

Future Energy
Lab

BERICHT

Digitale Identitäten im Energiesektor

Ein Beitrag für eine zukunftsgerichtete
Dateninfrastruktur

Ein Projekt der

dena

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
futureenergylab@dena.de

Internet:

www.dena.de

Autorinnen und Autoren:

Matthias Babel, Fraunhofer FIT
Felix Paetzold, Fraunhofer FIT
Tobias Ströher, Fraunhofer FIT
Prof. Dr. Jens Strüker, Fraunhofer FIT
Linda Babilon, dena
Irene Adamski, dena
Moritz Schlösser, dena
Philipp Richard, dena

Konzeption und Gestaltung:

die wegmeister gmbh

Stand:

Juli 2025

Alle Rechte sind vorbehalten. Die Nutzung steht unter dem Zustimmungsvorbehalt der dena.

Bitte zitieren als:

Deutsche Energie-Agentur (Hrsg.) (dena, 2025): Digitale Identitäten im Energiesektor. Ein Beitrag für eine zukunftsgerichtete Dateninfrastruktur

DIVE – Digitale Identitäten als Vertrauensanker im Energiesystem

- 01 – Überblick, Einordnung und Evaluation
- 02 – Technische Details und Umsetzung der Basisinfrastruktur
- 03 – Mehrwerte für die energiewirtschaftlichen Anwendungsfälle
- 04 – Rechtliche Analyse



Bundesministerium
für Wirtschaft
und Energie

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

Vorwort

Für viele Leser dürfte der Begriff „Energiewende“ ein Wort sein, das sie seit vielen Jahren oder schon Jahrzehnten begleitet. Die Wende geht voran – mit 59 Prozent erneuerbaren Energien im deutschen Strommix 2024. Sie wird aber auch mit immer größerer Dringlichkeit gebraucht. Für Kenner ist dabei klar, dass der Aufbau erneuerbarer Erzeugungskapazitäten und mehr Energieeffizienz nur einen Teil des Aufgabenpakets der Energiewende bilden: Die Herausforderung besteht jetzt vor allem darin, das Energiesystem aus dezentralen Erzeugern, flexiblen und neuen Verbrauchern sowie vielen unterschiedlichen Akteuren effizient zu beobachten, zu koordinieren und zu steuern.

In Zukunft müssen wir verstärkt auf Automatisierung durch den Einsatz digitaler Technologien setzen, um diese komplexen Aufgaben zu meistern und auch kleine Anlagen in die erforderlichen Flexibilitätslösungen und Nachweissysteme zu integrieren. Das bedeutet, wir müssen Prozesse Ende-zu-Ende digital und ohne Medienbrüche umsetzen – von den Anlagen und Geräten im Energiesystem bis in die Anwendungen hinein. Bricht man diese Anforderung auf ihre Grundbausteine herunter, wird klar: Eine hohe Datenqualität – also vollständige, aktuelle, integre und verifizierbare Daten – sowie ein vertrauenswürdiger Datenaustausch werden zunehmend kritische Erfolgsfaktoren der Energiewende.

Hier leistet das Projekt „DIVE – Digitale Identitäten als Vertrauensanker im Energiesystem“ einen innovativen Beitrag: Ein bisher zu wenig bedachtes Werkzeug der Energiewende, um Daten anlagenscharf und automatisiert für kurze Zeiträume erheben, verwalten und zur Verfügung stellen zu können, sind **digitale Identitäten für Anlagen und Geräte**. Sie können helfen, das lange bestehende Daten-Dunkelfeld im Energiesystem aufzulösen. Netzbetreiber erhalten Klarheit über die verfügbaren Anlagen und müssen sich weniger gegen Fehlangaben absichern, Verbraucher können individuell über die Verwendung der Daten ihrer Geräte entscheiden und die insgesamt sinkenden Verwaltungskosten können perspektivisch die gesamte Volkswirtschaft entlasten.

Die dezentralen technischen Lösungskonzepte – Basisinfrastruktur genannt –, die in diesem Vorhaben entwickelt wurden, setzen dabei stark auf einen sicheren Umgang mit den Daten, Datensparsamkeit und die Datensouveränität der Anlagenbesitzer. Sektorenübergreifende Interoperabilität und Anwendungsoffenheit sind weitere Merkmale der hier eingesetzten digitalen Maschinen-Identitäten. Damit trägt das Projekt auch dazu bei, dass wir mehr branchenübergreifende Lösungen finden, die nicht nur die systemkritischen Anwendungen des Energiesystems umsetzen, sondern auch Offenheit für neue, datenbasierte Mehrwerte schaffen und perspektivisch eine Datenökonomie ermöglichen.

Im Praxischeck am Beispiel eines Einfamilienhauses mit Photovoltaik-Anlage, Heimspeicher und Heim-Energiemanagementsystem (HEMS) konnte sich der Lösungsansatz beweisen: Die Anlagen wurden mit digitalen Identitäten ausgestattet und die Registrierung in verschiedenen Datenbanken und Anwendungsfällen wurde erfolgreich durchgeführt.

Das Projekt DIVE weist einen möglichen Weg und zeigt bereits: Eine Ende-zu-Ende-Digitalisierung ist mittels digitaler Identitäten machbar und dabei mit relativ geringem Aufwand für Endverbraucher, Systemakteure und Infrastruktur verbunden. Entscheidend hierfür waren unter anderem die Fortschritte, die in den letzten Jahren im Bereich der **selbstsouveränen digitalen Identitäten (SSI)** erzielt wurden: Die Technologie hat den notwendigen Reifegrad erreicht und konnte sich beispielsweise in den Beratungen zur Novellierung der eIDAS-Verordnung gegenüber proprietären Plattformlösungen durchsetzen (Web3-Lösungen ersetzen das Web 2.0) und kommt nun schrittweise in die breite Anwendung, etwa durch die bald startende EUDI-Wallet. Digitale Identitäten werden also nach und nach Einzug in das öffentliche Leben und die öffentliche Verwaltung halten. Das DIVE-Projekt bietet hier als Vorreiter den Brückenschlag von der allgemeinen Verwaltung hin zu den besonderen Anforderungen der Energiebranche. Indem schon jetzt, vor der breiten Anwendung von digitalen Identitäten, Testumgebungen und Reallabore zur Verfügung stehen, hat die Branche die Möglichkeit, sich frühzeitig mit den kommenden Entwicklungen auseinanderzusetzen und sie im eigenen Interesse zu begleiten und zu gestalten.

Mit der vorliegenden **Berichtsreihe werden fachspezifisch Grundlagen, Konzepte und Erfahrungen zur Verfügung** gestellt: Das in diesem Bericht skizzierte „Zielbild 2034“ beschreibt allgemeinverständlich die Vision einer zukunftsgerichteten Dateninfrastruktur für das Energiesystem der Zukunft und die Herausforderungen, die dafür noch zu bewältigen sind. Die Publikation „DIVE 01 – Überblick, Einordnung und Evaluation“ charakterisiert die Identitätslücke und ordnet den Lösungsansatz des Projekts gegenüber den Anforderungen des Energiesystems an digitale Identitäten ein. Der Bericht „DIVE 02 – Technische Details und Umsetzung der Basisinfrastruktur“ skizziert die Architektur rund um HEMS, Anlage, Smart Meter Gateway (SMGW), Kommunikationskanäle, Register und Datendrehscheibe und stellt technische Details aus der Anwendung der digitalen Identitäten nach SSI-Standard bereit. In „DIVE 03 – Mehrwerte für die energiewirtschaftlichen Anwendungsfälle“ werden konkrete Umsetzungsbeispiele (etwa Anlagenregistrierung, Lieferantenwechsel an der E-Ladesäule, automatisierte Vermeidung von Doppelvermarktung) vorgestellt. „DIVE 04 – Rechtliche Analyse“ identifiziert Rollen und Aufgaben sowie Vertragsbeziehungen für ein schlüssiges Governance-Konzept, beleuchtet haftungsrechtliche Fragestellungen und beschreibt Lösungsansätze für verbleibende juristische Grauzonen.

In nächsten Schritten wird es darum gehen, im Dialog mit der Branche sinnvolle Governance-Strukturen zu erarbeiten und die notwendige Infrastruktur aufzubauen. Vom Prototyp ausgehend, sollte mittelfristig ein Branchenstandard gefunden und etabliert werden.

Wir als Future Energy Lab der Deutschen Energie-Agentur (dena) freuen uns, diesen Pfad im Austausch mit bestehenden und neuen Partnern und Stakeholdern weiterzuverfolgen.



Philipp Richard – Bereichsleiter Digitale Technologien & Start-up Ökosystem



Linda Babilon – Teamleiterin Digitale Technologien

Inhalt

Vorwort	3
Executive Summary	6
1. Motivation – Digitalisierung der Energiewirtschaft	8
2. Hintergründe – Der Energiesektor im Wandel	11
3. Ziel – Digitale Identitäten in der Energiewirtschaft	15
3.1 Blitzlichter – Ein Tag im Jahr 2034	16
3.2 Die digitale Identitätslücke	18
3.3 Digitale Identitäten für ein digitales Energiesystem	20
3.4 Anforderungen an digitale Identitäten	20
4. Ein Weg – Digitale Identitäten für das Energiesystem	24
Fazit – Vom Zielbild zur Umsetzung	27
Literaturverzeichnis	28
Abkürzungen	31

Executive Summary

Die Energiewende erfordert eine grundlegende Transformation des Stromsystems. Die Erzeugung von Strom verlagert sich zunehmend von konventionellen, mit fossilen Energieträgern betriebenen Großkraftwerken hin zu einer Vielzahl kleiner, dezentraler Erneuerbare-Energien-Anlagen wie Photovoltaik- und Windkraftanlagen. Gleichzeitig steigt der Stromverbrauch durch die fortschreitende Sektorenkopplung und die damit zunehmende Anzahl von Wärmepumpen und Elektrofahrzeugen massiv. Diese Anlagen müssen untereinander koordiniert werden, um die Transformation des Systems zukunftssicher und wirtschaftlich effizient zu gestalten. Parallel dazu gewinnt die Bilanzierung von Emissionen für Unternehmen durch regulatorische Vorgaben (z. B. die EU-Richtlinie zur Nachhaltigkeitsberichterstattung von Unternehmen (Corporate Sustainability Reporting Directive, CSRD)) sowie die Anforderungen von Investoren (z. B. Kriterien in Bezug auf die Environmental, Social and Corporate Governance) und Kunden (z. B. Berücksichtigung von Nachhaltigkeitsinformationen bei Konsumentenscheidungen) an Bedeutung. Vor diesem Hintergrund wird auch die präzise Nachweisbarkeit von Emissionsdaten in Unternehmen immer wichtiger. Angesichts dieser zunehmenden Komplexität des Energiesystems wird die Bedeutung einer umfassenden Digitalisierung offensichtlich: Eine zukunftsorientierte Dateninfrastruktur erlaubt nicht nur eine präzise und zuverlässige Kommunikation zwischen Anlagen, Betreibern und weiteren Akteuren, sondern ermöglicht auch die zuverlässige Erfassung von Emissionsdaten, um mehr Transparenz hinsichtlich der Herkunft des Stroms zu schaffen und steigende Anforderungen an die Nachhaltigkeitsberichterstattung zu erfüllen.

Die digitale Identitätslücke: ein zentrales Hindernis für die Energiewende

Trotz der offensichtlichen Vorteile einer umfassenden Digitalisierung weist das heutige Energiesystem in Deutschland signifikante Defizite in seiner digitalen Infrastruktur auf (Leinauer et al. 2024). Relevante Informationen über die Eigenschaften von Anlagen im Energiesystem, wie beispielsweise Art oder Standort, sind nur lückenhaft erfasst und nur eingeschränkt digital zugänglich. Dies führt zu manuellen und damit aufwendigen und fehleranfälligen Prozessen bei der Erfassung von Anlagenstammdaten und untergräbt das Vertrauen in diese Daten. Eine fehlende Interoperabilität und eine unzureichende Stakeholder-Orientierung führen dazu, dass vorhandene Daten mehrfach erhoben werden müssen, was innovative und sektorenübergreifende Anwendungsfälle behindert. Die wiederholte Erhebung derselben Daten resultiert zudem in mangelnder Skalierbarkeit: Mit einer steigenden Anzahl von Anlagen wächst der Aufwand der Datenerhebung exponentiell, insbesondere wenn dieselben Daten für verschiedene Zwecke – wie im Marktstammdatenregister und im Herkunftsnachweisregister – erhoben werden müssen. Darüber hinaus erschwert das Fehlen vertrauenswürdiger Stammdaten von Anlagen ihre effiziente Einbindung,

beispielsweise zur Flexibilitätserbringung. Diese verschiedenen Probleme charakterisieren die „**digitale Identitätslücke**“.

Digitale Maschinen-Identitäten: ein Baustein zur Schließung der digitalen Lücke

Aktuelle Bestrebungen zum Aufbau von digitalen Identitäten

Es gibt bereits mehrere Bestrebungen im nationalen, europäischen und internationalen Kontext, die digitale Identitäten im Energiesektor und darüber hinaus untersuchen. Ein Auszug relevanter Bestrebungen ist nachfolgend dargestellt.



Abbildung 1: Bestrebungen zum Aufbau von digitalen Identitäten

Ein fundamentaler Baustein zur Schließung dieser digitalen Identitätslücke sind digitale Maschinen-Identitäten. Insbesondere in einem zukünftigen Energiesystem mit einer hohen Anzahl an Stakeholdern bieten digitale Identitäten für Anlagen die notwendige Basis für eine Zusammenarbeit in diesem komplexen, dezentralen Umfeld. Es gibt bereits Pilotprojekte sowie regulatorische Bemühungen zur Etablierung und Harmonisierung von digitalen Identitäten für Personen und Organisationen, beispielsweise im Rahmen der Novellierung der EU-Verordnung über elektronische Identifizierung und Vertrauensdienste (eIDAS 2.0).

Digitale Identitäten für Maschinen können ebenfalls für vertrauenswürdige Interaktionen im digitalen Raum eingesetzt werden und einen sicheren Austausch von Daten gewährleisten (Babel et al. 2023). Wenn diese digitalen Identitäten von den

Anlagenbetreibern selbstbestimmt genutzt werden können, eröffnen sich vielfältige und bisher nicht realisierbare Anwendungen im Energiesystem durch die Förderung von offenen Identitätsökosystemen. Diese Ökosysteme können den Energiemarkt zunächst für weitere Anwendungsfälle und perspektivisch auch für weitere Sektoren öffnen. Darunter fällt beispielsweise eine aktive Beteiligung von privaten Kleinanlagen am Strommarkt über Aggregationsplattformen (dena 2023a; Körner et al. 2024). Auch können digitale Identitäten die Grundlage für feingranulare CO₂-Zertifikate bieten, indem sie eine eindeutige Zuordnung der Zertifikate zu den ausstellenden Anlagen ermöglichen (Babel et al. 2022) und somit die Basis für Nachhaltigkeitsinformationen schaffen.

Anforderungen an digitale Identitäten für Maschinen im Energiesystem

Damit digitale Identitäten die aufgezeigte Identitätslücke im Energiesystem schließen können, müssen sie die folgenden Anforderungen erfüllen:

- **Hohe Datenqualität:** Die Stammdaten der Maschinen sollten jederzeit richtig, aktuell und verifizierbar sein, um als vertrauenswürdige Basis für Transaktionen zu dienen. Um dies zu erreichen, sollten digitale Identitäten von vertrauenswürdigen Akteuren ausgestellt werden. Dies können Akteure sein, die bereits in der analogen Welt hohes Vertrauen genießen und im digitalen Raum als Qualitätsgarant auftreten.
- **Eindeutige Identifizierung:** Digitale Identitäten sollten eine eindeutige Zuordnung zu jedem Akteur und jeder Anlage oder Entität gewährleisten. Dies ermöglicht ein effizientes und sicheres Zusammenspiel im dezentralen Energiesystem. Durch eine eindeutige Identifizierung kann eine spezifische Ansteuerung erreicht und die Authentizität von Bewegungsdaten sichergestellt werden.

- **Sektorenübergreifende Interoperabilität:** Digitale Identitäten für Maschinen sollten über verschiedene Sektoren hinweg verwendbar sein, sodass dieselbe Identität für unterschiedliche Anwendungen verwendet werden kann. Die Schaffung eines solchen sektorenübergreifenden Identitätsökosystems ermöglicht Skaleneffekte und kann somit die Kosten der Infrastruktur auf eine Vielzahl verschiedener Anwendungsfälle verteilen. Dies setzt technische und semantische Interoperabilität sowie sektorenübergreifendes Vertrauen in die in der digitalen Identität enthaltenen Daten voraus.

- **Selbstbestimmtheit in der Nutzung:** Nutzer sollten autonom über die Freigabe und Verwendung der Identitätsdaten ihrer Anlagen entscheiden können, um so die Datensouveränität der verschiedenen Akteure zu wahren. Dabei sollten Datenschutzprinzipien wie „Privacy by Design“ integriert werden, um die Sicherheit und Vertraulichkeit der Nutzerdaten zu gewährleisten.

- **Konformität mit gesetzlichen Regularien:** Digitale Identitäten müssen den bestehenden Vorschriften und Datenschutzrichtlinien wie der Datenschutz-Grundverordnung (DSGVO) entsprechen. Als Kritische Infrastruktur nach dem IT-Sicherheitsgesetz erfordert die Energiedateninfrastruktur zudem umfangreiche Schutzmaßnahmen gegen physische und cyberspezifische Bedrohungen.

Die Umsetzung dieser Anforderungen ist entscheidend, um das Potenzial digitaler Identitäten zur Schließung der digitalen Lücke im Energiesystem auszuschöpfen und somit die Energiewende aktiv zu unterstützen.

1. Motivation – Digitalisierung der Energiewirtschaft

Im Zuge der Energiewende werden neben der Windkraft Millionen von Photovoltaik-Anlagen in Deutschland zu einer wesentlichen Säule der Energieerzeugung. Zugleich werden durch die Elektrifizierung der Sektoren Mobilität und Wärme Millionen von zusätzlichen dezentralen Stromverbrauchern Teil des Energiesystems. Die Komplexität erhöht sich dadurch beträchtlich. In die gleiche Richtung wirken die steigenden Anforderungen an Echtzeitdaten über die Herkunft sowie den Zeitpunkt der Erzeugung und den Verbrauch von Strom, die mit der CO₂-Bilanzierung in Unternehmen einhergehen. Treiber dieser Entwicklung sind unter anderem der EU Green Deal und regulatorische Vorgaben wie die EU-Richtlinie zur Nachhaltigkeitsberichterstattung von Unternehmen (Corporate Sustainability Reporting Directive, CSRD) oder die EU-Lieferkettenrichtlinie (Corporate Sustainability Due Diligence Directive, CSDDD) (Körner et al. 2023).

Um das Energiesystem auch bei diesem Ausmaß an Komplexität zukünftig effizient und sicher zu steuern, wird eine **digitale Kommunikation zwischen Anlagen und weiteren Akteuren** wie beispielsweise Netzbetreibern als unerlässlich angesehen (dena 2023b, 2024b). Manuelle Mechanismen können schlicht nicht gewährleisten, dass Millionen von Anlagen effizient und flexibel in verschiedene Anwendungsfälle, wie beispielsweise virtuelle Kraftwerke, im Energiesektor eingebunden werden. Eine zukunftssichere Energieversorgung kann nur gewährleistet werden, wenn die Anlagen mit ihren zugehörigen Daten lückenlos und in nahezu Echtzeit in eine digitale Dateninfrastruktur integriert sind. Dies umfasst sowohl Stammdaten, wie Art und Besitzer der Anlagen, als auch Bewegungsdaten, wie gemessene Erzeugungs- und Verbrauchsdaten (dena 2024b).

Stammdaten werden derzeit für die einzelnen Anwendungsfälle in separaten Registern verwaltet, beispielsweise im Marktstammdatenregister (MaStR) oder im Herkunftsnachweisregister (HKNR). Diese Register werden isoliert voneinander geführt, was zur Folge hat, dass jede einzelne Anlage für jeden Anwendungsfall separat in die Register eingetragen und aktualisiert werden muss. Darüber hinaus erfasst das Marktstammdatenregister aktuell weder kleine noch nicht ortsfeste Verbrauchsanlagen wie Elektroautos und private Wärmepumpen. Zusätzlich zu diesen Herausforderungen bei den Stammdaten gibt es auch Einschränkungen bei der sicheren Übermittlung und **Nutzung von Bewegungsdaten**. Die sich im Aufbau befindliche Smart-Meter-Gateway-Infrastruktur steht zurzeit nur für eine sehr begrenzte Anzahl von Anwendungsfällen, wie die Übertragung von Verbrauchsdaten zu Abrechnungszwecken, zur Verfügung (BSI 2023; Bundesnetzagentur 2024b). Diese Einschränkungen führen dazu, dass andere Anwendungsfälle, die verifizierbare Bewegungsdaten benötigen, nur unzureichend umgesetzt werden können. Weiterhin fehlt bisher eine Möglichkeit, Anlagen verifizierbar in die Smart-Meter-Gateway-Infrastruktur einzubinden (BSI 2024; VDE FFN 2024). So werden derzeit unter anderem nur erzeugungsseitige

Potenziale für den aktuellen Redispatch 2.0 genutzt, während ein ganzheitlicher Ansatz zur Nutzung lastseitiger Flexibilitäten noch nicht existiert (Bundesnetzagentur 2024a; dena 2024b). Angesichts der dargestellten Herausforderungen wird deutlich, dass die bestehende digitale Infrastruktur nicht zukunftssicher für die Transformation des Energiesystems hin zu einem auf erneuerbaren Energien basierendem System ist.

Aufgrund der beschriebenen Herausforderungen sind die Sicherstellung der **Korrektheit und Integrität der auszutauschenden Daten sowie ihre anwendungsübergreifende Verwendbarkeit** eine entscheidende Aufgabe der Digitalisierung des Energiesystems. Ein möglicher Ansatz zur Bewältigung der Herausforderungen bei der Bereitstellung von Stammdaten ist die Implementierung von digitalen Identitäten für Anlagen (Babel et al. 2023; Elia Group 2023). **Digitale Identitäten** können die Genauigkeit und Verfügbarkeit der relevanten Stammdaten von Anlagen erhöhen, als Vertrauensanker im Energiesystem fungieren und so als **sichere Referenzpunkte** im digitalen Umfeld dienen. Sie ermöglichen eine eindeutige Identifizierung und Authentifizierung von Anlagen und Akteuren und gewährleisten die Integrität und Authentizität der übertragenen Daten. Ein dezentraler Ansatz, bei dem die eigenen Identitätsdaten direkt bei der Anlage oder in einer Digital Wallet des Anlagenbetreibers sicher verwaltet und übermittelt werden, verspricht eine effiziente und sichere Integration der Anlagen in das Energiesystem (Elia Group 2023). Dies ermöglicht nicht nur die Erfassung, sondern auch einen effizienten Einsatz der Anlagen. Die exponentiell steigende Zahl neuer Energieanlagen könnte so effektiver integriert und verwaltet werden. Zudem ermöglicht der dezentrale Ansatz, dass die Stammdaten nicht in einer zentralen Datenbank gespeichert werden müssen. Dadurch bleibt die **digitale Souveränität des Anlagenbetreibers** gewahrt, da die Daten nur mit seiner aktiven Zustimmung weitergegeben werden können. Zudem bietet eine dezentrale Infrastruktur für potenzielle Cyberangriffe eine deutlich geringere Angriffsfläche als ein zentraler „Honeypot“.

Die technologische Umsetzung von digitalen Identitäten für Maschinen im Allgemeinen und im Energiesektor im Besonderen befindet sich jedoch noch im Anfangsstadium. Die Entwicklung von Standards, Protokollen und Sicherheitsmaßnahmen für eine breite und sichere Anwendung von Maschinen-Identitäten im Energiesektor bleibt eine zentrale Herausforderung, die bisher nur in beschränktem Maße adressiert wurde (dena 2023b). Es braucht nach den geleisteten Vorarbeiten nun Diskurs und größere Praxisprojekte wie Reallabore, um diese Aufgabe weiter anzugehen. Im Rahmen dieser Begleitstudie zum DIVE-Piloten wird anhand konkreter Blitzlichter die aktuelle Lücke zu einem digitalen Energiesystem im Energiesektor aufgezeigt. Darauf aufbauend wird diskutiert, inwiefern digitale Identitäten die bestehende digitale Identitätslücke schließen und was bei ihrer Ausgestaltung berücksichtigt werden sollte.

Die vorliegende Studie wurde im Rahmen des Forschungsprojekts DIVE (Digitale Identitäten als Vertrauensanker im Energiesystem) erstellt, das unmittelbar an den vom Future Energy Lab der dena geleiteten Piloten „Blockchain Machine Identity Ledger“ (BMIL) anschließt (dena 2023b). Aufbauend auf den technischen Erkenntnissen des BMIL-Projekts zur Machbarkeit digitaler Identitäten, entwickelte und testete ein Konsortium aus sechs Industrie- und Forschungspartnern spezifische

Anwendungsfälle an realen Energieanlagen. Ziel und Ergebnis des Projekts DIVE war es, diese Anlagen mit digitalen Identitäten auszustatten, um zukünftig schnell und flexibel zwischen verschiedenen Anwendungen wechseln zu können, dadurch innovative und zukunftsorientierte Anwendungen zu ermöglichen und zugleich die Souveränität der Marktteilnehmer zu gewährleisten (dena 2023a).

2. Hintergründe – Der Energiesektor im Wandel

Die Elektrifizierung von Sektoren mit hohem Verbrauch an fossilen Energieträgern wie Wärme und Verkehr ist notwendiger Baustein zur Dekarbonisierung des Energiesystems. Allerdings trägt diese Elektrifizierung nur dann zur Dekarbonisierung dieser Sektoren bei, wenn gleichzeitig ein hoher Anteil der Stromerzeugung aus erneuerbaren Energien erfolgt (Papadis und Tsatsaronis 2020). Mechanismen, die eine klare und messbare Differenzierung zwischen Strom aus verschiedenen Quellen ermöglichen, können dazu beitragen, die Durchdringung der erneuerbaren Stromerzeugung weiter voranzutreiben (Babel et al. 2022; Körner et al. 2023). So können beispielsweise Unternehmen im Rahmen ihrer Nachhaltigkeitsberichterstattung aufzeigen, dass sie grünen Strom bezogen haben, wodurch die direkte Nachfrage nach erneuerbaren Energien gesteigert wird. Strom hat jedoch einige spezifische Eigenschaften, die diese Differenzierung erschweren: Er wird aktuell als ein homogenes Gut behandelt, das nach der Einspeisung ins Netz physisch nicht mehr unterschieden und zurückverfolgt werden kann. Diese und weitere Besonderheiten der Stromwertschöpfungskette, wie insbesondere die Trennung von physischem und bilanziellem Strom, werden im Folgenden detailliert erläutert, um die komplexe Dynamik der modernen Energieversorgung und ihre Herausforderungen an eine digitale Energiedateninfrastruktur zu verdeutlichen.

Die Wertschöpfungskette von Strom

Um die Zusammenhänge der Wertschöpfungskette zu verdeutlichen, werden im Folgenden ihre grundlegenden Aspekte beschrieben. Die Wertschöpfungskette von Strom besteht aus Erzeugung, Transport, Handel und Speicherung sowie Verteilung und Belieferung der Verbraucher (Graebig et al. 2023).

Bei der **Erzeugung** von Strom wird unterschieden zwischen konventionellen und regenerativen Anlagen. Konventionelle Anlagen, die auf fossilen Energieträgern wie Gas, Kohle oder Kernkraft basieren, weisen in der Regel eine hohe Erzeugungskapazität auf und sind an höhere Spannungsebenen angeschlossen. Regenerative Anlagen, zu denen vor allem Wasser-, Wind-, Solar-, Geothermie- und Biomassekraftwerke gehören, sind dagegen meist kleiner und auf niedrigeren Spannungsebenen angeschlossen. Sie sind dezentral verteilt mit einer Konzentration an Standorten mit hoher Verfügbarkeit erneuerbarer Energien (z. B. Küstenregionen bei der Windenergie). Zudem unterliegen regenerative Anlagen einer stärkeren Volatilität bei der Stromproduktion. Um die Vielzahl dezentraler Anlagen effektiv zu erfassen, hat die Bundesnetzagentur (BNetzA) das zentrale und öffentliche Marktstammdatenregister (MaStR) eingeführt. Es zielt darauf ab, mehrere bislang separat geführte Register zu konsolidieren, damit die Datenqualität zu erhöhen und gleichzeitig den bürokratischen Aufwand zu verringern (Bundesnetzagentur 2024b). Betreiber von Erzeugungsanlagen (sowie großer Verbrauchsanlagen) müssen diese Anlagen im MaStR registrieren.¹ Netzbetreiber überprüfen und validieren die Angaben zu Anlagen und Betreibern in ihrem Gebiet. Das MaStR umfasst dabei ausschließlich Stammdaten der Anlage wie Betreiber, Ort und Leistungswerte

und erfasst keine sogenannten Bewegungsdaten wie Produktionsmengen oder Speicherfüllstände (Bundesnetzagentur 2024b).

Der **Transport** des erzeugten Stroms über große Entfernungen erfolgt über Höchst- und Hochspannungsnetze durch Übertragungsnetzbetreiber. Die lokale Verteilung an die Kunden geschieht typischerweise auf der Mittel- und Niederspannungsebene durch Verteilnetzbetreiber. Stromnetze stellen ein reguliertes Monopol der Netzbetreiber dar und werden in Deutschland durch die BNetzA beaufsichtigt und reguliert (Graebig et al. 2023).

Handel und Speicherung umfassen den Kauf und Verkauf von Strom. Energie kann an Börsen (z. B. European Energy Exchange, EEX) oder am OTC-Markt (Over the Counter) gehandelt werden. Aktuell spielen Speicher im Stromsektor noch eine untergeordnete Rolle, werden mit der fortschreitenden Energiewende aber zunehmend an Bedeutung gewinnen. Diese besondere Stellung kommt auch in der Regelung von § 11c Energiewirtschaftsgesetz (EnWG) zum Ausdruck, wonach die Errichtung und der Betrieb von Anlagen zur Speicherung elektrischer Energie im überwiegenden öffentlichen Interesse liegen.

Stromlieferanten sind für die kaufmännische und vertragliche **Belieferung** mit Strom zuständig. Kunden können ihren Energielieferanten selbst wählen (Graebig et al. 2023). Einbau, Betrieb und Wartung von Messeinrichtungen und -systemen, die Messung des Stromverbrauchs sowie die Übertragung der entsprechenden Daten an Stakeholder wie Netzbetreiber fallen in den Aufgabenbereich des Messstellenbetreibers.² Derzeit erfolgt in Deutschland der sogenannte Rollout von intelligenten Messsystemen (sogenannte Smart Meter)³, unter anderem mit dem Ziel, detaillierte Daten über den Verbrauch zu erfassen. Bislang manuelle Prozesse wie das Ablesen von Verbrauchsdaten können zukünftig digital durchgeführt und mittels einer Kommunikationseinheit, des sogenannten Smart Meter Gateway (SMGW), in kurzen Zeitintervallen (z. B. 15 Minuten) an den Messstellenbetreiber übertragen werden. Dieser wiederum leitet die Daten je nach Anwendungsfall an weitere Akteure weiter. Dies können beispielsweise Energielieferanten sein, die die Daten für Abrechnungszwecke benötigen. Diese feingranularen Bewegungsdaten sollen zukünftig für neue Anwendungsfälle, wie die flexible Anpassung von Erzeugung und Verbrauch, verwendet werden (dena 2024c).

Steigende Komplexitäten in der Wertschöpfungskette

Die Komplexität der Stromwertschöpfungskette mit ihrer Vielzahl an unterschiedlichen Akteuren unterstreicht die Bedeutung von standardisierten Koordinations- und Kommunikationsverfahren. Seit der Liberalisierung des europäischen Energiemarktes wird das „Harmonised Electricity Market Role Model“ (ENTSO-E, EFET, ebIX 2022) kontinuierlich weiterentwickelt, um die Koordination zwischen den Marktteilnehmern der

1 Vgl. Marktstammdatenregisterverordnung: § 3 MaStRV (Registrierung von Marktakteuren)

2 Vgl. Messstellenbetriebsgesetz: § 3 (2) MsbG

3 Im Gesetz zum Neustart der Digitalisierung der Energiewende wurde die weitere Beschleunigung des Rollouts von intelligenten Messsystemen priorisiert.

Energiewirtschaft zu verbessern. Mit dem Marktrollenmodell, das in Deutschland vom Bundesverband der Energie- und Wasserwirtschaft (BDEW) definiert wird, soll jede Verantwortung und Aufgabe in der Marktkommunikation genau einer Rolle zugeordnet werden, um Marktprozesse und ausgetauschte Daten präzise zu definieren und anzuwenden (BDEW 2023). Zudem beeinflussen behördliche Vorschriften, einschließlich der Festlegungen der Bundesnetzagentur, die Umsetzung von energiewirtschaftlichen Anforderungen. Zur Verbesserung der digitalen Marktkommunikation wurde beispielsweise im Jahr 2024 mit einer Festlegung der BNetzA⁴ eine Umstellung des Übertragungsweges vom vorherigen Standard (E-Mail via SMTP (Simple Mail Transfer Protocol) und AS2 (Applicability Statement 2)) auf AS4 beschlossen, was die Effizienz und Sicherheit der Datenübertragung erhöht. Darüber hinaus wurde die Nutzung der Smart Meter Public Key Infrastructure (SM-PKI) entsprechend den kryptografischen Vorgaben des Bundesamtes für Sicherheit in der Informationstechnik (BSI) für die sichere Kommunikation vorgeschrieben (BDEW 2024).

Sektorenkopplung

Sektorenkopplung bezeichnet die systematische Verknüpfung verschiedener Energiesektoren wie Strom, Wärme, Verkehr und Industrie, um die Energieeffizienz zu steigern und den Einsatz erneuerbarer Energien zu maximieren (Wietschel et al. 2018). Durch die Kopplung mehrerer Sektoren können Angebot und Nachfrage gemeinsam betrachtet werden. So kann beispielsweise überschüssiger Strom aus Windkraft in anderen Sektoren wie Mobilität effizient genutzt werden. Umgekehrt kann der Stromverbrauch zu Zeiten, in denen nicht genügend erneuerbare Energie zur Verfügung steht, sektorenübergreifend reduziert werden. Die Sektorenkopplung von Mobilität und Strom ermöglicht es zum Beispiel, Verkehrsemissionen durch den Umstieg von Verbrennungs- auf Elektromotoren zu reduzieren und perspektivisch mit Elektrofahrzeugen, die bidirektionales Laden unterstützen, dezentrale Speicher für (erneuerbaren) Strom bereitzustellen.

Mit der Energiewende verändert sich diese bestehende Wertschöpfungskette grundlegend (dena 2023a). Neue technologische Ansätze wie Speicher und digitale Aggregatoren ermöglichen neue Geschäfts- und Betriebsmodelle (Körner et al. 2024). So kann beispielsweise durch die koordinierte Steuerung mehrerer Anlagen ein virtuelles Kraftwerk gebildet werden, das flexibel auf Stromnachfrage und -produktion reagiert und so zur Stabilisierung des Netzes beiträgt (dena 2024a). Diese Entwicklungen fördern die Entstehung sogenannter Prosumer (von engl. „producer“ und „consumer“, also Verbraucher, die zeitweise auch als Erzeuger fungieren) und führen zu einem bidirektionalen Stromfluss, insbesondere in Verteilnetzen (Graebig et al. 2023). Diese Veränderung in der Wertschöpfungskette erfordert eine grundlegende Anpassung der bisherigen Marktrollen und der Marktkommunikation. Die bisher im Energiesystem vorhandene klare Trennung zwischen Stromerzeugern und -verbrauchern muss aktualisiert werden, um neue Konzepte wie Energiegemeinschaften

sowie virtuelle Kraftwerke abzubilden und in der Praxis umzusetzen (dena 2024a; Bogensperger und Regener 2023).

Aktuelle Digitalisierungsbemühungen in Deutschland und der EU

Um die Energiewende erfolgreich gestalten zu können, wird die Digitalisierung des Energiesektors in Deutschland und der EU durch eine Reihe von zentralen Gesetzen, Verordnungen und Richtlinien vorangetrieben. Sie bilden zusammen mit Programmen und Initiativen wie dem *Digital Europe Programme* und *Horizon Europe* sowie generellen Bestimmungen wie der Datenschutz-Grundverordnung (DSGVO) den regulatorischen und strategischen Rahmen für die zukünftige Gestaltung des Energiesektors. Die Ziele dieser Bemühungen sind es, den technologischen Fortschritt und die Vorteile der Digitalisierung zu nutzen, die individuelle digitale Souveränität natürlicher und rechtlicher Personen zu wahren, die wachsende Zahl dezentraler Anlagen effizient zu integrieren und damit die Klimaziele – Treibhausgasneutralität bis 2045 gemäß dem Deutschen Klimaschutzgesetz und bis 2050 gemäß dem EU Green Deal – zu erreichen.

Die Priorität, die die Europäische Union (EU) der Digitalisierung im Strommarkt einräumt, spiegelt sich in mehreren Strommarkt-reformen wider. So wurden beispielsweise im Paket *Saubere Energie für alle Europäer* (2016) eine Reihe von Verordnungen und Richtlinien verabschiedet, die unter anderem darauf abzielen, den europäischen Strommarkt integrativer zu gestalten, den Wettbewerb zu fördern und die Verbraucherrechte zu stärken. Die *Richtlinie (EU) 2019/944* legt den Rechtsrahmen für den Elektrizitätsbinnenmarkt fest, einschließlich Regelungen zur Förderung von Smart Grids und Smart Metering. Endkunden sollen beispielsweise zeitnahen und kostenlosen Zugang zu ihren Verbrauchsdaten erhalten, um ihren eigenen Stromverbrauch nachhaltiger zu gestalten. Im Jahr 2024 wurde mit der *Richtlinie (EU) 2024/1711* der Elektrizitätsbinnenmarkt aktualisiert und eine aktive Rolle für die Endkunden eingeführt, um ihre Möglichkeiten zur Teilnahme am und Einflussnahme auf den Strommarkt zu stärken. Zudem werden unter anderem die Übertragungsnetzbetreiber in die Verantwortung genommen, ihre Netze zu digitalisieren. Ergänzend enthält die *Verordnung (EU) 2019/943* spezifische Bestimmungen zur Netzstabilität und zur Integration erneuerbarer Energien. Dafür verpflichtet sie unter anderem den Europäischen Verband der Übertragungsnetzbetreiber *ENTSO-E* zur Digitalisierung der Übertragungsnetze und die Europäische Organisation für Verteilnetzbetreiber *EU-DSO Entity* zur Digitalisierung der Verteilnetze. Die *Verordnung (EU) 2018/1999* über das Governance-System für die Energieunion und für den Klimaschutz legt den Rahmen für die strategische Planung und Berichterstattung der Mitgliedstaaten im Bereich Energie und Klimaschutz fest und betont dabei die Bedeutung der Digitalisierung. Die *Richtlinie (EU) 2023/2413* (RED III) unterstützt die Digitalisierung durch die Förderung von Technologien, die eine bessere Integration erneuerbarer Energien ermöglichen. Dazu gehört beispielsweise das Ziel, die Ausstellung von feingranularen,

⁴ BK6-21-282 Festlegung zur künftigen Absicherung der elektronischen Marktkommunikation Strom

verifizierbaren Herkunftsnachweisen in nahezu Echtzeit zu ermöglichen. Die Umsetzung solcher Ideen und Projekte zur Entwicklung neuer Technologien und Konzepte wird durch zahlreiche Forschungs- und Innovationsprogramme im Energiebereich unterstützt.

In Deutschland forciert das *Erneuerbare-Energien-Gesetz* (EEG) die Förderung erneuerbarer Energien und enthält dabei Regelungen zur Digitalisierung des Energiesektors, insbesondere in Bezug auf die Integration erneuerbarer Energien in das Stromnetz und die Steuerung dezentraler Erzeugungseinheiten. Das *Gesetz zur Digitalisierung der Energiewende* (GDEW) bildet auf nationaler Ebene den rechtlichen Rahmen für die Einführung von Smart Metern und die Digitalisierung der Stromnetze. Es enthält unter anderem das *Messstellenbetriebsgesetz* (MsbG), das festlegt, wie der Betrieb der Smart Meter organisiert wird. Es regelt die Rechte und Pflichten der Messstellenbetreiber und schafft einen Rahmen für die Marktöffnung in diesem Bereich. Die Einführung von zertifizierten modernen Messeinrichtungen und Smart Meter Gateways in der Energiewirtschaft ist ein wesentlicher Schritt zur Digitalisierung des deutschen Energiesystems. Sie erlaubt die präzise Erfassung und Übermittlung von Netzzustandsdaten, was zu einer höheren Transparenz bei den Leistungsflüssen im Verteilnetz führt. Steuerbare Verbrauchseinrichtungen, Stromspeicher und dezentrale Erzeugungsanlagen können in Zukunft über ein Smart Meter Gateway angesteuert und somit netz- und marktdienlich eingesetzt werden (BSI 2023).

Die europäische Datenstrategie

Über die spezifischen Maßnahmen zur Digitalisierung des Energiesystems hinaus verfolgt die EU das strategische Ziel, die digitale Souveränität ihrer Bürgerinnen und Bürger sowie der Unternehmen zu stärken. Der kürzlich verabschiedete *Data Act* verbessert den Zugang zu und die Nutzung von Daten, unabhängig von ihrem Speicher- oder Verarbeitungsort. Dies schließt Regelungen zum Datenaustausch, zur Datensicherheit und zum Datenschutz ein, die darauf abzielen, Nutzern eine verstärkte Kontrolle über ihre persönlichen Daten zu ermöglichen. Parallel dazu fokussiert der *Digital Markets Act* (DMA) auf die Regulierung von Online-Plattformen und „Gatekeepern“, um faire Wettbewerbsbedingungen in digitalen Märkten zu schaffen, mit Vorschriften zur Interoperabilität und Transparenz von Algorithmen sowie zur Portabilität zwischen verschiedenen Diensten. Ein zentrales Element der europäischen Datenstrategie ist die Schaffung von Datenräumen (*Data Spaces*), in denen Organisationen und Einzelpersonen über digitale Infrastrukturen zusammenarbeiten, um Daten gemeinsam zu nutzen und zu analysieren, wobei stets der Datenschutz und die Kontrolle über die eigenen Daten gewährleistet sind. Besonders im Energiesektor wird das Potenzial von Energiedatenräumen hervorgehoben, unterstützt durch EU-weite Initiativen und nationale Projekte wie *energy data-X⁵*, das vom Bundesministerium für Wirtschaft und Energie (BMWi) gefördert wird.

3. Ziel – Digitale Identitäten in der Energiewirtschaft

Dieses Kapitel zeigt, wie digitale Identitäten dazu beitragen können, die bestehende digitale Identitätslücke im Energiesystem zu schließen. Zunächst wird anhand konkreter Szenarien für das Jahr 2034 dargestellt, wie digitale Identitäten die Energiewende

unterstützen können. Anschließend wird die derzeit bestehende digitale Identitätslücke aufgezeigt. Abschließend widmen wir uns den notwendigen Anforderungen an digitale Identitäten, um diese Identitätslücke schließlich erfolgreich zu schließen.

3.1 Blitzlichter – Ein Tag im Jahr 2034

Blitzlicht 1: Grünstahl GmbH

Die deutsche Grünstahl GmbH produziert Stahl im wasserstoffbasierten Direktreduktionsverfahren. Die umfangreichen Investitionen in diese umweltfreundliche Produktionsmethode während der vergangenen Jahre ermöglichen es dem Unternehmen heute, besonders emissionsarm zu produzieren. Die Grünstahl GmbH hatte sich im Vergleich zu vielen Wettbewerbern frühzeitig für diesen Wechsel entschieden. Ausgangspunkt waren sowohl die gestiegenen regulatorischen Anforderungen und CO₂-Preise als auch die zunehmenden Erwartungen von Kunden und Investoren hinsichtlich der Überprüfbarkeit der Emissionsreduktion.

Im Mittelpunkt stand zunächst die Einführung eines umfassenden CO₂-Monitorings und -Managements. Dies hat der Grünstahl GmbH geholfen, Emissionsdaten systematisch und digital zu erfassen und die gewünschten Informationen sowohl für Kunden als auch für Investoren auf vertrauenswürdige Weise offenzulegen. Darüber hinaus haben diese Daten auch die Optimierung der eigenen Produktions- und Beschaffungsprozesse hinsichtlich ihrer Umweltverträglichkeit unterstützt und es dem Unternehmen ermöglicht, strategische Entscheidungen wie den Kauf von lokal produziertem grünem Wasserstoff zu priorisieren. Dadurch ist der Anteil von grünem Wasserstoff in der Stahlproduktion des Unternehmens schrittweise gestiegen, was bei steigenden CO₂-Preisen zu einer Senkung der Produktionskosten und somit zu einem zusätzlichen Wettbewerbsvorteil für die Grünstahl GmbH geführt hat.

Im Rahmen des digitalen Nachhaltigkeitsmanagements kann heute jeder Einheit produzierten Stahls eine präzise Menge an emittierten CO₂-Emissionen zugeordnet werden. Die Betrachtung der Emissionen hört dabei nicht an den Unternehmensgrenzen auf, sondern es erfolgt eine digitale, lückenlose und verifizierbare Nachverfolgung über die gesamte Lieferkette

hinweg. Dabei bezieht die Grünstahl GmbH die Informationen aller Zulieferer mit ein. Die direkten Zulieferer für Wasserstoff produzieren diesen auf Basis von Elektrolyse und verwenden dazu größtenteils selbst erzeugten Strom aus erneuerbaren Energien. Dies können sie nachweisen, indem sie ein digitales Zertifikat übermitteln, das bis zu den einzelnen Erzeugungsanlagen rückverfolgbar ist. Das Zertifikat wird kryptografisch mit der digitalen Identität der Elektrolyseanlage verknüpft, was eine Überprüfung sowohl der Authentizität des Zertifikats als auch der Plausibilität der enthaltenen Daten möglich macht. Die Emissionen, die durch Strom aus nicht erneuerbaren Energiequellen verursacht werden, sind ebenfalls im Zertifikat enthalten, werden dem Wasserstoff entsprechend zugerechnet und gehen schließlich in die CO₂-Bilanz des Stahls ein.

Die Emissionsdaten werden anschließend an den Kunden übermittelt, wenn die Grünstahl GmbH den produzierten Stahl an den französischen Autohersteller Voiture Verte SE liefert, um auch den Anforderungen aus dem europäischen Binnenmarkt gerecht zu werden. Der Autohersteller kann somit gegenüber dem Endkunden, Investoren und auch öffentlichen Stellen die Verwendung von grünem Stahl über die Landesgrenzen hinweg bis hin zum von den Wasserstoffproduzenten verwendeten Strom nachweisen. Das macht der Autohersteller nicht nur beim Stahl, sondern auch bei allen anderen Vorprodukten für jedes Auto. Die Zertifikate belegen lückenlos, in welchem Umfang entlang der Wertschöpfungskette – von den Vorprodukten wie Wasserstoff bis hin zu den verwendeten Rohstoffen – CO₂ emittiert wurde. Da die VoitureVerte SE die CO₂-Intensität über die gesamte Lieferkette ihrer Fahrzeuge gleichzeitig jederzeit digital beweisen kann, sind die Angaben glaubhaft für ihre Kunden. Dies hat es der Voiture Verte SE ermöglicht, Vorwürfe des Greenwashings stets wirkungsvoll zu entkräften und Marktanteile gegenüber der globalen Konkurrenz zu behaupten.

Blitzlicht 2: Das Smart Home von Alice im virtuellen Kraftwerk

Alice nutzt seit Kurzem eine moderne und interaktive Smart-Home-Lösung, die ihre Photovoltaik-Anlage, ihre Wärmepumpe und ihren Energiespeicher mit ihrem Energiemanagementsystem vernetzt und aufeinander abstimmt. Dadurch kann sie beispielsweise den Stromverbrauch einzelner Geräte oder das Ladeverhalten ihres Elektrofahrzeugs dynamisch und automatisch an die Markt- und Netzbedingungen anpassen. Für die Flexibilitätserbringung hat Alice ihre Smart-Home-

Anlagen bei ihrem Netzbetreiber angemeldet. Die Anmeldung war innerhalb von fünf Minuten abgeschlossen, da die meisten Daten über ihre Anlagen bereits in Alices digitalem Identitätsmanagementsystem gespeichert sind und von dort aus automatisch in das digitale Formular übertragen wurden. Alice musste die Angaben nur noch bestätigen.

Nach der erfolgreichen Anmeldung trat sie einem virtuellen Kraftwerk bei. Dieser Beitrittsprozess war genauso unkompliziert: Mithilfe digitaler Identitätsnachweise über sich selbst,

ihre Anlagen und ihren Meldestatus beim Netzbetreiber konnte sich Alice einfach über ihr Smartphone ausweisen und die Anmeldung ihrer Anlage bestätigen. Das virtuelle Kraftwerk bietet Alice seitdem die Möglichkeit, ihre Energieflexibilität zu vermarkten.

Heute ist ein sonniger Tag und Alices Photovoltaik-Anlage erreicht ihre maximale Leistung von 10 Kilowatt. Alice ist außer Haus an ihrer Arbeitsstätte und ihr eigener Speicher ist vollständig geladen, weshalb die Stromproduktion den Bedarf ihres Smart Home übersteigt. Deswegen wird der überschüssige Strom automatisch als Teil der Leistung des virtuellen Kraftwerks an andere Stromverbraucher geliefert. Diese Verteilung erfolgt vollautomatisch über eine digitale Plattform, sodass Alice keine manuellen Eingriffe vornehmen muss und sich ungestört ihrer Arbeit widmen kann. Dank der intelligenten Steuerung wird der selbst produzierte Strom effizient genutzt und Strom aus dem Netz systemdienlich bezogen. Das Energiesystem als Ganzes profitiert von solchen Anwendungsfällen, da die dezentral bereitgestellten Flexibilitäten zur Stabilität und Effizienz des Gesamtsystems beitragen.

Verteilnetzbetreiber können die Flexibilität zur Bewältigung von lokalen Netzengpässen beispielsweise über einen markt-basierten Redispatch 3.0 erwerben: Je nach aktuellem Strombedarf bietet das virtuelle Kraftwerk dabei Flexibilität an, indem es den Stromverbrauch reduziert, zum Beispiel durch das Laden von Speichern, oder überschüssigen Strom ins Netz einspeist. Durch die Kombination verschiedener Stromerzeuger und -speicher ist es möglich, dass das virtuelle Kraftwerk die Leistungskapazität eines konventionellen Kraftwerks phasenweise übersteigt und dabei nahezu

konstant Strom nach Bedarf bereitstellen kann. Diese Bereitstellung kann nahezu in Echtzeit erfolgen. So können auch größere Mengen an Reserveenergien auf höherer Spannungsebene durch den Übertragungsnetzbetreiber flexibel genutzt werden, etwa zur Frequenzhaltung, zur Spannungshaltung oder zum Netzwiederaufbau im Falle von Stromausfällen.

Für alle Arten der Flexibilitätserbringung erhält Alice eine finanzielle Entlohnung – anteilig zum Beitrag ihres Smart Home an den Erlösen des virtuellen Kraftwerks. Wie bei allen Prozessen innerhalb des virtuellen Kraftwerks erfolgt auch die Zuteilung der finanziellen Vergütung vollautomatisch. Ab ihrer erfolgreichen Anmeldung erhält Alice diese Vergütung also zusätzlich ohne Mehraufwand.

Das Smart Home sowie das gesamte virtuelle Kraftwerk orientieren sich bei der Entscheidung, wann der Stromverbrauch erhöht und der selbst produzierte Strom genutzt werden soll, an den aktuellen, lokalen Marktpreisen und optimieren dadurch den ökonomischen Mehrwert für die am virtuellen Kraftwerk Beteiligten. Alice profitiert dabei von weiteren finanziellen Anreizen, wie zum Beispiel dynamischen Netzentgelten, die ein solches Verhalten von virtuellen Kraftwerken incentivieren. Neben der Entlastung des Stromnetzes und der Ausschöpfung des vollen Potenzials ihres Stroms aus erneuerbaren Energien hat das Vorgehen also auch einen finanziellen Nutzen für Alice. Ihr Wechsel zwischen den Rollen als Stromproduzent und -konsument verläuft dabei fließend, automatisch und sicher – und durch die digitale Identifizierung der Anlagen zu jedem Zeitpunkt völlig transparent für den Netzbetreiber.

Blitzlicht 3: Bobs neues Elektroauto

Da Bob eine Mietwohnung ohne Solaranlage bewohnt, konnte er bisher nicht an Flexibilitätsmärkten teilnehmen. Er hat sich deshalb heute ein Elektroauto gekauft, das bidirektionales Laden unterstützt. Es dient also nicht nur als Stromspeicher, sondern kann auch Strom zurück ins Netz einspeisen. Der Stromanbieter EnergyFlex GmbH kann diese Flexibilität von Bobs Auto zu guten Konditionen nutzen: Angeboten wird ein besonders attraktiver Stromtarif, mit dem Bob durch die Flexibilität seines Fahrzeugs zur Netzstabilität und zur CO₂-Reduktion beitragen und gleichzeitig finanziell profitieren kann, wenn er sein Auto auf seinem Stellplatz in der Tiefgarage lädt.

Bobs bisheriger Stromanbieter ist nicht auf flexible Produkte spezialisiert und kann ihm deshalb kein gutes Angebot für die Flexibilität seines Elektroautos machen. Bob ist mit seinem alten Stromanbieter allerdings sehr zufrieden und da er schon seit mehreren Jahren dort Kunde ist, bezieht er den Strom für seine Mietwohnung zu sehr guten Konditionen, die er nicht aufgeben möchte. Es ist Bob aber möglich, mit der EnergyFlex GmbH einen Liefervertrag speziell und ausschließlich für sein Elektroauto abzuschließen – und dabei den bestehenden

Stromliefervertrag für seine Mietwohnung zum gewohnten Tarif zu behalten. Diese maßgeschneiderte Lösung erlaubt es ihm, das individuell beste Angebot für seine Lebenssituation zu erhalten und damit auch seine finanzielle Lage zu optimieren.

Da das Elektroauto an der Ladesäule durch eine digitale Identität in Echtzeit erkannt wird, kann der geladene Strom dem Elektroauto und Bob als Fahrzeughalter individuell zugeordnet und somit über seinen separaten Stromliefervertrag für das Elektroauto abgerechnet werden. Auf diese Weise kann die EnergyFlex GmbH Bobs Auto an jeder beliebigen Ladesäule identifizieren, also auch wenn es nicht an seiner eigenen Wallbox, sondern beispielsweise an einer öffentlichen Ladesäule angesteckt ist. Damit profitiert Bob auch dann von seinem neuen Tarif, wenn er das Auto zum Beispiel am Arbeitsplatz auflädt oder auf Dienstreise innerhalb des europäischen Stromnetzes unterwegs ist. Durch die automatische Erkennung an der Ladesäule können die angebotenen Flexibilitäten des Autos überall in nahezu Echtzeit genutzt werden. Die Abrechnung erfolgt dabei auch über Ländergrenzen hinweg automatisch und unkompliziert. Nach der Vertragsunterzeichnung und der digitalen Übermittlung seiner Daten erhält Bob einen

digitalen Identitätsnachweis über seine Kundenzugehörigkeit zur EnergyFlex GmbH. Durch diesen Nachweis kann Bob sein Auto direkt an verschiedenen Ladesäulen anschließen, ohne sich bei jedem Ladevorgang explizit authentifizieren zu müssen. Seine persönlichen Ladepräferenzen sind selbstverständlich im Nachweis enthalten, sodass seine Batterie trotz Teilnahme am Flexibilitätsmarkt immer ausreichend geladen ist.

Durch diese neue Form des selektiven Lieferantenwechsels wird Bob ohne spürbare Einstiegsbarrieren vom reinen Konsumenten zum Prosumer. Die Flexibilität, die durch das bidirektionale Laden seines Elektroautos entsteht, eröffnet Bob die Möglichkeit, nicht nur seinen eigenen Energieverbrauch zu optimieren und finanzielle Vorteile zu erzielen, sondern auch einen wertvollen Beitrag zu einem nachhaltigen Energiesystem zu leisten.

3.2 Die digitale Identitätslücke

Die in den Blitzlichtern beschriebenen Anwendungsfälle setzen eine robuste Energiedateninfrastruktur voraus, die nur durch eine tiefgreifende digitale Transformation des Energiesektors erreicht werden kann (Leinauer et al. 2024). Dabei müssen mehrere digitale Lücken geschlossen werden, um ein zukunftsfähiges Energiesystem zu schaffen und zugleich die Kosten der Energiewende auf ein volkswirtschaftlich effizientes Maß zu reduzieren (dena 2022). Dieses Unterkapitel widmet sich mit der Identitätslücke einer der aktuell größten digitalen Lücken.

Vertrauen in Daten

Vertrauen in die Vollständigkeit, Korrektheit, Aktualität und Integrität von Daten ist eine grundlegende Anforderung für eine digitalisierte Energiewirtschaft. Im Kontext dieser Studie bezieht sich Vertrauen auf das Vertrauen in externe Datenquellen, bekannt als *Oracles* (Barr et al. 2015). Dies kann durch eine sinnvolle Integration von vertrauenswürdigen Parteien wie zertifizierten Installateuren gewährleistet werden. Diese Parteien bestätigen die Korrektheit der Anlagenstammdaten und stellen eine signierte und unveränderliche digitale Identität mit diesen Informationen aus (Babel et al. 2023). Sobald das Vertrauen in die Stammdaten etabliert ist, kann eine kryptografische Verknüpfung mit Bewegungsdaten die Authentizität und Integrität der ausgetauschten Informationen sichern. Dies erlaubt es den Empfängern, die unmittelbar von den Anlagen gemessenen Primärdaten zu verifizieren (Chadwick et al. 2023). Gegenwärtig werden Primärdaten zu Stromerzeugung und -verbrauch durch eine moderne Messeinrichtung gemessen und über die Smart-Meter-Gateway-Infrastruktur geteilt (dena 2024c).

Aktuell sind oft die Anlagenbetreiber selbst die Oracles für Stammdaten. Gemäß der Marktstammdatenregisterverordnung (MaStRV)⁶ tragen sie die Verantwortung für die Dateneingabe, während Institutionen wie die Bundesnetzagentur (BNetzA) und die Netzbetreiber als Kontrollinstanzen fungieren. Die erforderliche manuelle Dateneingabe erweist sich jedoch durch die steigende Komplexität des Energiesystems als fehleranfällig und zeitintensiv (Kotthoff et al. 2025). Beispielsweise berichtet die BNetzA, dass im Jahr 2023 bei der Meldung neuer Balkonanlagen eine erhebliche Dunkelziffer durch fehlende Registrierungen im MaStR bestehen könnte (Bundesnetzagentur 2024c). Somit fehlt

aktuell ein verlässlicher und vollständiger Nachweis über die Stammdaten aller Anlagen im Energiesystem. Dies erschwert nicht nur die Sicherstellung der Datenqualität und -aktualität und schwächt somit das Vertrauen in die Stammdaten, sondern verursacht auch Zeit- und Kostenaufwand für die Marktteilnehmer. Folglich müssen für Anwendungsfälle wie die Integration in virtuelle Kraftwerke die Existenz und die Eigenschaften von Anlagen oft physisch vor Ort noch einmal überprüft und validiert und anschließend entsprechende Datensätze individuell neu erstellt werden, anstatt sie nahtlos durch digitale Prozesse zu integrieren.

Zur Sicherung des Vertrauens in Bewegungsdaten müssen aktuell alle Komponenten des Smart Meter Gateway (SMGW) vor ihrem Einsatz Test- und Zertifizierungsprozesse des BSI durchlaufen (BSI 2021). Durch die Notwendigkeit solcher Zertifizierungen und Registrierungen (z. B. als aktiver externer Marktteilnehmer) sowie den Betrieb der Infrastruktur durch den SMGW-Administrator fallen derzeit für den Zugriff auf SMGW-Daten erhebliche Kosten an. Diese Kosten erschweren eine wirtschaftliche Nutzung der Bewegungsdaten für weiterführende Anwendungsfälle. Darüber hinaus schränken bestehende regulatorische Vorgaben und technische Restriktionen den Zugriff auf die erhobenen Daten aktuell so ein, dass bisherige Anwendungsfälle der Smart-Meter-Infrastruktur lediglich die Erfassung und die automatisierte Bereitstellung abrechnungsrelevanter Daten umfassen. Innovative digitalisierte Anwendungen, die feingranulare und aktuelle Bewegungsdaten benötigen, können so nur schwer bis gar nicht umgesetzt werden (dena 2024c).

Sektorenübergreifende Interoperabilität

Eine erfolgreiche Sektorenkopplung erfordert eine ganzheitliche Betrachtung und Gewährleistung der Interoperabilität der Daten über Sektorengrenzen hinweg. Eine solche sektorenübergreifende Interoperabilität umfasst eine technische und eine semantische Dimension (BDEW 2021). Während die technische Interoperabilität in diesem Kontext ermöglicht, dass Daten verschiedenen Sektoren zugänglich gemacht werden, gewährleistet die semantische Interoperabilität, dass die Daten auch sektorenübergreifend auslesbar und nutzbar sind (Pliatsios et al. 2023). Nur wenn sowohl der Datenaustausch als auch die konsistente Interpretation sichergestellt sind, wird vollständige Interoperabilität erreicht (Rahman und Hussain 2020). Zur Schaffung technischer und semantischer Interoperabilität bedarf es verbindlicher

6 Vgl. § 3 MaStRV (Registrierung von Marktakteuren)

Regeln und Rahmenbedingungen (Governance), die nicht nur einen sektorenübergreifenden Datenaustausch fördern, sondern auch den Umgang mit den Daten vereinheitlichen und so Vertrauen in die Daten über Sektorengrenzen hinweg ermöglichen (vgl. oben „Vertrauen in Daten“). Eine digitale Infrastruktur, die Daten über Sektorengrenzen hinweg aktuell und konsistent abbildet, kann Anwendungsfälle ermöglichen, die feingranulare und echtzeitnahe Daten benötigen (z. B. Engpassmanagement auf niedrigen Spannungsebenen) (Burges et al. 2022).

Im aktuellen Energiesystem gibt es die Herausforderung, dass bisher keine Register existieren, die die Stammdaten aller für das Energiesystem relevanten Anlagen einheitlich erfassen. Beispielsweise werden Kleinanlagen wie Wärmepumpen oder mobile Anlagen wie Elektroautos nicht in das Marktstammdatenregister eingetragen (siehe § 5 MaStRV). Daten, die im MaStR vorhanden sind, können derzeit nicht automatisiert mit Stammdaten aus dem Herkunftsnachweisregister (HKNR) verglichen werden. Im Mobilitätssektor gibt es ebenfalls spezifische Register, die die Stammdaten von Elektrofahrzeugen verwalten, jedoch sind diese Daten für den Energiesektor nicht zugänglich. Die fehlenden Möglichkeiten, erhobene Stammdaten konsistent über Sektorengrenzen hinweg darzustellen, limitiert ihre Verfügbarkeit für weitere Anwendungen. Aktuelle Herausforderungen beschränken sich dabei nicht nur auf das Fehlen einer technischen Vereinbarung über Datenaustauschformate wie JSON (JavaScript Object Notation), CSV (Comma-separated Values) und XML (Extensible Markup Language), sondern umfassen auch die Zugänglichkeit und konsistente Interpretation dieser Daten (Burges et al. 2022; BDEW 2021).

Sichere Ansteuerung

Die Möglichkeit zur Ansteuerung von dezentralen Anlagen im Energiesystem ist eine grundsätzliche Voraussetzung für die skalierbare Nutzung von Flexibilitätpotenzialen im Energiesystem. Die volatile Einspeisung aus Erneuerbare-Energien-Anlagen kann durch die gezielte Steuerung von flexiblen Verbrauchern und Speichern ausgeglichen werden, was eine effizientere und effektivere Integration der Anlagen ermöglicht. Die Sicherheit bei der Ansteuerung von Anlagen der kritischen Energieinfrastruktur⁷ erfordert dabei eine robuste Authentifizierung und Autorisierung der beteiligten Entitäten. Der Aufbau eines sicheren Kommunikationskanals zwischen diesen Entitäten muss gewährleistet sein, um mögliche Angriffe auf die Energieinfrastruktur abwehren zu können (Buck et al. 2023).

In der gegenwärtigen Ausgestaltung der SMGW-Infrastruktur erhält zwar die moderne Messeinrichtung eine digitale Identität, die dann einen sicheren Kommunikationskanal zwischen dem lokalen Messpunkt und dem Energieversorger bzw. Netzbetreiber aufbaut. Allerdings wird weder die etwaige Erzeugeranlage selbst noch ein eventuelles (Heim-)Energiemanagementsystem, das die mögliche Flexibilität anbietet, mit einer eigenen digitalen Identität ausgestattet, wodurch ein Vertrauensanker nur bis zur

Messstelle besteht. Im Energiesystem existieren daher nur vertrauenswürdige Stammdaten für das Smart Meter Gateway selbst, nicht aber für die nachgelagerten Anlagen, was die Entwicklung einer vertrauenswürdigen und belastbaren Flexibilitätsinfrastruktur behindert.

Ausrichtung an Stakeholdern

Um eine breite Unterstützung für eine digitale Transformation des Energiesektors zu gewinnen, ist die Akzeptanz der Maßnahmen und Veränderungen in der Bevölkerung sowie unter den beteiligten Akteuren unerlässlich. Deshalb sollte das zukünftige Energiesystem an den Stakeholdern – von den Netzbetreibern und Energieversorgern über die Regulierungsbehörden bis hin zu den Endverbrauchern – ausgerichtet sein. Ausrichtung an Stakeholdern bedeutet in diesem Kontext, sicherzustellen, dass das Energiesystem so gestaltet und verwaltet wird, dass es die Bedürfnisse, Interessen und Erwartungen aller beteiligten Parteien berücksichtigt und adressiert. Dazu gehören der offene Zugang zum und die aktive Teilnahme am Markt sowie die Schaffung von Anreizen für private Akteure, sich als Prosumer aktiv am Energiesystem zu beteiligen (Elia Group 2021; dena 2024a). Erforderlich ist hierfür unter anderem der einfache und nutzerorientierte Zugang zu den eigenen Daten. Zudem sollten Daten über offene Schnittstellen bereitgestellt werden, um eine nahtlose Weiterverwendung unter Berücksichtigung von Datenschutzanforderungen zu ermöglichen.

Die bestehende Lücke zeigt sich beispielsweise in den aktuellen politischen Bemühungen wie den Richtlinien (EU) 2019/944 und (EU) 2024/1711 zur Reformierung des Elektrizitätsbinnenmarktes. Diese Richtlinien sollen die Rechte der Verbraucher stärken, aktiv am Strommarkt teilnehmen zu können und so an der Energiewende mitzuwirken. Die dafür erforderliche IT-Infrastruktur, die von den Mitgliedstaaten bereitgestellt werden soll, ist in Deutschland jedoch bisher nur unzureichend umgesetzt worden. Insbesondere ist der Zugang zu den eigenen Stromverbrauchs- und Erzeugungsdaten, die über die Smart-Meter-Gateway-Infrastruktur erfasst werden, für die Verbraucher nicht umfassend gewährleistet. Dies schränkt nicht nur die Nutzung der eigenen Daten zur aktiven Teilnahme am Markt ein, sondern auch die Kontrolle der Verbraucher über ihre eigenen Energieverbräuche (Elia Group 2021; dena 2024a).

Skalierbarkeit

Durch die zunehmende Interaktionsdynamik und die Anzahl an dezentralen Erzeugungs- und Verbrauchsanlagen (vgl. **Kapitel 1**) erhöhen sich der Kommunikationsbedarf und das Volumen der ausgetauschten Daten im modernen Energiesystem, wie durch die Anwendungsfälle in den Blitzlichtern skizziert. Eine hohe Skalierbarkeit der analogen wie digitalen Ebenen der Infrastruktur ist daher entscheidend. Das bedeutet, dass das Gesamtsystem nicht nur die Fähigkeit besitzen muss, die exponentiell steigende Anzahl von Akteuren und Transaktionen zu bewältigen, sondern auch die Flexibilität und Erweiterbarkeit aufweisen

⁷ Laut § 2 BStG (Begriffsbestimmungen) sind Kritische Infrastrukturen Einrichtungen, Anlagen oder Teile davon, die den Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser und Ernährung, Finanz- und Versicherungswesen sowie Siedlungsabfallentsorgung angehören und von großer Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden.

muss, um neue Anlagen effizient zu integrieren und sich an zukünftige Entwicklungen anzupassen.

Die derzeitigen und geplanten Register im Energiesektor sind fragmentiert und nicht für eine skalierbare digitale Identifizierung von Anlagen oder eine nahtlose Authentifizierung ihrer Stammdaten ausgelegt. So muss beispielsweise jede Verbrauchseinheit, die am Hoch- oder Höchstspannungsnetz angeschlossen ist, im MaStR registriert werden.⁸ Dies umfasst zum Beispiel Elektrolyseanlagen für die Gewinnung von Wasserstoff (50Hertz et al. 2024). Zusätzlich wäre bei einer solchen Anlage eine separate Registrierung im Herkunftsnachweisregister Gas, Wärme und Kälte erforderlich, um die Herkunft des produzierten Wasserstoffs zu dokumentieren.⁹ Diese Mehrfachregistrierung ist in der Regel mit einem erheblichen Zeit- und Kostenaufwand verbunden.

3.3 Digitale Identitäten für ein digitales Energiesystem

Digitale Identitäten spielen eine entscheidende Rolle bei der Identifizierung, Authentifizierung oder Autorisierung im digitalen Raum. Sie können für natürliche und rechtliche Personen und inzwischen auch für Maschinen-Entitäten erstellt werden und sich über verschiedene Plattformen und Dienste erstrecken – von Accounts auf Social-Media-Plattformen bis hin zu hoheitlichen Identitäten, die ein rechtssicheres Signieren von Dokumenten ermöglichen (Europäische Kommission 2022; Schellinger et al. 2022).

Zentrale Identitätsansätze, die aktuell für eine Vielzahl von digitalen Anwendungsfällen verwendet werden, haben sich mit der fortschreitenden Digitalisierung der Gesellschaft als problematisch erwiesen. Sie führen zu Datensilos, die die Interoperabilität zwischen verschiedenen Diensten einschränken und den Nutzern nur eine begrenzte Kontrolle über ihre Daten gewährleisten. Vor diesem Hintergrund wird die Notwendigkeit von alternativen Ansätzen für digitale Identitäten immer deutlicher. Dezentrale Ansätze versprechen eine verbesserte Nutzerkontrolle, eine erhöhte Sicherheit und eine umfassendere Interoperabilität, indem sie offene, nutzerzentrierte Identitätsökosysteme fördern (Preukschat 2021; Sedlmeir et al. 2021).

Bei dezentralen Identitätsmodellen wie Self-Sovereign Identities (SSI) werden persönliche Informationen direkt bei den Nutzern in einer sicheren Applikation gespeichert, die als digitale Wallet bezeichnet wird. Dies ermöglicht es den Nutzern, ihre Identitäten selbstbestimmt über verschiedene Plattformen und Dienste hinweg zu verwalten (Schellinger et al. 2022). Bestrebungen hin

zu solchen selbstverwalteten dezentraleren Identitätsparadigmen bilden die Grundlage für die Weiterentwicklung der aktuellen eIDAS-Verordnung¹⁰ zu eIDAS 2.0, die darauf abzielt, eine länderübergreifende und autonome digitale Identitätsinfrastruktur in Europa zu etablieren und neue Anwendungsfälle über die reine Darstellung der Personalausweis-Daten hinaus zu ermöglichen (Europäische Kommission 2022).

Die Anwendbarkeit der Grundprinzipien digitaler Identitäten auf nicht menschliche Entitäten verdeutlicht die Vielzahl an Einsatzmöglichkeiten (Strüker et al. 2021). Digitale Maschinen-Identitäten können das notwendige Vertrauen – analog zu digitalen Personen-Identitäten – für Interaktionen zwischen diesen Entitäten schaffen, wenn sie von einem vertrauenswürdigen Akteur etabliert werden. Verschiedene Attribute können von unterschiedlichen, jeweils vertrauenswürdigen Akteuren verifiziert werden. Bei Maschinen im Energiesektor können beispielsweise zertifizierte Installateure spezifische Eigenschaften der Maschine wie Typ, Standort und Spitzenleistung verifizieren und diese als eindeutige Attribute in einer digitalen Maschinen-Identität verankern (Babel et al. 2023). In diesem Kontext fungieren digitale Identitäten als vertrauenswürdige Grundlage für die Authentifizierung und Verschlüsselung der Kommunikation, um die Sicherheit und Integrität der Datenübertragung zu gewährleisten (Eckert 2018).

Um die Identität und die mit ihr verbundenen Attribute sicher und dauerhaft mit der Maschine zu verbinden, können die Identitätsdaten auf einer sicheren Hardware (sogenannte Hardware Security Modules) gespeichert werden. Diese Maßnahme stellt sicher, dass die digitale Identität eindeutig der Maschine zugeordnet bleibt und nicht auf andere Maschinen übertragbar ist (Babel et al. 2023; dena 2023a). Wie bei persönlichen Identitätsdaten, die im Rahmen der eIDAS-2.0-Verordnung verwaltet werden, können auch digitale Identitäten von Maschinen in einer digitalen Wallet gespeichert und verwaltet werden. Dies ermöglicht eine sichere und verständliche Handhabung der Identitätsdaten, wobei die Nutzer – oder im Falle von Maschinen die Betreiber – die vollständige Kontrolle über die Verwendung und den Zugriff auf diese Daten behalten.

3.4 Anforderungen an digitale Identitäten

Um die in Kapitel 3.2 beschriebene digitale Identitätslücke zu schließen, können digitale Identitäten einen entscheidenden Beitrag leisten (vgl. Tabelle 1). Im Folgenden wird aufgezeigt, wie digitale Identitäten gestaltet werden sollten, um die bestehende digitale Identitätslücke zu schließen:

8 Vgl. § 3 MaStRV (Registrierung von Marktakteuren)

9 Vgl. Gas-Wärme-Kälte-Herkunftsnachweisregister-Verordnung: GWKHV § 11 (Antrag auf Registrierung)

10 Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG



Anforderung	Aufgabe von digitalen Identitäten	Ausgestaltung von digitalen Identitäten	Beitrag zur digitalen Energiewirtschaft
Hohe Datenqualität	Vertrauensanker für die Authentizität und Verifizierbarkeit von Stammdaten	Stammdaten bei den Anlagen, Zertifizierungen, sichere Hardware	Stärkung des Vertrauens der Akteure in die Integrität und Richtigkeit der Daten
Eindeutige Identifizierung	Möglichkeit zur eindeutigen Identifizierung von Anlagen und relevanten sonstigen Entitäten	Ausstellung einer digitalen Identität pro Anlage oder Entität	Effiziente und sichere Interaktion mit Anlagen und Entitäten im dezentralen Energiesystem
Sektorenübergreifende Interoperabilität	Sichere, sektorenübergreifende Kommunikation nahe Echtzeit	Sichere Kommunikationsprotokolle auf Basis von einheitlichen Standards	Unterstützung bei der Sektorenkopplung
Selbstbestimmtheit in der Nutzung	Kontrolle über die Freigabe und Verwendung von Daten	Dezentrale Speicherung von Daten, bilateraler Datenaustausch, selektive Offenlegung	Erhöhung der Nutzerakzeptanz durch Transparenz und Kontrolle
Konformität mit gesetzlichen Regularien	Einhaltung von Datenschutzstandards und rechtlichen Anforderungen	Datenminimierung, selektive Offenlegung, bilaterale Kommunikation	Sicherheit, Privatsphäre und Vertrauen der Nutzer

Table 1: Die digitale Identitätslücke und die Anforderungen an digitale Identitäten zu ihrer Schließung

Hohe Datenqualität

Datenqualität wird durch Korrektheit, Aktualität, Vollständigkeit und Integrität der Daten charakterisiert. Diese Aspekte sind entscheidend, damit die als digitale Identitäten ausgestellten, verifizierbaren Stammdaten in einer sektorengekoppelten Energiewirtschaft als Vertrauensanker für digitale Transaktionen dienen können (Sedlmeir et al. 2021; Strong et al. 1997). Diese Stammdaten bilden den Ausgangspunkt jeder Transaktion in diesem digitalisierten System (vgl. **Kapitel 3.2**) und enthalten fundamentale Informationen über die Akteure und Anlagen, wie beispielsweise Erzeugungskapazität oder Marktllokation. Nur wenn diese Voraussetzungen erfüllt sind, können die Akteure der Energiewirtschaft den Informationen vertrauen und sie als zuverlässigen Ausgangspunkt für Transaktionen nutzen. Allerdings können Register allein nicht die Qualität und Richtigkeit der Daten garantieren. Daher sind klare Governance-Richtlinien zur Sicherung der Datenqualität erforderlich. Beispielsweise sollte die digitale Identität nur von einem vertrauenswürdigen Akteur wie einem zertifizierten Installateur verifiziert werden (Babel et al. 2023). Eine nachträgliche Manipulation der erfassten Daten lässt sich durch eine starke Bindung der Anlage an ihre digitale Identität (z. B. durch ein Hardware Security Module) sowie durch kryptografische Maßnahmen verhindern (dena 2023b). Eine hohe Qualität der Stammdaten überträgt sich zudem auch auf die Bewegungsdaten. Sobald die Bewegungsdaten einer Anlage, deren Erfassung durch zertifizierte Smart Meter sichergestellt ist, kryptografisch mit der digitalen Identität verknüpft sind, sind die Authentizität und Integrität der in den Bewegungsdaten enthaltenen Informationen gewährleistet.

Ein Beispiel hierfür ist Blitzlicht 1, in dem sowohl die Grünstahl GmbH als auch die Voiture Verte SE sowie weitere Stakeholder in der Lieferkette wie Endkunden den präzisen Daten zu CO₂-Emissionen der Stromerzeugung vertrauen können.

Eindeutige Identifizierung

Eine eindeutige Verknüpfung von Akteuren mit ihren jeweiligen Anlagen ist der Ausgangspunkt für effiziente und sichere Interaktionen im dezentralen Energiesystem. Hierfür benötigt jeder Akteur und jede Anlage – egal ob Photovoltaik-Anlage, Windkraftanlage, Batteriespeicher oder Elektroauto – eine eindeutige digitale Identität (Elia Group 2023). Eine aggregierte Zusammenfassung, wie sie in der heutigen Smart-Meter-Gateway-Infrastruktur für Haushalte erfolgt, ist unzureichend und ermöglicht keine anlagenscharfe Steuerung und nachweisbare Rückverfolgung von Bewegungsdaten bis zur einzelnen Anlage (vgl. **Kapitel 3.1**). Deshalb sollte eine gerätescharfe Identifizierung gewährleistet werden, die eine eindeutige (semantisch interoperable) Kennung der Anlage sicherstellt. Darüber hinaus sollte bei der Identitätsvergabe gewährleistet werden, dass die Anlagen in der Lage sind, aktiv am Netz teilzunehmen, und die angegebenen Stammdaten der Identität authentisch sind.

Digitale Identitäten ermöglichen die erforderliche Skalierbarkeit durch eindeutige Stammdaten. Statt in mehreren Registern

parallel die gleichen Informationen zu speichern, können relevante Stammdaten von den digitalen Identitäten an die Register übermittelt werden, sofern diese eine entsprechende Schnittstelle besitzen (dena 2023b). Ein gerätezentriertes Identitätsmanagement skaliert die Datenhaltung mit der Anzahl an Geräten, da jedes Gerät zunächst seine eigenen Daten („on Edge“) verwaltet. Die für einen Anwendungsfall benötigten Daten können dann entsprechend weitergegeben werden. Dadurch sinkt für Anbieter der Bedarf an umfangreichen separaten Datenbanken sowie deren Wartungsbedarf. Datenbestände können verschlankt und die Aktualisierung kann stärker automatisiert werden. Dies erleichtert nicht nur den Dienstleistungsanbietern die Handhabung der Kundendaten, sondern reduziert insbesondere die Risiken, die sich aus der Haltung dieser sensiblen Daten (z. B. hinsichtlich des Datenschutzes) ergeben.

Das Elektroauto von Bob aus Blitzlicht 3 kann beispielsweise auf Basis der digitalen Identität identifiziert und die Vertragszugehörigkeit datenminimal abgeleitet werden. So können sowohl der alte als auch der neue Energieversorger sicher sein, dass es sich um Bobs Elektroauto handelt, wenn etwa ein Ladevorgang auch an einer fremden Ladesäule gestartet wird.

Sektorenübergreifende Interoperabilität

Um digitale Identitäten effizient in das Energiesystem zu integrieren und Skaleneffekte zu realisieren – insbesondere durch die Verteilung der Onboarding-Kosten einer Anlage auf mehrere Anwendungen – sind sektorenübergreifende Interoperabilität und Anwendungsoffenheit essenziell. Sie ermöglichen die Nutzung einer digitalen Identität über mehrere Anwendungen hinweg. Neben der semantischen Interoperabilität, die ein einheitliches Verständnis der Daten gewährleistet, ist auch ein sektorenübergreifendes Vertrauen in die Datenqualität der ausgestellten digitalen Identitäten entscheidend. Dies erfordert unter anderem, dass die Herausgeber digitaler Identitäten sowie die technischen Verfahren zur Sicherstellung der Datenintegrität und -authentizität eines Sektors auch in anderen Sektoren als vertrauenswürdig anerkannt werden.

Die digitale Identität eines Elektroautos, die beispielsweise vom Hersteller ausgestellt wird, kann so nicht nur für fahrzeugbezogene Dienstleistungen genutzt werden, sondern auch für Anwendungsfälle im Energiesystem, indem auf Basis der verifizierbaren Informationen über den Speicher des Autos Flexibilitätsoptionen angeboten werden (Elia Group 2023). Die Kosten für die Installation und den Betrieb dieser Infrastruktur können dadurch auf viele Anwendungsfälle verteilt werden, wodurch eine deutliche Effizienzsteigerung erreicht wird. Folglich sinken der monetäre Aufwand pro Anwendungsfall sowie die Belastung der einzelnen Akteure, was die Nutzung insgesamt wirtschaftlicher und praktikabler macht. Diese sektorenübergreifenden Skaleneffekte führen zur beschleunigten und kostengünstigeren Integration digitaler Identitäten in das Energiesystem.

Eine solche Infrastruktur ermöglicht es den Empfängern dieser Dienste (z. B. Endnutzern), selbst zu entscheiden, für welche Anwendungsfälle sie die Stammdaten ihrer Anlagen verwenden möchten. Die nahtlose Integration digitaler Identitäten ohne Medienbrüche ist dabei von größter Bedeutung, um einen reibungslosen Informationsfluss innerhalb des Energiesystems zu gewährleisten, der für verschiedene skizzierte Anwendungen, wie virtuelle Kraftwerke, notwendig ist (Leinauer et al. 2024).

Im Fall von Bob aus Blitzlicht 3 ermöglicht eine anwendungs-offene digitale Identität die nahtlose, automatisierte und medienbruchfreie Nutzung seiner Elektroauto-Stammdaten für verschiedene Zwecke in unterschiedlichen Sektoren – vom Energiesektor für die Abrechnung beim neuen Stromanbieter bis zum Mobilitätssektor für die Wartung des Elektroautos.

Selbstbestimmtheit in der Nutzung

Die Selbstbestimmtheit in der Nutzung digitaler Identitäten ermöglicht den Nutzern, über die Freigabe und Verwendung ihrer persönlichen Identitäten selbst zu bestimmen, und stellt die Stakeholder-Orientierung auf dieser Ebene sicher. Dieses Prinzip ist von grundlegender Bedeutung für die Wahrung der Datensouveränität, indem es die Nutzer befähigt, eine aktive Rolle bei der Verwaltung ihrer eigenen digitalen Identität zu übernehmen. Die Kontrolle über und die Transparenz hinsichtlich der Verwendung der eigenen Daten sind entscheidend für die Akzeptanz digitaler Identitäten durch die Nutzer und ihre Bereitschaft zur Teilnahme an neuartigen Diensten (Wanner et al. 2022). Dies ermöglicht einen bilateralen und selbstbestimmten Datenaustausch, bei dem Nutzer selbst entscheiden, mit wem sie Daten teilen. Jede Datenfreigabe erfordert die aktive Zustimmung des Nutzers (Sedlmeir et al. 2021). Dies entspricht den Prinzipien von „Privacy by Design“, bei dem Datenschutzaspekte bereits in der Konzeption von Systemen integriert werden, um die Sicherheit und Vertraulichkeit der Nutzerdaten durchgehend zu gewährleisten (Cavoukian 2009). Mit diesem Ansatz kann der Umfang der Daten, die von Akteuren im Stromsystem erhoben werden, minimiert werden, wodurch die Notwendigkeit, große Datenmengen zu verwalten, reduziert wird. Damit werden auch rechtliche Risiken für alle beteiligten Akteure im digitalen Energiesystem verringert.

Wie in Blitzlicht 2 dargestellt, wird Alice bei der Anmeldung darüber informiert, welche Daten abgefragt und wofür sie im Anwendungsfall verwendet werden (z. B. Adresse und technische Spezifikationen der Photovoltaik-Anlage). Der Hersteller der Anlage erhält keine Information darüber, bei welchem virtuellen Kraftwerk Alice sich anmeldet. Das verhindert die Erstellung eines detaillierten Profils über Alice auf Basis mehrerer Interaktionen.

Konformität mit gesetzlichen Regularien

Digitale Identitätsregister im Energiesektor sind – wie die bestehende Energiedateninfrastruktur auf Basis des Smart Meter

Gateway – an geltende Vorschriften gebunden. Eine ganzheitliche Evaluation potenziell notwendiger regulatorischer Änderungen übersteigt den Rahmen dieser Studie. Einzelne Aspekte wurden im Rahmen des DIVE-Projekts jedoch untersucht.¹¹

Die relevanten Regularien beinhalten dabei nicht nur sektorenspezifische Anforderungen, sondern auch strenge Datenschutzrichtlinien, die für die Gewährleistung der Sicherheit, der Privatsphäre und des Vertrauens der Nutzer entscheidend sind. Diese Richtlinien, insbesondere die Datenschutz-Grundverordnung, definieren unter anderem die Grundsätze der Datenminimierung und Zweckbindung (Art. 5 Abs. 1 DSGVO¹²), wonach nur zwingend notwendige Daten für spezifische Zwecke erhoben werden dürfen. Transparenz stellt ebenfalls ein zentrales Element der Verordnung dar. Nutzer müssen jederzeit nachvollziehen können, welche ihrer Daten erhoben, wie sie verwendet und wie lange sie gespeichert werden.

Die Energieinfrastruktur ist nach § 2 Abs. 10 des IT-Sicherheitsgesetzes¹³ als Kritische Infrastruktur (KRITIS) klassifiziert. Diese Einstufung unterstreicht die essenzielle Bedeutung des Schutzes dieser Infrastrukturen, die durch die fortlaufende Digitalisierung mit steigenden Sicherheitsanforderungen konfrontiert sind. Die Erfüllung dieser Anforderungen erfordert umfangreiche Sicherheitsmaßnahmen, die sowohl den physischen als auch den cyberspezifischen Schutz der kritischen Daten und Systeme sicherstellen (Buck et al. 2023). Die Implementierung digitaler Identitätsregister im Energiesektor muss daher spezifische Schutzmaßnahmen integrieren, die die Resilienz gegenüber Bedrohungen stärken und die durchgehende Versorgungssicherheit garantieren.

In Blitzlicht 2 wird so ergänzend zu den Ausführungen in der Anforderung *Selbstbestimmtheit in der Nutzung* nicht nur Transparenz hinsichtlich der erhobenen Informationen geschaffen und eine Profilbildung unmöglich, sondern es dürfen nur unbedingt erforderliche Informationen von berechtigten Marktteilnehmern abgefragt werden, vom Netzbetreiber beispielsweise Marktlokation und Erzeugungskapazität der neuen Anlage.

11 Vgl. DIVE-Bericht „Rechtliche Analyse“

12 Art. 5 DSGVO (Grundsätze für die Verarbeitung personenbezogener Daten)

13 Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG)

4. Ein Weg – Digitale Identitäten für das Energiesystem

Die Einführung digitaler Identitäten sollte als mehrstufiger Weg betrachtet werden. Im Rahmen dieses Weges sollte untersucht werden, wie bestehende Technologien, Prozesse und Dateninfrastrukturen integrativ implementiert werden können, um die Anschlussfähigkeit zu gewährleisten. Gleichzeitig sollten neue Anforderungen durch innovative Anwendungsfälle wie Redispatch 3.0 oder Energy Sharing Communities und Technologien wie Data Spaces oder Künstliche Intelligenz in der Energiewirtschaft berücksichtigt werden, um diese zukunftsorientierten Anwendungen zu ermöglichen. Dazu müssen die zahlreichen Stakeholder der Energiewirtschaft auf unterschiedlichen Ebenen eingebunden werden, um die diversen Interessen angemessen zu berücksichtigen und damit die erforderliche Unterstützung für die Einführung digitaler Identitäten zu gewinnen. Im Laufe des Weges wird gemeinsam erarbeitet, wie die konkrete Umsetzung von digitalen Identitäten und die Anbindung an die bestehende, aber auch die zukünftige Energiedateninfrastruktur gestaltet werden sollen und somit letztlich die digitale Identitätslücke geschlossen werden kann.

Die fünf Schritte eines Weges vom Status quo bis zur Schließung der digitalen Identitätslücke durch digitale Identitäten wurden durch einen intensiven Austausch erarbeitet. Dieser erfolgte im Rahmen von internen Diskussionen innerhalb des Konsortiums, zwei Experten-Workshops mit Teilnehmerinnen und Teilnehmern aus Forschung und Energiewirtschaft sowie mehreren Interviews mit Expertinnen und Experten aus verschiedenen Stakeholder-Gruppen. Diese Schritte sind in Abbildung 2 dargestellt und werden im Folgenden erläutert.

1) Aufzeigen und Kommunizieren des Mehrwertes digitaler Identitäten im Energiesystem

Der erste Schritt besteht darin, den Mehrwert digitaler Identitäten im Energiesystem systematisch aufzuzeigen. Dazu sollten bereits bestehende synergetische Betrachtungen von Anwendungsfällen und digitalen Identitäten durch Forschungsprojekte (z. B. BANULA und DEER), die von verschiedenen politischen Akteuren wie dem BMW E gefördert und in enger Kooperation mit Industrie und Forschung durchgeführt werden, fortgesetzt werden. Dabei sollte auf bestehendes Wissen und vorhandene Ressourcen aus vorherigen Projekten (z. B. BMIL oder DIVE) angeknüpft werden, mit dem Ziel, den Nutzen von anlagenspezifischen digitalen Identitäten für verschiedene Anwendungsfälle evidenzbasiert zu demonstrieren und zu kommunizieren.

2) Schaffung von gesellschaftlicher und politischer Akzeptanz sowie eines gemeinsamen Verständnisses

Der zweite Schritt besteht darin, gesellschaftliche und politische Akzeptanz für die digitale Transformation des Energiesektors zu schaffen. Die Lehren aus vergleichbaren Projekten bezüglich einer digitalen Dateninfrastruktur wie eIDAS 2.0 oder GAIA-X zeigen, dass eine erfolgreiche Umsetzung nur möglich ist, wenn die zentralen Stakeholder von Beginn an eingebunden werden. Dies schafft die Grundlage für eine breite Akzeptanz und damit eine umfassende Unterstützung für die Einführung digitaler Identitäten in Energiewirtschaft, Industrie und Politik.

Gleichzeitig soll in diesem Schritt ein gemeinsames Verständnis über die angestrebte Ausgestaltung digitaler Identitäten geschaffen werden. Im Rahmen von öffentlichen Diskursen, Dialogangeboten und Online-Plattformen sollen verschiedene Ausgestaltungsmöglichkeiten digitaler Identitäten diskutiert werden. Zentrale Aspekte wie die der Governance, der Finanzierung und der eingesetzten Technologien sind dabei kritisch zu analysieren und die damit zusammenhängenden Fragen zu beantworten.

3) Demonstration der Durchführbarkeit und Skalierbarkeit

Nachdem der Mehrwert von digitalen Identitäten aufgezeigt und eine gesellschaftliche und politische Akzeptanz geschaffen wurde, fokussiert sich der dritte Schritt auf den praxisnahen Nachweis der Durchführbarkeit. Dieser Schritt ist notwendig, um die bisherigen Prototypen und Piloten auf ein größeres Umfeld (z. B. in abgegrenzten Modellregionen) auszuweiten und darin zu erproben. Als Vorbild für ein Vorgehen kann das Vorhaben der *Schaufenster Sichere Digitale Identitäten* des BMW E dienen, bei dem in verschiedenen Schwesterprojekten (ID-Ideal, IDUnion, ONCE und SDIKA) gemeinsam mit Wirtschaft, öffentlicher Verwaltung, Forschung und Technologieunternehmen verschiedene Anwendungen, Architekturen und Technologien erprobt werden.

In vergleichbarer Weise könnten in diesem Schritt in verschiedenen, eng miteinander verbundenen Projekten unterschiedliche Ansätze digitaler Identitäten im Energiesektor anhand einer Vielzahl von Anwendungsfällen und Interessengruppen evaluiert werden. Dadurch können die Ergebnisse des gemeinsamen Diskurses aus Schritt 2 anhand einer realen Umsetzung überprüft und die Ergebnisse zur weiteren Präzisierung der Ausgestaltung digitaler Identitäten genutzt werden.

4) Weiterentwicklung von Technologien und Standards

Sobald die Durchführbarkeit in einem großen Umfeld demonstriert wurde, sollten die Technologien und Standards systematisch vorangetrieben werden. Dies zielt darauf ab, von funktionalen Piloten zu einer produktionsreifen Umgebung für digitale Identitäten zu gelangen und eine breite Anwendung im Energiesektor zu ermöglichen. Das erfordert eine enge Zusammenarbeit von Expertinnen und Experten aus Forschung und Industrie. Dieser Schritt hat zwei wesentliche Bestandteile: Zum einen sollen von den Akteuren akzeptierte Regeln und Governance-Strukturen für digitale Identitäten im Energiesystem erarbeitet werden. Ähnlich wie bei der Marktkommunikation müssen dazu alle Rollen und Verantwortlichkeiten beschrieben werden. Zum anderen sollen hier eine finale technische Infrastruktur sowie eine standardisierte Interoperabilität festgelegt und weiterentwickelt werden. Dies betrifft beispielsweise die Architektur von Schnittstellen, die Formate von Daten oder auch Absicherungen und Anreizsysteme bezüglich der Bereitstellung von Daten.

Gleichzeitig sollten Plattformen etabliert werden, um Wissen und Technologien für alle Akteure der Energiewirtschaft und darüber hinaus zugänglich zu machen. Diese Plattformen sind vor allem für kleinere Akteure wie private Anlagenbetreiber und kleine Verteilnetzbetreiber von Bedeutung, die häufig nicht über die

gleichen Ressourcen und Kompetenzen verfügen wie größere Unternehmen. Der Wissensaustausch kann durch Webportale, Fachkonferenzen, Workshops und kontinuierliche Weiterbildungsprogramme gefördert werden, um sicherzustellen, dass alle Beteiligten die neue Dateninfrastruktur effektiv nutzen können. Dieser sektorenübergreifende Wissensaustausch knüpft an die nationalen Bestrebungen zum Aufbau eines Dateninstituts an, das als „Think and Do Tank“ fungieren und zur Bündelung von Expertise sowie zur Bereitstellung von Lösungen und Methodenkompetenz genutzt werden soll (BMI 2023).

5) Etablierung eines ausgereiften Marktes mit sicherem Rechtsrahmen

Der letzte Schritt auf dem Weg zur Implementierung digitaler Identitäten im Energiesystem ist die Etablierung eines ausgereiften Marktes mit einem rechtssicheren Rahmen. Aufbauend auf den in Schritt 4 determinierten Technologien und Standards zielt dieser Schritt darauf ab, die breite Anwendung und Akzeptanz digitaler Identitäten bei allen relevanten Akteuren zu fördern. Ein wesentlicher Aspekt dieses Schrittes ist die verbindliche regulatorische Umsetzung der zuvor festgelegten Standards und

Governance-Strukturen. Diese Umsetzung sollte sicherstellen, dass der rechtliche Rahmen für die Nutzung digitaler Identitäten eindeutig definiert und in der Praxis durchsetzbar ist. Das bietet den Marktteilnehmern die nötige Rechtssicherheit, um Vertrauen in die neuen digitalen Prozesse und Technologien zu entwickeln und es nachhaltig zu erhalten.

Darüber hinaus sollten Anreizstrukturen für Endnutzer geschaffen werden, um die Nutzung digitaler Identitäten im Energiesystem zu fördern. Dies kann durch die Entwicklung einer Vielzahl von sektorenübergreifenden Anwendungsfällen erreicht werden, die den Mehrwert der Verwendung digitaler Identitäten für Endnutzer transparent aufzeigen und auf der zuvor aufgebauten Infrastruktur aufbauen. Dabei sollte ein möglichst niedrigschwelliger Zugang für Endnutzer geschaffen werden. Das bedeutet, dass der Zugang zu digitalen Identitäten und ihrer Nutzung ohne große technische oder administrative Hürden ermöglicht wird. Dazu können eine breit angelegte Informationskampagne, umfassende Hilfestellungen auf Basis der zuvor aufgebauten Wissensplattformen sowie die Anknüpfung an bestehende Identitätsökosysteme wie eIDAS 2.0 beitragen.

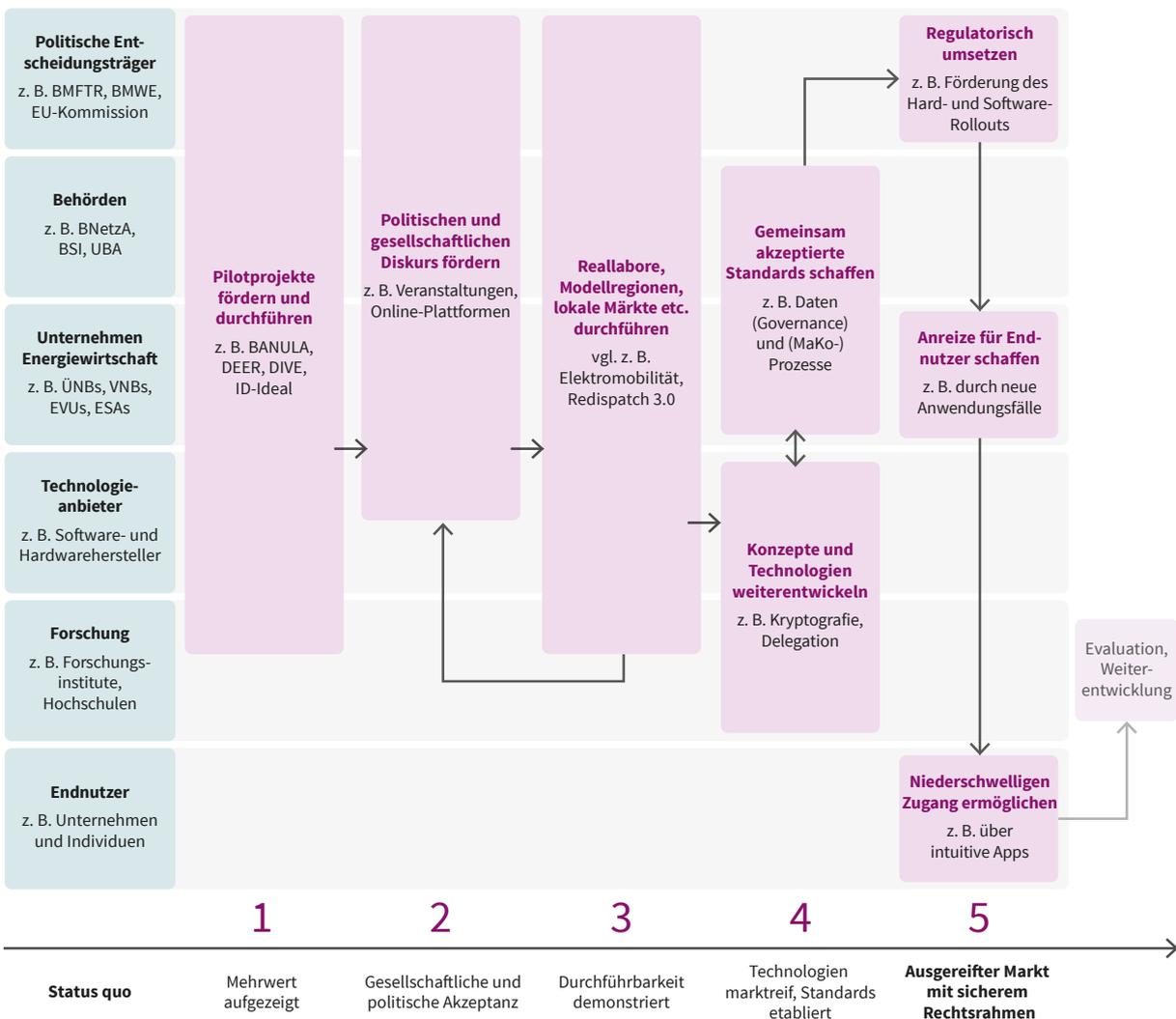


Abbildung 2: Ein Weg zur Schließung der digitalen Identitätslücke

Fazit – Vom Zielbild zur Umsetzung

Der Erfolg der Energiewende ist maßgeblich von einer umfassenden digitalen Transformation abhängig. Nur eine durchgängige Digitalisierung, die sich bis auf die Ebene einzelner Geräte und Anlagen erstreckt, ermöglicht diese Transformation. Um diese herausfordernde Aufgabe zu bewältigen, müssen Skaleneffekte genutzt werden, indem dieselbe Dateninfrastruktur sektorenübergreifend für verschiedenste Anwendungsfälle eingesetzt wird. Digitale Identitäten sind ein Baustein zum Erzielen dieser Skaleneffekte, da sie eine eindeutige Identifikation von Anlagen im Energiesystem ermöglichen und den vertrauenswürdigen Austausch von Stamm- und Bewegungsdaten für innovative Anwendungsfälle (z. B. virtuelle Kraftwerke oder feingranulare Emissionszertifikate) sichern. Die Nutzung eines dezentralen Ansatzes für digitale Identitäten reduziert redundante Datenhaltung und ermöglicht es Anlagenbetreibern, ihre Daten selbstbestimmt und flexibel zu verwenden.

Durch die digitale Einbindung von Erzeugungs- und Verbrauchsanlagen mittels digitaler Identitäten können bestehende manuelle und papierbasierte Prozesse ersetzt werden. Ziel sollte eine grundlegende Transformation des Energiesystems sein, die dabei über die reine Digitalisierung bestehender Prozesse hinausgeht und nahtlose, automatisierte Interaktionen zwischen Anlagen und Akteuren ermöglicht. Dies erfordert eine grundlegende Neustrukturierung der Abläufe und Prozesse (Elia Group 2023). Die in den Blitzlichtern genannten Beispiele, wie die Nachverfolgung von CO₂-Emissionen über die gesamte Lieferkette und die skalierbare Umsetzung von virtuellen Kraftwerken, unterstreichen das transformative Potenzial einer digitalisierten Energiewirtschaft. Die neu ermöglichten Anwendungsfälle sowie die effizientere Gestaltung bestehender Anwendungsfälle durch neue, digitale Prozesse stellen die wesentlichen Werttreiber des Zielbildes für digitale Identitäten dar. Aktuelle Forschungsprojekte (z. B. BANULA, DEER und ID-Ideal) verdeutlichen sowohl die Notwendigkeit dieser Technologie als auch ihr Potenzial, um den Herausforderungen der Energiewende zu begegnen.

Berücksichtigung von technischen und regulatorischen Rahmenbedingungen

Das DIVE-Projekt wählt bewusst keinen Greenfield-Ansatz, der den Aufbau einer völlig neuen Architektur ohne Rücksicht auf bestehende Systeme vorsieht. Stattdessen wird eine integrierende Herangehensweise verfolgt, die existierende Strukturen und Prozesse aufgreift und in die Ausgestaltung einbezieht. Dieser Ansatz zielt darauf ab, die vorhandene Infrastruktur zum Austausch von Energiedaten zu nutzen und zielgerichtet weiterzuentwickeln.

Vor diesem Hintergrund wurde im Projekt auch die Anbindung an die Smart-Meter-Gateway-Infrastruktur erprobt. Diese Infrastruktur wird zukünftig eine Schlüsselrolle bei der Erfassung und dem Austausch von feingranularen Messdaten spielen. Somit kann die SMGW-Infrastruktur einen Baustein für die Etablierung digitaler Identitäten für Anlagen darstellen und ihre Einführung beispielsweise durch die Mitbenutzung bestehender Schnittstellen beschleunigen. Die vollständige Realisierung der skizzierten Anwendungsfälle erfordert jedoch regulatorische und technische Anpassungen, insbesondere hinsichtlich der Berechtigung zur Nutzung der von modernen Messeinrichtungen erhobenen Daten und bereitgestellten Kommunikationskanäle.

Zusammenarbeit aller Stakeholder

Um eine umfassende Transformation des Energiesystems auf Basis digitaler Identitäten zu ermöglichen, muss eine kritische Masse an Stakeholdern erreicht werden. Das Spektrum der erforderlichen Akteure erstreckt sich über verschiedene Ebenen und Sektoren. Von den etablierten Akteuren der Stromwertschöpfungskette – Stromerzeuger, Netzbetreiber und Energieversorger – bis hin zu Technologieanbietern, Regulierungsbehörden und Endverbrauchern: Jeder dieser Akteure bringt wichtige Perspektiven und spezielle Expertise ein, die jeweils von entscheidender Bedeutung sind, um einen effektiven und ganzheitlichen Transformationsprozess zu gestalten. Insbesondere die partizipative Einbindung von Technologieanbietern und Endverbrauchern ist entscheidend, um innovative Lösungen zu entwickeln, die sowohl an das aktuelle Stromsystem anknüpfen können als auch benutzerzentriert sind und damit den Erfolg und die Akzeptanz digitaler Innovationen im Energiesektor fördern.

Literaturverzeichnis

50Hertz; Amprion; TenneT; Transnet BW (2024): Technische Anforderung für den Anschluss von Elektrolyseanlagen. Online verfügbar unter https://www.netztransparenz.de/xspproxy/api/staticfiles/ntp-relaunch/dokumente/%C3%BCber%20uns/studien%20und%20positionspapiere/anforderungen%20an%20elektrolyseanlagen/2024_technische_anforderungen_f%C3%BCr_den_anschluss_von_elektrolyseanlagen.pdf.

Babel, Matthias; Gramlich, Vincent; Guthmann, Claus; Schober, Marcus; Körner, Marc-Fabian; Strüker, Jens (2023): Vertrauen durch digitale Identifizierung: Über den Beitrag von SSI zur Integration von dezentralen Oracles in Informationssysteme. In: HMD 60 (2), S. 478–493. DOI: 10.1365/s40702-023-00955-3.

Babel, Matthias; Gramlich, Vincent; Körner, Marc-Fabian; Sedlmeir, Johannes; Strüker, Jens; Zwede, Till (2022): Enabling end-to-end digital carbon emission tracing with shielded NFTs. In: Energy Inform 5 (S1). DOI: 10.1186/s42162-022-00199-3.

Barr, Earl T.; Harman, Mark; McMinn, Phil; Shahbaz, Muzammil; Yoo, Shin (2015): The Oracle Problem in Software Testing: A Survey. In: IEEE Trans. Software Eng. 41 (5), S. 507–525. DOI: 10.1109/TSE.2014.2372785.

BDEW (2021): Digitale Transformation für die Energiewende – Energiewende für die digitale Transformation. Strategiepapier mit Impulsen der Energiewirtschaft zur digitalen Transformation für die nächste Legislaturperiode. Online verfügbar unter https://www.bdew.de/media/documents/210909_BDEW_Strategiepapier_Digitale_Transformation_f%C3%BCr_die_Energiewende_final.pdf.

BDEW (2023): Rollenmodell für die Marktkommunikation im deutschen Energiemarkt. Arbeitsgrundlagen Marktkommunikation. Bundesverband der Energie- und Wasserwirtschaft e.V. Online verfügbar unter https://www.bdew.de/media/documents/2023-03-06-AWH-Rollenmodell_MaKo_V2.1_BcwsudV.pdf.

BDEW (2024): Regelungen zum Übertragungsweg für AS4. Regelungen zum sicheren Austausch von Übertragungsdateien. Online verfügbar unter https://www.bundesnetzagentur.de/DE/Beschlusskammern/BK06/BK6_83_Zug_Mess/835_mitteilungen_datenformate/Mitteilung_41/Anlagen/Regelungen_zum_%C3%9Cbertragungsweg_AS4_2.2.pdf?__blob=publicationFile&v=1.

BMI (2023): Dateninstitut. Bundesministerium des Innern und für Heimat. Online verfügbar unter <https://www.bmi.bund.de/DE/themen/it-und-digitalpolitik/it-des-bundes/dateninstitut/dateninstitut-node.html>.

Bogensperger, Alexander; Regener, Vincenz (2023): Energiegemeinschaften und die Rolle des Prosumers. Hrsg. v. FfE. Online verfügbar unter <https://www.ffe.de/wp-content/uploads/2023/06/Energiegemeinschaften-und-die-Rolle-des-Prosumers-Diskussionspapier.pdf>.

BSI (2021): Technische Richtlinie BSI TR-03109-1. Anforderungen an die Interoperabilität der Kommunikationseinheit eines intelligenten Messsystems. Online verfügbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03109/TR03109-1.pdf?__blob=publicationFile&v=4.

BSI (2023): Smart-Meter-Gateway. Cybersicherheit für die Digitalisierung der Energiewirtschaft. Online verfügbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Smart-Meter-Gateway.pdf?__blob=publicationFile&v=8

BSI (2024): Impulspapier Steuerung mit Nachweisführung im Smart-Meter-Gateway. Online verfügbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03109/TR-03109_Impulspapier_Steuerung.html.

Buck, Christoph; Eymann, Torsten; Jelito, Dennis; Schlatt, Vincent; Schweizer, André; Strobel, Jacqueline; Weiß, Florian (2023): Cyber-Sicherheit für kritische Energieinfrastrukturen – Handlungsempfehlungen zur Umsetzung einer Zero-Trust-Architektur. In: HMD 60 (2), S. 494–509. DOI: 10.1365/s40702-023-00944-6.

Bundesnetzagentur (2024a): Webhilfe des Marktstammdatenregisters. Online verfügbar unter <https://www.marktstammdatenregister.de/MaStRHilfe/subpages/registrierungVerpflichtendAnlagen.html>.

Bundesnetzagentur (2024b): Zielsetzung des Marktstammdatenregisters. Bundesnetzagentur. Online verfügbar unter <https://www.marktstammdatenregister.de/MaStRHilfe/subpages/GrundlagenZielsetzung.html>.

Bundesnetzagentur (2024c): Zubau Erneuerbarer Energien 2023. Online verfügbar unter https://www.bundesnetzagentur.de/SharedDocs/Pressemitteilungen/DE/2024/20240105_EEGZubau.html.

Burges, Karsten; Creutzburg, Philipp; Maas, Nele; Nabe, Christian (2022): Netzdienliche Flexibilitätsmechanismen. Synthesebericht 2 des SINTEG Förderprogramms, Studie im Auftrag des BMWK. Online verfügbar unter https://www.researchgate.net/publication/361760745_Netzdienliche_Flexibilitatsmechanismen_Synthesebericht_2_des_SINTEG_Forderprogramms.

Cavoukian, Ann (2009): Privacy by Design. The 7 Foundational Principles. Information and privacy commissioner of Ontario, Canada.

Chadwick, David W.; Kubach, Michael; Sette, Ioram; Johnson Jeyakumar, Isaac Henderson (2023): Establishing Trust in SSI Verifiers. In: Open Identity Summit 2023. Online verfügbar unter <https://dl.gi.de/server/api/core/bitstreams/bb2f71fc-6d0b-4add-87e2-61d73d0e1edf/content#page=16>.

dena (2022): Energy Communities: Beschleuniger der dezentralen Energiewende. Mit digitalen Technologien auf dem Weg zu neuen Rollen im Energiesystem der Zukunft. Hrsg. v. Deutsche Energie-Agentur GmbH. Online verfügbar unter https://www.dena.de/fileadmin/dena/Publikationen/PDFs/2022/dena-ANALYSE_Energy_Communities_Beschleuniger_der_dezentralen_Energiewende.pdf.

dena (2023a): Das dezentralisierte Energiesystem im Jahr 2030. Ein systemischer Bottom-up-Ansatz zur Marktintegration dezentraler Verbrauchs- und Erzeugungseinheiten. Hrsg. v. Deutsche Energie-Agentur GmbH. Online verfügbar unter https://www.dena.de/fileadmin/dena/Publikationen/PDFs/2023/231130_dena_Das_dezentralisierte_Energiesystem_im_Jahr_2030_WEB.pdf.

dena (2023b): Digitale Maschinen-Identitäten als Grundbaustein für ein automatisiertes Energiesystem. Aufbau eines Identitätsregisters auf Basis der Blockchain-Technologie (Pilot: Blockchain Machine Identity Ledger). Hrsg. v. Deutsche Energie-Agentur GmbH. Online verfügbar unter https://future-energy-lab.de/app/uploads/2022/08/Digitale_Maschinen-Identitaeten_als_Grundbaustein_fuer_ein_automatisiertes_Energiesystem.pdf.

dena (2024a): Energy Sharing in Deutschland. Vom Konzept zur energiewirtschaftlichen Umsetzung. Hrsg. v. Deutsche Energie-Agentur GmbH. Online verfügbar unter https://www.dena.de/fileadmin/dena/Publikationen/PDFs/2024/dena_FEL_Energy-Sharing_Bericht_Web.pdf.

dena (2024b): Grundlagen und Bedeutung von Datenräumen für die Energiewirtschaft. Hrsg. v. Deutsche Energie-Agentur GmbH. Online verfügbar unter https://future-energy-lab.de/app/uploads/2024/04/dena_Bericht_Grundlagen-und-Bedeutung-von-Datenraeumen-fuer-die-Energiewirtschaft-dena-ENDA.pdf.

dena (2024c): Intelligentes Messsystem. Grundpfeiler zur Digitalisierung des Energiesystems. Hrsg. v. Deutsche Energie-Agentur GmbH. Online verfügbar unter https://www.dena.de/fileadmin/dena/Publikationen/PDFs/2024/SET_Hub_Intelligentes_Messsystem.pdf.

Eckert, Claudia (2018): IT-Sicherheit. De Gruyter.

Elia Group (2021): Towards a Consumer-Centric and Sustainable Electric System. Online verfügbar unter https://www.elia.be/-/media/project/elia/shared/documents/elia-group/publications/studies-and-reports/20210618_elia_ccmd-white-paper_en.pdf.

Elia Group (2023): SSI in the Energy sector: A study. Unter Mitarbeit von Vincent Gramlich, Marc-Fabian Körner, Anne Michaelis und Jens Strüker. Online verfügbar unter https://innovation.eliagroup.eu/-/media/project/elia/innovation/images/innovationprojects/ssi-in-the-energy-sector---a-study/20231116_studyssi.pdf.

ENTSO-E, EFET, eBIX (2022): The harmonised electricity market role model. Online verfügbar unter https://eepublicdownloads.entsoe.eu/clean-documents/EDI/Library/HRM/Harmonised_Role_Model_2022-01.pdf.

Europäische Kommission (2022): Revision of the eIDAS Regulation. Finding on its implementation and application. Online verfügbar unter [https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/699491/EPRS_BRI\(2022\)699491_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/699491/EPRS_BRI(2022)699491_EN.pdf).

Graebig, Markus; Rogler, Niko; Erdmann, Georg; Uhlig, Ingo (2023): Strom, Netz, Fluss: Ein Atlas unserer Stromwelt und ihres Wandels. 2. Aufl. Ellery Studio.

Kotthoff, F., Muschner, C., Tepe, D., Vogt, E., & Hülk, L. (2025): Monitoring Germany's Core Energy System Dataset: A Data Quality Analysis of the Marktstammdatenregister. ACM SIGENERGY Energy Informatics Review, 4(4), 88-99. Online verfügbar unter <https://dl.acm.org/doi/abs/10.1145/3717413.3717421>.

Körner, Marc-Fabian; Schober, Marcus; Ströher, Tobias; Strüker, Jens (2023): Digital Carbon Accounting for Accelerating Decarbonization: Characteristics of IS-Enabled System Architectures. Online verfügbar unter <https://www.fim-rc.de/Paperbibliothek/Veroeffentlicht/1580/wi-1580.pdf>.

Leinauer, Christina; Wagon, Felix; Strüker, Jens (2024): Leveraging Twin Transformation. Digital Infrastructures to Advance Decarbonisation at the Nexus of Energy and Mobility. Online verfügbar unter https://www.fit.fraunhofer.de/content/dam/fit/wirtschaftsinformatik/dokumente/Leveraging-Twin-Transformation_Digital-Infrastructures-to-Advance-Decarbonisation-at-the-Nexus-of-Energy-and-Mobility.pdf.

Papadis, Elisa; Tsatsaronis, George (2020): Challenges in the decarbonization of the energy sector. In: Energy 205, S. 118025. DOI: 10.1016/j.energy.2020.118025.

Platsios, Antonios; Kotis, Konstantinos; Goumopoulos, Christos (2023): A systematic review on semantic interoperability in the IoT-enabled smart cities. In: Internet of Things 22, S. 100754. DOI: 10.1016/j.iot.2023.100754.

Preukschat, Alex (2021): Self-Sovereign Identity. Decentralized digital identity and verifiable credentials. Manning Publications.

Rahman, Hafizur; Hussain, Md. Iftekhar (2020): A comprehensive survey on semantic interoperability for Internet of Things: State of the art and research challenges. In: Trans Emerging Tel Tech 31 (12), Artikel e3902. DOI: 10.1002/ett.3902.

Schellinger, Benjamin; Sedlmeir, Johannes; Willburger, Lukas; Strüker, Jens; Urbach, Nils (2022): Mythbusting Self-Sovereign Identity (SSI): Diskussionspapier zu selbstbestimmten digitalen Identitäten. Online verfügbar unter https://www.fit.fraunhofer.de/content/dam/fit/de/documents/Whitepaper_Mythbusting_Self-Sovereign_Identity.pdf.

Sedlmeir, Johannes; Smethurst, Reilly; Rieger, Alexander; Fridgen, Gilbert (2021): Digital Identities and Verifiable Credentials. In: Business & Information Systems Engineering 63 (5), S. 603–613. DOI: 10.1007/s12599-021-00722-y.

Strong, Diane M.; Lee, Yang W.; Wang, Richard Y. (1997): Data quality in context. In: Commun. ACM 40 (5), S. 103–110. DOI: 10.1145/253769.253804.

Strüker, Jens; Urbach, Nils; Guggenberger, Tobias; Lautenschlager, Jonathan; Ruhland, Nicolas; Schlatt, Vincent et al. (2021): Self-Sovereign Identity. Grundlagen, Anwendungen und Potenziale portabler digitaler Identitäten. Online verfügbar unter <https://www.fim-rc.de/wp-content/uploads/2021/06/Fraunhofer-FIT%5fSSI%5fWhitepaper.pdf>.

VDE FFN (2024): VDE FNN Hinweis: Anforderungen an die technische Ausgestaltung der physikalischen und logischen Schnittstellen der Steuerungseinrichtung zum Anschluss und zur Übermittlung des Steuerbefehls an eine steuerbare Verbrauchseinrichtung oder ein Energie-Management-System. Online verfügbar unter https://www.bundesnetzagentur.de/DE/Beschlusskammern/1_GZ/BK6-GZ/2022/BK6-22-300/Mitteilung/Mitteilung_2/VDE%20FNN%20Empfehlung%20zu%20Tenorziffer%20a.pdf?__blob=publicationFile&v=1.

Wanner, Jonas; Herm, Lukas-Valentin; Heinrich, Kai; Janiesch, Christian (2022): The effect of transparency and trust on intelligent system acceptance: Evidence from a user-based study. In: Electron Markets 32 (4), S. 2079–2102. DOI: 10.1007/s12525-022-00593-5.

Wietschel, Martin; Plötz, Patrick; Pfluger, Benjamin; Klobasa, Marian; Eßer, Anke; Haendel, Michael et al. (2018): Sektorkopplung. Definition, Chancen und Herausforderungen.

Abkürzungen

ARF	Architecture and Reference Framework
AS4	Applicability Statement 4
BANULA	Barrierefreie und NUTzerfreundliche LAdemöglichkeiten schaffen
BDEW	Bundesverband der Energie- und Wasserwirtschaft
BMFTR	Bundesministerium für Forschung, Technologie und Raumfahrt
BMI	Bundesministerium des Innern
BMIL	Blockchain Machine Identity Ledger
BMWE	Bundesministerium für Wirtschaft und Energie
BNetzA	Bundesnetzagentur
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIG	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik
CSDDD	Corporate Sustainability Due Diligence Directive
DEER	Dezentraler Redispatch. Für ein Energiesystem von morgen und eine Elektrifizierung der Zukunft
CSRD	Corporate Sustainability Reporting Directive
DSGVO	Datenschutz-Grundverordnung
EBSI	European Blockchain Services Infrastructure
eIDAS 2.0	EU-Verordnung über elektronische Identifizierung und Vertrauensdienste (Electronic Identification, Authentication and Trust Services)
ESA	Energieserviceanbieter
eSSIF	European Self-Sovereign Identity Framework
EUDIW	Europäische Brieftasche für die digitale Identität (European Digital Identity Wallet)
EVU	Energieversorgungsunternehmen



HEMS	Heim-Energiemanagementsystem
Fraunhofer FIT	Fraunhofer-Institut für Angewandte Informationstechnik
GWKHV	Gas-Wärme-Kälte-Herkunftsnachweisregister-Verordnung
HKNR	Herkunftsnachweisregister
MaKo	Marktkommunikation
MaStR	Marktstammdatenregister
MaStRV	Marktstammdatenregisterverordnung
MsbG	Messstellenbetriebsgesetz
SMGW	Smart Meter Gateway
SM-PKI	Smart Meter Public Key Infrastructure
SSI	Self-Sovereign Identity
UBA	Umweltbundesamt
ÜNB	Übertragungsnetzbetreiber
VNB	Verteilnetzbetreiber

