Future Energy
Lab

BERICHT

DIVE – Digitale Identitäten als Vertrauensanker im Energiesystem

01 – Überblick, Einordnung und Evaluation

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
Claus Guthmann, Fraunhofer FIT
Felix Paetzold, Fraunhofer FIT
Tobias Ströher Fraunhofer FIT
Prof. Dr. Jens Strüker, Fraunhofer FIT
Linda Babilon, dena
Irene Adamski, dena

Konzeption und Gestaltung:
die wegmeister gmbh

Stand:
Juli 2025

Bitte zitieren als:
Deutsche Energie-Agentur (Hrsg.) (dena, 2025): DIVE – Digitale Identitäten als Vertrauensanker im Energiesystem. 01 – Überblick, Einordnung und Evaluation

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.

DIVE in aller Kürze

Warum braucht es digitale Identitäten?

Die Entwicklung digitaler Identitäten wird seit mehreren Jahren vorangetrieben. Sie sollen in unserer zunehmend digitalisierten und automatisierten Welt einen Vertrauensanker bilden. Digitale Identitäten garantieren, dass wir mit dem richtigen Gegenüber kommunizieren (digitale Identifizierung), dem wir unsere Daten auch wirklich anvertrauen wollen und dass diese Personen, Organisationen oder auch Maschinen echt sind (digitale Authentifizierung). Darüber hinaus müssen wir – vor allem in sensiblen Bereichen wie kritischen Infrastrukturen – sicherstellen können, dass die ausgetauschten Daten vollständig, korrekt und aktuell sind (digitale Verifikation). Während in der analogen Welt für diese Art der Überprüfung viele Wege und Möglichkeiten entwickelt wurden, steht dies in der digitalen Welt erst am Anfang: die EUDI-Wallet wird gerade in allen EU-Staaten auf den Weg gebracht, um natürliche Personen mit digitalen Identitäten auszustatten; eine EU-Business-Wallet für Organisationen und juristische Personen wird derzeit erarbeitet. Die Bereitstellung von digitalen Identitäten für Maschinen und Anlagen ist eine dritte und völlig neue Entwicklung, die für eine konsequente Automatisierung von Prozessen jedoch essenziell ist. Diese Maschinenidentitäten konnte das Team des DIVE-Projektes nicht nur für verschiedene Geräte und Anlagen (z.B. Photovoltaik-Anlagen, Wärmepumpen, Speicher) bereitstellen, sondern auch für aktuelle Prozesse und innovative Anwendungsfälle in die praktische Erprobung bringen.

Ein Vertrauensdreieck für mehr digitale Souveränität

DIVE verwendet ein digitales Identitätsmanagementsystem, welches auf den Prinzipien von selbst-souveränen digitalen Identitäten (SSI) aufbaut. Es geht dabei um eine Gewaltenteilung zwischen den drei Akteuren, die es für eine digitale Identifizierung, Authentifizierung und Verifizierung braucht: jemanden, der eine digitale Identität für sich beansprucht (Rolle 1, Holder), beispielsweise Name, Adresse oder Alter. Da es sich dabei aber anfangs nur um Behauptungen handelt, werden die gemachten Angaben einer vertrauenswürdigen Autorität zugesandt (Rolle 2, Issuer), mit der Bitte um Bestätigung (vergleichbar mit einem Stempel oder Siegel auf beglaubigten Dokumenten). Sind die Angaben korrekt und verifiziert, wird ein digitaler Nachweis über die Richtigkeit ausgestellt. Dieser Nachweis kann dann gegenüber Dritten (Rolle 3, Verifier) ausweisen, dass die Angaben zu einer Person, Organisation oder eben Anlage (bspw., dass die Anlage Grünstrom erzeugt) richtig, echt und aktuell sind. Man spricht hierbei von einem sogenannten Vertrauensdreieck: Holder und Verifier kennen sich nicht, aber vertrauen jeweils dem Issuer. Durch den Nachweis des Issuers können beide vertrauensvoll miteinander interagieren.

Neu bei dieser Art der Interaktion ist, dass der gesamte Vorgang digital, automatisiert und in Echtzeit erfolgen kann und dass dafür keine Inhalte ausgetauscht werden müssen, sondern eingangs nur eine Wahr-oder-Falsch-Meldung über die Vertrauenswürdigkeit der Daten. Der Vertrauensaufbau kann so datensparsam wie möglich erfolgen und alle sensiblen Daten verbleiben im größtmöglichen Umfang unter der Kontrolle und im Eigentum von Nutzern und realen Personen – die digitale Identität wird souverän selbstverwaltet.

Glaubwürdig und automatisierbar – digitale Maschinenidentitäten sind Grundlage für die Skalierung der Energiewende

Trotz der Fortschritte bei der Digitalisierung des Energiesystems fehlt bisher eine sektorenübergreifende, skalierbare Dateninfrastruktur, die eine sichere, effiziente und flexible Einbindung von Anlagen in verschiedene Anwendungsfälle (z.B. Flexibilität, granulare Herkunftsnachweise) im dezentralen Energiesystem ermöglicht. Insbesondere die Marktintegration von Kleinanlagen ist bisher mit erheblichem Aufwand verbunden. Eine effiziente Energieversorgung kann zukünftig jedoch 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 (bspw. Art und

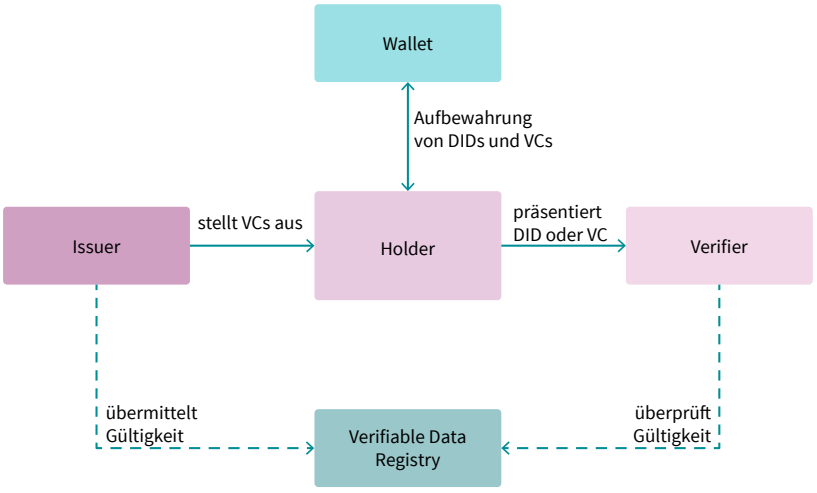

Abbildung 1: Vertrauensdreieck

Besitzer der Anlagen) als auch Bewegungsdaten (bspw. gemessene Erzeugungs- und Verbrauchsdaten) (dena 2024b). Die mangelhafte Datenerfassung und Verifizierbarkeit von Eigenschaften von kleinen und beweglichen Anlagen (bspw. E-Autos) im Energiesystem wird als „digitale Identitätslücke“ bezeichnet. Die DIVE-Basisinfrastruktur liefert einen Lösungsweg, um diese Lücke zu schließen. Im Pilotvorhaben konnten unterschiedliche Prozesse (bspw. Anmeldung einer Anlage in einem Register, Wechsel zwischen Anwendungsfällen) von der Anlage bis zum Anwendungsbereich (z.B. Grünstromnachweis) erfolgreich über digitale Identitäten durchgeführt und verwaltet werden.

Die DIVE-Basisinfrastruktur als Blaupause

DIVE zeigt einen anschlussfähigen Lösungsweg für die digitale Identitätslücke im Energiesystem: Mithilfe bereits im Markt vorhandener Komponenten und Standards sowie unter Ausnutzung bereits bestehender Strukturen und Abläufe im Energiesystem (bspw. SMGW) können sektorenübergreifende Lösungen für Endverbraucher, Netzbetreiber und Anbieter von neuen Dienstleistungen, wie virtuelle Kraftwerke oder Grünstromvermarktung, angeboten werden.

Als „DIVE-Basisinfrastruktur“ wird das im Projekt erprobte Zusammenspiel von Hardware und Software-Komponenten bezeichnet: Energiemanagementsystem (EMS), intelligentes Messsystem, Digitale Identitäten (DID), Digitale Nachweise (VCs), verifizierbares Register.

Im Ergebnis konnte DIVE zeigen, wie digitale Identitäten für Maschinen – in diesem Fall insbesondere Kleinanlagen des Energiesystems – mit relativ geringem Aufwand eingeführt werden können, um notwendige Aufgaben zur Stabilisierung und Verwaltung der Stromnetze einfacher zu machen und innovative neue Anwendungsfälle leichter zu integrieren.

Anforderungen an digitale Identitäten und die Frage der Rechtskonformität

Eine große Hürde bei der Einführung neuer Technologien ist oft die Frage von Haftung und Datenschutz. Im Energiesystem spielen zudem Cybersicherheitsanforderungen an kritische Infrastrukturen eine wichtige Rolle. Um diese Hürde abzubauen, wurde das DIVE-Projekt von Anfang an durch juristische Fachexpertise begleitet und beraten.

Während an einzelnen Stellen noch Verbesserungspotenzial für den Gesetzgeber besteht, was die Berücksichtigung dezentraler und verteilter Systeme bspw. bei Haftungsregelungen betrifft, ist hervorzuheben, dass die DIVE-Basisinfrastruktur als rechtskonforme Lösung angelegt ist, die im derzeit geltenden regulatorischen Rahmen betrieben werden kann. Es wurde eine praxistaugliche Governance-Struktur konzipiert und die Anwendbarkeit auf bekannte Anwendungsfälle (bspw. Anknüpfung ans Marktstammdatenregister, Lieferantenwechsel an der Ladesäule, Flexibilitätserbringung) geprüft.

Nächste Schritte

Das DIVE-Projekt liefert einen Vorschlag für eine Basisinfrastruktur, die die Anforderungen an Sicherheit und Leistungsfähigkeit sowie die Bedürfnisse der betrachteten energiewirtschaftlichen Anwendungsfälle erfüllt. Die einzelnen Komponenten sind durchdacht – energiewirtschaftlich, technisch, juristisch – aber müssen sich bei der Skalierung und Ausweitung im realen Umfeld unter Beweis stellen. Der Ansatz von Digitalen Identitäten als Vertrauensanker im Energiesystem dient daher als Ausgangspunkt für weitere Projekte, um die Diskussion um das digitale Identitätsökosystem im Energiesystem mit einem breiteren Stakeholderkreis fortzusetzen.

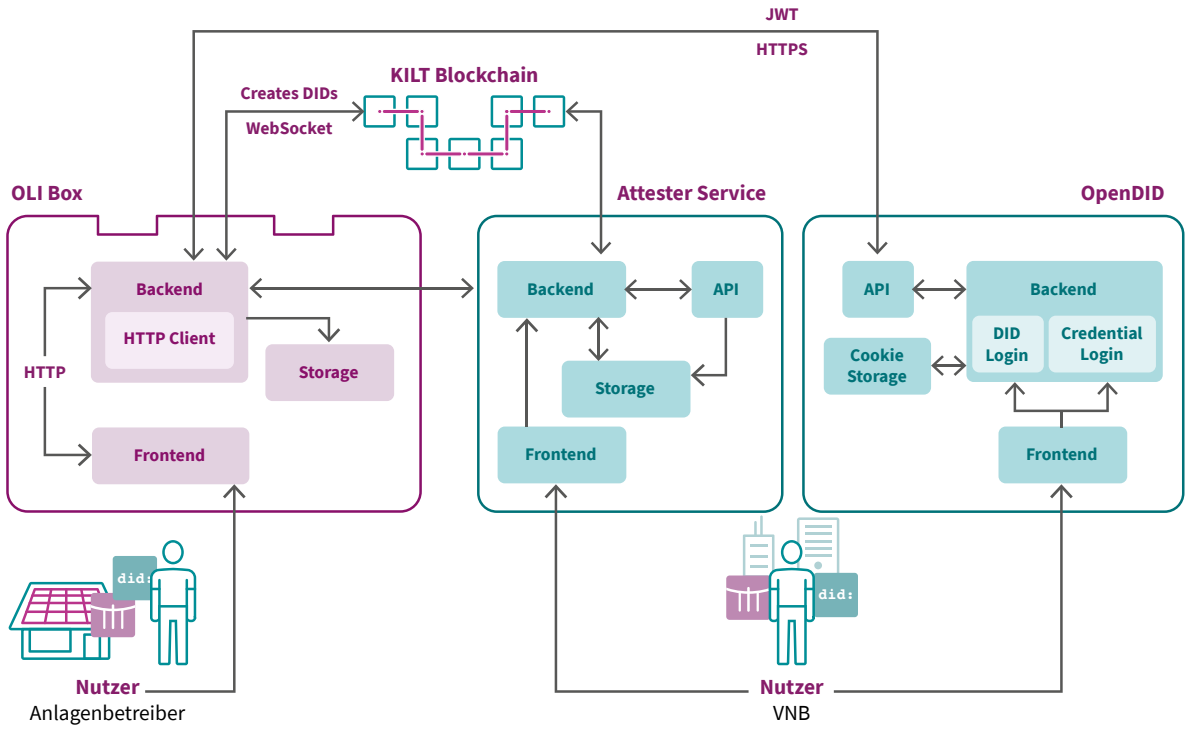

Abbildung 2: DIVE Basisinfrastruktur

Inhalt

1. Das Energiesystem im Wandel

Die Energiewende erhöht zusammen mit der damit verbundenen Sektorenkopplung die Komplexität des Energiesystems. Die Dezentralisierung der Stromerzeugung durch den Ausbau erneuerbarer Energien ist dabei ein wesentlicher Treiber: Dezentrale Anlagen wie Photovoltaik-Anlagen – aktuell über 4 Millionen in Deutschland mit einer installierten Leistung von 99,8 Gigawatt (AGEE-Stat, Destatis)– ersetzen zunehmend zentrale fossile Kraftwerke. Bis 2030 soll diese Kapazität auf 215 Gigawatt durch den Bau neuer Anlagen steigen. Gleichzeitig steigen durch die fortschreitende Elektrifizierung von Sektoren wie Mobilität und Wärme der Stromverbrauch und die Anzahl der Verbraucher. Diese zunehmende Dezentralisierung von Erzeugung und neue Verbraucher erfordern immer mehr und teilweise komplexere Eingriffe, um Netzengpässe zu vermeiden und die Stabilität des Stromsystems zu gewährleisten.

Parallel zu den technischen Herausforderungen entwickelt sich ein immer anspruchsvollerer und über das Energiesystem hinausreichender regulatorischer Rahmen. Zentrale Elemente dieses erweiterten Rahmens sind der *EU Green Deal*, die *Corporate Sustainability Reporting Directive* (CSRD) und die *Corporate Sustainability Due Diligence Directive* (CSDDD). Im Kern verlangen die Regulierungen von Unternehmen und Organisationen eine präzise und transparente Berichterstattung über Emissionen und weitere Nachhaltigkeitskriterien. Damit stellen sie hohe Anforderungen an die Qualität und Verfügbarkeit energierelevanter Daten (Körner et al. 2024b).

Um die steigende Komplexität zu bewältigen und gleichzeitig diese regulatorischen Anforderungen effizient zu erfüllen, wird eine konsequente Ende-zu-Ende-Digitalisierung bis auf die Anlagenebene diskutiert (Elia Group 2021). Die Gestaltung dieser Digitalisierung wird bereits in zahlreichen nationalen und internationalen Projekten konkret untersucht. Dabei konzentrieren sich Initiativen wie dena-ENDA, der Use Case „Energie“ im Dateninstitut (derzeit im Aufbau) sowie energy data-X[1] auf den Aufbau sektorenspezifischer Datenräume und damit die Schaffung einer Dateninfrastruktur für den Austausch feingranularer Energiedaten. Projekte wie DEER[2] und BANULA[3] veranschaulichen die Umsetzung innovativer Anwendungsfälle in einem digitalisierten Energiesystem. Trotz dieser Fortschritte fehlt weiterhin eine gemeinsame, sektorenweite und sektorenübergreifende Dateninfrastruktur, die eine sichere und effiziente Einbindung von Anlagen in ein digitalisiertes Energiesystem ermöglicht. Insbesondere für Kleinstanlagen ist die Anbindung an eine solche Dateninfrastruktur bislang mit erheblichem Aufwand verbunden.

Das *Projekt Digitale Identitäten als Vertrauensanker im Energiesystem* (DIVE) schließt diese Lücke, indem es dezentrale Anlagen mithilfe digitaler Identitäten in das Energiesystem integriert. Durch die eindeutige Identifizierung und Authentifizierung von Anlagen ermöglicht DIVE zukunftsorientierte Anwendungsfälle wie feingranulare Treibhausgaszertifikate oder marktbasierte Maßnahmen zur Netzstabilisierung (Babel et al. 2023). Aufbauend auf dem abgeschlossenen Projekt *Blockchain Machine Identity Ledger* (BMIL) pilotiert DIVE die Ausstattung von Energieanlagen mit digitalen Identitäten, um ihre Einbindung in flexible und skalierbare Nutzungsszenarien zu ermöglichen, ohne die digitale Souveränität der Anlagenbetreiber zu beeinträchtigen (dena 2023b).

1 https://www.energydata-x.eu/

2 DEER – Dezentraler Redispatch. Für ein Energiesystem von morgen und eine Elektrifizierung der Zukunft, https://www.deer-projekt.de/

3 BArrierefreie und NUtzerfreundliche LAdemöglichkeiten schaffen, https://www.banula.de/

Digitalisierung des Energiesystems

Die digitale Transformation der Energiewirtschaft in Deutschland und der Europäischen Union (EU) dient der Erreichung des übergeordneten Ziels der Treibhausgasneutralität bis 2045 (Deutschland) bzw. 2050 (EU). Zur Unterstützung dieser Transformation wurden zentrale Programme wie das *Digital Europe Programme* und *Horizon Europe* etabliert. Diese Programme zielen unter anderem darauf ab, die Energiewende durch den gezielten Einsatz von digitalen Technologien und Innovationen zu beschleunigen.

Die digitale Transformation des Energiesystems zeigt sich konkret in umfangreichen Reformen des europäischen Strommarktes. So strebt das Paket *Clean Energy for all Europeans* durch verschiedene Verordnungen und Richtlinien einen integrativen Elektrizitätsmarkt an, der den Wettbewerb fördert und die Verbraucherrechte stärkt. Insbesondere die *Richtlinie (EU) 2019/944* (EU-Richtlinie mit gemeinsamen Vorschriften für den Elektrizitätsbinnenmarkt) treibt die Entwicklung digitaler und intelligenter Energiesysteme voran und schafft den rechtlichen Rahmen für den Strombinnenmarkt. Diese europäischen Vorgaben bilden die Grundlage für nationale Umsetzungsmaßnahmen.

Auf nationaler Ebene forciert das *Erneuerbare-Energien-Gesetz* (EEG) den Ausbau erneuerbarer Energien und enthält Regelungen zur Digitalisierung des Energiesektors. Ergänzend dazu schafft das *Gesetz zur Digitalisierung der Energiewende* (GDEW) den Rahmen für den flächendeckenden Einsatz digitaler Technologien im Stromnetz. Während das EEG vorrangig auf die Förderung und Integration erneuerbarer Energien abzielt, legt das GDEW den Fokus auf die Digitalisierung der Infrastruktur, die eine effiziente Nutzung und Steuerung dieser dezentralen Erzeugungseinheiten ermöglicht. Ein zentrales Element dieser Digitalisierung ist der Rollout von zertifizierten intelligenten Messsystemen (iMys), die in die Smart-Meter-Gateway-Infrastruktur (SMGW-Infrastruktur) eingebunden werden (dena 2024b). Aktuell erproben mehrere Pilotprojekte die Anbindung von Erzeugungs- und Verbrauchseinheiten über die CLS-Schnittstelle (Controllable Local System) an diese Infrastruktur (BSI 2024). Dies ermöglicht die sichere Ansteuerung von Anlagen, die praktische Umsetzung regulatorischer Vorgaben sowie die Entwicklung neuer Anwendungsfälle.

Europäische Datenstrategie und Datenräume

Die EU verfolgt mit ihrer Datenstrategie das Ziel, einen Binnenmarkt für Daten zu etablieren, der Europas globale Wettbewerbsfähigkeit stärkt und die Datensouveränität sichert. Der Energiesektor wurde als Schlüsselsektor identifiziert, in dem die verbesserte Nutzung von Energiedaten von großer strategischer Relevanz ist (Leinauer et al. 2024). Zentrale Bedeutung kommt dabei dem Data Act zu, der den Zugang und die Nutzung von Daten unabhängig vom Speicher- oder Verarbeitungsort reguliert. Ein Kernkonzept dieser Strategie sind Datenräume (Data Spaces) – föderierte Dateninfrastrukturen, die Unternehmen, Individuen und Maschinen die sichere Erzeugung, den Austausch und die Analyse von Daten ermöglichen (dena 2024a). Insbesondere im Energiesektor wird das Potenzial von Datenräumen hervorgehoben. Diese Datenräume ermöglichen einen effizienten und sicheren Datenaustausch zwischen den verschiedenen Akteuren des Sektors unter Wahrung der digitalen Souveränität aller Beteiligten. Ein Beispiel ist das vom Bundesministerium für Wirtschaft und Energie (BMWE) geförderte Projekt energy data-X, das einen datensouveränen und hochskalierbaren Energiedatenaustausch demonstriert.

2. Grundlagen digitaler Identitäten

2.1 Von zentralisierten zu dezentralisierten Identitätsmodellen

Digitale Identitäten bilden das Fundament für vertrauenswürdige Interaktionen in vernetzten Systemen. Sie ermöglichen die eindeutige Identifizierung, sichere Authentifizierung und gezielte Autorisierung von Personen und Entitäten in digitalen Prozessen. Digitale Identitäten erstrecken sich über diverse Plattformen und Dienste, wobei diese von Social-Media-Accounts bis hin zu beruflichen oder hoheitlichen Identitäten reichen, die ein rechtssicheres Signieren von Dokumenten ermöglichen (Europäische Kommission 2022; Schellinger et al. 2022).

Digitale Identitäten sind nicht nur für Personen, sondern auch für Organisationen und Maschinen von großer Bedeutung, besonders im Kontext digitalisierter Energiesysteme. Digitale Maschinen-Identitäten können verifizierbare Attribute wie die Art der Anlage, die Leistung und den Standort enthalten – ähnlich wie personenbezogene Stammdaten. Diese Identitäten schaffen Vertrauen in digitale Interaktionen, besonders wenn sie durch vertrauenswürdige Akteure wie zertifizierte Installateure oder Verteilnetzbetreiber ausgestellt werden (dena 2023b). Um die Sicherheit und dauerhafte Zuordnung dieser Identitäten zu gewährleisten, können die Daten in Hardware Security Modules (HSMs) gespeichert werden, wodurch eine eindeutige Zuordnung zur jeweiligen Maschine sichergestellt wird (Babel et al. 2023; dena 2023b). Mittels einer kryptografischen Verknüpfung von Stamm- und Bewegungsdaten lässt sich das Vertrauen in digitale Identitäten auf die Echtzeitdaten einer Anlage ausweiten, um Integrität und Authentizität der Daten sicherzustellen. Diese Verknüpfung erlaubt die lückenlose Rückverfolgbarkeit zur ursprünglichen Anlage und ermöglicht Anwendungsfälle wie die Ausstellung feingranularer CO_2-Zertifikate, wie sie im Rahmen des Innovationswettbewerbs „Schaufenster Sichere Digitale Identitäten“ des BMWE im Projekt *ID-Ideal* umgesetzt wurden (Körner et al. 2024b).

Self-Sovereign Identities (SSI) und eIDAS 2.0

Traditionell werden digitale Identitäten bislang in zentralisierten Systemen verwaltet, die parallel und unabhängig voneinander operieren. Dies führt zu einer Fragmentierung der Identitätsdaten, da sie mehrfach in verschiedenen Systemen geführt werden müssen (Preukschat 2021; Sedlmeir et al. 2021a). Föderierte Modelle adressieren zwar diese Fragmentierung durch eine verbesserte Interoperabilität, führen jedoch zu einer Konzentration auf wenige große Plattformen und deren Identitätsprovider (sogenanntes Single Sign-On). Dies resultiert in einer erhöhten Abhängigkeit sowie einer eingeschränkten Kontrolle der Nutzer über ihre Daten. Dezentrale Identitätsmodelle, insbesondere das SSI-Paradigma, adressieren diese Herausforderungen, indem sie den Nutzern die volle Kontrolle über ihre Identitätsdaten ermöglichen. Persönliche Informationen werden als Verifiable Credentials in Digital Wallets gespeichert und können selbstbestimmt genutzt werden. Dieser nutzerzentrierte Ansatz fördert ein datenschutzfreundliches Identitätsmanagement (Strüker et al. 2021).

Die Europäische Union greift diese Entwicklung mit der Novellierung der eIDAS-Verordnung (eIDAS 2.0, EU-Verordnung über elektronische Identifizierung und Vertrauensdienste) auf und treibt sie damit entscheidend voran. Ein wesentliches Element dieser Verordnung ist die Einführung der European Digital Identity (EUDI) Wallet. Diese digitale Brieftasche ermöglicht es EU-Bürgerinnen und -Bürgern, ihre Identitätsnachweise, Zertifikate und andere verifizierbare Berechtigungsnachweise (Verifiable Credentials) sicher in der EUDI-Wallet zu speichern und anwendungsübergreifend zu nutzen. Dabei werden die sensiblen Identitätsdaten ausschließlich auf den Geräten der Nutzer gespeichert. Die praktische Umsetzung der EUDI-Wallet erfolgt in enger Abstimmung zwischen den EU-Mitgliedstaaten, wobei verschiedene Large Scale Pilots die technische Machbarkeit und Nutzerakzeptanz evaluieren. Ziel ist es, dass bis 2027 Unternehmen die EUDI-Wallet akzeptieren und bis 2030 mindestens 80 Prozent der EU-Bevölkerung EUDI-Wallets nutzen (Urbach et al. 2024).

2.2 Grundzüge eines SSI-Systems

Ein auf SSI basierendes System setzt sich aus mehreren Schlüsselkomponenten zusammen. Im Folgenden werden die grundlegenden Elemente beschrieben, die aus dezentralen Identifikatoren (Decentralized Identifiers), verifizierbaren Nachweisen (Verifiable Credentials), Digital Wallets und fest definierten Rollen bestehen (Sedlmeir et al. 2021a; Preukschat 2021).

Decentralized Identifiers (DIDs) ermöglichen die Identifikation von Personen oder Entitäten, wie beispielsweise Anlagen oder Unternehmen, und bieten eine dezentrale, unabhängige digitale Identität. DIDs verweisen auf korrespondierende DID-Dokumente, die kryptografische Schlüssel und Metadaten enthalten und zur Interaktion und Authentifizierung verwendet werden.

Verifiable Credentials (VCs) sind digitale Zertifikate, die Informationen über eine Person oder Entität wie Stammdaten oder Berechtigungen enthalten. VCs können unterschiedliche Aussagen umfassen, beispielsweise Stammdaten aus einem Personalausweis oder aus Mitgliedskarten für Fitnessstudios oder Stammdaten für eine Anlage. Ein Verifiable Credential wird bei seiner Erstellung digital signiert und ist dadurch verifizierbar: So lässt sich kryptografisch überprüfen, von welchem Aussteller

es stammt und ob die enthaltenen Informationen unverändert sind. Fortgeschrittene kryptografische Technologien wie Zero-Knowledge Proofs (ZKPs) ermöglichen die selektive Offenlegung von Attributen, wobei die Privatsphäre des Nutzers geschützt und gleichzeitig die Datenintegrität gewährleistet wird.

Eine **Digital Wallet** ist eine Softwareanwendung, mit der Nutzer ihre eigenen Identitätsdaten sicher verwalten können. Sie ermöglicht das sichere Speichern der Credentials direkt auf einem eigenen Gerät wie einem Smartphone sowie ihre selektive Präsentation mittels kryptografischer Beweise. Vergleichbar mit einer physischen Brieftasche können verschiedene Credentials in der Anwendung gespeichert werden. Der Nutzer kann dabei selektiv entscheiden, welche Informationen geteilt werden sollen, und behält so die volle Kontrolle über jede Transaktion. Die Wallet zeigt vor jeder Freigabe, welche Daten mit welchen Empfängern geteilt werden sollen (Babel et al. 2024).

Abbildung 3 veranschaulicht, wie DIDs und VCs gemeinsam eine digitale Maschinen-Identität formen. Der menschliche Besitzer der Anlage erzeugt in einem einfachen Verfahren an seinem Endgerät einen individuellen Identifier, aus dem eine eindeutige DID-Kennung erzeugt wird (die Anlage ist eindeutig identifizierbar).

In einem zweiten Schritt werden der Anlage Attribute zugeordnet (z. B. Erzeugungsleistung, Speicherkapazität etc.). Sie werden durch ein VC digital zur Verfügung gestellt. Nach Verifizierung durch eine vertrauenswürdige Authorität (z. B. ein Mitarbeiter des lokalen Netzbetreibers) wird das VC der Anlagen-DID zugeordnet. Die entstandene Maschinen-Identität kann die Anlage im digitalen Raum eindeutig identifizieren und vertrauenswürdige Aussagen über die Anlageneigenschaften präsentieren.

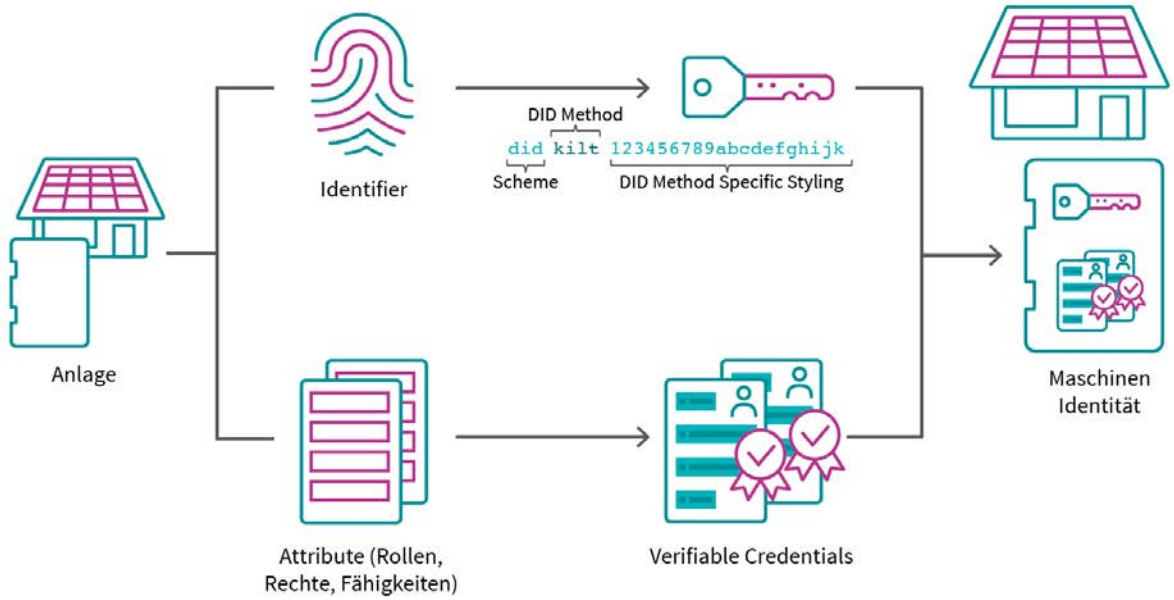

Abbildung 3: Schematische Darstellung der Verwendung von DIDs und VCs im Kontext von digitalen Maschinen-Identitäten

Abbildung 4 bietet eine Übersicht über die verschiedenen Rollen und ihre Interaktionen in einem SSI-basierten System (Mühle et al. 2018). In diesem Vertrauensdreieck agieren der Issuer und der Verifier nicht direkt miteinander, sondern kommunizieren indirekt über den Holder und das Verifiable Data Registry:

- **Issuer:** Eine vertrauenswürdige Instanz, die VCs ausstellt. Diese VCs sind kryptografisch signiert und gewährleisten die Integrität und Authentizität der Daten.
- **Holder:** Die Person oder Entität, die VCs in einer Digital Wallet speichert und bei Bedarf verwendet, um sich oder ihre Attribute verifizierbar nachzuweisen.
- **Verifier:** Ein Akteur, der vom Holder eine Verifiable Presentation der benötigten Daten anfordert. Hierbei wird nachgewiesen, dass die Informationen gültig sind und vom Issuer nicht widerrufen wurden.
- **Verifiable Data Registry:** Ein vertrauenswürdiges Verzeichnis zur Überprüfung der Gültigkeit und Authentizität von VCs, ohne dass der Issuer direkt kontaktiert werden muss.

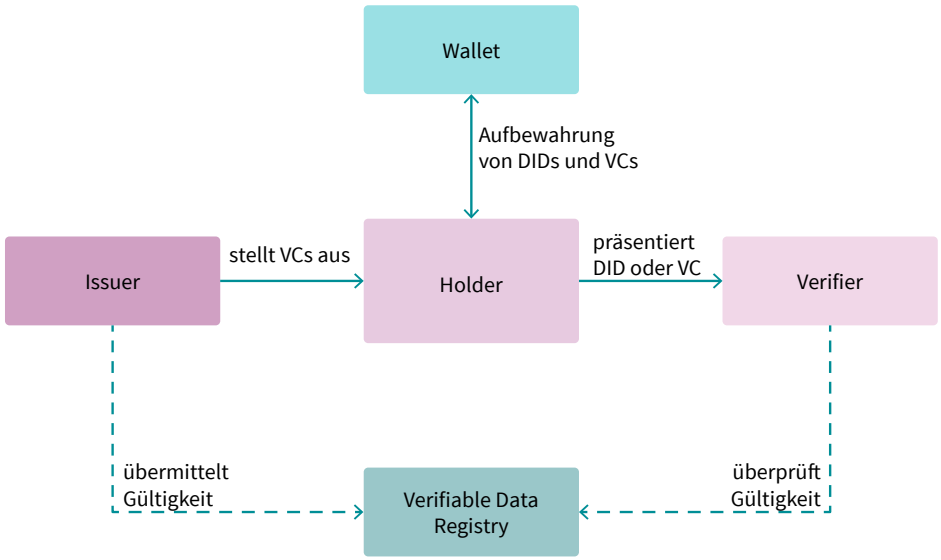

Abbildung 4: Rollen eines SSI-Systems

3. Die digitale Identitätslücke

Die bestehenden Infrastrukturen für das Austauschen von Energiedaten sind heue nicht ausreichend, um den wachsenden Anforderungen eines zunehmend dezentralen Energiesystems gerecht zu werden. Diese Diskrepanz manifestiert sich in einer fundamentalen digitalen Lücke: Während die Komplexität des Energiesystems durch die Integration erneuerbarer Energien und neuer Marktteilnehmer kontinuierlich steigt, befindet sich die Ende-zu-Ende-Digitalisierung der bestehenden Infrastrukturen noch ganz am Anfang. Die durchgängige Digitalisierung des Energiesektors ist jedoch eine wichtige Voraussetzung für eine nachhaltige, kosteneffiziente und schnelle Energiewende (Leinauer et al. 2024; BDEW 2021).

Die digitale Lücke zeigt sich in drei zentralen Bereichen: Erstens fehlt eine skalierbare Dateninfrastruktur für den sicheren und kontinuierlichen Austausch von Bewegungsdaten innerhalb des Energiesektors (Möller et al. 2024; dena 2024a). Ebenso existiert bislang kein Interoperabilitätskonzept für eine sektorenübergreifende Datennutzung, die für die Umsetzung der Sektorenkopplung als zentrales Element der Energiewende erforderlich ist (European Coalition for bidirectional Charging 2024; Leinauer et al. 2024). Bisher ist beispielsweise ein Elektroauto nicht im Marktstammdatenregister angelegt, sodass das Anbieten und Durchführen von Systemdienstleistungen durch ein E-Fahrzeug nicht ohne Weiteres möglich sind. Der dritte Bereich umfasst die digitale Identitätslücke, deren Schließung im Projekt DIVE adressiert wird. Denn relevante Stammdaten zu den Eigenschaften von Anlagen im Energiesystem, wie beispielsweise Typ oder Standort, sind häufig unvollständig, uneinheitlich, nicht qualitätsgesichert verfügbar und nur selten kryptografisch verifiziert (Elia Group 2023; dena 2023b). Diese Limitation verhindert die nahtlose digitale Integration dezentraler Anlagen – sowohl innerhalb des Energiesektors als auch sektorenübergreifend. Zusätzlich erschwert dies die kryptografisch gesicherte Verknüpfung von Echtzeit-Bewegungsdaten mit verifizierbaren Stammdaten, wodurch eine präzise und nachweisbare Nutzung bzw. Berücksichtigung der erzeugten oder verbrauchten Energie der Anlagen nur teilweise möglich ist (Babel et al. 2023).

3.1 Charakteristika der digitalen Identitätslücke im Energiesystem

Im Folgenden wird diese digitale Identitätslücke im Energiesystem anhand von fünf zentralen Dimensionen skizziert:

Vertrauen in die Anlagendaten bildet das Fundament für die erfolgreiche Digitalisierung des Energiesystems. Der sichere und effiziente Betrieb kritischer Energieinfrastrukturen erfordert eine durchgängig hohe Datenqualität. Systemrelevante Akteure müssen darauf vertrauen können, dass die erhobenen und ausgetauschten Daten vollständig und korrekt sind. Derzeit sind die Datenerhebung und der Austausch durch fehleranfällige Medienbrüche und manuelle Prozesse beeinträchtigt, was die Datenqualität erheblich mindert (BDEW 2021). Digitale Identitäten können diese Fehlerquellen reduzieren, indem vertrauenswürdige Stellen die Richtigkeit der Stammdaten gewährleisten und sie als signierte und unveränderliche Stammdaten bereitstellen (Babel et al. 2023).

Die erfolgreiche Umsetzung der Sektorenkopplung erfordert einen nahtlosen Datenaustausch zwischen den verschiedenen Sektoren des Energiesystems (European Coalition for bidirectional Charging 2024; Leinauer et al. 2024). Innerhalb des Energiesektors existieren gegenwärtig erhebliche Defizite hinsichtlich der Interoperabilität digitaler Infrastrukturen, sowohl auf technischer als auch auf semantischer Ebene. Dies verhindert eine effektive sektorenübergreifende Datennutzung. Die **technische Interoperabilität** bildet durch die Verwendung gleicher Protokolle und Datenformate die Grundlage für die systemübergreifende Kommunikation, während die **semantische Interoperabilität** die einheitliche Interpretation der ausgetauschten Daten sicherstellt. So muss beispielsweise ein Übertragungsnetzbetreiber sicherstellen, dass seine Definitionen und Anforderungen an ein Elektrofahrzeug mit der vom Fahrzeughersteller ausgestellten digitalen Identität des Fahrzeugs übereinstimmen. Ein sektorenübergreifender Identifikator kann eine einheitliche und verlässliche Nutzung von Stammdaten sowie von anlagenbezogenen Bewegungsdaten über verschiedene Systeme hinweg ermöglichen (Elia Group 2021; BDEW 2021).

Das zunehmend dezentralisierte Energiesystem bringt auch neue Herausforderungen für die Stabilität des Stromnetzes mit sich (dena 2023a). Nur durch eine präzise Steuerung, die in Echtzeit stattfindet und sowohl Stromerzeuger als auch Verbraucher einbezieht, lassen sich Engpässe vermeiden und lässt sich Netzstabilität sichern (Körner et al. 2024a) Derzeit fehlt jedoch ein sicheres Verfahren für die **Authentifizierung und Autorisierung** zwischen den energiewirtschaftlichen Akteuren und Anlagen, was die gezielte Steuerung der Anlagen erschwert (Buck et al. 2023; Körner et al. 2024a). Digitale Identitäten adressieren diese Herausforderung durch die Bereitstellung kryptografischer Vertrauensanker, die eine eindeutige Identifizierung und sichere Authentifizierung aller Akteure ermöglichen sowie die Integrität, Aktualität und Vollständigkeit der ausgetauschten Bewegungsdaten, Stammdaten und Steuersignale garantieren. Zudem erlauben sie durch ihre maschinenlesbaren technischen Schnittstellen eine schnelle und automatisierbare Weiterverarbeitung.

Die erfolgreiche Transformation des Energiesystems erfordert die aktive **Partizipation aller relevanten Stakeholder**, wobei insbesondere Prosumer eine Schlüsselrolle einnehmen. Ein wesentliches Hindernis stellt dabei ihr derzeit eingeschränkter Zugang zum Energiemarkt dar (Bogensperger und Regener 2023; Michaelis et al. 2024). So schränken die bestehenden digitalen Infrastrukturen die Datensouveränität der Akteure ein und verhindern damit eine selbstbestimmte Kontrolle über die eigenen Daten und ihre Nutzung für weitere Anwendungsfälle. Zukunftsfähige digitale Systeme müssen daher die spezifischen Anforderungen aller Stakeholder adressieren und insbesondere Prosumern die volle Kontrolle über ihre Anlagen- und Verbrauchsdaten ermöglichen (Elia Group 2021; Wanner et al. 2022). Digitale Identitäten schaffen hierfür die technische Grundlage: Sie ermöglichen die sichere Integration der eigenen Anlagen und damit die Marktbeteiligung der Prosumer für verschiedene Anwendungsszenarien.

Eine **skalierbare und flexible Dateninfrastruktur** bildet das technische Fundament für die Transformation des Energiesystems. Diese Infrastruktur muss zwei zentrale Anforderungen erfüllen: einerseits die Integration einer exponentiell wachsenden Anzahl dezentraler Anlagen und Akteure, andererseits die Ermöglichung innovativer Anwendungsfälle durch den Austausch von Echtzeitdaten (BDEW 2021). Bestehende Dateninfrastrukturen im Energiesystem sind jedoch nicht für die wachsende Anzahl an Anlagen und Anwendungsfällen ausgelegt (dena 2024a). Digitale Identitäten ermöglichen die automatisierte und skalierbare Einbindung von Anlagen in digitale Infrastrukturen: Nach der einmaligen Ausstellung einer digitalen Maschinen-Identität kann diese flexibel für verschiedene Anwendungsfälle verwendet werden.

3.2 Anforderungen an digitale Identitäten im Energiesystem

Im Folgenden werden die spezifischen Anforderungen an digitale Identitäten detaillierter beschrieben und anschließend wird in einem Zielbild skizziert, wie diese Anforderungen im Energiesystem ausgestaltet werden können.

Digitale Identitäten bieten verifizierbare Stammdaten und dienen als Vertrauensanker für sichere digitale Transaktionen im Energiesystem. Eine **hohe Datenqualität** – insbesondere hinsichtlich der Korrektheit und Vollständigkeit dieser Stammdaten – ist unerlässlich (Babel et al. 2023). Um die Erfüllung dieser Qualitätsanforderungen systematisch und nachhaltig zu gewährleisten, ist ein strukturierter Rahmen für Vertrauensbeziehungen zu empfehlen. Ein entsprechendes Trust-Framework sollte durch klare Regeln und Prozesse sicherstellen, dass eine durchgängig hohe Datenqualität gewährleistet wird. Dieses Framework legt dann unter anderem fest, welche Attribute eine digitale Identität enthält und welche Akteure, beispielsweise zertifizierte Installateure oder Verteilnetzbetreiber, berechtigt sind, diese Daten zu bestätigen. Diese autorisierten Akteure stellen Verifiable Credentials mit Aussagen über die Anlagen aus und gewährleisten damit die Korrektheit der Stammdaten. Die Integrität der Daten wird durch kryptografische Verfahren sowie durch eine starke Bindung der Anlage an ihre digitale Identität sichergestellt. Die Implementierung dieser Sicherheitsmaßnahmen kann, abhängig vom erforderlichen Schutzniveau, entweder softwarebasiert oder durch ein Hardware Security Module erfolgen (dena 2023b).

Die Gewährleistung einer hohen Datenqualität ermöglicht eine vollständig automatisierte Integration dezentraler Energieanlagen in systemrelevante Anwendungsfälle, wodurch zeit- und kostenintensive manuelle Validierungsprozesse eliminiert werden können.

Die **eindeutige Identifikation** von Anlagen sowie die eindeutige Identifikation der beteiligten Akteure bilden eine elementare Voraussetzung für ihre Integration in ein digitalisiertes Energiesystem (Elia Group 2023). Die gegenwärtige Identifikationsinfrastruktur beschränkt sich auf die Netzanschlussebene über die SMGW-Infrastruktur. Aktuelle Weiterentwicklungen schlagen vor, diese Infrastruktur um digitale Maschinen-Identitäten auf Einzelanlagenebene zu erweitern, um auf diese Weise eine präzise Anlagensteuerung zu ermöglichen (BSI 2024; VDE FFN 2024). Für Anlagenbetreiber mit mehreren Anlagen ist die Verwaltung benutzerfreundlich und intuitiv zu gestalten. Durch die Möglichkeit, Maschinen-Identitäten eines Haushalts oder eines Unternehmens gebündelt zu präsentieren, können Anlagenbetreiber diese effizient verwalten, ohne dass die Anforderungen an eine anlagenscharfe Identifikation beeinträchtigt werden.

Eine eindeutige Identifikation ermöglicht die gezielte Ansteuerung für Flexibilitätsabrufe. Dies schafft die Voraussetzung für eine sichere und effiziente Integration dezentraler Flexibilitätspotenziale.

Die Umsetzung der europäischen Datenstrategie[4] erfordert eine **sektorenübergreifende Anwendungsoffenheit** von digitalen Identitäten. Eine einzelne digitale Identität muss in verschiedenen Anwendungsdomänen – vom Energiesektor über den Mobilitätsbereich bis hin zur Industrie – einsetzbar sein (Leinauer et al. 2024; Möller et al. 2024). Die daraus resultierende domänenübergreifende Nutzbarkeit schafft ein durchgängiges Identitätsökosystem und reduziert technische und organisatorische Eintrittsbarrieren. Die standardisierte Verwendung von Stammdaten in heterogenen digitalen Infrastrukturen unterstützt dabei zentrale Zielsetzungen der europäischen Datenstrategie hinsichtlich Interoperabilität und Datensouveränität (Leinauer et al. 2024).

Ein exemplarischer Anwendungsfall ist die Nutzung der digitalen Identität eines Elektrofahrzeugs: Die verifizierten Stammdaten können sowohl für Abrechnungsprozesse an Ladeinfrastrukturen im Energiesektor als auch für die Wartungs- und Servicedokumentation im Mobilitätssektor verwendet werden.

Digitale Identitäten sollten den Nutzern die volle Kontrolle über ihre Daten gewährleisten. Sie müssen **selbstbestimmt entscheiden** können, welche spezifischen Daten sie zu welchem Zweck mit welchen Akteuren teilen möchten. Diese Form der individuellen Datensouveränität ist entscheidend für die Akzeptanz digitaler Infrastrukturen (Sedlmeir et al. 2021a). Nach dem „Privacy by Design"-Ansatz sollten Systeme so gestaltet sein, dass Datenschutzaspekte von vorneherein berücksichtigt und nur minimale Daten erhoben werden (Cavoukian 2009). Ansätze wie die der selbstverwalteten digitalen Identitäten (Self-Souvereign Identities, SSI) unterstützen dies, indem sie persönliche Daten direkt in den Wallets der Nutzer speichern und sie erst nach ausdrücklicher Zustimmung freigeben.

Ein Beispiel ist die Anmeldung bei einem neuen Energiedienstleister, bei der Anlagenbetreiber transparent nachvollziehen können, welche Daten zu welchem Zweck abgefragt werden.

4 https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_de

Digitale Identitäten müssen den **gesetzlichen Regularien** des Energiesystems und der digitalen Infrastruktur entsprechen.[5] Die Verarbeitung personenbezogener Daten unterliegt der Datenschutz-Grundverordnung (DSGVO), die die Einhaltung von Grundsätzen wie Datenminimierung und Zweckbindung vorschreibt. Nutzer müssen daher informiert werden, welche Daten erhoben, wie sie verwendet und wie lange sie gespeichert werden. Gleichzeitig muss der Schutz vor unbefugten Zugriffen auf sensible Daten, die insbesondere im Energiesystem anfallen, zu jeder Zeit gegeben sein (Buck et al. 2023). Zusätzlich eröffnet die dezentrale Speicherung in Digital Wallets neue Angriffsvektoren wie Social Engineering, was durch technische Maßnahmen wie Verifier-Authentifizierung und Nutzersensibilisierung adressiert werden muss. Die Energieinfrastruktur ist gemäß § 2 Absatz 10 des IT-Sicherheitsgesetzes als Kritische Infrastruktur (KRITIS) klassifiziert. Diese Einstufung erfordert besondere Sicherheitsmaßnahmen, um die Resilienz und kontinuierliche Verfügbarkeit der Infrastruktur zu gewährleisten (Buck et al. 2023).

Die dezentrale Speicherung der Stammdaten direkt in den digitalen Geldbörsen der Anlagenbetreiber erhöht die Resilienz des Systems, da zentrale Speicherpunkte vermieden werden.

Die folgende Tabelle bietet eine strukturierte Übersicht über die verschiedenen Aspekte und Anforderungen, die durch digitale Identitäten im Energiesystem adressiert werden:

Digitale Identitätslücke				
Vertrauen in Daten	Sektorenübergreifende Interoperabilität	Sichere Ansteuerung	Ausrichtung an Stakeholdern	Skalierbarkeit

Anforderung	Einsatz 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

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

5 Eine ausführliche Diskussion erfolgt im Berichtsteil „Rechtliche Analyse".

4. DIVE-Projekt

Das folgende Kapitel stellt die im DIVE-Projekt entwickelte Basisinfrastruktur für digitale Identitäten im Energiesystem vor. Neben der technischen Architektur werden implementierte Anwendungsfälle präsentiert, die das Potenzial der digitalen Identitätsinfrastruktur für die Digitalisierung des Energiesystems demonstrieren. Die detaillierte technische und energiewirtschaftliche Analyse erfolgt in den entsprechenden Berichtsteilen.

4.1 Ziele von DIVE

Das DIVE-Projekt baut auf den Erkenntnissen des BMIL-Projekts (dena 2023b) auf und erforscht die Implementierung digitaler Maschinen-Identitäten für energiewirtschaftlich relevante Anlagen wie Photovoltaik-Anlagen, Wärmepumpen und Speicher.

Kernziel ist die Erarbeitung eines Proof of Concept, der die praktische Anwendung der entwickelten Infrastruktur demonstriert und die Integration vertrauenswürdiger digitaler Identitäten in bestehende energiewirtschaftliche Systeme aufzeigt – insbesondere in die Smart-Meter-Gateway-Infrastruktur und (Heim-)Energiemanagementsysteme ((H)EMS).

Das Projekt demonstriert erstmals die Implementierung und Nutzung digitaler Maschinen-Identitäten auf Basis des SSI-Paradigmas in energiewirtschaftlichen Anwendungen. Die entwickelte DIVE-Infrastruktur zeigt einen konkreten Lösungsansatz zur Schließung der digitalen Identitätslücke im Energiesystem und ermöglicht damit eine durchgängige Ende-zu-Ende-Digitalisierung.

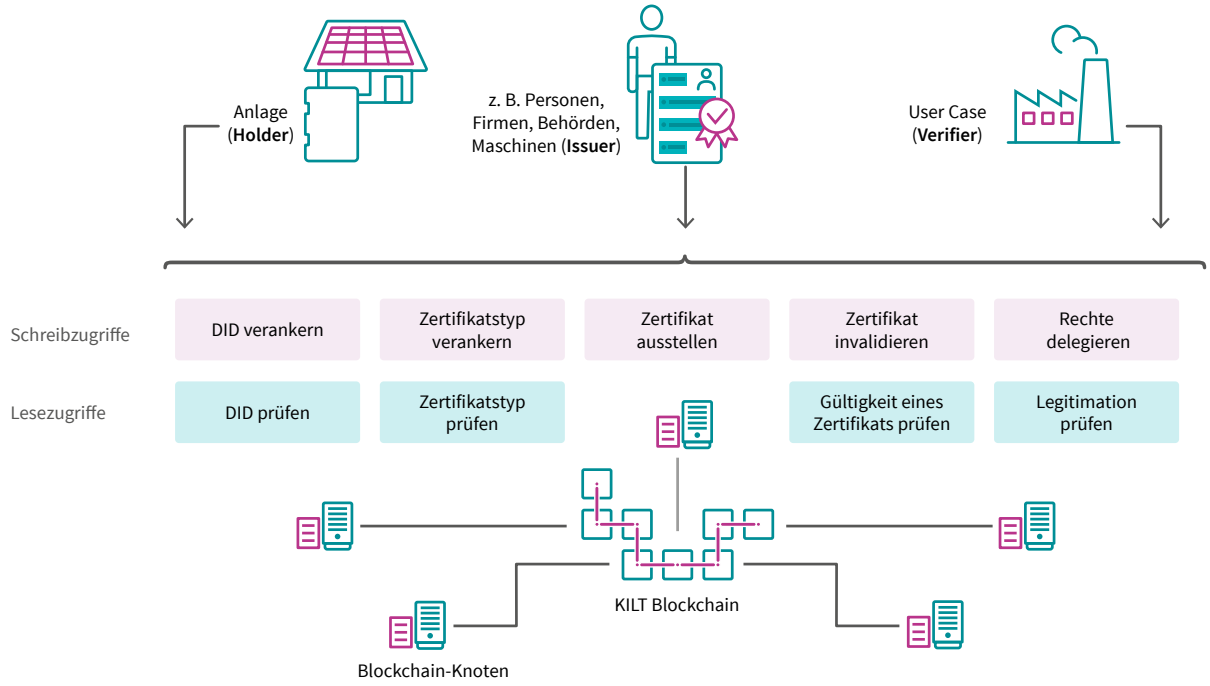

Abbildung 5: Lese- und Schreibzugriffe auf der DIVE-Basisinfrastruktur

4.2 Ausstellung und Nutzung digitaler Maschinen-Identitäten

Im DIVE-Projekt wurden zwei zentrale Prozesse definiert: die Ausstellung von digitalen Identitäten für Anlagen im Energiesystem und ihre Nutzung in verschiedenen Anwendungsfällen. Beide Prozesse orientieren sich an bestehenden Verfahren und gewährleisten eine nahtlose Integration in vorhandene Systemarchitekturen.

1. Ausstellen der digitalen Maschinen-Identität
Sowohl bestehende Anlagen als auch Neuanlagen können mit einer eindeutigen digitalen Maschinen-Identität ausgestattet werden. Als Identitätsmerkmal wird ein Digital Identifier (DID) unveränderlich auf der Blockchain gesichert. Anlagenspezifische Stammdaten werden in einem Verifiable Credential (VC) dokumentiert und in der Digital Wallet des jeweiligen Anlagenbetreibers gespeichert. Während die DID-Sequenz öffentlich auf der Blockchain lesbar ist, wird für das VC nur ein kryptografisch gehashter Anker auf der Blockchain hinterlegt. Dieses Verfahren gewährleistet sowohl den Datenschutz durch Vermeidung der direkten Speicherung personenbezogener Daten als auch die Möglichkeit, ungültige Credentials zu widerrufen. Angelehnt an bestehende Prozesse wird das VC vom Verteilnetzbetreiber gemäß den bestehenden energiewirtschaftlichen Prozessen ausgestellt und enthält die gemäß Marktstammdatenregisterverordnung (MaStRV) spezifizierten Stammdaten.

2. Anmeldung der Anlage bei Anwendungsfällen
Die Anlagenbetreiber verfügen über die Möglichkeit, die digitale Identität einer Anlage anwendungsübergreifend zu nutzen, ohne redundante Identitätsausstellungen oder Mehrfacherfassungen vorzunehmen. Das System unterstützt die gleichzeitige Präsentation mehrerer VCs zur Übermittlung in einer Transaktion. Zur Einhaltung energiewirtschaftlicher Regularien erfolgt eine automatisierte Prüfung auf bestehende Registrierungen von Anwendungsfällen, wodurch beispielsweise die Doppelvermarktung von Grünstrom verhindert wird.

4.3 Betrachtete Anwendungsfälle

Im Rahmen des DIVE-Projekts wurde die Anbindung der DIVE-Infrastruktur anhand von drei verschiedenen Anwendungsfällen evaluiert, um deren Interoperabilität und den resultierenden Mehrwert zu demonstrieren.

Anwendungsfall 1: Digitale Herkunftsnachweise für die Stromproduktion dezentraler Kleinstanlagen
Herkunftsnachweise stellen einen essenziellen Bestandteil der Energiewende dar, da sie Stromverbrauchern eine transparente Verifizierung der Stromherkunft aus erneuerbaren Energiequellen ermöglichen und dadurch Anreize für die Nutzung von Grünstrom schaffen. Die gegenwärtigen Systeme für Herkunftsnachweise basieren auf manuellen Prozessen – insbesondere bei der individuellen Registrierung und Prüfung von Anlagen – und sind mit einem erheblichen administrativen Aufwand verbunden. Aufgrund dieser administrativen Hürden und der fehlenden Automatisierung werden Herkunftsnachweise für den von Prosumern erzeugten Strom in der Regel nicht ausgestellt. Zudem erfolgt die Zertifikatserfassung in unzureichender zeitlicher und räumlicher Auflösung, was eine präzise Zuordnung von Stromerzeugung und -verbrauch erschwert und somit die Glaubwürdigkeit der Zertifikate beeinträchtigt (Sedlmeir et al. 2021b).

Im Projekt DIVE erfolgte eine vollständige Digitalisierung und Automatisierung des Anmelde- und Validierungsprozesses für Anlagen im System **Energy Web Green Proofs**, einschließlich der automatisierten Überprüfung von Stammdaten und der systematischen Integration von Bewegungsdaten. Ein solches System ermöglicht die Ausstellung von Grünstromzertifikaten auch für Kleinstanlagen. Anlagenbetreiber können mittels VCs die relevanten Stammdaten ihrer Anlage bereitstellen, wobei eine automatisierte Prüfung der regulatorischen Konformität für die Ausstellung von Grünstromzertifikaten erfolgt. Das System stellt somit die Einhaltung der Marktregeln der Energiewirtschaft sicher und verhindert systematisch eine Doppelvermarktung des erzeugten Stroms. Die Erfassung hochaufgelöster Produktionsdaten erfolgt über das Smart Meter Gateway, das als Grundlage für die präzise Ausstellung von Herkunftsnachweisen dient.

Digitale Identitäten ermöglichen die automatisierte Ausstellung von verifizierbaren Herkunftsnachweisen, wodurch die Transparenz und Glaubwürdigkeit der Zertifikate erhöht wird.

Anwendungsfall 2: Netzmanagement durch Flexibilisierung dezentraler Energieanlagen
Das zukünftige Energiesystem mit einer hohen Anzahl an dezentralen Anlagen stellt fundamentale Herausforderungen an das Netzengpassmanagement. Neben der Integration zahlreicher kleiner dezentraler Erzeugungsanlagen steigt die Komplexität des Netzes aufgrund zusätzlicher Verbraucher wie Wärmepumpen und Elektrofahrzeugen deutlich an. Die bestehenden Stromnetze sind für die steigende Nachfrage und die zunehmende Dezentralisierung der Erzeugung nicht ausgelegt. Um Netzengpässe zu vermeiden, ist eine koordinierte Steuerung von Stromverbrauch und -erzeugung erforderlich. Anlagenbetreiber können durch die Bereitstellung von Flexibilität zusätzliche Erlöse erzielen, was jedoch eine erfolgreiche Präqualifikation der Anlagen voraussetzt. Dieser Präqualifikationsprozess ist bisher mit aufwendigen manuellen Prüfungen und einem hohen administrativen Aufwand verbunden. Dadurch bleiben Flexibilitätspotenziale kleiner Anlagen wie Wärmepumpen oder Ladesäulen für die Netzstabilisierung unerschlossen (Körner et al. 2024a).

Im Rahmen des DIVE-Projekts wurde in Zusammenarbeit mit BANULA ein optimierter Präqualifikationsprozess für Ladesäulen unter Verwendung von VCs entwickelt. BANULA demonstriert, wie die Ladeflexibilitäten mehrerer Elektrofahrzeuge aggregiert und effizient in netzdienliche Steuerungsmaßnahmen integriert werden können. Die Digitalisierung und automatisierte Validierung essenzieller Nachweise – einschließlich Anlagenregistrierung

und technischer Spezifikationen – mittels VCs ersetzt die bisherige papierbasierte Prozessabwicklung durch den Übertragungsnetzbetreiber und senkt die Kosten der Einbindung signifikant.

Digitale Identitäten ermöglichen ein automatisiertes Onboarding dezentraler Anlagen für Netzdienstleistungen, wodurch die Aggregation von Flexibilitätspotenzialen auch für eine große Anzahl kleiner Anlagen wirtschaftlich realisierbar wird.

Anwendungsfall 3: Nutzung individueller Stromverträge an öffentlichen Ladesäulen

Die aktuelle Ausschreibung für die nationale Lkw-Schnellladeinfrastruktur an Autobahnparkplätzen sieht vor, dass Lkw-Fahrerinnen und -Fahrer die speditionseigenen Stromlieferverträge auch an öffentlichen Ladesäulen nutzen können (Autobahn GmbH 2024). Ein solches Durchleitungsmodell ist bisher technisch nicht oder nur mit erheblichen Zusatzkosten realisierbar, da bestehende Systeme die Abrechnung ausschließlich über den Betreiber der Ladesäule vorsehen. Folglich sind Nutzer öffentlicher Ladesäulen an den Stromlieferanten des Betreibers gebunden und können weder kostengünstigere Tarife noch Verträge mit höherem Grünstromanteil wählen.

In Zusammenarbeit mit dem Projekt **ReBeam**[6] wurde demonstriert, dass digitale Identitäten verschiedene neue Anwendungsfälle an öffentlichen Ladesäulen ermöglichen. Die eindeutige Identifikation von Fahrzeug und Fahrzeughalter an der Ladesäule, authentifiziert über VCs, ermöglicht die Zuordnung des Stromverbrauchs zum individuellen Vertrag. Zusätzlich gewährleistet das System die direkte Übermittlung von Herkunftsnachweisen für den geladenen Strom, wodurch dessen Herkunft und Grünstromanteil transparent und nachvollziehbar werden.

Digitale Identitäten ermöglichen ein Durchleitungsmodell, das Speditionen nicht nur kosteneffizientes Laden ermöglicht, sondern auch verifizierbare CO_2-Zertifikate bereitstellt. Diese dienen als verlässlicher Nachweis für das Nachhaltigkeits-Reporting der Speditionsunternehmen und ihrer Kunden.

4.4 Evaluation der DIVE-Infrastruktur

Die Evaluation der DIVE-Infrastruktur basiert auf einem mehrstufigen methodischen Ansatz, wobei sich der vorliegende Bericht auf die Analyse der technischen Aspekte der Systemarchitektur konzentriert. Die im Rahmen des Projekts entwickelte Infrastruktur für digitale Identitäten wurde einer systematischen Untersuchung unterzogen, die insbesondere die Fortschritte zur Schließung der digitalen Identitätslücke und die daraus resultierenden Verbesserungen gegenüber dem Status quo analysiert.

Die systematische Untersuchung umfasst drei zentrale Dimensionen: generische Anforderungen (Sicherheit und Performance) sowie die zuvor hergeleiteten energiesystemspezifischen Anforderungen an digitale Maschinen-Identitäten. Für jede dieser Dimensionen wurden definierte Metriken und quantifizierbare Indikatoren entwickelt und analysiert. Die Ergebnisse dieser Analyse sind in Tabelle 2 zusammengefasst und werden in den nachfolgenden Abschnitten erläutert. Zur Gewährleistung einer ganzheitlichen Bewertung wurde die Infrastruktur zusätzlich aus energiewirtschaftlicher und regulatorischer Perspektive evaluiert. Diese weiterführenden Analysen sind in den entsprechenden Berichtsteilen ausführlich dokumentiert.

6 https://innovation.eliagroup.eu/en/projects/rebeam

Dimension	Metrik	Zusammenfassung der Evaluation	Bewertung
Sicherheit	**Vertraulichkeit**	Das System bietet durch die dezentrale Speicherung der VCs ein hohes Maß an Vertraulichkeit. Allerdings kann erkennbar sein, dass dieselbe Anlage in mehreren Anwendungsfällen registriert ist.	↗
	Integrität	Die verwendete SSI-Architektur ermöglicht eine hohe Integrität der ausgetauschten Daten.	↑
	Verfügbarkeit	Durch die Dezentralisierung des Netzwerks bietet die Blockchain-basierte Infrastruktur eine hohe Verfügbarkeit. Einzelne zentrale Komponenten existieren, sind jedoch nicht kritisch für die Systemverfügbarkeit.	↑
Performance	**Transaktionsdurchsatz**	Das System zeigt eine hohe Performance und einen ausreichenden Transaktionsdurchsatz für das Energiesystem.	↑
	Systemanforderungen	Die DIVE-Infrastruktur hat geringe Systemanforderungen für die Teilnahme. Anlagen können über standardisierte HEMS-Hardware eingebunden werden, die keine spezifischen Anpassungen erfordert.	↑
Anforderungen an digitale Identitäten im Energiesystem	**Usability**	Im Projekt DIVE wurde eine grundlegende Benutzeroberfläche implementiert. Die Benutzerfreundlichkeit ist jedoch eingeschränkt und für eine breite Nutzergruppe noch unzureichend.	↗
	Hohe Datenqualität	Die DIVE-Infrastruktur bietet eine hohe Datenqualität, die für verschiedene Anwendungsfälle verifizierbar geteilt wird. Ein Trust-Framework muss jedoch noch entwickelt werden.	↗
	Selbstbestimmtheit der Nutzung	Durch die SSI-Prinzipien ermöglicht die DIVE-Infrastruktur allen Teilnehmern eine hohe digitale Selbstbestimmung über die eigenen Daten.	↑
	Anlagenscharfe Maschinen-Identitäten	Jede Anlage kann eine eindeutige digitale Maschinen-Identität erhalten und ist dadurch eindeutig identifizierbar und ansteuerbar.	↑
	Flexibilität	Die modulare Architektur der DIVE-Infrastruktur erlaubt eine flexible Anpassung an zukünftige Anforderungen durch den Austausch oder die Aktualisierung einzelner Komponenten.	↑
	Interoperabilität	Die DIVE-Infrastruktur bietet eine hohe Interoperabilität durch die Verwendung von etablierten Standards, die die Kompatibilität mit anderen Systemen sicherstellen.	↑

Tabelle 2: Ergebnisse der Evaluation

LegendeTabelle: ↑ – vollständige Erfüllung | ↗ – weitgehende Erfüllung

Das System bietet durch die dezentrale Speicherung der VCs ein hohes Maß an Vertraulichkeit. Allerdings kann erkennbar sein, dass dieselbe Anlage in mehreren Anwendungsfällen registriert ist.

Vertraulichkeit

- **Indikator 1:** Dezentrale Speicherung der VCs in der Digital Wallet. Die VCs werden dezentral in den Digital Wallets der jeweiligen Anlagen und Betreiber gespeichert. Ein Zugriff auf diese Daten durch Drittparteien kann ausschließlich nach expliziter Freigabe durch den Besitzer erfolgen.

- **Indikator 2:** Datenschutzkonformes Speichern von Daten auf der Blockchain. Kryptografische Maßnahmen gewährleisten die Einhaltung der Datenschutzanforderungen für Daten, die auf der Blockchain gespeichert sind.

Die verwendete SSI-Architektur ermöglicht eine hohe Integrität der ausgetauschten Daten.

Integrität

- **Indikator 1:** Stammdaten werden als VC gespeichert. Die Anlagendaten werden in Form von VCs gespeichert, die durch autorisierte Akteure kryptografisch signiert sind. Die Integrität wird durch diese digitalen Signaturen dauerhaft sichergestellt.

- **Indikator 2:** Die VCs sind auf der Blockchain verankert. Die Hash-Werte der VCs werden auf der Blockchain gesichert, was die Rückverfolgbarkeit und den Widerruf von Credentials jederzeit ermöglicht.

Durch die Dezentralisierung des Netzwerks bietet die Blockchain-basierte Infrastruktur eine hohe Verfügbarkeit. Einzelne zentrale Komponenten existieren, sind jedoch nicht kritisch für die Systemverfügbarkeit.

Verfügbarkeit

- **Indikator 1:** Dezentrale Blockchain-Infrastruktur mit redundanter Systemarchitektur. Das System basiert auf einer öffentlichen Blockchain, die durch geografisch verteilte, redundante Netzwerkknoten (Nodes) in verschiedenen Ländern betrieben wird. Diese dezentrale Redundanz gewährleistet eine hohe Resilienz.

- **Indikator 2:** Verfügbarkeit des Systems unabhängig von externen Komponenten. Die Basisinfrastruktur der DIVE-Plattform operiert unabhängig von den Systemen der Issuer und Anwendungsfälle. Das Ausstellen und Verifizieren von Credentials kann jedoch durch Ausfälle dieser externen Systeme temporär eingeschränkt sein.

Das System zeigt eine hohe Performance und einen ausreichenden Transaktionsdurchsatz für das Energiesystem.

Transakionsdurchsatz[7]

- **Indikator 1:** Hohe Transaktionskapazität des Blockchain-Netzwerks für das Ausstellen neuer Identitäten. Die KILT Blockchain ermöglicht die Erstellung von durchschnittlich 36.000 DIDs oder 150.000 VCs pro Stunde. Die Generierung einer neuen digitalen Identität wird innerhalb von durchschnittlich 30 Sekunden abgeschlossen.

- **Indikator 2:** Horizontale Skalierbarkeit beim Verifizieren der Credentials. Die verwendete Blockchain-Infrastruktur erlaubt als öffentliches Netzwerk ohne Zugangsbeschränkungen den Betrieb eigener, lokaler Nodes. Nutzer mit hohem Verifikationsaufkommen können dadurch Credentials auf eigenen Nodes verifizieren.

Die DIVE-Infrastruktur hat geringe Systemanforderungen für die Teilnahme. Anlagen können über standardisierte (H)EMS-Hardware eingebunden werden, die keine spezifischen Anpassungen erfordert.

Systemanforderungen

- **Indikator 1:** Die Einbindung der Anlagen erfolgt über ein (H)EMS. Anlagen werden über ein (H)EMS angebunden, sodass keine speziellen Anforderungen an die Anlagen selbst gestellt werden.

- **Indikator 2:** Die Nutzersteuerung erfolgt über einen Webservice. Das System bietet ein browserbasiertes Steuer-Interface sowie Digital-Wallet-Funktionalität. Diese Implementierung als Webanwendung ermöglicht einen plattformunabhängigen Zugriff ohne zusätzliche Softwareinstallation.

Im Projekt DIVE wurde eine grundlegende Benutzeroberfläche implementiert. Die Benutzerfreundlichkeit ist jedoch eingeschränkt und für eine breite Nutzergruppe noch unzureichend.

Usability

- **Indikator 1:** Das System stellt eine lokale Benutzeroberfläche für den Anlagenbetreiber bereit. Das System bietet über das (H)EMS eine webbasierte Benutzeroberfläche für Anlagenbetreiber zur Registrierung verschiedener Anwendungsfälle. Eine für technisch unerfahrene Nutzer geeignete Benutzerführung steht noch aus.

- **Indikator 2:** Die Registrierung von Use Cases verfügt derzeit noch nicht über eine spezifische Benutzeroberfläche. Die Registrierung erfolgt hauptsächlich durch die Erstellung

7 Die Evaluation konzentriert sich auf die Kernprozesse der DIVE-Infrastruktur: die Erstellung und Nutzung digitaler Maschinen-Identitäten. Weitere Prozesse wie die Revokation von Credentials werden aufgrund ihres erwartbar geringen Anteils am Gesamttransaktionsvolumen nicht betrachtet.

entsprechender Daten auf der KILT Blockchain, die mit der zugehörigen KILT-Software durchgeführt wird. Eine bisher spezifische Benutzeroberfläche für die Registrierung ist jedoch noch nicht vorhanden.

Die DIVE-Infrastruktur bietet eine hohe Datenqualität, die für verschiedene Anwendungsfälle verifizierbar geteilt wird. Ein Trust-Framework muss jedoch noch entwickelt werden.

Hohe Datenqualität

- **Indikator 1:** Die Datenqualität wird durch einen vertrauenswürdigen Akteur sichergestellt. Vertrauenswürdige Akteure können die digitalen Identitäten ausstellen und so eine hohe Datenqualität gewährleisten.

- **Indikator 2:** Die Aktualität der Daten kann prozessgesteuert sichergestellt werden. Ausgestellte VCs können vom Issuer zurückgezogen werden. Automatisierte Mechanismen zur Kommunikation von Änderungen und möglichen Rückrufen der VCs an die Anwendungsfälle sind jedoch noch nicht implementiert.

Durch die SSI-Prinzipien ermöglicht die DIVE-Infrastruktur allen Teilnehmern eine hohe digitale Selbstbestimmung über die eigenen Daten.

Selbstbestimmtheit der Nutzung

- **Indikator 1:** SSI-Architektur als Grundlage für digitale Identitäten. Die Credentials jeder Anlage und jedes Betreibers werden in der persönlichen Digital Wallet gespeichert, wodurch die Nutzer die volle Kontrolle über die Weitergabe ihrer Daten behalten.

- **Indikator 2:** Sensible Daten müssen nur mit vertrauenswürdigen Akteuren geteilt werden. Sensible Informationen müssen lediglich bei der Erstellung der Credentials mit dem Issuer geteilt werden.

Jede Anlage kann eine eindeutige digitale Maschinen-Identität erhalten und ist dadurch eindeutig identifizierbar und ansteuerbar.

Anlagenscharfe Maschinen-Identitäten

- **Indikator 1:** Bestehende und neue Anlagen können mit digitalen Maschinen-Identitäten ausgestattet werden. Sowohl Bestands- als auch Neuanlagen können über das (H)EMS mit eindeutigen digitalen Identitäten ausgestattet werden.

- **Indikator 2:** Jede Anlage soll eine eigene Identität erhalten. Digitale Identitäten werden grundsätzlich anlagenscharf ausgestellt und nicht auf Haushaltsebene aggregiert. Dies ermöglicht eine präzise Identifikation und Steuerung jeder einzelnen Anlage im System.

Die modulare Architektur der DIVE-Infrastruktur erlaubt eine flexible Anpassung an zukünftige Anforderungen durch den Austausch oder die Aktualisierung einzelner Komponenten.

Flexibilität

- **Indikator 1:** Die im Projekt realisierte Implementierung dient als Beispiel für ein digitales Identitätsökosystem. Die DIVE-Infrastruktur ermöglicht durch ihren modularen Aufbau eine flexible Anpassung und Erweiterung der Infrastrukturkomponenten nach spezifischen Anforderungen.

- **Indikator 2:** Die Kryptografie kann sowohl hardware- als auch softwarebasiert umgesetzt werden. Das System unterstützt sowohl hardware- als auch softwarebasierte kryptografische Lösungen, wobei je nach Sicherheitsanforderung zwischen Flexibilität (softwarebasierter Ansatz) und erhöhter Sicherheit (hardwarebasierter Ansatz) gewählt werden kann.

Die DIVE-Infrastruktur bietet eine hohe Interoperabilität durch die Verwendung von etablierten Standards, die die Kompatibilität mit anderen Systemen sicherstellen.

Interoperabilität

- **Indikator 1:** Nutzung des W3C-DID-Standards für digitale Identitäten. Die verwendeten Protokolle folgen dem W3C-DID-Standard und gewährleisten damit Kompatibilität mit anderen standardkonformen Netzwerken.

- **Indikator 2:** Die DIVE-Infrastruktur wurde als offenes Ökosystem gestaltet. Die modulare DIVE-Infrastruktur ermöglicht durch standardisierte Schnittstellen eine nahtlose Integration in bestehende digitale Systeme, wie zum Beispiel die SMGW-Infrastruktur.

5. Handlungsempfehlungen

Abbildung 6: Handlungsempfehlungen des Projekts DIVE

Das Projekt DIVE demonstriert die Implementierung und Anwendung digitaler Identitäten im Energiesystem. Die durchgeführte Pilotierung liefert konkrete Einblicke in die praktische Ausgestaltung einer digitalen Identitätsinfrastruktur und validiert ihr Anwendungspotenzial. In diesem Zusammenhang zeigt das Projekt auf, dass zusätzliche Maßnahmen erforderlich sind, um sowohl innerhalb des Energiesektors als auch sektorenübergreifend die Nutzung von digitalen Maschinen-Identitäten zu ermöglichen. Basierend auf den Projektergebnissen wurden sechs zentrale Handlungsempfehlungen abgeleitet.

Die Handlungsempfehlungen reichen von der strategischen Einbettung in die europäische Datenstrategie über die Schaffung notwendiger Strukturen und Rahmenbedingungen bis hin zur konkreten Umsetzung und zum Abbau von regulatorischen Unsicherheiten. Diese Empfehlungen adressieren somit interdisziplinäre Fragestellungen, die sowohl die technischen Aspekte der Dateninfrastruktur als auch die praktische Integration in die Energiewirtschaft umfassen.

Nutzung digitaler Maschinen-Identitäten als Baustein der europäischen Datenstrategie

Die europäische Datenstrategie verfolgt das Ziel, einen Binnenmarkt für Daten zu etablieren, um Europas globale Wettbewerbsfähigkeit sowie die europäische Datensouveränität nachhaltig zu stärken. Für die Umsetzung im Energiesystem ist ein interoperables digitales Identitätsökosystem erforderlich, das technische Standards, Prozesse und Vertrauensbeziehungen integriert. Dieses ermöglicht die nahtlose Unterstützung von Initiativen im Rahmen der europäischen Datenstrategie, wie beispielsweise des energiewirtschaftlichen Use Case zum Aufbau des Dateninstituts. Es wird dabei empfohlen, beim Aufbau des digitalen Identitätsökosystems den Fokus auf Maschinen-Identitäten zu legen. Diese Priorisierung adressiert eine kritische Lücke: Während für Personen und Organisationen bereits Lösungen wie eIDAS 2.0 existieren, fehlt bislang eine standardisierte Lösung für die zunehmende Zahl dezentraler technischer Anlagen im Energiesystem. Damit kann an die bestehenden Lösungen angeknüpft werden, ohne eine parallele Infrastruktur aufzubauen. Es sollten klare Ziele und eine detaillierte Roadmap kommuniziert werden, die unter anderem die Förderung von Pilotprojekten und Änderungen bestehender Prozesse frühzeitig aufzeigen.

Etablierung einer Plattform für Dialog, Kompetenzentwicklung und Innovationsförderung

Die Bedeutung einer zentralen Koordinationsplattform für den Aufbau digitaler Infrastrukturen wurde anhand des eIDAS-2.0-Ökosystems untersucht (Degen und Teubner 2024). Eine vergleichbare Plattform sollte auch für das Energiesystem etabliert werden, die dabei folgende Kernfunktionen erfüllen sollte:

- die strategische Vernetzung relevanter Akteure
- die systematische Entwicklung und Verbreitung von Kompetenzen
- die gezielte Förderung von Innovationen

Bei der Umsetzung dieser Funktionen könnten zukünftig auch Einrichtungen wie das geplante Dateninstitut der Bundesregierung eingebunden werden (BMWK und BMI 2023).

Die Entwicklung der eIDAS-2.0-Infrastruktur demonstriert, wie Akteure erfolgreich eingebunden werden können. Die Europäische Kommission koordiniert die Architektur- und die Konsultationsverfahren auf EU-Ebene zwischen den Mitgliedstaaten und Experten, während das Bundesministerium des Innern (BMI) die nationale Umsetzung der EUDI-Wallet im Rahmen eines Innovationswettbewerbs leitet. Diese Beispiele verdeutlichen insbesondere die Bedeutung von zentralen Koordinierungsstellen für die systematische Einbindung der Industrie und relevanter Stakeholder in die verschiedenen Entwicklungsphasen des Ökosystems (Degen und Teubner 2024). Für eine effektive Umsetzung und den nachhaltigen Betrieb der Infrastruktur erscheint es empfehlenswert, die Ergebnisse der Konsultationen sowie Best Practices und interdisziplinäres Know-how öffentlich bereitzustellen. Ein Schwerpunkt sollte dabei auf die Entwicklung von Open-Source-Lösungen und standardisierten Komponenten der Identitätsinfrastruktur gelegt werden. Diese Maßnahmen stärken die digitale Resilienz Kritischer Infrastrukturen und reduzieren technologische Abhängigkeiten. Besonders Open-Source-Lösungen verringern die technologischen und finanziellen Hürden für mittelständische oder aufstrebende Marktakteure, wodurch die Teilnahme an der Infrastruktur effizienter und kostengünstiger wird. Der Fokus auf frei verfügbare Software unterstützt darüber hinaus die bundesweite Strategie zur Förderung von Open Source, die von der Initiative „Zentrum für Digitale Souveränität der öffentlichen Verwaltung“ koordiniert wird.

Konkretisierung eines Trust-Frameworks

Ein Trust-Framework definiert verbindliche Regeln und Standards für vertrauenswürdige digitale Interaktionen im Energiesektor. Die Erkenntnisse aus den strukturierten Dialogprozessen der Plattform sollten direkt in die Entwicklung eines branchenübergreifend anerkannten Trust-Frameworks einfließen. Dieses Framework sollte **vier zentrale Aspekte** adressieren, die eng miteinander verknüpft sind:

- die Schaffung von Vertrauen durch Datenqualität
- die Sicherstellung von Authentizität und Interoperabilität
- die Etablierung verlässlicher Vertrauensketten zwischen Ausstellern und Prüfern von Identitäten
- die Umsetzung dieser Anforderungen durch eine flexible technische Infrastruktur [8]

Um vertrauenswürdige Interaktionen zu ermöglichen, sollten klare Regeln und Verantwortlichkeiten für die Erstellung, Nutzung und Verwaltung von Daten definiert werden. Dabei müssen sowohl die Authentizität der Daten als auch die Vertrauenswürdigkeit der beteiligten Akteure sichergestellt werden. Hierfür ist eine transparente Hierarchie von Vertrauensbeziehungen notwendig, die festlegt, welche Aussteller für welche Arten von Identitätsnachweisen autorisiert sind und welchen Prüfinstanzen vertraut werden kann (Preukschat 2021). Dabei sollten unterschiedliche Vertrauensniveaus ermöglicht werden, die sich beispielsweise an der Anlagengröße orientieren.[9] Die Interoperabilität erfordert standardisierte Datenstrukturen und -formate, um einen effizienten sektorenübergreifenden Datenaustausch sowie die gegenseitige Anerkennung des Trust-Frameworks zu gewährleisten. Dadurch kann die Kompatibilität mit etablierten Frameworks wie eIDAS 2.0 und der SMGW-Infrastruktur sichergestellt werden. Die technische Interoperabilität kann durch die Verwendung von offenen Standards wie beispielsweise durch W3C-Credentials erzielt werden. Anstelle einer monolithischen Lösung sollte ein modularer Architekturansatz verfolgt werden. Dieser Ansatz ermöglicht die flexible Kombination zentraler und dezentraler Komponenten entsprechend den spezifischen Anforderungen an digitale Identitäten in unterschiedlichen Anwendungsfällen.

Integration von digitalen Identitäten in bestehende Infrastrukturen und Prozesse

Die Integration digitaler Identitäten in das Energiesystem erfordert die systematische Einbindung in bestehende technische Infrastrukturen und regulatorische Prozesse. Das Potenzial der SMGW-Infrastruktur wird durch die Einbindung digitaler Maschinen-Identitäten für Energieanlagen erweitert. Dies ermöglicht eine sichere und effiziente Einbindung steuerbarer Anlagen in Echtzeitkommunikation, wie es im Impulspapier des Bundesamts für Sicherheit in der Informationstechnik (BSI 2024) beschrieben wurde. Im Projekt DIVE wurde demonstriert, wie die CLS-Schnittstelle eines SMGW für digitale Maschinen-Identitäten genutzt werden kann und somit die Einsatzmöglichkeiten existierender Systeme erweitert werden – ohne dass hierfür neue, spezialisierte Hardware eingeführt oder bestehende Hardware angepasst werden muss. Weitere Effizienzgewinne ergeben sich

8 Ein Beispiel für ein Trust-Framework ist das Architecture and Reference Framework der eIDAS-2.0-Infrastruktur. Weiterführende Informationen sind frei abrufbar unter dem folgenden Link: https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework?tab=readme-ov-file

9 Die Orientierung an der Anlagengröße ermöglicht einen ausgewogenen Kompromiss zwischen Sicherheit und Flexibilität. Während kleinere Anlagen durch softwarebasierte Lösungen kostengünstiger und mit angemessenen Sicherheitsanforderungen angebunden werden können, benötigen größere Anlagen aufgrund ihres höheren Risikopotenzials ein Hardware Security Module zur sicheren Verknüpfung mit der digitalen Identität.

durch die konsequente Weiterentwicklung von energiewirtschaftlichen Prozessen. Dabei sollten digitale Maschinen-Identitäten in die Marktkommunikation integriert werden, um eine zukunftsorientierte und leistungsfähige Ausrichtung zu ermöglichen. Die Integration verifizierbarer Stammdaten der Anlagen in die Marktkommunikationsprozesse kann zusätzliche Informationen zu Marktlokationen bereitstellen. Hierdurch könnte beispielsweise ein Lieferantenwechsel durch die direkte Übermittlung verifizierter Anlageninformationen erheblich vereinfacht werden. Dies gilt insbesondere für spezielle Angebote wie Heiz- oder Ladestrom und könnte auch Echtzeit-Marktrollenwechsel von Prosumern (Haushalte ebenso wie Unternehmen) unterstützen. Die Einbindung in bestehende Register wie das Marktstammdatenregister oder das Herkunftsnachweisregister ermöglicht durch automatisierte Verifikation und Aktualisierung von Anlagen-Stammdaten eine verbesserte Datenqualität und reduziert den administrativen Aufwand.

Zielbildorientierte Gestaltung digitaler Identitäten

Die digitale Transformation des Energiesystems erfordert eine zukunftsorientierte Ausgestaltung digitaler Identitäten. Konkrete Zielsetzungen sind unter anderem im EU-Aktionsplan zur Digitalisierung des Energiesystems und in mehreren Whitepapern von Arbeitsgruppen (European Coalition for bidirectional Charging 2024) oder Übertragungsnetzbetreibern (Elia Group 2021) zu finden. Diese Zielbilder verdeutlichen, welche Anwendungsfälle ein digitalisiertes Energiesystem ermöglicht und welche Anforderungen an digitale Identitäten gestellt werden. Für die Weiterentwicklung der digitalen Maschinen-Identitäten ist es essenziell, dass bei der Erprobung innovativer Anwendungsfälle in Testmärkten oder Reallaboren die digitale Identitätsinfrastruktur als integraler Bestandteil der Erprobung einbezogen wird. Dies ermöglicht es nicht nur, die Skalierbarkeit der Identitätsinfrastruktur zu evaluieren, sondern auch die Anforderungen der einzelnen Anwendungsfälle zu erfassen. Dafür ist ein offenes regulatorisches Umfeld erforderlich, um aus der praktischen Umsetzung der Anwendungsfälle wertvolle Impulse zu generieren.

Die architektonischen Vorteile einer technologieoffenen und hardwareunabhängigen Lösung schaffen dabei den notwendigen Rahmen für sektorenübergreifende Pilotimplementierungen. Die Ausgestaltung der digitalen Identitätsinfrastruktur sollte sektorenübergreifende Anwendungsfälle wie die Nachhaltigkeitsberichterstattung und digitale Produktpässe einbeziehen (Körner et al. 2024b). Dies entspricht den Interoperabilitätsanforderungen des europäischen Data Act und ermöglicht Synergieeffekte über Sektorengrenzen hinweg, wie sie beispielsweise in der Kooperation der auf Gaia-X basierenden Datenökosysteme Catena-X [10] (Automobilwirtschaft) und energy data-X [11] (Energiesektor) bereits angestrebt werden. Ein konkretes Beispiel hierfür ist die Nutzung von Fahrzeugsensordaten aus dem Automobilsektor für die Verbesserung der Einspeise- und Verbrauchsprognosen der Übertragungsnetzbetreiber.

Abbau regulatorischer Unsicherheiten

Die erfolgreiche Implementierung digitaler Identitäten erfordert die Beseitigung regulatorischer Unsicherheiten in drei zentralen Bereichen. Diese Bereiche adressieren sowohl grundlegende rechtliche Rahmenbedingungen als auch konkrete Anforderungen für die praktische Umsetzung. Eine ausführliche Darstellung der Handlungsempfehlung befindet sich im Berichtsteil „Rechtliche Analyse“.

Bei der Entwicklung neuer regulatorischer Rahmenbedingungen sollten digitale Identitäten als grundlegende Enabler berücksichtigt werden. Diese frühzeitige Integration ermöglicht die Schaffung notwendiger Schnittstellen und rechtlicher Grundlagen für innovative Anwendungsfälle. Für eine erfolgreiche Implementierung ist die Interaktion mit bestehenden Systemen relevant. Die Verknüpfung mit Registern wie dem Marktstammdatenregister erfordert eindeutige gesetzliche Vorgaben zum Datenaustausch. Die Bundesnetzagentur (BNetzA) könnte durch Verordnungen entsprechende Schnittstellen ermöglichen und zur verbindlichen Verwendung verpflichten. Im Bereich des Cybersicherheitsrechts fehlt bisher eine klare Einordnung dezentraler Systeme. Dabei gilt es insbesondere zu definieren, unter welchen Bedingungen diese Systeme vom Anwendungsbereich der Cybersicherheitsvorschriften erfasst werden und welche Akteure die entsprechenden Betreiberpflichten erfüllen müssen.

10 https://catena-x.net/de/
11 https://www.energydata-x.eu/

Fazit

Die vollständige Ende-zu-Ende-Digitalisierung stellt einen zentralen Baustein für die nachhaltige, kosteneffiziente und schnelle Umsetzung der Energiewende dar. Im Energiesektor erproben bereits verschiedene Initiativen sektorenweite Datenräume zur Etablierung eines einheitlichen und automatisierten Datenaustauschs. Für ihre erfolgreiche Implementierung fehlt jedoch eine Infrastruktur zur Bereitstellung vertrauenswürdiger Stammdaten. Das DIVE-Projekt schließt diese Lücke und demonstriert erfolgreich, wie digitale Identitäten als Vertrauensanker genutzt werden können, um dezentrale Erzeuger und Verbraucher nahtlos in ein digitalisiertes Energiesystem zu integrieren. Die dabei umgesetzten digitalen Maschinen-Identitäten schaffen Vertrauen in Anlagendaten durch kryptografische Verifizierbarkeit, ermöglichen die sektorenübergreifende Interoperabilität durch standardisierte Schnittstellen und gewährleisten die sichere Ansteuerung dezentraler Anlagen.

Anstelle eines Greenfield-Ansatzes – also einer Neuentwicklung ohne Rücksicht auf bestehende Systeme – zeigt das Projekt DIVE auf, wie digitale Maschinen-Identitäten in etablierte Infrastrukturen und Prozesse wie die Smart-Meter-Gateway-Infrastruktur integriert werden können. Diese Anschlussfähigkeit reduziert nicht nur den Aufwand beim Rollout, sondern gewährleistet auch eine effiziente Einbindung in bestehende Marktprozesse. Insbesondere im Austausch mit anderen Forschungsprojekten wie DEER, BANULA und den Data-Space-Initiativen zeigte sich die Relevanz einer digitalen Identitätsinfrastruktur deutlich und verspricht eine größere Akzeptanz in der Branche. Diese Entwicklung wird durch die europäische Datenstrategie und die eIDAS-2.0-Regulierung weiter gestärkt, die interoperable digitale Identitätslösungen als Schlüsselelement definieren.

Auf Basis der Projektergebnisse wurden konkrete Handlungsempfehlungen für die praktische Einführung digitaler Maschinen-Identitäten entwickelt. Eine zentrale Empfehlung adressiert die Einbettung in die europäische Datenstrategie, um die Interoperabilität und Skalierbarkeit der Lösungen im gesamten Energiesektor zu gewährleisten und gleichzeitig das europäische Ziel eines einheitlichen Binnenmarktes für Strom zu unterstützen. Die Etablierung einer Koordinations- und Austauschplattform vernetzt dabei technologische, regulatorische und energiewirtschaftliche Akteure für die effiziente Umsetzung eines Identitätssystems. Über diese Plattform ist die Entwicklung eines gemeinsamen Verständnisses von digitalen Maschinen-Identitäten im Sinne eines Trust-Frameworks mit verbindlichen Standards für ihre Ausgabe und Nutzung möglich. Ein solches Framework gewährleistet eine konsistente und sichere Umsetzung von digitalen Identitäten im Energiesystem und bietet damit auch die Grundlage für einen sektorenübergreifenden Einsatz. Die Integration in bestehende Strukturen minimiert Implementierungshürden, während eine klare Ausrichtung auf zukünftige Anwendungsfälle die nachhaltige Entwicklung der Identitätsinfrastruktur sichert. Neben diesen technischen Aspekten wurde im Projekt deutlich, dass bei der Anwendung digitaler Identitäten weiter regulatorische Unsicherheiten bestehen – insbesondere in Bezug auf Cybersicherheit und die Integration in das Energiesystem. Um sie zu überwinden, ist ein kontinuierlicher Dialog zwischen Wirtschaft und Politik unerlässlich.

Diese Handlungsempfehlungen verdeutlichen den Weg zur erfolgreichen Einführung digitaler Maschinen-Identitäten als Baustein für die Transformation des Energiesektors. Mit der Einführung digitaler Maschinen-Identitäten wird nicht nur das Vertrauen für sichere digitale Interaktionen zwischen Akteuren und Anlagen geschaffen, sondern auch der Weg für eine effiziente und skalierbare Digitalisierung geebnet. Dies ermöglicht ein zukunftsfähiges, nachhaltiges und digitalisiertes Energiesystem.

Abbildungsverzeichnis

Tabellenverzeichnis

Literaturverzeichnis

Autobahn GmbH (2024): Projektexposé: Planung, Errichtung und Betrieb von öffentlich zugänglicher Schnellladeinfrastruktur für E-Lkw an unbewirtschafteten Rastanlagen entlang der Bundesautobahnen in der Bundesrepublik Deutschland. Online verfügbar unter https://www.autobahn.de/storage/user_upload/qbank/Projektexpose_Auschreibung_LKW-Schnellladenetz_unbewirtschaftete_Rastanlagen.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; Willburger, Lukas; Lautenschlager, Jonathan; Völter, Fabiane; Guggenberger, Tobias; Körner, Marc-Fabian et al. (2024): Self-Sovereign Identity: A Paradogm for Wallet-Based IdentityManagement. In: Electronic Markets. [Status: accepted, to be published.]

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.

BMWK; BMI (2023): Konzept zum Aufbau des Dateninstituts. Ausgangslage und Hintergrund zum Konzept. Online verfügbar unter https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/themen/it-digitalpolitik/dateninstitut/konzeptpapier_dateninstitut.pdf?__blob=publicationFile&v=7.

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 (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.

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

Degen, Konrad; Teubner, Timm (2024): Wallet wars or digital public infrastructure? Orchestrating a digital identity data ecosystem from a government perspective. In: Electron Markets 34 (50). DOI: 10.1007/s12525-024-00731-1.

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): 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 (2024b): 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.

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.

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.

European Coalition for bidirectional Charging (2024): Joint Report of the European Working Groups 1 and 2. Online verfügbar unter https://www.bmwk.de/Redaktion/DE/Downloads/P-R/coalition-of-the-willing-on-bidirectional-charging-en.pdf?__blob=publicationFile&v=8.

Körner, Marc-Fabian; Nolting, Lars; Heeß, Paula; Schick, Leo; Lautenschlager, Jonathan; Zwede, Till et al. (2024a): A digital infrastructure for integrating decentralized assets into redispatch. Decentralized Redispatch (DEER): Interfaces for providing flexibility. Bayreuther Arbeitspapiere zur Wirtschaftsinformatik. Online verfügbar unter https://www.econstor.eu/bitstream/10419/287771/1/1884577040.pdf.

Körner, Marc-Fabian; Paetzold, Felix; Ströher, Tobias; Strüker, Jens (2024b): Digital Proofs of Origin for Sustainability. Assessing a Digital Identity-Based Approach in the Energy Sector. Online verfügbar unter https://www.fim-rc.de/wp-content/uploads/2024/07/DigitalProofsofOriginforSustainability.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/witschaftsinformatik/dokumente/Leveraging-Twin-Transformation_Digital-Infrastructures-to-Advance-Deccarbonisation-at-the-Nexus-of-Energy-and-Mobility.pdf.

Michaelis, Anne; Hanny, Lisa; Körner, Marc-Fabian; Strüker, Jens; Weibelzahl, Martin (2024): Consumer-centric electricity markets: Six design principles. In: Renewable and Sustainable Energy Reviews 191, S. 113817. DOI: 10.1016/j.rser.2023.113817.

Möller, Frederik; Jussen, Ilka; Springer, Virginia; Gieß, Anna; Schweihoff, Julia Christina; Gelhaar, Joshua et al. (2024): Industrial data ecosystems and data spaces. In: Electron Markets 34 (41). DOI: 10.1007/s12525-024-00724-0.

Mühle, Alexander; Grüner, Andreas; Gayvoronskaya, Tatiana; Meinel, Christoph (2018): A survey on essential components of a self-sovereign identity. In: Computer Science Review 30, S. 80–86. DOI: 10.1016/j.cosrev.2018.10.002.

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

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 (2021a): Digital Identities and Verifiable Credentials. In: Business & Information Systems Engineering 63 (5), S. 603–613. DOI: 10.1007/s12599-021-00722-y.

Sedlmeir, Johannes; Völter, Fabiane; Strüker, Jens (2021b): The next stage of green electricity labeling. In: SIGENERGY Energy Inform. Rev. 1 (1), S. 20–31. DOI: 10.1145/3508467.3508470.

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.

Urbach, Nils; Guggenberger, Tobias; Pfaff, Hendrik; Stoetzer, Jens-Christian; Feulner, Simon; Babel, Matthias et al. (2024): EU Digital Identity Wallet. Online verfügbar unter https://publica.fraunhofer.de/handle/publica/470622.

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%202a.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.

Abkürzungen

BANULA	BArrierefreie und NUtzerfreundliche LAdemöglichkeiten schaffen
BMIL	Blockchain Machine Identity Ledger
BMWE	Bundesministerium für Wirtschaft und Energie
CLS	Controllable Local System
DEER	Dezentraler Redispatch. Für ein Energiesystem von morgen und eine Elektrifizierung der Zukunft
DID	Digital Identifier, eine Sequenz von Zahlen und Buchstaben; je nach Kontext wird auf den Identifier als Konzept oder die DID-Sequenz als Datum referiert
EEG	Erneuerbare-Energien-Gesetz
eIDAS-Verordnung	EU-Verordnung über elektronische Identifizierung und Vertrauensdienste (Electronic Identification, Authentication and Trust Services)
EU	Europäische Union
EUDI-Wallet	Europäische Brieftasche für die digitale Identität (European Digital Identity Wallet)
GDEW	Gesetz zur Digitalisierung der Energiewende
(H)EMS	(Heim-)Energiemanagementsystem
SMGW	Smart Meter Gateway
SSI	Self-Sovereign Identity
VC	Verifiable Credential
VNB	Verteilnetzbetreiber
W3C	World Wide Web Consortium

Glossar

Begriff	Definition
Aggregator (digitaler)	Aggregatoren sind Einheiten, die mehrere einzelne Einheiten, zum Beispiel Verbrauchseinheiten wie (Wohn-)Gebäude mit einzelnen Haushalten oder Unternehmen und Erzeugungseinheiten wie Photovoltaik-Anlagen auf Hausdächern, zusammenfassen und steuern. Die aus der Aggregation resultierende Flexibilität wird gebündelt und an die nächste Ebene, beispielsweise Netzbetreiber, weitergegeben.
Anlage (technische) **Weitere Bezeichnungen: Technische Einheit, DIVE-Gerät**	Eine technische Anlage im Kontext von DIVE sind Assets wie Photovoltaik-Anlagen bzw. Wechselrichter, Batteriespeicher und deren Steuerelektronik, Wallboxen sowie Wärmepumpen.
AS4-Standard	Die Marktkommunikation muss seit dem 1. April 2024 über den Übertragungsweg AS4 (Applicability Statement 4) durchgeführt werden. Abgesichert mit TLS (Transport Layer Security) unter Nutzung der Smart Meter Public Key Infrastructure (SM-PKI) wird die Sicherheit der Übertragung erhöht.
Attester	Siehe Issuer.
Bewegungsdaten (dynamische Daten)	Die Bewegungsdaten einer Anlage sind das dynamische Pendant zu den Stammdaten. Sie enthalten Informationen wie die derzeitige Produktion bzw. den Verbrauch der Anlage, Daten zu einem Ladevorgang eines E-Autos oder auch die Telemetrie. Bewegungsdaten sind zum Beispiel Messdaten von Anlagen und weisen einen hohen Datendurchsatz auf, da sie die zeitliche Veränderung von Zuständen darstellen und somit kontinuierlich aktualisiert werden. Im Energiesystem ist die zeitnahe Verfügbarkeit von Bewegungsdaten von besonderer Bedeutung, vor allem durch die Volatilität der erneuerbaren Energien, die steigende Anzahl von Elektrofahrzeugen und die Zunahme steuerbarer Lasten.
Collator	Collators sind eine spezifische Art von Node, die Transaktionen sammeln und sie zu Blöcken bündeln.

Datenraum (Data Space)	Datenräume ermöglichen den souveränen und selbstbestimmten Austausch von Daten über organisatorische Grenzen hinweg. Um Datensicherheit, Datensouveränität, Interoperabilität, Portabilität und Vertrauen zwischen den Akteuren zu gewährleisten, wird ein föderalistischer Ansatz mit definierten Standards, Technologien und Governance-Modellen genutzt.
Decentralized Identifier (DID)	DIDs sind eine neue Art von Identifikatoren, die eine überprüfbare, dezentralisierte digitale Identität ermöglichen. Eine DID bezieht sich auf ein beliebiges Subjekt (z. B. eine Person, eine Organisation, eine Sache, ein Datenmodell, eine abstrakte Entität usw.). Im Gegensatz zu typischen, föderierten Identifikatoren sind DIDs so konzipiert, dass sie von zentralen Registern, Identitätsanbietern und Zertifizierungsstellen entkoppelt werden können. (Quelle: https://www.w3.org/TR/did-core/)
Digitale Identitäten	Digitale Identitäten im Energiesektor beziehen sich auf eindeutige digitale Repräsentationen von Energieanlagen oder Akteuren und ermöglichen eine sichere und effiziente Durchführung von Transaktionen und Interaktionen im digitalen Energiemarkt. Sie umfassen wesentliche Stammdaten wie Eigentumsverhältnisse, Standort, Kapazität und technische Spezifikationen.
DIVE-Basisinfrastruktur	Die im Projekt DIVE pilotierte Basisinfrastruktur bietet die Funktionalitäten zur Nutzung in neuen Anwendungsfällen und bei bestehenden Akteuren im Energiesystem, wie die Anlagenregistrierung oder die Einhaltung von Marktregeln.
EMS	siehe (H)EMS.
Energy Communities (dt. Energiegemeinschaften)	Bei Energy Communities schließen sich mehrere Akteure (z. B. Bürgerinnen und Bürger sowie Kommunen und KMUs) zusammen, betreiben eigene Anlagen zur Erzeugung erneuerbarer Energien, verbrauchen die erzeugte Energie gegebenenfalls direkt selbst, vermarkten sie oder bieten weitere Energiedienstleistungen an. Für den Aufbau von Energy Communities ist die räumliche Nähe häufig entscheidend.
Flexumer	Kofferwort aus „Flexibilität“ und „Prosumer“. Es beschreibt das Konzept, dass Akteure oder Anlagen im Energiesektor ihre Erzeugungs- wie auch Verbrauchskapazitäten flexibel nutzen und nach bestimmten Parametern optimieren können (sollen).
Hardware Secure Module (HSM, Krypto-Chip)	Ein Hardware Secure Module (HSM) ist ein Hardwaremodul, das bestimme kryptografische Operationen oder Funktionen (bzw. Primitiven) in einem System umsetzt. Die Funktionen beinhalten zum Beispiel das Erstellen von Schlüsselpaaren mit hoher Entropie, das sichere Verwahren der Keys und das Signieren von Daten mithilfe des Private Key. Die Features könnten prinzipiell auch ausschließlich mit Software umgesetzt werden, ein HSM ermöglicht durch das strikte Abtrennen der Sub-Systeme innerhalb des Betriebssystems allerdings eine deutliche Steigerung der Sicherheit bezüglich verschiedener Angriffsvektoren.
(H)EMS	Ein (Heim-)Energiemanagementsystem stellt den lokalen Datenaustausch für den optimierten Einsatz und die Visualisierung von Energieanlagen und Verbrauchern in Ein- und Mehrfamilienhäusern, Liegenschaften und Gewerben sicher.
Holder	Ein Holder (auch Claimer) ist eine Person oder eine Entität, die die Kontrolle über seine bzw. ihre eigenen digitalen Identitätsdaten besitzt und diese verwaltet. Holder speichern und verwenden Verifiable Credentials in einer Digital Wallet, um ihre Identität oder bestimmte Attribute davon gegenüber Dritten zu authentifizieren und zu verifizieren.

Intelligentes Messsystem (iMSys)	siehe Moderne Messeinrichtung.
Issuer	Ein Issuer (auch Attester) ist eine vertrauenswürdige Instanz oder Autorität, die Verifiable Credentials ausstellt. Die VCs werden vom Issuer kryptografisch signiert, was nicht nur die Integrität der Daten sicherstellt, sondern es auch dem Verifier ermöglicht, zu erkennen, von wem sie ausgestellt wurden.
Kritische Infrastruktur (KRITIS)	Als Kritische Infrastrukturen (KRITIS) werden Einrichtungen und Organisationen bezeichnet, die für das staatliche Gemeinwesen wichtig sind. Dazu gehören beispielsweise die Bereiche Energie und Gesundheit. Der Ausfall Kritischer Infrastrukturen kann unter anderem zu Versorgungsengpässen, erheblichen Störungen der öffentlichen Sicherheit und volkswirtschaftlichen Schäden führen.
Moderne Messeinrichtung (mME) / Intelligentes Messsystem (iMSys)	Die moderne Messeinrichtung (oftmals auch „digitaler Stromzähler“ genannt) ist der in Deutschland vorgeschriebene Stromzähler und ersetzt den Ferraris-Zähler. Die mME hält neben einem Display zur Anzeige verschiedener Informationen auch weitere Schnittstellen bereit. Erst in Verbindung mit einem Smart Meter Gateway (SMGW) kann eine mME energiewirtschaftlich relevante Daten übertragen und wird damit zu einem intelligenten Messsystem (iMSys).
Netzbetreiber	Die Netzbetreiber sind für den sicheren Netzbetrieb verantwortlich. Dabei wird zwischen Übertragungs- und Verteilnetzbetreibern unterschieden.
Node (Knoten)	Eine Infrastruktur-Einheit in einem verteilten System. Der Node bündelt verschiedene Transaktionen zu einem Block, der kryptografisch verschlüsselt und dann in das bestehende System integriert wird. Die Anzahl, Rechenleistung und Art von Nodes entscheiden über die Sicherheit, Latenz und Art eines dezentralen Systems (in der Regel ein DLT- oder Blockchain-System).
openEMS	openEMS ist eine modulare und auf Open-Source-Komponenten basierende Software für EMS-Anwendungen. Neben der openEMS Association e. V. wird es von freien Softwareentwicklern kontinuierlich weiterentwickelt und stellt einen Ausgangspunkt für Eigenentwicklungen dar.
Prosumer	Als Prosumer werden in der Energiewirtschaft Akteure oder Anlagen bezeichnet, die sowohl als Erzeugungs- wie auch als Verbrauchseinheit agieren können. Das Wort setzt sich zusammen aus „Produzent/Producer“ und „Konsument/Consumer“.
Public Key Infrastructure (PKI) / Smart Meter PKI (SM-PKI)	Eine Public Key Infrastructure (PKI) ist notwendig, um die korrekte asymmetrische Verschlüsselung von Nachrichten sicherzustellen. Hierbei gibt es verschiedene Umsetzungsarten. Die Smart Meter PKI (SM-PKI) ist die eigene PKI für Smart-Meter-Anwendungen in Deutschland und besitzt ein Wurzelzertifikat (Root) als Vertrauensanker, das vom BSI beaufsichtigt wird. Mit dem Wurzelzertifikat können weitere, zum Ausstellen neuer Zertifikate berechtigte Entitäten, sogenannte Sub-CAs (Sub Certification Authorities) definiert werden. Mit der SM-PKI wird auf diese Weise Vertrauen durch ein Rollenmodell vom Root über die Sub-CAs bis zu den Marktteilnehmern hergestellt.
Public-permissionless Blockchain	Eine Public-permissionless Blockchain ist eine öffentlich zugängliche, dezentrale Blockchain, bei der jeder ohne Erlaubnis teilnehmen kann.

Redispatch	Unter Redispatch versteht man die Anpassung des Kraftwerkseinsatzes durch die Netzbetreiber, um Netzengpässe zu vermeiden. Dazu werden Erzeugungseinheiten vor dem Engpass gedrosselt und Erzeugungseinheiten hinter dem Engpass hochgefahren. Mit Redispatch 3.0 sollen auch Flexibilitätspotenziale von (Kleinst-)Anlagen (< 100 Kilowatt) wie zum Beispiel Elektrofahrzeugen zur Vermeidung von Netzengpässen berücksichtigt werden.
Sektorenkopplung	Sektorenkopplung beschreibt das Zusammenspiel der verschiedenen Sektoren des Energiesystems. Denn nur wenn die verschiedenen Sektoren (wie Strom, Wärme und Mobilität) integriert betrachtet werden, kann der Strom aus erneuerbaren Energien optimal genutzt werden.
Self-Sovereign Identity (SSI) (selbstbestimmte oder selbstsouveräne Identität)	Eine Self-Sovereign Identity (SSI) erlaubt es einer Person, Organisation oder Anlage, eine digitale Identität zu erzeugen und vollständig zu kontrollieren, ohne dass es der Erlaubnis eines Vermittlers oder einer zentralen Stelle bedarf. Zudem erlaubt sie die Kontrolle darüber, wie die persönlichen Daten geteilt und verwendet werden.
Shoveler	Als Shoveler wird eine IT-Werkzeug-Komponente bezeichnet. Mithilfe eines Shovelers wird die Migration von Daten von einem lokalen System in eine Cloud-Umgebung vereinfacht.
Smart Meter Gateway (SMGW)	Das Smart Meter Gateway (SMGW) ist eine besonders gesicherte Schnittstelle für die Datenkommunikation von modernen Messeinrichtungen. Es verbindet Verbraucherinnen und Verbraucher sowie Erzeugerinnen und Erzeuger von Strom mit den Betreibern der Stromnetze und Versorgungsunternehmen. Das Smart Meter Gateway ermöglicht eine datenschutz- und datensicherheitskonforme Einbindung von Zählern in das intelligente Stromnetz.
Stammdaten	Stammdaten bilden häufig die Grundlage für verschiedene Marktprozesse in der Energiewirtschaft. Daher sind die Vollständigkeit und Richtigkeit für die Marktkoordination und -kommunikation unerlässlich. Mit Stammdaten sind im Energiekontext (größtenteils) statische Informationen über technische Anlagen oder Marktrollen gemeint. Dazu gehören unter anderem Datenpunkte wie die Kennungen (ID) in den verschiedenen Systemen (EEG-Nummer, Seriennummer des Herstellers etc.), die installierte Kapazität, der Installationsort sowie der Betreiber und seine ID. Die Liste lässt sich je nach Anlagentyp beliebig lang fortsetzen und ist schwierig abzuschließen. Die Informationen im Marktstammdatenregister stellen ein Beispiel für Stammdaten dar.
Tarifanwendungsfall (TAF)	Tarifanwendungsfälle sind insgesamt 14 vordefinierte Prozedere und Funktionen, die in einem Smart Meter Gateway standardisiert aktiviert und abgebildet werden können. Ein einfaches Beispiel hierfür ist der TAF 7, der das SMGW dazu veranlasst, im Zusammenspiel mit der modernen Messeinrichtung (mME) 15-minütlich Messwerte an einen externen Marktteilnehmer zu übertragen.
Trust-Framework	Ein Trust-Framework beschreibt in der IT ein offizielles Rahmenwerk, das die Handhabung und Anerkennung von Zertifikaten und Formaten zwischen Akteuren regelt. Neben der Harmonisierung bei der Zusammenarbeit stehen in Trust-Frameworks die Ziele Interoperabilität und Datensouveränität im Vordergrund.
Übertragungsnetzbetreiber	Übertragungsnetzbetreiber sind für die Übertragungsnetze, das heißt für die Höchstspannungsleitungen, zuständig, verantwortlich. Sie sorgen für die Sicherheit und Stabilität des Netzes innerhalb einer Regelzone. Die vier Regelzonen in Deutschland verteilen sich auf die vier Übertragungsnetzbetreiber 50Hertz, Amprion, TenneT und TransnetBW.

Validator	Bestimmte Art von Nodes (Knoten) in dezentralen Systemen, die für die kryptografische Prüfung von verschlüsselten Transaktionsblöcken verantwortlich sind.
Verifiable Credentials (VCs)	Verifiable Credentials (VCs) sind ein offener Standard für digitale Ausweise. Sie können Informationen darstellen, die in physischen Ausweisen wie einem Reisepass oder Führerschein enthalten sind, aber auch neue Dinge, die keine physische Entsprechung haben, wie die Inhaberschaft eines Bankkontos. Sie haben zahlreiche Vorteile gegenüber physischen Ausweisen, insbesondere die Tatsache, dass sie digital signiert sind, was sie fälschungssicher und sofort überprüfbar macht. (Quelle: https://en.wikipedia.org/wiki/Verifiable_credentials)
Verifier	Ein Verifier fragt beim Holder die für den Anwendungsfall notwendigen Informationen in Form einer Verifiable Presentation an. Im Rahmen der Präsentation wird kryptografisch bewiesen, dass die zur Verfügung gestellten Informationen gültig sind und weder modifiziert noch vom Issuer widerrufen wurden.
Verteilnetzbetreiber	Die Verteilnetzbetreiber sind für die Nieder-, Mittel- und Hochspannungsnetze zuständig. Sie sind verantwortlich für den Transport und die Verteilung von Strom oder Gas sowie für den Betrieb, die Wartung und den Ausbau des eigenen Netzes in einem bestimmten Gebiet und gegebenenfalls der Verbindungsleitungen zu anderen Netzen. In Deutschland gibt es derzeit über 850 Verteilnetzbetreiber.
Wallet	Eine Wallet ist eine digitale Brieftasche, in der beispielsweise Bezahlkarten, Tickets oder auch Identitätsnachweise abgelegt werden können. In DIVE wurde die Krypto-Wallet Sporran eingesetzt (siehe DIVE-Berichtsteil „Technische Details und Umsetzung der Basisinfrastruktur“). Eine (Krypto-)Wallet ist eine digitale „Geldbörse“, die zur Aufbewahrung, zum Senden und zum Empfangen von Kryptowährung verwendet wird. Dabei speichert die Wallet nicht die Kryptowährungen selbst, sondern die Schlüssel, die den Zugriff auf die Kryptowährungen ermöglichen.
Zero-Knowledge Proof (ZKP)	Mit einem „Null-Wissen-Beweis“ kann nachgewiesen werden, von einem Geheimnis Kenntnis zu haben, ohne das Geheimnis selbst zu offenbaren. Einsatzgebiete finden sich beispielsweise in der Kryptografie und bei der Authentifizierung.

Ein Projekt der

dena

www.dena.de

future-energy-lab.de