Whitepaper

Einsatz der SSI-Technologie bei der Implementierung der OZG-Nutzerkonten

Version 1.3, 18. Juli 2022

Inhalt

Abbildungsverzeichnis

Abkürzungsverzeichnis

BMI	Bundesministerium des Innern und für Heimat
BSI	Bundesamt für Sicherheit in der Informationstechnik
CEF	Connecting Europe Facility
CEN	Europäisches Komitee für Normung
DID	Dezentraler Identifikator
DLT	Distributed Ledger Technologie, z.B. Blockchain
DSGVO	Datenschutzgrundverordnung
EEFTA	Europäische Freihandelsassoziation
eID	elektronische ID
eIDAS	electronic IDentification, Authentication and trust Services
ETSI	Europäische Institut für Telekommunikationsnormen
EWR	Europäischen Wirtschaftsraum
GAFA	Google, Apple, Facebook und Amazon
GwG	Geldwäschegesetz
IETF	Internet Engineering Task Force
IoT	Internet der Dinge
ISO	Internationale Organisation für Normung
LoA	Level of Assurance
OOP	Once-Only-Principle
OOTS	Once Only Technical System
OZG	Onlinezugangsgesetz
PKC	Public Key Cryptography
PKI	Public Key Infrastructure
RegMoG	Registermodernisierungsgesetz
SDG-VO	Single-Digital Gateway Verordnung
SGB	Sozialgesetzbuch
SSI	Self-Sovereign Identity
TOOP	The Once-Only Principle Project
TR	Technische Richtlinie
TS	Technical Specification
VC	Verifiable Credential
VwGO	Verwaltungsgerichtsordnung
W3C	World Wide Web Consortium
ZKP	Zero-Knowledge-Proof
ZPO	Zivilprozessordnung

Rechtliche Informationen und weitere Hinweise

Aus Gründen der besseren Lesbarkeit wird auf die gleichzeitige Verwendung der Sprachformen männlich, weiblich und divers (m/w/d) verzichtet. Sämtliche Personenbezeichnungen gelten somit gleichermaßen für alle Geschlechter.

Um die eindeutige Zuordnung von Fachbegriffen zu gewährleisten, werden in diesem Dokument die englischen Begriffe verwendet.

1. Management Summary

In diesem Whitepaper soll das neue Konzept der Self-Sovereign Identity (SSI) vorgestellt und im Hinblick auf einen Einsatz zur Identifizierung und Autorisierung in Verbindung mit dem vom OZG geforderten Nutzer- bzw. Servicekonto beschrieben werden. Dabei will das Dokument das Konzept von SSI technologisch neutral und ohne technologische Vorgaben vorstellen. Durch die Verwendung der so genannten „Verifiable Credentials“ (VC) sowie der „Wallets“ bei den Nutzern ist dieses Konzept prädestiniert für die nutzerzentrierte Verwendung von Nachweisen aus unterschiedlichen Quellen und auch mit unterschiedlicher Regulatorik und unterschiedlichen Vertrauensniveaus. Nicht nur das Speichern, sondern auch das Weitergeben von Nachweisen unter Kontrolle der Nutzer lässt ein großes Einsatzgebiet erwarten, bei dem auch Aspekte wie Datensparsamkeit und die Idee von „Once-Only“ eine Rolle spielen. Für Bürger sowie Unternehmen könnte diese ganzheitliche Lösung einen Mehrwert bieten, da das Konzept offen ist für Anwendungsfälle aus dem täglichen Leben (z.B. Fischereischein, Schülerausweis, Ehrenamtskarte, Vereinsmitgliedschaft, Steuerbescheid).

Technologisch wird SSI öfter im Zusammenhang mit einer Distributed Ledger Technology (DLT) bzw. Blockchain genannt. Hier muss deutlich herausgestellt werden, dass eine Blockchain nicht Grundvoraussetzung für SSI ist.

SSI ist perspektivisch eine anzustrebende Lösung, die in kleinen Schritten erprobt werden muss, um die derzeitigen offenen Punkte (Sicherheit, Interoperabilität und Regulatorik) zum Wohle der Bürger sowie Unternehmen zu lösen.

Verfasser

GovPart GmbH: Helmut Nehrenheim (Federführer)

Anstalt für Kommunale Datenverarbeitung in Bayern: Stefan Michalk

Bayerisches Staatsministerium für Digitales: Christian Sombeck

Bundesdruckerei GmbH: Jörg Fischer, Micha Kraus, Robert Musick, Paul Bastian

DATEV eG: Michael Dellermann, Constantin Werner

Governikus GmbH & Co. KG: Hartje Bruns, Sarah Bomme, Silke Thaidigsmann

Stadt Köln: Sebastian Zickau

msg systems ag: Tobias Link, Steffen Schwalm

Technische Universität Berlin: Christopher Ritter, Hakan Yildiz

Universität der Bundeswehr München: Michael Grabatin, Wolfgang Hommel, Daniela Pöhn

2. Einführung

Das Gesetz zur Verbesserung des Onlinezugangs zu Verwaltungsleistungen - Onlinezugangsgesetz (OZG)[1] - schreibt vor, dass Bund und Länder ihre Verwaltungsleistungen auch elektronisch über Verwaltungsportale anbieten sollen. Dabei spielt die Bereitstellung eines Nutzerkontos eine bedeutende Rolle.

Insbesondere sind folgende Teile des OZG für die Betrachtung relevant:

- Gemäß § 3 Absatz 2: Bund und Länder stellen im Portalverbund **Nutzerkonten** bereit, über die sich Nutzer für die im Portalverbund verfügbaren elektronischen Verwaltungsleistungen von Bund und Ländern einheitlich identifizieren und authentifizieren können.
- Gemäß § 8 Absatz 1: Der Nachweis der Identität des Nutzers eines Nutzerkontos kann auf unterschiedlichen **Vertrauensniveaus** erfolgen und muss die Verwendung, des für das jeweilige Verwaltungsverfahren erforderlichen Vertrauensniveaus, ermöglichen.
- Gemäß § 8 Absatz 8: Die Bundesregierung wird ermächtigt, durch Rechtsverordnung, mit Zustimmung des Bundesrates, festzulegen, welche elektronischen **Identifizierungsmittel** im Rahmen der Interoperabilität der Nutzerkonten von Bund und Ländern zum Nachweis der Identität eingesetzt werden können, die Details eines Anerkennungsverfahrens festzulegen und die technischen Rahmenbedingungen zur Sicherstellung der Interoperabilität der Nutzerkonten zu bestimmen.
- Gemäß § 2 Absatz 7: Ein „**Postfach**“ ist eine IT-Komponente, über die eine Behörde Nutzern mit deren Zustimmung elektronische Dokumente und Informationen bereitstellen kann. Das Postfach ist Bestandteil eines Nutzerkontos. Die Nutzung eines Postfachs ist für die Nutzer freiwillig.

Somit ist festzustellen, dass

- die Einführung eines Nutzerkontos perspektivisch beim Bund und in allen Ländern erfolgen wird, bzw. größtenteils bereits erfolgt ist,
- die Frage des Vertrauensniveaus abhängig vom Verwaltungsverfahren ist und
- Identifizierungsmittel und auch die Anerkennungsverfahren vom Bund festgelegt werden können.

Ziel dieses Whitepapers ist, das neue Konzept der Self-Sovereign Identity (SSI) vorzustellen und dahingehend zu beschreiben, dass ein Mehrwert für Bürgerinnen und Bürger, aber auch der

[1] Bundesministerium des Inneren, für Bau und Heimat, 2017

Verwaltung erkennbar ist. Dabei bietet das bei SSI verwendete Konzept nicht nur ein Mittel zur Identifizierung und Authentifizierung, sondern kann durch Verwendung der so genannten Verifiable Credentials (VC) sowie der Wallets bei den Nutzenden auch als „Postfach“ im oben genannten Sinn dienen. Der Begriff VC wird in diesem Dokument technikneutral verwendet.

Seit vielen Jahren gilt in Europa die „Verordnung über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt“, abgekürzt eIDAS-Verordnung[2]. Der Entwurf der fortgeschriebenen eIDAS-Verordnung, kurz eIDAS 2.0[3], wurde im Juni 2021 veröffentlicht. Eine finale Verabschiedung wird für das 4. Quartal 2022 erwartet. Die europäische Kommission begründet die Revision der eIDAS-Verordnung wie folgt: "In nur einem Jahr hat sich infolge der COVID-19-Pandemie nicht nur die Rolle und die Bedeutung der Digitalisierung in unseren Gesellschaften und Volkswirtschaften grundlegend verändert, sondern auch ihr Tempo rasant beschleunigt. Infolge der zunehmenden Digitalisierung von Dienstleistungen ist die Nachfrage der Nutzer und Unternehmen nach Mitteln zur Identifizierung und Authentifizierung im Internet sowie nach einem digitalen Austausch von Informationen über Identitäten, Attribute oder Berechtigungen, die auf eine sichere Weise und mit einem hohen Datenschutzniveau erfolgen, drastisch angestiegen."

Als eine Lösungsmöglichkeit werden SSI- und Wallet-Ansätze gesehen, die in die Überarbeitung der eIDAS-Verordnung einfließen werden.

3. Was bedeutet SSI?

SSI steht für Self-Sovereign Identity (übersetzt: selbstbestimmte Identitäten) und bedeutet „Identitäten in der Hand des Nutzers“. Dieses Prinzip ist aus der analogen Welt bekannt - von Karten in der eigenen Brieftasche.

Mit dem Konzept SSI entwickelt sich aktuell ein internationaler Standard für eine neue Form der Digitalen Identitäten. Dabei trägt SSI der immer stärker werdenden Bedeutung der Identitäten von natürlichen oder juristischen Personen, aber auch Dingen (IoT) in einer digitalen Welt Rechnung. Viele Lebenslagen können somit abgebildet werden.

Mehrere Initiativen und Bestrebungen in Bund, Ländern und Kommunen, aber auch in der EU-Kommission, setzen auf dieses neue Konzept. Dabei bietet dieses Konzept nicht nur die Möglichkeit der Identifizierung und Authentifizierung. Das Konzept beruht darauf, dass einem Nutzer (Holder) Nachweise von einem Aussteller (Issuer) auf ein Wallet (Smartphone, Cloud-Wallet, etc.) in Form von VC übertragen werden. Diese können dann vom Nutzer einer anderen Stelle (Verifier) vorgelegt und

[2] eIDAS-Verordnung https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32014R0910
[3] eIDAS 2.0 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0281

durch diesen überprüft werden. So behalten die Nutzer die Souveränität über ihre Daten. Wichtig ist jedoch, dass den Nutzern die gleiche Sorgfaltspflicht obliegt, wie bei der eigenen Brieftasche.

Perspektivisch hat SSI auch das Potenzial, eine Alternative zu single sign-on Lösungen von großen Technologieanbietern oder anderen zentralen Identitäts-Anbietern zu werden, die im Verdacht stehen, Nutzerdaten kommerziell ohne Zustimmung der Nutzer zu benutzen. Dabei gilt es, im Hinblick auf die Akzeptanz von neu zu entwickelnden Lösungen neben dem starken Fokus auf die Sicherheit die Nutzerfreundlichkeit im Blick zu behalten.

Der dezentrale Ansatz der SSI verspricht, dass zu identifizierende Personen (Inhaber bzw. „Holder“) ihre Identitätsmerkmale und Berechtigungen in Form von kryptografisch gesicherten Nachweisen („VC“) ohne Intermediär selbstständig in einer digitalen Brieftasche („Wallet“) verwalten können.[4] Um sich bei einer Akzeptanzstelle („Verifier“), beispielsweise einem Diensteanbieter, zu identifizieren oder authentifizieren, weist der Inhaber diese VC vor und kann dabei selbst entscheiden, welche Daten („Claims“) der Akzeptanzstelle zur Prüfung übermittelt werden. Ähnlich wie auch in der analogen Welt ist die Überprüfung für die Akzeptanzstelle ohne direkten Kontakt zum Herausgeber („Issuer“) möglich. Die öffentlichen Metadaten von juristischen Personen (z.B. dezentrale Identifikatoren inkl. öffentliche Schlüssel und Sperrinformationen) stehen in einem dezentralen vertrauenswürdigen Register zur Verfügung. Dadurch können ausgestellte VC auch aktualisiert und widerrufen werden. Das Datenregister kann ein dezentraler Distributed Ledger (DLT), welches aus unterschiedlichen Knotenpunkten („Nodes“) besteht oder eine zentrale PKI sein. Voraussetzung ist, dass die Vertrauenswürdigkeit z.B. durch Prüfstellen bestätigt wird.[5] Zu beachten ist auch das vom BSI erstellte Eckpunktepapier.[6]

Im Folgenden wird das Konzept von SSI stellvertretend für technische Umsetzungen mit oder ohne DLT verwendet.

---

[4] Der Ansatz der Self-Sovereign Identity wird hier nicht im Detail erläutert. Allen (2016) definiert den/die Nutzer*in als zentralen Verwalter bzw. zentrale Verwalterin seiner/ihrer Identität, einschließlich aller existierenden Teilidentitäten. Daher muss es Nutzer*innen möglich sein, über alle verschiedenen Dienste hinweg die Kontrolle über ihre Identität zu wahren und damit eine Autonomie in der Verwaltung dieser Dienste zu erzielen.

[5] Eine solche Zertifizierung ist im Entwurf von eIDAS 2.0 vorgesehen.

[6] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Krypto/Eckpunkte_SSI_DLT.html

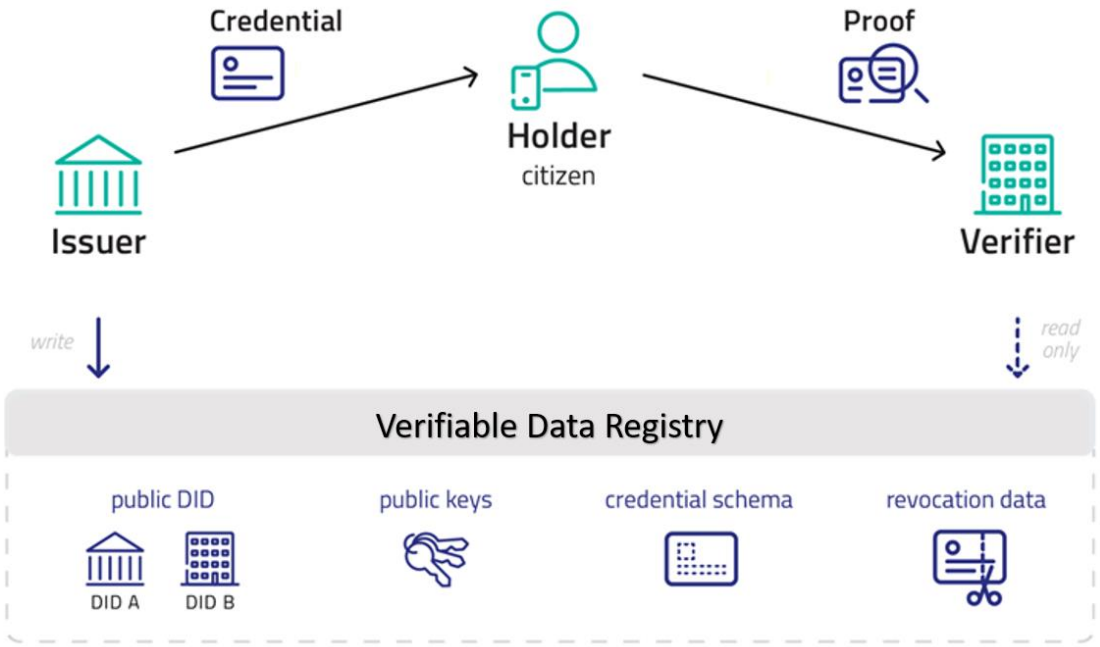

Abbildung 1: Das SSI Vertrauensdreieck

Vorteile von SSI

- Daten-Souveränität als Prinzip
- Verknüpfung der Identität mit weiteren digitalen Nachweisen
- Nutzerorientierte Verwendung von Nachweisen
- Peer-to-Peer Verbindungen für den Austausch und Nachweis von VC
- Selektive Offenlegung von Attributen und kenntnisfreie Beweise von Attributseigenschaften

Technik

Die technische Entwicklung in eIDAS 2.0 ist noch nicht abgeschlossen und kann daher noch nicht vollumfänglich berücksichtigt werden. Die technischen Grundsätze können dennoch wie folgt beschrieben werden.

Für die Umsetzung einer SSI-Lösung sind die folgenden fünf Elemente besonders relevant:

- **Verifiable Credentials (VC)** = W3C-Standard für kryptografisch gesicherte Datenformate zur Beschreibung von Identitätsattributen
- **Decentralized Identifiers (DID)** = W3C-Standard für dezentrale Identifier von beliebigen Entitäten, z.B. für natürliche und juristische Personen
- **Digital Wallets** = Software zur Aufbewahrung von VC und privaten Schlüsseln

- **Digital Agents** = Technische Endpunkte, die die Kommunikation zwischen den Protagonisten herstellen
- **SSI-Rollen (Issuer, Holder, Verifier)** = Protagonisten einer SSI-Lösung; stehen in einer Beziehung zueinander

Digitale Nachweise (folgend engl.: Credentials) sind der zentrale Baustein jeder SSI-Lösung. Attestierte Credentials werden in der SSI-Welt als VC bezeichnet. Erst durch eine einheitliche Standardisierung werden VC interoperabel anwendbar und müssen nicht für jeden Kontext neu ausgestellt werden. Für VC existiert bereits ein W3C-Standard, der vorgibt, wie die digitalen Zertifikate aufgebaut sind. VC enthalten Identitätsattribute in einem kryptografisch gesicherten Format und sind die Basis für einen vertrauenswürdigen und manipulationssicheren Austausch von Informationen aus digitalen Nachweisen. SSI basiert grundsätzlich auf dem Konzept der asymmetrischen Kryptografie (Public Key Cryptography, PKC). Das Konzept beruht auf generierten Private-Public-Key-Paaren (Schlüsselpaare).

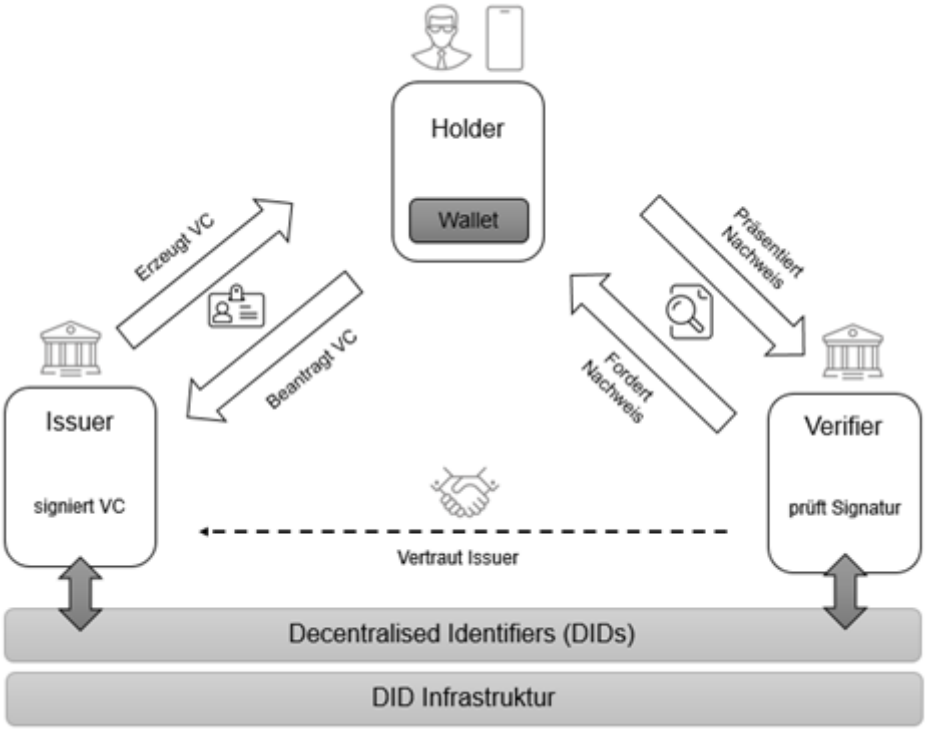

Abbildung 2: Trust Triangle

Der Ersteller eines VC, der im Folgenden Issuer genannt wird, erstellt mit seinem geheimen Schlüssel (Private Key) für das VC eine digitale Signatur. Diese hängt er als eine Art digitale Unterschrift an das VC an. Nun kann jeder Verifier mithilfe des öffentlichen Schlüssels des Issuers (Public Key) überprüfen, dass die Signatur mittels des zugehörigen Private Keys berechnet wurde, ohne den Private Key des Issuers jemals gesehen zu haben. Dabei ist zu beachten, dass es sich ohne Nutzung eines qualifizierten. Vertrauensdienstes nicht um eine digitale Signatur gem. eIDAS handelt.

Damit kann die Integrität des VC bestätigt werden, sofern der Verifier dem Issuer vertraut und davon überzeugt ist, dass der Issuer seinen Private Key geheim hält. Der Holder bewahrt die ihm ausgestellten VC in einem sogenannten Wallet auf, einem digitalen Äquivalent zur Brieftasche. Die in einem VC enthaltenen Identitätsattribute können vom Holder dann gegenüber einem Verifier präsentiert werden. Der Verifier überprüft die Integrität der übermittelten Informationen per Kryptographie. Die SSI-Protagonisten bilden im Rahmen der Issuer-Holder-Verifier Beziehung das sogenannte „Trust Triangle“, siehe Abb 2.

Der W3C-Standard für DID ermöglicht den SSI-Protagonisten das Herstellen einer verschlüsselten Peer-to-Peer-Kommunikation auf unterschiedlichen technischen Infrastrukturen, zum Beispiel für die Ausstellung von digitalen Nachweisen (Beziehung zwischen Holder und Issuer) oder die Verifizierung von Behauptungen durch den Verifier (Beziehung zwischen Holder und Verifier). In diesem Zusammenhang werden für die bilaterale Kommunikation auch noch sogenannte „Digital Agents“ als technischer Endpoint bzw. Treuhänder für den Identifier benötigt. Sie stellen die geschützte Kommunikation zwischen den einzelnen SSI-Rollen sicher und sollten analog zu E-Mail-Servern durchgehend erreichbar sein.

Eines der zentralen Ziele der SSI-Architektur ist, persönliche Daten zu schützen und nur so viele Daten über das Subjekt eines VC preiszugeben, wie unbedingt notwendig sind. Die SSI-Architektur ermöglicht grundsätzlich einen Austausch von verifizierbaren Daten zwischen Verifier und Holder, ohne dass der Issuer an der Interaktion beteiligt sein muss. Die übertragenen Informationen können vom Verifier durch Signaturverfahren auf Echtheit überprüft werden.

Credentials können in der SSI-Architektur als Einzelnachweise dem Verifier vorgelegt werden. Zusätzlich zu der Möglichkeit, Attribut-Informationen zu übermitteln, können auch durch kryptographische Beweise („Proofs“) nur Eigenschaften der Attribute des VC Inhabers (Holder) übertragen werden. Hierzu werden sogenannte Zero-Knowledge-Proofs eingesetzt (ZKP). Mit der Hilfe von ZKPs können Holder ggü. einem Verifier beispielsweise die Eigenschaft „Ich bin über 18 Jahre alt“ nachweisen, ohne das eigentliche Geburtsdatum preiszugeben zu müssen. ZKPs erhöhen somit den Schutz der Privatsphäre.

Außerdem können Nutzer von SSI-Wallets beliebige Attribute selektiv aus unterschiedlichen VC kombinieren („Selektive Informationsweitergabe“) und diese Attribute beispielsweise im Kontext einer Verwaltungsleistung nachweisen. Sobald ein gültiger „Proof“ über die ausgewählten und gleichzeitig notwendigen Attribute übermittelt wurde und vom Verifier überprüft wurde, kann die gewünschte Verwaltungsleistung von den Nutzern in Anspruch genommen werden.

4. Was kann SSI in Verbindung mit den Nutzerkonten leisten?

Nutzerkonten ermöglichen es den Nutzern, Onlinedienste des Bundes, der Länder und Kommunen zu verwenden. Dabei stellen die Länder und der Bund jeweils einen interoperablen Nutzerkontendienst zur Verwaltung der einzelnen Nutzerkonten zur Verfügung. Im Zusammenspiel mit den Onlinediensten der Verwaltung wird das Nutzerkonto eingesetzt, um die Identität des Nutzers festzustellen. Dabei können die interoperablen Nutzerkonten in zwei Rollen (Dipol-Architektur) auftreten: Zum einen als das zusichernde Nutzerkonto, welches als das "Heimat"-Nutzerkonto die Identifizierungsattribute der Bürger verwaltet. Zum anderen als das vertrauende Nutzerkonto, welches für Onlinedienste in einem anderen Bundesland, die Identifizierungsattribute der Bürger beim zusichernden Nutzerkonto abfragt.

Über verschiedene Authentifizierungsmethoden können die Nutzerkonten mit verschieden stark zugesicherten Attributen befüllt werden. Nach §8 OZG können – neben anderen, eher technischen – folgende Attribute für natürliche Personen übermittelt werden:

- Familienname
- Geburtsname
- Vornamen
- akademischer Grad
- Geburtstag
- Geburtsort
- Geburtsland
- Anschrift
- Staatsangehörigkeit

Die Verlässlichkeit der Zusicherung eines Attributes wird dabei als Vertrauensniveau (Level of Assurance, LoA) ausgedrückt. Das höchste Vertrauensniveau kann gegenwärtig nur über die Online-Ausweisfunktion des Personalausweises, des elektronischen Aufenthaltstitels und der eID-Karte für EU-Bürgerinnen und -Bürger oder entsprechend notifizierten eID-Mitteln der europäischen Mitgliedstaaten erreicht werden.

In dieser Architektur kann SSI in fünf Fällen eine Rolle spielen. Der erste und vermeintlich sehr häufig anzutreffende Fall ist, dass ein Nutzer einen Onlinedienst nutzen möchte, aber kein Nutzerkonto besitzt. In der Regel müsste er nun ein neues Nutzerkonto anlegen, indem er sich bei dem für ihn zuständigen Nutzerkonto registriert. Gerade für einfache Onlinedienste mit geringen Anforderungen an das Sicherheitsniveau ist dies ein Aufwand, der potenziell abschreckend wirkt. Wenn stattdessen aus einer vorhandenen SSI-Wallet Attribute zur Identifizierung verwendet werden könnten, um einmalig bzw. temporär einen Onlinedienst nutzen zu können, würde dies den Zugang zu vielen

Onlinediensten erleichtern. Dieses Szenario wird in den Nutzerkonten bereits als sogenanntes temporäres Nutzerkonto unterstützt, in dem dann ein SSI-Wallet zum Einsatz kommen könnte. Die Attribute in der vorhandenen SSI-Wallet können entweder durch die Ableitung einer eID erzeugt werden oder in Zukunft durch eine Vielzahl an Organisationen (z.B. Banken und Versicherungen) ausgestellt werden.

Wird das Nutzerkonto häufiger benötigt, können in dem zweiten Fall die im SSI-Wallet hinterlegten Attribute verwendet werden, um schneller und leichter ein permanentes Nutzerkonto anzulegen.

Auch bei einem schon bestehenden Nutzerkonto kann es in einem dritten Fall für die Bürger sinnvoll sein, VC zu verwenden, um das Nutzerkonto mit weiteren Informationen anzureichern bzw. beim Besuch eines Onlinedienstes Zusatzinformationen übermitteln zu können. Dies können Informationen sein, die nicht in einer eID enthalten sind, zum Beispiel ein VC zum Nachweis einer Telefonnummer oder einer E-Mail-Adresse. Diese können vom jeweiligen Anbieter ausgestellt werden und müssen dann nicht extra von dem Onlinedienst aufwändig verifiziert werden.

Der vierte Anwendungsfall ergibt sich aus der Rückrichtung, wenn in dem Onlinedienst Bescheinigungen ausgestellt werden und diese dem Bürger in sein Postfach zugestellt werden. Mit einem “Verifiable Credential Offer” kann der Onlinedienst feststellen, wann der Nutzer das VC im Wallet gespeichert hat und es damit sicher zugestellt wurde.

Der fünfte Anwendungsfall wäre das Nutzerkonto selbst als Cloud-Wallet zu gestalten. Die Nutzer melden sich dort an und können dort auf die für sie ausgestellten Nachweise bzw. Daten zugreifen und somit in anderen Verwaltungsprozessen vorlegen. Welche Technologie dahinter steht, sehen sie nicht.

5. Wann könnte SSI mit dem Servicekonto verfügbar sein?

Aktuell gibt es noch keine Servicekonten, welche das SSI-Konzept nutzen. Mit SSI ergeben sich viele neue Anwendungsmöglichkeiten, wodurch bestehende Lösungen ergänzt oder ersetzt werden können. Allerdings befinden sich die Spezifikationen und Umsetzungen auch noch in einer sehr frühen Phase. Gerade um die Möglichkeiten, die sich über SSI-Ansätze ergeben, auszuloten, wird in vielen Projekten SSI erprobt. Dabei spielen nicht nur die wichtigen Fragestellungen zu Technik und Interoperabilität eine entscheidende Rolle, sondern auch die gesetzeskonforme Umsetzungskraft. Im Innovationswettbewerbs „Schaufenster Sichere Digitale Identitäten“ hat das Bundesministerium für Wirtschaft und Energie (jetzt Bundesministerium für Wirtschaft und Klimaschutz) 2019 einen Wettbewerb ausgerufen, über den mit zahlreichen Anwendungsfällen die Alltagsrelevanz praktisch erprobt wird.

Außerhalb des behördlichen Umfelds sind Märkte und Anwendungen rund um SSI entstanden und es gibt bereits Anbieter von Wallet-Lösungen am Markt. Allerdings sind diese meist nicht interoperabel

und passen meist auch nur genau auf eine Anwendungsdomäne. Die europäische Kommission geht mit der eIDAS Novellierung („eIDAS 2.0“) einen mutigen Schritt weiter. Die grenzüberscheitende Nutzung von Wallets, die perspektivisch durch die Mitgliedstaaten herausgegeben werden, soll in den Angeboten der Verwaltung und sogar darüber hinaus ermöglicht werden. Die bestehende eIDAS-Infrastruktur wird um diese Möglichkeiten erweitert. Auch wenn sich das Gesetzgebungsverfahren und dementsprechend auch die technischen Spezifikationen in einem sehr frühen Stadium befinden, kann von einer breiten Nutzung von Wallets als Ergänzung zu den bestehenden eID-Systemen in den kommenden Jahren ausgegangen werden.

Auf dem Weg zur europaweiten Nutzbarkeit von Wallets, wie sie in der eIDAS Novellierung angedacht ist, sind Erprobungsprojekte in mehreren Regionen geplant. In den Anwendungen der öffentlichen Verwaltung, zu denen auch die Servicekonten gezählt werden können, könnte SSI sukzessive Einzug halten.

6. Wo gibt es Herausforderungen beim Einsatz von SSI?

Wesentliche Herausforderungen beim Einsatz von SSI bestehen derzeit vor allem hinsichtlich folgender Aspekte:

- Informationssicherheit und Interoperabilität
- regulatorische Rahmenbedingungen
- langfristige Nachweisfähigkeit

Informationssicherheit und Interoperabilität

Derzeit bestehen nur wenige nationale oder internationale Standards zur Informationssicherheit von SSI. Wie auch dem Eckpunktepapier des Bundesamts für Sicherheit in der Informationstechnik (BSI) zu SSI entnommen werden kann, sind derzeit noch viele Fragen hinsichtlich standardisierter Maßnahmen zur Informationssicherheit, konkrete Ausprägungen der Vertrauensniveaus, Sicherheit der verwendeten kryptographischen Mechanismen, Ablage der Kernidentitätsdaten im Mobilgerät, Erzeugung, Prüfung, sowie die Ablage des VC durch Issuer bzw. Verifier nicht vollständig beantwortet. Die notwendige Standardisierung erfolgt aktuell in den europäischen Gremien europäisches Institut für Telekommunikationsnormen (ETSI) und europäisches Komitee für Normung (CEN) sowie international Internet Engineering Task Force (IETF) und internationale Organisation für Normung (ISO). Erste Ergebnisse sind für ca. Ende 2022 zu erwarten.

Eine vergleichbare Situation besteht hinsichtlich der Interoperabilität, insbesondere wenn SSI auf Basis des VC-Datenmodells nach World Wide Web Consortium (W3C) sowie unter Nutzung von DLT umgesetzt wird. Aktuell ist es Gegenstand der Forschung wie eine Interoperabilität zwischen den

verschiedenen DID-Methoden und DLT-Protokollen hergestellt werden kann. Auch hier läuft aktuell europäische Standardisierung im Kontext eIDAS 2.0. Erste Ergebnisse sind für Ende 2022 zu erwarten.

Regulatorische Rahmenbedingungen

Mit eIDAS 2.0 wird aktuell der regulatorische Rahmen für vertrauenswürdige selbstbestimmte digitale Identitäten geschaffen. In bestehenden Gesetzen wird aktuell auf den Personalausweis oder weitere Identifizierungsverfahren Bezug genommen (z.B. GwG, SGB V etc.), was die Nutzung abgeleiteter Identitäten bspw. in einem Wallet zumindest einschränkt. Auch die Vertrauensniveaus beziehen sich derzeit vor allem auf die Kernidentität, also bspw. den Personalausweis, nicht jedoch auf weitere digitale Nachweise in Form von VC.

Die EU-Kommission schuf mit der eIDAS-Bridge eine Möglichkeit zur rechtssicheren Verwendung von VC auch im aktuellen regulatorischen Rahmen. Dabei wird das VC mit einer qualifizierten elektronischen Signatur oder Siegel eines qualifizierten Vertrauensdienstes nach eIDAS versehen. Dies lässt sich auf nahezu alle Anwendungsfälle übertragen, sofern nicht gesetzlich anderes bestimmt ist.

Langfristige Nachweisfähigkeit

Mit einem VC wird nachgewiesen, dass der Eigentümer (Holder) einen bestimmten Nachweis tatsächlich besitzt. Es ist insofern vergleichbar mit einem Signaturzertifikat, da es den Unterzeichner eines Dokuments eindeutig nachweist. Vor dem Hintergrund gelten Aufbewahrungsfristen zwischen 2 und 100 Jahren oder dauernd, die teilweise auch erst nach einem Ereignis in Jahrzehnten beginnen (z.B. Personaldaten). Bis zum Ende der Aufbewahrungsfrist sind die Authentizität, Integrität und Nachvollziehbarkeit digitaler Nachweise nachzuweisen, was deren Verkehrsfähigkeit erfordert. Auf Grundlage der sogenannten Public Key Infrastructure (PKI) liegen hierfür etablierte Lösungen vor (BSI TR-03125 für Bewahrungsprodukt, ETSI TS 119 511 für Bewahrungsdienst). Diese sind für dezentrale PKI auf Basis DLT erst zu schaffen. Ebenso sind bestehende Standards auf die Beweiswerterhaltung auf SSI zu übertragen, also den Nachweis, dass eine Person ein Zeugnis besaß. Daneben ist die Interpretierbarkeit des VC für die Dauer der Aufbewahrungsfrist zu sichern, damit auch nach 30 Jahren deutlich wird, dass es sich um ein Zeugnis handelt. Hier gilt es die bestehenden Standards weiterzuentwickeln, was derzeit in ETSI und CEN vorangetrieben wird.

Unabhängig von SSI ist in den Behörden weiterhin die Aktenführungspflicht zu beachten, um bestehende Dokumentations- und Nachweispflichten zu erfüllen.

7. Voraussetzungen zum Einsatz von SSI

eIDAS

Die eIDAS-Verordnung[7] , kurz eIDAS, schuf im Europäischen Wirtschaftsraum (EWR) einheitliche Vorgaben für vertrauenswürdige digitale Transaktionen auf Basis elektronischer Identifizierungsmittel sowie elektronischer Vertrauensdienste im Binnenmarkt. Als Identifizierungsmittel gilt hierbei insbesondere der elektronische Personalausweis in Deutschland sowie dessen europäische Pendants. Die eIDAS fokussiert aktuell staatliche i.d.R. notifizierte digitale Identitäten natürlicher Personen und weitere Identitätseigenschaften wie z.B. Prokura und Führerschein. Digitale Nachweise sind aktuell nicht im Umfang der eIDAS Regulierung. Das Gleiche gilt hinsichtlich Vorgaben für Maschinenidentitäten.

Gemäß Art. 6 eIDAS muss jede öffentliche Stelle, innerhalb der EU und Europäischen Freihandelsassoziation (EFTA), jede notifizierte eID annehmen und akzeptieren. Darüber hinaus sind beim Zugang zu elektronischen Diensten die notwendigen Vertrauensniveaus für den jeweils gewünschten Service durch die Institution zu beachten und zu prüfen, die den Service bereitstellt. Artikel 8 eIDAS unterscheidet die folgenden Vertrauensniveaus für Identifizierungsverfahren

- niedrig
- substantiell
- hoch

Detailliertere Anforderungen enthält der Durchführungsrechtsakt 2015/1502. Eine europaweite explizite Zertifizierung von Identifizierungsverfahren gegen ein LoA besteht, abgesehen von der Notifizierung staatlicher eID, nicht. Vielmehr sind die Prüfung und Entscheidung durch die anwendende Organisation notwendig. In Deutschland können im E-Government Anbieter ihre Verfahren durch das BSI über das BMI auf ein LoA bestätigen lassen – eine Pflicht besteht weder für Anbieter noch BSI oder BMI. Technische Grundlage der Prüfung, ob durch Behörde oder im Rahmen der Bestätigung, sind die TR-03147[8] und TR-03107[9] des BSI.

Die Modulzertifizierung nach Art. 24 eIDAS gilt ausschließlich für qualifizierte Vertrauensdienste, also z.B. der Erzeugung qualifizierter elektronischer Signaturen, und wird daher hier nicht weiter betrachtet.

Die Vertrauensdienste umfassen insbesondere elektronische Signaturen, Siegel, Zeitstempel, Verifikationsdienste (Prüfung von Signaturen, Siegeln etc.) und Bewahrungsdienste

[7] Vgl. Amtsblatt der Europäischen Union, 2014
[8] Vgl. BSI, 2018
[9] Vgl. BSI, 2014 und BSI, 2019

(Beweiswerterhaltung). Zudem definiert die eIDAS-Verordnung die Pflicht zur Anerkennung jeder mindestens fortgeschrittenen elektronischen Signatur bzw. Siegel bzw. Zeitstempel (Art. 25, 35, 41 eIDAS) jedes qualifizierten europäischen Vertrauensdienstes durch öffentliche Stellen. Die eIDAS-Verordnung definiert für die Bewahrungsdienste gemäß Artikel 34 eIDAS auch spezielle Anforderungen für die beweiswerterhaltende Aufbewahrung, was ebenso für VC relevant ist.

Im Zuge der Umsetzung der neuen eIDAS-Verordnung erfolgte der Erlass von Durchführungsrechtsakten welche unmittelbar auf die von europäischen und internationalen Normungsorganisationen und -einrichtungen, insbesondere CEN, ETSI festgelegten Normen und technischen Spezifikationen verweisen. Technische Vorgaben, die in Durchführungsrechtsakten erwähnt wurden, gewannen so regulatorische Verbindlichkeit wie z.B. die durch öffentliche Stellen verbindlich anzuerkennenden Signaturformate in 2015/1506.

Die nachstehende Grafik zeigt das Zusammenwirken vom Rechtsrahmen, mittels der eIDAS-Verordnung und den technischen Normen durch ETSI/CEN im Überblick.

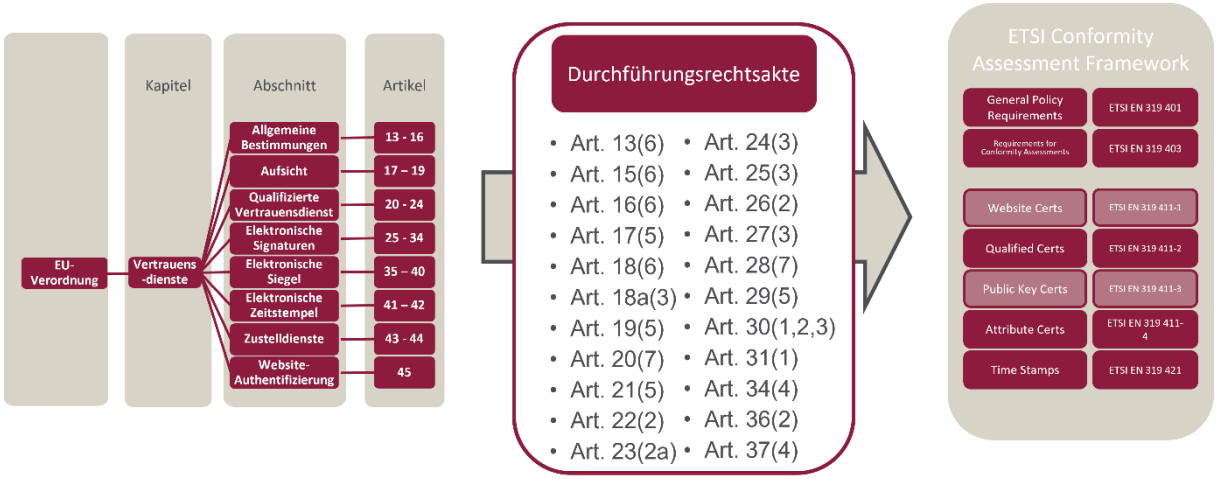

Abbildung 3: Zusammenwirken verschiedener Rechtsrahmen

Die Leitlinie der Bundesnetzagentur und des BSI[10] enthält die wesentlichen Maßgaben für Behörden, hinsichtlich (qualifizierter) elektronischer Signaturen, Siegel, Zeitstempel sowie zur Bewahrung. Bezüglich SSI ist dabei zu beachten, dass zwar digitale Signaturen auf Basis von VC erzeugt werden können, nur ist technisch a) die Gleichwertigkeit zum bestehenden Stand der Technik nachzuweisen und sie müssen zudem b) durch einen qualifizierten Vertrauensdienst ausgestellt sein, um die regulatorische Wirkung einer qualifizierten elektronischen Signatur zu erreichen.

[10] Vgl. Bundesamt für Sicherheit in der Informationstechnik, 2020

DSGVO

Neben der eIDAS-Verordnung ist auf europäischer Ebene insbesondere seit Mai 2018 die Europäische Datenschutzgrundverordnung[11] zu nennen. Diese definiert EU-weit einheitliche Vorgaben zur Erhebung, Verarbeitung und Speicherung personenbezogener Daten, wie sie insbesondere für digitale Zeugnisse typisch sind.

Die Vorgaben des Datenschutzes resp. der Vertraulichkeit sind für digitale Zeugnisse und andere Nachweise, sofern sie personenbezogene Daten enthalten, inkl. Meta-/Prozessdaten relevant. Im Kontext der Digitalisierung von Zeugnissen und deren langfristigem Nachweis sind besonders der Nachweis der Einwilligung des Betroffenen zur Erhebung und Verarbeitung seiner personenbezogenen Daten (Art. 6 DSGVO) die Informationspflicht gegenüber dem Betroffenen (Art. 13 und 14) sowie die Rechte des Betroffenen ins Blickfeld zu rücken. Hierzu zählen:

- Recht auf Auskunft (Art. 15),
- Recht auf Berichtigung (Art 16),
- Recht auf Datenübertragbarkeit in einem strukturierten, gängigen, maschinenlesbaren Format (Art. 20),
- Recht auf Löschung bzw. Recht auf „Vergessenwerden“ (Art. 17).

Weitere Regularien

Neben der eIDAS sind insbesondere die E-Government-Gesetze zu berücksichtigen, die jeweils einen verpflichtenden Zugang für den elektronischen Personalausweis vorsehen. Darüber hinaus ist das Onlinezugangsgesetz zu erwähnen, wonach durch Bund und Ländern dem Bürger sowie den Unternehmen Servicekonten zum einfachen Zugang zu bestimmten Verwaltungsleistungen angeboten wird.

In Bezug auf digitale Nachweise, wie sie durch VC in SSI abgebildet werden können, ist für die öffentliche Verwaltung zum einen die Aktenführungspflicht, sowie im Anwendungsfall die entsprechenden Fachgesetze zu prüfen. Eine Übersicht von Anforderungen an den Nachweis digitaler Transaktionen enthält Fußnote[12].

Abschließend ist der Beweiswert digitaler Aufzeichnungen und damit auch digitaler Nachweise wie VC in die Betrachtungen einzubeziehen:

Der Beweiswert elektronischer Unterlagen ergibt sich aus den §§ 371 ff. Zivilprozessordnung (ZPO). Diese Regelungen gelten gemäß u. a. § 98 Verwaltungsgerichtsordnung (VwGO) auch für die Verfahren,

[11] Vgl. Amtsblatt der Europäischen Union, 2016
[12] Vgl. M. Weber et. al., (2018)

die vor Verwaltungsgerichten geführt werden. Die nachfolgende Tabelle fasst den Beweiswert elektronischer Dokumente zusammen:

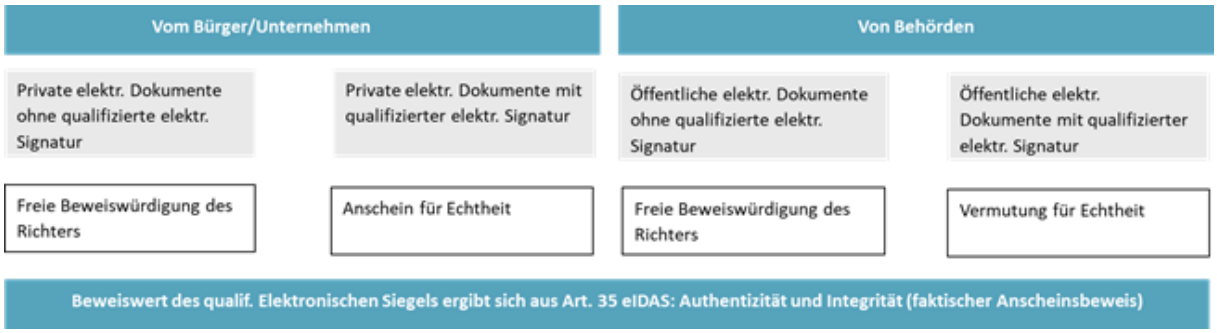

Abbildung 4: Beweiswert elektronischer Unterlagen

Für die öffentliche Verwaltung ist darüber hinaus zu beachten, dass der Beweis anhand von Akten und den darin enthaltenen Dokumenten geführt wird (§ 99 VwGO). Es ist also notwendig, erst einmal Akten zu bilden und Dokumente im Aktenzusammenhang zu führen und aufzubewahren. Das einzelne Dokument ist also nicht ausreichend. Vielmehr führt, unabhängig vom Beweiswert der elektronischen oder papiernen Dokumente, eine unvollständige Aktenführung regelmäßig zu einer Beweislastumkehr zuungunsten der Verwaltung.

Auch beim Einsatz von SSI ist also die Aktenführungspflicht sicherzustellen und der Beweiswert von VC zu betrachten.

Welches Vertrauensniveau ist durch SSI erreichbar?

Die Vertrauensniveaus (Level of Assurance) beziehen sich aktuell ausschließlich auf die Kernidentität einer natürlichen (bzw. juristischen) Person und hier auf die vollständigen Lifecycle-Prozesse der elektronischen Identität (vgl. (EU) 2015/1502)[13].

Digitale Nachweise, kurz VC, sind, sofern sie nicht die Kernidentität umfassen, nicht im regulatorischen Rahmen der aktuellen eIDAS-Verordnung und der dort definierten Vertrauensniveaus.

Für digitale Nachweise kann insofern weniger ein Vertrauensniveau, sondern nur die grundlegende Anforderung an die Nachweisfähigkeit behördlicher Prozesse betrachtet werden.

Digitale Nachweise ermöglichen die Erfüllung geltender Dokumentations- und Nachweispflichten insbesondere den Nachweis behördlicher Entscheidungen oder Geltendmachung von Ansprüchen aus

[13] Durchführungsverordnung (EU) 2015/1502 der Kommission vom 8. September 2015 zur Festlegung von Mindestanforderungen an technische Spezifikationen und Verfahren für Sicherheitsniveaus elektronischer Identifizierungsmittel gemäß Artikel 8 Absatz 3 der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt

Verträgen und anderen Rechtsgeschäften gegenüber Prüfbehörden, Gerichten und anderen vertrauenswürdigen Dritten. Hierzu sind durch digitale Nachweise regelmäßig die

- Integrität beinhaltet
    - Authentizität
    - Nachvollziehbarkeit
- Verfügbarkeit beinhaltet
    - Lesbarkeit/Nutzbarkeit
    - Verkehrsfähigkeit
- Vertraulichkeit

sicherzustellen und (insbesondere bei Authentizität und Integrität) nachzuweisen. Dabei sind die fachspezifischen Anforderungen des jeweiligen Anwendungsfalls (Aktenführungspflicht, maschinelle Auswertbarkeit etc.) zu beachten[14].

Diese Anforderungen sind bis zum Ablauf der geltenden Aufbewahrungsfristen sicherzustellen, was auch im Falle von SSI und der Nutzung von VC deren langfristige Bewahrung also Erhaltung der Information (Lesbarkeit/Nutzbarkeit) sowie des Beweiswerts nach dem Stand der Technik erfordert. Als Stand der Technik gilt hier in Deutschland die BSI TR-03125, die in der Version v1.2.2 auch hierfür angepasst vorliegt[15] und die eIDAS-Vorgaben durch digitalen Bewahrung nach Art. 34 und 40 eIDAS beinhaltet.

Dies gilt technologieunabhängig und insofern auch für SSI.[16] Im Ergebnis heißt dies, dass nur VC, bei denen Authentizität und Integrität bis zum Ablauf der Aufbewahrungsfristen eindeutig nachgewiesen werden können, auch einen verlustfreien digitalen Nachweis ermöglichen. Dies erfordert deren Verkehrsfähigkeit – also die Mittel für den Nachweis müssen sich am VC befinden. Dies bedeutet, die Signierung mittels einer qualifizierten elektronischen Signatur (Schriftform) oder qualifiziertem elektronischen Siegel (Bestätigung), wie dies auch in der eIDAS Bridge Spezifikationen der EU-Kommission vorgesehen ist.[17]

Für die Nachweisführung ist zu beachten, dass VC technisch im Kern nur ein Pendant zum Signaturzertifikat darstellen, mit dem Unterschied, dass sie Identitätseigenschaften bestätigen und nicht eine qualifizierte elektronische Signatur auslösen. Sie ersetzen jedoch nicht die elektronische Aktenführung oder den Nachweis in Form einer Studie, einer Dokumentation innerhalb einer Behörde

[14] Vgl. M. Weber et. al., 2018
[15] Vgl. BSI, 2021
[16] Vgl. DIN, 2020; T. Kusber et. al., 2020
[17] Vgl. European Commission, 2020

oder einen Antrag eines Bürgers oder Unternehmen. Vielmehr weist ein VC nur nach, dass ein Bürger oder Unternehmen über diesen Nachweis verfügt, also diese Eigenschaft (Führerschein, Abitur, Zahlungsfähigkeit etc.) nachweislich besitzt. Insofern umfassen die Nachweispflichten also das VC zzgl. der eigentlichen Daten (Bauantrag, Studie etc.).

SSI und eIDAS 2.0

Die fortgeschriebenen eIDAS-Verordnung eIDAS 2.0 schafft im Europäischen Wirtschaftsraum die regulatorische Grundlage für vertrauenswürdige, dezentrale selbstsouveräne digitale Identitäten. So wird jeder Mitgliedsstaat verpflichtet, seinen Einwohnern ein dezentrales European Digital Identity Wallet bereitzustellen. Diese Wallet gewährt dem Anwender die Hoheit über seine Kernidentität, die direkt im Wallet gespeichert ist. Damit wird eine aufwändige permanente Re-identifizierung, wie sie aktuell für digitale Transaktionen typisch ist, vermieden. Das Wallet ermöglicht dem Anwender die Anforderung, Bezug, Speicherung, Auswahl, Kombination und Teilen ihrer digitalen Identität und in transparenter wie prüfbarer Form selbstsouverän zu nutzen. Auch die Erzeugung qualifizierter elektronischer Signaturen mit Hilfe des European Digital Identity Wallet sollen möglich sein.

Das Wallet selbst wird LoA hoch erfüllen. Neben dem staatlichen (oder staatlich anerkannten) EU-Digital Wallet sind private denkbar, die gegen die notwendigen europäischen Standards zertifiziert sind.

Um eine europaweite Interoperabilität zu gewährleisten, sieht die eIDAS 2.0 vor, dass bis sechs Monate nach deren Inkrafttreten sog. Durchführungsrechtsakte durch die EU-Kommission erlassen werden, die wiederum auf europäische technische Standards von ETSI bzw. CEN verweisen. Ebenso beinhaltet die neue eIDAS eine verpflichtende Anerkennung des EU-Digital Wallet durch öffentliche Stellen, alle kritischen Infrastrukturen sowie die Internetgroßkonzerne[18] wie z.B. Google, Amazon, Meta oder Apple. Hinzu kommen Akzeptanzstellen, die entsprechend zertifiziert sind, dass sie die Anforderungen zum Zugriff auf das EU Digital Wallet erfüllen.

Darüber hinaus definiert die eIDAS 2.0 qualifizierte Attestation Services. Diese zertifizierten Vertrauensdiensteanbieter ermöglichen die vertrauenswürdige und damit nachweisbare Ausstellung von VC, kurz Attestations. Diese werden vom qualif. Attestation Services ausgestellt, so dass ein rechtssicherer Authentizitätsnachweis vorliegt. Eine wesentliche absehbare Aufgabe des Attestation Services wird es insofern sein, auch diejenigen Institutionen zu identifizieren, für deren Kunden der Attestation Service die Nachweise erzeugt hat. Auch hinsichtlich der Ausstellung von VC sieht die eIDAS

[18] Vgl. Art. 12 b Nr. 3 eIDAS 2 proposal

2.0 vor, dass bis sechs Monate nach deren Inkrafttreten sog. Durchführungsrechtsakte durch die EU-Kommission erlassen werden, die wiederum auf europäische technische Standards von ETSI bzw. CEN verweisen. Dies ist wesentlich, da nur zertifizierte Vertrauensdiensteanbieter VC ins EU-Digital Wallet ausstellen dürfen.

Ein durch einen Qualif. Attestation Services ausgestelltes VC wird also absehbar ein höheres Vertrauensniveau erreichen als ein selbst erstellter Nachweis.

Hinsichtlich SSI bleibt zu erwähnen, dass die eIDAS 2.0 keine Infrastruktur definiert. Es kann sich also um DLT oder auch eine andere PKI als technischer Grundlage der SSI handeln. Neben den Attestation Services sowie dem Wallet sieht die eIDAS 2.0 zudem qualif. Vertrauensdienste für elektronische Ledger vor, sodass auch eine vertrauenswürdige Nutzung von DLT ermöglicht wird.

Derzeit wird in der sogenannten „eIDAS Expert Group“, in die jeder Mitgliedstaat seine technischen Experten entsendet, an den technischen und regulatorischen Rahmenbedingungen gearbeitet. In verschiedenen Arbeitsgruppen werden Aspekte der neuen Regulierung besprochen und ausgearbeitet. Die europäischen Standardisierungsgremien ETSI und CEN sind in diesen Gruppen beteiligt. Auf diese Weise werden die technischen Rahmenbedingungen für eIDAS 2.0 geschaffen, auf die nach Inkrafttreten der eIDAS 2.0, die nach 6 oder 12 Monaten folgenden Durchführungsrechtsakte verweisen werden.

Servicekonten für natürliche Personen

Seitens Bund und Ländern werden aktuell die Nutzerkonten für natürliche Personen aufgebaut und zum Portalverbund zusammengeschlossen. Ziel ist es, von einem Nutzerkonto, in demjenigen des Bundes (bund*ID*) oder dem des jeweiligen Bundeslandes, alle digitalen Verwaltungsleistungen, die im Portalverbund verfügbar sind, nutzen zu können.

Die Identifizierung und Authentisierung, auf einem entsprechenden LoA (hoch), ist derzeit nur mit elektronischem Personalausweis möglich, digitale Nachweise werden im PDF übertragen.

Servicekonto für juristische Personen (Organisationen)

Über die Paragraphen §2 und §3 des Gesetzes zur Verbesserung des Onlinezugangs zu Verwaltungsleistungen (Onlinezugangsgesetz - OZG) wird ein einheitliches Konto für Organisationen – insbesondere Unternehmen ermöglicht. Der IT-Planungsrat hat die Länder Bayern und Bremen mit dem Aufbau und Betrieb des „einheitlichen Unternehmenskontos“ beauftragt. Unter dem einheitlichen Brand „Mein Unternehmenskonto“ (UK) wird ein zentraler Dienst für alle Bundesländer und den Bund aufgebaut. Bereitgestellt durch die Länder Bayern und Bremen umfasst „Mein Unternehmenskonto“ sechs unterschiedliche Bausteine, die von der Identifizierung und der

Autorisierung bis hin zu umfangreichen Postfachfunktionen reichen. Für Identifizierung und Authentisierung wir die sogenannte NEZO-Schnittstelle angeboten. Mit Hilfe einer Rollen- und Rechteverwaltung kann der Zugriff gesteuert werden.

VC können auch das Attribut „Ist ermächtigt“ oder „hat Prokura“ beinhalten

VC können die derzeit bestehende Herausforderung lösen, ob eine Person für ein Unternehmen handlungsberechtigt ist. Hierzu würde nur von einem Issuer (qualif. Attestation Service in eIDAS 2.0) nach Prüfung einer vertrauenswürdigen Datenquelle (trusted sources gem. eIDAS 2.0) z.B. des Handelsregisters, einer natürlichen Person ein Credential für die Prokura in deren Wallet ausgestellt. Im Ergebnis kann diese nicht nur am Unternehmenskonto, sondern bei jedem digitalen Service ihre Handlungsberechtigung nachweisen. Selbiges ließe sich ebenso auf Maschinen oder Fahrzeuge übertragen: Das Fahrzeug kann ebenso ein Wallet besitzen. In dieses wird von einem Issuer die Zuordnung zum Eigentümer sowie die Berechtigung eingetragen z.B. bis zu einer bestimmten Höhe Strom aufzunehmen oder zu parken. Im Ergebnis kann die Ladesäule oder das Parkhaus vollständig autonom genutzt werden – die Abrechnung erfolgt gegenüber dem verantwortlichen Unternehmen/Bürger. Damit wird die Vision, eine Identität mit allen notwendigen Attributen für alle Services Wirklichkeit:

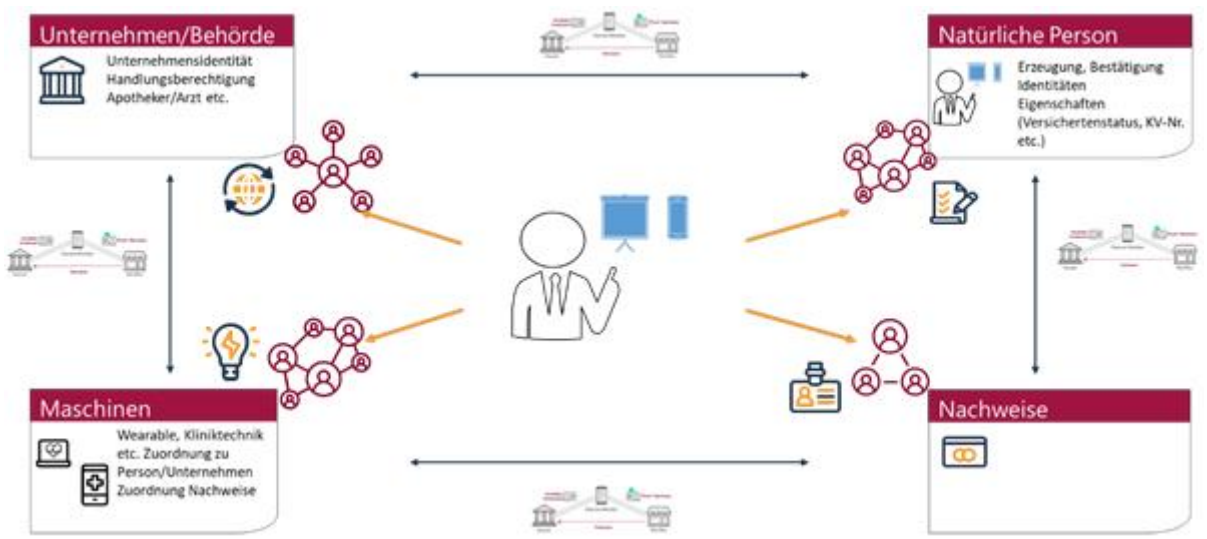

Abbildung 5: Vision einer Identität mit allen notwendigen Attributen für alle Services

8. Wo grenzt sich SSI von Once Only ab, wo ergänzen sich SSI und Once Only?

Der durchgehende Weg in die Digitalisierung führt über moderne eGovernment Anwendungen, die einfach durch Bürger und Organisationen genutzt werden können. Vor diesem Hintergrund stehen immer häufiger Aspekte wie Benutzerfreundlichkeit bei der Neugestaltung oder Überarbeitung von

Anwendungen im Fokus. Von der durchgehenden Nutzung vollständig digitalisierter Prozesse profitieren Bürger und Unternehmen genauso wie die öffentliche Verwaltung selbst.

Dass Bürger und Organisationen Unterlagen und Nachweise im Verwaltungshandeln beibringen müssen, deren Informationen entweder der Verwaltung bereits vorliegen oder die sogar von der Verwaltung selbst stammen, widerspricht nicht nur dem Grundsatz der Benutzerfreundlichkeit; dieses Vorgehen steigert den personellen und wirtschaftlichen Aufwand auf beiden Seiten und verringert die Sicherheit des Gesamtsystems z.B. dadurch, dass Fälschungen eingebracht werden könnten. Das Once-Only Prinzip adressiert genau diesen Umstand und fordert prinzipiell, den Abruf von Daten aus den Systemen der Verwaltung der Einreichung von Unterlagen vorzuziehen, wenn die Daten der öffentlichen Verwaltung vorliegen. Im Once-Only Prinzip wurden neue Ansätze, wie SSI noch nicht betrachtet, da diese zu dem Zeitpunkt, an dem die Prinzipien definiert wurden, praktisch nicht verfügbar waren. In diesem Abschnitt wollen wir daher die Ansätze gegenüberstellen.

Once-Only-Principle (OOP)

Für einige Registerabfragen existieren bereits etablierte Verfahren (z.B. Auskünfte aus dem Melderegister, Abruf der Renteninformationen) für andere sind die Verfahren unbekannt oder existieren nicht. Bisher ist bei allen Abfragen die Voraussetzung zu schaffen, dass eine gesetzliche Grundlage existiert, die eine Behördenkommunikation ohne explizite Zustimmung des Bürgers erlaubt. Auskünfte, die ihre Rechtsgrundlage nur auf der Basis einer Zustimmung eines Benutzers herleiten, sind aktuell nicht umgesetzt.

Um das OOP durchgehend in den Verwaltungsverfahren umsetzen zu können, müssen Registerauskünfte auch auf der Basis einer Zustimmung eines Bürgers ermöglicht werden. Dies auch grenzüberschreitend zu ermöglichen, ist unter anderem ein Ziel der Single-Digital Gateway Verordnung (“SDG-VO”). Für die Umsetzung wird ein Once Only Technical System (“OOTS”) definiert. Dieses technische System wird über den Artikel 14 der SDG-VO gefordert. Die Spezifikationen des OOTS setzen auf Ergebnissen europäischer Vorprojekte (Connecting Europe Facility - CEF - Building Blocks und „The Once Only Principle“ - TOOP-Projekt) auf und werden zwischen den Mitgliedstaaten und der EU-Kommission aktuell festgeschrieben. Mittels der Nutzung des OOTS wird die grenzüberschreitende Nachweis-Datenübermittlungen realisiert, die für die erfolgreiche Bearbeitung von Online-Verwaltungsverfahren innerhalb der EU erforderlich ist. Ab Ende 2023, so will es der Gesetzgeber, sollen die Dienste der Verwaltung online verfügbar und Once-Only grenzüberschreitend möglich sein. Gestützt wird die deutsche Umsetzung durch das Registermodernisierungsgesetz (“RegMoG”). Über das RegMoG kann die Bundesregierung das "Once-Only"-Prinzip verwirklichen. Bereits in Registern

gespeicherte Angaben und Nachweise müssen dann nicht immer wieder aufs Neue vorgelegt werden”[19].

Regelmäßig die gleichen Nachweise immer wieder zu erbringen, wird so also nicht mehr die Aufgabe des Bürgers sein, das gilt für papierhafte genauso wie für elektronische Nachweise. Über RegMoG und SDG-VO wird ein Bürger dann davon entlastet, Papier- oder elektronische Dokumente regelmäßig neu einzureichen.

Spielen SSI und Wallets dann bei Once-Only gar keine Rolle?

Es wird erwartet, dass SSI durch die Revision der eIDAS-Verordnung in den Kontext gesetzlicher Regulierungen gestellt werden wird. Im Rahmen einer “EU eID Wallet” sollen perspektivisch, zusätzlich zur eigentlichen Benutzeridentifikation, auch (qualifizierte) elektronisch attestierte Attribute das Anwendungsfeld von eIDAS erweitern. Diese Gesetzesinitiativen der Europäischen Kommission zur Etablierung von SSI-Prinzipien und die oben skizzierte SDG-VO schaffen ein großes Potential sich gegenseitig zu unterstützen. Aus regulatorischer Sicht kommt die Revision der eIDAS-VO zu spät, um bereits jetzt im OOTS Berücksichtigung zu finden, aber perspektivisch sollen beide Infrastrukturen voneinander profitieren. Denn hier kann die Verwaltung ja sowohl als Anbieter für attestierte Attribute auftreten, als auch als Konsument von elektronisch attestierten Attributen.

Aus Sicht der Behörden können Antragsprozesse immer dann durch den Einsatz von SSI beschleunigt werden, wenn die Nachweise nicht bereits aus einem Register abgerufen werden können. Auch könnten digitale Nachweise als Ergebnis von Online-Leistungen bereits im Zuge der OZG-Erfüllung ausgestellt werden. Diese digitalen Nachweise könnten bei weiteren Online-Leistungen bereits in der Antragsstellung als VC berücksichtigt werden. Hier wird die Schnittmenge der beiden Ansätze OOP und SSI deutlich. Es können über beide Lösungsansätze system- und medienbruchfreie Antragsprozesse realisiert werden, die Behörden eine schnelle und sichere Antragsbearbeitung ermöglichen. Auf der anderen Seite stehen beide Ansätze vor ähnlichen Herausforderungen, wie zum Beispiel die Vereinheitlichung der Nachweise – syntaktisch und semantisch. Ein einheitlicher Katalog von Nachweisen, die europaweit nutz- und verstehbar sind, ist daher für beide Lösungsansätze ein entscheidender Erfolgsfaktor.

Viele Fragen sind zwar noch offen, sowohl technischer als gesetzlicher Natur, aber die EU-Kommission schafft Arbeitsgruppen und bietet Seminare an, damit die Zusammenarbeit klappt und die Digitalisierung europaweit an großes Stück vorankommt.

[19] Vgl. Bundesministerium des Inneren und für Heimat, 2021

SSI kann also komplementär zu Once-Only Synergien sowohl für Bürger als auch für Unternehmen, Organisationen und Behörden schaffen.

9. Fazit

Durch die Hoheit über seine Daten und deren Weitergabe lassen sich Anwendungsbereiche regulatorisch einfacher implementieren. Dies macht jedoch die Einbindung vertrauenswürdiger Dritter nicht obsolet.

Durch die Nutzung einer Wallet können Bürger ihre digitalen Identitäten und Nachweise im Behördenkontakt ebenso einsetzen wie im privatwirtschaftlichen Umfeld. Als Ergänzung zu dem bereits mit der Online-Ausweisfunktion möglichen Einsatz bieten die Speicherung und auch Verwendung der Nachweise einen entscheidenden Vorteil für die Abwicklung von Geschäftsprozessen. Ein kritischer Erfolgsfaktor wird die Verfügbarkeit von Anwendungen sein, die die digitale Identität und die Nachweise akzeptieren.

Die Nutzung von Online-Leistungen durch Bürger unterscheidet sich von der Nutzung durch Unternehmen und Organisationen insbesondere hinsichtlich ihrer Häufigkeit. Unternehmen und Organisation agieren grenzübergreifend und sind im Austausch mit Bürgern, anderen Unternehmen sowie Behörden aus verschiedenen Ländern. Eine Wallet ermöglicht diesen Unternehmen und Organisationen den intersektoralen (Business-to-Business, Business-to-Government, Business-to-Customer) und EU-weiten Austausch von digitalen Nachweisen in einem einheitlichen Format.

SSI kann den Austausch von digitalen Nachweisen in der EU für Bürger sowie Unternehmen und Behörden vereinfachen.

Die EU hat die Chancen erkannt und stellt mit der Empfehlung zur eIDAS Novellierung und gezielten Fördermaßnahmen die Weichen. Details werden noch in den jeweiligen Gremien diskutiert.

Lösung bekannter Probleme, wie bspw. Prokura und Vertretungsberechtigungen können sehr leicht nachgewiesen werden. Offen sind noch die Langzeitaufbewahrung und Prüfbarkeit.

Wenn die Anforderungen der Regulatorik umgesetzt sind, können SSI-Wallets auch die eID im Vertrauensniveau „hoch“ beinhalten und interoperabel agieren; dies kann Servicekonten hinsichtlich ihrer Funktion als Identifizierungs- und Authentifizierungskomponente ergänzen.

Literaturverzeichnis

Allen, C., 2016. *The Path to Self-Sovereign Identity.* [Online]
Available at: http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html
[Accessed 10 03 2022].

Amtsblatt der Europäischen Union, 2014. *eIDAS.* [Online]
Available at: http://data.europa.eu/eli/reg/2014/910/oj

Amtsblatt der Europäischen Union, 2016. *Datenschutz-Grundverordnung.* [Online]
Available at: http://data.europa.eu/eli/reg/2016/679/oj

Bastian, P. et al., 2021. Self-Sovereign Identity - Vertrauensbasis für selbstbestimmte Identitätsnetzwerke. In: *Deutschland. Digital. Sicher..* Bonn: Bundesamt für Sicherheit in der Informationstechnik.

Bundesamt für Sicherheit in der Informationstechnik, 2014. *BSI Technische Richtline 03107-2: Elektronische Identitäten und Vertrauensdienste im E-Government,* Bonn: Bundesamt für Sicherheit in der Informationstechnik.

Bundesamt für Sicherheit in der Informationstechnik, 2018. *BSI Technische Richtlinie 03147: Vertrauensniveaubewertung von Verfahren zur Identitätsprüfung natürlicher Personen,* Bonn: Bundesamt für Sicherheit in der Informationstechnik.

Bundesamt für Sicherheit in der Informationstechnik, 2019. *BSI Technische Richtlinie 03107-1: Elektronische Identitäten und Vertrauensdienste im E-Government,* Bonn: Bundesamt für Sicherheit in der Infromationstechnik.

Bundesamt für Sicherheit in der Informationstechnik, 2020. *Leitlinie für digitale Signatur-, Siegel-, Zeitstempel- formate sowie technische Beweisdaten (Evidence Record),* Bonn: Bundesamt für Sicherheit in der Informationstechnik.

Bundesamt für Sicherheit in der Informationstechnik, 2021. *BSI Technische Richtlinie 03125 (TR-ESOR) - Beweiswerterhaltung kryptographisch signierter Dokumente,* Bonn: Bundesamt für Sicherheit in der Informationstechnik.

Bundesministerium des Inneren und für Heimat, 2021. *Registermodernisierungsgesetz verkündet.* [Online]
Available at:
https://www.bmi.bund.de/SharedDocs/pressemitteilungen/DE/2021/04/registermodernisierungsgesetz-verkuendet.html
[Accessed 11 02 2022].

Bundesministerium des Innern und für Heimat, 2017. *OZG im Wortlaut - Das Onlinezugangsgesetz (OZG).* [Online]
Available at: https://www.onlinezugangsgesetz.de/Webs/OZG/DE/grundlagen/info-ozg/info-ozg-wortlaut/ozg-im-wortlaut-node.html
[Accessed 11 02 2022].

Deutsches Institut für Normung, 2021. *DIN/TS 31648:2021-04 - Kriterien für vertrauenswürdige Transaktionen - Records Management und Beweiswerterhaltung in Distributed Ledger Technologien und Blockchain,* Berlin: Beuth Verlag GmbH.

Ehrlich, T., Richter, D., Meisel, M. & Anke, J., 2021. *Self-Sovereign Identity als Grundlage für universell einsetzbare Identitäten.* s.l., s.n.

European Commission, 2020. *eIDAS Bridge. Use cases and technical specifications.* [Online]
Available at: https://joinup.ec.europa.eu/sites/default/files/document/2020-04/SSI%20eIDAS%20Bridge%20-%20Use%20cases%20and%20Technical%20Specifications%20v1.pdf
[Accessed 11 02 2022].

European Commission, 2021a. *EMPFEHLUNG (EU) 2021/946 DER KOMMISSION vom 3. Juni 2021 für ein gemeinsames Instrumentarium der Union für ein koordiniertes Herangehen an einen Rahmen für die europäische digitale Identität,* Brüssel: Amtsblatt der Europäischen Union.

European Commission, 2021b. *European Digital Identity.* [Online]
Available at: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_en

Kubach, M., Schunck, C. H., Sellung, R. & Roßnagel, H., 2020. Self-Sovereign and Decentralized identity as the future of identity management?. In: *Open Identity Summit.* Bonn: Gesellschaft für Informatik.

Kusber, T., Schwalm, S., Shamburger, K. & Korte, U., 2020. Criteria for trustworthy digital transactions – Blockchain/DLT between eIDAS, GDPR, Data and Evidence Preservation. In: *OpenIdentity Summit.* Bonn: Gesellschaft für Informatik, pp. 49-60.

Weber, M., Schwalm, S., Vogt, T. & Krogel, W., 2018. *Records Management nach ISO 15489.* Berlin: Beuth.