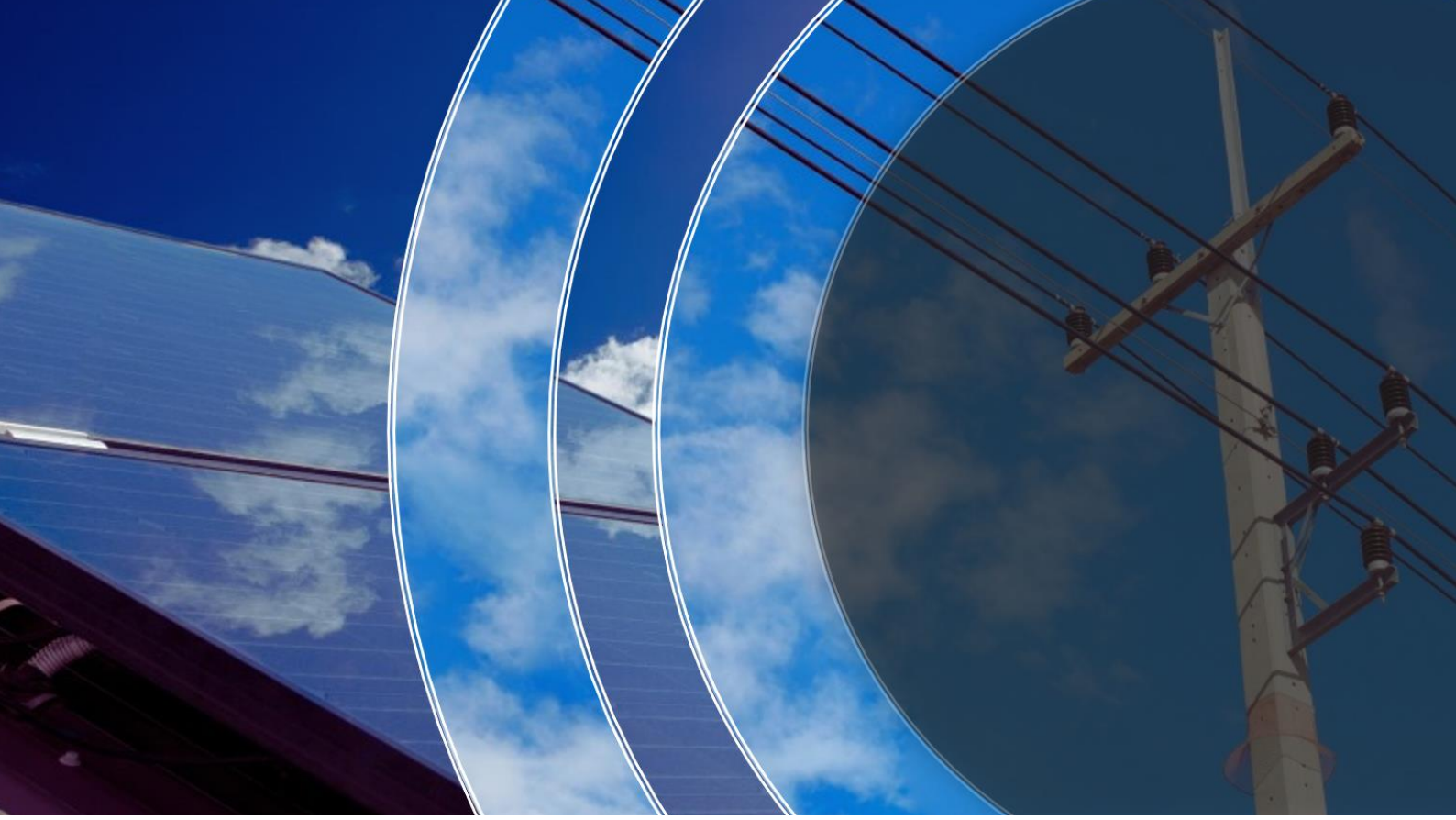


Analyse von Einsatzmöglichkeiten digitaler Identitäten in ÜNB-Prozessen

Meta-Analyse und Herleitung von Anwendungsfällen

Impressum

c.con Management Consulting GmbH
Altrottstraße 31 • D-69190 Walldorf
www.ccon.com • ccon@ccon.com
Amtsgericht Mannheim • HRB 702 656
USt-ID-Nr.: DE255266290

Studie

Analyse von Einsatzmöglichkeiten digitaler Identitäten in ÜNB- Prozessen – Meta-Analyse und Herleitung von Anwendungsfällen

Erstellt im Auftrag von

TransnetBW GmbH

Das dieser Veröffentlichung zugrundeliegende Vorhaben wurde mit Mitteln des Bundesministerium für Wirtschaft und Energie (BMWi) unter dem Förderkennzeichen 01MV21016F gefördert. Die Verantwortung für den Inhalt dieser Veröffentlichung liegt beim Autor.

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages
DLR Projektträger

Publikation

Januar 2024

Autoren

Dr. Jonas Maasmann

Senior Manager

c.con Management consulting GmbH

Jonas.Maasmann@ccon.com

+49 175 326 233 4

Dr. Rainer Enzenhöfer

Manager Disruptive Entwicklungen Netzwirtschaft

TransnetBW GmbH

r.enzenhoefer@transnetbw.de

+49 172 736 1603

Inhaltsverzeichnis

1 Einleitung 8
1.1 Einführung in das Untersuchungsgebiet 8
1.2 Problem und Zielstellung der Studie 11
2 Theoretische Grundlagen zu digitalen Identitätsmodellen 12
2.1 Digitale Identitäten und Identitätsmanagement 12
2.2 Modelle des Identitätsmanagements 13
2.2.1 Zentrales Identitätsmanagement 13
2.2.2 Dezentrales Identitätsmanagement 17
2.2.3 Eckpunkte für SSI und Technologiebausteine 20
2.3 Status Quo: Projekte zu SSI im energiewirtschaftlichen Bereich 24
2.3.1 BMIL – Blockchain Machine ID Ledger und Dive 24
2.3.2 GAIA-X 4 moveID 25
2.3.3 energy data-X 26
3 Anwendungsfälle für digitale Identitäten bei Übertragungsnetzbetreibern 27
3.1 Eigenschaften energiewirtschaftliche und nicht energiewirtschaftliche Anwendungsfällen 27
3.2 Übersicht ausgewählte Anwendungsfälle 30
3.3 Charakterisierung der Anwendungsfälle 37
4 Ausgestaltung und Analyse von Anwendungsfällen 45
4.1 Use-Case: IKT am Beispiel Maintenance 46
4.2 Use-Case: Vergabe und Verwaltung eindeutiger Identifikationscodes 47
4.3 Use-Case: Präqualifikation von Anlagen für Frequenzhaltung 48
4.4 Use-Case: Redispatch 50
4.5 Use-Case: Zugangsmanagement 51
4.6 Use-Case: Kunden-Datenbank 53
5 Zusammenfassung und Fazit 55

6 Literaturverzeichnis 56

Abkürzungen

API: Application Programming Interface

DID: Decentralized identifier, dezentralisierte Identifikatoren

EEG: Erneuerbare-Energien-Gesetz

EnWG: Energiewirtschaftsgesetz

IAM: Identity and Access Management, Identitätsmanagement

IoT: Internet-of-Things

PKI: Public-Key-Infrastruktur

KWKG: Kraft-Wärme-Kopplungsgesetz

SSI: Self-Sovereign Identity, selbstbestimmte Identität

StromPBG: Gesetz zur Einführung einer Strompreisbremse

VC: Verifiable credentials, überprüfbare Ausweise

1 Einleitung

1.1 Einführung in das Untersuchungsgebiet

Die Digitalisierung ist seit Jahrzehnten eines der vorherrschenden Themen in der Politik, Wirtschaft und Gesellschaft. Zuletzt wurde das Thema durch gesellschaftliche Veränderungen und externe Einflüsse (z.B. Klimakrise, Fachkräftemangel, Corona-Pandemie) noch weiter in den Mittelpunkt der Aufmerksamkeit gerückt (Future Energy Lab, 2022). Hierbei wurden die Schwächen im Bereich der deutschen Digitalisierung offenbart: Deutschland liegt im europäischen Vergleich der digitalen Wirtschaft und Gesellschaft lediglich im Mittelfeld auf dem dreizehnten Platz. Die stetig zunehmende Digitalisierung offenbart jedoch nicht nur Schwächen, sondern auch Chancen und Handlungsbedarfe (Europäische Kommission, 2022). Diese wurden insbesondere durch die Branche der Energie- und Wasserversorgung genutzt, welche im Jahr 2022 den deutlichsten Zuwachs realisieren konnte (BMWK, 2022). Um diese Chancen konsequent weiterhin zu nutzen, hat die Bundesregierung eine Digitalstrategie erarbeitet, in der die Digitalisierung der Energiewende eine große Rolle spielt (BMDV, 2022). Die Digitalisierung der Energiewirtschaft ist eine notwendige Voraussetzung für eines der größten deutschen IT-Projekte und ein Schüsselfaktor für eine erfolgreiche Energiewende (BDEW, 2022).

Eines der zentralen Themen in der Digitalisierung der Energiewirtschaft ist der Umgang mit Daten und Datenströmen (BDEW, 2022). Hierbei geht es insbesondere um das Identitätsmanagement, d.h. die Weitergabe und Verarbeitung von identitätsbezogenen Attributen und Dokumenten und letztlich dem Nachweisen der Identität einer Person oder Maschine (Entitäten) (Future Energy Lab, 2022). Die analoge Welt ist dem Internet hier einen Schritt voraus, da die eigene Identität durch inoffizielle und offizielle Dokumente beispielsweise einen Personalausweis nachweisbar ist. Dieser ist fälschungssicher gestaltet, wird von fast jeder Partei akzeptiert und die Datenhoheit wird gewährleistet, womit ein selbstsouveränes Identitätsmanagement sichergestellt ist. Im Gegensatz dazu ist das digitale Identitätsmanagement im digitalen Raum ein „Flickenteppich“. Es existieren verschiedenste Modelle, bspw. das zentralisierte oder föderierte Identitätsmodell, je-

doch werden die Daten von einer zu vertrauenden zentralen Stelle gespeichert, verwaltet und im Rahmen der Idendität des Nutzers eingesetzt. Weiterhin gewährleistet keiner dieser Ansätze die drei Attribute der Interoperabilität, Sicherheit und Datenschutz zur gleichen Zeit und das Fehlen einer selbstbestimmten digitalen Identität ist damit offensichtlich (Strüker, et al., 2021).

Dieses Defizit im digitalen Identitätsmanagement ist auch ein enormes Hemmnis bei der Digitalisierung der Energiewirtschaft und letztlich der Umsetzung der Energiewende. Insbesondere in einem dezentralen und integrierten Energiesystem (Future Energy Lab, 2022) entstehen große Datenmengen aus Einspeisung, Smart Metering und dem Netzbetrieb, die gemanagt werden müssen (BDEW, 2022). Weiterhin läuft ein Großteil des Informationsaustauschs zwischen diversen Marktteilnehmern bspw. dem Übertragungs- und Verteilnetzbetreiber als auch der Marktkommunikation, trotz existierender IT-gebundenem Datenaustausch, weitestgehend nicht digital und standardisiert. Folglich ergeben sich weiterhin Medienbrüche und digitale Identitäten sind somit unter anderem für Energieanlagen oder Anlagen die Grundvoraussetzung für effiziente und automatisierte Prozesse sowie Kommunikation in der Energiewirtschaft. Gerade im Umfeld der Elektromobilität, deren Ladeinfrastruktur und den damit verbunden Prozessen (z.B. Ladevorgangsabrechnung) findet ein neuer Anlagentyp mit massiven Auswirkungen und Herausforderungen Einzug ins Netz. Diese Auswirkungen und Herausforderungen sind nur durch hohe Digitalisierungsanstrengungen (wie zum Beispiel im Forschungsprojekt BANULA) und neuen Technologien zu bewerkstelligen.

Mit diesen Digitalisierungsprozessen und neuen Technologien gehen herausfordernde Themen wie eine Standardisierung von Software-Schnittstellen, Datensicherheit und -schutz sowie einer adäquaten -ökonomie bzw. Governance einher (Future Energy Lab, 2022).

Ein in der Wissenschaft und Praxis intensiv diskutierter Ansatz ist die „Solf-Sovereign Identity (SSI), welche eine massive Optimierung des Status-quo des digitalen Identitätsmanagements in Aussicht stellt (Schellinger, Sedlmeir, Willburger, Strüker, & Urbach, 2022). SSI zur Verwaltung von Personen- und Maschinenidentitäten soll mithilfe einer Blockchain die beschriebenen Herausforderungen adressieren und stellt einen möglichen adäquaten Lösungsansatz zur weiteren Digitalisierung energiewirtschaftlicher Prozesse dar (Future Energy Lab, 2022). Jedoch kann diese Lösung nicht als „missing key“ gehandelt werden (Richard, Mamel, & Vogel, 2019), da viele technische, regulatorische als auch ökonomische Fragestellungen und Herausforderungen noch nicht geklärt sind (Future Energy Lab, 2022).

1.2 Problem und Zielstellung der Studie

Das Forschungsgebiet der selbstbestimmten digitalen Identitäten (SSI) gewinnt sowohl auf nationaler als auch auf internationaler Ebene in der Politik und Wirtschaft immer mehr an Momentum.

Damit einhergehend sind immer neue und weiterführende Technologien, Konzepte und Varianten, die unter anderem für die Energiewirtschaft einen hohen Mehrwert stiften können (Richard, Mamel, & Vogel, 2019). Durch Studien, Forschungsprojekte und Konsortien wie GAIA-X wird der Einsatz der SSI-Technologie und der mögliche Mehrwert getestet und analysiert.

Eine Vielzahl der Studien sind im Bereich der Elektromobilität, Mobilitätsanwendungen, Prosumer-Anwendungen und digitalen Geschäftsmodellen angesiedelt (Klein, Kaßberger, & Buchwald, 2021). Diese Studien sind für diverse Marktrollen relevant und berücksichtigen daher viele relevante Aspekte. Hierbei werden jedoch keine Untersuchungen zu den Einsatzmöglichkeiten von SSI bei den speziellen Prozessen von Übertragungsnetzbetreibern durchgeführt.

Diese Studie konzentriert sich auf die skizzierte Forschungslücke und soll dazu beitragen ein Verständnis für SSI zu entwickeln sowie mögliche Anwendungsfälle auszugestalten, zu analysieren und dahingehend Handlungsempfehlungen abzuleiten und zu formulieren. Die Ergebnisse können sodann als Basis für tiefergehende Untersuchungen genutzt werden.

Die Studie ist wie folgt aufgebaut: Im Grundlagenteil werden die relevanten theoretischen Konzepte erläutert und definiert. Dabei wird zuerst das Konstrukt der digitalen Identität und damit einhergehend das Identitätsmanagement näher beleuchtet. Im Anschluss daran werden die verschiedenen Modelle abgegrenzt und analysiert. Darauf folgt eine genaue Betrachtung des SSI-Konzepts und den dazugehörigen Technologiebausteinen. Abschließend wird der Grundlagenteil mit dem aktuellen Status zu diversen Entwicklungsprojekten aufgezeigt.

Anschließend werden mögliche Anwendungsfälle für digitale Identitäten im Umfeld der Aufgaben eines Übertragungsnetzbetreibers identifiziert und aufgelistet. Diese beziehen sich sowohl auf die energiewirtschaftlichen Kernaufgaben der Übertragungsnetzbetreiber wie auch auf nicht energiewirtschaftliche Aufgaben. Einige ausgewählte Anwendungsfälle werden in Form von Steckbriefen weiter ausformuliert und beschrieben.

2 Theoretische Grundlagen zu digitalen Identitätsmodellen

Um den gesamtheitlichen Kontext zu verstehen, wird im Folgenden eine grundsätzliche Einführung in die Themen Digitale Identitäten und Identitätsmanagement (Kapitel 2.1) sowie Modelle des Identitätsmanagements (Kapitel 2.2) gegeben.

2.1 Digitale Identitäten und Identitätsmanagement

Eine Identität erlaubt die eindeutige Identifizierung einer Person oder Maschine (Future Energy Lab, 2022) und umfasst sämtliche Informationen, die mit ihr in Zusammenhang stehen (Clauß & Köhntopp, 2001). Digitale Identitäten stellen Personen, Organisationen und weitere Entitäten im digitalen Raum dar. Identitätsbestandteile sind beispielsweise Name und Anschrift sowie weitere Angaben zu Bank-/ Kunden-/ oder Steuernummern. Diese werden für den Zugang zu Ressourcen oder digitalen Dienstleistungen wie bspw. Online-Banking oder Mobilitätsangebote benötigt (Afting, 2021). Vor Nutzung bedarf es einer Authentifizierung und Autorisierung (Richter, Identitätsmanagement , 2022). Die Authentifizierung wird in der analogen Welt häufig durch ein offizielles Dokument, wie beispielsweise einen Personalausweis durchgeführt. Im digitalen Raum wird die Identität typischerweise durch diverse Nutzeraccounts mit Passwörtern verwendet. Nach erfolgreicher Authentifizierung erfolgt sodann die Autorisierung seitens des Anbieters (Richter, Identitätsmanagement , 2022). Durch die stark fortschreitende Digitalisierung und der damit einhergehenden Anzahl von digitalen Diensten, Interaktionen sowie dem Authentifizierungs- und Autorisierungsprozess, wird das Identitätsmanagement immer stärker fokussiert und erhält kontinuierlich mehr Aufmerksamkeit (Strüker, et al., 2021).

Das digitale Identitätsmanagement ermöglicht das informationelle Selbstbestimmungsrecht (Clauß & Köhntopp, 2001) und dient als System zur Verwaltung, Kontrolle und Übermittlung persönlicher Daten im digitalen Raum (Baier, 2005). Einhergehend hiermit ist die nachfolgende Definition: „Der Zweck des Identity and Access Management (IAM) ist die Vielzahl der Kennungen und personenbezogenen Informationen welche die Anwender für den Zugriff auf Applikationen, Ressourcen und

IT-Systeme benötigen, zu reduzieren und nach Möglichkeit in einer einzigen digitalen Identität zusammenzufassen“ (Richter, Identitätsmanagement, 2007).

2.2 Modelle des Identitätsmanagements

Der Sachverständigenrat für Verbraucherfragen hat im Zusammenhang digitaler Souveränität vier Leitlinien Wahlfreiheit, Selbstbestimmung, Sicherheit und Selbstkontrolle definiert (netzpolitik.org, 2023). Der Nutzer muss die Wahlfreiheit haben, welche personenbezogene Daten durch Dritten sichtbar gemacht werden oder auch nicht. Die Selbstbestimmung der Datenhoheit ist nicht per se gegeben, sollte aber dem Nutzer die Entscheidungshoheit über die Art der Verwendung seiner Daten ermöglichen, also ob die Daten beispielsweise nur anonymisiert weitergegeben werden dürfen. Die Datenhaltung/-speicherung, -erhebung und -weitergabe muss in einem geschützten Datenraum stattfinden. Grundsätzlich kann die Verwaltung von Identitätsdaten in ein dezentrales und zentrales Identitätsmanagement unterschieden werden, welche sich in deren funktionsweise und damit in vier Modelle unterscheiden lassen. Die vier existierenden Modelle unterscheiden sich in der Verantwortung und dem Management der zu verwaltenden Identitäten. Abbildung 1 gibt einen zusammenfassen Überblick der vier Modelle, welche im Nachfolgenden näher erläutert werden.

2.2.1 Zentrales Identitätsmanagement

Im Bereich des Identitätsmanagements werden weitestgehend personen- und maschinenbezogene Daten in einem zentralen Rechenzentrum gespeichert. Zentrale Identitätsmodelle sind inhärent von einer zentralen Partei geführt, in dessen Abhängigkeit sich ein Anwender begibt und dadurch stückweise seine digitale Souveränität verliert. Zentrale Modelle sind „zentral“, „nutzerorientiert“ und „föderiert“ gem. Abbildung 1.

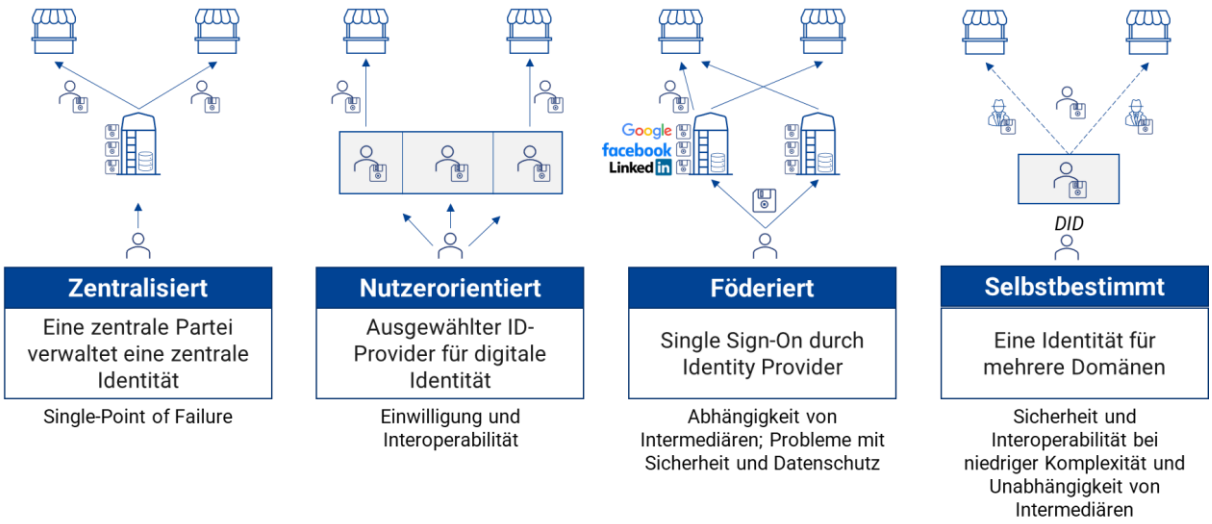


Abbildung 1: Modelle des Identitätsmanagements (Quelle: adaptiert nach Strüker et al. 2021, S. 12)

Zentralisiertes Identitätsmodell

Das zentralisierte Modell weist einer zentralen Partei, z.B. dem Administrator einer Organisation, die Datenhoheit einer digitalen Identität zu. Hierbei entscheidet der Administrator über die Wichtigkeit einzelner Daten und kann über deren Verwendung sowie Löschung verfügen. Dies verpflichtet die zentrale Partei dazu, eine abrufbare und sichere Datenspeicherungsinfrastruktur aufzubauen. Insgesamt bedeutet Obengenanntes, dass eine einzelne Organisation selbst den Verifikationsprozess, die Datenspeicherung sowie den Schutz der Daten für die benötigten digitalen Identitäten des Services übernimmt (Allen, 2016). Folglich ist der Nutzer von der zentralen Partei abhängig, wie diese mit dessen Daten umgeht, bzw. einen Löschungswunsch der Nutzerdaten ausführt. Des Weiteren besteht die Gefahr von technologischen bzw. partei-spezifischen Lock-In Effekten, so dass ein Anwender für jede Organisation/Partei jeweils eine eigene digitale Identität besitzt und verwaltet diese mit verschiedenen Zugängen.

Für Unternehmen bietet das zentralisierte Identitätsmodell eine einfache Implementation und Datenführung. Durch die zentralisierte Datenführung kann der Administrator selbst über die Verifikation und Datenangaben verfügen. Somit besteht kein Bedarf nach einem externen Verifikationsprozess der benötigten Daten (Fusillo, 2021).

Die Handlungsfreiheit einer Organisation bezüglich der digitalen Identitäten der Nutzer kann jedoch aus der Anwendersicht einige Risiken mit sich führen. Eine einzige Autorität hat das Recht die digitale Identität zu bestätigen oder abzulehnen. Dies gibt zentralisierten Hierarchien einen großen Teil der Macht. Zudem entsteht durch die zentrale Ansammlung von Nutzeraktionen der Identitäten bei einer Partei eine für den Nutzer nicht-bestimmbare Offenlegung an übergeordneten Informationen, welche eine zentrale Partei für sich ohne Einwilligung des Anwenders nutzbar macht. Hierzu gehört unter anderem die Auswertung des Nutzerverhaltens mehrerer MitarbeiterInnen bzgl. Softwarenutzung, etc. Des Weiteren besteht eine fehlende Interoperabilität, da Endnutzer für das Verwenden von verschiedenen Diensten mehrere Identitäten benötigen. Durch die Vielzahl an Identitäten entsteht aus Sicht des Nutzers eine Redundanz in der Datenspeicherung, die zu übermäßigem Datenverkehr und potenziellen Inkonsistenzen führt. (Tönsing, 2015). Falls ein Anwender die Daten löschen möchte, ist dies nur durch den Administrator durchführbar, wodurch der Dateninhaber die Datenhoheit verliert (Strüker, et al., 2021).

Nutzerorientiertes Identitätsmodell

Das nutzerorientierte Identitätsmodell bietet eine Datenstruktur, die dem Nutzer die administrative Kontrolle seiner Daten über mehrere Autoritäten überlasst. Hier wird insbesondere Wert auf die Einwilligung der Anwender gelegt. Die Daten werden somit nicht mehr administrativ, sondern je Dienst vom Nutzer selbst kontrolliert. Dazu gehört die Freigabe jeweiliger Daten für die verschiedenen Dienste (Allen, 2016).

Die Nutzer geben ihre Daten selbst an den jeweiligen Dienst weiter und haben die Macht darüber, welche Daten sie weitergeben. Somit besitzt der Nutzer für jeden Dienst eine andere digitale Identität. Dies führt zu einer Ansammlung an Zugangsdaten und unübersichtlichen Datenübermittlungsstrukturen. Durch das Erstellen verschiedener Accounts verliert der Nutzer die Übersicht, welche Daten er weitergibt und welche Passwörter er vergibt. Da einige User aus diesem Grund einfache Passwörter oder gleiche Passwörter verwenden, entsteht das Risiko des Datenklaus. Abhilfe können hierbei Passwort-Safes schaffen, die die Zugangsdaten zu jedem Account speichern, jedoch bringen diese auch ein Sicherheits-Risiko mit sich.

Des Weiteren können die verschiedenen Identitäten nicht miteinander kommunizieren, wodurch jede Verifikation vereinzelt stattfindet. Dies verlängert den Prozess des Nachweises von Echtheit. Somit bietet sich dieses Identitätsmodell nicht bei Kommunikationsstrukturen an, die in Echtzeit Identitäten verifizieren müssen.

Föderiertes Identitätsmodell

Das föderierte Identitätsmodell delegiert die administrative Kontrolle an mehrere Autoritäten, die in einem föderalistischen Geflecht agieren (Allen, 2016). Dieses Prinzip findet zum Beispiel bei einem Single Sign-On Anwendung, wobei Nutzer die Möglichkeit haben mit einem Konto mehrere Applikationen einer Organisation zu verwenden. Das bedeutet, dass ein dediziertes Unternehmen als Identitäts-Provider agiert und für mehrere Services eine Identität bietet. Somit liegt die Verantwortlichkeit der Verifikation, der Datenhaltung und der Sicherung der Daten in den Händen des ID-Providers (Strüker, et al., 2021).

Durch die Trennung der Kontrolle und der Verwendung der Identitätsdaten verschwindet die Hürde der vielen Identitäten, da einer bzw. wenige Identitäts-Provider die Datenhoheit übernimmt.

Da jedoch per Definition kein Datenmonopol herrscht, agieren mehrere ID-Provider auf dem Markt. Somit ist das Auftreten von mehreren Identitäten nicht vollständig behoben. Zudem birgt die Übermittlung zwischen dem Identitätsinhaber, dem ID-Provider und dem Online-Dienst eine mögliche Schnittstelle für Cyber-Angriffe, die in dem Fall eines einzelnen Administrators der Daten zu einem Single-Point of Failure führen (Strüker, et al., 2021). Des Weiteren ist die Freigabe der Daten an einen bestimmten ID-Provider, um die Dienste einer Organisation zu nutzen, notwendig, da eine Organisation zumeist nur mit einem Provider kooperiert. Falls der Anwender jedoch den Zugriff für den jeweiligen ID-Provider verweigert, bekommt dieser auch keinen Zugriff auf diesen. Anstelle eines Identitätsmanagements, welches das Prinzip des Föderalismus folgt, läuft das föderierte Identitätsmodell Gefahr, dass eher eine Oligarchie entsteht (Allen, 2016).

2.2.2 Dezentrales Identitätsmanagement

Selbstbestimmtes Identitätsmodell

Die sogenannte Self-Sovereign Identity, oder auch SSI genannt, ist eine Form der Verwaltung der eigenen digitalen Identität. Anstelle eines Dienstleisters oder Providers, bleibt die Kontrolle über die Daten bei dem Dateninhaber selbst. SSI ermöglicht, dass mittels einer digitalen Identität, nur der Inhaber der Identität selbst entscheiden kann, wem welche Daten preisgegeben werden. Das Ziel ist es, die Kontrolle über die Daten dezentral, bei jedem einzelnen Anwender zu behalten und nur die notwendigen Angaben (selective disclosure) offenlegen zu müssen (Kunert, 2021).

Die SSI-Umgebung besteht aus drei primären Rollen: Issuer, Holder und Verifier. Bei dem Issuer handelt es sich um einen vertrauenswürdigen Herausgeber der digitalen Identität, wie z. B. der Bundesnetzagentur. Diese beglaubigt mit der Herausgabe der digitalen Identität die Echtheit der Holder-Daten. Der Holder ist der Halter/Inhaber der Daten, welcher seine Identität dem Verifier (z.B. Stadtwerk) beweisen muss (Kunert, 2021). Damit dieses Ökosystem funktioniert bedarf es einer Datenbank, die die digitalen Identitäten sowie die zugehörigen Schlüssel speichert.

Für diesen Zweck können der Issuer und der Verifier mit einem Verifiable Data Registry interagieren, welche durch eine dezentrale Datenbank dargestellt wird. Dezentrale Datenbanken werden zumeist als Blockchain realisiert (Mamel, Babilon, Richard, Schlösser, & Seiter, 2022). Dezentrale Konzepte bzw. SSI bieten im Vergleich zu zentralen Identitätsmodellen einige Chancen in Bezug auf ein gesamtheitlich effizientes und digitales Energiesystem, da Datenmengen und Rechenkomplexität reduziert werden können.

Die SSI-Umgebung ist in der folgenden Abbildung 2 veranschaulicht.

Eine Identität ist im Kontext der Dezentralisierung die Summe von Merkmalen und Attributen, die eine Entität beschreiben. Hierbei sollte der Fokus auf den Begriff Entität liegen, da nicht nur Menschen digitale Identitäten zugewiesen werden, sondern auch Maschinen. Um eine digitale Identität unverwechselbar zu identifizieren, wird jeder Entität eine eindeutige Kennung, einem sogenannten Decentralized Identifier (DID), zugewiesen.

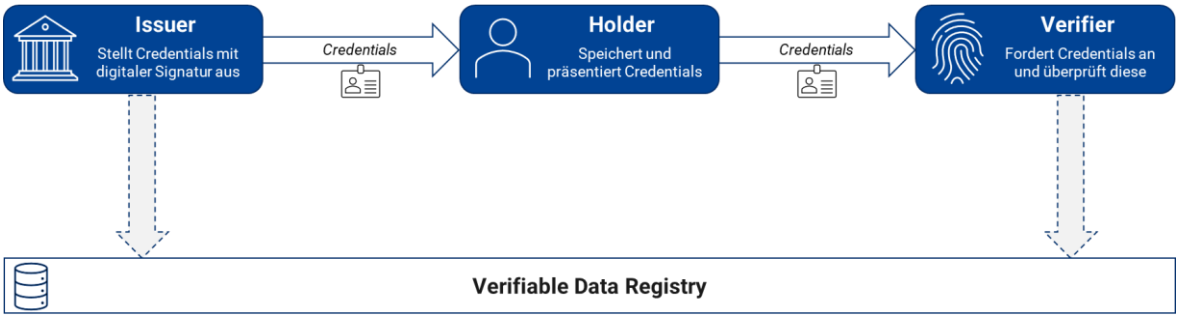


Abbildung 2: SSI Umgebung

Statt des Begriffs Attribut wird häufiger der Term Verifiable Credential (VC) verwendet. Ein VC stellt die Sammlung von mehreren Claims und der Proofs, also Beweisen, dar. Die Claims sind eine Abbildung der Eigenschaften. Ein Verifiable Credential ist somit ein Zertifikat, welches mehrere Eigenschaften beinhaltet. Mit einem passenden Schlüssel können nun selektiert die Claims freigegeben werden und ohne überschüssige Informationen weiterzugeben, ausgelesen werden (Mamel, Babilon, Richard, Schlösser, & Seiter, 2022). Bezüglich der Schlüssel ist es in dem Kontext noch von Interesse den Begriff Public-Key-Infrastruktur (PKI) einzuführen. Diese Infrastruktur basiert auf einem hierarchischen System zur Ausstellung, Verteilung und Prüfung von digitalen Zertifikaten. Die Verschlüsselung von Daten erfolgt hierbei asymmetrisch. Genanntes bedeutet, dass für jede Kommunikationsanfrage ein Schlüsselpaar aus einem privaten, also einem geheimen, und einem öffentlichen Schlüssel erstellt wird. So kann eine mit dem öffentlichen Schlüssel verschlüsselte Datei nur mit dem privaten Schlüssel entschlüsselt werden. Verifiable Credentials enthalten dabei den öffentlichen Schlüssel und der Anfrager der Kommunikation den privaten Schlüssel (BSI, o.D.).

Auf Grund der dezentralen Speicherung wird das Löschen von Daten erschwert. Dies schmälert die Akzeptanz der selbstbestimmten Identitäten, jedoch ist das Abrufen der Daten ohne einen passenden Schlüssel unmöglich.

Somit bietet SSI eine Reihe an Chancen, die das Identitätsmanagement neu definieren. Durch die Rollenverteilung besteht ein effizientes Geflecht der Arbeitsteilung und ermöglicht Echtzeit-Verifikation. Dadurch werden manuelle Prozesse, die bei der Prüfung von Daten oft Redundanzen aufweisen, eliminiert und durch eine hochverschlüsselte Datenstruktur ersetzt. Dies ermöglicht die bereits erwähnte Interoperabilität. Zudem ist besonders für die Entität ein Modell geschaffen, welches die Datenhoheit bei der Entität belässt und eindeutige Transparenz zur Datenverarbeitung aufweist (Strüker, et al., 2021).

Hiervon würde auch insbesondere die Energiewirtschaft profitieren. Die kleinteilige Struktur der Energiewirtschaft und die verstreuten Standorte der verschiedenen Anlagen bieten eine prädestinierte Marktlandschaft für die Implementation von dezentralen Datenbanken. Hinzu kommt der permanente Austausch über das Angebot und die Nachfrage von Strom und Gas (Knüsel & Richard, 2022). Diese Systemkonstellation kann über selbstbestimmte Identitäten organisiert werden. Im Folgenden werden Chancen einer selbstbestimmten Identität im Kontext der Energiewirtschaft genannt und erläutert.

Um eine Grundlage für den Automatisierungsbedarf wie zum Beispiel für Smart Meter Gateways zu schaffen, bedarf es einer Infrastruktur für dezentrale Kommunikation. In diesem Gebiet schaffen selbstbestimmte Identitäten das Fundament für eine automatisierte Kommunikation über die gehandelten Güter Strom und Gas (Mamel, Babilon, Richard, Schlösser, & Seiter, 2022).

Durch die digitale Identität wird Maschinen als auch Personen ermöglicht nur benötigte Daten zu teilen und keine überschüssigen Informationen bereitzustellen. Ein weiterer Punkt ist, dass für die Übermittlung selbst keine Kosten anfallen und dies in Echtzeit stattfindet. Die einzigen Kosten fallen für die Infrastruktur an, die einmalige Kosten mit sich bringen und die laufenden Stromkosten für die Verarbeitung der Daten sowie dem Betrieb der Datenbank (Mamel, Babilon, Richard, Schlösser, & Seiter, 2022).

Um die Daten dezentral speichern, aktualisieren und verifizieren zu können, bedarf es einer Datenbank. Hierfür gibt es verschiedene Möglichkeiten. Im Folgenden werden verteilte Datenbanken, verteilte Verzeichnisdienste und DLT-basierte Register weiter erläutert. Tabelle 1 fasst die relevanten Begriffe im Zusammenhang mit der SSI-Technologie zusammen.

Tabelle 1: Übersicht Begriffe SSI Quellen: (Future Energy Lab, 2022), (Strüker, et al., 2021)

Begriff	Definition
Self-Sovereign Identity (SSI)	Digitales Modell des Identitätsmanagements zur Verwaltung von Entitäten
Verifiable Credentials	Digital signierte Sammlung von Attributen einer Entität
Claims	Behauptungen über die Eigenschaften einer Entität
Decentralized Identifier (DID)	Identifikationskennung, die eine Entität identifiziert. Standard, der eine Ende-zu-Ende Kommunikation gewährleistet.
Issuer	Die Entität, die VCs an einen Holder ausstellt
Holder	Die Entität, die derzeit die VCs hält und sie dem Verifier vorlegt.
Verifier	Die Stelle, die die VCs vom Holder erhält. Im Gegenzug liefert der Verifier Leistungen.
Verifiable Data Registry	Ein über das Internet zugängliches Register, das alle wesentlichen Daten und Metadaten enthält, die den Betrieb des VC-Ökosystems ermöglichen.

2.2.3 Eckpunkte für SSI und Technologiebausteine

Verteilte Datenbanken

Während die Daten einer zentralen Datenbank zumeist auf einem Server gespeichert werden, werden diese bei einer verteilten Datenbank auf unterschiedlichen Servern hinterlegt, die räumlich sowie örtlich voneinander getrennt sind. Für den Endnutzer unterscheiden sich zentrale und verteilte Datenbanken im Abruf primär nicht. Die Systemstruktur ist so aufgebaut, dass die gespeicherten Daten über eine Schnittstelle abgerufen werden können. Jedoch bieten die verteilten Datenbänke in der Performance, Kosteneffizienz und der Ausfallsicherheit Vorteile. Da das Datenbankmanagementsystem aus mehreren Rechnern bzw. Servern besteht, sind diese bei der Verarbeitung von Daten deutlich schneller. Dies liegt an der verteilten Last. Endnutzer greifen nie alle zugleich auf eine Datenbank zu, sondern auf viele Verschiedene. Somit ist die Last auf eine einzelne Datenbank gering. Damit einher geht auch die Kosteneffizienz. Um mit einer einzelnen zentralen Datenbank eine große Menge von Anfragen zu verarbeiten, wird eine sehr kostspielige Datenbank-Infrastruktur benötigt. Im Vergleich dazu sind mehrere leistungsschwächere Server nicht nur günstiger, sondern auch stabiler im Abruf. Ein weiterer Vorteil ist, dass es keinen Single-Point of Failure gibt. Falls ein System ausfällt, bleiben die anderen noch bestehen. Zudem besteht die Möglichkeit von Kopien, sodass Nutzer im Ausnahmefall trotz eines Ausfalls, Zugriff auf ihre Daten haben (Datenbanken-Verstehen, 2022).

Bezüglich der Datenspeicherung gibt es zwei verschiedene Möglichkeiten: die Replikation und die Fragmentierung. Wie der Name Replikation schon indiziert, werden hierbei die Datenbanken repliziert. Das bedeutet, dass die Server an verschiedenen Orten platziert sind und die Redundanzen bei der Vermeidung von Datenverlust helfen. Jedoch muss das System so kommunizieren, dass alle Datenbanken aktuell gehalten werden, sodass keine veralteten Daten als Back-Up dienen. Bei der Fragmentierung werden Datenteilmengen auf die verschiedenen Datenbanken aufgeteilt. So können die Daten nach bestimmten Kriterien aufgeteilt werden. Die beiden Arten Replikation und Fragmentierung können zudem auch als Hybridlösung eingesetzt werden (Kraus, 2021).

Verteilte Verzeichnisdienste

Soll ein Netzwerk aus mehreren Endgeräten aufgebaut werden, die alle verschiedene administrative Berechtigungen und Zugriffe besitzen sollen, so bietet sich ein verteilter Verzeichnisdienst zur Datenverwaltung an (Joos & Donner, 2018). Der Verzeichnisdienst bietet die Möglichkeit eine Sammlung von Daten baumartig zu strukturieren. Dank dieser Struktur kann einer Vielzahl von Objekten verschiedene Werte zugewiesen werden. Durch den Aufbau des Verzeichnisdienstes entstehen insbesondere folgende Aufgaben: Verteilung der Verzeichnis-Struktur auf mehrere Server, Vererbung von Eigenschaften der Objekte, Verwaltung und Authentifizierung von Benutzern (Elektronik Kompendium, o.D.).

Distributed Ledger Technology (DLT)

Im Gegensatz zu der verteilten Datenbank und der verteilten Verzeichnisdienste basiert ein Distributed Ledger auf einer anderen Datenhaltungsstruktur. Bei einem Distributed Ledger, auch verteiltes Kassenbuch genannt, gibt es keine zentrale Datenhaltung oder Verwaltungsfunktion. Somit hat jeder Schreib- und Lesezugriff. In einem Ledger können autorisierte Nutzer folglich neue Datensätze hinzufügen. Falls neue Daten in das Ledger hinzugefügt werden, wird die Datenbank aktualisiert, sodass jeder Teilnehmer auf den neuesten Stand der Datenbank Zugriff hat (ComputerWeekly, 2022). In der Ausgestaltung von DLTs werden zwei verschiedene Arten abhängig von den Zugangsmöglichkeiten der Teilnehmer in einem Netzwerk unterschieden: permissioned und unpermissioned Ledgers. Bei unpermissioned Ledgers, welche meist öffentliche Blockchains sind, , werden bzw. wurden primär Proof-of-Work-Mechanismen eingesetzt, um ein maximales Sicher-

heitslevel für Datentransaktionen und Schreiben eines Blockes in Netzwerk (Validierung von neuen Dateneinträgen) zu erhalten, da keine Prüfung des Anwenders zur Teilnahme notwendig ist. Bei einem permissioned Ledger wird jedoch häufiger mit Proof-of-Stake, proof-of-Authority oder PBFT-Konsensmechanismen gearbeitet, die bereits bei der Zulassung zum Netzwerk eine Vertrauensbasis schafft (Metzger, 2022). Hierbei sei hinzuzufügen, dass Proof-of-Work und Proof-of-Stake zwei verschiedene Konsensmechanismen sind, um Transaktionen zu validieren und verifizieren. Im Proof-of-Work Konsens wird im Blockchain-Netzwerk eine Einigung erzielt, um Transaktionen zu validieren und neue Blöcke in der Kette hinzuzufügen (Moreland, 2019). Beim Proof-of-Stake wird wiederum in Abhängigkeit von der gehaltenen Coins-Anzahl entschieden, wer den nächsten Block in der Blockchain validiert (Moreland, 2019). In 2021 wurde Ethereum von einem proof-of-Work auf einen proof-of-stake Validierungsmechanismus migriert. Dies bietet den Vorteil zu geringeren Kosten und in schnellerer Zeit sowie geringerem Energieverbrauch Blöcke zu validieren. Ethereum bietet den Vorteil einer public Blockchain und ist die neutralste IT-Infrastruktur, welche die Möglichkeit von smart contracts ausübt. Polkadot ist eine open-source Multi-Chain-Plattform, welche versucht verschiedene Vorteile von Blockchainplattformen (z.B. permissioned) miteinander zu kombinieren und insbesondere skalierbar zu sein. Hyperledger ist ebenfalls ein open-source-Dachprojekt von IBM, SAP und Intel mit einem starken unternehmensbezogenen Fokus, z.B. private permissioned Blockchains. In einem Smart Contract sind mithilfe eines Codes Bedingungen gespeichert, die automatisch geprüft werden und bei Einhaltung eine Transaktion auslösen. Somit werden manuelle Aufwände, die Zeit und Geld kosten, minimiert.

Im Folgenden werden vier DID-spezifische Plattformen auf Basis von DLT kurz vorgestellt.

Hyperledger Indy

Hyperledger Indy bietet eine Open-Source Grundlage für Transaktionen mit digitalen Identitäten auf einer Blockchain-Basis. Durch die Distributed Ledger Technology ist es möglich replizierbare Komponenten wie eine digitale Identität zu erzeugen und zu verwalten. Die zu den digitalen Identitäten zugehörigen DIDs können ohne eine zentrale Institution entschlüsselt werden. Bezüglich der Selective Disclosure ermöglicht Hyperledger Indy u.a. die Validierungsmethodik Zero Knowledge Proofs. Dies sind Beweise, dass die Claims in einer DID bewiesen sind ohne zusätzliche Informationen darzulegen (Kuhrt & Bohan, 2022).

.

Hyperledger Aries

Hyperledger Aries wird als Instrument definiert, welches sich auf die Erstellung, den Transfer sowie die Speicherung digitaler VCs fokussiert. Dieses Konstrukt ist aus dem zuvor erarbeiteten Hyperledger Indy hervorgegangen (Hyperledger Foundation, 2022).

Im Gegensatz zu Hyperledger Indy liegt der Fokus bei Hyperledger Aries eher auf dem Austausch von Transaktionen über eine Blockchain. Der Ledger bietet eine Infrastruktur, um verifiable credentials peer-to-peer auszutauschen. Zudem besteht die Möglichkeit über ein verschlüsseltes Nachrichtensystem namens DIDComm, auf den DIDs basierend, zu kommunizieren (Huseby & Bohan, 2022).

EW-DOS

Das Energy Web Decentralized Operating System (EW-DOS) ist eine weitere blockchain-basierte Open-Source Infrastruktur, welche auf Ethereum aufsetzt. Diese Technologie wird mit Fokus auf die Energiewirtschaft entwickelt.

Insbesondere zwei Herausforderungen der Energiewirtschaft sollen mit dem EW-DOS behoben werden. Zum einen soll ein skalierbarer Zugang zu Netzflexibilität über Decentralized Energy Resources ermöglicht werden. Des Weiteren soll ein offener und skalierbarer Marktplatz für transparenten und effizienten Energiehandel von erneuerbaren Energien ermöglicht werden (Energy Web Foundation, 2022).

EW-DOS soll den Marktteilnehmern ermöglichen die kohlenstoffarmen Energieanlagen, Gebäude und Kunden zu integrieren und zu orchestrieren, die das Netz des 21. Jahrhunderts ausmachen. EW-DOS bietet die Möglichkeit als Industriestandard genutzt zu werden, wodurch die Marktteilnehmer ein gemeinsames Betriebssystem nutzen könnten (Energy Web, 2020).

KILT-Protokoll

Das KILT-Protokoll ist ein Open-Source-Blockchain-Protokoll und baut auf Polkadot auf, welches eine Basis für digitale Identitäten bietet. Es ermöglicht die Erstellung von digitalen Identitäten, die Beschreibung von Eigenschaften und das Bestätigen der Daten von Issuern (Future Energy Lab, 2022). Hierbei werden die Daten privat und im Besitz des Eigentümers gehalten. KILT kann auch verwendet werden, um Identifikatoren für Maschinen, Dienste und alles, worauf Identitäten aufgebaut werden können, zu erstellen (KILT Protocol, 2022).

Walt.Id

Walt.Id stellt eine open-source Wallet und Identitätsstruktur bereit , welche für eigene Anwendungsfälle genutzt werden können. Im Rahmen des Gaia-X Projektes moveID (https://moveid.org/) wird auf Basis des Technologie-Stacks eine Park & Chgarge-Lösung angeboten. Das online Wallet kann VCs, DIDs, Keys und NFTs anzeigen. walt.id basiert auf EBSI (European Blockchain Services Infrastructure) und dem Identitätsmanagement-Kodex von ESSIF (European Self Sovereign Identity Framework), welche von der EU-Kommission betrieben wird.

2.3 Status Quo: Projekte zu SSI im energiewirtschaftlichen Bereich

Die enorme Aufmerksamkeit die SSI momentan erhält, spiegelt sich in einer großen Anzahl von Studien und Forschungsprojekten. Um den aktuellen Stand der Forschung in Bezug auf die Energiewirtschaft zu skizzieren, werden im Folgenden drei relevante Projekte vorgestellt und näher beleuchtet.

2.3.1 BMIL – Blockchain Machine ID Ledger und Dive

Das Future Energy Lab konzentriert sich in dem Pilotprojekt: „Blockchain Machine Identity Ledger" auf die Etablierung eines Registers mit digitalen Maschinenidentitäten mithilfe einer Blockchain-Technologie. Das Ledger bietet eine effiziente Infrastruktur, um ein vollständig dezentrales Anlagenregister mit Millionen von dezentralen Erzeugungsanalgen zu führen. Die SSI-Technologie wird in diesem Kontext genutzt, um eine standardisierte und sichere digitale Identität für Erzeugungsanlagen zu erstellen und damit schließlich digitale Vertrauensketten zwischen diversen Marktakteuren sicherzustellen. Für die SSI-Technologie sind zwei Alternativen vorzustellen: zum einen das KILT-Protokoll zum Ausstellen von DID und VC sowie alternativ Energy Web Registry als Teil des EW-Decentralized OS.

Durch die Verknüpfung des Registers und den digitalen Identitäten für Energieanlagen mit der SMGW-Infrastruktur wird ein automatisierter An- und Abmeldeprozess der Anlagen sowie die effiziente Teilnahme am Energiemarkt gewährleistet. Hierzu wurden in dem Projekt drei verschiedene Verknüpfungsvarianten erarbeitet

und hinsichtlich technischer, rechtlicher und wirtschaftlicher Aspekte analysiert und bewertet.

Für die Realisierung des konkreten Anwendungsfalls müssen weitergehende Zusammenarbeiten mit diversen Stakeholdern sowie eine pilotenhafte Erprobung und Implementierung angestrebt werden (Future Energy Lab, 2022).

Diese Zusammenarbeit ist im Nachfolgeprojekt DIVE - Digitale Identitäten als Vertrauensanker im Energiesystem geplant und in der Umsetzung. Hier geht es darum Fehlern in klassischen Systemen mit der SSI-Technologie entgegenzuwirken. So ergeben sich typischer weise entlang der Wertschöpfungskette Medienbrüche, doppelte Datenhaltung bewirken Inkonsistenzen, Datensilos müssen aufwendig interoperabel in Prozessketten eingebunden werden und der Aufwand zur Einhaltung von Datenschutzbestimmungen verhindert mehrwertige Umsetzungsideen. In diesem Projektansatz verwalten digitale Identitäten Attribute und Zertifikate selbstbestimmt durch den Kunden oder dem digitalen Asset. Anlagenattribute werden so dezentral in einer digitalen Wallet gehalten und können über ein Identitätsregister adressierbar werden. So werden mit digitalen Identitäten perspektivisch Kleinstflexibilitätsanalgen automatisiert zum Beispiel in die Redispatch-Prozesse integrieren. Stammdaten werden nicht mehr in Silos gehalten, sondern sind immer aktuell mit höchstem Genauigkeitsgehalt.

2.3.2 GAIA-X 4 moveID

Das Forschungskonsortium GAIA-X beschäftigt sich in dem Projekt moveID mit dem Datenaustausch digitaler Services für (Elektro-) Fahrzeuge. Zu den Projektzielen gehören unter anderem der Austausch zwischen Fahrzeugen, Ladesäulen, Schranken, Lichtsignalanlagen sowie Parkplätzen. Das Forschungsprojekt soll eine Grundlage für die barrierefreie Kommunikation der Infrastruktur gewährleisten und somit eine Basis für Elektromobilität im digitalen Raum schaffen.

Für die Realisierung werden digitale Identitäten genutzt, um den Austausch von Maschinen untereinander zu ermöglichen. Als Grundlage werden bei diesem Projekt die bereits vorgestellten SSI-Technologien Hyperledger Indy und Aries verwendet. Der Austausch mit Schranken und Lichtsignalanlagen bietet die Möglichkeit für flüssigeren Verkehr und kürzere Standzeiten, wodurch der hohe Verbrauch von

Fahrzeugen durch den Start-Stopp-Verkehr in Städten sinkt. Zudem ist die Kommunikation von Fahrzeugen und Ladesäulen von Interesse, um eine simple und transparente Plattform von verfügbaren Ladesäulen in der Nähe oder auf der Route zu bieten. Dies bietet zudem für das Energiemanagement die Chance Prognosen zu erstellen, an welcher Ladesäule wie viel Strom benötigt wird (BOSCH, 2022).

2.3.3 energy data-X

Energy data-x ist ein Konsortium, welches sich mit dem Aufbau eines „Energy Data Spaces“ auseinandersetzt bzw. die Entwicklung eines Datenraum-Prototypen für die Energiewirtschaft. Dieser soll einen interdisziplinären Austausch zwischen Marktpartnern und die Vernetzung von Sektoren sicherstellen.

Durch den Einsatz von DID und SSI sollen relevante Daten aus unterschiedlichen externen IT-System gesammelt und zum weiteren Austausch sowie zur Verarbeitung bereitgestellt werden.

Der Fokus liegt in dem Projekt auf vier Themengebieten:

1. Einsatz von Künstlicher Intelligenz für Netzbetriebsprozesse, bspw. Leistungs- und Lastflussprognosen

2. Optimierung von Algorithmen für eine präventive Instandhaltung und Verfügbarkeitsvorhersagen basierend auf Anlagen- und Betriebsdaten

3. Weiterentwicklung von Smart-Meter-Gateways für einen optimierten Datenaustausch

4. Ermöglichung von Effizienz und Transparenz durch die Umsetzung neuer Varianten der Marktkommunikation

Durch den Energy Data Space sollen datenbasierte Innovationen gefördert werden, um somit einen Beitrag zur nationalen und europäischen Energie- und Klimapolitik zu leisten (Krengel, 2021).

3 Anwendungsfälle für digitale Identitäten bei Übertragungsnetzbetreibern

Der wachsende Bedarf nach Automatisierung und Regulierung schafft die Notwendigkeit von sicheren Vernetzungen zwischen Entitäten auch in den Handlungsfeldern von Übertragungsnetzbetreibern. Da Übertragungsnetzbetreiber insbesondere für den Betrieb überregionaler Stromnetze im Höchstspannungsbereich verantwortlich sind, haben sie eine hohe Anzahl an Berührungspunkten mit Entitäten. Dies können physikalische Systeme oder Komponenten (Assets), oder auch (Markt-)Partner sein.

3.1 Eigenschaften energiewirtschaftliche und nicht energiewirtschaftliche Anwendungsfällen

In enger Zusammenarbeit mit der TransnetBW unterstützt von Kooperationspartnern konnten bei der Betrachtung von Prozessen der TransnetBW, stellvertretend für klassische ÜNB-Aufgaben, insgesamt 35 Arbeitsfelder identifizieren werden, die die Möglichkeit für eine selbstbestimmte digitale Identität bieten. Außerdem floss in die Prozessanalyse zusätzliche Praxiserfahrung aus dem ÜNB-Umfeld ein.

Zur Beschreibung der Anwendungsfall sind verschiedene Attribute zugeordnet. Hierzu gehören unter anderem das Handlungsfeld innerhalb der ÜNB und die Kategorie des Anwendungsfalls sowie eine kurze generelle Erläuterung des energiewirtschaftlichen Anwendungsfalls. Das Thema deckt hierbei den Geschäftsbereich ab, indem der Anwendungsfall stattfindet. Zu den Themen gehören der Bau von Anlagen, Beschaffungsmanagment, der Betrieb, die Abwicklung von Gesetzen (EnWG, EEG, StromPBG und KWKG), das Gebäudemanagement, der Bereich IT, die Netzplanung, die Organisations- und Verwaltungseinheiten, die Netzwirtschaft die Systemdienstleistung und das Vertragsmanagement.

Die Einsatzmöglichkeiten einer digitalen Identität im energiewirtschaftlichen Zusammenhang sind im ersten Schritt identifiziert und anschließend in unterschiedliche Kategorien aufgeteilt. Hierzu gehören folgende Eigenschaften: Autorisierung, Zertifizierung, Authentifizierung, IoT („Internet-of-Things“), Stammdaten und Herkunftsnachweis. Um die Aufteilung der Kategorien nachvollziehen zu können, werden diese in dem nächsten Absatz erläutert.

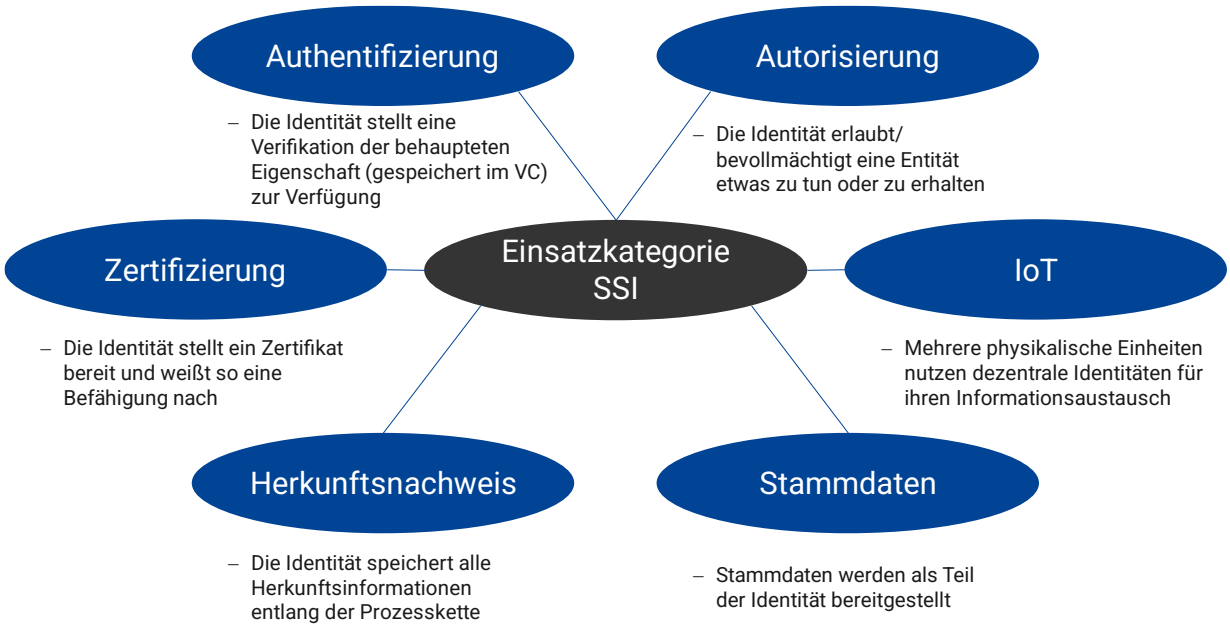


Abbildung 3: Einsatzkategorien

Die **Autorisierung** ist der Prozess, der einer Entität die Erlaubnis erteilt etwas zu tun oder zu erhalten. Eine selbstbestimmte Identität kann hierbei von Vorteil sein, da die Verifiable Credentials bereits die Zertifikate enthalten, dass die Entität die Erlaubnis besitzt etwas zu tun. Des Weiteren ist die **Authentifizierung** durch eine SSI bereits abgedeckt. Dieser Prozessschritt lenkt auf die Verifikation der behaupteten Eigenschaft, die auch in dem VC gespeichert ist. Durch die Kommunikation zwischen verschiedenen Assets und Entitäten besteht die Möglichkeit eines **IoT-Systems**, da mehrere Anlagen ein Netz aufspannen können und Daten untereinander austauschen. D.h. Anwendungsfälle mit dem Bedarf nach einer sicheren vernetzten Kommunikation werden dieser Kategorie zugeordnet. In den Kategorien **Stammdaten**, **Herkunftsnachweisen** sowie **Zertifizierungen** bieten selbstbestimmte Identitäten eine sichere Variante diese automatisiert mit anderen Entitäten auszutauschen, da die Identität immer die Echtheit und Unverfälschtheit sichert.

Um für jeden ausgewählten Anwendungsfall den möglichen Einsatz einer digitalen Identität zu erläutern, ist zu jedem Use-Case eine Erklärung zu dem Einsatz vorhanden. Das bedeutet es wird erklärt welcher Prozessschritt durch eine digitale Identität unterstützt werden sollte. Hierbei können bereits vereinzelt Einsatzfelder von digitalen Identitäten erarbeitet werden. Dazu gehören folgende Prozesse: Berechtigung erhalten, Berechtigung darlegen, Identitäts-Daten bereitstellen sowie diese zu verifizieren. In diesen Prozessen besteht die Möglichkeit von verschiedenen Abhängigkeiten der involvierten Kommunikationspartnern. Zwei häufig auftretende Vertrauensketten sind hierbei die Autorisierung von API und Mensch sowie Herkunftsnachweise.

Zudem wurden verschiedene Vorteile und Mehrwerte erarbeitet, die durch eine selbstbestimmte Identität entstehen. Hierbei ist zu betonen, dass dies Umstände sein müssen, die noch nicht bestehen wodurch die SSI einen wirklichen Mehrwert schafft. Vereinzelt bestehen bei manchen Anwendungsfällen bereits (Pilot-)Projekte mit digitalen Identitäten. Bei diesen Use-Cases sind teilweise Beispiele recherchiert und in der folgenden Tabelle zu finden. Ein letzter wichtiger Aspekt der Anwendungsfallbeschreibung ist die Ausarbeitung von kritischer Infrastruktur. Hierzu ist jedem Anwendungsfall die Antwort „Ja“ oder „Nein“ zu der Frage, ob ein KRITIS Prozess vorliegt, zugeordnet. Mit der Information steigt die Dringlichkeit Prozesse zu verbessern, sodass weniger Angriffsmöglichkeiten auftreten und das Vertrauen erhöht wird.

3.2 Übersicht ausgewählte Anwendungsfälle

Lfd. Nr.	Handlungsfeld	Kategorie	Energiewirtschaftlicher Anwendungsfall	Möglicher Einsatz von digitaler Identität	Beispiel
1	Bau	IoT	Durch cyber-physikalische Links kann ein digitaler Zwilling von Anlagen erstellt werden. (Zukünftige Anlage und Betriebsmittel im Feld werden durch digitalen Zwilling abgebildet und sind somit für den Bau digitalisiert)	Ein digitaler Zwilling ermöglicht die Interoperabilität zwischen Modellen und die selbstständige Wartungsinitiierung.	idFlexNetz
2	Bau	Autorisierung, Authentifizierung, IoT	Ein IEC 61850-Umspannwerk wird durch das Kommunikationsprotokoll und die herstellerübergreifende Interoperabilität definiert. Somit sorgt diese Norm für einen hohen Automatisierungsgrad eines Umspannwerks (IEC 61850 Digitales Umspannwerk).	Die Kommunikation zwischen Anlagen erfolgt durch digitale Identitäten und erhöht somit den Automatisierungsgrad.	idFlexNetz
3	Beschaffungsmanagement	Stammdaten, Zertifizierung	Der ÜNB verwaltet verschiedene Dienstleister im Beschaffungsmanagement. Dabei müssen zum Beispiel Bankverbindungen oder Qualitätsstandards (ISO-Norm) verifiziert werden (Dienstleisterverwaltung: Organisation von Dienstleistern und deren Eigenschaften).	Zertifikatsverwaltung (z.B. Abruf von Verifiable Credentials zu den digital gespeicherten Zertifikaten) oder Lieferanten Präqualifikation für Stromlieferanten und Systemdienstleistungen	IDunion
4	Betrieb	Stammdaten, Herkunftsnachweis	Der ÜNB verwaltet die Fahrpläne von regelzoneninternen und -überschreitenden Geschäften (Betriebsdaten- und Fahrplanaustausch).	Identifikation von Fahrplänen und Einbringen der Fahrplaninformationen	

Lfd. Nr.	Handlungsfeld	Kategorie	Energiewirtschaftlicher Anwendungsfall	Möglicher Einsatz von digitaler Identität	Beispiel
5	Betrieb	Stammdaten, Authentifizierung, IoT	Netzkundenabrechnung - Verwaltung von Stammdaten und Abrechnungsdaten der Netzkunden	Übermittlung von Daten der Messstellen, vor allem Vorgänge UNB in der Rolle VNB	
6	Betrieb	Stammdaten, Herkunftsnachweis, Authentifizierung	Verwendung, Auswertung und Weitergabe von Prognosedaten (Wetter, Last, Erzeugung) für unterschiedliche Prozesse (Prognose).	Identifikation und Herkunftsnachweis der Prognosedaten, Prognosedaten können darüber hinaus über Vertrauensketten aggregiert werden	
7	Betrieb	Authentifizierung, Stammdaten, IoT	Übertragungsnetzbetreiber verwalten verschiedene Anlagen und Komponenten. Eine Hauptaufgabe des Betriebes sind die Wartung und Instandhaltung (Maintenance). Hierfür sind regelmäßige oder ereignisorientierte Maintenance-Prozesse durchzuführen.	Mögliche Erinnerung über zukünftige Instandhaltung und Übermittlung von Fehlern: Anlagen können einen Wartungsbedarf melden und diese Meldung mit einer eindeutigen Identifikation versehen.	idFlexNetz
8	Betrieb	Stammdaten, Authentifizierung	Der ÜNB verwaltet verschiedene Anlagen, die durch Störungen in ihren Funktionen eingeschränkt sein können (Störungsmanagement).	Eine Anlage übermittelt im Falle einer Störung ihre Daten, die mit anderen Informationen aus dem Maintenance angereichert sind.	
9	EnWG, EEG, StromPBG und KWKG-Abwicklung	Authentifizierung, Herkunftsnachweis	Das EEG, KWKG und StromPBG verpflichtet die EVUs, Letztverbraucher und Eigenversorger dazu die Daten über gelieferte bzw. selbstverbrauchte Strommengen an den regelverantwortlichen ÜNB zu melden.	Bereitstellung verifizierter ID-Daten für das Meldungsportal sowie Stammdaten und Nachweis über gelieferte Energie	
10	EnWG, EEG, StromPBG und KWKG-Abwicklung	Authentifizierung	Der ÜNB muss im Zuge des EEGs, KWKGs und des StromPBGs die Einhaltung der gesetzlichen Abrechnungspflichten von EVUs, Letztverbrauchern und Anlagenbetreibern durch einen Wirtschaftsprüfer verifizieren lassen (Testierung EEG, KWKG, StromPBG).	Verifikation des Wirtschaftsprüfers, sowie Bescheinigung (erfolgt aktuell durch signierte Dateien), Einbringen von "echten" vertrauenswürdigen Messwerten, Abbilden von Vertrauensketten	

Lfd. Nr.	Handlungsfeld	Kategorie	Energiewirtschaftlicher Anwendungsfall	Möglicher Einsatz von digitaler Identität	Beispiel
11	EnWG, EEG, StromPBG und KWKG-Abwicklung	Stammdaten	Das EEG, EnWG und StromPBG verpflichtet UNBs dazu die TAM-Meldungen von Förderempfängern in die Transparenzdatenbank der Europäischen Kommission einzustellen (TAM-Meldungen).	Übermittlung von Daten in die Transparenzdatenbank der Europäischen Kommission und Verifikation sowie Bereitstellung von Daten von Meldenden	
12	Gebäudemanagement	Stammdaten	Beim Building Information Modelling (BIM) werden Kleinabnahmen und Baufortschritte über digitale Schnittstellen verfügbar gemacht.	Identifikation von Gebäudeteilen und Anreichern von Informationen.	Internes Projekt TNG / Energieausweis (Sparkasse, Gebäude Ressourcen-Pass)
13	IT	Authentifizierung	Jeder Mitarbeitende eines ÜNBs besitzt Berechtigungen und IT-Zugänge, die von dem Unternehmen selbst verwaltet werden (Verwaltung von IT-Zugängen und Berechtigungen).	Berechtigungen für Tools	Azure AD / ENTRA Wallet
14	Netzplanung	Stammdaten, Authentifizierung, IoT	Der Übertragungsnetzbetreiber interagiert mit vielen verschiedenen Assets und wertet die Asset-Daten aus (Verwaltung von Asset-Daten).	Bestimmung der Identität oder der Attribute des Assets über eine digitale Adressierung	Asset Administration Shell (International Digital Twin Association)
15	Organisation	Herkunftsnachweis	Bereitstellung von Nachhaltigkeitsbericht und ESG-Reporting	Bereitstellung von Nachhaltigkeitszertifikaten mit eindeutigem Identifier	DATEV
16	Netzwirtschaft	Authentifizierung, Zertifizierung	Um Bilanzierungsgebiete eindeutig identifizieren zu können, vergeben ÜNBs einen 16-stelligen Energy Identification Code (Code für Bilanzierungsgebiet).	Ausstellen eines Zertifikats für Bilanzierungsgebiete, um sich bei Marktpartnern zu autorisieren	

Lfd. Nr.	Handlungsfeld	Kategorie	Energiewirtschaftlicher Anwendungsfall	Möglicher Einsatz von digitaler Identität	Beispiel
17	Netzwirtschaft	Zertifizierung	Marktzugang in der Regelzone: Durchführung von Bilanzkreisabgleich /-monitoring	Sofortiger Entzug von Autorisierung bei Missständen / Abweichungen von Handelsbefugnissen durch unverzügliches Bekanntwerden der Information	
18	Netzwirtschaft	Zertifizierung, Herkunftsnachweis	NBs geben dem vorgelagerten ÜNB Nachweise über den vergüteten Strom und Strom aus erneuerbaren Energien weiter (Herkunftsnachweis). Das kann auch weitere "Stromeigenschaften" beinhalten, wie Handelseigenschaften oder Entstehungseigenschaften. Dies geschieht zur Ausweisung des EEG-Quotienten.	Verifikation des NBs und des übermittelten Herkunftsnachweises	E.ON, Dena, EnBW (über Blockchain)
19	Netzwirtschaft	Autorisierung, Stammdaten, Authentifizierung	Vergabe und Verwaltung eindeutiger Identifikationscodes für die Marktpartnerkommunikation im Rahmen der Bilanzkreisabrechnung. Die aktuelle Umsetzung erfolgt über Energie Identifikation Codes (EIC) durch den BDEW als zentrale Plattform für Codegenerierung und Verifikation.	Bereitstellung einer eindeutigen und vertrauenswürdigen Identität als alternative zum BDEW als Vertrauensanker.	
20	Organisation/Personal	Stammdaten, Herkunftsnachweis	Damit die Datenhoheit von Bewerbenden bei ihnen selbst bleibt, sind DSGVO konforme Bewerbungsprozesse notwendig.	Übermittlung der Bewerbung und der Bewerberdaten / Consent-Management	Velocity Network
21	Organisation/Personal	Zertifizierung	Um personalbezogene Prozesse durchführen zu können, werden zumeist Bescheinigungen benötigt (Bescheinigungen).	Berechtigungen / Bescheinigungen ausstellen (Unterschriften, Arbeitsbereiche, Arbeitsaufgaben, Werkzeuge)	KFZ-Ausgabe nach Berechtigung (z.B. Führerschein, EUDI wallet), BMW, COVID Pass

Lfd. Nr.	Handlungsfeld	Kategorie	Energiewirtschaftlicher Anwendungsfall	Möglicher Einsatz von digitaler Identität	Beispiel
22	Organisation/Personal	Autorisierung, Authentifizierung	Verwendung von digitalen Identitäten für ein Zugangsmanagement. Um digitale oder analoge Zugänge zu erlangen, bedarf es einem Verifikations- und Identifikationsprozess (Zugangsmanagement).	Über eine Wallet (z.B. auf Handy) werden die Zugangsberechtigungen dezentral gespeichert.	IDunion (Thema Zugangsmanagement)
23	Systemdienstleistung (Engpassbewirtschaftung, Spannungshaltung und Frequenzhaltung)	Autorisierung, Authentifizierung	Der ÜNB ist systemverantwortlich für die Frequenzhaltung. Hierzu bindet er für unterschiedliche Produkte (Primärregelleistung, Sekundärregelleistung und Minutenreserve) Geschäftspartner ein. Der ÜNB ruft diese Produkte im Rahmen seiner Betriebsführung ab.	Identifikation (Geschäftspartner) beim Abruf und Erlaubnis	BMIL, DIVE
24	Systemdienstleistung (Engpassbewirtschaftung, Spannungshaltung und Frequenzhaltung)	IoT, Stammdaten, Herkunftsnachweis	Der ÜNB ist systemverantwortlich für die Frequenzhaltung. Hierzu bindet er für unterschiedliche Produkte (Primärregelleistung, Sekundärregelleistung und Minutenreserve) Geschäftspartner ein. Die Anlagen, welche die Produkte erzeugen, müssen durch den ÜNB verwaltet und präqualifiziert werden.	Stammdatenverwaltung und Präqualifikation von frequenzgebundenen Systemdienstleistungsprodukten durch automatisierten von dezentralen Identitäten mit entsprechendem Herkunftsnachweis.	Tennet, BMIL, DIVE
25	Systemdienstleistung (Engpassbewirtschaftung, Spannungshaltung und Frequenzhaltung)	Stammdaten, Authentifizierung	Abruf von Blindleistung beim unterlagertem NB oder anderen Quellen (z.B. Kraftwerke)	Identifikation beim Abruf und Erlaubnis	
26	Systemdienstleistung (Engpassbewirtschaftung, Spannungshaltung und Frequenzhaltung)	Stammdaten, Authentifizierung	Der ÜNB benötigt für unterschiedliche Netzführungsaufgaben Flexibilitäten von Dritten, welche mit diesem abzurechnen sind. Hierfür sind abrechnungsrelevante Daten bzw. Messwerte notwendig.	Identifikation von Vorgängen für Flexibilitätsbereitstellungen und Bereitstellung von verifizierten Daten	idFlexNetz

Lfd. Nr.	Handlungsfeld	Kategorie	Energiewirtschaftlicher Anwendungsfall	Möglicher Einsatz von digitaler Identität	Beispiel
27	Systemdienstleistung (Engpassbewirtschaftung, Spannungshaltung und Frequenzhaltung)	Autorisierung, Zertifizierung	Der UNB reguliert die Leistungseinspeisung, um regional auftretende Überlastungen zu vermeiden oder zu beseitigen (Redispatch / Engpassbewirtschaftung).	Identifikation von Flexibilitätsanbietern (Lasten, Einspeiser, Aggregatoren), inkl. Gebotsmanagement durch das Einstellen von zertifizierten Geboten. Vor allem die aktuelle Ausbaustufe 2 und die zukünftige Ausbaustufe 3 des Redispatches haben hier einen hohen Bedarf an Automatisierung und Digitalisierung in allen Prozessen, da hier die Anzahl an beteiligten Partnern zunimmt. Durch Bereitstellung von Abrufzertifikaten kann der ÜNB die angebotene Flexibilität sicher in den Redispatchprozess einbinden.	DEER
28	Vertragsmanagement (Bilanzkreise, Bau, Lieferanten, Netzwirtschaft (DA/RE Nutzer) ...)	Authentifizierung	Im Vertragsmanagement sind Verträge mit unterschiedlichen Anforderungen an Echtheit zu verwalten. Bestimmte Prozesse bedingen schnelle Abschlussgeschwindigkeiten.	Verträge werden als Identität verwalten, um deren Echtheit zu gewährleisten (ggf. über Digitalen Zwilling). Alle Vertragspartner können mit Identität die Echtheit und Gültigkeit überprüfen.	BAMF
29	Vertragsmanagement (Bilanzkreise, Bau, Lieferanten, Netzwirtschaft (DA/RE Nutzer) ...)	Authentifizierung, Stammdaten	Management von Bilanzkreisen - Hierzu zählt die Parametrisierung der Bilanzkreisdaten (z.B. Handelsvolumen).	Verifizierte Identifikation und Autorisierung von Bilanzkreisdaten.	
30	Vertragsmanagement (Bilanzkreise, Bau, Lieferanten, Netzwirtschaft (DA/RE Nutzer) ...)	Autorisierung, Zertifizierung	Im Vertragsmanagement muss sichergestellt werden, dass die Unterschrift echt ist. Hier ist insbesondere die Wichtigkeit von digitalen Signaturen zu nennen (Verifikation der Unterschriften).	Digitale Signatur und die Berechtigung (Eintrag Handelsregister, interne Unterschriftenberechtigung …) dazu bereitstellen	BAMF
31	Vertragsmanagement (Bilanzkreise, Bau, Lieferanten, Netzwirtschaft (DA/RE Nutzer) ...)	Zertifizierung, Herkunftsnachweis	Abschließen gültiger Verträge	Die Herkunft und das Zustandekommen von Verträgen werden durch die ID bestätigt.	

Lfd. Nr.	Handlungsfeld	Kategorie	Energiewirtschaftlicher Anwendungsfall	Möglicher Einsatz von digitaler Identität	Beispiel
32	Netzwirtschaft, Netzführung	Authentifizierung, Stammdaten, Herkunftsnachweis	Speichern und Verteilen von Anlagenstammdaten Marktstammdatenregister	Marktstammdaten werden durch Vertrauensketten angereichert, um Herkunftsnachweise zu erzeugen.	Dena
33	Systemdienstleistung (Engpassbewirtschaftung, Spannungshaltung und Frequenzhaltung)	Authentifizierung, IoT	Einsatz eines IKT-Ökosystems für Prognose- und Betriebsmodelle im Netzbetrieb (IKT - Informations- und Kommunikationstechnologien)	Eindeutige Identifikation von Flexibilitäten	idFlexNetz
34	Organisation/Personal	Stammdaten, Herkunftsnachweis	Mitarbeiterprozesse - digitaler Mitarbeiterausweis	Speicherung persönlicher Einstellung und gegebenenfalls personenbezogener Daten in der dezentralen Wallet für unterschiedliche interne Organisationsthemen und Komfortfunktionen, wie Schreibtischhöhe, Direktbuchung und Einrichtung des shared desk	
35	Netzwirtschaft, Organisation, Systemdienstleistungen	Stammdaten	Unterschiedliche Kundenprozesse der ÜNB verwalten Stammdaten. Hierzu zählen beispielweise die energiewirtschaftlichen Stakeholder, wie Bilanzkreisverantwortlichen, Lieferanten, angeschlossene Netzbetreiber oder auch Bereitsteller von Systemdienstleistungen. Außerdem sind auch die Stammdaten weiterer Stakeholder zu verwalten (politische Ansprechpartner, Banken).	Dezentrale Identitäten können von den Kunden als Holder selbst verwaltet werden. So aktualisieren sich die Stammdaten durch Änderung des Kunden und ist beim nächsten Abruf aktuell.	

3.3 Charakterisierung der Anwendungsfälle

Um die verschiedenen Anwendungsfälle charakterisieren zu können, werden bestimmte Kriterien benötigt. Diese verhelfen zu einer Evaluation der Vorteile des Einsatzes von selbstbestimmten Identitäten. Zu den ausgewählten Bewertungskriterien zählen der (1) Mehrwert, (2) die Schwierigkeit der Umsetzung und (3) die Notwendigkeit der Compliance. Die hier durchgeführte Einsortierung soll ein erstes Indiz für eine detaillierte Bewertung sein, welche in einem späteren Umsetzung konkretisiert werden kann.

Der **Mehrwert** nach unterschiedlichen Eigenschaften des Anwendungsfalles bewertet. Dazu gehören die (i) Skalierbarkeit, (ii) die Aufwandsersparnis, (iii) die Standardisierungsmöglichkeiten, (iv) der Transfer und (v) die Anzahl der Teilnehmer. Die Skalierbarkeit ist ein wichtiger Punkt des Mehrwerts, da eine skalierbare Umgebung einen hohen Automatisierungsgrad, Reduzierung von Medienbrüchen und steigenden Umsatz bietet. Das Aufwandsersparnis ist zu beachten, weil der Prozess durch eine selbstbestimmte Identität vereinfacht werden soll und dementsprechend ein geringerer Aufwand entstehen soll. Die Standardisierungsmöglichkeiten sind mit dem Aufwandsersparnis verkettet, da bei einem standardisierten Grundgerüst, welches anwendbar ist, der Implementierungs- und Anwendungsaufwand sinkt. Eine große Anzahl an Teilnehmern eines Kommunikationsnetzes erfordert, aufgrund der Ineffizienz eines manuellen Vorgangs, das Dasein von Automatisierung. Somit wird das Anwenden vor allem bei einer großen Menge von Entitäten notwendig. Diese verschiedenen Aspekte tragen zu der Bewertung des Mehrwerts bei. Dieses Kriterium wird in die Werte niedrig, mittel und hoch eingestuft. Hierbei beziffert der Wert „niedrig“ den niedrigsten Mehrwert und der Wert „hoch“ den höchsten Mehrwert.

Die **Schwierigkeit der Umsetzung** ist vor allem eine Frage der Implementierung und Etablierung der Technologie innerhalb bestehender Prozesse. Der Anwendungsfall muss eine Situation bieten, die mit einfacher und eventuell bestehender Infrastruktur eine digitale Identitätslandschaft ermöglichen kann. Dieses Kriterium weist Ähnlichkeiten mit dem Mehrwert auf, da wenn die Komplexität der Umsetzung die Kompetenz des Möglichen überschreitet, überwiegt der Aufwand dem Nutzen. Somit soll durch dieses Kriterium eine Unwirtschaftlichkeit vermieden werden und mögliche Quick-Wins können identifiziert werden. Zudem gibt es einige Geschäftsprozesse, in denen nicht nur ein Übertragungsnetzbetreiber involviert ist, sondern noch andere Institutionen oder Unternehmen. In diesem Falle wäre die Umsetzung erschwert, da der Prozess bei vielen Akteuren angepasst werden müsste und damit die Komplexität steigt. Falls wiederum nur ein einige wenige interne und externe Beteiligte Prozess- und IT-Anpassungen durchführen müssen, ist die Schwierigkeit der Umsetzung im Aspekt der Anpassung niedriger bzw. ge-

ring . Die Werte des Kriteriums sind niedrig, mittel und hoch, wobei niedrig der anzustrebende Wert ist, um mit wenig Aufwand die Technologie in Prozessen zu etablieren.

Das Entscheidungskriterium der **Notwendigkeit der Compliance** bezieht sich auf den Schutzbedarf (IT-Sicherheit, Systemsicherheit, Datenschutz) des Anwendungsfalles. Hierbei werden insbesondere die kritischen Eigenschaften bewertet, die durch digitale Identitäten verbessert werden können. Zu den Themen gehören, wie in Kapitel 2 beschrieben, die Themen Autorisierung, Zertifizierung, Authentifizierung, IoT, Stammdatenpflege und Herkunftsnachweise. Da insbesondere das Thema des Datenschutzes und der eindeutigen Verifikation eines Assets oder einer Entität eine Rolle spielt, stellt sich hier zum Beispiel die Bewertung „hoch“ als förderlich für die Umsetzung einer selbstbestimmten Identität dar. Die Werte des Kriteriums sind niedrig, mittel und hoch. Wo hohe Anforderung abgeleitet sind, kommt das Potential von SSI besonders zum Tragen.

Lfd. Nr.	Möglicher Einsatz von digitaler Identität	Vorteil	KRITIS	Mehrwert	Schwierigkeit der Umsetzung	Notwendigkeit der Compliance
1	Ein digitaler Zwilling ermöglicht die Interoperabilität zwischen Modellen und die selbstständige Wartungsinitiierung.	Eindeutige Identität schon während der Planung und des Baus	ja	hoch	hoch	mittel
2	Die Kommunikation zwischen Anlagen erfolgt durch digitale Identitäten und erhöht somit den Automatisierungsgrad.	Herstellerübergreifendes Vertrauenslevel, Effizienz (zum Beispiel keine Passworteingabe an den Geräten notwendig, um Geräte untereinander zu authentifizieren)	ja	mittel	hoch	hoch
3	Zertifikatsverwaltung (z.B. Abruf von Verifiable Credentials zu den digital gespeicherten Zertifikaten) oder Lieferanten Präqualifikation für Stromlieferanten und Systemdienstleistungen	Automatische Aktualisierung der Stammdaten und Zertifikate (z.B. ISO-Nachweise) -> Mehrwert für die DL (eine ID) und aktuellere Daten für AG (vgl. CRUD)	nein	hoch	hoch	hoch
4	Identifikation von Fahrplänen und Einbringen der Fahrplaninformationen	Höheres Vertrauen in die angemeldeten Fahrpläne z.B. Vermeidung von Bilanzkreismissbrauch	nein	mittel	mittel	mittel
5	Übermittlung von Daten der Messstellen, vor allem Vorgänge ÜNB in der Rolle VNB	Höheres Vertrauen in die Datensicherheit	nein	mittel	hoch	hoch
6	Identifikation und Herkunftsnachweis der Prognosedaten, Prognosedaten können darüber hinaus über Vertrauensketten aggregiert werden	Höheres Vertrauen	nein	mittel	gering	mittel
7	Mögliche Erinnerung über zukünftige Instandhaltung und Übermittlung von Fehlern: Anlagen können einen Wartungsbedarf melden und diese Meldung mit einer eindeutigen Identifikation versehen.	Eindeutige IDs sind Voraussetzung für zukünftige Digitalisierungsansätze wie Predictive Maintenance. DiD und SSI erhöhen hierbei das Vertrauenslevel und machen Stamm- und Bewegungsdaten eindeutig.	nein	hoch	mittel	hoch
8	Eine Anlage übermittelt im Falle einer Störung ihre Daten, die mit anderen Informationen aus dem Maintenance angereichert sind.	Eindeutige Asset IDs sind Voraussetzung für zukünftige Digitalisierungsansätze, Erhöhtes Vertrauensnivau und somit erhöhte Sicherheit durch eindeutige Authentifizierung von Meldungen	nein	hoch	mittel	hoch

Lfd. Nr.	Möglicher Einsatz von digitaler Identität	Vorteil	KRITIS	Mehrwert	Schwierigkeit der Umsetzung	Notwendigkeit der Compliance
9	Bereitstellung verifizierter ID-Daten für das Meldungsportal sowie Stammdaten und Nachweis über gelieferte Energie	Höheres Vertrauens-Level und somit Korrektheit und Validität der Daten. Kein aufwändiges Identifikationsverfahren (PostID, Abgleiche mit Datenbanken wie Handelregister…) notwendig	nein	hoch	hoch	hoch
10	Verifikation des Wirtschaftsprüfers, sowie Bescheinigung (erfolgt aktuell durch signierte Dateien), Einbringen von "echten" vertrauenswürdigen Messwerten, Abbilden von Vertrauensketten	Alternative zu textbasierten Prüfungsvermerkten	nein	mittel	hoch	hoch
11	Übermittlung von Daten in die Transparenzdatenbank der Europäischen Kommission und Verifikation sowie Bereitstellung von Daten von Meldenden	Höheres Vertrauens-Level und somit Korrektheit und Validität der Daten. Kein aufwändiges Identifikationsverfahren (PostID, Abgleiche mit Datenbanken wie Handelregister…) notwendig.	nein	hoch	hoch	niedrig
12	Identifikation von Gebäudeteilen und Anreichern von Informationen.	Über Digitale Zwillinge werden Bauwerksteile/-gewerke digitalisiert und mit Informationen verbunden.	nein	hoch	mittel	niedrig
13	Berechtigungen für Tools	Eine ID für alle Tools (SSO), passwortlose Authentifizierung	Ggf.	hoch	mittel	hoch
14	Bestimmung der Identität oder der Attribute des Assets über eine digitale Adressierung	Erhöhtes Vertrauen in eindeutige Asset IDs	ja	hoch	mittel	hoch
15	Bereitstellung von Nachhaltigkeitszertifikaten mit eindeutigem Identifier	Höhere Zuverlässigkeit der Herkunftsnachweise	nein	mittel	gering	niedrig

Lfd. Nr.	Möglicher Einsatz von digitaler Identität	Vorteil	KRITIS	Mehrwert	Schwierigkeit der Umsetzung	Notwendigkeit der Compliance
16	Ausstellen eines Zertifikats für Bilanzierungsgebiete, um sich bei Marktpartnern zu autorisieren	Erhöhung des Vertrauens bei API-Kommunikation, Mehrwert der Digitalisierung (Reduktion der Medienbrüche) und nicht der papierbasierte Unterschriftenübermittlung z.B. VNB als benachbarter NB	nein	mittel	gering	hoch
17	Sofortiger Entzug von Autorisierung bei Missständen / Abweichungen von Handelsbefugnissen durch unverzügliches Bekanntwerden der Information	Hier kann bei Bilanzkreismissbrauch durch Vertrauensentzug schnell eingeschritten werden.	nein	gering	mittel	mittel
18	Verifikation des NBs und des übermittelten Herkunftsnachweises	Höhere Zuverlässigkeit der Herkunftsnachweise	nein	mittel	hoch	niedrig
19	Bereitstellung einer eindeutigen und vertrauenswürdigen Identität als alternative zum BDEW als Vertrauensanker.	Vereinfachung des Prozesses der Marktkommunikation, Erhöhte Sicherheit und Vertraulichkeit beim Datenaustausch.	nein	hoch	mittel	hoch
20	Übermittlung der Bewerbung und der Bewerberdaten / Consent-Management	Höherer Datenschutz, mehr Vertrauen in die Bewerberdaten	nein	hoch	hoch	hoch
21	Berechtigungen / Bescheinigungen ausstellen (Unterschriften, Arbeitsbereiche, Arbeitsaufgaben, Werkzeuge)	Erhöhtes Vertrauen in die ID und Berechtigungs-Management über Zertifikate	nein	hoch	mittel	hoch
22	Über eine Wallet (z.B. auf Handy) werden die Zugangsberechtigungen dezentral gespeichert.	Erhöhtes Vertrauen in die ID und zuverlässige Autorisierung	nein	hoch	gering	hoch

Lfd. Nr.	Möglicher Einsatz von digitaler Identität	Vorteil	KRITIS	Mehrwert	Schwierigkeit der Umsetzung	Notwendigkeit der Compliance
23	Identifikation (Geschäftspartner) beim Abruf und Erlaubnis	Vertrauen, Skalierbarkeit (Massenfähigkeit = digitale Schnittstelle ohne Medienbruch für Automatisierungsprozesse)	ja	mittel	hoch	hoch
24	Stammdatenverwaltung und Präqualifikation von frequenzgebundenen Systemdienstleistungsprodukten durch automatisierten von dezentralen Identitäten mit entsprechendem Herkunftsnachweis.	Erhöhtes Vertrauen in Identität der Partner und verifizierbare Präqualifikationsprofile	ja	mittel	hoch	hoch
25	Identifikation beim Abruf und Erlaubnis	Vertrauen, Skalierbarkeit	ja	mittel	hoch	hoch
26	Identifikation von Vorgängen für Flexibilitätsbereitstellungen und Bereitstellung von verifizierten Daten	Konkrete und verifizierte Daten, Skalierbarkeit	ja	hoch	hoch	hoch
27	Identifikation von Flexibilitätsanbietern (Lasten, Einspeiser, Aggregatoren), inkl. Gebotsmanagement durch das Einstellen von zertifizierten Geboten. Vor allem die aktuelle Ausbaustufe 2 und die zukünftige Ausbaustufe 3 des Redispatches haben hier einen hohen Bedarf an Automatisierung und Digitalisierung in allen Prozessen, da hier die Anzahl an beteiligten Partnern zunimmt. Durch Bereitstellung von Abrufzertifikaten kann der ÜNB die angebotene Flexibilität sicher in den Redispatchprozess einbinden.	Erhöhtes Vertrauen und IT-Sicherheit	ja	hoch	hoch	mittel

Lfd. Nr.	Möglicher Einsatz von digitaler Identität	Vorteil	KRITIS	Mehrwert	Schwierigkeit der Umsetzung	Notwendigkeit der Compliance
28	Verträge werden als Identität verwalten, um deren Echtheit zu gewährleisten (ggf. über Digitalen Zwilling). Alle Vertragspartner können mit Identität die Echtheit und Gültigkeit überprüfen.	Eindeutigkeit und Gültigkeit eines Vertrags ist überprüfbar. Kein potenzieller Datenmissbrauch durch eine Speicherung der Verträge bei Dritten (z.B. Adobe SignIn)	nein	hoch	hoch	hoch
29	Verifizierte Identifikation und Autorisierung von Bilanzkreisdaten.	Erhöhtes Vertrauen in die Bilanzkreisdaten und direktes Bekanntwerden aller Informationen bei Änderung	nein	mittel	hoch	hoch
30	Digitale Signatur und die Berechtigung (Eintrag Handelsregister, interne Unterschriftenberechtigung …) dazu bereitstellen	Eindeutige Identifikation der Vertragspartner und Berechtigung verlinken / Erweiterung zu eIDAS 1.0	nein	mittel	hoch	hoch
31	Die Herkunft und das Zustandekommen von Verträgen werden durch die ID bestätigt.	Erhöhtes Vertrauen	nein	mittel	hoch	hoch
32	Marktstammdaten werden durch Vertrauensketten angereichert, um Herkunftsnachweise zu erzeugen.	Erhöhtes Vertrauen in die Herkunftsnachweise	nein	hoch	hoch	hoch
33	Eindeutige Identifikation von Flexibilitäten	Erhöhtes Vertrauen und IT-Sicherheit		hoch	hoch	hoch
34	Speicherung persönlicher Einstellung und gegebenenfalls personenbezogener Daten in der dezentralen Wallet für unterschiedliche interne Organisationsthemen und Komfortfunktionen, wie Schreibtischhöhe, Direktbuchung und Einrichtung des shared desk	Dezentrale Speicherung personenbezogener Daten erhöht den Datenschutz, Komfort, Image bei Mitarbeiter	nein	mittel	gering	mittel

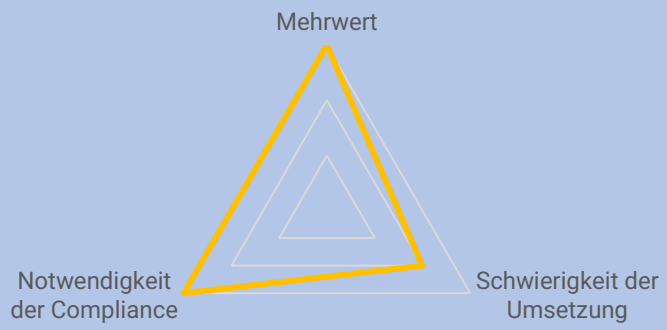
Lfd. Nr.	Möglicher Einsatz von digitaler Identität	Vorteil	KRITIS	Mehrwert	Schwierigkeit der Umsetzung	Notwendigkeit der Compliance
35	Dezentrale Identitäten können von den Kunden als Holder selbst verwaltet werden. So aktualisieren sich die Stammdaten durch Änderung des Kunden und ist beim nächsten Abruf aktuell.	Die Vorteile sind Effizienz, Reduktion von Ressourcen, single source of truth, und Aktualität. Außerdem müssen die Kunden nicht daran denken, wo Sie überall ihre Kontaktdaten, Ansprechpartner usw. hinterlegt haben. Sie aktualisieren die Daten nur in Ihrer Identität, die dann aktuell abgerufen wird.	nein	hoch	mittel	mittel

4 Ausgestaltung und Analyse von Anwendungsfällen

Im Folgenden wurden aus den 35 Anwendungsfällen eine kritische Auswahl getroffen, die hinsichtlich der Bewertungskriterien eine gute Umgebung zur Implementierung in Prozessen bietet. Hierzu sind diese verschiedenen Anwendungsfälle mit höchstem Potenzial mithilfe eines Steckbriefs beschrieben. Der Inhalt des Steckbriefs basiert auf den erarbeiteten Inhalten der Datensammlung. Bei den skizzierten Steckbriefen handelt es sich um Anwendungsfälle, bei denen es sinnvoll erscheint, dass sich ein ÜNB hiermit weiter auseinandersetzt oder deren Betrachtung einen Mehrwert schafft. So kann durch eine Umsetzungspiloten spezifisches Wissen zu der Technologie in Bezug auf Kernaufgaben der ÜNB erlernt werden. Diese Auswahl und Ausarbeitung der Steckbriefe stellt keine vollumfängliche Analyse und Bewertung dar, so dass für Entscheidungsfindung zur Implementierung eine detaillierte Analyse im Sinne eines Lastenheftes empfohlen wird.

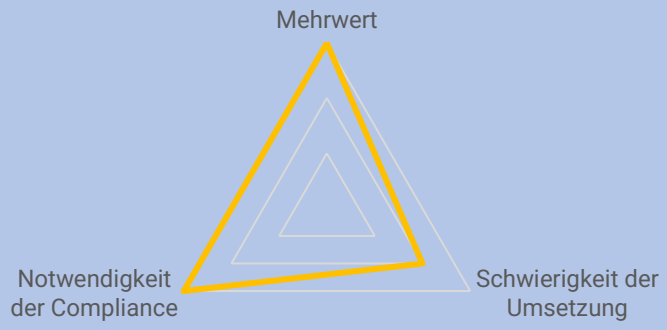
4.1 Use-Case: IKT am Beispiel Maintenance

Titel des Anwendungsfalls:
Selbstorganisierte und automatisierte IKT am Beispiel Maintenanceprozesse
Handlungsfeld:
Betrieb
Kategorie:
Autorisierung, IoT, Stammdaten
Beschreibung des Anwendungsfalls:
Übertragungsnetzbetreiber verwalten verschiedene Anlagen (z.B. Komponenten in Umspannwerke, Wetterstationen für Freileitunsgmonitoring, …) und Komponenten. Eine Hauptaufgabe des Betriebes sind die Wartung und Instandhaltung (Maintenance). Hierfür sind regelmäßige oder ereignisorientierten Maintenanceprozesse durchzuführen, welche intern oder durch externe Partner fristgerecht umgesetzt werden müssen. In einem komplexer werdenden Energiesystem mit immer intelligenter werdenden Komponenten werden auch die Maintenance-Aufgaben herausfordernder (z.B. Secuity-Updates) und verlangen einen höheren Grad an Automatisation (digitale Überprüfung der Durchführung von Wartungsarbeiten). So werden unter dem Begriff Predictive Maintenance selbstorganisierende und vollautomatische Wartungs- und Instandhaltungsverfahren beschrieben, die zum Beispiel dezentrale Datenauswertungen nutzen. Hierbei ist besonderes Augenmerk auf darauf zu legen, dass das Sicherheitsniveau sich nicht verschlechtert und die Systeme angreifbar werden.
Möglicher Einsatz von digitalen Identitäten:
Bei automatisierten Maintenanceprozessen ist ein eindeutiges und vertrauenswürdiges Identifikationsverfahren wichtig. Hier können digitale Identitätsverfahren den Authentifizierungsprozess abbilden. Mögliche Erinnerung über zukünftige Instandhaltung der Übermittlung von Fehlern durch die Anlagen selbst, setzen zum Beispiel voraus, dass der Identifikationsprozess eindeutig und nicht kompromittierbar ist. Neben Bewegungsinformationen können die Anlagen und Prozesse auch Ihre Stammdaten dezentral halten und als Teil ihrer Identität eindeutig verwalten. Auch können so Anlagen direkt Informationen zu sich oder über ihren Zustand austauschen (IoT).
Vorteile:
Eindeutige IDs sind Voraussetzung für zukünftige Digitalisierungsansätze wie Predictive Maintenance. SSI erhöhen hierbei das Vertrauenslevel und machen Stamm- und Bewegungsdaten eindeutig und echtzeitnah nachweisbar. Außerdem helfen sie dabei, dass Geräte, insbesondere von Dritten, ohne weitere Vertrauensinstanz direkt miteinander kommunizieren können.
Charakterisierung:

DIDs bringen einen hohen Mehrwert für den Anwendungsfall “Maintenance”. So sorgen sie für eine eindeutige Identifizierbarkeit und stellen eine aktuelle Stamm- und Bewegungsdatenlage der Technologie-Komponenten sicher. In der Umsetzung sind bei der Einführung neuer Maintenanceprozesse die Systeme so zu etablieren, dass die Technologie der digitalen Identität Anwendung findet. Die Altsysteme sind über entsprechende Schnittstellen anzubinden. Hier sind vor allem Anlagen und Systemhersteller einzubinden. 

4.2 Use-Case: Vergabe und Verwaltung eindeutiger Identifikationscodes

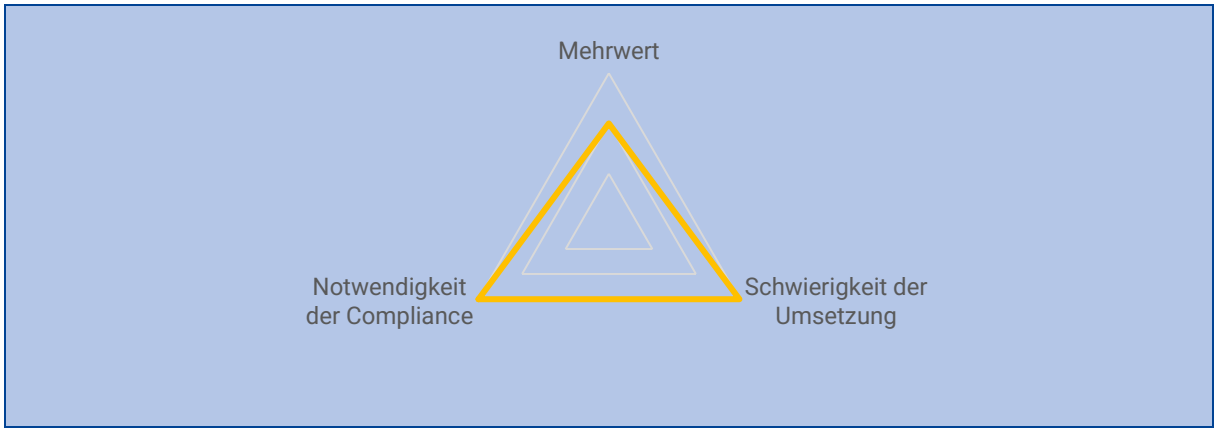
Titel des Anwendungsfalls:
Vergabe und Verwaltung eindeutiger Identifikationscodes für Marktpartnerkommunikation
Handlungsfeld:
Netzwirtschaft
Kategorie:
Authentifizierung, Autorisierung, Stammdaten
Beschreibung Anwendungsfalls:
Vergabe und Verwaltung eindeutiger Identifikationscodes für die Marktpartnerkommunikation im Rahmen der Blianzkreisabrechnung bzw. perspektivisch der Marktkommunikation im Allgemeinen. Dieser Code enthält auch Stammdaten zum Beispiel zum Bilanzierungsgebiet. Die aktuelle Umsetzung erfolgt über Energie Identifikation Codes (EIC) durch den BDEW. Hierbei stellt BDEW eine zentrale Plattform zur Verfügung, an welcher die Codes beantragt und verifiziert werden können. Die Beantragung, Deaktivierung und Änderung von

Informationen eines für ein Bilanzierungsgebiet erfolgt operativ beim jeweils zuständigen Übertragungsnetzbetreiber.
Möglicher Einsatz von digitalen Identitäten:
Bereitstellung einer eindeutigen und vertrauenswürdigen dezentralen Identität inklusive deren Stammdaten als Alternative zum BDEW als Vertrauensanker. So kann der Holder der Identität seine Daten dezentral zur Verfügung stellen und der ÜNB kann als Issuer das Bilanzierungsgebiet legitimieren.
Vorteile:
Vereinfachung des Prozesses der Marktkommunikation, erhöhte Sicherheit und Vertraulichkeit beim Datenaustausch. BDEW als Vertrauensanker zur Herausgabe der Marktrolle, welche der Marktpartner inne hat und aktueller Datenstand zu Stammdaten über alle Vertragspartner im Energiesystem hinweg durch dezentrale Datenhaltung.
Charakterisierung:
Die Vorteile einer dezentralen digitalen Identität für den Anwendungsfall der Identifikationscodes für Marktpartnerkommunikation schafft einen Mehrwert gegenüber der aktuellen Lösung. Hierbei ist Umsetzung nicht komplexer als die bisherige Lösung, wobei durchaus kritische Prozesse eine hohe Compliance fordern. 

4.3 Use-Case: Präqualifikation von Anlagen für Frequenzhaltung

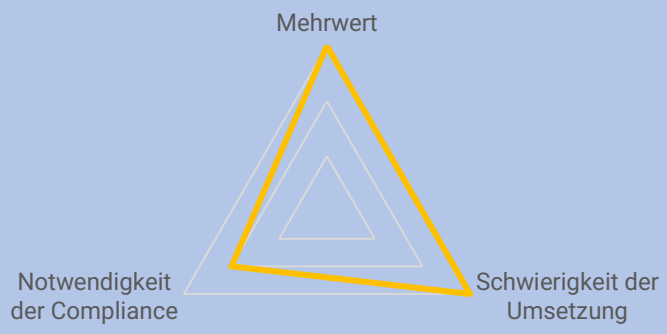
Titel des Anwendungsfalls:
Verwaltung und Präqualifikation von Anlagen für Frequenzhaltung
Thema:
Systemdienstleistung (Engpassbewirtschaftung, Spannungshaltung und Frequenzhaltung)

Kategorie:
IoT, Stammdaten, Herkunftsnachweis
Beschreibung des Anwendungsfalls:
Der ÜNB ist systemverantwortlich für die Frequenzhaltung. Hierzu bindet er für unterschiedliche Produkte (Primärregelleistung, Sekundärregelleistung und Minutenreserve) Geschäftspartner ein. Dies Partner stellen einen Alagenpool zur Verfügung, welche ein spezifisches Verhalten auf die Frequenzhaltungsprodukte haben. In der Regel werden diese Produkte durch technische Anlagen, wie zum Beispiel (dezentrale) Kraftwerke zukünftig auch wechselrichterbasiert generiert. Um sicherzustellen, dass diese Anlagen das richtige Verhalten aufweisen, haben sich die Anlagen durch standardisierte Tests zu präqualifizieren. Da sich zukünftig auch immer mehr kleinere Erzeugungsanlagen an der Frequenzhaltung beteiligen, steigt der Aufwand für die ÜNB diese Anlagen im Rahmen von Datenbanksystemen zu verwalten und zu präqualifizieren. Des weiteren bedingt ein Wechsel einer Anlage von einem Aggregator zu einem anderen Aggregator den kompletten Qualifizierungsprozess von vorne, so dass gewisse Lock-in-Effekte aktuell bestehen.
Möglicher Einsatz von digitalen Identitäten:
Stammdatenverwaltung und automatisierte Präqualifikationsfreigabe von bereits präqualifizierten Anlagen für frequenzgebundene Systemdienstleistungsprodukte (vgl. Typen-PQ) durch dezentralen Identitäten mit entsprechendem Herkunftsnachweis.
Vorteile:
Erhöhtes Vertrauen in Identität der Partner und verifizierbare Präqualifikationsprofile ohne Medienbrüche. Automatisierung der Identitätsverwaltung und Aufwandsreduktion auf Anbieter- und Bedarfsträgerseite Transferierbarkeit und Synergien für weitere Systemdiensleistungsprodukte (z.B. Redispatch 3.0)
Charakterisierung:
Da hier ein systemkritischer Prozess betrachtet wird, stellt sich eine hohe Anforderung an die notwendige Compliance. Zum aktuellen Stand gibt es einen etablierten Medienbruchbehafteten Prozess, der ggf. an zukünftige Systemanforderungen anzupassen ist. Hier kann der skizzierte Einsatz einen Mehrwert generieren. Die Umsetzung kann sich hierbei als anspruchsvoll erweisen, da eine Vielzahl von Partnern (z.B. OEMs, Aggregtoren, etc.) einzubeziehen ist und etablierte Prozesse geändert werden müssen.



4.4 Use-Case: Redispatch

Titel des Anwendungsfalls:
Nutzung von Flexibilität für Redispatch
Handlungsfeld:
Systemdienstleistung (Engpassbewirtschaftung, Spannungshaltung und Frequenzhaltung)
Kategorie:
Autorisierung, Zertifizierung
Beschreibung des Anwendungsfalls:
Der ÜNB reguliert die Leistungseinspeisung und -entnahme, um regional auftretende Überlastungen in seinem Netz zu vermeiden oder zu beseitigen (Redispatch / Engpassbewirtschaftung). Hierzu hat er mit einer Vielzahl von Marktpartnern und deren Anlagen zu kommunizieren, mit denen er nicht unbedingt ein Vertragsverhältnis hat bzw. diese kennt. Diese Marktpartner sollen (zukünftig) über marktliche Mechanismen Ihre Flexibilitätspotential anbieten (Redispatch 3.0) und vom ÜNB in die Redispatchprozesse integriert werden. Hierbei ist es wichtig, dass der tatsächliche Abruf auch richtig entgegengenommen werden kann und korrekt ausgeführt wird. Für die Kommunikation zwischen den Partnern auf den IT-Plattformen werden aktuell Zertifikate von Drittanbietern verwendet.
Möglicher Einsatz von digitalen Identitäten:
Identifikation von Flexibilitätsanbietern (Lasten, Einspeiser, Aggregatoren), inkl. Gebotsmanagement durch das Einstellen von zertifizierten Geboten. Vor allem die aktuelle Ausbaustufe 2.0 und die zukünftige Ausbaustufe 3.0 des Redispatches haben hier einen hohen Bedarf an Automatisierung und Digitalisierung in allen Prozessen, insbesondere im Datenaus-

tausch, da hier die Anzahl an beteiligten Partnern zunimmt. Durch Bereitstellung von Abrufberechtigungen und -Nachweisen kann der ÜNB die angebotene Flexibilität sicher in den Redispatchprozess einbinden.
Vorteile:
Durch die Verwendung von digitalen Identitäten kann das Vertrauen in den Anbieter und das Gebot und so die IT-Sicherheit erhöht werden. Medienbrüche können durch den SSI verhindert werden und sie werden so skalierbarer, da die Identitäten dezentral verwaltet werden.
Charakterisierung:
Das aufzubauende System hat eine hohe Komplexität mit vielen Teilnehmern bei einem mittleren Einfluss auf die Compliance, da in Bezug auf die Systemsicherheit Notfallprozesse vorhanden sind. Die Lösung bietet in diesem Umfeld einen hohen Mehrwert. 

4.5 Use-Case: Zugangsmanagement

Titel des Anwendungsfalls:
Verwendung von digitalen Identitäten für ein Zugangsmanagement
Handlungsfeld:
Personal
Kategorie:
Authentifizierung, Autorisierung
Beschreibung des Anwendungsfalls:

Die Übertragungsnetzbetreiber stehen als Betreiber von kritischer Infrastruktur bei der Sicherheit besonders im Fokus. Hierbei ist es besonders wichtig, dass die Prozesse und Systeme vor nicht autorisierten Zugriffen geschützt werden. Zugriffe können hierbei sowohl durch natürliche aber auch durch juristische Personen erfolgen. Außerdem können diese Personen physikalisch auf kritische Systembereiche Zugriff erhalten (Zugangskontrolle), oder auch digitalen Zugang zu Systemen erhalten (IT-Berechtigungskonzept), welche Nebenbedingungen bzw. Grundvoaraussetzungen nachweisen können. Für beide Prozesse ist ein personenbezogener Identifikations- und Autorisierungsmechanismus erforderlich.

Möglicher Einsatz von digitalen Identitäten:

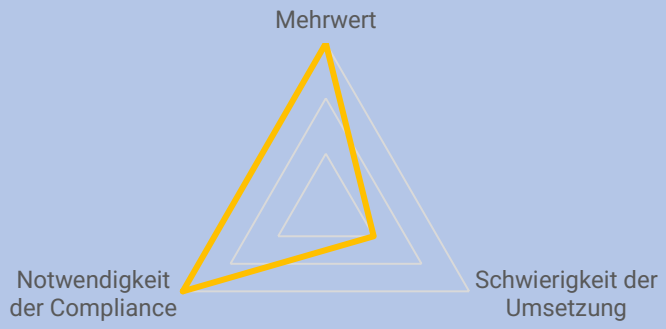
Über ein SSI-Verfahren (z.B. Wallet auf dem Handy) werden die Zugangsberechtigungen dezentral gespeichert und können so am Zugangspunkt abgefragt werden. Dies beinhaltet nicht nur den Nachweis zur Person, sondern auch zu gewissen Nebenbedingungen, wie Qualifikations,-Gesundheitseigenschaften, welche in den persönlichen Datenschutz fällt. Hierbei liegen die Daten dezentral beim Holder, wobei der Issuer die entsprechenden Berechtigungen erteilt und aktualisiert. Darüber hinaus können notwendige Zertifikate ebenfalls Bestandteil der Identität werden (Anwendungsfall 21).

Vorteile:

Das Vertrauen in die Identität und dessen Qualifizierungsstandard erhöht sich durch die Bereitstellung der SSI und einer zuverlässigeren Autorisierung.

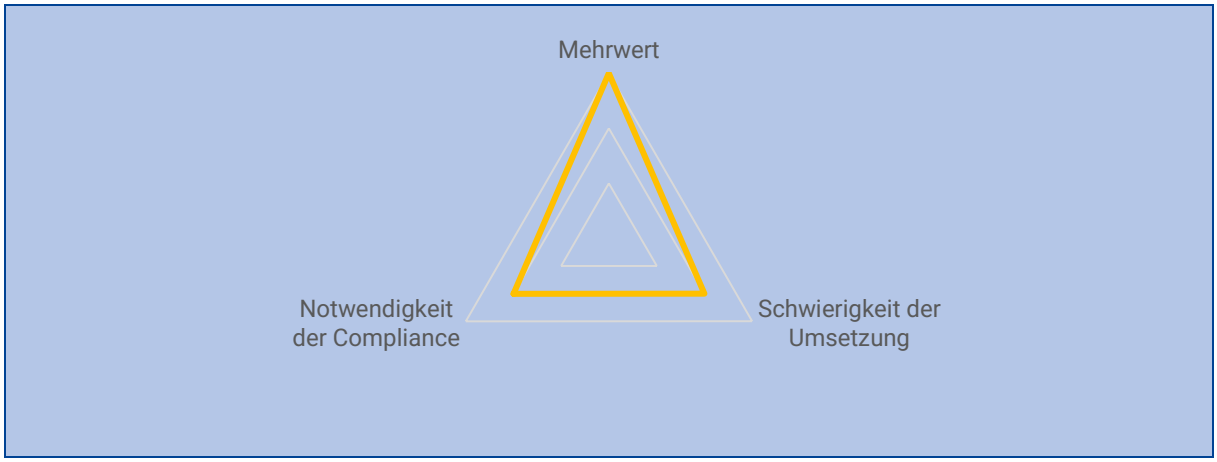
Charakterisierung:

Zugangsmanagement über SSI-Technologie stellt eine lohnende alternative zu klassischen, zentral organisierten Verfahren dar. Sie kann die notwendige hohe Compliance verbessern, bei gering höherem Aufwand gegenüber den aktuellen Lösungen.



4.6 Use-Case: Kunden-Datenbank

Titel des Anwendungsfalls:
Stammdatenmanagement bei Kunden-Datenbank
Handlungsfeld:
Netzwirtschaft, Organisation, Systemdienstleistungen
Kategorie:
Stammdatenmanagement
Beschreibung des Anwendungsfalls:
Unterschiedliche Kundeprozesse der ÜNB verwalten Stammdaten. Hierzu zählen beispielweise die energiewirtschaftlichen Stakeholder, wie Bilanzkreisverantwortlichen, Lieferanten, angeschlossene Netzbetreiber oder auch Bereitsteller von Systemdienstleistungen. Außerdem sind auch die Stammdaten weiterer Stakeholder zu verwalten (politische Ansprechpartner, Banken, Dienstleister, etc.).
Möglicher Einsatz von digitalen Identitäten:
Dezentrale Identitäten können von den Kunden als Holder selbst verwaltet werden. So aktualisieren sich die Stammdaten durch Änderung des Kunden und sie sind beim nächsten Abruf aktuell.
Vorteile:
Die Vorteile sind Effizienz, Reduktion von Ressourcen, single source of truth, und Aktualität. Außerdem müssen die Kunden nicht daran denken, wo Sie überall ihre Kontaktdaten, Ansprechpartner usw. hinterlegt haben, falls sie diese ändern oder löschen wollen. Sie aktualisieren die Daten nur in Ihrer Identität, die dann aktuell abgerufen wird. Selbst innerhalb eines Unternehmens werden Vertragspartner in unterschiedlichen Kundenstammdatenbanken gehalten, so dass bei einer Umfirmierung das umfirmierte Unternehmen sogar mehrere Ansprechpartner innerhalb eines Unternehmens kontaktieren muss, um die Änderung geltend zu machen.
Charakterisierung:
Die Umsetzung hat für einen ÜNB einen hohen Mehrwert, da er immer auf aktuelle Daten über Bereiche hinweg als single-source-of-truth zugreifen kann. Die Umsetzung gestaltet sich als eine mittelmäßige Herausforderung, allerdings sind die Kunden als Stakeholder von dem Konzept zu überzeugen und eine entsprechende Technologie-Umgebung (z.B. KILT, Hyperledger Indy) in einem akzeptierten „Energy Web“ einzuführen. An Compliance Themen steht vor allem der Datenschutz im Vordergrund, welcher mit verbessert werden kann.


Mehrwert
Notwendigkeit der Compliance
Schwierigkeit der Umsetzung

5 Zusammenfassung und Fazit

Ziel der vorliegenden Studie ist es, durch die Erarbeitung von Anwendungsfällen den Bedarf von digitalen Identitäten im Übertragungsnetzbereich zu beleuchten und abzuschätzen, ob digitale Identitäten für den Übertragungsnetzbetreiber (perspektivisch regulierte Unternehmen) eine Relevanz zur weiteren Untersuchung haben. Hierfür sind die Zusammenhänge und Technologien grundlegend beschrieben und anhand von Beispielen erläutert. Anschließend erfolgt eine Auflistung von 35 energiewirtschaftlicher und nicht energiewirtschaftlicher Anwendungsfälle. Hierzu sind zuerst deren Eigenschaften aus sich der digitalen Identität beschrieben. Anschließend erfolgt eine Übersicht und deren Charakterisierung. Abschließen wird auf sechs ausgewählte Anwendungsfälle mit Potenzial zur Vertiefung für den ÜNB näher eingegangen. Bei der Betrachtung und Analyse, welche Anwendungsfälle genauer betrachtet werden sollten, helfen die Kriterien: Mehrwert, Notwendigkeit der Compliance und Schwierigkeit der Umsetzung. Diese geben ein Indiz, bei welchen Anwendungsfällen sich eine Umsetzung lohnen könnte.

Zusammenfassend kann festgestellt werden, dass es eine Vielzahl von Anwendungsfällung bei ÜNBs gibt, die sich mit digitalen Identitäten und mit SSI-Technologie lösen lassen. So kann die Technologie vor allem dann sinnvoll sein, wenn eindeutige Identifikation und Authentifikation gefordert sind. Darüber hinaus kann die Identität eindeutige Stammdaten bereitstellen und diese dezentral verwalten und so Prozesse ablösen, bei denen es durch zentrale Datenhaltung zu Datenschiefständen kommen kann. Außerdem erhöht sich so das Vertrauenslevel in die Daten. Ein typischer Anwendungsfall hierfür ist der Abruf von Flexibilitäten hin zu Kleinstflexibilität. Hier kann die SSI einen Vertrauensanker bilden und klassische zertifikatsbasierte Systeme ablösen. So kann auf Medienbrüche und doppelte Datenhaltung verzichtet werden.

Es lässt sich also zusammenfassend vermuten, dass eine unternehmensweite, strategische Auseinandersetzung mit digitialen Identitäten und insbesondere SSI sinnvoll sein kann. Dies kann ein Baustein sein, um zukünftig energiewirtschaftliche und weitere Prozesse der ÜNB effizient abzuwickeln. So macht die Nutzung von selbstbestimmten Identitäten, Geschäftsprozesse vor allem sicherer und schneller.

6 Literaturverzeichnis

Afting, S. (29. Oktober 2021). *Im Fokus: Sichere digitale Identitäten*. Von Bundesministerium für Wirtschaft und Klimaschutz: https://www.bmwk.de/Redaktion/DE/Schlaglichter-der-Wirtschaftspolitik/2021/11/05-im-fokus-digitale-identit%C3%A4ten.html abgerufen

Allen, C. (25. April 2016). *The Path to Self-Sovereign Identity*. Von Life With Alacrity: http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html abgerufen

Babilon, L., Battaglia, M., & Robers, M. (2022). *Energy Communities: Beschleuniger der dezentralen Energiewende.* Berlin: Deutsche Energie-Agentur GmbH.

Baier, T. (23. Juni 2005). *Persönliches digitales Identitätsmanagement - Untersuchung und Entwicklung von Konzepten und.* Von Universität Hamburg : https://ediss.sub.uni-hamburg.de/bitstream/ediss/1186/1/TBaier-Diss-IDM.pdf abgerufen

BDEW. (2022). *Was bedeutet die Digitalisierung für die Energiewirtschaft?* Von Bundesverband der Energie- und Wasserwirtschaft: https://www.bdew.de/energie/digitalisierung/was-bedeutet-der-trend-der-digitalisierung-fuer-die-energiewirtschaft/ abgerufen

BMDV. (31. August 2022). *Digitalstrategie Gemeinsam digitale Werte schöpfen.* Von Bundesministerium für Digitales und Verkehr: https://digitalstrategie-deutschland.de/static/1a7bee26afd1570d3f0e5950b215abac/220830_Digitalstrategie_fin-barrierefrei.pdf abgerufen

BMWK. (November 2021). *Digitale Identitäten.* Von Bundesministerium für Wirtschaft und Klimaschutz: https://www.bmwk.de/Redaktion/DE/Infografiken/Schlaglichter/2021/11/im-fokus.pdf?__blob=publicationFile&v=6 abgerufen

BMWK. (14. Dezember 2022). *Digitalisierung der Wirtschaft in Deutschland - Digitalisierungsindex 2022*. Von DE.Digital: https://www.de.digital/DIGITAL/Redaktion/DE/Digitalisierungsindex/Publikationen/publikation-digitalisierungsindex-2022-kurzfassung.pdf?__blob=publicationFile&v=4 abgerufen

BOSCH. (2022). *Digitale Identität – Mit Blockchain-Technologie sichere Zusammenarbeit ermöglichen*. Von BOSCH: https://www.bosch.com/de/stories/self-sovereign-identities/ abgerufen

BOSCH. (08. September 2022). *Projekt „GAIA-X 4 moveID" entwickelt Grundlage für sicheren mobilen Datenaustausch*. Von BOSCH: https://www.bosch-presse.de/pressportal/de/de/projekt-gaia-x-4-moveid-entwickelt-grundlage-fuer-sicheren-mobilen-datenaustausch-245952.html abgerufen

BSI. (o.D.). *Public Key Infraustrukturen (PKIen)*. Von Bundesamt für Sicherheit in der Informationstechnik: https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Elektronische-Identitaeten/Public-Key-Infrastrukturen/public-key-infrastrukturen.html abgerufen

Bundeskanzleramt Gesamtprojekt „Europäische Digitale-Identitäten-Initiative. (Dezember 2020). *Digitale Identität - Wie ein Ökosystem digitaler Identitäten zu einem selbstbestimmten und zugleich nutzerfreundlichen Umgang mit dem digitalen Ich beitragen kann.* Von Bundesregierung: https://www.bundesregierung.de/resource/blob/992814/1898280/d9819a40553a9543b9e8f3acb620b0c2/digitale-identitaet-neu-download-bundeskanzleramt-data.pdf abgerufen

Bundestag. (29. August 2016). Gesetz zur Digitalisierung der Energiewende. Bonn, Nordrhein-Westfalen, Deutschland.

Bundestag, D. (4. Juli 2022). *Digitale Identitäten.* Von Bundestag: https://www.bundestag.de/resource/blob/901722/7b3b2d8edb2a64805bc1d96d71ecd42a/Kahlo-data.pdf abgerufen

Cameron, K., Posch, R., & Rannenberg, K. (05. Oktober 2008). *Proposal for a Common Identity Framework: A User-Centric Identity Metasystem.* Von Identity Blog: https://www.identityblog.com/wp-content/images/2009/06/UserCentricIdentityMetasystem.pdf abgerufen

Clauß, S., & Köhntopp, M. (2001). Identity management and its support of multilateral security . *Computer Networks* , S. 205-219.

ComputerWeekly. (Februar 2022). *Distributed-Ledger-Technologie (DLT)*. Von ComputerWeekly: https://www.computerweekly.com/de/definition/Distributed-Ledger-Technologie-DLT abgerufen

Datenbanken-Verstehen. (2022). *Verteilte Datenbanksysteme*. Von Datenbanken-Verstehen: https://www.datenbanken-verstehen.de/lexikon/verteilte-datenbanksysteme/ abgerufen

Der deutsche Gaia-X Hub. (kein Datum). Von Bundesministerium für Wirtschaft und Klimaschutz: https://www.bmwk.de/Redaktion/DE/Dossier/gaia-x.html abgerufen

Digitale Identität. (März 2021). Von Bundeskanzleramt: https://www.bundesregierung.de/resource/blob/992814/1898280/d9819a40553a9543b9e8f3acb620b0c2/digitale-identitaet-neu-download-bundeskanzleramt-data.pdf abgerufen

Dr. Zander, W., Rosen, U., & Dr. Nolde, A. (2018). *Digitalisierung der Energiewende*. Bundestministerium für Wirtschaft und Energie.

Elektronik Kompendium. (o.D.). *Verzeichnsidienste (X.500)*. Von Elektronik Kompendium: https://www.elektronik-kompendium.de/sites/net/0905011.htm abgerufen

Energy Web. (Juni 2020). *EW-DOS: The Energy Web Decentralized Operating System - The Open-Source Technology Stack for Accelerating the Energy Transition - PART 1: VISION & PURPOSE*. Von Energy Web: https://resource-platform.eu/wp-content/uploads/EnergyWeb-EWDOS-PART1-VisionPurpose-202006-vFinal.pdf abgerufen

Energy Web Foundation. (2022). *Energy Web Decentralized Operating System (EW-DOS): A digital infrastructure for a decentralized and decarbonized energy system*. Von Energy Web Foundation: https://energy-web-foundation.gitbook.io/energy-web/ abgerufen

Europäische Kommission. (Juli 2022). *Digitalisierungsgrad der EU-Länder gemäß dem Index für die digitale Wirtschaft und Gesellschaft (DESI*) im Jahr 2022*. Von Statista: https://de.statista.com/statistik/daten/studie/1243006/umfrage/digitalisierungsgrad-der-eu-laender-nach-dem-desi-index/ abgerufen

EY. (2019). *Blockchain-basierte Erfassung und Steuerung von Energieanlagen mithilfe des Smart-Meter-Gateways: Machbarkeitsstudie und Pilotkonzept*. Bundesministerium für Wirtschaft und Energie.

Fusillo, d. M. (12. Mäez 2021). *Digitale Identitätsmodelle*. Von SSI: https://www.selfsovereignidentity.it/digitale-identitatsmodelle/ abgerufen

Future Energy Lab. (Juni 2022). *Digitale Maschinen-Identitäten als Grundbaustein für ein automatisiertes Energiesystem*. Von Deutsche Energie-Agentur: https://www.dena.de/fileadmin/dena/Publikationen/PDFs/2022/Digitale_Maschinen-Identitaeten_als_Grundbaustein_fuer_ein_automatisiertes_Energiesystem.pdf abgerufen

Gödde, M., Kaiser, A., Sander, C., Seith, V., Stumpp, M., & Winter, K. (2020). *Energieherkunft und Peer-to-Peer Handel: Möglichkeiten dezentraler Energiemärkte auf Blockchain-Basis und deren technische Umsetzung*. Energie Baden-Württemberg AG.

Grabatin, M., & Hommel, W. (2021). *Digitale Identitäten für ServiceKonten: Umsetzungsstrategien, Richtlinien und Sicherheitsaspekte.* München: Bayerisches Staatsministerium für Digitales.

Grabatin, M., & Hommel, W. (30. März 2021). *Projekt Diskurs: Digitale Identitäten für Service Konten: Umsetzungsstrategien, Richtlinien und Sicherheitspakete.* Von Bayerisches Staatsministerium für Digitales: https://www.stmd.bayern.de/wp-content/uploads/2021/05/21_04_2021_Abschlussbericht_DISKURS.pdf abgerufen

Huseby, D., & Bohan, S. (08. Juli 2022). *Hyperledger Aries*. Von Hyperledger Foundation: https://wiki.hyperledger.org/display/ARIES abgerufen

Hyperledger Foundation. (2022). *Hyperledger Aries*. Von Hyperledger Foundation: https://www.hyperledger.org/use/aries abgerufen

Joos, T., & Donner, A. (03. 05 2018). *AD für Einsteiger - Wozu dient der Verzeichnisdienst*. Von IP Insider: https://www.ip-insider.de/ad-fuer-einsteiger-wozu-dient-der-verzeichnisdienst-a-709670/ abgerufen

KILT Protocol. (2022). *About KILT Protocol*. Von KILT Protocol: https://www.kilt.io/learn/about-us/ abgerufen

Klein, A., Kaßberger, J., & Buchwald , J.-P. (2021). *Vorstudie digitale Identitäten* .

Klein, A., Kaßberger, J., & Buchwald, J.-P. (30. Dezember 2021). Vorstudie Digitale Identitäten.

Knüsel, L., & Richard, P. (2022). *Die Datenökonomie in der Energiewirtschaft.* Berlin: Deutsche Energie-Agentur.

Kraus, C. (17. Dezember 2021). *Was ist eine verteilte Datenbank?* Von Dev Insider: https://www.dev-insider.de/was-ist-eine-verteilte-datenbank-a-1076385/ abgerufen

Krengel, U. (02. Juli 2021). *Konsortium „energy data-X" im GAIA-X Förderwettbewerb des Bundeswirtschaftsministeriums vorausgewählt*. Von idw - Informationsdienst Wissenschaft: https://idw-online.de/de/news772102 abgerufen

Kudra, A. (12. August 2019). *Chancen der Self-Sovereign Identities (SSI) aus Sicht von Unternehmen für das Identity & Access Management (IAM).* Von Digitale Welt: https://digitaleweltmagazin.de/chancen-der-self-sovereign-identities-ssi-aus-sicht-von-unternehmen-fuer-das-identity-access-management-iam/ abgerufen

Kuhrt, T., & Bohan, S. (08. Juli 2022). *Hyperledger Indy*. Von Hyperledger Foundation: https://wiki.hyperledger.org/display/indy/Hyperledger+Indy abgerufen

Kunert, J. (16. September 2021). *Die selbstbestimmte Identität – Durch Selbstverwaltung gegen den gläsernen Menschen*. Von T-Systems Multimedia Solutions: https://blog.t-systems-

mms.com/digital-stories/die-selbstbestimmte-identitaet-durch-selbstverwaltung-gegen-den-glaesernen-menschen abgerufen

Mamel, S., Babilon, L., Richard, P., Schlösser, M., & Seiter, F. (2022). *Digitale Maschinen-Identitäten als Grundbaustein für ein automatisiertes Energiesystem.* Berlin: Deutsche Energie-Agentur GmbH.

Metzger, J. (2022). *Distributed Ledger Technologie (DLT)*. Von Springer Gabler: https://wirtschaftslexikon.gabler.de/definition/distributed-ledger-technologie-dlt-54410 abgerufen

Moreland, K. (23. 10 2019). *Was ist Proof-of-Stake?* Von Ledger Academy: https://www.ledger.com/de/academy/was-ist-proof-of-stake abgerufen

Moreland, K. (23. 10 2019). *Was ist Proof-of-Work?* Von Ledger Academy: https://www.ledger.com/de/academy/blockchain/was-ist-proof-of-work abgerufen

netzpolitik.org. (14. 09 2023). *Netzpolitik.org*. Von https://netzpolitik.org/2017/verbraucherschutzgutachten-was-die-naechste-bundesregierung-fuer-die-nutzersouveraenitaet-tun-kann/ abgerufen

Pohlmann, N. (2022). *Decentralized Identifiers*. Von Norbert Pohlmann: https://norbert-pohlmann.com/glossar-cyber-sicherheit/decentralized-identifiers/ abgerufen

Pohlmann, N. (2022). *Verifiable Credentials*. Von Norbert Pohlmann: https://norbert-pohlmann.com/glossar-cyber-sicherheit/verifiable-credentials/ abgerufen

Richard, P., Mamel, S., & Vogel, L. (2019). *Blockchain in der integrierten Energiewende.* Berlin: Deutsche Energie-Agentur GmbH.

Richter, S. (12. 11 2007). *Identitätsmanagement*. Von Hasso Plattner Institut: https://hpi.de/fileadmin/_migrated/content_uploads/Identitaetsmanagement_v1.0.pdf abgerufen

Richter, S. (2022). *Identitätsmanagement* . Von HPI: https://hpi.de/fileadmin/_migrated/content_uploads/Identitaetsmanagement_-_Paper_v1.1.pdf abgerufen

Schellinger, B., Sedlmeir, J., Willburger, L., Prof.Dr. Strüker, J., & Prof.Dr. Urbach, N. (2022). *Self-Sovereign Identity (SSI).* Fraunhofer IPT.

Schellinger, B., Sedlmeir, J., Willburger, L., Strüker, J., & Urbach, N. (2022). *Mythbusting Self-Sovereign Identity (SSI) - Diskussionspapier zu selbstbestimmten digitalen Identitäten.* Von Fraunhofer Institut: https://www.fit.fraunhofer.de/content/dam/fit/de/documents/Whitepaper_Mythbusting_Self-Sovereign_Identity.pdf abgerufen

Strüker, J., Urbach, N., Guggenberger, T., Lautenschlager, J., Ruhland, N., Schlatt, V., . . . Völter, F. (2021). *Self-Sovereign Identity - Grundlagen, Anwendungen und Potenziale portabler digitaler Identitäten.* Von Fraunhofer Institut: https://www.fim-rc.de/wp-content/uploads/2021/06/Fraunhofer-FIT_SSI_Whitepaper.pdf abgerufen

Strüker, J., Weibelzahl, M., Körner, M.-F., Kießling, A., Franke-Sluijk, A., & Hermann, M. (2021). *Dekarbonisierung durch Digitalisierung.* Universität Bayreuth.

Tönsing, F. (2015). Digitale Identitäten – Was braucht man zukünftig für eine vertrauenswürdige digitale Identität? In V. D.-D. Udo Bub, *Sicherheit im Wandel von Technologien und Märkten* (S. 55-61). Wiesbaden: Springer Fachmedien Wiesbaden .

Urbach, N. (Januar 2022). *Selbstbestimmte Identitäten zur Stärkung der digitalen Souverinität.* Von Verbraucherforschung NRW: https://www.verbraucherforschung.nrw/sites/default/files/2022-02/zth-8-urbach-selbstbestimmte-identitaeten-zur-staerkung-der-digitalen-souveranitaet.pdf abgerufen

W3C. (3. März 2022). *Verifiable Credentials Data Model v1.1*. Von W3C: https://www.w3.org/TR/vc-data-model/#dfn-verifiable-credentials abgerufen

Young, E. &. (2013). *Kosten-Nutzen-Analyse für einen flächendeckenden Einsatz intelligenter Zähler.*