte SMGW werden die Sicherheitsanforderungen des Schutzprofils BSI-CC-PP-0073 nach § 22 MsbG erfüllen. Hierzu müssen SMGW-Hersteller als Nachweis das Zertifikat des BSI gegenüber dem GWA und dem zugehörigen Messstellenbetreiber vorlegen. Um diese zertifizierten SMGW zu betreiben, müssen die zugehörigen Zertifizierungsverfahren vom GWA erfolgreich abgeschlossen sein. Erst dann darf er an der SM-PKI gestützten Marktkommunikationsinfrastruktur für den zugehörigen MSB teilnehmen. Die Pflicht zum Nachweis der Konformität nach BSI TR-03109-1 ist für das Interimsmodell durch eine eichrechtliche Konformitätsbewertung (Verweis auf § 8 MsbG) zu erbringen. SMGW-Hersteller müssen zudem die Einhaltung eines oder mehrerer Geräteprofile durch eine verbindliche Konformitätserklärung gegenüber dem BSI bestätigen. Die funktionalen Anforderungen der Technischen Richtlinie zur sternförmigen Datenkommunikation, den Vorgaben zur souveränen zweckgebundenen Datenerhebung und

die Anforderungen an die Datensicherheit bzw. Datenschutz werden konform zu den Festlegungen des Zielmodells der Marktkommunikation bereitgestellt. Mit diesen beschriebenen möglichen Ergebnissen würde die BSI-Marktanalyse den Startschuss für den Rollout der G1-SMGW für das Interimsmodell der Marktkommunikation geben können.

4.2.3 Regelbetrieb des intelligenten Messsystems im Zielmodell

Nach dem Regelbetrieb im Interimsmodell steht der Regelbetrieb im Zielmodell an. Abbildung 19 gibt einen Überblick zu den Bewertungsbereichen im Zielmodell:

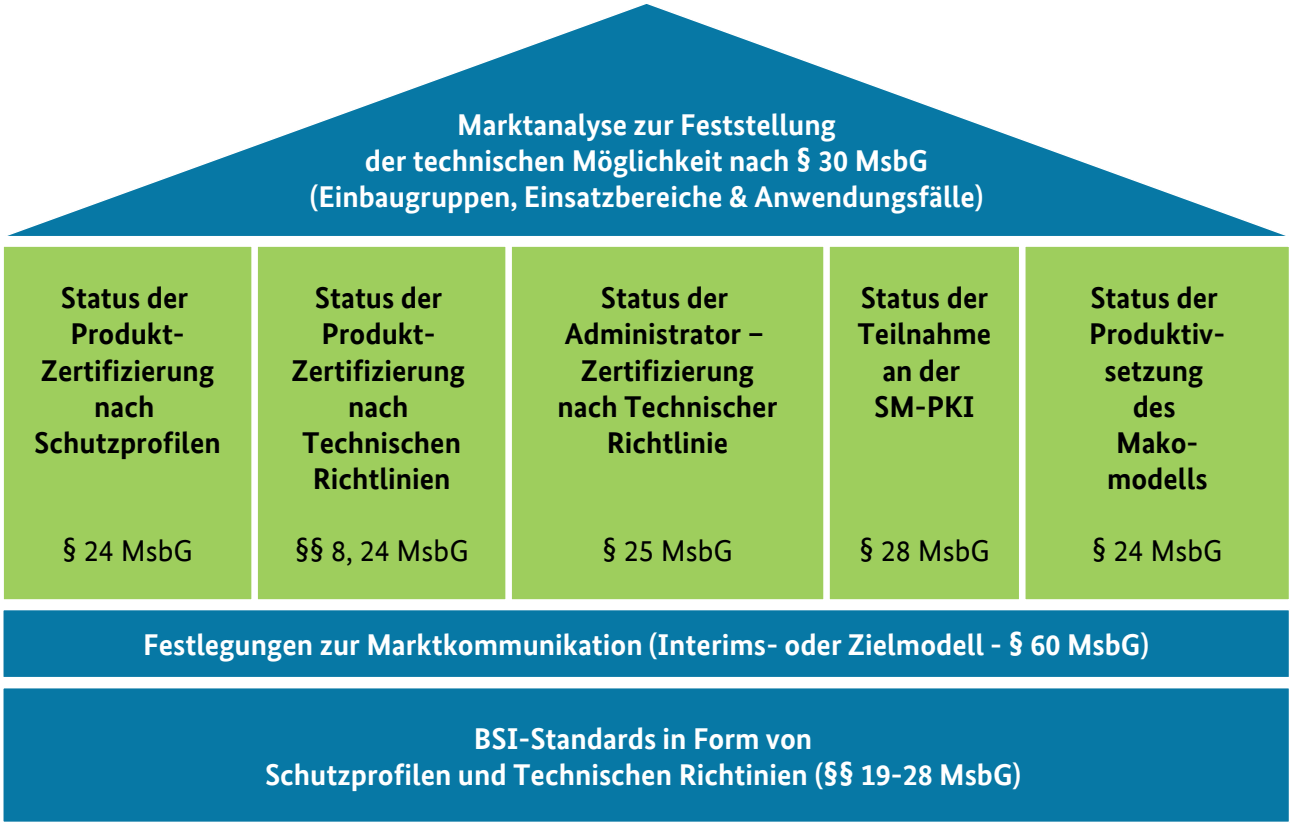

Abbildung 19 – Erwarteter Status der Bewertungen für die Freigabe nach § 30 MsbG für das Zielmodell

Auch hier müssen SMGW und GWA die zugehörigen Zertifizierungsverfahren erfolgreich abgeschlossen haben. Neu ist: Um eichrechtlich relevante Geschäftsprozesse mit den zertifizierten Gateways abwickeln zu können, müssen Hersteller von SMGW nun die Zertifizierungen nach der Technischen Richtlinie TR-03109-1 erfolgreich abgeschlossen haben. Darin werden alle eichrechtlichen Anforderungen der PTB-A50.8 für das SMGW integriert sein. Somit kann eine eichrechtliche Konformitätsbewertung auf den Ergebnissen der PP- und TR-Zertifizierung des BSI aufbauen. Der Nachweis der eichrechtlichen Anforderungen kann somit

aufbauend auf bundeseinheitlichen Mindestvorgaben des BSI erbracht werden. Für diese Phase müssen die Festlegungen der BNetzA zum Zielmodell umgesetzt worden sein. Schließlich baut die erfolgreiche Zertifizierung nach BSI TR-03109-1 u. a. auf die Realisierung der Zielmodell-Prozesse zur sternförmigen Datenkommunikation (inklusive Plausibilisierung und Ersatzwertbildung). Erst dann ist das Datenschutz- und Datensicherheitskonzept des MsbG aus § 60 vollständig umgesetzt.

Hersteller müssen für bereits verbaute SMGW nach Interimsmodell zertifizierte Software-Updates bereitstellen, um die SMGW für das Zielmodell aufzurüsten, sodass der Funktionsumfang der verbauten Geräte im Laufe der kommenden Jahre über Software-Updates erweitert werden kann. Die Migration des Regelbetriebs vom Interims- zum Zielmodell des SMGW obliegt jedoch in der Verantwortung der Hersteller und Betreiber einen kontinuierlichen Verbesserungsprozess (KVP) zu etablieren und diesen fortwährend über den Geräte-Lifecycle anzuwenden. Bei der Weiterentwicklung wird durch das BSI darauf geachtet, wo technisch möglich und sinnvoll Bewährtes zu überführen, sodass sich bereits frühzeitig Anwendungen für weitere Einsatzbereiche auf bereits vorhandenen Plattformen entwickeln können.

Verfehlen SMGW-Hersteller und Betreiber das Migrationsziel, dürfen nur noch bereits verbaute SMGW nach Interimsmodell für die Dauer der Gültigkeit des BSI-Zertifikats (max. 8 Jahre) betrieben werden. Voraussetzung hierfür: Hersteller müssen die regelmäßigen (zweijährigen) BSI-Neubewertungen (Re-Assessment, siehe Kapitel 3.4.2) bestehen. Mit der Freigabe für den Rollout durch das BSI dürfen nur noch SMGW nach Zielmodell verbaut und betrieben werden.

Im Ergebnis ermöglicht das MsbG Herstellern und Betreibern einen stufenweisen Rollout zur Etablierung der neuen digitalen Infrastruktur. Weitere Stufen des Schutzkonzepts zur Digitalisierung der Energiewende beschreibt das folgende Kapitel. Im Fokus stehen dabei die Weiterentwicklungen der BSI-Standards nach dem GDEW.

5 Potenziale ausschöpfen: Weiterentwicklung von BSI-Standards für die sektorübergreifende Digitalisierung

Leitsätze

- Das zukünftige Smart Grid wird nicht nur eine hohe Anzahl an steuerbaren Erzeugungsanlagen, Speicher- und Verbrauchseinrichtungen aktivieren, sondern kann auch den technologischen Brückenschlag zur Sektorkopplung leisten.
- Das GDEW ist auf die sektorübergreifende Digitalisierung angelegt: § 48 MsbG unterstellt den Bereich Elektromobilität ab 2021 dem Geltungsbereich; § 6 MsbG ermöglicht ab 2021 die Einbeziehung der Sparten Wärme (inkl. Heizwärme) und Wasser.
- § 33 MsbG erfordert Smart Grid-Fähigkeiten (u. a. zum Erzeugungsmanagement); § 21 MsbG verlangt für weitere Dienste (Smart Services oder Mehrwertdienste) gerüstet zu sein. Das Gesetz gibt damit den Fahrplan für die Weiterentwicklung der Standards vor.
- Das BMWi-Projekt „Digitalisierung der Energiewende: Barometer und Topthemen“ ist das energiewirtschaftliche Pendant zur technischen Roadmap. Das Barometer-Projekt beleuchtet die regulatorischen, die Roadmap die technischen Modernisierungspfade für die weitere Digitalisierung der Energiewende.
- Im Rahmen des SINTEG-Programms werden Lösungen für technische, wirtschaftliche und regulatorische Herausforderungen der Sektorkopplung entwickelt und demonstriert. Dabei stehen konkrete Anwendungen, Produkte und Geschäftsmodelle im Fokus. BMWi und BSI binden eigene Förderprojekte als Know-How Partner gezielt in den Weiterentwicklungsprozess ein. Mit dem SINTEG-Programm aber auch einzelnen Projekten wie dem BMWi-Elektromobilitätsprojekt DELTA wird dies bereits praktiziert. Sie unterstützen das BSI durch die Identifikation von Anwendungsfällen des Einsatzbereiches und prägen damit die Digitalisierung dieser Bereiche.
- Für die Weiterentwicklung der Standards wird es drei Schwerpunkt-Cluster geben:
    - Smart- & Sub- Metering
    - Smart-Grid & Smart-Mobility
    - Smart Home & Building & Services

Für eine sektorübergreifende Digitalisierung der Energiewende bedarf es weiterer Standards für ein sicheres Smart Grid. Denn dieses Smart Grid wird für die zukünftige Energieversorgung

nicht nur eine hohe Anzahl an steuerbaren Energieerzeugungsanlagen, Speicher- und Verbrauchseinrichtungen integrieren, sondern kann auch mit einem technologischen Brückenschlag die EE-Stromnutzung in den Sparten Wärme und Verkehr unterstützen. Im Rahmen des SINTEG-Programms werden deshalb Lösungen für technische, wirtschaftliche und regulatorische Herausforderungen der Sektorkopplung entwickelt und demonstriert. Dabei stehen konkrete Anwendungen, Produkte und Geschäftsmodelle im Fokus. Das MsbG enthält deshalb auch Regelungen für zukünftige Einsatzbereiche der SMGW-Kommunikationsplattform. Es ermöglicht hierzu die Entwicklung weiterer Standards, um somit neue digitale Informations- und Kommunikationstechnologien, getreu dem Zielbild des GDEW, zu etablieren. Das Schutzkonzept für die Digitalisierung der Energiewende wird dadurch weiter ausgebaut. Dabei wird strikt der stufenweise Rolloutansatz verfolgt. SMGW mit ihren Funktionsumfängen im Zielmodell bilden die Basis für die Einbeziehung aller weiteren Bereiche. Im Zuge der Weiterentwicklung durch das BSI wird darauf geachtet, wo technisch möglich und sinnvoll Bewährtes zu überführen, so dass sich bereits frühzeitig Anwendungen und Mehrwertdienste auf vorhandenen Plattformen entwickeln können. Das SINTEG-Programm aber auch einzelne Projekte wie das BMWi- Elektromobilitätsprojekt DELTA unterstützen das BSI bei der Identifikation von weiteren Energiewende-spezifischen Anwendungsfällen und zukunftsweisenden Standards.

Im folgenden Kapitel wird aufgezeigt, welche Schwerpunkte der Rechtsrahmen für die sektorübergreifende Digitalisierung identifiziert. Daraus leiten sich Arbeitsschwerpunkte für die zukünftige Standardisierung des BSI ab.

5.1 SMGW-Kommunikationsplattformen für die verschiedenen Einsatzbereiche

Die umfassende Weiterentwicklung der Standards entlang des Fahrplans des Gesetzes beginnt mit einer grundlegenden Analyse der Einsatzbereiche. Mit dem Ziel, energiewende-spezifische Anwendungsfälle aus weiteren Sektoren und Sparten zu integrieren, müssen Änderungs- und Ergänzungspotenziale für die Entwicklung der Standards identifiziert werden. Abbildung 20 zeigt die notwendigen weiteren sektorübergreifenden Digitalisierungsbereiche genauso wie die Arbeits-Cluster für die weitere Standardisierung auf.

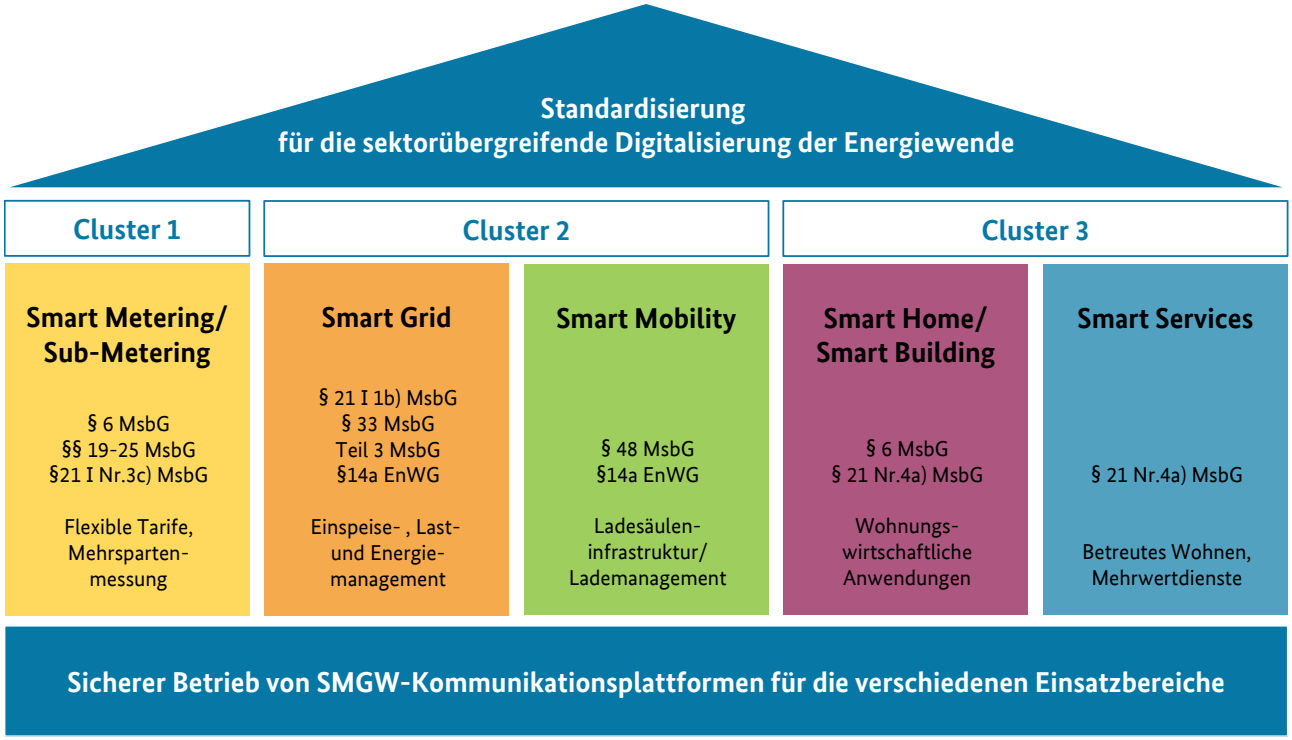

Abbildung 20 – Schwerpunkt-Cluster der Standardisierung für die sektorübergreifende Digitalisierung

Mit den nächsten Weiterentwicklungsstufen der Standards werden weitere Schritte in Richtung eines sicheren, steuerbaren Gesamtsystems unternommen. Nach §§ 26, 27 MsbG werden dem BSI die Aufgaben zugewiesen die Digitalisierungs-Standards für das SMGW zu überwachen, zu analysieren, zu planen und weiterzuentwickeln.

Die einzelnen Standardisierungsbereiche wird das BSI gesondert und im Zusammenhang betrachten. Mit dem Ziel, BSI-Standards für das GDEW-Schutzkonzept bereitzustellen, die selbst bei unterschiedlicher technischer Umsetzung durch Hersteller und Anwender nach erfolgreicher Prüfung eine einheitliche, sichere Integration von intelligenten Systemkomponenten in das Smart Grid mit Hilfe des SMGW ermöglichen.

Abbildung 21 illustriert dies und zeigt die Phasen auf, die künftig routinemäßig zur Einführung und Integration von Produkt- und Systemkomponenten für weitere Einsatzbereiche durchlaufen werden. Mit dem Beginn des Rollouts des SMGW nach Interimsmodell der Marktkommunikation und der SMGW nach Zielmodell der Marktkommunikation der SMGW-Kommunikationsplattform folgt die Produkt- und Systemarchitekturanalyse zur weiteren Planung und Ausgestaltung der BSI-Standards. Es schließen sich die Zertifizierungsprozesse

und der Marktanalyse-Prozess nach § 30 MsbG an. Nach Freigabe des Rollouts folgt der übliche Prozess zur Aufrechterhaltung des sicheren Betriebs.

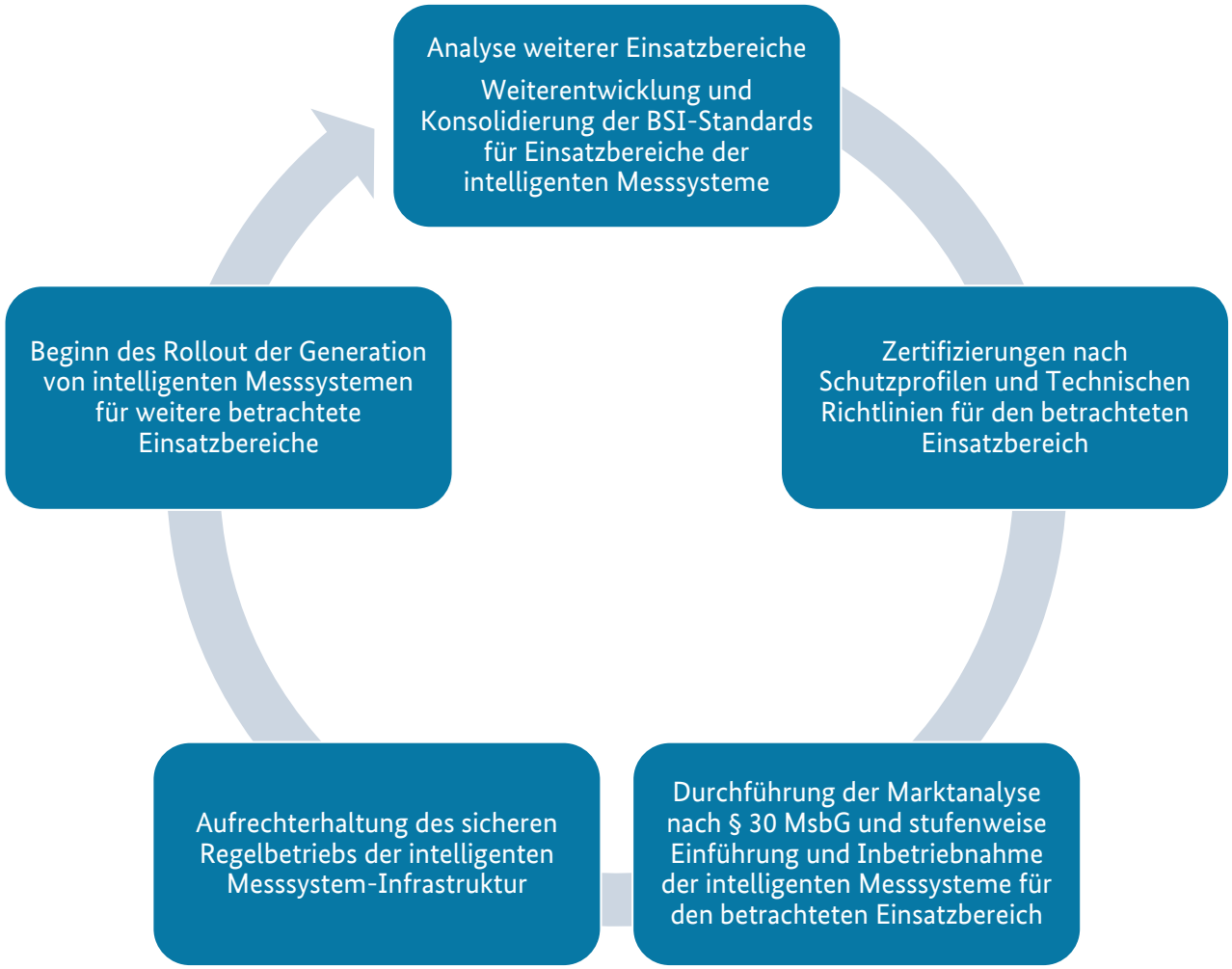

Abbildung 21 – Phasen zur Einführung von intelligenten Messsystemen für weitere Einsatzbereiche

Insgesamt wird das BSI eine modulare Weiterentwicklung seiner Vorgaben umsetzen. Ausgangspunkt jeder Entwicklung wird die energiewende-spezifischen Anwendungsfallbetrachtung aus den Digitalisierungsbereichen Smart Metering, Sub Metering, Smart Grid, Smart Mobility, Smart Home, Smart Building und Smart Services sein. Die Arbeit wird das BSI in drei Schwerpunkt-Clustern organisieren, die jeweils zwei bis drei Digitalisierungsbereiche umfassen. Das schließt nicht aus, dass zu den genannten Einsatzbereichen weitere Einsatzbereiche später noch ergänzt werden können.

In den folgenden Kapiteln werden die BSI-Projekte zur Produkt- und Systemarchitektur Analyse, zur modularen Weiterentwicklung der Standards für vertrauenswürdige Produkt-und Systemkomponenten sowie die bereits gestarteten BSI-Projekte näher erläutert.

5.2 Produkt- und Systemarchitektur Analyse für die fortschreitende Digitalisierung

Mit Veröffentlichung der vorliegenden Roadmap wird das BSI ein gesondertes Folgeprojekt zur Produkt- und Systemarchitektur Analyse aufnehmen. Das BSI-Projekt „Produkt- und Systemarchitekturanalyse für die fortschreitende Digitalisierung des intelligenten Netzes der Energiewende“ verfolgt das Ziel Leitplanken für die Weiterentwicklung der Standards der SMGW-Kommunikationsplattform mit spezifischen Funktionalitäten festzulegen. Dies erfolgt in den erwähnten Schwerpunkt-Clustern:

1. Smart- & Sub-Metering;
2. Smart-Grid & Smart-Mobility;
3. Smart Home & Building & Smart Services.

Abbildung 22 zeigt die Prozessschritte der Systemarchitektur-Analyse für diese Digitalisierungsbereiche:

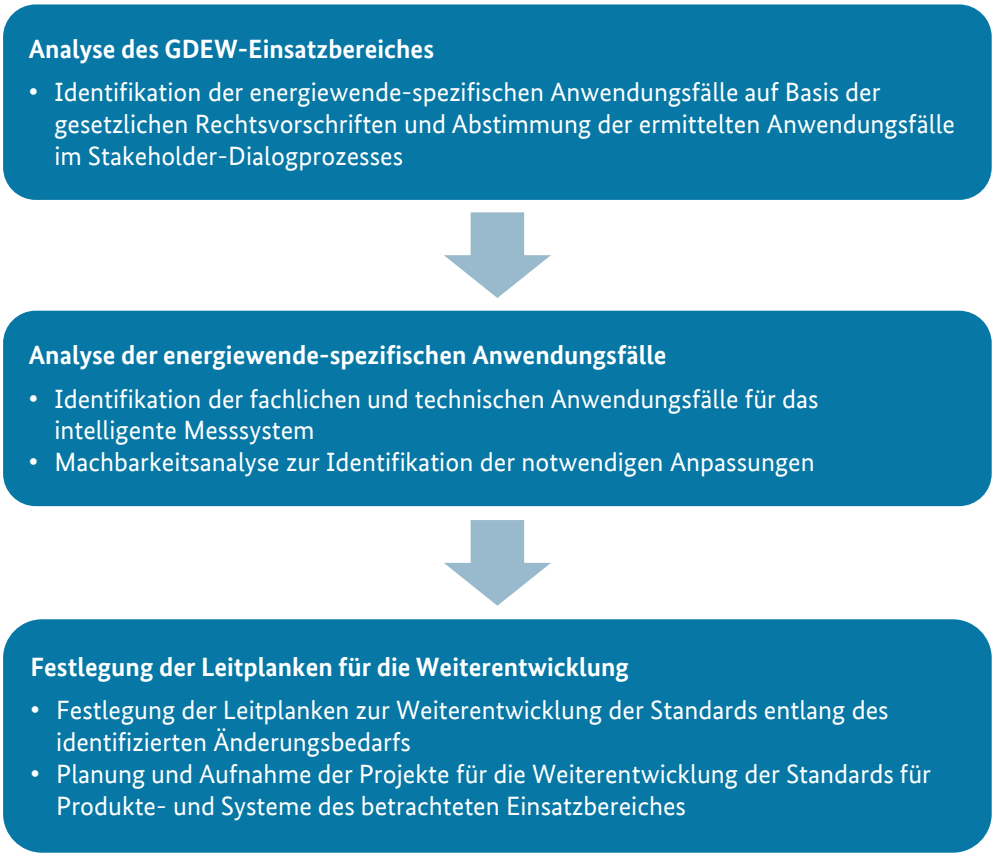

Abbildung 22 - Produkt- und Systemarchitektur Analyse zur Herleitung der Leitplanken

In allen Schwerpunkt-Clustern werden die gleichen Prozessschritte durchlaufen:

- Evaluierung des Einsatzbereichs,
- Durchführung einer Machbarkeitsanalyse,
- Festlegung der Leitplanken,
- Projektplanung für die Weiterentwicklung der Standards.

Im Zuge der Evaluierung des Einsatzbereichs werden fachliche und technische Anwendungsfälle für das intelligente Messsystem ermittelt. Die nächste Abbildung zeigt die Herleitung im Detail auf:

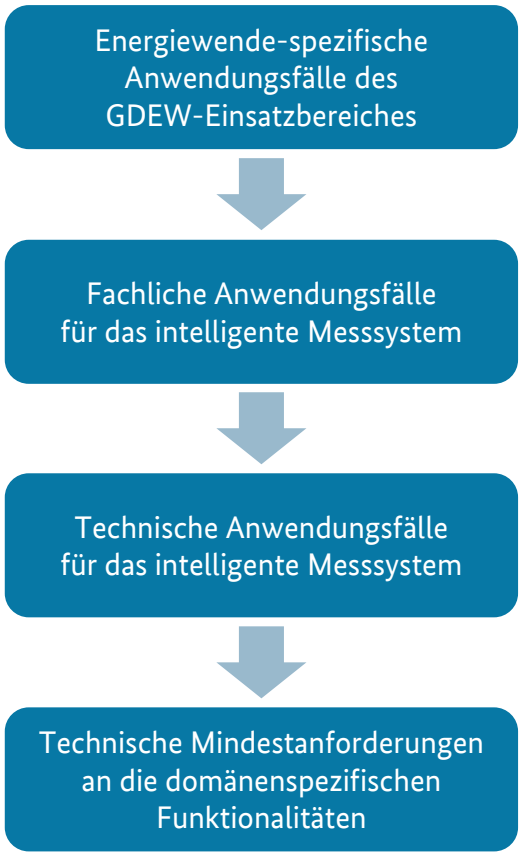

Abbildung 23 – Der Weg vom GDEW-Einsatzbereichs zur Identifikation der spezifischen Funktionalitäten

Anhand der Ergebnisse der Anwendungsfall-Analyse kann die Machbarkeitsanalyse durchgeführt und Anpassungsbedarf an den sicherheitstechnischen und funktionalen Anforderungen bestimmt werden. Für das Gesamtverständnis zeigt Abbildung 24 eine vereinfachte Darstellung der SMGW-Kommunikationsplattform und den domänenspezifischen Funktionalitäten.

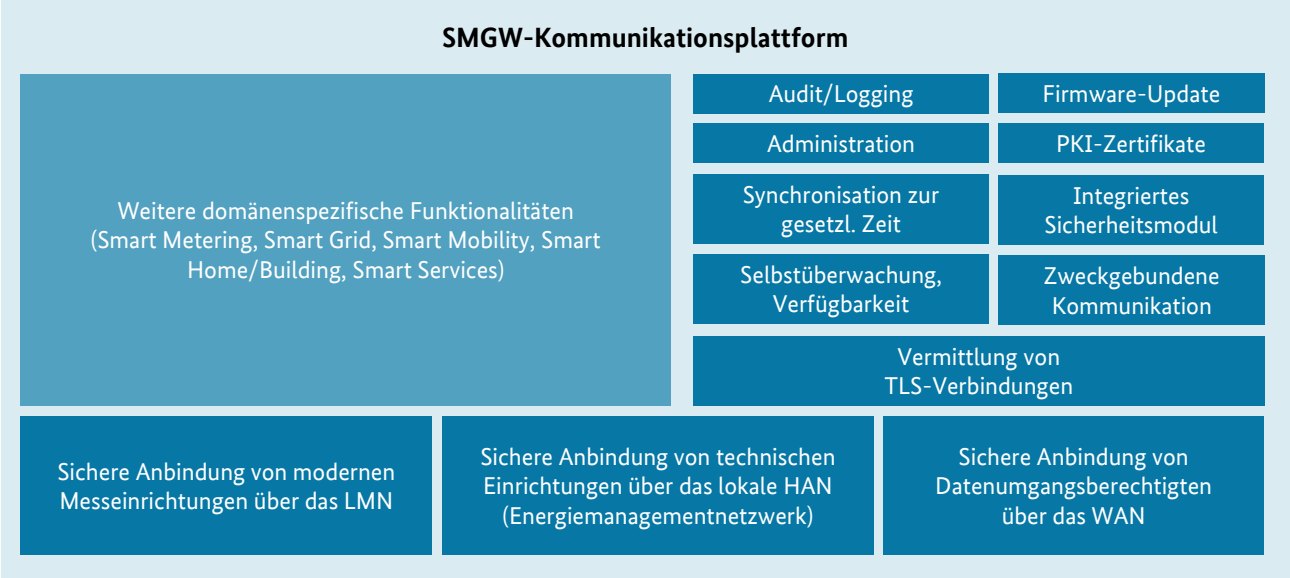

Abbildung 24 – Domänenspezifische Weiterentwicklung der SMGW-Kommunikationsplattform

Zur Feststellung der domänenspezifischen Funktionalitäten wird das BSI im Projekt zur Produkt- und Systemarchitekturanalyse in den verschiedenen Einsatzbereichen Anwendungsfälle mit den beteiligten Stakeholdern ermitteln und im Anschluss Leitplanken für die Weiterentwicklung der technischen Vorgaben in Form von PP und TR bereitstellen.

Neben den bereits identifizierten und hier dargestellten Einsatzbereichen kann es weitere GDEW-Einsatzbereiche geben, die nach und nach ergänzt werden können. Für die inhaltliche Ausgestaltung wird das BSI-Projekt zur Produkt- und Systemarchitekturanalyse mit seinen Phasen 1 bis 4 entsprechende Fachexperten-Arbeitsgruppen etablieren. Die resultierenden GDEW-Profile (Anwendungsfälle) werden dem Standardisierungsausschuss zur Verfügung gestellt und auf Basis dieser GDEW-Profile werden die entsprechenden Standardisierungs-Projekte durchgeführt. Zusätzlich wird das Projekt „Produkt- und Systemarchitekturanalyse“ wichtigen Input für die Marktanalyse zur Feststellung der technischen Möglichkeit nach § 30 MsbG liefern. Die folgenden Unterkapitel gehen näher auf die inhaltlichen Schwerpunkt-Cluster der Produkt- und Systemarchitektur-Analyse ein. Begonnen wird mit Cluster 1 „Smart- & Sub-Metering“ im Kapitel 5.2.1. Es folgen für das Cluster 2 „Smart Grid und Smart Mobility“ die Kapitel 5.2.2 und 5.2.3 und für Cluster 3 „Smart Home & Smart Building & Smart Services“ die Kapitel 5.2.4 und 5.2.5.

5.2.1 SMGW-Kommunikationsplattform für den Einsatzbereich Smart- und Sub-Metering

Das erste Schwerpunkt-Cluster der Systemarchitektur-Analyse bilden Smart- und Sub-Metering Anwendungsfälle für die SMGW-Kommunikationsplattform. § 6 MsbG fördert zum Zwecke der Energieeffizienzsteigerung die Bündelung von Messstellenbetrieben aus anderen Sparten, wie Fern- und Heizwärme, Gas und Wasser mit Strom. Zusätzlich muss beachtet werden, dass nach § 40 Abs. 2 MsbG ab dem 1. Januar 2025 neue Messeinrichtungen im RLM-Bereich Gas über die SMGW-Kommunikationsinfrastruktur in das intelligente Netz sicher eingebunden werden.

Für das SMGW heißt dies: Heizwärme- und weitere Sub-Metering Messeinrichtungen müssen genauso sicher angebunden werden können wie Strom-, Gas- und Wasser-Zähler. Auch variable Tarife müssen realisiert werden können. Jeder Anwendungsfall wird im Zuge der Evaluation des Einsatzbereiches bewertet, um den entsprechenden Änderungsumfang für den Standard festzulegen. Anhand dieser Leitplanken folgen BSI-Projekte zur Entwicklung der Standards für Produkte- und Systeme.

Die Ergebnisse der Produkt- und Systemanalyse adressieren den entsprechenden Änderungsumfang für den konkreten bestehenden Standard oder weisen Potenziale für neue Standardisierungsprojekte auf. Je nachdem ob hierzu die Produkt- und Systemarchitekturanalyse entsprechende Aussagen enthält, sind weitere Standardisierungsprojekte geplant.

5.2.2 SMGW-Kommunikationsplattform für den Einsatzbereich Smart Grid

Das zweite Schwerpunkt-Cluster der Systemarchitektur-Analyse bilden Smart-Grid und Smart-Mobility Anwendungsfälle für die SMGW-Kommunikationsplattform. Er ist für die SMGW-Kommunikationsplattform ein wichtiger Treiber der Digitalisierung der Energiewende. Mit der zunehmenden Bedeutung der erneuerbaren Energien für die Energieversorgung und der steigenden Anzahl steuerbarer Anlagen wächst die Notwendigkeit eines Energiemonitorings und -managements zur Sicherung der Netzstabilität. Ein sicheres digitales Energiemanagement, das perspektivisch die Möglichkeit zur vollautomatisierten Aussteuerung der dezentralen Energieerzeugung bietet, ist ohne eine vorangegangene sorgfältige Anwendungsfall-Analyse

des Einsatzbereiches Smart Grid undenkbar. Schließlich müssen alle energiewirtschaftlich notwendigen Handlungen stufenweise in Anwendungsfällen beschrieben und technisch „übersetzt“ werden. Das digitale Energiesystem muss in die Lage versetzt werden, in bestimmten (insbesondere zeitkritischen) Situationen vorab festgelegte Fahrpläne umzusetzen. Ein Einspeise- und Lastmanagements von Erzeugern und Verbrauchern ist deshalb genauestens auszugestalten, denn gemäß § 23 MsbG soll eine SMGW-Kommunikationsplattform dies einhalten.

Im Zuge der Herleitung der Smart Grid Anwendungsfälle für das Einspeise- und Lastmanagement müssen netzdienliche Steuerungs- und Energiemanagement-Anwendungsfälle beschrieben sowie die Performance-Anforderungen an die IKT berücksichtigt werden. Anhand der Evaluation der Anwendungsfälle werden Anforderungen zur Ausgestaltung des Steuerungs-Moduls identifiziert, das die notwendige Steuerung und Management der Anlagen sicher durchsetzen wird. Die logische oder physikalische Anbindung des Steuerungs-Moduls durch die SMGW-Kommunikationsplattform gewährleistet die sichere Integration in das Smart Grid. Sie setzt voraus, dass das Steuerungs-Modul in einem BSI-Standard beschrieben wird (siehe Zeitplan in Kapitel 6).

Zur Umsetzung eines sicheren Steuerungsmanagements im Stile der „Netzampel“ durch die SMGW-Kommunikationsplattform werden weitere BSI-Vorgaben zu erarbeiten sein. So müssen die involvierten Systemkomponenten in der Lage sein in der gelben und roten Ampelphase zu unterscheiden, wer die direkte Berechtigung besitzt, um zur Abwendung von Störungen entsprechende Steuerung der dezentralen Anlage durchzusetzen. Auf Basis der Evaluation der Anwendungsfälle werden BSI-Vorgaben für die SMGW-Kommunikationsplattform weiter ausgestaltet.

5.2.3 SMGW-Kommunikationsplattform für den Einsatzbereich Smart Mobility

Das Messstellenbetriebsgesetz zeigt bereits über § 48 die Ausgestaltung von verbindlichen Mindestanforderungen zur sicheren Integration der Ladesäuleninfrastruktur von Elektromobilen in das intelligente Netz auf. SMGW-Kommunikationsplattformen sollen ab 2021 hier auch die Standardlösung sein. Mit der steigenden Anzahl von dezentraler Energieerzeugern und dem Anteil von flexiblen Energieeinspeisungen in das intelligente Energienetz steigt die Notwendigkeit einer besseren Planbarkeit von Erzeugung und Verbrauch.

Elektromobile eigenen sich in hervorragender Weise als örtlich und zeitlich flexibler Abnehmer von Strom aus erneuerbaren Energien mit hoher Pufferkapazität. Plötzlich auftretende Netzschwankungen können ausgleichen, wenn leistungsfähige und vertrauenswürdige Kommunikations- und Energiemanagementsystem vorhanden sind.

Das Ziel einer optimalen Systemintegration von netzdienlichen Speichern und Lasten in das Smart Grid bedarf zunächst einer ausführlichen Analyse der netzdienlichen und netzkritischen Steuerungs-und Lade-Anwendungsfälle. Notwendig ist spätestens hier die gemeinsame Betrachtung dieses Einsatzbereichs mit den Smart-Grid Anwendungsfällen. Die gemeinsame Berücksichtigung in einem Arbeits-Cluster beim BSI trägt dem Rechnung.

Bereits jetzt zeichnen sich einige Grundparameter für ein Smart-Mobility-Modul des SMGW ab: Damit die SMGW-Kommunikation auch eichrechtliche Anforderungen per Design genügt, werden die entsprechenden Sicherheitsziele für das eichrechtlich korrekte Abrechnen von Ladevorgängen in den BSI-Vorgaben berücksichtigt. Auf Basis von nachweislich durchgesetzten Anforderungen zur Datensouveränität und Datenschutz für die SMGW-Kommunikationsplattform werden zukünftige Produkte und neue digitale Dienstleistungen auf Energie- und Netzzustandsdaten der Ladesäulen- und Elektromobilitätsinfrastruktur Zugriff erhalten können. Zusätzlich werden durch die BSI-Vorgaben die vereinheitlichten Rahmenbedingungen geschaffen, um das gesteuerte Laden von Elektromobilen zu ermöglichen. Darunter werden Anwendungsfälle zum Laden nach Tarifvorgaben als auch ein lokales Lademanagement in Verbindung mit angebundenen PV-Anlagen betrachtet.

Zur Vervollständigung der ersten Anwendungsfall-Evaluation wird das BSI-Projekt „Produkt- und Systemarchitekturanalyse“ vom BMWi-Förderprojekt DELTA unterstützt. Dabei werden die Anwendungsfälle zum sicheren Laden und Abrechnen der Ladevorgänge ermittelt und daraufhin eine Referenzarchitektur für die Ladesäulen-Systemarchitektur definiert.

5.2.4 SMGW-Kommunikationsplattform für den Einsatzbereich Smart Home und Smart Building

Das dritte Schwerpunkt-Cluster der Produkt- und Systemarchitekturanalyse bilden Anwendungsfälle für die SMGW-Kommunikationsplattform in den Bereichen Smart Home, Smart Building und Smart Services. Die SMGW-Kommunikationsplattform für

Anwendungsfälle im Einsatzbereich Smart Home und Smart Building zu betrachten ist eine logische Erweiterung zur Steigerung der Energieeffizienz. Fortschritte bei der Gebäudeenergieeffizienz können durch neue vernetzte digitale Systemlösungen der Gebäudeautomatisierung erzielt werden. Denn über die SMGW-Kommunikationsplattform kann Eigentümern, Nutzern und Dienstleistern die Durchführung eines besseren Gebäude- und Wohnraum Energiemanagements ermöglicht werden. Gekoppelt mit den Energiedaten der Smart Metering-Infrastruktur im Heimbereich können weitere Mehrwertdienste eingebunden werden. Gesetzlicher Anker ist § 6 MsbG, der auf die Bündelung von Messstellenbetrieben der Sparten Strom, Fern- und Heizwärme, Gas und Wasser abzielt. § 21 MsbG fordert die Offenheit von SMGWs für sog. Mehrwertdienste. Mehrwertdienste können z. B. auf ein besseres Monitoring der intelligenten Systemkomponenten im Gebäude- und Wohnbereich abzielen. Mit SMGW-Kommunikationsplattformen können nach entsprechenden modularen Weiterentwicklungen auch Heiz- oder Wärmerückgewinnungssysteme und weitere Energieeinsparsysteme sicher vernetzt werden. Um das Potenzial der SMGW-Kommunikationsplattform auszunutzen und im Interesse eines sicheren, komfortablen Zugangs für Eigentürmer, Nutzer und berechtigte Dienstleister sorgt das BSI dafür, dass die SMGW-Kommunikationsplattform für den Einsatzbereich Smart Home und Smart Building standardisierte Schnittstellen bereitstellt.

Für smarte Gebäude- und Wohnbereiche mit lokalen Ladepunkten für Elektromobile (u. a. auch sog. „wall-box“) wird das BSI-SMGW auch gerüstet sein. Hier wird es Lösungen geben, die ein Energiemanagement, lokales Last-, Lade- und Erzeugungsmanagement betrachten und austarieren. Die Weiterentwicklung der SMGW-Kommunikationsplattform wird die Anforderungen an das lokale Energiemanagementsystem der Zukunft erfüllen.

5.2.5 SMGW-Kommunikationsplattform für den Einsatzbereich Smart Services

Während die Analyse des Einsatzbereiches Smart Home und Smart Building den Fokus auf lokale effiziente Energienutzung und Energiemanagement legt, werden auf Basis des Einsatzbereiches Smart Services weitere digitale Mehrwertdienste nach § 21 MsbG für das Smart Grid angereizt, um so den Nutzen und die Akzeptanz beim Letztverbraucher zu erhöhen. Zu den Mehrwertdiensten zählen beispielsweise Anwendungsfälle des „betreuten Wohnen“ (Ambient Assisted Living) als auch Anwendungsfälle zur „Wohnungs- und Gebäudesicherheit“, die nach

§ 32 MsbG zur modernen Gebäudeinfrastruktur des Rollout-Ansatzes zugeordnet werden. Notwendig ist spätestens hier die gemeinsame Betrachtung dieses Einsatzbereichs mit den Smart Home und Smart Building-Anwendungsfällen. Die gemeinsame Berücksichtigung in einem Arbeits-Cluster beim BSI trägt dem Rechnung.

Dieser Teil der Produkt- und Systemarchitekturanalyse wird somit Anwendungsfälle betrachten, die die Adaptierbarkeit von Spezialanwendungen für die SMGW-Kommunikationsplattform analysieren. Hierzu gehören neben den erwähnten Mehrwertdiensten für den Wohn- und Gebäudebereich auch die Spezialanwendungen in der Rolloutgruppe >100.000 kWh und folglich auch die Analyse der Anwendungsfälle in der Mittel und Hochspannungsebene. Gemäß § 40 MsbG wird zudem der Spezialfall geregelt, dass ab dem 1. Januar 2025 eine registrierende Leistungsmessung für Gas bei Gewerbekunden über die SMGW-Kommunikationsinfrastruktur durchgeführt werden muss. Durch die Analyse des Einsatzbereiches werden somit spezielle Energiesystembereiche betrachtet, die durch die BSI-Vorgaben für diese Spezialanwendungen einen weiteren Anteil zur digitalen Transformation beitragen.

5.3 Schnittstellen für Fragen zur Weiterentwicklung der SMGW-Kommunikationsplattform

Im Interesse einer hohen Akzeptanz der BSI-Standardisierungs-Projekte bei Herstellern und Anwendern wird das BSI die beteiligten Akteure auch bei der Umsetzung der erarbeiteten Standards unterstützen. Daher wird das BSI bei der Entwicklung von Schutzprofilen und Technischer Richtlinien weiterhin sämtliche betroffenen Verbände aus den Bereichen Telekommunikation, Informationstechnik, Energie, Wohnungswirtschaft und Verbraucherschutz sowie die Datenschutzbeauftragten des Bundes (BfDI) und der Länder, die Bundesnetzagentur und die Physikalisch-Technische Bundesanstalt einbinden. Neben den Task-Forces mit Fachexperten werden solche BMWi-Förderprojekte in die Erstellung der BSI-Vorgaben eingebunden, die den klaren Förderungsauftrag erhalten haben, wichtige Digitalisierungs-Vorhaben auf Basis der SMGW-Kommunikationsplattform durch ihre Forschung und Pilotprojekte zu unterstützen.

Interessierte Verbände, die sich vor dem Hintergrund neuer Anwendungsbereiche an der Weiterentwicklung der BSI-Standards mit technischen Fachexperten beteiligen möchten, können sich gerne an das BSI wenden.

Folgende Schnittstellen wird das BSI für Fragen zur Weiterentwicklung der SMGW-Kommunikationsplattform für die verschiedenen Einsatzbereiche bereitstellen:

Für Fragen zur Produkt- und Systemarchitekturanalyse und der GDEW-Roadmap gdew-roadmap@bsi.bund.de

Für Fragen zur SMGW-Kommunikationsplattform für den Einsatzbereich Smart Metering: smartmeter@bsi.bund.de

Für Fragen zur SMGW-Kommunikationsplattform für den Einsatzbereich Smart Grid: smartgrid@bsi.bund.de

Für Fragen zur SMGW-Kommunikationsplattform für den Einsatzbereich Smart Mobility: smartmobility@bsi.bund.de

Für Fragen zur SMGW-Kommunikationsplattform für den Einsatzbereich Smart Home und Smart Building:

smarthome@bsi.bund.de

Für Fragen zur SMGW-Kommunikationsplattform für den Einsatzbereich Smart-Services: smartservices@bsi.bund.de

5.4 Zusammenarbeit des BSI mit den nationalen Normungsorganisationen DIN/DKE

Intelligente Stromnetze müssen allerorten in Europa für Stabilität in der Energieversorgung sorgen. Für die effiziente Vernetzung von Mess-, Steuer-, Regel- und Kommunikations-Systemen benötigen europäische Smart Grid der Zukunft ein hohes Maß an IT-Sicherheit, um letztlich auch die europäische Energieversorgung sicherzustellen bzw. keine unkalkulierbaren Risiken über Vernetzungen in die Energieversorgung hineinwirken zu lassen.

Das GDEW verankert verbindliche Standards zur Durchsetzung von Datenschutz, Datensicherheit und Interoperabilität für das intelligente Netz und bietet zugleich die Chance,

es als Sprungbrett für die konsequente Internationalisierung der Standards zu nutzen. Davon könnten die nationalen Standards genauso profitieren wie die internationalen, beides im Interesse einer Digitalisierung der gesamten kritischen Infrastruktur, die Cybersicherheit von Beginn an berücksichtigt. Nach dem GDEW entwickelt das BSI benötigte IT-Sicherheitsstandards für die Digitalisierung mit Interessengruppen der Wirtschaft. Wichtige Unterstützung erhält das BSI dabei durch die vertrauensvolle Zusammenarbeit mit Verbänden und DIN/DKE im Hinblick auf die Einbringung der Standards in die internationalen Normungsgremien.

Die nationale Normungsorganisation ist laut eines Vertrages mit der Bundesrepublik Deutschland das DIN (Deutsches Institut für Normung e. V.). DIN vertritt die Normungsinteressen Deutschlands als Mitglied im Europäischen Komitee für Normung (CEN) sowie als Mitglied in der Internationalen Organisation für Normung (ISO). Im Bereich der IT-Sicherheit leitet DIN die Arbeiten im internationalen Gremium ISO/IEC JTC SC 27 „IT-Sicherheitsverfahren“.

Die DKE (Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE) ist zuständig für die Normungsarbeiten, die in den entsprechenden internationalen und regionalen Organisationen (vor allem IEC, CENELEC und ETSI) behandelt werden. Sie vertritt somit die deutschen Interessen sowohl im Europäischen Komitee für elektrotechnische Normung (CENELEC) als auch in der Internationalen Elektrotechnischen Kommission (IEC).

Deshalb legt das BSI großen Wert darauf, dass Arbeitsgremien sowohl von Verbänden als auch vom DKE (Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE) eng bei der Ausgestaltung der BSI-Vorgaben eingebunden sind. In Deutschland übernimmt das DKE Systemkomitee „Smart Energy“ (DKE/K901) die Spiegelung des IEC Gremiums, welches sich mit der Sektorkopplung im Bereich Smart Grid, Advanced Metering, Smart Home sowie mit den Schnittstellen zur Elektromobilität befasst.

Da das Systemkomitee DKE/K901 selbst keine eigenen Normen erarbeitet, sondern für Kohärenz und Koordinierung der beteiligten Normungsbereiche sorgt, ist die Abstimmung im nationalen, europäischen und internationalen Umfeld zur Wahrung der Interessen der deutschen Wirtschaft von höchster Relevanz. Daher beteiligt sich neben verschiedenen Mitgliedsunternehmen von Bundesverbänden und Partnerbehörden auch das BSI selbst an den

Aktivitäten, um Einsicht in internationale und europäische Normungsaktivitäten zu erhalten und bei deren Kommentierung zielgerichtet mitwirken zu können.

Die im Digitalisierungsprozess eingebundenen Arbeitskreise des DKE sind fester Bestandteil der digitalen Transformationsstrategie des Bundes. Sie liefern dem BSI bei der agilen Standardisierung von IT-Sicherheits- und Interoperabilitätsvorgaben wichtigen Input und dienen zugleich als wechselseitige Austauschplattformen im Hinblick auf die europäische und internationale Standardisierung. Die DKE stellt mit ihren Spiegelgremien eine für die Wahrung der deutschen IT-Sicherheitsinteressen entscheidende Schnittstelle zur Kommentierung der Standardisierungsaktivitäten von IEC, CENELEC und Gremien der EU-Kommission dar.

Das BSI und die deutschen Normungsorganisationen DIN/DKE werden ihre Möglichkeiten nutzen, um auch Akzente auf internationaler Ebene im Sinne des GDEW und seiner Standards zu setzen. Schließlich lassen sich hieraus in hervorragender Weise generelle, europaweite Anforderungen für die Digitalisierung ableiten. Deutschland würde dann mit dem GDEW und den Standards des BSI ein erstes positives Umsetzungsbeispiel der neuen, allgemeinen europäischen Anforderungen abgeben können. Andere EU-Staaten wären frei, darauf aufzusetzen.

6 Zeitpläne für die sektorübergreifende Standardisierung nach dem GDEW

Leitsätze

- Das Standardisierungsprogramm dieser Roadmap spannt einen weiten Bogen: Von den Anwendungsfällen des Smart Metering über Smart Grid und Smart Mobility bis zu Smart Home und sog. Smart Services, die beide über reine Energie-Anwendungen hinausgehen.
- Das breite Programm hat seinen Grund: Dort, wo die Nutzung der BSI-Standards verpflichtend ist, eröffnen die weiteren Anwendungsfelder interessante Geschäftsfelder mit hohem Kundenutzen. Gleichzeitig kommt die sichere Infrastruktur jedem weiteren Geschäftsmodell selbst dann schon zugute, wenn der Rechtsrahmen noch gar keine Verpflichtungen zur Nutzung der BSI-Standards enthält.
- Schließlich ist die Sektorkopplung erklärtes Energiewendeziel. Technische Standards für Infrastrukturen müssen dies berücksichtigen und weitere Bereiche mit dem intelligenten Stromnetz verknüpfen.

Zur Weiterentwicklung der Standards für die SMGW-Kommunikationsplattform in den verschiedenen GDEW-Einsatzbereichen fasst dieses Kapitel die Projekt- und Zeitpläne der GDEW-Projekte zusammen.

Nach erfolgreicher Planungsphase mit Hilfe der Produkt- und Systemarchitekturanalysen folgt die Entwicklungsphase der Standards durch Umsetzung der verschiedenen Projekte zur Erstellung von Schutzprofilen und Technischen Richtlinien. Es folgt die Umsetzungs- und Zertifizierungsphase für die Produkt- bzw. Systemkomponenten durch Hersteller, Anwender, Prüf- und Zertifizierungsstelle. Nach erfolgreicher Feststellung der technischen Möglichkeit i. S. v. § 30 MsbG wird der Rollout der entsprechenden SMGW-Kommunikationsplattform in dem betrachteten Einsatzbereich gestartet. Abbildung 25 auf der folgenden Seite zeigt diese Abläufe im Gesamtkontext.

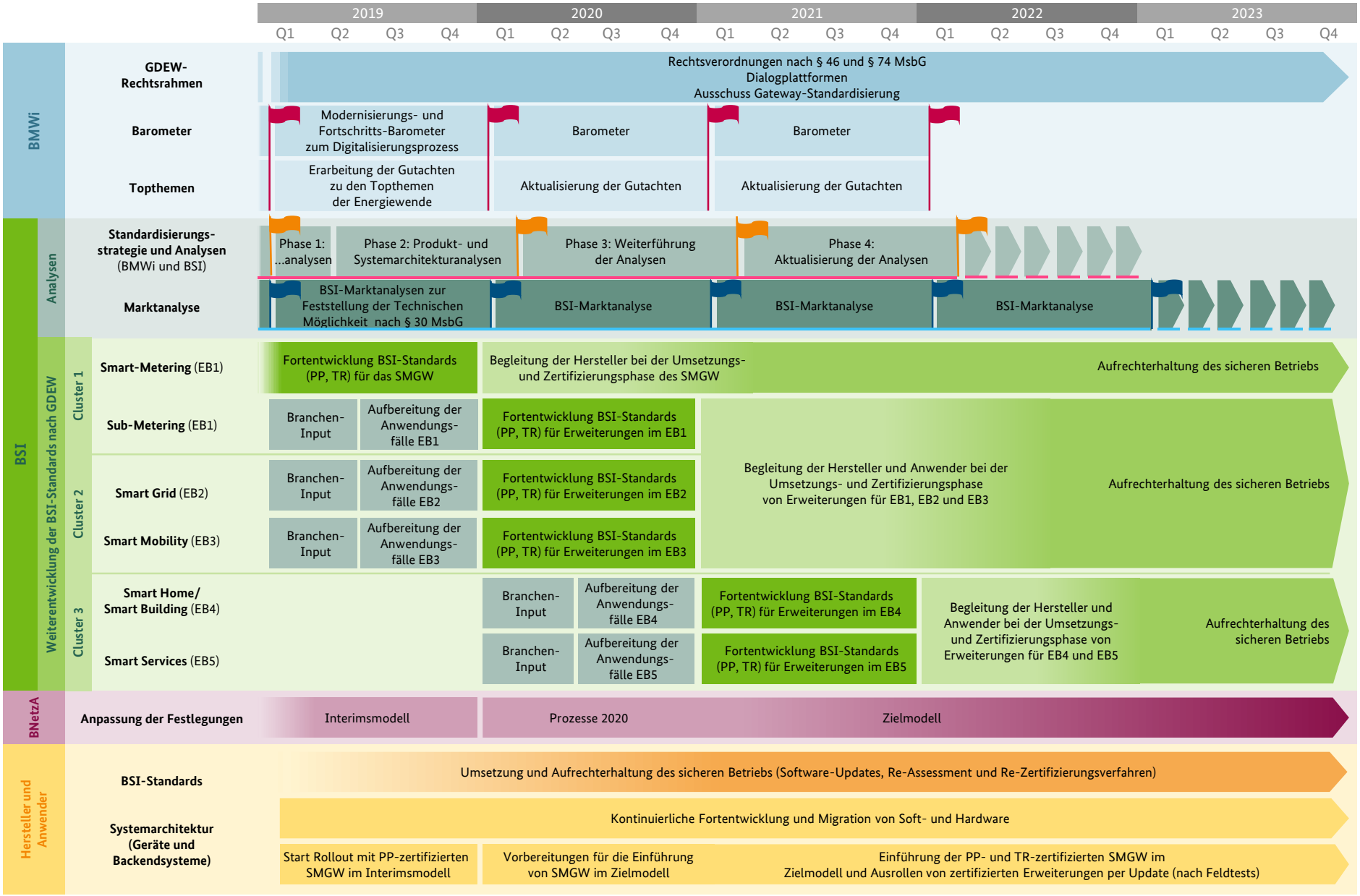

Abbildung 25 – Gesamt-Zeitplan der BMWi- und BSI-Projekte

Der Abschnitt „Weiterentwicklung der BSI-Sicherheitsstandards nach GDEW“ illustriert wie die eigentliche Erstellung bzw. Fortentwicklung von Schutzprofilen und Technischen Richtlinien (dunkelgrün gefärbte Balken) in den jeweiligen Einsatzbereichen (EB) vor- bzw. nachbereitet wird. Die (Fort-)Entwicklung der Standards beginnt mit den Projektschritten der Analyse- und Planungsphase zur Ermittlung der Anwendungsfälle. In diesem Rahmen wird auch der Branchen-Input zu Anwendungsfällen erhoben und berücksichtigt. Anschließend folgt eine Aufbereitung und Festlegung auf konkrete Anwendungsfälle. Anhand dieser Analysen wird sich der Änderungs- und Fortentwicklungsbedarf an bestehenden Standards bzw. die (Fort)-Entwicklung von neuen Standards für die Weiterentwicklung der SMGW-Kommunikationsplattform sowie die weitere Ausgestaltung der Zeitpläne für die jeweiligen Einsatzbereiche (EB 1-5) ergeben.

Die Anpassung der Marktkommunikation an die Erfordernisse des MsbG und die intelligenten Messsysteme erfolgt durch die Bundesnetzagentur (BNetzA) in mehreren Stufen (lila gefärbte Balken). Zunächst wurde das so genannte Interimsmodell zum 01. Oktober 2017 eingeführt, das die Integration der intelligenten Messsysteme mit seinen Grundfunktionalitäten ermöglicht. Mit der Marktkommunikation 2020 wird voraussichtlich ab dem 01. Dezember 2019 die Verantwortung für die Aufbereitung und Verteilung der erhobenen Messwerte entsprechend § 60 Abs. 1 MsbG vom Netzbetreiber auf den Messstellenbetreiber übertragen. Das Zielmodell, das alle Anforderungen des Messstellenbetriebsgesetzes inklusive der sternförmigen Verteilung aufbereiteter Messwerte direkt aus dem SMGW erfüllt, soll die Marktkommunikation 2020 zeitgleich mit der Verfügbarkeit der SMGW nach Zielmodell ablösen.

Der Abschnitt „Hersteller und Anwender“ stellt die Umsetzung und Aufrechterhaltung des sicheren Betriebs sowie die kontinuierliche Fortentwicklung und Migration von Soft- und Hardware für die SMGW-Systemarchitektur dar (gelb und orange gefärbte Balken). Hierbei wird dargestellt wie der Funktionsumfang der verbauten Geräte im Laufe der kommenden Jahre durch kontinuierliche Verbesserungen der Soft- und Hardware durch Hersteller etabliert und fortwährend über den SMGW-Geräte-Lifecycle angewendet werden kann. Für das Cluster 1 (Smart-/Sub-Metering und Mehrspartenmessung) existiert bereits ein Zeitplan zur (Weiter-)Entwicklung der einzelnen Standards und weiterer relevanter Veröffentlichungen. Dieser ist in Abbildung 26 auf der folgenden Seite dargestellt.

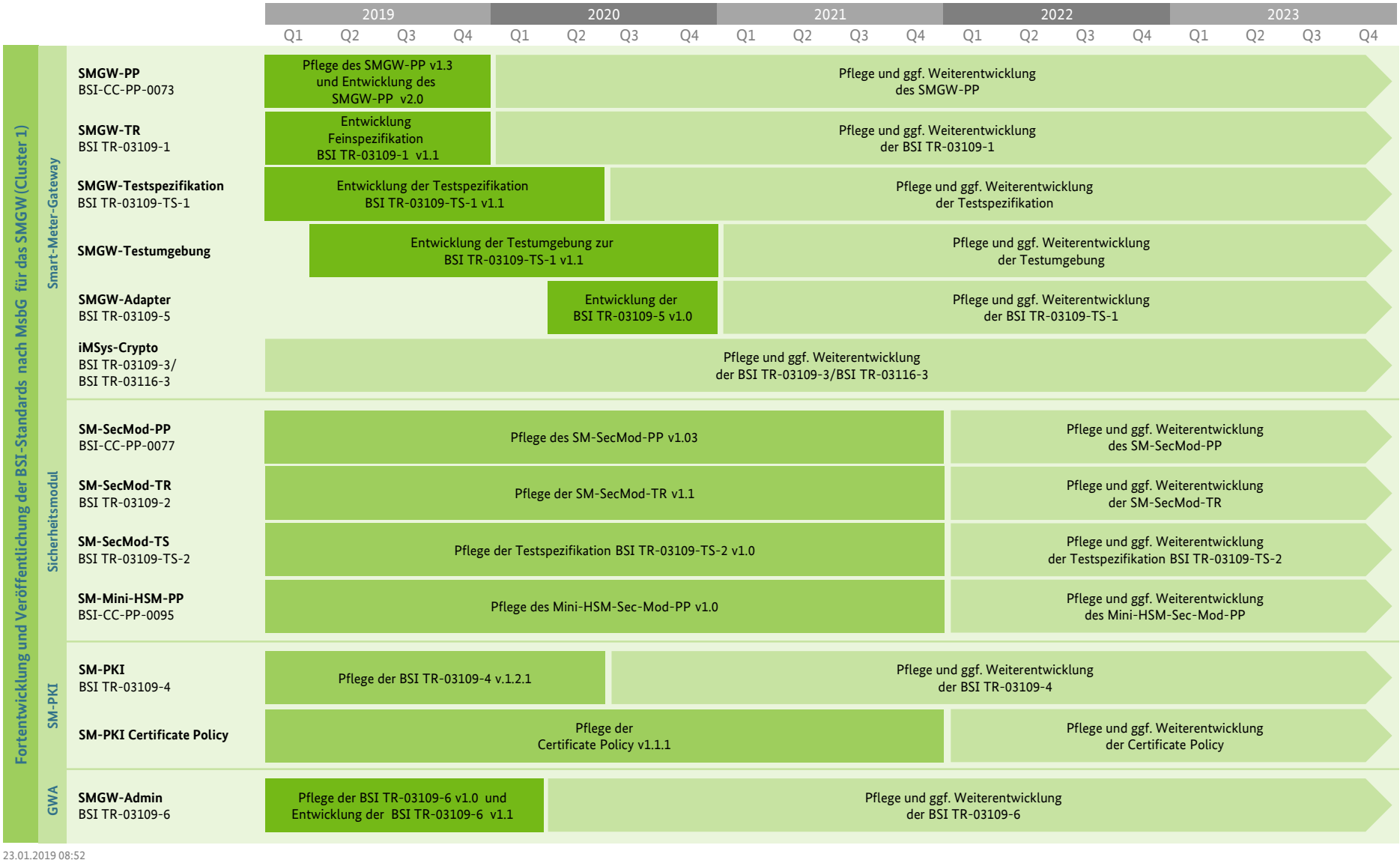

Abbildung 26 – Übersicht der Standardisierungsprojekte des BSI für den Einsatzbereich-Cluster 1

Anhang: Gesetzliche Mindestanforderungen zum Funktionsumfang nach MsbG

Die folgende Tabelle gibt einen Überblick über die gesetzlichen Mindestanforderungen an den Funktionsumfang von intelligenten Messsystemen nach dem MsbG.

Gesetzliche Anforderungen an den Funktionsumfang	***Vorschrift im MsbG***
Datenerhebung	
Zählerstandsgangmessung (allgemein): = Erhebung von Viertelstundenwerten (Strom) und Stundenwerten (Gas)	§ 3 Nr. 27 § 21 Abs. 1 Nr. 1b) VO-Ermächtigung in § 46 Nr. 9
Zählerstandsgangmessung (Verbraucher)	§ 21 Absatz 1 Nr. 1b) § 55 Absatz 1 Satz 2
Zählerstandsgangmessung (Erzeuger)	§ 21 Absatz 1 Nr. 1b) § 55 Absatz 3
Zählerstandsgangmessung (§ 14a-Anlagen)	§ 21 Absatz 1 Nr. 1b) § 23 Absatz 1 Satz 3 VO-Ermächtigung in § 46 Nr. 10 Ausnahme Elektromobilität: § 48
Abrufung Ist-Einspeisung von Erzeugern	§ 21 Absatz 1 Nr. 1c)
Erhebung von Netzzustandsdaten = Spannungs- und Stromwerte und Phasenwinkel sowie daraus errechenbare oder herleitbare Werte, die zur Ermittlung des Netzzustandes verwendet werden können	Definition: § 3 Nr. 16 § 21 Absatz 1 Nr. 1d) § 56

Erhebung von Stammdaten = Informationen über Art und technische Ausstattung, Ort und Spannungsebene sowie Art der kommunikativen Anbindung von an das SMGW angeschlossenen Anlagen	Definition: § 3 Nr. 22 § 21 Absatz 1 Nr. 6 § 57
Anbindung, Empfangbarkeit von Daten (SMGW)	
Allgemein: Spartenübergreifende Messung = Empfangbarkeit von Messwerten der Sparten Strom, Gas, Wasser, Wärme, Heizwärme	§ 21 Absatz 1 Nr. 3c) § 6 Absatz 1 Satz 2
Speziell: Anbindbarkeit von Gaszählern Neue Messeinrichtungen für Gas dürfen nur verbaut werden, wenn sie sicher mit SMGW verbunden werden können. Es gilt Übergangsregelung.	§ 20 Absatz 1 § 23 Absatz 1 Nr. 4 § 40 Absatz 2
Anbindbarkeit von Erzeugungsanlagen und weiteren lokalen Systemen	§ 21 Absatz 1 Nr. 3d) § 23 Absatz 1 Nr. 2 § 40 Absatz 1
Allgemein: Spartenübergreifende Messung = Empfangbarkeit von Messwerten der Sparten Strom, Gas, Wasser, Wärme, Heizwärme	§ 21 Absatz 1 Nr. 3c) § 6 Absatz 1 Satz 2
Anbindbarkeit Moderner Messeinrichtungen = Messeinrichtung, die den tats. Elektrizitätsverbrauch und die tats. Nutzungszeit widerspiegelt	Definition: § 3 Nr. 15 § 23 Absatz 1 Satz 1 § 40 Absatz 1
Offenheit für Mehrwertdienste und Schalthandlungen Mehrwertdienst = energieversorgungsfremde Dienstleistung („Smart Home“)	Definition Mehrwertdienst: § 3 Nr. 9 § 21 Absatz 1 Nr. 4a)

Datenverarbeitung	
Zeitstempelung, Verarbeitung, Speicherung, Löschung	§ 22 Absatz 1 Nr. 1
Messwertverarbeitung zu Abrechnungszwecken	§ 21 Absatz 1 Satz 1
Tarifierung (intern wie extern) = Zuordnung der gemessenen elektrischen Energie oder Volumenmengen zu verschiedenen Tarifstufen	Definition: § 3 Nr. 23 § 21 Nr. 3b)
Plausibilisierung und Ersatzwertbildung Hat perspektivisch automatisiert im Gateway zu erfolgen. Ist als Teil der Messwertaufbereitung Aufgabe des MSB. Interimsmodell als Übergangslösung.	Definition in § 3 Nr. 17 § 3 Absatz 2 § 35 Absatz 1 Satz 1 § 60 Absatz 2
Zeitsynchronisation des SMGW mit Zeitquelle im WAN	§ 22 Absatz 1 Nr. 3
Datenübermittlung	
Verbrauchsvisualisierung für den Verbraucher Allgemein: Energieverbrauch, Tarifinformationen und abrechnungsrelevante Messwerte müssen für Verbraucher über lokale Anzeigeeinheit oder Online-Portal sichtbar gemacht werden.	§ 21 Absatz 1 Nr. 2 § 61
Anzeige historischer Verbräuche: Je nach Abrechnungszeitraum für drei Jahre Tages-, wochen-, monats-, und jahresbezogene Energieverbrauchswerte sowie Zählerstandsgänge für die letzten 24 Monate	§ 21 Absatz 1 Nr. 2c) § 21 Absatz 1 Nr. 2d) § 61 Absatz 1 Nr. 3 § 61 Absatz 1 Nr. 4

Verbrauchereinsicht in das Logbuch	§ 21 Absatz 1 Nr. 2e) § 53 Absatz 1
Informationen für Anlagenbetreiber über Einspeisungen Allgemein: Einspeisung, abrechnungsrelevante Messwerte müssen für Verbraucher über lokale Anzeigeeinheit oder Online-Portal sichtbar gemacht werden.	§ 62
Anzeige historischer Einspeisewerte Tages-, wochen-, monats-, und jahresbezogene Einspeisewerte für die letzten 24 Monate	§ 62 Absatz 1 Nr. 3
Informationen für Anlagenbetreiber über Schaltprofile	§ 62 Absatz 1 Nr. 4
Einsicht des Anlagenbetreibers in das Logbuch	§ 62 Absatz 1 Nr. 5
Übermittlung von Stammdaten	§ 21 Absatz 1 Nummer 6 § 63
Übermittlung von Netzzustandsdaten	§ 21 Absatz 1 Nr. 1d) § 64
Tägliche Übermittlung aller Zählerstandsgänge für den Vortag • an den VNB • an den ÜNB und BiKo • an den Lieferanten	§ 60 Absatz 1 § 60 Absatz 1 Nr. 2 § 60 Absatz 1 Nr. 3 § 60 Absatz 1 Nr. 4
Monatliche Übermittlung der bezogenen Monatsarbeit an den VNB	§ 60 Absatz 3 Nr. 1

Jährliche Übermittlung von Jahreswerten • an den VNB • an den ÜNB und BiKo • an den Lieferanten	§ 60 Absatz 1 *Alle Fälle, die nicht unter* § 60 Absatz 1 Nr. 1 § 60 Absatz 1 Nr. 3 § 60 Absatz 1 Nr. 4 *fallen*
Fernsteuerbarkeit, Schaltprofile	
Fernsteuerbarkeit Unterstützung der Fernsteuerbarkeit von • Anlagen nach § 14a • EE-Anlagen • KWKG-Anlagen.	§ 21 I Nr. 1b) 2. Halbsatz § 33 Nr. 3
Schaltprofile Unterstützung von Schaltprofilen (§ 14a EnWG und EE/KWK)	Definition: § 3 Nr. 18 § 35 Absatz 1 Nummer 5
Administration	
SMGW-Admin betreibt SMGW im Dienste von Letztverbrauchern, Netzbetreibern und Marktakteuren. Er installiert, konfiguriert und administriert das SMGW.	§ 25
Intelligente Messsysteme müssen **Administration zugänglich** sein	§ 21 Absatz 1 Nr. 3a)
Ausschließlicher Zugriff des SMGW-Admin	§ 21 Absatz 1 Nr. 4b)
SMGW **muss Softwareupdates** empfangen und verarbeiten können	§ 21 Absatz 1 Nr. 4c)
Sonstiges	
Eigenstromverbrauch ist gedeckelt Festlegung der BNetzA entscheidet über Höhe	§ 21 Absatz 1 Nr. 5

Stromentnahme hat im ungemessenen Bereich zu erfolgen Dies dient der Aufrechterhaltung der Betriebsfähigkeit des Messsystems unabhängig von der Verwendung von Systemen mit „Breaker-Funktion“	§ 25 Absatz 2
Spannungsausfälle müssen von intelligentem Messsystem protokolliert werden Mit Datum und Zeitangabe	§ 21 Absatz 1 Nr. 1d)

Tabelle 2 – Gesetzliche Mindestanforderungen an den Funktionsumfang von intelligenten Messsystemen