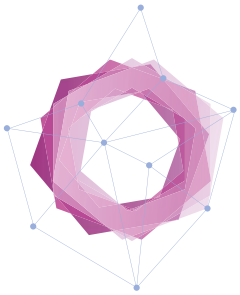
dena
Deutsche Energie-Agentur



Future Energy
Lab

BERICHT

Digitale Maschinen-Identitäten als Grundbaustein für ein automatisiertes Energiesystem

Aufbau eines Identitätsregisters auf Basis der Blockchain-Technologie (Pilot: Blockchain Machine Identity Ledger)

Impressum

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

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

E-Mail: futureenergylab@dena.de

Internet:
www.dena.de
future-energy-lab.de

Autorinnen und Autoren der dena:
Sara Mamel, Projektleiterin
Linda Babilon
Philipp Richard
Moritz Schlösser
Fabian Seiter

Gutachterinnen und Gutachter:
Matthias Babel, Fraunhofer FIT
Johannes Sedlmeir, Fraunhofer FIT
Prof. Dr. Jens Strüker, Fraunhofer FIT
Christian Wiethe, Fraunhofer FIT
Dr. Marius Buchmann, Jacobs University Bremen
Richard Hänsel, EY Law
Dr. Ing. Sven Rosinger, OFFIS

Konzeption und Gestaltung:
die wegmeister GmbH

Stand: Juni 2022

Bitte zitieren als:
Deutsche Energie-Agentur (Hrsg.) (dena, 2022) „Digitale Maschinen-Identitäten als Grundbaustein für ein automatisiertes Energiesystem. Aufbau eines Identitätsregisters auf Basis der Blockchain-Technologie (Pilot: Blockchain Machine Identity Ledger)“

Bundesministerium
für Wirtschaft
und Klimaschutz

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

Inhalt

Vorwort

Für die Energiewende ist das laufende Jahrzehnt die entscheidende Phase: Zur Erreichung der bundesweiten Klimaziele – einer Reduktion der Treibhausgase bis 2030 um 65 Prozent gegenüber dem Basisjahr 1990 – braucht es in den kommenden Jahren eine enorme Kraftanstrengung.

Dabei ist klar: Eine gelingende Energiewende muss auch eine digitale Energiewende sein. Anders sind die simultane Steuerung einer Vielzahl dezentraler Erzeugungs- und Verbrauchsanlagen, die Integration unzähliger Prosumer in das Energiesystem sowie eine Energiewirtschaft in Echtzeit nicht denkbar.

Das Pilotprojekt der Deutschen Energie-Agentur (dena) „Blockchain Machine Identity Ledger“ (BMIL) strebte an, unter Verwendung des Smart-Meter-Gateways und der Blockchain-Technologie eine wichtige Lücke auf dem Weg zur Umsetzung einer Echtzeit-Energiewirtschaft zu schließen: das Fehlen digitaler Identitäten für Energieanlagen. Wie das analoge Pendant erlauben digitale Identitäten die eindeutige Identifizierung einer Person oder Maschine, mit dem Unterschied, dass sie automatisiert geprüft und eingesetzt werden können. Die Ausstattung jeder am Energiesystem beteiligten Anlage mit einer digitalen Identität ist somit ein wichtiger Grundstein, ohne den eine skalierungsfähige, sichere und geschützte Digitalisierung des Gesamtsystems nicht möglich sein wird.

Das Projekt macht deutlich, dass eine digitale Energiewende wesentlich mehr beinhaltet als den Aufbau einer hinreichenden digitalen Messinfrastruktur. Es geht um die oben aufgeführte Frage, wie zukünftig viele dezentrale Anlagen und Marktteilnehmer aufeinander abgestimmt und gesteuert werden, wie Systemdienstleistungen vollautomatisch bereitgestellt und abgerufen werden, wie die Sektoren Strom, Wärme, Verkehr und Industrie effektiv und effizient miteinander gekoppelt werden und wie bei alledem ein ausreichendes Maß an Datensicherheit und Datenschutz gewährleistet wird. Kurzum: Es ist von großer Bedeutung, die gesamte digitale Wertschöpfung von der Infrastruktur zur Datenerfassung und -übertragung bis hin zur Datenanalyse zu betrachten und insbesondere auch die Frage der Datengovernance, also der Rahmensetzung für einen fairen und gleichzeitig wettbewerbsfähigen Datenaustauch, bei der Entwicklung neuer Ansätze mitzudenken. Und wir müssen alle diese Themen jetzt angehen, zeitlich parallel und nicht schrittweise, damit die Digitalisierung nicht der Flaschenhals auf dem Weg zur nachhaltigen Transformation des Energiesystems wird.

Das Future Energy Lab der dena sieht seine Aufgabe darin, die Potenziale digitaler Technologien für die integrierte Energiewende aufzugreifen, entsprechende Defizite in der Umsetzung aufzuzeigen, gemeinsam mit Stakeholdern aus Energie- und Digitalwirtschaft Lösungen zu entwickeln und diese in der Praxis zu erproben. Dabei kommt auch dem branchenübergreifenden Austausch eine wichtige Rolle zu. Denn viele Herausforderungen, vor denen der Energiesektor – gerade bei der Digitali-

sierung – steht, werden auch an anderer Stelle diskutiert. So spielt das Thema digitale Identitäten auch in der Zivilgesellschaft, etwa bei der Ausstellung digitaler Personalausweise, eine große Rolle und verschiedenste Branchen, wie zum Beispiel der Finanzsektor, befassen sich schon seit Längerem mit dezentralen Netzwerkarchitekturen, wie beispielsweise der Blockchain-Technologie, die mit einer Nachweisführung rund um digitale Identitäten oftmals in Verbindung gebracht wird. In diesem Projekt wurde daher bewusst der sektorübergreifende Kontakt und Austausch gesucht.

Der vorliegende Bericht ist in Zusammenarbeit mit 22 Projektpartnern entstanden, bei denen wir uns für die herausragende Zusammenarbeit und die unerlässlichen Beiträge an dieser Stelle ausdrücklich bedanken möchten. In über zwei Jahren haben, der Corona-Pandemie zum Trotz, alle beteiligten Akteure in Dutzenden Video-Calls und wenigen physischen Treffen dazu beigetragen, ein dezentral organisiertes und deutschlandweit umgesetztes Projekt zum Erfolg zu führen. Ein besonderer Dank gilt auch dem Bundesministerium für Wirtschaft und Klimaschutz (BMWK), das das Projekt ermöglichte und begleitete.

Wir bei der dena sind überzeugt: Die Energiewende funktioniert nur als digitale Energiewende. Die Ergebnisse des Pilotprojekts leisten einen Beitrag zum Gelingen der Energiewende und sind gleichzeitig Ausgangspunkt für weitere Schritte, die die dena jetzt schon mit einem Folgeprojekt in den Blick nimmt. Der letzte Punkt ist auch eine Aufforderung an Sie, liebe Leserinnen und Leser: Die Zeit eilt und nur gemeinsam können wir die vor uns liegenden Herausforderungen meistern. In der Hoffnung, eine wichtige Inspiration und Arbeitsgrundlage zu liefern, fordern wir Sie auf, weiter gemeinsam über die nächsten notwendigen Schritte zu diskutieren, und wünschen viel Spaß beim Lesen.

Andreas Kuhlmann
Vorsitzender der Geschäftsführung
der Deutschen Energie-Agentur (dena)

Philipp Richard
Bereichsleiter Digitale Technologien & Start-up
Ökosystem der Deutschen Energie-Agentur (dena)

1. Einleitung

Die Digitalisierung ist bereits seit einigen Jahren ein zentrales Thema in Politik, Wirtschaft und Gesellschaft. Es vergeht kein Tag, ohne dass Digitalisierungsvorhaben auf den Weg gebracht, neue Technologien vorgestellt oder wegverändernde digitale Geschäftsfelder erschlossen werden. Nicht zuletzt durch die Corona-Pandemie hat die Bedeutung der Digitalisierung einen zusätzlichen Schub erhalten. Im gleichen Zuge wurden erneut grundsätzliche Defizite offenbar, die nicht nur im Energiebereich zu beheben sind.

Das **dena-Projekt „Blockchain Machine Idendity Ledger" (BMIL)**, dessen Ergebnisse der vorliegende Bericht zusammenfasst, hat ein solches Digitalisierungsdefizit behandelt: das Fehlen standardisierter und damit skalierungsfähiger, sicherer, datenschutzkonformer und für alle relevanten Akteure **leicht zugänglicher digitaler Identitäten im Energiesektor**. Derartige digitale Identitäten bieten enorme Effizienzvorteile für die hohen Koordinationsanforderungen an das Energiesystem der Zukunft, in dem die Grundlage für eine sichere teil- bzw. vollautomatische Kommunikation gelegt wird.

Die zentrale Voraussetzung für die sichere und schnelle Kommunikation ist das fortlaufende Nachweisen und Überprüfen der Identitäten und Rechte von Akteuren (natürliche und juristische Personen), aber auch von Anlagen (Maschinen), die im Besitz dieser Akteure sind. Hintergrund ist, dass durch den sicheren Nachweis der Identität stets damit verknüpfte Identitäts- und Bewegungsdaten ebenfalls zugeordnet werden können und dadurch **digitale Vertrauensketten** verlässlich und schnell aufgebaut werden. Dabei können in einem stark dezentral geprägten und integrierten Energiesystem das erforderliche Volumen und die notwendige Geschwindigkeit für diese Prozesse nur digital gestützt erreicht werden, da andernfalls der Aufwand für eine zeitnahe und wirtschaftliche Umsetzung zu groß wäre.

Während es im Projekt BMIL speziell um digitale Identitäten für Energieanlagen ging, reicht die Relevanz des Themas weit über den Energiesektor hinaus. In der Auseinandersetzung mit digitalen Identitäten ergeben sich nicht nur zahlreiche Parallelen zu anderen Branchen, sondern auch Anknüpfungspunkte zu grundsätzlichen Fragestellungen der Digitalisierung, wie beispielsweise zu Governance-Strukturen (zentrale versus dezentrale Netzwerkarchitekturen), Datenökonomie sowie Datenschutz und -sicherheit. Es ist daher wichtig, digitale Identitäten nicht isoliert, sondern im Gesamtkontext der Digitalisierung und der Energiewende zu betrachten.

Warum überhaupt Digitalisierung?

Der Einsatz digitaler Technologien entfaltet grundsätzlich immer dann eine große Wirkung hinsichtlich Schnelligkeit und Effizienz von Prozessen, wenn große Datenmengen erfasst, übertragen, gesammelt, analysiert und / oder ausgewertet werden müssen. Dieser Bedarf existiert im Energiesektor seit jeher und zunehmend. Ursache ist die wachsende Systemkomplexität, in erster Linie bedingt durch den Ausbau volatiler und dezentral verteilter Erzeugungsanlagen sowie durch das Aufkommen neuer, steuerbarer und sektorübergreifender Verbraucher (z. B. Wärmepumpen, Elektromobilität). Eine Vielzahl von Anlagen partizipiert somit am Energiesystem und bedingt dadurch einen steigenden **Automatisierungsbedarf**. Diese Entwicklung zu einem dezentraleren Energiesystem bietet neue Chancen für Personen oder Gemeinschaften auf lokaler Ebene, beispielsweise als Energieerzeuger, als Aggregator oder perspektivisch auch mit Flexibilitätsangeboten und weiteren Geschäftsaktivitäten an der Energiewende mitzuwirken. Dies kann sich unter anderem positiv auf die Wettbewerbssituation im Energiemarkt, den Fortschritt beim Ausbau der erneuerbaren Energien und die Akzeptanz der Energiewende auswirken.[1]

Die Digitalisierung bietet zudem die Möglichkeit, zusätzlich notwendige Freiheitsgrade einer integrierten Energiewende durch die Kopplung verschiedener Sektoren und den sektorübergreifenden Ausgleich von volatiler Erzeugung und Last zeitlich und örtlich auszunutzen. Digitalisierung fungiert demnach sowohl als **Treiber als auch Enabler der Energiewende**. Der entscheidende Vorteil liegt dabei in der Fähigkeit, mithilfe von digitalen Technologien Informationen effektiv und effizient verarbeiten zu können, auch in großskaligen Systemen. Während heute häufig noch Menschen direkt miteinander kommunizieren, um Prozesse im Energiesystem zu steuern, sollte vieles davon in Zukunft voll automatisiert und echtzeitnah erfolgen, beispielsweise der Lieferantenwechselprozess, der in Deutschland noch bis zu 15 Tage benötigt. Der Arbeitsaufwand und damit die Kosten sind in der Folge geringer. Damit ermöglicht die Digitalisierung nicht nur die technische, sondern auch die wirtschaftliche Umsetzung der Energiewende.

Was sind Herausforderungen auf dem Weg zu einer digitalen Energiewende?

Ein breitflächiger Einsatz digitaler Technologien über Wertschöpfungsstufen hinweg wird durch die **Standardisierung** von Software-Schnittstellen und Datenformaten befördert. Eine fehlende Standardisierung kann nicht nur eine Hürde für die Digitalisierung darstellen, sondern gleichsam ein Flaschenhals für den Umbau des Energiesystems sein. Standards entstehen in der Regel, wenn viele Anbieter am Markt von einheitlichen Standards profitieren, es einen Monopol- oder Quasimonopolanbieter gibt, der seinen Standard durchsetzt, oder ordnungsrechtlich ein bestimmter Standard vorgegeben wird. Es sollte aber nicht übergangen werden, dass Standards auch gewisse Nachteile haben. So ist der Prozess von einem Standard zum nächsten in der Regel langsam, es entstehen mitunter

1 Vgl. dena (2022): Energy Communities: Beschleuniger der dezentralen Energiewende: https://future-energy-lab.de/fileadmin/dena/Publikationen/PDFs/2022/dena-ANALYSE_Energy_Communities_Beschleuniger_der_dezentralen_Energiewende.pdf

unerwünschte Pfadabhängigkeiten und neuere Technologien finden erst verspätet Anwendung. Gerade in der Energiewirtschaft ist es von besonderer Bedeutung, dass digitale Anwendungen auf zuverlässige Daten mit entsprechenden Gütekriterien zurückgreifen können, da Teile der Energiewirtschaft zur kritischen Infrastruktur gehören. Eine ausreichende Datenqualität für digitale Anwendungen beispielsweise zur Automatisierung mittels künstlicher Intelligenz ist bisher jedoch in der Energiewirtschaft nicht immer gegeben. Standards – sofern nicht bereits vorhanden – können hier für Einheitlichkeit und dadurch für Effizienz und Sicherheit sorgen. Eine Herausforderung besteht darin, durch das richtige Maß einen verlässlichen Rahmen für Investitionen zu bieten, ohne Innovationen durch eine Durchstandardisierung zu bremsen.

Die Potenziale der Digitalisierung für das Energiesystem erschließen sich nur, wenn notwendige Daten überhaupt verfügbar sind. Dies ist sowohl eine technische (vorhandene Messinfrastruktur u. a.) als auch eine ökonomische (bestehende wirtschaftliche Anreize) Fragestellung, die durch den Regulierungsrahmen beeinflusst wird. Es braucht eine wettbewerbsfähige und zugleich faire Governance, quasi eine **Datenökonomie**[2] mit einem geeigneten Ordnungsrahmen, innerhalb dessen Akteuren entweder wirtschaftliche Anreize gesetzt werden, um Daten von öffentlichem Interesse zu teilen, oder Regularien eingeführt werden, die zum Teilen dieser Daten verpflichten. Gleichzeitig ist zu respektieren, dass Unternehmen auch ein nachvollziehbares Interesse daran haben, besonders attraktive Informationen für sich zu behalten, etwa um eigene Marktpositionen abzusichern und nachhaltiges Wirtschaften sicherzustellen. Welche Voraussetzungen gegeben sein müssen, damit Informationen im wettbewerblichen Umfeld nicht ohne Gegenwert oder Zustimmung geteilt werden müssen, ist daher ebenfalls eine entscheidende Frage, die insbesondere in einem entflochtenen Energiesystem von übergeordneter Bedeutung ist.

Eine funktionierende **Datengovernance** bzw. Datenökonomie für das Energiesystem der Zukunft braucht daher zunächst auch klare Regeln bezüglich der Eigentumsrechte von Daten, die so auszugestalten sind, dass sie die Energiewende fördern und nicht behindern, ohne die zurecht hohen Erwartungen an Datenschutz und Datensicherheit zu vernachlässigen. Mit Blick auf digitale Identitäten macht es einen klaren Unterschied, ob sie selbst verwaltet werden oder nicht und ob sie zentral oder dezentral abgelegt werden. Der vorliegende Bericht setzt sich insofern mit den genannten Fragen exemplarisch auseinander.

Im Energiesektor ist **Datensicherheit** von übergeordneter Bedeutung. Wenn Daten, die beispielsweise die Basis für einen automatischen Energiehandel liefern, manipuliert oder beeinträchtigt werden, kann dies verheerende Folgen haben. Energiemengen, die beispielsweise in einem virtuellen System ordnungsgemäß verkauft und eingeplant werden, tragen dazu bei, dass Bilanzkreise „auf dem Papier“ ausgeglichen sind, und stärken den Eindruck, dass das System im Gleichgewicht ist. Sollte jedoch der einer Energieanlage zugeordnete Datensatz zum Beispiel zu einer bestimmten Viertelstunde gefälscht sein und die Energiemenge faktisch gar nicht existieren, sorgt dies für eine Schieflage, die das physikalische System ins Ungleichgewicht bringt. Auch an diesem Beispiel wird deutlich, wie bedeutsam digitale Identitäten sind, um einen verlässlichen Anker für darauf fußende Datensätze zu liefern, mit dem Ziel, die Datensicherheit zu fördern.

Auch **Datenschutz** wird im Kontext der Energiewende ein immer relevanteres Thema. Zum einen, weil es deutlich mehr elektronische Geräte gibt, die grundsätzlich Daten erfassen und teilen, die wiederum in ihrer Gesamtheit Rückschlüsse auf personenbezogene Informationen zulassen. Zum anderen, weil Daten zunehmend einen Wert erhalten und entsprechend ein Wirtschaftsgut darstellen. An dieser Stelle ist es wichtig, zu betonen, dass es sichere und effektive Methoden gibt, um digitale Daten zu schützen. Dies ist sowohl eine technische als auch eine organisatorische Herausforderung, worauf im Rahmen des Berichts eingegangen wird.

Vor dem Hintergrund dieser allgemeinen Einordnung der Herausforderungen in der digitalen Energiewende steigt das folgende Kapitel 2.1 tiefer in die Themen digitale Identitäten und digitales Identitäten-Register ein. Denn die allgemeinen Herausforderungen finden sich in diesem spezifischen Anwendungsfall wieder.

Der weitere Bericht ist folgendermaßen aufgebaut: Kapitel 2 gibt einen Überblick zur durchgeführten Pilotierung und dem Erreichten, inkl. Beschreibung der bestehenden Lücke in der Energiewirtschaft, dem Pilotierungskonzept zum Schließen der genannten Lücke mit den drei verschiedenen erprobten Varianten sowie den wichtigsten Ergebnissen und Empfehlungen für nächste Schritte. Die nachfolgenden Kapitel gehen auf die verschiedenen Aspekte vertiefter ein und liefern die ausführliche technische, ökonomische und regulatorische Bewertung. Kapitel 3 legt die Motivation und Ausgangslage für das Projekt ausführlich dar. In Kapitel 4 werden die drei verschiedenen Anbindungsvarianten im Detail beschrieben und bewertet. Die Anwendungsmöglichkeiten der automatisierten Geräteanbindung und digitalen Identitätsverwaltung wurden als Showcases im Rahmen der Pilotierung analysiert und werden in Kapitel 5 beschrieben und bewertet.

2 Vgl. dena (2022): Die Datenökonomie in der Energiewirtschaft: https://www.dena.de/fileadmin/dena/Publikationen/PDFs/2022/ANALYSE_Die_Datenoekonomie_in_der_Energiewirtschaft.pdf

2. Projektüberblick – ein Baustein für das automatisierte Energiesystem

2.1 Die digitale Lücke in der Energiewirtschaft – von Blockchain, SSI und Maschinenidentitäten

Von der Idee zur Pilotierung

2022 ist die Bedeutung einer Ende-zu-Ende-Digitalisierung für die Dekarbonisierung in der Energiewirtschaft weitgehend unbestritten. Insbesondere das Fehlen digitaler Personen- und Maschinenidentitäten wird zunehmend als eines der größten Digitalisierungshemmnisse im Energiesystem wahrgenommen. Das Pilotierungsprojekt „Blockchain Machine Identity Ledger" adressiert diese digitale Lücke und mit seinem erfolgreichen Abschluss ist es nun an der Zeit, den zurückgelegten wie den noch vorausliegenden Weg zu reflektieren.

Im Jahr 2016 ist das Gesetz zur Digitalisierung der Energiewende (GDEW) in Kraft getreten und regelt seitdem die Ausstattung und den Betrieb intelligenter Messsysteme (Smart Meter). Seit dem Jahr 2017 gilt auch die Marktstammdatenregisterverordnung (MaStRV), nach der ein zentrales elektronisches Verzeichnis über verifizierbare energiewirtschaftliche Stammdaten aufzubauen ist, in dem alle Stromerzeugungsanlagen (das heißt auch kleine Balkonanlagen), Gaserzeugungsanlagen und Stromspeicher zu registrieren sind, die unmittelbar oder mittelbar an ein Strom- oder Gasnetz angeschlossen sind. Das Marktstammdatenregister (MaStR) verfolgt damit den Zweck, bislang getrennte Register für Identitätsdaten – die Kraftwerksliste, das Anlagenregister und das Photovoltaik-Meldeportal – zusammenzuführen.

Bei dieser Ausgangslage reifte die Idee, das geplante Kommunikationsmodul intelligenter Messsysteme, das sogenannte Smart-Meter-Gateway (SMGW), mit dem neuen Anlagenregister konzeptionell wie technisch digital zu verbinden. Dabei verstärkte die zunehmende Bereitschaft, innovative neue Technologien zu erproben, den bestehenden Optimismus und Elan. Konkret sollte eine **Blockchain** für die digitale Verwaltung eines weiterentwickelten Anlagenregisters anstatt einer herkömmlichen Datenbank genutzt werden, um so eine teilautomatisierte Registrierung, Verwaltung und Nutzung von Marktstammdaten in einem möglichst offenen System zu ermöglichen. Insbesondere die **Verbindung des SMGW mit dem Anlagenregister über den eingebauten Kryptochip** versprach so eine sichere und jederzeit elektronisch überprüfbare Identifikation und Authentifizierung von Anlagen. Das SMGW war vorgesehen, hierbei zu einem teilnehmenden Rechner (Knoten) in einer Blockchain zu werden. Die Vorteile lagen auf der Hand: Für Verteilnetzbetreiber würden sich damit einige der ihnen gemäß MaStRV zugewiesenen Prüfaufgaben erheblich vereinfachen und beschleunigen und es würde auch eine höhere Datenqualität im Sinne einer einheitlichen und konsistenten Datenbasis sichergestellt werden. Konkret könnten Identitäten und Rechte von Personen und Anlagen kostengünstig und sicher in Echtzeit digital verifiziert werden, um hierauf dann hochdynamische Vertrauensketten zwischen einer Photovoltaik-Anlage, einem SMGW und dem MaStR zu ermöglichen: Der schnelle Wechsel von Anlagen zwischen Eigenverbrauch, dem Anbieten von Systemdienstleistungen und der Teilnahme an Handelsmärkten könnte technisch umgesetzt werden. Digitale Personen- und Maschinenidentitäten wurden dementsprechend als ein wichtiger Dreh- und Angelpunkt in der entstehenden Echtzeit-Energiewirtschaft definiert. Insgesamt verbreitete sich ab dem Frühjahr 2018 die Einsicht, die mangelnde Ende-zu-Ende-Digitalisierung durch den Aufbau digitaler Vertrauensketten zu adressieren. Zur selben Zeit wurde der Austausch mit zuständigen Ministerien zu diesem Thema aufgenommen.

Zunächst startete jedoch Ende April 2018 die Stakeholder-Studie der Deutschen Energie-Agentur „Blockchain in der integrierten Energiewirtschaft". Schnell stellte sich heraus, dass eine Reihe von Industriepartnern ähnliche Auffassungen und Ideen hatten. So wurde in einer Reihe von Workshops unter anderem der Use Case „Anmeldung von Anlagen im Marktstammdatenregister (MaStR)" definiert. Im Ergebnis entstand ein Prozess, der eine Blockchain für die digitale Verwaltung eines Registers vorsieht, die teilautomatisierte Registrierung und Verwaltung von Marktstammdaten ermöglicht und die selektive Bereitstellung von Marktstammdaten vorsieht. Die technische, ökonomische und regulatorische Machbarkeit wurde geprüft und die Prüfung fiel grundsätzlich positiv aus.[3]

Weitere Abstimmungen und Diskussionen mit dem BMWi führten im Anschluss an die Studie „Blockchain in der integrierten Energiewirtschaft" schließlich zur Vergabe der Machbarkeitsstudie „Blockchain-basierte Erfassung und Steuerung von Energieanlagen mithilfe des Smart-Meter-Gateways: Machbarkeitsstudie und Pilotkonzept" im Mai 2019[4]. Mitte des Jahres 2019 startete schließlich die Deutsche Energie-Agentur gemeinsam mit Forschern und mehr als einem Dutzend Unternehmen das Projekt „Blockchain-basiertes Geräte-ID-Register für die Energiewirtschaft" zur Erarbeitung eines konkreten Pilotierungskonzepts, was schließlich in 2020 zum Umsetzungsprojekt „Blockchain Machine Identity Ledger" (BMIL) als Teil des Future Energy Lab der Deutschen Energie-Agentur führte.

Von Blockchain zu SSI

Über die verschiedenen Projekte und einzelnen Schritte hinweg hat sich insbesondere das Verständnis hinsichtlich der Rolle einer Blockchain für das Verwalten von Unternehmens-, Personen- und Maschinenidentitäten in den letzten Jahren entscheidend weiterentwickelt. So gewann das Konzept **Self-Sovereign Identities (SSI) für die Verwaltung von Personen- und Maschinenidentitäten** immer mehr an Bedeutung.[5] Ausgehend von den ersten intuitiven Vorstellungen von der Rolle von Blockchains im Anwendungsszenario erwiesen sich insbesondere zwei Aspekte als kritisch.

Kapitel 2.1: Autoren: Matthias Babel, Johannes Sedlmeir, Jens Strüker und Christian Wiethe (Fraunhofer FIT)

3 Strüker, Jens et al. (2019): Technisches und Ökonomisches Gutachten im Rahmen der Multi-Stakeholder-Studie „Blockchain in der integrierten Energiewende" der Deutschen Energie-Agentur, S. 86–155, https://www.dena.de/newsroom/publikationsdetailansicht/pub/blockchain-in-der-integrierten-energiewende/
4 https://www.bmwi.de/Redaktion/DE/Downloads/Studien/blockchain-smart-meter-gateway-kurzfassung.html
5 Siehe auch Sedlmeir et al. (2021): Digital identities and verifiable credentials, Business & Information Systems Engineering 63, S. 603-613

Zum einen bestehen bei einem **SMGW als teilnehmendem Rechner (Knoten) in einer Blockchain** erhebliche Herausforderungen hinsichtlich der Skalierbarkeit. Anders als bei zentralen Netzwerken werden Operationen wie beispielsweise die Ausführung von Finanztransaktionen und Smart Contracts oder die Speicherung von Daten nicht nur von einem Einzelnen, sondern von mehreren Instanzen redundant ausgeführt. Dazu müssen die notwendigen Informationen an alle Systemknoten weitergeleitet und der aktuelle Zustand des Netzwerks muss von ihnen gespeichert werden. Das SMGW müsste als Blockchain-Knoten also auch die Informationen aller anderen Blockchain-Akteure herunterladen, verarbeiten und speichern, ist aber – aus guten Gründen – nicht für diese Prozesse der hochskalierten Datenverarbeitung ausgelegt. Aufgrund der beschriebenen inhärenten Redundanz der Blockchains bringen die Rechenleistung, der notwendige Speicherplatz und die (bislang äußerst geringe) Bandbreite, die für SMGWs vorgesehen sind, wesentliche Einschränkungen in Bezug auf die Leistungsfähigkeit einer solchen Blockchain mit sich. Lösungen sind zwar weiterhin vielversprechend [6] , aber aktuell stehen die Herausforderungen noch nicht in einem angemessenen Verhältnis zum Nutzen: Dezentralisierung ist kein Selbstzweck, sondern ein Mittel, um ein hohes Maß an Resilienz und Verfügbarkeit zu erlangen sowie ein dezentraleres, automatisiertes Rechtemanagement auf einer gemeinsamen IT-Infrastruktur zu schaffen, auf die sich alle Akteure im Energiesektor (leichter) verständigen können. Beide Ziele können bereits durch einen moderaten Grad an Dezentralisierung erreicht werden, etwa durch Knoten bei den wesentlichen Institutionen im Energiesektor. Für alle weiteren Akteure dürfte eine Client-Applikation (Schnittstelle auf einem Netzwerk-Endgerät zu einem Zentralrechner) auf den entsprechenden Systemen ausreichen, die sich mit einem Blockchain-Knoten einer anderen Institution, dem hinsichtlich der auszuführenden Operation vertraut wird, für Lese- und Schreibzugriff verbinden kann.

Neben dem SMGW als Knoten stellte sich auch immer deutlicher das unmittelbare Speichern von Stamm- und Bewegungsdaten auf der Blockchain als besondere Herausforderung für eine Blockchain-Technologie heraus.[7] Denn zwei der Kerneigenschaften der Blockchain-Technologie sind die Unveränderlichkeit und die Transparenz der auf ihr gespeicherten Daten. Auf die Blockchain geschriebene Anlagenstammdaten können entsprechend zu einem späteren Zeitpunkt nicht mehr gelöscht werden. Außerdem sind diese Daten, sofern sie nicht verschlüsselt abgelegt sind, für alle Netzwerkteilnehmer einsehbar. Da insbesondere Kleinstanlagen meist eng mit ihrem Eigentümer verknüpft sind, kollidiert dieser Ansatz schnell mit der Datenschutz-Grundverordnung (DSGVO). Dies ist zum einen der Fall, weil das dort festgehaltene Recht auf Vergessenwerden nicht mehr eingeräumt werden kann: Aufgrund der replizierten Datenhaltung verliert der Eigentümer regelrecht die Hoheit über die Stammdaten seiner Anlage. Zum anderen sind verschlüsselte Daten auf der Blockchain gerade wegen ihrer Unveränderlichkeit datenschutzrechtlich problematisch. Es ist nicht garantiert, dass aktuell als sicher geltende Verschlüsselungsverfahren in Zukunft weiterhin Bestand haben. Ein anschauliches Beispiel ist die asymmetrische Verschlüsselung, deren Sicherheit durch Quantencomputer gefährdet wird. Blockchain-Protokolle könnten zwar durch Anpassung der Verschlüsselungsverfahren für neue Transaktionen geschützt werden, für zurückliegende Transaktionen ist dieser Weg aber versperrt. Darüber hinaus können auch für Außenstehende unkenntlich gemachte Daten, wie es durch Verschlüsselung oder Hash-Funktionen erreicht werden kann, direkt oder durch die damit verbundenen Metadaten sensitive Daten darstellen. So ergeben sich aus deren Spur auf der Blockchain wiederum schützenswerte Informationen. Dieser Sachverhalt verhält sich ähnlich wie die Pseudonymisierung eines Accounts auf der Bitcoin-Blockchain. Auf der anderen Seite sind verschlüsselte Daten auf einer Blockchain etwa für die Verwendung in Smart Contracts weitgehend nutzlos. [8]

Eine weitere Herausforderung, die aus der redundanten Speicherung der Daten resultiert, ist die eingeschränkte Skalierbarkeit, die Blockchain-Lösungen aufgrund der replizierten Verarbeitung von Informationen meist mit sich bringen. Zwar gibt es aktuell diverse Verfahren, sie zu adressieren, wie Roll-ups oder Sharding, jedoch ist sie immer noch eine der stärksten Limitationen, denen sich die Blockchain-Technologie stellen muss, und hat auch bei reiner Datenspeicherung mit dem Zweck von Verfügbarkeit ohne komplexe Berechnungen nur begrenzte Möglichkeiten.

SSI-basierte Maschinenidentitäten für eine konsequente Ende-zu-Ende-Digitalisierung

Das Konzept von SSI verspricht die beschriebenen Herausforderungen zu adressieren und besinnt sich dabei auf ein seit mehr als 30 Jahren bekanntes und auch erfolgreich in der Praxis angewendetes Paradigma, das eine Teilmenge von kryptografischen Verfahren nutzt. Diese genießen heute unter anderem durch das Aufkommen von Blockchains ein verstärktes Maß an Aufmerksamkeit. Dieses Paradigma sind sogenannte digitale Zertifikate basierend auf digitalen Signaturen und allgemein asymmetrischer Verschlüsselung, die auf einer Public Key Infrastructure (PKI) aufbauen. Dieser Ansatz findet seit Jahrzehnten erfolgreich Anwendung auf sicheren Websites (https), in vielen sicherheitsbewussten Unternehmen sowie in kritischen Infrastrukturen. Digitale Zertifikate wurden dabei noch nicht regelmäßig für domänenübergreifende Anwendungen geöffnet. [9] Genau dies ist nun die Neuerung, die das Hinzufügen von Blockchains verspricht: ein kollaborativer Ansatz, bei dem eine PKI gemeinsam von vielen Akteuren betrieben wird.

6 Vgl. Blockchain-Protokolle wie Mina: https://minaprotocol.com
7 Vgl. Überblick in Bogensperger et al. (2021): Welche Zukunft hat die Blockchain-Technologie in der Energiewirtschaft, Diskussionspapier, https://stiftung-umweltenergierecht.de/wp-content/uploads/2021/07/InDEED_Diskussionspapier-Blockchain-Energiewirtschaft_2021-07-22.pdf
8 Siehe dazu auch Sedlmeir et al. (2022): The transparency challenge of blockchain in organizations, Electronic Markets, https://doi.org/10.1007/s12525-022-00536-0
9 Siehe auch Schellinger et al. (2022): Mythbusting Self-Sovereign Identity (SSI) - Diskussionspapier zu selbstbestimmten digitalen Identitäten, https://www.fim-rc.de/wp-content/uploads/2022/06/Whitepaper_SSI_Mythbusting_German_version_compressed.pdf

Ein zertifikatsbasierter Ansatz erlaubt den bilateralen Austausch verifizierbarer Informationen und damit in gewisser Weise eine noch dezentralere Architektur, als es bei einer Datenverarbeitung über Blockchain-Knoten der Fall wäre. Das bilaterale Vorzeigen von Zertifikaten ermöglicht die datenschützende Überprüfung von behaupteten Eigenschaften und Attributen einer Anlage bzw. von Rechten ihrer Eigentümer. Die lokale Speicherung von Zertifikaten ermöglicht wiederum die selektive Bereitstellung von Daten und damit die Minimierung von ausgetauschten Daten auf das Notwendige, was gerade hinsichtlich der Zunahme von Kleinstanlagen für die informationelle Selbstbestimmung von Endnutzerinnen und -nutzern, aber auch in Bezug auf die Wahrung von Unternehmensgeheimnissen erstrebenswert ist. Das einheitliche Momentum hinsichtlich Blockchain-unterstützter, zertifikatsbasierter digitaler Identitäten für Personen und Unternehmen in Politik (Projekte beim Bundeskanzleramt) und Wirtschaft (Schaufensterprojekte wie ID-Ideal und IDunion) sowie für Maschinen verspricht zudem mittelfristig eine Konsolidierung der zu entwickelnden Standards und Komponenten und kommt damit der Effizienz und Sicherheit zugute.[10] SSI-Komponenten sind daher unter anderem auch in GAIA-X und weiteren Projekten im Gespräch.[11]

Im Kontext der Umsetzung in BMIL können bei einem SSI-basierten Ansatz Attribute von Anlagen im Energiesektor durch die sogenannten Verifiable Claims, die auf von Autoritäten einmalig ausgestellten Zertifikaten beruhen, bis zu deren Widerruf belegt werden. Eine dieser Autoritäten, insbesondere für bereits existierende Anlagen, könnte das bestehende MaStR sein, das weiterhin seine Daten nicht auf einem vollständig öffentlich zugänglichen System hält. Solche Autoritäten können im Allgemeinen über Zertifikatsketten verifiziert werden. So könnte beispielsweise die Bundesnetzagentur vertrauenswürdige Zertifizierer (Market Authorities) ernennen, die dann wiederum Zertifizierer für Anlagen (Physical Asset Authorities) zertifizieren. Diese wiederum können dann durch eine digitale Signatur (Zertifikate) verifizierbare Claims für die Anlagen ausstellen. Diese Vertrauensketten können über Schemata und Rückruflisten (Revocation Registries) auf einer öffentlichen Blockchain jederzeit auf Korrektheit und Aktualität geprüft werden. Denkbar ist demnach auch, dass Einträge in das MaStR auf Basis von Verifiable Claims direkt durch die Wallet der Anlage vorgenommen werden könnten. Zudem ist auch eine Echtzeitbestätigung von Claims ohne Zertifikate bilateral von Autoritäten grundsätzlich möglich.

Eine öffentliche Blockchain (aber auch von den Autoritäten verwaltete Datenbanken mit breiten Leserechten) könnte an dieser Stelle genutzt werden für die Registrierung von öffentlichen Identitäten von Autoritäten und von Zertifikatsschemata sowie für die Bereitstellung von Revocation Registries für die genannten Zertifikate (sowohl für Zertifikate von Anlagen als auch für Zertifikate von Authorities). Revocation Registries erlauben es, ein Zertifikat für ungültig zu erklären. Grundsätzlich können hier in Zukunft auch verschiedene Blockchains oder herkömmliche Datenbanken nebeneinander zum Einsatz kommen: Da es in erster Linie um Lesezugriff geht, ist eine Interoperabilität letztlich nur eine Frage der Standardisierung. Man benötigt keine Bridges zwischen den Blockchains. Sobald langfristig Anlagen an mehreren Märkten auf unterschiedlichen Blockchains agieren, wird jedoch unter Umständen die Option von Bridges zwischen Blockchains notwendig, um Double-Spends, etwa in Form von Doppelvermarktung der Erzeugungsleistung, durch die Registrierung auf mehreren Blockchains zu verhindern. Dabei ist zu betonen, dass Bridges zwischen Blockchains für Anwendungsfälle benötigt werden, weniger aber hin zu einer Blockchain, die öffentliche Identitäten von Zertifizierern oder Revocation Registries verwaltet – es sei denn, eine Identitätsverifizierung muss auch im Rahmen eines Smart Contract erfolgen, was aber aufgrund der Sensitivität von Daten nur selten sinnvoll sein dürfte.

Heute ist der Informationsaustausch zwischen Verteiler- und Übertragungsnetzbetreibern von einer medienbruchfreien Ende-zu-Ende-Digitalisierung noch immer weit entfernt. Ähnliches gilt für das Engpassmanagement oder die Marktkommunikation. Millionen von PV-Anlagen und Tausende von Wärmepumpen, Heimspeichern und BHKWs sind bislang nicht digital in das Energiesystem integriert. Entsprechend bedeutet ein Wechsel von Erzeugungsanlagen und Speichern vom Eigenverbrauch hin zur Bereitstellung von Systemdienstleistungen oder zur Teilnahme am Stromhandel weiter fehleranfällige und zeitintensive Prozesse in Papierform. Das Projekt BMIL verspricht mit einem weiterentwickelten dezentralen Anlagenregister einen entscheidenden Beitrag zur weiteren Digitalisierung energiewirtschaftlicher Prozesse.

Es sollte angestrebt werden, ein digitales Zielbild der integrierten Energiewirtschaft zu entwerfen und anschließend konsequent zu verfolgen. Heute sind nicht nur kommunikationsfähige Strom- und Wärmezähler und das Anlagenregister konzeptionell und digital getrennt, sondern auch das Herkunftsnachweisregister steht unverbunden zum Anlagenregister. Ein Zielbild, das die Transformation leiten kann, würde helfen. Hierfür kann die Implementierung und Erprobung des Blockchain Machine Identity Ledger bereits wertvolle Gestaltungshinweise liefern.

2.2 Projektaufbau und Pilotierungskonzept

In dem Pilotierungsvorhaben Blockchain Machine Identity Ledger brachte die dena insgesamt 22 Unternehmen, Organisationen und Start-ups der Energie- und Digitalwirtschaft sowie der Wissenschaft zusammen, um gemeinsam einen wesentlichen Baustein für die digitale Infrastruktur des zukünftigen Energiesystems aufzubauen. Die grundlegende Herangehensweise war, wie bei

10 Siehe auch Sedlmeir et al. (2021): Digital identities and verifiable credentials, Business & Information Systems Engineering 63, S. 603-613
11 Vgl. GAIA-X: https://www.data-infrastructure.eu/GAIAX/Navigation/EN/Home/home.html; Id-Ideal: https://id-ideal.de/ sowie IDunion: https://idunion.org/

allen Pilotierungsvorhaben im Future Energy Lab, ein hohes Maß an Offenheit unter den beteiligten Partnern sicherzustellen und somit die Anschlussfähigkeit für aufbauende Innovationen zu ermöglichen.

Im Folgenden wird der Projektaufbau inklusive Problemstellung, Zielsetzung und grundlegender Annahmen erläutert.

2.2.1 Der Partnerkreis

Das Partnerkonsortium vereinte etablierte Unternehmen mit viel Erfahrung mit jungen Start-ups. Dabei wurde der gleichberechtigten Zusammenarbeit, die auf Größenunterschiede keine Rücksicht nimmt, eine besondere Bedeutung beigemessen. Die Projektleitung und -steuerung lag bei der dena.

Ein Team aus erfahrenen Akteuren der Wissenschaft begleitete das Projekt in der technischen (OFFIS), ökonomischen (Jacobs University) und regulatorischen (EY Law) Evaluation. Parallel wurde durch eine weitere wissenschaftliche Begleitung (Fraunhofer FIT) sichergestellt, dass der operative Projektverlauf mit der wissenschaftlichen Evaluation gut verzahnt wurde, indem insgesamt vier Fortschrittsberichte über die circa zwei Jahre andauernde Pilotierungsphase verfasst wurden.

Der Kreis der beauftragten Partnerunternehmen bestand aus Unternehmen mit stärkerer Ausrichtung auf Blockchain (-Infrastruktur) und digitale Identitäten (Energy Web, KILT, OLI Systems, Parity, Riddle&Code, Spherity, T-Systems, YOUKI) sowie aus Akteuren der Energiewirtschaft bzw. Anlagenanbindung, darunter zertifizierte Smart-Meter-Hersteller (PPC, Theben), Gateway-Administratoren und Unternehmen aus dem Bereich Messstellenbetrieb (GWAdriga, meterpan, Voltaris) und Energieversorgung (VSE).

Schließlich begleiteten weitere assoziierte Unternehmen mit ihrem zusätzlichen energie- und digitalwirtschaftlichem Wissen den Projektfortschritt und wirkten als Sounding Board für die erzielten Ergebnisse (EnBW, E.On, SAP und 50Hertz).

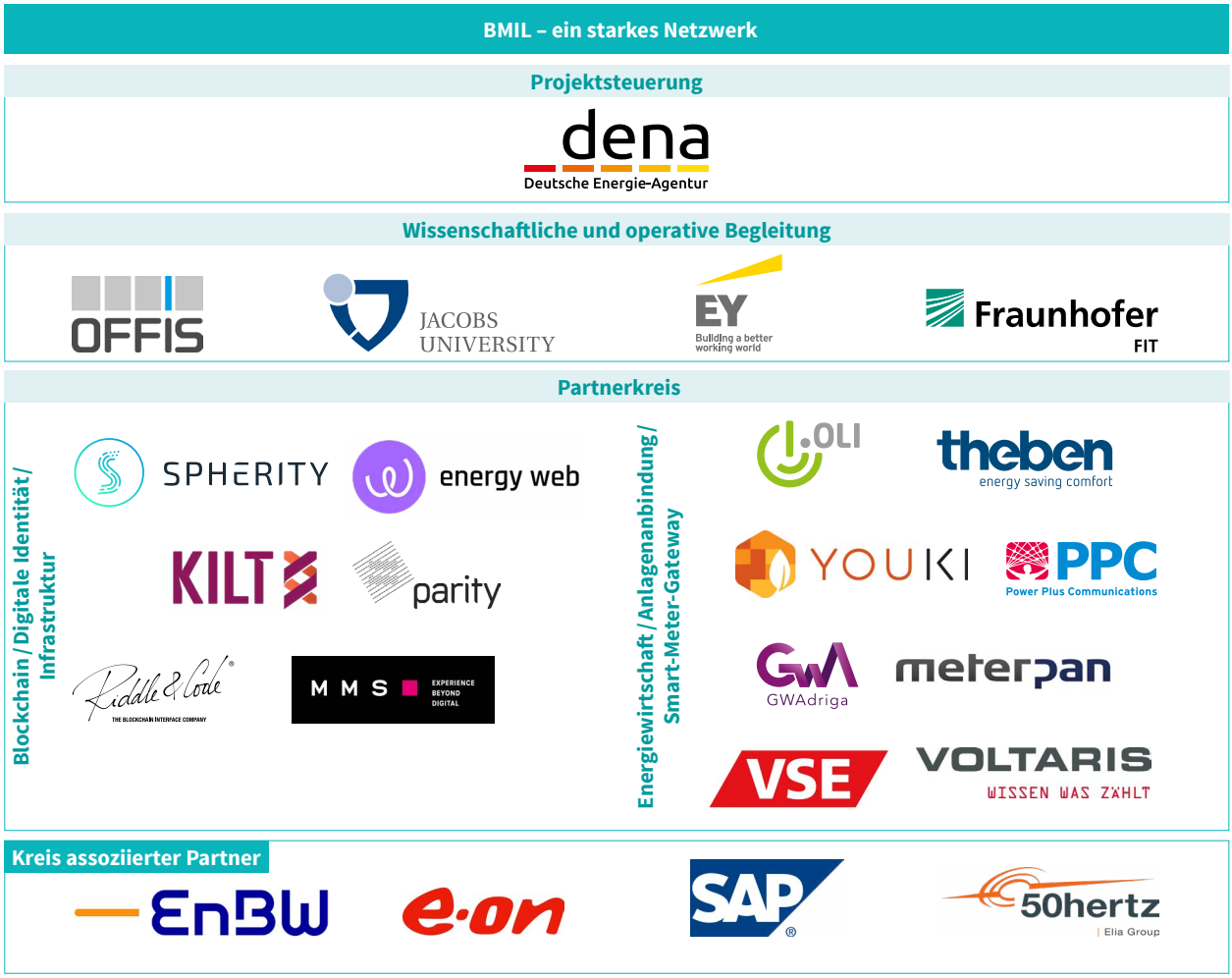


Abbildung 1: Übersicht über die beteiligten Projektpartner

2.2.2 Die Projektziele

Die zugrunde liegende Vision des Projekts ist die automatisierte An- und Abmeldung von Anlagen im Energiesystem sowie die unkomplizierte Teilhabe an wechselnden Märkten. Erreicht werden sollte dies mittels der Verknüpfung der SMGW-Infrastruktur mit digitalen Identitäten und einem Blockchain-basierten Anlagenregister, wie in der folgenden Abbildung dargestellt.

Im Zentrum des Pilotierungsvorhabens befindet sich ein dezentrales, Blockchain-basiertes Identitätsregister, mit dem sich Energieanlagen über die sichere SMGW-Infrastruktur bzw. Smart-Home-Geräte verknüpfen lassen und dort ihre Identität vermerken – für alle Akteure nutzbar, nachvollziehbar und manipulationssicher.

Dieses Register wird von den Anlagen anschließend als gemeinsame Basis genutzt, um sich in der Kommunikation mit systemrelevanten Diensten und verschiedensten marktlichen Anwendungen automatisiert auszuweisen. Über die Verknüpfung digitaler Identitäten mit dem Prinzip einer lokalen Datenspeicherung sowie kryptografischer Verfahren folgt das Vorhaben zudem dem Ansatz, nur diejenigen Daten weiterzugegeben, die tatsächlich für die jeweilige Anwendung bzw. den jeweiligen Systemdienst benötigt werden („Selective Disclosure“).

Diese Grundausrichtung markierte den Start des Projekts Blockchain Machine Identity Ledger (BMIL).

Im Rahmen der Pilotierung führte dieses Zielbild konkret zu folgenden Aufgaben mit dem Fokus, den Beweis für die technische Machbarkeit in folgenden drei Teilbereichen zu demonstrieren:

1 **Erstellen einer Geräte-Identität (Machine Identity)**
Für den Geräte-Identitäten-Aspekt (Machine Identity) wurde das Ziel gesetzt, eine digitale, selbstsouveräne und dezentrale Geräte-Identität zu erschaffen.

2 **Übertragung und Sicherheitsanker (SMGW)**
Für die Übertragung bzw. Kommunikation der Identität und ihrer Merkmale wurde das Ziel gesetzt, die im Regelbetrieb befindliche Smart-Meter-Gateway-Infrastruktur als zusätzlichen Sicherheitsanker einzusetzen.

3 **Eintragung in das Register (Ledger)**
Drittes Ziel war, ein dezentrales digitales Register (Ledger) Blockchain-basiert aufzubauen und dabei zwei unterschiedliche Blockchains zu erproben.

Zudem sollten einige Showcase-Anwendungsbeispiele der Projektpartner im Bereich Herkunftsnachweise, Flexibilitätsmärkte, smarte CO_2-Zertifikate und Energy Communities den potenziellen Mehrwert digitaler Identitäten anschließend hervorheben.

Der Kreis der Unternehmen, die an der BMIL-Pilotierung beteiligt waren, wurde auch unter dem Aspekt aufgebaut, die heterogenen

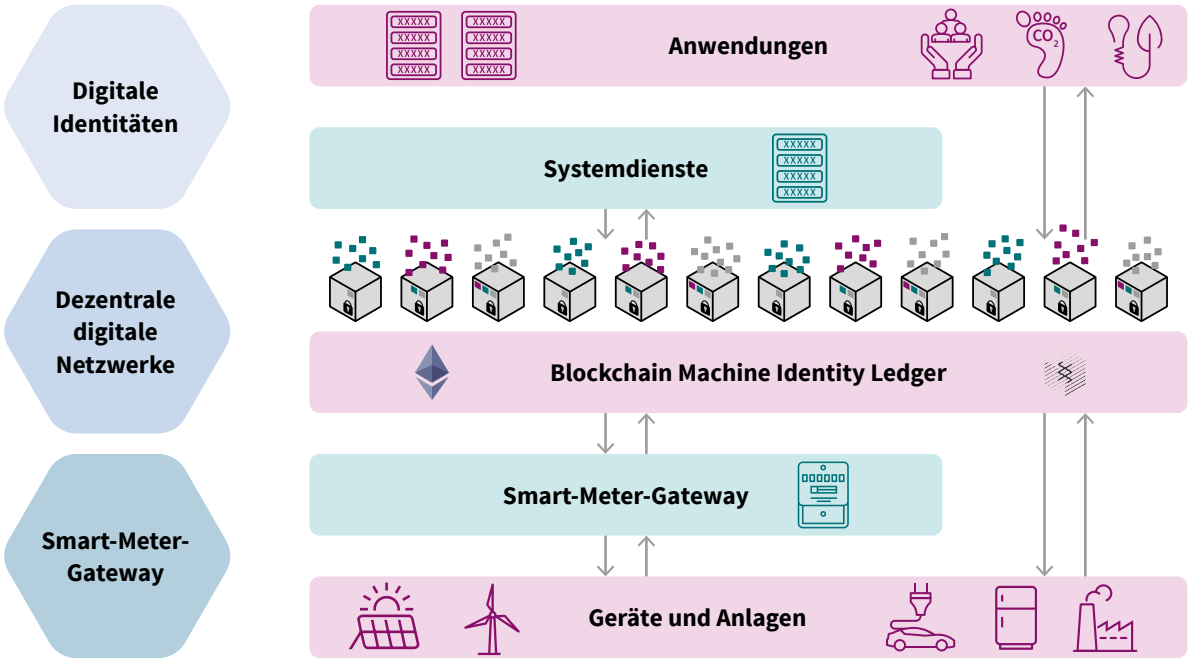


Abbildung 2: BMIL-Infrastruktur für das Energiesystem der Zukunft

technologischen Entwicklungen im Bereich dezentraler Netzwerktechnologien (Blockchain-Technologie) hinreichend abzubilden. Gerade die hochdynamischen Entwicklungen der Blockchain- und Identitäts-Ökosysteme hat es erfordert, mehrere verschiedene Technologieanbieter mit unterschiedlichen Ansätzen in das Vorhaben zu integrieren.

Ziel der BMIL-Pilotierung war auch, einen Ausblick auf eine mögliche Serienimplementierung im heterogenen Energie- und Blockchain-Ökosystem zu geben, weshalb zwei verschiedene Blockchain-Umgebungen pilotiert wurden: Ein Register basiert auf dem Technologie-Umfeld der Ethereum-Blockchain, während das andere Register auf der Entwicklungsumgebung Substrate aus dem Polkadot-Ökosystem aufgebaut wurde. Um gleichzeitig jedoch nicht den Rahmen des Projekts, zum Beispiel durch den Bau von Brücken (Bridges) zwischen den beiden Blockchain-Protokollen, zu sprengen, stand zu Beginn auch die Einigung auf einen Identitätsstandard im Fokus, den alle verwendeten Protokolle bzw. Anlagenanbindungsvarianten produktiv nutzen konnten.

2.2.3 Das Synergiepotenzial von digitalen Identitäten und der Blockchain-Technologie

Nachfolgend wird der Aufbau von digitalen Identitäten im Detail beschrieben und wie dieser im Projekt vorteilhaft im Zusammenspiel mit der Blockchain-Technologie genutzt wurde. Abbildung 3 zeigt exemplarisch, wie eine digitale Identität im Allgemeinen, für Personen oder für Maschinen aufgebaut ist.

Wie die Grafik veranschaulicht, setzen sich digitale Identitäten aus zwei Bestandteilen zusammen: einer „ID-Nummer“, dem sogenannten Identifier, sowie bestimmten, diesem Identifier zugeordneten Merkmalen bzw. Attributen.

Im Kontext einer Person ist der Identifier zum Beispiel die Nummer auf dem Personalausweis (eindeutig und unveränderbar), während die Attribute weitere Informationen zur Biografie und Identität der Person enthalten, wie unterschiedliche Abschlüsse und Zertifikate, Interessen, physische Merkmale etc.

Im Kontext einer (Energie-)Anlage wäre der Identifier lediglich eine Nummer, während die Attribute der Anlage sich beispielsweise aus ihrem Standort, dem Namen ihres Eigentümers, ihrer Nennleistung und ihrem Netzanschlusspunkt zusammensetzen. In erster Linie handelt es sich dabei um Stammdaten, die in der Regel statisch, das heißt über die Zeit unveränderlich sind. Zusätzlich sind jedoch auch Merkmale denkbar, die dynamisch sind, das heißt, die sich über den Zeitverlauf verändern, wie beispielsweise die Erzeugungsleistung oder der Verbrauch zu einer bestimmten Zeit.

Aus der Aufteilung der digitalen Identität in die Bestandteile Identifier und Attribute ergibt sich ein unmittelbarer Vorteil: Beide Komponenten lassen sich getrennt voneinander ablegen, anders als beispielsweise bei einem Personalausweis, der die Ausweisnummer und die Attribute in einem Dokument untrennbar vereint.

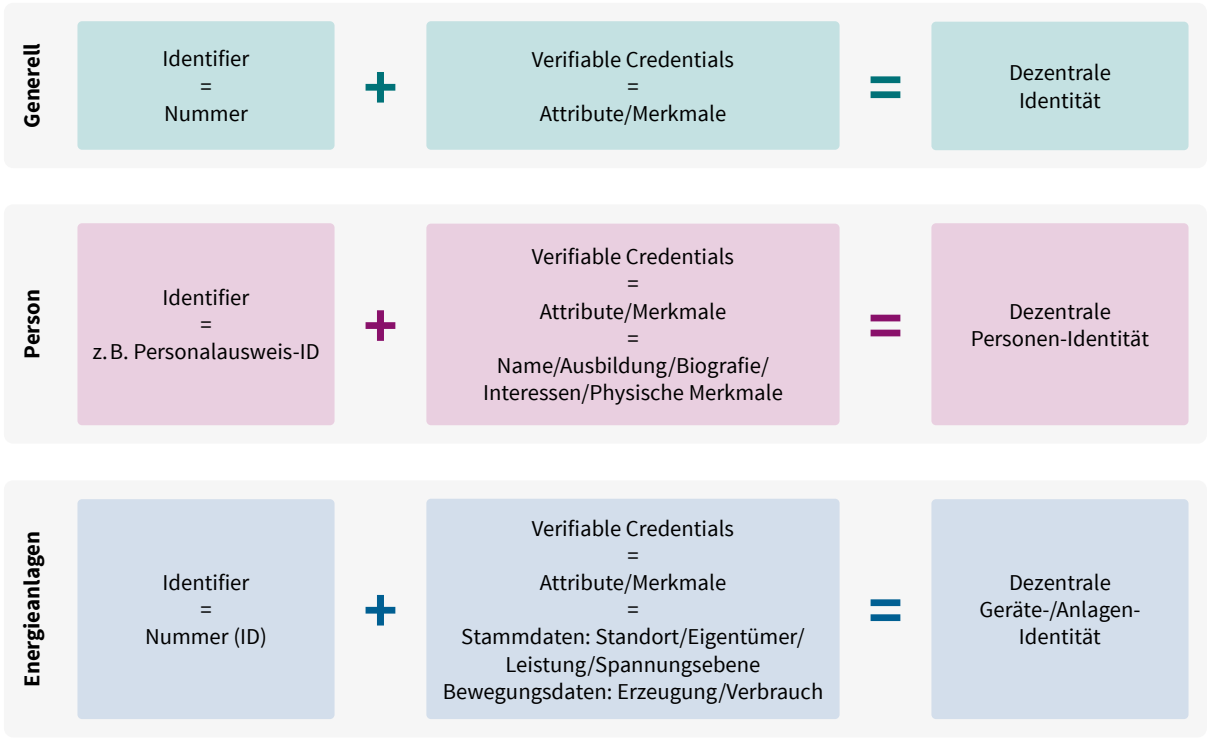


Abbildung 3: Grundlagen zu digitalen Identitäten

Abbildung 4 zeigt exemplarisch das Spannungsfeld auf, in dem sich die Digitalisierung branchenübergreifend befindet, und wie die Trennung des Identifier von den Attributen und die dezentrale Ablage von Merkmalen dazu beitragen können, das Dilemma zu lösen. Indem der Identifier bei Bedarf unabhängig von den Attributen auf einem für alle einsehbaren Register gespeichert werden kann, kann dem Erfordernis nachgekommen werden, zu jeder Zeit sichtbar zu machen, dass eine Anlage im System angemeldet ist. Damit profitiert das Projekt von den besten Eigenschaften der Blockchain-Technologie, indem die Identifier der Anlagen auf eine dezentrale, für alle Akteure transparente sowie manipulationssichere Art und Weise verwahrt werden. Auf der anderen Seite ermöglicht die Trennung grundsätzlich eine dezentrale Datenhaltung, sodass die Prinzipien von Datenschutz und Datensparsamkeit unterstützt werden. Auch fördert eine dezentrale Datenhaltung die Idee der Datensouveränität und ermöglicht grundsätzlich eine Datenökonomie, da eine selektive Datenweitergabe möglich wird. Insbesondere ist hervorzuheben, dass bei Verwendung einer Blockchain zwar die Möglichkeit besteht, Identifier auf der Blockchain zu hinterlegen, dies aber keinesfalls zwangsläufig notwendig ist. Wenn Sichtbarkeit und Verfügbarkeit im Vordergrund stehen, kann also der Identifier (ggf. sogar gemeinsam mit Attributen) auf einer hochverfügbaren Blockchain abgelegt werden; falls sehr hohe Datenschutzanforderungen bestehen, kann man auch ganz davon absehen, Identifier oder Attribute auf der Blockchain zu speichern, und nur etwa die Identität des Ausstellers von Verifiable Claims auf der Blockchain verankern.

2.2.4 Die drei Varianten der Anlagenanbindung

Auch hinsichtlich der Ablage der Attribute bestehen grundsätzlich verschiedene Optionen, wie Abbildung 5 verdeutlicht. Das Projekt hatte den Anspruch, drei verschiedene Ablageorte zu untersuchen. Dies hatte seinen Grund darin, dass heute nicht eindeutig absehbar ist, welche Variante sich in welchen Anwendungsfällen letztlich durchsetzt oder wo möglicherweise sogar verschiedene Optionen parallel bestehen bleiben.

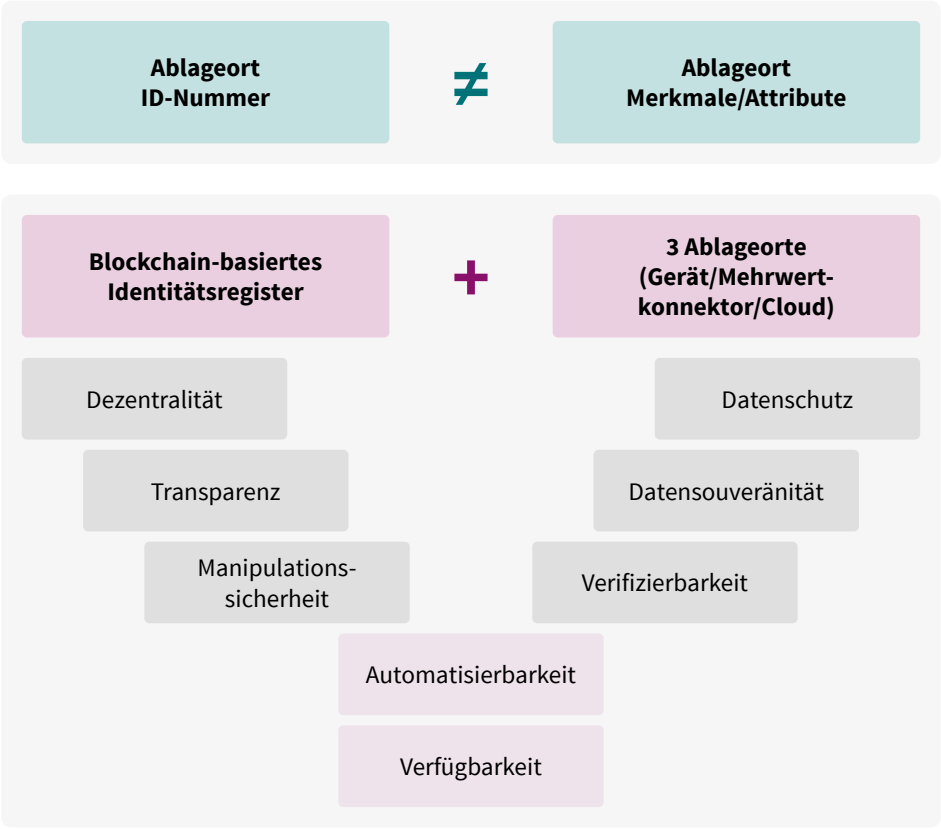


Abbildung 4: Das Synergiepotenzial von digitalen Identitäten und der Blockchain-Technologie

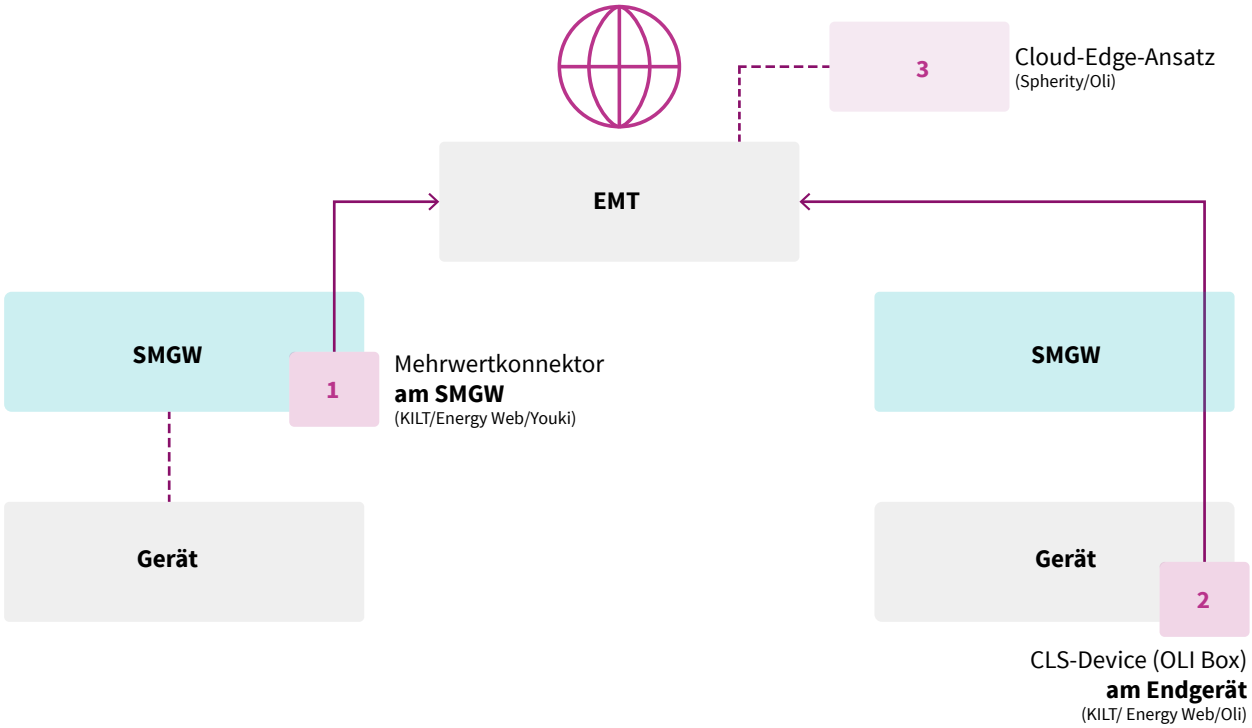


Abbildung 5: Die drei Anbindungsvarianten im BMIL

Folgenden drei Varianten wurden untersucht:

1. **Variante: am SMGW**
   In dieser Variante werden die Merkmale der Identität direkt am Smart-Meter-Gateway auf einem adaptierten Mehrwertmodul der Firma YOUKI abgelegt.

   Diese Variante wurde im Pilotvorhaben von den Unternehmen Theben (Smart Meter), YOUKI (Mehrwertmodul am SMGW), KILT (Blockchain-basiertes Identitätsprotokoll) und meterpan (MSB) umgesetzt.

2. **Variante: am Gerät**
   In dieser Variante werden die Merkmale der Identität direkt an der Anlage auf einem dedizierten CLS-Device (Controllable Local System) abgelegt.

   Diese Variante wurde im Pilotvorhaben von den Unternehmen PPC (Smart Meter), OLI Systems (CLS-Device), KILT (Blockchain-basiertes Identitätsprotokoll) und GWAdriga (Gateway-Administrator) umgesetzt.

3. **Variante: am digitalen Zwilling in der Cloud**
   In dieser Variante werden die Merkmale der Identität in einer Cloud abgelegt.

   Diese Variante wurde im Pilotvorhaben von den Unternehmen Spherity (Cloud-Edge-Prinzip), PPC (Smart Meter), OLI Systems (CLS-Device), GWAdriga (Gateway-Administrator), VSE (Energieversorgung) und Voltaris (Messstellenbetrieb) umgesetzt.

Detaillierte technische Informationen zu allen drei Varianten sowie ihre detaillierte technische, ökonomische und regulatorische Analyse finden sich in diesem Bericht ab Kapitel 4.

2.3 Zusammenfassung und Handlungsempfehlungen

Da es sich beim BMIL-Projekt um eine Pilotierung, also eine tatsächliche Umsetzung handelt, war der Nachweis der technischen Machbarkeit ein zentrales Anliegen. Die Realisierbarkeit wurde erfolgreich für alle drei genannten Meilensteine der Umsetzung (Erstellen einer Geräte-Identität, Übertragung und Sicherheitsanker (SMGW), Eintragung in das Register) erfolgreich gezeigt. Damit wird ein wichtiger Schritt in Richtung der formulierten Vision gegangen und ein Grundbaustein für das automatisierte Energiesystem beigetragen, an den zukünftig mit konkreten Anwendungsfällen angedockt werden kann.

Mit dem BMIL-Pilotprojekt wurden wesentliche **Rahmenvoraussetzungen und Standards für die Nutzung digitaler Identitäten im Energiesystem** entwickelt und erprobt. Im Detail konnte …

- … eine **Verständigung auf Identitätsstandards** im Partnerkreis abgeschlossen werden.
- … eine **digitale, selbstsouveräne und dezentrale Geräte-Identität** aufgesetzt werden.
- … eine **Verankerung der Identität auf den Geräten** (Varianten 1 und 2) bzw.
- … eine **Verankerung eines digitalen Zwillings in der Cloud** (Variante 3) realisiert werden.
- … eine **Übertragung der digitalen Identität** per SMGW-Infrastruktur im Regelbetrieb erfolgreich umgesetzt werden.
- … eine **Verknüpfung mit zwei Blockchain-basierten Identitätsregistern** (Ethereum und Substrate) aufgebaut werden.

Aus der wissenschaftlichen Evaluierung des Pilotvorhabens werden nachfolgend technische, ökonomische und regulatorische Kernaussagen sowie jeweilige Handlungsempfehlungen kurz zusammengefasst, die insbesondere die Themenstränge SMGW-Infrastruktur, digitale Identitäten (SSI) und Interoperabilität betreffen.

Im bisherigen Untersuchungsrahmen wurden keine grundsätzlichen Hürden identifiziert, die einer Serienimplementierung der BMIL-Infrastruktur entgegenstehen, dennoch sind noch weitere Fragen offen. In nachfolgenden Analysen sollte eine weitere Evaluierung des Speicherorts der Identifier und der Gerätestammdaten sowie der Gerätekontrolle bezüglich Sicherheit, Effizienz und Zugangsoffenheit erfolgen.

2.3.1 Technische Bewertung

- Die auf digitalen Identitäten (SSI) basierende Geräteregistrierung und das selbstbestimmte Identitätssystem können innerhalb der Smart-Meter-PKI im Regelbetrieb und unter Einsatz von am Markt verfügbaren intelligenten Messsystemen umgesetzt werden. Eine Vielzahl technischer Fragestellungen bleibt zum jetzigen Zeitpunkt aber noch unbeantwortet. Insbesondere lässt sich aus technischer Sicht nicht eindeutig beurteilen, welchem Ansatz der Vorzug gegeben werden sollte für die Integration der Identitätsbildung sowie darüber hinaus der Geschäftslogik von Mehrwertanwendungen, da das Spektrum der Mehrwertanwendungen ganz unterschiedliche Anforderungen an die Ausführungsplattform mitbringt.
- Die Skalierbarkeit des gewählten Identitäts-Verzeichnisses auf Blockchain-Basis ist im Hinblick auf eine spätere Serienimplementierung grundsätzlich gegeben. Zudem ist die Koexistenz von unterschiedlichen Geräteregistern möglich und demnach keine Festlegung auf eine bestimmte Blockchain-Technologie notwendig (Stichwörter: Interoperabilität, Bridges), wenngleich zukünftig weitere Standardisierungsbemühungen erforderlich sein werden.

- Technische Grenzen in Bezug auf verfügbare Kommunikationskanäle, Rechenleistung von Edge-Devices, Bandbreiten und Latenzzeiten stellen für die digitale Identitäten-basierte Geräteregistrierung und das selbstbestimmte Identitätssystem keine Einschränkung dar, werden für darauf aufbauende Anwendungsfälle aber in den Fokus rücken und müssen detaillierter betrachtet werden. Eine Auskunftspflicht des Messstellenbetreibers (MSB) über die Anbindbarkeit jeder Messlokation (inklusive Verfügbarkeit des CLS-Kanals) würde Sicherheit und Transparenz darüber schaffen, welche Anwendungsfälle jeweils technisch möglich sind. Der Status einer Messlokation umfasst dabei sowohl die Auskunft, ob und welches SMGW verbaut wurde, als auch eine Qualifizierung der Erreichbarkeit (abhängig von Gerätebandbreite und Kommunikationstechnologie) in Stufen.

- Aktuell ist eine fehlende Standardisierung nicht funktionaler Eigenschaften des Kommunikationsweges CLS-Kanal als technische Fragestellung herauszustellen. Bei der weiteren Standardisierung sollten zukünftig weitere Faktoren wie Mindestanforderungen an den CLS-Kanal in Bezug auf Verfügbarkeit, Übertragungsbandbreite und Latenz berücksichtigt werden.

- Der Kapselung des Endpunkts der CLS-Vertrauenskette über ein zertifiziertes Mehrwertmodul oder einen zertifizierten CLS-Proxy kommt in allen Anbindungsvarianten eine gemeinsame und besonders große Bedeutung zu, da sie den Entwicklungsaufwand für zukünftige Mehrwertanwendungen gering hält und den Herstellern und Entwicklern die Fokussierung auf die Anwendungslogik ermöglicht. Aus dem Projekt kann abgeleitet werden, dass eine Kombination aus potentem Mehrwertmodul (also der Möglichkeit selbst gehosteter Anwendungen) mit der reinen durchleitenden Proxy-Funktionalität eine wünschenswerte Umsetzung des Endpunkts der CLS-Vertrauenskette darstellen würde. Diese Variante wäre technologieoffen und würde insbesondere allen beschriebenen Anbindungsvarianten des Identitätsmanagements eine entsprechende Ausführungsplattform bieten. Die Grundvoraussetzung der Offenheit des CLS-Kanals muss also erhalten bleiben. Eine Durchstandardisierung der Mehrwertanwendungen würde Innovationen bremsen.

2.3.2 Ökonomische Bewertung

- Die Transaktionskosten der Identitätsfeststellung können potenziell bei allen drei Anbindungsvarianten deutlich reduziert werden. Dabei gilt jedoch, dass die verschiedenen Anbindungsvarianten unterschiedliche Kosten und unterschiedliche Nutzen und Mehrwerte erzeugen können. Dies impliziert, dass in dieser frühen Phase der Entwicklung der verschiedenen Anbindungsvarianten die Sicherung eines effektiven Technologiewettbewerbs unter Beachtung des notwendigen Datenschutz- und Datensicherheitsniveaus hohe Priorität haben sollte, um hier keine Technologieoption zu diskriminieren. Potenzielle Hemmnisse für den Technologiewettbewerb liegen in verschiedenen wettbewerbsrelevanten Aspekten: mögliche Pfadabhängigkeiten im Zusammenhang mit dem Smart-Meter-Rollout, Markteintrittsbarrieren durch Rückwirkungen des Wettbewerbs im Messstellenmarkt auf die möglichen Anbindungsvarianten und Rückwirkungen durch verschiedene Wettbewerbsformen bei den Anwendungen, die auf den Anbindungsvarianten basieren. Um konkretere Handlungsoptionen zu entwickeln, mit denen der Technologiewettbewerb zwischen den verschiedenen Anbindungsvarianten gesichert werden kann, sollten die Hemmnisse weiter untersucht werden.

- Eine zentrale Voraussetzung, um Transaktionskosten bei der Identitätsfeststellung zu reduzieren, ist die Interoperabilität der digitalen Identitäten. Netzwerkeffekte spielen hier eine wichtige Rolle. Zur Überwindung von Pfadabhängigkeiten könnte im Energiesektor eine Standardisierung der SSI-Bestandteile notwendig sein, um so eine stärkere Marktdurchdringung des SSI-Konzepts überhaupt zu ermöglichen. Daher sollte geprüft werden, in welchen Bereichen eine Standardisierung des SSI-Konzepts im Energiesektor vorangetrieben werden kann, ohne den Technologiewettbewerb einzuschränken und um gleichzeitig mögliche Synergien mit anderen Sektoren heben zu können.

- Grundsätzlich kann ein gleichzeitiger Einbau mit SMGW die Installationskosten für die Anbindungsvarianten bzw. für den notwendigen CLS-Proxy senken. Es gilt hier aber, zwischen potenziellen Kostenersparnissen bei der Installation der Geräte und der etwaigen Einschränkung von Wettbewerb (und damit von Effizienzvorteilen) abzuwägen. Die Marktakteure können durch parallele Inbetriebnahme eines Mehrwertmoduls oder eines CLS-Proxys einen doppelten Technikerbesuch und damit höhere Kosten sowie den zeitlichen Verzug beim Ausrollen der für die Anbindungsvarianten kritischen Komponenten vermeiden.

2.3.3 Regulatorische Bewertung

- Alle Anbindungsvarianten halten die IT-sicherheitsregulatorischen Vorgaben des Messstellenbetriebsgesetzes (MsbG) und der Technischen Richtlinie TR-03109 des Bundesamtes für Sicherheit in der Informationstechnik (BSI) ein und entsprechen somit dem aktuellen rechtlichen Rahmen. Für ausgewählte Kommunikationswege fehlen jedoch regulatorische Standards. Eine Festlegung dieser Standards würde die forcierte Interoperabilität fördern, eine Serienimplementierung erleichtern und Rechtssicherheit gewährleisten (vgl. ökonomische Betrachtung).

- In allen drei Anbindungsvarianten werden sowohl nicht personenbezogene als auch personenbezogene Daten verarbeitet. Die erforderliche Rechtmäßigkeit wie auch die Zweckbindung der Daten kann im Anwendungsbereich des Datenschutzrechts und der Verarbeitung personenbezogener Daten überwiegend bejaht werden (vgl. Kapitel 4.3.4). Für eine Serienimplementierung des BMIL muss jedoch sichergestellt werden, dass der Transparenzgrundsatz über die Verarbeitung von Daten gegenüber den Betroffenen jederzeit eingehalten werden kann. Die Wahrung der Betroffenenrechte (Art. 15 bis 21 DSGVO) in allen Anbindungsvarianten muss durch entsprechende Handlungsoptionen (z. B. Vereinbarung mit den Betroffenen) zunächst sichergestellt werden.

- Eine Auseinandersetzung mit der Konkretisierung von Governance-Strukturen für digitale Identitäten im Energiesektor ist notwendig, um Klarheit zu Verantwortlichkeiten für die Beteiligten zu schaffen. Hinsichtlich der Verantwortlichkeit für die Daten zur Erstellung des Decentralized Identifier (DID) (Haftung bei einer Fehlinformation) besteht eine große Rechtsunsicherheit, wer für die Richtigkeit der Daten einzustehen hat (Anlagenbetreiber, Beteiligter im Identitätsfeststellungsprozess oder derjenige, der die Daten eingetragen hat). Da das MsbG hierzu keine Regelung trifft, ist ein Rückgriff auf zivilrechtliche und allgemeingültige Normen notwendig. Eine Prüfung des Einzelfalls ist somit unentbehrlich und birgt für die Beteiligten ein hohes Risiko, für eine etwaige Datenverletzung haftbar gemacht zu werden. Eine eindeutige Regelung, wer bei der Identitätsfestlegung bzw. bei dem Identitätsprozess für welche Daten verantwortlich ist, würde die Rechtssicherheit für die Marktakteure erhöhen und somit eine Serienimplementierung vorantreiben. Es sollte eine weitere Analyse zu einem Rechte- und Rollenkonzept für das BMIL-Identitätsmodell in der Energiewirtschaft (Rechte für Organisationen und Institutionen) durchgeführt werden und basierend darauf eine weitere datenschutzrechtliche Bewertung der neuen Identitätsstandards erfolgen.

2.3.4 Ausblick

Im BMIL-Projekt hat sich gezeigt, dass es vorteilhaft ist, die Lösungserarbeitung in technischer, wirtschaftlicher und rechtlicher Hinsicht parallel anzugehen und über die unterschiedlichen Felder hinweg frühzeitig zusammenzuarbeiten. Um eine zukünftige Verwendung der BMIL-Infrastruktur im Produktivbetrieb voranzutreiben, muss dieser Stakeholder-Prozess mit etablierten wie jungen Akteuren aus Digital- und Energiebranche auf Augenhöhe fortgesetzt werden. Es sollte mit Blick auf andere Schaufensterprojekte und Pilotvorhaben (u. a. ID-Ideal, IDunion, InDE-ED) auch projektübergreifend nach Optionen zur Zusammenarbeit und Verknüpfung der Ergebnisse gesucht werden, um perspektivisch Netzwerkeffekte zu erzielen. Auch die im Projektverlauf geführten Diskussionen mit zentralen Akteure wie der Bundesnetzagentur und dem BSI sind fortzusetzen.

Es sollte angestrebt werden, ein digitales Zielbild der integrierten Energiewirtschaft zu entwerfen und anschließend konsequent zu verfolgen. Heute sind nicht nur kommunikationsfähige Strom- und Wärmezähler und das Anlagenregister konzeptionell und digital getrennt, sondern auch das Herkunftsnachweisregister steht unverbunden zum Anlagenregister. Ein Zielbild, das die Transformation leiten kann, würde helfen. Hierfür können die Implementierung und Erprobung des Blockchain Machine Identity Ledger bereits wertvolle Gestaltungshinweise liefern.

Die weitere Digitalisierung des Energiesystems verspricht insbesondere die Prozesseffizienz deutlich zu erhöhen. Dies ist auch dringend notwendig angesichts der deutlich steigenden Koordinationsanforderungen in einem immer dezentraleren Energiesystem. Digitalisierung fungiert daher als bedeutender Treiber und Enabler bei der Dekarbonisierung der Energiewirtschaft und wir sollten diese Chance konsequent nutzen.

3. Motivation der Blockchain Machine Identity Ledger Pilotierung

Autoren: Dr. Ing. Sven Rosinger, OFFIS; Richard Hänsel, EY Law; Dr. Marius Buchmann, Jacobs University Bremen; Christian Wiethe, Matthias Babel, Fraunhofer FIT

3.1 Klimaschutz und Energiewende

Eine der größten und drängendsten globalen Herausforderungen ist heute die Erderwärmung. Bereits 1997 haben 191 Staaten im sogenannten Kyoto-Protokoll vereinbart, ihre Treibhausgasemissionen zu senken. Seitdem folgen jährlich neue internationale Klimakonferenzen und Klimaabkommen[12] mit dem Ziel, die Erwärmung der Erde auf ein Niveau von möglichst 1,5 °C, zumindest aber unter 2 °C zu begrenzen.[13] Polarisierendes Thema 2021 war hierbei das Bundes-Klimaschutzgesetz (KSG). In einer der wichtigsten Entscheidungen der letzten Jahrzehnte hat das Bundesverfassungsgericht (BVerfG) die Bundesrepublik Deutschland zum Schutz der zukünftigen Generationen verpflichtet, das Ziel der Klimaneutralität in einem Umsetzungsplan auch über das Jahr 2030 hinaus festzulegen.[14] Aus Sicht des Bundesumweltministeriums wurde hierdurch ein „Window of Opportunity" geschaffen, um neue Ziele und Maßnahmen durchzusetzen, die bis dahin politisch nicht möglich waren.[15] In diesem Zuge hat sich Deutschland mit der Novellierung des Bundes-Klimaschutzgesetzes nunmehr verpflichtet, bis 2045 Klimaneutralität zu erreichen (§ 3 Abs. 2 KSG).[16]

Im Fokus steht hierbei die Energiewende, das heißt insbesondere der Umstieg von fossilen Brennstoffen und Atomenergie auf erneuerbare Energien. Insoweit ist die Energiewirtschaft wie kein anderer Sektor durch das Bundes-Klimaschutzgesetz betroffen. Allein bis 2030 sollen die CO_2-Emissionen um knapp 40 Prozent auf maximal 108 Millionen Tonnen pro Jahr abgesenkt werden (vgl. Anlage 2 KSG). Mit dem Umstieg auf erneuerbare Energien findet jedoch nicht bloß eine Veränderung im Strommix statt, vielmehr wird hierdurch das bisherige Strommarktsystem vollständig umgebaut und neu gestaltet. Die Energiewirtschaft der Zukunft ist von einem noch dezentraleren und volatileren System geprägt, das sowohl neue Marktakteure impliziert als auch bisherige Marktrollen verändert und weiterentwickelt. Ein Bereich, in dem diese Veränderungen zu neuen Konzepten führen, ist das Energiemarktdesign. Wie in Kapitel 5 weiter ausgeführt wird, können etwa Flexibilitätsmärkte genutzt werden, um die verteilten Anlagen zur Erbringung von Netzdienstleistungen, die bisher zentral über größere Kraftwerke erbracht wurden, einzubinden.

Diese und ähnliche Entwicklungen im Energiesektor bringen zusätzlich neue Herausforderungen in den Bereichen Marktkommunikation, Lastenmanagement und Datenerfassung mit sich, die zwangsläufig eine Digitalisierung der Energiewirtschaft erfordern. Die Herausforderung besteht insbesondere darin, die vielen verteilten Teilnehmer am Energiesystem, von dezentralen Erzeugern über eine Vielzahl an Verbrauchern (Elektrofahrzeuge, Wärmepumpen, Speicher, Sektorenkopplungstechnologien etc.) bis hin zur Netzinfrastruktur, zu koordinieren. Durch diese Koordination können sowohl technische als auch ökonomische Potenziale zur Effizienzsteigerung gehoben werden, sodass die Kosten der Transformation maßgeblich durch die Koordination der Teilnehmer des Energiesystems beeinflusst werden.[17] Voraussetzung hierfür ist jedoch häufig eine Verzahnung der verschiedenen Bereiche, Marktakteure und Assets durch eine digitale Marktkommunikation, um dem dynamisch werdenden Energiemarkt Rechnung zu tragen.[18]

Den Startschuss für die Umsetzung einer digitalen Energiewirtschaft hat der Gesetzgeber bereits 2016 mit dem Gesetz zur Digitalisierung der Energiewende (GDEW) sowie dessen Umsetzung im Messstellenbetriebsgesetz (MsbG) gegeben. Kernziel des GDEW ist die Schaffung eines digitalen Grundgerüsts, auf dem sicherheitsrelevante Anwendungen in den Bereichen des Smart Metering, des Sub-Metering, des Smart Grid, der Smart Mobility, des Smart Home / Building und der Smart Services erbracht werden können. Grundlage hierfür sind der Smart-Meter-Rollout sowie die Einführung einer sternförmigen Kommunikation der unterschiedlichen Marktakteure über Smart-Meter-Gateways (SMGWs).

Der Smart-Meter-Rollout bietet dabei Potenziale für neue digitale Anwendungsmöglichkeiten, zum Beispiel bei dem Herkunftsnachweis für Strom oder der Bildung von Flexibilitätsmärkten und Energy Communities sowie dem Monitoring von CO_2-Emissionen und dem Handel entsprechender Zertifikate. In Kapitel 5 werden diese Anwendungsfälle und die Mehrwerte, die sich durch eine Kombination des SMGW mit dem hier untersuchten BMIL-Ansatz ergeben, spezifiziert. Wesentlich ist hierbei, dass der BMIL-Ansatz eine grundlegende Funktionalität bieten soll, um automatisierte dezentrale Prozesse zu ermöglichen, die wiederum eine notwendige Voraussetzung dafür sein können, das technische und ökonomische Potenzial von verschiedenen Anwendungsmöglichkeiten zu erschließen. Dabei bildet der BMIL zwar nur einen, aber einen zentralen Grundbaustein für diese Mehrwertanwendungen, wie unten weiter ausgeführt wird.

Darüber hinaus lassen sich im Rahmen der Digitalisierung der Energiewende neue Potenziale zur Kosteneinsparung heben. Die Kosten-Nutzen-Analyse zum Smart-Meter-Rollout geht davon

12 Greenpeace, Internationale Klimakonferenzen, abrufbar unter: https://www.greenpeace.de/themen/klimakrise/klimaschutz/internationaleklimakonferenzen?BannerID=0818018015001047&gclid=EAIaIQobChMItpmjl_LD8QIVkc53Ch2mnwGpEAAYASAAEgKiUvD_BwE
13 Vgl. Übereinkommen von Paris, Art. 2 Abs. 1
14 BVerfG, Beschluss vom 24.03.2021 – 1 BvR 2656/18
15 Morgenstern: EWeRK Online-Fachseminar – Das neue Klimaschutzgesetz – Auswirkungen auf die Energiewirtschaft, Vortrag: Das neue Klimaschutzgesetz im Überblick, 30. Juni 2021
16 Bisher sollte das Ziel der Klimaneutralität erst 2050 erreicht werden.
17 Vgl. 1) Ernst & Young GmbH (2013): Kosten-Nutzen-Analyse für einen flächendeckenden Einsatz intelligenter Zähler, Endbericht zur Studie im Auftrag des BMWi ; 2) dena (2014): dena-Smart-Meter-Studie: Einführung von Smart Meter in Deutschland. Analyse von Rolloutszenarien und ihrer regulatorischen Implikationen; 3) Jens Strüker et al.: Dekarbonisierung durch Digitalisierung: Thesen zur Transformation der Energiewirtschaft, https://doi.org/10.15495/EPub_UBT_00005596
18 Ernst & Young GmbH (2018): Barometer Digitalisierung der Energiewende, Berichtsjahr, Studie erstellt im Auftrag des BMWi

aus, dass jeder Haushalt durch Lastverschiebung jährlich im Mittel zwischen 2,50 und 75 Euro und maximal zwischen 4,50 und 130 Euro an Stromkosten einsparen könnte.[19] Dies stellt jedoch zunächst ein theoretisches Potenzial mit einer sehr breiten Streuung dar, bei dem der Grad der Ausschöpfung signifikant davon abhängt, welche Transaktionskosten sich im Kontext der Lastverschiebung für Nutzer und Anbieter ergeben. Digitale Lösungen können zu einer Reduktion dieser Transaktionskosten beitragen und damit den Grad der Ausschöpfung des Potenzials erhöhen. Ebenso wird davon ausgegangen, dass mit SMGWs Netzausbaukosten von bis zu 400 Euro je Messgerät eingespart werden könnten.[20]

Hierbei handelt es sich jedoch jeweils um ein theoretisches Maximum, dessen praktische Realisierung stark von der Sicherheit und Verlässlichkeit der zugrunde liegenden Daten und der Datenkommunikation abhängt. Vor diesem Hintergrund sind im Rahmen der Digitalisierung Prozesse nötig, die sowohl Identitätsinformationen über Maschinen als auch deren Bewegungsdaten weitestgehend automatisch validieren und so eine vertrauenswürdige Kommunikation ermöglichen.

3.2 Bedeutung und Notwendigkeit digitaler Identitäten unter Berücksichtigung der Blockchain-Technologie

Ein großer Teil der vertraglichen Beziehungen, die genutzt werden, um das gesellschaftliche Zusammenleben zu organisieren, setzen voraus, dass die Parteien sich gegenseitig ihre Identität bestätigen und auf die Sicherheit der zugrunde liegenden Daten vertrauen. Hierbei haben sich in der Praxis verschiedene Prozesse etabliert, um Vertrauen in die Echtheit einer Identität aufzubauen. Sie reichen von der persönlichen Identifizierung (etwa durch den Personalausweis) bis hin zu komplexen Systemen, die umfangreiche Informationen zur Identität bereitstellen, wie etwa die KYC-Prozesse (Know Your Customer) zur Identitätsverifizierung und Vertraulichkeitsprüfung der Geschäftspartner. In verschiedenen Sektoren werden aktuell Ansätze entwickelt und umgesetzt, die auf digitale Identitäten und ihre selbstbestimmte Verwaltung zur Identifizierung von Personen und zur Validierung von Daten abzielen.

Solche digitalen Identitäten könnten auch in der Energiewirtschaft die Grundlage für die weitere Digitalisierung der Marktkommunikation sowie die Vereinheitlichung der Übertragungswege und damit für eine nachvollziehbare Marktkommunikation bilden, indem beispielsweise Stamm- und Echtzeitdaten von dezentralen Erzeugungsanlagen digitalisiert und für eine automatisierte Anwendung bereitgestellt werden. Einen ersten Schritt in diese Richtung bildet das seit 2019 bestehende Marktstammdatenregister. Hier werden die Stammdaten der Marktakteure und Erzeugungsanlagen von den Betreibern digital in einem von der Bundesnetzagentur betriebenen Register erfasst und verwaltet. Die Thematik des digitalen Identitätsmanagements wird dabei aber aktuell weder durch das Marktstammdatenregister noch durch andere regulatorische Vorgaben geregelt, sodass für die Energiewirtschaft noch keine Möglichkeit geschaffen wurde, dezentrale digitale Identitäten in verschiedenen Szenarien anzuwenden und von vertrauens- und glaubwürdiger Stelle bestätigende Aussagen über sie zu treffen. Unter dieser Ausgangslage (Fehlen eines vertrauenswürdigen digitalen Identitätsmanagements) sind digitale Daten aktuell für die Realisierung neuartiger Mehrwertdienste wie der Umsetzung von Energy Communities oder der Tokenisierung von Energie und deren Zertifizierungen nur bedingt nutzbar, da es neben Vertrauensproblemen auch an Schnittstellen und automatisierten Möglichkeiten zur selektiven und barrierefreien Datennutzung für verschiedene Anwendungsfälle fehlt. Dies umfasst mehrere Herausforderungen: Zum einen ist es aktuell nur mit hohem Aufwand und zeitlichen Verzögerungen möglich, zwischen verschiedenen Marktrollen zu wechseln.[21] Mit steigender Anzahl an möglichen Anwendungsfällen, an denen verteilte Anlagen teilnehmen können, steigt aber der Bedarf, zwischen diesen Anwendungsfällen zu wechseln (potenziell auch mit einer hohen Häufigkeit). Zum anderen gilt es auch, das Vertrauen zu sichern, dass die Marktaktivitäten einzelner Anlagen auch erfüllt werden. Hier steht vor allem die Frage im Fokus, wie sichergestellt werden kann, dass eine Anlage zu einem Zeitpunkt lediglich einen Anwendungsfall bedient und das Angebot hier entsprechend verlässlich ist. Beide Herausforderungen können über verschiedene Ansätze (zentral und dezentral) adressiert werden.

Um Datensilos, die Risiken für Datenschutz, Verfügbarkeit und Marktmacht mit sich bringen, zu verhindern, gelten dezentrale Architekturen zunehmend als potenzielle Basistechnologien der Digitalisierung des Energiemarktes. Dazu gehört sowohl die Möglichkeit, rein bilateral verifizierbare Identitätsinformationen auszutauschen, etwa mithilfe von digitalen Zertifikaten, als auch in einem Peerto-Peer-Netzwerk verbindliche Transaktionen einzugehen, etwa mittels der Blockchain-Technologie. Die Blockchain-Technologie kann beispielsweise direkte Vertragsbezie-

19 Ernst & Young GmbH (2013): Kosten-Nutzen-Analyse für einen flächendeckenden Einsatz intelligenter Zähler, Endbericht zur Studie im Auftrag des BMWi
20 dena (2014): dena-Smart-Meter-Studie: Einführung von Smart Meter in Deutschland. Analyse von Rolloutszenarien und ihrer regulatorischen Implikationen
21 Strüker, J., Weibelzahl, M., Körner, M.-F., Kießling, A., Franke-Sluijk, A., Hermann, M. (2021): Dekarbonisierung durch Digitalisierung – Thesen zur Transformation der Energiewirtschaft. Hrsg.: Universität Bayreuth, Projektgruppe Wirtschaftsinformatik des Fraunhofer-Instituts für Angewandte Informationstechnik FIT und TenneT, Bayreuth, abrufbar unter: https://doi.org/10.15495/EPub_UBT_00005596

hungen zwischen Akteuren des Energiemarktes ohne Intermediär ermöglichen und hierbei für ein hohes Maß an Transparenz und Fälschungssicherheit sorgen.

Die Blockchain-Technologie ist ein sogenanntes Distributed-Ledger-System, das aus einem Peer-to-Peer-Netzwerk besteht und Nutzern die Interaktion über Transaktionen ermöglicht. Eine zentrale Verwaltungsinstanz wird dabei nicht benötigt, sondern durch Konsens-Algorithmen im Netzwerk ersetzt. Unter dem Begriff „Blockchain" wird dabei eine Aufführung aller im System durchgeführten Transaktionen verstanden, wobei eine Menge von Transaktionen wiederum in einem Block zusammengefasst wird. Immer wenn Konsens bezüglich eines vorher definierten Konsensmechanismus erreicht ist (z. B. Proof of Work, Proof of Stake etc.), wird ein neuer Block erstellt und noch nicht zugeordnete Transaktionen werden diesem Block zugeordnet. Die Blöcke bilden eine Kette, indem jeder Block einen kryptografischen Verweis auf den vorherigen Block besitzt. Der Zustand eines Blockchain-Systems wird dabei nicht zentral auf einem Server gespeichert, sondern individuell dezentral bei jedem Knoten (engl. Node, d. h. jeder Rechner, der am Blockchain-Netzwerk teilnimmt). Die Transaktionen werden zwischen den einzelnen Teilnehmern durchgeführt ohne die direkte Beteiligung von Dritten. Bereits ausgeführte und vollständige Transaktionen können nicht widerrufen werden und werden dauerhaft gespeichert.

Die technischen Vorteile eines Blockchain-Systems im Vergleich zu einem zentralisierten System sind vielseitig: Es wird maximale Transparenz der Transaktionen gewährleistet, indem jede Transaktion auf der Blockchain für alle Teilnehmer einsehbar ist. Im Gegensatz zu Blockchain-Systemen sind die Transaktionen in einem zentralisierten System ausschließlich für dessen Betreiber einsehbar. Hierdurch wirkt die Blockchain-Technologie einer Informations-Asymmetrie entgegen.[22] Die Informationsverbreitung in Blockchain-Systemen beinhaltet, dass jeder Teilnehmer die ganzen oder zumindest die aktuell wichtigsten Daten vorliegen hat (Full Node und Light Node). Diese Art der Datenverteilung sichert gegen Systemausfälle und Datenverlust ab, wodurch Robustheit gegenüber Cyberangriffen und somit auch eine höhere Verfügbarkeit gewährleistet werden können. Darüber hinaus finden kryptografische Verfahren Anwendung, die zum Beispiel gegen Distributed-Denial-o-Service-Angriffe (DDOS) schützen. Zentralisierte Systeme hingegen können deutlich einfacher von einer einzelnen Instanz manipuliert oder durch gezielte Angriffe (temporär) ausgeschaltet werden, als dies bei dezentralen Systemen der Fall ist.[23]

Vor diesem Hintergrund findet aktuell eine breite Erprobung der Blockchain-Technologie in Wirtschaft, Wissenschaft und Verwaltung statt, die sich immer wieder auch mit der Erzeugung von (selbstbestimmten) digitalen Identitäten beschäftigt. Hierbei lassen sich drei primäre Treiber für die Anwendung Blockchain-basierter digitaler Identitäten in den verschiedenen Sektoren identifizieren:

Erstens sollen Blockchain- und zertifikatsbasierte digitale Identitäten (häufig auf Basis einer Blockchainbasierten Public Key Infrastructure (PKI), insbesondere für Institutionen, die Zertifikate ausstellen und / oder überprüfen wollen) die Fälschungssicherheit der Daten, zum Beispiel bei digitalen Personalausweisen oder Ausbildungs- und Gesundheitsnachweisen, auch international gewährleisten. So werden im Projekt IDunion im Rahmen des Innovationswettbewerbs „Schaufenster Sichere Digitale Identitäten" des BMWK (vormals: BMWi) bereits die Möglichkeiten einer digitalen Ausweisfunktion auf dem Smartphone evaluiert, weitere Schaufensterprojekte sollen folgen.[24] Die Blockchain-basierte Ausstellung von digitalen Ausbildungs- und Gesundheitsnachweisen wird international ebenfalls anmehreren Stellen erprobt und von der EU gefördert.[25]

Die Reduktion der Transaktionskosten stellt die zweite Hauptmotivation zur Umsetzung von digitalen Identitäten dar. Sie werden vor allem in Wirtschaftszweigen diskutiert, in denen identische Daten von mehreren Unternehmen parallel zum gleichen Zweck verarbeitet werden. Einsparpotenziale treiben Bemühungen zu KYC-Pflichten in unterschiedlichen Sektoren, wie zum Beispiel in der Pharma- und Automobilindustrie, an.[26] Mit der zunehmenden Dezentralisierung der Energiewirtschaft werden auch hier KYC-Aufgaben in vergleichbarem oder sogar größerem Umfang erwartet, weil neben der Vielzahl der Marktakteure auch Distributed Energy Resources (DER) und andere Assets digital identifizierbar sein müssen, um eine höhere und / oder einfachere Automatisierung neuer Anwendungsfälle zur Flexibilisierung von Energieverbrauch und -erzeugung zu ermöglichen.

Der dritte Treiber für Blockchain- und zertifikatsbasierte digitale Identitäten ist der Datenschutz. Über die digitale Identität wird ermöglicht, Dienstleistungsanbietern die Kontrolle über den Zugang zu ihren Produkten zu gewährleisten und gleichzeitig die Privatsphäre der Dienstleistungsnutzerinnen und -nutzer zu schützen. Mithilfe von digitalen Identitäten können Personen Eigenschaften bei Minimierung der Offenlegung personenbezogener Daten vorweisen und Berechtigungen, in Anspruch ge-

22 Lockl et al. (2020): Toward Trust in Internet of Things (IoT) Ecosystems: Design Principles for Blockchain-Based IoT Applications. In: IEEE Transactions on Engineering Management, Vol. 67, No. 4, p. 1256–1270
23 Guggenberger, T., Schlatt, V., Schmid, J., Urbach, N. (2021): A structured overview of attacks on blockchain systems. In: PACIS 2021 Proceedings. AIS, Dubai. URL = https://eref.uni-bayreuth.de/66899/
24 https://www.bmwi.de/Redaktion/DE/Pressemitteilungen/2021/03/20210401-startschuss-digitaler-personalausweis.html
25 Vgl. Bitkom (2020); Grech et al. (2021); COVID-19 Credentials Initiative (2021); IATA (2021)
26 Vgl. Bitkom (2020)

nommene Leistungen, durchgeführte Transaktionen und Absprachen etc. können transparent dokumentiert werden. Die personenbezogenen Daten der Nutzerinnen und Nutzer können dabei dezentral auf den Nutzergeräten gespeichert bleiben, sodass die Gefahr des Datendiebstahls oder -missbrauchs eingeschränkt wird. Die Nutzung von sogenannten Zero-Knowledge-Proofs ermöglicht es zudem den Dateneigentümern, Nachweise über Identitätsdaten zur Verfügung zu stellen, sodass keine weiteren, nicht benötigten Informationen übermittelt werden.[27] Gerade bei Blockchain-basierten Anwendungen ist die gezielte, sparsame und manchmal auch anonymisierte Übermittlung von Berechtigungen und Eigenschaften von großer Bedeutung.

Im Vergleich zu den dargestellten Beispielen kommen Blockchain- und zertifikatsbasierte digitale Identitäten im Energiesektor derzeit kaum zum Einsatz. Dies mag zum Teil daran liegen, dass es historisch bedingt üblich war, dass Service Provider über eigene Nutzer- und Datenbanken verfügen. Mit der immer stärkeren Vernetzung rückt auch die Interoperabilität immer stärker in den Vordergrund[28], weshalb sich eine dezentrale, allgemeine Lösung empfiehlt.

Trotz bestehender Unsicherheiten wird der Blockchain-Technologie in der Energiewirtschaft für die Zukunft eine große Bedeutung beigemessen.[29] Ein Großteil der heute bestehenden oder in Planung befindlichen Blockchain-Lösungen dient dabei jedoch nicht einem allgemeinen Identitätsmanagement, das sich interoperabel und in Verbindung mit dem SMGW auf verschiedene Anwendungsfälle ausweiten lässt. Vielmehr handelt es sich hier um einzelne Vorstöße auf konkreter Use-Case-Ebene, die sich vor allem mit dem Energiehandel beschäftigen. Daneben sind eine Vielzahl neuer Anwendungsfälle für die neuen Themen wie Energy Communities, Elektromobilität, Tokenisierung von Energie und Zertifizierungen im Fokus der Blockchain-Anwendungen in Vorbereitung und Pilotierung.[30] Der Erfolg dieser Entwicklungen hängt sehr stark von der Automatisierung der KYC-Prozesse und der daraus resultierenden Senkung der Transaktionskosten ab.

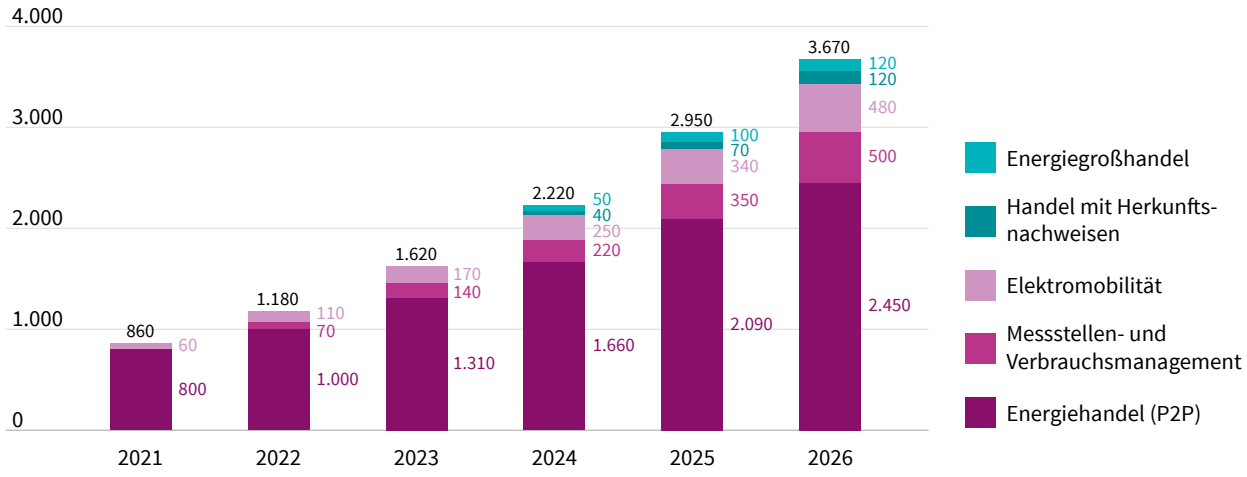


Abbildung 6: Erwartete Entwicklung des globalen Investitionsvolumens von Blockchain-Projekten in der Energiewirtschaft, 2021 bis 2026, in Millionen US-Dollar

27 Wang & De Fillipi (2020)
28 Bogensperger, A., Zeiselmair, A., Hinterstocker, M., Dossow, P., Hilpert, J., Wimmer, M., ... & Völter, F. (2021): Welche Zukunft hat die Blockchain-Technologie in der Energiewirtschaft? (No. 68), Bayreuther Arbeitspapiere zur Wirtschaftsinformatik
29 dena (2018): Multi-Stakeholder Studie – Blockchain in der integrierten Energiewende
30 PwC/BDEW (2019): Blockchain Radar

Die Potenziale der Blockchain-Technologie werden nicht nur von den Marktakteuren, sondern auch von der Bundesregierung erkannt. Mit der Herausgabe ihrer Blockchain-Strategie hat es sich die Bundesregierung zur Aufgabe gemacht, eine praxisorientierte Forschung, Entwicklung und Demonstration in der Energiewirtschaft zu fördern. Demnach gebe es auch aus Sicht der Bundesregierung verschiedene Anwendungsfälle für die Blockchain-Technologie, bei denen sie einen Mehrwert schaffen kann. Dies reiche von der Preisgestaltung über den Anbieterwechsel bis hin zur Ausgestaltung von Prosumer-Rollen. Neben den möglichen Potenzialen sieht die Bundesregierung die Umweltauswirkungen der Blockchain-Technologie aber durchaus als relevanten Faktor. So muss besonders im Rahmen von energiewirtschaftlichen Anwendungen die Gesamteffizienz in den Blick genommen werden. Manche Formen der Blockchain-Technologie gehen mit einem erheblichen Strombedarf einher, der die Gefahr birgt, etwaige positive Effekte bei den Themen Transparenz, Datensicherheit und Prozesseffizienz wieder durch deutliche negative Effekte beim Klima- und Ressourcenschutz aufzuheben.[31] Um diesem Problem entgegenzutreten, werden daher weitere Konsensmechanismen entwickelt oder existieren bereits (z. B. Proof of Authority, Proof of Stake), die ohne große Anforderungen an Rechenkapazität und somit ohne nennenswerte negative Effekte beim Klima- und Ressourcenschutz einhergehen.[32]

Neben den Aspekten des Klimaschutzes werden im Zusammenhang mit der Blockchain-Technologie in der Energiewirtschaft auch immer wieder regulatorische Herausforderungen offenbar. So bestehen aufgrund der Verteilung von Daten an alle Blockchain Nodes sowie der fehlenden Möglichkeit der Löschung nicht nur grundsätzliche Herausforderungen hinsichtlich des Datenschutzes oder haftungsrechtlicher Fragen, sondern auch spezifische energiewirtschaftliche Probleme, die sich oft aus der Regulatorik energiewirtschaftlicher Prozesse sowie der Marktkommunikation ergeben.[33, 34]

Zusammenfassend stehen sich bei dem Einsatz der Blockchain-Technologie in der Energiewirtschaft erhebliche Potenziale und Herausforderungen gegenüber, die im Einzelfall bewertet werden müssen, um den Mehrwert der Technologie herauszuarbeiten.[35, 36] Das vorliegende Pilotprojekt konzentriert sich dabei auf die Frage, welcher Mehrwert durch Blockchain- und zertifikatsbasierte digitale Identitäten im Kontext des Smart-Meter-Rollouts zusammen mit der regulatorischen Kommunikation über das SMGW generiert werden kann.

3.3 Aufbau und Grundfunktionalität der Self-Sovereign Identity

Die am häufigsten auftretenden Identitätsmodelle sind das Account-basierte und das föderierte Identitätsmodell. Im **Account-basierten Identitätsmodell** werden die Kontrolle und die Verwaltung einer Identität von zentralen Stellen übernommen, indem beispielsweise eine Nutzerin oder ein Nutzer einen neuen Account auf einer Internetseite erstellt, um bestimmte Dienste der Seite nutzen zu können. Dies ist das Standardverfahren für den Umgang mit Identitäten im Internet, das allerdings mit bedenklichen Sicherheitsrisiken verbunden ist. So ist ein häufiges Nutzerverhalten, dass für mehrere Identitäten und Accounts dasselbe Passwort verwendet wird.

Dies geschieht vorrangig aufgrund mangelnder Interoperabilität einer Identität: Sie kann häufig nicht für andere Login-Verfahren und Service-Anbieter wiederverwendet werden, sodass die Nutzerinnen und Nutzer mehrere Identitäten und Accounts anlegen müssen. Eine derartige redundante Datenhaltung führt dazu, dass der Verwaltungsaufwand der Identitäten für die Nutzerinnen und Nutzer immer größer wird, je mehr Dienstleistungen in Anspruch genommen werden. Zudem ist zu bemängeln, dass die Kontrolle über die Daten und die Identität in diesem Modell an Dritte abgegeben wird und ein transparenter Umgang mit den Daten nicht gewährleistet ist.

Um Schwachstellen des zentralisierten Identitätsmodells zu beheben, wurde die **föderierte Identität** entwickelt. Hierbei wird ein Identitäts-Dienstleister (engl.: Identity Provider, IDP) eingeführt, bei dem eine Nutzerin oder ein Nutzer eine Identität anlegen kann. Über die bei dem IDP erstellte Identität kann die Nutzerin oder der Nutzer sich dann auf anderen Internetseiten, bei Service-Anbietern und bei Apps anmelden (bekannt als Single Sign-on, SSO). Zum Beispiel werden Protokolle wie OpenID Connect oder OAuth, die hinter den Login-Buttons sozialer Netzwerke (Facebook, Instagram, Twitter, Google etc.) stehen, zur Umsetzung verwendet. Die föderierte Identität adressiert das Problem der redundanten Datenhaltung mehrerer gleicher Identitäten und die Nutzerinnen und Nutzer erhalten mehr Kontrolle über ihre Identität, indem sie bestimmen können, wo diese verwendet wird. Jedoch werden immer noch sensible Daten zentral gespeichert und die Nutzerinnen und Nutzer sind ebenso nicht vor dem Missbrauch ihrer Daten geschützt. Ein zusätzlicher Nachteil ist zudem die noch weiter gesteigerte Datenaggregation.

31 Blockchain-Strategie der Bundesregierung, S. 8, https://www.bmwi.de/Redaktion/DE/Publikationen/Digitale-Welt/blockchain-strategie.pdf?__blob=publicationFile&v=8
32 Sedlmeir, J., Buhl, H.U., Fridgen, G., Keller, R. (2020): The energy consumption of blockchain technology: beyond myth. In: Business & Information Systems Engineering, 62(6), pp. 599–608
33 Vgl. EY: Blockchain-basierte Erfassung und Steuerung von Energieanlagen mithilfe des Smart-Meter-Gateways: Machbarkeitsstudie und Pilotkonzept, Studie im Auftrag des BMWI, Stand: 18.12.2019, S. 31 ff.; dena: Multi-Stakeholder-Studie – Blockchain in der integrierten Energiewende, Stand 02/2019, S. 156 ff.
34 Schellinger, B., Völter, F., Urbach, N., Sedlmeir, J. (2022): Yes, I Do: Marrying Blockchain Applications with GDPR. 55th Hawaii International Conference on System Sciences
35 dena (2018): Multi-Stakeholder Studie – Blockchain in der integrierten Energiewende
36 Strüker, J., Utz, M., Sedlmeir, J.: Einsatz der Blockchain-Technologie für Smart Grid Dienstleistungen durch E-PKW im Reallabor „EnStadt:Pfaff“

Self-Sovereign Identity (SSI)

Die Self-Sovereign Identity (SSI) ist ein relativ neues Paradigma im Bereich der digitalen Identitätsmanagementsysteme mit aktuell großem Momentum in Wissenschaft und Praxis. Die SSI behebt die Herausforderungen und Probleme der bestehenden Identitätsmodelle, die vor allem Sicherheit, Portabilität digitaler Identitäten und individuelle Kontrolle nicht angemessen adressieren können.[37,38] In einem SSI-System werden digitale Zertifikate verwendet, um Identitätsattribute anzugeben. Die Zertifikate (auch Credentials genannt) werden durch Dritte ausgestellt oder durch Selbstattestierung erstellt. Eine weit verbreitete und im Folgenden durchgehend betrachtete Ausgestaltung der attestierten Zertifikate wird als **Verifiable Credentials (VCs)** bezeichnet und durch einen entsprechenden Standard[39] definiert. VCs ermöglichen es, Identitätsinformationen auf sichere und verifizierbare Weise zwischen den unterschiedlichen Rollen in einer SSI-Lösung auszutauschen und bilden das zentrale Datenmodell für die Identitätsverwaltung. Eine sichere Kommunikation zwischen den Rollen (Issuer, Holder, Verifier) wird durch den Standard **Decentralized Identifier (DID)**[40] gewährleistet, der eine Ende-zu-Ende-Verschlüsselung zwischen Digital Agents als technischen Endpoints ermöglicht.

Identität

Identität ist die Summe von Merkmalen, Attributen und Eigenschaften, die eine Entität oder ein Objekt beschreiben und es als Individuum von anderen unterscheiden. Diesem Ansatz folgend wird die Identität eines Geräts auf zwei Bestandteile heruntergebrochen:

- **Identifier,** der das Gerät eindeutig identifiziert. Identifiers werden über Decentralized Identifiers (DIDs) abgebildet. DIDs ermöglichen dezentrale und digitale Identitäten, die im Gegensatz zu den bekannten föderierten Identitätsansätzen von zentralen Identitätsanbietern und Registern entkoppelt sind.[41] DIDs zeigen ähnlich wie eine URL auf ein sogenanntes DID-Dokument, das beschreibt, wie mit dem entsprechenden DID-Subjekt interagiert werden kann.

- **Eigenschaften** bzw. Attribute des Geräts, wie zum Beispiel Rechte, Rollen und Fähigkeiten, die dynamisch sind und sich über den Lifecycle des Geräts ändern können. Eigenschaften werden über Verifiable Credentials implementiert. Verifiable Credentials sind das digitale Äquivalent von physikalischen Ausweisen und Zertifikaten. Sie sind kryptografisch gesichert und können digital verifiziert werden.[42]

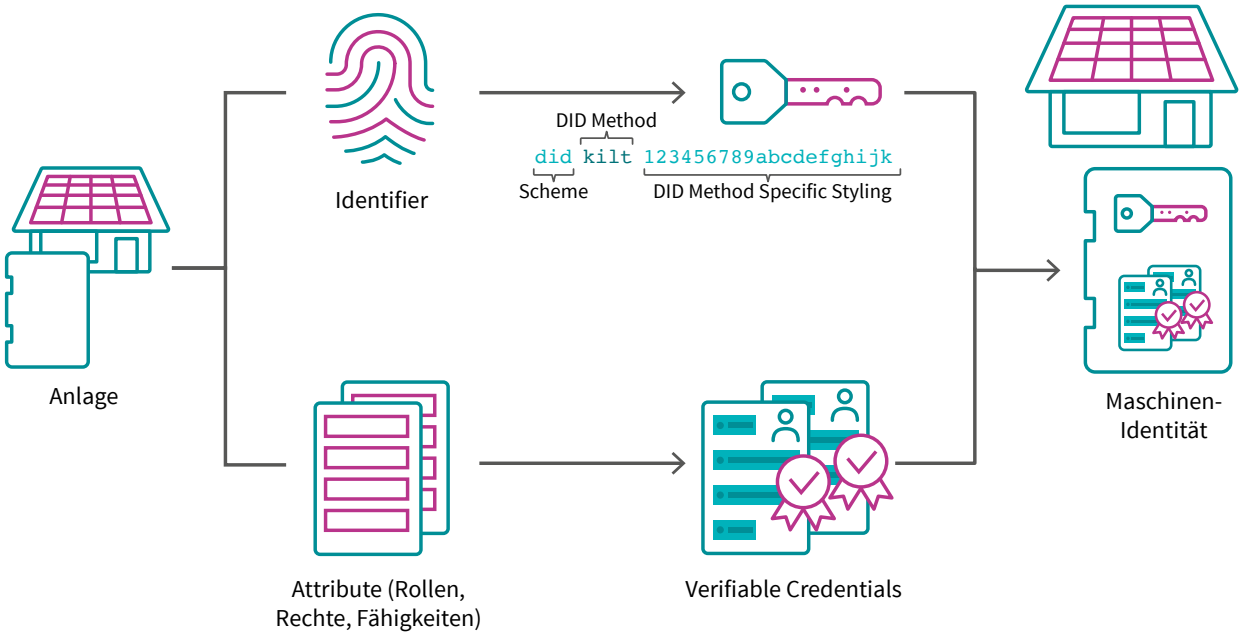


Abbildung 7: Identität (Quelle: Eigene Darstellung BOTLabs GmbH)

37 Christopher Allen (2016): The Path to Self-Sovereign Identity, http://www.lifewit-halacrity.com/2016/04/the-path-to-selfsovereign-identity.html
38 Smethurst, R., Rieger, A., Fridgen, G. (2021): Digital Identities and Verifiable Credentials. In: Business & Information Systems Engineering
39 https://www.w3.org/TR/vc-data-model/
40 https://www.w3.org/TR/did-core/
41 https://www.w3.org/TR/did-core/
42 https://www.w3.org/TR/vc-data-model/

Bei VCs und DIDs handelt es sich um Standards, die durch das World Wide Web Consortium (W3C) standardisiert werden und deren Adaption in Projekten, unter anderem GAIA-X, in der europäischen Cloud Infrastructure[43] und im Rahmen der Decentralized Identity Foundation (DIF)[44] mit Unternehmen wie zum Beispiel Microsoft vorangetrieben wird.

Verifiable Credentials

VCs sind ein offener Standard für digitale Berechtigungs- und Eigenschaftsnachweise[45], der auf Basis asymmetrischer Kryptografie funktioniert. VCs ermöglichen das sichere, überprüfbare und manipulationsfreie Teilen der Informationen eines Subjekts, die zur eindeutigen Identifizierung und Beschreibung genutzt werden können. Zum Beispiel können dies demografische Daten einer Person oder technische Eigenschaften einer Photovoltaik-Anlage sein. VCs bestehen formal gesehen aus einem oder mehreren Claims, seinen Metadaten und einem oder mehreren Proofs.[46] Die Claims stellen dabei die Eigenschaften dar, während die Proofs zur kryptografischen Überprüfung genutzt werden können. Sie dienen dazu, die Urheberschaft zu überprüfen und Manipulationen zu erkennen. Zum anderen gewährleistet der VC-Standard laut Preukaschat u. Reed (2021)[47], dass

1. Daten nicht kopiert werden können,

2. das Stehlen der Daten besonders schwierig ist,

3. nur bestimmte Informationen eines VC mit anderen Parteien geteilt werden können (Selective Disclosure),

4. keine Kosten für die Erstellung anfallen und

5. VCs an andere delegiert werden können.

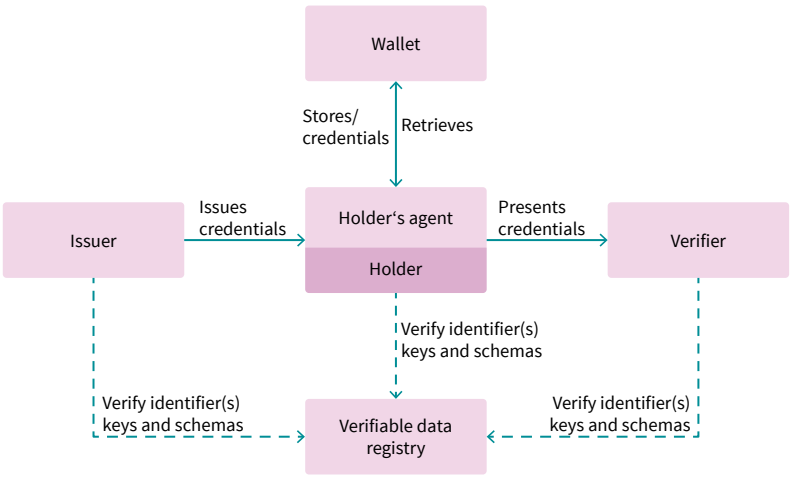


Abbildung 8: Architektur für Verifiable Credentials mit Holder im Zentrum[48]

In Abbildung 8 ist die VC-Architektur dargestellt, deren Komponenten die folgenden Aufgaben übernehmen:

- **Issuer** – Die Entität, die VCs an einen Holder ausstellt. Der Issuer ist öffentlich einsehbar und wird zur Überprüfung der VCs herangezogen.
- **Subjekt** – Die Entität, deren Eigenschaften in den VCs gespeichert sind. Ein Subjekt kann alles mit einer Identität sein: eine Person, eine Organisation, ein von Menschenhand geschaffenes Objekt, ein natürliches Ding.
- **Holder** – Die Entität, die derzeit die VCs hält und sie dem Verifier vorlegt. In den meisten Fällen handelt es sich bei dem Subjekt und dem Holder um dieselbe Entität.
- **Verifier** – Die Stelle, die die VCs vom Holder erhält. Im Gegenzug liefert der Verifier Leistungen. Beispielsweise wird ein Benutzer bei einem Online-Service angemeldet oder es werden andere Aktionen durchgeführt.
- **Wallet** – Die Entität, die die VCs für den Holder hält. In vielen Fällen ist die Digital Wallet integraler Bestandteil des Digital Agent, aber das Modell ermöglicht auch die Existenz einer Remote-Wallet, wie beispielsweise einer Cloud-Wallet.

43 https://www.data-infrastructure.eu/GAIAX/Navigation/EN/Home/home.html
44 https://identity.foundation/
45 https://www.w3.org/TR/vc-data-model/
46 Fraunhofer-Institut für angewandte Informationstechnik FIT, Projektgruppe Wirtschaftsinformatik: Whitepaper Self-Sovereign Identity – Grundlagen, Anwendungen und Potenziale portabler digitaler Identitäten
47 Preukaschat, A., Reed, D. (2021): Self-Sovereign Identity: Decentralized Digital Identity and Veridiable Credentials
48 Preukaschat, A., Reed, D. (2021): Self-Sovereign Identity: Decentralized Digital Identity and Veridiable Credentials

- **Digital Agent des Holder** – Die Software, die im Namen des Holder mit dem VC-Ökosystem interagiert. Dies kann eine App sein oder eine andere beliebige Software.

- **Verifiable Data Registry** – Ein über das Internet zugängliches Register, das alle wesentlichen Daten und Metadaten enthält, die den Betrieb des VC-Ökosystems ermöglichen. Beispiele für die Arten von Daten und Metadaten, die in dieser Registrierung gespeichert werden können, sind
  - die öffentlichen Schlüssel der Issuers
  - das Schema oder die Ontologie für alle Eigenschaften, die die VCs enthalten können
  - Widerrufslisten widerrufener VCs
  - die Themeneigenschaften, die ein Issuer unbedingt für die Erstellung der VCs benötigt

Decentralized Identifiers

Ein Decentralized Identifier (DID) ist eine neue Art von Universally Unique Identifier (UUID): eine Identifikationskennung, die eine Ressource identifiziert und spezielle Eigenschaften besitzt. Eine Ressource kann alles sein, das identifiziert werden kann, beispielsweise eine Person, eine Website oder eine Maschine. Typische Informationen, die in einem DID-Dokument hinterlegt sind, sind:

- Ein oder mehrere öffentliche Schlüssel, die verwendet werden können, um das DID-Subjekt zu authentifizieren

- Ein oder mehrere dem DID-Subjekt zugeordnete Services, die eine Interaktion erlauben. Dies kann unterschiedliche Protokolle umfassen und beispielsweise ein Service Endpoint zum Abrufen von VCs sein.

- Zusätzliche Metadaten wie Zeitstempel, digitale Signaturen und andere kryptografische Nachweise

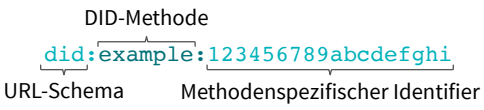


Abbildung 9: Bestandteile eines DID[49]

Ein DID ist vergleichbar mit einer URL-Adresse. Jede Adresse verlinkt eindeutig auf eine Website, allerdings können durchaus mehrere URLs auf dieselbe Website verweisen. Im Vergleich dazu wird ein DID auf Basis spezieller kryptografischer Verfahren erstellt. Dabei wird durch die deterministische Methodik bei der Erstellung sichergestellt, dass keine zwei DIDs identisch sind. Bei der Generierung kann auf unterschiedliche Verfahren zurückgegriffen werden, solange der Standard eingehalten wird. Im SMGW-Ökosystem kann es zum Beispiel sinnvoll sein, auf die bestehende PKI zurückzugreifen, indem für die Generierung die Zertifikate des SMGW genutzt werden, um gesetzeskonforme Identitäten zu unterstützen.

In Abbildung 9 ist ein Beispiel für einen DID zu sehen. Sie besteht aus drei Teilen: einem URL-Schema, dem Namen einer DID-Methode und dem methodenspezifischen Identifier. Eine DID-Methode bestimmt, wie genau ein DID erstellt wird und an welchem Ort und auf welche Weise das dazugehörige DID-Dokument gespeichert und abgerufen werden kann. Ein Beispiel für eine DID-Methode ist ethr, die auf Basis einer Transaktionsadresse einer Ethereum-Blockchain einen methodenspezifischen Identifier generiert und das zum DID zugehörige DID-Dokument auf einer Ethereum-Blockchain speichert. Dieser Prozess wird in diesem Dokument auch als Verankerung des DID bezeichnet. Über den DID kann das DID-Dokument auf der Ethereum-Blockchain abgerufen werden. Es werden zudem noch weitere Verfahren unterstützt, die nicht immer Blockchain-basiert sein müssen.[50]

Wallets

Ein Wallet ist eine Software, die es ihren Benutzerinnen und Benutzern ermöglicht, ihre kryptografischen Schlüssel, Geheimnisse und anderen sensiblen privaten Daten zu generieren, zu speichern, zu verwalten und zu schützen. Darunter fallen beispielsweise die folgenden Daten:

- Decentralized Identifiers (DIDs)

- Verifiable Credentials (VCs), deren Holder sie sind

- Digitale Kopien physischer Ausweise wie Fahrgestellnummer, Fahrerausweise, Lizenzen, Geburtsurkunden, Diplome und andere Zeugnisse, die noch nicht in VCs vorhanden sind

- Anlagenspezifische Daten aller Art, beispielsweise Herstellungsdatum und Chargen-ID

- Lebensläufe und andere biografische Informationen

- Benutzernamen, Passwörter, kryptografische Schlüssel und andere Daten, die normalerweise in einem Passwortmanager verwaltet werden

Darüber hinaus kann ein Digital Wallet auch als Adressbuch verwendet werden, um verschiedene Kontakte und Belege zu vergangenen Interaktionen zu speichern. Digitale Wallets bilden aus Anwendersicht das Kern-Paradigma von SSI-Lösungen.[51]

49 Fraunhofer-Institut für angewandte Informationstechnik FIT, Projektgruppe Wirtschaftsinformatik: Whitepaper Self-Sovereign Identity – Grundlagen, Anwendungen und Potenziale portabler digitaler Identitäten
50 https://www.w3.org/TR/did-spec-registries/
51 Barbereau, T., Weigl, L., Rieger, A., Fridgen, G. (2022): The Social Construction of Self-Sovereign Identity: An Extended Model of Interpretive Flexibility. 55th Hawaii International Conference on System Sciences

Holders Agents

Die Benutzerinnen und Benutzer einer Wallet benötigen eine Software, um die entsprechenden Aktionsmöglichkeiten verwalten und ausführen zu können. Diese Softwarekomponente wird Holders Agent oder auch Digital Agent genannt. Die Aufgaben eines Digital Agent im SSI-Kontext können nicht trennscharf definiert werden, allerdings sind typische Aktionen folgende:

- Generierung von kryptografischen Schlüsselpaaren und DIDs aus der (Digital) Wallet anfordern
- Initiierung und Verhandlung von DID-zu-DID-Verbindungen, um neue Beziehungen aufzubauen
- Ausstellung eines VC anfordern, die ausgestellten und akzeptierten VCs im Digital Wallet aufbewahren
- Aufforderung von einem Verifier, einen Proof eines oder mehrerer Claims für ein VC zu prüfen: Holder nach Zustimmung zur Freigabe des VC fragen, den Proof berechnen und ihn an den Verifier übertragen

Referenzarchitektur für ein Self-Sovereign Identity System

Die folgende Abbildung 10 ist eine mögliche Referenzarchitektur für ein SSI-System und wird zum weiteren Verständnisaufbau vorgestellt. In Kapitel 4 wird diese Abbildung dann dazu verwendet, die Lösungswege für die unterschiedlichen Anbindungsvarianten zu beschreiben und vergleichbar zu machen.

Die Referenzarchitektur besteht aus drei Schichten (Layer), die Application Layer, Self-Sovereign Layer und Verifiable Data Registry Layer genannt werden. Im Application Layer sind Anwendungsfälle beschrieben, für die die darunterliegende Schicht Identitätsdienste bereitstellt. Unter anderem sind im Application Layer beispielhaft Anwendungsfälle genannt, die in Kapitel 5.2 bis 5.5 als Mehrwertanwendungen beschrieben werden. Im SSI-Layer sind wesentliche funktionale Komponenten aufgeführt. Die PKI des GDEW fasst zum Beispiel das SMGW-Ökosystem zusammen. In der Komponente Holders Agent ist die Schnittstelle, die zur Speicherung von VCs sowie deren Prozessschritte verwendet wird, angegeben. Die Verknüpfung zwischen den beiden Komponenten ist essenziell, weil dadurch der bereits durch die SMGW-Umgebung vorhandene Vertrauensanker genutzt werden kann, um DIDs und VCs im bestehenden Ökosystem vertrauenswürdig etablieren zu können. Im Verifiable Data Registry Layer ist das öffentliche Register beschrieben, das über dezentrale Speichertechnologien umgesetzt wird. DID- und Schema-Informationen nehmen eine zentrale Rolle in dieser Schicht ein.

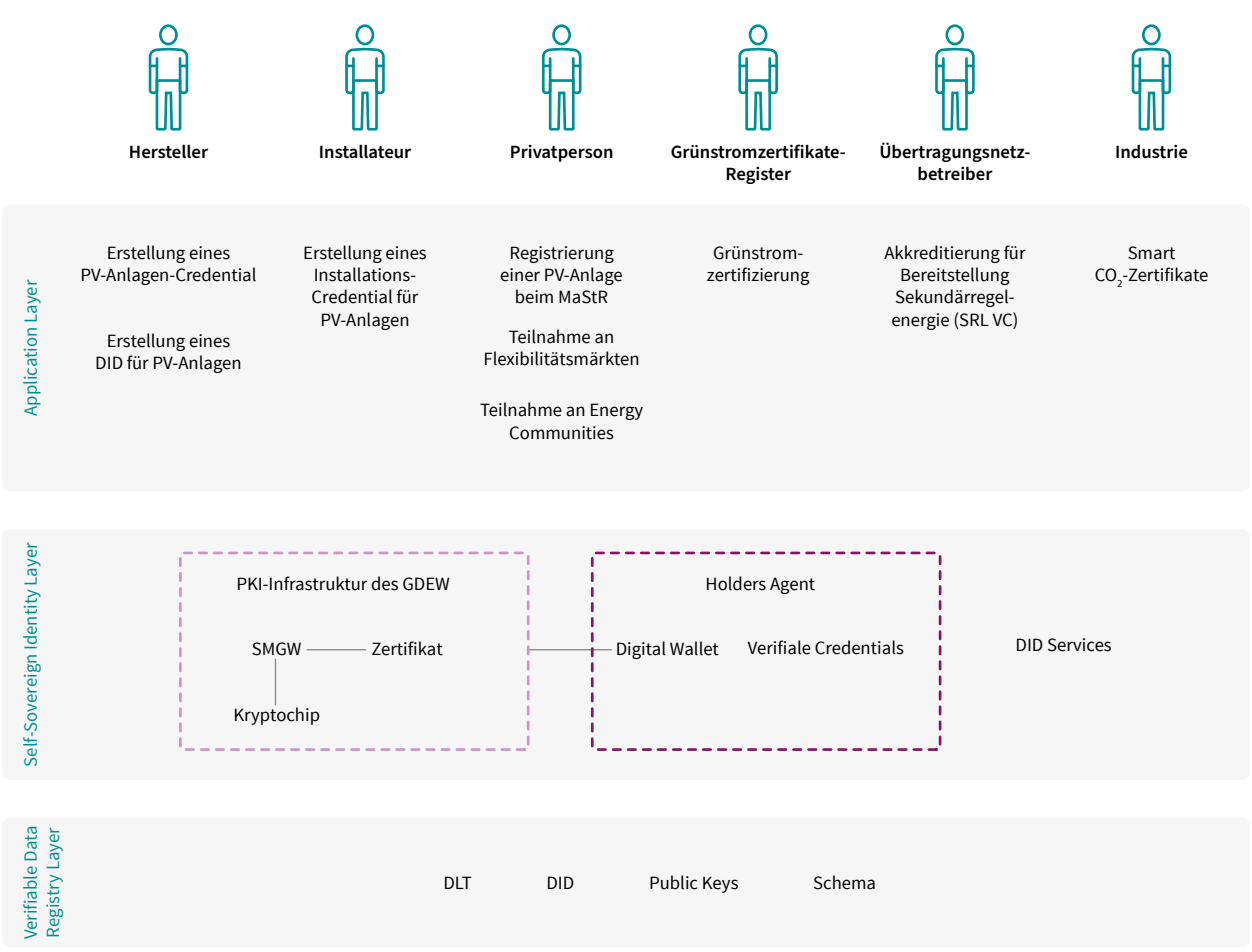


Abbildung 10: Referenzarchitektur für ein Self-Sovereign Identity System (Quelle: Eigene Darstellung OFFIS e. V.)

Beispielablauf für die Nutzung der Self-Sovereign Identity im Kontext von dezentralen Energieanlagen

Das folgende Anwendungsszenario soll am Beispiel der Identitätsbildung und Anlagenregistrierung einer Photovoltaik-Anlage (PV-Anlage) die Anwendung und Nutzung der SSI im Kontext dezentraler Energieanlagen veranschaulichen. Bei der Darstellung wurden zahlreiche Vereinfachungen vorgenommen und zudem sind Aspekte und Fragestellungen rund um die Personenidentität explizit ausgeklammert worden.

Bei der Anmeldung einer PV-Anlage müssen unterschiedliche Daten an mehrere Stellen übermittelt werden, um ein ordnungsgemäßes Betreiben der PV-Anlage nach dem Erneuerbare-Energien-Gesetz (EEG) zu ermöglichen. Die zu übermittelnden Daten umfassen eine Reihe notwendiger Anlagendaten wie Anlagentyp, Name der Anlage, Erzeugungsdaten und Anlagenstandort und können beispielsweise durch mehrere VCs beschrieben werden, die diese Informationen abbilden und ihre Richtigkeit attestieren. Zur Vereinfachung wird im Folgenden von einer Selbstattestierung dieser Informationen durch Betreiber, Hersteller und Installateur ausgegangen, in Bezug auf die Glaubwürdigkeit wäre aber auch eine Attestierung durch Dritte möglich.

Die Registrierung beim Marktstammdatenregister (MaStR) bei der Bundesnetzagentur (BNetzA) benötigt beispielsweise ein MaStR-VC, wobei sich dieses aus mehreren VCs zusammensetzen lässt. Ein MaStR-VC muss dafür die folgenden grundlegenden Informationen beinhalten:

- Personen- und Standortdaten (Betreiber-VC) werden durch den Betreiber erstellt (Issuer, Holder).
- Informationen über die Anlage (Anlagen-VC) werden durch den Hersteller erstellt (Issuer) und dem Betreiber zur Aufbewahrung übergeben (Holder).
- Inbetriebnahmedaten (Installations-VC) werden durch den Installateur erstellt (Issuer) und dem Betreiber zur Aufbewahrung übergeben (Holder).

Bei der Übermittlung der Daten müsste die BNetzA (Verifier) die Informationen überprüfen, indem sie für jedes VC über die Verifiable Data Registry herausfinden kann, ob die vorgezeigten Informationen tatsächlich durch den entsprechenden Issuer ausgestellt wurden, und dadurch die Authentizität der Daten sicherstellen (vgl. Abbildung 8). Der Hersteller, die PV-Anlage, der Betreiber und der Installateur sind dementsprechend ebenfalls auf der Verifiable Data Registry in Form eines DID hinterlegt. Im Rahmen von Mehrwertanwendungen, die auf dieser Basis des Identitätsregisters aufgebaut sind, wären dann insbesondere Transaktionspartner in der Rolle der Verifiers, da diese sicherstellen wollen, dass ihr Gegenüber tatsächlich existiert und alle genannten Eigenschaften korrekt sind.

3.4 Digitale Identitäten im Kontext des Smart-Meter-Rollouts

Der Smart-Meter-Rollout soll einen wichtigen Grundstein für den Datenaustausch im Energiesektorlegen. Das SMGW ist dabei die zentrale Kommunikationseinheit im Intelligenten Messsystem (iMSys), das durch die Vorgaben des Bundesamtes für Sicherheit in der Informationstechnik (BSI) eine sichere Datenübertragung gewährleistet. Der Betrieb des iMSys wird durch den Gateway-Administrator (GWA) verantwortet. Über das SMGW werden dabei sowohl technische als auch personelle Sicherheitsanker installiert, die ein hohes Maß an Datenschutz und Datensicherheit bei der Datenkommunikation ermöglichen. In diesem Kontext werden Blockchain-basierte digitale Identitäten jedoch nicht überflüssig, sondern ermöglichen eine Sicherstellung der Vertrauenswürdigkeit im Sinne von KYC und damit verbunden insbesondere eine Senkung der Transaktionskosten bei neuen Mehrwertdiensten.

So kommt EY(im Rahmen einer durch das BMWK (vormals BMWi) durchgeführten Vorstudie zu dem Ergebnis, dass die Verknüpfung der Blockchain-Technologie mit dem SMGW in der Lage ist, eine sichere, skalierbare und interoperable Grundlage für dezentrale Geschäftsmodelle zu schaffen. Demnach können Blockchain-basierte digitale Identitäten eine asynchrone, redundante und damit fehleranfällige Datenhaltung vermeiden und gleichzeitig die Ausfallsicherheit des Gesamtsystems erhöhen sowie die Aktualität und Richtigkeit der ausgetauschten Daten sicherstellen. Das SMGW ist dabei grundsätzlich in der Lage, als ausführende Instanz zu fungieren und einen transparenten und gesicherten Kanal zwischen den Geräten, die an das SMGW angeschlossen sind, Marktakteuren und Registern (wie dem MaStR) herzustellen und sie so in die sichere Vertrauenskette des SMGW einzubinden.[52]

Insoweit kann die digitale Identität einen Beitrag dazu leisten, das Potenzial des Smart-Meter-Rollouts stärker auszuschöpfen, als dies aktuell der Fall ohne digitale Identitäten ist. Dabei gilt jedoch, dass die digitale Identität lediglich einen ersten Schritt darstellt, um das Potenzial zu heben. Aufbauend auf der digitalen Identität können dann neue Dienstleistungen und Prozesse wirtschaftlich werden (z. B. durch reduzierte Transaktionskosten) bzw. neu entwickelt werden, die zu einer tatsächlichen Realisierung dieses Potenzials führen. Beispielsweise gehen Kooperationen der Energy Web Foundation mit Austrian Power Grid und mit der Elia Group in diese Richtung. Beide Kooperationen zielen derzeit auf eine effiziente Einbindung der Flexibilität aus dezentralen Ressourcen zu Bilanzierungszwe-

52 EY: Blockchain-basierte Erfassung und Steuerung von Energieanlagen mithilfe des Smart-Meter-Gateways: Machbarkeitsstudie und Pilotkonzept, Studie im Auftrag des BMWi, Stand: 18.12.2019

cken ab.[53] Die oben vorgestellten Vorteile der Blockchain-basierten digitalen Identitäten werden genutzt, um den Zugang von dezentralen Ressourcen zum Bilanzierungsmarkt zu erleichtern. Weitere auf digitalen Identitäten basierende Anwendungsbeispiele wie etwa die Umsetzung von Energy Communities oder der Tokenisierung von Energie und deren Zertifizierungen werden derzeit erarbeitet und im Rahmen von diesem und ähnlichen Pilotprojekten erprobt.[54, 55]

3.5 Blockchain Machine Identity Ledger Pilotierung

Die Energiewirtschaft steht vor der Herausforderung eines massiven Anstiegs an markt- und netzrelevanten Endgeräten. Zukünftige Geschäftsmodelle erfordern dabei eine Senkung der Transaktionskosten sowie der Kosten, die aus notwendigen Meldevorgängen und Registrierungen, der Erstellung von Nachweisen etc. hervorgehen. Grundvoraussetzung für diese Anwendungsbeispiele ist immer eine automatisierte Identitätsverwaltung, die nur mit der Hilfe einer stringenten Digitalisierung und damit einhergehend einer Reduktion von Fehlern beim Datenaustausch sowie gesteigertem Vertrauen durch die Vermeidung von Medienbrüchen erreicht werden kann.

Die Herausforderungen hinsichtlich der Akzeptanz eines derartigen dezentralen Identitätsmanagements auf der Basis der Smart-Meter-Infrastruktur sind vielfältig und insbesondere stark mit einer zu erreichenden Interoperabilität verbunden. Diese muss dabei ein breites Spektrum an unterschiedlichen Ebenen abdecken. Während auf Geräteebene mit der Gateway- und SM-PKI-Standardisierung bereits eine Basis existiert, lässt die Protokollebene bewusst Freiheiten zur Übertragung von Daten über die CLS-Schnittstelle (Controllable Local System). In Bezug auf die Interoperabilität der Geräte-Identitäten kann bei der Implementierung auf Standards wie DIDs und Verifiable Credentials zurückgegriffen und aus Vorhaben des Innovationswettbewerbs „Schaufenster Sichere Digitale Identitäten“ gelernt werden, die nutzbare ID-Ökosysteme schaffen. Als weitere Ebene schließt die Blockchain-Ebene an, auf der ein Interoperabilität zwischen unterschiedlichen Blockchain-Netzwerken ebenfalls durch den Einsatz von Standards wie DIDs und Verifiable Credentials erreicht werden kann. Die Verknüpfung einer digitalen Identitätsverwaltung mit der PKI des SMGW als Rückgrat für die Digitalisierung der Energiewende legt eine genauere Betrachtung der Umsetzbarkeit aus technischer, wirtschaftlicher und regulatorischer Sicht nahe. Ziel des Blockchain Machine Identity Ledger Pilotvorhabens (kurz: BMIL-Pilot) war es daher, zu überprüfen, ob

- die Blockchain-basierte Verknüpfung von Anlagen der Energieerzeugung, der Energiespeicherung und des Energieverbrauchs (Lasten) mithilfe des SMGW und einer digitalen Anlagendatenbank und Identitätsverwaltung **technisch** machbar ist,

- nennenswerte **ökonomische** Vorteile mit Blick auf die Effizienz, insbesondere in Bezug auf Transaktionskostenreduktionen und die Hebung von Synergie- und Wettbewerbseffekten, erreicht werden können und

- **rechtliche oder regulatorische** Rahmenbedingungen bestehen, die Anwendungen in diesem Bereich aktuell beschränken, bzw. welche regulatorischen Fragen geklärt werden müssten.

Im Rahmen der Umsetzung und der Bewertung des betrachteten Pilotvorhabens in Kapitel 4 wurden folgende Thesen zur Umsetzbarkeit und Bedeutung der digitalen Identitäten-basierten Geräteregistrierung aufgestellt:

- Die digitale Identitäten-basierte Geräteregistrierung und das selbstbestimmte Identitätssystem können aus technischer Sicht
  - mittels Smart-Meter-PKI unter Berücksichtigung des standardisierten Rollenmodells im Regelbetrieb von intelligenten Messsystemen sowie
  - auf der Basis von am Markt verfügbaren SMGWs und
  - im Rahmen der vorhandenen technischen Restriktionen in Bezug auf verfügbare Kommunikationskanäle, Rechenleistung von Edge Devices, Bandbreiten und Latenzzeiten umgesetzt werden.

- Die technische Skalierbarkeit des gewählten „Identitäts-Verzeichnisses auf Blockchain-Basis“ als Infrastrukturgrundlage des Piloten im Hinblick auf eine spätere Serienimplementierung ist gegeben.

- Durch die digitale Identitäten-basierte Geräteanbindung können aus wirtschaftlicher Sicht Transaktionskosten potenziell reduziert werden für
  - verschiedenste Dienstleister (Vertriebe, Netzbetreiber, Aggregatoren) bei der Kundenanbindung und -abrechnung sowie
  - Energiekunden und Anlagenbetreiber bei der Registrierung in und der Teilnahme an verschiedenen Anwendungsbereichen und Märkten (überregionaler Strommarkt, Flexibilitätsmarkt, Peer-to-Peer-Handel, Grünstromzertifikatehandel etc.) durch Prozessautomatisierung.

53 Elia (2021); Energy Web Foundation (2020)
54 Elia (2021); Energy Web Foundation (2020)
55 Strüker, J., Utz, M., Sedlmeir, J. (2021): Einsatz der Blockchain-Technologie für Smart Grid Dienstleistungen durch E-PKW im Reallabor „EnStadt:Pfaff“

- Im Zusammenspiel mit der SMGW-Architektur bestehen für das Umsetzen des digitalen Identitätsmanagements Synergiepotenziale, die eine hohe Sicherheit gewährleisten und Kosten für eine eigenständige sichere Identitätsmanagement-Infrastruktur vermeiden würden.

- Die digitale Identitäten-basierte Geräteregistrierung und das Identitätsmanagement können aus regulatorischer Sicht
  - eine sichere und BSI-konforme Validierung und eine darüber hinausgehende Verwaltung der Daten im Rahmen einer digitalen Kommunikation über das SMGW ermöglichen und
  - dabei die datenschutzrechtliche Compliance wahren.

- Die vorhandenen technischen Richtlinien zur Einbindung und Kommunikation mittels SMGW sind jedoch teilweise unzureichend, um den vollständigen Validierungs- und Kommunikationsprozess für das digitale Identitätsmanagement rechtssicher abzubilden. Darüber hinaus fehlt es an hinreichenden Regeln für eine sichere Marktkommunikation außerhalb des SMGW.

Im Rahmen der BMIL-Pilotierung wurde der Fokus auf drei Ausprägungen der Implementierung der selbstbestimmten Identität und Geräteanbindung gelegt, die als technische Durchstiche umgesetzt und erprobt wurden. In den Kapiteln 4.1.3, 4.1.4 und 4.2 werden diese drei Ausprägungen im Detail vorgestellt.

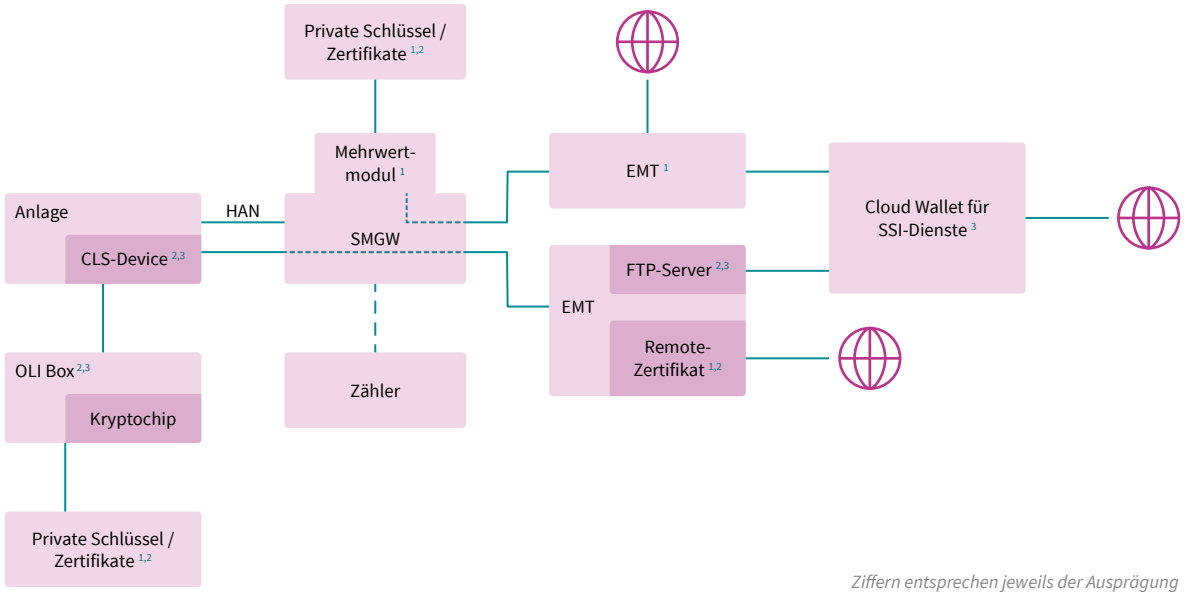


Abbildung 11: Gesamtarchitektur mit allen drei Anbindungsausprägungen (Quelle: Eigene Darstellung Fraunhofer FIT)

- **Ausprägung 1: Gerätezentrierte Identitätsverwaltung im Verbund mit einem SMGW Mehrwertmodul**

  Diese Ausprägung setzt auf einen bidirektionalen Kommunikationsweg zwischen CLS und einem externen Marktteilnehmer (EMT) (beide Parteien sind sowohl Sender als auch Empfänger) zur dezentralen Identitätsverwaltung auf einem adaptierten YOUKI-Mehrwertmodul des Herstellers Theben an einem Theben CONEXA 3.0 SMGW. Dabei wird das KILT Protocol als zugrunde liegende Blockchain-Technologie zum Verwalten der SSIs eingesetzt. Eine detaillierte Beschreibung findet sich in Kapitel 4.1.3.

- **Ausprägung 2: Gerätezentrierte Identitätsverwaltung im Verbund mit einem dedizierten CLS Device**

  Diese Ausprägung setzt ebenfalls auf einen bidirektionalen Kommunikationsweg zwischen CLS und EMT. Auch hier wird das KILT-Protokoll als zugrunde liegende Blockchain-Technologie zum Verwalten der SSIs eingesetzt. Im Unterschied zu Ausprägung 1 kommt ein dediziertes CLS-Device in Form einer OLI Box (Embedded Hardware auf Basis eines Raspberry Pi 3b) des Herstellers OLI Systems zum Einsatz. Eine detaillierte Beschreibung findet sich in Kapitel 4.1.4.

- **Ausprägung 3: Cloud-Wallet-basierte Identitätsverwaltung**

  Ausprägung 3 setzt auf die Delegation an eine Cloud Wallet von Spherity zur cloudseitigen Verwaltung der digitalen Geräte-Identitäten. Die technische Umsetzung erfolgte im Rahmen des 24 Piloten wie in Ausprägung 2 ebenfalls unter Einsatz einer OLI Box. Die Kommunikation verläuft dabei unidirektional über den CLS-Kanal vom CLS-Device ausgehend. Die unidirektionale Variante ist im Gegensatz zu den bidirektionalen Varianten in den Ausprägungen 1 und 2 insbesondere für ältere Liegenschaften relevant, die nicht aufwendig nachgerüstet werden können oder sollen. Eine detaillierte Beschreibung findet sich in Kapitel 4.2. Sowohl die dezentrale bzw. gerätezentrierte (Ausprägung 1 und 2) als auch die Cloud-Wallet-basierte Identitätsverwaltung (Ausprägung 3) zeichnen sich durch die Implementierung eines Identitätsnetzwerks nach den Maßstäben einer SSI aus. Der Ansatz der Identitätsverwaltung direkt auf dem Gerät ermöglicht dabei ein höheres Maß an Dezentralität, erhöht jedoch gleichzeitig den Kommunikationsaufwand durch die – aktuell noch streng limitierten – Kanäle des SMGW.

Die Blockchain nimmt im BMIL-Piloten vorrangig eine infrastrukturelle Aufgabe für die Überprüfbarkeit der Gültigkeit von VCs (Revocation, Selective Disclosure via Merkle Proofs) und (teilweise) die Speicherung von DID-Dokumenten wahr. Im Rahmen von weiterführenden Mehrwertanwendungen ist sie zudem als Infrastruktur für deren Umsetzung zu verstehen.

Bei der Auswahl der betrachteten und auf dem Basisdienst der Geräteregistrierung und Identitätsverwaltung aufbauenden Mehrwertanwendungen des BMIL-Piloten war es ein Ziel, den Nutzen des Einsatzes der Blockchain-Technologie und der Interoperabilität zwischen verschiedenen Blockchain-Netzwerken besonders deutlich herauszuarbeiten. Ebenso war es auch Teil der Überlegungen, grundlegende Prozesse in der Realwirtschaft zu berücksichtigen, die Akteure in mehreren Märkten umfasst und den länderübergreifenden Austausch von Energie und Waren bedeutet. Diese Überlegungen führten zu den in den Kapiteln 5.2 bis 5.5 beschriebenen Mehrwertanwendungen: Grünstromzertifikate, Netzdienstleistungen von Kleinanlagen und Fahrzeugen, CO_2 Certificates sowie Energy Communities.

4. Basisdienst Geräte-registrierung und Identitätsverwaltung

Autoren: Dr. Marius Buchmann, Jacobs University Bremen; Richard Hänsel, EY Law; Dr. Ing. Sven Rosinger, OFFIS

Im folgenden Kapitel 4.1 wird die gerätezentrierte Identitätsverwaltung im Verbund mit einem SMGW Mehrwertmodul (Ausprägung 1) sowie im Verbund mit einem dedizierten CLS-Device (Ausprägung 2) im Detail vorgestellt. Kapitel 4.2 stellt die Cloud-Wallet-basierte Identitätsverwaltung vor (Ausprägung 3). Die technische, ökonomische und rechtliche Bewertung der Anbindungsvarianten folgt in Kapitel 4.3.

4.1 Gerätezentrierte Identitätsverwaltung

4.1.1 Das KILT Protocol

Das KILT Protocol wird bei den im Folgenden beschriebenen Anbindungsvarianten als zugrunde liegende Blockchain-Technologie zum Verwalten der Self-Sovereign Identities, im Fall dieses Projekts der Geräte-Identitäten, verwendet. Das KILT Protocol ist ein auf Parity Substrate basierendes und von der BOTLabs GmbH entwickeltes Open-Source-Blockchain-Protokoll. Es ermöglicht Entitäten, eine digitale Identität zu erstellen, Eigenschaften zu beschreiben und sich diese von vertrauenswürdigen Issuers (Attestern) durch das Ausstellen von digitalen Zertifikaten bestätigen zu lassen, um sie dann Dritten zugänglich zu machen. Die Zertifikate verbleiben unter der Kontrolle der beschriebenen Entität und werden, um ihre Gültigkeit nachvollziehen zu können, auf der Blockchain verankert.

4.1.1.1 Funktionalitäten der KILT Blockchain

Bei den Funktionalitäten der Blockchain wird zwischen Schreib- und Lesezugriffen auf der Blockchain unterschieden:

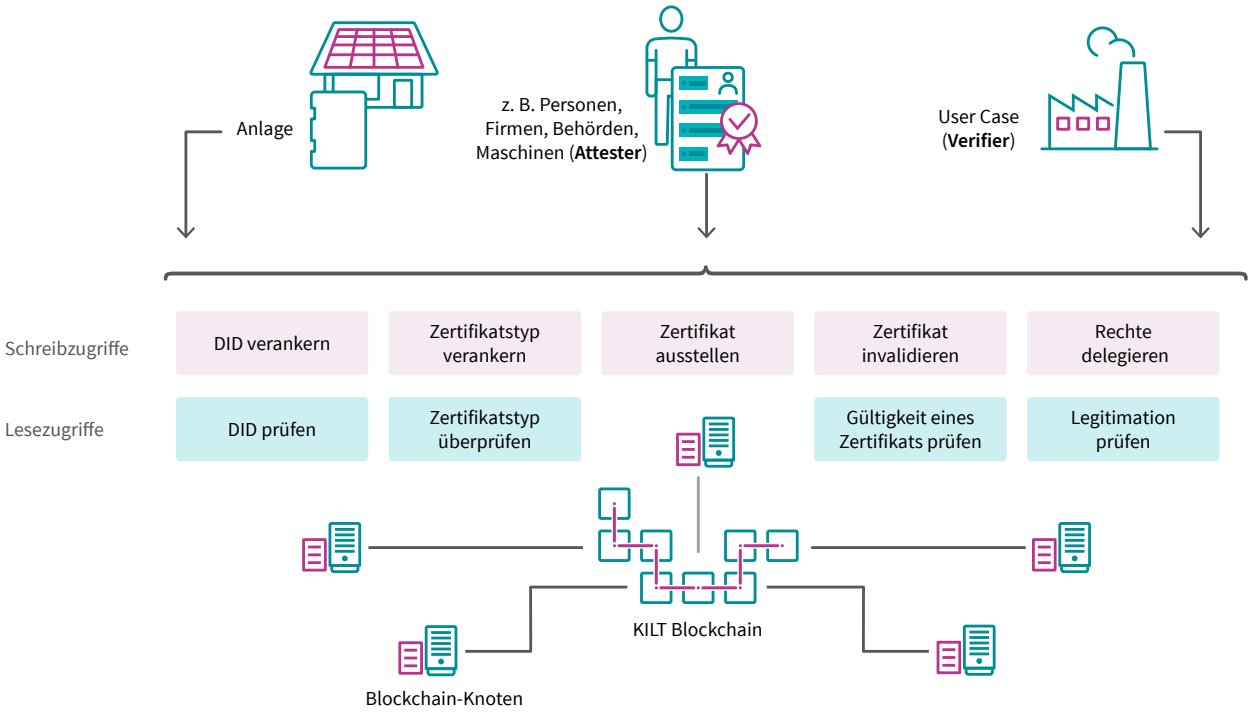


Abbildung 12: Funktionalitäten der KILT Blockchain (1) (Quelle: Eigene Darstellung BOTLabs GmbH)

DID verankern / DID überprüfen

Durch das Erzeugen eines Public / Private Key Pair wird ein eindeutiger Identifier für das Gerät erzeugt. Die Entität, die Zugriff auf das Key Pair hat, kontrolliert den Identifier und somit die Identität. Das kann ein einzelner Benutzer oder ein Gerät sein. Durch die Generierung eines DID auf Basis des Key Pair wird der Identifier des Geräts auf der Blockchain verankert und kann dort durch Dritte verifiziert bzw. überprüft werden. Für die Erzeugung der Identifiers auf der OLI Box unter Benutzung des Kryptochips siehe Abbildung 26. Für das Erzeugen eines Identifier bei YOUKI siehe Abbildung 27. Das Registrieren des DID auf der KILT Blockchain wird in Abbildung 28 dargestellt.

Zertifikatstyp verankern / Zertifikatstyp überprüfen

Um das System des Blockchain Machine Identity Ledger in die Lage zu versetzen, über Eigenschaften von Identitäten zu kommunizieren, bedarf es nicht nur einer Standardisierung der Art und Weise, wie die Akteure miteinander kommunizieren,

Kapitel 4.1: Zu diesem Kapitel haben folgende Projektpartner beigetragen: Energy Web, BOTLabs, OLI Systems, YOUKI, Riddle&Code

sondern auch dessen, was sie kommunizieren, das heißt der inhaltlichen Struktur von Eigenschaften und Zertifikaten. Da es unmöglich ist, die Inhaltsstruktur für eine unendliche Anzahl von Anwendungsfällen zu standardisieren, ist hier ein Abstraktionslevel notwendig. Dazu werden Claim-Typen (CTYPEs) eingeführt, bei denen es sich um die JSON-Beschreibung (JavaScript Object Notation) einer Datenstruktur handelt. Sie enthält eine Liste von Schlüssel-Wert-Paaren, wobei jeder Wert von einem definierten Typ ist. Ein CTYPE definiert somit das Schema für die Erstellung eines Zertifikats.

Damit die Akteure im System überprüfen können, ob ein Claim wirklich mit einem Claim-Typ übereinstimmt, wird jeder Claim-Typ lokal erstellt und als Hash auf der Blockchain registriert. Da die Hashes einmalig sind, können sich die Akteure im System auf die Verwendung eindeutig identifizierbarer Datenstrukturen einigen.

Zertifikat ausstellen

Das Gerät behauptet als Eigenschaft zum Beispiel seine Existenz, indem es einen Claim auf Basis eines definierten CTYPE und unter Verwendung seines Identifier erstellt und bei sich abspeichert. Dieser Claim muss, um Dritten gegenüber Glaubwürdigkeit zu erlangen, von einer vertrauenswürdigen Institution, dem sogenannten Attester, bestätigt (attestiert) werden. Bei diesem attestierten Claim handelt es sich dann um das Zertifikat. Da sich die Eigenschaften eines Geräts ändern oder ungültig werden können, muss die Validität des Zertifikats auf der Blockchain durch den Aussteller des Zertifikats verankert werden. Dazu wird nicht das ganze Zertifikat, sondern es werden nur ein Hash des Zertifikats, seine Validität und die notwendigen Informationen zum Attester auf die Blockchain geschrieben. Es werden somit keine personenbezogenen Daten auf der Blockchain gespeichert. Die bestätigten Zertifikate bleiben unter der Kontrolle des Geräts, das darüber entscheidet, wer auf das Zertifikat für welchen Zweck zugreifen darf. Damit wird die Selbst-Souveränität des Geräts sichergestellt. Das Ausstellen eines Zertifikats in Form eines VC ist in Abbildung 29 und in Abbildung 30 dokumentiert.

Zertifikat invalidieren / Gültigkeit eines Zertifikats überprüfen

Wenn sich die Eigenschaften eines Geräts ändern oder ungültig werden, muss das entsprechende Zertifikat invalidiert werden. Zum einen kann das Zertifikat durch die kontrollierende Entität auf dem Gerät gelöscht werden, zum anderen kann der Issuer des Zertifikats das Zertifikat auf der Blockchain auf ungültig setzen und somit invalidieren, wie in Abbildung 32 dargestellt. Um auf ein Zertifikat zuzugreifen, fragt der Service das Zertifikat, in dem die bestätigten Eigenschaften dokumentiert sind, bei dem Gerät an. Das Gerät kann dann dem Service das ganze Zertifikat oder auch nur Teile davon zugänglich machen. Über eine kryptografische Challenge stellt der verifizierende Service sicher, dass das Gerät wirklich Eigentümer des Zertifikats ist, und muss als Nächstes entscheiden, ob er dem Aussteller des Zertifikats vertraut, und prüfen, ob das Zertifikat auf der Blockchain noch gültig ist (siehe Abbildung 33).

Rechte delegieren / Legitimation überprüfen

Der Grad des Vertrauens in die ausgestellten Zertifikate wird durch die Vertrauenswürdigkeit der Organisation bestimmt, die das Zertifikat ausgestellt hat. Dies setzt voraus, dass das Gerät, das Eigenschaften über sich behauptet, und der verifizierende Service wissen, wem sie als Zertifikatsaussteller vertrauen können. Dies kann auf mehrere Arten geschehen:

- Der verifizierende Service vertraut dem Aussteller des Zertifikats direkt.
- Der Aussteller des Zertifikats erbt das Vertrauen von einer übergeordneten Stelle und kann das Zertifikat in deren Namen ausstellen. Die übergeordnete Vertrauenskette wird Bestandteil des Zertifikats.

Bei der übergeordneten Vertrauenskette handelt es sich um eine hierarchische Top-down-Vertrauensstruktur. Ein vertrauenswürdiger Knotenpunkt delegiert Vertrauen für die Ausstellung von Zertifikaten eines bestimmten CTYPE an weitere unter ihm stehende Knotenpunkte. Diese erben das Vertrauen von den über ihnen stehenden Knotenpunkten.

Das bedeutet, dass der verifizierende Service, wenn er einem übergeordneten Knotenpunkt vertraut, dann auch dem Aussteller des Zertifikats vertrauen wird. Die Vertrauenskette wird auf der Blockchain verankert und bei der Ausstellung von Zertifikaten auf ihre Gültigkeit hin überprüft (siehe Abbildung 31).

4.1.1.2 Software Development Kit (SDK)

Zum KILT Protocol gehört ein Software Development Kit (SDK), das alle Funktionalitäten des KILT Protocol implementiert. Das SDK enthält eine vollständige Spezifikation sowie eine kohärente Softwarebibliothek, die auf die aktuelle Version des KILT Protocol abgestimmt ist. Dieses SDK ermöglicht es Anwendungsentwicklern, Dienste und Anwendungen auf der Grundlage des KILT Protocol zu entwickeln, ohne tiefere Kenntnisse der Blockchain-Technologie zu benötigen. Die Einbindung des SDK zur Generierung des Identifier und zum Management der VCs in die OLI Box bzw. YOUKI ist in Abbildung 25 dargestellt.

4.1.1.3 Blockchain-Typologie des KILT Protocol

Das KILT Protocol verwendet standardmäßig die KILT Blockchain, um die Konsistenz und Validität der Daten sicherzustellen. Je nach Anforderung durch das Projekt kann die öffentliche KILT Blockchain verwendet oder eine private KILT Blockchain gestartet werden, die exklusiv für das jeweilige Projekt verwendet wird. Welche der beiden Varianten eingesetzt wird, ist eine strategische Entscheidung des jeweiligen Projekts. Im Falle

einer privaten Blockchain werden die Knoten der Blockchain von einem Konsortium betrieben und auch der Lese- und der Schreibzugriff auf die Blockchain können auf einen definierten Teilnehmerkreis beschränkt werden. Die Mitglieder des Konsortiums sollten sich gegenseitig vertrauen, da sie gemeinsam über Konsistenz und Validität der einzelnen Datensätze entscheiden. Sollte dieses Vertrauen nicht vorhanden sein oder soll das System so weit offen gestaltet sein, dass auch neue Mitglieder hinzukommen können, die nicht notwendigerweise das Vertrauen der anderen Teilnehmer genießen, bietet sich die Verwendung der öffentlichen Blockchain an. Hier wird das Vertrauen durch die mathematische Wahrheit ersetzt, sodass Teilnehmer in einer „vertrauenslosen" Umgebung miteinander interagieren können.

Um diese mathematische Wahrheit zu generieren, verwendet die KILT Blockchain ein zweistufiges Konzept. Die KILT-Blockchain-Knoten (sogenannte Collators) sammeln die Transaktionen und Schreibzugriffe auf der Blockchain, zum Beispiel für das Ausstellen von Zertifikaten, von allen Akteuren im System ein und verdichten sie zu einem Block. Jeder einzelne Block wird dann durch ein unabhängiges externes System auditiert und auf seine Konsistenz zum letzten finalisierten Block hin überprüft. Wenn dieses Audit erfolgreich war, hängen alle Collators den Block als finalisierten Block an die KILT Blockchain an. Bei der KILT Blockchain lassen sich über die auf der Blockchain gespeicherten Daten keine Rückschlüsse auf die Akteure und die Art der Daten ziehen, da sie nur als Hashes auf der Blockchain gespeichert werden.

Das externe unabhängige System ist im Falle von KILT das Kusama-[56] bzw. das Polkadot[57]-Netzwerk. Kusama und Polkadot sind öffentliche Blockchains ohne Zugangsbeschränkung (public permissionless), deren Sicherheit auf einem Proof-of-Stake-Mechanismus beruht. Die Stakes liegen derzeit im zweistelligen Milliarden-Euro-Bereich, was einen erfolgreichen Angriff sehr teuer und damit sehr unwahrscheinlich macht.

KILT ist eine sogenannte Parachain zur Kusama / Polkadot Relay Chain und damit ein Teil des Polkadot / Kusama-Ökosystems. Parachains sind berechtigt, ihre Blöcke zur Validierung (Audit) an die Relay Chain zu schicken und sie auf diese Weise finalisieren zu lassen. So profitieren die Parachains von der sehr hohen Sicherheit der mit vielen Milliarden Euro abgesicherten Relay Chain. Darüber hinaus löst dieses System das Skalierungsproblem älterer Blockchains wie Bitcoin oder Ethereum. Die Umsetzung von DIDs und VCs in diesem Projekt müsste beispielsweise auf Ethereum durch Smart Contracts erfolgen. Alle Smart Contracts aller Projekte konkurrieren aber um die Rechenleistung der einen Ethereum-Blockchain. Je mehr das System genutzt wird, desto knapper wird die Rechenzeit und desto höher wird der Preis einer Transaktion. Die Transaktionskosten werden nach Angebot und Nachfrage berechnet und sind nicht gedeckelt. Für eine industrielle Anwendung ist ein solches System nicht geeignet, da die Betriebskosten nicht im Vorfeld planbar sind.

Im Polkadot-Ökosystem ist die zentrale Relay Chain lediglich für die Bereitstellung der Sicherheit verantwortlich. Die einzelnen Parachains übernehmen dedizierte Aufgaben. So behandelt KILT ausschließlich die Thematik DIDs und Verifiable Credentials, während andere Parachains andere Aufgaben übernehmen. Transaktionen auf der KILT Blockchain konkurrieren also nur noch mit anderen DID- und VC-Anfragen. Dadurch kann der Durchsatz sehr hoch und der Transaktionspreis dauerhaft niedrig und nur geringfügig fluktuierend gehalten werden. Es entsteht Planbarkeit für industrielle Anwendungen bei allen Vorteilen, die die Verwendung einer public permissionless Blockchain bietet.

4.1.2 Übersicht Anbindungsvarianten auf KILT-Basis

Die folgenden zwei Anbindungsvarianten zeigen auf, wie das KILT SDK in die lokale Geräteebene eingebettet werden kann. Die bidirektionale Kommunikation der auf den Geräten installierten KILTKomponenten mit den Services in der Cloud läuft im limitierten Kontext des BMIL hierbei über ein zweites WAN, damit die Dezentralisierung und die damit einhergehende, anfänglich komplexe Kommunikation zwischen den vielen verschiedenen Projektteilnehmern voll ausgeschöpft werden kann. Die Nutzung eines CLS-Proxy-Kanals direkt über das SMGW sollte unter Berücksichtigung der derzeit bestehenden Limitierungen des SMGW insbesondere für ein Folgeprojekt den Vorrang haben. Die technischen Komponenten, die derzeit von verschiedenen Marktteilnehmern insbesondere im Kontext der Ladesäulenthematik entwickelt werden, sollten den Grundbaustein für den CLS-Proxy-Kanal bilden können. Am Ende der Beschreibung der Anbindungsvarianten wird auch kurz auf die Architektur eines solchen Systems eingegangen, damit klar wird, dass die hier erstellten Prozesse in Zukunft auf den CLS Proxy übertragbar sein sollten.

Auf der Softwareebene ermöglicht das Einbetten der Claimer Applikation und des Key und Claim Storage in die lokale Geräteebene die Erzeugung und Speicherung der Geräte-Identität in Form der Schlüsselpaare, des Identifier und der Verifiable Credentials direkt auf dem Gerät. Dadurch wird ein hoher Grad an Dezentralität erreicht, da für das Erzeugen, Vorhalten und Nutzen der Geräte-Identitäten keine zentralen Dienste benötigt werden.

56 https://kusama.network/, Zugriff am 18.08.2021
57 https://polkadot.network/, Zugriff am 18.08.2021

YOUKI nutzt SMGWs oder intelligente Energie-Messsysteme, um eine Software-as-a-Service-Plattform für Anwendungen im Bereich der Blockchain-Technologie zu etablieren. Jedes SMGW wird neben seiner originären Funktion als Datendrehscheibe für die Kommunikation mit einer Messstelle bzw. dem Smart Meter und damit dem Messstellenbetrieb an sich als Blockchain-Knoten (Node) in einem separaten Netzwerk verwendet. Dabei stellt YOUKI Softwaretools für die Entwicklung darauf basierender decentralized Applications (dApps) zur Verfügung und sichert den Betrieb des dezentralen Node-Netzwerks administrativ und systemtechnisch ab. YOUKI nutzt dazu eine Softwareintegration auf einem Mehrwertmodul, das auf der originären SMGW-Hardware sitzt. Bei dem „YOUKI-ready“-Mehrwertmodul handelt es sich um ein leistungsgesteigertes Theben-Aufsteckmodul mit höherer Prozessorleistung und einem größeren internen SSD-Speicher. Details dieser Anbindungsvariante sind in Kapitel 4.1.3 dargestellt.

Bei der Anbindungsvariante mit der OLI Box (siehe Kapitel 4.1.4) wird zur Generierung des Key Pair auf dem Gerät das Hardware Secure Module genutzt, indem es den Random-Input zur Erstellung des Key Pair zur Verfügung stellt. Dies erhöht die Sicherheit, weil die generierten Zufallswerte weniger vorhersagbar sind als der „Pseudo-Random“ des Raspberry Pi. Auf Basis des Key Pair wird der DID auf dem Gerät erzeugt und auf der Blockchain verankert und das DID-Dokument außerhalb des Geräts im Internet gespeichert, sodass andere Akteure mit dem DID, respektive dem Gerät, interagieren können. Darüber hinaus wird das Hardware Secure Module auch zur Verschlüsselung des Claim und Key Storage auf der OLI Box genutzt.

Über die Claimer-Applikation auf den jeweiligen Geräten wird der Zertifikats-Workflow, unter anderem das Claimen der Eigenschaften, die Anfrage zur Ausstellung des Zertifikats sowie das Speichern und Teilen des ausgestellten Zertifikats, auf den Geräten implementiert.

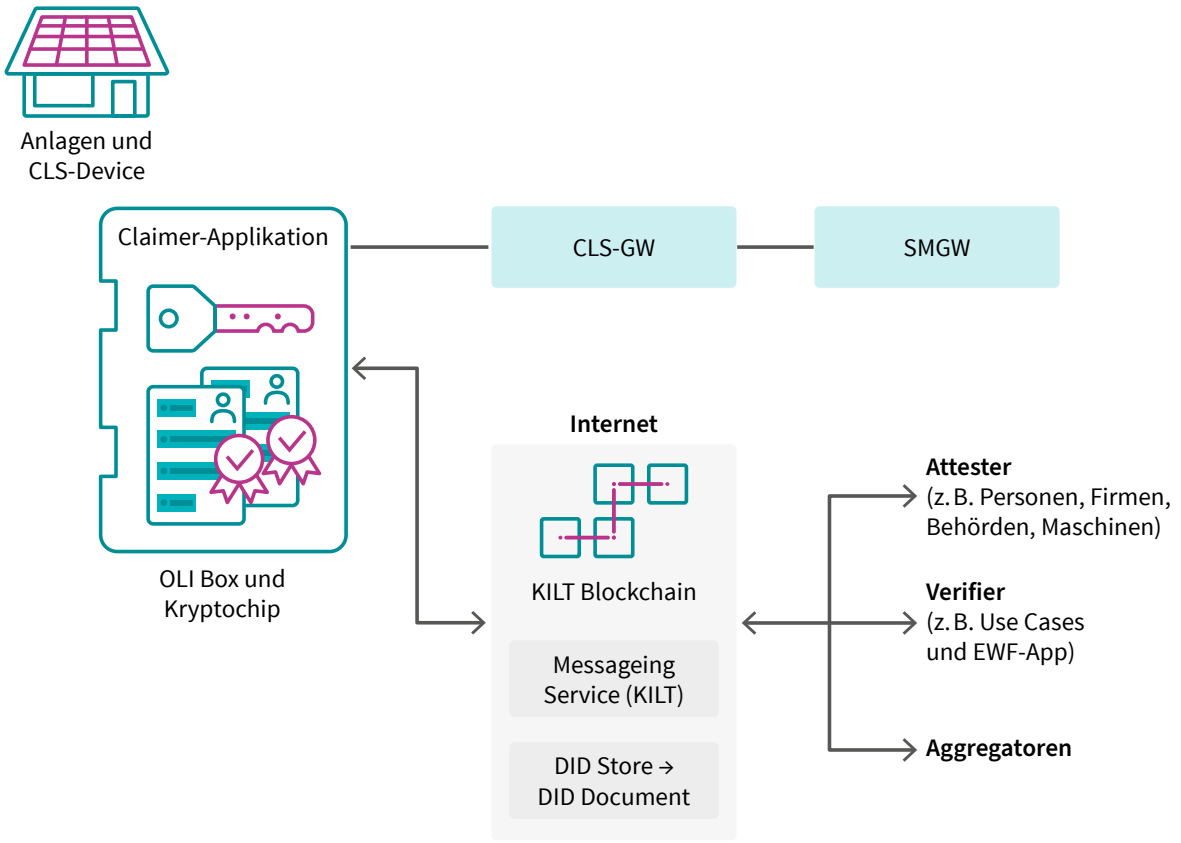


Abbildung 13: Funktionalitäten der KILT Blockchain (2) (Quelle: Eigene Darstellung BOTLabs GmbH)

Da bei der Implementierung der Geräte-Identitäten auf Standards wie DIDs und Verifiable Credentials zurückgegriffen wird, ermöglicht diese Lösung die Interoperabilität mit anderen Blockchains. Dafür kommt in diesem Projekt ein rollenbasiertes Rechtemanagement zum Einsatz, das auf der Energy Web Chain läuft und in den KILT-Zertifikaten auf den Geräten abgelegt wird.

Damit ist es möglich, die Berechtigungen von Geräten granular und komfortabel zu verwalten. Rollen und damit verbundene Berechtigungen können weiteren Geräten zugewiesen werden, um zum Beispiel eine ganze Klasse von Geräten für einen Anwendungsfall zuzulassen. Durch das Invalidieren einer Rolle kann die Berechtigung später zurückgezogen werden.

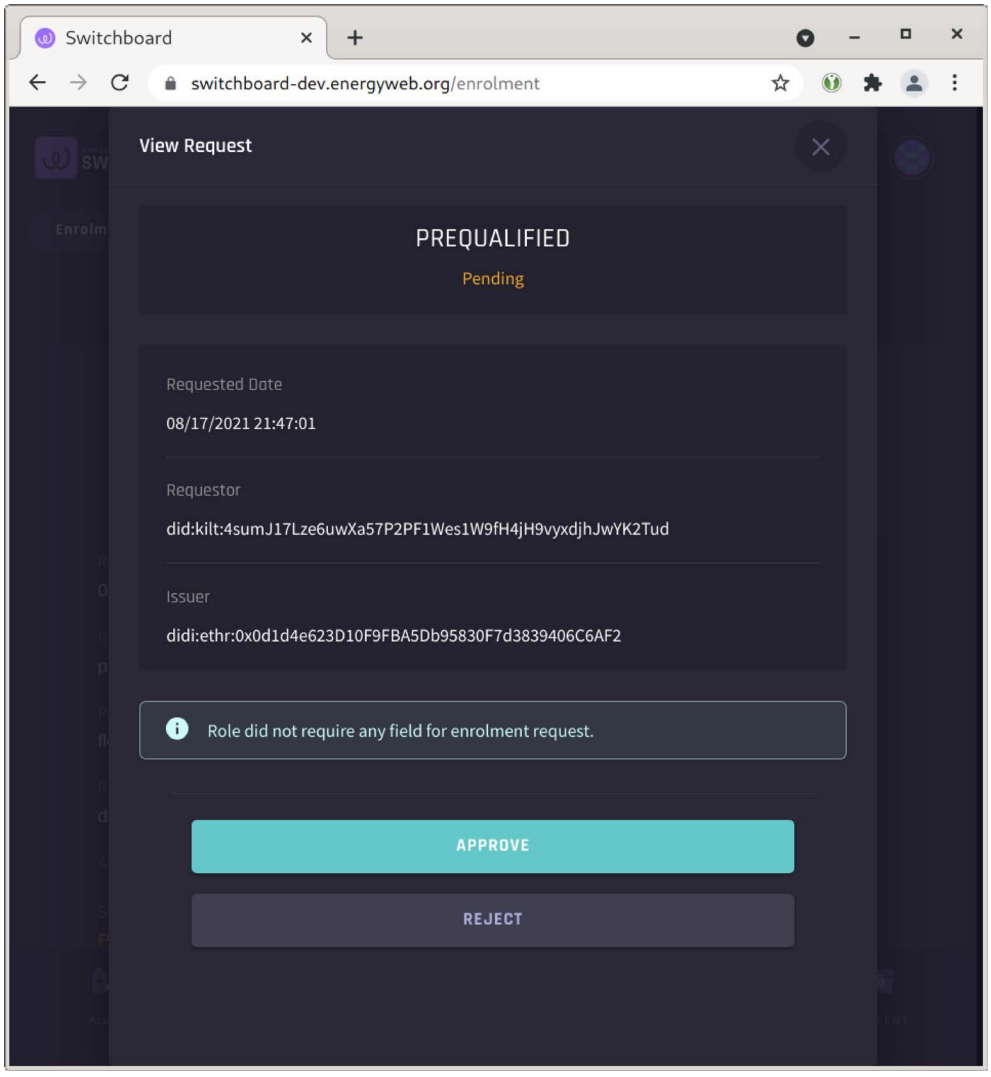


Abbildung 14: Verwalten von Rollen und Berechtigungen im Energy Web Switchboard (Quelle: Eigene Darstellung Energy Web Foundation)

4.1.3 Gerätezentrierte Identitätsverwaltung im Verbund mit einem SMGW-Mehrwertmodul

4.1.3.1 Blockchain-Integration in das SMGW-Mehrwertmodul

Die YOUKI-Systemarchitektur besteht aus drei sogenannten Layern (siehe Abbildung 15). Die Basis des YOUKI-Netzwerks ist das dezentrale SMGW-Netzwerk, das als Blockchain-Node-Netzwerk fungiert (Physical Layer). Je SMGW wird ein Blockchain Node in einem baulich verbundenen Mehrwertmodul betrieben. Darauf aufbauend werden Blockchain-Zonen (separierte kleinere Netzwerke) aus einer flexiblen Anzahl von YOUKI Nodes gebildet (>15 und <250 Nodes). Endkundenanwendungen bilden schließlich den Application Layer. Dabei handelt es sich um spezielle dApps, die auf den darunter liegenden Blockchain-Bereich zugreifen und den Kunden einen Mehrwert liefern. Auf dieser Anwendungsebene lassen sich Mehrwert-Geschäftsmodelle abbilden.

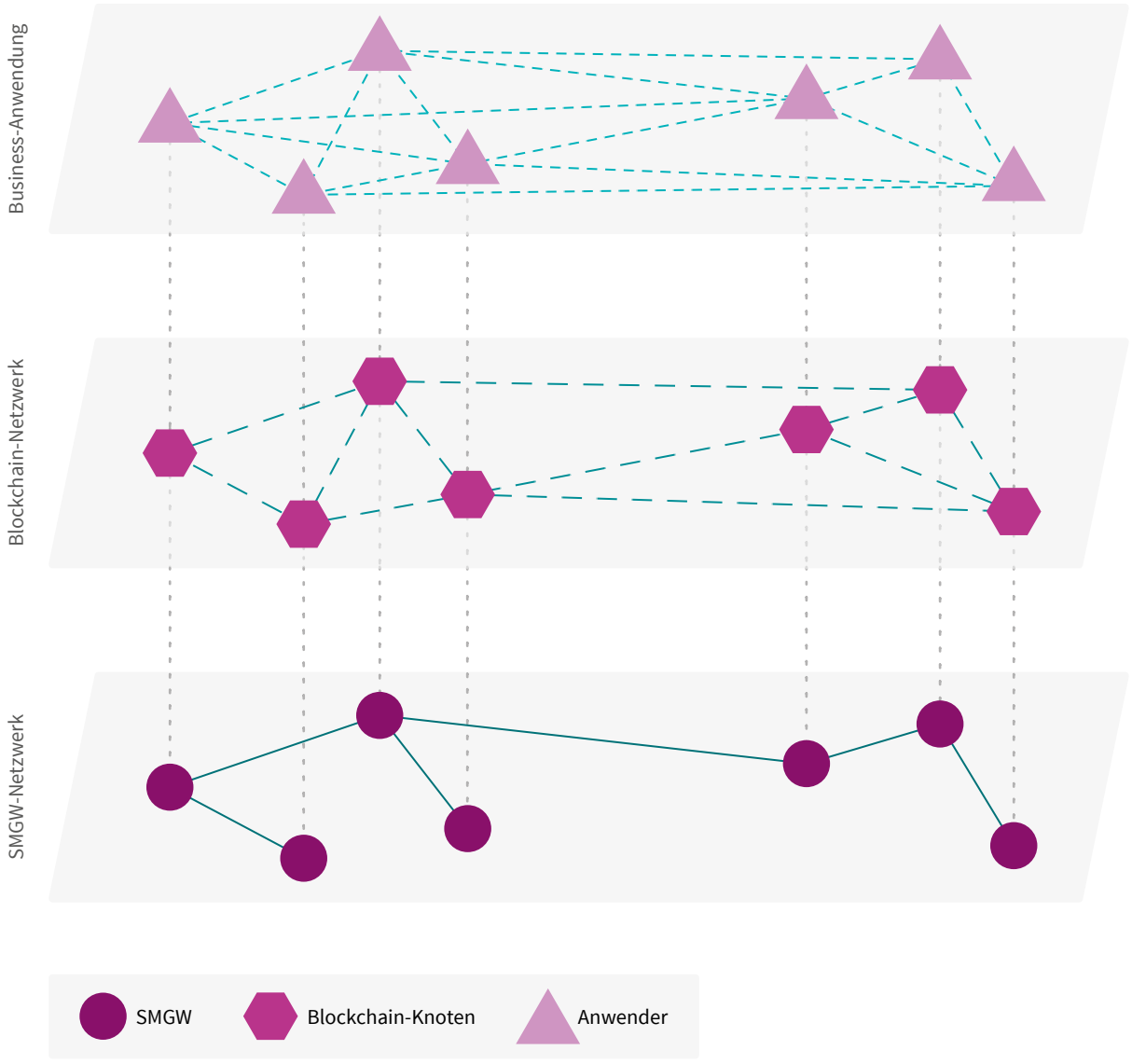


Abbildung 15: Die drei Ebenen des YOUKI-Netzwerks (Quelle: Eigene Darstellung YOUKI GmbH)

Die 3-Ebenen-Systemarchitektur wurde von YOUKI entwickelt und verfolgt das Ziel, das Ökosystem vor nachteiligen Auswirkungen oder Änderungen in der Blockchain-Technologie und deren Entwicklung zu schützen. Dabei erfolgt keine Fixierung auf einen dedizierten Blockchain Software Stack. Dennoch wird die Nutzung der Vorteile einer hohen Software- / Hardwareintegration in den Geschäftsmodellen ermöglicht.

Die Vorteile des 3-Ebenen-Modells liegen in der

- physischen Dezentralisierung des Blockchain-Node-Netzwerks mit zufälliger Zuweisung einer vorher spezifizierten Anzahl (je dApp-Anforderung) von Nodes, da die Hardware von der Blockchain-Software und -Plattform sowie von der Anwendungsebene getrennt ist. Physische Änderungen wie zum Beispiel der Ausfall eines Node in einer Region wirken sich praktisch nicht auf das Gesamtsystem aus.

- Datenunabhängigkeit bei weiteren „Blockchain-Evolutionen". Das bedeutet, dass Änderungen an Blockchain Stacks im Network Layer keine Auswirkungen auf den Application Layer und demnach auf die kundenspezifischen Anwendungen haben. Allgemein kann von einer höheren Robustheit gegenüber Änderungen und Weiterentwicklungen gesprochen werden.

4.1.3.2 Detailbeschreibung

Im Rahmen der Durchführung des BMIL-Projekts stellte YOUKI seine hauseigene SMGW / Blockchain-Laborumgebung zur Verfügung, die die gemeinsame Hardware- und Software-Testumgebung für die YOUKI-Anbindungsvariante bildete. Das Labor wurde so modifiziert, dass die Software- / Blockchain-Entwickler einen direkten Zugriff auf die SMGW-Infrastruktur und damit die Mehrwertmodule hatten.

Konfiguration im Detail:

- 3 separate Zählerschränke in unterschiedlicher Zählerausstattung, um alle Varianten der MS2020-Basiszähler nach FNN-Lastenheft abzubilden:
  - 3-Punkt-Basiszähler (BZ)
  - Elektronische Haushaltszähler (eHZ)
  - 3-Punkt-BZ, FNN-konform
  - Die Möglichkeit, Energiedienstleistungs-Haushaltszähler mit BABKommunikationsadapter für Bestandszähler abzubilden, bestand ebenfalls, wurde aber im Rahmen des BMIL nicht umgesetzt.

- Insgesamt 24 Theben CONEXA 3.0 SMGW
  - Zählerschrank 1: 10 Stück SMGW inklusive Mehrwertmodul (YOUKI Upgrade)
  - Zählerschrank 2: 10 Stück SMGW inklusive Mehrwertmodul (YOUKI Upgrade)
  - Zählerschrank 3: 1 Stück SMGW inklusive EEBUS-Mehrwertmodul (zur Anbindung)
  - Messkoffer: 3 Stück SMGW inklusive Mehrwertmodul (YOUKI Upgrade)

- Flexible Nutzung: Alle 24 Theben CONEXA 3.0 SMGWs können sowohl im „Mehrwertmodul-Betrieb" nach AP 3a als auch im „CLS-Mehrwertgeräte-Betrieb" nach AP 3b und im „Mischbetrieb" nach Ap 3a / 3b / 3c via Blockchain verbunden werden.

- Experimental-Wand
  - Einbindung von bis zu 24 CLS-Mehrwertgeräten (Konnektoren; gegebenenfalls unterschiedliche Hersteller) zum Aufbau einer CLS-Vertrauenskette
  - Einbindung Theben-Steuerbox 324
  - Gegebenenfalls Einbindung weitere Datenquellen, um die Nutzung der Blockchain-Infrastruktur für weitere Anwendungsfälle zu ermöglichen: (KNX-)Sensoren / Aktuatoren, Ladestations-Simulatoren und deren Logik etc.

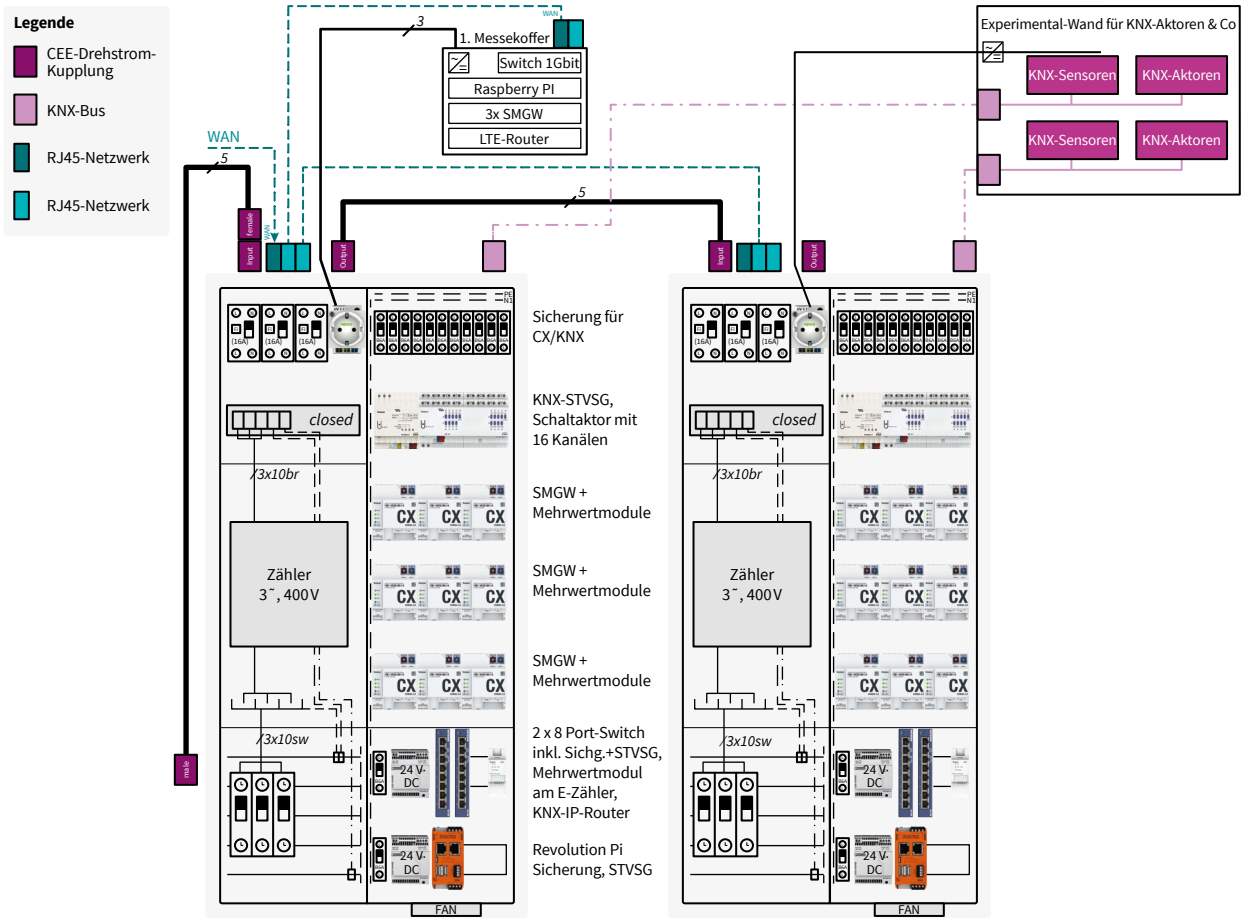


Abbildung 16: YOUKI-SMGW / Blockchain-Labor in „dena-BMIL-Konfiguration“ (Quelle: Eigene Darstellung YOUKI GmbH)

Abbildung 17: Laboraufbau in „dena-BMIL-Konfiguration“ (Quelle: Eigenes Bild YOUKI GmbH)

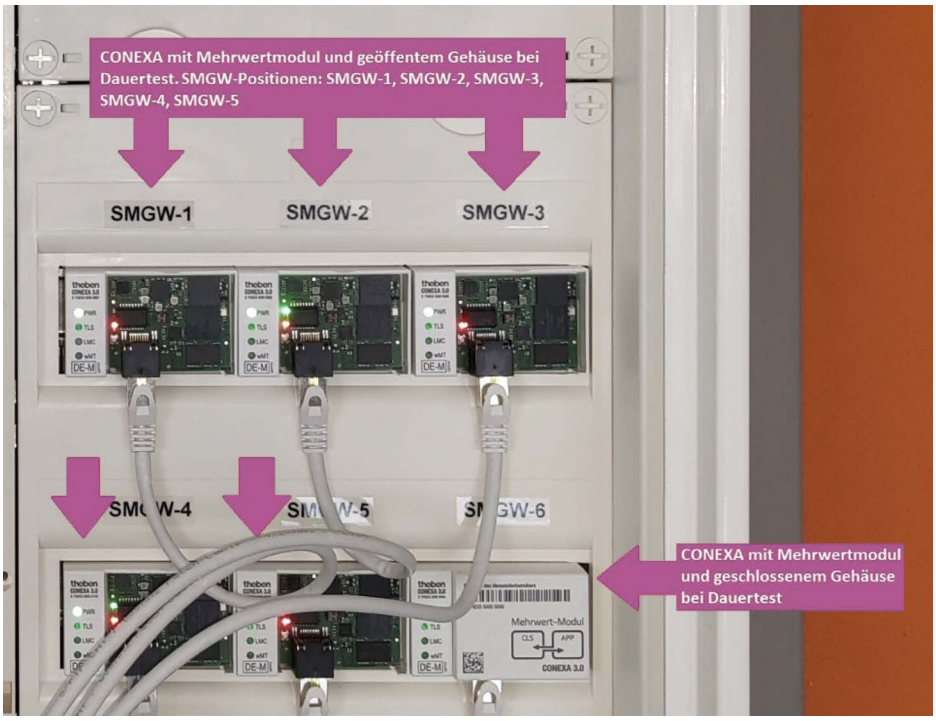


Abbildung 18: SMGWs mit Mehrwertmodulen im Feldtest (Quelle: Eigene Darstellung YOUKI GmbH)

Das Besondere an der YOUKI-Laborumgebung ist die hohe Flexibilität, um eine Vielzahl an Anwendungsfällen darstellen und prüfen zu können, und dass sich sowohl die eingesetzten (SMGW-)Komponenten als auch die Einbausituation möglichst nah am Marktstandard orientieren.

4.1.3.3 BMIL-Anbindungsvariante – wie ursprünglich geplant

Im Rahmen des BMIL-Projekts wurde eine hochflexible und modifizierbare Anlagen- und Geräteanbindung auf Basis der Theben CONEXA 3.0 SMGWs und der YOUKI-Test- und Laborinfrastruktur mit Geräteanbindung der SMGWs und Mehrwertkonnektor realisiert. Es wurden, neben den bereits im Knotenbetrieb befindlichen SMGWs von YOUKI, weitere BSI-konforme Installationen via einer sicheren Lieferkette in Energieerzeugungsanlagen (durch unser eigenes, zertifiziertes Personal) in der Testeinrichtung ausgerollt und daran angebunden.

Alle für den BMIL zur Verfügung gestellten Knoten der Testeinrichtung sind fernaktivierbar und können über einen Remote-Zugriff in ein definierbares, zonenbasiertes Blockchain-Netzwerk für Integrationstests in den Machine Identity Ledger eingebunden werden.

Zur Verarbeitung des Machine Identity Ledger mittels der Blockchain sind alle Knoten über eine direkte TCP / IP-P2P-Verbindung mittels CLS-Kanal (gemäß BSI TR-03109) verbunden.

4.1.3.4 Neuausrichtung – Blockchain als Parachain ohne Deployment auf Mehrwertmodule

Die Zielrichtung des BMIL ging ursprünglich von einem direkten Deployment der Blockchain auf die Mehrwertmodule von YOUKI aus. Ziel war es, jede sogenannte Zone bestehend aus >15 Knoten über einen Orchestration Service aufzusetzen und zu einer Blockchain zu verknüpfen.

Aufgrund der nach Projektstart neu definierten Projektarchitektur, die verstärkt den Einsatz digitaler Identitäten in den Fokus rückte, wurde ein Deployment auf die YOUKI-Mehrwertmodule respektive Blockchain Nodes nicht mehr durchgeführt. Es kam stattdessen eine sogenannte Parachain zur Kusama / Polkadot Relay Chain durch KILT zum Einsatz.

Damit beschränkte sich der Einsatz der BMIL-Projektgruppe auf einen dedizierten, von YOUKI eingerichteten VPN-Netzwerkzugang auf ein Mehrwertmodul mit CONNEXA 3.0 SMGW von Theben.
Die YOUKI-Systemarchitektur (siehe Abbildung 15) wurde dahingehend lediglich auf dem physischen Layer (SMGW-Netzwerk) durch das BMIL-Projekt in Anspruch genommen.

4.1.3.5 Anwendbarkeit der Lösung – Regulatorischer Rahmen / Sichere Lieferkette (SiLKe)

Für eine marktfähige Lösung aller im Projekt BMIL vorgestellten Anbindungsvarianten ist die Einhaltung der regulatorischen Rahmenbedingungen Voraussetzung. Insbesondere sind dabei das Messstellenbetriebsgesetz (MsbG) und die daraus resultierenden, durch das BSI im Auftrag des BMWK (vormals: BMWi) erlassenen Anforderungen an Systemarchitektur und Sicherheitstechnik und Technischen Richtlinien (TR) bis hin zu den Auflagen von Administration und Betrieb zu beachten.[58] In diesen TR sind sämtliche Festlegungen zu Datenschutz und Datensicherheit wie zum Beispiel zur Kommunikationsschnittstelle sowie kryptografische Vorgaben für Infrastruktur, PKI und GWA definiert.

Diese Dokumente sind sowohl Grundlage für die Zertifizierung der jeweiligen SMGWs als auch für die Anforderungen an die Sichere Lieferkette (SiLKe) und deren herstellerbezogene Freigabe und Anwendung. Jeder Hersteller hat dabei seine Geräte von der verwendeten bzw. entwickelten Hardware über die Software (alle vorgegebenen Funktionalitäten) bis hin zu Produktion, Versand und Installation entsprechend darzustellen und dem BSI zur Prüfung und Abnahme vorzulegen. Nur dies führt zu einem entsprechenden Zertifikatsnachweis (nach § 24 MsbG) und damit zur Möglichkeit, diese Geräte in Umlauf zu bringen. Das BSI hat alle maßgeblichen Dokumente hierzu veröffentlicht.[59]

Das bedeutet für die YOUKI-Anbindungsvariante:

Es werden jegliche dieser technischen und prozeduralen Anforderungen befolgt – sowohl im Rahmen der Rolle als wettbewerblicher Messstellenbetreiber (wMSB) wie auch als Gateway-Administrator (GWA) und aktiver externer Marktteilnehmer (aEMT) im energiewirtschaftlichen Marktumfeld und damit beim Aufbau des YOUKI-Core-Netzwerks. Ein Abweichen von diesen gesetzlichen Forderungen führt unweigerlich zu einer nicht genehmigten Messstelle und verhindert damit eine marktreife Umsetzung.

Für YOUKI im Speziellen bedeutet dies, dass die Theben-Zertifizierung[60] und die darin durch das BSI freigegebenen Vorgaben umgesetzt werden, begonnen bei der Bestellung der SMGWs bei Theben mit Versand der SIM-Karten, des elektronischen Lieferscheins (eLS) und des elektronischen Bestellscheins (eBS) inklusive Initialer Konfigurationsdatei (IKD). Daraufhin wird ein Produktionsauftrag bei Theben erstellt und die SMGWs sowie das Mehrwertmodul werden im Werk parametrisiert.

Der Versand erfolgt via SiLKe (Theben setzt hier auf ein Produkt der Firma LockYourWorld) und unter Einsatz der Safety / Sky Box mit den notwendigen Hardwareschlüsseln (pyKeys). Um an diesem Prozess teilzunehmen, ist eine Schulung bei Theben erforderlich. Das bedeutet, dass alle, die mit diesen Geräten umgehen (Logistiker / Elektriker), zwingend eine Schulung absolvieren müssen, bei Theben namentlich nachgehalten werden, über einen personalisierten pyKey-Schlüssel (zum Öffnen der Versandboxen) verfügen und unter anderem wöchentlich mit verschlüsselter E-Mail-Signatur (S / MIME) eine TAN-Liste anfordern etc.

Nur wer in diesem Ökosystem registriert und autorisiert ist, darf dann die Vorbereitung der SMGWs und der damit parametrisierten Zähler treffen wie auch den Einbau beim Kunden vor Ort durchführen. Bei YOUKI wurden daher alle involvierten Mitarbeiterinnen und Mitarbeiter geschult und die Prozesse der SiLKe umgesetzt.

Diesen BSI-Vertrauensanker und die daraus entstehende Integrität nutzt YOUKI für das Mehrwertmodul und das darauf implementierte Blockchain-Netzwerk. Die gezeigte YOUKI-Anbindungsvariante besteht im Kern darin, den Vertrauensanker des SMGW mit dem der Blockchain zu verheiraten.

Das Mehrwertmodul ist ebenso dazu geeignet, als Ablageort für digitale Identitäten (Verifiable Credentials) zu fungieren.

4.1.3.6 YOUKI Core – MSB-konforme Anbindung

Der regulatorische Rahmen und die Nutzung dieses BSI-Vertrauensankers werden im YOUKI-Core-System MSB-konform umgesetzt. Dabei erfolgt sämtliche Kommunikation nach der BSI TR-03109-4 „Smart Metering PKI – Public Key Infrastruktur für Smart-Meter-Gateways“.[61] Der Orchestration Service zum Aufsetzen der jeweiligen Blockchain Nodes bzw. der jeweiligen Blockchain Zone, notwendige Software-Updates wie auch das Monitoring und der Betrieb tun dies ebenfalls.

58 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Smart-Meter-Gateway.pdf?__blob=publicationFile&v=2
59 https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/SmartMeter/smartmeter_node.html
60 https://www.bsi.bund.de/SharedDocs/Zertifikate_CC/CC/SmartMeter_Gateway/0918_0918V2.html?nn=449840
61 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03109/TR-03109-4_PKI.html

4.1.4 Gerätezentrierte Identitätsverwaltung im Verbund mit einem dedizierten CLS-Device

4.1.4.1 Systemsicht

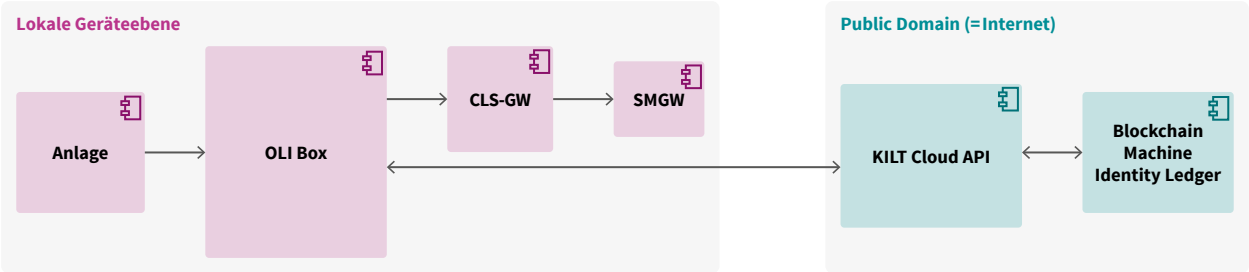


Abbildung 19: Systemsicht „Identitätsverwaltung im Verbund mit einem dedizierten CLS-Device“ (Quelle: Eigene Darstellung OLI Systems GmbH)

Aus der Systemsicht sind zwei Ebenen sichtbar:

- Die **Lokale Gerätebene** bildet die Haus- und Anlagenelektrik sowie das informationstechnische, IP-basierende Netzwerk ab.
- Die **Public Domain** könnte umgangssprachlich in diesem Kontext auch als „Internet“ bezeichnet werden. Es handelt sich um Dienste, die nicht in abgeschlossenen, lokalen Netzwerken installiert sind, jedoch meist mit einer Authentifizierung bzw. einem API-Key (Application Programming Interface) gesichert sind. Im BMIL befinden sich hier die Dienste von KILT sowie die Blockchain.

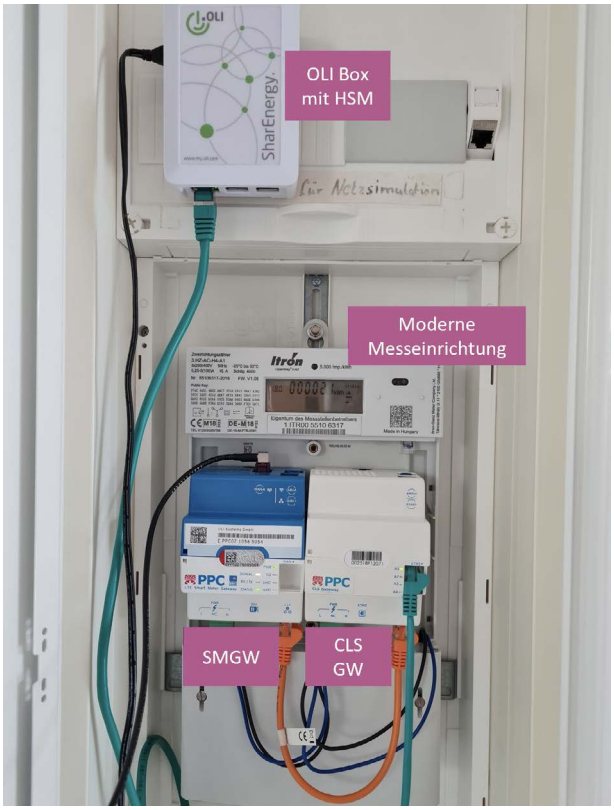


Abbildung 20: Installation der OLI Box und eines iMSys im Smart-Grid-Labor der Technischen Hochschule Ulm (Quelle: Eigene Darstellung OLI Systems GmbH)

4.1.4.2 Building-Block-Sicht Anlage

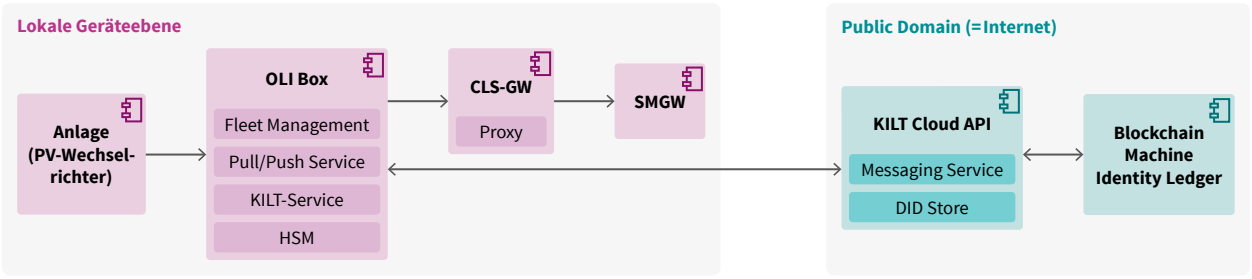


Abbildung 21: Building-Block-Sicht „Gerätezentrierte Identitätsverwaltung mit einem dedizierten CLS-Device“ (Quelle: Eigene Darstellung OLI Systems GmbH)

Anlage

Bei der Anlage handelt es sich um eine Energieanlage, die eine Identität mithilfe der BMIL-Lösung verliehen bekommen soll. Beispiele hierfür sind unter anderem eine Photovoltaik-Anlage bzw. derzugehörige Wechselrichter, eine Batterie und Steuer-elektronik, eine Wärmepumpe oder eine Ladesäule bzw. Wallbox.

OLI Box

Die OLI Box ist ein speziell für den Energiesektor konfigurierter Einplatinencomputer auf Basis des Raspberry Pi 3B. Je nach Einsatzort und -zweck erfüllt die OLI Box verschiedene Aufgaben. Darunter fallen die Datenerfassung an den verschiedenen Anlagen und Zählern, die Datenprozessierung und -aufbereitung sowie der Versand der Datenpakete in der Rolle eines Gateways. Im Kontext des BMIL übernimmt die OLI Box die notwendigen zusätzlichen Funktionen für die Anlage. Perspektivisch kann der Code, der sich derzeit auf der OLI Box befindet, in die Anlage bzw. deren Steuermodul oder deren Prozessor migriert werden, sollten diese in Zukunft die notwendigen Anforderungen erfüllen. Der Code ist im Falle des BMIL in Python geschrieben und läuft auf einer leicht modifizierbaren Debian-Distribution.

Abbildung 22: OLI Box in Verbindung mit einem PV-Wechselrichter (Quelle: Eigene Darstellung OLI Systems GmbH)

Fleet Management

Bei dem Fleet Management handelt es sich um eine Softwarekomponente auf der OLI Box, die insbesondere während der Debugging- und Entwicklungsphase benötigt wird. Sie übernimmt neben der Übertragung des Health-Status (Geräte online / offline, derzeitige IP und weitere Parameter) auch die Bereitstellung eines SSH-Kanals (Secure Shell) über den Port 22 – selbst bei Firewalls und dynamischen IPs. Insbesondere im Laborumfeld ist das Teilen des Zugriffs mit Projektpartnern eines der wichtigsten Features. Das derzeitige Fleet Management kann – je nach Art und Weise der Instandhaltung der OLI Box – auch im Produktivbetrieb genutzt werden. Jedoch sollte dann insbesondere der SSH-Zugriff stark eingeschränkt bzw. ganz unterbunden und stattdessen ein Postfach-System eingesetzt werden.

Pull Service

Der Pull Service auf der OLI Box ist ein zyklisch ablaufender Cronjob, der in konfigurierbaren Zeitabständen die im Beispiel des BMIL auf dem Modbus-TCP-Register (SunSpec-Protokoll) basierenden Daten der Anlage ausliest (Pull). Die Daten werden daraufhin in eine JSON-Datei geschrieben und lokal in der OLI Box abgelegt (master_data.json).

Hardware Secure Module (HSM)

Die OLI Boxen verfügen über ein Hardware Secure Module (umgangssprachlich auch „Kryptochip“ genannt), das bestimmte kryptografische Operationen durchführen kann. Durch die Nutzung dieser zusätzlichen, dedizierten Hardwareplattform wird das Sicherheitsniveau weiter angehoben. Das HSM ist auch tatsächlich physisch von der eigenen OLI-Box-Platine getrennt und nur über eine API erreichbar. Funktional wären die Operationen auch auf Softwarebasis möglich, jedoch vermehren sich dadurch die Angriffsvektoren. Im BMIL kam die Hardware HSM6 des Herstellers Zymbit zum Einsatz. Hierbei handelt es sich um eine Plattform im Beta-Status, sprich: eine Entwicklungsumgebung, wobei sowohl die Hardware als auch die Software im HSM noch nicht final sind. Zu den im BMIL in Frage kommenden Funktionen des HSM6 gehören:

- **Entropie für Private-Key-Erstellung:** Viele softwarebasierte Libraries haben Schwächen bei der RNG (Random Number Generation), da die internen Zahlen- und Zufallsbereiche nicht das volle mögliche Spektrum abdecken. Durch die eingeschränkte Entropie vieler Libraries erhöht sich die Gefahr durch Brute-Force-Angriffe. Das HSM verfügt über eine eigene hardwarebasierende Entropie, um diesem Problem entgegenzuwirken.

- **Key Storage:** Neben der Generierung der Private Keys kann ein HSM diese auch intern abspeichern und agiert dadurch ähnlich wie ein Hardware Wallet. Die Private Keys verlassen dabei das HSM nicht.

- **Verschlüsselung:** Mit dem HSM können auch lokale Dateien verschlüsselt werden, was erweiterte Möglichkeiten hinsichtlich der Zugriffssteuerung bietet. Unter anderem werden dabei als kryptologische Hash-Funktionen ECDSA, ECDH, AES-256 und SHA256 unterstützt.

- **Signing:** Wenn die Private Keys in dem HSM abgelegt sind, muss der Chip auch zum eigenständigen Signieren von Nachrichten fähig sein. Diese Funktion ist für eine kleine Zahl an Kurven verfügbar, darunter auch in dem neuesten Beta-Release von Zymkey, der „Koblitz“ secp256k1, die von Ethereum und Bitcoin genutzt wird. Die von KILT genutzte ed25519-Kurve wird derzeit noch nicht unterstützt, weshalb das Signing per Software abgebildet wird. Im Herbst wird Zymbit hier ein Firmware-Update veröffentlichen, das diese Kurve dann ebenfalls unterstützt.

CLS-GW und SMGW

Das CLS-GW (Controllable Local System Gateway) und das Smart-Meter-Gateway (SMGW) von PPC sollen an dieser Stelle zusammen beschrieben werden. Beide Geräte (und darüber hinaus auch der aEMT) sind mit den nach der BSI-Richtlinie TR-03109 vorgeschriebenen Zertifikaten und Konfigurationen ausgestattet und bilden korrekt und praxisnah die Kommunikation über den CLS-Kanal ab. Das SMGW ist in unserem Fall mit einem LTE-WAN ausgestattet und kommuniziert im BMIL über die Test-PKI. Das CLSGW bildet eine Brücke zwischen dem lokalen Home Area Network (HAN) und der HAN-CLS-Schnittstelle des SMGW, sodass faktisch zwei getrennte Netzwerke vorliegen. Wie im folgenden Abschnitt beschrieben, haben wir uns dagegen entschieden, die bidirektionale Kommunikation des KILT-Service auf der OLI Box in eine unidirektionale Kommunikation über den transparenten Kanal zu komprimieren, da so wichtige Aspekte der SSI-Lösung verloren gehen würden. Die beiden Geräte sind installiert und bereit, benötigen aber noch Anpassungen auf dem CLS-GW sowie dem aEMT, um die bidirektionale Kommunikation zu ermöglichen.

4.1.4.3 Ausblick auf die Anbindungsvariante unter Einbeziehung eines Proxys

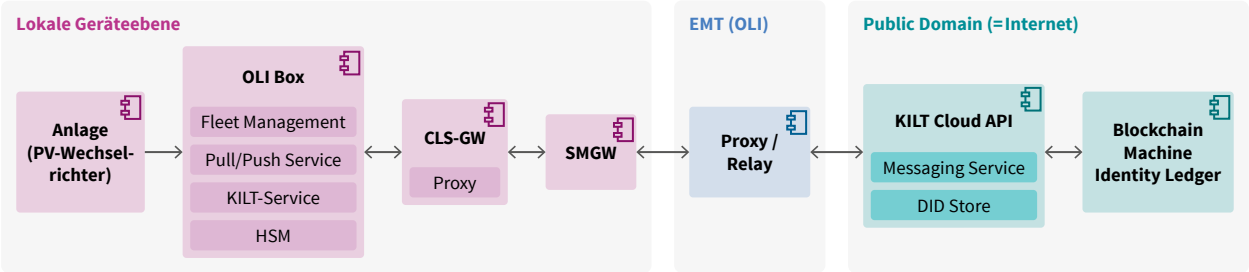


Abbildung 23: Proxy/Relay beim EMT für die bidirektionale Kommunikation über das SMGW hin zur Public Domain (Quelle: Eigene Darstellung OLI Systems GmbH)

Die derzeitige Kommunikation der KILT-Softwarekomponenten auf der OLI Box läuft über ein zweites WAN ab, wodurch die KILT-Dienste in der Public Domain barrierefrei bidirektional angesprochen werden können. Dies ermöglicht die dynamischen Abläufe und Entwicklungen dieser SSIImplementierung vollständig abzubilden und dabei unabhängig zu sein von den derzeit noch vorhandenen Limitierungen der iMSys-Kommunikationsstrecke. Applikations- und protokollunabhängige bidirektionale Kommunikation von der lokalen Geräteebene durch einen transparenten TLS-Kanal (Transport Layer Security) hin zu der Public Domain und den darin befindlichen Cloud-Diensten ist eine Anforderung, die sich derzeit in der Industrie weiter herausbildet. Besonders Ladesäulenbetreiber und -hersteller pochen auf eine einfache Lösung an dieser Stelle, die dem ursprünglichen Gedanken des iMSys einer vorkonfigurierten 1:1-Kommunikationslösung auf den ersten Blick entgegenläuft. Trotz der Komplexität sehen wir – abgesehen von der regulatorischen Notwendigkeit – einige große Vorteile in der Nutzung des Smart-Meter-Gateway und des dazugehörigen SMGW-WAN für die Kommunikation:

- Von staatlichen Behörden bereits zertifizierte sichere Kommunikationsstrecke mit definierten Start- und Endpunkten inklusive PKI-basierter Integritätsmechanismen, aufbauend auf bestehenden energiewirtschaftlichen Prozessen (z. B. Tarifanwendungsfälle) und Datenendpunkten (SMGW-ID, Zähler-ID, Messlokation usw.)

- Kostensparende Mehrfach- und Mehrzwecknutzung des ohnehin vorhandenen intelligenten Messsystems; keine zweite Kommunikationsstrecke notwendig, was die Komplexität reduziert und die ökonomische (und auch ökologische) Bilanz weiter verbessert

- Abgeschlossenes informationstechnisches und IP-basierendes Energienetzwerk vor Ort mit eigenen, spezifizierten Regeln, was die Akzeptanz und Integrität im Vergleich zur „FritzBox-Haushalt-LAN / HAN-Lösung“ weiter erhöht, Stichwort: „Verplombung“

Wir haben die Anforderungen vonseiten der SSI-Lösungen an eine Umsetzung im BMIL-Kontext gesammelt, um diesen Kanal umsetzen zu können, jedoch sollten hierzu ausreichend Zeit und Kapazität eingeplant werden.

Insbesondere die Weiche (bzw. der Proxy / das Relay) des externen Marktteilnehmers, die die eingehende und ausgehende Kommunikation verwaltet, wird entscheidend sein. Dabei darf der Proxy / das Relay möglichst wenig in die ausgetauschten Datenpakete eingreifen, um den Integrationsaufwand der CLS-Anwendungsentwickler gering zu halten und gleichzeitig die strenge 1:1-Kommunikationslogik einzuhalten. Unsere Recherchen haben ergeben, dass diesbezüglich an mehreren Stellen weitere Lösungsansätze in Entwicklung sind, wie zum Beispiel an der Technischen Hochschule Ulm.

4.1.5 Softwarearchitektur und Prozesse der KILT-Integration

Die Softwarearchitektur und die Prozesse der beiden Anbindungsvarianten unterscheiden sich nur bei der Verwendung des Hardware Secure Module und werden somit, wenn nicht anders angegeben, in den Diagrammen zusammen behandelt.

Bei der Integration der Maschinen-Identitäten mit dem KILT Protocol liegen die Identitäten, also der Identifier und die Zertifikate bzw. Credentials, direkt auf dem jeweiligen Gerät.

Im ersten Schritt wird das Private / Public Key Pair auf dem Gerät generiert, bei OLI unter Einbeziehung des Kryptochips. Dann wird auf dem Gerät der DID erzeugt und durch das Schreiben des Public Key auf der KILT Blockchain dort verankert. Die Box signiert das DID-Dokument, um es mit dem DID zu verknüpfen, und speichert es im DID Store, sodass Dritte mit dem DID interagieren können. Das Key Pair wird verschlüsselt im Key Storage gespeichert.

Die Zertifikatsprozesse, wie zum Beispiel das Anfordern eines Zertifikats, das Speichern eines ausgestellten Zertifikats und das Teilen eines Zertifikats, finden direkt auf dem Gerät statt.

Dazu gehört auch die Möglichkeit, beim Teilen eines Zertifikats nicht das gesamte Zertifikat, sondern nur bestimmte Inhalte mit Dritten zu teilen. Selbst wenn nicht alle Inhalte des Zertifikats geteilt werden, kann es kryptografisch verifiziert werden.

Die verschiedenen Akteure des Systems, wie zum Beispiel die Geräte, die zertifikatsausstellenden Instanzen und die Use Cases, die auf das Zertifikat zugreifen, kommunizieren über den KILT Messaging Service per verschlüsselten Nachrichten miteinander.

4.1.5.1 Systemsicht der Anbindungsvarianten

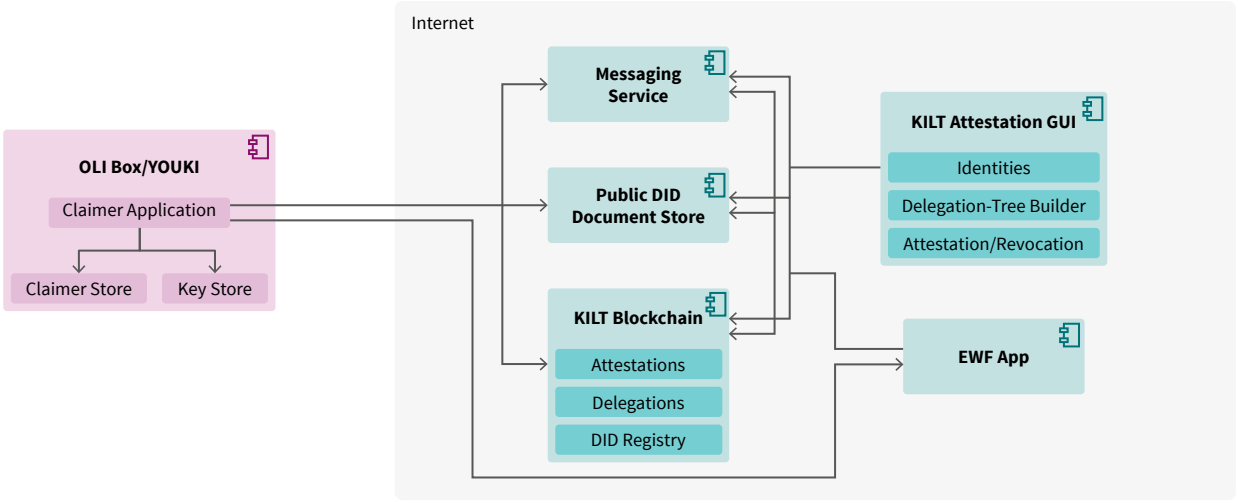


Abbildung 24: Systemsicht KILT-Integration (Quelle: Eigene Darstellung OLI Systems GmbH)

Claimer Application
Die Claimer Application stellt Endpoints zur Generierung des Identifier und zur Registrierung dem DID auf der Blockchain bereit. Zusätzlich pollt die Claimer Application Nachrichten vom Messaging Service, zum Beispiel Anfragen zur Ausstellung eines Zertifikats, zum Teilen eines Zertifikats etc.

Key Store
Im Key Store werden das Private / Public Key Pair sowie der Seed für das Wiederherstellen des Key Pair abgelegt.

Claim Store
Im Claim Store werden die ausgestellten Zertifikate und, wenn noch nicht zertifiziert, der Claim und die Anfrage zur Zertifizierung gespeichert.

Messaging Service
Die Akteure kommunizieren per verschlüsselten Nachrichten über den Messaging Service. Für die Implementierung wird der KILT Messaging Service genutzt. Es steht den Akteuren aber frei, einen eigenen Messaging Service zu implementieren und zu nutzen.

Public DID Document Store
Im KILT DID Store werden die DID-Dokumente abgelegt. Der DID Store steht im Internet, damit Services auf das DID-Dokument zugreifen können, um mit der entsprechenden Identität zu interagieren.

KILT Blockchain
Siehe Kapitel 4.1.1.1 Funktionalitäten der KILT Blockchain.

KILT Attestation GUI
Über die KILT Attestation GUI erzeugt der Aussteller eines Zertifikats sein Private / Public Key Pair, nimmt Anfragen zur Ausstellung von Zertifikaten entgegen, signiert die Zertifikate mit seinem Private Key, schreibt das gehashte Zertifikat auf die Blockchain und kann es dort auch invalidieren. Über die Attestation GUI werden auch die Delegationsstrukturen angelegt. Jeder Attester kann seine eigene Instanz der KILT Attestation GUI betreiben oder seine eigene Attestation GUI auf Basis des KILT SDK implementieren.

Applikation der Energy Web Foundation
Eine Applikation zur Prequalifizierung von Geräte-Identitäten für unterschiedliche Anwendungsfälle durch eine VC-basierte Rollenvergabe. Die Präqualifizierung ist beispielhaft für die Use Cases Netzdienstleistungen und Grünstromzertifikate-Register implementiert.

4.1.5.2 Building-Block-Sicht der Anbindungsvarianten

Bei der Building-Block-Sicht wird der Fokus auf die Claimer-Applikation und den Key und Claim Storage gelegt, die beide auf den jeweiligen Geräten laufen. Die Claimer-Applikation nutzt das KILT SDK[62] zur Generierung des Identifier in Form des Key Pair und dem DID und zum Management der VCs.

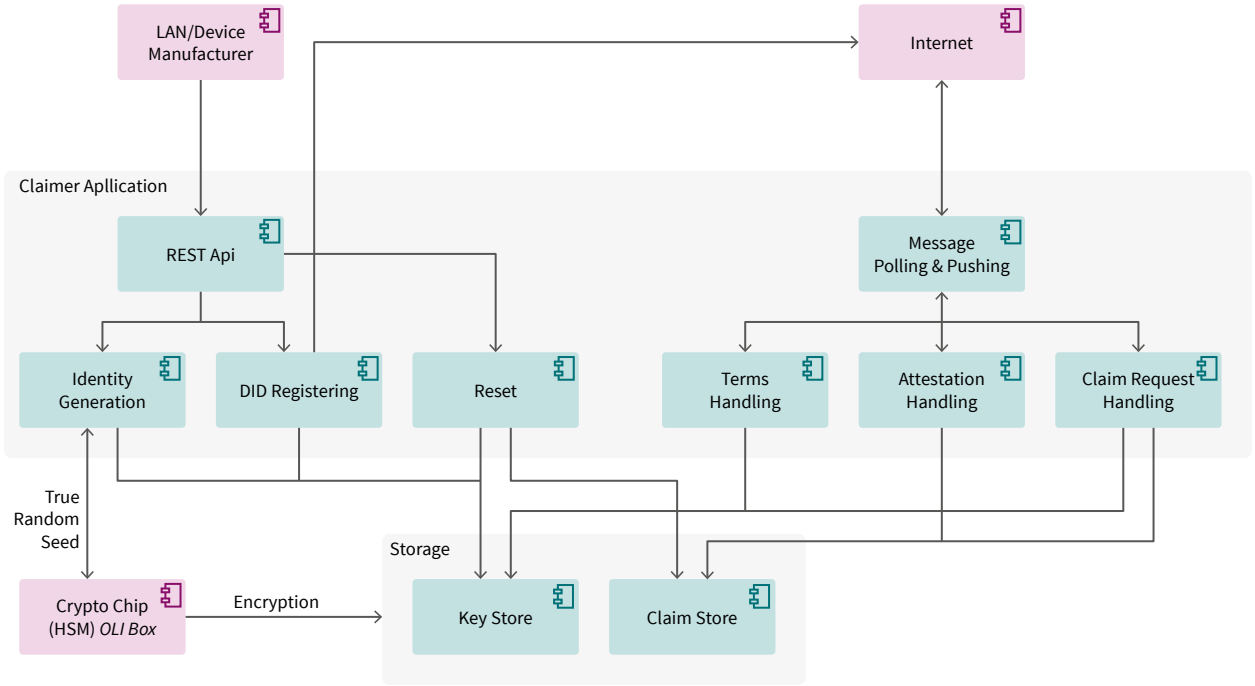


Abbildung 25: Building-Block-Sicht KILT-Integration (Quelle: Eigene Darstellung BOTLabs GmbH)

62 https://dev.kilt.io/#/, Zugriff am 25.08.2021

4.1.5.3 Datenflusssicht der Anbindungsvarianten, Erzeugung des Identifier und Registrieren des DID auf der KILT Blockchain

Der Hersteller triggert die Generierung des Private / Public Key Pair auf den Geräten, das dann im Key Store auf dem Gerät abgelegt wird. Bei der OLI Box wird das Key Pair mithilfe des Kryptochips erzeugt.

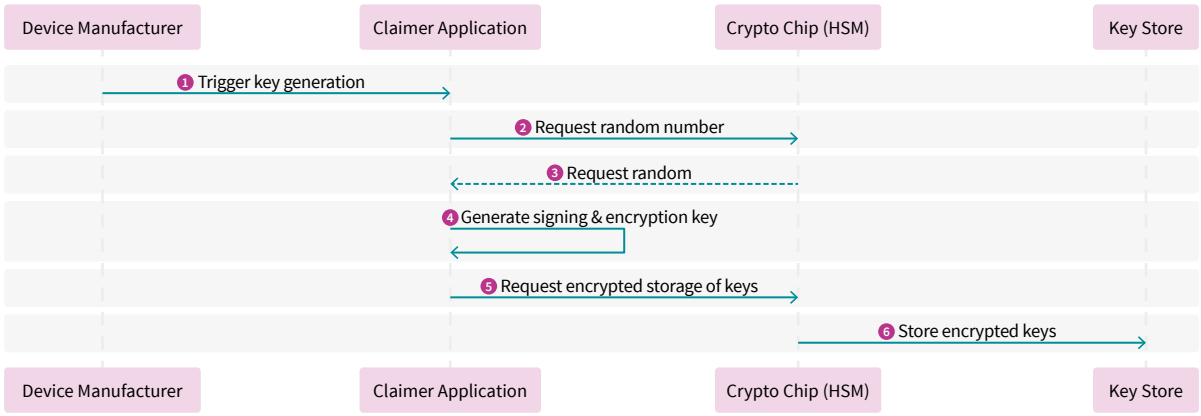


Abbildung 26: Sequenzdiagramm Generierung des Key Pair – OLI Box (Quelle: Eigene Darstellung YOUKI GmbH)

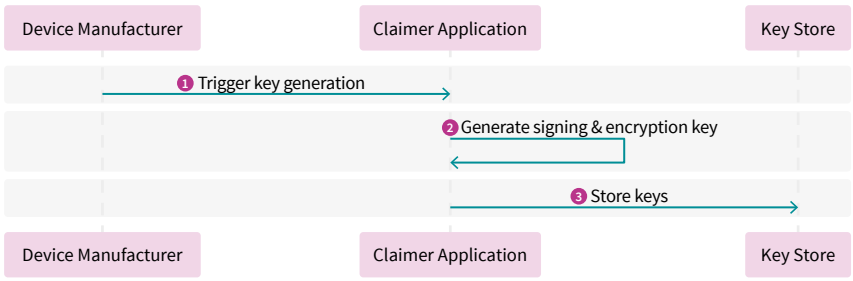


Abbildung 27: Sequenzdiagramm Generierung des Key Pair – YOUKI (Quelle: Eigene Darstellung BOTLabs GmbH)

Registrierung des DID auf der KILT Blockchain

Auf Basis des vorab generierten Key Pair wird der DID als Identifier für das Gerät erzeugt und auf der Blockchain registriert. Das DID-Dokument wird im Public DID Document Store gespeichert, sodass zum Beispiel die Use Cases mit dem DID interagieren können.

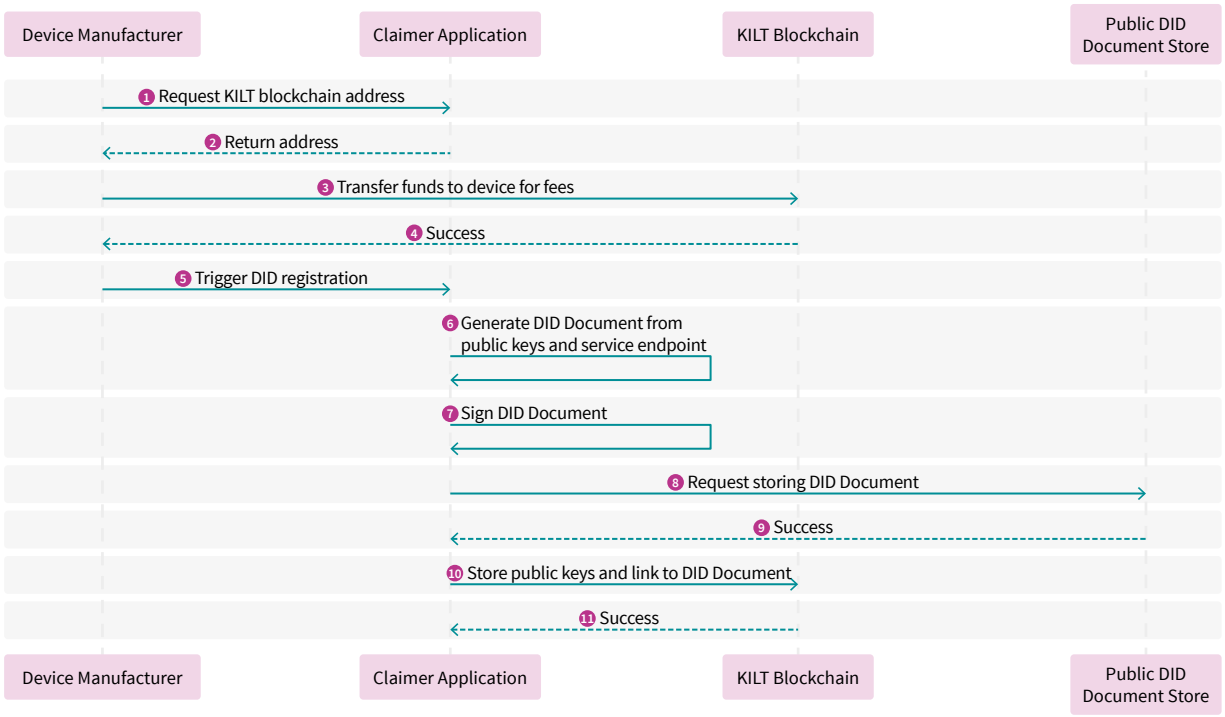


Abbildung 28: Sequenzdiagramm Registrierung dem DID auf der KILT Blockchain (Quelle: Eigene Darstellung BOTLabs GmbH)

Ausstellung des Zertifikats BMILInstallationCredential

Das Zertifikat BMILInstallationCredential wird vom Issuer ausgestellt, im Claim Store der OLI Box bzw. von YOUKI abgespeichert und vom Issuer auf der KILT Blockchain verankert.

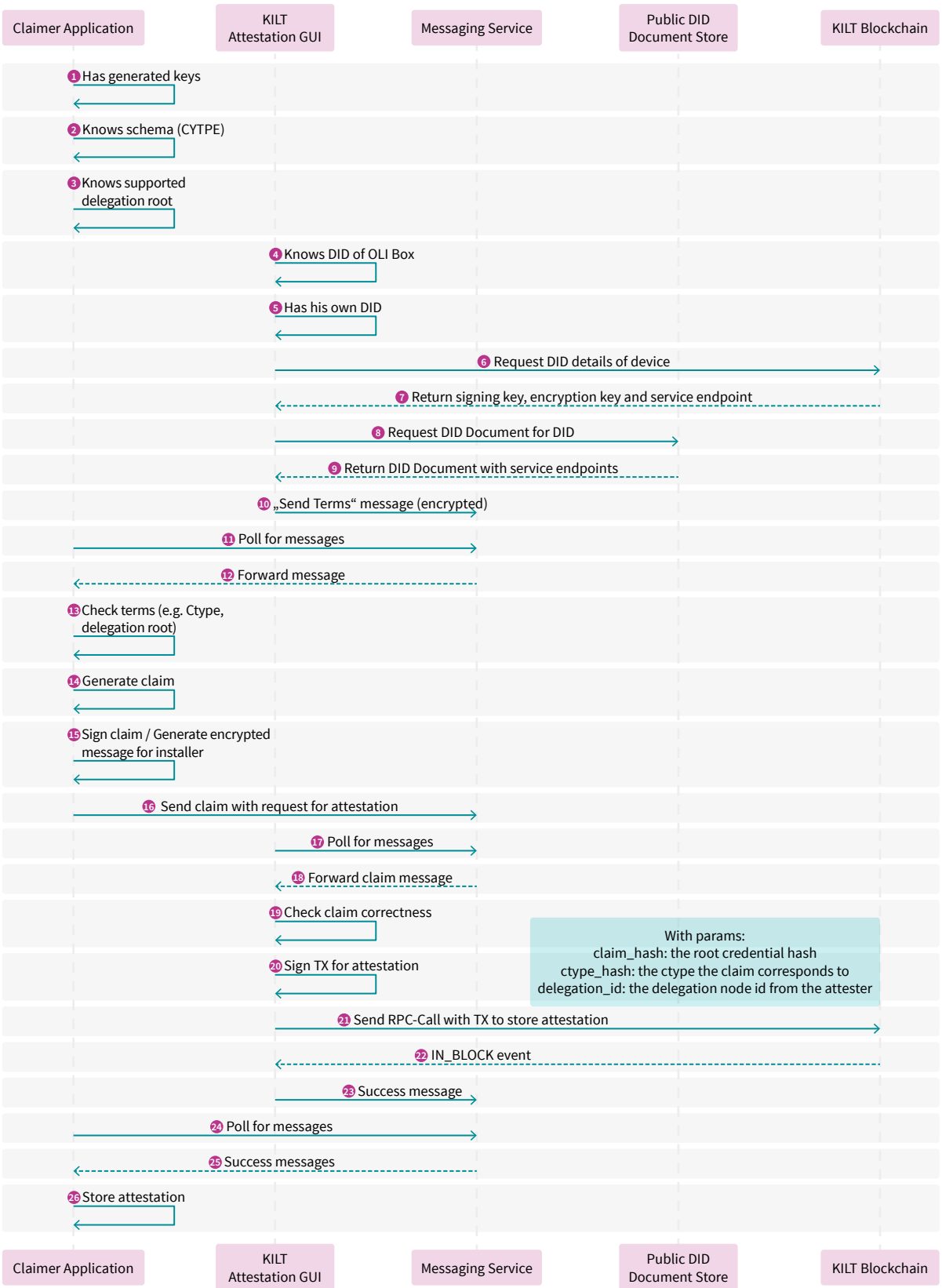


Abbildung 29: Sequenzdiagramm Ausstellung des Zertifikats BMILInstallationCredential (Quelle: Eigene Darstellung BOTLabs GmbH)

Ausstellung des Zertifikats EnergyWebRoleCredential

Die Applikation der Energy Web Foundation (EWF) stellt als Issuer des EnergyWebRoleCredential das Zertifikat aus und verankert es auf der Blockchain. Das Zertifikat wird direkt im Claim Store der OLI Box bzw. von YOUKI gespeichert.

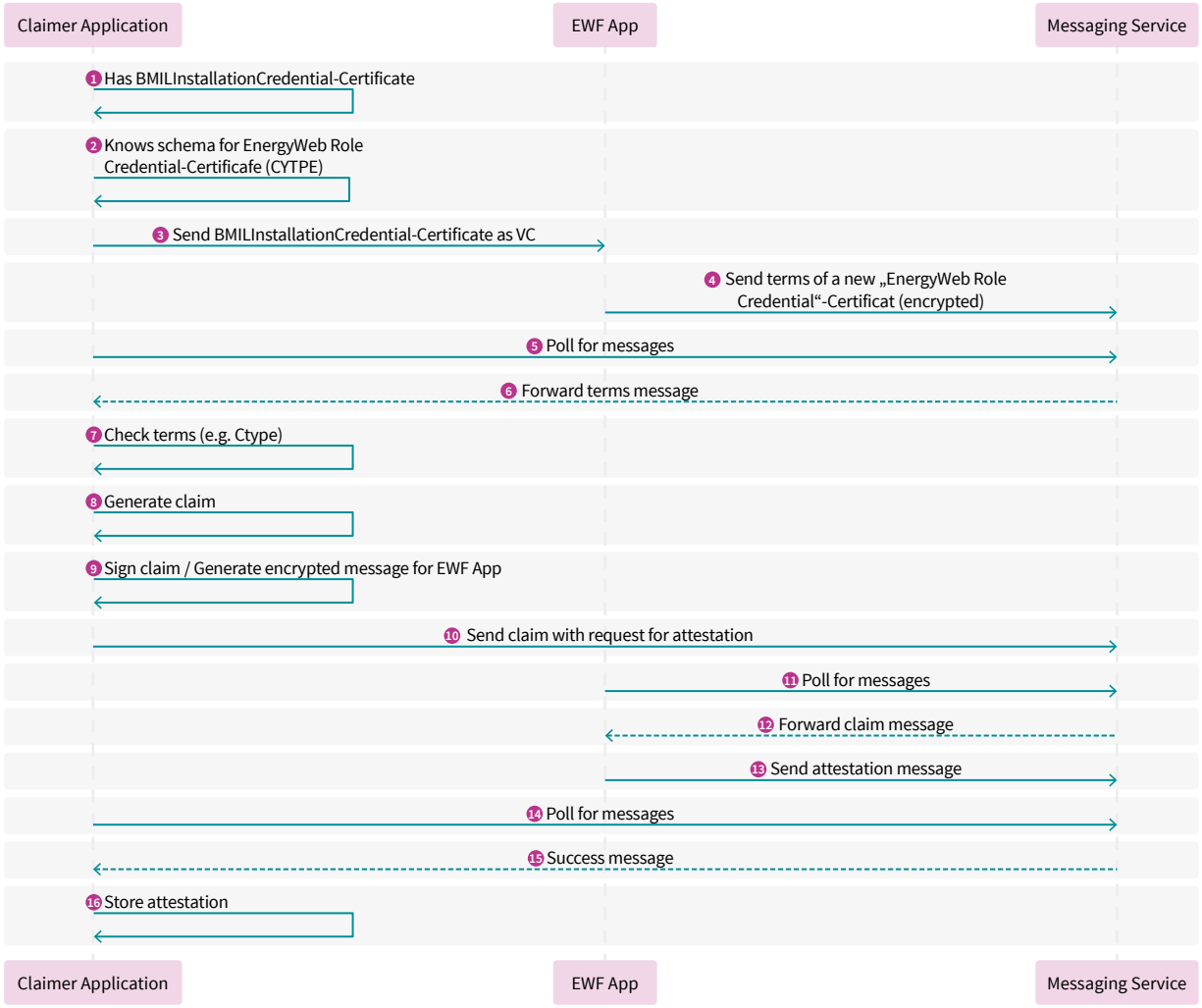


Abbildung 30: Sequenzdiagramm Ausstellung des Zertifikats EnergyWebRoleCredential (Quelle: Eigene Darstellung BOTLabs GmbH)

Erzeugung einer Delegationsstruktur

Das Recht zum Ausstellen von Zertifikaten eines bestimmten Zertifikatstyps kann von einer übergeordneten Stelle nach unten delegiert werden. Die Delegationsstruktur wird auf der Blockchain verankert, ist Teil des Zertifikats und kann vom Verifier geprüft werden.

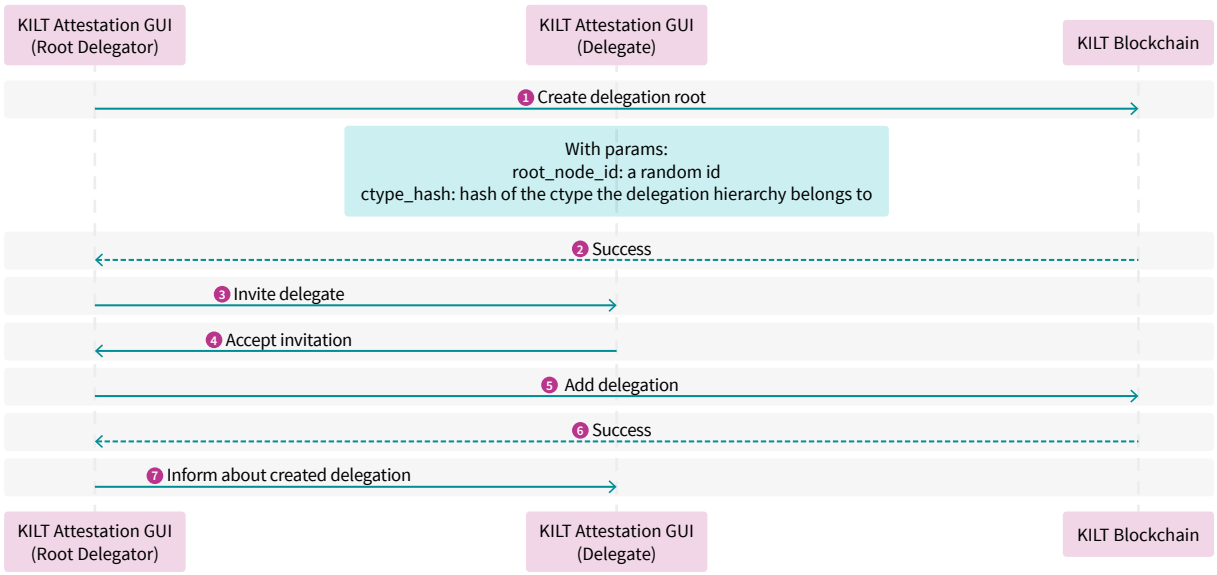


Abbildung 31: Sequenzdiagramm Erzeugung einer Delegationsstruktur (Quelle: Eigene Darstellung BOTLabs GmbH)

Invalidieren eines Zertifikats

Ein auf der Blockchain verankertes Zertifikat kann durch den Issuer des Zertifikats auf der Blockchain invalidiert werden.

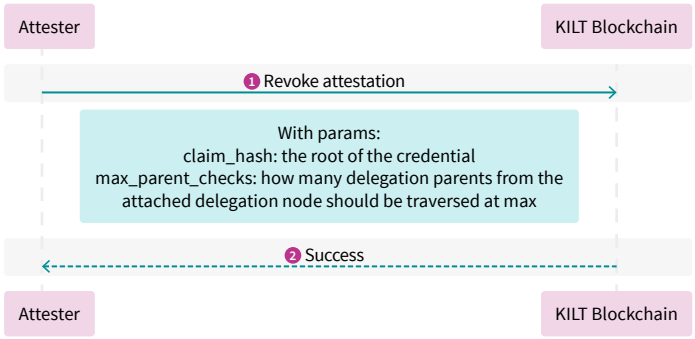


Abbildung 32: Sequenzdiagramm Invalidieren eines Zertifikats (Quelle: Eigene Darstellung BOTLabs GmbH)

Überprüfen eines Zertifikats

Das Gerät entscheidet, welche Attribute vom Zertifikat es mit dem Verifier teilt. Das Zertifikat enthält Informationen über die nicht geteilten Attribute, mit denen die kryptografische Integrität des Zertifikats sichergestellt werden kann.

Der Verifier überprüft, ob

- die gezeigten Attribute zu dem CTYPE passen
- der Digest vom „Selective Disclosure"-Algorithmus stimmt
- die Claimer-Signatur valide ist
- er dem Issuer des Zertifikats oder der Delegationsstruktur vertraut.

Der Verifier überprüft darüber hinaus, ob das Zertifikat auf der Blockchain verankert ist und nicht invalidiert wurde.

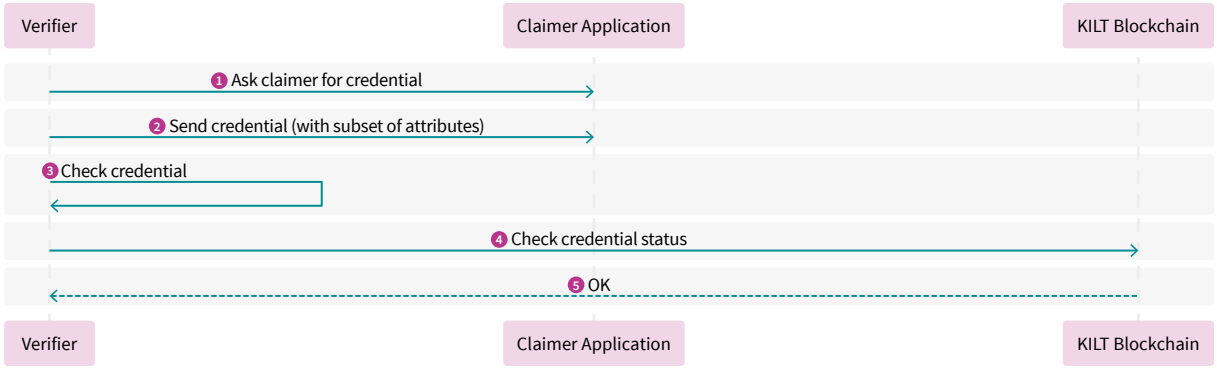


Abbildung 33: Sequenzdiagramm Überprüfen eines Zertifikats (Quelle: Eigene Darstellung BOTLabs GmbH)

4.1.5.4 Exemplarischer Autorisierungsprozess

Um die oben gezeigten Sequenzdiagramme zu veranschaulichen, wird im Folgenden ein Beispielprozess beschrieben. Basierend auf dem KILT-Ansatz und in Kooperation mit der Energy Web Foundation wurde ein exemplarischer Autorisierungsprozess umgesetzt, der eine mögliche Interaktion der verschiedenen Akteure und Systeme demonstriert. Der beschriebene Ansatz zur Vergabe der Basisdaten und Rollen kann als Beispiel für einen Autorisierungsprozess für die in Kapitel 5 aufgeführten Anwendungsfälle gesehen werden.

Ziel des Ansatzes ist es, einer Anlage ein Zertifikat auszustellen, um sie somit für die Nutzung in der EWF-Applikation zu präqualifizieren. Der hier beschriebene Prozess ist auch in diesem Video[63] dokumentiert.

Zur Umsetzung dieses Autorisierungsprozesses werden zwei Zertifikatsschemata, also zwei sogenannte Claim-Typen (CTYPEs), definiert und auf der KILT Blockchain erzeugt:

1. BMILInstallationCredential

- Owner
- facility_type
- registration_date
- deregistration_date
- zip_code
- city
- country
- latitude
- longitude
- nominal_capacity
- grid_connection
- name
- device_manufacturer
- device_serialnumber
- device_address
- device_sunspec_did

2. Präqualifizierung EWF

- role

Folgende Akteure werden mit einem Identifier auf der KILT Blockchain angelegt:

- Eine übergeordnete Instanz, die das Recht zur Ausstellung von Zertifikaten des CTYPE BMILInstallationCredential an eine untergeordnete Instanz delegiert
- Der Zertifikatsaussteller vor Ort (z. B. der Installateur, der die Anlage vor Ort in Betrieb nimmt),der das Zertifikat ausstellt

Diese Delegationsstruktur wird auf der KILT Blockchain gespeichert und kann dort verifiziert werden. Dies hat den Vorteil, dass Akteure, die auf das Zertifikat zugreifen, nur der übergeordneten Instanz vertrauen müssen und nicht jedem Installateur.

63 https://www.youtube.com/watch?v=ki0iBLwxPqA

Erzeugung des Identifier auf der OLI Box

Auf der OLI Box wird im ersten Schritt der Identifier bestehend aus einem Private / Public Key Pair generiert. Im Anschluss an die Generierung des Key Pair registriert die OLI Box ihren DID auf der KILT Blockchain. Das Erzeugen des Identifier, also das Generieren des Key Pair und das Registrieren des DID, könnte zum Beispiel schon beim Hersteller der Box durchgeführt werden.

Ausstellen des Zertifikats

Bei der Inbetriebnahme der OLI Box vor Ort stellt der Installateur als Zertifikatsaussteller das Zertifikat BMILInstallationCredential aus.

Dazu schickt er den vorausgefüllten Claim basierend auf dem CTYPE BMILInstallationCredential als Vorschlag an die OLI Box, wobei er die Device-spezifischen Angaben nicht einträgt, da diese von der Box zu einem späteren Zeitpunkt automatisch ergänzt werden. Bestandteil des vorausgefüllten Claims ist unter anderem auch die Delegationsstruktur, über die der Installateur das Zertifikat ausstellt. Die OLI Box prüft den Vorschlag hinsichtlich des CTYPE und der Delegationsstruktur. Bei erfolgreicher Überprüfung ergänzt sie die Device-spezifischen Informationen und schickt eine Anfrage zum Ausstellen des Zertifikats zurück an den Installateur. Dieser prüft die Angaben, stellt das Zertifikat aus und verankert es auf der KILT Blockchain. Die OLI Box speichert das Zertifikat bei sich im Claim Store ab.

Im nächsten Schritt wird das Zertifikat von der OLI Box als Verifiable Credential an die EWF-App geschickt.

Sobald das Credential von der EWF-App empfangen wurde, überprüft die App die Signatur des Ausstellers auf dem Credential und ob der Aussteller gemäß der CTYPE-Delegationsstruktur gültig ist. Das Credential wird dann mit dem Gerät in der EWF-App-Datenbank verknüpft und auf dem EV Dashboard zur Überprüfung durch den Administrator angezeigt.

EWF-App

Das EV Dashboard, das Energy Web zusammen mit der Elia Group vor dem BMIL-Projekt entwickelt hat, wurde so modifiziert, dass es neben den bereits vorhandenen Fahrzeugen und Ladepunkten auch die BMIL-Assets enthält und somit eine einheitliche Schnittstelle für Netzbetreiber wie die Elia Group bildet, um auf Geräte-Identitäten und -Attribute zuzugreifen. Diese Änderung zeigt, dass ein Blockchainübergreifender und Multi-DID-Methoden-Ansatz funktioniert und Lock-in Effekte vermeidet, die geschlossene Ökosysteme mit sich bringen. Ursprünglich (außerhalb des BMIL-Projekts) verwendet das EV Dashboard die Energy Web Chain und die did:ethr-Methode, um Fahrzeuge und Ladestationen zu adressieren.

Jetzt (als Teil des BMIL-Projekts) beinhaltet das Dashboard zusätzlich die KILT Chain und die did:kilt-Methode. Damit werden neben den bereits vorhandenen Fahrzeugen und Ladestationen auch die OLI Box und YOUKI Assets einbezogen.

Über das Dashboard können Geräteeigentümer ihre Assets registrieren und die Eintragung ihrer Geräte für bestimmte Anwendungsfälle beantragen. Jeder Anwendungsfall kann unterschiedliche Anforderungen haben. Es ist Sache des Eigentümers des Anwendungsfalls, zum Beispiel eines Netzbetreibers wie der Elia Group, diese Anforderungen zu definieren und durchzusetzen. Im Dashboard wird dies durch die folgenden Schritte umgesetzt:

- Eine „request enrollment“-Anfrage pro Gerät an den Eigentümer des Anwendungsfalls
- Überprüfung und Genehmigung der Identität des Geräts und der zugehörigen Attribute durch den Eigentümer des Anwendungsfalls
- Hinzufügen der genehmigten Registrierungsanfrage zur Brieftasche des Geräts

Nachdem diese Schritte einmal durchgeführt wurden, kann das Gerät nun dem Betreiber des Anwendungsfalls und jedem, der ihm vertraut, beweisen, dass es in der Lage und autorisiert ist, an dem Anwendungsfall teilzunehmen.

4.1.5.5 Genutzte Verschlüsselungs- und Hash-Algorithmen[64]

Zur Signierung nutzen wir im Projekt: Ed25519
Zur Verschlüsselung: Curve25519-XSalsa20-Poly1305
Es werden außerdem noch folgende Signatur-Algorithmen unterstützt:

- Sr25519
- Secp256k1

Als Hashing-Algorithmus wird „blake2“ genutzt.

64 https://substrate.dev/docs/en/knowledgebase/advanced/cryptography

4.1.5.6 Kompatibilitätslayer

Die KILT-DID-Methode, die im vorangegangenen Abschnitt erläutert wurde, ist mit dem bereitgestellten KILT SDK implementiert. Um die Interoperabilität der Verifiable Credentials zu gewährleisten, haben wir uns darauf verständigt, die Bibliothek vc-js[65] zu verwenden. So können die von KILT erzeugten Zertifikate auf der Seite von Energy Web gelesen und dem Anwender präsentiert werden. Darüber hinaus können so auch andere mittels vc-js erzeugte Verifiable Credentials gelesen werden.

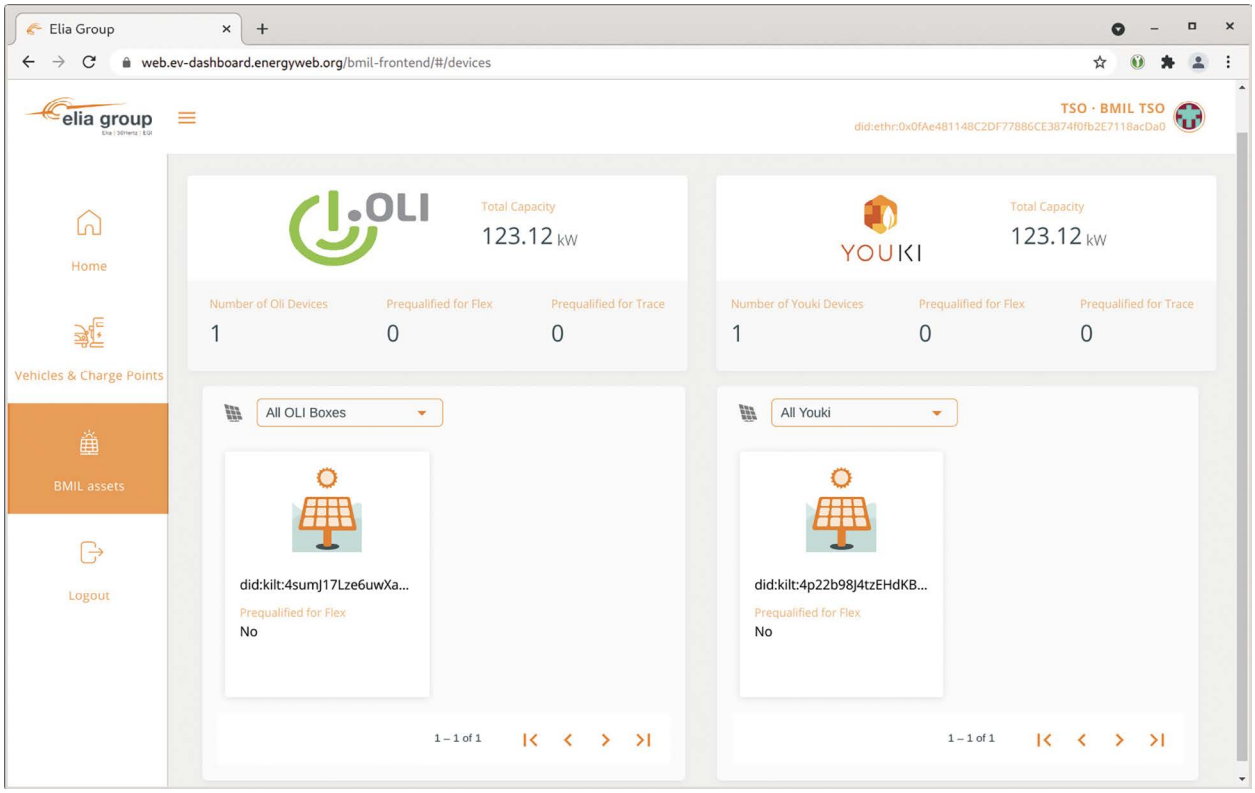


Abbildung 34: Die Anlagen von OLI Systems und YOUKI mit ihrer KILT-Identität im EV Dashboard

4.2 Cloud-Wallet-basierte Identitätsverwaltung

4.2.1 Beschreibung der Anbindungsvariante

Dieser Ansatz beschreibt eine Variante zur Erstellung eindeutiger elektronischer Identitäten für Energieanlagen, die auf einer Blockchain verankert werden. Als Blockchain oder Distributed Ledger kommt in diesem Ansatz Ethereum (permissioned) zum Einsatz.

4.2.1.1 Der Cloud-Edge-Ansatz

Dieser Ansatz beschreibt das Konzept der zweigeteilten Verantwortung eines Blockchain Machine Identity Ledger, bei dem der sicherheitskritische Teil der Verantwortung vom Smart-Meter-Gateway übernommen wird und der andere Teil von einer Cloud-Komponente. Der Ansatz implementiert eine sichere und effiziente Lösung für das dezentrale Energiesystem und die darin enthaltenen diversen Rollen, Geräte und Abhängigkeiten.

Bei der vorgestellten Lösung bleibt das Schlüsselmaterial auf der lokalen Geräteebene (Controllable Local System, CLS) und wird per BSI-zertifizierten Smart-Meter-Gateway an einen (vordefinierten) aktiven externen Marktteilnehmer (aEMT) übermittelt, der als nachgelagertes Gateway für die verschiedenen Services agiert. Das Management der Prozesse und die Business-Logik werden weitgehend in die Cloud verlagert. Dieser Ansatz wird auch Cloud-Edge-Ansatz genannt, wobei der Cloud-Teil oft als Digital Twin (digitaler Zwilling) referenziert wird.

Kapitel 4.2: Zu diesem Kapitel haben folgende Projektpartner beigetragen: OLI Systems, Spherity, PPC, GWAdriga

65 https://github.com/digitalbazaar/vc-js

Der Cloud-Edge-Ansatz ermöglicht es, folgende Szenarien abzudecken:

- **Offline-Betrieb:** Der Cloud-Edge-Ansatz ermöglicht, dass bestimmte Funktionen weiterhin verfügbar sind, auch wenn die CLS-Geräte selbst aktuell offline sind. Grundsätzlich kann man von der Cloud-Komponente schnellere Antwortzeiten erwarten als von einem iMSys und dem aEMT, die in privaten, abgeschlossenen Netzwerken stehen. Dadurch sind die Prozesse weniger anfällig für Störungen auf den teils langen und komplexen Übertragungswegen über verschiedene Infrastrukturen (LTE, Cloud, VPNs etc.)

- **Software-Updates:** Die Cloud-Komponente kann ohne Ausfallzeiten auf neue Softwareversionen migriert werden. Dies ermöglicht einen durchgängigen Betrieb der kritischen Infrastruktur und gleichzeitig das einfache Updaten neuer Funktionalitäten „onthe-fly".

- **Hardware-unabhängig:** Durch die Trennung von Cloud Edge ist auch eine Flexibilität bezüglich der Hardwareauswahl möglich. Im Projekt werden OLI Boxen stellvertretend für die Anlage genutzt; zusätzlich kann jede beliebige andere Hardware sowie die Anlagen selbst – ausgestattet mit der notwendigen Prozessorleistung – die Edge-Funktionen übernehmen.

- **Bulk Operations:** Um im Netzwerk einen möglichst gleichen Softwarestand zu pflegen, müssen die Geräte möglichst gleichzeitig aktualisiert werden. Durch den Cloud-Edge-Ansatz kann dies per Knopfdruck durch Massenaktualisierung (Bulk Operations) der Cloud-Komponenten erfolgen. Auch Netzwerkkonfigurationen können effizient per Bulk Operations durchgeführt werden.

- **Blockchain-unabhängig:** Durch die Zweiteilung der Verantwortung ist es möglich, die Smart-Meter-Gateways Blockchain-unabhängig bzw. interoperabel zu machen. Die Cloud Komponente übernimmt hier die Abstraktion zu den verschiedenen Distributed-Ledger-Technologien (DLT). Die Spherity Wallet ermöglicht es zum Beispiel, vom aktuell eingesetzten Ethereum auf Hyperledger Indy zu wechseln. Da sich DLTs aktuell noch stark weiterentwickeln, ist dies ein zukunftsorientiertes Konzept.

- **User Experience:** Die Cloud Agents der Anlagen bzw. der OLI Boxen lassen sich komfortabel in einem Dashboard darstellen, überwachen und verwalten. Auch kann von verschiedenen Geräten bzw. User Interfaces auf die Cloud Agents zugegriffen werden.

- **Tests, Simulationen und Prognosen:** Neue Funktionalitäten, wie zum Beispiel die Einführung von Grünstromzertifikaten, können per Cloud-Umgebung einfach getestet werden. Nach veränderter Software kann die Netzsicherheit mit digitalen Zwillingen getestet werden, bevor eine Live-Schaltung erfolgt. Auch Simulationen zur Netzoptimierung und hinsichtlich von Flexibilitäten können mit Klonen der digitalen Zwillinge durchgeführt werden. Entsprechend der GAIA-X-Vision[66] ist es möglich, Prognosen über die Entwicklung der Energienetze zu entwickeln.

- **Key Management:** Durch den Cloud-Edge-Ansatz stehen verschiedene Key-Management-Lösungen zur Verfügung. Durch den Key-Delegationsmechanismus ist es zum Beispiel möglich, bestimmte Operationen dem digitalen Zwilling zu übertragen. Das bedeutet, dass die Cloud-Komponente im Namen der Anlage handeln kann. Ermöglicht wird dies durch einen kryptografischen Vorgang, der den öffentlichen Schlüssel der Cloud-Komponente mit dem der Anlage (bzw. stellvertretend der OLI Box) verknüpft. Key-Delegation ist ein wesentlicher Teil dieser Lösung und wird später im Detail beschrieben.

Die oben genannten Eigenschaften des Lösungsansatzes entschärfen die Limitationen eines „Edge only"-Konzepts wie geringere Bandbreite und Verfügbarkeit, eingeschränkte Rechenleistung, schwierigere Software-Updates vor allem aus Sicherheitsgründen und neu durchzuführende BSIZertifizierung.

4.2.1.2 Die Edge-Komponente: OLI Box und SMGW / iMSys

Die Edge-Komponente auf der lokalen Geräteebene wird im BMIL durch die Kombination der eigentlichen Energieanlage (zum Beispiel PV-System, Batterie, E-Fahrzeug usw.), einer OLI Box, dem CLS-GW und dem SMGW dargestellt. Die OLI Box agiert als Kommunikationseinheit für die Anlage, die diese Funktion selbst zumeist nicht übernehmen kann. Das CLS-GW und das SMGW von PPC übernehmen die Kommunikation zum aktiven externen Marktteilnehmer (aEMT), der von GWAdriga gestellt wird.

Die iMSys-Komponenten kommunizieren in der Test-PKI und bilden sämtliche Prozesse korrekt nach der BSI-Richtlinie TR-03109 ab. Die Kommunikationsprozesse laufen ausschließlich über die HANKommunikationsszenarien (HKS) und werden vom Smart-Meter-Gateway-Administrator gehandelt. Das CLS-GW, das SMGW und der aEMT sind vollständig konfiguriert und mit den notwendigen Zertifikaten ausgestattet.

66 https://www.bmwi.de/Redaktion/DE/Publikationen/Schlaglichter-der-Wirtschaftspolitik/schlaglichter-der-wirtschaftspolitik-09-2020.html

Die Vorteile der Nutzung des Smart-Meter-Gateway und des dazugehörigen WAN für die Kommunikation ergeben sich aus folgenden Punkten:

- Von staatlichen Behörden bereits zertifizierte sichere Kommunikationsstrecke mit definierten Start- und Endpunkten inklusive SM-PKI-basierter Integritätsmechanismen, aufbauend auf bestehenden energiewirtschaftlichen Prozessen (z. B. Tarifanwendungsfälle) und Datenendpunkten (SMGW-ID, Zähler-ID, Messlokation usw.)

- Kostensparende Mehrfach- und Mehrzwecknutzung des ohnehin vorhandenen intelligenten Messsystems; keine zweite Kommunikationsstrecke notwendig, was die Komplexität reduziert und die ökonomische (und auch ökologische) Bilanz weiter verbessert

- Abgeschlossenes informationstechnisches und IP-basierendes Energienetzwerk vor Ort mit eigenen, spezifizierten Regeln, was die Akzeptanz im Vergleich zur „FritzBox-Haushalt-LAN / HAN-Lösung“ weiter erhöht; Stichwort: „Verplombung“

Die OLI Boxen verfügen über ein Hardware Secure Module (umgangssprachlich auch „Kryptochip“ genannt), das bestimmte kryptografische Operationen durchführen kann. Durch die Nutzung dieser weiteren, dedizierten Hardwareplattform wird das Sicherheitsniveau weiter angehoben. Das HSM ist auch tatsächlich von der eigenen OLI-Box-Platine physisch getrennt und nur über eine API erreichbar. Funktional sind die Operationen auch auf Softwarebasis möglich, jedoch vermehren sich dadurch die Angriffsvektoren.

4.2.1.3 Die Cloud-Komponente: Spherity Cloud Identity Wallet

Die Spherity Cloud Identity Wallet, in den folgenden Diagrammen als „Cloud API“ referenziert, ist eine Cloud-basierte Technologie-Suite, die eine sichere Kommunikation zwischen Firmen, Maschinen und Personen und deren digitalen Identitäten ermöglicht.

Die Spherity Cloud Identity Wallet implementiert folgende für diesen Use Case relevante Funktionen:

- Ein Wallet-Nutzer kann gemäß dem W3C-Standard „Decentralized Identifiers“[67] eine digitale Identität erstellen und sie auf der Blockchain verankern. In unserer Variante erhalten die Anlage (bzw. die OLI Box), der Manufacturer und der Installateur eine digitale Identität und eine dazugehörige Wallet-Instanz.

- Ein Wallet-Nutzer kann in alle Rollen des W3C-Standards „Verifiable Credentials“[68] schlüpfen, nämlich Issuer, Holder und Verifier, und somit Zertifikate ausstellen, signieren, erhalten, vorzeigen und verifizieren (siehe Abbildung 35).

- Ein Wallet-Nutzer, zum Beispiel der Manufacturer, kann mit anderen Wallets, zum Beispiel dem Installer, kommunizieren (beispielsweise via DIDComm-Protokoll[69]).

- Neben den grundsätzlichen Funktionen sind auch weiterführende Funktionen verfügbar, die in den oben genannten Standards definiert sind, zum Beispiel Credential Revokation, Credential Chaining und die für diesen Anwendungsfall wichtige Key-Delegation zum Etablieren des digitalen Zwillings. Neben der Ethereum-Blockchain könnten die Identitäten auch auf Hyperledger Indy / Sovrin oder Quorum abgelegt werden.

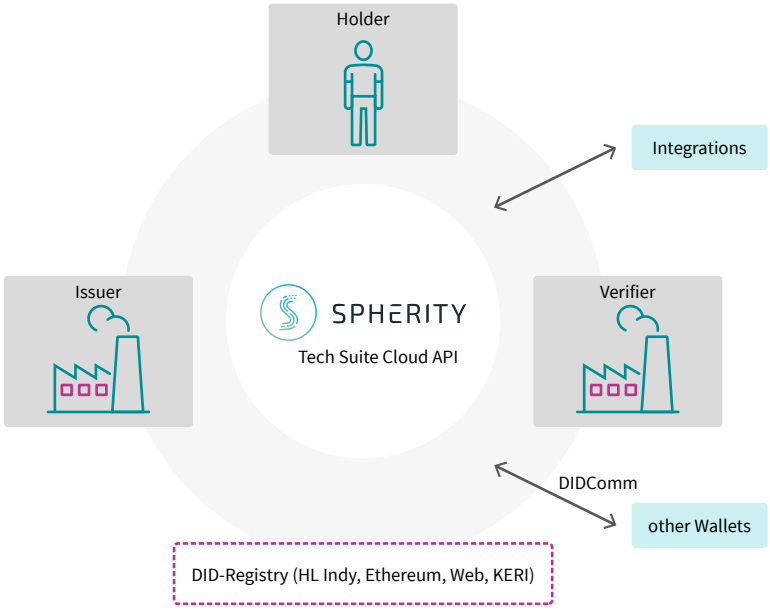


Abbildung 35: Die Spherity Cloud Identity Wallet (Quelle: Eigene Darstellung Spherity GmbH)

67 Decentralized Identifiers (DIDs) v1.0, https://www.w3.org/TR/did-core/
68 Verifiable Credentials Data Model 1.0, https://www.w3.org/TR/vc-data-model/
69 DIDComm Messaging, https://identity.foundation/didcomm-messaging/spec/

4.2.2 Systemsicht der Anbindungsvariante

Die Systemsicht gibt einen Überblick über die eingesetzten Systeme auf höchster Ebene.

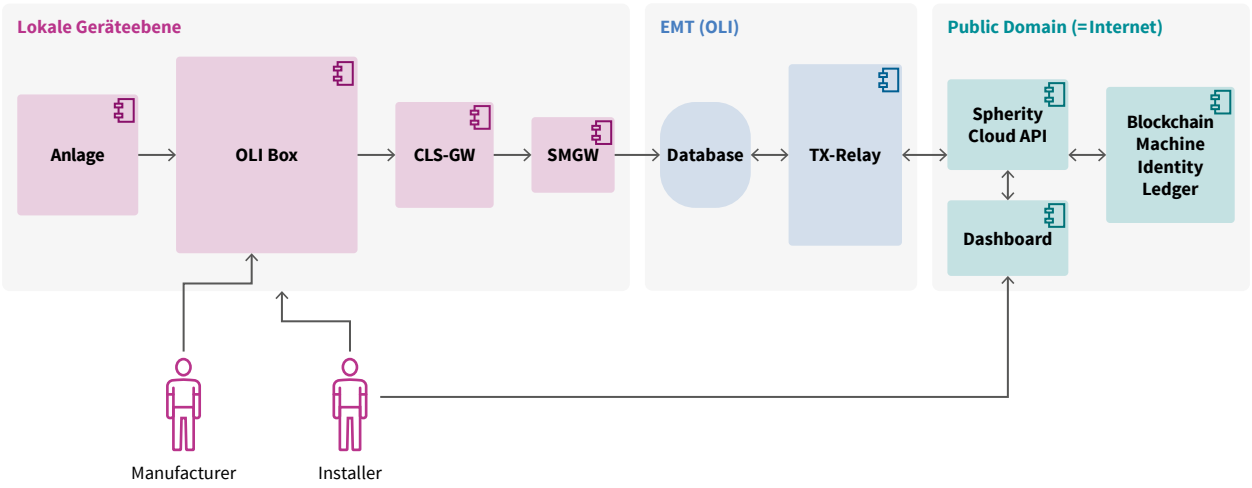


Abbildung 36: Systemsicht „Cloud-Wallet-basierte Identitätsverwaltung“ (Quelle: Eigene Darstellung OLI Systems GmbH)

Aus der Systemsicht sind drei Bereiche sichtbar:

- Die **Lokale Geräteebene** bildet die Haus- und Anlagenelektrik sowie das informationstechnische, IP-basierende Netzwerk ab.
- Der **externe Marktteilnehmer (EMT)** ist in der iMSys-Architektur ein potenzieller, in das WAN eingebundener Kommunikationspartner des SMGW. Der in die Test-PKI integrierte aktive EMT (aEMT) kann im Gegensatz zu einem rein passiven EMT neben dem Datenempfang (z. B. über Tarifandwendungsfälle) auch Steuerbefehle initiieren. Beispiele für EMTs sind etwa Aggregatoren, Lieferanten, Netzbetreiber oder Messstellenbetreiber.
- Die **Public Domain** kann umgangssprachlich in diesem Kontext auch als „Internet“ bezeichnet werden. Es handelt sich um Dienste, die nicht in abgeschlossenen, lokalen Netzwerken installiert sind, jedoch meist mit einer Authentifizierung bzw. einem API-Key gesichert sind. In der Public Domain befinden sich die Spherity Cloud Identity Wallet sowie die Blockchain, die von der Spherity Cloud Identity Wallet angesteuert wird und auf der Maschinen-Identitäten verankert werden.

4.2.3 Building-Block-Sicht der Anbindungsvariante

Die Building-Block-Sicht geht auf die nächste Detailebene herunter. Hier sind auch Teilsysteme der Lösung sichtbar. Abbildung 20 und Abbildung 22 zeigen den Installationsaufbau der lokalen Geräteebene auf der Basis der OLI Box in Verbindung mit einem PV-Wechselrichter sowie der Installation einer OLI Box und eines iMSys in einem Laboraufbau im Smart-Grid-Labor der Technischen Hochschule Ulm.

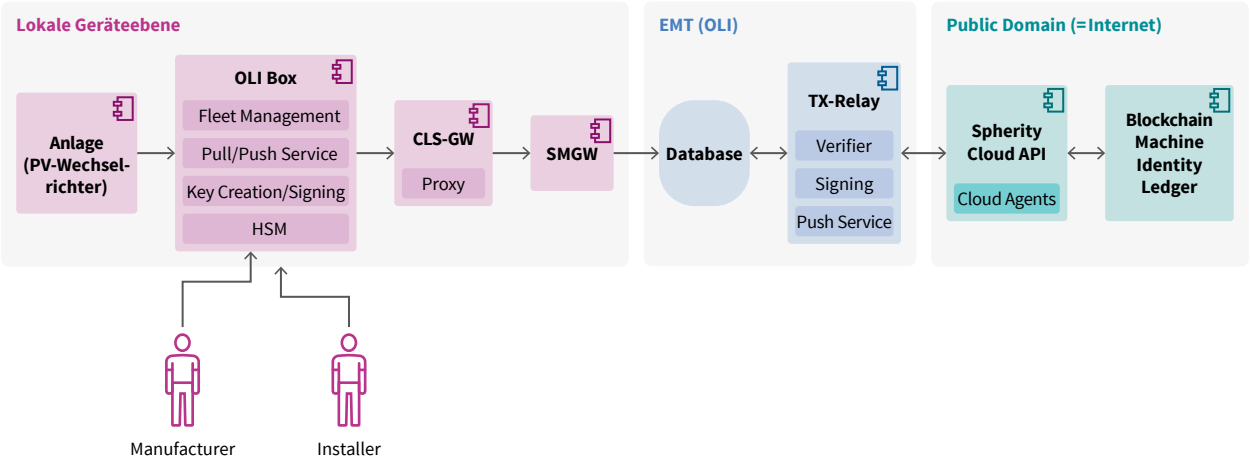


Abbildung 37: Building-Block-Sicht „Cloud-Wallet-basierte Identitätsverwaltung"

4.2.3.1 Anlage

Bei der Anlage handelt es sich um eine Energieanlage, die eine Identität mithilfe der BMIL-Lösung verliehen bekommen soll. Beispiele hierfür sind unter anderem eine PV-Anlage bzw. der dazugehörige Wechselrichter, eine Batterie und Steuerelektronik, eine Wärmepumpe, eine Ladesäule oder eine Wallbox.

4.2.3.2 OLI Box

Die OLI Box ist ein speziell für den Energiesektor konfigurierter Einplatinencomputer auf Basis des Raspberry Pi 3B. Je nach Einsatzort und -zweck erfüllt die OLI Box verschiedene Aufgaben. Darunter fallen die Datenerfassung an den verschiedenen Anlagen und Zählern, die Datenprozessierung und -aufbereitung sowie der Versand der Datenpakete in der Rolle eines Gateways. Im Kontext des BMIL übernimmt die OLI Box die notwendigen zusätzlichen Funktionen für die Anlage. Perspektivisch kann der Code, der sich derzeit auf der OLI Box befindet, in die Anlage bzw. deren Steuermodul oder deren Prozessor migriert werden, sollten diese in Zukunft die notwendigen Anforderungen erfüllen. Der Code ist im Falle des BMIL in Python geschrieben und läuft auf einer leicht modifizierbaren Debian-Distribution.

Fleet Management

Bei dem Fleet Management handelt es sich um eine Softwarekomponente auf der OLI Box, die insbesondere während der Debugging- und Entwicklungsphase benötigt wird. Sie übernimmt neben der Übertragung des Health-Status (Geräte online / offline, derzeitige IP und weitere Parameter) auch die Bereitstellung eines SSH-Kanals (Secure Shell) über den Port 22 – selbst bei Firewalls und dynamischen IPs. Insbesondere im Laborumfeld ist das Teilen des Zugriffs mit Projektpartnern eines der wichtigsten Features.

Das derzeitige Fleet Management kann – je nach Art und Weise der Instandhaltung der OLI Box – auch im Produktivbetrieb genutzt werden. Jedoch sollte dann insbesondere der SSH-Zugriff stark eingeschränkt bzw. ganz unterbunden und stattdessen ein Postfach-System eingesetzt werden.

Pull / Push Service und Signing

Der Pull Service auf der OLI Box ist ein zyklisch ablaufender Cronjob, der in konfigurierbaren Zeitabständen die im Beispiel des BMIL auf dem Modbus-TCP-Register (SunSpec) basierenden Daten der Anlage ausliest (Pull). Die Daten werden daraufhin in eine JSON-Datei geschrieben und lokal in der OLI Box abgelegt. Welche Daten die Anlage übergeben kann, variiert stark vom Anlagentyp und Hersteller sowie von der Art und Implementierungsform der Schnittstelle selbst. Neben dem Pulling führt der Service zum jeweiligen Zeitpunkt auch ein Pushing durch, bei dem eine vom HSM signierte Commissioning Notification an das CLS-GW übermittelt wird. Das CLS-GW führt dann die weitere Kommunikation über das SMGW hin zum EMT durch.

Hardware Secure Module (HSM)

Die OLI Boxen verfügen über ein Hardware Secure Module (umgangssprachlich auch „Kryptochip" genannt), das bestimmte kryptografische Operationen durchführen kann. Durch die Nutzung dieser zusätzlichen, dedizierten Hardwareplattform wird das Sicherheitsniveau weiter angehoben. Das HSM ist auch tatsächlich physisch von der eigenen OLI-Box-Platine getrennt und nur über eine API erreichbar. Funktional wären die Operationen auch auf Softwarebasis möglich, jedoch vermehren sich dadurch die Angriffsvektoren. Im BMIL kam die Hardware HSM6 des Herstellers Zymbit zum Einsatz. Hierbei handelt es sich um eine Plattform im Beta-Status, sprich: eine Entwicklungsum-

gebung, wobei sowohl die Hardware als auch die Software im HSM noch nicht final sind. Zu den im BMIL in Frage kommenden Funktionen des HSM6 gehören:

- **Entropie für Private-Key-Erstellung:** Viele softwarebasierte Libraries haben Schwächen bei der RNG (Random Number Generation), da die internen Zahlen- und Zufallsbereiche nicht das volle mögliche Spektrum abdecken. Durch die eingeschränkte Entropie vieler Libraries erhöht sich die Gefahr durch Brute-Force-Angriffe. Das HSM verfügt über eine eigene hardwarebasierende Entropie, um diesem Problem entgegenzuwirken.

- **Key Storage:** Neben der Generierung der Private Keys kann ein HSM diese auch intern abspeichern und agiert dadurch ähnlich wie ein Hardware Wallet. Die Private Keys verlassen dabei das HSM nicht.

- **Signing:** Wenn die Private Keys in dem HSM abgelegt sind, muss der Chip auch zum eigenständigen Signieren von Nachrichten fähig sein. Diese Funktion ist für eine kleine Zahl an Kurven verfügbar, darunter nun auch in dem neuesten Beta-Release von Zymkey, der „Koblitz“ secp256k1, die von Ethereum und Bitcoin genutzt wird. Im BMIL wurden sowohl software- wie auch hardwarebasierende Signing-Vorgänge genutzt.

4.2.3.3 CLS-GW und SMGW

Das CLS-GW (Controllable Local System Gateway) und das Smart-Meter-Gateway (SMGW) von PPC sollen an dieser Stelle zusammen beschrieben werden. Beide Geräte (und darüber hinaus auch der aEMT) sind mit den nach der BSI-Richtlinie TR-03109 vorgeschriebenen Zertifikaten und Konfigurationen ausgestattet und bilden korrekt und praxisnah die Kommunikation über den CLS Kanal ab. Das SMGW ist in unserem Fall mit einem LTE-WAN ausgestattet und kommuniziert im BMIL über die Test-PKI der GWAdriga Smart Energy CA. Das CLS-GW bildet eine Brücke zwischen dem lokalen Home Area Network (HAN) und der HAN-CLS-Schnittstelle des SMGW, sodass faktisch zwei getrennte Netzwerke vorliegen.

Die OLI Box und andere Geräte können auf einer vorkonfigurierten IP sowie auf einem vorkonfigurierten Port einen Proxy erreichen, der über einen HTTP-POST eine (signierte) Nachricht (zum Beispiel die Commisioning Notification) an den EMT (TLS-Kanal) übermittelt. Das CLS-GW sorgt dabei für den Kommunikationsaufbau über HKS3 und die Abbildung der notwendigen Protokolle nach der TR-03109.

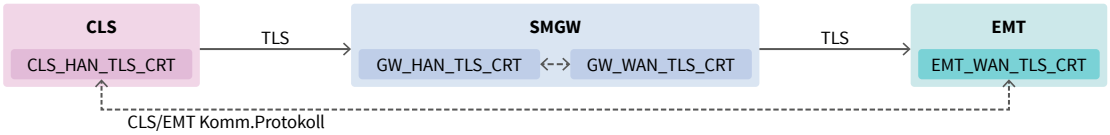


Abbildung 38: HKS3-Ablauf aus der TR-03109 (Quelle: Technische Richtlinie BSI TR-03109-1 Anforderungen an die Interoperabilität der Kommunikationseinheit eines intelligenten Messsystems Version 1.1 (2021))

4.2.3.4 Externer Marktteilnehmer (aEMT)

Der aktive externe Marktteilnehmer erhält per HTTP-POST über den TLS-Kanal die von der OLI Box und vom Installateur signierte Commissioning Notification in Stage #2. Der aEMT führt daraufhin einen Verifikationsprozess der Nachricht durch und stellt sie bei Erfolg inklusive der Signaturen als Verifiable Credential über die Spherity Cloud API aus. Je nach Ausgestaltung der Cloud API können weitere Prozesse in das TX-Relay beim aEMT integriert werden. Das Relay sollte zum Beispiel in jedem Fall die signierten Nachrichten der Anlagen überprüfen (verify). Außerdem kann der aEMT selbst auch als weiterer Akteur in die SSI-Umgebung eingebunden werden und Teil der Trust-Kette werden.

Im Rahmen des BMIL wird der aEMT von GWAdriga gestellt. Eine Datenbank (hier ein FTP-Server) innerhalb der EMT-Umgebung speichert die Nachrichten aus der lokalen Geräteebene ab. Die Datenbank wird daraufhin in die OLI-Umgebung gespiegelt und die weiteren Prozesse werden dort abgebildet.

4.2.3.5 Spherity Cloud API

Die Spherity Cloud API ist der Zugang für die Cloud Agents der verschiedenen Akteure. Für diesen Use Case werden die Cloud Agents OLI Box, Manufacturer und Installer instanziiert. Jeder dieser Agents ist eine eigenständige Instanz und kann Verifiable Credentials anfordern, ausstellen, verifizieren, abspeichern usw. Dies wird später in den Sequenzdiagrammen näher erklärt.
Die Spherity Cloud API verwaltet auch den Zugriff auf die Blockchain, sie erstellt zum Beispiel das DID-Dokument mit der Identity der Anlage und legt es auf dem Machine Identity Ledger ab.

4.2.3.6 Machine Identity Ledger / Blockchain

Der Machine Identity Ledger ist in dieser Anwendungsvariante eine permissioned Ethereum-Blockchain. Da die Spherity Cloud Identity Wallet Blockchain-unabhängig ist, könnte auch eine andere Blockchain eingesetzt werden. Da sich der Bereich der Blockchain-Technologie noch sehr stark entwickelt, ist dies eine zukunftsorientierte Lösung.

Der Machine Identity Ledger dient allein dazu, die Identität der Anlage zu verankern. Die vom Manufacturer, von der OLI Box und vom Installateur ausgestellten Verifiable Credentials werden nicht auf der Blockchain gespeichert, sondern in deren Wallets bzw. einem Credential Store. Dies hat den Vorteil, dass nicht jeder die Credentials einsehen kann und damit, trotz Verankerung der Identität auf der Blockchain, ein höchstmöglicher Datenschutz gewährleistet werden kann.

4.2.4 Datenflusssicht der Anbindungsvariante

Die Sequenzdiagramme für die Cloud-Edge-Integration der OLI Box sind mit den relevanten Partnern (OLI Systems, GWAdriga, PPC) finalisiert worden. Die folgenden Sequenzdiagramme zeigen den Ablauf der Erstellung des Machine Identity Ledger. Zuvor wurden eine Spherity Cloud Identity Wallet für die Akteure und eine Ethereum-Blockchain in der Open Telecom Cloud aufgesetzt.

Die Funktion der Implementierung beinhaltet das Erzeugen des digitalen Zwillings und dessen Verankerung auf dem Machine Identity Ledger während des Herstellungsprozesses der OLI Box. Anschließend stellt der Hersteller ein Masterdata-Zertifikat über die OLI Box aus, das die Gerätedaten der OLI Box (nicht der Anlage) enthält. Im nächsten Schritt wird die Inbetriebnahme vom Installateur angestoßen. Dabei stellt die OLI Box Informationen, die sie automatisch von der Anlage auslesen kann, zunächst als Commissioning Notification und dann als Inbetriebnahme-Zertifikat bereit. Jetzt werden vom Installateur Angaben zum Beispiel über den Ort und die Zeit der Installation gemacht und als Installations-Zertifikat ausgestellt. Damit ist die ordnungsgemäße Installation der Anlage abgeschlossen.

Das folgende Sequenzdiagramm (Stage #1) zeigt das Erzeugen und Verankern der dezentralen Identität der Anlage. Dies wird von dem Hersteller (Manufacturer) der OLI Box während der Herstellung des Geräts vorgenommen. Außerdem wird zu diesem Zeitpunkt auch das Masterdata Verifiable Credential (Gerätestammdaten-Zertifikat) für die OLI Box erzeugt.

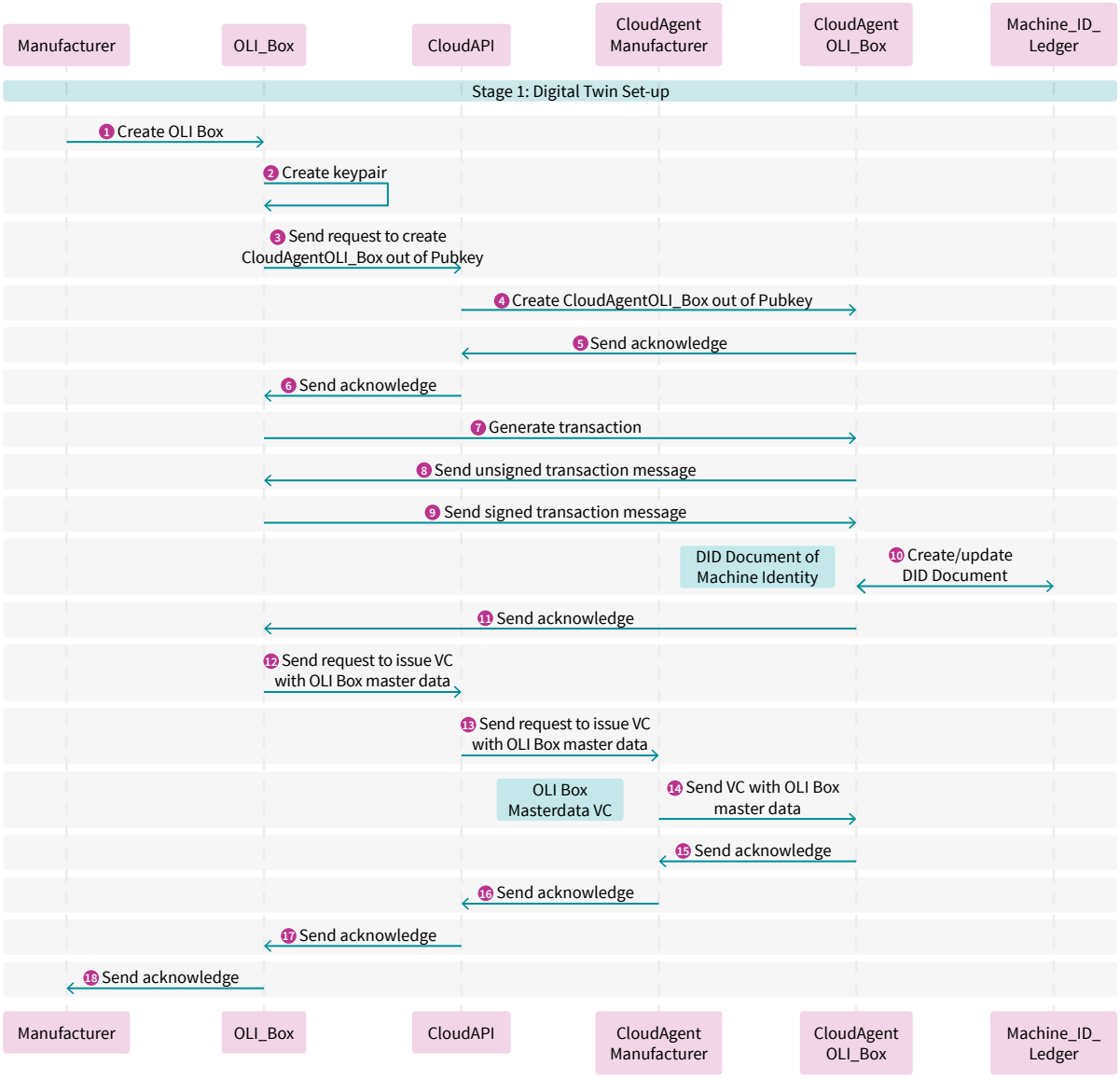


Abbildung 39: Sequenzdiagramm Erzeugen des digitalen Zwillings für den Cloud-Edge-Ansatz und Verankerung des neuen DID-Dokuments auf dem Machine Identity Ledger (Quelle: Eigene Darstellung OLI Systems GmbH)

Detaillierte Beschreibung der Schritte des Sequenzdiagramms „Aufsetzen der Cloud-Identität und Verankerung auf dem Machine Identity Ledger“:

Vorbedingung: Der Manufacturer besitzt einen eigenen Cloud Agent und ist in der Lage, der OLI Box Verifiable Credentials auszustellen.

1. Der Hersteller produziert das CLS-Gerät: In unserem Projekt ist der Hersteller OLI Systems und die OLI Box ist das CLS-Gerät.

2. Auf dem HSM (Hardware Security Module) der OLI Box wird nun das asymmetrische Schlüsselpaar erstellt. Es besteht aus einem öffentlichen und einem privaten Schlüssel. Der private Schlüssel verlässt die OLI Box (bzw. das HSM) nie.

3. Nun initiiert die OLI Box das Erstellen des digitalen Zwillings in der Spherity Cloud und spricht hierzu die entsprechende Cloud API des Spherity Cloud Wallet Service an.

4. Die Cloud API erstellt den OLI Box Cloud Agent. Hierbei handelt es sich um eine voll funktionsfähige Wallet, die Holder-, Verifier- und Issuer-Funktionalitäten hat.

5. bis 6.
Message 5 und 6 bestätigen der OLI Box den erfolgreich durchgeführten Schritt 4.

7. Hier wird eine rohe Transaktion für eine Blockchain-Transaktion generiert, die dem digitalen Zwilling der OLI Box das Recht gewährt, im Namen der OLI Box Nachrichten zu unterschreiben.

8. Diese rohe Transaktion wird an die OLI Box gesendet mit der Bitte, sie zu unterschreiben.

9. Hier wird die Nachricht von der OLI Box mit dem privaten Schlüssel signiert und an die Blockchain gesendet.

10. Somit kann der Cloud Agent der OLI Box das DID-Dokument auf dem Machine Identity Ledger verankern, in dem nun der öffentliche Schlüssel der OLI Box sowie auch der öffentliche Schlüssel des OLI Box Cloud Agent (auch Delegation Key genannt) publiziert wird.

11. Der Cloud Agent der OLI Box bestätigt der OLI Box den erfolgreich durchgeführten Schritt 10.

12. Dieser und die folgenden Schritte dienen der Zuordnung der Gerätestammdaten der OLI Box durch ein Masterdata VC. Dies kann neben dem technischen Beweis der Zugehörigkeit als logischer oder thematischer Beweis für die Verbindung von digitalem Zwilling und OLI Box betrachtet werden.

13. Hier wird der Request an den Cloud Agent des Manufacturer weitergeleitet, damit dieser das VC ausstellen kann.

14. Der Cloud Agent des Manufacturer stellt das Masterdata Verifiable Credential an den Cloud Agent der OLI Box aus.

15. bis 18.
    Schritt 15 bis 18 melden das insgesamt erfolgreiche Anlegen des digitalen Zwillings der Anlage auf dem Machine Identity Ledger an die Cloud API, die OLI Box und den Manufacturer OLI Systems zurück.

Das folgende Sequenzdiagramm (Stage #2) zeigt den wichtigen Durchstich von der BSI-zertifizierten Anlagenebene zur Cloud-Umgebung. Stage #2, die verifizierbare Installation, wird durch den Installateur angestoßen. Zunächst wird die Commissioning Notification initiiert. Nach erfolgreichem Erhalt der Notification auf dem EMT wird ein Commissioning Verifiable Credential (Inbetriebnahme-Zertifikat) vom Cloud Agent des Installateurs erstellt. Dieser wichtige Schritt weist nach, dass die Informationen direkt von der Anlage kommen und nicht modifiziert wurden. In der gleichen Form können später Messdaten verifizierbar als VC erzeugt werden. Im letzten Schritt stellt der Installateur das Installation Verifiable Credential (Installations-Zertifikat) aus.

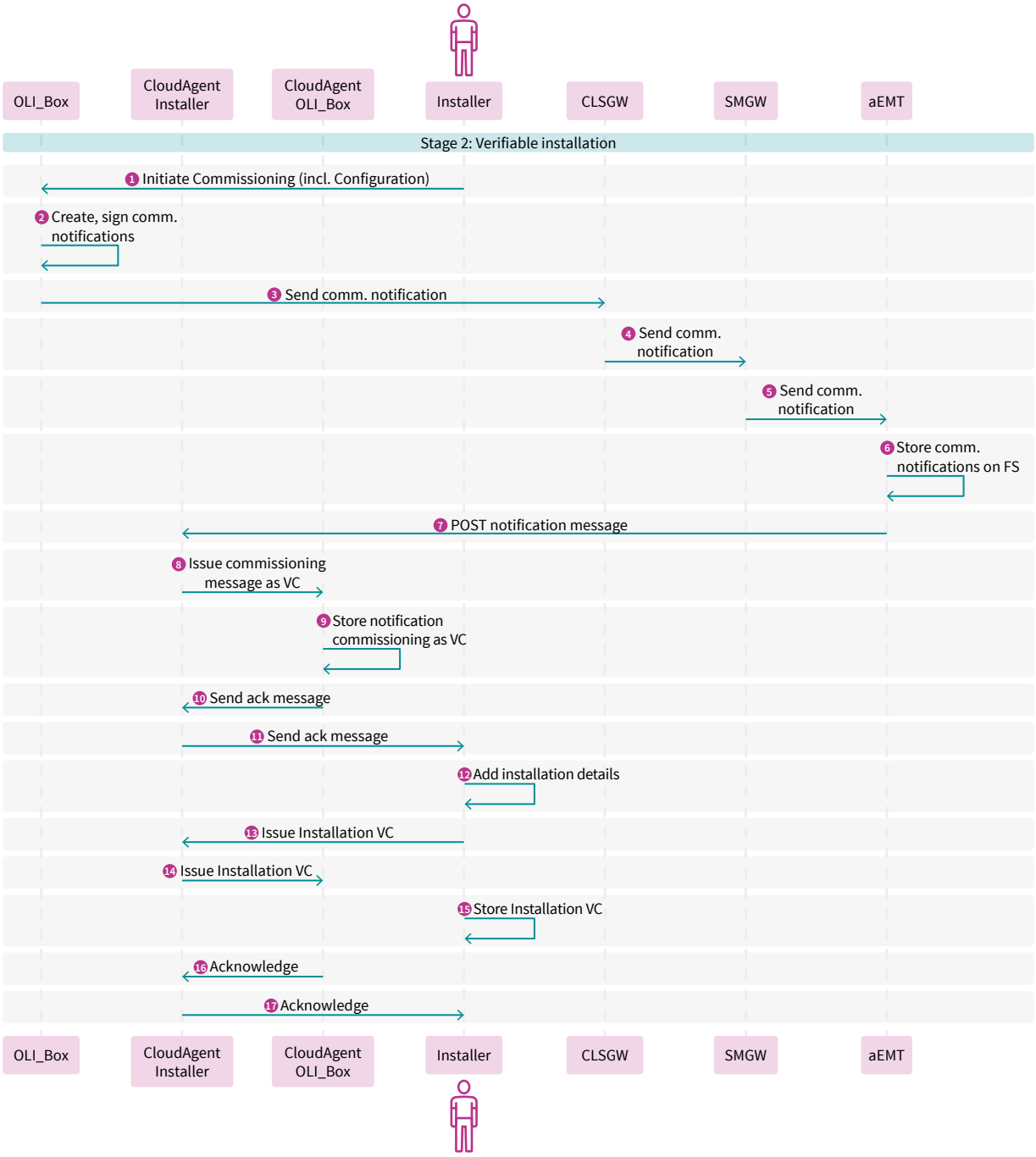


Abbildung 40: Sequenzdiagramm Durchführen der verifizierbaren Installation (Quelle: Eigene Darstellung OLI Systems GmbH, Spherity GmbH)

1. Der Installateur installiert die OLI Box vor Ort. Zunächst stößt er die Erzeugung der Inbetriebnahmedaten an.

2. Die OLI Box liest jetzt per Skript die Inbetriebnahmedaten der Anlage aus, erstellt daraus eine Nachricht und signiert sie mit dem Private Key der OLI Box (bzw. der Anlage).

3. Die OLI Box sendet die signierte Commissioning Notification über den BSI-zertifizierten Kommunikationsweg an das CLS-GW.

4. Die signierte Commissioning Notification wird über den BSI-zertifizierten Kommunikationsweg an das SMGW weitergeleitet.

5. Die signierte Commissioning Notification wird über den BSI-zertifizierten Kommunikationsweg an den aEMT weitergeleitet.

6. Die signierte Commissioning Notification wird auf einem FTP-Server von OLI Systems gespeichert und geprüft. Zusätzlich wird der Cloud Agent des Installateurs angestoßen, um

7. aus den Inbetriebnahmedaten ein Inbetriebnahme-Verifiable-Credential für die Anlage in Kombination mit der OLI Box auszustellen.

8. Der Cloud Agent Installer stellt das Inbetriebnahme-VC aus und schickt es an den Cloud Agent der OLI Box.

9. Der Cloud Agent der OLI Box speichert das Credential über seine Inbetriebnahmedaten ab und

10. schickt dem Cloud Agent Installer eine Acknowledge-Meldung.

11. Jetzt kann der Installer über die Bedienoberfläche (z. B. das Spherity Dashboard) sehen, dass eine neue Anlage vorliegt.

12. Nun kann der Installer Informationen über die Installation erfassen (z. B. Tag der Installation, Ort der Anlage, Messergebnisse) und sie

13. mithilfe seines Cloud Agent als Installation Verifiable Credential ausstellen

14. und an den Cloud Agent OLI Box senden.

15. Der Cloud Agent OLI Box speichert dieses Credential über sich ab und die Installation wird mit 16. Ack und 17. Ack beendet.

Stage #2 schafft die Basis für verifizierbare Daten direkt aus der Anlage. Hierbei werden auf die gleiche Weise wie bei der Inbetriebnahme-Message die Messdaten mit dem privaten Schlüssel der Anlage signiert. Somit lässt sich nachvollziehen, ob die Messdaten von der fachgerecht installierten Anlage kommen und ob sie nachträglich modifiziert worden sind. Diese Funktionalität kann in der nächsten Entwicklungsstufe umgesetzt werden und dient als Basis für Flexibilitätsmärkte und Proofof-Origin-Zertifikate.

4.2.5 Future Work

In dem oben beschriebenen Ansatz werden verschiedene Verifiable Credentials (Zertifikate) eingesetzt, die Aussagen über die energieerzeugende Anlage treffen. Beispielsweise wird die Anlage vom Hersteller angelegt. Die Signatur des Verifiable Credential kann mithilfe des öffentlichen Schlüssels auf dem Machine Identity Ledger auf Echtheit geprüft werden. Dies bietet bereits eine hohe Sicherheit, dass das Zertifikat echt ist. Die aktuelle Architektur bietet die Basis für das Ausstellen weiterer statischer und dynamischer Daten als Verifiable Credential. Mit dem Cloud-Edge-Ansatz können Zertifikate für diese Use Cases spezifisch durch vertrauenswürdige Dritte oder die OLI Box bzw. andere CLS-Geräte selbst signiert und ausgestellt werden.

Um eine noch höhere Sicherheitsstufe zu erreichen, kann man nachprüfbar machen, ob der Hersteller und der Installateur echt und berechtigt waren, Aussagen über die Anlage zu treffen. Dies ist durch das sogenannte Credential Chaining möglich. Hierbei wird überprüft, ob zum Beispiel der Installateur ein Berechtigungs-Zertifikat von einer vertrauenswürdigen Stelle vorweisen kann, zum Beispiel von dem Netzbetreiber bzw. einem Regulator wie der Bundesnetzagentur. Das Installations-Zertifikat und das Berechtigungs-Zertifikat des Installateurs werden dafür miteinander verknüpft. Außerdem kann man die X.509-Zertifikate der iMSys-Architektur in den Prozessablauf einbinden, um das bestehende Sicherheitskonzept mit dem hier vorgeschlagenen zu verknüpfen.

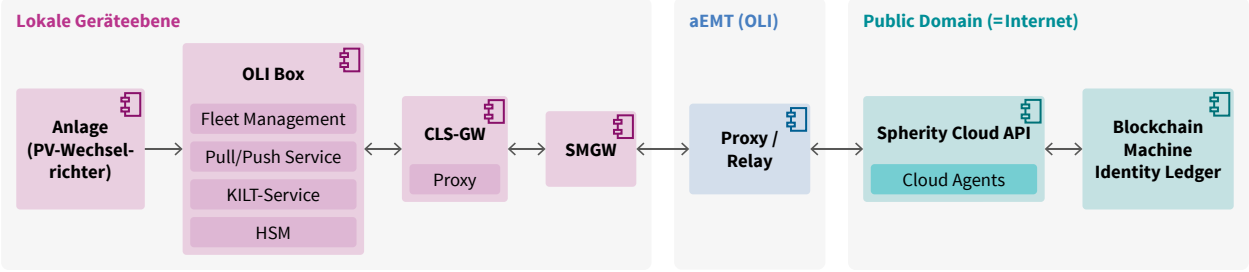


Abbildung 41: Proxy/Relay beim aEMT für die bidirektionale Kommunikation über das SMGW hin zur Public Domain (Quelle: Eigene Darstellung OLI Systems GmbH)

Bei der jetzigen Ausbaustufe werden die Zertifikate implizit durch die Nutzung des CLS-Kanals mit einbezogen. Dies kann jedoch auch expliziter geschehen, indem zum Beispiel ein Fingerprint des eigentlichen Verbindungsaufbaus des TLS-Kanals in dem Credential mit abgelegt wird. Neben der Nutzung der BSI SM-PKI könnte auch ein bidirektionaler, transparenter Kanal zur Kommunikation der lokalen Geräteebene mit dem aEMT umgesetzt werden, was jedoch aufgrund der Komplexität der Kommunikationsstrukturen und der Verbindung von Private und Public Domain zum jetzigen Zeitpunkt durchaus herausfordernd ist. Unsere Applikation hat jedoch gezeigt, dass ein solcher Informationsaustausch große Vorteile mit sich bringt, die Mehrwerte der iMSys-Architektur hebt und für ein Gelingen dieser Architektur perspektivisch notwendig ist. Unsere Konzepte für diese Future-Work-Themen sind heute schon verfügbar und können in der nächsten Ausbaustufe in einem Folgeprojekt umgesetzt werden.

4.3 Bewertung der Anbindungsvarianten

4.3.1 Ziele und Methodik der Evaluation

Das vorliegende Projekt soll einen Beitrag zum Aufbau einer digitalen Infrastruktur für das Energiesystem der Zukunft leisten. Dabei handelt es sich um ein Pilotierungsvorhaben, das in diesem Bereich erste Erkenntnisse sammelt und auf dessen Arbeitsergebnis weitere Vorhaben aufgesetzt werden sollen. Aufgrund des zum Teil experimentellen Charakters ist es umso wichtiger, dass die Ergebnisse des Piloten evaluiert werden, um die bestehenden Erfolge und Herausforderungen zu qualifizieren und in den Kontext des Energiesystems einzubetten. Hierdurch werden die Ergebnisse zusätzlich auf eine wissenschaftlich fundierte Basis gestellt, die es erlaubt, den Blockchain Machine Identity Ledger einer Serienimplementierung für die Energiewirtschaft zugänglich zu machen.

Vor diesem Hintergrund besteht die Zielsetzung der Evaluation darin, jeweils die technischen, ökonomischen und regulatorischen Aspekte einer möglichen Serienimplementierung für das Energiesystem darzulegen. In diesem Zusammenhang wird explizit darauf eingegangen, wie sich die drei Aspekte gegenseitig beeinflussen. So kann der regulatorische Rahmen beispielsweise unmittelbare Auswirkungen auf die Entwicklung einzelner technischer Aspekte des Blockchain Machine Identity Ledger haben oder sich der Einsatz unterschiedlicher Technologien auf die Wirtschaftlichkeit in einer Serienimplementierung auswirken. Die durchgeführte Evaluation basiert auf einer zweigeteilten Datengrundlage. Zum einen wurden als Begleitung des Piloten vier operative Fortschrittsberichte erstellt, die den jeweiligen Projektfortschritt beschreiben, Erfolge dokumentieren und auf eventuelle Risiken und Herausforderungen hinweisen. Zum anderen wurde ein iterativer Fragenkatalog erstellt, der zur systematischen Abfrage folgender Punkte genutzt wurde:

- Beschreibung der Lösungsstrategien mit Detailabfragen zu
  - eingesetzten Technologien und unterschiedlichen Sichten auf die Umsetzungbeispielsweise in Form von Architektur- und Sequenzdiagrammen
  - ökonomischen Aspekten, insbesondere mit Fokus auf potenzielle Effizienzgewinne und Herausforderungen für die Serienimplementierung
  - regulatorischen Anforderungen beispielsweise an die Datenkommunikation sowie identifizierten Hürden des aktuellen regulatorischen Rahmens
- Selbsteinschätzung der technischen / ökonomischen / regulatorischen Mehrwerte und Herausforderungen
- Einordnung der Lösung in Bezug auf spätere adressierte Anwendungsfälle und damit verbundene Anforderungen und Risiken
- Alternative Ansätze und begründete getroffene Designentscheidungen
- Weitere notwendigerweise getroffene Annahmen und Rahmenbedingungen

Aufbauend auf den erhaltenen Informationen wurde der Fokus der technischen Evaluation insbesondere auf die Analyse und Bewertung der Implikationen von getroffenen technischen Entwurfs- und Architekturentscheidungen für eine Serienimplementierung gelegt. Die Evaluation der technischen Umsetzung adressiert daher unter anderem folgende Analyse- und Evaluationskriterien:

- Bewertung der technischen Skalierbarkeit des gewählten „Identitäts-Verzeichnisses auf Blockchain-Basis“ als Infrastrukturgrundlage des Piloten bezüglich einer späteren Serienimplementierung im Hinblick auf die gewählte Blockchain-Technologie. Diese Betrachtung ist aufgrund der zu erwartenden Menge an zukünftig angebundenen Geräten verschiedenster Art aus den Kategorien Erzeugung, Speicher und Verbraucher von elementarer Bedeutung.

- Analyse der Anlagen- und Gerätekommunikation für die zu betrachtenden Anbindungsvarianten im Hinblick auf die technischen Mindestanforderungen an die SMGWKommunikationsinfrastruktur. Darunter fallen insbesondere Fragestellungen zu nicht funktionalen Anforderungen wie Rechenleistung, Kommunikationsbandbreiten und Latenzzeiten an SMGW-Administratoren, Anlagenverantwortliche und andere relevante Marktteilnehmer.

- Analyse und Bewertung der technischen „Kompatibilität" der umgesetzten Lösungsvarianten bezüglich der relevanten Technischen Richtlinien des BSI und weiterer Regelungen aus dem Gesetz zur Digitalisierung der Energiewende. Die Ergebnisse hieraus sind zudem relevant für die regulatorische Evaluation.

Die ökonomische Evaluation zielt primär auf die Identifizierung der möglichen Effizienzgewinne, die durch die Anbindungsvarianten erzielt werden könnten, und der Herausforderungen, die einer Erschließung dieser Potenziale aus ökonomischer Sicht entgegenstehen. Drei Kriterien wurden dabei vertiefend betrachtet, um zu bewerten, wie die durch den BMIL bereitgestellte digitale Identität genutzt werden kann, um Effizienzhemm nisse zu beheben. Zwei Effizienzkriterien stehen dabei im Fokus:

- Einfluss auf die Kosten der (digitalen) Identitätsfeststellung. Hier stehen mögliche Transaktionskostenreduzierungen im Fokus, die anhand der Anwendungsfälle illustriert werden, etwa im Hinblick auf den Abbau von Markteintrittsbarrieren.

- Eng damit verbunden werden die Potenziale zur Hebung von Synergien (Economies of Scope) mit dem SMGW-Rollout analysiert.

In Bezug auf die Serienimplementierung zeigte sich im Verlauf des Projekts, dass hier die Interoperabilität der Anbindungsvarianten untereinander wie auch insbesondere der mit der SSI verbundenen Datenmodelle notwendig ist, um die identifizierten Effizienzpotenziale zu heben. Hier fokussiert sich die Analyse insbesondere auf die Frage, wie die Interoperabilität genutzt werden kann, um Skaleneffekte (Economies of Scale) zu heben und damit die Diffusion der digitalen Identitäten basierend auf dem BMIL-Ansatz zu ermöglichen.

Im Rahmen der regulatorischen Evaluation wurde überprüft, ob die Durchführung des Piloten stets in Übereinstimmung mit der bestehenden Rechtslage erfolgt ist. Ziel war es hierbei, unter Berücksichtigung einer möglichen Serienimplementierung zusammenzufassen, welche regulatorischen Herausforderungen für den Piloten identifiziert wurden und wie mit diesen Herausforderungen umgegangen wurde. Gleichzeitig wurde festgestellt, wo derzeit regulatorische Grenzen bestehen und wie diese Hemmnisse für eine Serienimplementierung praktikabel abgebaut werden könnten. Eine detaillierte regulatorische Evaluation der Anwendungsfälle zu jeder Anbindungsvariante erfolgt ebenso wie bei der ökonomischen Evaluation nicht. Grundstein für die regulatorische Evaluation ist der geltende Rechtsrahmen, der sich grob in die ITsicherheitsregulatorischen Anforderungen an das Maschinen-Identitäten-Register und die datenschutzrechtlichen Anforderungen an die Verarbeitung der verwendeten Informationen unterteilen lässt. Darauf aufbauend wurden insbesondere folgende Aspekte untersucht:

- IT-sicherheitsregulatorische Anforderungen
  - Zuständigkeit und Aufgaben des Smart-Meter-Gateway-Administrators (GWA) (§§ 3 Abs. 1 Satz 2, 25 MsbG)
  - Technische Anforderungen hinsichtlich der Funktionalität und Interoperabilität des SMGW (§§ 22, 23 MsbG i.V.m. den Technischen Richtlinien des BSI)
  - Vorgaben zur Datenkommunikation (§§ 49 ff. MsbG)

- Datenschutzrechtliche Anforderungen
  - Anwendbarkeit der Datenschutz-Grundverordnung (DSGVO) sowie des Bundesdatenschutzgesetzes (BDSG) und Prüfung des Vorliegens personenbezogener Daten
  - Wahrung von Betroffenenrechten
  - Wahrung anderer datenschutzrechtlicher Grundsätze, wie zum Beispiel Datenminimierung und Privacy-by-Design

Der nachfolgenden Evaluation lagen dabei folgende Annahmen und Einschränkungen zugrunde:

- Die Hardwaresicherheit der verwendeten Smart-Meter-Gateways, Mehrwertmodule / CLSProxys und dedizierten CLS-Geräte (OLI Box) wird als gegeben angenommen und ist nicht Teil der Betrachtung.

- Die Umsetzung der Softwareimplementierungen sowie die Konfiguration der Cloud-Infrastruktur erfüllen alle Sicherheitsanforderungen.

- Die Auswahl der Distributed-Ledger-Technologie-Implementierung wird als beispielhaft und austauschbar angenommen.

- Die auf der Basis des BMIL angedachten Anwendungsfälle werden im Rahmen der ökonomischen Analyse als Fallbeispiele für die potenziellen Effizienzgewinne herangezogen. Eine Detailanalyse der Anwendungsfälle erfolgt nicht.

Entsprechend der generellen Zielsetzung des BMIL-Piloten ist zudem herauszustellen, dass die Exploration und Technologieoffenheit von Beginn an eine wesentliche Prämisse darstellten und eine bewusste Entscheidung für die Umsetzung und Erprobung unterschiedlicher Ansätze und Anbindungsvarianten getroffen wurde. Die beschriebenen Lösungsansätze stellen damit keine Standardisierungsaktivität dar.

4.3.2 Technische Bewertung

Im Rahmen der BMIL-Pilotierung wurde der Fokus auf drei Ausprägungen der Implementierung der selbstbestimmten Identität und Geräteanbindung gelegt und diese wurden wie in Kapitel 4.1 und 4.2 beschrieben als technische Durchstiche umgesetzt und erprobt. Die gerätezentrierte Identitätsverwaltung im Verbund mit einem SMGW-Mehrwertmodul setzt auf einen bidirektionalen Kommunikationsweg zwischen CLS und EMT (beide Parteien sind sowohl Sender als auch Empfänger) zur dezentralen Identitätsverwaltung auf einem adaptierten YOUKI-Mehrwertmodul des Herstellers Theben AG an einem Theben CONEXA 3.0 SMGW. Dabei wird das KILT Protocol als zugrunde liegende Blockchain-Technologie zum Verwalten der SSIs eingesetzt.

Die gerätezentrierte Identitätsverwaltung im Verbund mit einem dedizierten CLS-Device setzt ebenfalls auf einen bidirektionalen Kommunikationsweg zwischen CLS und EMT. Auch hier wird das KILT-Protokoll als zugrunde liegende Blockchain-Technologie zum Verwalten der SSIs eingesetzt. Im Unterschied zur ersten Umsetzungsvariante kommt ein dediziertes CLS-Device in Form einer OLI Box (Embedded Hardware auf Basis eines Raspberry Pi 3b) des Herstellers OLI Systems zum Einsatz.

Die Cloud-Wallet-basierte Identitätsverwaltung setzt auf die Delegation an eine Cloud Wallet von Spherity zur cloudseitigen Verwaltung der digitalen Geräte-Identitäten. Die technische Umsetzung erfolgte im Rahmen des Piloten wie in der zuvor genannten Ausprägung ebenfalls unter Einsatz einer OLI Box. Die Kommunikation verläuft dabei unidirektional über den CLS-Kanal vom CLS-Device ausgehend.

Tabelle 1 enthält eine Gegenüberstellung der drei betrachteten Varianten, bildet diese auf die Referenzarchitektur aus Abbildung 10 ab und stellt wesentliche charakteristische Eigenschaften der Varianten gegenüber.

	Gerätezentrierte Identitätsverwaltung im Verbund mit einem SMGW-Mehrwertmodul	**Gerätezentrierte Identitätsverwaltung im Verbund mit einem dedizierten CLS-Device**	**Cloud-Wallet-basierte Identitätsverwaltung**
Abbildung der Variantenumsetzung auf die Referenzarchitektur aus Abbildung 10			
Holders Agent	YOUKI-Mehrwertmodul	OLI Box	Cloud
Wallet	YOUKI-Mehrwertmodul	OLI Box	Cloud
Verortung der Blockchain Nodes	Internet	Internet	Cloud
Speicherort der VCs	YOUKI-Mehrwertmodul	OLI Box	Cloud
Speicherort der Private Keys	Allokationsanreize	HMS Key Storage der OLI Box	HSM Key Storage der OLI Box
DID	Preissetzung	Verifiable Data Registry	Verifiable Data Registry
DID Services	Netzausbau	OLI Box	OLI Box, Cloud
Mehrwertanwendung	Als Decentralized App auf YOUKI-Mehrwertmodul	OLI Box	Cloud

Bewertung der Variantenumsetzung			
Wesentliche variantenspezifische Eigenschaften	■ Software-as-a-Service-Plattform auf einem Mehrwertmodul, das bereits in Produktivsystemen eingesetzt wird ■ YOUKI Core ermöglicht Umsetzung vollständig dezentraler Blockchain Nodes auf Mehrwertmodul	■ Einsatz eines dedizierten CLS-Geräts zur einfachen Nachrüstung, wenn bereits ein CLS-Proxy vorhanden ist	■ Zur Registrierung der Identität wird vollständig die SMGW-Infrastruktur genutzt ■ Auf Standards basierender Key-Delegation-Mechanismus ermöglicht Übertragung bestimmter Operationen an einen digitalen Zwilling in der Cloud und bietet Vorteile in Bezug auf Performance, Skalierbarkeit und Update-Fähigkeit durch cloudseitig implementierte Mehrwertanwendungen
Eingesetzte Blockchain-Technologie und deren Skalierbarkeit	■ KILT Blockchain ist Teil des PolkadotÖkosystems ■ Durch das Polkadot-Protokoll keine Skalierungsprobleme	■ KILT Blockchain ist Teil des PolkadotÖkosystems ■ Durch das Polkadot-Protokoll keine Skalierungsprobleme	■ Private Ethereum-Blockchain ist erst mit Layer-2-Upgrades skalierbar, kann aber auch durch beliebige Blockchain-Technologie ausgetauscht werden
Einschränkungen im Rahmen der Pilotierung	■ Im Rahmen des Piloten zweite WAN-Verbindung notwendig	■ Im Rahmen des Piloten zweite WAN-Verbindung notwendig	■ Im Rahmen des Piloten nur unidirektionale Kommunikation umgesetzt, die für die Registrierung der Identität zweckmäßig ist, aber Mehrwertanwendungen derzeit nur sehr eingeschränkt zulässt

Tabelle 1: Gegenüberstellung der drei betrachteten Umsetzungsvarianten

4.3.2.1 Diskussion aufgestellter Thesen

These: *Die digitale Identitäten-basierte Geräteregistrierung und das selbstbestimmte Identitätssystem können mittels Smart-Meter-Public-Key-Infrastruktur unter Berücksichtigung des standardisierten Rollenmodells im Regelbetrieb und auf der Basis von am Markt verfügbaren intelligenten Messsystemen umgesetzt werden.*

Sämtliche im Rahmen des Piloten eingesetzten SMGWs sind als Kommunikationseinheiten des intelligenten Messsystems vom BSI zertifiziert. Zum Einsatz kamen das CONEXA 3.0 Version 1.1 von der Theben AG sowie das SMGW Version 1.1.1 von der OPENLiMiT SignCubes GmbH Power Plus Communications AG, die vom BSI unter der Nummer BSI-DSZ-CC-0918-V2-2021 bzw. BSI-DSZ-CC-0831-V3-2021 zertifiziert wurden.[70] Da es sich um Laboraufbauten handelt, wird zum Teil auf die Ausführung in der Test-PKI zurückgegriffen, was unter anderem das Handling der Gateway- Administration vereinfacht. Generell lässt sich aus den Ausführungen der Partner aber kein technischer Grund ableiten, der einem Regelbetrieb unter Berücksichtigung des Rollenmodells und der standardisierten Abläufe und Zuständigkeiten in der Wirk-PKI entgegenstehen würde.

In der Anbindungsvariante „Gerätezentrierte Identitätsverwaltung im Verbund mit einem dedizierten CLS-Device“ kommt ein am Markt verfügbarer CLS-Proxy zum Einsatz, an dem ein außerhalb der CLS Vertrauenskette liegendes Edge Device angeschlossen ist. Dagegen kommt in der Anbindungsvariante „Gerätezentrierte Identitätsverwaltung im Verbund mit einem SMGWMehrwertmodul“ ein modifiziertes Mehrwertmodul mit erweiterter Rechenleistung und erweitertem Speicher zum Einsatz. Die Notwendigkeit dafür liegt aber nicht in der Komplexität der Identitätsverwaltung, sondern in der generell von YOUKI anvisierten Integration einer dedizierten Blockchain für

70 https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Smartmetering/Smart-Meter-Gateway/Zertifikate24Msbg/produkte.html

den BMIL auf dem Mehrwertmodul, die jedoch nicht als Teil des Piloten untersucht wurde. Die Cloud-Wallet-basierte Identitätsverwaltung basiert auf dem identischen Hardware-Setup wie die gerätezentrierte Identitätsverwaltung im Verbund mit einem dedizierten CLS-Device, sodass auch hier eine Umsetzung auf der Basis von am Markt verfügbarer Hardware erfolgt.

These: *Die digitale Identitäten-basierte Geräteregistrierung und das selbstbestimmte Identitätssystem können im Rahmen der vorhandenen technischen Restriktionen in Bezug auf verfügbare Kommunikationskanäle, Rechenleistung von Edge Devices, Bandbreiten und Latenzzeiten umgesetzt werden.*

In der Technischen Richtlinie BSI TR-03109-1 definiert der WAN-Anwendungsfall 6 „Kommunikation aktiver EMT mit CLS“ lediglich die Notwendigkeit der Kommunikation eines aktiven EMT mit einem CLS-Gerät unter Nutzung der Proxy-Funktionalität des SMGW (siehe REQ.WAN.TlsProxy.10 in BSI TR-03109-1). Darüber hinausgehend sind in der Technischen Richtlinie keine weiteren nicht funktionalen Anforderungen an die WAN-Kommunikationsstrecke definiert.

Die isolierte Betrachtung des Basisdienstes der Geräteregistrierungen sowie des Identitätsmanagements, wie sie in den Kapiteln 4.1.3, 4.1.4 und 4.2 beschrieben sind, hat gezeigt, dass die Informationsobjekte zur Übertragung des DID-Dokuments mit der Definition der Machine Identity sowie der Verifiable Credentials zur Inbetriebnahme sowie zur Installation nur wenige Kilobyte umfassen. Beispielhafte Datenpakete dazu sind dem Anhang in Kapitel 7 zu entnehmen. Sie lassen sich über alle am Markt befindlichen SMGWs mit ihren unterschiedlichen WANKommunikationen per Ethernet zum Anschluss an DSL-, Kabel- oder Glasfasernetze, per Mobilfunk über LTE und CDMA 450 sowie per Breitband-Powerline ohne zu erwartende Einschränkungen übertragen. Zudem sind Antwortzeiten bei der einmaligen Geräteregistrierung sowie beim Identitätsmanagement ebenfalls als unkritisch einzustufen.

In Bezug auf die Verfügbarkeit der Bandbreiten und die Latenzzeiten der Kommunikationskanäle kann daher rein für den Basisdienst der Geräteregistrierung und das selbstbestimmte Identitätssystem davon ausgegangen werden, dass sie keine relevante Restriktion darstellen. **Die fehlende Standardisierung nicht funktionaler Eigenschaften der Kommunikationsstrecke zwischen EMT und einem CLS über das Gateway** hinsichtlich der Latenzzeiten sowie der Anforderungen an den Datendurchsatz wird in Zukunft in Bezug auf mehrwertanwendungsspezifische Daten zu einem zentralen Problem werden.

Ein weiterer Aspekt der Evaluation ist die Betrachtung der Rechenleistung der Edge Devices für die Ausführung des Basisdienstes der Geräteregistrierung und des Identitätsmanagements, also im Rahmen dieses Pilotvorhabens die Bewertung der Rechenleistung der OLI Box und des genutzten modifizierten Mehrwertmoduls. Auf der Basis der zur Verfügung gestellten Datengrundlage in Form der dargestellten Sequenzdiagramme zur Generierung der Key Pairs und zur Registrierung des DID auf der Blockchain lässt sich dazu jedoch keine abschließende Aussage machen. Es ist jedoch davon auszugehen, dass bei isolierter Betrachtung des Basisdienstes der einmaligen Geräteregistrierung dieser die verfügbare Rechenleistung bei Weitem nicht ausschöpfen wird und der überwiegende Teil der verfügbaren Rechenleistung für Mehrwertanwendungen zur Verfügung steht.

These: *Die technische Skalierbarkeit des gewählten „Identitäts-Verzeichnisses auf Blockchain-Basis“ als Infrastrukturgrundlage des Piloten im Hinblick auf eine spätere Serienimplementierung ist gegeben.*

Das Identitäts-Verzeichnis muss die Verwaltung und Verarbeitung einer großen Anzahl an Identitäten gewährleisten, um ein zuverlässiges und leistungsfähiges System für die zukünftigen Mehrwertanwendungen darstellen zu können. Zum Beispiel sollten die Latenzen für Transaktionen und Smart Contracts möglichst gering und konstant sein. Die Energieeffizienz einer Blockchain-Technologie ist im Kontext der Energiewende ebenfalls ein bedeutendes Thema, da der Energiebedarf für den Betrieb bestimmter Blockchains sehr hoch sein kann. Die Erweiterbarkeit und Flexibilität der Blockchain-Technologie bei der Umsetzung des Identitäts-Verzeichnisses müssen deshalb gegeben sein, um neue Technologien und zukünftige Entwicklungen integrieren zu können.

Bei der gerätezentrierten Identitätsverwaltung wird die KILT Blockchain verwendet, die das Polkadot-Protokoll[71] umsetzt, wodurch mehrere unterschiedliche Blockchains zu einer heterogenen Multichain verknüpft werden können. Die Multichain kann zur Lösung der Skalierungsprobleme genutzt werden, weil davon ausgegangen werden kann, dass Transaktionen parallelisiert und neue, für Anwendungsfälle maßgeschneiderte Blockchains integriert werden können. Zudem wird auch eine gewisse Interoperabilität unterschiedlicher Blockchains gewährleistet. Die Auswahl der Blockchain-Technologie für die gerätezentrierte Identitätsverwaltung ist dementsprechend zukunftssicher und unterstützt die Technologieoffenheit, die auch durch den DID-Standard verfolgt wird.

71 Polkadot: Lightpaper – An introduction to Polkadot, April 2020, https://polkadot.network/Polkadot-lightpaper.pdf

Die Cloud-Wallet-basierte Identitätsverwaltung wird im Rahmen der Pilotierung durch die Ethereum-Blockchain umgesetzt. Eine Serienimplementierung auf Basis der Ethereum-Blockchain würde insbesondere bei paralleler Nutzung der Blockchain als Speicherort in Mehrwertanwendungen schnell auf Skalierungsprobleme stoßen, solange Ethereum-Layer-1-Lösungen zum Einsatz kommen.[72] Ethereum-Layer-2-Lösungen ermöglichen dagegen eine deutlich bessere Skalierbarkeit.[73] Da die Spherity Cloud zudem Schnittstellenerweiterungen ermöglicht, können prinzipiell aber auch unterschiedliche Blockchain-Technologien für das Identitäts-Verzeichnis genutzt werden. In einer Serienimplementierung kann daher zum Beispiel statt der Ethereum-Blockchain eine Multichain genutzt werden. Um Synergieeffekte des Pilotprojekts zu heben, würde sich die Integration der KILT Blockchain über die Spherity Cloud anbieten, um Migrationspfade und zusätzliche Entwicklungsarbeiten gering zu halten.

4.3.2.2 Diskussion am Beispiel eines visionären Szenarios

Neben der Betrachtung der zu Beginn aufgestellten Thesen sowie der Gegenüberstellung der Anbindungsvarianten soll im Folgenden ein Szenario betrachtet und diskutiert werden, bei dem ein Smart-Meter-Gateway die Rolle als zentrale Kommunikationseinheit mit entsprechend großem Funktionsumfang und einer Vielzahl von lokal angeschlossenen CLS-Endgeräten einnimmt. Es ist angelehnt an die in der „BMWi-BSI-Roadmap“ (Standardisierungsstrategie zur sektorübergreifenden Digitalisierung nach dem GDEW) skizzierten Anwendungsbereiche des Clusters 1 und 2 (siehe Abbildung 42) und stellt ein aktuell visionäres, aber insbesondere unter technischen und ökonomischen Gesichtspunkten anstrebenswertes Szenario dar. Als Ausgangslage wird ein Mehrfamilienhaus mit acht Wohneinheiten angenommen, deren Basiszähler über ein zentrales SMGW angebunden sind. Darüber hinaus besitzt das Wohngebäude eine Dach-Photovoltaik-Anlage sowie einen Batteriespeicher. Zwei der im Haus lebenden Familien fahren zudem ein Elektrofahrzeug und laden ihr Fahrzeug an einer jeweils eigenen Wallbox in der Tiefgarage.

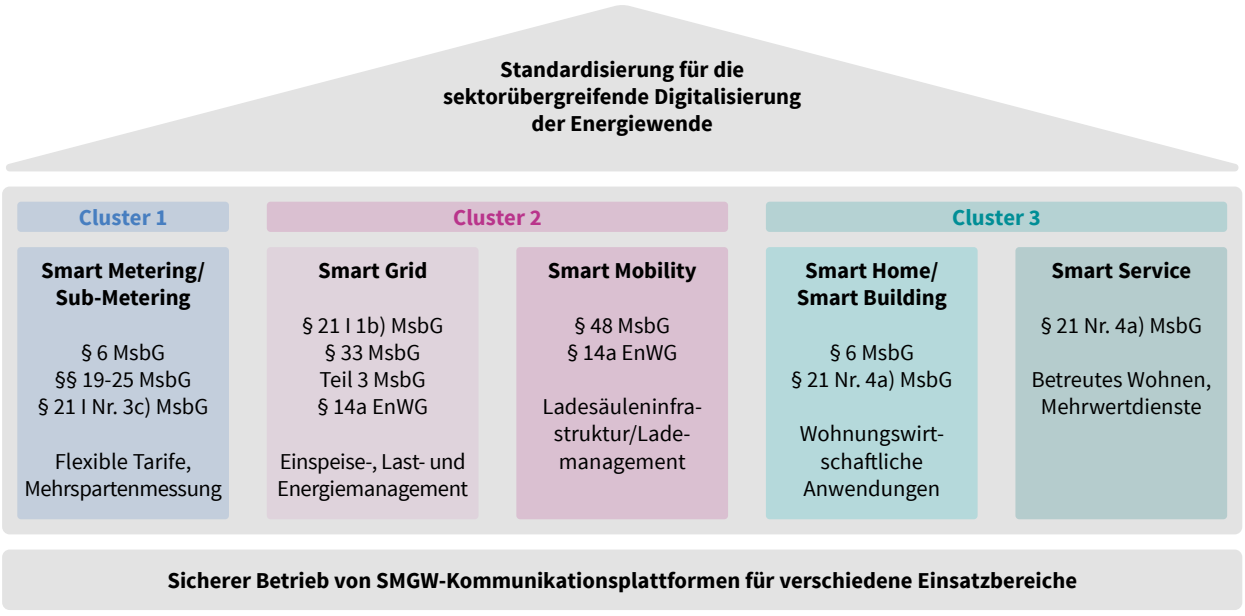


Abbildung 42: Standardisierungsstrategie zur sektorübergreifenden Digitalisierung nach dem GDEW (Quelle: BMWi/BSI (2019): Standardisierungsstrategie zur sektorübergreifenden Digitalisierung nach dem GDEW, Abb. 3)

72 Dennis, R., Disso, J.P. (2019): An Analysis into the Scalability of Bitcoin and Ethereum. In: Yang , XS., Sherratt, S., Dey, N., Joshi, A. (Hrsg.): Third International Congress on Information and Communication Technology. Advances in Intelligent Systems and Computing, Vol 797. Springer, Singapore. https://doi.org/10.1007/978-981-13-1165-9_57

73 Vitalik Buterin: Layer 2 is the future of Ethereum scaling, https://forkast.news/vitalik-buterin-layer-2-future-of-ethereumscaling/

Auf Grundlage der in Kapitel 5 skizzierten Mehrwertanwendungen wird für das Szenario weiterhin angenommen, dass überschüssige Erträge der Dach-Photovoltaik-Anlage als Teil einer größeren Energy Community vermarktet werden und der Batteriespeicher sowie die beiden Elektrofahrzeuge als regelbare Kleinanlagen an einem Flexibilitätsmarkt teilnehmen. Allein in dieser Konstellation würden damit zwei Mehrwertanwendungen und damit verbunden vier Geräte-Identitäten über ein SMGW realisiert und angebunden werden müssen. Unter Einbeziehung von Cluster 3 sind zudem noch weitere Mehrwertanwendungen aus den Bereichen Smart Home, Smart Building und Smart Services denkbar, die ebenfalls vom Konzept der digitalen Identitäten Gebrauch machen und profitieren können. Die Anzahl der über ein SMGW angebundenen CLS-Geräte und realisierten Mehrwertanwendungen kann demnach ohne Weiteres in Zukunft weiter steigen.

Zur Anbindung der skizzierten Geräte im Mehrfamilienhaus werden in diesem Szenario entweder ein am SMGW angeschlossenes Mehrwertmodul, ein angeschlossener CLS-Proxy oder eine Kombination beider Varianten sowie darüber hinausgehend befähigte lokale Steuergeräte für die individuellen Anlagen PV-Anlage, Speicher und Wallboxen benötigt. Für die Umsetzung der Mehrwertanwendungen sind unter diesen Annahmen ganz unterschiedliche Lösungsvarianten denkbar, die zahlreiche aktuell ungeklärte Fragestellungen aufwerfen.

In einer ersten Variante könnte sich ein **App-Ökosystem rund um das Mehrwertmodul** entwickeln, sodass Mehrwertanwendungen von unterschiedlichen Anbietern zukünftig parallel auf einem Mehrwertmodul betrieben werden. Wie in Kapitel 4.1.3 dargestellt, wird bereits im BMIL-Piloten ein Mehrwertmodul mit gesteigerter Prozessorleistung und vergrößertem internen Speicher eingesetzt. Zukünftige Marktentwicklungen in Richtung eines App-Ökosystems werfen dabei aber neben der Leistungsfähigkeit des Mehrwertmoduls insbesondere Fragestellungen zum **Parallelbetrieb bzw. zur Mandantenfähigkeit der Mehrwertanwendungen, zur Realisation des Datenschutzes und zur Kapselung der Anwendungen über Containerisierungen, zur Update-Fähigkeit sowie zu Backup-Strategien** auf. Ebenso ergeben sich Fragestellungen zum **Betrieb eines App-Ökosystems zum Beispiel im Hinblick auf die Betreiberrolle und die übergeordnete Konfiguration des Mehrwertmoduls.**

In einer zweiten Variante mit Nutzung eines CLS-Proxys und daran angeschlossenen dedizierten Endgeräten ergeben sich ebenso zahlreiche Fragestellungen. Anforderungen an die Leistungsfähigkeit eines Proxys können dabei als weniger kritisch angesehen werden, da die Funktionalität im Wesentlichen auf die Zurverfügungstellung und die Durchleitung der Daten durch den CLS-Kanal reduziert ist. In den Vordergrund rücken aber ebenfalls Fragestellungen zur **Betreiberrolle und zur übergeordneten Konfiguration des Proxys** beispielsweise zur Verwaltung der Endgeräte.

Ein weiterer Aspekt, der im skizzierten Szenario generell als kritisch zu betrachten ist, ist die **fehlende Standardisierung nicht funktionaler Eigenschaften der Kommunikationsstrecke zwischen EMT und einem CLS über das Gateway** zum gegenwärtigen Zeitpunkt. Relevant können insbesondere potenzielle zusätzliche Anforderungen an Datendurchsatz und Latenz sein, die aus lokal ausgeführten Mehrwertanwendungen resultieren, deren Algorithmik nicht in die Cloud verlagert wurde. Da die Umsetzung und praktische Erprobung der Mehrwertanwendungen nicht Teil des Pilotvorhabens waren und zudem die Möglichkeit eines CLS-Bypasses über ein zweites WAN besteht, soll an dieser Stelle lediglich auf die fehlende Standardisierung nicht funktionaler Eigenschaften des Kommunikationsweges CLS-Kanal hingewiesen werden. Insbesondere für Mehrwertanwendungen des Clusters 3 wird dies jedoch kritisch werden.

4.3.2.3 Zusammenfassung der technischen Bewertung

Im Rahmen der BMIL-Pilotierung wurde eindrucksvoll gezeigt, dass auf der Basis der Self-Sovereign Identity als neues Paradigma der **digitalen Identitätsmanagementsysteme eine digitale Identitätenbasierte Geräteregistrierung innerhalb der Smart-Meter-PKI im Regelbetrieb und unter Einsatz von am Markt verfügbaren intelligenten Messsystemen** umgesetzt werden kann. Sie kann **eine signifikante Bereicherung für die Digitalisierung der Energiewende** und damit verbundene zukünftige Mehrwertanwendungen darstellen. Gleichwohl wurde deutlich, dass eine **Vielzahl technischer Fragestellungen zum aktuellen Zeitpunkt** als **unbeantwortet** angesehen werden müssen.

Insbesondere die **Frage, ob einer Integration der Identitätsbildung** sowie darüber hinaus der Geschäftslogik von Mehrwertanwendungen **in ein Mehrwertmodul,** einer **Verortung** von beiden in **einem dedizierten und am CLS-Proxy angeschlossenen Endgerät,** einer darüber hinausgehenden perspektivischen Integration in bestehende Energieanlagen wie zum Beispiel in Wechselrichter **oder dem beschriebenen Cloud-Edge-Ansatz der Vorzug gegeben werden sollte, lässt sich technisch nicht eindeutig beantworten.**

Das Spektrum der möglichen Mehrwertanwendungen, von der einmaligen Erzeugung der digitalen Identität, um den gesetzlichen Belangen nach einem Geräteregister zu genügen, bis hin zu einem Edge-basierten Handel von tokenisierten Energiemengen in Echtzeit, bringt dabei ganz unterschiedliche Anforderungen an die Ausführungsplattform mit sich. In der vorangegangenen Diskussion des visionären Szenarios wurden daher zahlreiche technische Fragestellungen aufgeworfen und die

aktuell **fehlende Standardisierung nicht funktionaler Eigenschaften des Kommunikationsweges CLS-Kanal** wurde herausgestellt. Der Kapselung des Endpunktes der CLS-Vertrauenskette über ein zertifiziertes Mehrwertmodul oder einen zertifizierten CLS-Proxy kommt in allen Anbindungsvarianten eine gemeinsame und besonders große Bedeutung zu. Sie ermöglicht es erst, den Aufwand für die Entwicklung zukünftiger Mehrwertanwendungen gering zu halten, und gibt den Herstellern und Entwicklern die Möglichkeit, den Fokus auf die Anwendungslogik zu legen. Aus den vorangegangenen Betrachtungen kann daher abgeleitet werden, dass eine **Kombination aus potentem Mehrwertmodul** (also der Möglichkeit selbst gehosteter Anwendungen) **mit der reinen durchleitenden Proxy-Funktionalität eine wünschenswerte Umsetzung des Endpunktes der CLS-Vertrauenskette** darstellen würde. Diese Variante wäre technologieoffen und würde insbesondere allen beschriebenen Anbindungsvarianten des Identitätsmanagements eine entsprechende Ausführungsplattform bieten.

Die BMIL-Pilotierung hat zudem gezeigt, dass die **Skalierbarkeit des gewählten „Identitäts-Verzeichnisses auf Blockchain-Basis" im Hinblick auf eine spätere Serienimplementierung grundsätzlich gegeben** und eine **Co-Existenz von unterschiedlichen Geräteregistern möglich** ist. Technologisch ist demnach **keine Festlegung auf beispielsweise das KILT-Protokoll oder die Ethereum-Blockchain notwendig.** Die Interoperabilität im Hinblick auf die gewählte Blockchain-Technologie wurde im Rahmen des Piloten allerdings als Proof of Concept demonstriert und **erfordert** weiterhin eine grundlegende Betrachtung und insbesondere **Standardisierungsbemühungen in zukünftigen Arbeiten.**

4.3.3 Ökonomische Bewertung

Wie bereits einleitend in Kapitel 4.3.1 kurz dargestellt wurde, zielt die ökonomische Evaluation primär auf die Identifizierung der möglichen Effizienzgewinne, die durch die Anbindungsvarianten erzielt werden könnten, und die Herausforderungen, die einer Erschließung dieser Potenziale aus ökonomischer Sicht entgegenstehen, ab. Drei Kriterien wurden dabei vertiefend betrachtet, um zu bewerten, wie die durch den BMIL bereitgestellte digitale Identität genutzt werden kann, um Effizienzhemmnisse zu beheben. Zwei Effizienzkriterien stehen dabei im Fokus:

- Einfluss auf die Kosten der (digitalen) Identitätsfeststellung. Hier stehen mögliche Transaktionskostenreduzierungen im Fokus, die anhand der Anwendungsfälle illustriert werden, etwa im Hinblick auf den Abbau von Markteintrittsbarrieren.

- Eng damit verbunden werden die Potenziale zur Hebung von Synergien (Economies of Scope) mit dem SMGW-Rollout analysiert.

In Bezug auf die Serienimplementierung zeigt sich, dass hier die Interoperabilität der Anbindungsvarianten untereinander wie auch insbesondere der mit der SSI verbundenen Datenmodelle notwendig ist, um die identifizierten Effizienzpotenziale zu heben. Hier fokussiert sich die Analyse insbesondere auf die Frage, wie die Interoperabilität genutzt werden kann, um Skaleneffekte (Economies of Scale) zu heben und damit die Diffusion der digitalen Identitäten basierend auf dem BMIL-Ansatz zu ermöglichen.

Im Folgenden stellen wir die Kernaussagen der Evaluation zu diesen drei Aspekten und die wesentlichen offenen Punkte dar, die in einem nächsten Schritt hin zur Serienimplementierung detaillierter betrachtet werden sollten. Einschränkend sei an dieser Stelle angemerkt, dass es sich bei den oben beschriebenen Erprobungen der Anbindungsvarianten um Demonstratoren in einem frühen Entwicklungsstadium handelt, die noch keine genauen Kosten-Nutzen-Analysen zulassen. Solche Analysen können erst in einer späteren Phase, in der die Anbindungsvarianten weiterentwickelt werden, erfolgen. Daher beschränkt sich die vorliegende Evaluation darauf, die wesentlichen Potenziale des BMIL-Ansatzes im Hinblick auf die drei untersuchten Kriterien darzustellen. Auch hier gilt aber, dass zwar der Entwicklungsstand der Anbindungsvarianten durchaus erste Rückschlüsse auf die ökonomischen Potenziale zulässt, diese sich aber durchaus mit der Weiterentwicklung der Ansätze zukünftig verändern können und dies auch sehr wahrscheinlich ist. Zudem sei darauf verwiesen, dass die Bewertung der möglichen Effizienzgewinne durch den BMIL im Vergleich zum Status quo der Identitätsfeststellung vorgenommen wurde.

4.3.3.1 Mögliche Effizienzgewinne durch den BMIL bzw. die verschiedenen Anbindungsvarianten

Effizienzgewinne durch Transaktionskostenreduzierung bei der (digitalen) Identitätsfeststellung

Die Identitätsfeststellung und das Identitätsmanagement, die hier im Fokus stehen, sind relevante Bestandteile für den Abschluss und die Abwicklung von Verträgen im Energiesektor, zum Beispiel für die Energielieferung, den Erwerb von Grünstromzertifikaten etc., und von Vorgängen innerhalb von Unternehmen, beispielsweise für die Abrechnung getätigter Lieferungen. Ökonomisch spricht man dabei von Transaktionen. Bei der Nutzung des Marktes (z. B. für Kauf, Verkauf oder Miete) oder innerbetrieblicher Hierarchien entstehen Transaktionskosten, sowohl vor (z. B. Anbahnungs- und Informationsbeschaffungskosten) als auch während (z. B. Verhandlungs- und Einigungskosten) und nach Abschluss der Transaktion (z. B. Kontroll- und Anpassungskosten). Je spezifischer die Transaktion und je geringer die Häufigkeit, desto höher fallen diese Kosten pro Transaktion aus.

Für die Identitätsfeststellung, die am Anfang aller Transaktionen im Energiesektor steht, fallen hauptsächlich Anbahnungs- und Informationsbeschaffungskosten an. Für die Teilnahme an einem (lokalen) Strommarkt und am Grünstromzertifikatehandel oder bei Vertragsabschlüssen mit Aggregatoren müssen die Stammdaten einer Anlage und der Betreiber dem jeweiligen Transaktionspartner bekannt sein. Dies erfordert die fehlerfreie und fälschungssichere Informationsübermittlung. In der aktuellen Situation (ohne automatisierte Geräteanbindung und digitale Identitätsverwaltung) sind eine manuelle Registrierung der Anlagenbetreiber und Anlagen sowie eine Kontrolle (zum Teil mit Vor-Ort-Begehungen) und gegebenenfalls manuelle Korrektur der Angaben für jeden einzelnen Anwendungsfall erforderlich. Die Abfrage der benötigten Daten ist nicht standardisiert, sodass auch die Eingabe jeweils individuell angepasst werden muss.

Im Anwendungsfall Grünstromzertifikate (siehe Kapitel 5.2) ist zum Beispiel zunächst die Anmeldung des Anlagenbetreibers und der Anlage im Herkunftsnachweisregister (HKNR) erforderlich. Sie erfolgt durch die manuelle Registrierung (elektronisches Formular) des Betreibers, inklusive eines PostIdent-Verfahrens zum Nachweis der Identität, sowie die manuelle Registrierung der Anlage. Für Letztere muss der Anlagenbetreiber eine Reihe von Daten übermitteln (z. B. Standort, Netzbetreiber, Energieträger etc., nach § 21 HkRNDV). Der zuständige Netzbetreiber muss anschließend ebenfalls die Stammdaten der Anlage an die Registerverwaltung übermitteln. Bei bestimmten Anlagen ist für die Registrierung zusätzlich die Bestätigung der Richtigkeit der Angaben durch einen Umweltgutachter erforderlich.

Im Anwendungsfall der Netzdienstleistungen von Kleinanlagen und Fahrzeugen (siehe Kapitel 5.3) wäre der Eintrag der Anlagenstammdaten im Marktregister erforderlich. Anschließend würden diese durch den zuständigen Netzbetreiber geprüft und einem Marktgebiet zugeordnet (vgl. z. B. für den Flexmarkt im SINTEG-Projekt enera (enera 2021)). Wird auch Regelenergie als eine Form der Flexibilität mitbetrachtet, so wäre im aktuellen Fall auch die Übermittlung der relevanten Anlagendaten an den Übertragungsnetzbetreiber als Teil der Präqualifikation einer Anlage notwendig. Für den Anwendungsfall der Energy Communities bzw. des Peer-to-Peer-Handels zwischen Prosumern (siehe Kapitel 5.5) gibt es aktuell nur den teilweise vergleichbaren Referenzfall des Energiegroßhandels – über die Börse oder den „Over-the-Counter"-Handel. Auch hier gibt es jeweils spezifische Verfahren zur Identitätsfeststellung.

In allen aktuellen Prozessen der Identitätsfeststellung im Energiesektor fallen folglich Transaktionskosten für die Beschaffung der notwendigen Informationen und das Ausfüllen der Formulare durch die Betreiber sowie für die Prüfung der Angaben und gegebenenfalls die Korrektur der Daten durch Netzbetreiber, Registerbetreiber und unter Umständen Umweltgutachter an. Quantifizieren lassen sich diese Kosten etwa in Zeitaufwand, Personalkosten, Fahrtkosten für Vor-Ort-Termine, Registrierungsgebühren etc. Ähnliche Identitätsfeststellungsverfahren mit den entsprechend verbundenen Transaktionskosten sind für weitere Anwendungsfälle erforderlich. Die Identitätsfeststellung erfolgt jeweils einmalig (geringe Häufigkeit) und die Eingabe der Daten findet manuell statt, obwohl oftmals die gleichen Daten je Anwendungsfall benötigt werden, und ist nicht standardisiert (mittlere bis hohe Spezifität).

Dies ist zumindest der Fall, solange es kein einzelnes zentrales und fälschungssicheres Register aller Anlagenstammdaten gibt, dem alle Transaktionspartner vertrauen. Das Marktstammdatenregister (MaStR) der Bundesnetzagentur könnte perspektivisch diese Rolle übernehmen, erfüllt sie aber aktuell noch nicht vollumfänglich. Dies zeigt sich zum Beispiel daran, dass das ebenfalls durch eine Behörde geführte Herkunftsnachweisregister nicht auf die Stammdaten im MaStR zurückgreift, sondern die gleichen Daten noch einmal beim Besitzer bzw. Anlagenbetreiber und beim Netzbetreiber abfragt.

Die aktuell genutzten Verfahren zur Identitätsfeststellung haben zur Folge, dass in jedem Anwendungsfall die Haltung und Pflege der erfassten Anlagen- und Betreiberdaten notwendig werden. Da in den Fällen häufig die gleichen Daten erforderlich sind, kommt es zu einer redundanten Datenhaltung. Zudem erhöht dies den Anpassungsaufwand, wenn sich Änderungen in den Stammdaten ergeben. Sie müssen wiederum an alle Stellen, die diese Daten vorhalten, übermittelt und gegebenenfalls von ihnen überprüft werden.

Wie die Beispiele aus den Anwendungsfällen zeigen, können die beschriebenen Transaktionskosten je Identifikationsprozess durchaus relevante Größenordnungen erreichen, die in Summe dazu führen können, dass es insbesondere für verteilte Anlagen (Dach-PV-Anlagen, Wärmepumpen, Batteriespeicher etc.) kaum einen wirtschaftlichen Anreiz gibt, an den beschriebenen Anwendungsfällen zu partizipieren. Zwar sind die Aufwände zur Identifikation nur ein Aspekt unter mehreren, die insbesondere verteilte Anlagen von einem Markteintritt abhalten, ein Markteintritt dezentraler Anlagen könnte aber durch eine Reduktion dieser Transaktionskosten durchaus erleichtert werden.

Auch bei der Identitätsfeststellung unter Verwendung des BMIL müssen die Stammdaten der Anlagen und Betreiber fehlerfrei und manipulationssicher erfasst sein und sicher übermittelt werden können. Allerdings ist bei diesem Ansatz die Herstellung einer vertrauenswürdigen Identität nur einmal (und nicht für jeden Anwendungsfall von Neuem) erforderlich. Dies kann zum Beispiel durch die Inbetriebnahme der Anlage einschließlich der Bestätigung der Stammdaten durch einen autorisierten Installateur (Attester) und die Überprüfung durch einen Dritten (Verifier, z. B. Verteilnetzbetreiber, Übertragungsnetzbetreiber oder andere) umgesetzt werden. Das Vertrauen in die Integrität der Daten wird dann über die Blockchain hergestellt. Sobald die Vertrauenskette einmal aufgestellt ist, wird die Identitätsfeststellung für die verschiedensten Anwendungsfälle vereinfacht; der Zugriff auf die benötigten Stammdaten kann über den DL-Ansatz (Distributed Ledger) automatisiert erfolgen, vorausgesetzt der Betreiber stimmt dem zu. Der Eigentümer des Anwendungsfalls prüft die bereitgestellten Daten und erteilt bei positivem Ergebnis anschließend die Freigabe für den Anwendungsfall.

Damit könnten die oben skizzierten Kosten zur Informationsbeschaffung für alle Transaktionspartner deutlich reduziert werden – so würden etwa manuelle Eingaben, Prüfungen und Korrekturen der Daten, Vor-Ort-Termine etc. für die verschiedenen Anwendungsfälle entfallen oder zumindest stark reduziert werden. Dabei gilt, dass die tatsächlichen Einsparungen bei den Transaktionskosten fallabhängig sind und für jeden Anwendungsfall individuell quantifiziert werden müssten, um das gesamte Einsparungspotenzial einer sicheren automatisierten Geräteanbindung und digitalen Identitätsverwaltung zu beziffern.

Das Potenzial zur Transaktionskostensenkung der BMIL-Lösung hängt von der Standardisierung der übermittelten Stammdaten, der Verbreitung und Interoperabilität der SSI-Lösungen sowie der Ausgestaltung der Blockchain-Lösung ab. Sollten die übermittelten Stammdaten etwa nicht alle für einen spezifischen Anwendungsfall notwendigen Daten enthalten, müssten diese wiederum bei der Anmeldung zusätzlich angegeben und überprüft werden, was entsprechende Transaktionskosten verursachen würde. **Ebenso würde das Kostensenkungspotenzial durch mangelnde Verbreitung oder Interoperabilität der SSI-Lösung(en) eingeschränkt.** Auch die Identitätsfeststellung im BMIL Ansatz verläuft nicht völlig transaktionskostenlos, vielmehr hängen die Kosten von der Rechenleistung der Blockchain ab.

Auf ähnliche Weise wie bei der ersten Erfassung kann der **DL-Ansatz die Transaktionskosten des Identitätsmanagements für den Fall reduzieren, dass sich die Stammdaten ändern** (z. B. durch Vergrößerung der Anlage, Standortwechsel des Betreibers etc.) oder Ergänzungen notwendig werden. In diesem Fall können wiederum die Angaben einmalig dezentral bestätigt und durch Dritte überprüft sowie über die Blockchain unveränderlich festgeschrieben werden. Eine Korrektur der Daten bei allen Transaktionspartnern und zentralen Registern entfällt. Dies ermöglicht es zudem, den Anforderungen verschiedener und zukünftiger Anwendungsfälle gerecht zu werden. **Insgesamt könnte so eine redundante Datenhaltung entfallen,** da nicht mehr jeder Marktakteur, der mit einer Anlage interagieren will, die Anlagendaten individuell vorhalten muss, sondern über den DL-Ansatz beim Betreiber selbst auf sie zugreifen kann.

Allen drei Anbindungsvarianten ist gemeinsam, dass sie die Transaktionskosten des Identitätsfeststellungsprozesses (potenziell signifikant) reduzieren und über die Nutzung der Blockchain-Technologie eine hohe Datensicherheit gewährleisten können. Wie genau das Kosten-Nutzen-Verhältnis bei den Anbindungsvarianten ausfällt, hängt auch maßgeblich davon ab, welches **Potenzial für Synergien mit der SMGW-Infrastruktur besteht und wie diese Synergien gehoben werden können.** Diesen Aspekt greifen wir im Folgenden kurz auf.

Effizienzgewinne durch Hebung von Synergieeffekten (Economies of Scope) und mögliche Wettbewerbseffekte

Die Synergiepotenziale der Anbindungsvarianten beziehen sich zum einen auf die Nutzung der sicheren Infrastruktur rund um das SMGW, zum einen auch auf den SMGW-Rollout selbst. Da alle drei betrachteten Anbindungsvarianten auf der gesicherten SMGW-Infrastruktur aufbauen, werden redundante Infrastrukturen (deren Kosten erheblich wären, wenn sie ein ähnlich hohes Sicherheitsniveau wie das SMGW erreichen sollen) vermieden.

Darüber hinaus können aber auch **Synergien in Bezug auf den SMGW-Rollout** mit dem in allen Anbindungsvarianten notwendigen, mit dem SMGW verbundenen CLS-Proxy entstehen. Hierbei **unterscheidet sich das Potenzial zur Hebung von Synergieeffekten zwischen den Anbindungsvarianten.** Wir unterscheiden hier vier Fälle, bei denen unterschiedliche Wettbewerbseffekte zu erwarten wären:

		Installation mit SMGW	
		Gemeinsam	**Getrennt / nachträglich**
Art des CLS-Endpunktes	**„Einfacher“ durchleitender CLS-Proxy**	a	b
	Mehrwertmodul (leistungsstarkes CLS-Modul)	c	d

Tabelle 2: Unterschiedliches Potenzial zur Hebung von Synergieeffekten zwischen den Anbindungsvarianten

Die Besonderheit der Anbindungsvariante über das Mehrwertmodul liegt darin, dass das Mehrwertmodul selbst als CLS-Proxy fungiert. Daher kann es hier nur zu Synergieeffekten mit dem SMGW-Rollout kommen, wenn ein solches leistungsstarkes Modul mit dem SMGW zusammen installiert wird (Fall c). Die Anbindungsvarianten über ein CLS-Device setzen hingegen lediglich voraus, dass ein CLS-Proxy vorhanden ist. Dabei kann es sich auch um ein Mehrwertmodul handeln, das gleichzeitig als CLS-Proxy für CLS-Devices fungiert. Hier können folglich in potenziell mehr Fällen (a und c) Synergieeffekte mit dem SMGW entstehen als bei der Anbindungsvariante über das Mehrwertmodul.

Bei einer nachträglichen Installation von CLS-Proxy oder Mehrwertmodul (Fälle b und d) müssten die Installation und die Anbindung des CLS-Proxys bzw. des Mehrwertmoduls durch den Gateway-Administrator separat erfolgen. Dies würde zu zusätzlichen Kosten im Vergleich zu den Fällen a und c führen. Ob sich diese nachträgliche Investition lohnt, hängt dann entscheidend von der Anzahl der CLS-Devices ab, über die sich die Kosten verteilen, und / oder von den Mehrwerten, die durch die Anbindung der CLS-Devices bzw. durch die Anwendungen auf dem Mehrwertmodul gehoben werden können.

Die Wirtschaftlichkeit der Nachrüstung eines CLS-Proxys (oder Mehrwertmoduls) hängt auch davon ab, ob bereits ein Mehrwertmodul (oder ein CLS-Proxy) vorhanden ist (z. B. in den Fällen a und c), das heißt davon, ob der zusätzliche Nutzen der dann ermöglichten Anbindungsvariante die zusätzlichen Kosten deckt. In dem obigen Szenario eines Mehrfamilienhauses wird dieser Bezug deutlich: Zum einen sinken die durchschnittlichen Anschlusskosten für den CLS-Proxy (bzw. das Mehrwertmodul) mit der Anzahl der CLS-Devices (bzw. der an das Mehrwertmodul angeschlossenen Geräte), die in dem Haus genutzt werden. Gleichzeitig ist aber auch entscheidend, ob in dem Mehrfamilienhaus (gemeinsam mit dem SMGW) ein CLS-Proxy oder ein Mehrwertmodul verbaut wurde. Davon hängt ab, welche Anwendungen durch welche Geräte in dem Haus genutzt werden können. Wird etwa ein Wechselrichter nachgerüstet und ein CLS-Proxy ist vorhanden, so kann hier frei zwischen verschiedenen CLS-Devices gewählt werden. Ist hingegen ein Mehrwertmodul verbaut, dann kann entweder ein Wechselrichter genutzt werden, der von dem Mehrwertmodul (bzw. den Anwendungen darauf) unterstützt wird, oder es muss ein CLS-Proxy-Kanal durch das Mehrwertmodul bereitgestellt werden, um die gleiche Wahlfreiheit zu haben wie im Falle der Anbindung über das CLS-Device. Wird dieser Kanal durch das Mehrwertmodul nicht bereitgestellt, wird die Wahlfreiheit der Bewohnerinnen und Bewohner des Mehrfamilienhauses eingeschränkt.

Offen ist in allen Fällen auch die Frage, welcher Akteur einen CLS-Proxy und seine Einbindung beauftragen kann: Muss dies immer zwangsläufig über den Messstellenbetreiber laufen oder ist dieser lediglich notwendig, um die Einbindung über den Gateway-Administrator sicherzustellen? Fraglich ist dann, ob die separate nachträgliche Installation eines CLS-Proxys oder eines Mehrwertmoduls dennoch wirtschaftlich darstellbar ist. Die Wirtschaftlichkeit der Nachrüstung entscheidet darüber, ob Wettbewerb zwischen verschiedenen CLS-Proxy-Anbietern bzw.

entsprechend auch zwischen verschiedenen Mehrwertmodulen entstehen kann (Competition in the Market) oder ob die Kosten der nachträglichen Installation des CLS-Proxys bzw. des Mehrwertmoduls nicht eher für eine Competition for the Market sprechen.

Ein weiterer wettbewerbsrelevanter Aspekt auch bei einer gemeinsamen Installation mit dem SMGW (Fall a und Fall c) ist die Frage, ob eine – wenngleich grundsätzlich technisch mögliche – Kombination von verschiedenen Herstellern für SMWG und CLS-Proxy wirtschaftlich darstellbar ist oder ob die potenziellen Kosteneinsparungen (Synergieeffekte bei Bestellung und Ausführung) durch die Nutzung eines Lieferanten für beide Geräte dazu führen, dass SMGW und CLS-Proxy von einem Hersteller bezogen und direkt gemeinsam installiert werden. Sollte Letzteres der Fall sein, könnte das bedeuten, dass der Wettbewerb auf dem Markt für Messstellen ausschlaggebend für mögliche Wettbewerbseffekte bei den CLS-Proxys (einschließlich Mehrwertmodulen) und damit für die Anbindungsvarianten würde. Dies kann unterschiedliche Effekte auf die verschiedenen Anbindungsvarianten haben, je nachdem, ob der installierte CLS-Proxy die Anbindungsvariante ermöglicht oder nicht. Die Anbindungsvarianten über CLS-Devices wären sowohl mit einem „einfachen“ CLS-Proxy als auch mit einem Mehrwertmodul möglich. Sie würden nur dann verhindert, wenn ein Mehrwertmodul installiert wird, das nicht gleichzeitig als CLS-Proxy für weitere CLS-Devices fungiert. Im Falle des Mehrwertmoduls sind die potenziellen Wettbewerbseffekte etwas anders gelagert: Diese Anbindungsvariante würde potenziell unwirtschaftlicher, wenn bereits vorher ein „einfacher“ CLS-Proxy installiert wurde.

Für die Anbindungsvariante über das Mehrwertmodul ist dann die zentrale Fragestellung, ob der Marktzutritt in den CLS-Proxy-Markt hinreichend gesichert ist oder ob der Marktzugang durch Abhängigkeiten vom Messstellenmarkt und vom Wettbewerb zwischen verschiedenen Messstellenbetreibern eingeschränkt wird. Durch die Abhängigkeit von einem Mehrwertmodul würden sich etwaige Markteintrittsbarrieren auf CLS-Proxy-Ebene daher potenziell stärker auf das Mehrwertmodul und dessen Diffusion im Markt auswirken, als dies bei einem CLS-Device der Fall wäre, solange immer ein CLS-Proxy vorhanden ist, um ein CLS-Device anzubinden. Im Kern bedeutet dies: Während eine nachträgliche Installation eines CLS-Device in Ergänzung zu einem anderen CLS-Device durchaus wirtschaftlich sein kann, ist eine nachträgliche Installation eines Mehrwertmoduls in Ergänzung zu einem vorhandenen CLS-Device (inklusive CLS Proxy) wahrscheinlich aus den oben genannten Gründen wirtschaftlich schwieriger darstellbar. Zu prüfen wäre hier insbesondere, inwiefern der Wettbewerb zwischen den Messstellenherstellern die möglichen Effizienzgewinne durch den Wettbewerb zwischen verschiedenen Mehrwertmodul-Anbietern limitiert. Da das Mehrwertmodul zusätzlich noch in Konkurrenz zu den anderen Anbindungsvarianten steht, kann sich so eine komplexe Wettbewerbssituation für die Mehrwertmodul-Anbieter ergeben. Hier gibt es noch umfassenden Klärungsbedarf, um insbesondere die Vor- und Nachteile durch einen gemeinsamen Rollout der Mehrwertmodule (wie auch des CLS-Proxys) mit dem SMGW zu bewerten. **Insbesondere gilt es, den potenziellen Trade-off zwischen Kostenersparnissen bei der Installation der Geräte gegen die potenzielle Einschränkung von Wettbewerb (und damit von Effizienzvorteilen) abzuwägen.**

Über die Synergien mit dem SMGW-Rollout hinaus können sich die Installationskosten der Anbindungsvarianten weiterhin (potenziell signifikant) unterscheiden. Bei den beiden Anbindungsvarianten mit Nutzung eines dedizierten CLS-Device erfolgt die Installation über die technische Aufrüstung der Endgeräte (z. B. Wechselrichter, Wärmepumpe oder Ladestation). Im Rahmen des Piloten wurde dies durch die Nachrüstung einer OLI Box umgesetzt. Eine solche nachträgliche Anbindung an den BMIL ist zwar technisch möglich, führt allerdings zu zusätzlichen Installationskosten für die Anbindung des CLS-Device. Perspektivisch könnten aber die technischen Voraussetzungen (Kryptochip und Logik) für die Anbindung an den BMIL auch direkt durch die Hersteller der Geräte geschaffen werden. Eine entsprechende Nachrüstung eines CLS-Device könnte dann entfallen und die Anbindung der Endgeräte an den BMIL (über einen bereits vorhandenen oder nachzurüstenden CLS-Proxy) direkt bei deren Installation erfolgen. Letzteres würde die Transaktionskosten der Anbindung über ein CLS-Device deutlich reduzieren.

Die alternative Anbindung erfolgt über ein SMGW-Mehrwertmodul, dessen Installationskosten primär davon abhängen, ob das Mehrwertmodul direkt mit dem SMGW installiert wird oder ob es zu einem nachträglichen Einbau kommt. Im Falle des nachträglichen Einbaus (Fall d) ergibt sich die analoge Situation wie beim dedizierten CLS-Device, dass hier je Geräte-Installation zusätzliche Kosten entstehen. Jedoch fallen diese bei dem SMGW-Mehrwertmodul nur einmalig an, wohingegen ein dediziertes CLS-Device je Endgerät installiert werden müsste. Im Falle der Nachrüstung wäre also davon auszugehen, dass die Installationskosten für die Nachrüstung beim SMGW-Mehrwertmodul

(Fall d) niedriger sind als bei einem dedizierten CLS-Device (Fall b), zumindest wenn mehr als ein Endgerät über das SMGW-Mehrwertmodul an den BMIL angeschlossen wird. Dieser Unterschied hat besteht aber nicht mehr, wenn das CLS-Device direkt in den Endgeräten verbaut wird, da dann kein zusätzlicher Aufwand bei der Installation gegenüber der reinen Installation der Endgeräte entsteht.

Bei allen drei Anbindungsvarianten könnten die Kosten für die Anbindung an den BMIL signifikant durch die Installationskosten beeinflusst werden, jedoch könnten sich hier auch relevante Markteintrittsbarrieren für die Anbieter von Identifikationsinfrastruktur (Mehrwertmodule, CLS-Devices) ergeben. Wie oben schon skizziert wurde, gilt es noch zu klären, inwiefern solche Markteintrittsbarrieren bei der Installation im Falle der Nutzung eines SMGW-Mehrwertmoduls entstehen und ob die potenziellen Effizienzverluste durch den eingeschränkten Wettbewerb durch andere Vorteile der Anbindungsvariante gerechtfertigt werden können. Im Falle eines dedizierten CLS-Device wäre hingegen zu erwarten, dass sich hier analog zu dem Wettbewerb bei den Endgeräten (Wechselrichter, Ladestationen etc.) Wettbewerb einstellt und daher geringere Markteintrittsbarrieren entstehen.

Ein weiterer Unterschied zwischen den Anbindungsvarianten besteht in der Möglichkeit, den Wettbewerb im Anwendungsbereich potenziell zu begrenzen. Während die Anbindung durch ein SMGW-Mehrwertmodul die Nutzung von Anwendungen auf die von dem Mehrwertmodul unterstützten Services beschränken kann (es sei denn, das Mehrwertmodul bietet auch einen Proxy-Kanal für weitere CLS-Devices), ist die Auswahl bei den dedizierten CLS-Devices kaum beschränkt und kann beliebig (soweit ein entsprechend günstiges Kosten-Nutzen-Verhältnis besteht) erweitert werden. Auch hier sind wieder verschiedene wettbewerbliche Ausprägungen denkbar. Zum einen wäre es möglich, dass es primär zu einem Plattformwettbewerb zwischen verschiedenen Mehrwertmodul-Anbietern kommt, der letztlich in einer stärkeren Konzentration mündet. Dies hätte dann für die Anbieter von Anwendungen den Vorteil, dass sie über einzelne Plattformen einen größeren Markt erschließen können. Allerdings können sich so auch Wettbewerbseinschränkungen ergeben, insbesondere wenn es zu Markteintrittshürden bei den Plattformen kommt. Ein Plattformwettbewerb mit den entsprechenden Entwicklungen könnte auch bei der Cloud-Edge-Lösung mit CLS-Devices entstehen. Alternativ könnte sich ein plattformunabhängiger Wettbewerb basierend auf den CLS-Devices entwickeln, der dann stärker zu einer hohen Auswahl an verschiedenen Anbietern führt. Dies kann zum einen Effizienzvorteile bieten, aber zum anderen auch die Gefahr von Koordinationsverlusten bergen. Drittens wäre auch eine Kombination der Modelle möglich, bei denen die Mehrwertmodule als CLS-Proxy für weitere CLS-Devices fungieren. Dabei würde es zu einer Art Plattformwettbewerb zwischen den Mehrwertmodulen kommen, der aber um weitere Anbieter ergänzt würde, die nicht das Mehrwertmodul-Ökosystem selbst, sondern die Mehrwertmodule lediglich als Anbindung an die sichere SMGW-Infrastruktur nutzen.

Welche Rahmenbedingungen geschaffen werden sollten, um diese Wettbewerbsformen zu ermöglichen, gilt es weiter zu untersuchen. Insbesondere stellt sich hier die Frage, **ob es im bestehenden Rahmen Hemmnisse für die jeweiligen Anbindungsvarianten gibt, die einen fairen Technologiewettbewerb zwischen den Varianten (bzw. auch weiteren möglichen Anbindungsvarianten) ausschließen,** und wie diese Hemmnisse adressiert werden könnten (vergleiche dazu einführend unten bei der regulatorischen Evaluation). Wie in der technischen Evaluation bereits skizziert, kann die Bandbreite der kommunikativen Anbindung des SMGW auch im Falle der dedizierten CLS-Devices eingrenzend auf den Wettbewerb wirken. Wird die vorhandene Kapazität zur Datenübertragung ausgeschöpft, stellt sich dann die Frage, wie diese knappe Ressource zwischen den verschiedenen Nutzern aufgeteilt wird. Es sollte geprüft werden, inwieweit hier ein weiterer Regelungsbedarf besteht, um den Wettbewerb nicht auszubremsen und entsprechende Rahmenbedingungen zu definieren.

Bei der Anbindung über ein dediziertes CLS-Device gilt es dann noch zwischen der Anwendung des Cloud-Edge-Ansatzes und der dezentralen Lösung zu unterscheiden, bei der nicht nur die Datenspeicherung, sondern auch die Logiken und Anwendungen dezentral ausgeführt werden. In Bezug auf die Transaktionskosten ermöglicht die Cloud-Edge-Variante, dass Anwendungen skaliert werden können, ohne durch die Bandbreite der Telekommunikationsinfrastruktur des SMGW eingeschränkt zu werden. Potenziell ließen sich so etwaige wettbewerbslimitierende Faktoren, die sich durch die Kommunikationsinfrastruktur des SMGW ergeben könnten, umgehen. Zudem könnte ein (leicht) senkender Effekt auf die Transaktionskosten der Identitätsfeststellung bei der Cloud-Lösung durch potenziell kürzere Antwortzeiten und eine weniger störanfällige Kommunikationsinfrastruktur im Vergleich zur dezentralen Lösung

entstehen. Welche der beiden Lösungen dabei aber aus ökonomischer Sicht sinnvoller ist, wird nicht nur durch die Transaktionskosten bestimmt und muss fallabhängig untersucht werden.

4.3.3.2 Zentrale Herausforderung auf dem Weg zur Serienimplementierung: Interoperabilität

Eine **zentrale Voraussetzung**, um die oben beschriebenen Potenziale zur Reduktion der Transaktionskosten bei der Identitätsfeststellung zu heben, ist die **Interoperabilität der digitalen Identitäten**. Ohne eine solche Interoperabilität wird ein wesentlicher Teil der oben beschriebenen Effizienzsteigerungen, die durch einen BMIL theoretisch möglich wären, nicht realisiert. Gleichzeitig reduziert sich auch das Anwendungspotenzial des BMIL, je geringer die Interoperabilität zwischen verschiedenen Anbindungsvarianten und Services, die auf dem BMIL aufsetzen könnten, ist. Zentraler Ansatzpunkt ist hier die Interoperabilität zwischen den genutzten Datenmodellen für Verifiable Credentials, Wallets und die zu generierenden DIDs. Zwar gibt es zu diesen zentralen Elementen des SSI-Konzepts erste Standardisierungsinitiativen, sie sind aktuell aber noch nicht Teil eines industrieweiten Standardisierungskonzepts im Energiesektor.

Aus ökonomischer Sicht basiert das SSI-Konzept bzw. basieren die Potenziale, die mit dem SSI-Konzept gehoben werden können, primär auf Netzwerkeffekten. Das heißt, der Nutzen der SSI für den einzelnen Anwender nimmt mit der steigenden Gesamtzahl der SSI-Anwender zu. Anders ausgedrückt: Je mehr Anwendungen die SSI unterstützen, desto interessanter ist die Nutzung von SSI für die verschiedenen Anwender. Je mehr Anwender eine SSI besitzen, desto interessanter ist es für die Anwendungsanbieter, eine SSI zu unterstützen. Im Endeffekt benötigt der SSI-basierte BMIL eine kritische Größe an Anwendungen und Anwendern, um nachhaltig im Einsatz zu bleiben und einen relevanten Teil der im Energiesektor notwendigen Identifikationsprozesse bedienen zu können.[74]

Grundsätzlich könnte hier Wettbewerb zwischen verschiedenen Initiativen zur Standardisierung der SSI genutzt werden, um über den Markt den Standard mit dem größten Marktpotenzial zu identifizieren. Hier wäre dann auch denkbar, dass zwischen den Lösungsansätzen zur Identitätsfeststellung, die sich am Markt durchsetzen, Interoperabilität hergestellt wird. Dies ist aber nicht zwangsläufig im Interesse der Anbieter der jeweiligen Lösung, da Interoperabilität eventuell die Wettbewerbsintensität erhöhen (bzw. Markteintrittshürden abbauen) könnte. Diese Anreizproblematik kann wiederum die Interoperabilität verschiedener SSI-Konzepte einschränken. Es besteht hier dann ein zentraler Zielkonflikt zwischen potenziellen Effizienzgewinnen durch Wettbewerb bei der Standardisierung der SSI einerseits und einer nur eingeschränkten Ausnutzung des Potenzials von SSI zur Transaktionskostenreduzierung durch potenziell mangelnde Interoperabilität andererseits. **Darüber hinaus besteht auch das Risiko, das aufgrund von Pfadabhängigkeiten und eines aus Sicht der Anwender erhöhten Risikos, auf den falschen Standard zu setzen, es erst gar nicht zur Anwendung eines SSI-Konzepts kommt,** da ein relevanter Anteil der Investoren abwartet und so nie eine kritische Masse an Anwendern erreicht wird.

Im Falle des Energiesektors **bestehen solche Pfadabhängigkeiten insbesondere durch das bereits etablierte und verpflichtende Marktstammdatenregister, die Einbindung des MaStR in unternehmensinterne Prozesse und getätigte Investitionen in alternative Identifikationsmaßnahmen** bzw. Prozesse, die zwar zu hohen Datenredundanzen führen, aber bereits Teil der etablierten Prozesse sind (z. B. das Herkunftsnachweisverfahren für den Grünstromzertifikatehandel). Eine Umstellung der etablierten Prozesse zur Identifikation einzelner Akteure auf einen SSI-basierten Ansatz, wie er mit dem BMIL verfolgt wird, würde dann dazu führen, dass diese Investitionen zu versunkenen Kosten werden und entsprechend abgeschrieben werden müssen. Gleichzeitig müssten weitere Investitionen getätigt werden, um eine Anbindung an den BMIL herzustellen und die unternehmensinternen Prozesse entsprechend umzustellen. Zusammengenommen können so (erhebliche) **Umstellungshemmnisse für den BMIL-Ansatz entstehen, die eine breite Diffusion von SSI-basierten Ansätzen behindern.** Damit könnte die Wahrscheinlichkeit sinken, dass eine kritische Masse an Anwendern erreicht wird, die das SSI-basierte Identifikationskonzept umsetzen, die aber aufgrund der Netzwerkeffekte notwendig wäre, um eine marktgetriebene Verbreitung des SSI-basierten Ansatzes sicherzustellen. Aufgrund dieser Hemmnisse erscheint es aus heutiger Sicht nicht gesichert, dass sich ohne eine entsprechende institutionelle Standardisierung der Datenmodelle im Kontext der SSI ein SSI-basierter Ansatz wie der BMIL im Energiesektor durchsetzen kann. **Damit wird die frühzeitige Etablierung eines entsprechenden Standards für SSI im Energiesektor zu einer zentralen Weichenstellung für die Serienimplementierung des BMIL-Ansatzes.** Um entsprechende Pfadabhängigkeiten zu überbrücken, ist aus heutiger Sicht auch fraglich, inwiefern nicht nur die grundlegenden Elemente

74 In der Literatur wird dies unter dem Konzept der kritischen Masse und den Risiken von Excess Inertia diskutiert (vgl. Cabral 2000).

der SSI standardisiert werden sollten, sondern ob auch ein Bedarf besteht, die Dateninfrastruktur, in der die Identitäten verwaltet werden (im Falle des BMIL die Blockchain-Anwendung), zu standardisieren. Einerseits sprechen der geringe Technologiereifegrad und das damit einhergehende perspektivische Weiterentwicklungspotenzial dafür, hier zunächst einen Technologiewettbewerb zu ermöglichen, um die effektivsten und effizientesten technologischen Lösungsmöglichkeiten zu identifizieren. Andererseits kann aber bei einer geringen Interoperabilität der verschiedenen Blockchain-Anwendungen die Diffusion der SSI-Anwendungen generell ausgebremst werden (siehe die Argumente zuvor zur kritischen Masse und zu den Netzwerkeffekten). Hier gilt es, noch genauer zu prüfen, wie weit sich der Standardisierungsbedarf erstreckt bzw. inwiefern durch entsprechende Interoperabilitätskonzepte hinreichende Wettbewerbsfähigkeit sichergestellt werden kann.

4.3.3.3 Zusammenfassung der ökonomischen Bewertung

Im Rahmen der ökonomischen Betrachtung sind drei Kerneinsichten hervorzuheben:

Erstens haben alle drei Anbindungsvarianten einen **Lösungsweg aufgezeigt, um das Potenzial von digitalen Identitäten zur Transaktionskostenreduzierung für verschiedene Anwendungsfälle im Energiesektor zu erschließen.** Dieses Potenzial wird in Kapitel 5 anhand der Anwendungsfälle skizziert. Wesentlich ist dabei für die vorliegende Betrachtung, dass alle drei Anbindungsvarianten einen potenziellen Lösungsweg darstellen, um diese Effizienzgewinne im Energiesektor zu realisieren. Dabei gilt jedoch, dass **die verschiedenen Anbindungsvarianten verschiedene Kosten und unterschiedliche Nutzen und Mehrwerte erzeugen können.** Dies impliziert, dass in dieser frühen Phase der Entwicklung der verschiedenen Anbindungsvarianten die **Sicherung eines effektiven Technologiewettbewerbs** hohe Priorität haben sollte, um hier keine Technologieoption zu diskriminieren.

Zweitens zeigen die Betrachtungen auch, dass es verschiedene wettbewerbsrelevante Aspekte zu beachten gilt, die potenziell den Technologiewettbewerb zwischen den Anbindungsvarianten signifikant beeinflussen könnten. Dies bezieht sich zum einen auf **mögliche Pfadabhängigkeiten im Kontext des Smart-Meter-Rollouts (Synergieeffekte)** und mögliche **Markteintrittsbarrieren durch Rückwirkungen des Wettbewerbs im Messstellenmarkt auf die möglichen Anbindungsvarianten.** Zum anderen könnten die **verschiedenen Wettbewerbsformen (insbesondere Plattformwettbewerb)** bei den Anwendungen, die auf den Anbindungsvarianten basieren, **auf den Wettbewerb zwischen verschiedenen Anbindungsvarianten rückwirken. Diese potenziellen Hemmnisse sollten weiter untersucht werden,** um mögliche Handlungsoptionen zu entwickeln, mit denen Technologiewettbewerb zwischen verschiedenen Anbindungsvarianten gesichert werden kann.

Drittens gilt es, die **Interoperabilität insbesondere im Kontext der SSI sicherzustellen.** Hier zeigen die obigen Betrachtungen, dass **Netzwerkeffekte** eine relevante Rolle im Kontext der SSI spielen. Zur Überwindung von **Pfadabhängigkeiten könnte im Energiesektor eine Standardisierung der SSI-Bestandteile notwendig** sein, um so eine stärkere Marktdurchdringung des SSI-Konzepts überhaupt zu ermöglichen. Daher sollte geprüft werden, in welchen Bereichen eine Standardisierung des SSI-Konzepts im Energiesektor vorangetrieben werden kann, ohne den Technologiewettbewerb einzuschränken und gleichzeitig mögliche Synergien mit anderen Sektoren heben zu können.

4.3.4 Rechtliche Bewertung

Die rechtliche und regulatorische Evaluation legt den Fokus, wie in Kapitel 4.3.1 beschrieben, auf die IT-sicherheitsregulatorischen wie auch die datenschutzrechtlichen Anforderungen. Hierbei wurden folgende Aspekte untersucht:

- IT-sicherheitsregulatorische Anforderungen
  - Zuständigkeit und Aufgaben des Smart-Meter-Gateway-Administrators (GWA) (§§ 3 Abs. 1 Satz 2, 25 MsbG)
  - Technische Anforderungen hinsichtlich der Funktionalität und Interoperabilität des SMGW (§§ 22, 23 MsbG i.V.m. den Technischen Richtlinien des BSI)
  - Vorgaben zur Datenkommunikation (§§ 49 ff. MsbG)

- Datenschutzrechtliche Anforderungen
  - Anwendbarkeit der Datenschutz-Grundverordnung (DSGVO) sowie des Bundesdatenschutzgesetzes (BDSG) und Prüfung des Vorliegens personenbezogener Daten
  - Wahrung von Betroffenenrechten
  - Wahrung anderer datenschutzrechtlicher Grundsätze, wie zum Beispiel Datenminimierung und Privacy-by-Design

Im Folgenden wird demnach eine rechtliche Bewertung der Einbindung des Smart-Meter-Gateway sowie der entsprechenden Marktakteure unter Berücksichtigung des Messstellenbetriebsgesetzes (MsbG) und der entsprechenden Technischen

Richtlinien des BSI vorgenommen. Des Weiteren wird die Anwendbarkeit des Datenschutzrechts näher geprüft und der Austausch der Daten im BMIL-Piloten eingeordnet und bewertet. Soweit möglich, werden auch haftungsrechtliche Verantwortlichkeiten für die Qualität der Daten aufgezeigt und bewertet. Schließlich werden Hemmnisse und Herausforderungen für die Serienimplementierung des BMIL abgeleitet und die Verknüpfung zur technischen und ökonomischen Evaluation wird hergestellt. Über die vier Fortschrittsberichte und den iterativen Fragenkatalog hinaus bildet der Anhang (siehe Kapitel 7) die Grundlage für die rechtliche Evaluation. Der Anhang enthält insbesondere Angaben zu den ausgetauschten Daten in den drei Anbindungsvarianten.

4.3.4.1 Die drei Anbindungsvarianten und die Kommunikationswege

Die drei Anbindungsvarianten lassen sich grundsätzlich in folgende **Kommunikationswege** unterteilen:

i. Anlage zu OLI Box / Mehrwertmodul,
ii. OLI Box / Mehrwertmodul zu CLS,
iii. CLS zu SMGW,
iv. SMGW zu EMT und
v. EMT zu Public Domain.
vi. In der gerätezentrierten Identitätsverwaltung im Verbund mit einem dedizierten CLS-Device (Anbindungsvariante 2, siehe Kapitel 4.1.4) besteht die Besonderheit, dass die KILT-Dienste auf der OLI Box direkt mit der KILT Blockchain kommunizieren.
vii. Bei der Cloud-Wallet-basierten Identitätsverwaltung wird die Identität einmalig erstellt und bestimmte damit verbundene Operationen und Rechte werden an einen digitalen Zwilling in einer Cloud delegiert (Anbindungsvariante 3, siehe Kapitel 4.2).

Es ist zu evaluieren, ob die Kommunikationswege die IT-sicherheitsregulatorischen Anforderungen erfüllen. Hierzu sei vorab erwähnt, dass sämtliche im Rahmen des BMIL-Piloten eingesetzten SMGWs und Kommunikationseinheiten des intelligenten Messsystems entweder vom BSI oder von einer dazu autorisierten Stelle zertifiziert sind (siehe auch Kapitel 4.3.2 Technische Bewertung).

4.3.4.2 IT-sicherheitsregulatorische Anforderungen

Zuständigkeiten und Aufgaben des Gateway-Administrators

Die Funktion des Gateway-Administrators (GWA) wird gemäß § 3 Abs. 1 Satz 2 MsbG grundsätzlich dem Messstellenbetreiber zugeordnet. Dem GWA obliegen gemäß § 25 Abs. 1 MsbG folgende Aufgaben:

- Gewährleistung eines zuverlässigen technischen Betriebs des intelligenten Messsystems
- Verantwortung für die Organisation einschließlich der Installation, Inbetriebnahme, Konfiguration, Administration, Überwachung und Wartung des Smart-Meter-Gateway und der informationstechnischen Anbindung von Messgeräten und von anderen an das Smart-Meter-Gateway angebundenen technischen Einrichtungen
- Durchführung von weiteren Anwendungen und Diensten, soweit es technisch möglich und wirtschaftlich zumutbar ist
- Ausschließliche Verwendung von Smart-Meter-Gateways mit gültigen Zertifikaten und unverzügliche Mitteilung von Sicherheitsmängeln und Änderungen von Tatsachen, die für die Erteilung des Zertifikats wesentlich sind, an das BSI

Zudem werden in § 25 Abs. 2 MsbG weitere technische Vorgaben für das intelligente Messsystem gemacht. Gemäß § 25 Abs. 4 MsbG werden weitere organisatorische Anforderungen an den GWA gestellt, deren Erfüllung er durch Zertifikate vom BSI oder von einer Zertifizierungsstelle nach dem Akkreditierungsstellengesetz nachweisen kann. Hierzu gehören unter anderem die Einrichtung, der Betrieb und die Dokumentation eines Informationssicherheitsmanagementsystems. Nach den uns zur Verfügung gestellten Informationen unterstellen wir, dass vorliegend die weiteren organisatorischen Anforderungen und mithin die Anforderungen aus § 25 Abs. 4 MsbG erfüllt wurden. Für eine Serienimplementierung ist es notwendig, sämtliche Aufgaben und Anforderungen dauerhaft zu beachten.

Technische Anforderungen nach dem MsbG

Um ein einheitliches und sehr hohes Sicherheitsniveau zu gewährleisten, erklärt § 22 Abs. 1 i.V.m. Abs. 2 MsbG **Schutzprofile und Technische Richtlinien für intelligente Messsysteme zur Gewährleistung von Datenschutz, Datensicherheit und Interoperabilität** für verbindlich. Sie wurden im Auftrag des BMWK (vormals: BMWi) vom BSI gemeinsam mit Branchenvertretern unter enger Einbindung des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, der Bundesnetzagentur und der Physikalisch-Technischen Bundesanstalt erarbeitet.

Demnach hat das SMGW eines intelligenten Messsystems zur Gewährleistung von Datenschutz, Datensicherheit und Interoperabilität **nach dem Stand der Technik folgende Anforderungen** zu erfüllen:

1. Die Verarbeitung, insbesondere die Erhebung, Zeitstempelung, Übermittlung, Speicherung und Löschung, von Messwerten, damit zusammenhängenden Daten und weiteren über ein intelligentes Messsystem oder Teilen davon geleiteten Daten,

2. Den Zugriffsschutz auf die im elektronischen Speicher- und Verarbeitungsmedium abgelegten Messdaten,

3. Die sichere Zeitsynchronisation des Smart-Meter-Gateway mit einer vertrauenswürdigen Zeitquelle im Weitverkehrsnetz und

4. Die Interoperabilität der intelligenten Messsysteme und Teilen davon.

Die **Einhaltung des Standes der Technik** dieser Anforderungen wird vermutet, **wenn die in der Anlage aufgeführten Schutzprofile und Technischen Richtlinien des BSI oder deren Weiterentwicklungen eingehalten werden.** Aktuell ist die BSI-Richtlinie TR-03109 für die Anforderungen des § 22 Abs. 1 MsbG maßgeblich.

Die Technische Richtlinie TR-03109 enthält für eine Vielzahl von Kommunikationswegen eines intelligenten Messsystems, insbesondere zu den unter 4.3.4.1 aufgeführten, technische Vorgaben. Bei der gerätezentrierten Anbindungsvariante im Verbund mit einem SMGW-Mehrwertmodul (Anbindungsvariante 1, siehe Kapitel 4.1.3) werden sämtliche Kommunikationswege gemäß der BSI TR-03109-4 „Smart Metering PKI – Public Key Infrastruktur für SMGW“ durchgeführt und die eingesetzten Geräte sind entsprechend zertifiziert.

Bei der gleichfalls gerätezentrierten Identitätsverwaltung nach der Anbindungsvariante 2 ist dies ebenso der Fall, lediglich der genannte Kommunikationsweg von OLI Box zu EMT (siehe Kapitel 4.3.4.1, Ziffer vi.) stellt eine Besonderheit dar. Hierzu führt die Richtlinie BSI TR-03109-1 im WAN-Anwendungsfall 6 unter „Kommunikation aktiver EMT mit CLS“ aus, dass die Notwendigkeit der Kommunikation eines aktiven EMT mit einem CLS-Gerät unter Nutzung der Proxy-Funktionalität des SMGW erfolgen muss. Darüberhinausgehend sind in der Technischen Richtlinie keine weiteren nicht funktionalen Anforderungen an diesen Kommunikationsweg definiert (siehe auch Kapitel 4.3.2 Technische Bewertung).

Für die Anbindungsvariante 3, die Cloud-Wallet-Lösung, bestehen kaum Standards für die Ablage des DID in der Cloud. Infolgedessen ist davon auszugehen, dass die Zulässigkeit der Variante sichergestellt ist, da die Projektpartner mit zulässigen Zertifikaten gearbeitet haben.

Alle drei Anbindungsvarianten erfüllen somit die IT-sicherheitsrelevanten Anforderungen nach § 22 MsbG.

Partiell **fehlt** es jedoch an einer **regulatorischen Standardisierung** der Kommunikationswege. Wie in der technischen und ökonomischen Bewertung bereits ausgeführt, ist teilweise unklar, welcher Standard bei den Kommunikationswegen anzuwenden ist. So mangelt es unter anderem bei dem Kommunikationsweg OLI Box zu EMT an einer Festlegung zu Latenzzeiten oder Datendurchsatz. Durch die fehlende regulatorische Standardisierung kann es zu Hemmnissen bei der Serienimplementierung kommen. Denn wenn, wie im visionären Szenario in Abschnitt 4.3.2.2 ausgeführt, mehrere Letztverbraucher Zugriff auf den DID benötigen und keine entsprechenden Mindestdatendurchsätze festgelegt sind, kann dies zu Schwierigkeiten bei der Auslesung der benötigten Daten bei den jeweiligen (zeitgleich) zugreifenden Anwendungen führen. Um diese potenziellen Hemmnisse zu beseitigen, ist eine Konkretisierung der regulatorischen Anforderungen wünschenswert. Mit einer regulatorischen Standardisierung aller im BMIL-Piloten dargestellten Kommunikationswege wäre es für die Marktteilnehmer einfacher, die im MsbG forcierte Interoperabilität herzustellen. Jedoch ist zu beachten, dass die Standardisierung nicht zu weitgehend spezifiziert werden darf, um nicht den potenziellen Wettbewerb (siehe Kapitel 4.3.3 Ökonomische Bewertung) zu begrenzen.

4.3.4.3 Datenschutzrechtliche Anforderungen im Bereich Smart Metering

In der EU wird das allgemeine Datenschutzrecht maßgeblich durch die europaweit geltende Datenschutz-Grundverordnung (DSGVO)[75] geprägt. Der deutsche Gesetzgeber hat mit dem Bundesdatenschutzgesetz (BDSG) für alle Bereiche, in denen personenbezogene Daten verarbeitet werden, zudem eine „Grundregulierung“[76] geschaffen. Für bestimmte Technologien gelten spezifische Regeln; die Regeln für Smart Metering sind durch das MsbG festgelegt.

Regelungssystematik und Gegenstand

Die DSGVO ist hinsichtlich der Verarbeitung personenbezogener Daten sowie der Rechtsfolgen bei Verstößen als Verordnung im Sinne des Art. 288 Abs. 2 AEUV (Vertrag über die Arbeitsweise der Europäischen Union) unmittelbar und abschließend geltendes Recht.[77] Sofern nationale Normen der EU-Mitgliedstaaten den Regelungen der DSGVO entgegenstehen, müssen sie aufgrund des Anwendungsvorrangs des Gemeinschaftsrechts unbeachtet bleiben. Das Recht der EU-Mitgliedstaaten (z. B. im Bundesdatenschutzgesetz) kann nur dann von der DSGVO abweichen, wenn dies in einer der (zahlreichen) Öffnungsklauseln[78] ausdrücklich vorgesehen ist oder eine nationale Vorschrift die ePrivacy-Richtlinie (Richtlinie 2002 / 58 / EG) umsetzt (siehe Art. 95 DSGVO).

Gegenstand der DSGVO ist der Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (Art. 1 Abs. 1 DSGVO). Die DSGVO behält die in der Datenschutzrichtlinie vorgesehenen wichtigsten Grundsätze und Rechte der betroffenen Person bei und baut sie weiter aus. Darüber hinaus hat sie neue Verpflichtungen eingeführt, die die Umsetzung von Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen, die unter bestimmten Voraussetzungen zu erfolgende Ernennung eines Datenschutzbeauftragten, die Einhaltung eines neuen Rechts auf Datenübertragbarkeit und die Einhaltung des Grundsatzes der Verantwortlichkeit vorschreiben.

Räumlicher Anwendungsbereich

Räumlich findet die Verordnung nach Art. 3 Abs. 1 DSGVO auf die Verarbeitung personenbezogener Daten Anwendung, soweit die Verarbeitung im Rahmen der Niederlassung eines Verantwortlichen oder eines Auftragsverarbeiters in der Europäischen Union erfolgt, aber unabhängig davon, ob die Verarbeitung selbst in der EU stattfindet. Für die Verarbeitung personenbezogener Daten durch in Deutschland oder in Österreich ansässige Energieversorgungsunternehmen (EVU), Messstellenbetreiber o. Ä. ist der **räumliche Anwendungsbereich** der Verordnung **damit regelmäßig eröffnet.**[79]

Sachlicher Anwendungsbereich

Der **sachliche Anwendungsbereich** der DSGVO wird in Art. 2 Abs. 1 DSGVO **weit definiert.**[80] Danach gilt die DSGVO sachlich für die **ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten** sowie für die nicht automatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen.

Art. 4 DSGVO enthält Begriffsbestimmungen, die bei der Verarbeitung personenbezogener Daten bedeutsam sind. Im Folgenden werden die für die Evaluation relevanten Begriffsbestimmungen und Grundsätze der DSGVO für die Anwendungsvarianten beschrieben.

Personenbezogene Daten

Der Begriff der personenbezogenen Daten ist das Eingangstor zur Anwendung der DSGVO. Gemäß Art. 4 Nr. 1 DSGVO **sind personenbezogene Daten alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Als identifizierbar wird eine natürliche Person gesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.**

75 Verordnung (EU) 2016/679 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) Zwischen Systemgestaltung und Selbstregulierung, Springer, Wiesbaden, S. 315–336

76 Hornung, G. (2018): Sind neue Technologien datenschutzrechtlich regulierbar? Herausforderungen durch „Smart Everything“. In: Roßnagel, A., Friedewald, M., Hansen, M. (Hrsg.): Die Fortentwicklung des Datenschutzes.

77 Vgl. hierzu grundlegend EuGH, Urteil vom 15.07.1964 – 6/64, NJW 1964, 2371; Kirchhof, NVwZ 2014, 1537 ff.; Hirsch, NJW 2000, 1817 ff.; Hirsch, NJW 1996, 2457 ff.; Ruffert (2011), in: Calliess/Ruffert: EUV/AEUV, 4. Aufl., AEUV Art. 288 Rn. 20, Art. 1 Rn. 16 ff.

78 Siehe hierzu Reibach DSRITB 2018, 131 (132 ff.); so auch ausdrücklich zur Durchführung der DSGVO-Schlussanträge des Generalanwalts vom 19. 12. 2017 – C-40/17, Beck RS 2018, 32835, Rn. 47 – Fashion ID

79 Vgl. ähnlich Bartsch, in: Danner/Theobald: Energierecht, 98. EL Juni 2018, Rn. 5, 6

80 Roßnagel/Kroschwald: ZD 2014, S. 495 (496)

Die Einführung von Smart-Meter-Gateways wird durch das BMWK als wesentlich für die Digitalisierung der Energiewende angesehen.[81] Ihre Verwendung ist jedoch gleichzeitig besonders datenschutzrechtssensibel, weil sich SMGWs gerade dadurch auszeichnen, dass sie eine Vielzahl von Daten erfassen und an die entsprechenden Stellen weitergeben.[82] Intelligente Messsysteme, wie die des BMIL, verfolgen das Ziel, Versorgungssicherheit wie auch weitere Anwendungen in den Energienetzen zu gewährleisten bzw. zu ermöglichen.[83] Sie sollen insbesondere den Letztverbraucherinnen und -verbrauchern, Netzbetreibern und Energieerzeugern die erforderlichen Verbrauchsinformationen bereitstellen, um einerseits den Letztverbraucherinnen und -verbrauchern gezieltes energiesparendes Verhalten und andererseits den EVU ein nachfrageabhängiges Einspeisemanagement zu ermöglichen.[84]

SMGWs erfassen den Verbrauch jedes Abnehmers detailliert und stetig aktualisiert (Verbrauchs-, Erzeugungs- und Einspeisungsdaten). Die Daten dieser SMGWs erlauben Rückschlüsse darauf, wie, wann und in welchem Umfang Energie genutzt wird. Stammdaten (z. B. Name, Anschrift, Bankverbindung, Kundennummer, Mess- und Marktlokation) und Bewegungsdaten (z. B. Abrechnungs- oder Einspeisedaten) der Letztverbraucherinnen und -verbraucher bzw. Anschlussnutzerinnen und -nutzer, die natürliche Personen sind, stellen deshalb regelmäßig personenbezogene Daten dar.[85] Da jedes SMGW als Endgerät mittels einer individuellen Kennung einer Anschlussnutzerin oder einem Anschlussnutzer zugeordnet[86] werden kann, ist eine Identifizierung der natürlichen Person möglich. Im Falle des BMIL werden ebensolche Daten erfasst, sodass eine Allokation zu einer Anlage und dem dahinterstehenden Anlagenbetreiber möglich ist.

Datenverarbeitung

Faktisch jede Handlung mit einem Bezug zu personenbezogenen Daten kann als eine Verarbeitung angesehen werden. So umfasst der Begriff der Verarbeitung gemäß Art. 4 Nr. 2 DSGVO **jeden mit oder ohne Hilfe automatisierter Verfahren** ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie **das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.**

Verstöße gegen die Grundsätze der Verarbeitung personenbezogener Daten können ein Bußgeld von bis zu 20 Millionen Euro oder – auch im Falle eines Unternehmens der Energiewirtschaft – von bis zu 4 Prozent des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres eines Unternehmens sowie weitere Maßnahmen der Aufsichtsbehörde nach sich ziehen.[87]

Hinsichtlich der Smart-Meter-Gateways besteht die Datenverarbeitung grundsätzlich im Erfassen und in der Speicherung von Messwerten zum Zwecke der Abrechnung eines Energieliefervertrags. Auch die Offenlegung personenbezogener Daten von Letztverbraucherinnen und -verbrauchern durch Übermittlung an andere Marktpartner im Rahmen der energiewirtschaftlichen Geschäftsprozesse, zum Beispiel nach der Festlegung einheitlicher Geschäftsprozesse und Datenformate zur Abwicklung der Belieferung von Kunden mit Elektrizität[88] oder der Festlegung einheitlicher Geschäftsprozesse und Datenformate beim Wechsel des Lieferanten bei der Belieferung mit Gas[89], ist eine Form der Verarbeitung.[90]

Die Erstellung des DID in den drei Anbindungsvarianten stellt eine Datenverarbeitung dar, da anlagenspezifische Informationen automatisiert erhoben und dezentral auf der Blockchain gespeichert werden. Auch bei der „Verankerung“ des DID oder eines VC auf der Blockchain, wie dies im KILT-Ansatz der Fall ist, handelt es sich um eine Datenverarbeitung, da sowohl den DID als auch das Zertifikat Daten enthalten, deren „Verankern“ mindestens eine Verknüpfung im Sinne der DSGVO (wie oben beschrieben) darstellt. Ebenso finden, erforderlichenfalls mit vorheriger Zustimmung des Geräts, eine Übermittlung und teilweise auch eine Bereitstellung oder Veränderung der Daten statt. Dies gilt insbesondere, wenn eine Invalidierung (siehe Kapitel 4.1.1.1) erfolgt oder in einem Anwendungsfall die Daten zur Abwicklung von Transaktionen genutzt werden.

81 BMWi: Fahrplan für die weitere Digitalisierung der Energiewende, 01/2020, abrufbar unter: https://www.bmwi.de/Redaktion/DE/Downloads/F/fahrplan-fuer-die-weitere-digitalisierung-der-energiewende.pdf?__blob=publicationFile&v=10.
Am 31.01.2020 hat das BSI per Allgemeinverfügung festgestellt, dass die technische Möglichkeit zum Einbau intelligenter Messsysteme besteht, und somit einen weiteren Schritt in Richtung Smart-Meter-Rollout beschritten; BSI: Allgemeinverfügung zur Feststellung der technischen Möglichkeit zum Einbau intelligenter Messsysteme vom 31.01.2020, Az: 610 01 04 /2019_001; Schlosser, ew 4/2020, 68; Heuell, ew 4/2020, 70 (70)
82 Bretthauer, in: EnWZ 2017, 56 (56)
83 BT-Drs. 18/7555, 62; vgl. Wiesemann in FHS Betrieblicher Datenschutz, Teil VI, Kap. 7, Rn. 27; Wengeler, in: EnWZ 2014, 500 (501)
84 BT-Drs. 18/7555, 62, 66
85 Vgl. ebd. mit Verweis auf Soetebeer/Bartsch: IR 2013, S. 30 f., und Gola, in: Gola: DSGVO, Art. 4, Rn. 5
86 Vgl. § 2 Nr. 3 MsbG
87 Vgl. Art. 83 Abs. 5 lit. a DSGVO
88 BK6–06-009 (GPKE); Beschluss der BNetzA vom 11.07.2006 wegen der Festlegung einheitlicher Geschäftsprozesse und Datenformate zur Abwicklung der Belieferung von Kunden mit Elektrizität, BK6–06-009. Dieser wird seit 01.12.2019 durch die Anlage 1 zum Beschluss BK6-18-032 vom 20.12.2018 ersetzt.
89 BK7-06-067 (GeLi Gas); Beschluss der BNetzA vom 20.08.2007 wegen der Festlegung einheitlicher Geschäftsprozesse und Datenformate beim Wechsel des Lieferanten bei der Belieferung mit Gas, BK7-06-067
90 Vgl. Bartsch, in: Danner/Theobald: Energierecht, 98. EL Juni 2018, Rn. 9

Für Datenverarbeitungen enthält die DSGVO gemäß Art. 5 insbesondere die folgenden Grundsätze:

Rechtmäßigkeit der Verarbeitung[91]

Die durch Smart Meter erfolgende personenbezogene Datenverarbeitung fällt **grundsätzlich** in den Anwendungsbereich der DSGVO, wobei mit Art. 6 DSGVO Erlaubnistatbestände zur Verfügung stehen, die Messstellenbetreibern bzw. GWAs grundsätzlich eine rechtskonforme Datenverarbeitung ermöglichen:

1. Einwilligungslösung durch den Anschlussnutzer (Art. 6 Abs. 1 lit. a i.V.m. Art. 7 DSGVO)

2. Erlaubnistatbestandslösung (Art. 6 Abs. 1 lit. c, e DSGVO)

Zweckbindung

Nach Art. 5 Abs. 1 lit. b DSGVO sieht das Prinzip der Zweckbindung Datenverarbeitungen nur für festgelegte, eindeutige und rechtmäßige Zwecke vor. Verantwortliche müssen vor der Erhebung einen Zweck für die Datenverarbeitung festlegen und die Betroffenen darüber informieren. Im Falle einer Zweckentfremdung drohen gemäß Art. 83 Abs. 5 DSGVO Sanktionen aufgrund eines dann vorliegenden Datenschutzverstoßes. Gemäß Art. 6 Abs. 1 lit. a DSGVO ist eine datenschutzkonforme Weiterverarbeitung von Energieverbrauchsdaten zu neuen Zwecken rechtmäßig, wenn die Weiterverarbeitung auf der Einwilligung der betroffenen Person oder einer Rechtsvorschrift beruht.
Bei der Implementierung aller drei Anbindungsvarianten wird der Anlagenbetreiber grundsätzlich über die Prozesse und die Erstellung des DID aufgeklärt bzw. aufgeklärt werden müssen, sodass mit der Installation jeder Anbindungsvariante sowohl die Rechtmäßigkeit der Verarbeitung der Daten als auch die Zweckbindung gegeben sein werden.

Transparenz

Der Transparenzgrundsatz ergibt sich unter anderem aus Art. 5 Abs. 1 lit. a DSGVO i.V.m. Art. 12 ff. DSGVO (Informationspflichten), Art. 25 DSGVO und Erwägungsgrund 78 (Datenschutz durch Technik (Data Protection by Design) und datenschutzfreundliche Voreinstellungen (Data Protection by Default)) sowie Art. 42 lit. f DSGVO und Erwägungsgrund 100 (Datenschutzniveau) DSGVO.

Der Verantwortliche muss alle erforderlichen Schritte unternehmen, um die Verarbeitung von Daten gegenüber den Betroffenen möglichst transparent zu gestalten. Die Mehrheit der Datenschutzbeauftragten empfiehlt, dass der Verantwortliche Techniken und Mechanismen anbietet, die es den Betroffenen laufend erlauben, ihr Datenkonto beim Verantwortlichen zu kontrollieren. Dies umfasst nicht bloß die Energieverbrauchsdaten, sondern auch eine Protokollierung, wer auf die Daten zugegriffen hat und wozu diese Daten verarbeitet wurden. Der Grundsatz der Transparenz soll eine verdeckte Verarbeitung von Betroffenendaten verhindern. Daher sollten Betroffene über die Erhebung und Verarbeitung ihrer Daten und über ihre Betroffenenrechte (Art. 15 bis 21 DSGVO) umfassend unterrichtet werden (Art. 13 bis 14 DSGVO). Die Unterrichtung muss in leicht zugänglicher Art und Weise und in einer klaren und verständlichen Sprache erfolgen. Verantwortliche müssen Dateninformationen und -auskunft zur Verfügung stellen, die den notwendigen Datenverkehr erläutern.

Im Rahmen des BMIL und der drei Anbindungsvarianten sind die Identitätsabfrage und somit die Unterrichtung der Betroffenen möglich, sodass der Grundsatz der Transparenz einer Serienimplementierung nicht entgegensteht. Fraglich ist jedoch, ob die Betroffenenrechte jederzeit eingehalten werden können. Nach den uns zur Verfügung gestellten Informationen ist nicht eindeutig, ob die Betroffenen jederzeit über die Verwendung ihres DID oder ihrer VCs unterrichtet werden. Sollte die Unterrichtung erfolgen, ist darüber hinaus nicht eindeutig, wie die Unterrichtung stattfindet. Die DSGVO fordert sowohl die Unterrichtung in einer leicht zugänglichen Art und Weise wie auch in klarer und verständlicher Sprache. Aufgrund dessen ist im Einzelfall zu prüfen, ob ein potenzieller Verstoß gegen Betroffenenrechte vorliegt. Bei der Serienimplementierung muss demnach darauf geachtet werden, dass die Betroffenenrechte stets gewahrt werden. Dies kann unter anderem über eine dahingehende Vereinbarung mit den Betroffenen gelöst werden, in der sie der entsprechenden Unterrichtung zustimmen.

91 Vgl. Art. 5 Abs. 1 lit. a i.V.m. Art. 6 DSGVO

Datenminimierung[92]

Der Grundsatz der Datenminimierung aus Art. 5 Abs. 1 lit. e DSGVO besagt, dass personenbezogene Daten unverzüglich gelöscht werden müssen, sobald sie für die Wahrnehmung der jeweils zugewiesenen Aufgaben nicht mehr benötigt werden. Sowohl bei der Erstellung der VCs als auch bei der Erstellung des DID ist zu prüfen, ob der Grundsatz der Datenminimierung eingehalten wird. VCs sind das digitale Äquivalent von physikalischen Ausweisen und Zertifikaten und enthalten somit umfangreiche (personenbezogene) Daten (siehe hierzu Kapitel 3.3). Aus dem VC können nur benötigte Daten herausgezogen werden, jedoch stellt sich im Umkehrschluss die Frage, ob es dann notwendig ist, das VC mit allen möglichen Daten zu erstellen.

Der DID ist eine Identifikationskennung, die eine Ressource identifiziert, spezielle Eigenschaften besitzt (siehe hierzu Kapitel 3.3) und somit auch personenbezogene Daten enthält. Fraglich ist demnach, ob der Grundsatz der Datenminimierung sowohl bei den VCs als auch bei der Erstellung des DID in den drei Anbindungsvarianten eingehalten werden kann. Speziell mit Blick auf die Anwendungsfälle ist nicht jede Information erforderlich, sodass grundsätzlich bei jedem Anwendungsfall lediglich einen DID mit den erforderlichen Informationen für den Anwendungsfall vorhanden sein sollte. Ebenso ist bei der Erstellung des VC zu hinterfragen, ob für die Erstellung des Zertifikats alle Informationen erforderlich sind. Nicht benötigte Daten müssten dann gelöscht oder dürften gar nicht erst erhoben werden. Nach dem Wortlaut von Art. 5 Abs. 1 lit. e DSGVO ist jedoch auch eine dahingehende Auslegung denkbar, dass die Löschpflicht nur personenbezogene Daten betrifft. Im Rahmen jedes Anwendungsfalls ist es daher notwendig, zu prüfen, welche Daten bei der Erstellung eines VC und auch des DID benötigt werden.

Öffnungsklausel in Art. 89 Abs. 3 DSGVO

Die DSGVO enthält bei genauerer Betrachtung zahlreiche Öffnungsklauseln, die den Mitgliedstaaten in vielen Bereichen Regelungskompetenzen überlassen.[93] Vor diesem Hintergrund soll die DSGVO zu keiner Vollharmonisierung führen.[94]

Zwar findet sich keine auf Smart Meter oder zumindest auf den Energiesektor zugeschnittene Öffnungsklausel in Kapitel IX der DSGVO, die eine Reihe an allgemeinen Öffnungsklauseln enthält. Generalklauselartig gestattet die DSGVO jedoch auch nationale Regelungen zur Datenverarbeitung, die im „öffentlichen Interesse“ liegen. Insbesondere enthält Art. 89 Abs. 3 DSGVO die allgemeine Anordnung, dass die Mitgliedstaaten in Fällen, in denen eine Datenverarbeitung im öffentlichen Interesse vorgenommen wird, von bestimmten Rechten der Betroffenen aus Art. 15 bis 21 DSGVO abweichen können. In Art. 21 DSGVO ist festgelegt, dass sämtliche „Betroffenenrechte“ aus Art. 12 bis 20 durch nationales Recht eingeschränkt werden können, unter anderem wenn dies durch wichtige Ziele des öffentlichen Interesses bedingt ist (Art. 21 Abs. 1 lit. c DSGVO).

§§ 49 ff. MsbG als spezifische Datenschutzbestimmungen i. S. v. Art. 6 Abs. 3 DSGVO

Mit Verabschiedung der DSGVO und des MsbG stehen zwei divergierende Datenschutzregime zur Verfügung: einerseits die DSGVO, die einen einheitlichen europäischen Rechtsrahmen herstellen möchte, und andererseits das MsbG, das als bereichsspezifische Regelung die Datenkommunikation in intelligenten Energienetzen und somit auch bei Smart Meter reguliert.

Verhältnis des MsbG zur DSGVO

Gemäß Art. 6 Abs. 2 DSGVO haben die Mitgliedstaaten eine Normsetzungskompetenz nur für „spezifischere Bestimmungen zur Anpassung der Anwendung der Vorschriften“ der DSGVO. Mitgliedstaatliche Bestimmungen dürfen die Vorgaben der DSGVO daher zwar konkretisieren, nicht aber die Vorgaben der DSGVO verlassen.[95] Eine zulässige Spezifizierung setzt voraus, dass die mitgliedstaatliche Regelung die jeweilige Datenverarbeitung präziser regelt als die DSGVO[96], sich aber gleichwohl innerhalb der Rechtmäßigkeitsvoraussetzungen der DSGVO bewegt.

Die §§ 49 ff. MsbG werden vor diesem Hintergrund mehrheitlich als **ohne Weiteres verordnungskonform** angesehen[97], gerade auch aufgrund ihrer Detailtiefe.[98] Die §§ 49 ff. MsbG erfüllen die in Art. 6 Abs. 3 DSGVO normierten Anforderungen, sodass die Mitgliedstaaten – hier also Deutschland – spezifische Bestimmungen beibehalten können.

Auf nationaler Ebene hat bereichsspezifisches Datenrecht, vorliegend das MsbG, **Anwendungsvorrang** (vgl. § 1 Abs. 2 Satz 1 BDSG). Die Datenschutzregelungen der §§ 49 ff. MsbG gehen somit grundsätzlich anderen nationalen Datenschutzregeln vor.[99] Gegenüber anderen nationalen Datenschutzbestimmungen gelten die sektorspezifischen Regelungen des MsbG zum Datenschutzrecht abschließend.[100]

92 Vgl. Art. 5 Abs. 1 lit. c DSGVO
93 Siehe Überblick bei Kraska, ZD-Aktuell 2016, 04173
94 Kraska, ZD-Aktuell 2016, 04173
95 Plath, in: Plath (2016), 2. Aufl., DSGVO Art. 6 Rn. 25
96 Kühling/Martini et al.: DSGVO und nationales Recht, 33, abrufbar unter: http://www.uni-speyer.de, zuletzt abgerufen am 26.10.2021
97 Herb, in: Steinbach/Weise, MsbG § 49 Rn. 11; Wiesemann, in FHS: Betrieblicher Datenschutz, Teil VI, Kap. 7, Rn. 27; Bretthauer, in: EnWZ 2017, 56 (61); Heun/Assion, in: BB 2018, 579 (584); aA wohl: Verbraucherzentrale Bundesverband: Smart Meter Einbau: Zwangsdigitalisierung durch die Kellertür – Stellungnahme vom 09.10.2015 zum Entwurf eines Gesetzes zur Digitalisierung der Energiewende 9, abrufbar unter: https//www.vzbv.de/pressemitteilung/smart-meter-verbraucher-lehnen-zwangsdigitalisierung-ab, zuletzt abgerufen am 26.10.2021
98 Bretthauer, in: EnWZ 2017, 56 (61)
99 Bartsch/Dippold, in: vom Wege, Weise: Praxishandbuch Messstellenbetriebsgesetz, 2019, Kapitel 9 Rn. 29 ff.
100 Bartsch/Danner/Theobald, Teil 230, Rn. 112

Berechtigte Stellen

§ 49 Abs. 2 MsbG spezifiziert zunächst ausdrücklich und abschließend, welche verschiedenen **Marktakteure** überhaupt nur zum Umgang mit personenbezogenen Daten **berechtigt** sind.[101] Das sind Messstellenbetreiber, Netzbetreiber, Bilanzkoordinatoren, Direktvermarktungsunternehmen und Energielieferanten sowie jede Stelle, die über eine Einwilligung der Anschlussnutzerin oder des Anschlussnutzers verfügt. Somit ist der Kreis der datenverarbeitenden Stellen klar umgrenzt, sodass außerhalb dieses Kreises ein Verbot des Datenumgangs besteht.[102] **Datenschutzrechtlich Betroffene** im MsbG sind die Anschlussnutzerinnen und -nutzer, demnach die zur Nutzung des Netzanschlusses berechtigten Letztverbraucherinnen und -verbraucher, deren Daten erhoben, verarbeitet oder genutzt werden sollen (vgl. § 50 Abs. 1 i. V. m. § 2 Nr. 3 MsbG). Das sind üblicherweise somit die Mieterinnen und Mieter bzw. Eigentümerinnen und Eigentümer von Häusern oder Wohnungen (siehe insbesondere Kapitel 4.3.2.2). Verarbeitet werden dürfen wiederum solche Daten, die aus einer Messeinrichtung, einer modernen Messeinrichtung, einem Messsystem oder **einem intelligenten Messsystem** stammen (§ 50 Abs. 1 MsbG). Gemeint sind hiermit folglich **alle Arten von Smart Metern,** da das MsbG den Themenkomplex „Smart Metering" einer umfassenden Regelung zuführt.[103] Dabei kann es sich insbesondere um Messdaten, Tarifdaten, Daten der Basiskommunikation und Steuersignale handeln.

Alle drei Anbindungsvarianten erstellen einen DID, die ebensolche Daten enthält, die im Rahmen des SMGW ausgetauscht werden. Die Daten des DID sind verschlüsselt auf der Blockchain gespeichert. Je nach Anwendungsfall ist dann zu prüfen, ob der Marktakteur zum Umgang mit den Daten des DID berechtigt ist. Eine fehlende Berechtigung führt dazu, dass der erstellte DID nicht verwendet werden darf und dies demnach einer Serienimplementierung je nach Anwendungsfall im Wege stehen würde. Grundsätzlich besteht jedoch die Möglichkeit, dass die Daten (von Betroffenen) von jedem Berechtigten verarbeitet werden dürfen.

Zweckbindung auch im MsbG erforderlich

Die §§ 50 Abs. 1, 2 MsbG normieren schließlich **konkrete Zwecke,** zu denen Daten erhoben, verarbeitet und genutzt werden dürfen. So ist dies beispielsweise zur Erfüllung von Verträgen mit den Anschlussnutzerinnen und -nutzern (§ 50 Abs. 1 Nr. 1 MsbG) oder zur Wahrnehmung einer Aufgabe des Netzbetreibers, die in Ausübung ihm übertragener hoheitlicher Befugnisse erfolgt (§ 50 Abs. 4 MsbG), zulässig. § 50 Abs. 1 Nr. 1 MsbG meint insbesondere Fälle, in denen die Anschlussnutzerinnen und -nutzer aufgrund eines variablen Stromtarifvertrags (personenbezogene) Daten in kurzen Zeitintervallen übermitteln müssen, sodass der Stromanbieter einen variablen Stromtarif anbieten und somit seiner Vertragsverpflichtung nachkommen kann.[104] Durch diese strenge Zweckbindung wird die informationelle Selbstbestimmung der Anschlussnutzerinnen und -nutzer in besonderer Weise geschützt.[105] Bereits im berühmten Volkszählungsurteil hatte das Bundesverfassungsgericht angemahnt, dass ein Zwang zur Angabe personenbezogener Daten voraussetzt, dass der Gesetzgeber den Verwendungszweck bereichsspezifisch und präzise bestimmt und dass die Angaben für diesen Zweck geeignet und erforderlich sind.[106] Das MsbG normiert hier bereichsspezifische Anforderungen an den Datenschutz, da eine Datenverwendung zu anderen Zwecken ausgeschlossen ist.[107]

Dies entspricht dem Grundsatz der Zweckbindung der DSGVO. Die Erstellung des DID und somit der Austausch von Daten dienen dem Zweck, spezifische Anwendungsfälle zu bedienen. Die Datenverwendung wie auch die Erstellung des DID erfolgen demnach in allen drei Anbindungsvarianten zu einem bestimmten Zweck.

Zu beachten ist ferner, dass sich der Anwendungsbereich der Regelungen nach der Gesetzesbegründung zu § 50 Abs. 1 MsbG nicht nur auf personenbezogene oder personenbeziehbare Daten, sondern auch auf solche ohne Personenbezug erstrecken soll.[108] Erfasst werden soll damit jegliche Kommunikation in intelligenten Energienetzen.[109]

101 BT-Drs. 18/7555, 105
102 So für § 21g EnWG Lorenz/Raabe, in: Säcker (o. Fn. 8), § 21g Rn. 16
103 BT-Drs. 18/7555, 3
104 Vgl. kritisch zu den quantitativen Auswirkungen variabler Stromtarife auf die Stromkosten von Kleinverbrauchern eine Kurzstudie des Wissenschaftlichen Instituts für Infrastruktur und Kommunikationsdienste (WIK) vom 11.11.2015, http://zap.vzbv.de/ce0ba83d-8d69-4aed-bbc3-af50e58fdf59/Auswirkungen-variabler-Stromtarife-auf-Stromkosten-Haushalte-WIK-vzbv-November-2015.pdf, zuletzt abgerufen am 02.01.2017
105 BT-Drs. 18/7555, 105
106 BVerfGE 65, 1 (46), abrufbar unter: www.beck-online.beck.de
107 So auch schon unter Geltung von § 21g EnWG; Britz/Hellermann/Hermes, EnWG, § 21g Rn. 5
108 Vgl. BT-Drs. 18/7555, u. a. S. 105; ablehnend: Steinbach/Weise/Herb, § 49 MsbG Rn. 4
109 Vgl. insofern auch Art. 5 Abs. 2 des Kommissions-Vorschlags für eine Verordnung des Europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG („ePrivacy Verordnung", 2017/0003 (COD)), der Maschine-zu-Maschine-Kommunikation vom Anwendungsbereich des ePrivacy-VO-E umfasst sieht, wenn sich diese Kommunikation auf Endnutzerinnen und Endnutzer bezieht

Somit könnten alle ausgetauschten Daten, die im Rahmen der Erstellung des DID erhoben, erstellt, verarbeitet oder gespeichert werden, den datenschutzrechtlichen Regelungen des MsbG unterworfen sein.

- **Weitere Betroffenenrechte: Datenverarbeitung und -nutzung sowie Löschungspflichten**

Eine weitere Anforderung, die insbesondere der Datensicherheit dient und somit auch die Datenverarbeitungsverfahren näher ausgestaltet, folgt aus § 52 Abs. 1 MsbG. So besteht die Verpflichtung bei der Datenverarbeitung personenbezogener Daten, dass eine verschlüsselte elektronische Kommunikation erfolgen muss. Darüber hinaus dürfen personenbezogene Daten, Stammdaten und Netzzustandsdaten nur zwischen Teilnehmern an der Smart-Metering-Public-Key-Infrastruktur des BSI kommuniziert werden (§ 52 Abs. 4 MsbG). Außerdem müssen personenbezogene Daten anonymisiert oder pseudonymisiert werden, soweit dies im Hinblick auf den Verwendungszweck möglich ist (§ 52 Abs. 3 MsbG). Schließlich sind im Regelungskonzept des MsbG für personenbezogene Daten spezifische Löschungspflichten vorhanden (vgl. §§ 60 Abs. 6, 64 Abs. 2, 66 Abs. 3, 67 Abs. 3, 68 Abs. 3, 69 Abs. 3 MsbG), sodass die Daten nicht für eine unbegrenzte Dauer gespeichert werden dürfen und damit eine dauerhafte Bevorratung von Daten auch im Energiesektor nicht möglich ist.

Es ist fraglich, ob aufgrund der Erstellung des DID in allen drei Anbindungsvarianten diese Vorgaben eingehalten werden können. Sofern insbesondere die Daten dauerhaft ohne Zweckbindung gespeichert werden, könnte ein potenzieller Verstoß gegen die Vorgaben des MsbG vorliegen. Dies ist je nach Einzelfall bei der Implementierung der drei Anbindungsvarianten zu prüfen. Aus den iterativen Fragenkatalogen ging hervor, dass diese Herausforderung erkannt, jedoch nur teilweise in den Identitätsfeststellungsprozess integriert wurde. Somit besteht die Gefahr, die datenschutzrechtlichen Vorgaben zu verletzen. Dies würde zu einer Sanktionierung führen und somit die Umsetzung der Anbindungsvarianten in Serie hemmen.

- **Verantwortlichkeit für die Daten**

Eine weitere Herausforderung besteht in der Frage, wer für die Richtigkeit der Daten verantwortlich ist. Nach den uns zur Verfügung gestellten Informationen müssen die Daten der Anlage händisch eingetragen werden, sofern keine automatisierte Erfassung erfolgt (siehe auch Kapitel 4.3.3.1). Anschließend werden diese Daten für die Erstellung des DID verwendet. Bei allen drei Anbindungsvarianten erfolgt der Identitätsfeststellungsprozess auf Basis dieser Daten. An der automatischen Erstellung des DID sind jedoch weitere „Parteien“ wie Claimer, Identifier oder Attester beteiligt. In der Anwendungsvariante „Gerätezentrierte Identitätsverwaltung im Verbund mit einem dedizierten CLS-Device“ mit KILT (siehe Kapitel 4.1.4) sind keine weiteren Rollen involviert, jedoch bei der Ausstellung des Zertifikats, des VC. Ein Dritter, der in einem Anwendungsfall auf die Daten des DID oder auch möglicherweise des VC zugreift, wird sich auf die Richtigkeit der Daten verlassen müssen. Im Falle einer Fehlinformation ist fraglich, wer für die Richtigkeit der Daten einzustehen hat. Dies könnte der Anlagenbetreiber, derjenige, der die Daten eingetragen hat, oder ein Beteiligter im Identitätsfeststellungsprozess sein. Hierzu trifft das MsbG keine Regelung, sodass eine große Rechtsunsicherheit hinsichtlich der Verantwortlichkeit in diesem Fall besteht. Ein Rückgriff auf zivilrechtliche und allgemeingültige Normen ist demnach notwendig, was zu einer zwingenden Einzelfallprüfung führt. Die Prüfung eines jeden Einzelfalls würde wiederrum Ressourcen beanspruchen, was aus ökonomischer Sicht (siehe Kapitel 4.3.3) zu einer Hemmung der Serienimplementierung führt. Insofern ist eine eindeutige Festlegung der rechtlichen Verantwortlichkeit für die Daten erstrebenswert.

4.3.4.4 Zusammenfassung der rechtlichen Bewertung

Grundsätzlich halten alle Anbindungsvarianten die IT-sicherheitsregulatorischen Vorgaben des MsbG und der Technischen Richtlinie TR-03109 des BSI ein und **entsprechen somit dem aktuellen rechtlichen Rahmen.** Für ausgewählte Kommunikationswege **fehlen jedoch regulatorische Standards.** Eine Festlegung dieser Standards würde die forcierte Inter-

operabilität fördern, eine Serienimplementierung erleichtern und Rechtssicherheit gewährleisten (hierzu siehe auch Kapitel 4.3.3.3 Zusammenfassung der ökonomischen Bewertung).

In allen drei Anbindungsvarianten werden sowohl nicht personenbezogene als auch personenbezogene Daten verarbeitet. Der Anwendungsbereich des Datenschutzrechts ist stets eröffnet. Die **erforderliche Rechtmäßigkeit wie auch die Zweckbindung der Daten können überwiegend bejaht werden,** jedoch ist die **Wahrung der Betroffenenrechte in allen Anbindungsvarianten nicht immer möglich.** Die potenzielle Gefahr der Verletzung von datenschutzrechtlichen Vorgaben kann zu möglichen Hemmnissen bei der Serienimplementierung des BMIL führen. Die Anbindungsvarianten sollten Handlungsoptionen beinhalten, die die Wahrung der Betroffenenrechte sicherstellen können, sodass keine datenschutzrechtlichen Verletzungen der Serienimplementierung des BMIL im Weg stehen.

Die Verantwortlichkeit für die Daten ist gesetzlich derzeit nicht geregelt. Insofern **besteht eine große Rechtsunsicherheit hinsichtich der Frage, wer bei einer Fehlinformation haftbar gemacht werden könnte.** Eine Prüfung des Einzelfalls ist unentbehrlich und birgt für die Beteiligten ein hohes Risiko, für eine etwaige Datenverletzung haftbar gemacht zu werden. Eine eindeutige Festlegung, wer bei der Identitätsfestlegung bzw. bei dem Identitätsprozess für welche Daten verantwortlich ist, würde die Rechtssicherheit für die Marktakteure erhöhen und somit eine Serienimplementierung vorantreiben.

5. Anwendungsmöglichkeiten der automatisierten Geräteanbindung und digitalen Identitätsverwaltung

Autoren: Dr. Marius Buchmann, Jacobs University Bremen; Richard Hänsel, EY Law; Dr. Ing. Sven Rosinger, OFFIS. Beschreibung der Anwendungsfälle: Riddle&Code, Energy Web

Mit dem BMIL wird die Teilnahme von Geräten an einer Vielzahl von Anwendungsfällen ermöglicht. Dabei sind grundlegend zwei Schritte notwendig, die für jeFden der Use Cases analog ablaufen:

1. Auf dem Gerät wird die Teilnahme an einem Use Case angefragt und damit die Zustimmung zur Teilnahme gegeben. Damit wird dem Use Case ermöglicht, auf ausgewählte Gerätedaten zuzugreifen. So ist eine datensparsame Verwendung möglich. Technisch fordert das Gerät ein Verifiable Credential an, das die Rolle zur Use-Case-Teilnahme beinhaltet.

2. Der Eigentümer des Use Case prüft die zur Verfügung gestellten Daten, führt gegebenenfalls weitere Prüfungen durch und erteilt dann die Freigabe zur Teilnahme am jeweiligen Use Case. Technisch wird in diesem Schritt das Verifiable Credential, das das Energy Web Role Credential für den Use Case beinhaltet, signiert und an das Gerät geschickt, das das neue Credential akzeptiert. So kann die Anlage im Weiteren beweisen, dass sie am Anwendungsfall teilnehmen kann, ohne dass

   a. Daten über das Gerät zentral vorgehalten werden und
   b. bereits geprüfte Daten erneut geprüft werden müssen.

Zur Demonstration wurde der Ablauf der Use-Case-Teilnahme exemplarisch implementiert. Mit der Web-Oberfläche kann die Teilnahme eines Geräts an den beiden nachfolgenden Use Cases gesteuert und überprüft werden. Ebenso ist es möglich, das gesamte DID-Document mitsamt den relevanten Credentials einzusehen. Diese Daten werden gecacht und so dem Frontend bereitgestellt.

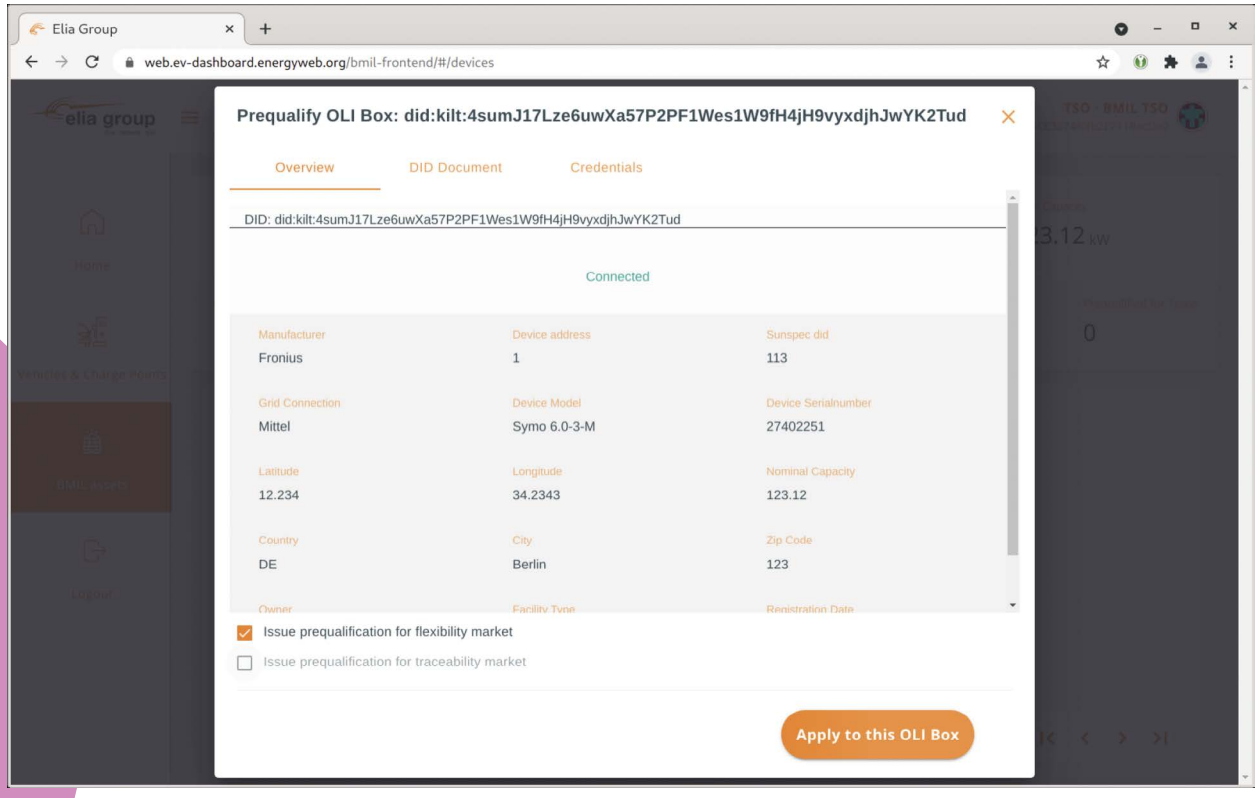


Abbildung 43: Die Zustimmung zur Teilnahme an den Use Cases im EV Dashboard

Bei der Auswahl der Use Cases des BMIL-Projekts ging es den beteiligten Unternehmen nicht nur darum, die vorliegenden Fälle inhaltlich gemäß den Ausschreibungsbedingungen auszuwählen, sondern auch darum, andere Aspekte mit zu berücksichtigen. So war es ein Ziel, den Nutzen des Einsatzes der Blockchain-Technologie und der Interoperabilität zwischen verschiedenen Blockchain-Netzwerken besonders deutlich herauszuarbeiten. Ebenso war es auch Teil der Überlegungen, grundlegende Prozesse in der Realwirtschaft zu berücksichtigen – die natürlich Akteure in mehreren Märkten umfasst und den länderübergreifenden Austausch von Energie und Waren bedeutet. Da Lieferketten heute schon weitgehend international sind, sollten auch Elektrizitätsmärkte und entsprechend Energiebilanzen, etwa in der industriellen Komponenten-Produktion, in Zukunft grenzüberschreitend erfasst werden. Eine neu entwickelte Technologie sollte den stärkeren Ausbau des internationalen Austauschs in Elektrizitätsmärkten vereinfachen.

Ebenso muss ein Verzeichnis energieerzeugender Geräte damit umgehen können, dass in benachbarten Regionen andere Detailvorschriften für die Registrierung solcher Geräte bzw. deren Identitäten gelten werden – somit ist also auch der Nachweis der Interoperabilität mit anders gelagerten Geräte-Identitäts- und Datenformatansätzen ein eminent wichtiger Aspekt einer praxisnahen und zukunftssicheren Entwicklung. Denn nur so lässt sich eine breite industrielle Anwendung effizient bewerkstelligen und wird ein Rollout nicht mit weiteren, bürokratisch bedingten Zwischenschritten belastet.

Entsprechend haben wir bewusst auch zwei weitere, in den Kapiteln 5.4 und 5.5 dargestellte Use Cases ausgewählt, die im benachbarten Ausland, nämlich in Österreich, angesiedelt sind, um eben diese oben geschilderten Herausforderungen anzunehmen und zu zeigen, wie die Lösungsansätze, die das BMIL-Projekt bereitstellt, hier zur Anwendung kommen können.

5.1 Allgemeine Zielvorstellungen und Anforderungen einer DID-basierten Geräteanmeldung

Die Hauptanforderungen an ein solches System sind kryptografische Schlüsselpaare, die auf dem Gerät abgelegt sind, eine dezentrale Geräte-Identität, Basisdaten, die mit dieser Identität verknüpft sind, und eine rollenbasierte Authentifizierung.
Eine ideale Lösung für die Geräteregistrierung sollte folgende Prozessschritte abbilden:

1. **Vorhandene digitale Identität und Basisdaten**
   Geräte können bereits während des Herstellungsprozesses eine digitale Identität erhalten, die beim Installationsprozess mit Basisdaten verknüpft wird (siehe Kapitel 4.1). Die Basisdaten können digital nachverfolgbar von einem bestimmten verantwortlichen Marktteilnehmer verifiziert werden. Ein Beispiel dafür könnte ein vom Verteilnetzbetreiber autorisierter Installateur sein. Eine Verankerung der Basisdaten-Vergabe als Transaktion auf der Blockchain kann das Vertrauen in den Prozess stärken und insbesondere eine automatisierte Nachverfolgung und fälschungssichere Verifizierung der Transaktion erlauben. Somit können alle mit dem Gerät verknüpften Daten im Falle eines Fehlers zu dem für die Registrierung verantwortlichen Marktteilnehmer zurückverfolgt werden. Marktteilnehmer, die ungenau arbeiten oder sich nicht regel- oder rechtskonform verhalten, können so einfach identifiziert und sanktioniert werden. Es muss sichergestellt sein, dass die Basisdaten möglichst alle für die Präqualifizierung für den speziellen Anwendungsfall benötigten Gerätedaten enthalten. Ist dies nicht der Fall, können über die Basisdaten hinausgehende Daten für spezielle Anwendungsfälle in Form von Verifiable Credentials hinzugefügt werden.

2. **Einleiten der Registrierung**
   Geräte, die eine digitale Identität besitzen und bereits beim Installationsprozess mit einem Set von verifizierten Basisdaten verknüpft wurden, können ohne weitere Voraussetzungen automatisch autorisiert werden. Der Anlagenbesitzer könnte mit einem Mausklick die digitale Autorisierung der Anlage für einen Anwendungsfall beantragen. Das Onboarding kann dabei komplett automatisiert ablaufen und es würde weniger bis keiner weiteren Aktion durch den Anlagenbesitzer bzw. den Register-Betreiber bedürfen.

3. **Verifizierung der Basisdaten**
   Wenn ein Gerät mit DID und verknüpften Basisdaten eine Registrierung beantragt hat, kann das Register automatisch die Basisdaten verifizieren und, wenn alle Voraussetzungen erfüllt sind, die Anlage automatisch freischalten. Falls nötig, können Registrierungen natürlich auch manuell eingesehen und überprüft werden. Ein großer Vorteil ist, dass die Identität und die benötigten Basisdaten ohnehin bereits vorliegen und nicht speziell für eine spezifische Anwendung neu angelegt werden müssen. Das reduziert die Transaktionskosten einer Registrierung und baut Hürden insbesondere für Kleinstanlagen ab.

Die Nutzung von kryptografischen Methoden mit öffentlichen und privaten Schlüsseln oder Public Key Infrastructure, die direkt auf dem Gerät liegen, kann den Prozess vereinfachen und ihn absichern. Die Verifizierbarkeit der Basisdaten des Geräts kann somit stark vereinfacht werden, da die Anlage sich über sein Key Pair identifiziert. Die Nutzung dieser Art von kryptografiebasierter Authentifizierung ist technisch fälschungssicher. Wenn angenommen werden kann, dass die Anmeldung der Basisdaten korrekt abgelaufen ist, kann mit absoluter Sicherheit gesagt werden, dass es sich um das richtige Gerät handelt, das die Registrierung beantragt. Und auch die korrekte Vergabe der Basisdaten und die Verknüpfung mit der Geräte-Identität sind durch die Nutzung der Geräteschlüssel und die Verankerung der Transaktionen auf der Blockchain kryptografisch nachweisbar.

4. **Rollenvergabe**
   Um die Vergabe von Rechten für den spezifischen Anwendungsfall effizient zu gestalten, sollte es ein rollenbasiertes Autorisierungssystem geben. Geräte sollten basierend auf ihren Basisdaten eine Rolle im System erhalten, die ihnen bestimmte Rechte gibt. Dabei sollte die Freischaltung der Geräte für die Nutzung des Registers basierend auf vollständigen und korrekt verifizierten Basisdaten im Vordergrund stehen. Die Rolle sollte kryptografisch mit dem DID, die das Gerät repräsentiert, verbunden und auf der Blockchain verankert sein.

5. **Freigabe der Nutzung**
   Das Geräte-Register sollte die Freigabe zur Nutzung und spezielle Rechte innerhalb des Systems, zum Beispiel das automatisierte Stellen von Zertifikatsanfragen basierend auf der Rolle des Geräts, regeln. Geräte, deren Basisdaten korrekt verifiziert wurden und die darauf basierend eine Rolle im System erhalten haben, können sich mit ihren Geräteschlüsseln authentifizieren. Auf dem Geräte-Register aufbauende Lösungen können die verknüpften Rollen abrufen und basierend darauf den Zugriff erlauben und die speziellen Rechte gewähren.

5.2 Anwendungsfall Grünstromzertifikate

In diesem Anwendungsfall geht es um die Nachverfolgung und den Handel des grünen Attributs von Strom. Ins Netz eingespeister Strom hat unabhängig von der Erzeugungsform, also durch eine Erneuerbare-Energien-Anlage oder durch eine konventionelle Anlage, dieselben physikalischen Eigenschaften. Daher kann die Herkunft von Strom im Netz nicht ohne Weiteres nachgewiesen werden. Außerdem wird heute jede Wattstunde, die an der Strombörse gehandelt wird, unabhängig von der Herkunft als Fungible Commodity betrachtet. Um den Strom als erneuerbar zu identifizieren und ihn auf den Märkten als solchen zu kennzeichnen, muss die grüne Herkunft separat nachverfolgt werden.

Grünstromzertifikate-Register machen das grüne Attribut von Strom wie folgt nachverfolgbar und handelbar. Zunächst werden Erzeugungsdaten von Anlagen für einen bestimmten Zeitraum gesammelt. Die Energiemengen werden verifiziert und dann wird für eine bestimmte Erzeugungsanlage und einen definierten Zeitraum ein Zertifikat erzeugt. Ein solches Zertifikat enthält somit eine Referenz auf die Erzeugungsanlage und ihre Stammdaten, den Erzeugungszeitraum, für den das Zertifikat ausgestellt wurde, und die Energiemenge, die von der Anlage in dem Zeitraum erzeugt wurde. Die Energiemengen der Zertifikate können gehandelt werden und Käufer können sie für einen bestimmten Verbraucher entwerten.

5.2.1 Rahmenbedingungen und Problemstellung

Rahmenbedingungen

Ein Großteil des Stroms aus Regenerative-Energien-Erzeugungsanlagen wird in Deutschland über die EEG-Umlage finanziert.[110] Dabei sind die Netzbetreiber verpflichtet, den Strom zu einem festen Preis abzunehmen (bzw. über die Markt- und Managementprämie zu bezuschussen), und die Kosten werden auf einen Großteil der Stromkunden in Deutschland umgelegt. Die Anlagen sind beim jeweils zuständigen Netzbetreiber angemeldet und die Vergütung wird über diese Netzbetreiber abgewickelt. Da der EEG-Strom auf alle Stromkunden aufgeteilt und der grüne Anteil nicht gehandelt wird, werden für Anlagen in der EEG-Vergütung keine Grünstromzertifikate ausgestellt. Das bedeutet, dass ein Großteil der Anlagen in Deutschland noch nicht in einem Grünstromzertifikate-Register registriert ist

110 https://www.umweltbundesamt.de/sites/default/files/medien/1410/publikationen/2019-08-15_cc_30-2019_marktanalyse_oekostrom_ii.pdf

und für die Erzeugung keine Grünstromzertifikate ausgestellt werden. Durch die auslaufende EEG-Förderung für Erneuerbare-Energien-Erzeugungsanlagen erhöht sich der Anteil von Grünstrom, der direkt auf dem Markt gehandelt wird. Jede Wattstunde, die in Zukunft als Grünstrom vermarktet wird, muss in einem Register als Grünstromzertifikat geführt werden. Das Register in Deutschland ist das Herkunftsnachweisregister (HKNR) des Umweltbundesamtes. Um eine korrekte Zertifizierung zu ermöglichen, müssen alle Erzeugungsanlagen im Register registriert sein und jedes Grünstromzertifikat muss einer speziellen Erzeugungsanlage und einem Erzeugungszeitraum zugeordnet werden.

Die Funktionsweise des HKNR und des Großteils der Grünstromzertifikate-Register weltweit kann wie folgt beschrieben werden: Es handelt sich um Internetplattformen, auf denen Anlagen und Zertifikate von Organisationen digital verwaltet werden. Organisationen registrieren sich im Register und erhalten verschiedene Rechte basierend auf ihrer Rolle. Diese Rollen sind zum Beispiel Anlagenbetreiber, Händler, Energieversorgungsunternehmen oder Verbraucher. Anlagenbetreiber registrieren Anlagen im Register und beantragen die Zertifikatsausstellung. Zertifikate werden ausschließlich in der Einheit Megawattstunde ausgestellt. Händler handeln ausgestellte Zertifikate und verkaufen sie an Energieversorgungsunternehmen und Verbraucher, die die Zertifikate entwerten, um ihren Elektrizitätsverbrauch im Rahmen ihres Nachhaltigkeits-Reports als grün zu kennzeichnen.

Erzeugungsanlagen müssen heute einzeln und manuell im HKNR registriert werden. Zunächst müssen Anlagenbetreiber ein Nutzerkonto im HKNR anlegen. Der Betrieb des Kontos ist je nach Transaktionsvolumen mit Kosten von 50 bis 750 Euro pro Jahr verbunden.[111] Mit einem aktivierten Anlagenbetreiber-Nutzerkonto können neue Anlagen angelegt werden. Eine Anlagenart kann ausgewählt und basierend auf der Auswahl müssen die benötigten Anlagendaten in ein Webformular eingetragen werden. Jede Anlage wird einem oder mehreren (z. B. im Falle eines größeren Windparks) bestimmten technischen Zählpunkten im Netz zugeordnet. Eine gegebenenfalls vorhandene Anlagenförderung muss angegeben werden. Optionale Qualitätsmerkmale können manuell hinzugefügt werden. Die Neuanmeldung einer Anlage kostet einmalig 50 Euro. Um Strom als regional zu kennzeichnen, müssen Anlagen zusätzlich im Regionalnachweisregister registriert werden mit eigenen Konto- und Anmeldegebühren.

Die Registrierung und das Ausstellen von Grünstromzertifikaten können nur erfolgen, wenn bestimmte Voraussetzungen für die Erzeugungsanlage erfüllt sind. Sie müssen zum Teil durch Umweltgutachter und in manchen Fällen sogar durch Vor-Ort-Inspektionen geprüft werden.[112] Ein benötigtes Audit der Anlage wird im HKNR angezeigt und es kann ein entsprechender Umweltgutachter zugeordnet werden. Der Vertrag über das Audit muss außerhalb des HKNR abgeschlossen werden. Nach dem erfolgreichen Audit wird der Status der Anlage geändert und sie ist für die Nutzung im HKNR freigeschaltet.

Erzeugungsdaten der Anlage können über den technischen Zählpunkt in das HKNR importiert werden. Erst nach erfolgreichem Import kann die Ausstellung von Grünstromzertifikaten beantragt werden. Pro Megawattstunde und Transaktion fallen Kosten von 0,01 Euro für Ausstellung, Transfer und Rückbuchung und 0,02 Euro für die Entwertung an. Kontoinhaber haben die Möglichkeit, Dienstleistern die Kontrolle über ihr Konto zu überlassen. Diese können dann alle Aktionen im Register, wie Anlagenanmeldung und Zertifikatsausstellung, für sie ausführen.

Problemstellung

Die oben aufgeführten Kosten zeigen, dass die Anmeldung im HKNR heute recht aufwendig und kostspielig ist. Der Anmeldevorgang des HKNR ist nicht für Kleinstanlagen ausgelegt und die anfallenden Kosten machen die Anmeldung in vielen Fällen unwirtschaftlich. So gab es Stand 2017 nur zwischen 700 und 800 aktive Anlagenbetreiber-Accounts im HKNR, die größtenteils große Wasserkraft- und Biomasseanlagen verwalten.[113] Der Anteil von registrierten Windkraft- und Photovoltaik-Anlagen ist vernachlässigbar. In einer Zukunft, in der mehr und mehr Besitzer von großen und kleinen Erzeugungsanlagen ihren Grünstrom mithilfe von Grünstromzertifikaten nachverfolgbar machen und vermarkten sollen, wird ein neuartiges System benötigt.

5.2.2 Zielvorstellung und Gestaltungsvorschlag

Zielvorstellung

Zukünftige Grünstromzertifikate-Register sollten besser auf ein Energiesystem mit einer Vielzahl kleiner und dezentraler Erzeugungsanlagen eingestellt sein. Das bedeutet nicht, dass zwangsläufig alle Haushalte mit Dachsolaranlage ohne die Hilfe von Aggregatoren ihre eigenen Grünstromzertifikate verwalten und handeln sollen, aber es bedeutet, dass es idealerweise

111 http://www.gesetze-im-internet.de/hkngebv/BJNR270300012.html
112 https://www.umweltbundesamt.de/sites/default/files/medien/372/dokumente/einsatz_des_umweltgutachters_210408.pdf
113 https://www.umweltbundesamt.de/sites/default/files/medien/1410/publikationen/2019-08-15_cc_30-2019_marktanalyse_oekostrom_ii.pdf

so wenige technische und prozessuale Hürden wie möglich geben sollte, die die einfache Integration von Kleinstanlagen erschweren. Ein Grünstrom-Register, in dem auch Kleinstanlagen wie Dachsolaranlagen einzeln registriert werden können und deren Erzeugung effizient zertifiziert werden kann, sollte eine simple Anmeldung der Nutzer und Anlagen erlauben. Ideal wäre es, wenn die Anmeldung so automatisiert wie möglich stattfindet und bereits verfügbare Informationen so effektiv wie möglich nutzt. Das würde helfen, menschliche Fehler zu vermeiden und so eine niedrige Datenqualität zu verhindern sowie aufwendige nachträgliche Korrekturen zu verringern.

Gestaltungsvorschlag

Es gibt die Möglichkeit, dass mit einigen rechtlichen und technischen Änderungen Dienstleister ähnlich wie beim Konzept des virtuellen Kraftwerks Anlagen aggregieren und im HKNR verwalten könnten. In dem Positionspapier „Kleine Direktvermarktung für post-EEG-Anlagen“ werden Konzepte dafür und nötige Gesetzesänderungen diskutiert.[114] Doch auch wenn theoretisch mit einem leicht modifizierten bestehenden System umsetzbar, könnte auch die vorgeschlagene „Kleine Direktvermarktung“ von der Effizienz digitaler Verifizierbarkeit und der Sicherheit einer DID-basierten Geräteanmeldung profitieren.

Das Onboarding zu einem neuartigen Grünstromzertifikate-Register sollte idealerweise der in Kapitel 5.1 beschriebenen DID-basierten Geräteanmeldung folgen. Die Hauptanforderungen an ein solches Onboarding sind kryptografische Schlüsselpaare, die auf dem Gerät abgelegt sind, eine dezentrale Geräte-Identität, Basisdaten, die mit dieser Identität verknüpft sind, und eine rollenbasierte Authentifizierung.

Außerdem sollten die weiteren Funktionen des Grünstromzertifikate-Registers effizient umgesetzt werden. Dazu würde sich das von der Energy Web Foundation (EWF) entwickelte Origin Software Development Toolkit anbieten. Das Toolkit erlaubt jegliche Art der Sammlung von Erzeugungsdaten und ist somit offen für unterschiedliche Methoden, die heute und in Zukunft bei Kleinstanlagen Anwendung finden. Basierend auf den gesammelten Erzeugungsdaten werden On-Chain-Zertifikate ausgestellt. Die Zertifikate sind als Blockchain Token mit einer speziellen Architektur abgebildet und bestehen aus einem non-fungiblen Teil und einem fungiblen Teil. Non-fungibel heißt in diesem Zusammenhang spezifisch bzw. unverwechselbar und fungibel austauschbar bzw. dass eine Einheit mit einer anderen absolut identisch ist. Der non-fungible Teil trägt die statischen Daten, die das Zertifikat einzigartig machen, wie die Erzeugungsanlage und den Erzeugungszeitraum. Der fungible Teil trägt die Energiemenge, die durch diese Architektur effizient in jeder möglichen Teilung gehandelt und entwertet werden kann, wobei jede Einheit immer mit dem non-fungiblen Teil und damit den statischen Daten verknüpft bleibt. Die Granularität bzw. Einheit der Energiemenge kann dabei frei gewählt werden. So können die Ausstellung und der Handel auf dem Level von Kilowattstunden oder sogar Wattstunden ermöglicht werden.

Ein auf Grünstromzertifikate optimierter Handel kann mit dem Origin-Zertifikatebörse-Modul ermöglicht werden, das Verkaufsofferten neben Energievolumen und Preis um Attribute wie Anlagentyp, -ort und -alter und Erzeugungszeitraum erweitert. Käufer können den Markt nach den Attributen filtern und in ihren Kaufofferten bestimmte Attribute voraussetzen.

Der Transfer und die Entwertung der Zertifikate können durch die Verankerung auf der Blockchain technisch nachverfolgbar und verifizierbar gemacht werden. Da jeder Transfer und jede Entwertung als Transaktion auf der Blockchain gespeichert wird, kann das Zertifikat durch Kombination mit einem Identitätssystem digital und fälschungssicher nachverfolgt werden. Die Daten der Zertifikate, die auf der Blockchain abgesichert sind, können nicht mehr gefälscht werden. Doppelverkäufe oder -entwertungen der Blockchain-Zertifikate sind technisch ausgeschlossen. Alle Transaktionen können automatisiert verifiziert und so kann ein Audit vereinfacht werden.

5.2.3 Spezielle Vorteile bei Grünstromzertifikaten

Wird eine Geräte-Identität für alle energiewirtschaftlichen Anwendungen genutzt, ergeben sich für die Ausstellung von Grünstromzertifikaten einige Vorteile. Eine eindeutige Identifizierung der Anlage ist essenziell, da nur eine Verknüpfung des digitalen Zertifikats mit der digitalen Repräsentation der Anlage eine effiziente Nachverfolgung der Herkunft des Zertifikats erlaubt. Sind Zertifikat und Geräte-Identität auf einer Blockchain verankert und verknüpft, kann das Vertrauen in den Herkunftsnachweis noch verstärkt werden, da die Ausstellung des Zertifikats für eine spezielle Geräte-Identität fälschungssicher und nachverfolgbar als Transaktion gespeichert wird.

Außerdem können für Erzeugungsanlagen potenziell unterschiedliche Zertifikate ausgestellt werden. Für die gleiche Erzeugung könnten theoretisch Grünstromzertifikate oder Carbon-Offsets ausgestellt werden. Wird eine Geräte-Identität für alle Services genutzt, ist es sehr viel einfacher, zu identifizieren, wenn eine Anlage an beiden Anwendungen teilnimmt, und Doppelausstellungen werden vermieden.

Durch die Verwendung von Geräteschlüsseln könnten Grünstromzertifikate-Register die automatisierte Zertifikatsausstellung nur für Anlagen erlauben, die eine kryptografisch verknüpfte Datenquelle haben oder deren einzelne Erzeugungsdaten von dem Geräteschlüssel signiert wurden, und damit die Sammlung der Erzeugungsdaten absichern.

114 https://www.enbw.com/media/presse/docs/gemeinsame-pressemitteilungen/2020/20200615_positionspapier_kleine_direktvermarktung.pdf

5.3 Anwendungsfall Netzdienstleistungen von Kleinanlagen und Fahrzeugen

5.3.1 Rahmenbedingungen und Problemstellung

Netzdienstleistungen wie Regelleistung werden von Übertragungsnetzbetreibern angefordert und eingekauft, um einen stabilen und zuverlässigen Netzbetrieb zu gewährleisten.[115]

Alle Arten der Regelleistung haben gemeinsam, dass sie eine große Mindestanlagengröße voraussetzen. Zwar ist eine Bündelung von Anlagen möglich, allerdings betragen die Mindestgebote 1 Megawatt Primärregelleistung bzw. 5 Megawatt Sekundär- und Minutenreserve.[116] Zielsetzung dieses Anwendungsfalls ist, dass auch Fahrzeuge mit entsprechender Ladeinfrastruktur Netzdienstleistungen zur Verfügung stellen und sogar am Regelleistungsmarkt teilnehmen können. Ähnliches kann für Lasten wie Blockheizkraftwerke und Wärmepumpen untersucht werden.

Dazu gilt es, zwei Fragestellungen zu beantworten:

1. Wie muss ein regulatorisches Framework aussehen, das es ermöglicht, dass kleinere, nicht stationäre Anlagen wie Elektrofahrzeuge Netzdienstleistungen zur Verfügung stellen und sogar am Regelleistungsmarkt teilnehmen können, sodass der stabile und zuverlässige Netzbetrieb auch sichergestellt wird?
2. Wie kann die Prüfung der Eignung einer Anlage (Präqualifikation) technisch so unterstützt werden, dass der Aufwand der Übertragungsnetzbetreiber verhältnismäßig bleibt und eine sichere und überprüfbare Anbindung der Anlagen sichergestellt ist?

5.3.2 Zielvorstellung und Gestaltungsvorschlag

Aktuell haben kleine Anlagen (<1 Megawatt) keinerlei Sichtbarkeit bei den Übertragungsnetzbetreibern. Sie können daher nur gebündelt am Regelleistungsmarkt teilnehmen, da die Voraussetzung für die Präqualifizierung unter anderem ein Mindestgebot von 1 Megawatt beinhaltet. Jedoch verschleiert die Bündelung wiederum die Identität und die Eigenschaften der einzelnen Anlagen, sodass eine Präqualifizierung kleiner Anlagen auch später über diesen Weg nicht möglich ist.

In verschiedenen Projekten wird die proprietäre Anbindung von kleineren Anlagen und auch Fahrzeugen untersucht.[117] Dabei ist aber kein Wechsel zwischen den Anbietern möglich, da das gesamte Vertrauen von den Diensteanbietern ausgeht statt vom Gerät und dessen Eigentümer selbst.

Erschwerend kommt hinzu, dass erst die Einheit aus Fahrzeug und Ladesäule gemeinsam die Eigenschaften der gesamten Anlage beschreibt. Bei öffentlichen Ladesäulen ergeben sich hierdurch dynamisch neue Anlageneigenschaften, die sich aus den Eigenschaften der einzelnen Geräte ergeben. Ohne verifizierbare Geräte-Identität ist es daher bislang nicht allgemein möglich, Fahrzeuge und Ladesäulen am Flexibilitäts- und Regelleistungsmarkt teilnehmen zu lassen.

Die Elia Group bezeichnet daher in ihrem Vision Paper zur E-Mobilität Blockchain-basierte digitale Identitäten, um Fahrzeuge ins Stromnetz zu integrieren[118], als einen der wichtigen Eckpfeiler ihrer Konzernstrategie.

5.3.3 Spezielle Vorteile bei Netzdienstleistungen von Kleinanlagen und Fahrzeugen

Durch die Geräte-Identitäten, die der BMIL bereitstellt, können Fahrzeuge, Ladesäulen und andere kleinere Anlagen identifiziert werden. Nachdem die Prozesse der Präqualifizierung erfolgreich abgeschlossen sind, werden die Ergebnisse als Verifiable Credential auf Geräteebene festgehalten.

Dies hat vor allem zwei Vorteile für kleine Anlagen:

1. Der Aufwand der Übertragungsnetzbetreiber (ÜNB) wird reduziert, da die Ergebnisse der Präqualifikation dezentral und kryptografisch abgesichert vorgehalten werden. Damit kann datensparsam gearbeitet werden. Ein Austausch von Daten zwischen ÜNB ist nicht notwendig, da die Anlage selbst ihre Daten präsentiert.

2. Dadurch wird die Teilnahme von kleinen Anlagen am Regelleistungsmarkt wirtschaftlich. Anreize können direkt an die Betreiber der Anlagen weitergegeben werden. Bei nicht ortsfesten Anlagen wie Elektrofahrzeugen ergibt sich noch ein dritter, erheblicher Vorteil:

3. Die tatsächlichen Eigenschaften des Verbunds von Fahrzeug und Ladesäule werden bei jedem Ladevorgang erneut automatisiert festgestellt. Dies wäre ohne eine anlagenscharfe Identifizierung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich.

5.4 Anwendungsfall Smart (CO_2) Certificates

Ähnlich wie bei den oben beschriebenen Grünstromzertifikaten bildet der Nachweis des CO_2-Fußabdrucks die Fortschreibung einer spezifischen Kenngröße zukünftigen industriellen Handelns ab.

Je wichtiger und ambitionierter die auf staatlicher, supranationaler oder auf Ebene einzelner Industrien getroffenen CO_2-Einsparungsvereinbarungen werden und je ökonomisch relevanter der CO_2-Emissionsrechtehandel wird, desto höher steigt der Druck auf die produzierende Ebene, den CO_2-Verbrauch auch entlang der vielen Produktionsschritte oder gar entlang der Nutzung eines industriell gefertigten Produkts nachzuweisen.

115 https://www.regelleistung.net/ext/static/technical
116 https://eepublicdownloads.azureedge.net/clean-documents/Publications/Market%20Committee%20publications/ENTSO-E_Balancing_Report_2020.pdf
117 https://www.elaad.nl/projects/frequency-containment-reserve-pilot/
118 Übersetzt, engl.: Blockchain based digital identities to integrate EVs into the power system https://www.eliagroup.eu/en/news/press-releases/2020/11/20201120_publication-vision-paper-on-e-mobility, Seite 7

Zu diesem Zweck muss zweierlei gelingen: Erstens müssen Verbräuche von CO_2 entlang der internationalen Wertschöpfungsketten kompatibel gestaltet werden (wobei sich die Verwendung der Blockchain als Technologie für eine solche interoperable Registerführungsebene hervorragend eignet) und darüber hinaus muss auch der CO_2-Footprint in einem Daten-Container und einem Datenformat vorgehalten werden, die universell einsetzbar und mit anderen regulatorischen Vorschriften synergetisch verwendet werden können. Denn auch bei solchen datenindustriellen Prozessen sind Fragen nach der Energieeffizienz berechtigt, entsprechend sollten nicht unnötigerweise verschiedene Systeme parallel zueinander etabliert werden, wenn sich dieselben Informationen auch auf einer Ebene verdichten lassen.

Vor diesem Hintergrund geht es im hier gezeigten Use Case des CO_2-Trackings darum, beides zu ermöglichen. Dabei wird die Einführung eines international einsetzbaren Prozesses zur Erfassung und zum Transport des CO_2-Footprints von Materialien und Produkten entlang der Wertschöpfungskette gezeigt. Er setzt auf seit Langem bestehenden Normen wie der EN 10204 für Materialprüfzeugnisse für Metall- und Kunststoffe, die im Wesentlichen einen Material-Passport definieren, sowie neueren Entwicklungen wie der DIN SPEC 901, die elektronische Materialprüfzeugnisse und Konformitätsbestätigungen definiert, auf. Dieses Konzept umfasst Referenzen auf Materialien, Komponenten und Prozesse und stellt damit inhaltlich einen Product Passport dar.

Dieser Use Case wurde gemeinsam mit S1Seven | Material Identity erarbeitet. Die S1Seven GmbH bietet eine dezentrale Softwareplattform, die digitale und datenschutzkonforme Qualitätszertifikate-as-a-Service für Stahl, Metall und Kunststoffe zur Verfügung stellt. Die auf der Blockchain-Technologie basierende Lösung ermöglicht es Stakeholdern, in allen Phasen der Lieferkette maschinenlesbare Daten anstelle von papierbasierten Dokumenten auszutauschen, um sie für die intelligente Fertigung zu nutzen, Nachhaltigkeitsmerkmale zu berücksichtigen und somit auch die Überprüfung der Material- und Prozessherkunft zu automatisieren.

5.4.1 Anwendungsfall, Zielvorstellung und Anforderungen

Anwendungsfall

Mit einem Zulieferer der deutschen Automobilindustrie in Salzburg wurde eine Studie durchgeführt, um den CO_2-Footprint einer Komponente zu berechnen, die am Ende in die Fahrzeuge eines deutschen Automobilherstellers verbaut wird. Die Berechnung des potenziellen Beitrags zum Klimawandel erfolgte gemäß dem aktuellen Stand der Ökobilanzierung Environmental Footprint Initiative Version 3.0.

Das in diesem Fall verwendete Ausgangsmaterial ist Aluminium, aber auch in anderen Zulieferindustrien, etwa im Bereich der Plastikbauteile, gibt es ähnliche Anforderungen auf Ebene der Konformitätszeugnisse.

Zielvorstellung

Ergebnis der Studie ist, dass im konkreten Fall zwei Größen den CO_2-Footprint wesentlich bestimmen:

1. Der CO_2-Footprint der Vormaterialien – beginnend beim Abbau über die Verhüttung bis zur Anlieferung am Werkstor

2. Der Energiebedarf für das Erwärmen / Schmelzen / Verarbeiten des Vormaterials

3. Alle anderen Materialien und zum Einsatz kommenden Betriebsmittel sind vernachlässigbar bzw. über Konstanten abbildbar.

Anforderungen

Darauf basierend wurde folgender Proof of Concept entwickelt:

1. Der chargenspezifische CO_2-Footprint des Vormaterials wird in Materialprüfzeugnissen gemäß EN 10204 3.1 durch den Materiallieferanten bereitgestellt.

2. Diese Werkszeugnisse werden als elektronische Dokumente gemäß der DIN SPEC 9012 umgesetzt und durch den Aussteller, dem zertifizierten Prüflabor des Materiallieferanten, auf der Blockchain notarisiert.

3. Der Energieverbrauch sowie die Qualität der Energie werden laufend auf der Blockchain protokolliert und stehen zum Zeitpunkt der Berechnung des CO_2-Footprints zur Verfügung.

4. Für jede hergestellte Komponente wird der exakte CO_2-Footprint berechnet, basierend auf den Daten aus dem Materialprüfzeugnis des verwendeten Vormaterials sowie der zum Einsatz gekommenen Energie und deren Qualität. Für jede Komponente wird eine elektronische Konformitätsbestätigung erstellt, die den exakten CO_2-Footprint enthält. Sie enthält eine Referenz auf das Werkszeugnis der Vormaterialien sowie den Energieverbrauch.

Da das Unternehmen ein eigenes Wasserkraftwerk besitzt und somit zu 100 Prozent mit Grünstrom versorgt ist, wurde das Konzept vereinfacht.

- Wird zum Zeitpunkt der Herstellung kein Strom bezogen, wird das Bauteil als mit 100 Prozent Grünstrom hergestellt in der Konformitätsbestätigung ausgewiesen.

- Wird Strom bezogen, so wird der Anteil auf 0 Prozent gesetzt.

5.4.2 Illustrative Ausschnitte aus der Konformitätsbestätigung

In die Konformitätsbestätigung wurden folgende weitere Qualitätsmerkmale aufgenommen:

1. Referenz auf die Berechnungsgrundlage – im Beispiel **Documentation Certification**
2. Indikator, dass der Grünstrom-Anteil 100 Prozent ist – im Beispiel **Share Renewable Energy**
3. DID des Zählers – im Beispiel **Metering Point**
4. Referenz auf Materialprüfzeugnis mit CO_2-Footprint – im Beispiel **Material Inspection Certificate**
5. CO_2-Footprint des eingesetzten Materials – im Beispiel im Attribut **CO_2 Footprint** des Materials


```
"ObjectOfDeclaration": [
        {
          "ObjectId": "1",
          "ObjectName": "Part Name",
          "ObjectType": "Part",
          "Quantities": [
            {
              "Amount": 1,
          ],
          "AdditionalObjectProperties": [
            {
                "Name": "CO2 Footprint",
                "Value": [
                  "28.67 kg CO2e"
                ]
            },
            {
                "Name": "Share Renewable Energy",
                "Value": [
                  "100 %"
                ]
            },
            {
                "Name": "Metering Point",
                "Value": [
                  "did:r3c:8z6uqiAA1XJLhFfVatuVpG1kuCFCYVzGfPe55tinkBoo"
                ]
            },

            {
              "Name": "Documentation Certification",
              "Value": [
                "202012_Dokumentation_CarbonFootprint_1.pdf"
              ]
            },
            {
              "Name": "DocumentHashSHA256",
              "Value": [
                "de211cf4fa0f8e16e08a06565550d8450720f705011ede11045d6c64ced9f9f5"
              ]
            }
          ]
        },
        {
          "ObjectId": "2",
          "ObjectName": "Material Name",
          "ObjectType": "Material",
          "Quantities": [
            {
              "Amount": 0.83  ,
              "Unit": "kg"
          ],
          "AdditionalObjectProperties": [
            {
                "Name": "CO2 Footprint",
                "Value": [
                  "7.1   kg CO2e"
                ]
            },
            {
              "Name": "Material Inspection Certificate",
              "Value": [
                "MaterialInspectionCertificate_1.pdf"
              ]
            }
          ]
        }
```


Ausschnitt aus der Konformitätsbestätigung

Durch die Installation eines BMIL-kompatiblen Zählers

1. können die Identität der Messgeräte sowie der Ort ihrer Installation automatisch validiert werden.

2. kann die Qualität der zum Herstellungszeitpunkt eingesetzten Energie überprüft werden.

In einem Szenario, in dem nur teilweise Grünstrom eingesetzt wird, sind Zähler an den wesentlichen Verbrauchern und Erzeugern von Energie und eine Zuordnung der Qualitäten zu ihnen sowie eine Bilanzierung der Mengen und Qualitäten nötig.

5.4.3 Status quo der Geräteanbindung und aktuelle Alternativen

Das Unternehmen ist in der besonderen Lage, auf dem Werksgelände ein eigenes Wasserkraftwerk zu besitzen und damit die Produktion ausschließlich mit Grünstrom versorgen zu können. Das Unternehmen ist dazu entsprechend durch einen externen Auditor zertifiziert. Daher wurde auf eine Umsetzung der Geräteanbindung verzichtet.

In anderen Fällen, wenn sich also die Stromversorgung für die Produktion aus (mehreren) externen Quellen speist, würde dann die Zusammensetzung der gesamten Energie-Provenienz durch BMIL-geführte Assets nachgewiesen werden und die Firma sowie deren Versorger könnten durch die verschiedenen im Projekt aufgezeigten Anbindungsoptionen mit Blockchain-basierter Datenhaltung und SMGW-Anbindung agieren.

5.4.4 Abschließende Bemerkungen

Die deutsche Automobilindustrie hat 2021 die Initiative Catena-X gestartet[119]. Einer der Anwendungsfälle, die im Rahmen der Initiative umgesetzt werden sollen, ist der Nachweis des CO_2-Fußabdrucks und in der Folge seine Minimierung. Für den Nachweis und die Umsetzung von Maßnahmen zur Reduktion bedarf es detaillierter, vertrauenswürdiger Daten, die automatisch auditiert werden können. Nachdem für den CO_2-Fußabdruck eines Teils und am Ende eines Autos der CO_2-Fußabdruck der Materialien sowie die Energie bestimmend sind, ist die einfache Verschränkung dieser Daten anhand interoperabler Blockchain-basierter Identitäten von großem Vorteil.

5.4.5 Spezielle Vorteile bei Smart (CO_2) Certificates

Den größten Nutzen in diesem Use Case bzw. entlang der hier involvierten industriellen Wertschöpfungskette sehen die Unternehmen in den nachgelagerten Wertschöpfungsstufen, denn sie können folgende Effekte erzielen:

1. Viele dieser Unternehmen investieren in die automatische Validierung aller eingehenden Qualitätsdokumente. Der Übergang von PDF-Dokumenten zu elektronischen Formaten wie JSON, abgesichert durch die Blockchain-Technologie, vereinfacht dies und senkt damit die nicht unwesentlichen Qualitätskosten dieser Industrien.
   Ein wesentlicher Bestandteil dieser Prüfungen wird in Zukunft die Validierung der Angaben zum CO_2-Footprint sein.

2. Exakte Werte, wie etwa maschinell verarbeitbare Daten zum CO_2-Footprint von Bauteilen, um diese dann zu aggregieren und als Gesamtwert des Endprodukts belastbar nachweisen zu können, werden an sich zu einem Mehrwert oder mittelfristig zu einer geforderten Leistung.

3. Nachvollziehbarkeit der Herkunft der Materialien im Sinne des Lieferkettengesetzes

Ein öffentliches Geräteregister ermöglicht somit als unabdingbare Voraussetzung eine kosteneffiziente und vertrauenswürdige Validierung der Herkunft der für die industrielle Produktion eingesetzten Energie – potenziell entlang aller Wertschöpfungsschritte.

Abschließend kann festgestellt werden, dass ein öffentliches Geräteregister Mehrwert im Zusammenspiel mit Regularien in anderen Industrien liefern kann, der aus einer primär energiewirtschaftlichen Sicht nicht ersichtlich ist. Denn wenn erst einmal ein Datenformat vorgegeben wird und ein „Datencontainer" etabliert ist, kann dieser mit anderen nützlichen oder erforderlichen Daten und Credentials angereichert werden.

119 https://catena-x.net/de/

5.5 Anwendungsfall Energy Communities

Mit Energy Communities werden grundsätzlich Vorteile wie die verbesserte Akzeptanz für regionalen erneuerbaren Strom, verstärkter Zubau von Erneuerbare-Energien-Anlagen, wirtschaftliche Partizipation an der Energiewende oder auch die Entlastung des Stromnetzes durch die passgenaue Bilanzierung des lokalen Angebots und der Nachfrage verbunden. Dabei ermöglichen digitale Technologien innovative Geschäftsmodelle wie Peer-to-Peer Energy Sharing.[120]

In diesem Use Case geht es um den Austausch von Energie im lokalen Kontext – dort also, wo durch die räumliche Nähe der Teilnehmer an einer solchen Energy Community die lokalen „Spielregeln" der Energiegemeinschaft einfacher erklärbar werden und teilweise auch durch die Partizipation der Energiekunden mitgestaltet werden können. Ein weiterer Vorteil eines solchen Setups ist, dass der Austausch von Energie in einem solchen Rahmen ortsangepasst incentiviert werden kann, um das jeweils gewünschte Verhalten zu erzielen.

Einen entsprechenden Case hat der in Wien ansässige BMIL-Projektteilnehmer Riddle&Code GmbH in Zusammenarbeit mit dem in der Bundeshauptstadt ansässigen Versorgungsunternehmen Wien Energie GmbH realisiert.

5.5.1 Anwendungsfall, Zielvorstellung und Anforderungen

Anwendungsfall und Zielvorstellung

Mit dem Grünen Energiepaket[121], insbesondere der Richtlinie (EU) 2018 / 2001 zur Förderung der Nutzung von Energie aus erneuerbaren Quellen und der Richtlinie (EU) 2019 / 944 über gemeinsame Vorschriften für den Elektrizitätsbinnenmarkt, hat die Europäische Kommission nicht nur eine umfassende Neuordnung des europäischen Subventionsrahmens im Bereich der erneuerbaren Energien eingeleitet, sondern auch die Frage der Bürgerbeteiligung aufgegriffen – mit dem Ziel, die Energiewende in Europa zu unterstützen.

Als eines der ersten EU-Mitgliedstaaten hat Österreich mit dem Beschluss des „Erneuerbaren-Ausbau-Gesetzes"[122] (EAG) die im EU-Richtlinienpaket vorgesehenen Rahmenbedingungen zur Gründung und zum Betrieb von „Erneuerbare-Energien-Gemeinschaften" (Renewable Energy Communities, RECs) und „Bürgerenergiegemeinschaften" (Citizen Energy Communities, CECs) geschaffen und in nationales Recht umgesetzt. Das Gesetz ist am 1. Januar 2022 in Kraft getreten.

Dementsprechend hoffen die Projektparteien Wien Energie und Riddle&Code, mit dem Anwendungsfall „Peer-to-Peer im Quartier", angesiedelt in der österreichischen Bundeshauptstadt Wien, bereits heute eine wertvolle Perspektive auf die Abläufe und technischen Anforderungen in Bezug auf künftige, ähnlich geartete Gesetzgebungen in Deutschland und anderen EU-Mitgliedstaaten aufzeigen zu können. Denn im Rahmen dieses Projekts wurden bereits zentrale Kriterien Erneuerbarer-Energien-Gemeinschaften erfüllt und auch die Anbindung an die BMIL-Architektur wurde durch Darstellung der Interoperabilität von Datensätzen auf der DID-Ebene vorgenommen.

Das übergeordnete Ziel des Energy Community Use Case sind die Entwicklung und Testung einer Infrastruktur für die Steigerung des Eigenverbrauchs (Produktion durch Gemeinschafts-PV-Anlagen) einer Energy Community mithilfe eines Peer-to-Peer-Handelssystems sowie die Optimierung der Bewirtschaftung eines Community-Stromspeichers.

Der Use Case wurde im sogenannten „Viertel Zwei" im zweiten Wiener Gemeindebezirk umgesetzt, einem Stadterneuerungsgebiet zwischen dem Campus der neuen Wirtschaftsuniversität Wien und der Trabrennbahn Krieau.

Die Nutzergruppe für den Use Case umfasste die Bewohnerinnen und Bewohner von 292 Wohneinheiten im Viertel. Die genutzte Infrastruktur bestand hauptsächlich aus den PV-Anlagen auf den Studiowohnungen sowie dem im Viertel Zwei installierten Quartierspeicher.

Im speziellen Anwendungsfall wurden der gemeinschaftliche Besitz und die Nutzung der Erzeugungsanlage über die Anbindung eines in diesem Projekt „Trusted Gateway" genannten Device, das einen Kryptochip zur direkten und sicheren Anbindung an eine Blockchain umfasst, dargestellt, mit dem Ziel der Eigenverbrauchsoptimierung der Gemeinschaft. Die Verwendung des Trusted Gateway als separates Device mit eingebautem Kryptochip ergab sich durch die lokale Situation in Österreich im Hinblick auf die dortige Regulierung im Bereich von Smart Metern – das Trusted Gateway ist also nicht als Alternative zu den oben vorgestellten Anbindungsvarianten des BMIL-Projekts an die BSI-zertifizierten Smart-Meter-Gateways in Deutschland zu verstehen, sondern als ein Gerät, das aufgrund anderer Marktumstände in Österreich mit einer Blockchain- und hardwarebasierten digitalen Identität versehen wurde, die mit den entsprechenden Geräte-Identitäten im Rahmen des BMIL interoperabel gestellt werden muss, wenn ein grenzüberschreitendes Projekt im BMIL abgebildet werden soll.

120 https://future-energy-lab.de/newsroom/publikationsdetailansicht/pub/dena-analyse-energy-communities-beschleuniger-der-dezentralen-energiewende/
121 https://ec.europa.eu/energy/topics/energy-strategy/clean-energy-all-europeans_en
122 https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20011619

Um jedenfalls die Bedingungen für die Gründung einer Erneuerbare-Energien-Gemeinschaft im österreichischen Markt zu erfüllen, müssen sich alle Gemeinschaftsmitglieder sowie die Erzeugungsanlagen in einer Netzebene (Netzebenen 5–7) befinden.

Die Verteilung bzw. Zuordnung der erzeugten Strommenge auf die Gemeinschaftsmitglieder erfolgt über einen standardisierten „dynamischen Aufteilungsschlüssel" durch den Verteilnetzbetreiber wie bei dem bestehenden Modell „Gemeinschaftliche Erzeugungsanlagen".[123] Für die innerhalb der Community verbrauchte Erzeugungsmenge fällt ein reduziertes Netzentgelt (Ortsnetztarif) an. Zusammen mit einer Reduktion der Abgaben kann so eine signifikante Verringerung des Gesamtstrompreises auf Endkundenseite erzielt werden. Reststrommengen werden weiterhin aus dem öffentlichen Netz bezogen und unterliegen somit der klassischen Stromverrechnung. Jedes Gemeinschaftsmitglied darf den Energielieferanten für den Reststrombezug frei auswählen.

Während auf den Aufteilungsschlüssel selbst kein Einfluss genommen werden kann, lässt sich durch die Nutzung der auf der Blockchain notarisierten und vom Trusted Gateway signierten Daten zu Erzeugung, Verbrauch und Speichernutzung dann manuell (zum Beispiel: Dashboard zeigt Erzeugungsüberschuss, Nutzer schaltet Waschmaschine ein) oder automatisiert (Quartierspeicher speichert Überschuss) Einfluss auf das Verbrauchsverhalten nehmen.

Als am besten geeignetes Optimierungsziel hat sich die Betrachtung der gesamten Gemeinschaft gezeigt, da dadurch die lokale Nutzung der PV-Produktion sichergestellt und eine Benachteiligung einzelner Teilnehmerinnen und Teilnehmer vermieden werden konnte.

Das System wurde entsprechend auf drei Ebenen implementiert:

- Die erste Ebene ist die Energieinfrastruktur für die gemeinschaftliche Nutzung der Energie. Dafür wird die vorhandene Infrastruktur im Quartier durch Smart-Meter-Auslesegeräte ergänzt, die die Stromflüsse nahezu in Echtzeit überwachen und – durch das Trusted Gateway signiert – damit eine vertrauenswürdige Datengrundlage liefern. Zusätzlich wird das Steuerungssystem des Quartierspeichers mit eingebunden.
- Die zweite Ebene bezieht sich auf die sichere und nachvollziehbare Blockchain-Datenhaltung als Grundlage aller weiteren Anwendungen. Auf dieser Ebene können dann auch externe Stellen auf die Projektdaten und die assoziierten Geräte-Identitäten zugreifen – sofern sie denn dazu autorisiert sind.
- Die dritte Applikationsebene beinhaltet die Schnittstellen zu den Pilotkundinnen und -kunden. Dazu gehören das User Interface, das einen Überblick über die aktuellen und historischen Stromflüsse und Transaktionen bietet, sowie die automatische Erstellung der Abrechnungen unter Berücksichtigung der Peer-to-Peer-Lieferbeziehungen.

Die Blockchain-Technologie und der damit verbundene Einsatz vertrauensbildender Gateways (etwa des Trusted Gateway) und dezentraler Identitäten schafft in diesem Zusammenhang völlig neue Möglichkeiten für die Gestaltung von Community-Anwendungen mit besonderem Fokus auf die Beschleunigung vertraglich gebundener On- und Offboarding-Prozesse sowie die Vereinfachung des Energiehandels und -austauschs.

Anforderungen

Ziel der Anbindung dieses Use Case war es, die Interoperabilität zwischen den Identitäten zu zeigen, die in der Peripherie verschiedener Blockchains verwaltet werden.

Das bedeutet, dass in Zukunft unterschiedliche, in einem Projekt zusammen verwendete Blockchains interoperabel gestellt werden und entsprechend Identitäten und Projektdaten zueinander in Beziehung gebracht werden können, ohne dass ein solches Gesamtprojekt Abstriche bei der Eindeutigkeit der Identifizierung der verwendeten physikalischen Assets machen müsste. Ebenso lassen sich die in den Blockchains notarisierten Daten und Credentials projektübergreifend verwenden und zu den eindeutig identifizierbaren physikalischen Assets in Beziehung setzen.

Der Konsortialpartner EWF hatte angeregt, das Konzept der DIDs zusammen mit überprüfbaren Berechtigungsnachweisen zu verwenden, um mit diesen dezentralen Identitäten zu interagieren und eine Möglichkeit zur Überprüfung ihrer Authentizität zu bieten. EWF verwaltet die Identitäten für das BMIL-Projekt entsprechend auf dem KILT-Protokoll, um die Interoperabilität mit der Energy Web Chain herzustellen.

123 https://energytransition.klimafonds.gv.at/wp-content/uploads/sites/7/2019/03/Infoblatt-Gemeinschaftliche-Erzeugungsanlage-20170921-1.pdf

Das P2P-Projekt mit der Wien Energie basiert hingegen auf BigchainDB, einem Blockchain-Netzwerk, das im Wesentlichen die Funktionalitäten einer dezentralen Datenbank bietet.[124]

Entsprechend wurde auch von Riddle&Code der „Universal Resolver" verwendet, um die Identitäten aufzulösen, und vc-js als JavaScript-Implementierung des W3C-Standards Verifiable Credentials, um die Anmeldeinformationen zu verifizieren.

Im Fall dieses Use Cases verbinden wir das im Projekt mit der Wien Energie verwendete Trusted Gateway (siehe unten) mit Energiequellen, um diesen eine fälschungssichere digitale Identität zu geben. Diese Identitäten werden mithilfe des durch die IPDB Foundation geführten öffentlichen BigchainDB-Netzwerks bzw. in einer von Riddle&Code auf dieser Basis optimierten projektspezifischen Sidechain von BigchainDB verwaltet. Es handelt sich dabei um eine Tendermint-basierte Anwendung, die MongoDB benutzt, um Transaktionsdaten zu speichern, und „Crypto Conditions"[125] verwendet, um Transaktionen zu validieren.

In regelmäßigen Abständen werden also Assets auf BigchainDB erstellt, um die Produktionsdaten der im Projekt etablierten Identitäten zu beglaubigen.

Die Implementierung für das BMIL-Projekt gestaltete sich dabei wie folgt:

- Basierend auf der Universal-Resolver-Infrastruktur von Markus Sabadello[126] wurde ein Resolver erstellt, der DIDs aus BigchainDB zur Verfügung stellt.
- Alle identitätsrelevanten Dokumente („Subject" in der DID-Terminologie) wurden auf BigchainDB bereitgestellt, sodass die nativen Transaktionsinformationen von BigchainDB einbezogen werden können.
- Die entsprechenden BMIL-Credentials wurden an die Geräte-Identitäten in diesem Use Case ausgegeben (auf diese Weise wird garantiert, dass die Identitäten gemäß BigchainDB vertrauenswürdig sind).
- Die Identitäten verwenden die Credentials und speichern sie zusammen mit den Produktionsdaten, um die Authentizität überprüfbar zu machen.
- Eine Demo-Anwendung wurde erstellt, um den Prozess zu verifizieren.

Die enge Abstimmung zwischen allen beteiligten Konsortialpartnern ermöglichte es, die geschaffene Interoperabilität zwischen dem Use Case in Wien und dem BMIL zu zeigen.

Auswirkungen auf den Energy Community Use Case

Mit DIDs und überprüfbaren Berechtigungsnachweisen bieten wir eine Möglichkeit, die Authentizität einer auf BigchainDB verwalteten Identität zu überprüfen. Darüber hinaus können alle Transaktionen, die von den Projektidentitäten auf BigchainDB erstellt werden, von jeder Anwendung oder jedem System mithilfe unseres DID-Resolvers und vc-js überprüft werden.

Die Produktionsdaten werden also auf BigchainDB gespeichert und können von jeder Anwendung abgefragt werden. Zusammen mit den Produktionsdaten speichern wir die Anmeldeinformationen der Identitäten, wodurch es einer Anwendung oder einer dritten Partei möglich ist, zu überprüfen, dass die Produktionsdaten aus diesem Energy-Communities-Projekt als vertrauenswürdig eingestuft werden.

Somit ist also sowohl die Interoperabilität von Projektdaten und Credentials dargestellt als auch durch die Anbindung dieses Use Case an die vorgeschlagene BMIL-Architektur aufgezeigt worden, dass Blockchains mit spezifischen Fähigkeiten nahtlos in einer komplexen industriellen Anwendungsumgebung zusammenwirken können, ohne dass in Sachen Datensicherheit oder Vertrauen in die Datenherkunft Abstriche gemacht werden müssen.

Dies hat als Resultat zur Folge, dass verschiedene Anwendungen oder Teilnehmer oder andere Maschinen diese überprüfbaren Berechtigungsnachweise nutzen können, um sicherzugehen, dass die Daten aus einer vertrauenswürdigen Quelle stammen, und sich diese Provenienz, wie gezeigt, auch zwischen unterschiedlichen Blockchain-Identitätslösungen interoperabel und automatisierbar handhaben lässt.

5.5.2 Status quo der Geräteanbindung und aktuelle Alternativen

In diesem P2P Energy Communities Use Case wird ein „Trusted Gateway" genanntes Device mit einem eingebauten Kryptochip („Secure Element") verwendet, das architektonisch ähnlich wie die oben in diesem Bericht beschriebene OLI Box aufgebaut ist: Das Trusted Gateway beinhaltet die aktuellste Raspberry

124 Siehe: https://www.bigchaindb.com/. Das Netzwerk wird noch im Juni 2022 in Planetmint umbenannt werden.
125 https://datatracker.ietf.org/doc/html/draft-thomas-crypto-conditions-03
126 https://medium.com/decentralized-identity/the-universal-resolver-infrastructure-395281d2b540

Pi-Version als Host Device und ein Secure Element als Kryptochip, das alle für das Projekt benötigten Krypto-Acceleratoren sowie sonstige Bauteile, etwa für eine flexible und leistungsfähige Funkanbindung, beinhaltet, um die für eine hochsichere Anbindung an Blockchains nötigen kryptografischen Prozesse und Signaturen zu ermöglichen.

Die Notwendigkeit eines solchen separaten Gateways war auch im österreichischen Markt gegeben, da die Smart-Meter-Regulierung dort weniger weit fortgeschritten ist als in Deutschland und die benötigten Produktionsdaten der energieerzeugenden Anlagen zum Zeitpunkt des Projektstarts noch nicht direkt durch die Endverbraucherinnen und -verbraucher aus den eingesetzten Geräten ausgelesen werden konnten. Somit wurden diese Daten nicht aus der Bestandsinfrastruktur ausgelesen und der Kryptochip zur Blockchain-Anbindung wurde nicht direkt darin verbaut, sondern es wurde ein separates Gerät eingeführt.

Da der beschriebene Use Case aber in der Zwischenzeit mit etwas anderen Schwerpunkten auch kommerziell den Kundinnen und Kunden von Wien Energie angeboten wird[127], können das Trusted Gateway und die im Projekt verwendete Infrastruktur noch weitere Features abbilden:

So bildet das Gerät mithilfe des Secure Element eine komplette Hardware-Wallet ab und kann entsprechend mit verschiedenen Blockchains interagieren und Transaktionen in diese Ziel-Blockchains signieren und schreiben. Ebenso wird im Backend eine hochsichere Key-Management-Cloud-Plattform von Riddle&Code eingesetzt, die auch im Bankensektor verwendet wird. Damit kann ein flexibles, rollenbasiertes System zur Orchestrierung von Zugriffs- und Zugangsbeschränkungen hinzugeschaltet werden, um Sicherheit und Automatisierbarkeit zu ermöglichen, wenn neben menschlichen Akteuren auch Geräte mit entsprechenden Mandaten zu autonomen Teilnehmern eines solchen Netzwerks werden.

Diese über die reine Gateway-Funktionalität hinausgehenden Möglichkeiten zeigen, dass die Blockchain-Technologie einen größeren Leistungsumfang bereitstellen kann als „nur“ höhere Prozesssicherheit und vertrauenswürdige Registerführung.

5.5.3 Spezielle Vorteile bei Energy Communities

Die Schaffung einer eindeutigen und jederzeit überprüfbaren Geräte-Identität sowie assoziierter Metadaten hat hoffentlich das Potenzial, die Zusammenführung aktuell noch oder wieder getrennter Strompreiszonen (wie im deutschen und österreichischen Fall) zu unterstützen – bei gleichzeitiger Gewährleistung oder Etablierung höchster Sicherheitsansprüche.

Des Weiteren ist es für kommerzielle Anwendungen und die Einführung neuer Business-Modelle (wie im Beispiel der Energy Communities und der Tokenisierung von Anlagen wie im hier beschriebenen Projekt von Wien Energie) essenziell, vertrauenswürdige Geräte-Identitäten als Grundlage zu haben, da sonst gerade bei Projekten, in denen die produzierte Energie selbst handelbar gemacht wird und potenziell zu bilanzierende Werte geschaffen werden, eine Aufblähung dieser Werte über nicht autorisierte, hinzugefügte oder verfälschte Geräte möglich wäre. Ebenso lässt sich auf Basis registrierter und durch ein Blockchain-Backend ansteuerbarer Anlagen eine Erhöhung der Cybersicherheit erreichen, indem auch die Netzwerkintegrität und das Funktionieren der Anlagen gemäß gewünschten und im Fall einer weitergehenden Regulierung, die auch Smart Contracts umfasst, vorgeschriebenen Kriterien überprüfbar macht.

Für die Umsetzung neuer Business-Modelle ist es des Weiteren essenziell, dass die Masterdaten aller beteiligten Marktteilnehmer – hier eben der betreffenden Anlagen – überprüfbar sind. Hierbei würde der BMIL als Register wertvolle Dienste leisten. Nur so können auch die notwendigen Voraussetzungen für das reibungslose und effiziente Managen von Energy Communities geschaffen werden – idealerweise in einem technisch dezentralen Setup und ohne zentralisiertes technisches Backend, aber mit einheitlicher Governance.

So werden sich von der Incentivierung durch den Einsatz von Tokens bis hin zur sicheren Prozessautomatisierung in Zukunft viele wichtige Module in zukunftsweisende energiewirtschaftliche Projekte mit einbinden lassen, basierend auf einer sicheren und eindeutigen Geräte-Identität. Informationsaustausch lässt sich auf dieser Basis vertrauenswürdig als Transaktionen strukturieren und IoT-Geräte werden zu Handelspartnern nach präzise festgelegten Marktregeln. Nur so wird eine Echtzeit-Energiewirtschaft mit Milliarden von Transaktionen und zahllosen Teilnehmern überhaupt erst möglich.

5.6 Zusammenfassende Bewertung der Vorteile der BMIL-Geräteanbindung für die Mehrwertanwendungen

Eine DID-basierte Geräteanbindung mit Geräteschlüsseln hat einige Vorteile gegenüber der bestehenden Geräteanbindung in den betrachteten Anwendungsfällen (mit Ausnahme des Energy-Community-Beispiels, wo schon eine dazu ausgestattete Hardwarelösung verwendet wird).

127 https://www.trendingtopics.at/riddle-code-tokenisiert-mit-wien-energie-die-groesste-solaranlage-oesterreichs/

Die Vorteile lassen sich in verschiedene Kategorien einteilen: Vorteile durch Nutzung einer einzigen digitalen Geräte-Identität, durch Nutzung von Geräteschlüsseln, durch die Verankerung auf der Blockchain und durch die dezentrale Speicherung von Credentials.

Eine Identität

Wenn Geräte oder Anlagen digital von genau einem DID repräsentiert werden, die kryptografisch mit ihren Geräteschlüsseln verknüpft ist, dann stellt das einen großen Unterschied zum Status quo dar. Heute benötigen Geräte eine digitale Repräsentation in Form einer Anmeldung für jede einzelne Anwendung, an der sie teilnehmen sollen. So müssen Anlagen unabhängig beim Netzbetreiber und unterschiedlichen Anwendungsfällen wie im HKNR sowie bei potenziellen Aggregatoren, Energy Communities und Flexibilitätsmärkten registriert werden. Wird die Anlage im digitalen Raum von genau einem DID repräsentiert, dann kann das zu erheblichen Effizienzgewinnen führen. So benötigen die meisten Dienstleistungen und Märkte im Energiesektor ähnliche Stammdaten von der Anlage. Beispiele sind die Kapazität, das Inbetriebnahmedatum und der Installationsort etc.

Werden diese Basisdaten in einem allgemein anerkannten und sicheren Prozess mit der Anlage verknüpft und können zugänglich gemacht werden, so können sie für die Registrierung und Autorisierung aller Services genutzt werden. Ähnlich wie es heute durch ein „Login mit Google“ ermöglicht wird, brauchen Anlagen nicht einzeln bei den Services registriert zu werden, sondern können sich direkt mit ihrem DID authentifizieren.

Muss ein Anmeldeprozess einer Anlage nicht ausschließlich für die Authentifizierung in einem Anwendungsfall wie einem Grünstromzertifikate-Register durchgeführt, sondern kann für viele verschiedene Anwendungen genutzt werden, so können die Kosten für den Anmeldeprozess auf die unterschiedlichen Anwendungen aufgeteilt werden, was einen erheblichen Einfluss auf die Profitabilität des Anwendungsfalls haben kann. Ist der Anmeldeprozess weiterhin so gut gestaltet, dass alle relevanten Daten bereits bei der Installation mit dem DID verknüpft werden können, anstatt dass weiter Audits oder Begehungen stattfinden, können insgesamt die Kosten für die Anmeldung stark verringert werden.

Geräteschlüssel

Geräteschlüssel können Vertrauen in den Anmeldeprozess steigern, da die Schlüssel auf der Anlagen-Hardware liegen und damit verknüpft sind. Nur wer direkt Zugriff auf das Gerät hat, kann die Schlüssel nutzen, um Daten zu signieren. Basisdaten, die mithilfe der Geräteschlüssel kryptografisch mit der Geräte-Identität verknüpft und auf der Blockchain verankert sind, können nicht einfach geändert werden. So können Anwendungen sicher sein, dass die Basisdaten, die vorgelegt werden, die sind, die als Teil des allgemein anerkannten Anmeldeprozesses angelegt wurden, oder aber mögliche Änderungen einsehen und nachverfolgen.

Die Nutzung von Geräteschlüsseln erlaubt es, Anlagen eindeutig und sicher zu identifizieren. Jede Anwendung kann dabei sicher sein, dass die Anlage, mit der sie interagiert, wirklich die ist, die kryptografisch mit der Geräte-Identität und den Basisdaten verknüpft wurde. Das vereinfacht den Autorisierungsprozess und sichert ihn ab. Die Anwendung kann so den Zugriff und mögliche Transaktionen nur für die Anlage autorisieren, die den Geräteschlüssel vorlegen kann.

Verankerung der Transaktionen auf der Blockchain

Der Einsatz von Geräteschlüsseln wird mit der Verankerung aller durchgeführten Transaktionen auf der Blockchain zu einem schlüssigen Gesamtkonzept. Die Verankerung der Transaktionen auf einer Blockchain ermöglicht es, dass die Verknüpfung der Basisdaten und mögliche Änderungen effizient nachverfolgt und verifiziert werden können. Akteure können verifizieren, wann die Transaktion von wem durchgeführt wurde, und sicher sein, dass diese Information fälschungssicher gespeichert wurde. Außerdem sind eine automatische Verifizierung der Berechtigungen und ihre digitale Nachverfolgung möglich, um das mehrfache Einsetzen und Anmelden derselben Ressource („Double Spending“) zu vermeiden. Prozesse können einfach digitalisiert und automatisiert werden. Dies führt auch dazu, dass menschliche Fehler reduziert werden.

Dezentrale Speicherung von Credentials

Da die Basisdaten in Form eines Credential dezentral auf der Anlagen-Hardware gespeichert werden, können sie jeder Anwendung unabhängig zur Verfügung gestellt werden. Anstatt dass zum Beispiel das Grünstromzertifikate-Register direkten Zugriff auf das System braucht, in dem die Erstanmeldung stattgefunden hat, kann es die Daten direkt von der Anlage beziehen. Das erleichtert die Kooperation zwischen verschiedenen Anwendungen und verhindert die Zentralisierung und die Einrichtung von Paywalls für den wichtigen Service der Ausstellung der Basisdaten.

Abkürzungsverzeichnis

aEMT	aktiver externer Marktteilnehmer
AEUV	Vertrag über die Arbeitsweise der Europäischen Union
API	Application Programming Interface
BAB	BSI-konformer Adapter für Bestandszähler
BDSG	Bundesdatenschutzgesetz
BMIL	Blockchain Machine Identity Ledger
BMWK	Bundesministerium für Wirtschaft und Klimaschutz (vormals: Bundesministerium für Wirtschaft und Energie, BMWi)
BNetzA	Bundesnetzagentur
BSI	Bundesamt für Sicherheit in der Informationstechnik
BT-Drs.	Bundestagsdrucksache
BVerfG	Bundesverfassungsgericht
BVerfGE	Entscheidung des Bundesverfassungsgerichts
BZ	Basiszähler
CLS	Controllable Local System
CLS-GW	Controllable Local System Gateway
dApp	decentralized Application
DDOS	Distributed Denial of Service
DER	Distributed Energy Resource
DID	Decentralized Identifier
DIF	Decentralized Identity Foundation
DL	Distributed Ledger
DLT	Distributed Ledger Technology
DSGVO	Datenschutz-Grundverordnung
eBS	elektronischer Bestellschein
EDL	Energiedienstleistung
EEG	Erneuerbare-Energien-Gesetz
eHZ	elektronischer Haushaltszähler
eLS	elektronischer Lieferschein
EMT	Externer Marktteilnehmer
EVU	Energieversorgungsunternehmen
EWF	Energy Web Foundation
FNN	Forum Netztechnik / Netzbetrieb
FTP	File Transfer Protocol
GDEW	Gesetz zur Digitalisierung der Energiewende
GUI	Graphical User Interface
GW	Gateway
GWA	Gateway-Administrator
HAN	Home Area Network
HKNR	Herkunftsnachweisregister
HkRNDV	Herkunfts- und Regionalnachweis-Durchführungsverordnung
HKS	Haupt-Kommunikationsszenarien
HSM	Hardware Secure Module
IDP	Identity Provider
IKD	Initiale Konfigurationsdatei
iMSys	intelligentes Messsystem
IoT	Internet of Things
IP	Internet Protocol
JSON	JavaScript Object Notation
KSG	Bundes-Klimaschutzgesetz

KYC	Know Your Customer
LTE	Long Term Evolution
MaStR	Marktstammdatenregister
MSB	Messstellenbetreiber
MsbG	Messstellenbetriebs-Gesetz
P2P	Peer-to-Peer
PKI	Public Key Infrastructure
PV	Photovoltaik
RNG	Random Number Generator
SDK	Software Development Kit
SiLKe	Sichere Lieferkette
SMGW	Smart-Meter-Gateway
SM-PKI	Smart Meter Public Key Infrastructure
SSD	Solid State Drive
SSH	Secure Shell
SSI	Self-Sovereign Identity
SSO	Single Sign-on
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TR	Technische Richtlinie
ÜNB	Übertragungsnetzbetreiber
URL	Uniform Resource Locator
UUID	Universally Unique Identifier
VC	Verifiable Credential
VPN	Virtual Private Network
W3C	World Wide Web Consortium
WAN	Wide Area Network
wMSB	wettbewerblicher Messstellenbetreiber

Anhang

Informationsobjekte der gerätezentrierten Identitätsverwaltung

Die Informationsobjekte werden hier als unverschlüsselte Nachrichten dokumentiert, bei der Kommunikation zwischen den verschiedenen Komponenten werden aber nur verschlüsselte Nachrichten übermittelt. Zur Implementierung der Applikationen und der Prozesse wurde das SDK des KILT Protocol verwendet.[128]

Informations-objekt	Sender	Empfänger	Größe in Bytes	Beispielnachricht	Protokoll	Referenz Sequenz-diagramm
Trigger Key Generation	Device Manufac-turer	Claimer Application	-	-	http - POST	Create Keypair
Request KILT Blockchain address	Device Manufac-turer	Claimer Application	-	-	http - POST	Register DID
Return address	Claimer Application	Device Manufacturer	50	4q53QUDPk5axVnjGS1KUr4z9U9Em63RHWtzsnRP1JvLEvSoe	http - Response	Register DID
Request storing of DID Docu-ment	Claimer Application	Public DID Document Store	1294	{ "id": "did:kilt:4q53QUDPk5axVnjGS1KUr4z9U9Em63RHWtzsnRP1JvLEvSoe", "@context": "https://w3id.org/did/v1", "authentication": [{ "publicKey": ["did:kilt:4q53QUDPk5axVnjGS1KUr4z9U9Em63RHWtzsnRP1JvLEvSoe#key-1"], "type": "Ed25519SignatureAuthentication2018" }], "publicKey": [{ "controller": "did:kilt:4q53QUDPk5axVnjGS1KUr4z9U9Em63RHWtzsnRP1JvLEvSoe", "id": "did:kilt:4q53QUDPk5axVnjGS1KUr4z9U9Em63RHWtzsnRP1JvLEvSoe#key-1", "publicKeyHex": "0x5f50e725fd149e12e0fed26c673e186158e6052ec37083f6c78e-a431c315456b", "type": "Ed25519VerificationKey2018" }, { "controller": "did:kilt:4q53QUDPk5axVnjGS1KUr4z9U9Em63RHWtzsnRP1JvLEvSoe", "id": "did:kilt:4q53QUDPk5axVnjGS1KUr4z9U9Em63RHWtzsnRP1JvLEvSoe#key-2", "publicKeyHex": "0xf93be5fb63b70fa44b1c06ffdeffdb56977814021fa7972af642c-795c444702d", "type": "X25519Salsa20Poly1305Key2018" }], "service": [{ "serviceEndpoint": "https://services.kilt.io/messaging", "type": "KiltMessagingService" }], "signature": "0x00f6d79f49c2ac3629f1f7aacafed4d8f713771203ff418db556ec5df7f2578cf1d9148bb-908c95409b90a8af0c3136a1afd60d39aa92d666d394acfe0eb15400e" },	http - POST	Register DID

128 https://dev.kilt.io/docs/sdk/introduction

Informations-objekt	Sender	Empfänger	Größe in Bytes[118]	Beispielnachricht	Protokoll	Referenz Sequenzdiagramm

Store public keys and link to DID document			627	{
				"id": 42,
				"jsonrpc": "2.0",
				"method": "author_submitAndWatchExtrinsic",
				"params": [
				"0x050484184e59207177d2b777fd1ba01da661e8b5dd5815dceb633ca7dae03c-8041920501c41ace2
				89b8147fd356f0477d62636885295fabd7892746559d60a56b9daf12e1c8bfb31027d-7238f4e6d86aab
				064cba2292c6524082ea15c7774ad37c77b38d6502d0000c00d507eda0658bd-2f1a170143525879c3
				43b0635307ed2d17daf4c07e8b161e637184e59207177d2b777fd1ba01da-661e8b5dd5815dceb633c
				a7dae03c804192050159016874747073 3a2f2f7365727669636 5732e6b-696c742e696f3a3434332f63
				6f6e74616374732f346f54774647444c674b346e55706e5654596b5738724159784347334e6f656468
				637a35594e7a57736f787755334a31"
				]
				}		

Send Terms message	KILT Attestation GUI	Claimer Application	2028 (verschlüsselt)	{
				"createdAt": 1629991825523,
				"hash": "0x9529322dc2f9752019168ef41cc84972ef7a9dfe6e25684cf4377da8c83a8a-de",
				"signature":
				"0x01a44e1f27e1789b67a997cfaa135447d76dd3461fd9c6e586675840a9ebd9e-b0625954e7e278ccc
				0deccb901dd726a3906085969b72b68a47ef486dc1aa3d0782",
				"receiverAddress": "4rBR1RWHs44Juc2MNtvxVmHfgFmKygFa5oiYM41SxeoJF6xW",
				"senderAddress": "4oTwFGDLgK4nUpnVTYkW8rAYxCG3Noedhcz5YNzWsoxwU3J1",
				"senderBoxPublicKey":
				"0xd507eda0658bd2f1a170143525879c343b0635307ed2d17daf4c07e8b161e637",
				"messageId": "e23cc86f-ea65-4856-b961-a1cf6d2bf1b8",
				"receivedAt": 1629991825837,
				"body": {
				"content": {
				"claim": {
				"cTypeHash": "0x7b431dfb20a2344939712d28c384e8198ed08f6f505b5153f6ea64704bae61c9",
				"contents": {
				"owner": "did:kilt:4p1AjpMzcSmJYCzqjx9BreaiZFZ2emy5Br359uatQyC2H5gM",
				"facility_type": "Solar",
				"registration_date": "2021-04-08",
				"deregistration_date": "2100-12-12",
				"zip_code": "10787",
				"city": "Berlin",
				"country": "Germany",
				"latitude": 52497161,
				"longitude": 13.346865,
				"nominal_capacity": 450,
				"grid_connection": "Mittel",
				"name": "oli/youki",
				"device_manufacturer": "",
				"device_model": "",
				"device_serialnumber": "",
				"device_address": "",
				"device_sunspec_did": ""
				}
				},
				"legitimations": [],
				"delegationId": "0xcc890baeffd152e22657d41139af67a105236448fc9bd-777f7432494098d7eea"
				},
				"type": "submit-terms"
				}
				}
					KILT	BMIL Installation Credential-Zertifikat

Send Claim with Request For Attestation	Claimer Application	KILT Attestation GUI	9243 (verschlüsselt)	{
				"createdAt": 1629992085907,
				"hash": "0x78e1e83a99516686f2cd6abbdf3649cc5dcf91a36d2afbade963e-11e67173c9d",
				"signature":
				"0x01387b7c93901d488c652f571592b90ef7af02f925f089b40ef9d6bfa5cf72c5282a-208132d02824a9
				8b37676011ea71ce4d738fa98123be1545b652c4e89afe82",
				"receiverAddress": "4oTwFGDLgK4nUpnVTYkW8rAYxCG3Noedhcz5YNzWsoxwU3J1",
				"senderAddress": "4rBR1RWHs44Juc2MNtvxVmHfgFmKygFa5oiYM41SxeoJF6xW",
				"senderBoxPublicKey":
				"0x8d0fa18587c9381707ca3990fc721524aab677f0e40ad7018aabd1bd49879d7b",
				"messageId": "7feccaae-e52f-4044-a29d-3fdbe3c6ca4a",
				"receivedAt": 1629992086187,
				"body": {
				"content": {
				"requestForAttestation": {
				"claim": {
				"cTypeHash": "0x7b431dfb20a2344939712d28c384e8198ed08f6f505b5153f6ea-64704bae61c9",
				"contents": {
				"owner": "did:kilt:4p1AjpMzcSmJYCzqjx9BreaiZFZ2emy5Br359uatQyC2H5gM",
				"facility_type": "Solar",
				"registration_date": "2021-04-08",
				"deregistration_date": "2100-12-12",
				"zip_code": "10787",
				"city": "Berlin",
				"country": "Germany",
				"latitude": 52497161,
				"longitude": 13.346865,
				"nominal_capacity": 450,
				"grid_connection": "Mittel",
				"name": "oli/youki",
				"device_manufacturer": "Fronius",
				"device_model": "Symo 6.0-3-M",
				"device_serialnumber": "27402251",
				"device_address": "1",
				"device_sunspec_did": "113"
				},		

				"owner": "4rBR1RWHs44Juc2MNtvxVmHfgFmKygFa5oiYM41SxeoJF6xW"
				},
				"claimHashes": [
				"0x059cdecb8a18160c4ceabf2562fa1d9553cd37788044120a61cdd130ddbbb0a5",
				"0x16d31a37d399fee043d203414d9e05b3341a598e46b688cb6455ee5e5457107e",
				"0x1c596bdb71c42abef439dfd28c14ae285708bcf8d260502db04970a5101c878f",
				"0x25a7aaa34153e98e3536e6e35738cb68ba3c08429e07dccdabb743bf5660a551",
				"0x2c87658202e6b047c42c29964756b66699e88b1ee4b824a6fa23fcc4ada1064e",
				"0x3bb384cfcc16b034a20c7040e6fb2f5e4f9a78ce5da471db82239f8503f30576",
				"0x88ddd08830c34a7bba3161cd8b1c1341cb2fa3627d06bb4d064e1b613631aa22",
				"0x96d101e428066ac8b55cdf4eb0c5ec3d74e3ea563d0cb77af82c1a9fc949f57c",
				"0xa1537d7c5da1c9de4d2759d00c49b1c902571ac3ff7a48634c15636b67616ee9",
				"0xa3d7d25fe014bb385e64a2bb0bf84e5b36d55e3fdae586d4e5bf3322be4487fa",
				"0xcf53719b7c05a7fa9bcff6223410797c768b1b0688e796aafcf34f21941b5db1",
				"0xd42eb913710ab9651b6f39fd0d2cc6c4a772695749e400398ab6f887db3ebe03",
				"0xdaa3b346e833d1ee80c3171ba4e40a84f62427f2c68db3a190be5a153ffdeebb",
				"0xdfe4e96a35bd716a16ccfb0953d7a0e081b2a303696d0b3600ea1099b8882430",
				"0xf15823c237f31ff83ecce22c6445d892348453ba7a88bb70a1c040fb26ffd62d",
				"0xf340516570993267c7148da51ae6f32adb021a37bd2832e1c2c9f4bb19605901",
				"0xf5141df3bb39c8bb1420367408ca0acc14f028110a37ac3fe3f37c85ea7fb962",
				"0xf70e64c4e17193f3c647d12488bd3d322b4d090f721bc427690a7b542590a96a"
				],
				"claimNonceMap": {
				"0x7873e03f99858f30efc79940909cf66b1a31616b172fe0b579cbf4b9616b8a58":
				"c22887e6-872f-489a-a35d-513116fa78d2",
				"0x4dc4fbaa40a5c7d6c65d625190c93e8e0be2efd5a5ac9c87ced56cd6ea7b2720":
				"26d40bdc-7db5-4ae8-a46c-5fd484e99d0e",
				"0x237a88b07bcaa3f0d2ee36a710c9a2c905b033d6e43d311917fa1c9d0441e5ab":
				"434fbf22-6d89-4b52-8a14-2cda6f6a9fd3",
				"0x489e3623d51148d3f66cf63843b3789a253472d5714c7c5e114a1671f5687b73":
				"9f90ba73-e2ae-4982-848d-dff5ba0d7f3f",
				"0x7cf33ed9b71b7b614fe67f21d95e8f2cd6f8979d60212d5a1af573442e68c78c":
				"a685975e-3e97-4a20-92c7-77f1cfe6037e",
				"0x8fbc127372279edc1278be50b9ea09f74098c47f07584c63b76d64c8c828011e":
				"7aed8c9c-9980-4117-b007-2e73198d9101",
				"0x4fd35588e848c381fdea1c46268fdc5f2bc8c51553c5062f9768c3a2e7e3608d":
				"01f68293-56f8-4309-9911-69b9d074959b",
				"0x6aacf923590cd1b383097e4fd6d447d527abc873376b5d2fb9c92929b3f75847":
				"7c717568-1530-4326-9866-cf2306837c87",
				"0x34e278162b773d5999019cf55f293878c2b77969ed7efdb9b30a0466816d444a":
				"e67f2cb0-7b70-40ef-ab4b-219555a00322",
				"0x7c7f520d3c5c1e6922ca3ffaa9b047ba6dd92b2121d4b895e0602d897e45d223":
				"7e335bca-6296-482d-9801-0c4a0791d6a2",
				"0x7c294bf43335d6973ce926fccba55db3dbd8c141785d3722845768a498ec64cb":
				"232d879d-c8ba-4b9c-a9a0-5053d18f1fc3",
				"0x12bfe1388b139c6ee7b58f0a0bb11c16b015ec8d24696555be30c655d25f1976":
				"ab44c097-9ee5-44bf-8569-dc254eab3d2a",
				"0x1413868fb014bf5e9eb1f3080b90e86c5b408f24beab1b5060a3cd5a5c81b312":
				"320b65a4-67cb-452c-995e-50abb7974615",
				"0x0e995c12bc481c1a529dbdbbd8099855c02e96e336ed82ad2b58d6aee6998121":
				"c6d6ac98-74db-49fa-8db7-7742c91f2795",
				"0x33eb602ab195a9721c4cae90a54b3fcb635bff548bb8967630692fe28eb32d64":
				"caa9dc92-cec9-488d-befd-86eec5a9d04a",
				"0xdc331e845c7bd4eaa597858b72a1d41e370ab95ab0100fa3b6ac3f00f8182960":
				"aaf014e8-51f3-4821-9b4e-1883f7298a34",
				"0x6a7307516f69d1f29b7b123ed949eb0943e3f6a29a268cab678a74b6f148cdef":
				"c326a9df-a311-421b-990f-87f35f0151ef",
				"0x30d78b5e22fcaf9f43414504744 70fa927070369b515efa510fc7c83942da1a4":
				"e3772d8b-9833-46c2-80cb-650706f51170"
				},
				"legitimations": [],
				"delegationId": "0xcc890baeffd152e22657d41139af67a105236448fc9bd-
				777f7432494098d7eea",
				"rootHash": "0xa29fa92766b3ed0de839b1fb928f6c8e380a25f431fc63efc0e-
				4da53af7337b4",
				"claimerSignature":
				"0x0114f775d3ec225988c9265e23ae7f3fd7ea72e3b926623d5f9ad032f7498e-
				9767117b8ab7907cb5
				b2ab307c7c32bd811e4dc18ad534660fa2847ebe85db58db80"
				}
				},
				"type": "request-attestation-for-claim"
				}}
				}
					KILT	BMIL Installation Credential-Zertifikat

Success Message	KILT Attestati-on GUI	Claimer Application	1483
			(ver-schlüsselt)
				{
				"createdAt": 1629992570210,
				"hash": "0x2f9e14c4ddc22f337d075c9d2cfef2a9462bd16a666739a36b6e20c6340d-
				a1b2",
				"signature":
				"0x016a7980b27786c4c9c9f400e1691ee6418609ae95123f89c797f5699d98e70413a-
				c9e93bd162c51
				70f545a48e7a241ce46e084bb0ca64bfb4052fcfdcbed8e686",
				"receiverAddress": "4rBR1RWHs44Juc2MNtvxVmHfgFmKygFa5oiYM41SxeoJF6xW",
				"senderAddress": "4oTwFGDLgK4nUpnVTYkW8rAYxCG3Noedhcz5YNzWsoxwU3J1",
				"senderBoxPublicKey":
				"0xd507eda0658bd2f1a170143525879c343b0635307ed2d17daf4c07e8b161e637",
				"messageId": "cb73aab3-6153-484e-b7e0-5a18ef75e946",
				"receivedAt": 1629992570470,
				"body": {
				"content": {
				"attestation": {
				"claimHash": "0xa29fa92766b3ed0de839b1fb928f6c8e380a25f431fc63efc0e-
				4da53af7337b4",
				"cTypeHash": "0x7b431dfb20a2344939712d28c384e8198ed08f6f505b5153f6ea-
				64704bae61c9",
				"delegationId": "0xcc890baeffd152e22657d41139af67a105236448fc9bd-
				777f7432494098d7eea",
				"owner": "4oTwFGDLgK4nUpnVTYkW8rAYxCG3Noedhcz5YNzWsoxwU3J1",
				"revoked": false
				}
				},
				"type": "submit-attestation-for-claim"
				}
				}
					KILT	BMIL Installation Credential-Zertifikat

Informations-objekt	Sender	Empfänger	Größe in Bytes[118]	Beispielnachricht	Protokoll	Referenz Sequenzdiagramm

Attestation Data on Blockchain	-	-	-	{
				"claimHash": "0xa29fa92766b3ed0de839b1fb928f6c8e380a25f431fc63efc0e-4da53af7337b4",
				"cTypeHash": "0x7b431dfb20a2344939712d28c384e8198ed08f6f505b5153f6ea-64704bae61c9",
				"delegationId": "0xcc890baeffd152e22657d41139af67a105236448fc9bd-777f7432494098d7eea",
				"owner": "4oTwFGDLgK4nUpnVTYkW8rAYxCG3Noedhcz5YNzWsoxwU3J1",
				"revoked": false
				}
					KILT	

Create Delegation Root	KILT Attestation GUI (Root Delegator)	KILT Blockchain	-	pub fn create_hierarchy(origin: OriginFor<T>, root_node_id: DelegationNodeIdOf<T>, ctype_hash: CtypeHashOf<T>) -> DispatchResult	JSON-RPC call / documentation of function declaration in code	-

Invite Delegate	KILT Attestation GUI (Root Delegator)	KILT Attestation GUI (Delegate)	1268	{
				"createdAt": 1630063753806,
				"hash": "0x615d42af44744cc335874fd245378a73ef39bb58845fc139bf32f-533de33d837",
				"signature":
				"0x0156e79a853bd15737ae9f16a112fdd5038838e92cf3bcddb68e96c256ac0d-b41a658762680d7c61
				e3b99de9e1f242244c9377ce3260c34ee43aed2b265f2a1480",
				"receiverAddress": "4oTwFGDLgK4nUpnVTYkW8rAYxCG3Noedhcz5YNzWsoxwU3J1",
				"senderAddress": "4pZRhNcdBSVjCDQbarnpuNPusvLkXf6364BUDG82rXhzFMMr",
				"senderBoxPublicKey":
				"0x2bdbfcc8be81ce1d96a49da04aba8973184efec33b514a7c3a7c2e2f7b284e64",
				"messageId": "220dceeb-071b-4e02-82f6-db63774fcfdb",
				"receivedAt": 1630063753921,
				"body": {
				"content": {
				"delegationData": {
				"account": "4oTwFGDLgK4nUpnVTYkW8rAYxCG3Noedhcz5YNzWsoxwU3J1",
				"id": "0xf1d59f691e3b5f640ac82b406adb7bba313e4adec07bf17ca1625128f-8d553e6",
				"isPCR": false,
				"parentId": "0x0e644d8488852f1274a17b460ed1180d6d9f51b80d2933b63a-602ba7ee198b8f",
				"permissions": [
				1
				]
				},
				"metaData": {
				"alias": "root delegation"
				},
				"signatures": {
				"inviter":
				"0x0148282d0e2dfc336cf2d2169da0e1ff8e5ac546ecb55cec6d87c07af42e267304d-74393ba7c4cef0
				72999ae829978027385b5d382b3e88ad73ca4e177b3098e8e"
				}
				},
				"type": "request-accept-delegation"
				}
				}
					KILT Messaging over https	

Accept invitation	KILT Attestation GUI (Delegate)	KILT Attestation GUI (Root Delegator)	1358	{
				"createdAt": 1630063897988,
				"hash": "0x4ef7bf5919945f1a6060ddfcad827af48126bf14a13aa7e51ab-8922de1519d25",
				"signature":
				"0x0140dc4c4fe642aef76e10a769d40ceef26bf8c8c8d52009d1511f97958ab9f35b-cf75ddfbe1c055ed
				a3abbccebd922729a5dc012c23937096fd5e700a0719e38e",
				"receiverAddress": "4pZRhNcdBSVjCDQbarnpuNPusvLkXf6364BUDG82rXhzFMMr",
				"senderAddress": "4oTwFGDLgK4nUpnVTYkW8rAYxCG3Noedhcz5YNzWsoxwU3J1",
				"senderBoxPublicKey":
				"0xd507eda0658bd2f1a170143525879c343b0635307ed2d17daf4c07e8b161e637",
				"messageId": "723ba7bf-009f-4090-b5a8-740dc938ff81",
				"receivedAt": 1630063898147,
				"body": {
				"content": {
				"delegationData": {
				"account": "4oTwFGDLgK4nUpnVTYkW8rAYxCG3Noedhcz5YNzWsoxwU3J1",
				"id": "0xf1d59f691e3b5f640ac82b406adb7bba313e4adec07bf17ca1625128f-8d553e6",
				"isPCR": false,
				"parentId": "0x0e644d8488852f1274a17b460ed1180d6d9f51b80d2933b63a-602ba7ee198b8f",
				"permissions": [
				1
				]
				},
				"signatures": {
				"inviter":
				"0x0148282d0e2dfc336cf2d2169da0e1ff8e5ac546ecb55cec6d87c07af42e267304d-74393ba7c4cef0
				72999ae829978027385b5d382b3e88ad73ca4e177b3098e8e",
				"invitee":
				"0x019c6c0f8423d80501c0d0df44309fe8094f46128e7c371a387e917b-c18c534519085cd56914f2e67
				990117d26ed00d21eebe2f1f45b3274ab352fece844eac88f"
				}
				},
				"type": "submit-accept-delegation"
				}
				}
					KILT Messaging over https	

Informations-objekt	Sender	Empfänger	Größe in Bytes[118]	Beispielnachricht	Protokoll	Referenz Sequenzdiagramm
Add Delegation	KILT Attestation GUI (Root Delegator)	KILT Blockchain	-	pub fn add_delegation(origin: OriginFor<T>, delegation_id: DelegationNodeIdOf<T>, parent_id: DelegationNodeIdOf<T>, delegate: DelegatorIdOf<T>, permissions: Permissions, delegate_signature: DelegateSignatureTypeOf<T>,) -> DispatchResult	JSON-RPC call / documentation of function declaration in code	

Inform about created delegation	KILT Attestation GUI (Delegate)	KILT Attestation GUI (Root Delegator)	782	{
				"CREATEDAT": 1630064080244,
				"HASH": "0XF6406EF53C1511B02B9C0B558B2A16EE5C-7C23DDCAA3D3044B8B0EE78DCF538E",
				"SIGNATURE":
				"0X0188EF6CF7FBB311A252499EA74819F7859793C13BDD1DA392838CB971BB5F2F-4D948680998C1F533
				EC05BCA42A2169D90D6EE7DDFF892A6E15FF895EE246FB089",
				"RECEIVERADDRESS": "4OTWFGDLGK4NUPNVTYKW8RAYXCG3NOEDHCZ5YNZWSOX-WU3J1",
				"SENDERADDRESS": "4PZRHNCDBSVJCDQBARNPUNPUSVLKXF6364BUDG82RX-HZFMMR",
				"SENDERBOXPUBLICKEY":
				"0X2BDBFCC8BE81CE1D96A49DA04ABA8973184EFEC33B514A7C3A7C2E2F-7B284E64",
				"MESSAGEID": "31FCDFF7-66B2-4AD3-BBF7-01B8822FDCA7",
				"RECEIVEDAT": 1630064080309,
				"BODY": {
				"CONTENT": {
				"DELEGATIONID": "0XF1D59F691E3B5F640AC82B406ADB7BBA313E4ADEC07BF-17CA1625128F8D553E6",
				"ISPCR": FALSE
				},
				"TYPE": "INFORM-CREATE-DELEGATION"
				}
				}
					KILT Messaging over https	

Revoke attestation	Attestation GUI („Zertifikatsaussteller“)	KILT Blockchain	-	pub fn revoke(origin: OriginFor<T>, claim_hash: ClaimHashOf<T>, max_parent_checks: u32,) -> DispatchResultWithPostInfo JSON	JSON-RPC call / documentation of function declaration in code	

Attestation Data on Blockchain (Invalidiert)	-	-	-	{
				"claimHash": "0xa29fa92766b3ed0de839b1fb928f6c8e380a25f431fc63efc0e-4da53af7337b4",
				"cTypeHash": "0x7b431dfb20a2344939712d28c384e8198ed08f6f505b5153f6ea-64704bae61c9",
				"delegationId": "0xcc890baeffd152e22657d41139af67a105236448fc9bd-777f7432494098d7eea",
				"owner": "4oTwFGDLgK4nUpnVTYkW8rAYxCG3Noedhcz5YNzWsoxwU3J1",
				"revoked": true
				}
					The example just shows the data stored on-chain	

Ask Claimer for Credential	KILT Verifier GUI	Claimer Application	969 (verschlüsselt)	{
				"createdAt": 1630066263056,
				"hash": "0xf84cd18c7a2b00e4ac8c028aeb88ed80324823f17eb711b518a2f6ada-febee90",
				"signature":
				"0x01eed7a785f7c2b1bfce2488f6d512876d2776f69411623204be27f3a1d-48b9664a9248189e87c91
				bc5d03e7f8a4c44e22ddad6f43b39155cdbdeb6aeb264f5d88",
				"receiverAddress": "4rBR1RWHs44Juc2MNtvxVmHfgFmKygFa5oiYM41SxeoJF6xW",
				"senderAddress": "4rQ2vmWQsxcKwxjzLcPqke593vNiJ6p6sc6zdUus6PTTVLU6",
				"senderBoxPublicKey":
				"0x46509eb19cf63464ac84e0d4652ff61a28f51936f8e33bd0ab0bb73851c3515d",
				"messageId": "1b2523c4-1390-4b3d-b6d4-ef08d371ec87",
				"receivedAt": 1630066263177,
				"body": {
				"content": [
				{
				"cTypeHash": "0x7b431dfb20a2344939712d28c384e8198ed08f6f505b5153f6ea-64704bae61c9"
				}
				],
				"type": "request-claims-for-ctypes"
				}
				}
					KILT Messaging over https	

Informations-objekt	**Sender**	**Empfänger**	**Größe in Bytes[118]**	**Beispielnachricht**	**Protokoll**	**Referenz Sequenzdiagramm**

Send Credential (with subset of attributes)	Claimer Application	KILT Verifier GUI	7483 (verschlüsselt)	{
				"createdAt": 1630066477294,
				"hash": "0x8eb5b598c12bf505ef9b2f8e7bb8a032a791d2a086e256fba274ef-b3d55e7e78",
				"signature":
				"0x0148619b7a2f8f1c1275de85f8cab7035d406a88a7c02c03ec08cffb-15b6a783249a0dfe4b7730d01
				86a2dffeaa73c3c59b92cb7df952ab3128e891eef22d88681",
				"receiverAddress": "4rQ2vmWQsxcKwxjzLcPqke593vNiJ6p6sc6zdUus6PTTVLU6",
				"senderAddress": "4rBR1RWHs44Juc2MNtvxVmHfgFmKygFa5oiYM41SxeoJF6xW",
				"senderBoxPublicKey":
				"0x8d0fa18587c9381707ca3990fc721524aab677f0e40ad7018aabd1bd49879d7b",
				"messageId": "7e498d85-ab3b-4adb-b35e-c48c532a14db",
				"receivedAt": 1630066477502,
				"body": {
				"content": [
				{
				"request": {
				"claim": {
				"cTypeHash": "0x7b431dfb20a2344939712d28c384e8198ed08f6f505b5153f6ea-64704bae61c9",
				"contents": {
				"registration_date": "2021-04-08",
				"deregistration_date": "2100-12-12",
				"nominal_capacity": 450,
				"device_manufacturer": "Fronius",
				"device_model": "Symo 6.0-3-M",
				"device_serialnumber": "27402251",
				"device_address": "1",
				"device_sunspec_did": "113"
				},
				"owner": "4rBR1RWHs44Juc2MNtvxVmHfgFmKygFa5oiYM41SxeoJF6xW"
				},
				"claimHashes": [
				"0x1ac4f77ca15f50047d615fa7d37a25cd781638f987e3f927a970c8b2c9910ebb",
				"0x28d4874e45ba35819d78f2c4d0e9a016cde68dabac91e06a357617de39b4b403",
				"0x2e6e0e31f251f7e8672782acd7b3ad4a965f16758f781513cbf3673a457ee7ee",
				"0x30e83066cb79415a845c67cca08881b23b374f3fb5e094d5cff4f37ee9a59ee6",
				"0x42bcd078039068d00c5783403d511a6701bbb92a057ee1e926a30698ecaeef59",
				"0x4e2210dbe5431d45b65053b0cd2f3084e7322baa3568cf14ddf5da3a9a1fc592",
				"0x650e06078ea39275b5528566b77d9b84177d8b126d517547cf32d9bd5e5b945d",
				"0x7edb425dbeaf5e7c1ca1a324d9009d8a274481043f00e48ec6399d97c129740f",
				"0x8874bfe252594c0092bcfd1dd0bd942477bfbb13de4ee4aaf012e410bf68030a",
				"0x8d9531bd7fbcccc5f0074981bfa7b3ed52ac1550070808757bc7e4f5d7b936b3",
				"0xab9007f795908fa9f1dabb8f03e65409c0ce88e18ee22dcc27ea92f2a111c8ce",
				"0xc4f16e1f75b097a66e0a06a5b359524459b4d22cee81350a56f67f9874d9c90b",
				"0xcd53e2488bcdf4ba2605604e23b1cf5fb85c27abed6885d5434bc527bde16aeb",
				"0xe1ec5f4316fb40982691d8a5759e4d304851000e135fc52172b20006076474c3",
				"0xe39147209137e219a457e0c9308416d6a2a8e5cb80132699eb1187b3bf66d6d3",
				"0xe4fbacf6d2764b988748e321d084a1c706464576d3217678 4f28a479aa11dfde",
				"0xf952889140b60e400d094be4fe2399321224ace96531bcfaebc5646bf13ca89b",
				"0xfe2e94962e1ed6973cd7235bcb6e305125d3dc440bfaa773b624dabc7b7a9553"
				],
				"claimNonceMap": {
				"0x7873e03f99858f30efc79940909cf66b1a31616b172fe0b579cbf4b9616b8a58":
				"2e137f12-8068-4c3e-903f-11bf9fe7bec0",
				"0x489e3623d51148d3f66cf63843b3789a253472d5714c7c5e114a1671f5687b73":
				"cf07ca4d-7646-454d-9ccc-4bbca0e6d737",
				"0x7cf33ed9b71b7b614fe67f21d95e8f2cd6f8979d60212d5a1af573442e68c78c":
				"11c9dbbe-5fd2-4e00-9813-31775ad48794",
				"0x7c294bf43335d6973ce926fccba55db3dbd8c141785d3722845768a498ec64cb":
				"5bb611de-a75d-4055-94a7-3183925e5c58",
				"0x0e995c12bc481c1a529dbdbbd8099855c02e96e336ed82ad2b58d6aee6998121":
				"e598a1a8-efe5-4706-9f79-6bff6d50ccac",
				"0x33eb602ab195a9721c4cae90a54b3fcb635bff548bb8967630692fe28eb32d64":
				"fa2a8b70-c841-49dc-99a9-224e02a107ce",
				"0xdc331e845c7bd4eaa597858b72a1d41e370ab95ab0100fa3b6ac3f00f8182960":
				"6b32c9c0-54b5-49ae-80db-ef0f4b629cfe",
				"0x6a7307516f69d1f29b7b123ed949eb0943e3f6a29a268cab678a74b6f148cdef":
				"c85e8ac7-f735-4728-9e16-9e6db6ca0358",
				"0x30d78b5e22fcaf9f43414504747 0fa927070369b515efa510fc7c83942da1a4":
				"6ee1415e-73e7-be81e86f958c24b5cb39fb14a22716ad61efd1fadd359dd080"
				},
				"attestation": {
				"claimHash": "0x91b595f0ff18ac6ba564a61135f4f0d30f09a15d4802f2ac46317e-8a93c467b3",
				"cTypeHash": "0x7b431dfb20a2344939712d28c384e8198ed08f6f505b5153f6ea-64704bae61c9",
				"delegationId": "0x7970b3ba3a0431f46dd4e06b39b13be101e741285b2d65d4b1a 4e9236527800e",
				"owner": "4oTwFGDLgK4nUpnVTYkW8rAYxCG3Noedhcz5YNzWsoxwU3J1",
				"revoked": false
				}
				}
				],
				"type": "submit-claims-for-ctypes-classic"
				}
				}
					KILT Messaging over https	

Tabelle 3: Informationsobjekte der KILT-basierten Anbindungsvarianten

Informationsobjekte der Cloud-Wallet-basierten Identitätsverwaltung

Im Folgenden werden die relevanten Informationsobjekte der Cloud-Edge-Lösung detaillierter betrachtet. Relevante Informationsobjekte im Datenflussdiagramm #1 „dena Machine Identity Ledger – Aufsetzen der Cloud-Identität und Verankerung auf dem Machine Identity Ledger" (siehe Abbildung 39) sind:

- Das **DID-Dokument**, das die Machine Identity definiert und auf dem Blockchain Machine Identity Ledger verankert wird
- Das Verifiable Credential über die **OLI Box Masterdata** (OLI Box Gerätestammdaten)

Relevante Informationsobjekte im Datenflussdiagramm #2 „dena Machine Identity Ledger – Verifizierbare Installation" (siehe Abbildung 40) sind:

- Die **Commissioning Notification Message**. Diese Nachricht wird durch den Installer durch ein Skript angestoßen. Die Daten werden von der OLI Box (unter anderem auch über die Anlage) generiert. Sie sind als sicher anzusehen, da sie durch die BSI-zertifizierte Umgebung des SMGW geleitet werden und zusätzlich von der OLI Box signiert sind.
- Das **Inbetriebnahme** (Commissioning) Verifiable Credential wird ausgestellt durch den Cloud Agent der OLI Box. Dieses Credential enthält Informationen, die in Schritt 1 von der OLI Box automatisch unter anderem auch über die Anlage ausgelesen werden konnten.
- Das **Installation Verifiable Credential** wird ausgestellt durch den Installateur. Er fügt Details der Installation hinzu, zum Beispiel Tag und Ort der Installation.

Die folgende Tabelle beinhaltet die relevanten Gerätestammdaten der OLI Box aus dem **OLI Box Masterdata VC.** Das OLI Box Masterdata VC enthält technische Daten über die OLI Box (nicht die Anlage oder die Installation).

master_data.json (erstellt in der Fabrik des Manufacturer der OLI Box)

Name	Beispiel
timestamp	02-03-2021 07:56
oliboxSerialNr	71
oliboxDID	did:ethr:spherity:testnet:0x039b76d8d80b68716 3d4565bab8511748543ef3a8f2511f9a8e0287ef0 3810e6ba
oliboxMacAddress	B8:27:EB:86:AF:4D
manufacturingDate	01-03-2021

Tabelle 4: OLI Box Masterdata VC

```
{ "@context": [
    "https://www.w3.org/2018/credentials/v1",
"https://spherity.github.io/oci/contexts/credentials/v1-extensions", "https://w3c-ccg.github.io/ldsjws2020/
contexts/lds-jws2020-v1.json"
    ],
    "type": [
        "VerifiableCredential"],
    "issuer": {
    "type": "Issuer",
    "Id": "did:ethr:spherity:testnet:
0x03000cb6a437d391aab1efd6f5238d0d959da1c2b6ec9438dac8dc922b57386a92",
        "name": "Manufacturer"},
    "credentialSubject": {
        "id": "did:ethr:spherity:testnet:
0x039b76d8d80b687163d4565bab8511748543ef3a8f2511f9a8e0287ef03810e6ba",
        "manufacturingDate": "01-03-2021",
        "oliboxDID": "did:ethr:spherity:testnet:
0x039b76d8d80b687163d4565bab8511748543ef3a8f2511f9a8e0287ef03810e6ba",
        "oliboxMacAddress": "B8:27:EB:86:AF:4D",
        "oliboxSerialNr": "71" },
    "issuanceDate": "2021-08-27T13:27:08.083Z",
    "id": "did:ethr:spherity:testnet: 0xf19559c95ddff28dc432c2d17fafdc6dba797ee4",
    "proof": {
        "type": "JsonWebSignature2020",
        "created": "2021-08-27T13:27:08.551Z",
        "jws":
"eyJhbGciOiJFUzI1NksiLCJiNjQiOmZhbHNlLCJjcml0IjpbImI2NCJdfQ..E_Sul6LdQTUh9iTmZveEBCjlMKiV
4ONOAhtKVye29bwYQhujS_hXAbDCtc2jR0FUip3Wy6_BLdKcbP-70vOTWg",
        "proofPurpose": "assertionMethod",
        "verificationMethod":
"did:ethr:spherity:testnet:0x03000cb6a437d391aab1efd6f5238d0d959da1c2b6ec9438dac8dc922b5
7386a92#controllerKey"
    }
}
```

Die folgende Tabelle beinhaltet die relevanten Inbetriebnahmedaten der OLI Box aus dem Commissioning VC. Das **Commissioning VC** enthält technische Daten über die OLI Box und Daten, die die OLI Box von der Anlage (hier: „device“) automatisch auslesen konnte bzw. die die Anlage selbst über sich kennt.
commissioning.json (wird über SMGW in Stage #2 versendet)

Name	Beispiel
timestamp	05-03-2021 10:34
additionalData	z. B. Zählerstand, Softwareversion etc.
deviceMacAddress	22:7A:4E:08:3A:66
deviceSerialNr	27402251
installationSuccessfull	True
oliboxDID	did:ethr:spherity:testnet:0x039b76d8d80b68716 3d4565bab8511748543ef3a8f2511f9a8e0287ef0 3810e6ba
oliBoxSerialNr	71
oliboxSig	0x5d7c12059b8c1295100cc2d42a8a5775c0f61faf 4cb20b91e4a59af46893ec835446d9ebcc3d104ae b937d9de2f3718039d0b19c917a5a6a02ce0a600f af80851b

Tabelle 5: Commissioning VC

```
{
    "@context": [
        "https://www.w3.org/2018/credentials/v1",
 "https://spherity.github.io/oci/contexts/credentials/v1-extensions",
"https://w3cccg.github.io/lds-jws2020/contexts/lds-jws2020-v1.json"
    ],
    "type": [
        "VerifiableCredential"
    ],
    "issuer": {
        "type": "Issuer", "id":
"did:ethr:spherity:testnet:0x02a533b5893fbe6d25d7da976b1c3f9ebe74d029db24e00923feb48476f
4f8c420",
        "name": "Installer"
    },
    "credentialSubject": {
        "id":
"did:ethr:spherity:testnet:0x039b76d8d80b687163d4565bab8511748543ef3a8f2511f9a8e0287ef03
810e6ba",
        "additionalData": "-",
        "deviceMacAddr": "22:7A:4E:08:3A:66",
        "deviceSerialNr": "27402251",
        "installationSuccessfull": "true",
        "oliboxDID": "0x1d64382b142D02e2840841c55Cb2850163239C34",
        "oliboxSerialNr": "71",
            "oliboxSig":
"0x5d7c12059b8c1295100cc2d42a8a5775c0f61faf4cb20b91e4a59af46893ec835446d9ebcc3d104ae
b937d9de2f3718039d0b19c917a5a6a02ce0a600faf80851b"
    },
    "issuanceDate": "2021-08-30T14:46:19.647Z",
    "id": "did:ethr:spherity:testnet:0xb0751f5e5d9d4e598102837f05b61e5d28a9f1ed",
    "proof": {
        "type": "JsonWebSignature2020",
        "created": "2021-08-30T14:46:21.118Z",
        "jws":
"eyJhbGciOiJFUzI1NksiLCJiNjQiOmZhbHNlLCJjcml0IjpbImI2NCJdfQ..xOYBhIlhwIt3bie_kzNHWVSU9b3
dydPMRA7VWij9bjNQ6oNwZC6cfAWOAZSvfilh51Iu0U81o7prJ8Pff4Auzw",
        "proofPurpose": "assertionMethod",
        "verificationMethod":
"did:ethr:spherity:testnet:0x02a533b5893fbe6d25d7da976b1c3f9ebe74d029db24e00923feb48476f
4f8c420#controllerKey"
    }
}
```

Die folgende Tabelle beinhaltet die relevanten Installationsdaten der OLI Box aus dem **Installation VC**, die weder die Anlage noch die OLI Box über sich selbst kennen und die vom Installateur über die Anlage (inklusive OLI Box) ausgesagt werden. Das Installation VC wird vom Installer Cloud Agent signiert.
Installer_data.json

Name	Beispiel
Installer ID by BNetzA	05-03-2021 10:48
Installer ID by BNetzA	Installer:123456
installationLocation	Albert-Einstein-Allee 55, 89081 Ulm
installationDate	05-03-2021
installationSuccessfull	True
meteringPointOperatorAddr	Street 123 / DID

Tabelle 6: Installer VC

```
{ "@context": [
        "https://www.w3.org/2018/credentials/v1",
"https://spherity.github.io/oci/contexts/credentials/v1-extensions",
"https://w3c-ccg.github.io/lds-jws2020/contexts/lds-jws2020-v1.json"],
    "type": ["VerifiableCredential"],
    "issuer": {
        "type": "Issuer",
        "id":
"did:ethr:spherity:testnet:0x02a533b5893fbe6d25d7da976b1c3f9ebe74d029db24e00923feb48476f
4f8c420",
        "name": "Installer"},
    "credentialSubject": {
        "id":
"did:ethr:spherity:testnet:0x039b76d8d80b687163d4565bab8511748543ef3a8f2511f9a8e0287ef03
810e6ba",
        "Installer ID by BNetzA": "Installer:123456",
        "installationDate": "05-03-2021",
        "installationLocation": "Albert-Einstein-Allee 55, 89081 Ulm",
        "installation Successful": "True",
        "meteringPointOperatorAddr": "Street 123" },
    "issuanceDate": "2021-08-27T13:40:10.099Z",
    "id": "did:ethr:spherity:testnet:0x5929ee6cc12d512c2a865431469fd14477285b41",
    "proof": {
        "type": "JsonWebSignature2020",
        "created": "2021-08-27T13:40:11.439Z",
        "jws":
"eyJhbGciOiJFUzI1NksiLCJiNjQiOmZhbHNlLCJjcml0IjpbImI2NCJdfQ..a8OB1pCGODKxErrrtULCPPZIf9yu
r9lpPQJGeoCxtppRD2dx4sLMbEd_DDI-dO6GuJ_I7cp2Tb9Igm2PileaXA",
        "proofPurpose": "assertionMethod",
        "verificationMethod":
"did:ethr:spherity:testnet:0x02a533b5893fbe6d25d7da976b1c3f9ebe74d029db24e00923feb48476f
4f8c420#controllerKey"
    }
}
```

Quellenverzeichnis

1 Vgl. dena (2022): Energy Communities: Beschleuniger der dezentralen Energiewende: https://future-energy-lab.de/fileadmin/dena/Publikationen/PDFs/2022/dena-ANALYSE_Energy_Communities_Beschleuniger_der_dezentralen_Energiewende.pdf

2 Vgl. dena (2022): Die Datenökonomie in der Energiewirtschaft: https://www.dena.de/fileadmin/dena/Publikationen/PDFs/2022/ANALYSE_Die_Datenoekonomie_in_der_Energiewirtschaft.pdf

3 Strüker, Jens et al. (2019): Technisches und Ökonomisches Gutachten im Rahmen der Multi-Stakeholder-Studie „Blockchain in der integrierten Energiewende“ der Deutschen Energie-Agentur, S. 86–155, https://www.dena.de/newsroom/publikationsdetailansicht/pub/blockchain-in-der-integrierten-energiewende/

4 https://www.bmwi.de/Redaktion/DE/Downloads/Studien/blockchain-smart-meter-gateway-kurzfassung.html

5 Siehe auch Sedlmeir et al. (2021): Digital identities and verifiable credentials, Business & Information Systems Engineering 63, S. 603-613

6 Vgl. Blockchain-Protokolle wie Mina: https://minaprotocol.com

7 Vgl. Überblick in Bogensperger et al. (2021): Welche Zukunft hat die Blockchain-Technologie in der Energiewirtschaft, Diskussionspapier, https://stiftung-umweltenergierecht.de/wp-content/uploads/2021/07/InDEED_Diskussionspapier-Blockchain-Energiewirtschaft_2021-07-22.pdf

8 Siehe dazu auch Sedlmeir et al. (2022): The transparency challenge of blockchain in organizations, Electronic Markets, https://doi.org/10.1007/s12525-022-00536-0

9 Siehe auch Schellinger et al. (2022): Mythbusting Self-Sovereign Identity (SSI) - Diskussionspapier zu selbstbestimmten digitalen Identitäten, https://www.fim-rc.de/wp-content/uploads/2022/06/Whitepaper_SSI_Mythbusting_German_version_compressed.pdf

10 Siehe auch Sedlmeir et al. (2021): Digital identities and verifiable credentials, Business & Information Systems Engineering 63, S. 603-613

11 Vgl. GAIA-X: https://www.data-infrastructure.eu/GAIAX/Navigation/EN/Home/home.html; Id-Ideal: https://id-ideal.de/ sowie IDunion: https://idunion.org/

12 Greenpeace, Internationale Klimakonferenzen, abrufbar unter: https://www.greenpeace.de/themen/klimakrise/klimaschutz/internationaleklimakonferenzen?BannerID=0818018015001047&gclid=EAIaIQobChMItpmjl_LD8QIVkc53Ch2mnwGpEAAYASAAEgKiUvD_BwE

13 Vgl. Übereinkommen von Paris, Art. 2 Abs. 1

14 BVerfG, Beschluss vom 24.03.2021 – 1 BvR 2656/18

15 Morgenstern: EWeRK Online-Fachseminar – Das neue Klimaschutzgesetz – Auswirkungen auf die Energiewirtschaft, Vortrag: Das neue Klimaschutzgesetz im Überblick, 30. Juni 2021

16 Bisher sollte das Ziel der Klimaneutralität erst 2050 erreicht werden.

17 Vgl. 1) Ernst & Young GmbH (2013): Kosten-Nutzen-Analyse für einen flächendeckenden Einsatz intelligenter Zähler, Endbericht zur Studie im Auftrag des BMWi ; 2) dena (2014): dena-Smart-Meter-Studie: Einführung von Smart Meter in Deutschland. Analyse von Rolloutszenarien und ihrer regulatorischen Implikationen; 3) Jens Strüker et al.: Dekarbonisierung durch Digitalisierung: Thesen zur Transformation der Energiewirtschaft, https://doi.org/10.15495/EPub_UBT_00005596

18 Ernst & Young GmbH (2018): Barometer Digitalisierung der Energiewende, Berichtsjahr, Studie erstellt im Auftrag des BMWi

19 Ernst & Young GmbH (2013): Kosten-Nutzen-Analyse für einen flächendeckenden Einsatz intelligenter Zähler, Endbericht zur Studie im Auftrag des BMWi

20 dena (2014): dena-Smart-Meter-Studie: Einführung von Smart Meter in Deutschland. Analyse von Rolloutszenarien und ihrer regulatorischen Implikationen

21 Strüker, J., Weibelzahl, M., Körner, M.-F., Kießling, A., Franke-Sluijk, A., Hermann, M. (2021): Dekarbonisierung durch Digitalisierung – Thesen zur Transformation der Energiewirtschaft. Hrsg.: Universität Bayreuth, Projektgruppe Wirtschaftsinformatik des Fraunhofer-Instituts für Angewandte Informationstechnik FIT und TenneT, Bayreuth, abrufbar unter: https://doi.org/10.15495/EPub_UBT_00005596

22 Lockl et al. (2020): Toward Trust in Internet of Things (IoT) Ecosystems: Design Principles for Blockchain-Based IoT Applications. In: IEEE Transactions on Engineering Management, Vol. 67, No. 4, p. 1256–1270

23 Guggenberger, T., Schlatt, V., Schmid, J., Urbach, N. (2021): A structured overview of attacks on blockchain systems. In: PACIS 2021 Proceedings. AIS, Dubai. URL = https://eref.uni-bayreuth.de/66899/

24 https://www.bmwi.de/Redaktion/DE/Pressemitteilungen/2021/03/20210401-startschuss-digitaler-personalausweis.html

25 Vgl. Bitkom (2020); Grech et al. (2021); COVID-19 Credentials Initiative (2021); IATA (2021)

26 Vgl. Bitkom (2020)
27 Wang & De Fillipi (2020)
28 Bogensperger, A., Zeiselmair, A., Hinterstocker, M., Dossow, P., Hilpert, J., Wimmer, M., ... & Völter, F. (2021): Welche Zukunft hat die Blockchain-Technologie in der Energiewirtschaft? (No. 68), Bayreuther Arbeitspapiere zur Wirtschaftsinformatik
29 dena (2018): Multi-Stakeholder Studie – Blockchain in der integrierten Energiewende
30 PwC/BDEW (2019): Blockchain Radar
31 Blockchain-Strategie der Bundesregierung, S. 8, https://www.bmwi.de/Redaktion/DE/Publikationen/Digitale-Welt/blockchain-strategie.pdf?__blob=publicationFile&v=8
32 Sedlmeir, J., Buhl, H.U., Fridgen, G., Keller, R. (2020): The energy consumption of blockchain technology: beyond myth. In: Business & Information Systems Engineering, 62(6), pp. 599–608
33 Vgl. EY: Blockchain-basierte Erfassung und Steuerung von Energieanlagen mithilfe des Smart-Meter-Gateways: Machbarkeitsstudie und Pilotkonzept, Studie im Auftrag des BMWI, Stand: 18.12.2019, S. 31 ff.;
dena: Multi-Stakeholder-Studie – Blockchain in der integrierten Energiewende, Stand 02/2019, S. 156 ff.
34 Schellinger, B., Völter, F., Urbach, N., Sedlmeir, J. (2022): Yes, I Do: Marrying Blockchain Applications with GDPR. 55th Hawaii International Conference on System Sciences
35 dena (2018): Multi-Stakeholder Studie – Blockchain in der integrierten Energiewende
36 Strüker, J., Utz, M., Sedlmeir, J.: Einsatz der Blockchain-Technologie für Smart Grid Dienstleistungen durch E-PKW im Reallabor „EnStadt:Pfaff“
37 Christopher Allen (2016): The Path to Self-Sovereign Identity, http://www.lifewit-halacrity.com/2016/04/the-path-to-selfsoverereign-identity.html
38 Smethurst, R., Rieger, A., Fridgen, G. (2021): Digital Identities and Verifiable Credentials. In: Business & Information Systems Engineering
39 https://www.w3.org/TR/vc-data-model/
40 https://www.w3.org/TR/did-core/
41 https://www.w3.org/TR/did-core/
42 https://www.w3.org/TR/vc-data-model/
43 https://www.data-infrastructure.eu/GAIAX/Navigation/EN/Home/home.html
44 https://identity.foundation/
45 https://www.w3.org/TR/vc-data-model/
46 Fraunhofer-Institut für angewandte Informationstechnik FIT, Projektgruppe Wirtschaftsinformatik: Whitepaper Self-Sovereign Identity – Grundlagen, Anwendungen und Potenziale portabler digitaler Identitäten
47 Preukaschat, A., Reed, D. (2021): Self-Sovereign Identity: Decentralized Digital Identity and Veridiable Credentials
48 Preukaschat, A., Reed, D. (2021): Self-Sovereign Identity: Decentralized Digital Identity and Veridiable Credentials
49 Fraunhofer-Institut für angewandte Informationstechnik FIT, Projektgruppe Wirtschaftsinformatik: Whitepaper Self-Sovereign Identity – Grundlagen, Anwendungen und Potenziale portabler digitaler Identitäten
50 https://www.w3.org/TR/did-spec-registries/
51 Barbereau, T., Weigl, L., Rieger, A., Fridgen, G. (2022): The Social Construction of Self-Sovereign Identity: An Extended Model of Interpretive Flexibility. 55th Hawaii International Conference on System Sciences
52 EY: Blockchain-basierte Erfassung und Steuerung von Energieanlagen mithilfe des Smart-Meter-Gateways: Machbarkeitsstudie und Pilotkonzept, Studie im Auftrag des BMWi, Stand: 18.12.2019
53 Elia (2021); Energy Web Foundation (2020)
54 Elia (2021); Energy Web Foundation (2020)
55 Strüker, J., Utz, M., Sedlmeir, J. (2021): Einsatz der Blockchain-Technologie für Smart Grid Dienstleistungen durch E-PKW im Reallabor „EnStadt:Pfaff“
56 https://kusama.network/, Zugriff am 18.08.2021
57 https://polkadot.network/, Zugriff am 18.08.2021
58 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Smart-Meter-Gateway.pdf?__blob=publicationFile&v=2
59 https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/SmartMeter/smartmeter_node.html
60 https://www.bsi.bund.de/SharedDocs/Zertifikate_CC/CC/SmartMeter_Gateway/0918_0918V2.html?nn=449840
61 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03109/TR-03109-4_PKI.html
62 https://dev.kilt.io/#/, Zugriff am 25.08.2021
63 https://www.youtube.com/watch?v=ki0iBLwxPqA
64 https://substrate.dev/docs/en/knowledgebase/advanced/cryptography
65 https://github.com/digitalbazaar/vc-js

66 https://www.bmwi.de/Redaktion/DE/Publikationen/Schlaglichter-der-Wirtschaftspolitik/schlaglichter-der-wirtschaftspolitik-09-2020.html
67 Decentralized Identifiers (DIDs) v1.0, https://www.w3.org/TR/did-core/
68 Verifiable Credentials Data Model 1.0, https://www.w3.org/TR/vc-data-model/
69 DIDComm Messaging, https://identity.foundation/didcomm-messaging/spec/
70 https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Smartmetering/Smart-Meter-Gateway/Zertifikate24Msbg/produkte.html
71 Polkadot: Lightpaper – An introduction to Polkadot, April 2020, https://polkadot.network/Polkadot-lightpaper.pdf
72 Dennis, R., Disso, J.P. (2019): An Analysis into the Scalability of Bitcoin and Ethereum. In: Yang , XS., Sherratt, S., Dey, N., Joshi, A. (Hrsg.): Third International Congress on Information and Communication Technology. Advances in Intelligent Systems and Computing, Vol 797. Springer, Singapore. https://doi.org/10.1007/978-981-13-1165-9_57
73 Vitalik Buterin: Layer 2 is the future of Ethereum scaling, https://forkast.news/vitalik-buterin-layer-2-future-of-ethereumscaling/
74 In der Literatur wird dies unter dem Konzept der kritischen Masse und den Risiken von Excess Inertia diskutiert (vgl. Cabral 2000).
75 Verordnung (EU) 2016/679 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) Zwischen Systemgestaltung und Selbstregulierung, Springer, Wiesbaden, S. 315–336
76 Hornung, G. (2018): Sind neue Technologien datenschutzrechtlich regulierbar? Herausforderungen durch „Smart Everything“. In: Roßnagel, A., Friedewald, M., Hansen, M. (Hrsg.): Die Fortentwicklung des Datenschutzes.
77 Vgl. hierzu grundlegend EuGH, Urteil vom 15.07.1964 – 6/64, NJW 1964, 2371; Kirchhof, NVwZ 2014, 1537 ff.; Hirsch, NJW 2000, 1817 ff.; Hirsch, NJW 1996, 2457 ff.; Ruffert (2011), in: Calliess/Ruffert: EUV/AEUV, 4. Aufl., AEUV Art. 288 Rn. 20, Art. 1 Rn. 16 ff.
78 Siehe hierzu Reibach DSRITB 2018, 131 (132 ff.); so auch ausdrücklich zur Durchführung der DSGVO-Schlussanträge des Generalanwalts vom 19. 12. 2017 – C-40/17, Beck RS 2018, 32835, Rn. 47 – Fashion ID
79 Vgl. ähnlich Bartsch, in: Danner/Theobald: Energierecht, 98. EL Juni 2018, Rn. 5, 6
80 Roßnagel/Kroschwald: ZD 2014, S. 495 (496)
81 BMWi: Fahrplan für die weitere Digitalisierung der Energiewende, 01/2020, abrufbar unter: https://www.bmwi.de/Redaktion/DE/Downloads/F/fahrplan-fuer-die-weitere-digitalisierung-der-energiewende.pdf?__blob=publicationFile&v=10. Am 31.01.2020 hat das BSI per Allgemeinverfügung festgestellt, dass die technische Möglichkeit zum Einbau intelligenter Messsysteme besteht, und somit einen weiteren Schritt in Richtung Smart-Meter-Rollout beschritten; BSI: Allgemeinverfügung zur Feststellung der technischen Möglichkeit zum Einbau intelligenter Messsysteme vom 31.01.2020, Az: 610 01 04 /2019_001; Schlosser, ew 4/2020, 68; Heuell, ew 4/2020, 70 (70)
82 Bretthauer, in: EnWZ 2017, 56 (56)
83 BT-Drs. 18/7555, 62; vgl. Wiesemann in FHS Betrieblicher Datenschutz, Teil VI, Kap. 7, Rn. 27; Wengeler, in: EnWZ 2014, 500 (501)
84 BT-Drs. 18/7555, 62, 66
85 Vgl. ebd. mit Verweis auf Soetebeer/Bartsch: IR 2013, S. 30 f., und Gola, in: Gola: DSGVO, Art. 4, Rn. 5
86 Vgl. § 2 Nr. 3 MsbG
87 Vgl. Art. 83 Abs. 5 lit. a DSGVO
88 BK6–06-009 (GPKE); Beschluss der BNetzA vom 11.07.2006 wegen der Festlegung einheitlicher Geschäftsprozesse und Datenformate zur Abwicklung der Belieferung von Kunden mit Elektrizität, BK6–06-009. Dieser wird seit 01.12.2019 durch die Anlage 1 zum Beschluss BK6-18-032 vom 20.12.2018 ersetzt.
89 BK7-06-067 (GeLi Gas); Beschluss der BNetzA vom 20.08.2007 wegen der Festlegung einheitlicher Geschäftsprozesse und Datenformate beim Wechsel des Lieferanten bei der Belieferung mit Gas, BK7-06-067
90 Vgl. Bartsch, in: Danner/Theobald: Energierecht, 98. EL Juni 2018, Rn. 9
91 Vgl. Art. 5 Abs. 1 lit. a i.V.m. Art. 6 DSGVO
92 Vgl. Art. 5 Abs. 1 lit. c DSGVO
93 Siehe Überblick bei Kraska, ZD-Aktuell 2016, 04173
94 Kraska, ZD-Aktuell 2016, 04173
95 Plath, in: Plath (2016), 2. Aufl., DSGVO Art. 6 Rn. 25
96 Kühling/Martini et al.: DSGVO und nationales Recht, 33, abrufbar unter: http://www.uni-speyer.de, zuletzt abgerufen am 26.10.2021

97 Herb, in: Steinbach/Weise, MsbG § 49 Rn. 11; Wiesemann, in FHS: Betrieblicher Datenschutz, Teil VI, Kap. 7, Rn. 27; Bretthauer, in: EnWZ 2017, 56 (61); Heun/Assion, in: BB 2018, 579 (584); aA wohl: Verbraucherzentrale Bundesverband: Smart Meter Einbau: Zwangsdigitalisierung durch die Kellertür – Stellungnahme vom 09.10.2015 zum Entwurf eines Gesetzes zur Digitalisierung der Energiewende 9, abrufbar unter: https//www.vzbv.de/pressemitteilung/smart-meter-verbraucher-lehnen-zwangsdigitalisierung-ab, zuletzt abgerufen am 26.10.2021
98 Bretthauer, in: EnWZ 2017, 56 (61)
99 Bartsch/Dippold, in: vom Wege, Weise: Praxishandbuch Messstellenbetriebsgesetz, 2019, Kapitel 9 Rn. 29 ff.
100 Bartsch/Danner/Theobald, Teil 230, Rn. 112
101 BT-Drs. 18/7555, 105
102 So für § 21g EnWG Lorenz/Raabe, in: Säcker (o. Fn. 8), § 21g Rn. 16
103 BT-Drs. 18/7555, 3
104 Vgl. kritisch zu den quantitativen Auswirkungen variabler Stromtarife auf die Stromkosten von Kleinverbrauchern eine Kurzstudie des Wissenschaftlichen Instituts für Infrastruktur und Kommunikationsdienste (WIK) vom 11.11.2015, http://zap.vzbv.de/ce0ba83d-8d69-4aed-bbc3-af50e58fdf59/Auswirkungen-variabler-Stromtarife-auf-Stromkosten-Haushalte-WIK-vzbv-November-2015.pdf, zuletzt abgerufen am 02.01.2017
105 BT-Drs. 18/7555, 105
106 BVerfGE 65, 1 (46), abrufbar unter: www.beck-online.beck.de
107 So auch schon unter Geltung von § 21g EnWG; Britz/Hellermann/Hermes, EnWG, § 21g Rn. 5
108 Vgl. BT-Drs. 18/7555, u. a. S. 105; ablehnend: Steinbach/Weise/Herb, § 49 MsbG Rn. 4
109 Vgl. insofern auch Art. 5 Abs. 2 des Kommissions-Vorschlags für eine Verordnung des Europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG („ePrivacy Verordnung“, 2017/0003 (COD)), der Maschine-zu-Maschine-Kommunikation vom Anwendungsbereich des ePrivacy-VO-E umfasst sieht, wenn sich diese Kommunikation auf Endnutzerinnen und Endnutzer bezieht
110 https://www.umweltbundesamt.de/sites/default/files/medien/1410/publikationen/2019-08-15_cc_30-2019_marktanalyse_oekostrom_ii.pdf
111 http://www.gesetze-im-internet.de/hkngebv/BJNR270300012.html
112 https://www.umweltbundesamt.de/sites/default/files/medien/372/dokumente/einsatz_des_umweltgutachters_210408.pdf
113 https://www.umweltbundesamt.de/sites/default/files/medien/1410/publikationen/2019-08-15_cc_30-2019_marktanalyse_oekostrom_ii.pdf
114 https://www.enbw.com/media/presse/docs/gemeinsame-pressemitteilungen/2020/20200615_positionspapier_kleine_direktvermarktung.pdf
115 https://www.regelleistung.net/ext/static/technical
116 https://eepublicdownloads.azureedge.net/clean-documents/Publications/Market%20Committee%20publications/ENTSO-E_Balancing_Report_2020.pdf
117 https://www.elaad.nl/projects/frequency-containment-reserve-pilot/
118 Übersetzt, engl.: Blockchain based digital identities to integrate EVs into the power system https://www.eliagroup.eu/en/news/press-releases/2020/11/20201120_publication-vision-paper-on-e-mobility, Seite 7
119 https://catena-x.net/de/
120 https://future-energy-lab.de/newsroom/publikationsdetailansicht/pub/dena-analyse-energy-communities-beschleuniger-der-dezentralen-energiewende/
121 https://ec.europa.eu/energy/topics/energy-strategy/clean-energy-all-europeans_en
122 https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20011619
123 https://energytransition.klimafonds.gv.at/wp-content/uploads/sites/7/2019/03/Infoblatt-Gemeinschaftliche-Erzeugungsanlage-20170921-1.pdf
124 Siehe: https://www.bigchaindb.com/. Das Netzwerk wird noch im Juni 2022 in Planetmint umbenannt werden.
125 https://datatracker.ietf.org/doc/html/draft-thomas-crypto-conditions-03
126 https://medium.com/decentralized-identity/the-universal-resolver-infrastructure-395281d2b540
127 https://www.trendingtopics.at/riddle-code-tokenisiert-mit-wien-energie-die-groesste-solaranlage-oesterreichs/
128 https://dev.kilt.io/docs/sdk/introduction

Abbildungsverzeichnis

Tabellenverzeichnis

www.dena.de future-energy-lab.de

dena
Deutsche Energie-Agentur