Dezentrale Identifikatoren (DIDs)

Die nächste PID-Evolution: selbstsouverän, datenschutzfreundlich, dezentral

Nicolas Bach, Student, Hochschule der Medien Stuttgart

Zusammenfassung

Dieser Beitrag behandelt den zuletzt vom W3C hervorgebrachten Standard für dezentrale Identifikatoren (Decentralized Identifiers, kurz: DIDs) in Bezug auf den Bereich des Forschungsdatenmanagements. Es wird dargelegt, dass die aktuell im wissenschaftlichen Publikationswesen häufig verwendeten persistenten Identifikatorensysteme (Persistent Identifiers, PIDs) wie Handle, DOI, ORCID und ROR aufgrund ihrer Zentralisierung fundamentale Probleme hinsichtlich der Datensicherheit, dem Datenschutz und bei der Sicherstellung der Datenintegrität aufweisen. Dem werden als mögliche Lösung das System der DIDs gegenübergestellt: eine neuartige Form von weltweit eindeutigen Identifikatoren, die durch jedes Individuum oder jede Organisation selbst generiert und auf jeder als vertrauenswürdig erachteten Plattform betrieben werden können. Blockchains oder andere Distributed-Legder-Technologien können dabei als vertrauenswürdige Datenregister fungieren, aber auch direkte Peer-to-Peer-Verbindungen, auf bestehende Internetprotokolle aufsetzende Methoden oder statische DIDs sind möglich. Neben dem Schema wird die technische Spezifikation im Sinne von Datenmodell und die Anwendung von DIDs erläutert sowie im Vergleich die Unterschiede zu zentralisierten PID-Systemen herausgestellt. Zuletzt wird der Zusammenhang mit dem zugrundeliegenden neuen Paradigma einer dezentralen Identität, der Self-Sovereign Identity, hergestellt. SSI repräsentiert ein gesamtes Ökosystem, in dem Entitäten ein kryptografisch gesichertes Vertrauensnetzwerk auf der Basis von DIDs und digitalen Identitätsnachweisen bilden, um dezentral manipulationsgesichert und datenschutzgerecht identitätsbezogene Daten auszutauschen. Zum Schluss der Abhandlung stellt der Autor fünf zuvor herausgearbeitete Anforderungen in Bezug auf eine zeitgemäße Umsetzung von persistenten Identifikatoren vor.

Summary

This paper discusses the latest W3C standard for decentralized identifiers (DIDs) with respect to research data management. It is shown that due to their centralization, persistent identifier systems (PIDs) currently used in scientific publishing, such as Handle, DOI, ORCID, and ROR, involve fundamental problems with regard to data security, data privacy and data integrity. This is contrasted with DIDs as a possible solution, a new form of globally unique identifiers that can be generated by any individual or organization and operated on any platform deemed trustworthy. Blockchains or other distributed ledger technologies can act as verifiable data registries, but direct peer-to-peer connections, methods built on existing Internet protocols, or static DIDs are also possible. In addition to the scheme, the technical specification in terms of the data model and the usage of DIDs are explained. The differences in comparison to centralized PID systems are outlined as well. Finally, the connection to the underlying new paradigm of a decentralized identity, called Self-Sovereign Identity, is shown. SSI represents an entire ecosystem in which entities form a cryptographically secured trust network based on DIDs and digital proofs of identity to exchange identity-related data in a decentralized, tamper-proof, and privacy-preserving manner. The author concludes by

presenting five requirements derived from the discussion related to a state-of-the-art approach to the implementation of persistent identifiers.

Zitierfähiger Link: https://doi.org/10.5282/o-bib/5755

Schlagwörter: Persistent Identifier, Dezentralisierung, Privatsphäre, Manipulationssicherheit, Forschungsdatenmanagement, Self-Sovereign Identity

1. Status quo: Zentrale Identifikatorensysteme

Identifikatoren sind inzwischen im Forschungsdatenmanagement nicht mehr wegzudenken, als Querschnittsthema sind sie hierbei in allen Phasen bedeutsam.[1] In Forschungsdatenrepositorien werden Forschungsdaten mit persistenten Identifikatoren (Persistent Identifiers, kurz: PIDs) versehen, um die dauerhafte Zugänglichkeit sicherzustellen.[2] Ein PID wird dabei allgemein definiert als ein „dauerhafter, digitaler Identifikator, bestehend aus Ziffern oder alphanumerischen Zeichenfolgen, welcher einem Datensatz (oder einem anderen digitalen Objekt) zugeordnet wird".[3] PIDs werden auch in den für die Veröffentlichung von Forschungsdaten oft vorausgesetzten FAIR-Prinzipien an erster Stelle unter „to be Findable" genannt: „F1. (meta)data are assigned a globally unique and eternally persistent identifier".[4]

Laut den Erhebungen von Scholze et al., die mit Stand Juli 2020 die im größten internationalen Verzeichnis re3data über 2500 eingetragenen Repositorien näher betrachtet haben, nutzen 46 Prozent davon persistente Identifikationssysteme wie z.B. DOI (Digital Object Identifier), Handle oder URN (Uniform Resource Name).[5]

Um das Erfordernis von dezentralen Identifikatoren (Decentralized Identifiers, kurz: DIDs) zu verstehen, muss zuerst auf diese aktuell im wissenschaftlichen Publikationswesen etablierten Identifikatorensysteme eingegangen werden. In einem späteren Abschnitt werden deren Schwächen herausgestellt und diesen schließlich das System der DIDs gegenübergestellt.

1 Dierkes, Jens: Planung, Beschreibung und Dokumentation von Forschungsdaten, in: Putnings, Markus; Neuroth, Heike; Neumann, Janna (Hg.): Praxishandbuch Forschungsdatenmanagement, Berlin/Boston 2021, S. 305. Online: <https://doi.org/10.1515/9783110657807-018>.

2 Pampel, Heinz; Elger, Kirsten: Publikation und Zitierung von digitalen Forschungsdaten, in: Putnings, Markus; Neuroth, Heike; Neumann, Janna (Hg.): Praxishandbuch Forschungsdatenmanagement, Berlin/Boston 2021, S. 523. Online: <https://doi.org/10.1515/9783110657807-028>.

3 Scholze, Frank; Ulrich, Robert; Goebelbecker, Hans-Jürgen: Wissenschaftlicher Datenmarkt, in: Putnings, Markus; Neuroth, Heike; Neumann, Janna (Hg.): Praxishandbuch Forschungsdatenmanagement, Berlin/Boston 2021, S. 170. Online: <https://doi.org/10.1515/9783110657807-009>.

4 FORCE11: The FAIR Data Principles, force11.org, 2016, <https://www.force11.org/group/fairgroup/fairprinciples>, Stand: 15.07.2021. (Hervorhebungen im Original)

5 Scholze; Ulrich; Goebelbecker, Hans-Jürgen: Wissenschaftlicher Datenmarkt, 2021, S. 167–171.

1.1. PIDs für Publikationen

PIDs sind für Publikationen erforderlich geworden, da URLs, auf denen diese hochgeladen sind:

- sich ändern können, z.B. indem sie verschoben werden;
- nicht eindeutig sind, weil Publikationen auf mehreren Servern mit unterschiedlichen URLs hochgeladen werden können und somit schwer zitierfähig werden;
- keine Neutralität gewährleisten, da sie häufig semantische Hinweise auf die Domain enthalten.[6]

DOI, das Handle-System und URN sind die aktuell gängigsten Identifikationssysteme für Veröffentlichungen. Den Erkenntnissen von Scholze et al. zufolge sind auch im Bereich der Forschungsdaten DOI und Handle am meisten verbreitet.[7]

Das Handle-System wurde 1995 maßgeblich durch Robert Kahn, einem der „Väter des Internets", und Robert Wilensky konzeptioniert und wird seither zentral durch die Corporation for National Research Initiatives (CNRI) betrieben.[8] Kommerzielle Handle-Lizenzen müssen von Forschungseinrichtungen und institutionellen Repositorien erworben werden, um lokale Handle-Systeme einrichten zu können[9], ein Beispiel dafür ist in der europäischen Forschungslandschaft etwa das European Persistent Identifier Consortium (ePIC)[10]. Handle wird inzwischen auch als Basis für andere übergeordnete Systeme wie DOI verwendet.

DOI basiert auf der Kombination eines eigens entwickelten Metadatenmodells und dem Resolving durch das Handle-System. Die Gründung des DOI-Systems geht auf die gemeinsame Initiative von drei US-amerikanischen Fachverbänden der Verlagsbranche zurück: der International Publishers Association; der International Association of Scientific, Technical and Medical Publishers und der Association of American Publishers. Im Jahr 1997 wurde es auf der Frankfurter Buchmesse vorgestellt und wird seitdem durch die dafür begründete International DOI Foundation (IDF) zentral betrieben und weiterentwickelt. Das DOI-System wurde im November 2010 als ISO-Standard anerkannt und zwei Jahre später unter der ISO 26324:2012[11] veröffentlicht. Für die Vergabe von Identifikatoren sind DOI-Registrierungsagenturen verantwortlich. Die IDF wird ihrerseits von den Mitgliedern der Registrierungsagenturen kontrolliert. Zu den bekanntesten Agenturen im wissenschaftlichen Bereich zählen DataCite und Crossref. Die Vergabe von DOIs ist üblicherweise mit einer Gebühr verbunden, die vom Geschäftsmodell der Registrierungsagentur abhängt. Das Resolving von DOIs ist hingegen kostenlos und nicht von der Agentur abhängig, weil es über Handle abgewickelt wird.[12]

6 Universität Konstanz: Persistente Identifikatoren, forschungsdaten.info, 2021, <https://www.forschungsdaten.info/themen/veroeffentlichen-und-archivieren/persistente-identifikatoren/>, Stand: 15.07.2021.
7 Scholze; Ulrich; Goebelbecker, Hans-Jürgen: Wissenschaftlicher Datenmarkt, 2021, S. 170.
8 Sun, Sam X.; Lannom, Larry; Boesch, Brian.: Handle System Overview, Request for Comments: 3650, Internet Society, 2003, S. 18. Online: <https://www.rfc-editor.org/rfc/rfc3650.txt>.
9 Corporation for National Research Initiatives: Prefix Registration, handle.net, 2018, <https://www.handle.net/prefix.html>, Stand: 15.07.2021.
10 https://www.pidconsortium.net
11 https://www.iso.org/standard/43506.html
12 International DOI Foundation: 1 Introduction, DOI Handbook, 2015, <https://www.doi.org/doi_handbook/1_Introduction.html>, Stand: 15.07.2021.

Die DOI-Vergabe für deutsche Einrichtungen übernehmen die deutschen Mitglieder von DataCite: GESIS, TIB, ZB MED und ZBW.[13]

URNs wurden ursprünglich 1994 in der Internet Community vorgestellt, um eine abstrakte Ressource selbst zu bezeichnen, während URLs die Ressource lokalisier- und auffindbar machen sollen.[14] Im Jahr 1997 wurden sie schließlich formalisiert[15] und sind heute durch das W3C (World Wide Web Consortium) und die IETF (Internet Engineering Task Force) standardisiert[16]. URN-Namensräume müssen bei der zentralen Internet Assigned Numbers Authority (IANA) beantragt und durch diese genehmigt werden. Es gibt keine zentrale Verwaltung oder zentrale Infrastruktur für das Resolving und es werden auch keine Lizenzkosten für die Vergabe von URNs erhoben. URN-Registrierungsagenturen müssen selbst die Infrastruktur für die Vergabe und das Resolving in ihrem Namensraum stellen.[17] Das URN-System wird unter dem Namensraum *urn:nbn:* (Uniform Resource Names for National Bibliography Numbers) hauptsächlich von wissenschaftlichen Bibliotheken in Europa verwendet und verstärkt von der deutschen und schweizerischen Nationalbibliothek vorangetrieben, zumal diese etwa massenhaft URNs bei der Pflichtablieferung von Netzpublikationen oder E-Books vergeben[18]. Für wissenschaftliche Publikationen im deutschsprachigen Raum vergibt die DNB kostenlos URNs im Namensraum *urn:nbn:de*.[19]

1.2. PIDs für Personen

Für in der Forschung tätige Personen braucht es PIDs wiederum unbedingt, weil:

- diese sonst bei Institutionswechseln durch zeitlich begrenzte Tätigkeiten schwer auffindbar sind;
- durch Namensgleichheit, Namenswechsel, Namensansetzungen oder langer Inaktivität eine eindeutige Identifikation erschwert wird.[20]

Maßgeblich durchgesetzt hat sich hier im wissenschaftlichen Bereich inzwischen die ORCID (Open Research and Contributor ID).

13 Universität Konstanz: Persistente Identifikatoren, 2021.
14 Sollins, Karen; Masinter, Larry: Functional Requirements for Uniform Resource Names, Request for Comments: 1737, Internet Society, 1994, S. 1. Online: <https://www.rfc-editor.org/rfc/rfc1737.txt>.
15 Moats, Ryan: URN Syntax, Request for Comments: 2141, Internet Society, 1997. Online: <https://www.rfc-editor.org/rfc/rfc2141.txt>.
16 W3C: URIs, URLs, and URNs: Clarifications and Recommendations 1.0, W3C Note, 2001, <https://www.w3.org/TR/uri-clarification/>, Stand: 15.07.2021.
17 Daigle, Leslie L.; Gulik, Dirk-Willem van; Iannella, Renato; Faltstrom, Patrick: Uniform Resource Names (URN) Namespace Definition Mechanisms, Request for Comments: 3406, Internet Society, 2002, S. 3–4. Online: <https://www.rfc-editor.org/rfc/rfc3406.txt>.
18 Deutsche Nationalbibliothek: URN-Service, dnb.de, 2021, <https://www.dnb.de/DE/Professionell/Services/URN-Service/urn-service_node.html>, Stand: 15.07.2021.
19 Universität Konstanz: Persistente Identifikatoren, 2021.
20 Ebd.

Eine ORCID-ID [sic!] wird mittels einer kostenlosen Selbstregistrierung über die zentrale Web-Domain orcid.org von der betreffenden Person selbst angelegt. In einem dazugehörigen ORCID-Profil können dann über die Website oder eine spezielle Schnittstelle (API) etwa Orte der Anstellung und Publikationen eingetragen werden.[21] Seit Anfang 2019 werden ORCID-IDs außerdem in die Gemeinsame Normdatei (GND) der DNB eingespielt[22], im Dezember 2020 wurde dabei die 100.000ste ORCID-ID in einem Personendatensatz verknüpft[23]. Hinter ORCID steht eine 2012 gegründete weltweite Non-Profit-Organisation, die sich aus den Beiträgen ihrer Mitglieder finanziert.[24] Zu den Gründungsmitgliedern gehören sowohl wissenschaftliche Verlagsgrößen wie Elsevier, die Nature Publishing Group und Wiley als auch reputable Forschungsinstitutionen wie beispielsweise das MIT und CERN.[25]

1.3. PIDs für Organisationen

Auch für wissenschaftliche Einrichtungen, die oftmals als Affiliation bei forschenden Personen mit Erwähnung finden, braucht es eindeutige Bezeichner, allein um den Umstand der verschiedenen Schreibweisen und Sprachbarrieren auf internationaler Ebene zu bewältigen.

Der Bereich wird derzeit dominiert von im kommerziellen Verlagswesen angesiedelten Anbietern wie Ringgold, Scopus (Elsevier) und Web of Science (Clarivate), die alle im Wissenschaftsbereich stark etabliert sind und eindeutige Identifikatoren ausschließlich innerhalb ihrer hinter Bezahlschranken verborgenen Fachdatenbanken vergeben.

Als eine der wenigen vollkommen offenen Lösungen erlangt die ROR (Research Organization Registry) zunehmend weltweite Popularität. Diese ging Anfang 2019 aus der im Jahr 2016 gegründeten Org-ID-Initiative hervor, an der auch Crossref, DataCite und ORCID beteiligt waren. ROR verfolgt momentan einen Minimalansatz der zu erfassenden Organisationsdaten: Es werden nur der Name der Einrichtung in englischer Sprache samt seiner Namensvarianten, URL, andere Identifikatoren, Land und Einrichtungstyp erfasst.[26]

Betrieben wird ROR aktuell durch die California Digital Library, Crossref und DataCite, beraten durch eine größere Steuerungsgruppe weiterer Wissenschafts- und Bibliotheksorganisationen, auf einem zentralen Amazon Web Services-Server in Irland.[27] Die Organisationsdaten werden ausschließlich durch die ROR selbst kuratiert und auf ror.org veröffentlicht. Organisationen müssen Neueinträge

21 ORCID: Benefits for Researchers, info.orcid.org, 2020, <https://info.orcid.org/benefits-for-researchers/>, Stand: 15.07.2021.
22 Deutsche Nationalbibliothek: Normdaten in der Wissenschaft – Vernetzung von GND und ORCID, dnb.de, 2020, <https://www.dnb.de/DE/Professionell/ProjekteKooperationen/projekteKoop_node.html#sprg446188>, Stand: 15.07.2021.
23 Schrader, Antonia: 100.000 GND-Personendatensätze mit ORCID-Records verknüpft!, ORCID DE, 2020, <https://www.orcid-de.org/100000-gnd-orcid-verknuepft/>, Stand: 15.07.2021.
24 ORCID: About, info.orcid.org, 2021, <https://info.orcid.org/what-is-orcid/>, Stand: 15.07.2021.
25 ORCID: Board of Directors, about.orcid.org, 2012, <https://web.archive.org/web/20120909022005/http://about.orcid.org/board-of-directors>, Stand: 15.07.2021.
26 Vierkant, Paul: Was ist das Research Organization Registry (ROR)?, ORCID DE, 2020, <https://www.orcid-de.org/was-ist-das-research-organization-registry-ror/>, Stand: 15.07.2021.
27 ROR: Facts, ror.org, o. D., <https://ror.org/facts/>, Stand: 15.07.2021; DomainTools: Whois Record for ror.org, Whois Lookup, o. D., <https://whois.domaintools.com/ror.org>, Stand: 15.07.2021.

und Änderungsmeldungen über ein auf der Website verlinktes Google Docs-Formular unter Angabe ihrer Kontaktdaten einreichen.[28] Richtlinien und Verfahren zur Verwaltung der Daten sollen in der nächsten Stufe des Projekts konkretisiert werden.[29]

Die von Digital Science seit 2015 betriebene Global Research Identifier Database (GRID), die unter den selben Voraussetzungen (Offenheit und Interoperabilität) wie ROR operierte und ihr ursprünglich als Datenbasis diente, hat für das vierte Quartal 2021 ihre Einstellung zugunsten des Weiterbetriebs der ROR angekündigt.[30]

1.4. Schwächen zentraler Identifikatorensysteme

Aus den vorangegangenen Darstellungen etablierter Identifikatorensysteme lassen sich bereits die wesentlichsten Kritikpunkte ableiten.

Das maßgebliche Problem ist, dass Identifikatoren wie DOI, Handle, ORCID oder ROR in einer zentralen Datenbank unter Verantwortung einer zentralen Autorität (z.B. einer Dach- oder federführenden Organisation oder einer beauftragten Registrierungsagentur) gespeichert werden.

Die Zunahme von Daten-Leaks der letzten Jahre zeigt eindeutig, dass zentrale Datenbanken riesige potenzielle Gefahrenquellen für ihre Nutzer*innen darstellen.[31] Vor allem im Fall eines Resolving-Dienstes, der auf Abruf URLs ausliefert, ist ein besonderes Gefahrenpotenzial gegeben: Für Nutzer*innen ist hier im Vorhinein schlicht nicht erkennbar, ob die URL hinter einem Identifikator Schadsoftware oder ähnliche kompromittierende Inhalte enthalten könnte.

Hier offenbart sich ein fundamentaler Denkfehler in dem Ansatz konventioneller PID-Dienste: Diese sind selbst nur per URL über das Web erreichbar. Würden die Domains doi.org, handle.net, orcid.org oder ror.org entweder durch einen Serverausfall oder im schlimmsten Fall durch böswilliges Domain-Hijacking[32] nicht mehr erreichbar sein, sind die damit verbundenen Identifikatoren unbrauchbar oder sogar schädlich. Das Konzept der zentralen Identifikatorensysteme ersetzt somit nur eine Abhängigkeit (sich verändernde URLs) mit einer neuen Abhängigkeit (zentralisierte web-basierte PID-Dienste).

Hinzu kommt noch die Problematik, dass jeder Anbieter eines Identifikatorensystems seine eigenen Sicherheits- und Datenschutzrichtlinien festlegt, denen die Nutzer*innen des Systems unterliegen. Entsprechend hat der Sitz der Organisation eine bedeutende Auswirkung darauf, ob die strikten Datenschutzvorgaben der europäischen Datenschutz-Grundverordnung (DSGVO) eingehalten

28 ROR: ROR Curation, ror.org, o. D., <https://ror.org/curation/>, Stand: 15.07.2021.
29 ROR: Facts, o. D.
30 Digital Science: GRID - Global Research Identifier Database, grid.ac, 2021, <https://grid.ac>, Stand: 15.07.2021.
31 Bundesamt für Sicherheit in der Informationstechnik: Die Lage der IT-Sicherheit in Deutschland 2020, Bonn 2020, S. 20. Online: <https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2020.pdf?__blob=publicationFile&v=1>.
32 Änderungen der Registrierungsdaten einer Domain ohne die Einwilligung des Domaininhabers.

werden oder nicht. Die International DOI Foundation beispielsweise sitzt in den USA[33], genauso wie die ORCID Inc[34] und ROR[35]. Bei der Handle.Net Registry wird es schon undurchsichtig, weil die Server von einer US-amerikanischen Organisation betrieben werden[36], aber die verantwortende Stiftung in der Schweiz ansässig ist[37]. In der Datenschutzerklärung von DOI und Handle finden sich zu den über die Webseiten-Besucher*innen gespeicherten Daten gerade einmal drei Sätze[38], während ORCID in mehreren Abschnitten DSGVO-konform auf Art und Umfang der Datenerhebung und die Nutzerrechte eingeht[39].

Aus diesem Zusammenhang ergibt sich auch ein weiterer Problempunkt: die fehlende Gewährleistung der Datenintegrität. Keines der bisher behandelten Identifikatorensysteme stellt technisch sicher, dass die Integrität der dort gespeicherten (Meta-)Daten gewahrt bleibt. Es gibt keine öffentlich einsehbaren Änderungshistorien oder verifizierbare Prüfsummen der Datensätze. Höchstens der Vermerk von Erstellung und letzter Aktualisierung sind vorgesehen, etwa bei DOI[40] oder ORCID[41]. Jede Person mit Zugriff auf die zentrale Datenbank des Systems könnte also nicht nur die URL, sondern auch die (Meta-)Daten eines Identifikators beliebig verändern oder austauschen.

Sobald Nutzer*innen also zentrale Identifikatorensysteme verwenden, legen sie die alleinige Gewährleistung über die Authentizität ihrer referenzierten Daten in die Hände des jeweiligen Anbieters. Fehlende Maßnahmen gegen Datenmanipulation könnten in diesem Fall beiden Seiten schaden, die Abwesenheit von Transparenz hilft im Zweifelsfall aber nur dem Anbieter. Einzig ORCID verfolgt gegenwärtig mit ihrer Public Data File Use Policy einen Ansatz, der diesem Problem zumindest teilweise Rechnung trägt, indem sie der Öffentlichkeit jährlich komplette Datasets der ORCID-Registry zum Download zur Verfügung stellt.[42]

33 International DOI Foundation: 7 International DOI Foundation, DOI Handbook, 2018, <https://www.doi.org/doi_handbook/7_IDF.html>, Stand: 15.07.2021.
34 ORCID: What is the relationship between the ORCID Initiative and ORCID, Inc.?, ORCID Support, 2018, <https://support.orcid.org/hc/en-us/articles/360006897814-What-is-the-relationship-between-the-ORCID-Initiative-and-ORCID-Inc->, Stand: 15.07.2021.
35 ROR: Governance, ror.org, o. D., <https://ror.org/governance/>, Stand: 15.07.2021.
36 Corporation for National Research Initiatives: Projects, CNRI System & Technology Demonstration Projects, 2020, <http://www.cnri.reston.va.us/projects.html>, Stand: 15.07.2021.
37 DONA Foundation: About DONA, <dona.net>, 2020, <https://www.dona.net/aboutus>, Stand: 15.07.2021.
38 International DOI Foundation: Privacy Policy, DOI.ORG, 2012, <https://www.doi.org/w3c/privacy.html>, Stand: 15.07.2021 ; Corporation for National Research Initiatives: Privacy Policy, handle.net, 2015, <https://handle.net/privacy_policy_hnet.html>, Stand: 15.07.2021.
39 ORCID: Privacy Policy, info.orcid.org, 2021, <https://info.orcid.org/privacy-policy/>, Stand: 15.07.2021.
40 DataCite Metadata Working Group: DataCite Metadata Schema Documentation for the Publication and Citation of Research Data and Other Research Outputs: Version 4.4, 2021, S. 46–47. Online: <https://doi.org/10.14454/3w3z-sa82>.
41 ORCID: Record Schema, info.orcid.org, 2021, Abschn. Create and last modified dates, <https://info.orcid.org/documentation/integration-guide/orcid-record/>, Stand: 15.07.2021.
42 ORCID: Public Data File Use Policy, info.orcid.org, 2021, <https://info.orcid.org/public-data-file-use-policy/>, Stand: 15.07.2021.

2. Dezentrale Identifikatoren (DIDs)

Ein System, das auf dezentralen Identifikatoren (DIDs) beruht, kann die im vorherigen Abschnitt beschriebenen Probleme zentraler Identifikatorensysteme lösen und bietet darüber hinaus noch weitere Möglichkeiten in der Anwendung.

DIDs sind eine durch das W3C spezifizierte neue Art von weltweit eindeutigen Identifikatoren, die durch jedes Individuum oder jede Organisation selbst generiert und auf jeder Plattform betrieben werden können, die als vertrauenswürdig erachtet wird. Sie sind in ihrer Essenz mittels kryptografischer Authentifizierungsmechanismen steuerbar, wodurch jede Entität, die einen dezentralen Identifikator erstellt hat, über diesen verfügen kann.[43]

DIDs sind unbegrenzt gültig, portabel und sie basieren auf einer verifizierbaren digitalen Identität, die unabhängig von einer zentralen Instanz funktioniert (siehe Abschnitt 2.5).

Bei dem W3C handelt es sich um das weltweite Gremium zur Standardisierung des Webs, das in der Vergangenheit Web-Standards wie HTML, CSS und XML hervorgebracht hat. Seit 2019 befasst sich dort eine Arbeitsgruppe, die W3C DID Working Group, dezidiert mit dem Thema dezentrale Identifikatoren und hat mit den Arbeiten an einem Standard begonnen, die im September 2021 abgeschlossen sein sollen.[44]

Die ursprüngliche Erforschung und Entwicklung der ersten DID-Spezifikation ging auf eine Förderung durch das U.S. Department of Homeland Security (DHS) zurück. Die Ergebnisse wurden Ende 2016 veröffentlicht und anschließend in die W3C Credentials Community Group eingebracht, um den Standardisierungsprozess anzustoßen. Dieser Prozess führte zur Gründung der Arbeitsgruppe.[45]

Technisch gesehen entsprechen DIDs dem Standard eines URI (Uniform Resource Identifier), also einer Zeichenfolge, die eine abstrakte oder physische Ressource identifiziert.[46] Ähnlich den URNs im Web geben DIDs Ressourcen ebenfalls weltweit eindeutige Namen, wodurch diese dauerhaft identifizierbar sind. Ein DID ist jedoch gleichzeitig sowohl konkret auflösbar (resolvable) wie eine URL als auch ein abstrakter Identifikator wie eine URN.[47]

43 W3C: Decentralized Identifiers (DIDs) v1.0: Core architecture, data model, and representations, W3C Candidate Recommendation Draft, 2021, Abschn. Introduction, <https://www.w3.org/TR/did-core/>, Stand: 15.07.2021.

44 W3C: Decentralized Identifier Working Group Charter, W3C Decentralized Identifier Working Group Charter, 2019, <https://www.w3.org/2019/09/did-wg-charter.html>, Stand: 15.07.2021.

45 Reed, Drummond; Joosten, Rieks; Van Deventer, Oskar: The basic building blocks of SSI, in: Preukschat, Alex; Reed, Drummond (Hg.): Self-Sovereign Identity: Decentralized digital identity and verifiable credentials, Shelter Island, NY 2021, S. 32.

46 Berners-Lee, Tim; Fielding, Roy T.; Masinter, Larry: Uniform Resource Identifier (URI): Generic Syntax, Request for Comments: 3986, Internet Society, 2005, S. 1. Online: <https://www.rfc-editor.org/rfc/rfc3986.txt>.

47 Reed, Drummond; Sabadello, Markus: Decentralized identifiers, in: Preukschat, Alex; Reed, Drummond (Hg.): Self-Sovereign Identity: Decentralized digital identity and verifiable credentials, Shelter Island, NY 2021, S. 158–160.

Die Syntax eines DIDs ist an das URN-Schema angelehnt. Der URI beginnt mit dem Namen des Schemas „did“, eine Autorität entfällt, stattdessen folgt mit Doppelpunkt-Trennern der Schema-spezifische Teil: die DID-Methode und dann der DID-Methoden-spezifische String.[48]

did:<DID-Methode>:<DID-Methoden-spezifischer String>

Der dritte Teil des DID-Formats (der Teil nach dem zweiten Doppelpunkt) wird auch als „methoden-spezifischer Identifikator“ bezeichnet und ist typischerweise eine lange Zeichenkette, die mit Hilfe von Zufallszahlen und kryptografischen Funktionen erzeugt wird. Er ist innerhalb des DID-Methoden-Namensraums immer garantiert eindeutig.[49]

Die vier Haupteigenschaften von DIDs sind nach Reed und Sabadello[50]:

1. Persistenz: Sie müssen nie geändert werden.
2. Auflösbarkeit: Sie geben durch ein Resolving einen standardisierten Satz an Metadaten zurück.
3. Kryptografische Überprüfbarkeit: Ihr Inhaber kann allein mit Kryptografie nachgewiesen werden.
4. Dezentralisierung: Sie erfordern keine zentrale Registrierungsstelle.

Die beiden letzten Punkte (3. und 4.) in Kombination sind dabei das Alleinstellungsmerkmal der DIDs gegenüber allen bisherigen konventionellen Identifikatoren.

Im Vergleich zu anderen Identifikatoren (siehe Abbildung 1) sind DIDs einzig nicht delegierbar. Das bedeutet, innerhalb eines DID-Systems können DIDs nicht von einer Autorität einer anderen Entität zugewiesen werden. Der Hintergrund dazu ergibt sich aus den Ausführungen in den folgenden Abschnitten. Bei konventionellen Identifikatorensystemen wie Handle oder URN delegieren hierarchisch höher gestellte Autoritäten (z.B. DataCite oder die DNB) etwa Präfixe (DOI) oder Namensräume (URN) an andere untergeordnete Autoritären (z.B. Verlage oder wissenschaftliche Bibliotheken), die dann wiederum in ihrem Raum als Vergabestelle agieren können.[51]

48 W3C: Decentralized Identifiers (DIDs) v1.0: Core architecture, data model, and representations, 2021, Abschn. DID Syntax.
49 Reed, Drummond; Sabadello, Markus: Decentralized identifiers, 2021, S. 164.
50 Ebd., S. 160.
51 DataCite: How do I get DOIs?, DataCite Support, 2020, <https://support.datacite.org/docs/how-do-i-get-dois>, Stand: 15.07.2021 ; Deutsche Nationalbibliothek: URN-Service, 2021.

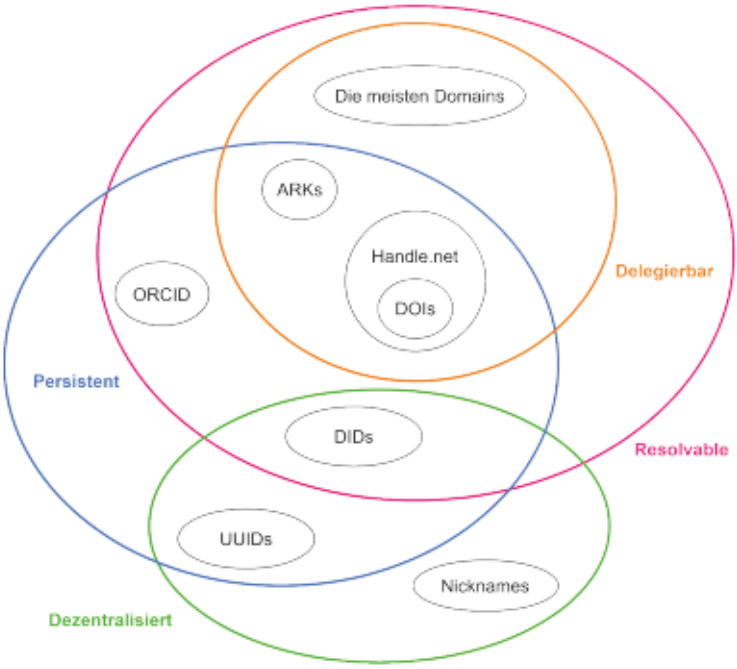

Abb. 1: DIDs im Vergleich zu anderen Identifikatoren[52]

2.1. DID-Methoden

Ein DID wird nicht in einer Datenbank oder einem Netzwerk angelegt oder verwaltet, sondern durch eine DID-Methode. Mit einer entsprechenden Software kann ein DID nach einer bestimmten DID-Methode erzeugt und sofort verwendet werden. Inzwischen gibt es viele verschiedene Arten von DIDs, respektive dahinter auch unterschiedliche Arten von DID-Methoden (siehe Tabelle 1). Sie unterstützen zwar alle die gleiche Grundfunktionalität, unterscheiden sich aber in der Art und Weise, wie diese Funktionalität implementiert wird, z.B. wie genau ein DID erstellt wird oder wo und wie das zugehörige DID-Dokument gespeichert und abgerufen wird.[53]

Tabelle 1: Beispiele von DID-Methoden

did:btcr:x705-jznz-q3nl-srs	Bitcoin-Blockchain
did:peer:1zQmZMygzYqNwU6Uhmewx5Xepf2VLp5S4HLSwwgf2aiKZuwa	Peer-to-Peer
did:key:z6Mkfriq1MqLBoPWecGoDLjguo1sB9brj6wT3qZ5BxkKpuP6	Statisch
did:github:gjgd	Github

52 In Anlehnung an Reed, Drummond; Sabadello, Markus: Decentralized identifiers, 2021, S. 170.
53 Reed, Drummond; Sabadello, Markus: Decentralized identifiers, 2021, S. 163.

Aktuell (Stand: 24. Juni 2021) umfasst das durch die W3C Credentials Community Group betreute DID-Methoden-Register 103 verschiedene DID-Methoden, die sich derzeit in Entwicklung befinden.[54]

Für jede DID-Methode ist eine eigene technische Spezifikation erforderlich, in der die folgenden Aspekte definiert werden müssen[55]:

- Die Syntax des DID-methodenspezifischen Strings
- Die vier grundlegenden CRUD-Operationen, die mit einem DID ausgeführt werden können:
  - Create: Wie ein DID und das zugehörige DID-Dokument erstellt werden kann.
  - Read: Wie das das zugehörige DID-Dokument abgerufen werden kann.
  - Update: Wie der Inhalt des DID-Dokuments geändert werden kann.
  - Deactivate[56]: Wie sich ein DID deaktivieren lässt, sodass er nicht mehr verwendet werden kann.
- Spezielle Sicherheits- und Datenschutzüberlegungen bezüglich der DID-Methode.

Durch die W3C-DID-Arbeitsgruppe wird auch ein Kriterienkatalog zur Auswahl der DID-Methode[57] und ein Dokument zu Voraussetzungen und Use Cases von DIDs[58] bereitgestellt, anhand derer sowohl Nutzer*innen als auch Entscheidungsträger*innen ihre Abwägung treffen können, welches bestehende DID-System sie als vertrauenswürdig erachten oder ob ein eigenes entwickelt werden muss.

Obwohl jede DID-Methode dieselben Grundfunktionen erfüllt, kann sie je nach Anwendungsfall technisch auf einer anderen Plattform angelegt sein. Einige basieren auf Blockchain bzw. anderen Distributed-Ledger-Technologien (DLT), andere auf einer direkten Peer-to-Peer-Verbindung, sind statisch oder setzen auf bestehende Internetprotokolle wie Web-Domains auf. DID-Methoden können sich daher im Grad der Dezentralisierung oder der Vertrauenswürdigkeit unterscheiden. Außerdem spielen Faktoren der Skalierbarkeit, Leistung oder Kosten der zugrundeliegenden technischen Infrastruktur eine Rolle.[59]

54 W3C: DID Specification Registries: The interoperability registry for Decentralized Identifiers, W3C Working Group Note, 2021, Abschn. DID Methods, <https://www.w3.org/TR/did-spec-registries/>, Stand: 15.07.2021.

55 Reed, Drummond; Sabadello, Markus: Decentralized identifiers, 2021, S. 164.

56 Entgegen dem gängigen IT-Verständnis steht im Kontext von DIDs das „D“ der CRUD-Operationen für „Deactivate“ und nicht für „Delete“. Hier wird sich an dem von Blockchains bekannten Prinzip der Unveränderbarkeit orientiert. Eine Blockchain garantiert Manipulationssicherheit dadurch, dass rückwirkend kein Block in der Kette verändert werden kann und Änderungen bestehender Daten nur als eine Art Vermerk in einem neuen Block hinzukommen. DIDs bestehen entsprechend solange unveränderbar fort, bis sich die Ersteller*innen dafür entscheiden, diesen zu deaktivieren. Der DID wird sodann als deaktiviert markiert und kann ab dem Zeitpunkt nicht mehr genutzt werden.

57 <https://w3c.github.io/did-rubric/>

58 <https://www.w3.org/TR/did-use-cases/>

59 Reed, Drummond; Sabadello, Markus: Decentralized identifiers, 2021, S. 164.

2.2. DID-Dokument

Mit DIDs können Nutzer*innen sich selbst kryptografisch einen Identifikator ohne das Zutun eines Dritten oder einer externen Autorität generieren, der sich auch nach einer Schlüsselrotation weiter verifizieren lässt. Das wird ermöglicht durch eine dezentrale Public-Key-Infrastruktur (DPKI).

Zur Erstellung veröffentlichen die Nutzer*innen ihren erstellten Public Key und ihren DID in einem initialen DID-Dokument. Ein DID-Dokument enthält außerdem[60]:

- Authentifizierungsmethoden
- Service Endpoints (zur Interaktion)
- Zeitstempel (als Audit-Historie)
- Signaturen (zur Sicherstellung der Integrität)

Ab diesem Zeitpunkt kann zum einen der*die Nutzer*in über den DID mittels kryptografischem Schlüssel verfügen (ihn kontrollieren) und zum anderen jeder Dritte die Verknüpfung zwischen DID und zugehörigem Public Key kryptografisch verifizieren.

2.3. DID-Resolving

DIDs sind genau wie die meisten PIDs resolvable, jedoch steckt dahinter eine andere Funktionsweise als bei gewöhnlichen PID-Diensten (siehe Abbildung 2).

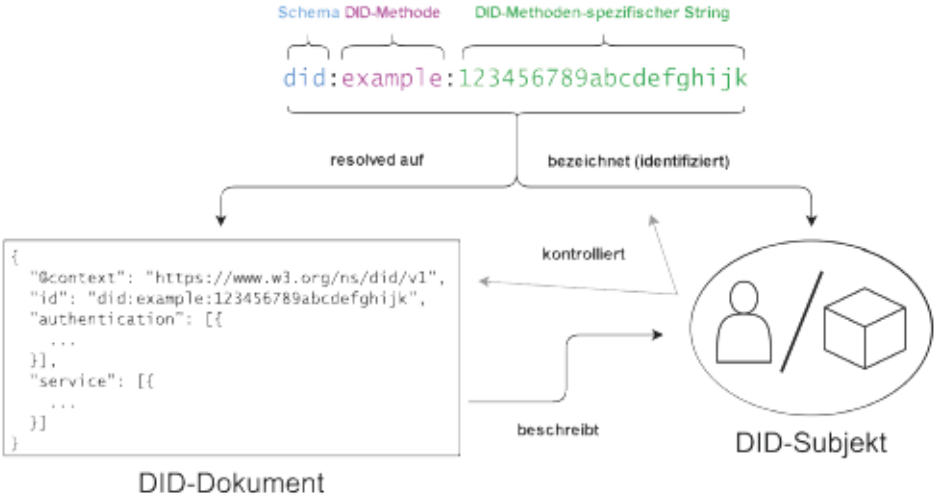

Abb. 2: Auflösung (Resolving) eines DIDs[61]

60 W3C: DID Specification Registries: The interoperability registry for Decentralized Identifiers, 2021, Abschn. Property Names.

61 In Anlehnung an Reed, Drummond; Sabadello, Markus: Decentralized identifiers, 2021, S. 162.

Der DID wird mittels spezieller Software (oder Hardware) an einen DID-Resolver übermittelt und damit eine standardisierte Datenstruktur (das DID-Dokument) aufgerufen. Diese zurückgegebene Datenstruktur ist nicht als Anzeige für die Endnutzer*innen (im Browser oder durch eine App) gedacht, sondern wird direkt durch Anwendungen oder Dienste für digitale Identitäten wie Wallets, Agents oder Data Stores genutzt, die DIDs als eine ihrer Komponenten weiterverarbeiten.[62]

Jeder DID hat genau ein zugehöriges DID-Dokument. Das DID-Dokument ist gewöhnlich im JSON-LD-Format gehalten und enthält Metadaten über das DID-Subjekt. Es ist die technische Basis für alle Interaktionen, die zwischen Akteuren in dem Netzwerk stattfinden. Als DID-Subjekt wird die Entität bzw. das Objekt bezeichnet, das durch den DID identifiziert und durch das DID-Dokument beschrieben wird. Die Entität, die den DID und das zugehörige DID-Dokument kontrolliert, wird als DID-Controller bezeichnet und ist in den meisten Fällen dieselbe wie das DID-Subjekt.[63]

Wie im Abschnitt „Schwächen zentraler Identifikatorensysteme“ weiter oben erläutert, bieten etablierte PID-Dienste keine Möglichkeit des Resolvings, sobald deren Webserver nicht erreichbar ist. Im Fall von DIDs stehen nicht nur die Resolver der Entwickler*innen zur Verfügung[64], sondern jede*r kann selbst einen Resolver aufsetzen. Entwickelte DID-Applikationen sind in einer Vielzahl als Open-Source-Software veröffentlicht. Ebenso werden in der Spezifikation der jeweiligen DID-Methode die Verfahren dargelegt, wie ein DID resolved werden kann. So ist es prinzipiell jedem möglich, selbst eine Applikation zu programmieren, die DIDs dieser Methode resolven kann. Darüber hinaus lässt sich auch ein Resolver umsetzen, der im Stande ist, mehrere DID-Methoden aufzulösen. Durch die Decentralized Identity Foundation (DIF) wird bereits testweise ein solcher universeller Resolver betrieben[65].

Es kommt noch hinzu, dass Handle, DOI, ORCID und Konsorten zwar bekannt geben, wie sich ihr PID syntaktisch zusammensetzt, aber nicht, wie das Resolving technisch funktioniert oder es sich sogar nachbauen ließe. Sollte, wie es in den meisten Fällen ist, hinter einem konventionellen PID-Dienst eine zentrale Datenbank stehen, dann ist nur dem damit verbundenen Server (also dem PID-Dienst-Anbieter und von ihm autorisierten Instanzen) exklusiv das Resolving erlaubt. Gleichzeitig stellt, wie oben bereits ausgeführt, solch eine zentrale Datenbank einen Single Point of Failure dar, weil das gesamte System nicht mehr funktioniert, sobald eine solche Komponente (Domain, Datenbank oder eben der Resolver) ausfällt.

62 Reed, Drummond; Sabadello, Markus: Decentralized identifiers, 2021, S. 161.
63 Ebd., S. 161–163.
64 Diese sind üblicherweise im jeweiligen Eintrag des DID-Methoden-Registers aufgeführt, siehe Abschnitt „DID-Methoden“.
65 <https://uniresolver.io>

2.4. DID-URLs

DIDs können zudem auch als fortschrittlichere URLs genutzt werden. So können einem DID auch syntaktische Komponenten, wie sie von HTTP-URLs bekannt sind, angehängt werden: ein optionaler Pfad, ein optionaler Query-String und ein optionales Fragment.

did:example:1234;service=hub/my/path?query#fragment

DIDs fungieren hier als die Root-Autorität einer DID-URL und es entsteht ein Raum innerhalb des Identifikators, in dem sich zusätzliche Ressourcen in Verbindung mit dem DID unterbringen lassen.[66]

2.5. Self-Sovereign Identity (SSI)

DIDs sind einer der Grundpfeiler eines neuen Paradigmas: das der dezentralen Identität, in der Fachcommunity auch Self-Sovereign Identity (SSI) genannt.

Das herrschende Paradigma der zentralisierten Identität, in der Nutzer*innen nur virtuelle Repräsentationen ihrer Identität in Form mehr oder minder kontrollierbarer Accounts unter willkürlichen Bedingungen bei verschiedenen Identitätsprovidern wie Facebook, Google, Twitter usw. anlegen müssen, soll damit überwunden werden.

Essenziell geht es um eine Verlagerung der Kontrolle in die Hände der Nutzer*innen (siehe Abbildung 3). Die Nutzer*innen werden vom Rand des Beziehungsnetzes, in dem wir alle existieren und interagieren, nun in das Zentrum gestellt.

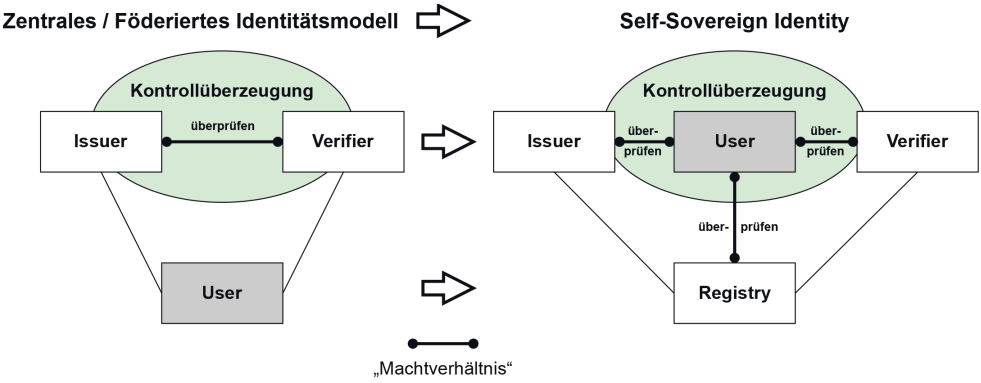

Abb. 3: Verschiebung der Kontrollsphäre der digitalen Identität[67]

66 Reed, Drummond; Sabadello, Markus: Decentralized identifiers, 2021, S. 166–167.

67 In Anlehnung an Preuschkat, Alex; Reed, Drummond, Why the internet is missing an identity layer – and why SSI can finally provide one, 2021, S. 12.

SSI zeichnet sich nach Reed et al. durch eine einzigartige Kombination von insgesamt sieben Grundpfeilern aus[68]:

- Verifiable Credentials (VCs): Sie stellen das digitale Äquivalent zu physikalischen Credentials (Ausweisdokumente, Zertifikate, Quittungen etc.) dar, mit denen wir uns im Alltag gegenüber anderen ausweisen.
- Dem Vertrauensdreieck: Das allgemeine Funktionsprinzip hinter Verifiable Credentials (siehe Abbildung 4). Durch die Interaktion der drei Rollen Issuer (Herausgeber[69]), Holder (Inhaber) und Verifier (Akzeptanzstelle) werden Credentials ausgestellt, in ein Wallet transferiert und verifiziert.
- Wallets: Die digitalen Äquivalente zu physikalischen Brieftaschen, in denen wir unsere Credentials aufbewahren – ähnlich den Wallets für Kryptowährungen, nur nach offenen Standards.
- Agents: Programme oder Apps (z.B. Browser), die es uns ermöglichen, ein Wallet zur Verwaltung von Verifiable Credentials zu nutzen, sich mit anderen Agents zu verbinden und VCs innerhalb einer SSI-Infrastruktur auszutauschen.
- Dezentrale Identifikatoren (DIDs): DIDs werden in einem SSI-Ökosystem zur Adressierung der am Netzwerk teilenehmenden Identitäten genutzt.
- Blockchains und andere Verifiable Data Registries (Vertrauenswürdige Datenregister)[70]: Diese gelten als das Rückgrat eines SSI-Ökosystems, weil auf diesen verteilten, kryptografisch gesicherten Datenbanken DIDs manipulationssicher gespeichert und VCs darüber unabhängig von Dritten verifiziert werden können. Sie gelten daher als zuverlässige Quelle.
- Governance[71] Frameworks: Sie ermöglichen, bestimmte wirtschaftliche, rechtliche und technische Konstrukte in einer SSI-Infrastruktur abzubilden, wodurch ganze interoperable Vertrauens-Ökosysteme entstehen können. Die Verifizierung von VCs kann so in etwas wie Vertrauens-Domänen (Governance Frameworks, auch Trust Frameworks genannt) geschehen, die jeweils unter bestimmten Bedingungen von vertrauenswürdigen Autoritäten angelegt wurden.

68 Reed, Drummond; Joosten, Rieks; Van Deventer, Oskar: The basic building blocks of SSI, 2021, S. 21–36.
69 Die deutschen Übersetzungen der Rollen in diesem Abschnitt stammen von Ehrlich et al., 2021, S. 250, 254.
70 DIDs sind protokoll-agnostisch konzipiert, daher umfasst der W3C-Begriff Verifiable Data Registry alle Plattformen, die die Grundfunktionen der DID-Spezifikation, wie sie im Abschnitt „DID-Methoden“ beschrieben wurden, erfüllen.
71 Der Begriff Governance meint hier nicht automatisch regierungsbezogene Lenkung, sondern generell strukturelle Organisationsformen.

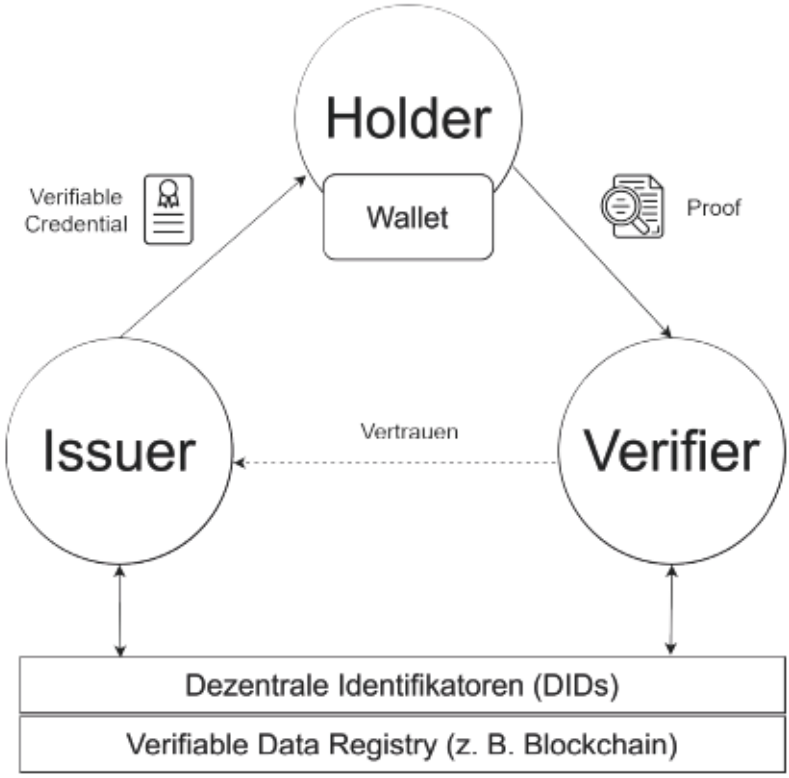

Abb. 4: Vertrauensdreieck eines SSI-Ökosystems[72]

DIDs und SSI gibt seinen Nutzer*innen die Tools und die Technologie in die Hände, über die eigene digitale Identität selbst zu verfügen, diese selbst zu verwalten und selbst zu bestimmen, wie, wann und in welchem Umfang Daten mit anderen Parteien geteilt werden.

SSI bedient sich dazu der modernsten technologischen Verfahren, um die manipulationssicherste und unabhängigste Möglichkeit für einen Austausch und die Ablage von digitalen Daten zu bieten, bei der die Identitäten von Sender*in und Empfänger*in eindeutig gesichert sind.

Eine solche angestrebte „Kultur des signierten Datenaustauschs" über DIDs und SSI würde Identitätsdiebstahl und Datenmanipulation nahezu unmöglich bzw. unwirksam machen.

SSI hat daher aufgrund dieser fundamental anderen Herangehensweise nicht nur technologische, sondern auch wirtschaftliche, rechtliche und soziale Dimensionen.

72 In Anlehnung an Reed, Drummond; Joosten, Rieks; Van Deventer, Oskar: The basic building blocks of SSI, 2021, S. 25.

3. Fünf Anforderungen zur Umsetzung von PIDs

Im Verlauf der Auseinandersetzung mit dem Thema entstanden diese fünf Anforderungen an eine zeitgemäße Umsetzung von persistenten Identifikatoren:

1. Persistente Identifikatoren müssen von jedem, schnell und auch in Masse günstig anzulegen sein.
2. Persistente Identifikatoren müssen beständig einem Subjekt zu einem festen Zweck zugewiesen und unveränderbar sein.
3. Persistente Identifikatoren müssen dauerhaft resolvable sein, damit auf Langzeit mindestens die Metadaten abrufbar sind.
4. Persistente Identifikatoren müssen nachhaltig und unabhängig sein, indem sie nicht auf zentralen Registrierungsstellen, Identitätsprovidern oder anderen zwischengeschalteten Autoritäten basieren, die anfällig sind für Hacks, Manipulation und Datenleaks.
5. Persistente Identifikatoren müssen sicher sein. Eine Person oder Organisation muss im Stande sein, nachweisen zu können, dass sie über einen Identifikator verfügt oder eben nicht verfügt. Kryptografie ist für diesen Zweck die aktuell einzig verlässliche Technologie, ohne sich auf die Fehlbarkeit von Menschen verlassen zu müssen.

Literaturverzeichnis

- Berners-Lee, Tim; Fielding, Roy T.; Masinter, Larry: Uniform Resource Identifier (URI): Generic Syntax, Request for Comments: 3986, Internet Society, 2005. Online: <https://www.rfc-editor.org/rfc/rfc3986.txt>.
- Bundesamt für Sicherheit in der Informationstechnik: Die Lage der IT-Sicherheit in Deutschland 2020, Bonn 2020. Online: <https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2020.pdf?__blob=publicationFile&v=1>.
- Corporation for National Research Initiatives: Projects, CNRI System & Technology Demonstration Projects, 2020, <http://www.cnri.reston.va.us/projects.html>, Stand: 15.07.2021.
- Corporation for National Research Initiatives: Prefix Registration, handle.net, 2018, <https://www.handle.net/prefix.html>, Stand: 15.07.2021.
- Corporation for National Research Initiatives: Privacy Policy, handle.net, 2015, <https://handle.net/privacy_policy_hnet.html>, Stand: 15.07.2021.
- Daigle, Leslie L.; Gulik, Dirk-Willem van; Iannella, Renato u. a.: Uniform Resource Names (URN) Namespace Definition Mechanisms, Request for Comments: 3406, Internet Society, 2002. Online: <https://www.rfc-editor.org/rfc/rfc3406.txt>.
- DataCite: How do I get DOIs?, DataCite Support, 2020, <https://support.datacite.org/docs/how-do-i-get-dois>, Stand: 15.07.2021.

- DataCite Metadata Working Group: DataCite Metadata Schema Documentation for the Publication and Citation of Research Data and Other Research Outputs: Version 4.4, 2021. Online: <https://doi.org/10.14454/3w3z-sa82>.
- Deutsche Nationalbibliothek: URN-Service, dnb.de, 2021, <https://www.dnb.de/DE/Professionell/Services/URN-Service/urn-service_node.html>, Stand: 15.07.2021.
- Deutsche Nationalbibliothek: Normdaten in der Wissenschaft – Vernetzung von GND und ORCID, dnb.de, 2020, <https://www.dnb.de/DE/Professionell/ProjekteKooperationen/projekteKoop_node.html#sprg446188>, Stand: 15.07.2021.
- Dierkes, Jens: Planung, Beschreibung und Dokumentation von Forschungsdaten, in: Putnings, Markus; Neuroth, Heike; Neumann, Janna (Hg.): Praxishandbuch Forschungsdatenmanagement, Berlin/Boston 2021, S. 303–325. Online: <https://doi.org/10.1515/9783110657807-018>.
- Digital Science: GRID – Global Research Identifier Database, grid.ac, 2021, <https://grid.ac>, Stand: 15.07.2021.
- DomainTools: Whois Record for ror.org, Whois Lookup, o.D., <https://whois.domaintools.com/ror.org>, Stand: 15.07.2021.
- DONA Foundation: About DONA, dona.net, 2020, <https://www.dona.net/aboutus>, Stand: 15.07.2021.
- Ehrlich, Tobias; Richter, Daniel; Meisel, Michael u. a.: Self-Sovereign Identity als Grundlage für universell einsetzbare digitale Identitäten, in: HMD Praxis der Wirtschaftsinformatik 58 (2), 2021, S. 247–270. Online: <https://doi.org/10.1365/s40702-021-00711-5>.
- FORCE11: The FAIR Data Principles, force11.org, 2016, <https://www.force11.org/group/fairgroup/fairprinciples>, Stand: 15.07.2021.
- International DOI Foundation: 7 International DOI Foundation, DOI Handbook, 2018, <https://www.doi.org/doi_handbook/7_IDF.html>, Stand: 15.07.2021.
- International DOI Foundation: 1 Introduction, DOI Handbook, 2015, <https://www.doi.org/doi_handbook/1_Introduction.html>, Stand: 15.07.2021.
- International DOI Foundation: Privacy Policy, DOI.ORG, 2012, <https://www.doi.org/w3c/privacy.html>, Stand: 15.07.2021.
- Moats, Ryan: URN Syntax, Request for Comments: 2141, Internet Society, 1997. Online: <https://www.rfc-editor.org/rfc/rfc2141.txt>.
- ORCID: About, info.orcid.org, 2021, <https://info.orcid.org/what-is-orcid/>, Stand: 15.07.2021.
- ORCID: Privacy Policy, info.orcid.org, 2021, <https://info.orcid.org/privacy-policy/>, Stand: 15.07.2021.
- ORCID: Record Schema, info.orcid.org, 2021, <https://info.orcid.org/documentation/integration-guide/orcid-record/>, Stand: 15.07.2021.
- ORCID: Public Data File Use Policy, info.orcid.org, 2021, <https://info.orcid.org/public-data-file-use-policy/>, Stand: 15.07.2021.
- ORCID: Benefits for Researchers, info.orcid.org, 2020, <https://info.orcid.org/benefits-for-researchers/>, Stand: 15.07.2021.

- ORCID: What is the relationship between the ORCID Initiative and ORCID, Inc.?, ORCID Support, 2018, <https://support.orcid.org/hc/en-us/articles/360006897814-What-is-the-relationship-between-the-ORCID-Initiative-and-ORCID-Inc->, Stand: 15.07.2021.
- ORCID: Board of Directors, about.orcid.org, 2012, <https://web.archive.org/web/20120909022005/http://about.orcid.org/board-of-directors>, Stand: 15.07.2021.
- Pampel, Heinz; Elger, Kirsten: Publikation und Zitierung von digitalen Forschungsdaten, in: Putnings, Markus; Neuroth, Heike; Neumann, Janna (Hg.): Praxishandbuch Forschungsdatenmanagement, Berlin/Boston 2021, S. 521–536. Online: <https://doi.org/10.1515/9783110657807-028>.
- Preukschat, Alex; Reed, Drummond: Why the internet is missing an identity layer—and why SSI can finally provide one, in: Preukschat, Alex; Reed, Drummond (Hg.): Self-Sovereign Identity: Decentralized digital identity and verifiable credentials, Shelter Island, NY 2021, S. 3–20.
- Reed, Drummond; Joosten, Rieks; Van Deventer, Oskar: The basic building blocks of SSI, in: Preukschat, Alex; Reed, Drummond (Hg.): Self-Sovereign Identity: Decentralized digital identity and verifiable credentials, Shelter Island, NY 2021, S. 21–38.
- Reed, Drummond; Sabadello, Markus: Decentralized identifiers, in: Preukschat, Alex; Reed, Drummond (Hg.): Self-Sovereign Identity: Decentralized digital identity and verifiable credentials, Shelter Island, NY 2021, S. 157–188.
- ROR: Facts, ror.org, o. D., <https://ror.org/facts/>, Stand: 15.07.2021.
- ROR: ROR Curation, ror.org, o. D., <https://ror.org/curation/>, Stand: 15.07.2021.
- ROR: Governance, ror.org, o. D., <https://ror.org/governance/>, Stand: 15.07.2021.
- Scholze, Frank; Ulrich, Robert; Goebelbecker, Hans-Jürgen: Wissenschaftlicher Datenmarkt, in: Putnings, Markus; Neuroth, Heike; Neumann, Janna (Hg.): Praxishandbuch Forschungsdatenmanagement, Berlin/Boston 2021, S. 165–173. Online: <https://doi.org/10.1515/9783110657807-009>.
- Schrader, Antonia: 100.000 GND-Personendatensätze mit ORCID-Records verknüpft!, ORCID DE, 2020, <https://www.orcid-de.org/100000-gnd-orcid-verknuepft/>, Stand: 15.07.2021.
- Sollins, Karen; Masinter, Larry: Functional Requirements for Uniform Resource Names, Request for Comments: 1737, Internet Society, 1994. Online: <https://www.rfc-editor.org/rfc/rfc1737.txt>.
- Sun, Sam X.; Lannom, Larry; Boesch, Brian: Handle System Overview, Request for Comments: 3650, Internet Society, 2003. Online: <https://www.rfc-editor.org/rfc/rfc3650.txt>.
- Universität Konstanz: Persistente Identifikatoren, forschungsdaten.info, 2021, <https://www.forschungsdaten.info/themen/veroeffentlichen-und-archivieren/persistente-identifikatoren/>, Stand: 15.07.2021.
- Vierkant, Paul: Was ist das Research Organization Registry (ROR)?, ORCID DE, 2020, <https://www.orcid-de.org/was-ist-das-research-organization-registry-ror/>, Stand: 15.07.2021.

- W3C: Decentralized Identifiers (DIDs) v1.0: Core architecture, data model, and representations, W3C Candidate Recommendation Draft, 2021, <https://www.w3.org/TR/did-core/>, Stand: 15.07.2021.
- W3C: DID Specification Registries: The interoperability registry for Decentralized Identifiers, W3C Working Group Note, 2021, <https://www.w3.org/TR/did-spec-registries/>, Stand: 15.07.2021.
- W3C: Decentralized Identifier Working Group Charter, W3C Decentralized Identifier Working Group Charter, 2019, <https://www.w3.org/2019/09/did-wg-charter.html>, Stand: 15.07.2021.
- W3C: URIs, URLs, and URNs: Clarifications and Recommendations 1.0, W3C Note, 2001, <https://www.w3.org/TR/uri-clarification/>, Stand: 15.07.2021.