dena
Deutsche Energie-Agentur

SET Hub

Analyse

Intelligentes Messsystem

Grundpfeiler zur Digitalisierung des Energiesystems

Impressum

Herausgeber
Deutsche Energie-Agentur GmbH (dena)
Chausseestraße 128 a
10115 Berlin

Tel.: +49 30 66 777-0
Fax: +49 30 66 777-699

E-Mail: info@dena.de
Internet: www.dena.de

Redaktion:
Jasmin Wagner (dena)
Anika Lange (dena)
Moritz Schlösser (dena)
Anna Sibirtceva (dena)

Stand:
07/2024

Bitte zitieren als:

Deutsche Energie-Agentur (Hrsg.) (dena, 2024): „Intelligentes Messsystem – Grundpfeiler zur Digitalisierung des Energiesystems."

Bundesministerium für Wirtschaft und Klimaschutz

Die Veröffentlichung dieser Publikation erfolgt im Auftrag des Bundesministeriums für Wirtschaft und Klimaschutz. Die Deutsche Energie-Agentur GmbH (dena) unterstützt die Bundesregierung in verschiedenen Projekten zur Umsetzung der energie- und klimapolitischen Ziele im Rahmen der Energiewende.

Inhalt

Abkürzungen

Abkürzung	Beschreibung
aEMT	Aktiver externer Marktteilnehmer
APDU	Application Protocol Data Unit
BCMS	Business Continuity Management System
BMWK	Bundesministerium für Wirtschaft und Klimaschutz
BSI	Bundesamt für Sicherheit in der Informationstechnik
CC	Common Criteria
CLS	Controllable Local System
CON	Anschlussnutzer
CP	Certificate Policy
DAkkS	Deutsche Akkreditierungsstelle
DVGW	Deutscher Verein des Gas- und Wasserfaches
EEG	Erneuerbare-Energien-Gesetz
EMT	Externer Marktteilnehmer
EnWG	Energiewirtschaftsgesetz
ESA	Energieserviceanbieter
EUV	Energieversorgungsunternehmen
GDEW	Gesetz zur Digitalisierung der Energiewende
gMSB	Grundzuständiger Messstellenbetreiber
GNDEW	Gesetz zum Neustart der Digitalisierung der Energiewende
GWA	Gateway-Administrator
HAN	Home Area Network
HKE	HAN-Kommunikationsadaptereineit
HSM	Hardware Security Module
iMSys	Intelligentes Messsystem
ISMS	Information Security Management System
kW	Kilowatt
kWh	Kilowattstunde
LMN	Local Metrological Network
mME	Moderne Messeinrichtung
MSB	Messstellenbetreiber
MsbG	Messstellenbetriebsgesetz
OMS	Open Metering System
OSI	Open Systems Interconnection
pEMT	Passiver externer Marktteilnehmer
PKI	Public Key Infrastructure
PP	Protection Profiles
SE	Steuereinheit
SET Hub II	Start-up Energy Transition Hub II
SME	Submeter-Einheit

Abkürzung	Beschreibung
SMGW	Smart Meter Gateway
TAF	Tarifanwendungsfall
TR	Technische Richtlinie
ÜNB	Übertragungsnetzbetreiber
VNB	Verteilnetzbetreiber
WAN	Wide Area Network
wMSB	Wettbewerblicher Messstellenbetreiber

1 Einleitung

Für das erfolgreiche Voranschreiten der Energiewende, die geprägt ist von einer zunehmenden Dezentralisierung, ist die Stärkung der Digitalisierung des Energiesystems essenziell. Die Basis hierfür ist eine sichere und funktionierende Kommunikation von Daten und Steuerungsbefehlen, die auf einer standardisierten Infrastruktur aufbaut. Hierbei spielt das intelligente Messsystem (iMSys) eine zentrale Rolle, denn es ist dafür verantwortlich, Messdaten zu erfassen und sicher zu übermitteln. Somit sorgt es auf der einen Seite dafür, dass die Verbraucherinnen und Verbraucher Transparenz hinsichtlich ihres Nutzungsverhaltens bekommen und darauf aufbauende Mehrwerte nutzen können. Auf der anderen Seite sind iMSys darauf ausgelegt, die Steuerung von Verbrauchs- und Erzeugungsanlagen zu ermöglichen, und haben damit Einfluss auf das Last- und Erzeugungsmanagement im Netzbetrieb.

Doch was sind intelligente Messsysteme eigentlich genau? Wie sind sie aufgebaut, welchen Regulierungen sind sie unterworfen und welche Möglichkeiten eröffnen sie uns? Motiviert durch diese Fragen, schaut sich die Deutsche Energie-Agentur (dena) diese Fragestellungen etwas genauer an.

Ziel ist die Aufarbeitung des aktuellen Stands geltender regulatorischer Rahmenrichtlinien, des technischen Aufbaus sowie bereits existierender und zukünftig möglicher Marktanwendungen rund um intelligente Messsysteme. Dieses Papier gibt einen Überblick über verschiedene Themen, die auf Basis der Quellenverweise weiter vertieft werden können. Dabei ist zu beachten, dass sich Regularien in einem stetigen Novellierungsprozess befinden und die hier aufgeführten Inhalte dem Stand Januar 2024 entsprechen.

Zur Beantwortung der vorgestellten Fragestellungen wird zunächst in Kapitel 2 ein Überblick über wesentliche Regularien gegeben. Dies beinhaltet zeitlichen Vorgaben wie auch die preisliche Ausgestaltung des Rollouts der Messtechnik. Dem folgen Grundlagen zu intelligenten Messsystemen: die relevanten Akteure, die möglichen Einstellungen eines Smart Meter Gateway zur Übermittlung der Daten sowie die Vorstellung der drei Netzwerke, welche zur Kommunikation mit dem System notwendig sind. In Kapitel 3 wird vertieft, welche sicherheitstechnischen Anforderungen intelligente Messsysteme erfüllen müssen. Diese Ausführungen werden ergänzt durch einen Exkurs zum Mess- und Eichrecht. Das folgende Kapitel schließt das Papier ab mit einem Ausblick auf die Anwendungsmöglichkeiten, die intelligente Messsysteme bieten.

Der Bericht wurde im Rahmen des vom Bundesministerium für Wirtschaft und Klimaschutz (BMWK) geförderten Projekts Start-up Energy Transition Hub II (SET Hub II) erstellt. Der SET Hub stellt mit der SET Academy, dem SET Mentoring und dem SET Network ein Informations-, Beratungs- und Vernetzungsangebot für Start-ups im Energiebereich dar. Im Rahmen der SET Pilots werden zudem Pilotierungsprojekte gefördert, die die technologische Weiterentwicklung im Kontext der Digitalisierung der Energiewende zum Ziel haben. Im Zentrum dieser Projekte steht dabei die Etablierung intelligenter Messsysteme als Sicherheitsanker und Plattform für den Datenaustausch in allen Anwendungsbereichen des Energiesektors.

2 Regulatorischer Rahmen

Mit den dritten Binnenmarktrichtlinien Strom und Gas (2009/72/EU und 2009/73/EU) wurde bereits 2009 europaweit festgelegt, dass die Mitgliedsstaaten bis 2020 80 Prozent der Verbraucherinnen und Verbraucher mit Smart Metern ausrüsten müssen. Ziel war dabei, den Endkundinnen und Endkunden zu ermöglichen, Maßnahmen zur Energieeffizienzsteigerung und Energieeinsparung zu ergreifen, indem man ihnen den eigenen Energieverbrauch transparent darlegt. In Deutschland trat hierfür 2016 das **Gesetz zur Digitalisierung der Energiewende (GDEW)** in Kraft und legte den Grundstein und verbindlichen Rechtsrahmen für den stufenweisen Ausbau zu einem intelligenten Energienetz in Deutschland.

Als besonderes Kernstück führte das GDEW das **Messstellenbetriebsgesetz (MsbG)** ein. Das MsbG aus dem Jahr 2016 beschreibt den Infrastruktur-Rollout und definiert Rollen und ihre Aufgaben sowie wichtige Prozesse im Messstellenbetrieb, bei der Datenverarbeitung und bei der Datenkommunikation. Zusätzlich werden technische Mindestanforderungen und Vorgaben zum Schutz intelligenter Messsysteme beschrieben. Diese Vorgaben werden ergänzt um die Pflichten und Kompetenzen der jeweils zuständigen Behörden. [1]

Im Mai 2023 trat das **Gesetz zum Neustart der Digitalisierung der Energiewende (GNDEW)** in Kraft. Das Gesetz umfasst die Änderung mehrerer bereits bestehender Regularien, wie beispielsweise des Energiewirtschaftsgesetzes (EnWG) und des Erneuerbare-Energien-Gesetzes (EEG). Die umfangreichsten Änderungen wurden jedoch im Messstellenbetriebsgesetz vorgenommen. Im Fokus steht dabei der beschleunigte und vereinfachte Rollout der Kommunikationsinfrastruktur. Dem Rollout kommt eine besondere Bedeutung zu, da er die Grundvoraussetzung für die Datenerfassung und damit für alle darauf aufbauenden Anwendungen einer digitalisierten Energiewirtschaft darstellt. [2]

Die beiden folgenden Abschnitte beschreiben den zeitlichen Ablauf(-plan) des Rollouts der digitalen Infrastruktur sowie die technischen Hintergründe und die Akteure rund um ein iMSys.

2.1 Rollout der digitalen Infrastruktur

Dem zentralen Element der Kommunikationsinfrastruktur wurden im MsbG (2016) fest definierte Technologien zugeordnet. Maßgeblich ist die Unterscheidung in **moderne Messeinrichtungen (mME)** und **intelligente Messsysteme (iMSys)**. Unter modernen Messeinrichtungen werden digitale Stromzähler verstanden, die den aktuellen Stromverbrauch mindestens im 15-Minuten-Takt messen und die Stromverbrauchswerte für die letzten 24 Monate darstellen können. Die gespeicherten Daten werden nicht dauerhaft übertragen. Ein intelligentes Messsystem besteht neben der modernen Messeinrichtung zusätzlich aus einem Kommunikationsmodul, dem sogenannten Smart Meter Gateway (SMGW). Durch das SMGW ist das iMSys in der Lage, die erfassten Messwerte zu übertragen.

Rollen beim intelligenten Messsystem

Rund um das iMSys gibt es eine Reihe an verschiedenen Akteuren, die jeweils eine vordefinierte Rolle einnehmen:

- Verbraucherinnen und Verbraucher: Sind natürliche oder juristische Personen, die Strom, Gas, Wasser und Wärme beziehen. Sie sind die Eigentümerinnen und Eigentümer der im SMGW verarbeiteten und gespeicherten Messwerte. [3]

- Servicetechnikerinnen und -techniker: Nutzen vor Ort die lokale Diagnoseschnittstelle des SMGW, um Daten und weitere Diagnosen aus dem System-Logbuch zu erhalten. Die Rolle beinhaltet lediglich Leserechte. [3]
- Gateway-Administratorinnen und -Administratoren (GWA): Konfigurieren, steuern und überwachen das SMGW. Dies beinhaltet auch die Administration und die Erstellung von Profilen zur Tarifierung sowie die Aktualisierung der Software. Um den sicheren Betrieb zu gewährleisten, ist für die zentrale Rolle des GWA nach § 25 MsbG eine Zertifizierung nötig. Sie kann durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) oder die Deutsche Akkreditierungsstelle (DAkkS) erfolgen. Die Technische Richtlinie TR-03109-6 regelt Maßnahmen für die Mindestsicherheit beim Administrator sowie die einheitlichen organisatorischen und technischen Anforderungen der Rolle (vgl. Kapitel 3.1, Abschnitt „Technische Richtlinien“). [4] [3] Zum Schutz der Daten müssen gewisse technische Vorkehrungen getroffen werden, die die Aktionen des GWA beschränken oder Aktionen verhindern. Besitzt das SMGW ein Betriebssystem, darf der GWA nicht zeitgleich die Rolle des Betriebssystem-Administrators besetzen. Überwacht wird der GWA durch Behörden, denen gegenüber er jederzeit auskunftspflichtig ist. [5]
- Messstellenbetreiber (MSB): Für den Betrieb, vor allem aber auch für den Einbau der Kommunikationseinheiten ist der Messstellenbetreiber zuständig. Es wird zwischen dem **grundzuständigen Messstellenbetreiber (gMSB)** und dem **wettbewerblichen Messstellenbetreiber (wMSB)** unterschieden. Der grundzuständige Messstellenbetreiber ist für die Umsetzung des Rollouts sowie für die nach MsbG festgelegten Aufgaben des Messstellenbetriebs verantwortlich. In der Regel übernimmt der örtliche Netzbetreiber diese Rolle. Wettbewerbliche Messstellenbetreiber sind Unternehmen, die als Dritte die Aufgaben des Messstellenbetriebs nach § 9 MsbG wahrnehmen. [6] Außerdem ist bei dem MSB der GWA angesiedelt. Dabei übernimmt der MSB selbst die entsprechenden Aufgaben oder gibt sie an einen Unterauftragnehmer ab.
- Externe Marktteilnehmer (EMT): Akteure, die berechtigt sind, über das Weitverkehrsnetz (Wide Area Network, WAN) mit dem SMGW Daten auszutauschen. Dabei kann es sich um verschiedene Marktteilnehmer wie Übertragungsnetzbetreiber (ÜNB), Verteilnetzbetreiber (VNB), Messstellenbetreiber (MSB), Energieversorgungsunternehmen (EUV) und weitere Dienstleister wie Mehrwertanbieter oder Plattformanbieter handeln. [3] Die externen Marktteilnehmer können in zwei Gruppen untergliedert werden: die aktiven und die passiven externen Marktteilnehmer.

  Passive externe Marktteilnehmer (pEMT) sind Marktteilnehmer, die Daten (vor allem Messwerte) vom SMGW ausschließlich empfangen. Ein pEMT kann beispielsweise in Marktrollen wie Energielieferant, Netzbetreiber für Netzzustandsdaten oder Messstellenbetreiber agieren.

  Aktive externe Marktteilnehmer (aEMT) empfangen im Gegensatz zu pEMT nicht nur Daten vom SMGW, sondern können auch an die lokalen steuerbaren Anlagen (wie zum Beispiel Speicher, Ladeeinrichtungen für E-Autos und intelligente Haushaltseinrichtungen) über das entsprechende CLS-Proxy (siehe Glossar) Signale senden und die Anlagen somit steuern. [7]
- Energieserviceanbieter (ESA): Erfragen mit Zustimmung der Anschlussnutzerinnen und -nutzer die Messdaten beim Messstellenbetreiber über einen standardisierten und automatisierten Prozess. Die Analyse, Aufbereitung und Visualisierung der Energiedaten, die der ESA durchführt, sollen eine Steigerung der Energie- und Kosteneffizienz bei den Anschlussnutzerinnen und -nutzern ermöglichen. Der Abruf der Verbrauchsdaten ist eine Zusatzleistung nach § 35 Abs. 2 MsbG, sodass die Bereitstellung dem MSB vergütet werden muss.

- Anschlussnutzer und Anschlussnehmer: Um den Rollout-Prozess abschließend beschreiben zu können, wurden darüber hinaus noch die Nutzerinnen und Nutzer der Messgeräte näher bestimmt. In § 2 MsbG wird hierzu der Unterschied zwischen einem **Anschlussnutzer** und einem **Anschlussnehmer** definiert. Ein Anschlussnutzer ist derjenige, der den Hausanschluss zur Entnahme von Strom bzw. Gas aus dem Netz nutzt. Meistens ist das die Mieterin oder der Mieter. Ein Anschlussnehmer ist die Eigentümerin oder der Eigentümer eines Grundstücks oder Gebäudes, das an das Niederspannungsnetz bzw. Niederdrucknetz angeschlossen ist. [1]

Neben der Klärung dieser Begrifflichkeiten wurden zudem die zentralen Fragenstellungen zum zeitlichen Ablauf und zur Kostenverteilung des Rollouts angepasst.

Bezüglich des Zeitplans wurde im GNDEW ein **verpflichtender Fahrplan** (§ 45 MsbG) für den Einbau der Messsysteme festgelegt, um den Prozess des Rollouts unbürokratischer zu gestalten und zu beschleunigen. Der Fahrplan beschreibt sowohl die vom Verbrauch und von der Erzeugung abhängigen **Pflichteinbaufälle** als auch die jeweils zeitlich zu erfüllenden **Einbauquoten** bzw. **Ausstattungspflichten** der gMSB.

Wie in Abbildung 1 dargestellt, sieht der Fahrplan vor, dass bis 2030 bzw. 2032 (je nach Verbrauchsgröße bzw. installierter Leistung) mindestens 95 Prozent der Verbraucherinnen und Verbraucher sowie der Erzeugerinnen und Erzeuger mit einem iMSys ausgestattet sind. Der **verpflichtende Einbau** und die Erfüllung der Ersten Einbauquoten beginnt 2025 für Verbraucherinnen und Verbraucher mit einem Verbrauch zwischen 6.000 und 100.000 Kilowattstunden sowie für Erzeugerinnen und Erzeuger mit einer installierten Leistung zwischen 7 und 100 Kilowatt. Für Verbraucherinnen und Verbraucher mit einem Jahresverbrauch unter 6.000 Kilowattstunden und Erzeugerinnen und Erzeuger mit einer installierten Leistung bis 7 Kilowatt ist die Installation eines iMSys optional (nach § 29 Abs. 3 MsbG).

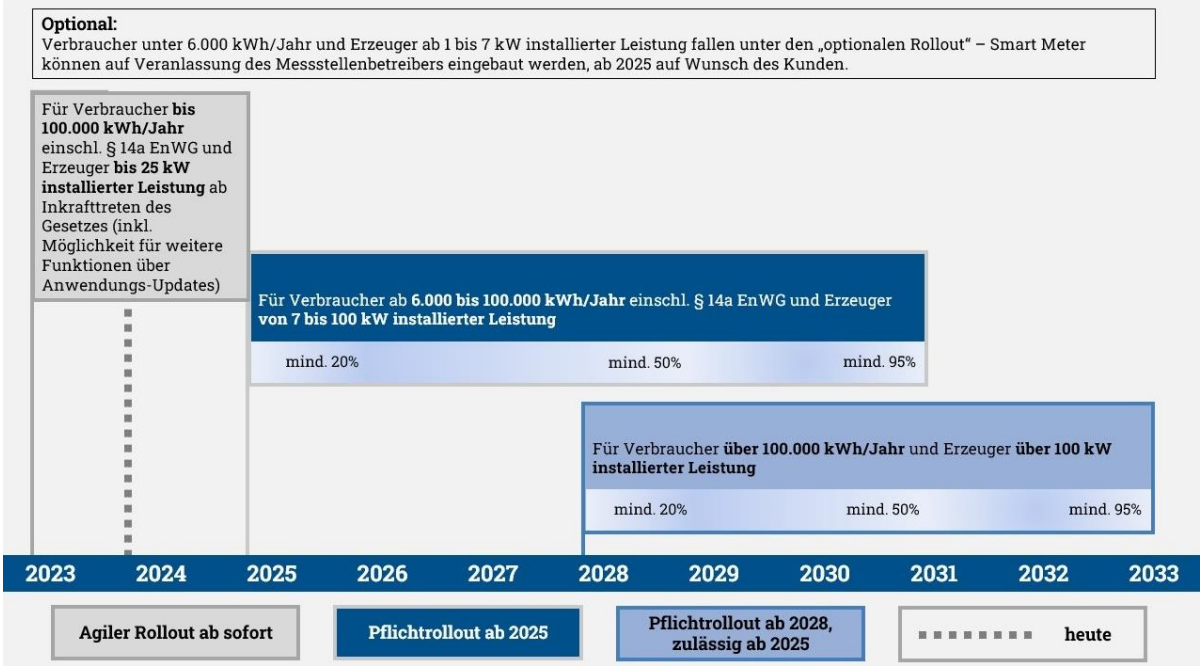

Abbildung 1: Rollout-Prozess gemäß dem gesetzlichen Rollout-Fahrplan [8]

Auch die **Preisobergrenzen** der Selbstbeteiligung der Nutzerinnen und Nutzer der jeweiligen Einbaukategorien wurden mit dem GNDEW angepasst – sie sind nun niedriger. Danach dürfen gMSB für eine mME unabhängig vom Jahresverbrauch maximal 20 Euro/Jahr in Rechnung stellen. Anschlussnutzerinnen und -nutzer mit einem Jahresverbrauch von mindestens 10.000 Kilowattstunden sowie Verbraucherinnen und Verbraucher nach § 14a EnWG müssen mit Kosten von mindestens 50 Euro pro Jahr rechnen. Für einen freiwilligen Einbau, den eine Verbraucherin oder ein Verbraucher selbst beauftragt, gilt eine Preisobergrenze für Zusatzleistungen in Höhe von einmalig 30 Euro. [9] [10]

Tabelle 1: Pflichteinbau von intelligenten Messsystemen [10]

Preisobergrenze (pro Jahr in Euro)	Verbraucherinnen und Verbraucher (Jahresverbrauch in kWh)	Erzeuger (in kW)
20	> 6.000 – 10.0000	< 7 – 15
50	Steuerbare Verbrauchseinrichtungen	-
50	> 10.000 – 20.000	> 15 – 30
90	> 20.000 – 50.000	-
120	> 50.000 – 100.000	> 30 – 100
Angemessen	> 100.000	> 100

2.2 Systemarchitektur eines intelligenten Messsystems

Das intelligente Messsystem, bestehend aus – wie in Kapitel 2.1 aufgeführt – einer moderner Messeinrichtung und einem Smart Meter Gateway, unterliegt einer Vielzahl an technischen Regularien und ist zudem in ein komplexes Betreiber- und Rollensystem eingebettet. In diesem Kapitel wird zum einen die technische Ausgestaltung eines iMSys, zum anderen der Aufbau der Systemumgebung und die Koordination der Prozesse innerhalb dieser dargestellt.

Technische Mindestanforderungen an ein iMSys

Die technischen Mindestanforderungen an ein iMSys sind in § 21 und § 22 des MsbG definiert. Demnach muss ein iMSys ein SMGW beinhalten und

- eine zuverlässige Datenverarbeitung wie auch Datenerhebung, -übermittlung, -protokollierung, -speicherung und -löschung gewährleisten,
- eine Visualisierung der Verbrauchswerte ermöglichen,
- eine sichere Verbindung in den Kommunikationsnetzen in der SMGW-Umgebung umsetzen,
- die Vorgaben zum Eigenstromverbrauch einhalten (dieser kann den Kundinnen und Kunden gegenüber nicht abgerechnet werden [11]) und
- die Stammdaten der angeschlossenen Anlagen übermitteln können.

Um sicherzustellen, dass diese Mindestanforderungen nach aktuellem Stand der Technik erfüllt werden, werden sie in Technischen Richtlinien genauer definiert und laufend angepasst (vgl. Kapitel 3.1, Abschnitt „Technische Richtlinien“).

Technische Komponenten und Schnittstellen

Um die im vorherigen Absatz benannten Anforderungen zu erfüllen, braucht das iMSys unterschiedliche Komponenten und Zugriff auf verschiedene Netzwerke. Technisch bildet das **SMGW** inklusive des integrierten **Sicherheitsmoduls** das Herzstück des intelligenten Messsystems. Zudem befinden sich am SMGW drei Schnittstellen:

- Lokales Metrologisches Netz (Local Metrological Network, LMN)
- Heimnetz (Home Area Network, HAN)
- Weitverkehrsnetz (Wide Area Network, WAN)

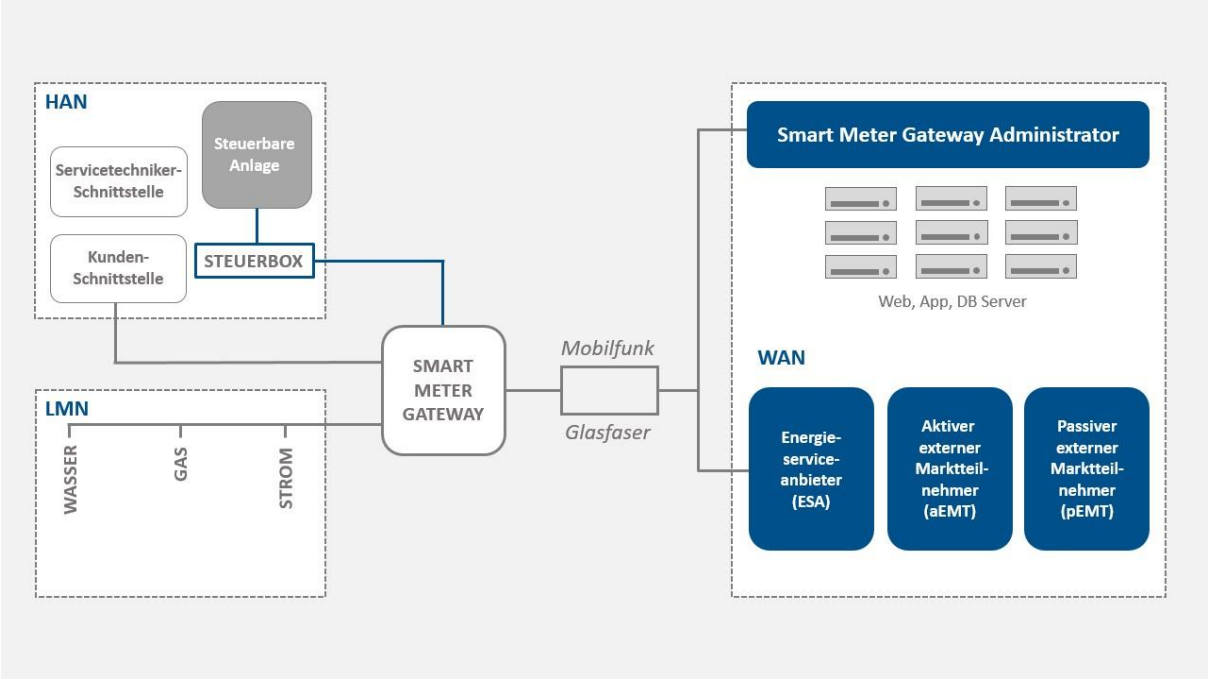

Abbildung 2: Netzwerke eines Smart Meter Gateway

Über das **LMN** sind die Zähler zur Erfassung der Verbrauchswerte mit dem SMGW verbunden. Sind diese **Zähler** nicht LMN-kompatibel, wird technisch entsprechend ein **Kommunikationsadapter** hinzugefügt (vgl. auch Kapitel 3.1, Abschnitt „Technische Richtlinien“). [5] Über dieses Netzwerk erfolgt also die lokale Datenakquisition und -speicherung der Verbrauchsdaten in einem einheitlichen Darstellungsformat (**zertifizierte Zählerprofile**). Ein wichtiger Parameter ist hierbei das Zeitintervall der erfassten Werte. [5]

Im **HAN** kann das SMGW bei entsprechender technischer Umsetzung dieser Option des Kommunikationsadapters, über eine **Steuerbox** mit den steuerbaren Energieverbrauchern kommunizieren (z. B. intelligente Haushaltsgeräte) und Energieerzeugungseinrichtungen (Controlable Local Systems, CLS). Dies ist möglich über eine bestimme Kommunikationsschnittstelle: die CLS-Schnittstelle. Die HAN-Schnittstelle bietet zudem eine Möglichkeit verschiedene Daten lokal auszulesen, die beispielsweise zur

Rechnungsprüfung sowie der Erfassung von Fehlern und Störungen für Servicemitarbeiterinnen und -mitarbeiter genutzt werden können. [5]

Über das WAN werden Daten „nach außen“ gesendet. Die Datenübertragung im **WAN** erfolgt in der Regel über **Funk**. Dem GWA kommt hier aktuell eine zentrale Rolle zu: Er ist dafür zuständig, die Daten aus dem iMSys den Berechtigten zur Verfügung zu stellen. Die externen Marktteilnehmer haben also keinen direkten Zugriff auf die originäre Messwertliste, sie erhalten lediglich die Messwerte für ihren Anwendungsfall, abgeleitet vom GWA. [5]

Messwertverarbeitung über Protokolle

Die verschiedenen Funktionen und Kommunikationswege werden über Zähler-, Auswertungs- und Kommunikationsprofile durch den GWA ermöglicht und koordiniert. Jedes Profil muss hierzu vorgeschriebene Mindestparameter enthalten, wie beispielsweise die Adresse des Empfängers und die maximale Sitzungslänge bei Kommunikationsprofilen (vgl. auch BSI TR-03109, siehe dazu Kapitel 3.1, Abschnitt „Technische Richtlinien“). [3] Die **Zählerprofile** ermöglichen im LMN die Datenerfassung. Aufbauend auf diesen Daten werden die gesammelten Messwerte auf Basis der Konfiguration der **Auswertungsprofile** verarbeitet, die für die Zusammenstellung der Daten für die Tarifanwendungsfälle (TAF, vgl. Abschnitt „Tarifanwendungsfälle“) im WAN relevant sind. Die meisten Mindestparameter gelten für die **Kommunikationsprofile**. Sie folgen auf die Auswertungsprofile und sind gemeinsam mit diesen die Grundlage für die Übermittlung der Messdaten an die Endverbraucherinnen und Endverbraucher sowie an die passiven EMT. Das Proxy-Kommunikationsmodul dient der bidirektionalen Kommunikation zwischen dem SMGW und dem aktiven EMT über das WAN, die entsprechenden Steuerbefehle werden vom SMGW über das HAN umgesetzt. [3]

Die Kommunikation zwischen dem SMGW und seinem Umfeld findet auf sieben Schichten des Referenzmodells Open Systems Interconnection (OSI) statt – einem Netzwerkprotokoll für die Kommunikation zwischen unterschiedlichen technischen Systemen. Jede Schicht deckt eine bestimmte Aufgabe und Funktion ab, ist in sich abgeschottet und verwendet unterschiedliche Verfahren und Protokolle. [12]

Das SMGW kommuniziert mit den drei Netzwerken und dem Sicherheitsmodul. Im HAN-Netzwerk existieren drei Schnittstellen zu den Rollen Servicetechniker, Letztverbraucher und CLS. Ein SMGW kann nur mit einem Servicetechniker verbunden werden, die Anzahl von Letztverbrauchern und CLS ist aber nicht begrenzt. Im WAN-Netzwerk gibt es eine Schnittstelle, über die mit einer unbegrenzten Anzahl an EMT kommuniziert werden kann. Das LMN-Netzwerk besitzt eine Schnittstelle, über die der Datenaustausch von den Messgeräten an das SMGW sowohl drahtgebunden als auch drahtlos erfolgen kann. Eine Besonderheit stellt die Schnittstelle zum Sicherheitsmodul dar. Hier wird für die Kommunikation eine APDU (Application Protocol Data Unit) nach ISO 7816 verwendet. [13]

Tarifanwendungsfälle (TAF) [14]

Tarifanwendungsfälle (TAF) sind die Mindestfunktionen, die ein iMSys erfüllen muss. Sie wurden vom BSI für die Regelung der für iMSys benötigten Parameter entwickelt. Insgesamt sind bisher 14 Tarifnutzungsszenarien beschrieben, die Dienstleistungen für die Kundschaft darstellen.

Die konkreten Tarifanwendungsfälle sind in Tabelle 2 dargestellt [15]. Diese Liste ist nicht abschließend und kann in Zukunft um weitere Tarifanwendungsszenarien ergänzt werden. Zudem werden nicht alle TAFs von den bisher zertifizierten SMGWs unterstützt. Zum aktuellen Zeitpunkt werden die Tarifanwendungsfälle 1, 2, 6 und 7 in der Stufe 1 und 9,10 sowie 14 in der Stufe 2 unterstützt.

Tabelle 2: Tarifanwendungsfälle von iMSys

TAF	Anwendung	Beschreibung
TAF 1	Datensparsame	Der Zählerstand wird als die Summe von Verbrauch und Einspeisung mehrerer Zähler ausgelesen.
TAF 2	Zeitvariable	Ein dem heutigen Hochtarif/Niedertarif-System ähnlicher Stromtarif, der zeitabhängig und für mehrere Tarifstufen geeignet ist.
TAF 3	Lastvariable	Ein Stromtarif für mehrere Laststufen, der von Leistungen abhängig ist.
TAF 4	Verbrauchsvariable	Die verbrauchte Energie wird in unterschiedliche Verbrauchsstufen eingeteilt, jede Stufe weist ein Mengenkontingent auf. Falls das Kontingent einer Stufe überschritten wird, schaltet das System auf die nächsthöhere Stufe um.
TAF 5	Ereignisvariable	Ein Stromtarif in definierten Tarifstufen, der von Ereignissen abhängig ist. Diese können sowohl SMGW-intern als auch durch einen externen berechtigten Akteur hervorgerufen werden.
TAF 6	Ablesung von Messwerten im Bedarfsfall	Ein Stromtarif für Situationen, die nicht planbar sind (z. B. Umzug, Lieferantenwechsel etc.). Es werden die täglichen Messwerte der letzten 6 Wochen gespeichert.
TAF 7	Zählerstandsgangmessung	Ein Stromtarif für die Erfassung (im Zyklus des Einschreibungszeitraums) sowie die Versendung von Zählerständen (Verbrauch und Erzeugung).
TAF 8	Erfassung von Extremwerten	Minimaler- und maximaler Leistungswert innerhalb eines Abrechnungszeitraumes.
TAF 9	Abruf der Ist-Einspeisung	Die Leistungen werden im Rahmen einer Energiemanagementmaßnahme abgefragt und dürfen nicht zu Abrechnungszwecken verwendet werden.
TAF 10	Abruf von Netzzustandsdaten	Die Netzzustandsdaten werden periodisch oder bei einem Ereignis (Über- oder Unterschreitung eines Schwellenwertes) abgerufen.
TAF 11	Steuerung von unterbrechbaren Verbrauchseinrichtungen und Erzeugungsanlagen	Der Zählerstand und der Zeitpunkt werden in Echtzeit festgehalten, wenn ein Steuersignal oder andere externe Ereignisse empfangen werden.
TAF 12	Prepaid-Tarif	Durch vorausbezahlte Guthaben wird eine bestimmte Menge an Energie bereitgestellt. Im Fall einer Überschreitung oder bei einem definierten Schwellenwert wird ein Signal an den EMT und den Kunden generiert.
TAF 13	Letztverbraucher-visualisierung	Die Messwerte werden für die Letztverbrauchervisualisierung nicht an der HAN-, sondern an der WAN-Schnittstelle zur Verfügung gestellt.
TAF 14	Hochfrequente Messwertbereitstellung für Mehrwertdienste	Die hochaufgelösten Daten werden visualisiert, damit die darauf aufbauenden Dienstleistungen umgesetzt werden können.

3 Datenschutz, Datensicherheit und Interoperabilität

Das SMGW erfordert als notwendige Kommunikationseinheit eines digitalen Energiesystems neue Konzepte im Bereich Sicherheit. Hier ist die Einhaltung der **Schutzziele der Informationssicherheit** von besonderer Wichtigkeit. Dazu zählen **Vertraulichkeit**, **Integrität** und **Verfügbarkeit** sowie weitere daraus abgeleitete Schutzziele wie Authentizität, Verbindlichkeit und Autorisation. [13] Hierfür definierte Standards sorgen aber nicht nur für eine hohe Sicherheit, sondern stellen auch den interoperablen Einsatz von iMSys sicher.

Eine besondere Aufgabe erfüllt hierbei das Bundesamt für Sicherheit in der Informationstechnik. Das BSI ist dafür verantwortlich, die Einhaltung des Datenschutzes, der Datensicherheit und der Interoperabilität des SMGW zu überwachen. Um die hohen Sicherheitsstandards zu erfüllen, hat das BSI über die Formulierung von Schutzprofilen und Technischen Richtlinien verbindliche Vorgaben für das SMGW gemacht. Sie wurden im Auftrag des BMWK zusammen vom BSI, Vertreterinnen und Vertretern aus der Branche und Datenschützern erarbeitet. Das BSI ist auch für die Zertifizierung der auf dem Markt erhältlichen SMGW verantwortlich. Sie müssen die Erfüllung gesetzlicher Mindestanforderungen an Datensicherheit, Datenschutz und Interoperabilität nachweisen. [16] Die verschiedenen Standards und Richtlinien des BSI werden im ersten Teil dieses Kapitels genauer beschrieben und im zweiten Teil mit dem Mess- und Eichrecht in Verbindung gesetzt.

3.1 Anforderungen des BSI an das intelligente Messsystem

Das BSI hat eine Reihe an Maßnahmen geschaffen, um einen ausreichend hohen Schutz der SMGW sicherzustellen. Hauptelemente dieser Schutzmaßnahmen sind die im Folgenden vorgestellten technischen Standards und Schutzprofile sowie die Technischen Richtlinien. Die technischen Standards umfassen dabei allgemein beschlossene Regeln für die konsistente Organisation von Informationen. Dies ermöglicht es, dass technische Systeme von mehreren unabhängigen Anwendungen verwendet werden können. Bei Schutzprofilen handelt es sich auch um die Formulierung generischer Anforderungen an die Fiktionalitäten und die Vertrauenswürdigkeit einer Produktkategorie mit dem Ziel, damit eine bestimmte Menge von Sicherheitszielen zu erreichen. Technische Richtlinien ergänzen technische Prüfvorschriften des BSI, die den Aufbau und die Absicherung von IT-Systemen adressieren. Ziel ist die Sicherstellung angemessener IT-Sicherheitsstandards. [17] [18]

Gemäß § 19 Abs. 2 des Messstellenbetriebsgesetzes sind für die Verarbeitung von Daten im Bereich der Energieversorgung ausschließlich technische Systeme und Komponenten zulässig, die den definierten Mindestanforderungen an intelligente Messsysteme und Smart Meter Gateways entsprechen. Diese Anforderungen sind in den Schutzprofilen und Technischen Richtlinien gemäß §§ 21, 22 MsbG präzise festgelegt.

Technische Standards

Technische Standards (BSI-Standards) zeigen als Teil der IT-Grundschutz-Methodik Anwenderinnen und Anwendern Methoden, Prozesse, Verfahren und Maßnahmen auf, um Geschäftsprozesse und Daten zu sichern. [19]

Der **BSI-Standard 200-1** enthält allgemeine Anforderungen an ein Managementsystem für Informationssicherheit (Information Security Management System, ISMS). Er ist weiterhin kompatibel mit der ISO 27001, der international anerkannten Norm für ein ISMS. Der **BSI-Standard 200-2** etabliert drei zusätzliche Vor-

gehensweisen zum Aufbau eines ISMS. Im **BSI-Standard 200-3** sind alle risikobezogenen Arbeitsschritte gebündelt. Der Standard ermöglicht es, mit deutlich reduziertem Aufwand ein angestrebtes Sicherheitsniveau zu erreichen, indem nach erfolgreicher Anwendung der IT-Grundschutz-Methodik direkt eine Risikoanalyse durchgeführt wird. Eine praxisnahe Anleitung zum Aufbau eines Business Continuity Management System (BCMS) ist im **BSI-Standard 200-4** beschrieben. Ein BCMS zielt darauf ab, Unternehmen resilient gegenüber Krisen zu machen.

Ergänzend zu den Standards ist mit dem „Leitfaden zur Basis-Absicherung nach IT-Grundschutz: In drei Schritten zur Informationssicherheit“ [20] ein kompakter Einstieg zum Aufbau eines ISMS verfasst worden. Bei der Umstellung auf den modernisierten IT-Grundschutz muss das ISMS gemäß BSI-Standard BSI 100-2 und den IT-Grundschutz-Katalogen aufgebaut sein. [19]

Schutzprofile

In Schutzprofilen schreibt das BSI Mindestsicherheitsanforderungen an die Funktionalitäten der Komponenten und die Vertrauenswürdigkeit einer Produktkategorie fest. Damit wird eine bestimmte Menge an Sicherheitszielen, wie beispielsweise IT-Sicherheitseigenschaften oder Bedingungen für den sicheren Einsatz eines Produkts, abgedeckt. In Schutzprofilen werden auch die verschiedenen Daten und ihre Verarbeitung beschrieben sowie Annahmen zu typischen Einsatzumgebungen, einzuhaltende gesetzliche Auflagen und abzuwehrende Bedrohungen definiert. Die Zertifizierung eines Schutzprofils bedeutet, dass es vollständig, konsistent und stimmig ist. Die Inhalte der Schutzprofile beziehen sich oft auf Technische Richtlinien (siehe nächster Abschnitt). Als Collaborative Protection Profiles werden international geltende Schutzprofile bezeichnet. [4]

Für das SMGW existieren aktuell drei Schutzprofile: BSI-CC-PP-0073 (Schutzprofil für das SMGW), BSI-CC-PP-0077 (Schutzprofil für das Sicherheitsmodul) und BSI-CC-PP-0095 (Schutzprofil für das Mini Hardware Security Module (HSM)). [4]

Die **BSI-CC-PP-0073** beschreibt mögliche Bedrohungen eines SMGW in seiner Einsatzumgebung – wie den Versuch, über physischen Zugang erhobene Daten zu ändern oder durch einen Eingriff über das WAN die Integrität der Daten einzuschränken – und definiert Mindestanforderungen für entsprechende Sicherheitsmaßnahmen. Das SMGW konzentriert sich auf die zu erfüllenden Sicherheitsleistungen, definiert sicherheitstechnische Anforderungen an die Schnittstellen zu den drei Netzen LMN, HAN und WAN und sichert so die Kommunikationswege kryptografisch ab. Damit sind die Authentizität, die Integrität und die Vertraulichkeit der Messwerte gewährleistet. Jedes SMGW muss dieses Schutzprofil für eine Zertifizierung erfüllen. [4] [21]

Ergänzend hierzu werden in der **BSI-CC-PP-0077** die Bedrohungen und Sicherheitsanforderungen für das Sicherheitsmodul des SMGW definiert, das kryptografische Kernroutinen für die Signaturerstellung und -prüfung, die Schlüsselgenerierung sowie die Zufallszahlengenerierung bereitgestellt. Außerdem dient es als sicherer Speicher des kryptografischen Schlüsselmaterials. [21]

Die **BSI-CC-PP-0095** beschreibt die Sicherheitsanforderungen (das Schutzprofil) des Mini-HSM. Dieses erfüllt ähnlich wie das Sicherheitsmodul des SMGW unter anderem Verschlüsselungsaufgaben, wird jedoch beispielsweise bei den Gateway-Administrator, den EMT oder den Herstellern der SMGW eingesetzt. [22]

Technische Richtlinien

Die Technischen Richtlinien des BSI gewährleisten die Interoperabilität der verschiedenen Komponenten von iMSys und spezifizieren bzw. ergänzen die Sicherheitsanforderungen der Schutzprofile. Sie definieren ange-

messene IT-Sicherheitsstandards wie Kriterien und Methoden zur Konformitätsprüfung der Interoperabilität von IT-Sicherheitskomponenten und IT-Sicherheitsanforderungen. Sie richten sich an alle Akteure, die mit dem Aufbau oder der Sicherung von IT-Systemen zu tun haben. Hierfür werden bereits bestehende Standards nach Common Criteria (internationaler Standard zur Bewertung und Prüfung von Sicherheitseigenschaften von IT-Produkten) oder Interoperabilitätsstandards referenziert und ergänzt. [4]

Im Umfeld der Smart Meter gibt die TR-03109 Anforderungen hinsichtlich der Funktionalität, Interoperabilität und Sicherheit der Komponenten vor. [3] Die TR-03109 gliedert sich in mehrere Teile und bezieht sich sowohl auf das SMGW als auch auf das Sicherheitsmodul und die Infrastruktur. Hierzu zählen beispielsweise die Public Key Infrastructure (PKI) oder der Gateway-Administrator. [23] Die einzelnen Teile der Technischen Richtlinie gliedern sich thematisch in folgende Bereiche:

1. **Anforderungen an die Interoperabilität der Kommunikationseinheit eines iMSys (TR-03109-1)**

   Der erste Teil der Technischen Richtlinie beschreibt funktionale Mindestanforderungen an das SMGW. Die Technische Richtlinie gibt den aktuellen Stand der Technik wieder und wird daher regelmäßig angepasst. Schwerpunkte sind die technischen Vorgaben der drei Netzwerke WAN, LAN und HAN. Zusätzlich werden interne logische Abläufe wie die Tarifierung je nach Anwendungsfall oder das Zusammenspiel von SMGW und dem Sicherheitsmodul beschrieben. [23]

2. **Anforderungen an die Funktionalität und Interoperabilität des Sicherheitsmoduls (TR-03109-2)**

   Im zweiten Teil werden Anforderungen in Bezug auf das Sicherheitsmodul beschrieben. Der verpflichtende Einsatz eines zertifizierten Sicherheitsmoduls wird im Schutzprofil für das SMGW gefordert. Das Sicherheitsmodul unterstützt das SMGW bei der Signaturerstellung und -prüfung, zusätzlich wirkt es bei der Schlüssel- und Zufallszahlengenerierung mit. [23]

3. **Kryptografische Vorgaben für die Infrastruktur von intelligenten Messsystemen (TR-03109-3)**

   Vorgaben zu kryptografischen Verfahren oder Schlüssellängen werden im dritten Teil der Technischen Richtlinie definiert. Basis der Richtlinie sind weitere Richtlinien wie unter anderem die TR-02102 „Kryptographische Verfahren: Empfehlungen und Schlüssellängen“ und die TR-03111 „Elliptische-Kurven-Kryptographie“. [23]

4. **Smart Metering PKI – Public Key Infrastructure für Smart Meter Gateways (TR-03109-4)**

   Die Architektur der Smart Metering Public Key Infrastructure (SM-PKI) wird im vierten Teil der technischen Richtlinie ausgeführt. Die SM-PKI stellt die Grundlage zur Absicherung der WAN-Kommunikation sicher. Hierfür wird die Authentizität der eingesetzten öffentlichen Schlüssel verifiziert. [24] Des Weiteren werden die Mindestanforderungen an die Interoperabilität und die Sicherheit der SM-PKI spezifiziert, sie müssen auch in der Zertifizierungsrichtlinie (Certificate Policy, CP) für die SM-PKI berücksichtigt werden. Weiterhin werden die Profile für die einzusetzenden Zertifikate und Sperrlisten beschrieben. [23]

5. **Kommunikationsadapter (TR-03109-5)**

   Ein Kommunikationsadapter ist eine logische Einheit, die eine einheitliche und sichere kommunikative Anbindung von technischen Einrichtungen an das SMGW unterstützt und in einer physischen Komponente realisiert ist. Ein Kommunikationsadapter ist an allen Schnittstellen des SMGW (WAN, LMN und HAN) denkbar.

6. Smart-Meter-Gateway-Administration (TR-03109-6)

Dieser Teil der Technischen Richtlinie spezifiziert die Mindestanforderungen an den SMGW-Administrator zur Durchsetzung der Informationssicherheit, wodurch der technisch sichere Betrieb gewährleistet wird. Der Nachweis der Erfüllung der Mindestanforderungen kann über eine ISO-27001-Zertifizierung auf Basis des IT-Grundschutzes oder durch eine Zertifizierung gemäß ISO/IEC 27001 erbracht werden. [16]

Eine Übersicht über die Schutzprofile und Technischen Richtlinien finden Sie auf der Website des BSI. **[18]**

Datenschutz und Datensicherheitskonzept

Im MsbG ist ein umfassendes Konzept zur Datensicherheit und zum Datenschutz entwickelt worden, das die Umsetzung sowohl der Schutzprofile als auch der Technischen Richtlinien fordert. [25] Hierbei muss das SMGW im Sinne der Datensparsamkeit, Datensouveränität und Effizienz in der Lage sein, die Datenübertragung Ende-zu-Ende-verschlüsselt an die jeweilige Rolle im Rahmen ihrer Berechtigungen durchzuführen. Im Logbuch wird eine Übersicht über die erfassten Daten gegeben und ihre Verbreitung und die dazugehörigen Kommunikationsschritte können dort nachvollzogen werden. [4]

3.2 Eichrechtliche Anforderungen an intelligente Messsysteme

Die bisher vorgestellten Regularien des BSI werden von der Physikalisch-Technischen Bundesanstalt (PTB) in der PTB-A 50.8 um eichrechtliche Anforderungen ergänzt. Eine vollständige Harmonisierung beider Vorgaben ist nicht möglich, da sie unterschiedlichen Rechtsgrundlagen unterliegen. Das Mess- und Eichrecht wurde zuletzt Ende 2023 / Anfang 2024 angepasst, um Prozesse zu vereinfachen und so den Rollout von Smart Metern zu beschleunigen. Beispielsweise wurden Genehmigungsprozesse zur Durchführung von Software-Updates vereinfacht und es wurde eine unbegrenzte Eichgültigkeit eingeführt. [5] [26]

Während sich die Regularien des BSI lediglich auf das SMGW und die daran anschließenden Netzwerke LMN, HAN und WAN beziehen, legt die PTB-A 50.8 auch Anforderungen für an den Netzwerken angeschlossene Komponenten fest. Zu den eichrechtlich relevanten Komponenten gehören, wie in Abbildung 3 dargestellt, unter anderem **Kommunikationsadapter**, die aus den Zählern stammende Messdaten in für das LMN geeignete Übertragungsprotokolle konvertieren. Ein Adapter wird von allen Zählern benötigt, die nicht über ein im LMN zulässiges Protokoll kommunizieren können. Eichrechtlich relevant sind hierbei die beiden funktionalen Einheiten des Adapters in Form eines Eingangs, in dem das Eingangssignal konvertiert wird, und eines Ausgangs, der die Schnittstelle zum TLS-Kanal (Transport Layer Security) im LMN und damit zum SMGW bildet. Eine Absicherung der Signalübertragung vom Zähler zum Adapter mittels Benutzersicherung ist in der Regel ausreichend. Die Schnittstellen für das Eingangssignal sind vielfältig, beispielsweise werden hierfür Modbus (Kommunikationsprotokoll) oder Impulsschnittstellen genutzt. Eine Task Force aus BSI, Deutschem Verein des Gas- und Wasserfaches (DVGW), Forum Netztechnik/Netzbetriebe (FNN), Open Metering System (OMS), Physikalisch-Technischer Bundesanstalt (PTB) und Bundesnetzagentur (BNetzA) erarbeitet Feinspezifikationen für diese Schnittstellen, womit diese dann eichrechtlich korrekt sind. [27]

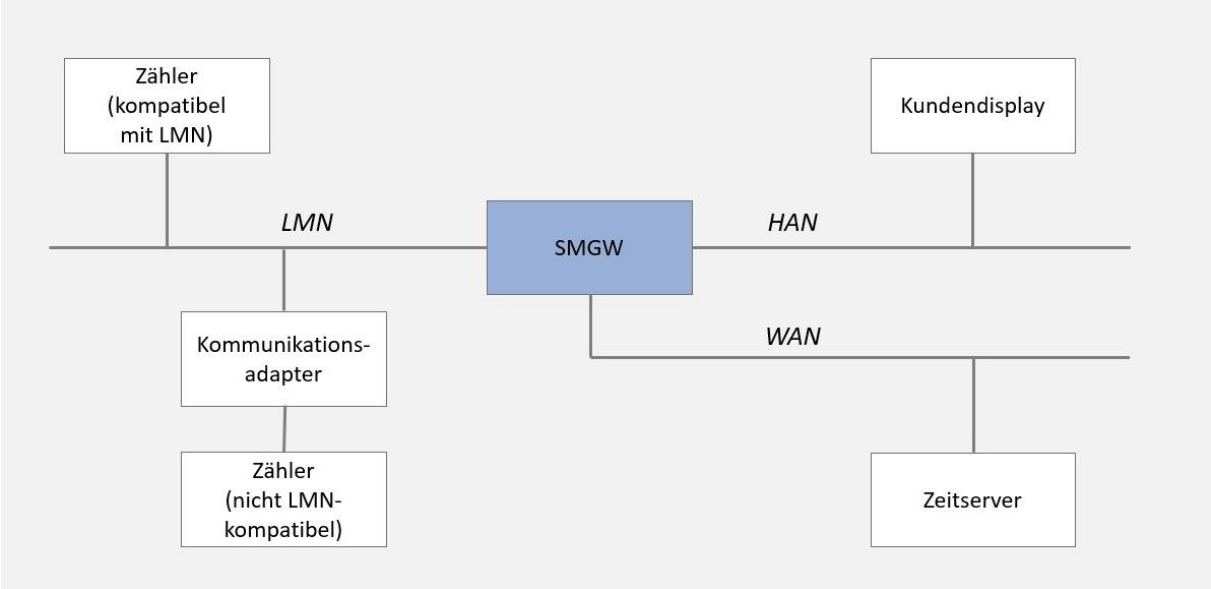

Abbildung 3: Eichrechtlich relevante Komponenten eines intelligenten Messsystems [5]

Darüber hinaus sind auch Vorgaben für die vorgeschriebene **Anzeige** der im SMGW erzeugten Messwerte und **Zeitserver** für die Synchronisation der Zeitbasen in der PTB-A 50.8 festgeschrieben.

Die Zeitbasensynchronisierung ist für eine Reihe an Funktionen des SMGW wichtig, die einen Bezug zur gesetzlichen Zeit verlangen, wie beispielsweise die vorgeschriebene Zeitstempelung der zu erfassenden Messwerte. Die TR-03109-1 (vgl. Kapitel 3.1, Abschnitt „Technische Richtlinien“) schreibt dafür eine hierarchische Struktur vor, bei der das SMGW durch den **Zeitserver** des GW-Administrators synchronisiert wird und dieser wiederum von den Zeitservern der PTB zu synchronisieren ist. Beide Stufen werden durch das Network Time Protocol (Standard für die Versorgung von intelligenten Endgeräten mit der Uhrzeit) realisiert. [5]

Jedes SMGW muss zudem in der Lage sein, eine **Anzeige** mit eichrechtlich relevanten Daten zu generieren. Die deutschen Technischen Richtlinien (TR) und die internationalen Protection Profiles (PP) definieren lediglich die Anforderungen an die hierfür vorgesehene HAN-Schnittstelle. Die PTB-A 50.8 schreibt wiederum Anforderungen an die Visualisierung dieser Daten mittels eines Kundendisplays fest. [28] Die Umsetzung des Kundendisplays kann auf drei verschiedene Arten erfolgen. Eine Möglichkeit wäre die Anzeige über ein integriertes Kundendisplay, weiterhin könnten die Daten über ein Hardware-Kundendisplay angezeigt werden, das über die Anschlussnutzer-Schnittstelle (IF_GW_CON) angebunden ist. Zudem besteht die Möglichkeit, ein Kundendisplay über einen Webbrowser bereitzustellen. Hier erfolgt die Datenübertragung über einen TLS-Kanal. Für diesen Lösungsansatz ist nur die Nutzung einer eichrechtlich validierten und zertifizierten Anwendung zugelassen. [27]

Den Letztverbraucherinnen und -verbrauchern dürfen dabei nur Daten angezeigt werden, die sie selbst betreffen. Zudem müssen die Daten vor unautorisiertem Zugriff oder Manipulation geschützt werden. Die für die Rechnungsprüfung notwendigen Informationen enthalten neben den eigentlichen historischen Messwerten weitere Daten, wie Stammdaten und Tarifinformationen. [5] [27]

4 Einsatzbereiche

Smart Meter Gateways sind als Mess-, Steuer- und Kommunikationsinfrastruktur des Energiesystems von morgen konzeptioniert und somit für eine Vielzahl von energiewirtschaftlichen und für die Energiewende relevanten Anwendungsfällen unabdingbar. In dieser Publikation werden drei Einsatzbereiche vorgestellt: Smart Metering / Sub-Metering, Smart Grids und Smart Mobility sowie Smart Home / Smart Building und Smart Services.

4.1 Smart Metering / Sub-Metering

Beim **Smart Metering** werden die Verbrauchswerte für Strom, Gas, Wasser und Wärme durch Smart Meter digital erfasst und über die sicheren Kommunikationskanäle des SMGW an externe Marktteilnehmer (z. B. Verteilnetzbetreiber) übermittelt. Beim „klassischen“ Metering werden Verbrauchswerte nur jährlich für die Endabrechnung von den Verbraucherinnen und Verbrauchern abgelesen. Beim Smart Metering können Daten in sehr kurzen zeitlichen Intervallen erfasst werden. Dies bildet die Grundlage für eine Vielzahl von Anwendungsfällen, die die Einbindung erneuerbarer Energien ermöglichen und die Kosten der Endverbraucherinnen und -verbraucher senken. Beispielsweise können die Verbräuche für die Endkundschaft auf Endgeräten visualisiert und dadurch Transparenz und ein Bewusstsein für die eigenen Verbräuche geschaffen werden. Außerdem ermöglicht eine hochfrequente und digitale Aufzeichnung der Verbräuche das Angebot variabler Stromtarife, durch die eine Anpassung des Verbrauchs erzielt werden soll. [4]

Beim **Sub-Metering** werden die Abrechnungen für die Verbräuche von Strom, Wasser und Wärme unterschiedlicher Parteien durch Sub-Metering-Anbieter für beispielsweise die Vermieterinnen und Vermieter erstellt. Die Grundlage bilden die von dedizierten Smart Metern erfassten Daten, die über das SMGW an den Sub-Metering-Anbieter übertragen werden. [29]

Sowohl beim Smart Metering als auch beim Sub-Metering dient das SMGW zur geschützten Übertragung von Daten an die an der Abrechnung beteiligten Parteien.

4.2 Smart Grid & Smart Mobility

Smart Grid – Einspeise-, Last- und Energiemanagement

Unter einem Smart Grid wird ein durch moderne Regelungs- und Leittechnik automatisiertes Stromnetz verstanden. Die aktuell fortschreitende Automatisierung bezieht sich besonders auf die Niederspannungsebene, die im Vergleich zur Mittel- und zur Hochspannungsebene noch deutlich weniger mit der zur Überwachung des Netzes und zur Ansteuerung seiner Erzeugungs- und Verbrauchsanlagen notwendigen Technik ausgestattet ist.

Durch die gezielte Ansteuerung der sich im Netz befindenden Anlagen wird die Flexibilität des Energiesystems erhöht. Das heißt, dass der Energieverbrauch an die fluktuierende Energieerzeugung von Erneuerbare-Energien-Anlagen angepasst werden kann. Zudem ermöglicht ein Smart Grid eine bessere Nutzung der Netzinfrastruktur. Sie ist im Niederspannungsbereich nicht für die Einspeisung von Leistung vorgesehen. In einem flexiblen Netz können Netzengpässe und andere kritische Zustände vermieden werden. [30]

Smart Meter Gateways ermöglichen die Realisierung eines Smart Grid auf zwei Arten: Durch die digitale und hochfrequente Übertragung von Messwerten können die Netzzustände besser erfasst werden. Dadurch können notwendige Steuereingriffe von den Verteilnetzbetreibern abgeleitet werden. Diese Steuereingriffe könnten wiederum über das Smart Meter Gateways realisiert werden.

Smart Mobility – Ladesäuleninfrastruktur / Lademanagement

Die Ausrüstung von öffentlichen Ladesäulen mit intelligenten Messsystemen und die darauf basierenden Lösungen werden als Smart Mobility bezeichnet. Die Kommunikationskanäle der SMGW bieten die Möglichkeit, die Authentifizierung und Administration der Nutzer sowie die Messwertverarbeitung und Abrechnung datenschutzkonform durchzuführen. Zudem werden dadurch die Ladesäulen in das Smart Grid integriert. E-Mobile und ihre elektrischen Speicher können dann netzdienlich zum Beispiel durch die Bereitstellung von Regelleistung eingesetzt werden. [4]

4.3 Smart Home / Smart Building & Smart Services

Um Eigenheime und Gebäude in **Smart Homes und Smart Buildings** zu verwandeln, kommt auch in diesem Bereich moderne Informations- und Kommunikationstechnologie zum Einsatz. Das Ziel ist dabei, die Qualität und die Sicherheit des Wohnens zu erhöhen, aber auch die Energieverbräuche entsprechend den Bedürfnissen der Bewohnerschaft anzupassen und dadurch Energie einzusparen. Dazu können beispielsweise Heizungen erst dann aufgedreht werden, wenn sich die Bewohnerinnen und Bewohner dem Gebäude nähern. Auch in diesem Bereich können die entsprechenden Signale über die SMGW-Infrastruktur gesendet bzw. empfangen werden.

Bei **Smart Services bzw. Mehrwertdiensten** handelt es sich um energieversorgungsfremde Dienstleistungen. Ähnlich wie beim Einsatzbereich Smart Home dienen hier die Smart Meter Gateways dem Senden und Empfangen von Daten. Ein Beispiel für einen Mehrwertdienst sind Energiespartipps, die auf Grundlage der vom SMGW ausgesendeten Verbrauchsdaten zur Verfügung gestellt werden. Außerdem wird diskutiert, dass SMGW auch Daten von Sensoren empfangen könnten, die keine Verbräuche messen, sondern beispielsweise Bewegungen innerhalb des Hauses registrieren. Pflegedienste könnten diese Daten erhalten und auswerten und in Notsituationen von pflegebedürftigen Personen schneller reagieren.

5 Fazit

Intelligente Messsysteme sind eines der zentralen Instrumente, um das immer dezentralere Energiesystem weiter sicher und effizient betreiben zu können. So sehr das iMSys die Datenerhebung und den Datenaustausch automatisiert und erleichtert, so sehr muss auch auf die Sicherheit des Systems geachtet werden, denn als Kritische Infrastruktur ist die Stromversorgung besonders schützenswert.

Regulatorischer Rahmen

Das durch das Gesetz zum Neustart der Digitalisierung der Energiewende novellierte Messstellenbetriebsgesetz bildet den rechtlichen Rahmen für den Einsatz von iMSys. So wird im MsbG beispielsweise festgehalten, dass bis 2030 bzw. 2032 mindestens 95 Prozent der Pflichteinbaufälle umgesetzt sein müssen. Auch legt das MsbG technische Mindestanforderungen für iMSys fest.

Datenschutz, Datensicherheit und Interoperabilität

Das Smart Meter Gateway gewährleistet für die Digitalisierung der Energiewende Datenschutz, Datensicherheit und Interoperabilität. Die Erfüllung der entsprechenden Anforderungen spielt im Rahmen der Vernetzung der Akteure im intelligenten Energiesystem eine entscheidende Rolle. Daten, die über das SMGW ausgetauscht werden können, sind sehr sensibel, da sie zum Beispiel Aufschluss über das individuelle Verbrauchsverhalten geben und so als personenbezogene Daten einem besonderen Schutz unterliegen oder im Hinblick auf Daten zum Netzzustand besonders gegen Angriffe zu schützen sind. Diese Anforderungen wurden in Kapitel 3 dargelegt.

Einsatzbereiche

Mit der zunehmenden Vernetzung und der bundesweiten Einführung von SMGW ergibt sich ein großes Potenzial für die Entwicklung von integrierten Lösungen, Anwendungsfällen und Geschäftsmodellen, die die digitale Energiewende befördern können. Sie bewegen sich zukünftig in den für die Energiewende relevanten Einsatzbereichen Sub-Metering, Smart Grid, Smart Mobility, Smart Home/Building und Smart Services und können in konkreten Endkundenprodukten wie beispielsweise variablen Stromtarifen münden. Zudem ergeben sich umfangreiche Möglichkeiten zur Erfassung von Daten zur Energieerzeugung und zum Energieverbrauch sowie für Lösungen, die sich über verschiedene Sektoren erstrecken und spartenübergreifend sind. Wann es zu einem breiten Einsatz dieser Anwendungen kommt, hängt jedoch maßgeblich von der Geschwindigkeit des Rollouts der iMSys ab. Mit den jüngsten regulatorischen Änderungen wurde ein gesetzlicher Zeitplan hierfür geschaffen.

Literaturverzeichnis

[1] Bundesamt für Justiz, „Gesetz über den Messstellenbetrieb und die Datenkommunikation in intelligenten Energienetzen (Messstellenbetriebsgesetz - MsbG),“ 29. August 2016. [Online]. Available: https://www.gesetze-im-internet.de/messbg/BJNR203410016.html

[2] Bundestag, „Gesetz zum Neustart der Digitalisierung der Energiewende,“ 22. Mai 2023. [Online]. Available: https://www.recht.bund.de/bgbl/1/2023/133/VO.html

[3] Forschungsstelle für Energiewirtschaft e. V., „Grundlagen zu intelligenten Messsystemen (iMSys),“ 15. September 2020. [Online]. Available: https://www.ffe.de/wp-content/uploads/2020/08/20200918_iMSys_Erklaerung.pdf

[4] Bundesamt für Sicherheit in der Informationstechnik (BSI), „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,“ 29. Januar 2019. [Online]. Available: https://www.bmwk.de/Redaktion/DE/Downloads/S-T/standardisierungsstrategie.pdf?__blob=publicationFile

[5] U. Grottker, M. Esche und M. Elfroth, „PTB-Mitteilungen 125 (2015), Heft 3. PTB-Anforderungen 50.8 an BSI-zertifizierte Smart Meter Gateways,“ Oktober 2015. [Online]. Available: https://oar.ptb.de/resources/show/10.7795/310.20150304

[6] Bundesnetzagentur, „Messstellenbetreiber (grundzuständiger),“ [Online]. Available: https://www.bundesnetzagentur.de/SharedDocs/A_Z_Glossar/M/Messstellenbetreiber_grundzustaendig.html

[7] VOLTARIS GmbH, „Resiliente Polynetze. Ein innovatives Mess- und Steuerkonzept liefert im Bundesforschungsprojekt PolyEnergyNet wichtige Grundlagen für den robusten Netzbetrieb,“ Juni 2017. [Online]. Available: https://voltaris.de/wp-content/uploads/2017/10/502_6-17_VOLTARIS.pdf

[8] Bundesministerium für Wirtschaft und Klimaschutz, „Gesetzlicher Rolloutfahrplan,“ [Online]. Available: https://www.bmwk.de/Redaktion/DE/Downloads/S-T/230111_ueberblick-smart-meter-rollout.pdf?__blob=publicationFile&v=1

[9] BDEW Bundesverband der Energie- und Wasserwirtschaft e.V., „Das Messstellenbetriebsgesetz 2016,“ 14. Oktober 2019. [Online]. Available: https://www.bdew.de/media/documents/Awh_20191014_MsbG-5Auflage-Kapitel-1-7.pdf

[10] Bundesnetzagentur, „Messeinrichtungen / Zähler - Kosten / Leistungen,“ [Online]. Available: https://www.bundesnetzagentur.de/DE/Vportal/Energie/Metering/Kosten_table.html

[11] Bundesnetzagentur, „Messeinrichtungen / Intelligente Messsysteme,“ [Online]. Available: https://www.bundesnetzagentur.de/DE/Vportal/Energie/Metering/start.html#:~:text=Muss%20ich%20den%20Strom%20bezahlen,darf%20daher%20nicht%20abgerechnet%20

[12] it-zeugs.de, „Was ist das ISO/OSI Modell?“ 13. März 2019. [Online]. Available: https://www.it-zeugs.de/was-ist-das-iso-osi-modell.html

[13] R. Prof. Dr.-Ing. Bermbach, „Forschungsbericht "Sicherheit im Smart Grid – Anforderungen an das Smart Metering Gateway"," [Online]. Available: https://www.ostfalia.de/cms/de/pws/bermbach/.content/documents/Forschungsbericht-WF-4_WS13_Be.pdf

[14] Discovergy GmbH, „Was sind die Tarifanwendungsfälle eines intelligenten Messsystems?,“ 21. Januar 2022. [Online]. Available: https://discovergy.com/blog/tarifanwendungsfaelle

[15] Forschungsstelle für Energiewirtschaft (FfE), „Messen und Steuern über iMSys – Funktioniert das?,“ 22. Mai 2019. [Online]. Available: https://www.ffe.de/veroeffentlichungen/messen-und-steuern-ueber-imsys-funktioniert-das/

[16] Bundesamt für Sicherheit in der Informationstechnik (BSI), „Das Smart-Meter-Gateway. Cyber-Sicherheit für die Digitalisierung der Energiewirtschaft,“ 23. Mai 2022. [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Smart-Meter-Gateway.pdf?__blob=publicationFile&v=6

[17] Bundesamt für Sicherheit in der Informationstechnik, „Schutzprofile nach Common Criteria (CC) für IT-Produkte,“ [Online]. Available: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Zertifizierung-und-Anerkennung/Zertifizierung-von-Produkten/Zertifizierung-nach-CC/Schutzprofile-Protection-Profiles-PP/schutzprofile-protection-profiles-pp_node

[18] Bundesamt für Sicherheit in der Informationstechnik, „Übersicht Schutzprofile und Technische Richtlinien,“ [Online]. Available: https://www.bsi.bund.de/dok/smartmeter-pp-tr

[19] Bundesamt für Sicherheit in der Informationstechnik (BSI), „BSI-Standards,“ Oktober 2017. [Online]. Available: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/BSI-Standards/bsi-standards_node.html

[20] Bundesamt für Sicherheit in der Informationstechnik, „Leitfaden zur Basis-Absicherung nach IT-Grundschutz: In drei Schritten zur Informationssicherheit,“ 20. Oktober 2017. [Online]. Available: https://www.bsi.bund.de/dok/10051454

[21] Bundesamt für Sicherheit in der Informationstechnik (BSI), „Schutzprofil für das Sicherheitsmodul eines Smart Meter Gateways (BSI-CC-PP-0077),“ [Online]. Available: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Smart-metering/Sicherheitsmodul/Schutzprofil/schutzprofil.html

[22] Bundesamt für Sicherheit in der Informationstechnik, „Protection Profile for the Security Module of a Smart Meter - Mini-HSM (Mini-HSM Security Module PP),“ 23. Juni 2017. [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Reporte/ReportePP/pp0095b_pdf.pdf?__blob=publicationFile&v=1#download=1

[23] Bundesamt für Sicherheit in der Informationstechnik (BSI), „Technische Richtlinie BSI TR-03109,“ 22.

September 2021. [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03109/TR03109.pdf?__blob=publicationFile&v=3

[24] IBM, „Was ist Ende-zu-Ende-Verschlüsselung?," [Online]. Available: https://www.ibm.com/de-de/topics/end-to-end-encryption

[25] Digitale Marktkommunikation für das Energiesystem der Zukunft, August 2021. [Online]. Available: https://www.dena.de/fileadmin/dena/Publikationen/PDFs/2021/dena_BR_Future_Energy_Lab_Gutachten_Digitale_Marktkommunikation_WEB.pdf

[26] Power Plus Communications AG (PPC), „Bürokratieabbau im Smart Meter Rollout und Wegfall der Januarspitze," 08 09 2023. [Online]. Available: https://www.ppc-ag.de/de/blog/buerokratieabbau-im-smart-meter-rollout-und-wegfall-der-januarspitze/

[27] D. H. Többen, „Eichrechtliche Anforderungen an Smart Meter Gateways - PTB-A 50.8 -," 27 November 2013. [Online]. Available: https://www.ptb.de/cms/fileadmin/internet/fachabteilungen/abteilung_9/9.2_gesetzliches_messwesen_und_konformitaetsbewertung/9.21/VV-2013/4_Toebben.pdf

[28] Smart Grids-Plattform Baden-Württemberg e.V., „Smart Meter Rollout in Deutschland – ein juristischer Rück- und Ausblick," 10. August 2021. [Online]. Available: https://smartgrids-bw.net/public/uploads/2021/08/SmartMeterRollout_Essay_final.pdf

[29] C. Jäger, „Submetering: Mit weniger Aufwand zur genauen Energieabrechnung," 19. November 2020. [Online]. Available: https://energie-digitalisieren.de/knowhow/submetering-mit-weniger-aufwand-zur-genauen-energieabrechnung/

[30] Umwelt Bundesamt, „Was ist ein "Smart-Grid"?," 03. August 2013. [Online]. Available: https://www.umweltbundesamt.de/service/uba-fragen/was-ist-ein-smart-grid

[31] Deutsche Energie-Agentur (dena), „Digitale Marktkommunikation für das Energiesystem der Zukunft," April 2021. [Online]. Available: https://www.dena.de/fileadmin/dena/Publikationen/PDFs/2021/dena_BR_Future_Energy_Lab_Gutachten_Digitale_Marktkommunikation_WEB.pdf

[32] Forschungsstelle für Energiewirtschaft (FfE), „Interoperabilität: Begriffsklärung, Bewertung und Anwendung," 16. November 2022. [Online]. Available: https://www.ffe.de/veroeffentlichungen/interoperabilitaet-begriffsklaerung-bewertung-und-anwendung/

[33] IT-SERVICE.NETWORK, „Was ist ein Proxy?," [Online]. Available: https://it-service.network/it-lexikon/proxy

[34] Bundesamt für Sicherheit in der Informationstechnik, „Public Key Infrastrukturen (PKIen)," [Online]. Available: https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Elektronische-Identitaeten/Public-Key-Infrastrukturen/public-key-infrastrukturen.html

[35] Datacenter Insider, „Was ist ein Software-Stack?,“ [Online]. Available: https://www.datacenter-insider.de/was-ist-ein-software-stack-a-841053/

Abbildungsverzeichnis

Tabellenverzeichnis

Glossar

Begriff	Definition
Authentizität	Die Echtheit bzw. Vertrauenswürdigkeit von Daten eines Systems. Daten gelten als authentisch, wenn sie einem Teilnehmer des Systems direkt oder verschlüsselt zugeordnet werden können und die eindeutige Identifikation dieses Teilnehmers sichergestellt werden kann. [31]
Ende-zu-Ende-Verschlüsselung	Ein sicheres Kommunikationsverfahren, das verhindert, dass Dritte auf die von einem Endpunkt zu einem anderen Endpunkt übertragenen Daten zugreifen können. [24]
Integrität	Die Eigenschaft, dass Daten in einem System nicht unbemerkt hinzugefügt, verändert oder gelöscht werden können. Damit gewährleistet Integrität die Korrektheit und Unversehrtheit von Daten, wobei die Teilnehmer eines Systems den jeweils aktuellen Status der betroffenen Daten einsehen können, ohne der Gefahr einer ungewollten Manipulation der Daten ausgesetzt zu sein. [31]
Interoperabilität	Die Fähigkeit von zwei oder mehr Systemen oder Komponenten, Informationen auszutauschen und die ausgetauschten Informationen zu nutzen. Die Funktionsfähigkeit muss auch bei keiner oder geringer Kenntnis über die besonderen Merkmale der einzelnen Einheiten gewährleistet sein. [32]
Proxy	Ein Proxy ist ein sogenannter „Vermittler“ innerhalb eines Netzwerks. Verläuft die Kommunikation in einem Netzwerk über einen solchen „Vermittler“, kann sie sicherer gemacht oder beschleunigt werden. [33]
Public Key Infrastructure (PKI)	Eine Public Key Infrastructure (Infrastruktur für öffentliche Schlüssel) macht eine vertrauenswürdige verschlüsselte Kommunikation zwischen zwei Einheiten möglich. Sie kann digitale Zertifikate ausstellen, verteilen und prüfen. Dadurch kann die PKI die Vertrauenswürdigkeit öffentlicher Schlüssel für die Entschlüsselung sicherstellen. Eine anschauliche Erläuterung findet sich auf der Seite des BSI. [34]
Softwarestack	Ein hierarchischer Stapel von aufeinander aufbauenden Softwarepaketen. Zusammengenommen ergeben sie eine Plattform und arbeiten zusammen, um die gemeinsamen Aufgaben zu erfüllen. [35]
Verfügbarkeit	Die Robustheit eines Systems gegen Missbrauch oder Eingriffe von außen. Ein System gilt als robust, wenn Angriffe nicht zu Ausfällen des gesamten oder zumindest von Teilen des Systems führen und somit die hinterlegten Daten jederzeit verfügbar sind. [31]

www.dena.de www.set-hub.de