Future Energy
Lab

BERICHT

DIVE – Digitale Identitäten als Vertrauensanker im Energiesystem

03 – Mehrwerte für die energie-wirtschaftlichen Anwendungsfälle

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:
Dr.-Ing. Alexander Bogensperger, FfE
Andreas Bruckmeier, FfE
Robert Sprunk, Energy Web
Felix Paetzold, Fraunhofer FIT
Felix Förster, OLI Systems
Linda Babilon, dena
Irene Adamski, dena

Konzeption & Gestaltung:
die wegmeister gmbh

Stand:
Juli 2025

Bitte zitieren als:
Deutsche Energie-Agentur (Hrsg.) (dena, 2025): DIVE – Digitale Identitäten als Vertrauensanker im Energiesystem. 03 – Mehrwerte für die energiewirtschaftlichen Anwendungsfälle

DIVE – Digitale Identitäten als Vertrauensanker im Energiesystem

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

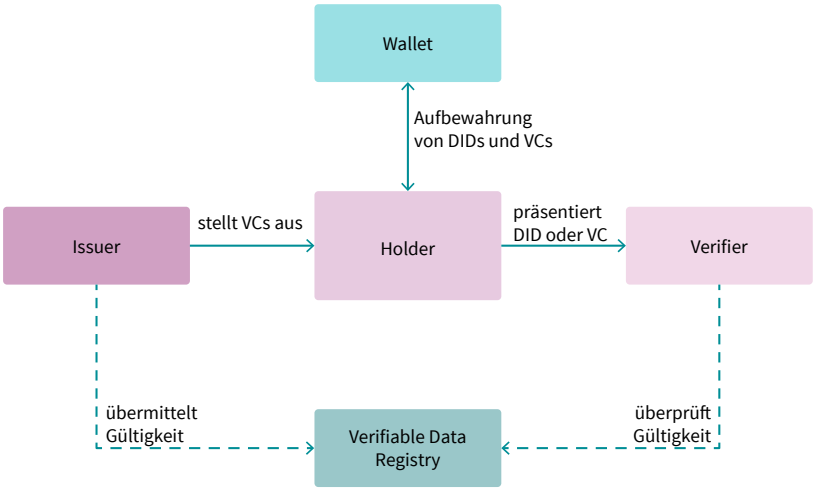

Abbildung 1: Vertrauensdreieck

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.

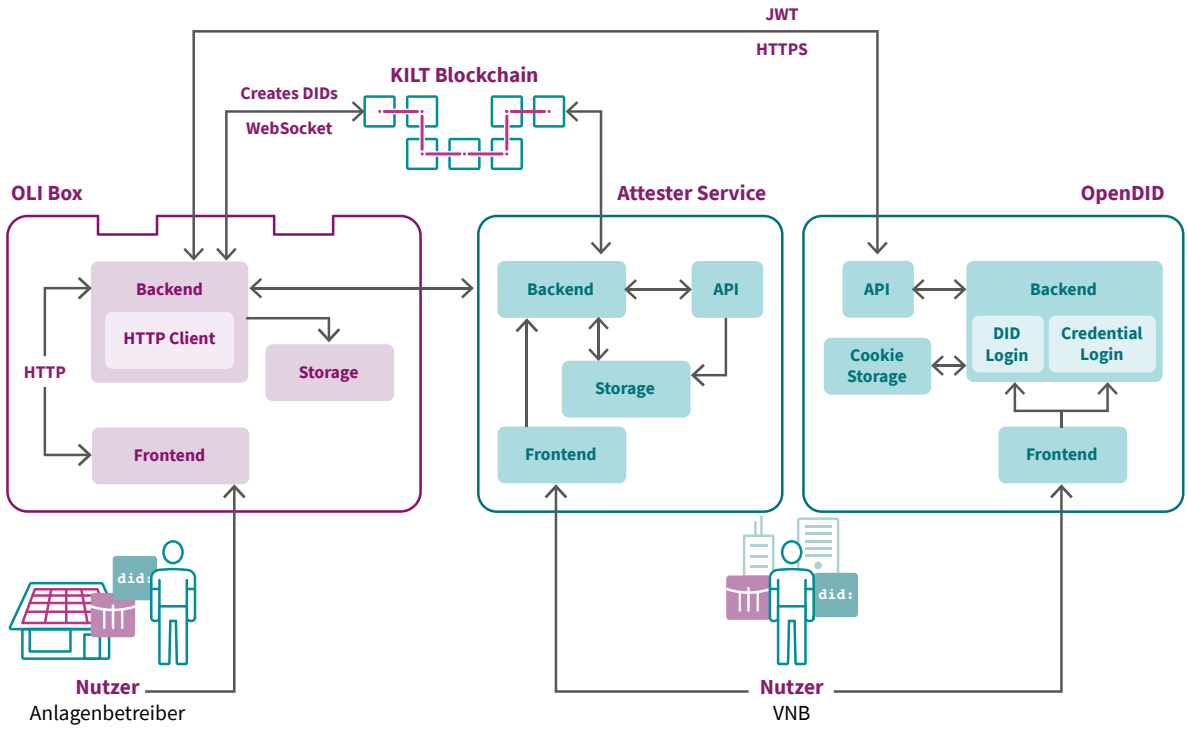

Abbildung 2: DIVE Basisinfrastruktur

Inhalt

1. Das Energiesystem im Wandel

Die für die Dekarbonisierung des Energiesystems entscheidende Energiewende und Sektorenkopplung erfordern eine intelligente Abstimmung zwischen der volatilen Erzeugung aus erneuerbaren Energien und modernen, flexiblen Verbrauchern. Die Digitalisierung ist hierbei die Verbindung zwischen allen Teilnehmern und technischen Einheiten im Energiesystem – vom Netz über die Verbraucher und Erzeuger bis hin zu den Anbietern von Flexibilität. Ohne die entsprechenden digitalen Schnittstellen, Prozesse und Systeme ist die Energiewende nicht effizient umsetzbar. Dabei ist das intelligente Messsystem (iMSys), das Verbrauchs- und Erzeugungswerte misst und übermittelt und die Möglichkeit eröffnet, Flexibilität zu steuern, nur der erste Schritt hin zu einer digitalen Energiewirtschaft.

Die Energiewirtschaft setzt zunehmend auf einen Pluralismus an Stakeholdern, die ihre Dienstleistungen in mehreren, teils verschiedenen Anwendungsfällen erbringen und miteinander interagieren. Die Mehrheit der Dienstleistungen und Interaktionen ist dabei auf digitale Schnittstellen und Daten angewiesen. Dabei ist entscheidend, dass diese Daten verlässlich und über sichere Kanäle bereitgestellt werden und inhaltlich auf ihre Vollständigkeit und Vertrauenswürdigkeit hin überprüfbar sind. Zudem muss die Energiewirtschaft aus ökonomischer Perspektive sicherstellen, dass die notwendigen digitalen Ressourcen ausreichend skalierbar sind und von allen relevanten Stakeholdern genutzt werden können. Gleichzeitig muss auf die Einhaltung globaler Marktregeln geachtet werden, um ein faires Marktgeschehen sowie die Stabilität und das Funktionieren des Energiesystems zu gewährleisten. Daher müssen auch für den wachsenden digitalen Bereich des Energiesystems sogenannte Governance-Regeln entwickelt und verankert werden.

Systemsicherheit braucht Marktregeln

Ein systemkritisches Beispiel für die Bedeutung von Marktregeln ist die Vermarktung von Flexibilität. Sie kann in Zukunft über § 14c Energiewirtschaftsgesetz (EnWG) an den Verteilnetzbetreiber oder über Regelleistung, marktbasierten Redispatch 3.0 oder § 13k EnWG an die Übertragungsnetzbetreiber vermarktet werden. Aggregatoren und Händler können Flexibilität für die Optimierung ihrer Intraday- oder Day-Ahead Beschaffung einsetzen und Bilanzkreisverantwortliche für die Optimierung ihres Bilanzkreises. Das Smart Meter Gateway (SMGW) und die Marktkommunikation stellen im Status quo dabei nur den Bezug von Messwerten sicher, nicht jedoch die Vermeidung von Doppelvermarktung. Wird beispielsweise die Flexibilität an mehrere Akteure gleichzeitig vermarktet, entstehen neben Mehrkosten insbesondere systemische Risiken, da jeder Nachfrager sich im Abruffall auf eine gesicherte Lieferung verlassen muss. Es ist daher unerlässlich, Marktregeln zu etablieren und sie automatisiert, skalierbar, sicher und zuverlässig prüfen zu können. Nur so ist eine Energiewende mit vielen dezentralen Flexibilitäten realisierbar.

Neue Anwendungsfälle müssen leicht skalierbar sein

In naher Zukunft wird es als Letztverbraucher – vor allem mit Energieerzeugungsanlagen als Prosumer (privat und gewerblich) oder mit einem Stromspeicher als Flexumer – möglich sein[1], eine Vielzahl an Dienstleistungen wahrzunehmen und mit eventuell verfügbarer Flexibilität sogar einen aktiven Beitrag zur Stabilisierung des Energiesystems zu leisten.

Zukünftige Anwendungsfälle für Prosumer und Flexumer wären,

- ihren Eigenverbrauch unkompliziert und automatisiert nach dynamischen Tarifen oder dem CO_2-Ausstoß auszurichten,
- an Energiegemeinschaften teilzunehmen und ihren überschüssigen Strom lokal mit ihrer Nachbarschaft zu teilen, direkt zu verkaufen oder zu spenden,
- ihre Flexibilität direkt einzusetzen, um das Verteilnetz zu entlasten (lokaler Flexibilitätsmarkt),
- vom Verteilnetzbetreiber abgeregelt zu werden, um das Netz zu entlasten (§ 14a EnWG),
- ihre Flexibilität über einen Aggregator auf dem Strommarkt oder für das Übertragungsnetz (z. B. Redispatch oder Regelleistung) einzusetzen,
- ihre Flexibilität direkt an den Übertragungsnetzbetreiber zu vermarkten (nur gewerblich),
- die grüne Eigenschaft ihres Erneuerbare-Energien-Überschusses über das Herkunftsnachweisregister oder einen anderen Anbieter zu verkaufen und so zusätzliche Erlöse zu erwirtschaften,
- ihren Stromverbrauch mit Dienstleistern zu teilen, um maßgeschneiderte Analysen zu erhalten,
- ihren Stromversorger in nahezu Echtzeit zu wechseln,
- oder an vielen anderen Mehrwertdiensten teilzunehmen, die ihnen angeboten werden.

Betrachtet man diese verschiedenen möglichen Anwendungsfälle (Use Cases) für Letztverbraucher, Prosumer oder Flexumer, wird deutlich, dass stets die gleichen Stammdaten über den Anschlussnutzer, die technischen Einheiten (z. B. Photovoltaik-Anlage oder Stromspeicher) und den Ort und die gleichen zusätzlichen Informationen (z. B. staatliche Förderungen) benötigt werden. Darüber hinaus müssen anwendungsspezifisch weitere Daten und Nachweise vorgelegt werden: Im konkreten Fall des Herkunftsnachweisregisters wird eine zusätzliche Identifikation über ein Postident-Verfahren gefordert, in anderen Fällen eine Präqualifikation der Regelleistung einer Anlage oder ein spezielles Gutachten. Heutzutage muss jeder Betreiber eines Anwendungsfalls (z. B. Umweltbundesamt, Netzbetreiber oder Lieferant) diese Stammdaten bei der Registrierung selbst erfassen und gegebenenfalls eine individuelle Prüfung beispielsweise durch einen Umweltgutachter durchführen lassen, um die Daten zu validieren.

1 Die Voraussetzung dafür ist eine Digitalisierung des Energiesektors und der Prozesse.

Allerdings wurden viele der dafür notwendigen Stammdaten bereits vom Verteilnetzbetreiber bei Inbetriebnahme der Anlage geprüft und teilweise im Marktstammdatenregister (MaStR) hinterlegt. Das MaStR kann jedoch nach heutigem Stand nur eingeschränkt für die oben genannten Zwecke genutzt werden (bereitgestellte Schnittstellen sind beispielsweise nicht maschinenlesbar). Die Daten müssen also von jedem Anbieter eines Anwendungsfalls neu erfasst und von den Teilnehmern neu eingetragen werden. In jedem dieser Systeme erhält der Teilnehmer eine eindeutige Identifikation, die akteursübergreifend jedoch nicht immer genutzt werden kann und zwischen den Akteuren nicht immer eindeutig ist.

Damit Dienstleistungen skalierbarer werden, braucht es einen standardisierten, schnellen und unkomplizierten Datenaustausch zwischen allen Akteuren. Zudem sollten Prozesse wie Registrierungsvorgänge automatisiert werden, um Kunden und Nutzern einen schnellen Zugang zu ermöglichen. Das steigert die Akzeptanz und den Mehrwert für alle Beteiligten und erleichtert den Markteintritt.

Anlagen müssen eindeutig und automatisiert identifizierbar sein

Durch die Vielzahl an Akteuren im Energiesystem werden Daten über Anlagen und Kunden an unterschiedlichen Stellen erhoben, gespeichert und gepflegt (z. B. Kundendaten bei verschiedenen Lieferanten). Neben vielen anderen Nachteilen ist durch diese redundante Datenhaltung die eindeutige Identifizierung von Anlagen oder Kunden, vor allem im Austausch zwischen Akteuren, mit einem hohen und zum Teil manuellen Abstimmungsaufwand verbunden. Es gibt heute zwar eine Vielzahl an Identifikationsnummern und Zertifikaten für die Identifikation und/oder Authentifizierung[2] im Energiesystem, es fehlt jedoch eine einheitliche und eindeutige Identifikation für Anlagen und Betreiber sowie die Möglichkeit, sich damit zwischen verschiedenen Marktteilnehmern automatisiert zu identifizieren und zu authentifizieren. Zwar ist dies im Rahmen der Smart Meter Public Key Infrastructure (SM-PKI) und der Marktkommunikation mittels Applicability Statement 4 (AS4)[3] mittlerweile für etablierte Akteure (z. B. Lieferanten) mit viel Aufwand realisiert, jedoch nicht für Letztverbraucher zugänglich.

Eine schnelle und eindeutige Identifikation im Segment der Letztverbraucher und Kleinstanlagen wird mit deren zunehmender Teilnahme an Anwendungsfällen im Energiesystem essenziell, um einerseits Systemstabilität und eine bessere Skalierbarkeit zu erreichen und andererseits die Einstiegshürden für eine Teilnahme an Anwendungsfällen zu minimieren.

Digitale Identitäten als Vertrauensanker im Energiesystem (DIVE)

Das Projekt DIVE – Digitale Identitäten als Vertrauensanker im Energiesystem – greift diese Herausforderungen auf und hat zum Ziel, Anlagen mittels digitaler Identitäten eindeutig zu identifizieren, zu authentifizieren und zu autorisieren. Dafür wurde eine Basisinfrastruktur geschaffen, um Datennutzung, Prozesse und Anwendungen sicher, vertrauenswürdig und skalierbar zu realisieren. Letztverbraucher bzw. Anlagenbesitzer sollen durch DIVE nur noch einmalig ihre Daten angeben müssen und daraufhin einfach, schnell und sicher am Energiesystem und entsprechenden Anwendungen teilnehmen sowie sich dabei stets eindeutig authentifizieren können. Zusätzlich stellt die DIVE-Infrastruktur automatisiert sicher, dass definierte Marktregeln eingehalten und die oben beschriebenen weiteren Risiken für die Systemsicherheit vermieden werden. Dafür werden sowohl bestehende Prozesse in der Energiewirtschaft als auch die entstehende Smart-Meter-Infrastruktur bestmöglich genutzt oder um notwendige Funktionalitäten erweitert.

Zum Berichtsteil

In diesem Berichtsteil „Mehrwerte für die energiewirtschaftlichen Anwendungsfälle“ wird zunächst auf die Anforderungen aus der Energiewirtschaft an eine Identitätsinfrastruktur geblickt und der Status quo aufgezeigt (Kapitel 2). In Kapitel 3 wird vorgestellt, wie die im Projekt umgesetzte DIVE-Basisinfrastruktur funktioniert und wie sie energiewirtschaftlich integriert ist. Die folgenden Kapitel 4 bis 6 zeigen, wie die DIVE-Basisinfrastruktur Mehrwerte für die beispielhaften Anwendungsfelder Herkunftsnachweise, Flexibilitätserbringung und Freiheit bei der Wahl des Stromlieferanten an Ladesäulen bieten kann. Der Berichtsteil schließt mit einem Fazit und Ausblick ab.

2 Zum Beispiel Stromnetzbetreibernummer, BDEW-Codenummer / Marktpartneridentifikationsnummer / Global Location Number, EIC-X-Codes (Energy Identification Codes (EIC), MaStR-Nr., BNetzA-Betriebsnummer, ACER-Codes, SMGW Public Keys, S/MIME-Zertifikate, Ressourcen-IDs, Marktlokations-ID, Messlokations-ID und Netzlokations-ID

3 Die Marktkommunikation muss seit dem 1. April 2024 über den Übertragungsweg AS4 durchgeführt werden. Abgesichert mit TLS (Transport Layer Security) unter Nutzung der SM-PKI wird die Sicherheit der Übertragung erhöht.

2. Anforderungen an ein digitales Energiesystem

Die Basis für ein digitales Energiesystem bildet eine digitale Mess- und Steuerungsinfrastruktur, die nachfolgend kurz vorgestellt wird. Dies ist ein erster Schritt auf dem Weg zu einem digitalen Energiesystem. Für eine Ende-zu-Ende-Digitalisierung aller Akteure und Anlagen bestehen weitere energiewirtschaftliche Anforderungen, auf die in diesem Kapitel eingegangen wird.

2.1 Grundlagen zum intelligenten Messsystem

Intelligente Messsysteme (iMSys) – auch Smart Meter genannt – sind ein wichtiger Schritt hin zu einem digitalen Energiesystem. Sie erweitern Zählpunkte mit geeichten Zählern (moderne Messeinrichtungen, mME) um eine sichere Kommunikationseinheit (Smart Meter Gateway, SMGW), die die Übermittlung von Messdaten und das Steuern von flexiblen Erzeugern und Verbrauchern über einen CLS-Kanal (Controllable Local Systems) erlaubt. Auf einem Sicherheitsmodul des SMGW werden private Schlüssel und entsprechende Zertifikate gehalten, mit denen ein Smart Meter eindeutig identifiziert werden kann und mit deren Hilfe im Rahmen der Smart Meter Public Key Infrastructure (SMPKI) die Authentifizierung und verschlüsselte Kommunikation erfolgen. Jeder Marktteilnehmer, der mit dem SMGW interagieren will, benötigt ebenfalls ein entsprechendes Schlüsselpaar und ein Zertifikat, das die Teilnahme an der SM-PKI erlaubt. Die Zertifikate ermöglichen eine Verknüpfung digitaler Signaturen und öffentlicher Schlüssel mit realen Unternehmen oder Smart Metern. Um einen Zugang zur SM-PKI zu erhalten und eine Kommunikation direkt zum SMGW aufzubauen, sind zum jetzigen Zeitpunkt jedoch große technische und finanzielle Ressourcen, zum Beispiel für die Beschaffung der Infrastruktur und die Erfüllung von Sicherheitsanforderungen oder hinsichtlich der Kosten von Software-as-a-Service-Lösungen, erforderlich. Seit der Einführung des AS4-Standards erfordert nun auch die Marktkommunikation die Verwendung von SM-PKI-Zertifikaten. Beides ermöglicht den sicheren Austausch zwischen eindeutig identifizierbaren Marktteilnehmern untereinander (via Marktkommunikation und AS4-Standard) sowie mit Smart Metern (SM-PKI).

Die Umsetzung der Grundidee, eine sichere, verlässliche, geeichte und standardisierte Mess- und Steuerungsinfrastruktur zu schaffen, ist für die Energiewende entscheidend. Es besteht jedoch eine zentrale Herausforderung darin, dass die vorhandenen Kommunikationskanäle zwar sicher und vertrauenswürdig, aber nicht für alle Teilnehmer im Energiesystem, vor allem Letztverbraucher, nutzbar sind. Ein immer stärker dezentralisiertes System mit vielen neuen Akteuren benötigt jedoch eine sichere Kommunikation, wie zum Beispiel eine eindeutige Authentifizierung zwischen den Prosumern in einer Energiegemeinschaft oder von einem Elektrofahrzeug gegenüber einer öffentlichen Ladesäule, dem jeweiligen Backend des Charge Point Operators (CPO), dem E-Mobility Service Provider, dem Stromlieferanten und gegebenenfalls dem Netzbetreiber.

Schalten mit dem SMGW (BNetzA 2024)

Mit dem Smart Meter Gateway müssen nach § 19 Abs. 2 MsbG und § 34 MsbG (Messstellenbetriebsgesetz) alle abrechnungs-, bilanzierungs- und netzrelevanten Standardleistungen abgewickelt werden. Das heißt, die Abrechnung dynamischer Tarife (Geschäftsprozesse zur Kundenbelieferung mit Elektrizität, GPKE) und die Bilanzierung (Marktregeln für die Durchführung der Bilanzkreisabrechnung Strom, MaBis) dürfen nur auf Basis von Messwerten aus dem SMGW erfolgen.

Bei der Schaltung ist die Sachlage differenzierter. Hier müssen alle durch oder für den Netzbetreiber durchgeführten Schalthandlungen über das SMGW erfolgen. Dies beinhaltet alle Schalthandlungen nach § 13 EnWG und § 14 a/c EnWG. Auch die Direktvermarktung nach dem Erneuerbare-Energien-Gesetz (EEG) muss über das SMGW abgewickelt werden.

Ausgenommen davon sind dagegen all diejenigen Anwendungsfälle, die nur den Energieserviceanbieter sowie den Lieferanten betreffen und die zum Beispiel auf eine Optimierung des Stromverbrauchs hinter dem Zähler zielen.

2.2 Energiewirtschaftliche Anforderungen

Im Projekt DIVE sollen die für das SMGW erdachten Grundsätze in eine für alle Marktteilnehmer generell nutzbare Form überführt werden. Dies soll es ermöglichen, Anlagen eindeutig zu identifizieren und Daten, die nicht direkt über das SMGW erfasst werden (und damit nicht geeicht sind) vertrauenswürdiger bereitzustellen. Zudem soll eine Grundlage geschaffen werden, um skalierbare und sichere Prozesse zu etablieren und dabei die Einhaltung globaler Marktregeln (wie beispielsweise den Wechsel zwischen Dienstleistungen) sicherzustellen.

Abbildung 3 zeigt, wie sich die DIVE-Basisinfrastruktur im Kontext der SM-PKI und der Marktkommunikation einordnet. Daraus wird deutlich, dass das DIVE-Ökosystem in den Bereichen, die bisher größtenteils unreguliert sind, einen Mehrwert bietet, nämlich beim Letztverbraucher und bei Anwendungen.

Derzeit wird die SM-PKI bis zum Smart Meter beim Letztverbraucher reguliert (durch den CLS-Kanal gegebenenfalls noch bis zum Energiemanagementsystem). Die regulierte Marktkommunikation (MaKo) verbindet die SM-PKI über den Messstellenbetreiber (MSB) mit den Marktteilnehmern. Je nach Anwendungsfall können oder müssen Daten und Schaltsignale die offiziellen Übertragungswege der MaKo und die SM-PKI nutzen oder können direkt zum Energiemanagementsystem (EMS) übertragen werden. Muss ein Anwendungsfall zum Bezug von Messdaten die MaKo-Prozesse nutzen, ist dies auf zwei Wegen möglich: Der Anbieter der Anwendung kann ein Energieserviceanbieter (ESA) werden oder er nutzt ein Messprodukt beim MSB der Anlage. In beiden Fällen ist der Datenaustausch reguliert und für die entscheidenden Akteure im Energiesystem transparent. Messdaten und Schalthandlungen hingegen, die direkt mit dem EMS oder Anlagen beim Letztverbraucher kommuniziert werden, unterliegen bisher keinen Regularien. Die DIVE-Basisinfrastruktur bietet hier eine einheitliche Kommunikationsgrundlage, da sie auch Akteure wie Prosumer, Letztverbraucher oder Anbieter von

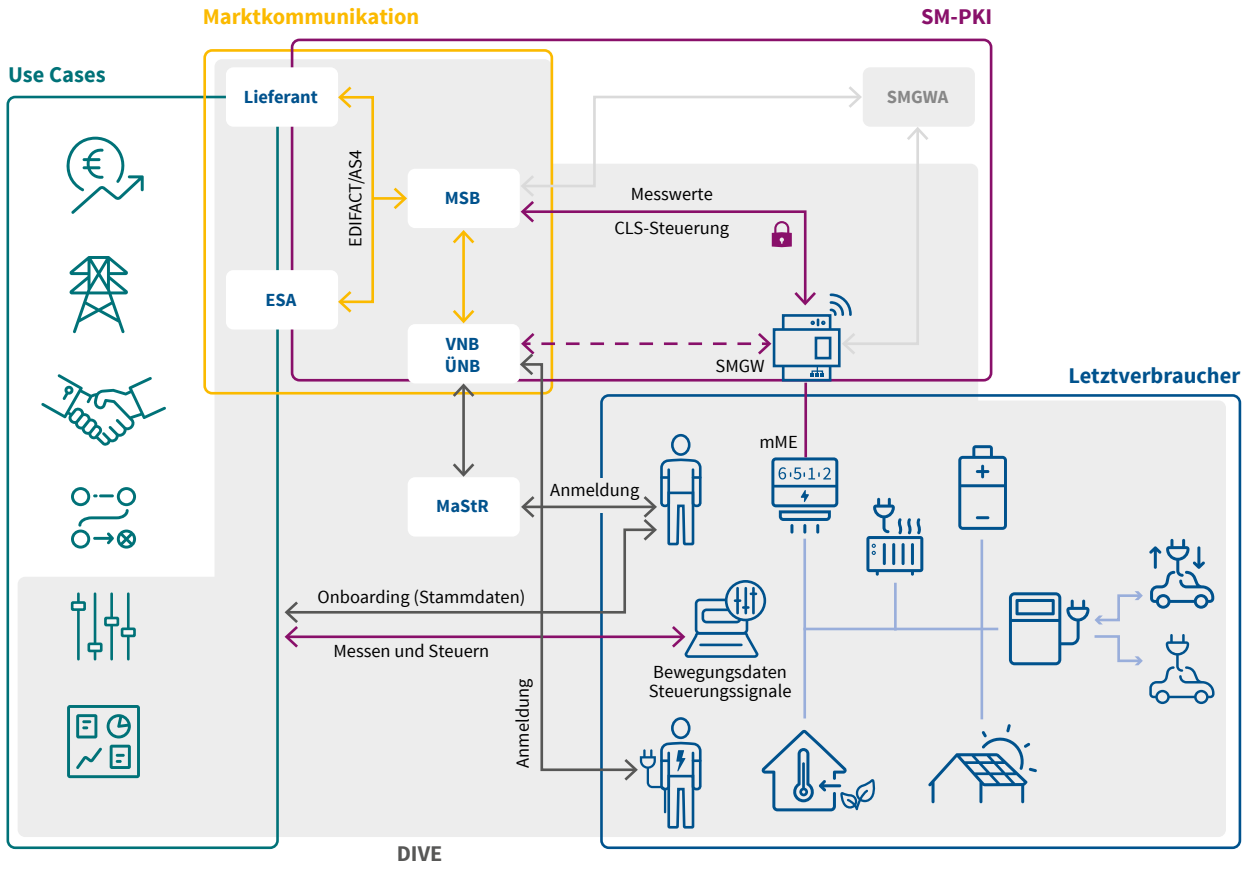

Abbildung 3: Wirkbereich der DIVE-Basisinfrastruktur im Kontext der SM-PKI und der Marktkommunikation

Dienstleistungen mit einbezieht, die bisher in der energiewirtschaftlichen Kommunikation nicht oder kaum berücksichtigt wurden.

In diesem nicht regulierten Bereich und im regulierten Bereich existieren Anforderungen, die die DIVE-Basisinfrastruktur zu erfüllen versucht. Hier eine Auswahl dieser Anforderungen:

Als Betreiber von Kritischer Infrastruktur in einem digitalen Energiesystem

- … muss ich mich auf Bewegungs- und Stammdaten verlassen können, da sie die Basis für einen sicheren Systembetrieb sind.
- … müssen Marktregeln (z. B. keine Doppelvermarktung von Flexibilität) zwingend eingehalten werden, um die Systemstabilität nicht zu gefährden.
- … müssen alle Marktpartner eindeutig identifiziert und authentifiziert werden, um eine sichere Kommunikation gewährleisten zu können.

Als Letztverbraucher oder Prosumer in einem digitalen Energiesystem

- … möchte ich einfach und schnell an Dienstleistungen jeder Art teilnehmen, ohne dass dadurch unnötige Kosten oder Mehraufwand (z. B. durch die erneute Registrierung) für mich entstehen.
- ... möchte ich die Datenhoheit über meine personenbezogenen Daten sicherstellen, damit ich selbst entscheiden kann, wer wann Zugriff auf meine Daten hat.

Als Anbieter einer Dienstleistung in einem digitalen Energiesystem

- … möchte ich meinen Kunden (z. B. Prosumern) einen möglichst niederschwelligen Einstieg zu meinen Dienstleistungen ermöglichen.
- … benötige ich verifizierte Mess- und Stammdaten als vertrauenswürdige und einheitliche Grundlage für alle Anwendungsfälle.

- … benötige ich verifizierte Bewegungsdaten als vertrauenswürdige und einheitliche Grundlage für von mir angebotene Flexibilitätsdienstleistungen.[4]

- … möchte ich eine skalierbare, sichere und unkomplizierte Authentifizierungsfunktion für alle Anlagen und alle Akteure. Diese verringert das Risiko von Identitätsbetrug, Datenverletzungen und unbefugtem Zugriff und ermöglicht mir die Konzentration auf mein Kerngeschäft.

- … möchte ich eine Lösung, um schnell und unkompliziert überprüfen zu können, ob meine Kunden gegen Marktregeln verstoßen oder nicht, und dementsprechend einer Teilnahme an meinem Anwendungsfall zuzustimmen oder sie abzulehnen.

Als Hersteller von neuen energietechnischen Anlagen (z. B. Speichern)

- … möchte ich diese Anlagen effizient und schnell am Energiesystem anmelden bzw. darin einbinden.

- … möchte ich meinen Kunden die Teilnahme an jeglichen Dienstleistungen eines digitalen Energiesystems schnell und einfach ermöglichen und so den Mehrwert meiner Produkte steigern.

- … möchte ich die Kosten meiner Produkte nicht durch zusätzliche Funktionalitäten unnötig in die Höhe treiben.

Als Akteur in einem digitalen Energiesystem

- … benötige ich die eindeutige und systemübergreifende Identifikation von Anlagen, damit ich mit anderen Marktakteuren zu jeder Zeit über dieselbe Anlage bei demselben Datenstand sprechen kann. Das vermeidet Probleme mit inkonsistenten Daten, die viel Korrekturaufwand und Kosten verursachen (z. B. aktuell beim Lieferantenwechsel) oder Doppelvermarktung (§ 80 EEG) zulassen.

Als Regulator eines digitalen Energiesystems

- … muss ich sicherstellen, dass globale Marktregeln eingehalten werden und ich dies auch prüfen kann. Dies stellt beispielsweise die Vermeidung von Doppelvermarktung sicher.

Als Betreiber einer Bestandsanlage

- … benötige ich eine einfache und kostengünstige Opt-in-Integration für meine Bestandssysteme in ein digitales Energiesystem.

Als Netzbetreiber

- … möchte ich den Prozess der Prüfung einer Anlage im Marktstammdatenregister sowie die Aktualisierung von bestehenden Daten möglichst effizient abwickeln, um eine vollständige und aktuelle Datengrundlage zu schaffen.

- … möchte ich meinen Anschlussnutzern und Anschlussnehmern möglichst einfache Prozesse zur Verfügung stellen, um alle Daten zu erhalten, die ich für den sicheren Betrieb meiner Netze benötige.

Die vorgestellten Anforderungen bilden die Grundlage für die im Rahmen des Projekts entwickelte DIVE-Basisinfrastruktur. Sie zielt darauf ab, vielen bestehenden Herausforderungen zu begegnen und viele Lücken in der digitalen Infrastruktur zu schließen.

2.3 Mehrwerte durch digitale Identitäten in DIVE

Die im Projekt entwickelte DIVE-Basisinfrastruktur bietet ein digitales und dezentrales Identitätsmanagement für die Anforderungen eines digitalen Energiesystems. Digitale Identitäten, die in der DIVE-Basisinfrastruktur eingesetzt werden, basieren auf international anerkannten und geprüften Standards.[5] Konkret werden Self-Sovereign Identities (SSI) eingesetzt. Dabei wird für jede Entität ein sogenannter Decentralized Identifier (DID) ausgestellt, der einen Akteur oder eine Anlage eindeutig identifiziert.[6] Für die Verwendung und Verwaltung von DIDs wird ein sogenanntes digitales Schlüsselpaar verwendet, bestehend aus einem privaten und einem daraus abgeleiteten öffentlichen Schlüssel. Darüber wird kryptografisch sichergestellt, dass die zur digitalen Identität gehörende DID nicht von anderen Akteuren verwendet werden kann.

Das System der digitalen Identitäten in DIVE ist vergleichbar mit einer Public-Key-Infrastruktur, wie sie auch im Rahmen der SMGW-Infrastruktur vom Bundesamt für Sicherheit in der Informationstechnik (BSI) realisiert wurde. Das in DIVE entwickelte Ökosystem ist jedoch offener und dezentraler gestaltet als die SM-PKI und setzt vor allem darauf, dezentrale Anlagen und Akteure in den Energiemarkt zu integrieren. Diesen Akteuren ist es aufgrund technischer, ökonomischer und rechtlicher Hürden bisher nicht möglich, an der Marktkommunikation oder der SM-PKI aktiv teilzunehmen.

Die DIVE-Infrastruktur soll diese Lücke schließen und eine skalierbare Lösung darstellen, um notwendige Funktionen aus der SM-PKI und der Marktkommunikation auf Millionen dezentrale Anlagen zu übertragen, ohne das bestehende System zu kompromittieren oder grundlegend anpassen zu müssen. Damit wird das digitale Energiesystem sicherer und nutzerfreundlicher.

4 Über das SMGW erhalte ich nur geeichte Messwerte (in der Regel des Summenzählers), zur möglichst genauen Berechnung der verfügbaren Flexibilität werden jedoch beispielsweise auch alle Daten zu Geräten hinter dem Zähler und weitere Bewegungsdaten (z. B. State of Charge des Hausspeichers) benötigt.

5 Die Schlüsselkomponenten Decentralized Identifier (DID) und Verifiable Credential (VC) wurden von der Decentralized Identity Foundation (DIF) entwickelt und vom W3C standardisiert: https://www.w3.org/TR/did-core/ und https://www.w3.org/TR/vc-data-model/.

6 Der Identifier besteht optisch aus einer Reihe von Sequenzen von Zahlen und Buchstaben, die nach bestimmten Regeln aufgebaut und dadurch einmalig sind. In der Praxis ist diese DID-Sequenz entscheidend, weshalb im deutschen Sprachgebrauch allgemein und auch in den DIVE-Berichten sowohl die Begriffe „der digitale Identifier" als auch „die DID" verwendet werden.

Die DIDs werden – ähnlich wie bei digitalen Zertifikaten – mit zusätzlichen Nachweisen über Stammdaten (auch Attribute oder Eigenschaften), den sogenannten Verifiable Credentials (VCs), angereichert. In der Praxis können das zum Beispiel Anlagendetails wie der Besitzer oder die installierte Leistung der Anlage sein. Diese Nachweise über die Stammdaten des Identitätsinhabers, des sogenannten Holders (siehe Abbildung 4), werden beim Holder selbst gespeichert. Er entscheidet selbstbestimmt und ausschließlich, welche seiner Daten mit wem geteilt werden sollen. Die VCs werden dabei von einem vertrauenswürdigen Akteur, einem sogenannten Issuer (z. B. einer Behörde) überprüft und bescheinigt. Der Holder, also der Inhaber des Credentials, kann das Credential vollständig oder nur Teile davon mit Dritten teilen. Der Issuer ist in diesen Vorgang nicht mehr direkt eingebunden. Die dritte Partei, der sogenannte Verifier, kann der Authentizität des Credentials trauen, da dies kryptografisch überprüfbar ist. Einzige Voraussetzung ist, dass der Verifier die Vertrauenswürdigkeit des Issuers akzeptiert. Das so entstehende Vertrauensdreieck ist in Abbildung 4 dargestellt.

Die Gültigkeit des Verifiable Credentials kann über eine Verifiable Data Registry überprüft werden. Dies dient unter anderem dem Zweck, VCs zu einem späteren Zeitpunkt wieder zurückziehen zu können, wenn sie ihre Gültigkeit verlieren. Die Verifiable Data Registry ist im Piloten des Projekts DIVE dezentral mit der KILT Blockchain realisiert, was prinzipiell jedoch auch durch eine zentrale, für alle beteiligten Akteure vertrauenswürdige Partei umgesetzt werden könnte. In jedem Fall enthält die Verifiable Data Registry ausschließlich Informationen über die Echtheit eines VC, die Inhalte eines Credentials liegen stets beim Identitätsinhaber selbst.

Der Prozess, Verifiable Credentials zu erstellen und zu prüfen, läuft ähnlich zu Prozessen der Marktstammdatenregisterverordnung (MaStRV), nach der entweder der Anlagenbetreiber oder der Installateur die Anlage im MaStR registriert und die Stammdaten hinterlegt (Rolle des Holders) und der Netzbetreiber sie prüft und freigibt (Rolle des Issuers). Das in DIVE genutzte System setzt jedoch darauf, dass die so entstandenen verifizierten Daten (Verifiable Credentials) nicht auf einer zentralen Plattform liegen und dort verwaltet werden, sondern digital beim Holder (z. B. der Anlage selbst) gehalten und verwaltet werden.

Ein Akteur oder eine technische Anlage kann sich mittels DID eindeutig ausweisen, die Kommunikation digital verschlüsseln und seine bzw. ihre VCs nutzen, um mit bestätigten Stammdaten zum Beispiel die Registrierung bei energiewirtschaftlichen Anwendungsfällen schnell und unkompliziert abzuwickeln. Das bedeutet für alle Beteiligten weniger Aufwand für die Teilnahme am Energiesystem, klar definierte Schnittstellen und einen sicheren Datenaustausch. Die DID erfüllt die Funktion einer Authentifizierung, ohne dass dafür Abhängigkeiten von zentralen Plattformen entstehen (und damit auch keine „Single Points of Failure“ oder „Honeypots“).

Für Anbieter von Anwendungsfällen wird der Prozess zur Registrierung von Anlagen deutlich vereinfacht und die angegebenen Daten sind vertrauenswürdiger, da sie bereits von unabhängigen Dritten geprüft wurden. Zudem kann die Kommunikation zwischen verschiedenen Marktteilnehmern vereinfacht werden, da alle Teilnehmer die korrekten Stammdaten der Anlagen besitzen

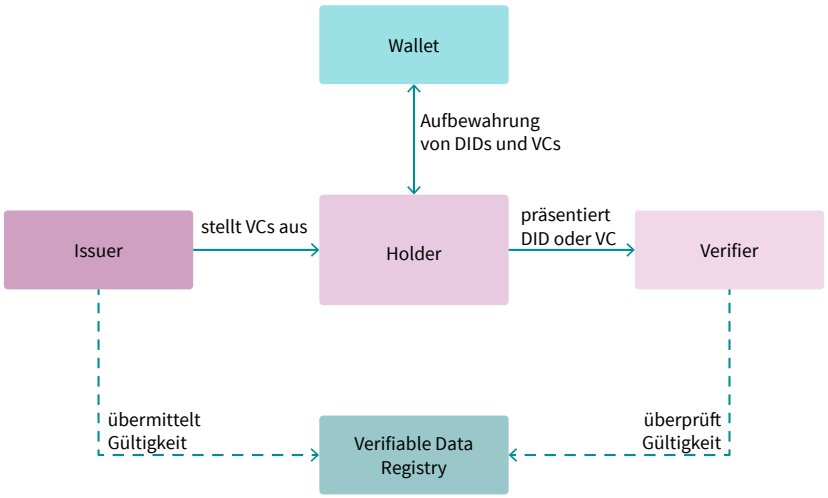

Abbildung 4: Vertrauensdreieck

und über die DID auch eindeutig über dieselben Anlagen sprechen können.

Detailliertere Erläuterungen zur Architektur und Funktionsweise finden sich im Berichtsteil „Technische Details und Umsetzung der Basisinfrastruktur“ in Kapitel 3 und 4.

2.4 Einhaltung von Marktregeln

Die DIVE-Basisinfrastruktur ist nicht nur hilfreich, um dezentrale Anlagen und die vielen Akteure einfach ins Energiesystem zu integrieren. Sie ist vor allem die Grundlage für eine energiesystemisch relevante Funktion, nämlich die Einhaltung von Marktregeln. Die DIVE-Basisinfrastruktur stellt über kryptografische Verfahren sicher, dass zuvor definierte Marktregeln eingehalten werden. Beispielhaft sei hier der Prozess des Lieferantenwechsels genannt, der aktuell sehr aufwendig ist, teils viel manuellen Aufwand erfordert (zum Beispiel wenn Daten inkonsistent sind) und daher noch relativ lange dauert. Durch die DIVE-Basisinfrastruktur kann beispielsweise ausgeschlossen werden, dass Verbraucher Lieferverträge mit mehreren Lieferanten gleichzeitig eingehen. Noch bedeutender ist jedoch, dass Flexibilität nicht gleichzeitig an Verteilnetzbetreiber, Übertragungsnetzbetreiber, Aggregatoren oder Energiegemeinschaften vermarktet werden kann oder dass die Stromherkunft in der lokalen Energiegemeinschaft nicht visualisiert wird, ohne dass auch Herkunftsnachweise der Anlage vorliegen.

Die Einhaltung von Marktregeln in skalierbarer Form ist eine Grundvoraussetzung für ein digitales Energiesystem, in dem Millionen von Anlagen, Geräten innerhalb des IoT (Internet of Things) u.v.m. untereinander und mit energiewirtschaftlichen Akteuren sicher, schnell und vertrauenswürdig kommunizieren können.

3. Die DIVE-Basisinfrastruktur

Die DIVE-Basisinfrastruktur verbindet alle Ebenen des Energiesystems miteinander, um Identitäten zu verwalten und um damit Datennutzung, Prozesse und Anwendungen sicher, vertrauenswürdig und skalierbar zu realisieren. Mit dieser Infrastruktur werden die im vorherigen Kapitel 2.2 aufgeführten energiewirtschaftlichen Anforderungen an ein zukünftiges digitales Energiesystem adressiert.

Abbildung 5 zeigt die Verknüpfung der verschiedenen oben genannten Komponenten und Akteure mit der DIVE-Basisinfrastruktur und hebt ausgewählte funktionale Komponenten hervor. Darauf folgend werden die Vorgänge zur Registrierung von Anlagen und Akteuren in der DIVE-Basisinfrastruktur sowie Funktionalitäten zur Einhaltung von Marktregeln und für den erleichterten Zugriff auf Messdaten von Anlagen beschrieben.

technischen Anlagen per Software mitgeliefert oder mit höherem Sicherheitsstandard mittels Krypto-Chip bereitgestellt werden. Bei Bestandsanlagen kann dies durch Nachrüstung eines Energiemanagementsystems (EMS) geschehen. Dieses übernimmt dann die für die DIVE-Basisinfrastruktur benötigten Funktionalitäten für alle technischen Einheiten innerhalb eines Gebäudes bzw. hinter einem Zähler. Marktakteure können das Schlüsselpaar der Anlage oder des EMS in einer sogenannten Wallet sicher verwahren – ähnlich wie dies bei digitalen Zertifikaten heute bereits in ERP-Systemen (Enterprise Resource Planning) oder beim digitalen Personalausweis der Fall ist.

Es entsteht ein digitaler Ort direkt bei der Anlage, an dem alle zu einer Anlage gehörenden Daten in ihrer aktuellsten Form vorliegen. Da diese Daten direkt vom Anlagenbesitzer oder teils auto-

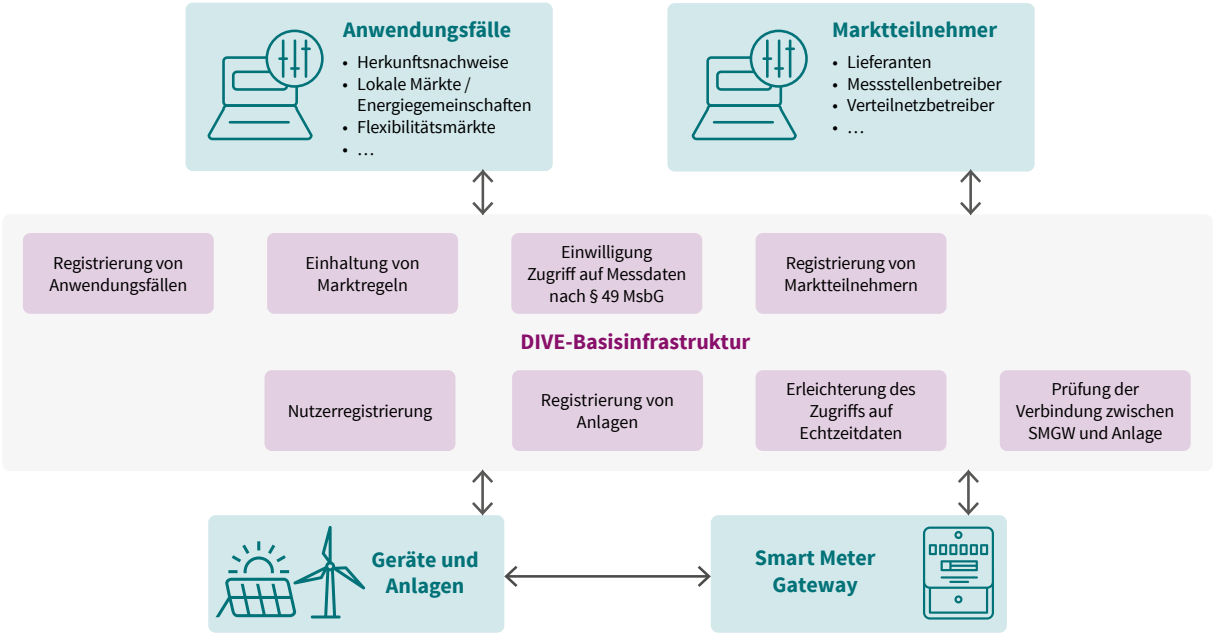

Abbildung 5: Funktionales Architekturschaubild der DIVE-Basisinfrastruktur im Kontext von energiewirtschaftlichen Anlagen und Akteuren; einzelne Funktionalitäten der Basisinfrastruktur werden hervorgehoben

Die einzelnen technischen Komponenten, auf deren Basis die DIVE-Basisinfrastruktur betrieben wird, werden im Berichtsteil „Technische Details und Umsetzung der Basisinfrastruktur“ dieser Berichtsreihe intensiver beleuchtet. In diesem Kapitel wird nur kurz auf technische Aspekte eingegangen, während der Fokus auf der energiewirtschaftlichen Integration von Anlagen und Akteuren des Energiesystems in die DIVE-Basisinfrastruktur liegt.

3.1 Technische Komponenten

Analog zur Smart-Meter-Infrastruktur setzt die DIVE-Basisinfrastruktur auf asymmetrische Verschlüsselung mittels eines Schlüsselpaars aus privatem und öffentlichem Schlüssel. Dieses Schlüsselpaar kann entweder direkt bei neu produzierten

matisiert von der Anlage selbst aktualisiert und verwaltet werden, können Redundanzen und Inkonsistenzen bei der Datenhaltung vermieden werden. Werden zudem Bewegungsdaten von der Anlage versandt (z. B. aktueller Batteriefüllstand), können die Daten verschlüsselt und authentifiziert übermittelt werden, wodurch sichergestellt ist, dass die Daten tatsächlich von der Anlage selbst stammen.

3.2 Registrierung energiewirtschaftlicher Akteure

Eine Integration der DIVE-Basisinfrastruktur in die bestehende Energiewirtschaft benötigt zunächst die Registrierung der Geräte und Anlagen sowie der Akteure des Energiesystems.

Abbildung 6 zeigt das funktionale Architekturschaubild der DIVE-Basisinfrastruktur mit Fokus auf die Schnittstellen zu energiewirtschaftlichen Anlagen und Akteuren. Für die verschiedenen Akteure bedarf es unterschiedlicher Onboarding-Prozesse.

- Der Onboarding-Prozess für Anlagen sorgt dafür, dass Bestands- und Neuanlagen sowohl eine eindeutige digitale Identität als auch erste verifizierte Anlagendaten als VCs erhalten. Die Anlagen sind im Anschluss daran eindeutig identifizierbar und authentifizierbar und können mit den von etablierten Marktakteuren geprüften Stammdaten an verschiedenen Anwendungsfällen teilnehmen.

- Der Onboarding-Prozess für Marktteilnehmer dient dem Zweck, etablierte Marktakteure, die sich bereits in der SM-PKI und/oder der Marktkommunikation befinden, mit einer DID und zugehörigen VCs zu versehen. Dies ist notwendig, damit sie ebenfalls die DIVE-Basisinfrastruktur nutzen können. Beispielsweise würde hier ein Verteilnetzbetreiber registriert, um anschließend als vertrauenswürdiger Systemakteur VCs über die Stammdaten neu registrierter Anlagen auszustellen.

- Der Onboarding-Prozess der Smart-Meter-Infrastruktur verfolgt das Ziel, die bestehenden Smart Meter mit der DIVE-Basisinfrastruktur zu verbinden und so eine Vertrauenskette über die SM-PKI hinaus zu etablieren, ohne diese sicherheitstechnisch zu kompromittieren. Zudem wird ein Prozess etabliert, mit dem einfach, schnell und sicher ein Zugriff auf Messwerte aus dem Smart Meter Gateway mittels der DIVE-Basisinfrastruktur autorisiert werden kann (§ 49 Abs. 7 MsbG).

- Der Onboarding-Prozess für Anlagen in Anwendungsfällen (z. B. Herkunftsnachweise, Regelleistung) stellt eine Basisfunktionalität zur Verfügung, um beliebige Anlagen oder Geräte, die bereits Teil der DIVE-Basisinfrastruktur sind, zu integrieren. Anlagen können auf diese Weise einfach, schnell und sicher an Anwendungsfällen teilnehmen und zwischen Anbietern wechseln. Dabei werden Marktregeln eingehalten und Doppelvermarktung wird ausgeschlossen.

Nachfolgend werden die einzelnen Onboarding-Vorgänge in Kurzform beleuchtet.

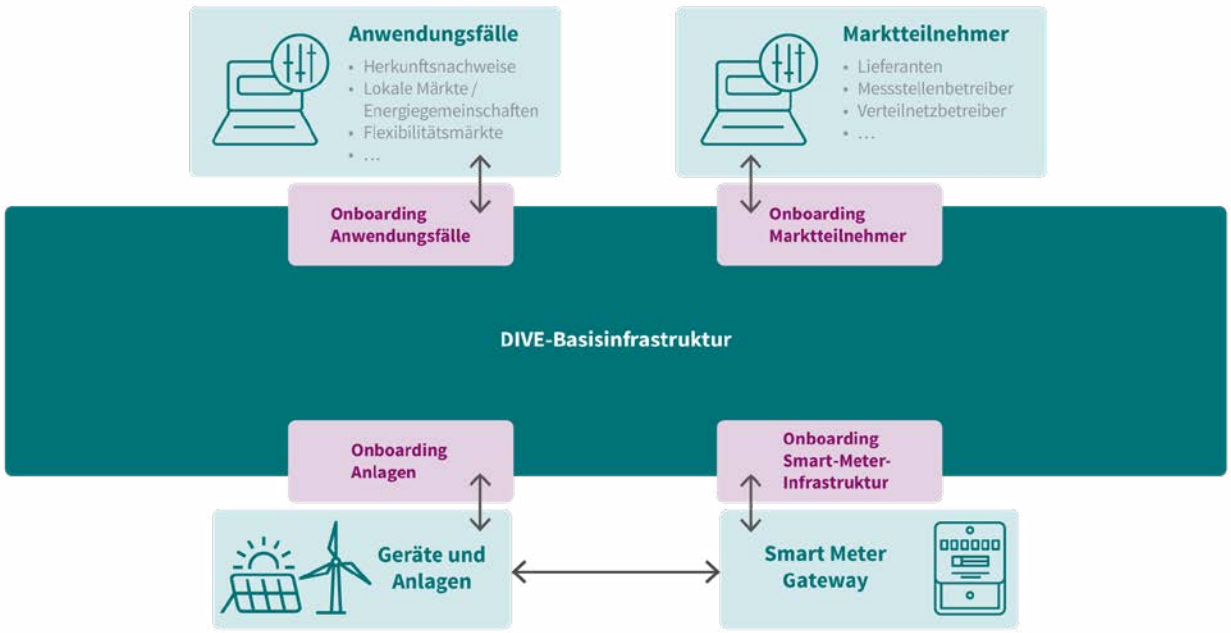

Abbildung 6: Das funktionale Architekturschaubild der DIVE-Basisinfrastruktur zeigt die Schnittstellen zu energiewirtschaftlichen Teilnehmern, die einer Integration durch Registrierung bedürfen

3.2.1 Onboarding von Anlagen

Für die Teilnahme an der DIVE-Basisinfrastruktur benötigen Anlagen bestimmte Funktionalitäten, die von den Herstellern bereitgestellt werden können. Bei Bestandsanlagen können diese Funktionen von einem Zusatzmodul, beispielsweise einem Energiemanagementsystem, für die Anlage übernommen werden. Damit kann die Anlage sowohl mit einer DID als auch mit Verifiable Credentials ausgestattet werden. Bei Anlagen mit integrierter DIVE-Funktionalität kann der Hersteller bereits einige Stammdaten und Anlagenspezifikationen für ein Credential hinterlegen bzw. vorausfüllen, beispielsweise die Nennleistung, die Speicherkapazität oder auch Schnittstellendefinitionen zum Messdatenabruf.

Der Prozess, wie eine Anlage weitere Credentials (z. B. den Netzanschlusspunkt) erhält, orientiert sich an bestehenden energiewirtschaftlichen Prozessen. So muss bereits heute nach der existierenden Marktstammdatenregisterverordnung (MaStRV) der Verteilnetzbetreiber (VNB) alle Daten von neu in seinem Netz angeschlossenen Anlagen (z. B. Erneuerbare-Energien-Anlagen und Speicher) prüfen. Zudem müssen beispielsweise private Ladestationen für Elektrofahrzeuge nach § 19 Niederspannungsanschlussverordnung (NAV) beim VNB angemeldet und bei über 11 Kilowatt Leistung vom VNB genehmigt werden. Diese (und weitere) Prozesse werden durch die DIVE-Basisinfrastruktur weitestgehend automatisiert und vereinfacht. Durch die Verifizierung der Daten und die Möglichkeit, ihre Gültigkeit jederzeit zu aktualisieren, sind die Daten dann auch für weitere Anwendungsfälle oder andere Energiesystemakteure weiter nutzbar.

zusätzlichen Geräts bzw. einer zusätzlichen Anlage mit DIVE-Funktionalität) werden viele Daten zu den bereits installierten Anlagen erfasst. Diese Daten können durch eine Abfrage im MaStR teilweise bereits automatisch bezogen werden, sodass der Aufwand für Anlagenbetreiber gering ist. Falls erforderlich, weil nicht durch das MaStR übertragen, müssen die Werte vom Installateur (oder VNB) geprüft und bestätigt werden. Wenn zudem in einer für alle nutzbaren Datenbank in Form von VCs gespeicherte Informationen zu Anlagen (z. B. Hersteller, Typ und zugehörige Stammdaten) abrufbar sind, entfällt jeglicher Prüfaufwand für diese Daten durch den VNB.

Abbildung 7 zeigt in abstrahierter Form den Vorgang des Onboardings einer Anlage in die DIVE-Basisinfrastruktur. Der Berichtsteil „Technische Details und Umsetzung der Basisinfrastruktur“ geht detailliert auf die Umsetzung des Onboarding-Prozesses für Anlagen ein.

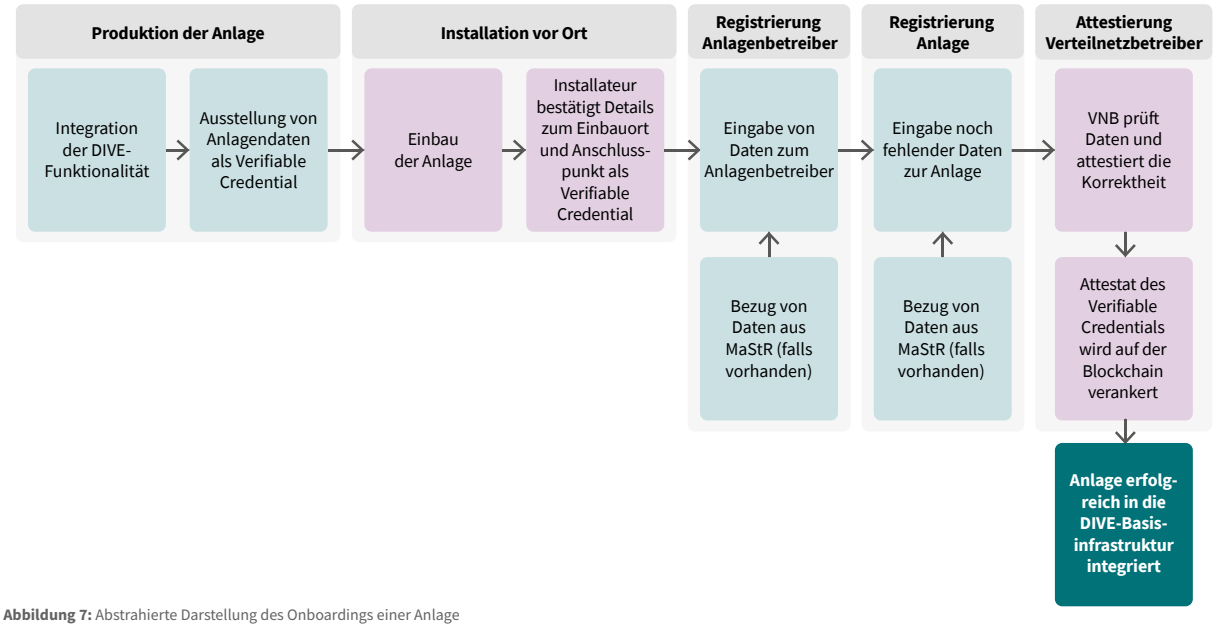

Abbildung 7: Abstrahierte Darstellung des Onboardings einer Anlage

Bei der Installation der Anlage werden sämtliche vom VNB verlangten Daten gemeldet. Hierbei kann auf bereits vom Hersteller ausgestellte VCs zurückgegriffen werden. Der VNB prüft die Daten, die zusätzlich zu denen vom Hersteller geprüft werden müssen, und bestätigt schließlich die Korrektheit aller Angaben, indem er das VC durch seine eigene DID signiert. Die so neu entstandenen und vom VNB bestätigten VCs werden zurück an die Anlage übertragen und dort gespeichert. Die Anlage ist erfolgreich in der DIVE-Basisinfrastruktur angelegt und kann diese Daten nun beliebigen Akteuren vorzeigen, um sich zu authentifizieren und zu registrieren, zum Beispiel im Marktstammdatenregister (MaStR).

Bei einem Retrofit wird ein EMS oder ein zusätzliches Gerät (z. B. Wallbox, Wärmepumpe o. Ä.) nachträglich in den Bestand installiert, das für Bestandsanlagen die DIVE-Funktionalität bereitstellen kann. Im Zuge des Installationsprozesses des EMS (oder eines

Die Anlage verfügt nach erfolgreichem Abschluss der oben skizzierten Prozesse über eine eindeutige DID und erste VCs. Damit kann sie eindeutig identifiziert werden und nachweisen, dass die Stammdaten (in Form von VCs) bereits von anderen Parteien geprüft und bestätigt wurden. Die Daten liegen bei der Anlage (oder im EMS) und können ab jetzt genutzt werden, um die Anlage mit wenig Aufwand bei einem beliebigen Anwendungsfall zu registrieren.

3.2.2 Onboarding von Marktteilnehmern

Beim Onboarding von Anlagen zeigt sich, dass der VNB ebenfalls eine DID benötigt, also Teilnehmer der DIVE-Basisinfrastruktur werden muss, um die VCs von Anlagen verifizieren zu können. Existierende Marktrollen (wie VNB, MSB, Lieferanten etc.) sind bereits Teil der Marktkommunikation und häufig als externe Marktteilnehmer auch Teil der SM-PKI. Da sie dadurch bereits

eindeutig mittels digitaler Zertifikate identifizierbar sind, fußt das Onboarding in die DIVE-Basisinfrastruktur auf diesem Fundament. Der Prozess des Onboardings ist in Abbildung 8 dargestellt und hat folgende Schritte:

- Ein Marktteilnehmer erstellt eine DID.
- Der Marktteilnehmer schickt eine zu definierende Standard-Nachricht mit allen notwendigen Stammdaten via E-Mail über die Marktkommunikation (MaKo) mit Übertragungsweg per AS4 an die Bundesnetzagentur (BNetzA). Anstelle der BNetzA könnten auch andere Akteure für diese Aufgabe in Frage kommen.
- Die BNetzA attestiert automatisch das VC für den Marktteilnehmer und sendet eine Bestätigung via MaKo zurück.
- Der Marktteilnehmer kann sich nun gegenüber allen anderen Marktteilnehmern identifizieren und gegebenenfalls authentifizieren (z. B. in seiner Rolle als VNB die VCs von Anlagen ausstellen).

Basisinfrastruktur stellt sicher, dass das SMGW mit den dahinterliegenden Anlagen auch verknüpft ist. Zu diesem Zweck wird im Rahmen des Onboardings von Anlagen (wenn ein SMGW vorhanden ist) im Auftrag des Verteilnetzbetreibers, der die Anlage zur Registrierung prüft, vom Messstellenbetreiber ein CLS-Kanal zum SMGW aufgebaut. Über diesen Kanal kann geprüft werden, ob die gewünschte Anlage bzw. das EMS auch an der angegebenen Marktlokation erreichbar ist oder nicht. Die Bestätigung dieser Verknüpfung wird im Nachgang durch den MSB als VC an die Anlage übertragen. Abbildung 9 zeigt konzeptionell den Prüfungsvorgang.

Der MSB kann diese Prüfung regelmäßig wiederholen. Auch können Marktakteure, die Teil der SM-PKI sind (z. B. aktive externe Marktteilnehmer), die Anlage fortan via CLS ansteuern und erhalten so auch ohne das Marktlokations-VC die Sicherheit, dass die Messdaten des SMGW auch zu den Stammdaten der Anlage gehören.

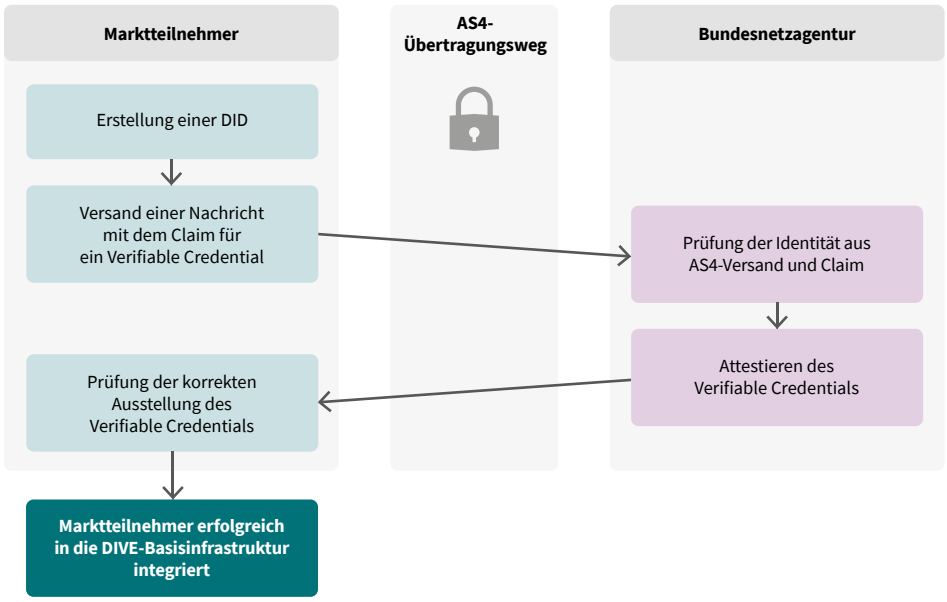

Abbildung 8: Abstrahierte Darstellung des Onboardings eines Marktteilnehmers, beispielsweise eines Verteilnetzbetreibers

Der Vorteil liegt hier darin, dass im Rahmen der MaKo und der SM-PKI bereits eine Authentifizierung existiert. Auch werden dafür bereits Schlüsselpaare sicher gespeichert und für das digitale Signieren von Nachrichten verwendet. Etablierte Marktakteure sind entsprechend bereits mit dieser Funktionalität vertraut, an die die DIVE-Basisinfrastruktur einfach anschließen kann.

3.2.3 Onboarding der Smart-Meter-Infrastruktur

Die Smart-Meter-Infrastruktur ist die aktuell beste Quelle für geeichte und abrechnungsrelevante Messwerte. Die DIVE-

Ein Vorteil, der sich daraus ergibt, ist, dass zum Beispiel im Zuge der Freigabe nach § 49 Abs. 7 MsbG der Letztverbraucher oder Anlagenbetreiber einfach über die Anlage oder das EMS die Freigabe zur Datenübermittlung an einen Energieserviceanbieter (ESA) anstoßen und auch widerrufen kann.

3.2.4 Onboarding von Anlagen bei Anwendungsfällen

Den Betreibern von Anwendungsfällen (z. B. Verteilnetzbetreiber, Übertragungsnetzbetreiber, Lieferanten, Aggregatoren, Energieserviceanbieter u.v.m.) wird es mittels der DIVE-Basisinfrastruktur

und der vorhandenen, verifizierten Daten ermöglicht, den Prozess des Onboardings neuer Anlagen in ihren Anwendungsfall standardisiert, effizient, sicher und mit bereits verifizierten Stammdaten zu implementieren. Dafür müssen sie lediglich die standardisierten DIVE-Onboarding-Prozesse nutzen, die perspektivisch über ein entsprechendes Software Development Kit (SDK)[7] einfach zu integrieren sein werden.

Nutzer können dann über ihre Anlage den gewünschten Anwendungsfall auswählen und sich dort automatisiert registrieren. Dafür müssen sie nur die Allgemeinen Geschäftsbedingungen (AGB) akzeptieren und bestätigen, dass die entsprechenden VC-Daten für die Teilnahme am Anwendungsfall verwendet werden dürfen. Für Nutzer ist dann die Teilnahme an beispielsweise einer Energiegemeinschaft, beim Herkunftsnachweisregister oder nach § 14a EnWG so einfach wie die Installation einer App auf dem Smartphone („User Experience").

Bei einzelnen Anwendungsfällen (z. B. Regelleistung) sind zusätzliche Angaben oder Nachweise erforderlich, die im Standard-Onboarding von Anlagen noch nicht erstellt wurden (z. B. Präqualifikation einer Anlage zur Erbringung von Flexibilität). Betreiber von Anwendungsfällen können entsprechend für das Onboarding noch weitere VCs einfordern, die selbst oder auch von einem anderen Akteur (z. B. Gutachter) attestiert werden sollen. Ein entsprechender Onboarding-Prozess muss dann für die Nutzer bereitgestellt und eventuell mit einer zusätzlichen Anleitung versehen werden. Der Vorteil ist auch hier: Wird beispielsweise durch den Übertragungsnetzbetreiber (ÜNB) eine Präqualifikation ausgestellt, kann der Anlagenbetreiber dieses VC später auch dem VNB zeigen und sich so den gegebenenfalls großen Aufwand für eine neue Präqualifikation gegenüber dem Verteilnetzbetreiber (z. B. im Zuge von § 14c EnWG) sparen.

3.3 Einhaltung von Marktregeln

Ein wichtiges Ziel der mit DIVE entwickelten Basisinfrastruktur ist die Erhöhung der Systemsicherheit, Zuverlässigkeit und Effizienz durch digital überprüfbare Marktregeln. Im Zuge der Registrierung von Anlagen in Anwendungsfällen erfolgt im Hintergrund eine automatische Überprüfung, ob gewisse energiewirtschaftliche Regeln eingehalten werden. Beispielsweise darf eine Erneuerbare-Energien-Anlage die erzeugte Energie nicht mehrfach als

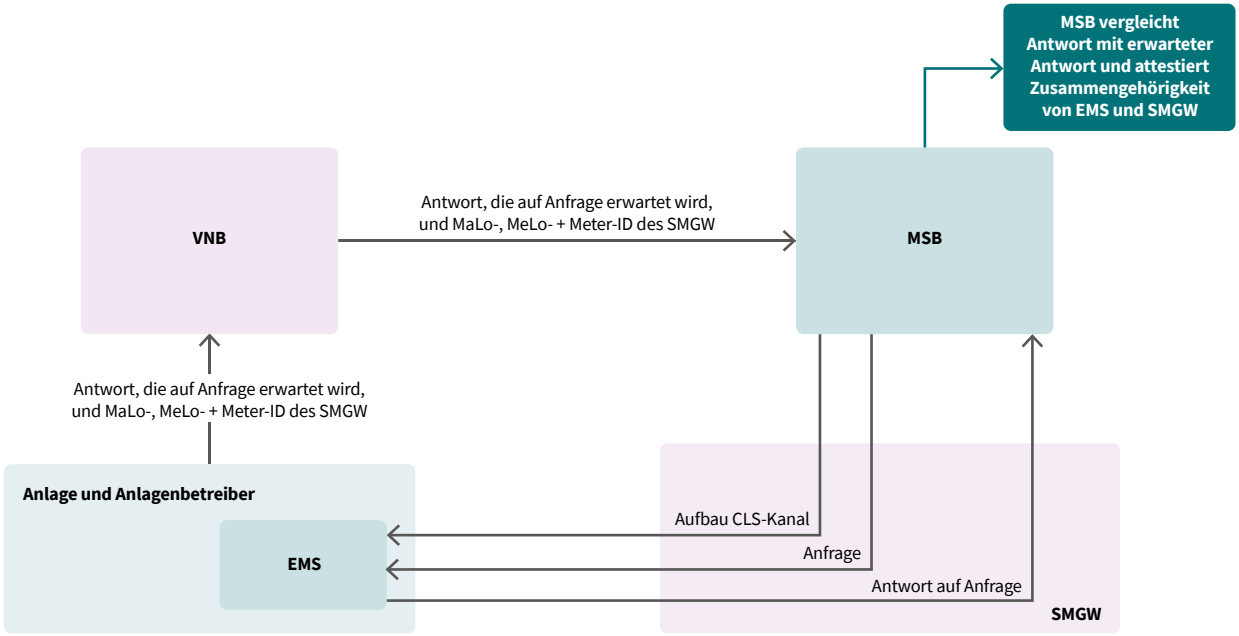

Abbildung 9: Konzeptionelle Darstellung einer Prüfung, ob eine Anlage mit einem SMGW tatsächlich verbunden ist

erneuerbar ausweisen und kann somit nicht an mehreren Labeling-Anwendungsfällen gleichzeitig teilnehmen.

Dazu ist es notwendig, dass sämtliche Anwendungsfälle, die Herkunftsnachweise ausstellen oder eine sonstige Ausweisung von erneuerbar erzeugtem Strom vornehmen, sich gegenseitig in Kenntnis setzen, wenn eine Anlage bereits Teil eines solchen Anwendungsfalls ist. Somit wissen andere Anwendungsfälle, dass eine Anlage nicht an einem weiteren solchen Anwendungsfall teilnehmen darf.

Diese Funktionalität wird sicher und datenschutzkonform von der DIVE-Basisinfrastruktur bereitgestellt. Anwendungsfälle müssen lediglich Anfragen über den Status einer Anlage stellen und neu in die eigenen Anwendungsfälle aufgenommene

7 Im Projekt DIVE wurde unter https://github.com/xyz eine Dokumentation verfasst, die Entwicklern von Anwendungsfällen als Blaupause dafür dienen kann, DIVE-Funktionalitäten in den eigenen Anwendungsfall zu integrieren. Diese Dokumentation ist der erste Schritt hin zu einem Software Development Kit.

Anlagen entsprechend melden. In Kapitel 4.3 wird auf diese Funktionalität zur Einhaltung von Marktregeln anhand eines Beispiels eingegangen. Im Berichtsteil „Technische Details und Umsetzung der Basisinfrastruktur“ werden in Kapitel 4.3 technische Details erläutert.

Das in DIVE umgesetzte Beispiel kann auf beliebige andere Felder mit mehr Kritikalität, bei denen die Einhaltung von Marktregeln notwendig ist, ausgeweitet werden (z. B. die Vermarktung von Flexibilität auf unterschiedlichen Märkten an verschiedene Stakeholder).

3.4 Übertragung von Bewegungsdaten

DIVE möchte mit der Basisinfrastruktur Anwendungsfällen den Zugriff auf verschiedene Messdaten von teilnehmenden Anlagen erleichtern. Im Status quo stehen einerseits bei vorhandenem SMGW abrechnungsrelevante Messdaten einer Anlage zur Verfügung, die über den zuständigen Messstellenbetreiber angefordert werden können. Andererseits benötigen Anwendungsfälle zum Teil nicht abrechnungsrelevante Daten, die das SMGW nicht erfasst, wie beispielsweise Ladezustände von Batterien in Heimspeichern oder Elektrofahrzeugen oder gewünschte Batteriefüllstände, mit denen Anwendungsfälle Mehrwerte für die Teilnehmer generieren können.

Zugriff auf SMGW-Messdaten

Die DIVE-Basisinfrastruktur kann beim Bezug von abrechnungsrelevanten SMGW-Daten dahingehend unterstützen, dass für eine Anlage ein Verifiable Credential mit Informationen zu einem vorhandenen SMGW und dem dafür zuständigen Messstellenbetreiber hinterlegt ist. Damit weiß ein Anwendungsfall, bei wem die Anlage registriert ist und bei welchem MSB angefragt werden muss, um beispielsweise den Universalbestellprozess für Messdaten zu starten. Der Anwendungsfall nimmt dabei die energiewirtschaftliche Rolle des Energieserviceanbieters ein. Um Daten vom Messstellenbetreiber abrufen zu dürfen, benötigt der Anwendungsfall jedoch nach § 49 MsbG eine Legitimation des Anlagenbetreibers. Auch hier kann die DIVE-Basisinfrastruktur einen Mehrwert bieten, indem der Anlagenbetreiber seine Zustimmung als Verifiable Credential ausstellt und dies wiederum vom Anwendungsfall genutzt werden kann, um die Legitimation beim MSB vorzuweisen. Ein manueller Vorgang mit Ausfüllen und Einscannen eines entsprechenden Formulars entfällt hierdurch.

Zugriff auf Anlagen-Messdaten

Das SMGW ist nur für den Bezug von Messdaten am Netzverknüpfungspunkt (und gegebenenfalls an weiteren Messlokationen) geeignet. Es werden jedoch in Zukunft auch viele weitere Bewegungsdaten relevant, die das SMGW nicht erfasst. Für einen Aggregator, der die Flexibilität von Prosumern vermarktet, sind beispielsweise viele Informationen wie Speicherfüllstände von Batteriespeichern, Anzahl zur Ladung angeschlossener Elektrofahrzeuge oder gewünschte Lademengen relevant, um die verfügbare Flexibilität im Pool des Aggregators bestmöglich zu prognostizieren.

Das EMS (oder die Anlage selbst) ist hierbei der Schlüssel für den Datenaustausch. Mit einer vom Anlagenbetreiber per ausgestelltem VC erteilten Erlaubnis, Messdaten zu beziehen, und einem weiteren VC mit Anweisungen für einen Datenabruf ist es dem Anwendungsfall möglich, Messdaten der gewünschten Anlagen abzurufen. Das VC mit Anweisungen für den Datenabruf sollte im besten Fall standardisiert sein und die Endpunkte sowie eine Definition der Schnittstelle, mit der kommuniziert werden soll, angeben. Eine Verbindung zur Anlage kann entweder über einen CLS-Kanal des SMGW erfolgen oder über andere existierende Kommunikationsanbindungen der Anlage.

Das SMGW ist zwar in der Lage, hochaufgelöste Messwerte zu erfassen, die bisher implementierten Systeme zur Umsetzung der Marktkommunikation verhindern jedoch eine Übertragung der Messdaten in Echtzeit (dena 2024). Stattdessen werden sie in der Regel am Folgetag gesammelt und in einer höchsten Auflösung von 15 Minuten als E-Mail versandt. Hier kann das EMS in der DIVE-Basisinfrastruktur eine weitere Aufgabe erfüllen, da es hochaufgelöste Messdaten des SMGW in Echtzeit und digital signiert (gegebenenfalls über den CLS-Kanal) direkt an einen Dritten übermitteln kann. Dies ist zwar nicht für die Abrechnung zulässig, hilft aber zum Beispiel für verbesserte Visualisierungen oder Prognosen.

4. Anwendungsfeld Herkunftsnachweise

Im Projekt DIVE wurde erforscht, wie Anlagen oder Geräte im Energiesystem mit sicheren digitalen Identitäten ausgestattet werden können. Es wurde die vorher beschriebene Basisinfrastruktur prototypisch umgesetzt und anhand verschiedener Anwendungen in den Bereichen feingranulare Herkunftsnachweise, Flexibilitätserbringung von Kleinstanlagen und schnelle Lieferantenmitnahme an Ladesäulen für Elektrofahrzeuge erprobt.

Dieses Kapitel widmet sich dem Anwendungsfeld Herkunftsnachweise (HKN) und der Frage, wie die DIVE-Basisinfrastruktur Mehrwerte für das HKN-System bereitstellen kann. Bei einer möglichen Öffnung des deutschen HKN-Systems für Drittanbieter kann die DIVE-Basisinfrastruktur weitere Funktionalitäten bereitstellen, auf die im Folgenden eingegangen wird.

4.1 Das deutsche Herkunftsnachweis-System

Eine detaillierte Erläuterung zum Status quo der HKN, Kritik am aktuellen System, Weiterentwicklungsmöglichkeiten sowie Zahlen und Fakten sind (Bogensperger 2023a)[8] zu entnehmen.

Was sind Herkunftsnachweise?

HKN sind ein elementarer Bestandteil der Energiewende. Solange der Strommix noch nicht vollständig grün ist, werden sie benötigt, um die grüne Eigenschaft von Strom gegenüber Verbrauchern nachzuweisen. Sie sind die Grundlage für Grünstromprodukte, grünen Wasserstoff, grüne Wärme und nachhaltige Produktion. Sie werden in Energiegemeinschaften benötigt, bilden die Grundlage für die Darstellung der marktbasierten Emissionen von Unternehmen und verschaffen in einer Zeit mit gestiegenem Umweltbewusstsein einen Wettbewerbsvorteil.

Status quo

Um die Stromherkunft heute nachzuweisen, wurde im Jahr 2013 das Herkunftsnachweisregister (HKNR) geschaffen. Wird in einer Erzeugungsanlage Strom aus erneuerbaren Energien produziert, kann durch das HKNR, das vom Umweltbundesamt (UBA) geführt wird, ein Herkunftsnachweis ausgestellt werden. Ein HKN entspricht heute 1 Megawattstunde erzeugtem (grünen) Strom. Ein Anlagenbetreiber kann sich einen HKN ausstellen lassen, sofern er nachweislich 1 Megawattstunde Strom erzeugt und geliefert hat und den Strom per sonstiger Direktvermarktung nach § 21a EEG verkauft. An EEG-geförderte Anlagen dürfen heute keine HKN ausgestellt werden (§ 80 EEG „Doppelvermarktungsverbot“).

Stromlieferanten und Anlagenbetreiber haben Konten beim HKNR, die den Handel mit HKN ermöglichen. Dieser Handel ist unabhängig vom physikalischen Stromfluss. Es gibt für HKN einen eigenen Markt mit eigener Preisbildung, der unabhängig vom Handel mit Strommengen ist. HKN können innerhalb der EU, des europäischen Wirtschaftsraums, der Schweiz und der Energiegemeinschaft (ECS 2023) gehandelt werden. Der Handel erfolgt meist außerbörslich „Over the Counter“ (OTC), direkt oder über Broker (Hauser et al. 2019). Außerdem werden HKN an der europäischen Strombörse EEX (European Energy Exchange) aus dem französischen HKNR in Auktionen gehandelt (EEXG 2022a, EEXG 2022b).

HKN werden durch die Stromlieferanten eingekauft und entwertet. Die Anzahl der entwerteten HKN entspricht der Strommenge der Lieferung eines bestimmten Stromprodukts oder der Belieferung eines bestimmten Kunden. Mit der Entwertung wird der Herkunftsnachweis für gelieferten Strom über einen Bilanzierungszeitraum von einem Kalenderjahr erbracht.

Öffnung des HKN-Systems für Kleinstanlagen und Drittanbieter

Die von der EU geforderte Einführung von Bürger- und Erneuerbare-Energie-Gemeinschaften (RED II (Renewable Energy Directive) und EMD (Elektrizitätsbinnenmarktrichtlinie)) macht es nötig, die Stromherkunft aus kleinen Anlagen nachzuweisen und den Nachweis deutlich zu vereinfachen. Da deshalb auch Kleinstanlagen zukünftig am HKN-System teilnehmen können, muss die Granularität von HKN auf weit unter 1 Megawattstunde abgesenkt und die Prozesse der Teilnahme müssen weniger aufwendig, automatisiert zugänglich und damit günstiger gestaltet werden (Bogensperger 2023b).

Es gibt grob zwei Lösungsansätze, wie das momentane HKN-System verändert werden könnte, um die Teilnahme von Kleinstanlagen zu ermöglichen:

1. Optimierung des vom UBA betriebenen HKNR, wobei die zeitliche und räumliche Auflösung sowie Prozesse und Kosten optimiert werden[9]

2. Öffnung des Herkunftsnachweismarktes für Drittanbieter bzw. Initiativen wie Energy Track & Trace[10], Energy Tag[11] oder Granular Energy[12]. Diese müssten jedoch als freie Alternativen zum HKNR betrieben werden. Dafür wären einheitliche Regeln notwendig.

Die DIVE-Basisinfrastruktur kann für beide Optionen einen Mehrwert liefern. Während dadurch in 1. der Onboarding-Prozess auf wenige „Klicks“ reduziert werden kann, können in 2. die entworfenen Marktregeln überwacht und damit kann die Arbeit des UBA erleichtert werden. Zudem kann eine Doppelvermarktung von Strom aus erneuerbaren Energien unterbunden werden.

4.2 Die Rolle der DIVE-Basisinfrastruktur bei Herkunftsnachweisen

Aufseiten des HKNR könnten durch eine Einführung der DIVE-Basisinfrastruktur die Kosten für Registrierung, Anlagenverwaltung

8 Siehe auch https://www.ffe.de/veroeffentlichungen/zukunftsfaehige-herkunftsnachweise/

9 Ein Vorschlag für „Zukunftsfähige Herkunftsnachweise“: https://www.ffe.de/veroeffentlichungen/zukunftsfaehige-herkunftsnachweise/

10 https://energytrackandtrace.com/

11 https://energytag.org/#top

12 https://www.granular-energy.com/insights/die-lage-von-herkunftsnachweisen-in-deutschland

und gegebenenfalls Prüfprozesse deutlich reduziert werden, da durch attestierte Verifiable Credentials Vertrauen in die Daten gegeben ist. Informationen wie Anschlussnehmer, Typ, Ort der Anlagen, Markt- und Messlokationen, EEG-Förderung usw. sind durch die vorherige Prüfung durch einen VNB bereits bestätigt. Dies könnte insbesondere bei Kleinanlagen das derzeit noch notwendige Postident-Verfahren bei der Registrierung überflüssig machen sowie die hohen Kosten für die Registerführung reduzieren.

Die DIVE-Basisinfrastruktur würde es zudem ermöglichen, private Anbieter von Herkunftsnachweis-Systemen mit im Vergleich zum HKNR erweiterter Funktionalität zuzulassen. Solange deren Systeme die gesetzlichen Vorgaben erfüllen, wäre hier ein freier Markt für verschiedene Anbieter möglich. Die DIVE-Basisinfrastruktur stellt sicher, dass Anlagen nur bei vom Umweltbundesamt zertifizierten Herkunftsnachweis-Plattformen[13] teilnehmen können und sich diese auch an alle gegebenen Regeln halten. Die Zertifizierung kann das UBA selbst als VC ausstellen und jederzeit bei Regelverstößen auch widerrufen.

Die Teilnahme von Anlagen am HKNR kann durch die DIVE-Basisinfrastruktur abgesichert werden. Anlagen können nicht bei mehreren Anbietern gleichzeitig Herkunftsnachweise erstellen lassen oder trotz einer aktiven EEG-Förderung partizipieren. Dies ist technisch ausgeschlossen. Das UBA hat entsprechend keinerlei Aufwand für die Prüfung, ob sich Anlagen oder Anbieter regelwidrig verhalten. Die Einhaltung des Doppelvermarktungsverbots nach § 80 EEG wäre sichergestellt.

Überdies könnten auch noch weitere Regeln eingeführt und ihre Befolgung könnte überprüft werden. Bei der Teilnahme eines Prosumers an einer Energiegemeinschaft könnten automatisch Herkunftsnachweise an den Community Operator übermittelt werden. Oder es wird automatisch ausgeschlossen, dass parallel HKN an andere Lieferanten übertragen werden. Entsprechende Regeln sind noch zu entwerfen, wenn Energiegemeinschaften in Deutschland ausgeweitet werden sollen.

4.3 Umsetzungsbeispiel mit Energy Web Green Proofs

Bei einer möglichen Öffnung des Herkunftsnachweismarktes für Drittanbieter kann neuen Anwendungsfall-Anbietern mit der DIVE-Basisinfrastruktur eine einfache Anbindung an das HKN-System ermöglicht werden. Im Projekt DIVE wurde eine solche Anbindung einer Anlage mit DIVE-Funktionalität an die Labeling-Anwendung *Energy Web Green Proofs* getestet. Green Proofs ermöglicht die Teilnahme von Geräten an Nachhaltigkeitsprogrammen und Zertifikatshandelsoptionen sowie die Zuordnung von Erzeugung und Verbrauch und damit die einhergehende Dokumentation von CO_2-Einsparungen.

Annahmen

Im Folgenden wird davon ausgegangen, dass die Nutzerin „Erna“ ein DIVE-kompatibles Gerät besitzt, das über die technischen Voraussetzungen verfügt, ein Token zur „Verhinderung von Nutzungskonflikten“ und ein Basis-VC mit den zur Registrierung beim Anwendungsfall geforderten Inhalten zu halten, zu aktualisieren und zu präsentieren (siehe Berichtsteil „Technische Details und Umsetzung der Basisinfrastruktur“, Kapitel 4.4). Dies alles ist mit der Registrierung der Anlage, wie in Kapitel 3.2.1 beschrieben, gegeben. Mit diesem Gerät führt Erna die folgenden Schritte aus bzw. diese werden automatisch ausgeführt, um das Gerät bei dem Use Case Energy Web Green Proofs anzumelden:

Prozessablauf

1. Erna erfährt von der Plattform Green Proofs und greift über ihren Webbrowser unter https://gp-dive-dev.energyweb.org/ auf die Website von Green Proofs zu. Dort folgt Erna den Schritten, um Green Proofs mit ihrem DIVE-kompatiblen Gerät, einer Photovoltaik-Anlage, bekannt zu machen. Dazu fügt sie die DID von Green Proofs auf dem Gerät hinzu: did:web:gp-dive-dev.energyweb.org. Daraufhin ruft das Gerät automatisch die Use-Case-Basisdaten ab und stellt Green Proofs in der Liste der bekannten Use Cases als Auswahloption zur Verfügung (siehe Abbildung 10).

Abbildung 10: Screenshot vom Nutzer-Interface zur Anmeldung bei einem Use Case für eine Anlage

13 Die Regeln sind hier noch zu definieren.

2. Nun wählt Erna im lokalen Webinterface der Photovoltaik-Anlage den Use Case Green Proofs aus. Sie liest die AGB sowie die Datenschutzerklärung und stimmt zu. Daraufhin klickt Erna auf den Anmelden-Button im Interface der Photovoltaik-Anlage.

3. Jetzt kontaktiert das Gerät die Anwendung Green Proofs und fährt automatisch mit der Aktualisierung des Konflikt-Tokens fort (siehe Berichtsteil „Technische Details und Umsetzung der Basisinfrastrukturr“, Kapitel 4.4), der eine Einhaltung von gültigen Marktregeln bei der Interaktion mit dem Anwendungsfall sicherstellt (z. B. die Vermeidung von Doppelvermarktung).

4. Green Proofs fordert eine Präsentation des Basis-VC von der Anlage an und stellt sicher, dass alle Voraussetzungen für die Teilnahme des Geräts erfüllt sind: Dazu prüft die Green-Proofs-Plattform zunächst, ob der Konflikt-Token des Geräts auf den richtigen Wert gesetzt wurde, also dass das Gerät somit bei keinem parallelen Use Case angemeldet ist. Im Anschluss prüft Green Proofs den Inhalt des Basis-VC, insbesondere ob der Typ der Anlage stimmt und ob die Anlage EEG-gefördert ist. Auch der technische Endpunkt zur Übertragung der Messdaten wird übermittelt.

5. Nach erfolgreicher Prüfung wird das Gerät angemeldet und darüber in Kenntnis gesetzt. Sollte einer der Tests fehlschlagen, wird das Gerät nicht angemeldet und Erna darüber im Webinterface informiert.

6. Nun erteilt das Gerät der Green-Proofs-Anwendung Zugriff auf die Messdaten und beginnt damit, zeitlich hochaufgelöste Messdaten zu senden. Es erscheint eine Erfolgsmeldung (siehe Abbildung 11).

Zertifikatsausgabe und -nutzung

Die Green-Proofs-Plattform empfängt die von der SMGW-Infrastruktur signierten Messdaten, stellt Zertifikate für die erzeugten Energiemengen aus und ordnet sie dem Konto von Erna zu. Erna, die Gerätebesitzerin, kann die ausgestellten Green-Proofs-Zertifikate an andere Konten senden oder für den eigenen Verbrauch verwenden. Dafür können automatische Algorithmen oder eine manuelle Zuordnung ausgewählt werden.

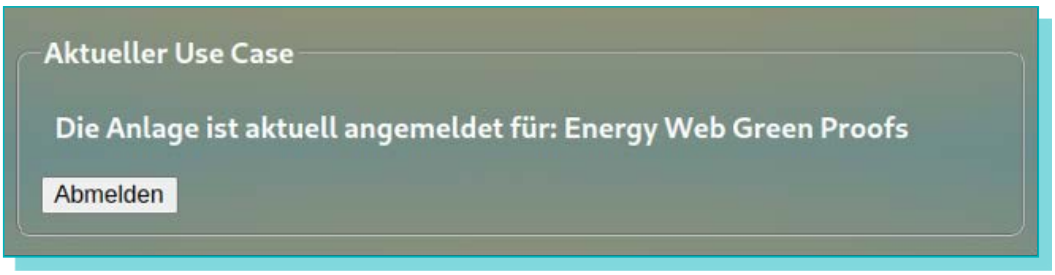

Abbildung 11: Screenshot vom Nutzer-Interface bei erfolgreicher Anmeldung bei einem Use Case für eine Anlage

5. Anwendungsfeld Flexibilitätserbringung

Im vorherigen Anwendungsfeld Herkunftsnachweise wurde demonstriert, wie neben einer erleichterten Registrierung für Anlagenbetreiber auch die Einhaltung von Marktregeln sichergestellt werden kann. Diese Vorteile sind auch im Anwendungsfeld Flexibilitätserbringung gegeben: Die DIVE-Basisinfrastruktur kann verhindern, dass Anlagen mehrfach Flexibilität vermarkten.

Das Projekt DIVE hat sich bei der Demonstration der DIVE-Basisinfrastruktur im Bereich Flexibilität daher auf einen weiteren Aspekt fokussiert, nämlich die Präqualifikation von Anlagen zur Erbringung von Flexibilität. Die Präqualifikation stellt sicher, dass Anlagen „die zur Gewährleistung der Versorgungssicherheit erforderlichen Anforderungen für die Erbringung einer oder mehrerer Arten von Regelreserve erfüllen“ (ÜNB 2024).

Der Nachweis einer Präqualifikation wurde im Projekt demonstrativ als ein weiteres, von einem Übertragungsnetzbetreiber attestiertes Verifiable Credential für die Anlage ausgestellt, das der Anlagenbetreiber wiederum bei der Anmeldung zu einem Flexibilitäts-Anwendungsfall vorlegen musste. In diesem Kontext wurde mit dem sektorenübergreifenden Forschungsprojekt BANULA[14] zusammengearbeitet.

5.1 Status quo

Die Stromproduktion in Deutschland wird vermehrt durch Erneuerbare-Energien-Anlagen auf der Basis von Sonnen- und Windenergie geleistet, die starken wetterbedingten Fluktuationen in der Produktion unterworfen sind. Durch den starken Zubau von Windkraftanlagen vor allem im Norden Deutschlands ist ein tendenziell starkes Nord-Süd-Gefälle in der Produktion vorhanden, was einen Bedarf für den Transport von Strom in Richtung Süden hervorruft. Des Weiteren führt eine zunehmende Sektorenkopplung durch den vermehrten Einbau von Wärmepumpen und die Nutzung von Elektrofahrzeugen zu einem deutschlandweit steigenden Strombedarf.

Die Übertragungs- und Verteilnetze stoßen stellenweise an ihre Grenzen, da sie für die veränderte Erzeugung und Last nicht ausgelegt sind. Der Ausbau des Netzes ist zwar im Gange, dauert jedoch lange und ist mit hohen Kosten verbunden. Gezielte Flexibilitätsmaßnahmen können den notwendigen Netzausbau reduzieren und damit die Investitionen für eine erfolgreiche Energiewende senken.

Kleinstanlagen besitzen oftmals ein Flexibilitätspotenzial bei ihrem Stromverbrauchsverhalten und können kumuliert einen signifikanten Beitrag zur Entlastung der Netze leisten (Körner 2024). Jedoch ist die Koordination einer großen Anzahl an Kleinstanlagen zur Erbringung von signifikanten Mengen an Flexibilität, die an Märkten angeboten werden kann, sehr aufwendig. Außerdem sind im momentanen System für Kleinstanlagen keine marktbasierten Anreize vorhanden, Flexibilität anzubieten: Redispatch 1.0 und Redispatch 2.0 decken eine Teilnahme von Anlagen mit geringer Leistung nicht ab. Die genaue Form der Umsetzung eines Redispatch 3.0, der auch Anlagen mit kleiner Leistung umfasst, ist aktuell noch nicht fixiert. Eine große Herausforderung ist die digitale und sichere Einbindung von Kleinstanlagen in gemeinsame Flexibilitätspools, in denen die Flexibilitäten der Kleinstanlagen aggregiert angeboten werden können. Des Weiteren ist der Prozess zur Präqualifikation von Anlagen zur Flexibilitätserbringung aufwendig und nicht digitalisiert. Für den Einsatz einer großen Menge an Kleinstanlagen ist dieser Prozess nicht skalierbar.

Ein Lösungsansatz ist der Einsatz von Flexibilitäts-Aggregatoren, die eine Flotte an Kleinstanlagen koordinieren und damit gebündelt Flexibilität bereitstellen können. Die Forschungsprojekte BANULA und DEER[15] untersuchen die Umsetzbarkeit einer Lösung mittels Aggregatoren.

5.2 Die Rolle der DIVE-Basisinfrastruktur bei der Flexibilitätserbringung

Die Verwaltung einer großen Flotte an Anlagen für die Aggregation von Flexibilität geht mit einem hohen Aufwand einher. Anlagen müssen vertrauensvoll registriert und verwaltet, Messdaten und Steuerbefehle vertrauensvoll und zuverlässig zwischen Anlagen und Aggregator ausgetauscht werden können.

Die DIVE-Basisinfrastruktur kann an dieser Stelle bei der Umsetzung von Anwendungsfällen unterstützen, vor allem bei der Anlagenregistrierung und -verwaltung, dem erleichterten Zugriff auf Messdaten sowie der Unterbindung einer Doppelvermarktung (von Flexibilität), wie bereits in den vorherigen Kapiteln gezeigt.

Flexibilitäts-Aggregatoren müssen gegenüber dem Übertragungsnetzbetreiber (ÜNB) glaubhaft beweisen können, dass sie die eingesammelten Flexibilitäten, die sie anbieten, tatsächlich abrufen können und dass die Energie durch präqualifizierte Anlagen erzeugt worden ist. Hierbei können die Präqualifikations-Credentials, die die Anlagen bei der Registrierung beim Anwendungsfall vorzeigen müssen, helfen: Nachweise der Präqualifikation werden von ÜNBs ausgestellt oder von Akteuren, denen die ÜNBs vertrauen. Durch das Vorzeigen dieser Credentials ist ein transparenter Beweis einer funktionierenden Flexibilitätserbringung möglich, da eingesehen werden kann, welche Akteure die Präqualifikation der einzelnen Anlagen attestiert haben. Nach der Erbringung der Regelenergie werden Nachweise erbracht, durch welche Anlagen sie erfolgt ist. Es kann ebenfalls nachgewiesen werden, dass diese Anlagen präqualifiziert waren. Weiterhin haben Aggregatoren die Möglichkeit, die bestehende Qualifikation zu prüfen, bevor die Anlagen in den Pool der Anlagen zur Leistungserbringung aufgenommen werden.

14 **BA**rrierefreie und **N**utzerfreundliche **LA**demöglichkeiten schaffen, https://banula.de/

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

5.3 Umsetzungsbeispiel im Projekt BANULA

Während der Projektlaufzeit war das Projektteam von DIVE im Austausch mit den Forschungsprojekten BANULA und DEER, die die Erbringung von Flexibilität aus Kleinstanlagen erforschen. Die DIVE-Basisinfrastruktur kann potenziell in diesen Projekten Mehrwerte liefern, um die Registrierung von Anlagen zu vereinfachen und das Management der verwendeten Assets zu betreiben.

Im Projekt BANULA wurde die DIVE-Basisinfrastruktur erfolgreich genutzt, um die Registrierung von Anlagen bei ihrer Anwendung zur Flexibilitätserbringung durchzuführen. Aufbauend auf der in DIVE umgesetzten Demonstration aus dem Anwendungsfeld Herkunftsnachweise wurde im Projekt BANULA ein weiteres Verifiable Credential neben dem Basis-Credential eingeführt, das den Nachweis einer Präqualifikation beinhaltet. In Anlehnung an bestehende Prozesse wird das Credential für die Präqualifikation vom Übertragungsnetzbetreiber ausgestellt und kann damit als Nachweis auch bei anderen ÜNBs akzeptiert werden.

Dieses in Abbildung 12 dargestellte Verifiable Credential mit dem Nachweis der Präqualifikation wird gemeinsam mit dem Basis-Credential bei der Registrierung zur Flexibilitätserbringung vom Anwendungsfall eingefordert. Die Anwendungsfälle können die vorgezeigten Credentials der Anlagen verwenden.

Die Vorteile einer DIVE-basierten Nachweisstruktur für die Präqualifikation ergeben sich für BANULA wie folgt:

- Für BANULA stehen DIVE-Softwarekomponenten für die Integration zur Verfügung, die die relevanten Schritte abbilden können.
- Der Schritt der Präqualifikation muss in einem dynamischen Energiesystem in bestimmten Zeitabschnitten wiederholt werden – diese Iterationen sind mit digitalen Nachweisen leichter und kosteneffizienter abzubilden.
- Aggregatoren, die im Auftrag der Eigentümer und Betreiber der Anlagen die Regelenergie anbieten, können über digitale Nachweise auf die bestehende Historie der akzeptierten Verifiable Credentials zurückgreifen und eventuellen Zweifeln vorbeugen.
- Die Präqualifikation durch den Übertragungsnetzbetreiber für baugleiche Anlagen kann automatisiert erfolgen, was diesen Prozess deutlich verschlankt.

Abbildung 12: Präqualifikation durch den Übertragungsnetzbetreiber (Transmission System Operator, TSO) über ein Verifiable Credential im Projekt DIVE für BANULA

6. Anwendungsfeld Freiheit bei der Wahl des Stromlieferanten an Ladesäulen

Im Bereich der Elektromobilität entsteht durch bewegliche Verbraucher, die sich an verschiedenen Ladesäulen anmelden, ein sich stets änderndes Umfeld von Stromabnehmern im öffentlichen Raum. Die DIVE-Basisinfrastruktur kann hier den Mehrwert liefern, die Stromversorgung durch die jeweils von den Fahrerinnen und Fahrern oder Fahrzeughalterinnen und -haltern gewünschten Lieferanten dynamisch zu gestalten, sodass für Elektromobilitätskunden eine freie Wahl des Stromlieferanten an öffentlichen und halböffentlichen Ladesäulen ermöglicht werden kann.

6.1 Status quo

Heute haben die Besitzerinnen und Besitzer von Elektrofahrzeugen keine Freiheit bei der Wahl ihres Energieversorgers oder der Herkunft des von ihnen verbrauchten Stroms. Stattdessen wählen die Betreiber der Ladestationen die Energieversorger aus, mit denen die Elektrofahrzeugbesitzerinnen und -besitzer dann zusammenarbeiten müssen. Eine Möglichkeit, um Elektromobilitätskunden die Wahl eines Stromlieferanten anzubieten, ist die Mitnahme des eigenen Stromlieferanten an die Ladesäule. Damit wird das Elektrofahrzeug während des Zeitraums, in dem es an einer Ladesäule angeschlossen ist, vom eigenen ausgewählten Lieferanten versorgt.

Die größte Herausforderung des Lieferantenwechsels an öffentlichen Ladesäulen besteht darin, allen beteiligten Parteien vertrauenswürdige und verifizierte Informationen zur Verfügung zu stellen. Die Datenquellen im Zusammenhang mit einem Ladevorgang lassen sich in drei Bereiche clustern: Benutzer, Mobilität und Energiesektor. In der Praxis sind alle drei Bereiche bisher in Sparten organisiert und der Datenaustausch ist bislang nicht standardisiert.

Die Option, an öffentlichen Ladesäulen den eigenen Stromlieferanten zu wählen, revolutioniert die Elektromobilität. Diese neue Flexibilität würde eine Vielzahl von Möglichkeiten eröffnen und sowohl für Unternehmen als auch für Privatpersonen zahlreiche Vorteile bieten.

Unternehmen profitieren von der Möglichkeit, individuelle Stromverträge für ihre Flotten abzuschließen und somit günstigere Tarife oder spezielle Konditionen nutzen zu können. Die transparente Zuordnung der Ladevorgänge zu einzelnen Fahrzeugen oder Kostenstellen ermöglicht eine genaue Kostenverfolgung und erleichtert die Umsetzung von Nachhaltigkeitsstrategien. Zudem können Unternehmen sicherstellen, dass der Strom für ihre Flotte aus erneuerbaren Quellen stammt. Die Grünstrom-Herkunftsnachweise für jeden Ladevorgang werden direkt vom Stromanbieter des Fahrzeughalters bereitgestellt.

Für **Privatpersonen** vereinfacht die Wahlfreiheit die Abrechnung der Ladekosten, insbesondere wenn das Elektrofahrzeug am Arbeitsplatz geladen wird. Durch den Vergleich verschiedener Stromtarife können Verbraucherinnen und Verbraucher den für sie günstigsten Anbieter auswählen und somit ihre Stromkosten senken.

Auch für die **Betreiber** öffentlicher Ladeinfrastruktur ergeben sich neue Geschäftsmodelle. Hotels, Supermärkte und andere Unternehmen können sich auf den Betrieb der Ladeinfrastruktur konzentrieren und den Strom über die Kundenverträge abrechnen. Dies erhöht die Attraktivität ihrer Standorte und kann zu einer Steigerung der Kundenfrequenz führen.

Für den **gesamten Markt** führt die Wahlfreiheit zu mehr Wettbewerb unter den Stromanbietern und fördert Innovationen im Bereich der Ladeinfrastruktur. Durch den Wettbewerb sinken die Preise für Ladevorgänge an öffentlichen Ladepunkten, was die Elektromobilität für noch mehr Menschen attraktiv macht. Zudem trägt die Wahlfreiheit dazu bei, die Akzeptanz der Elektromobilität zu erhöhen, da sie die Nutzung von Elektrofahrzeugen flexibler und kostengünstiger gestaltet.

Das Durchleitungsmodell, bei dem die Fahrerinnen und Fahrer von E-Autos ihren eigenen Stromtarif an öffentlichen Ladepunkten nutzen können, sollte daher nicht nur für kommerzielle Fahrzeuge wie E-Lkws, sondern auch für private E-Pkws flächendeckend eingeführt werden.

6.2 Umsetzungsbeispiel im Projekt ReBeam

Um diese Vielzahl von Anwendungsfällen zu ermöglichen, haben die Elia Group, die Energy Web Foundation und weitere Partner bereits im Jahr 2022 das ReBeam-Projekt erprobt. ReBeam ermöglicht es den Besitzerinnen und Besitzern von Elektrofahrzeugen, den benötigten Strom von dem von ihnen bevorzugten Energieversorger an privaten, halböffentlichen und öffentlichen Ladestationen zu beziehen. Das Projekt setzt dabei die gleichen Technologien wie die DIVE-Basisinfrastruktur ein: Self-Sovereign Identities (SSI), ergänzt um eine virtuelle Bilanzierungszone (VBA), um Vertrauen zwischen den Beteiligten zu schaffen und den Datenaustausch zu vereinfachen.

Das Herzstück von ReBeam sind digitale Identitäten. Jedes Fahrzeug, jede Ladesäule und jeder Energieversorger erhält durch eine entsprechende Software eine digitale Identität (SSI) – allerdings noch ohne Hardwaresicherheit und signierte Messdaten. Diese SSI dienen als digitaler Ausweis und ermöglichen eine sichere und transparente Kommunikation zwischen allen Beteiligten. Nachdem der Fahrzeughalter einen Stromliefervertrag bei einem Stromanbieter abgeschlossen hat, wird der Vertrag als Verifiable Credential in der SSI-Wallet des Fahrzeugs oder des Fahrzeughalters hinterlegt.

Wird das Elektroauto an eine Ladesäule angeschlossen und von der Fahrerin oder dem Fahrer freigegeben, findet eine automatische Kommunikation statt: Der Vertrag wird dem Ladesäulenanbieter digital verifizierbar präsentiert, der nach erfolgreicher Überprüfung des Credentials die Ladesäule freischaltet.

Daraufhin erfasst das Smart Meter der Ladesäule den Energieverbrauch in Echtzeit und übermittelt diese Daten an den Messstellenbetreiber. Von dort finden die signierten Messdaten sowie Informationen über den zugehörigen Lieferanten samt Mess- und Marktlokation ihren Weg zum Betreiber der virtuellen Bilanzierungszone. Mithilfe der digitalen Identitäten wird jeder Ladevorgang eindeutig einem bestimmten Kunden und Energieversorger zugeordnet.

Eine VBA sorgt dafür, dass die Energiemengen korrekt und transparent abgerechnet werden, und trägt zur Stabilität des Stromnetzes bei.

Die Rolle der DIVE-Basisinfrastruktur

In einem erfolgreichen Beispiel für Synergieeffekte zwischen Projekten konnte der im Projekt ReBeam identifizierte fehlende Baustein – vertrauenswürdige, signierte Messdaten, die den Ladevorgängen und dem Energielieferanten, der für den Ladevorgang am Fahrzeug zuständig sein soll, automatisch zugeordnet werden können – jetzt durch das DIVE-Projekt bereitgestellt werden. Im DIVE-Projekt wurden eindeutige, interoperable und skalierbare Maschinen-Identitäten von Ladepunkten hinter dem Smart Meter entwickelt und erprobt. Zusammen mit einer Fahrzeugidentität lassen sich dadurch Energiewirtschaft und Mobilitätssektor koppeln.

Dazu wird die Ladesäule von ihrem Betreiber gemäß dem DIVE-Protokoll am Use Case ReBeam angemeldet. Ist das Fahrzeug oder dessen Halterin bzw. Halter mit einem Stromvertrag und einem entsprechenden VC ausgestattet, kann das Credential verwendet werden, um den Stromvertrag digital nachzuweisen und den Ladevorgang zu starten.

Darüber hinaus erhalten Stromanbieter wertvolle Einblicke in das Verhalten der Stromverbraucher und können so Elektrofahrzeuge genauer bilanzieren, was zu geringeren individuellen und volkswirtschaftlichen Kosten führt. Die Mitnahme bzw. freie Wahl des Stromlieferanten an Ladesäulen für Elektrofahrzeuge profitiert dabei von der DIVE-Basisinfrastruktur und der dahinterliegenden SMGW-Infrastruktur.

Fazit und Ausblick

Die Energiewende ist ohne eine sichere und kostengünstige Digitalisierung nicht realisierbar. Smart Meter stellen einen ersten wichtigen Baustein der digitalen Infrastruktur dar. Das Projekt DIVE zeigt, dass viele Prozesse in der Energiewirtschaft jedoch noch nicht auf die Integration von Millionen dezentraler Erzeuger, Verbraucher und Stakeholder ausgelegt sind. Es ist essenziell, dass die Infrastruktur für den Datenaustausch an die sich verändernden Rahmenbedingungen angepasst und den Anforderungen aller Stakeholder Rechnung getragen wird.

Dies beginnt bei vertrauenswürdigen Stamm- und Bewegungsdaten und führt bis zur automatisierten Gewährleistung der Einhaltung von Marktregeln. Ohne adäquate digitale Infrastruktur und Daten-Governance kommt es zu hohen Transaktionskosten zwischen allen Marktakteuren und unnötigem Kommunikationsaufwand und der Markteintritt für neue Dienstleister, Prosumer usw. wird erschwert. Werden Marktregeln nicht eingehalten, führt dies zu marktwirtschaftlichen Ineffizienzen wie der Doppelvermarktung von Herkunftsnachweisen und im schlimmsten Fall zur Beeinträchtigung der Systemstabilität, zum Beispiel durch die Doppelvermarktung von Flexibilität.

Die im Projekt entwickelte DIVE-Basisinfrastruktur liefert einen relevanten Beitrag zu einem digitalen Energiesystem: eine Ende-zu-Ende-Digitalisierung von der Messdatenerfassung bis hin zu verschiedensten Anwendungsfällen, dem Identitätsmanagement und der Stammdatenverwaltung. Dadurch können Prozesse automatisiert und die Einstiegshürden für Kunden und Anbieter reduziert werden. DIVE erlaubt es Nutzern, ihre Anlagen einfach und schnell zu registrieren. Dabei wird eine digitale Identität – eine systemübergreifend eindeutige ID – erstellt und es werden digitale Stammdaten zur Anlage, zum Standort und zum Betreiber bzw. Nutzer im Rahmen einer Registrierung angelegt. Diese werden im Anschluss durch berechtigte, vertrauenswürdige Marktpartner wie beispielsweise durch den Verteilnetzbetreiber oder durch den Hersteller der Anlage auf ihre Richtigkeit geprüft. Ein ähnlicher Prozess ist bereits heute durch das Marktstammdatenregister etabliert, er wird jedoch um einige Funktionalitäten erweitert.

Sind die Daten einmal geprüft, liegen sie digital auf der Anlage oder einem Energiemanagementsystem vor und machen damit die Anmeldung bei energiewirtschaftlichen Dienstleistungen mit wenigen Klicks möglich. Es wird sichergestellt, dass alle Daten einheitlich sind, alle Marktakteure über die gleichen Informationen zur Anlage verfügen, diese ein hohes Maß an Vertrauenswürdigkeit mit sich bringen und alle über dieselbe Anlage sprechen, sollte es zu einem Austausch kommen.

Ferner ermöglicht es die DIVE-Basisinfrastruktur, übergeordnete Marktregeln zu prüfen und ihre Einhaltung sicherzustellen. Regeln beinhalten zum Beispiel das Verbot der Teilnahme am Herkunftsnachweis-System oder an lokalen Strommärkten, wenn eine Erneuerbare-Energien-Anlage eine EEG-Förderung erhält. Es wird auch ausgeschlossen, dass ein Verbraucher zur selben Zeit bei mehreren Lieferanten einen Vertrag hat oder die gleiche Flexibilität an den Verteil- und den Übertragungsnetzbetreiber sowie an ein virtuelles Kraftwerk zur Vermarktung der Flexibilität auf dem Intraday- oder Day-Ahead-Markt absichtlich oder unwissentlich mehrfach verkauft wird. Dies erfolgt vollautomatisch im Hintergrund und stellt somit die Stabilität auch im dezentralen Energiesystem sicher.

Die DIVE-Basisinfrastruktur bietet auch das Potenzial, Millionen dezentraler Anlagen in Anwendungsfälle für Unternehmen deutlich vereinfacht einzubinden. So ist kein individueller Anmeldeprozess mit Datenerfassung mehr nötig. Die bei der Registrierung übermittelten Daten weisen ein hohes Maß an Vertrauenswürdigkeit auf, der Datenaustausch ist standardisiert und viele Standardfunktionalitäten müssen nicht neu entwickelt werden, da sie bereits vorliegen und direkt genutzt werden können. Dies senkt die Markteintrittshürde für Unternehmen und ihre Kunden.

Ein weiterer Vorteil besteht darin, dass, wenn beispielsweise ein Gutachter eine Anlage inspiziert (vgl. Herkunftsnachweise) oder im Rahmen eines neuen Anwendungsfalls zusätzliche Eigenschaften einer Anlage geprüft werden müssen (z. B. Präqualifikation für Regelleistung), diese Daten auch in anderen Anwendungen bei anderen Marktakteuren wiederverwendet werden können. Im Laufe der Zeit steigt somit das Vertrauen in die Daten, die dahinterliegenden Anlagen und ihre Funktionalitäten – über alle Ebenen des energiewirtschaftlichen Kreislaufs hinweg. Dabei bleiben die eigentlichen Rohdaten immer lokal bei den Geräten der Anlagenbetreiber und aufgrund der Selbstverwaltung durch Self-Sovereign Identities wird ein hohes Niveau beim Datenschutz gewährleistet. Es entstehen keine zentralen Plattformen mit zu viel Marktmacht, kein „Single Point of Failure“ und kein Daten-„Honeypot“.

Zusammenfassend kann die DIVE-Basisinfrastruktur eine einfache, sichere und kosteneffiziente digitale Integration von Millionen neuer und bestehender Anlagen ins Energiesystem ermöglichen. Dafür wurden Konzepte entwickelt, entlang der realweltlichen energiewirtschaftlichen Prozesse geprüft und umgesetzt und in Praxispiloten Ende-zu-Ende demonstriert und getestet.

Gleichzeitig konnte DIVE nicht alle Fragen vollständig klären. Diese gilt es nun zeitnah anzugehen und mit weiterer Forschung

und Erprobung im Feld zu lösen. Wir haben dazu eine Reihe verschiedener Handlungsempfehlungen ausgearbeitet, die in Kapitel 6 des Berichtsteils „Überblick, Einordnung und Evaluation“ zu lesen sind. Sie beinhalten Empfehlungen zur Nutzung digitaler Maschinen-Identitäten als Baustein der europäischen Datenstrategie, zur Konkretisierung eines Trust-Frameworks, zum Abbau regulatorischer Unsicherheiten und zur Modernisierung bestehender Prozesse und Infrastrukturen in der Energiewirtschaft.

So wäre beispielsweise zu klären, inwiefern die im Rahmen von DIVE entwickelte und vorgeschlagene Funktionalität über das Smart Meter Gateway bzw. den CLS-Kommunikationsadapter abbildbar ist. Dieser beinhaltet bereits viele Funktionalitäten, beispielsweise die sichere Speicherung von Schlüsseln in einem Hardware Secure Module (HSM). Auch ist es dringend erforderlich – unabhängig von DIVE –, die Marktkommunikation zu reformieren. Auch sind Fragen zur Governance und zur Standardisierung zu klären. Des Weiteren ist die Verknüpfung von digitalen Identitäten und dem digitalen Produktpass offen. Ein wichtiger Punkt ist zudem die Entwicklung von im zunehmend komplexen Umfeld notwendigen Marktregeln. Auch sollte eine Überarbeitung des Marktstammdatenregisters in den Blick genommen werden. Während es bereits einen kleinen Teil der in DIVE identifizierten Funktionalitäten abdeckt, wäre es auch denkbar, übergangsweise die Funktionalität des MaStR zu erweitern, bis die Standardisierung und Etablierung von digitalen Identitäten stattgefunden haben.

Abschließend lässt sich festhalten, dass digitale Identitäten, wie sie in DIVE entwickelt und praktisch erprobt wurden, ein enormes Potenzial für eine sichere und kosteneffiziente Digitalisierung des Energiesektors aufweisen. Die im Projekt identifizierten Funktionalitäten sollten fester Bestandteil der Weiterentwicklung des digitalen Energiesystems sein.

Projektkonsortium

Die **dena** ist eine Projektgesellschaft und ein öffentliches Unternehmen. Sie vereint vielfältige Kompetenzen in allen relevanten Themenfeldern für Energiewende und Klimaschutz. Eckpfeiler ihrer Struktur sind fünf Fachbereiche, zwei Querschnittsbereiche und zwei Stabsstellen. Die Teams arbeiten kontinuierlich in rund 100 laufenden Projekten weltweit.

Die **FfE** (Forschungsstelle für Energiewirtschaft) bearbeitet unabhängig und energieträgerneutral relevante energietechnische und energiewirtschaftliche Themen. Die Forschungsergebnisse basieren auf wissenschaftlich fundierten Analysemethoden mit technischen, ökonomischen, ökologischen und gesellschaftlichen Kriterien. Die Neutralität der Arbeit wird durch die inhaltliche Breite der Projekte und die Diversität der Projektpartner gewährleistet.

Das Blockchain-Labor des **Institutsteils Wirtschaftsinformatik des Fraunhofer FIT** (Fraunhofer-Institut für Angewandte Informationstechnik) ist unter anderem im Bereich Energie und Energiewirtschaft auf die Erforschung und Anwendung emergenter Technologien wie Self-Sovereign Identities, Data Spaces und Blockchains spezialisiert. Durch Forschungs- und Praxisprojekte im Kontext der Energiewende hat das Forschungsinstitut tiefgreifendes Know-how zu den Anforderungen, Potenzialen und Herausforderungen des Einsatzes vorgenannter Technologien zur Digitalisierung des Energiesystems erlangt.

Die **OLI Systems GmbH** mit Sitz in Stuttgart entwickelt und vertreibt dezentrale Hard- und Softwarelösungen für Gewerbe- und Privatkunden sowie für Energieversorger. Seit 2017 entwickelt die OLI Systems GmbH Blockchain-basierte Pilotanwendungen im Bereich Flexibilität und lokale Energiemärkte für Kunden wie beispielsweise Technische Werke Ludwigshafen, Allgäuer Überlandwerk, e-regio, BOSCH, Technische Universität München oder WIRCON. Seit 2022 ist das Smart-Charging-Produkt „OLI Move“ für Privat- und Gewerbekunden am Markt. Die OLI Systems GmbH ist auch an Normungsaktivitäten im Bereich Smart Charging, digitaler Netzanschluss und Distributed-Ledger-Technologie bei der DKE (Deutsche Kommission Elektrotechnik Elektronik Informationstechnik) beteiligt.

Die **BOTLabs GmbH** ist der Erfinder und initiale Entwickler des KILT Protocol, einer dezentralen Identitäts-Blockchain als Infrastruktur zur Erzeugung von Decentralized Identifiers (DIDs) und Verifiable Credentials (VCs). BOTLabs wurde 2018 in Berlin gegründet und entwickelt Software und Dienstleistungen „built on KILT“, darunter SocialKYC, DIDsign, web3name, Stakeboard und Account Linking. Darüber hinaus hat die BOTLabs-Tochter B.T.E. BOTLabs Trusted Entity die Sporran-Wallet, den Checkout-Service und den Enterprise-Service von KILT entwickelt. BOTLabs ist ein Gründungsmitglied der International Association for Trusted Blockchain Applications (INATBA) und ein Mitglied der Decentralized Identity Foundation (DIF).

Die **Energy Web AG** verfolgt die Mission, ein dezentrales digitales Betriebssystem für den Energiesektor zu entwickeln und einzusetzen, um die Energiewende zu beschleunigen. Dazu werden die Entwicklung und Bereitstellung der Open-Source-Technologie-Plattform EW-DOS vorangetrieben. Der Fokus liegt dabei auf den drei Bereichen Asset Management, Data Exchange und Green Proofs. Energy Web ist international aktiv und zählt einige der größten Energieunternehmen der Welt zu seinen über 50 Mitgliedern. Gemeinsam betreiben sie die Energy Web Chain.

Fieldfisher ist eine europäische Wirtschaftskanzlei mit marktführender Praxis in vielen der dynamischsten Sektoren. Das zukunftsorientierte Unternehmen legt einen besonderen Fokus auf die Bereiche Energie und natürliche Ressourcen, Technologie, Finanzen und Finanzdienstleistungen sowie Life Sciences und Medien. Das Unternehmen umfasst mehr als 1.700 Mitarbeiterinnen und Mitarbeiter an 25 Standorten in Amsterdam, Barcelona, Belfast, Berlin, Birmingham, Bologna, Brüssel, Dublin, Düsseldorf, Frankfurt, Guangzhou, Hamburg, London, Luxemburg, Madrid, Mailand, Manchester, München, Paris, Peking, Rom, Shanghai, Turin, Venedig und Silicon Valley.

Assoziierte Partner

- 50Hertz Transmission GmbH
- CHARGING RADAR
- EnBW Energie Baden-Württemberg AG
- Numbat
- SMA, Equigy, TransnetBW GmbH, THU
- TenneT TSO

Abbildungsverzeichnis

Literaturverzeichnis

BNetzA (2024): Positionspapier zu energiewirtschaftlich relevanten Mess- und Steuerungsvorgängen nach § 19 Absatz 2 MsbG. Bonn: Bundesnetzagentur (BNetzA) Beschlusskammer 6, 2024.

Bogensperger, Alexander (2023a): Zukunftsfähige Herkunftsnachweise – Kurzfassung. München: Forschungsstelle für Energiewirtschaft e. V. (FfE), 2023.

Bogensperger, Alexander (2023b): Zukunftsfähige Herkunftsnachweise – Roadmap zur Weiterentwicklung. München: Forschungsstelle für Energiewirtschaft e. V. (FfE), 2023.

dena (2024): Regulatorische Vorgaben für externe Marktteilnehmer (EMT). Status quo der Anforderungen für die Kommunikation mit intelligenten Messsystemen und die Nutzung der Smart Meter Gateway Infrastruktur in Deutschland. Hrsg. v. Deutsche Energie-Agentur GmbH.

ECS (2023): Energy Community Homepage. Wien: Energy Community Secretariat, 2023. Online verfügbar unter https://www.energy-community.org. Abgerufen am 06.03.2023.

EEXG (2022a): EPEX SPOT SE: First pan-European GOs spot auction to take place in September 2022 – Press Release. Paris, Leipzig: EPEX SPOT SE, 2022.

EEXG (2022b): EEX Group: Successful start of pan-European spot market for Guarantees of Origin – Press Release. Leipzig: EEX Group, 2022.

Hauser, Eva et al. (2019): Marktanalyse Ökostrom II – Marktanalyse Ökostrom und HKN, Weiterentwicklung des Herkunftsnachweissystems und der Stromkennzeichnung. Saarbrücken: IZES gGmbH, 2019.

Körner, Marc-Fabian et al. (2024): A digital Infrastructure for Integrating Decentralized Assets into Redispatch. In: Bayreuther Arbeitspapiere zur Wirtschaftsinformatik. Bayreuth. DOI: 10.15495/EPub_UBT_0000769.

ÜNB (2024): Wie werde ich Regelenergieanbieter? (Präqualifikation). Berlin/Pulheim/Bayreuth/Stuttgart: 50Hertz Transmission GmbH, Amprion GmbH, TenneT TSO GmbH, TransnetBW GmbH, 2024. Online verfügbar unter https://www.regelleistung.net/de-de/Infos-f%C3%BCr-Anbieter/Wie-werde-ich-Regelenergieanbieter-Pr%C3%A4qualifikation. Abgerufen am 26.02.2024.

Abkürzungen

ACER	European Agency for the Cooperation of Energy Regulators
AGB	Allgemeine Geschäftsbedingungen
AS4	Applicability Statement 4
BANULA	BArrierefreie und NUtzerfreundliche LAdemöglichkeiten schaffen
BDEW	Bundesverband der Energie- und Wasserwirtschaft e. V.
BNetzA	Bundesnetzagentur
BSI	Bundesamt für Sicherheit in der Informationstechnik
CLS	Controllable Local System
DEER	Dezentraler Redispatch. Für ein Energiesystem von morgen und eine Elektrifizierung der Zukunft
DID	Decentralized Identifier, eine Sequenz von Zahlen und Buchstaben; je nach Kontext wird auf den Identifier als Konzept oder die DID-Sequenz als Datum referiert
EDIFACT	Electronic Data Interchange for Administration, Commerce and Transport
EEG	Erneuerbare-Energien-Gesetz
EMS	Energiemanagementsystem
EnWG	Energiewirtschaftsgesetz
ERP	Enterprise Resource Planning
ESA	Energieserviceanbieter
EU	Europäische Union
EUDI-Wallet	Europäische Brieftasche für die digitale Identität (European Digital Identity Wallet)
FfE	Forschungsstelle für Energiewirtschaft e. V.
GPKE	Geschäftsprozesse zur Kundenbelieferung mit Elektrizität
HKN	Herkunftsnachweis
HKNR	Herkunftsnachweisregister
iMSys	Intelligentes Messsystem
IoT	Internet of Things

MaBis	Marktregeln für die Durchführung der Bilanzkreisabrechnung Strom
MaLo	Marktlokation
MaKo	Marktkommunikation
MaStR	Marktstammdatenregister
MaStRV	Marktstammdatenregisterverordnung
MeLo	Messlokation
mME	Moderne Messeinrichtung
MSB	Messstellenbetreiber
MsbG	Messstellenbetriebsgesetz
SMGW	Smart Meter Gateway
SMGWA	Smart Meter Gateway Administrator
S/MIME	Secure/Multipurpose Internet Mail Extensions
SM-PKI	Smart Meter Public Key Infrastructure
SSI	Self-Sovereign Identity
TLS	Transport Layer Security
UBA	Umweltbundesamt
ÜNB	Übertragungsnetzbetreiber
VBA	Virtuelle Bilanzierungszone
VC	Verifiable Credential
VNB	Verteilnetzbetreiber

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