Future Energy
Lab

BERICHT

DIVE – Digitale Identitäten als Vertrauensanker im Energiesystem

02 – Technische Details und Umsetzung der Basisinfrastruktur

Ein Projekt der

dena

Impressum

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

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

E-Mail:
info@dena.de
futureenergylab@dena.de

Internet:
www.dena.de

Autorinnen und Autoren:
Matthias Möller, BOTLabs
Gustav Hemmelmayr, BOTLabs
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. 02 – Technische Details und Umsetzung der Basisinfrastruktur

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

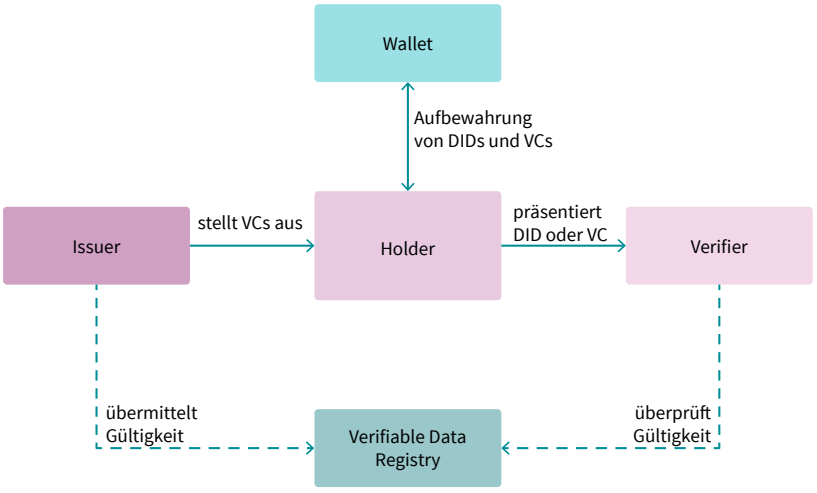

Abbildung 1: Vertrauensdreieck

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.

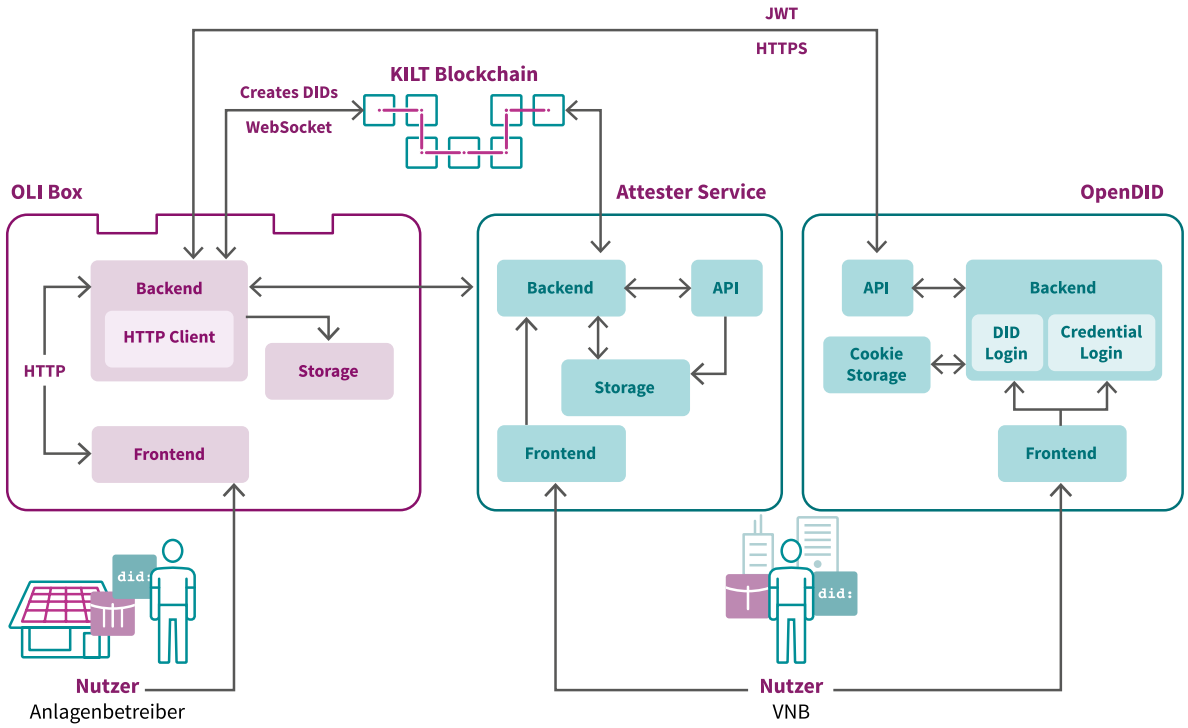

Abbildung 2: DIVE Basisinfrastruktur

Inhalt

1. Self-Sovereign Identities in der Energiewirtschaft

Der Ausbau der erneuerbaren Energien führt dazu, dass die Stromerzeugung in Deutschland zunehmend durch dezentrale und kleinere Anlagen erfolgt. Zusammen mit der fortschreitenden Elektrifizierung von Mobilität und Wärmeversorgung bedeutet dies einen organistorischen Aufwand hinsichtlich der involvierten Geräte und Anlagen. Millionen von Photovoltaik-Anlagen, Windrädern, Wärmepumpen, E-Ladestationen usw. müssen koordiniert und zu diesem Zweck auch identifiziert und authentifiziert werden. Gleichzeitig erfordern die zunehmende Sektorenkopplung von Strom, Wärme und Verkehr und die Einbindung neuer Akteure in das Energiesystem einen Ausbau von technischen Schnittstellen. Es braucht eine möglichst einheitliche Steuerung und Verwaltung, zumindest aber eine für die Verantwortlichen transparente und aussagekräftige Datengrundlage für Steuerungsentscheidungen.

Um diese Herausforderungen erfolgreich zu meistern und zukünftige Anwendungsfälle wie Flexibilitätsdienstleistungen oder Energy Communities zu ermöglichen, müssen die verfügbaren Anlagen zuverlässig, sicher und effizient eingebunden werden können. Zudem ist die Gewährleistung eines verlässlichen und flexiblen Datenaustauschs zwischen dezentralen Anlagen und Systemakteuren wie beispielsweise Netzbetreibern eine Grundvoraussetzung für das Gelingen der Energiewende. Nur durch eine solche nahtlose Integration kann die stetig zunehmende Komplexität des Energiesystems beherrschbar und die Versorgungssicherheit gewährleistet bleiben (Elia Group 2023; Körner et al. 2024).

Eine ebenso sichere wie zukunftsfähige Verwaltung und Steuerung dieser Anlagen bedarf technischer Schnittstellen und Konzepte zur Anbindung von Geräten und Anlagen in das Energiesystem. Ein vielversprechender Ansatz zur effizienten Anbindung und Verwaltung ist die Verwendung digitaler und dezentraler Identitäten: Durch eine eindeutige Identifizierung und Authentifizierung von Anlagen durch einen vertrauenswürdigen Energiesystemakteur kann eine digitale Identität einmalig erstellt und theoretisch für alle zukünftigen Interaktionen im Energiesystem genutzt werden (Babel et al. 2023). Eine Ausstattung von Anlagen und Geräten mit digitalen Identitäten bietet also das Potenzial dafür, den Verwaltungsaufwand durch digitalisierte und automatisierte Prozesse für alle Systemakteure enorm zu verringern.

Im Projekt DIVE wird dabei auf den konkreten Ansatz von selbstverwalteten Identitäten (Self-Sovereign Identities, SSI) gesetzt. Bei SSI handelt es sich um selbstsouveräne digitale Identitäten, bei denen bewusst auf eine zentrale Verwaltungsinstanz für Identitäten („Identitätsanbieter“) verzichtet wird. Ähnlich wie in der analogen Welt gibt es aber eine oder mehrere systeminterne Autoritäten, die hohes Vertrauen genießen („Vertrauensdienst“, hier z. B. Netzbetreiber). Dieser Vertrauensdienst prüft die Eigenschaften (hier z. B. Leistungsmerkmale der Anlage) und stellt darüber ein Verifiable Credential (vergleichbar mit einem Zertifikat) aus. Die ausgestellte Identität verbleibt beim Nutzer und kann mit den verifizierten Eigenschaften bei Bedarf selbstbestimmt (das heißt hier durch den Anlagenbesitzer und/oder -betreiber) eingesetzt werden. Eine solche Lösung stellt dem Energiesystem eine Option für ein skalierbares, sicheres und interoperables Fundament für die Energiewende zur Verfügung. Die **Prinzipien Open Source und Dezentralität** stellen sicher, dass die Lösung für die Weiterentwicklung offen bleibt. Dabei wurden im Projekt DIVE, wo vorhanden, alle gängigen Industriestandards verwendet, um Anbindung, **Anschlussfähigkeit** und maximale **Interoperabilität** zu gewährleisten. Neben der Anwendung dieser Industriestandards ist es darüber hinaus erforderlich, ein internes Regelwerk zu entwickeln. Dieses legt fest, worüber überhaupt kommuniziert wird (z. B. über welche Attribute einer Erzeugungsanlage) und welche Rollen im System befugt sind, die erforderlichen Attribute zu bestätigen (z. B. Marktrollen im Energiesystem).

Eine weitere Technologiekomponente, die im DIVE Projekt verwendet wird, ist eine Blockchain, die innerhalb der DIVE-Basisinfrastruktur als grundlegende technische Datenebene eine **vertrauenswürdige Verankerung und Bereitstellung von Identitäten** ermöglicht („Vertrauensanker“). Dies hat den Vorteil, dass die Akteure direkt miteinander kommunizieren können, ohne dass Dritte in die Kommunikation zur Identitätsprüfung involviert sind. Dadurch wird die Privatsphäre gewährleistet, die Sicherheit erheblich erhöht und der Mehraufwand durch einen Intermediär verhindert (BSI, 2021).

Durch den Einsatz einer dezentral aufgestellten und öffentlichen (public-permissionless) Blockchain, die also durch eine Vielzahl unabhängiger Blockchain-Knoten betrieben wird, kann die Ausfallwahrscheinlichkeit auf ein Minimum gesenkt und auch ein potenzielles „Gatekeeping“ verhindert werden. Somit wird möglichst vielen Akteuren (z. B. der Vielzahl an Kleinanlagen im Energiesystem) eine niederschwellige Teilnahme ermöglicht.

Der Bericht konzentriert sich im Weiteren auf drei Kernthemen. Zunächst wird in das Konzept von SSI sowie seine Herausforderungen und Vorteile eingeführt (Kapitel 2). Es folgt eine Beschreibung der Funktionsweisen und der einzelnen Schritte der KILT Blockchain sowie der einzelnen Schritte bei der Erstellung von digitalen Identitäten (Kapitel 3). Der Schwerpunkt des Berichts liegt bei der Abbildung von energiewirtschaftlichen Prozessen wie beispielsweise dem Onboarding einer Photovoltaik-Anlage unter realweltlichen Bedingungen mittels der in DIVE entwickelten Lösung (Kapitel 4). Ausführungen zur Datenverarbeitung und ein Ausblick schließen den Bericht ab.

2. Einführung in das Konzept von Self-Sovereign Identities

Gemeinhin wird die theoretische Vorarbeit zu selbstsouveränen digitalen Identitäten dem Informatiker und führenden Digital-Theoretiker Christopher Allen zugeschrieben, der in einem Artikel von 2016 zehn Prinzipien postuliert hat, die ein egalitäres und selbstbestimmtes Identitätsmanagement für das digitale Zeitalter erfüllen müsste[1]:

- Gesicherte Existenz (kein Bot)
- Kontrolle über eigene Daten
- Zugang zu Identitätsdaten
- Transparenz in Bezug auf den Umgang mit Daten
- Langlebigkeit der Identitätsdaten (entsprechend den Wünschen des Nutzers)
- Mobilität der Daten (der Nutzer kann sie wie gewünscht transferieren)
- Interoperabilität
- Zustimmungs- und Ablehnungsrechte
- Datenminimierung
- Sicherheit

Dabei ging es zunächst um die Handhabung von digitalen Identitäten für natürliche Personen, mit entsprechend hohen Erwartungen und Anforderungen an den Schutz der Privatsphäre. In den Folgejahren begann die globale, kollaborative Entwicklung von Protokollen, Pilotprojekten und schließlich ganzen Software Development Kits (SDKs). Daraus ging unter anderem die Gründung der Decentralized Identity Foundation (DIF) hervor, die sich dafür einsetzt, selbstsouveräne digitale Lösungen zu unterstützen und Alternativen zu proprietären Lösungen wie den Single-Sign-On-Modellen (z. B. bekannt durch Google, Apple oder Meta) zu etablieren. Inzwischen wurden diese technischen Grundlagen für SSI standardisiert und durch Aufnahme in das Repository des globalen Standardisierungsgremiums W3C zertifiziert.

2.1 Akteure und ihre Rollen

Das Grundkonzept von SSI ist eine Art Gewaltenteilung zwischen den Akteuren, die miteinander interagieren. Es soll vermieden werden, dass sich Daten und Rechte zu sehr an einem Punkt konzentrieren und dadurch Abhängigkeiten oder Sicherheitsrisiken entstehen. Zu diesem Zweck werden um die Identität herum drei Rollen definiert:

- Der **Identitätsinhaber (Identity Holder)** – die natürliche oder rechtliche Person, die identifiziert werden soll
- Der **Vertrauensdienst**, auch Herausgeber von Identitätsnachweisen **(Identity Issuer)** – eine anerkannte Autorität, die die Identität einer Person prüfen und bestätigen kann
- Die **Akzeptanz- oder Prüfstelle (Identity Verifier)** – in der Regel ein Dienstleister, der die Identität der Person auf Echtheit prüfen muss (beispielsweise um ein Online-Geschäft abzuwickeln oder einem digitalen Gerät Zugriff auf Daten zu gewähren)

2.2 Das Vertrauensmodell

Die Herausforderung eines Identitätsmanagements im digitalen Raum besteht in der Unmöglichkeit, direkt mit dem Gegenüber – sei es Mensch oder Anlage – in Kontakt zu treten. Anstatt der eigenen Wahrnehmung vertrauen zu können („Ich sehe, dass die Anlage an dieser Stelle steht."), müssen wir uns auf digitale Prozesse verlassen, die unsere eigene Wahrnehmung ersetzen sollen. Digitales Identitätsmanagement versucht daher über digitalisierte Verwaltungsprozesse, das Vertrauen aus der analogen Welt „nachzubauen".

Das Vertrauensmodell von SSI sieht vor, dass das Vertrauen in den Prozess durch eine vertrauenswürdige Entität verankert wird. Der Herausgeber von Identitätsnachweisen hat diese Schlüsselrolle. Da in der analogen Welt bereits ein Vertrauensverhältnis besteht (z. B. Netzbetreiber, Einwohnermeldeamt), reicht es, wenn abgesichert werden kann, dass

A. der Identitätsherausgeber tatsächlich die Entität ist, die er vorgibt zu sein.
   - **Herausgeber ist authentifiziert**

B. der Identitätsherausgeber gewissenhaft und ordnungsgemäß überprüft, ob **ein Identitätsinhaber tatsächlich die Eigenschaften besitzt**, für die ein Nachweis ausgestellt wird, und dass der ausgestellte Nachweis aktuelle Gültigkeit hat.
   - Nachweise (Credentials) können widerrufen werden
   - Nachweise sind durch Herausgeber signiert

C. der Identitätsinhaber tatsächlich die natürliche oder rechtliche Person ist, die er vorgibt zu sein.
   - **Inhaber ist authentifiziert**

D. der Identitätsinhaber die einzige Person oder Entität ist, die die ausgestellten Nachweise verwenden kann.
   - **Nachweise sind doppelt signiert** (von Herausgeber und Inhaber) **und somit nicht übertragbar**

1 Allen Christopher (2016): A Patch to self-sovereign identity. https://www.lifewithalacrity.com/article/the-path-to-self-sovereign-identity/

Kann dies technisch gewährleistet werden, können Prüfstellen bei der Interaktion darauf vertrauen, dass sie mit vertrauenswürdigen Akteuren interagieren. Abschließend muss dann in umgekehrter Richtung gewährleistet werden, dass

A. die Prüfstellen ein berechtigtes Anliegen haben, die Nachweise zu lesen.
   - **Prüfer ist authentifiziert**
   - **Zugriff von Prüfstellen auf Nachweiszertifikate erfolgt nur entsprechend festgelegten Regeln**

B. die Prüfstellen ordnungsgemäß mit den Daten umgehen.
   - Minimierung der abgefragten Daten
   - **Selbstbestimmte Weitergabe von Daten** durch den Dateninhaber

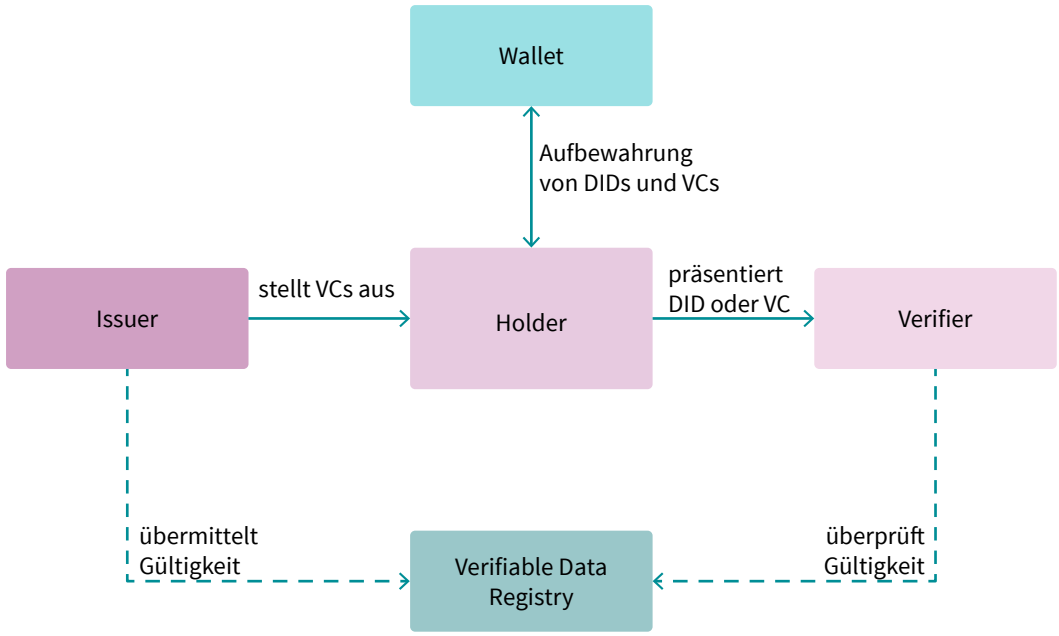

Abbildung 3: Vertrauensdreieck

3. Eine digitale Identitäts-infrastruktur für die Energiewirtschaft

Ziel der Entwicklungsarbeit in DIVE ist es, den Akteuren in der Energiewirtschaft, wie zum Beispiel Energieerzeugungsanlagen, den handelnden Personen oder Organisationen, die Registrierung ihrer Anlagen und die Teilnahme an Anwendungsfällen mithilfe ihrer selbstverwalteten Identitäten auf Basis der W3C-Standards für Decentralized Identifiers (DIDs) und Verifiable Credentials (VCs) zu ermöglichen.

Zur Umsetzung der selbstverwalteten Identitäten wird in DIVE das Blockchain-Protokoll KILT als Identitätsinfrastruktur genutzt. Das KILT Protocol ist ein public-permissionless Blockchain-Protokoll für digitale und dezentrale Identitäten, das die Standards für DIDs und VCs implementiert. Es wurde initial von der BOTLabs GmbH auf „Substrate“ – einem Open-Source-Framework zur Erstellung von Blockchains und Blockchain-Anwendungen – entwickelt. Es handelt sich um ein dezentrales, öffentliches und Open-Source-basiertes Blockchain-Protokoll. Zum KILT Protocol gehört ein Software Development Kit (SDK), das alle Funktionalitäten des KILT Protocol implementiert.[2]

Bei den Blockchain-Funktionalitäten wird zwischen Schreib- und Lesezugriff unterschieden. Während für Lesezugriffe keine Transaktionskosten anfallen, müssen für Schreibzugriffe Transaktionsgebühren entrichtet und es muss eine Kaution, das sogenannte Deposit, hinterlegt werden. Diese Kaution wird zurückgezahlt, wenn zum Beispiel eine DID wieder von der Blockchain gelöscht wird. Die Gebühren gehen an das Blockchain-Netzwerk. Andere Varianten der Verifiable Data Registry können andere Entlohnungsformen für die Bereitstellung und Wartung bedeuten.

Um die Funktionen des KILT Protocol für SSI zu nutzen, gibt es eine Vielzahl an Applikationen, die als Schnittstelle zwischen den Nutzern und der Identitätsinfrastruktur dienen. Viele der Applikationen kommen im Rahmen des DIVE-Projekts zum Einsatz, sind aber unabhängig vom DIVE-Projekt entstanden. Sie unterliegen überwiegend Open-Source-Lizenzen und können ohne Lizenzgebühren genutzt und bei Bedarf für die eigenen Anwendungsfälle angepasst werden.

3.1 Die Erzeugung von Self-Sovereign Identities auf der KILT-Infrastruktur

Auf technischer Ebene funktioniert SSI anhand von zwei Schlüsselkomponenten: Decentralized Identifiers (DIDs) und Verifiable Credentials (VCs), die von der Decentralized Identity Foundation (DIF)[3] entwickelt und vom W3C standardisiert[4] wurden.

DIDs sind Sequenzen von Zahlen und Buchstaben, die als eindeutiger Identifier dienen und von einer Entität erzeugt, verwaltet und kontrolliert werden können – ohne die Notwendigkeit eines zentralen Registers, eines Identitätsproviders oder einer Zertifizierungsstelle. Sie ermöglichen also sichere, verifizierbare

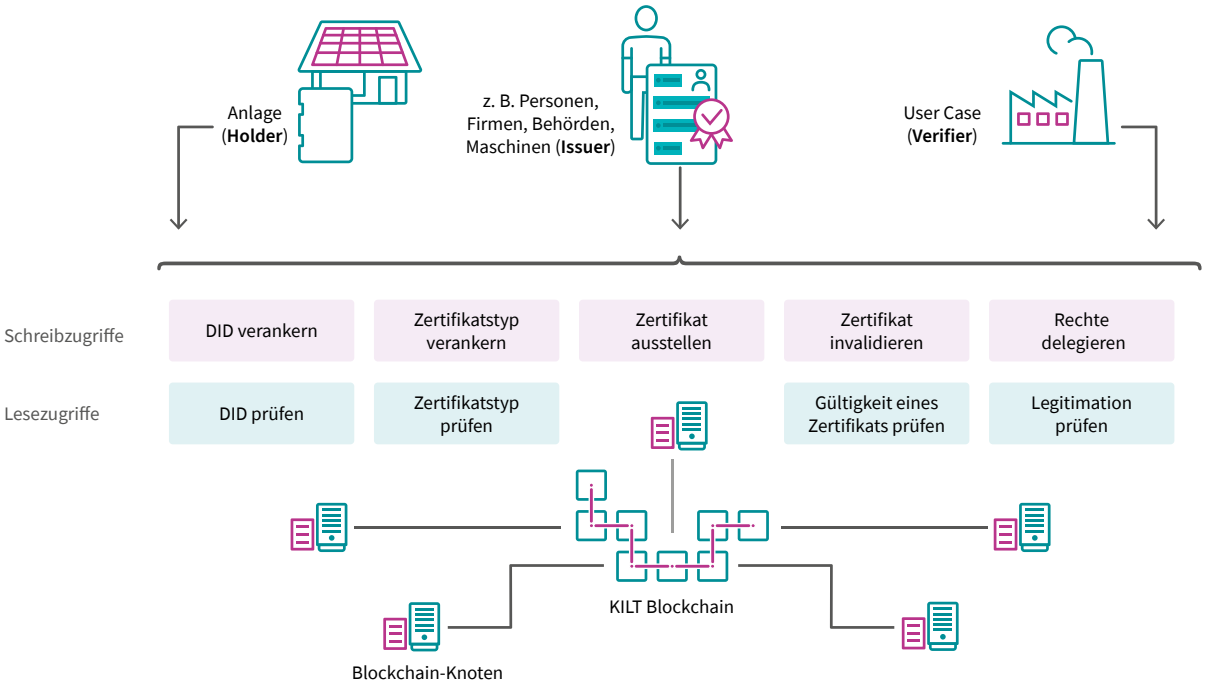

Abbildung 4: KILT Protocol: Schreib- und Lesezugriffe

2 Das SDK umfasst eine vollständige Spezifikation sowie eine kohärente Softwarebibliothek, die auf die aktuelle Version des KILT Protocol abgestimmt ist. Dieses SDK ermöglicht es Anwendungsentwicklern, Dienste und Anwendungen auf der Grundlage des KILT Protocol zu entwickeln, ohne tiefere Kenntnisse zur Blockchain-Technologie zu benötigen.

3 https://identity.foundation/

4 https://www.w3.org/TR/did-core/ und https://www.w3.org/TR/vc-data-model/

und dezentrale digitale Identitäten, bei denen der Besitz einer Identität ohne die Beteiligung einer zentralen Instanz nachgewiesen werden kann. Eine DID-Sequenz besteht aus einer eindeutigen Zeichenfolge, die sich aus drei Teilen zusammensetzt:

- dem DID-URI-Schema-Identifier
- dem Identifier für die DID-Methode
- dem DID-Methoden-spezifischen Identifier

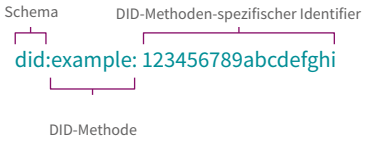

Abbildung 5: Bestandteile einer DID – Formatdarstellung

Der Inhaber einer DID kontrolliert sie durch private kryptografische Schlüssel (auch Private Key genannt), mit denen sich auch die Eigentümerschaft nachweisen lässt. Zu einer DID gehört neben dem privaten Schlüssel auch ein öffentlicher Teil, das sogenannte DID-Dokument. Dieses DID-Dokument enthält die öffentlichen Informationen, die für die Interaktion mit der DID erforderlich sind, wie beispielsweise öffentliche Schlüssel (auch Public Key genannt), Methoden zur Authentifizierung, Service-Endpunkte etc.

Bei Verifiable Credentials handelt es sich um kryptografisch überprüfbare Nachweise über Eigenschaften der betreffenden Identität, die von einer vertrauenswürdigen Instanz (Issuer) ausgestellt werden. Ein Verifiable Credential enthält eine Behauptung (einen sogenannten Claim) über die Attribute (z. B. das Inbetriebnahmedatum einer Anlage), Metadaten (z. B. das Ausstellungsdatum des VC) sowie kryptografische Beweise (z. B. digitale Signaturen). VCs ermöglichen den sicheren Austausch und die Überprüfung von Informationen und schaffen so Vertrauen zwischen den Parteien, ohne dass Vermittler oder zentrale Instanzen benötigt werden. Denn im Gegensatz zu zentralisierten Identitätssystemen, bei denen die Identitäten von einer zentralen Instanz verwaltet und kontrolliert werden, verbleibt bei diesem dezentralen Ansatz die Kontrolle über die Identitäten bei der jeweiligen Identität. Dies bietet die Vorteile, dass

- das System sehr gut **skalierbar** ist, da es ohne zentrale Instanzen auskommt, die zu einem potenziellen Engpass werden könnten, und die Verifiable Credentials beliebig oft verwendet werden können.
- sich die **Sicherheit** des Systems erhöht, da die Daten nicht mehr zentral gespeichert werden und somit das Risiko von Ausfällen und Angriffen gesenkt wird (kein „Single Point of Failure“ und kein „Honeypot“).
- die **Privatsphäre** erhöht wird, da die Identität entscheiden kann, welche Informationen sie offenlegt, und weder der Aussteller des Nachweises noch die Öffentlichkeit Informationen darüber erhält, mit wem und zu welchem Zweck der Identitätsinhaber Daten teilt.

3.1.1 Generieren einer DID

DIDs werden auf einem lokalen Gerät unter der Kontrolle der entsprechenden Entität (Mensch oder Anlage) erzeugt.

Zur Erzeugung einer DID wird mittels Entropie[5] ein Seed[6] erzeugt, aus dem ein Private/Public-Key-Paar erstellt wird. Mit diesem Schlüsselpaar kann kryptografisch sichergestellt werden, dass nur der Inhaber des Key Pair Operationen für diese DID ausführen kann. Auf Basis des Private/Public Key Pair wird dann die DID für eine Identität, zum Beispiel eine Anlage, generiert.

Eine DID setzt sich aus dem Identifier und dem DID-Dokument zusammen. Die Informationen, aus denen sich das DID-Dokument zusammensetzt, werden auf der KILT Blockchain gespeichert. Dabei handelt es sich beispielsweise um die Public Keys und – wenn vorhanden – den web3name (ein optionaler eindeutiger, menschenlesbarer Name, der eine DID repräsentiert) sowie Service Endpoints, über die mit der DID interagiert werden kann und die in diesem Projekt für die Integration mit den Anwendungsfällen genutzt werden.

Eine DID auf Basis des KILT Protocol benötigt also für die Verwaltung und Auflösung, das heißt das Abrufen und Lesen der Daten, die mit der DID verknüpft sind, zusätzlich die KILT Blockchain. Dies ermöglicht neben dem Schlüsselmanagement auch weitere Aktionen wie das Ausstellen von Credentials, das Anlegen von Credential-Formaten etc.

Im Folgenden ist ein Beispiel für eine vollständige KILT DID zu sehen:

Abbildung 6: Bestandteile einer DID – Beispiel

Die KILT-DID-Methode ist beim Universal Resolver, einem Service der DIF, registriert und kann dort so weit aufgelöst werden, dass die öffentlich hinterlegten Informationen zu dieser DID angezeigt werden. Dies funktioniert, indem man die komplette DID (Schema, Methode und DID-Methoden-spezifischer Identifier) dort in das Suchfeld eingibt.[7]

Identitäts-Wallet für Personen und Organisationen

Um eine selbstsouveräne digitale Identität anzulegen und zu verwalten, benötigen die Akteure, wie zum Beispiel Anlagenbetreiber oder Aussteller von Credentials, eine sogenannte

5 In der Informationstheorie beschreibt Entropie das Maß an Unsicherheit oder Zufälligkeit in einer Informationsquelle. Zufälligkeit wird benötigt, um Reproduzierbarkeit zu verhindern.

6 Ein Seed ist eine Folge von Zufallswörtern, in der die Daten gespeichert sind, die für den Zugriff auf Krypto-Wallets erforderlich sind.

7 https://dev.uniresolver.io/

Identitäts-Wallet. Der Begriff leitet sich vom englischen Wort für Geldbörse oder Brieftasche ab und wurde ursprünglich eingeführt, um digitale Software für die Aufbewahrung und Verwaltung von Kryptowährungen zu beschreiben. Während der Corona-Pandemie sind die meisten Bürgerinnen und Bürger Europas durch die Nachweis-Apps für Testergebnisse und Impfstatus bereits mit einer Form von Wallet in Berührung bekommen.

Im DIVE-Projekt wurde *Sporran* als Identitäts-Wallet eingesetzt. Sporran ist eine kostenlose Desktop-Browser-Erweiterung, die als Schnittstelle zu KILT und weiteren Web3-Diensten[8] dient.

Ähnlich wie eine herkömmliche Krypto-Wallet zeigt Sporran das KILT-Coin-Guthaben eines Nutzers an und unterstützt das Signieren und Senden von Transaktionen auf der KILT Blockchain. Darüber hinaus ermöglicht Sporran das Anlegen und Verwalten digitaler und dezentraler Identitäten.

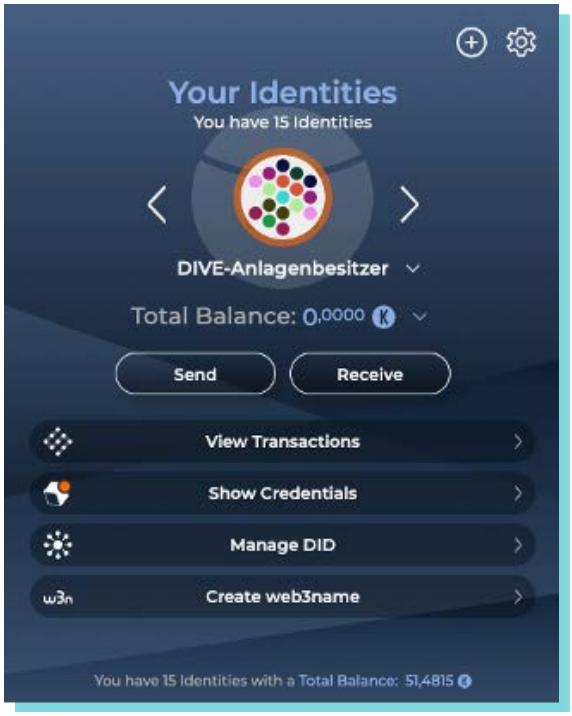

Abbildung 7: User Interface der Wallet

Entscheidend für den Einsatz in der DIVE-Basisinfrastruktur ist die Kompatibilität der Schnittstellen der jeweiligen Technologie-Komponenten. In der Praxis wären also auch beliebig viele andere Identitäts-Wallets, Blockchain-Anbieter oder auch Nicht-Blockchain-Lösungen möglich, solange sie die vorhandenen Schnittstellen nutzen können oder neue Schnittstellen nach Bedarf entwickeln.

Mithilfe einer Identitäts-Wallet kann der Identitätsinhaber einen „digitalen Fingerabdruck" in Form eines dezentralen Identifiers (DID) direkt auf seinem Rechner oder seinem Smartphone erstellen. Verifiable Credentials werden mit der DID-Sequenz verknüpft, indem sie bei Issuern angefordert und anschließend in der Wallet gespeichert werden. Auch das Teilen von Credentials erfolgt über die Wallet. Der Identitätsinhaber kann dort autorisierern, welches Credential und welche Informationen daraus mit wem geteilt werden sollen.

Es gibt inzwischen eine Vielzahl von Wallet-Anbietern, die sich zum Teil ausschließlich auf die Verwaltung von digitalen Identitäten konzentrieren. Auf EU-Ebene wurde mit der neuen eIDAS-Verordnung (EU-Verordnung über elektronische Identifizierung und Vertrauensdienste) zudem beschlossen, dass jedes EU-Mitgliedsland ab 2026 eine offizielle Identitäts-Wallet für seine Bürgerinnen und Bürger bereitstellen soll. Dafür hat ein technisches Expertengremium der EU eine Blaupause für die sogenannte European Digital Identity Wallet (EUDI-Wallet) veröffentlicht. Entsprechend dieser Blaupause werden gerade in allen Mitgliedstaaten Identitäts-Wallets entwickelt.

Durch die modulare Architektur der DIVE-Basisinfrastruktur können die beschriebenen Wallet-Funktionen mit wenig Aufwand in Zukunft also auch von EUDI-konformen Anbietern übernommen werden.

3.1.2 Das Ausstellen von Verifiable Credentials

Definition der Credential-Formate

Damit die verschiedenen Akteure miteinander kommunizieren können, bedarf es nicht nur einer Standardisierung der Art und Weise, wie die Akteure dies tun, sondern auch dessen, was sie kommunizieren, das heißt der inhaltlichen Struktur von Eigenschaften und Credentials.

Da es unmöglich ist, die Inhaltsstruktur für eine unendliche Anzahl von Anwendungsfällen zu standardisieren, ist hier ein Abstraktionslevel notwendig. Das KILT Protocol ermöglicht dies über die Einführung der Credential Types (CTYPE)[9], bei denen es sich um die JSON-Beschreibung einer Datenstruktur handelt. Sie enthält eine Liste von Schlüssel-Wert-Paaren, wobei jeder Wert von einem definierten Typ ist. Ein CTYPE definiert somit das Schema für die Erstellung eines Credentials unter der Benutzung des KILT Protocol als Identitätsinfrastruktur und ist mit einem Formular vergleichbar. Der Vorteil dieses Vorgehens ist, dass mit geringem Aufwand neue CTYPEs als Basis für Credentials generiert werden können, um das System zu erweitern und zum Beispiel neue Anwendungsfälle zu ermöglichen.

Zum Anlegen der Credential Types kann der CTYPE Hub[10] verwendet werden – eine Applikation zum Anlegen neuer und zum Nachschlagen von bestehenden CTYPEs, den „Formularen", auf denen die Verifiable Credentials aufbauen. Zum Anlegen eines neuen CTYPE werden eine KILT-kompatible Wallet, eine DID und ein Guthaben[11] an KILT Coins benötigt.

Im Rahmen des DIVE-Projekts wurden zwei CTYPEs definiert, angelegt und auf der Blockchain verankert:

8 https://de.wikipedia.org/wiki/Web3
9 https://docs.kilt.io/docs/concepts/credentials/ctypes
10 https://ctypehub.galaniprojects.de/
11 Die Kosten für so einen Vorgang lagen am 5. Juni 2024 bei 0,00082 KILT, was 0,00019 Euro entspricht.

das **Selbstauskunftszertifikat** für einen Anlagenbetreiber und das **DIVE-Anlagenzertifikat** für die Anlage selbst.

Für den Betreiber der Anlage wurde ein CTYPE (Selbstauskunftszertifikat) mit folgenden Feldern angelegt[12]:

- Name
- Betreiber
- Adresse

Für den Anlagen-CTYPE (DIVE-Anlagenzertifikat) wurden folgende Felder definiert:

- Anschlussnetzbetreiber
- Art der Anlage
- Betreiber
- Betreiberstatus
- Bruttoleistung
- EEG-Inbetriebnahmedatum
- EEG-Registrierungsdatum
- Errichtungsort (Lage)
- Inbetriebnahmedatum
- Installierte Leistung
- Marktlokations-ID
- Messlokations-ID
- Meter-ID
- Name der Einheit
- Registrierungsdatum im aktuellen Betriebsstatus
- SMGW-ID
- Standort
- Wechselrichterleistung

Beantragen und Ausstellen von Verifiable Credentials

Der Prozess zum Ausstellen von Credentials findet in drei Schritten statt: Im ersten Schritt erzeugt zum Beispiel die Anlage als Holder einen sogenannten Claim, entsprechend dem ausgewählten, definierten CTYPE. Einen Claim kann man sich als ausgefülltes Formular vorstellen, das heißt, der Holder gibt darin die erforderlichen Informationen, wie beispielsweise Anlagenart und Inbetriebnahmedatum, an und schickt das zu attestierende Credential an einen vertrauenswürdigen Issuer (z. B. einen Verteilnetzbetreiber), um es bestätigen zu lassen. Issuer benötigen eine Benutzeroberfläche zur Ausstellung von VCs. Dafür wird in DIVE der Attester Service verwendet, der in bestehende IT-Systeme der Issuer integriert werden kann. Dabei unterscheidet ein Authentifizierungsmechanismus zwischen „normalen“ Benutzern, also den Anlagenbetreibern, die Credentials beantragen, und den Mitarbeiterinnen und Mitarbeitern, die diese Credentials ausstellen. Anlagenbetreiber können die Ausstellung von Verifiable Credentials beantragen, die dann von den Beschäftigten geprüft und ausgestellt werden. Die Authentifizierung erfolgt über den Abruf eines JWT-Tokens[13] von OpenDID[14]. Anlagenbetreiber melden sich mit ihrer DID an, während Beschäftigte zusätzliche Anmeldedaten benötigen. Der Attester Service ist eine generische und wiederverwendbare Applikation, die unter einer Open-Source-Lizenz verfügbar ist. Die Plattform implementiert alle notwendigen Protokolle, um sowohl mit menschlichen Nutzerinnen und Nutzern als auch mit Maschinen zu kommunizieren. Der Attester Service kann als Off-the-Shelf-Komponente direkt innerhalb eines containerbasierten Software-Stacks eingesetzt oder als Grundlage für spezifische und einfache Frontends genutzt werden.

In einem zweiten Schritt prüft der Issuer dann die Gültigkeit des auszustellenden Credentials und stellt sicher, dass die darin enthaltenen Daten den Anforderungen an das Credential entsprechen (beispielsweise ob die Anlage wirklich erneuerbaren Strom erzeugt). Die Prüfung der Richtigkeit der Angaben durch den Issuer findet zum Beispiel durch Servicetechnikerinnen und -techniker vor Ort statt, die die Installation der Anlage überprüfen und dann das Credential ausstellen.

Das Credential enthält folgende Informationen:

- **cTypeHash**[15]**:** Bezug auf den zugrunde liegenden Credential Type
- **contents:** Die inhaltlichen Attribute des Credentials, in diesem Fall zum Beispiel Anschlussnetzbetreiber etc.
- **owner:** DID des Credential-Inhabers

12 Über den CTYPE-Hash kann der CTYPE nachgeschlagen und über Subscan kann die Verankerung des CTYPE auf der KILT Blockchain nachvollzogen werden.

13 JSON Web Token, ein Webstandard, um beliebige Daten zusammen mit einer Signatur zu präsentieren

14 https://github.com/KILTprotocol/opendid

15 „Eine Hashfunktion oder Streuwertfunktion ist eine Abbildung, die eine große Eingabemenge, die Schlüssel, auf eine kleinere Zielmenge, die Hashwerte, abbildet. Eine Hashfunktion ist daher im Allgemeinen nicht injektiv. Die Eingabemenge kann Elemente unterschiedlicher Längen enthalten, die Elemente der Zielmenge haben dagegen meist eine feste Länge.“ https://de.wikipedia.org/wiki/Hashfunktion

- **claimHashes:** Hash über die einzelnen Attribute. Wenn nur einzelne Attribute geteilt werden, lässt sich das Credential immer noch kryptografisch verifizieren.

- **claimNonceMap:** Enthält eine Zuordnung (Mapping) zwischen einem Claim (einem Attribut) und einem zufällig generierten Wert, der sogenannten Nonce. Dies ist notwendig, um zu verhindern, dass aus den Claim Hashes die zugrunde liegenden Attribute errechnet werden können, im Falle, dass nicht alle Attribute dem Verifier freigegeben werden.

- **delegationID:** Wenn die ausstellende Identität durch eine dritte Identität dazu autorisiert worden ist (z. B. eine Mitarbeiterin oder ein Mitarbeiter des Verteilnetzbetreibers)

- **legitimations:** Information darüber, ob das Credential eine Legitimation enthält

- **rootHash:** Bei dem Root Hash handelt es sich um die Signatur des Claims. Er wird aus allen Informationen des Claims sowie der DID des Ausstellers und des Claimers generiert.

Der Anlagenbetreiber als Inhaber des Credentials speichert das Credential auf einem Datenspeicher (z. B. in einer Wallet) seiner Wahl und unter seiner Kontrolle ab. Der Anlagenbetreiber kontrolliert und entscheidet, mit wem er das Credential teilt und welche Informationen daraus weitergegeben werden. Der Zugriff auf das Credential wird somit nicht durch Dritte, sondern ausschließlich durch der Anlagenbetreiber kontrolliert.[16]


```
"credential": {
    "claim": {
      "cTypeHash": "0x2a63756ff4934eb51d5c405476ea92dfa9413388a8a33c37755442e2111304b5",
      "contents": {
        "Anschlussnetzbetreiber": "RWE",
        "Art der Anlage": "Solar",
        "Betreiber": "Matthias",
        "Betreiberstatus": "Aktive",
        "Bruttoleistung": 100,
        "EEG Inbetriebnahmedatum": "2024-06-26",
        "EEG Registrierungsdatum": "2024-06-26",
        "Errichtungsort (Lage)": "Garten",
        "Inbetriebnahmedatum": "2024-06-26",
        "Installierte Leistung": 100,
        "Name der Einheit": "Solarpanel",
        "Registrierungsdatum im aktuellen Betriebsstatus": "2024-06-26",
        "Standort": "Berlin",
        "Wechselrichterleistung": 100
      },
      "owner": "did:kilt:4pWGHYTZiygyhG6R2WERuLcuwCrnBWawggG3EqngdyogAxJV"
    },
    "claimHashes": [
      "0x15a99d28a74299f8f37a379e6a56c910391930d31a97594102eaa6d9fa2dff91",
      "0x1611b308f75ad865f2f68a90532cd4f86e990b7e347b1bb74d91ca3d4cf27554",
      "0x3984bb6e0012087dbd7667b7648de39234bb83a03d99a7f8e0347121de82256f",
      "0x4be30e8b4b721a7ae1c619ade9ed690c1924fd8c6fd1d729c2a961d1bcd129d2",
      "0x5a720f32446e49de3ba442026a2ddeffa3030139ac09f327affc62c239a9d238",
      "0x5e407ba6381e327e8584600c734ad981b5bd0495903fdc4ec022f1d63721be5e",
      "0x7e032d6d3cc47253657582cf7ee8ea8b3a7f1b5e9708c5197bb2754b6998f384",
      "0x81659dc5c2e90a66c83d984611cd24856f7ea003cbfa86778dfd9ae22baa9cc9",
      "0x868f726af6f360c46f429757082fdfce1cc1cf9e701b4a603d13b457c26cb4b2",
      "0xa1ff48784ad666d45f77189a43dcfa91367821a07621feb6515024786a1a33cd",
      "0xa43ccaef23e6530242d2fb4e14a01ee006f4e116c2b7b6dc517d07725ee79049",
      "0xa9a48bd540999aec5df8acbb6014a65dd6969bf4a9c9275a0c3051041d97d212",
      "0xb2ae9e31e2096024a2301359654f7869dcadb29163ae842bf314da8c0d686873",
      "0xb2c42e1898e322d0c25c26887b2b1d181b668365399ea992344c8541c4eada1f",
      "0xf20bdcbc1824575981ad092c1583c637e3978875760a543178ad9d8aae51e589"
    ],
    "claimNonceMap": {
      "0x072ba3a6b6b1afcaa93614b16685660e11017e1ea0081ea498c8a9669f43b3c9": "68d367ff-50f0-44a6-8a77-95e24de29a5f",
      "0x321641af323a4fc4c8a6d6ed6e7f0d46440d72b6ff94399c0af73c205669e940": "07b49df8-0f7b-4185-8575-d3314c7257b2",
      "0x35dbdd55171245f76cca984132cfefcfbc005cf6a91ad4e2529e3ff935ea0697": "df7024e4-1f27-431f-ad39-121c0cb2c594",
      "0x408cbfe58cd4b0ed8c4be46281c53fd844951f4e98fa5232a2572e68cb038d3a": "77160665-98ef-4f6c-9868-2295372b41a8",
      "0x612ca41f911415a28d6919be9e42dbd7051c44c405dcbd8f366b8e9029c6dd4e": "e271cf71-ba2c-40d5-8cd1-81752dd8462a",
      "0x6b69f44d90054ad2ec19e1cae34fb1e80f6005bcd9aa055d139214631db02985": "c6b96f6a-f2a9-4cd7-9e12-a5961b1be36b",
      "0x73759ab4f78419281f8b88a6c1877cabb462e11a41baa8931bb8e6ffa027b47b": "782d84e8-c71a-4a83-9ac8-16e3dc5a72ee",
      "0x972644d0a780a69cf0cee813aafd76cd7afaf539e58cfdd3564465a5b9a61b6a": "d3e82266-92dd-423b-a355-a41a92040922",
      "0xa92b386a9b9cfc02128f6b6506e7a810f33bdc88f4899867a036d58a2f9fe0d2": "6d44364b-b84f-4a83-909d-97f713b7d7f4",
      "0xaa9991b23d65ec5bfff44199603367dd7edc1fa72a576835cab23eaa771e0762": "d4a6f8fc-2bae-4bea-b61c-939a60592200",
      "0xb935ac3ccd14fcedfa5b3e10fb8bb7f0fd9be0ca92378a346ebe4ad16f1a5371": "ec26fd67-9e61-4b62-9fff-af78dc1a3a7e",
      "0xc51159f600a2298dbf92db684616597c98b84847f0fd76d6fa3beffbda60ac24": "5250fae5-cfa1-4748-b6e5-db0d9d55bf66",
      "0xd257e3e01b29ef68cdc79f04787d40a354ae69a0ac73aeeb4662d9a44299f9ac": "b9f50047-8ab3-49dd-a09c-0fc482b27ece",
      "0xe9d96d5cae51599e535a69bf04fb522db81c1e33689559d9c0462aa4323d5090": "2245fc28-384a-4ace-8e45-6ac06d9bbe37",
      "0xf909240c27d913223515e03b3e3c28a97d03f68828be5cd962229d0cde067c68": "46fef1a3-85f5-4c13-9ff0-d05f2d3d3671"
    },
    "delegationId": null,
    "legitimations": [],
    "rootHash": "0x3a381f81d4f778cda34eb2c1fdf4331d2d49f2fd9e41eb56713395265abd35b3"
  },
```


Abbildung 8: Ein Credential im JSON-Format[17], das die oben beschriebenen Informationen enthält (die eingetragenen Werte haben keinen Bezug zur Realität)

16 Die Informationen des Credentials werden zu keinem Zeitpunkt auf der Blockchain gespeichert.

17 „JSON ist ein kompaktes Datenformat in einer einfach lesbaren Textform für den Datenaustausch zwischen Anwendungen". https://de.wikipedia.org/wiki/JavaScript_Object_Notation#:~:text=Die%20JavaScript%20Object%20Notation%20(JSON,existieren%20in%20allen%20verbreiteten%20Sprache

Im dritten Schritt schreibt der Aussteller des Credentials den Root Hash[18] des Credentials auf die KILT Blockchain und bescheinigt damit die Gültigkeit des Nachweises. Dies ist notwendig, damit im weiteren Zeitverlauf geprüft werden kann, ob das Credential weiterhin gültig ist oder zwischenzeitlich invalidiert wurde. Da es sich um einen Hash handelt, der sich nicht zurückrechnen lässt, lassen sich keine Rückschlüsse auf den Inhalt des Credentials und den Credential-Inhaber ziehen.

Die Daten auf der Blockchain sind dementsprechend zwar für alle öffentlich zugänglich, enthalten aber weder Informationen zum Inhalt noch zum Inhaber des Credentials, sondern lediglich zu dessen Gültigkeit.[19]

Im Folgenden ein Überblick über die Informationen, die auf der Blockchain für alle zugänglich gespeichert werden:

- **ctypeHash:** Der CTYPE, auf dem das Credential basiert
- **attester:** Aussteller des Credentials
- **authorizationID:** Genutzte Vertrauensstruktur (Delegation oder Legitimation)
- **revoked:** Gültigkeit des Credentials (false oder true)
- **deposit:** Informationen über den Inhaber des Deposits für die Transaktion (nicht der Inhaber des Credentials!)

Weitere kurze Ausführungen zu den Themen Legitimation und Vertrauensstrukturen finden sich im Anhang.

```
attestation.attestations: Option<AttestationAttestationsAttestationDetails>

{
  ctypeHash: 0x2a63756ff4934eb51d5c405476ea92dfa9413388a8a33c37755442e2111304b5
  attester: 4qGqegcXWctkdLToCSFfBAUQE5V5SBdwivaB6miWgXS6C6Cf
  authorizationId: null
  revoked: false
  deposit: {
    owner: 4qNLGrum9WxGrQkzwEhigiUmkoiYPq5vdzdZnsM25U5RbHu7
    amount: 120,950,000,000,000
  }
}
```

Abbildung 9: Gültiges Credential auf der Blockchain

18 Es handelt sich um den obersten Hash-Wert (die „Wurzel“) in einer Baumstruktur, der alle darunterliegenden Daten oder Hashes zusammenfasst und repräsentiert.

19 https://ipfs.io/ipns/dotapps.io/?rpc=wss%3A%2F%2Fspiritnet.kilt.io%2F#/chainstate

3.1.3 Teilen eines Credentials zur Verifizierung durch einen Dritten

Beim Verifizieren von Credentials, etwa wenn die Anlage an einem Anwendungsfall teilnehmen möchte, muss zunächst geprüft werden, ob das vorgelegte Credential korrekt und gültig ist.

Diese Überprüfung übernimmt der Verifier, zum Beispiel der Anbieter eines Anwendungsfalls. Im Rahmen des Verifizierungsprozesses überprüft der Verifier folgende Faktoren:

- Gültigkeit des Credentials
- Kryptografische Integrität des Credentials
- Besitzrechte (Ist die Anlage Eigentümer des Credentials?)
- Inhalt des Credentials
- Aussteller des Credentials

Die Anlage hat die Möglichkeit, über selektive Weitergabe nur einzelne Attribute des Credentials mit dem Verifier zu teilen. Das kann beispielsweise der Fall sein, wenn der Verifier nur Informationen über die Art der Anlage und ihren Standort benötigt. Dann teilt der Inhaber des Credentials nur diese Informationen und nicht das ganze Credential. Das Credential lässt sich in jedem Fall kryptografisch verifizieren.

Über den Credential Hash (Root Hash) lässt sich das auf der Blockchain verankerte Credential nachschlagen, um so den Issuer, die Gültigkeit und die Autorisierung des Credentials durch Dritte zu verifizieren.

In DIVE wird zur Umsetzung von Anmeldefunktionen (z. B. beim Anmelden des Verteilnetzbetreibers beim Attester Service) OpenDID[20] als Verifikationsservice eingesetzt. OpenDID ist ein Service, der den OpenID Connect Flow[21] verwendet und das Anmelden von Nutzern oder Maschinen mithilfe ihrer DID sowie von Credentials ermöglicht, was die Integration in bestehende Prozesse und Anwendungen erleichtert. Er fungiert als Vermittler, der die Kommunikation mit der Wallet der Nutzer oder der Anlage übernimmt, um nach bestimmten Credentials zu fragen und diese dann mithilfe der KILT Blockchain zu verifizieren. Im Erfolgsfall stellt der Service den Nutzern oder der Anlage ein einfaches JWT aus, das von OpenDID selbst signiert wird. Dieses JWT enthält alle Informationen, die vorher aus den angefragten Credentials entnommen werden konnten.

3.1.4 Invalidieren eines Credentials

Die Use-Case-Credentials können nicht nachträglich geändert werden. Bei Änderungen der Eigenschaften muss das bestehende Credential ungültig gemacht und ein neues ausgestellt werden. Das Löschen oder Invalidieren eines Credentials kann durch drei verschiedene Prozesse erfolgen:

- Der Credential-Inhaber löscht das Zertifikat. Der Nachteil an dieser Lösung ist, dass auf das zuverlässige Löschen der Einzelnen gesetzt wird, dies aber nicht durch Dritte verifiziert werden kann.
- Der Aussteller des Zertifikats, der Issuer, invalidiert das Zertifikat auf der Blockchain. Dazu ändert der Issuer den Status des Zertifikats auf der Blockchain von *revoked: false* zu *revoked: true*. Wenn der Verifier nun während des Verifikationsprozesses die Gültigkeit des Zertifikats auf der Blockchain überprüft, sieht er, dass das Zertifikat nicht mehr gültig ist, und wird es aus diesem Grund nicht mehr akzeptieren.
- Eine übergeordnete Instanz (die dem Issuer initial das Recht zur Ausstellung von Credentials erteilt hat), invalidiert das Credential auf der Blockchain. Dies kann zum Beispiel notwendig werden, wenn die Issuer-Instanz fälschlicherweise ein Credential ausgestellt hat.

```
attestation.attestations: Option<AttestationAttestationsAttestationDetails>

{
  ctypeHash: 0x2a63756ff4934eb51d5c405476ea92dfa9413388a8a33c37755442e2111304b5
  attester: 4qGqegcXWctkdLToCSFfBAUQE5V5SBdwivaB6miWgXS6C6Cf
  authorizationId: null
  revoked: true
  deposit: {
    owner: 4qNLGrum9WxGrQkzwEhigiUmkoiYPq5vdzdZnsM25U5RbHu7
    amount: 120,950,000,000,000
  }
}
```

Abbildung 10: Invalidiertes Credential auf der Blockchain

20 https://github.com/KILTprotocol/opendid

21 https://openid.net/developers/how-connect-works/

3.2 Der Blockchain-Ansatz des KILT Protocol

Das KILT Protocol verwendet standardmäßig die KILT Blockchain, um die Konsistenz und Validität der Daten sicherzustellen. Für dieses Projekt wird die öffentliche und dezentrale KILT Blockchain, das sogenannte KILT Spiritnet, eingesetzt.

Öffentliche und dezentrale Blockchain
Öffentlich heißt, dass jeder auf die Blockchain lesend und schreibend zugreifen kann. **Dezentral** bedeutet, dass der Betrieb und die Kontrolle des Netzwerks auf viele unabhängige Teilnehmer verteilt sind. Durch das Fehlen einer zentralen Instanz, die das Blockchain-Netzwerk betreibt, und das Verteilen des Betriebs auf zahlreiche unabhängige Akteure wird das Netzwerk robuster, sicherer und transparenter.

Da dem KILT Protocol eine öffentliche Blockchain zugrunde liegt, können Transaktionen über Blockchain Explorer (vergleichbar mit Suchmaschinen für Blockchains) nachvollzogen werden.[22]

Betrieben wird das KILT Spiritnet durch ein Netzwerk von den sogenannten Collators. Collators sind Knoten (Nodes), die Transaktionen sammeln, wie zum Beispiel das Ausstellen von Credentials (die Transaktion auf der Blockchain, nicht das Credential selbst!), und sie zu Blöcken bündeln. Eine weitere Art von Nodes sind die RPC-Nodes, die Remote-Procedure-Call-Schnittstellen bereitstellen. Über die RPC-Schnittstelle können Applikationen mit der Blockchain interagieren. Applikationen senden Anfragen an den RPC-Knoten, um etwa den Zustand der Blockchain abzufragen oder um Transaktionen zu senden.

Die Nutzung des KILT Spiritnet hat den Vorteil, dass die Skalierbarkeit dadurch gegeben ist. Es gibt eine Vielzahl von Collators, darunter auch Organisationen (z. B., Dotters Network und die BOTLabs GmbH), die Blockchain-Knoten betreiben.[23] Bei einer zukünftigen, breiten Einführung der Self-Sovereign Identities in der Energiewirtschaft empfiehlt es sich für Unternehmen und Organisationen, die Credentials ausstellen oder Anwendungsfälle anbieten wollen, optional eigene RPC Nodes zu betreiben – sofern für die Umsetzung eine Blockchain als Verifiable Data Registry zum Einsatz kommt.[24] Die Liste der Collators und RPC-Nodes ist öffentlich und kann durch jeden eingesehen werden.[25]

In einer Transaktion sieht man im Blockchain Explorer folgende Informationen[26]:

- **Timestamp:** Zeitstempel über den Zeitpunkt der Transaktion
- **Block Time:** Wann wurde der Block erstellt, in dem sich die Transaktion befindet?
- **Block:** Status des Blocks (*Finalized*, das heißt, es handelt sich um einen gültigen Block) und die Blocknummer
- **Life Time:** Legt fest, wie lange die Transaktion in einem Block hinzugefügt werden kann, bis sie ungültig wird
- **Extrinsic Hash:** Hash des Extrinsic[27]
- **Action:** Art der Transaktion
- **Sender:** Absender der Transaktion
- **Estimated Fee & Used Fee:** Geschätzte und tatsächliche Transaktionskosten
- **Nonce:** Stellt sicher, dass die gleiche Transaktion nicht mehrmals ausgeführt werden kann
- **Result:** Status, zum Beispiel *Success* für eine erfolgreiche oder *Failed* für eine fehlgeschlagene Transaktion
- **Parameters:** Inhaltliche Angaben zur Transaktion
- **Signature:** Signatur des Übermittlers der Transaktion (des Bezahlers der Transaktion)

22 https://spiritnet.subscan.io/ oder https://polkadot.js.org/apps/?rpc=wss%3A%2F%2Fspiritnet.kilt.io%2F#/explorer
23 Diese Liste der Collators verändert sich über die Zeit, wenn neue Collators hinzukommen und bestehende Collators ausscheiden.
24 https://docs.kilt.io/docs/develop/chain/fullnode-setup
25 https://telemetry.kilt.io/#list/0x411f057b9107718c9624d6aa4a3f23c165389829 7f3d4d529d9bb6511a39dd21
26 https://spiritnet.subscan.io/extrinsic/7023937-2
27 Extrinsics sind alle Befehle oder Daten, die in einem Block aufgenommen werden müssen.

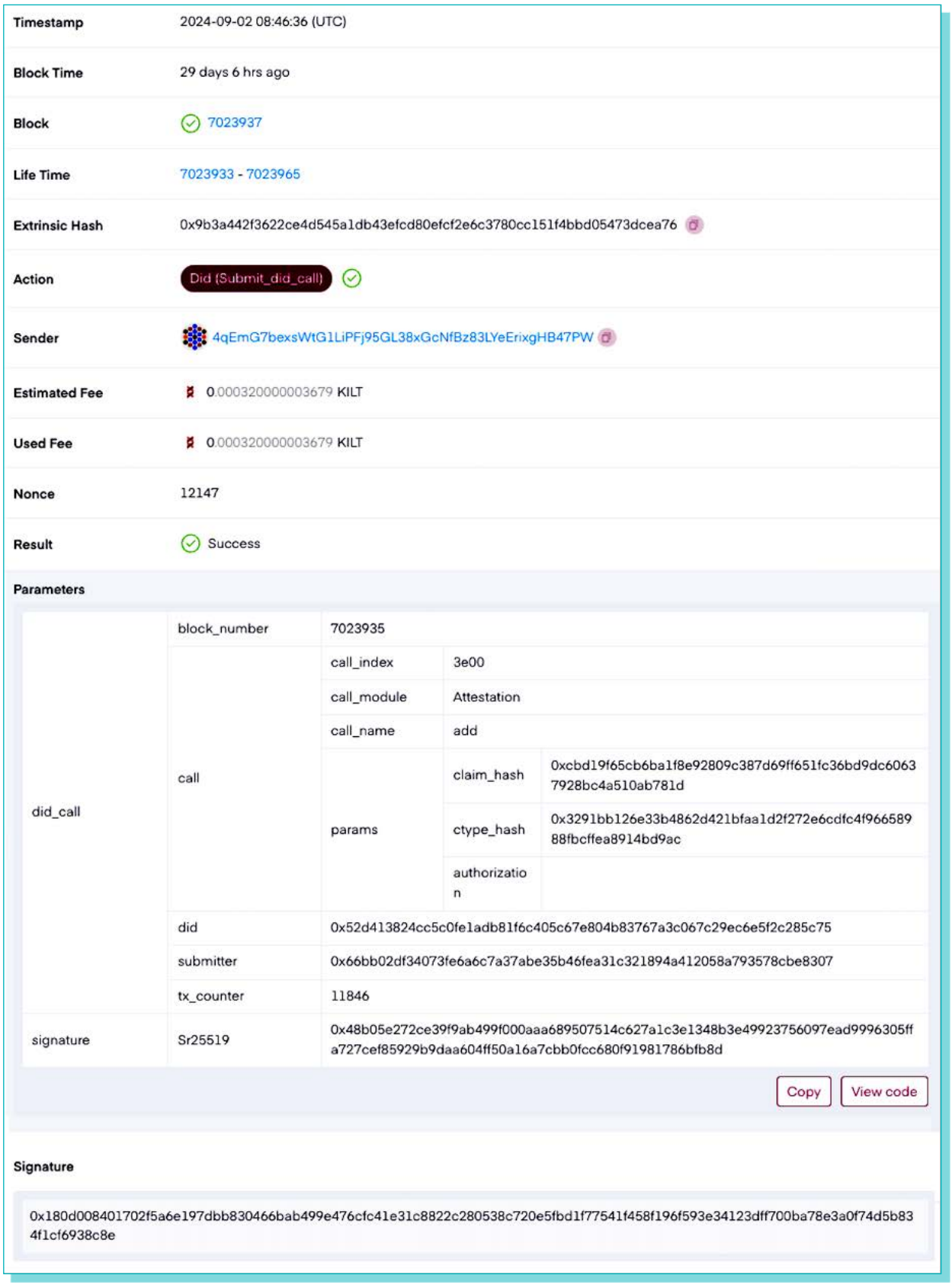

Abbildung 11: Transaktion auf der KILT Blockchain[28]

28 https://spiritnet.subscan.io/extrinsic/0x9b3a442f3622ce4d545a1db43efcd80efcf2e6c3780cc151f4bbd05473dcea76

In einem Block finden sich folgende Informationen[29]:

- **Timestamp:** Zu welchem Zeitpunkt wurde der Block geschrieben?
- **Block Time:** Wie lange ist die Blockerstellung her?
- **Status:** Status des Blocks, zum Beispiel *Finalized* oder *Unfinalized*
- **Hash:** Hash des Blocks
- **Parent Hash:** Hash des vorherigen Blocks
- **State Root:** Merkle Root[30] der gesamten Blockchain. Dadurch wird der Zustand der gesamten Blockchain in einem Hash dargestellt.
- **Extrinsics Root:** Alle Transaktionen dieses Blocks werden in einem Merkle Root dargestellt.
- **Validator:** Collator der Relay Chain[31], der den Block validiert hat
- **Spec Version:** Momentane Runtime-Version[32]

Abbildung 12: Block auf der KILT Blockchain

29 https://spiritnet.subscan.io/block/7023937

30 Ein Merkle Root ist ein kryptografischer Hash-Wert, der die Integrität und Konsistenz einer großen Menge von Daten sicherstellt.

31 Die Polkadot Relay Chain stellt die Sicherheit und den Konsens für das gesamte Netzwerk sicher.

32 Die Runtime ist der Teil der KILT Blockchain, der die Regeln und die Logik bestimmt, nach denen diese Blockchain funktioniert.

Bei einer öffentlichen Blockchain müssen sich die Teilnehmer nicht untereinander vertrauen. Das System ist offen gestaltet, sodass auch neue Mitglieder hinzukommen können, die nicht notwendigerweise das Vertrauen der anderen Teilnehmer genießen. Das Vertrauen wird durch die mathematische Wahrheit ersetzt, sodass Teilnehmer in einer „vertrauenslosen" Umgebung miteinander interagieren können. Um diese mathematische Wahrheit zu generieren, verwendet die KILT Blockchain ein zweistufiges Konzept. Vereinfacht dargestellt, sammeln die Blockchain-Knoten, die Nodes oder Collators, die Transaktionen und Schreibzugriffe auf der Blockchain, zum Beispiel das Ausstellen von Credentials, von allen Akteuren im System ein und verdichten sie zu einem Block. Jeder einzelne Block wird dann durch ein unabhängiges externes System auditiert und auf seine Konsistenz zum letzten finalisierten Block hin überprüft. Wenn dieses Audit erfolgreich war, hängen alle Collators den Block als finalisierten Block an die KILT Blockchain an. Dabei lassen sich über die auf der Blockchain gespeicherten Daten keine Rückschlüsse auf die Akteure und die Art der Daten ziehen, da sie nur als Hashes auf der Blockchain gespeichert werden.

Für das externe Audit nutzt KILT das System des Polkadot-Netzwerks. Polkadot verwendet neben dem Proof-of-Stake-Mechanismus[33] das sogenannte Relay-Chain-Verfahren. Dabei wird die benötigte Rechenleistung für die Validierung eines Blocks effizienter auf einzelne Chains, sogenannte Parachains, verteilt. Ziel ist es, die Transaktionskosten möglichst gering zu halten und eine Skalierbarkeit zu ermöglichen. Im Unterschied zu den klassischen Single-Chain-Methoden, bei denen das gesamte Netzwerk um die begrenzte Datenkapazität des nächsten Blocks konkurriert, wird im Relay-Chain-Verfahren die zentrale Relay Chain lediglich für die Bereitstellung der Sicherheit genutzt. Die einzelnen Parachains übernehmen dedizierte Aufgaben. So behandelt KILT ausschließlich die Thematik DIDs und Verifiable Credentials, während andere Parachains andere Aufgaben übernehmen. Transaktionen auf der KILT Blockchain konkurrieren in diesem Fall also nur noch mit anderen DID- und VC-Anfragen, wodurch der Durchsatz sehr hoch und der Transaktionspreis dauerhaft niedrig gehalten wird.

Das Whitepaper zur Polkadot Relay Chain wurde 2016 veröffentlicht, der Genesis-Block wurde im Mai 2020 bereitgestellt. Seit 2023 existiert eine 1.0.0-Version. Damit ist das Relay-Chain-Verfahren noch am Anfang seiner Entwicklung. Bei erfolgreicher Weiterentwicklung bietet es Skalier- und Planbarkeit für industrielle Anwendungen bei allen Vorteilen, die die Verwendung einer public-permissionless Blockchain bietet.

3.3 Privacy by Design und Datenschutz

Datenschutz und Privacy by Design sind essenziell, um die Sicherheit und Privatsphäre der Nutzer zu gewährleisten und Missbrauch zu verhindern. Ziel ist es, die Daten der Nutzer und Geräte vor unbefugtem Zugriff zu schützen und ihnen die Kontrolle über ihre eigenen Informationen zu geben. Personenbezogene Daten werden daher nur lokal und nur soweit notwendig erfasst.

Privacy-by-Design-Konzept
Die **Systematik** hinter diesem **Privacy-by-Design-Konzept** ist, dass der Nutzer in der **Blockchain** selbst auf die Infrastruktur zugreift, die für Blockchain-Adressen und DIDs angelegt wurde.

Der **Nutzer nutzt diese Infrastruktur** ähnlich wie jemand, der an eine bestehende Adresse zieht und dort ein Haus baut. In der Blockchain werden diese Adressen und DIDs – ähnlich wie Adressen in Google Maps – unabhängig von der konkreten Person, die sie benutzt, vorgehalten.

Die **Blockchain sammelt** also **keine Daten**, die einen Bezug zu einer Person haben. Stattdessen sind lediglich **Möglichkeiten für Adressen und DIDs implementiert** und der Nutzer kann sich eine dieser Möglichkeiten selbst erschließen.

Der Privacy-by-Design-Ansatz stellt sich in der konkreten Anwendung der Infrastruktur, wie sie im Rahmen des DIVE-Projekts aufgebaut wurde, wie folgt dar:

Geräte-ID
Der Nutzer erstellt eine Wallet-Adresse, die nicht öffentlich mit ihm verknüpft ist, und dazu eine Geräte-DID, die weder öffentlich mit ihm noch mit der Adresse verknüpft ist. Die Adresse und die DID sind in der Blockchain gespeichert. Sollte aus irgendeinem Grund ein Bezug zwischen der Person und der Adresse und/oder der DID öffentlich entstehen, kann der Nutzer jederzeit eine neue Adresse und eine neue DID erstellen.

Nutzer-ID und Credentials
Der Nutzer erstellt für sich eine Nutzer-DID, genauso wie oben für die Geräte-ID beschrieben. Mit Bezug auf diese Nutzer-ID interagiert er mit dem Betreiber off-chain, um sich ein Credential attestieren zu lassen, das heißt, die für das Credential benötigten Daten werden ausgetauscht (z. B. über eine Website oder per E-Mail). Der Issuer signiert nach Überprüfung der Daten das Credential, schreibt ausschließlich den entsprechenden Hash des Credentials auf die Blockchain und überträgt das Credential an den Nutzer. Dieser kann es fortan in seiner Wallet aufbewahren und allein entscheiden, wem er es zeigen möchte und wem nicht.

33 Beim Proof of Stake wird bei der Berechnung des nächsten Blocks über hinterlegte Geldwerte ermittelt, wer den nächsten Block kreieren darf. Es wird auf das Eigeninteresse der Stakeholder gesetzt, die Chain stabil und korrekt zu halten. Die Stakes bei Polkadot liegen derzeit im Milliarden-Euro-Bereich, was einen erfolgreichen Angriff sehr teuer und damit unwahrscheinlich macht.

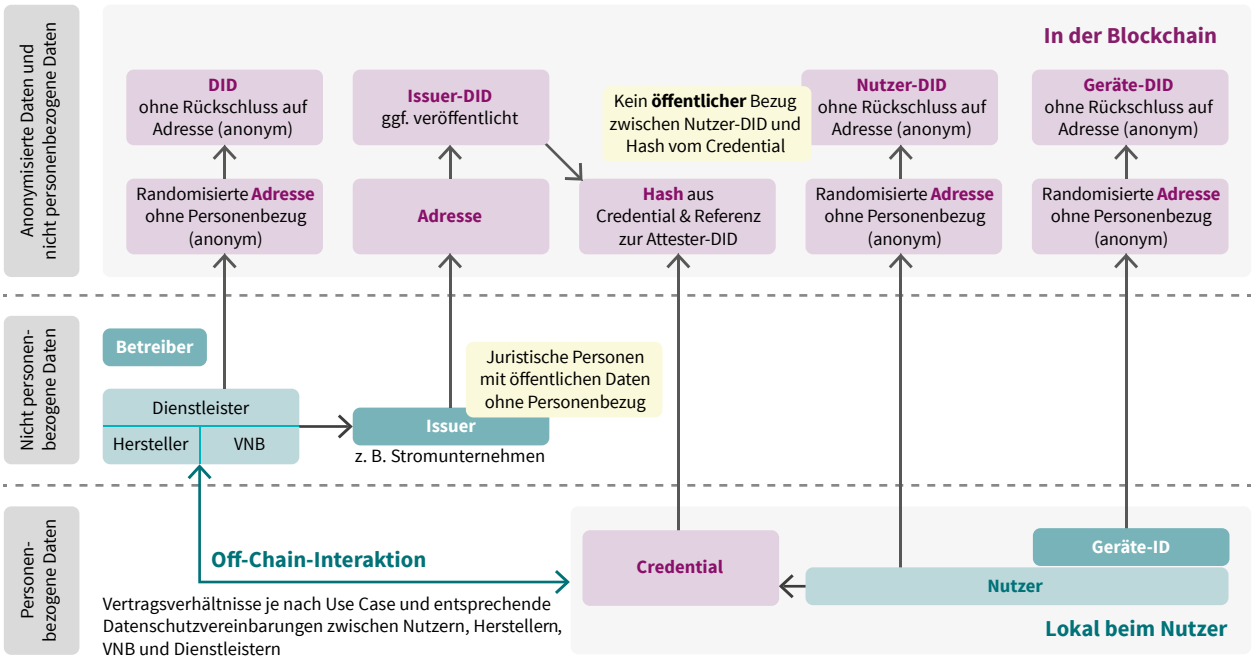

Abbildung 13: Daten in der Blockchain

Zur Verifizierung des Issuers wird ebenfalls eine DID genutzt. Typischerweise sind Issuer juristische Personen, sodass ihre DID jeweils öffentlich einsehbar gemacht werden kann, ohne dass dadurch datenschutzrechtliche Probleme entstehen.

Wie Abbildung 13 zeigt, verbleiben die DIDs immer beim jeweiligen Nutzer, ebenso die Credentials.

Der Austausch von personenbezogenen Daten erfolgt off-chain und unterliegt den üblichen Datenschutzanforderungen (Auftragsdatenschutzvereinbarung sowie Recht auf Einsicht, Löschung etc.). Lediglich ein Hash (eine durch einen Algorithmus generierte Zeichenfolge) des Credentials samt Referenz zum Issuer wird auf der Blockchain gespeichert. Der Hash ist den Daten eindeutig zuordenbar, ohne dass eine Rückrechnung der Daten möglich ist. Einem Außenstehenden ist nicht ersichtlich, worauf der Hash sich bezieht oder aus welchen Daten er erzeugt wurde. Der Hash auf der Blockchain gibt also einerseits keine personenbezogenen Daten preis und da der Hash nicht aus einzelnen personenbezogenen Daten, sondern aus dem gesamten Credential gewonnen wird, handelt es sich auch nicht um pseudonymisierte Daten. Selbst wenn jemandem die Daten einer Person bekannt sind, kann er ohne das Credential nicht den entsprechenden Hash errechnen oder erraten. Nur wenn das Credential jemandem offengelegt wird, kann derjenige damit denselben Hash generieren und die Blockchain danach durchsuchen. Somit kann ein Vertragspartner des Nutzers, dem das Credential samt Informationen über den Issuer (off-chain) vorgelegt wird, verifizieren, dass der Inhalt des Credentials und der Bezug zur konkreten Nutzer-ID unverändert sind, dass der Issuer dies tatsächlich bestätigt hat und dass das Credential noch valide ist. Für die Überprüfung der Echtheit, Integrität und Gültigkeit des Credentials verwendet ein Verifier lediglich die Look-up-Funktion der Blockchain. Dabei werden die öffentlichen Daten der Blockchain durchsucht; der Vorgang selbst wird auf der Blockchain nicht dokumentiert, sodass niemand sehen kann, wie oft oder von wem ein Credential überprüft wird.

Auf der Blockchain befinden sich keinerlei Daten über all diese Vorgänge – nur die jeweiligen KILT-Adressen und DIDs der unterschiedlichen Akteure und Geräte sowie die Hashes von ihren Credentials sind auf der Blockchain gespeichert, jedoch auch sie sind nicht öffentlich miteinander verknüpft.

Ob eine KILT-Adresse, eine DID oder ein Hash von einem Credential aus diesem Projekt stammt oder von anderen Akteuren generiert wurde, ist ebenfalls nicht einsehbar.

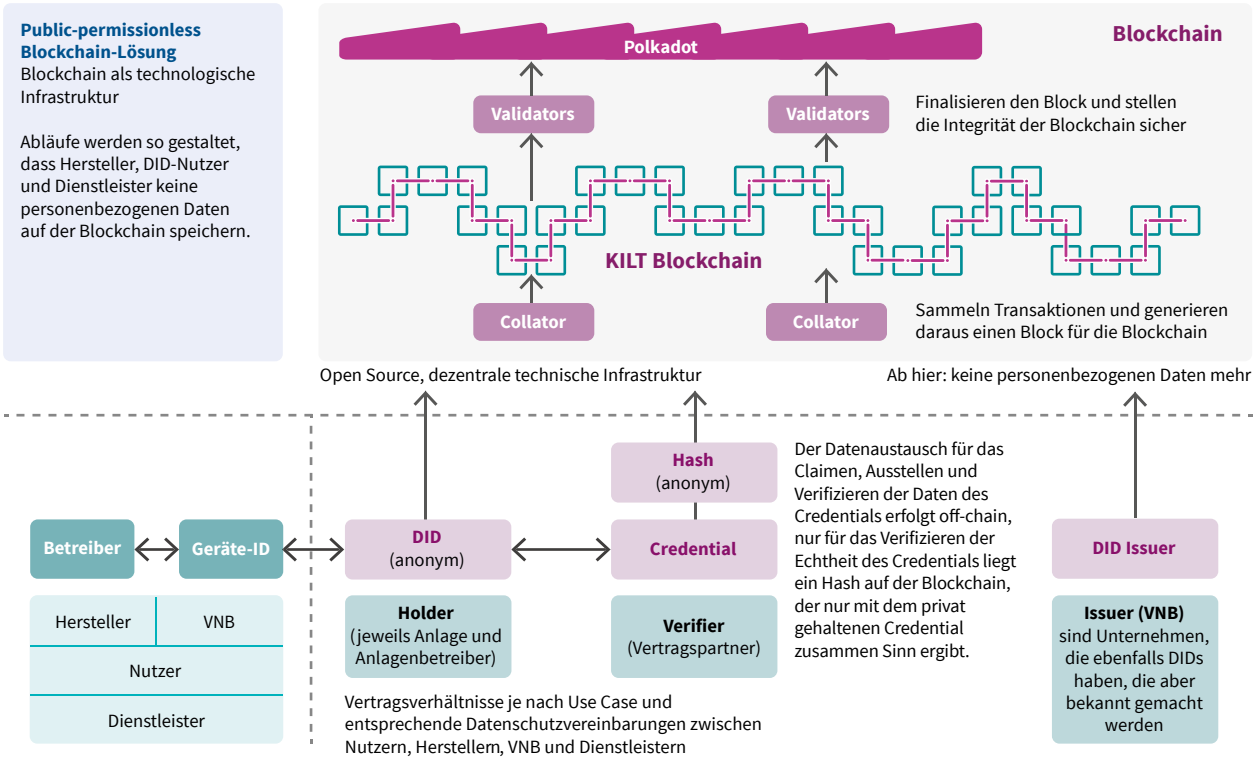

Abbildung 14: Übersicht aus der Privacy-by-Design-Perspektive

4. Die Umsetzung energiewirtschaftlicher Prozesse unter Nutzung der Self-Sovereign Identity und der Identitätsinfrastruktur

Um die in den vorherigen Kapiteln beschriebenen Konzepte von Self-Sovereign Identities einzusetzen, wurden bereits bestehende Applikationen und Services auf Basis des KILT Protocol zu einem Gesamtsystem zusammengeführt. In diese Systemarchitektur wurde mittels der OLI Box[34] ein **Energiemanagementsystem** (EMS) eingebunden, das befähigt wurde, **Self-Sovereign Identities anzulegen, zu verwalten und über sie zu kommunizieren**. Hierzu wurde im DIVE-Projekt Software, inklusive eines User Interface, entwickelt. Neben der technischen Integration der einzelnen Komponenten wurde ein energiewirtschaftlicher Prozess – die Inbetriebnahme von Energieerzeugungsanlagen und die Registrierung der Anlagenbetreiber – umgesetzt. Die Energieanlage interagiert in den nachfolgend beschriebenen Prozessen jeweils mit der OLI Box.

4.1 Die eingesetzten Basiskomponenten des Energiemanagementsystems und des intelligenten Messsystems

Für die Anwendung von digitalen Identitäten im Energiesystem sind einige Hardware- und Softwarekomponenten notwendig. In diesem Kapitel werden die im Rahmen von DIVE verwendeten Komponenten vorgestellt. Sie umfassen

- Hardware (insbesondere das EMS)
- Software für die Kommunikation mit den Anlagen[35]
- das Zählerwesen
- die Backend-Komponenten

Die verschiedenen Komponenten sind in Abbildung 15 in ihrer Gesamtheit aufgezeigt und werden nachfolgend näher beschrieben.

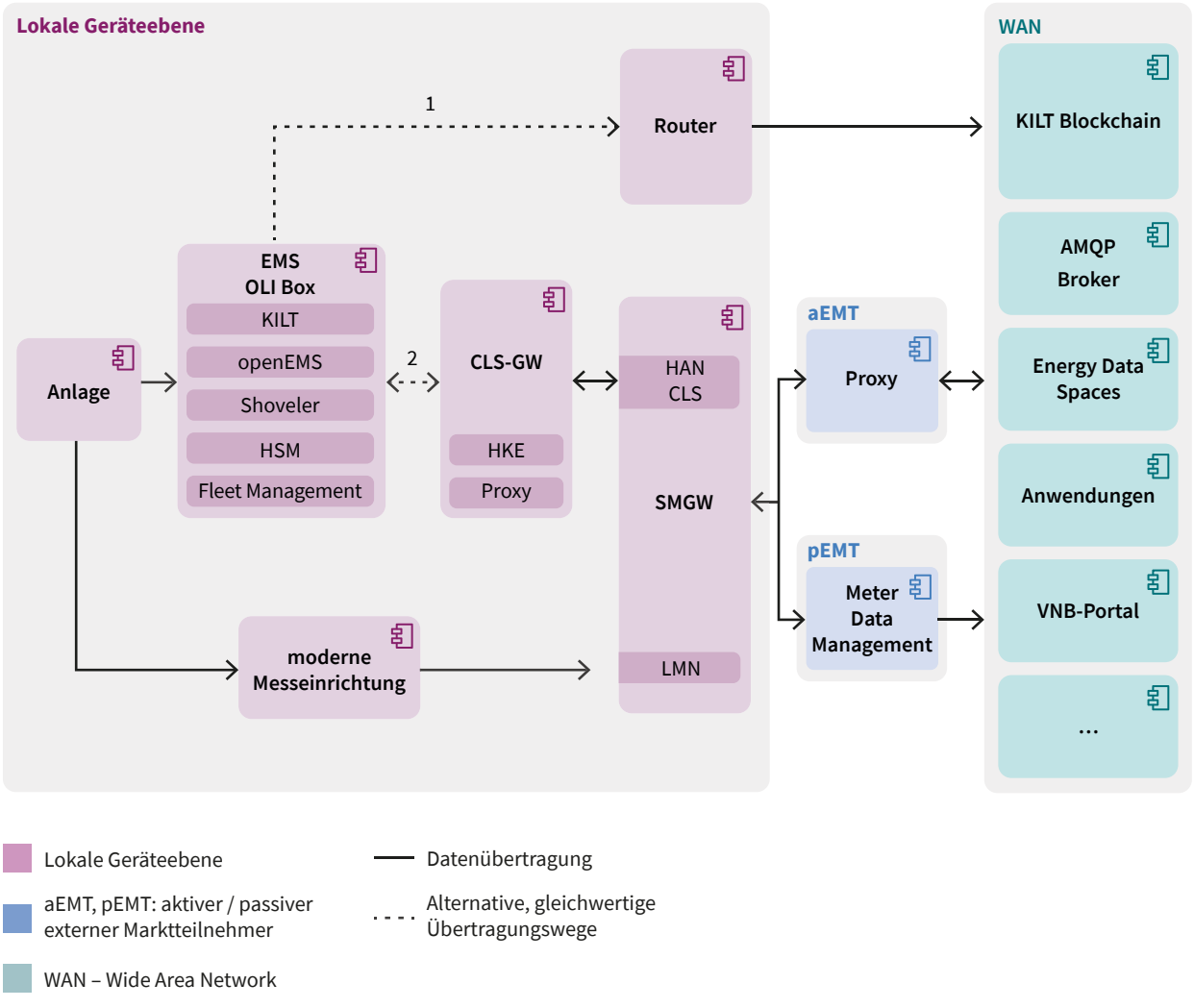

Abbildung 15: Technische Systemarchitektur von DIVE

34 https://www.my-oli.com/

35 Siehe auch Glossar. Bei Anlagen handelt es sich in DIVE um Wechselrichter, Wallboxen, Wärmepumpen und Speicher.

4.1.1 (Heim-)Energiemanagementsysteme ((H)EMS)

Ein (Heim-)Energiemanagementsystem ((H)EMS) ist als Komponente für den optimierten Einsatz und die Visualisierung der Daten von Energieanlagen und Verbrauchern in Ein- und Mehrfamilienhäusern, Liegenschaften und Gewerben sowohl im Bestand als auch im Neubau ein wichtiger Baustein.

Der Markt hat in den vergangenen Jahren verschiedenste Typen und Bauformen hervorgebracht, unter anderem Geräte, deren EMS auf der Cloud liegen, und solche, die über auf der lokalen Hardware installierte EMS verfügen. Für die Zwecke von DIVE wurde der Fokus vor allem auf EMS gelegt, die auf lokal installierter Hardware eingesetzt werden. Gründe dafür sind einerseits die Komplexität der Anwendungsfälle, die ein Mindestmaß an Flexibilität erfordert, und andererseits die (Sicherheits-)Prinzipien der Dezentralität und Selbstverwaltung. Generell bieten große Hersteller verschiedenster Energieanlagen mittlerweile ihr eigenes (H)EMS an. Die Kompatibilität zwischen EMS und Anlage ist dabei bei herstellereigenen Systemen de facto sichergestellt. Die Integration weiterer Hersteller ist durch die Nutzung gemeinsamer Standards wie SunSpec, EEBus oder weiterer Protokolle und Technologien möglich. Neben kommerziellen EMS gibt es auch frei verfügbare Software-Stacks (z. B. das openEMS), die durch eine immer größer werdende Liste an unterstützten Geräten eine gute Basis für Eigenentwicklungen parallel zu kommerziellen Lösungen darstellen.

Folgende Eigenschaften von EMS wurden als notwendige Voraussetzungen für DIVE definiert:

- Das EMS hat eine **eigene Hardwareeinheit** bzw. ist auf einer zentralen Anlage aufgespielt (z. B. Wechselrichter).
- Die wichtigsten Funktionen des EMS wie das Aggregieren der Daten (wie Momentan- und historische Werte für Bedarf und Lieferung von Energie sowie weitere Betriebsinformationen), ihre Verarbeitung und die Steuerbefehle werden **lokal durchgeführt und nicht an eine Cloud ausgelagert**.
- Das EMS bietet prinzipiell die Möglichkeit – mit Unterstützung des Herstellers –, die vorhandene Software um die in DIVE entwickelten **Softwarekomponenten und -prozesse zu erweitern**.
- Auf der EMS-Hardwareeinheit bzw. auf einer angeschlossenen Komponente (in DIVE: CLS-Gateway) kommt ein HAN-Kommunikationsadapter zum Einsatz, der die **lokale Kommunikation mit dem SMGW ermöglicht**.

In den Feldtests von DIVE wurde die von OLI Systems entwickelte OLI Box genutzt und steht stellvertretend für alle EMS, die obige Eigenschaften erfüllen. Bei der OLI Box handelt es sich um eine auf einem Raspberry Pi 3B basierende EMS-Plattform, die unter anderem openEMS nutzt, um Daten von verschiedenen Energieanlagen zu beziehen. Neben Stammdaten der Anlage sind auch Bewegungsdaten in einer lokalen Datenbank gespeichert. Die OLI Box kann als HEMS mit beliebiger weiterer Software ausgestattet werden, solange die Limitationen hinsichtlich der Hardwareleistung nicht überschritten werden. Ein Fernzugriff ist mit Fleet Management ebenfalls möglich, was insbesondere im Rapid Prototyping schnelle Fortschritte ermöglicht.

4.1.2 Intelligentes Messsystem

Das intelligente Messsystem (iMSys) ist eine zentrale Komponente im digitalen Energiesystem und in der DIVE-Infrastruktur (dena 2024). Für DIVE wird das iMSys als technische Komponente bzw. Baustein klassifiziert und aktiv in die Prozesse eingebunden. Zwei besondere Funktionalitäten des iMSys sind für digitale Identitäten sehr nützlich:

- Die Beschaffung von abrechnungsrelevanten Messwerten aus modernen Messeinrichtungen (mME) mit Signaturen in **viertelstündlicher Auflösung** bei Nutzung des Tarifanwendungsfalles TAF 7 (Zählerstandsgangmessung)
- Die Bereitstellung einer **Kommunikationsstrecke über die Smart Meter Public Key Infrastructure** (SM-PKI) per transparentem Kanal (CLS), wodurch prinzipiell ein anderes WAN per Betreiber-Router oder eigenem LTE-Modul überflüssig wird

Die in DIVE verwendeten iMSys wurden von PPC und robotron in der Form von Testkits bereitgestellt und stehen exemplarisch für alle Messsysteme, die obige Funktionen aufweisen. Neben der Hardware sind auch die notwendigen Systeme für die Rolle des aktiven bzw. passiven externen Marktteilnehmers (aEMT bzw. pEMT) im Backend vorhanden. Der transparente Übertragungskanal wird im nächsten Kapitel weiter beschrieben.

4.1.3 Kommunikation und Datenverarbeitung

Um für die Kommunikation zwischen Anlagen und EMS einerseits und den Anwendungen auf der anderen Seite eine Verknüpfung herzustellen, sind einige Komponenten notwendig (vgl. Abbildung 15):

- Eine oder mehrere Datenbanken, Datendrehscheiben, Energy Data Spaces oder Message Broker als vordefiniertes **Übertragungsziel** für statische und dynamische Daten und Informationen
- Robuste, modulare und flexible **Kommunikationsstrecken** über Heim-Router, LTE-Router oder das intelligente Messsystem
- **Software**, die die obigen Komponenten nutzt und EMS-Daten an die Anwendungen versendet

Die meisten EMS sind verpflichtend oder optional mit einer zentralen Hersteller-Cloud verbunden. Dadurch lassen sich Bewegungs-, Stamm- und betriebliche Daten per Edge Cloud (also von der Anlage hin zu den Anwendungen) transportieren. Dies kann

große Vorteile mit sich bringen, wie zum Beispiel die Sicherung von Daten außerhalb der eigenen vier Wände, den Fernzugriff von unterwegs und die Aktualisierung der Software per OTA-Updates (Over the Air), um Sicherheitslücken zu schließen und die verfügbaren Features zu erweitern. Nachteilig ist allerdings die existierende Abhängigkeit von der Hersteller-Cloud sowie die sich dadurch potenziell öffnenden Angriffsvektoren. Für DIVE wird von ausschließlich lokal und damit dezentral funktionierenden EMS ausgegangen, daher müssen die Daten erst in die Cloud transportiert werden.

Die Verbindung des EMS mit den in der Cloud befindlichen Anwendungen findet über verschiedene Transportwege statt. Neben dem Kunden- bzw. Betreiber-WAN (per Router und Internetverbindung über Glasfaser, Kabel, DSL oder LTE) steht auch ein per PKI gesicherter CLS-Kanal über das Smart Meter Gateway zur Verfügung. Er ist verpflichtend zu nutzen, wenn es sich bei den zu übertragenden Informationen um „energiewirtschaftlich relevante Daten“ (ERD) handelt. Darunter gefasst werden abrechnungsrelevante bzw. zur Bilanzierung notwendige Messwerte sowie Steuersignale mit Auswirkungen auf das Stromnetz. Daten, die nicht in diesen Bereich einzuordnen sind, werden als „betriebliche Daten“ bezeichnet und sind nicht verpflichtend über das SMGW zu übertragen.[36]

Darüber hinaus ist es den Anwendungsbetreibern überlassen, welche Daten wie genutzt werden.[37] Für DIVE wurde ein zweigleisiger Ansatz gewählt, um die mögliche Vielfalt der Anforderungen an die Transportwege abzudecken:

- Zum einen besteht die Möglichkeit, per Tarifanwendungsfall 7 (TAF 7) viertelstündliche Messwerte aus dem iMSys am Netzanschlusspunkt bzw. an der Anlage, falls die mME nur eine bestimmte Anlage misst, zu beziehen. Hierbei handelt es sich um eine konforme Übertragung von ERD. Für Abrechnungs- und Bilanzierungsvorgänge wird stets auf diese Datenreihen zurückgegriffen.
- Parallel findet auch eine Übertragung der aufkommenden betrieblichen Daten aus dem EMS an die Cloud statt. Hier ist sowohl die Übertragung per Betreiber-WAN als auch per SMGW möglich. Der in Abbildung 15 in der Komponente „EMS“ abgebildete Shoveler leitet diese Daten zu den Anwendungen weiter.

Für die Kommunikation zwischen Anlage und angeschlossener Hardware und den jeweiligen Anwendungen braucht es einen oder mehrere sogenannte Endpunkte, an dem Daten gesammelt, bereitgestellt und weitergeleitet werden können. Die Datenübertragung sollte zudem in Echtzeit oder echtzeitnah erfolgen, um die steigenden Flexibilitätsanforderungen des Energiemarktes zu erfüllen. Das DIVE-Projekt hat sich hierbei für das **Advanced Message Queuing Protocol (AMQP)** entschieden.[38] AMQP ist ein Nachrichtenübertragungs-Protokoll, das in verschiedenen Technologien bzw. Frameworks frei verfügbar ist und im Energiesektor verstärkt genutzt wird. Eine grafische Darstellung über die Zusammenhänge zwischen Rollen und technischen Komponenten findet sich in Abbildung 16:

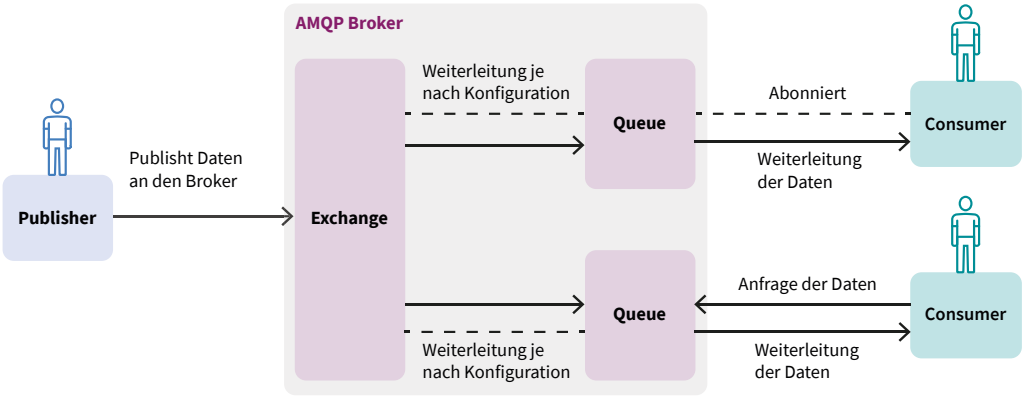

Abbildung 16: Aufbau des Advanced Message Queuing Protocol (AMQP) und Darstellung der Rollen (Lee 2024)

In AMQP kommt, ähnlich wie in anderen Protokollen, ein Publisher/Consumer/Broker-Paradigma[39] zum Einsatz. Die Besonderheit von AMQP ist, dass die Kommunikation mit Exchanges und Queues stärker differenziert wird, mit dem Ziel, Zugriffsrechte im industriellen Kontext einfacher zu gestalten.

Bei dem Broker handelt es sich um eine in der Cloud befindliche Softwarekomponente in der Domäne eines Energieserviceanbieters (ESA). Messages aus dem Publisher werden darauf abgelegt. Im Projektkontext agieren sowohl die EMS mit den betrieblichen

36 Zum Beispiel telemetrische Informationen zu den Anlagen und EMS wie „Alive-Signal“, Software-Updates, Fehlermeldungen usw. sowie Daten aus Sensoren wie der „State of Charge“ von Batterien für Visualisierungs- und Prognosezwecke

37 Beispielsweise kann ein Zwischenmesswert aus dem Bereich der betrieblichen Daten Mehrwerte für den Anwendungsfall mit sich bringen und entsprechend eingesetzt werden.

38 Vergleichbar mit AMQP ist das insbesondere im Smart-Home- und Telemetrie-Bereich weit verbreitete MQTT-Protokoll (Message Queuing Telemetry Transport). Der genutzte Stack im Projekt DIVE stammt von RabbitMQ.

39 Ähnlich wie das Client/Server-Paradigma verfolgt das Publisher/Consumer/Broker-Paradigma eine Rollenaufteilung in Bezug darauf, wer Daten schreibt, persistiert und konsumiert bzw. bezieht.

Daten als auch die Meter-Data-Management-Systeme mit den ERD aus TAF 7 von robotron als Publisher.

Als Consumer agieren die Anwendungen. Ein AMQP Broker hat nicht den Zweck, Daten zu persistieren. Stattdessen handelt es sich um eine Art „Zwischenstation". Ein Persistieren bzw. die weitere Verarbeitung finden in anderen Domänen anwendungsspezifisch statt.

In einem Produktivszenario der DIVE-Basisinfrastruktur ist davon auszugehen, dass nur vorab freigeschaltete Unternehmen Zugriff auf einen Broker erhalten. Es wird damit gerechnet, dass in einem Produktivsystem eine Vielzahl an (anwendungsspezifischen) Brokern entstehen würden, um ein Load Balancing (Lastverteilung)[40] sicherzustellen und gegebenenfalls Hierarchien zwischen Netzbetreibern, Energieversorgern und Energieserviceanbietern abbilden zu können. Offene Fragestellungen, die allerdings derzeit in Projekten rund um Datendrehscheiben und Energy Data Spaces bereits aktiv untersucht werden, sind die der passenden Betreibermodelle[41] und der Vermeidung von Silobildung.

4.1.4 Diskussion: Kryptografie, Hardware Secure Module und Krypto-Chip

In der DIVE-Basisinfrastruktur kann jedes EMS und damit jede Anlage mittels einer offenen PKI selbst Schlüsselpaare erstellen, signieren und weiterleiten. Um dabei Sicherheitsanforderungen und gängige Standards der Kryptografie zu erfüllen, werden folgende Funktionen für DIVE benötigt:

- Erstellung eines Schlüsselpaars mit bestimmten **kryptografischen Kurven**[42] **unter hoher Entropie**
- Speichern und Sichern des Schlüsselpaars bzw. des privaten Schlüssels in einer **abgeschlossenen Umgebung**, wodurch sichergestellt ist, dass sich nur bestimmte Software und bestimmte Nutzer Zugriff verschaffen können
- Zugriff auf das Schlüsselpaar gewähren per **lokaler, im Zugriff und Umfang streng restriktiver API (Application Programming Interface, Programmierschnittstelle)**, damit nur bestimmte Software die Schlüsselpaare nutzen kann

Prinzipiell sind diese Funktionen sowohl per Software[43] als auch mit zusätzlicher Hardware, die in dem EMS verbaut wird[44], umsetzbar. Viele EMS und auch Anlagen wie Wechselrichter besitzen bereits derartige Hardwarebausteine mit begrenztem Funktionsumfang.

Auf dem Markt sind eine Vielzahl an Hardware Secure Modules (HSM) für unterschiedliche Einsatzzwecke verfügbar. Unterschiede ergeben sich unter anderem durch

- die unterstützten kryptografischen Primitiven, Funktionen und Kurven
- die Bauform (als Chip direkt auf einem PCB (Printed Circuit Board) installiert oder als Aufsatz- bzw. Aufsteckmodul)
- den Preis pro Einheit (von wenigen Euro bis hin zu Kosten von über 1.000 Euro pro Stück)
- die Anzahl an Speicherplätzen (Slots) für Schlüsselpaare und weitere Parameter technischer Natur
- die Verfügbarkeit eines „Tamper Proofing", wodurch bei unsachgemäßer Behandlung bzw. Beschädigung des Geräts (z. B. unerlaubtes Öffnen) das Schlüsselpaar zerstört wird

Da die DIVE-Basisinfrastruktur für die Verankerung der Identitäten das KILT Protocol nutzt, das wiederum auf Substraten von Polkadot basiert, ist eine Unterstützung der ed25519-Kurve für die kryptografischen Prozesse wichtig. Die Wahl für das Test-HSM fiel deshalb auf das HSM6 des Herstellers Zymbit, das die wichtigsten Funktionen bereitstellt.[45]

Der Einsatz eines Hardware Secure Module muss allerdings nicht unbedingt für alle Einsatzzwecke und Installationsarten erfolgen, sollten wirtschaftliche bzw. organisatorische Faktoren dagegensprechen. Für größere Anlagen sind zusätzliche Kosten für ein HSM leichter zu decken als für Kleinanlagen und der wirtschaftliche Schaden durch eine eventuelle Attacke ist auch dementsprechend größer. Mit ausreichender Nutzung bei in der Industrie üblichen Best Practices ist ein Einsatz der DIVE-Basisinfrastruktur auch ohne HSM in einer Produktivumgebung möglich.

Dabei darf nicht außer Acht gelassen werden, dass ein Angreifer prinzipiell in einem ausreichend dezentralen System keinen Single Point of Failure bzw. keinen kritischen Angriffsvektor vorfinden kann, sondern einen Angriff auf verschiedene Systemkomponenten parallel durchführen müsste, um ausreichend Schaden anzurichten. Ein Angriff auf ein einzelnes EMS kann Schäden verursachen (z. B. Denial of Service für einzelne Anlagen oder Entwendung der privaten Schlüssel), würde jedoch das Gesamtsystem unberührt lassen. In jedem Falle ist hier, wie auch bei zentralen Systemen, ein Recovery-Prozess zu definieren.

40 Load Balancing soll sicherstellen, dass die Last in einem IT-System optimiert verteilt und somit eine Skalierung sichergestellt wird.

41 https://energydataspaces.eu/; https://www.cines.fraunhofer.de/de/angebot/Digitalisierung/Dataspace.html; https://future-energy-lab.de/projects/dena-ENDA/

42 In DIVE: ed25519

43 Zum Beispiel Softwarebibliotheken in nahezu allen Programmiersprachen und Frameworks

44 Hardware Secure Module (HSM), Sicherheitselement bzw. umgangssprachlich Krypto-Chip

45 https://www.zymbit.com/hsm6/

4.2 Umsetzung der Onboarding-Prozesse unter Nutzung der Self-Sovereign Identities

Eine konsequente Ende-zu Ende-Digitalisierung der energiewirtschaftlichen Prozesse bedeutet, dass auch Einzelanlagen in die Prozesse eingebunden werden müssen. Um Anlagen dazu zu befähigen, braucht es digitale Maschinen-Identitäten. Darüber hinaus müssen Anlagen und Akteure vertrauensvoll und gleichsam effizient miteinander interagieren können, was selbstverwaltete digitale Identitätsinfrastrukturen erforderlich macht. Um an den entsprechenden Prozessen teilnehmen zu können, wird eine entsprechend qualifizierte digitale Registrierung (sogenanntes Onboarding) der Anlagen benötigt. Um die DIVE-Basisinfrastruktur zu nutzen und sich niederschwellig zu authentifizieren und an Anwendungsfällen teilnehmen zu können, muss eine Energieanlage hinter einem Netzanschlusspunkt mit einem (H)EMS (z. B. einer OLI Box) ausgestattet werden, damit alle notwendigen Funktionalitäten vorhanden sind, und anschließend eine DID erzeugen. Der nächste Schritt ist dann die Registrierung der Anlage in der DIVE-Basisinfrastruktur, hier Onboarding genannt. Dabei wird ein Verifiable Credential erzeugt, in dem die Stammdaten der Anlage gespeichert werden. Dies wird dann an einen Issuer übermittelt, mit der Aufforderung, die Daten zu überprüfen und zu bestätigen. Indem der Verteilnetzbetreiber die Rolle des Issuers einnimmt, fügt sich der Registrierungsprozess bestmöglich in bestehende energiewirtschaftliche Prozesse ein.[46] Nach erfolgreicher Bestätigung des VC sind die Anlagen bereit für eine Teilnahme an Anwendungsfällen (z. B. Flexibilitätsplattformen oder Energiegemeinschaften).

4.2.1 Erstellung einer DID für die Anlage

Um ein (H)EMS wie die OLI Box in die Lage zu versetzen, digitale Identitäten selbst zu verwalten, müssen die Geräte zukünftig vom Hersteller ab Werk mit der erforderlichen Software sowie einer benutzerfreundlichen Bedienoberfläche ausgestattet sein.[47] Um die KILT Blockchain für die Verwaltung von SSI nutzen zu können, benötigt ein (H)EMS zudem ein ausreichendes Kontingent an KILT Coins, um die anfallenden Transaktionsgebühren für Blockchain-Transaktionen zu decken. Bei der OLI Box wird dazu ein Payment Account ab Werk bereitgestellt und mit ausreichend KILT Coins ausgestattet.

Nach der Lieferung wird das (H)EMS vom Installateur beim Anlagenbetreiber installiert und mit

- der Anlage,
- dem Internet,
- dem Home Area Network (HAN) und
- dem CLS-Gateway und damit mit dem Smart Meter Gateway (SMGW)

verbunden. Im nächsten Schritt kann der Anlagenbetreiber über das User Interface auf dem (H)EMS die DID für das Gerät erstellen. Im DIVE-Projekt wurde diese DID direkt auf der OLI Box generiert, wobei die privaten Schlüssel auf der OLI Box gespeichert und der öffentliche Teil der DID auf der KILT Blockchain hinterlegt wurde. Die Bezahlung der Transaktionskosten erfolgte durch den Payment Account im Hintergrund, ohne dass der Nutzer dies aktiv wahrnehmen musste.

Die DID der Anlage wird erst am Einsatzort durch den Betreiber der Anlage generiert, um sicherzustellen, dass keine unbefugten Dritten Zugriff auf den privaten Schlüssel erhalten und dadurch die Kontrolle über die Identität der Anlage übernehmen können. Für eine zukünftige großflächige Einführung des Systems kann optional ein QR-Code auf der Box angebracht werden, den der Betreiber der Box scannen kann, um direkt auf das User Interface des (H)EMS zuzugreifen. Durch die Selbstverwaltung der digitalen Identität durch den Anlagenbetreiber brauchen Installateure kein spezifisches Zusatzwissen zum Thema SSI und DID. Die Inbetriebnahme kann im Wesentlichen so erfolgen wie bisher.

Abbildung 17 zeigt links das User Interface der OLI Box, die noch über keine Identität verfügt. Über das Klicken auf den Button „Identität erstellen“ wird die DID für die OLI Box als Heimenergiemanagementsystem auf der OLI Box selbst generiert und der öffentliche Teil der DID auf die KILT Blockchain geschrieben.

Abbildung 17: User Interface der OLI Box ohne DID und mit DID

46 Eine energiewirtschaftliche Diskussion hierzu findet sich in den Berichtsteilen „Mehrwerte für die energiewirtschaftlichen Anwendungsfälle“ sowie „Überblick, Einordnung und Evaluation“ dieser Berichtsreihe.

47 https://github.com/KILTprotocol/dena_setup_box

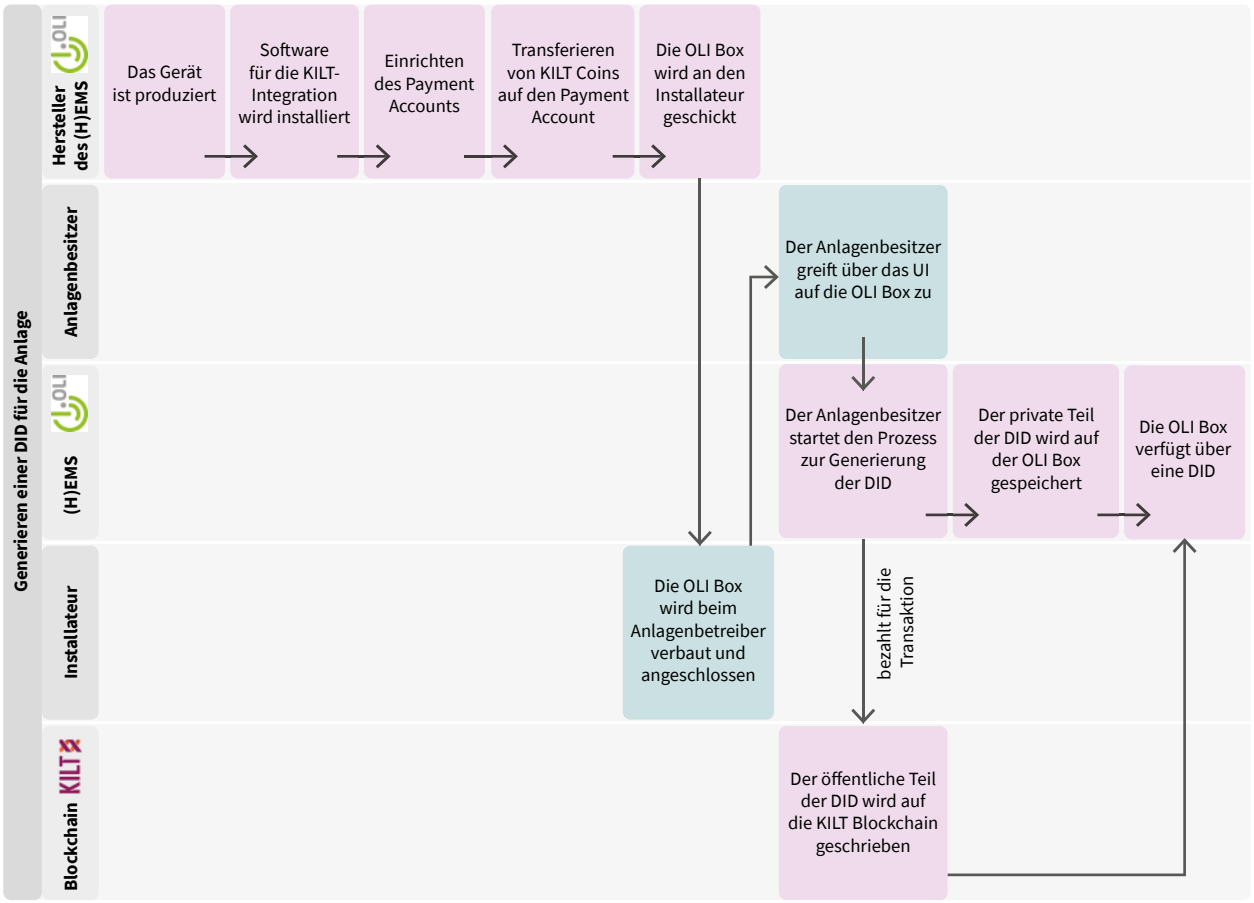

Abbildung 18: Prozess zum Generieren einer DID für die Anlage

4.2.2 Registrierung der Anlage

Ziel der Anlagenregistrierung ist es, dass der Verteilnetzbetreiber (VNB) der Anlage ein Verifiable Credential über die Attribute ausstellt und die Anlage so digital an den energiewirtschaftlichen Prozessen teilnehmen kann. Der Installateur oder auch der Anlagenbetreiber prüft die statischen und dynamischen Daten der Anlage, trägt sie in das User Interface der dort verbauten OLI Box ein und fordert beim VNB das Verifiable Credential an. Der VNB prüft auf seiner Seite die Daten, die vom Anlagenbetreiber übermittelt wurden, und stellt nach erfolgreicher Prüfung das Credential aus, das in der Wallet des Anlagenbetreibers gespeichert wird. Das Credential hat dort nun den Status *Beglaubigt*, das heißt, es handelt sich um ein gültiges Credential. Das Credential wird zusätzlich über einen Hash mit dem Status *revoked: false* auf der Blockchain verankert.

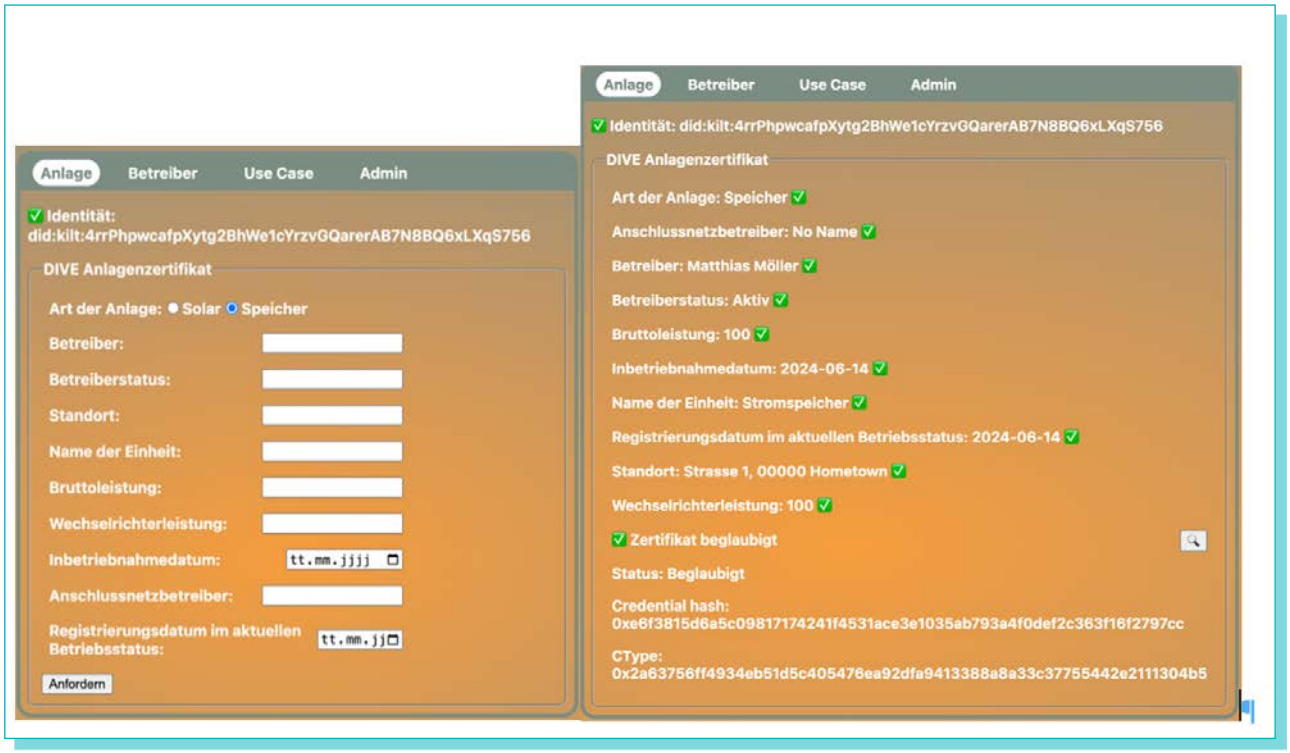

Abbildung 19: User Interface (Eingabemaske der OLI Box) für ein VC für einen Speicher (links); ausgestelltes Credential (rechts)

Ein ausgestelltes Credential wird im User Interface der OLI Box mit allen bestätigten Attributen, dem Credential-Status, dem Credential-Hash und dem CTYPE-Hash angezeigt. Da die Felder des CTYPE als optionale Felder definiert wurden, wird je nach Art der Anlage (z. B. Photovoltaik-Anlage oder Batteriespeicher) im User Interface ein individuelles Subset an Informationen abgefragt. Bei einem durch den VNB invalidierten Credential wird dies im User Interface der OLI Box durch einen entsprechenden Eintrag angezeigt und auf der Blockchain ändert sich der Status des Credentials von *revoked: false* zu *revoked: true*[48]. In Abbildung 17 ändern sich die Einträge *Zertifikat* und *Status* zu *Widerrufen*.

Abbildung 20: User Interface der OLI Box: invalidiertes Credential

Für einen zukünftigen flächendeckenden Rollout wäre es vorteilhaft, Daten zu den Anlagen von den Herstellern übernehmen zu können und so die VCs automatisch vorauszufüllen und eventuelle Fehlerquoten zu reduzieren.

Der VNB kann zum Ausstellen der Credentials den KILT Attester Service als Applikation in seine IT-Umgebung integrieren oder eine eigene Applikation entwickeln. Über den jeweiligen Service empfängt der VNB die Anfragen zur Prüfung von Credentials, kann die Credentials dort ausstellen und sie bei Bedarf invalidieren. Für diese Vorgänge benötigt der VNB ebenfalls eine DID, um die notwendigen Interaktionen, zum Beispiel mit der Blockchain, durchführen zu können (siehe Kapitel 3.1.1).

48 https://ipfs.io/ipns/dotapps.io/?rpc=wss%3A%2F%2Fspiritnet.kilt.io%2F#/chainstate

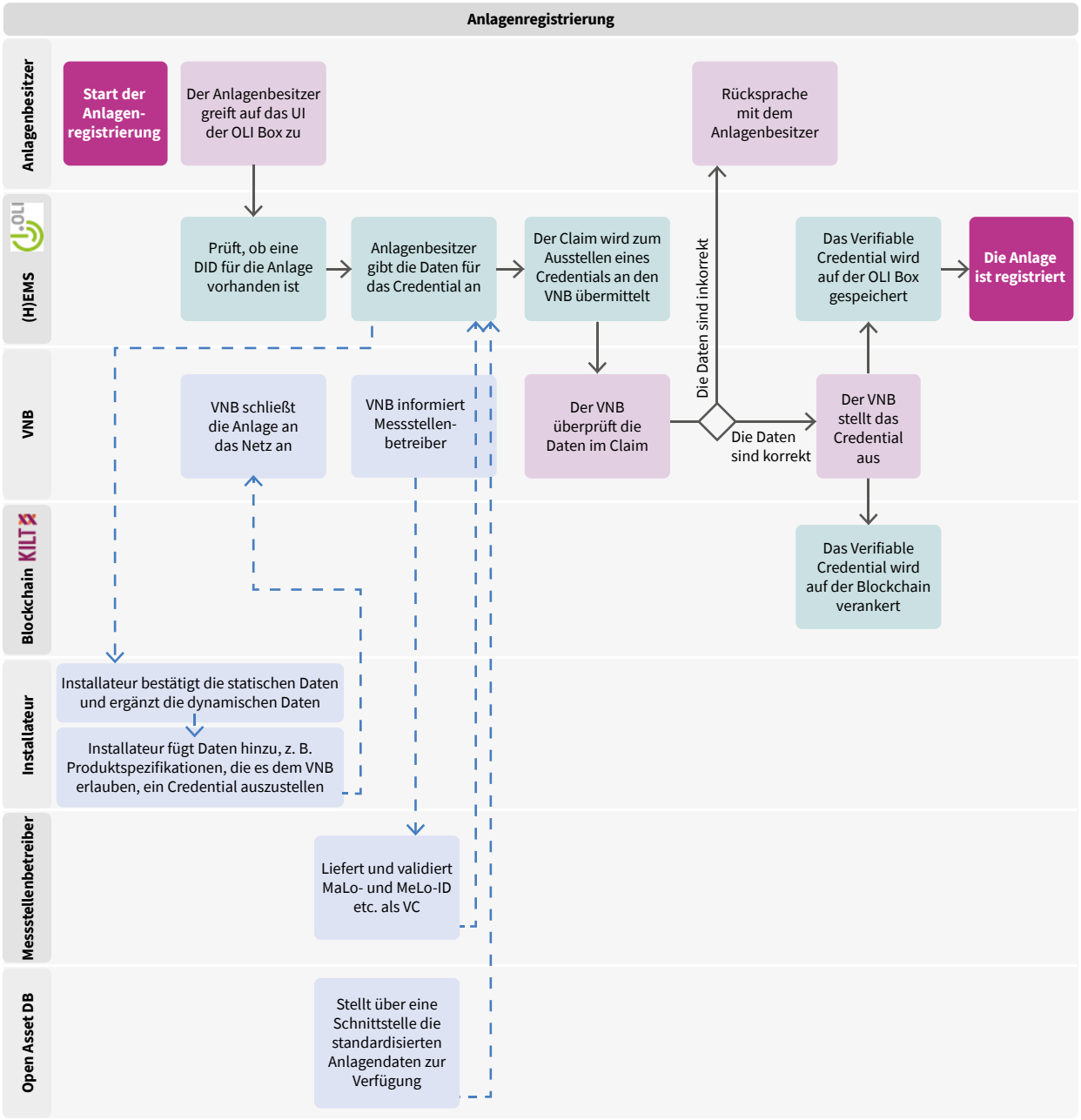

Abbildung 21: Prozessablauf der Anlagenregistrierung[49]

umgesetzter Prozessablauf

möglicher Ablauf einer automatisierteren Dateneingabe

49 Die grauen Prozessschritte wurden im Rahmen des Projekts nicht umgesetzt, sollten aber bei einem Rollout in der Fläche berücksichtigt werden.

4.2.3 Registrierung des Anlagenbetreibers

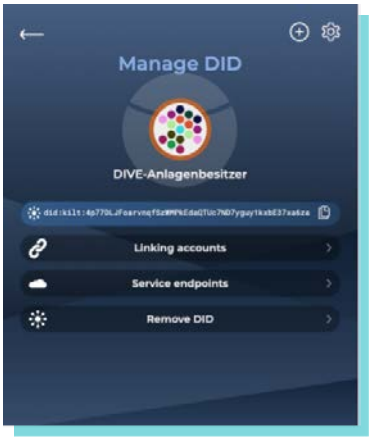

Abbildung 22: Beispiel für eine DID des Anlagenbetreibers

Neben der Anlage benötigt auch der Betreiber eine dezentrale und digitale Identität. Dazu muss der Benutzer eine Nutzer-Wallet (hier: Sporran als Browser-Plugin) installieren und einen Account anlegen.[50] Im zweiten Schritt wechselt der Betreiber dann auf das User Interface des (H)EMS (hier: via Webbrowser auf die OLI Box). Dort generiert der Betreiber seine eigene DID.

Die DID ist eine reine Nutzerkennung. Für weitere Informationen (z. B. Name und Anschrift (siehe auch Kapitel 3.1)) benötigt der Betreiber noch ein Credential, das weitere Informationen für die Überprüfung und anschließende Präsentation speichern kann. Das VC kann der Nutzer auf die folgenden drei Arten erhalten[51]:

- Der Betreiber gibt die Daten selbst ein.
- Der Installateur übernimmt die Daten aus dem Personalausweis des Betreibers.
- Bei einem zukünftigen Rollout kann der Betreiber seine Daten in der Maske eingeben und an die API des Marktstammdatenregisters zum Datenabgleich übermitteln. Wenn bereits ein Datensatz besteht, werden die Daten übernommen und durch den Betreiber überprüft und gegebenenfalls angepasst.

In allen drei Fällen wird das Credential durch die OLI Box ausgestellt. Ein Vertrauensdienst wird nicht benötigt. Es handelt sich also im Wesentlichen um eine Selbstauskunft. Im Fall, dass ein Selbstauskunftszertifikat nicht ausreicht, kann auf bestehende KYC-Integrationen (Know Your Customer) zurückgegriffen[52] oder es kann ein Credential durch den Installateur oder durch einen anderen Akteur (z. B. die BNetzA) ausgestellt werden.

Die DID und die VCs des Anlagenbetreibers werden final in der Wallet gespeichert und verwaltet und unterliegen somit der alleinigen Kontrolle des Betreibers.

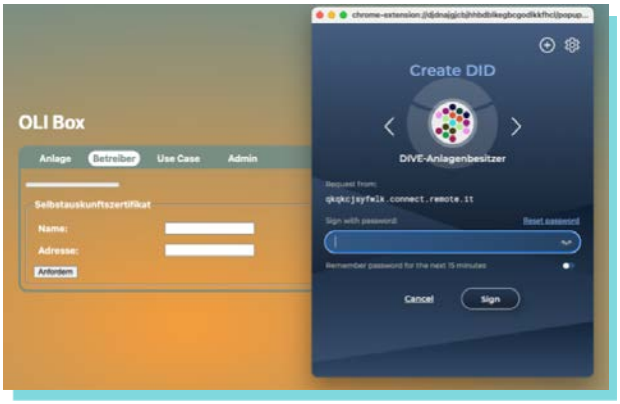

Abbildung 23: Generierung der DID des Anlagenbetreibers

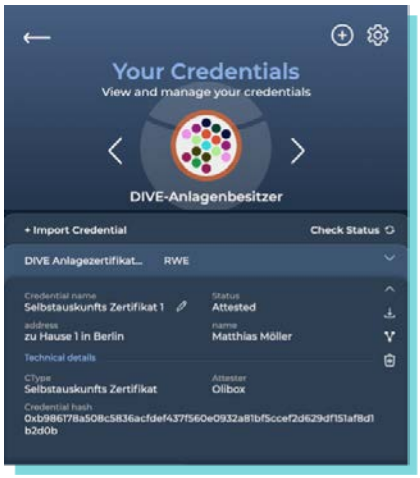

Abbildung 24: Credential des Anlagenbetreibers

4.3 Komponenten- und Systemarchitektur

Dieses Kapitel veranschaulicht die technische Integration und Kommunikation zwischen den einzelnen Komponenten, die eingesetzt werden, um die energiewirtschaftlichen Prozesse umzusetzen. Dies umfasst zum einen die Komponenten, die auf der OLI Box laufen, um die OLI Box in den Zustand zu versetzen, ihre Identität zu managen und zu nutzen, aber auch Services und

50 Dabei handelt es sich noch nicht um die DID (vgl. Kapitel 3.1.1).

51 Im Projekt ist die erste Option umgesetzt worden.

52 Bei einem KYC-Verfahren (Know Your Customer, „Kenne deinen Kunden“) wird anhand von offiziellen Dokumenten, wie zum Beispiel dem Personalausweis, und weiteren Verfahren die Identität einer Person festgestellt.

Applikationen, die beim Anlagenbetreiber und beim VNB als Issuer zum Einsatz kommen.

4.3.1 Integration der Self-Sovereign Identities auf der OLI Box

Auf der OLI Box läuft ein SSI-Server, der für die Verwaltung der Maschinen-Identität sowie für die Bereitstellung einer Benutzeroberfläche für den Betreiber verantwortlich ist. Während des Onboarding-Prozesses erstellt der SSI-Server kryptografisches Schlüsselmaterial, das genutzt wird, um eine dezentrale Identität auf der KILT Blockchain zu verankern (siehe Kapitel 3.1.1). Das Schlüsselmaterial wird auf der Box gespeichert. Um die öffentlichen Schlüssel zusammen mit der erzeugten DID auf die KILT Blockchain zu schreiben, wird eine geringe Menge an KILT Coins benötigt.

Über die Oberfläche, die zur einfachen Nutzung als Web-Applikation implementiert ist, können Betreiber verschiedene energiewirtschaftliche Prozesse (z. B. Anmeldung im Marktstammdatenregister) starten sowie die DID des Geräts und die ihr zugeordneten Credentials einsehen. Zusätzlich ermöglicht die Oberfläche den Betreibern, für sich selbst eine DID zu erstellen und Verifiable Credentials zu beantragen.

Auf der OLI Box laufen für die Umsetzung der Self-Sovereign Identities folgende Komponenten:

- **Backend:** Umfasst den SSI-Server, der mit der Blockchain kommuniziert
- **HTTP Client:** Kommuniziert als Teil des Backends mit OpenDID und dem Attester Service
- **Frontend:** Stellt die Nutzeroberfläche, über die der Anlagenbetreiber auf die Box zugreift, zur Verfügung
- **Storage:** Speichert die Seeds für die Geräte-DID und den Payment Account sowie die Verifiable Credentials

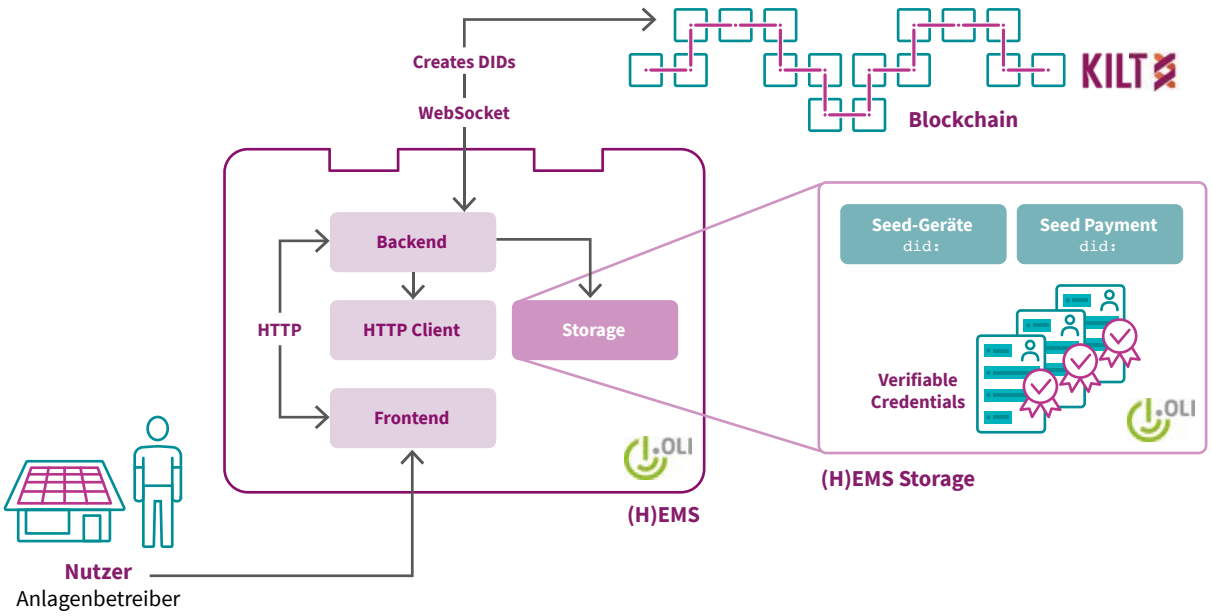

Abbildung 25: Komponentenübersicht SSI auf der OLI Box

4.3.2 OpenDID zur Authentifizierung der Akteure

Im Rahmen der Umsetzung wird OpenDID[53] eingesetzt, um innerhalb des Anlagenregistrierungsprozesses die OLI Box am Attester Service zu authentifizieren, das heißt, es ihr zu ermöglichen, in einer authentifizierten Weise die Ausstellung eines Credentials zu beantragen. Hierfür wird, der SIOPv2-Spezifikation[54] folgend, von der OLI Box ein selbstsigniertes ID-Token erzeugt, das die DID der OLI Box enthält. Dieses ID-Token wird OpenDID präsentiert und dort mithilfe der KILT Blockchain verifiziert, bevor es in ein von OpenDID signiertes JWT[55] übersetzt wird, das dann von der spezifischen Applikation des jeweiligen Anwendungsfalls weiterverwendet werden kann.

Die Betreiber authentifizieren sich, indem sie über ihren Webbrowser von der Anwendungsapplikation (in diesem Fall dem Attester Service) an OpenDID weitergeleitet werden. Dort präsentieren sie unter Nutzung der KILT Credential API [56], einer weiteren API, die das sichere Ausstellen von Credentials zwischen einer dapp[57] und einer Wallet ermöglicht, ihre Credentials. Können die Credentials der Anlagenbetreiber verifiziert werden, wird ihnen auch hier ein von OpenDID signiertes JWT ausgestellt.

Das Verfahren mit OpenDID wurde unter anderem wegen seiner einfachen und niederschwelligen Implementierungsmöglichkeiten gewählt: Die Nutzung von OpenDID für die Integration einer DID-basierten Benutzerauthentifizierung erfordert lediglich das Starten des OpenDID-Containers sowie die Einrichtung einer Weiterleitung von der Login-Seite der anwendungsfallspezifischen Applikation. Die Kommunikation zwischen Benutzer-Wallet und der Applikation sowie die Kommunikation mit der KILT Blockchain zur Verifizierung der präsentierten Credentials werden vollständig von OpenDID übernommen, sodass die Entwickler lediglich die spezifischen Autorisierungsregeln innerhalb ihrer Domäne umsetzen müssen und dafür auf die Informationen aus dem von OpenDID bereitgestellten JWT zurückgreifen können.

4.3.3 Gesamtübersicht der eingesetzten Komponenten

In der folgenden Grafik werden die verschiedenen Komponenten und ihre Kommunikation miteinander dargestellt.

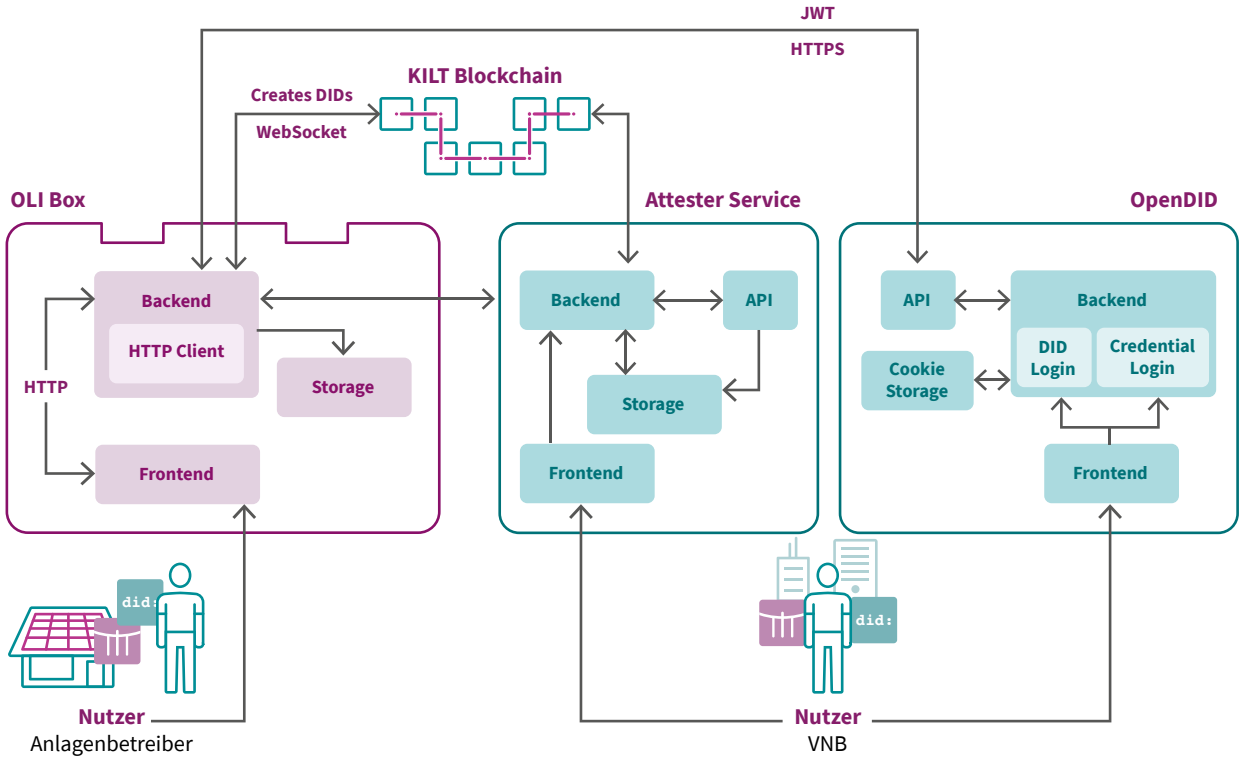

Abbildung 26: Komponentenübersicht Gesamtsystem

53 OpenDID ist eine Open-Source-Softwarekomponente für Websites, die zur Implementierung eines Logins mit einem KILT Credential verwendet werden kann. OpenDID nutzt den OpenID Connect Flow und generiert JWT-Tokens (JSON Web), ein offener Standard für den sicheren Austausch von Informationen zwischen zwei Parteien unter Verwendung des dezentralen Identifikators (DID) des Benutzers und überprüfbarer Zugangsdaten.

54 https://openid.net/specs/openid-connect-self-issued-v2-1_0-ID1.html

55 https://jwt.io/

56 https://github.com/KILTprotocol/spec-ext-credential-api

57 dapp ist eine App, die mit einer Blockchain kommuniziert.

- Der **Nutzer (Anlagenbetreiber)** verwaltet seine Self-Sovereign Identity über seine Identity Wallet (hier: Sporran).
- Über das **Frontend (H)EMS (hier: OLI Box)** wird das User Interface zur Verfügung gestellt, über das der Betreiber auf die OLI Box zugreift, um zum Beispiel seine eigene DID zu generieren, die DID für die OLI Box zu erzeugen oder deren Credentials anzufragen.
- Über den **Backend Service** kommuniziert die **OLI Box** mit der KILT Blockchain und den anderen Komponenten.
- Die Credentials der OLI Box und die Seeds für die DID und den Payment Account werden im **Storage der OLI Box** gespeichert.
- Zum Ausstellen der Credentials wird der **Attester Service** genutzt.
- Die **Beschäftigten zum Beispiel von Verteilnetzbetreibern** greifen unter Nutzung ihrer Self-Sovereign Identity auf den Attester Service zu.
- Die Nutzer des VNB loggen sich über **OpenDID** im Attester Service ein, um über den Attester Service Credentials auszustellen.
- Der **Attester Service** kommuniziert über sein **Backend** mit der KILT Blockchain.

Bei dem Attester Service und OpenDID handelt es sich um Komponenten, die bei den jeweiligen Issuern betrieben werden. Das heißt, jeder VNB, der Credentials ausstellt, muss solche Services für sich betreiben.

4.4 Technische Umsetzung mit Energy Web Green Proofs

Im Rahmen des Projekts wurde die Anwendbarkeit der DIVE-Basisinfrastruktur am Beispiel von Herkunftsnachweisen demonstriert. Dafür wurden Erzeugungsanlagen von Prosumern jeweils mit einer DID und mit VCs ausgestattet. Im Anschluss konnten die Prosumer ihre Anlagen bei der Herkunftsnachweis-Plattform *Energy Web Green Proofs* in wenigen Schritten anmelden. Dabei wurde automatisiert über ein Hintergrundverfahren mittels des sogenannten „Konflikt-Tokens“ sichergestellt, dass die Anlagen nicht bereits bei einer anderen Plattform zur Ausstellung von Herkunftsnachweisen registriert sind. Für diesen Test wurde ein Duplikat der Green-Proofs-Plattform betrieben, um verschiedene Anbieter zu simulieren.

Einen DIVE-Anwendungsfall mit einem DIVE-Gerät bekannt machen

Es wird vorausgesetzt, dass jede teilnehmende Anwendung eine eindeutige Kennung, eine DID vom Typ did:web, besitzt. Dies stellt sicher, dass ein eindeutiges digitales Format definiert ist, mit dem Prosumer neue Anwendungen zu ihren Geräten hinzufügen und diese Geräte dann Anwendungs-Metadaten automatisch abrufen können.

Darüber hinaus werden für die Teilnahme an DIVE keine weiteren, speziellen Softwarefunktionen mehr benötigt. Dieses Vorgehen ermöglicht einen freien Marktzugang für alle Anwendungsanbieter unabhängig von Modell, Hersteller oder Vertriebsweg der jeweiligen DIVE-kompatiblen Anlage.

Daraus ergeben sich folgende technische Anforderungen an Anwendungen und ihre Anbieter:

- Die Identität der DIVE-Anwendung ist mittels **did:web** veröffentlicht.
- Die Anwendung ist **kompatibel mit dem DIVE-Protokoll**.
  - Die Auflösung der Geräte-Identität (DID) und der Basis-Gerätedaten (VCs) ist möglich.
  - Die Überprüfung des Konflikt-Tokens ist möglich.

Weitere Anwendungen können mittels DID einfach hinzugefügt werden.[58] Dazu wird die DID direkt auf dem Webinterface des Prosumer-Geräts eingegeben. Das Gerät ruft alle weiteren Informationen automatisch von der Anwendung ab, beispielsweise:

- Anbieter der Anwendung
- Name der Anwendung
- Icon
- Link zu den AGB und zur Datenschutzerklärung
- Weitere technische Daten, Web-Endpunkt zur Kommunikation, der öffentliche Krypto-Schlüssel der Anwendung

Ein DIVE-Gerät bei einem Anwendungsfall anmelden

Ist die gewünschte Anwendung dem Gerät prinzipiell bekannt, kann der Nutzer die Anwendung im Webinterface des Geräts aus der Liste der bekannten Anwendungen auswählen. Daraufhin werden einige weitere Informationen zur Anwendung angezeigt. Der Nutzer muss den AGB und der Datenschutzerklärung der Anwendung zustimmen, bevor der Prozess zur Anmeldung gestartet werden kann.

Der erste Schritt des Anmeldeprozesses ist, die Einhaltung der Marktregeln zu prüfen, insbesondere die Prüfung, ob der Nutzer tatsächlich über das Gerät verfügen kann und dass das Gerät nicht bereits an einem parallelen Anwendungsfall teilnimmt (Konfliktfall).

58 Idealerweise würden Geräte zukünftig mit einer Liste von bekannten Anwendungen ausgeliefert.

Technisches Sicherstellen der Einhaltung von Marktregeln: Vermeidung von Doppelvermarktung

Entscheidet sich der Nutzer dazu, sein Gerät bei einem Anwendungsfall anzumelden, muss er zunächst lokal auf das Gerät selbst zugreifen und das Gerät anweisen, die Anmeldung bzw. Ummeldung vorzunehmen. Dazu wird das Gerät den Anwendungsfall kontaktieren und kryptografisches Material (Krypto-Schlüssel zur späteren Verschlüsselung des Anwendungsfall-Konflikt-Tokens)[59] anfordern, um eine spätere Überprüfung der korrekten Ab- und Anmeldung zu ermöglichen.

Das Gerät verschlüsselt damit auch ein sogenanntes Konflikt-Token und aktualisiert sein eigenes Verifiable Credential mit dem Wert des verschlüsselten Anwendungsfall-Konflikt-Tokens. Die Aktualisierung des VC wird abgeschlossen, indem das VC selbst signiert und der Hash-Wert auf der Blockchain verankert wird.

Dieser Aktualisierungsvorgang wird mittels Zeitstempel und Hash-Wert in einem Block auf der KILT Blockchain hinterlegt. Man spricht dabei von der Erzeugung eines Blockchain-Events. Die „Adresse" des Blocks, mit dem das Event verknüpft ist, erhalten sowohl der vorher genutzte Anwendungsfall als auch der neue. Der neue Anwendungsfall fordert daraufhin das VC vom Gerät an und überprüft den Inhalt des anwendungsspezifischen Konflikt-Tokens, das aufgrund des vorher ausgetauschten Schlüssels nur von diesem Anwendungsfall gelesen werden kann. Bei erfolgreicher Prüfung hat der neue Anwendungsfall die Sicherheit, dass das Gerät nun ausschließlich bei eben diesem Anwendungsfall angemeldet ist. Andere Anwendungsfälle können das Token nicht entschlüsseln, erfahren aber, dass eine An-, Um- oder Abmeldung dieses Geräts stattgefunden hat. Dritte können zu keinem Zeitpunkt erfahren, ob ein Gerät überhaupt bei einem Anwendungsfall angemeldet ist oder bei welchem.

Ist das Konflikt-Token aktualisiert, beginnt die eigentliche Anmeldung bei der Anwendung. Das Gerät ruft den Endpunkt der Anwendung auf und beginnt den Anmeldeprozess. Daraufhin prüft die Anwendung, ob das Konflikt-Token des Geräts auf den richtigen Wert gesetzt wurde, und fährt nach positivem Ergebnis dieser Prüfung fort. Die Anwendung fordert das Basis-VC vom Gerät an und prüft, ob das Gerät die Voraussetzungen zur Teilnahme erfüllt.[60]

Ist auch dieser Prüfvorgang erfolgreich, bestätigt die Anwendung die erfolgreiche Anmeldung. Von nun an erlaubt das Gerät den Abruf der Messdaten durch die Anwendung. So erhält Green Proofs automatisch Erzeugungsdaten mit einer zeitlichen Auflösung von 15 Minuten. Für jedes 15-minütige Segment wird ein digitaler Nachweis erstellt und dem Gerät und seinem Account zugeordnet.

Der so erzeugte Nachweis ist digital verifizierbar, da die Signaturen der Messdaten des iMSys verfügbar sind. Die Nachweise können an einen anderen Account transferiert und manuell oder automatisiert einem Stromverbrauch zugeordnet werden.

Nachdem der Nachweis über die grün erzeugte Energiemenge einem Verbrauch zugeordnet wurde, stellt Green Proofs die Menge des eingesparten CO_2 gegenüber einer vorher definierten Baseline dar.

Für Elektrofahrzeuge ist so eine Zuordnung zu einem konkreten Ladevorgang möglich. Für Flottenfahrzeuge kann automatisch ein Nachweis über Flottenemissionen erzeugt werden, der lückenlos bis zur Erzeugungsanlage eines jeden Ladevorgangs digital verifizierbar nachvollziehbar ist.

Technisches Sicherstellen weiterer Voraussetzungen zur Teilnahme am Use Case

Neben der Überprüfung zur Einhaltung der Marktregeln und zur Vermeidung von Doppelvermarktung kann jeder Anwendungsfall weitere individuelle Voraussetzungen definieren, die teilnehmende Geräte erfüllen müssen. Beim Beispiel der Energy Web Green Proofs wäre eine solche weitere Voraussetzung:

- Die Erzeugungsanlage ist nicht EEG-gefördert.

Auch Verbrauchsanlagen können sich bei Green Proofs anmelden, um eine granulare Zuordnung der erzeugten Energiemengen bzw. Zertifikate zu ermöglichen. Alle notwendigen Informationen sind im Basis-VC des Geräts enthalten und werden vom Anwendungsfall automatisch vom Gerät angefordert und im Anschluss an die Präsentation des VC überprüft. Kommt diese Überprüfung zu einem positiven Ergebnis, wird das Gerät bei Green Proofs angemeldet und das Resultat an das Gerät kommuniziert.

Zugriff auf Bewegungsdaten

Nach erfolgreicher Anmeldung am Anwendungsfall wird das Gerät nun den Abruf der Messdaten durch die Anwendung erlauben.

Datenschutz und Sicherheit

Um die Privatsphäre und Sicherheit der Gerätebesitzer zu gewährleisten, wird im Green-Proofs-Anwendungsfall der folgende Mechanismus implementiert:

Vertraulichkeit von Geräteinformationen: Erst wenn der Gerätebesitzer das Gerät explizit anweist, sich bei einem Anwendungsfall anzumelden, beginnt der Datenaustausch. Das bedeutet, dass ohne diesen Schritt alle Gerätedaten ausschließlich auf dem Gerät liegen.

Beschränkte Sichtbarkeit: Jede Anwendung kann lediglich überprüfen, ob ein Gerät bei ihr registriert ist oder nicht. Sie hat keine Möglichkeiten zum Zugriff auf Informationen über den Gerätebesitzer oder etwaige Anmeldungen bei anderen Anwendungsfällen, für die das Gerät registriert ist.

Diese Maßnahmen tragen dazu bei, die Daten der Gerätebesitzer zu schützen und sicherzustellen, dass nur autorisierte Personen Zugriff auf die relevanten Informationen haben.

59 Der Konflikt-Token in DIVE stellt sicher, dass eine Anlage zu einem Zeitpunkt nur bei genau einem Anwendungsfall angemeldet sein kann. Komplexere Marktregeln, z. B. Übergangsfristen, erfordern voraussichtlich auch komplexere technische Mechanismen.

60 Beispiel bei EW Green Proofs: Die Anlage ist nicht EEG-gefördert; die Anlage produziert erneuerbare („grüne") Energie.

Zusammenfassung

Der in diesem Dokument beschriebene und implementierte Ansatz zeigt, wie die Umsetzung der Interaktion und Kommunikation zwischen den Akteuren im Energiesystem (z. B. Anlagen, Anlagenbetreiber, Verteilnetzbetreiber oder Anwendungsfälle) auf Basis von Self-Sovereign Identities funktionieren kann. Ein darauf aufbauendes System kann die Echtzeit-Kommunikation zwischen den Akteuren der Energiewirtschaft ermöglichen.

Das DIVE-Projekt nutzt die W3C-Standards für Decentralized Identifiers (DIDs) und Verifiable Credentials (VCs) zur Implementierung von Self-Sovereign Identities (SSI). Diese Standards werden weltweit zunehmend von der Privatwirtschaft und öffentlichen Organisationen genutzt und adaptiert und bieten den Vorteil einer einfachen Integration weiterer Akteure und Anwendungsfälle. Der Einsatz dieser Standards ermöglicht es zudem, perspektivisch auch Akteure anderer Sektoren einzubinden (Sektorenkopplung).

Die Dezentralität des Systems ermöglicht eine Teilnahme als Anlage oder Anwendungsfall ohne eine zentrale Instanz, die als Gatekeeper fungiert. Alle Akteure – von der Anlage über die Betreiber bis hin zu den Organisationen, die Credentials ausstellen – verfügen über eine eigene Self-Sovereign Identity, die sie selbst kontrollieren. Über diese SSI kommunizieren die Akteure direkt miteinander, ohne auf zentrale Systeme angewiesen zu sein:

Die Anlage und die Betreiber kommunizieren direkt mit der Credentials ausstellenden Organisation, zum Beispiel dem Verteilnetzbetreiber.

Die Anlage kommuniziert direkt mit den Anwendungsfällen, an denen sie teilnehmen möchte, ohne dass eine Kommunikation zwischen Anwendungsfall und der Credentials ausstellenden Organisation erforderlich ist.

Dies ermöglicht einen hohen Grad an Effizienz, Flexibilität und Skalierbarkeit, um die Anforderungen eines zukunftssicheren Systems mit Millionen kleinster Anlagen zu erfüllen.

Das System gewährt den Nutzern zudem eine hohe Privatsphäre, da sie selbst über die Verwendung ihrer Identitäten bestimmen, ohne zentrale Instanzen einzubeziehen. Die Blockchain dient dabei als Nachschlageregister und dezentraler Vertrauensanker: Dienstleister können die Gültigkeit von Nachweisen durch VCs überprüfen, während Credential-Aussteller keine Informationen über die Verwendung der durch sie ausgestellten Credentials erhalten. Dies verbessert den Datenschutz und erhöht die Skalierbarkeit. Die dezentrale Speicherung der Daten eliminiert zudem zentrale Angriffspunkte und stärkt die Systemsicherheit.

Eine weitere essenzielle Komponente für die Implementierung des DIVE-Ansatzes stellt das intelligente Messsystem (iMSys) dar. Während die Energiemanagementsysteme zwar Anlagendaten beziehen und sie per DIVE an die Anwendungen weiterleiten können, fehlen insbesondere bei abrechnungsrelevanten Prozessen noch eichrechtskonforme Zählerdaten. Mithilfe des auf das iMSys aufgespielten Tarifanwendungsfalls 7 (Zählerstandsgangmessung) und der damit erhobenen viertelstündlichen Zählerdaten können Anwendungen korrekt abrechnen und Messdaten auf die statischen Daten in den Credentials zurückführen. Erst dann kann sich der „wirtschaftliche Kreis“ regulatorisch korrekt schließen.

Das DIVE-Projekt liefert nicht nur eine theoretische Grundlage dafür, wie ein flexibles Identitätsmanagementsystem für die Energiewirtschaft aussehen könnte, sondern hat dieses bereits praktisch umgesetzt. Diese Implementierung dient als Grundlage für die Umsetzung und den Rollout digitaler Anlagen-Identitäten in der Energiewirtschaft. Da es sich größtenteils um Open-Source-Software handelt, können die Services und Anwendungen an die jeweiligen Bedürfnisse der Anwendungsfälle angepasst werden.

Das DIVE-Projekt stellt somit einen innovativen und praxisnahen Ansatz zur Digitalisierung und Dezentralisierung im Energiesystem dar. Es zeigt, wie durch den Einsatz von Self-Sovereign Identities und etablierten Standards die Kommunikation und Interaktion zwischen Akteuren sicher und effizient gestaltet werden kann, und legt damit den Grundstein für ein zukunftssicheres, interoperables und datenschutzfreundliches Energiesystem.

Abbildungsverzeichnis

Abkürzungen

aEMT	Aktiver externer Marktteilnehmer
AGB	Allgemeine Geschäftsbedingungen
AMQP	Advanced Message Queuing Protocol
API	Application Programming Interface
CLS	Controllable Local System
CTYPE	Credential Type
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
DIF	Decentralized Identity Foundation
DSL	Digital Subscriber Line
EEG	Erneuerbare-Energien-Gesetz
eIDAS-Verordnung	EU-Richtlinie über die Resilienz kritischer Einrichtungen (Critical Entities Resilience)
EMS	Energiemanagementsystem
ERD	Energiewirtschaftlich relevante Daten
ESA	Energieserviceanbieter
EUDI-Wallet	Europäische Brieftasche für die digitale Identität (European Digital Identity Wallet)
GW	Gateway
HAN	Home Area Network
(H)EMS	(Heim-)Energiemanagementsystem
HKE	HAN-Kommunikationsadaptereinheit
HSM	Hardware Secure Module
HTTP	Hypertext Transfer Protocol
iMSys	Intelligentes Messsystem

JSON	JavaScript Object Notation
JWT	JSON Web Token
LMN	Local Metrological Network
LTE	Long Term Evolution
MaLo	Marktlokation
MeLo	Messlokation
mME	Moderne Messeinrichtung
MQTT	Message Queuing Telemetry Transport
pEMT	Passiver externer Marktteilnehmer
PKI	Public Key Infrastructure
RPC	Remote Procedure Call
SDK	Software Development Kit
SMGW	Smart Meter Gateway
SM-PKI	Smart Meter Public Key Infrastructure
SSI	Self-Sovereign Identity
TAF	Tarifanwendungsfall
UI	User Interface
URI	Uniform Resource Identifier
VC	Verifiable Credential
VNB	Verteilnetzbetreiber
W3C	World Wide Web Consortium
WAN	Wide Area Network

Literaturverzeichnis

Allen, Christopher (2016): A Patch to self-sovereign identity. Online verfügbar unter https://www.lifewithalacrity.com/article/the-path-to-self-soverereign-identity/. Abgerufen am 20.10.2024.

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

BSI (2021): Eckpunktepapier für Self-sovereign Identities (SSI) unter besonderer Berücksichtigung der Distributed-Ledger-Technologie (DLT). Online verfügbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Krypto/Eckpunkte_SSI_DLT.html. Abgerufen am 20.10.2024.

dena (2024): SET Pilot 1: Von Daten zum Mehrwert – Entwicklung und Evaluierung einer Verbrauchsvisualisierung und darauf aufbauender Mehrwertanwendungen unter Einbezug des Smart Meter Gateways. Hrsg. v. Deutsche Energie-Agentur GmbH. Online verfügbar unter https://www.dena.de/infocenter/set-pilot-1-von-daten-zum-mehrwert/. Abgerufen am 25.11.2024.

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

KILT Protocol (2024): CTYPES. Online verfügbar unter https://docs.kilt.io/docs/concepts/credentials/ctypes/. Abgerufen am 03.12.2024.

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

Lee, Ivan (2024): What is AMQP. Online verfügbar unter https://www.wallarm.com/what/what-is-amqp. Abgerufen am 25.11.2024.

Wikipedia (2024a): Web3. Online verfügbar unter https://de.wikipedia.org/wiki/Web3. Abgerufen am 03.12.2024.

Wikipedia (2024b): Hashfunktion. Online verfügbar unter https://de.wikipedia.org/wiki/Hashfunktionen. Abgerufen am 03.12.2024.

Wikipedia (2024c): JavaScript Object Notation. Online verfügbar unter https://de.wikipedia.org/wiki/JavaScript_Object_Notation#:~:text=Die%20JavaScript%20Object%20Notation%20(JSON,existieren%20in%20allen%20verbreiteten%20Sprachen. Abgerufen am 03.12.2024.

Wikipedia (2024d): Blockchain. Online verfügbar unter https://en.wikipedia.org/wiki/Blockchain. Abgerufen am 03.12.2024.

World Wide Web Consortium (W3C) (2022a): Decentralized Identifiers (DIDs) v1.0 Core architecture, data model, and representations W3C Recommendation 19 July 2022. Online verfügbar unter https://www.w3.org/TR/did-core/. Abgerufen am 03.12.2024.

World Wide Web Consortium (W3C) 2022b): Verifiable Credentials Data Model v1.1 W3C Recommendation 03 March 2022. Online verfügbar unter https://www.w3.org/TR/vc-data-model/. Abgerufen am 03.12.2024.

Anhang

Delegierte Vertrauensstrukturen und Legitimationen

Der Grad des Vertrauens in die ausgestellten Credentials wird durch das Vertrauen in die Organisation bestimmt, die die Credentials ausgestellt hat. Dieses Vertrauen ist aber abhängig vom konkreten Kontext, das heißt, man vertraut einem Issuer in einem spezifischen Kontext, zum Beispiel einem Verteilnetzbetreiber, der ein Credential über Daten einer bestimmten Anlage ausstellt. Das Gerät, das Eigenschaften über sich behauptet, und der verifizierende Service müssen also wissen, wem sie als Issuer vertrauen können. Dies kann auf mehrere Arten geschehen:

- **Direktes Vertrauen:** Der verifizierende Service vertraut dem Issuer direkt.

- **Hierarchische Top-down-Vertrauensstruktur:** Ein attestierender Service erbt Vertrauen von einer übergeordneten Instanz und kann Zertifikate in deren Namen ausstellen (beispielsweise delegiert eine Firma das Recht zum Ausstellen von Credentials an ihre Beschäftigten). Die Vertrauenskette wird in das Zertifikat eingebunden und auf der Blockchain verankert. Ein vertrauenswürdiger Knoten delegiert das Recht zur Ausstellung bestimmter Zertifikate an untergeordnete Knoten, die dieses Vertrauen weitervererben. Vertraut ein verifizierender Service dem übergeordneten Knoten, vertraut er auch dem Zertifikatsaussteller.

- **Legitimation:** Eine Legitimation weist nach, dass eine Entität berechtigt ist, bestimmte Handlungen auszuführen oder Rechte auszuüben. Im Fall von KILT stellt eine vertrauenswürdige Stelle ein Credential als Legitimation an eine Identität aus. Diese Identität kann dann bei der Ausstellung eines Credentials an Dritte ihre Legitimation hinzufügen, um Vertrauen zu stärken. Beispiel: Die Industrie- und Handelskammer bestätigt einer Firma durch ein Credential deren Existenz. Die Firma bestätigt wiederum ihren Mitarbeiterinnen und Mitarbeitern per Credential deren Anstellung, inklusive der IHK-Legitimation, wodurch Verifier die Existenz der Firma nachvollziehen können.

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