HOCHSCHULE
MITTWEIDA
University of Applied Sciences

BACHELORARBEIT

Herr
Paul Werner Anton Petzold

Entwicklung eines Verifiable Credential-Validierungs-Plugins für WordPress zur sicheren Anmeldung auf Webseiten im Vergleich mit Passkey-Technologien

Mittweida, 2023

Fakultät Angewandte Computer- und Biowissenschaften

BACHELORARBEIT

Entwicklung eines Verifiable Credential-Validierungs-Plug-ins für WordPress zur sicheren Anmeldung auf Webseiten im Vergleich mit Passkey-Technologien

Autor:
Herr Paul Werner Anton Petzold

Studiengang:
Medieninformatik und Interaktives Entertainment

Seminargruppe:
MI20w3-B

Erstprüfer:
Prof. Dr.-Ing. Andreas Ittner

Zweitprüfer:
Dipl.-Betriebswirt (FH) Jan Lippert

Einreichung:
Mittweida, 27.11.2023

Verteidigung/Bewertung:
Mittweida, 2023

Bibliografische Beschreibung:

Petzold, Paul Werner Anton:

Entwicklung eines Verifiable Credential-Validierungs-Plugins für WordPress zur sicheren Anmeldung auf Webseiten im Vergleich mit Passkey-Technologien

60 Seiten, Mittweida, Hochschule Mittweida – University of Applied Science, Fakultät Angewandte Computer- und Biowissenschaften, Bachelorarbeit, 2023

Referat:

Vor dem Hintergrund der stetigen Digitalisierung gewinnen ebenfalls der Schutz von Daten und die Privatsphäre im digitalen Raum an Bedeutung. Insbesondere das Management digitaler Identitäten befindet sich im Umbruch. Zentralisierte Identitätsprovider haben begonnen, mit dem Konzept der Passkey-Technologien ein neues Authentifizierungsverfahren in ihre Systeme zu implementieren, welches künftig das Passwort ablösen soll. Das Konzept Self-Sovereign Identity (SSI) bietet ein dezentralisiertes System zur eigenständigen Identitätsverwaltung. Die Arbeit befasst sich mit der prototypischen Entwicklung einer erweiterbaren Schnittstelle zur Validierung digitaler Nachweise in einem SSI-Ökosystem in Form eines Plugins für das Content-Management-System WordPress. Dieses Plug-in soll eine alternative Authentifizierungsmethode zu Passkey-Technologien von Identitätsprovidern darstellen.

Faculty of Applied Computer Sciences and Biosciences

BACHELOR THESIS

Development of a Verifiable Credential validation plugin for WordPress for secure login to websites in comparison with Passkey technologies

Author:
Mr. Paul Werner Anton Petzold

Course of Study:
Media Informatics and Interactive Entertainment

Seminar Group:
MI20w3-B

First Examiner:
Prof. Dr.-Ing. Andreas Ittner

Second Examiner:
Dipl.-Betriebswirt (FH) Jan Lippert

Submission:
Mittweida, 27.11.2023

Defence/Evaluation:
Mittweida, 2023

Bibliographic Disclosures:

Petzold, Paul Werner Anton:

Development of a Verifiable Credential validation plugin for WordPress for secure login to websites in comparison with Passkey technologies

60 pages, Mittweida, Hochschule Mittweida – University of Applied Science, Faculty of Applied Computer Sciences and Biosciences, Bachelor Thesis, 2023

Abstract:

In the context of ongoing digitalization, the importance of data protection and privacy in the digital space is gaining momentum. Particularly, the management of digital identities is undergoing a transformation. Centralized identity providers have initiated the integration of a new authentication method called Passkey Technologies into their systems, aiming to replace passwords in the future. The concept of Self-Sovereign Identity (SSI) provides a decentralized system for autonomous identity management. This study focuses on the prototype development of an expandable interface for validating digital credentials within an SSI ecosystem, manifested as a plugin for the WordPress Content Management System. This plugin aims to serve as an alternative authentication method to the Passkey Technologies offered by identity providers.

Inhaltsverzeichnis

Inhaltsverzeichnis ..... **I**

Abbildungsverzeichnis ..... **III**

Tabellenverzeichnis ..... **V**

Quellcodeverzeichnis ..... **VI**

Abkürzungsverzeichnis ..... **VII**

Glossar ..... **X**

1 Einleitung **1**

1.1 Die Problematik Passwort 1

1.2 Motivation und Problemstellung 7

1.3 Zielsetzung 7

2 Grundlagen **8**

2.1 Identitätsmanagement im digitalen Zeitalter 8

2.1.1 Digitale Identitäten 10

2.1.2 ID-Provider 14

2.1.3 Self-Sovereign Identity 20

2.1.4 Gegenüberstellung von IdP und SSI 25

2.2 Hidy Wallet 26

2.3 WordPress 27

2.3.1 Content-Management-Systeme 27

2.3.2 Gutenberg Editor ein Pagebuilder 28

3 Konzept **32**

3.1 Plug-in-Registrierung und Integration in WordPress 32

3.2 Block-Einbindung in Gutenberg Editor 33

3.3 Validierungsprozess 34

4 Implementierung **37**

4.1 Technologie-Stack 37

4.2 Softwarearchitektur ... 37
4.3 Funktionalitäten ... 40
4.4 Benutzeroberfläche ... 40

5 Demonstration ... 42
5.1 Einrichtung und Integration des Plugins auf der Webseite ... 42
5.2 Ablauf einer VC-Presentation aus Nutzersicht ... 45

6 Anwendungsmöglichkeiten ... 46
6.1 Digitale Identitätsverifikation ... 46
6.2 Alternative zu Passkey-Technologien ... 47
6.2.1 Vergleich von Passkey-Technologien und SSI ... 47
6.2.2 Potential von SSI-Lösungen ... 48

7 Fazit ... 50

8 Ausblick ... 51
8.1 Fertigstellung des Prototyps zu einer kompletten Softwarelösung ... 51
8.1.1 Login-Vorgang ... 51
8.1.2 dynamische Skalierbarkeit ... 53
8.1.3 Anpassungsfähige UI und Integration der SSI-Wallet ... 54
8.1.4 Veröffentlichen auf WordPress.org ... 55
8.2 Verifizierungsstelle in Plug-in integrieren ... 55
8.3 Ausstellen „privater“ Nachweise ... 56
8.4 Datenökonomie und Transparenz ... 57
8.5 Verfügbarmachung auf weiteren Systemen ... 59

Literaturverzeichnis ... XIII

Anlagenverzeichnis ... A

Anlage 1: Verzeichnisstruktur des Hidy-Validierungs-Plug-ins ... A-I

Anlage 2: Screenshots der Benutzeroberfläche des Hidy-Validierungs-Plug-ins ... A-II

Selbstständigkeitserklärung ... XXIII

Abbildungsverzeichnis

Abbildung 1: Umfrage zur Länge von Passwörtern in Deutschland 2022 2

Abbildung 2: Statistik über die Nutzung von unterschiedlichen Passwörtern für unterschiedliche Online-Dienste 2023 3

Abbildung 3: Umfrage zur Ablage von Passwörtern in Deutschland 2021 4

Abbildung 4: Anzahl Datenlecks und geklauter Datensätze in den USA von 2005 bis 2019 6

Abbildung 5: Statistik über Zunahme der Cyberkriminalität von 2020 zu 2021 10

Abbildung 6: Beispielbild für ein Cookie-Banner auf einer beliebigen Webseite 11

Abbildung 7: Umfrage zu Cookies und Cookie-Bannern auf Webseiten in Deutschland 2020 13

Abbildung 8: Modell Identity Provider 15

Abbildung 9: Screenshot des Login-Formulars des Online-Shops Instant-Gaming 16

Abbildung 10: Umsatz von Meta weltweit bis zum 3. Quartal 2023 17

Abbildung 11: Werbeumsätze von Meta weltweit bis 2022 17

Abbildung 12: Umsatz von Google weltweit bis 2022 18

Abbildung 13: Umsatz mit Werbung von Google bis 2022 19

Abbildung 14: Schema der Funktionsweise von digitalen Signaturen 21

Abbildung 15: SSI-Ökosystem für digitale Identitäten und Nachweise 22

Abbildung 16: Architektur von Self-Sovereign Identity 24

Abbildung 17: Grundmodell des Identitätsmanagements 25

Abbildung 18: Nutzungsanteil der Content-Management-Systeme (CMS) weltweit im Oktober 2023 28

Abbildung 19: Screenshot des Gutenberg Editor-Seitenmenüs zum Einfügen von Gutenberg Editor-Blöcken 29

Abbildung 20: Screenshot des Gutenberg Editor-Schnellmenüs zum Einfügen von Gutenberg Editor-Blöcken 30

Abbildung 21: Screenshot des Gutenberg Editor-Blockmenüs individuellen Anpassen bestimmter Blöcke nach vorgegebenen Richtlinien 30

Abbildung 22: Ranking der beliebtesten WordPress Pagebuilder nach Marktanteilen (Stand: 11.08.2023) 31

Abbildung 23: Sequenzdiagramm des Validierungsprozesses 35

Abbildung 24: Softwarearchitektur des Validierungs-Plug-ins nach MVVM-Muster 39

Abbildung 25: „Hidy-Button“ – ein UI-Element des Gutenberg Editor-Blocks 40

Abbildung 26: „Hidy-Pop-up" – ein UI-Element des Gutenberg Editor-Blocks 41

Abbildung 27: Installation des Hidy-Validierungs-Plug-ins in ZIP-Dateiformat 42

Abbildung 28: Hidy-Validierungs-Plug-in in der Plug-in-Übersicht von WordPress 43

Abbildung 29: Link zur Einstellungsseite des Plug-ins im Administrationsmenü 43

Abbildung 30: Hidy Authenticator-Kategorie und Hidy Auth Button im Seitenmenü des Gutenberg Editors 44

Abbildung 31: Hidy Auth Button im Schnellmenü des Gutenberg Editors 44

Abbildung 32: Einstellungsmenü des Gutenberg Blocks im Gutenberg Editor 44

Abbildung 33: Typischer Ablauf einer Verifiable Credential-Presentation aus Nutzersicht 45

Abbildung 34: Konzept des Checkboxen-Formulars zur Auflistung übermittelter Informationen zwischen Hidy Wallet und Webseite 59

Tabellenverzeichnis

Tabelle 1: Übersicht aller üblichen Tracking-Methoden im Online-Marketing 12

Tabelle 2: Zusammenfassung und Gegenüberstellung der wichtigsten Merkmale der beiden Konzepte zur Verwaltung von digitalen Identitäten ID-Providern und Self-Sovereign Identity 26

Tabelle 3: Zusammenfassung und Gegenüberstellung der wichtigsten Merkmale der beiden Identitätsbestätigungsmethoden Passkey und Self-Sovereign Identity..... 48

Quellcodeverzeichnis

Quellcode 1: Kopfzeile einer WordPress-Plug-in-Hauptdatei 33

Abkürzungsverzeichnis

API	(englisch Application Programming Interface) Schnittstelle zur programmatischen Interaktion mit einem Programm
Ajax	Asynchronous JavaScript and XML, JavaScript-Methode zur asynchronen Datenübertragung zwischen Client und Server
BCAM	Blockchain Academy Mittweida
BCCM	Blockchain Competence Center Mittweida
BMBF	Bundesministerium für Bildung und Forschung
BMWK	Bundesministerium für Wirtschaft und Klimaschutz
CMS	(englisch Content-Management-System) Inhaltsverwaltungssystem
CORS	(englisch Cross-Origin Resource Sharing) Ursprungsübergreifende Ressourcenfreigabe
CRUD	(englisch Create Read Update Delete) Erstellen Lesen Aktualisieren Löschen
CSRF	(englisch Cross-Site-Request-Forgery) Webseitenübergreifende Anfragenfälschung
CSS	(englisch Cascading Style Sheets) Formatierungssprache für HTML-, SVG- und XML-Dokumente
cURL	(englisch Client for URLs) Kommandozeilen-Tool und Bibliothek für Datenübertragung über verschiedene Protokolle, wie HTTP, HTTPS und FTP
DID	(englisch Decentralized Identifiers) dezentrale Identifikatoren
DLT	Distributed-Ledger-Technologie
DS-GVO	Europäische Datenschutz-Grundverordnung
eID	deutscher, elektronischer Personalausweis
FTP	(englisch File Transfer Protocol) Internetprotokoll zur Übertragung von Daten zwischen Computern
GE	Gutenberg Editor
GEB	Gutenberg Editor-Block
HSMW	Hochschule Mittweida

HTML	(englisch Hypertext Markup Language) Auszeichnungssprache zur Strukturierung textbasierter Inhalte von Webdokumenten
HTTP	(englisch Hypertext Transfer Protocol) zustandsloses Protokoll zur Übertragung von Daten auf der Anwendungsschicht über ein Rechnernetz
HTTPS	(englisch Hypertext Transfer Protocol Secure) sichere Version von HTTP durch Verwendung von SSL
IdP	ID-Provider oder Identitätsanbieter
IP	(englisch Internet Protocol) Internetprotokoll
IPFS	(englisch InterPlanetary File System) dezentrales, peer-to-peer-basiertes Dateispeichersystem
JS	JavaScript, Skriptsprache
KEL	(englisch Key Event Logs) Schlüsselereignisprotokoll
KERI	(englisch Key Event Receipt Infrastructure) Infrastruktur für Schlüsselereignisbelege
MVVM	(englisch Model-View-ViewModel) architektonisches Muster in der Softwareentwicklung
NFC	(englisch Near Field Communication) Nahfeldkommunikation
P2P	(englisch Peer-to-Peer) ugs. „Gleich-zu-Gleich“
PHP	Hypertext Preprocessor, ursprünglich Personal Home Page Tools, Skriptsprache für die Erstellung dynamischer Webseiten
PIN	Persönliche Identifikationsnummer
PKI	(englisch Public-Key-Infrastructure) Infrastruktur für öffentliche Schlüssel
SSI	(englisch Self-Sovereign Identity) eigenständige Identitätsverwaltung
SSL	(englisch Secure Sockets Layer) Verschlüsselungsprotokoll, das zur sicheren Übertragung von Daten im Internet verwendet wird.
SSO	(englisch Single Sign-on) eine Authentifizierungsmethode
TSL	(englisch Transport Layer Security) Verschlüsselungsprotokoll, zur sicheren Übertragung von Daten im Internet verwendet wird, Nachfolger von SSL
UI	(englisch User Interface) Benutzeroberfläche
URL	(englisch Uniform Resource Locator) Einheitlicher Ressourcenanzeiger, ugs. Internet- oder Webadresse
VC	(englisch Verifiable Credential) verifizierbare digitale Nachweise
VCV	(englisch Verifiable Credential-Validation) Validierung verifizierbarer digitaler Nachweise

VDR	(englisch Verifiable Data Registry) vertrauenswürdiges Datenregister
WP	WordPress, ein CMS
XHR	XMLHttpRequest, Programmierschnittstelle für JavaScript zum Übertragen von Daten über HTTP
XSS	(englisch Cross-Site-Scripting) Webseitenübergreifendes Skripting

Glossar

Add-in: Optionale Softwarekomponente, die Software um Funktionen od. bestehende Funktionen erweitert und dabei auf vorhandene Bibliotheken der Software, die sie erweitert, angewiesen ist. Add-ins greifen tief in die Basissoftware ein, sodass sie nicht entfernt werden können, ohne die Funktionalitäten der Basissoftware zu beeinträchtigen.

Add-on: Optionale Softwarekomponente, die Software um Funktionen od. bestehende Funktionen erweitert und dabei auf vorhandene Bibliotheken der Software, die sie erweitert, angewiesen ist. Add-ons sind nicht eigenständig ohne die Basissoftware lauffähig.

Backend: Der Teil einer Software, der im Hintergrund abläuft, sodass Nutzer nichts davon mitbekommen.

Block: In dieser Arbeit im Kontext des Gutenberg Editors, von WordPress oder des Validierungs-Plug-ins verwendet als Kurzschreibweise für „Gutenberg Editor-Block“.

Client: Synonym für Computer oder sonstiges digitales Endgerät, welches über ein bestimmtes Protokoll mit einem Server kommuniziert.

Cloud: Eine IT-Ressource, die via Internet verfügbar gemacht wird.

Cookies: Datenpakete, die von Webbrowsern und Internetseiten erzeugt werden, um individuelle Nutzerdaten zu speichern.

CORS: Ist ein Mechanismus zur Integration von Anwendungen. CORS bestimmt für Client-Webanwendungen, die in einer Domain geladen sind, eine Möglichkeit zur Interaktion mit Ressourcen in einer anderen Domain.

CPU-ID: Prozessor-ID, Kennzahl eines Prozessors, wodurch ein Computer eindeutig identifizierbar ist.

Credential: englisch, z. Dt. Ausweis oder Berechtigungsnachweis

Cross-Site-Request-Forgery: Cyber-Angriffsmethode, bei der die autorisierte Session eines Nutzers manipuliert und der Nutzer zum unwissentlichen Durchführen ungewünschter Aktionen bzw. Transaktionen gebracht wird.

Cross-Site-Scripting: Cyber-Angriffsmethode zum Einschleusen schädlichen Codes in Webanwendungen über Sicherheitslücken.

CRUD: Die vier grundlegenden Operationen zur Erstellung und Verwaltung persistenter Datenelemente in Datenbanken.

Distributed-Ledger-Technologie: Technologie zur Aufzeichnung von Informationen über eine auf mehrere Computersysteme verteilte Datenbanken.

Entität: eindeutig identifizierbarer konkreter oder abstrakter Gegenstand

Feedback: englisch, z. Dt. Rückmeldung

Framework: Eine vorgefertigte Struktur oder Plattform, die Entwicklern hilft, Anwendungen schneller zu erstellen, indem sie eine Grundlage für gemeinsame Funktionen und Prozesse bietet.

From scratch: englisch, ugs. z. Dt. von Anfang an

Frontend: Der Teil einer Software, der für Nutzer sichtbar ist.

ID-Provider/Identitätsanbieter: Zentrales Zugangssystem für Service-Provider-Dienste, bei dem sich Nutzer anmelden können.

IP-Adresse: Individuelle Adresse, die ein Gerät im Internet oder in einem lokalen Netzwerk identifiziert.

Kryptographie: Ist ein Teilgebiet der Kryptologie und befasst sich mit dem Verschlüsseln von Informationen.

Middleware: englisch, z. Dt. Zwischenanwendung, ein Softwareprogramm oder eine Softwarekomponente, über die verschiedene Anwendungen oder Komponenten miteinander kommunizieren, Daten austauschen oder Funktionen aufrufen.

Near Field Communication: Übertragungsstandard zum kontaktlosen Austausch von Daten per elektromagnetischer Induktion über eine Distanz von wenigen Zentimetern.

Open Source: Software, deren Quelltext frei verfügbar ist.

Passkey: Eine kurze Zeichenfolge oder ein Code, der zur Authentifizierung oder Autorisierung verwendet wird, um auf Ressourcen oder Systeme zuzugreifen.

Passwort: Zeichenkette bestehend aus Buchstaben, Zahlen und bestimmten Sonderzeichen.

Passwort-Manager: Ein Programm, das Benutzernamen und Passwörter verwaltet. Einige können Passwörter (zufällig) generieren.

Peer-to-Peer: Dezentrale Netzwerktopologie, in der die Teilnehmer gleichberechtigt und auf gleicher Ebene miteinander interagieren.

PIN: Zeichenkette ausschließlich bestehend aus Zahlen.

Plug-in: Optionale Softwarekomponente, die Software um Funktionen od. bestehende Funktionen erweitert und dabei auf keine vorhandenen Bibliotheken der Software, die sie erweitert, angewiesen ist, sie aber nutzen kann. Die Basisfunktionen von Plug-ins sind auch eigenständig ohne die Basissoftware lauffähig.

Pool: eine Sammlung oder eine Gruppe von Dingen oder Ressourcen

Pop-up: englisch „to pop up“, z. Dt. „plötzlich auftauchen“, Im Kontext von (Web-)Designs ein Element einer grafischen Benutzeroberfläche, das plötzlich auf dem Bildschirm erscheint und zusätzliche Informationen, Aktionen oder Benutzereingaben anzeigt, ohne die Hauptanwendung zu unterbrechen.

POST-Anfrage: Methode zur Übermittlung von Informationen an einen Server über HTTP. Häufig benutzt, um Formulardaten von einer Webseite an einen Server zu senden.

Proxy: Vermittler zwischen Client und Server in einem Computernetzwerk

Screenshot: englisch, Bildschirmaufnahme in rein bildlicher Form

Session: englisch, z. Dt. Sitzung, Beschreibt im Kontext der Webentwicklung die stehende Verbindung eines Clients mit einem Server.

Single Sign-on: Eine Authentifizierungsmethode, die es Benutzern ermöglicht, sich auf sichere Weise bei mehreren Anwendungen und Webseiten zu authentifizieren und dabei nur einmal ihre Anmeldeinformationen einzugeben.

Theme: englisch, z. Dt. Thema, Stellt im Kontext des (Web-)Designs eine Design-Vorlage dar, die als Grundlage für die Entwicklung von Designs genutzt werden kann.

Verteilte Systeme: Datenverarbeitungsumgebung, in der sich zahlreiche Komponenten auf mehrere Computer in einem Netzwerk verteilen.

Wallet: im Kontext von SSI: Bezeichnung für eine Software, die eine digitale Brieftasche darstellt, in welcher digitale Nachweise und persönliche Daten sicher abspeichert und verwaltet werden können. Z. T. können sie ebenfalls Online-Zahlungen durch bspw. digitale Versionen von Debit- und Kreditkarten oder Kryptowährungen ermöglichen.

Websocket: Mechanismus zur schnellen bidirektionalen Kommunikation zwischen einem Client und einem Server.

ZIP-Datei: ein komprimiertes Archivformat

1 Einleitung

„For the first time, we've begun rolling out passkeys, the easiest and most secure way to sign in to apps and websites and a major step toward a "passwordless future."“ [1]

Mit diesen Worten kündigte Google in ihrem Blog im Frühjahr 2023 das Ende des Passworts ein und kündigte damit gleichzeitig an, dass fortan Passkeys als zusätzliche Anmeldemöglichkeit für Google-Konten den Nutzern zur Verfügung stehen. Diese Arbeit beschäftigt sich mit einer Alternative zu u. a. Googles Passkey-Technologie, welche ebenfalls eine passwortfreie Zukunft anstrebt. [1]

1.1 Die Problematik Passwort

Passwörter sind Zeichenketten bestehend aus Buchstaben, Zahlen und bestimmten Sonderzeichen. Sie dienen zur Zugriffsverwaltung auf bestimmte Inhalte wie Nutzerkonten von Onlinediensten und Webseiten oder verschlüsselte Dokumente. Passwörter funktionieren nach dem simplen Prinzip, dass nur Personen, die das Passwort kennen, Zugriff auf die gesperrten Inhalte erhalten. Dieses Schema funktioniert jedoch nur, sofern alle Personen, die Zugriff auf diese Inhalte bekommen sollen, das entsprechende Passwort kennen und alle anderen Personen, die auf diese Inhalte keinen Zugriff haben sollen, das Passwort nicht kennen. Daraus ergeben sich zwei Probleme.

Zum einen müssen Passwörter möglichst komplex, lang und kontextunabhängig sein und sicher aufbewahrt werden, damit Dritte sie nicht entschlüsseln können. Dies führt in der Erstellung und Verwaltung von Passwörtern zu einem Mehraufwand, welcher oft nicht betrieben wird, wie einige Statistiken und Umfragen zeigen.

Laut einer Statistik aus dem März 2022 (Abbildung 1) benutzt die Mehrheit der Deutschen kurze Passwörter: 35 % der Befragten gaben an, bis zu zehn Zeichen für die Erstellung ihrer Passwörter zu benutzen, 24 % gaben an, bis zu zwölf Zeichen zu benutzen und 14 % der Befragten verwenden lediglich acht Zeichen für ihre Passwörter. Längere Passwörter, die schon aufgrund ihrer Länge komplexer werden, werden nur von einem geringen Anteil der Befragten genutzt. 8 % der Befragten benutzen 20 Zeichen. Mehr als 20 Zeichen benutzen nur noch 5 % der Befragten. [14]

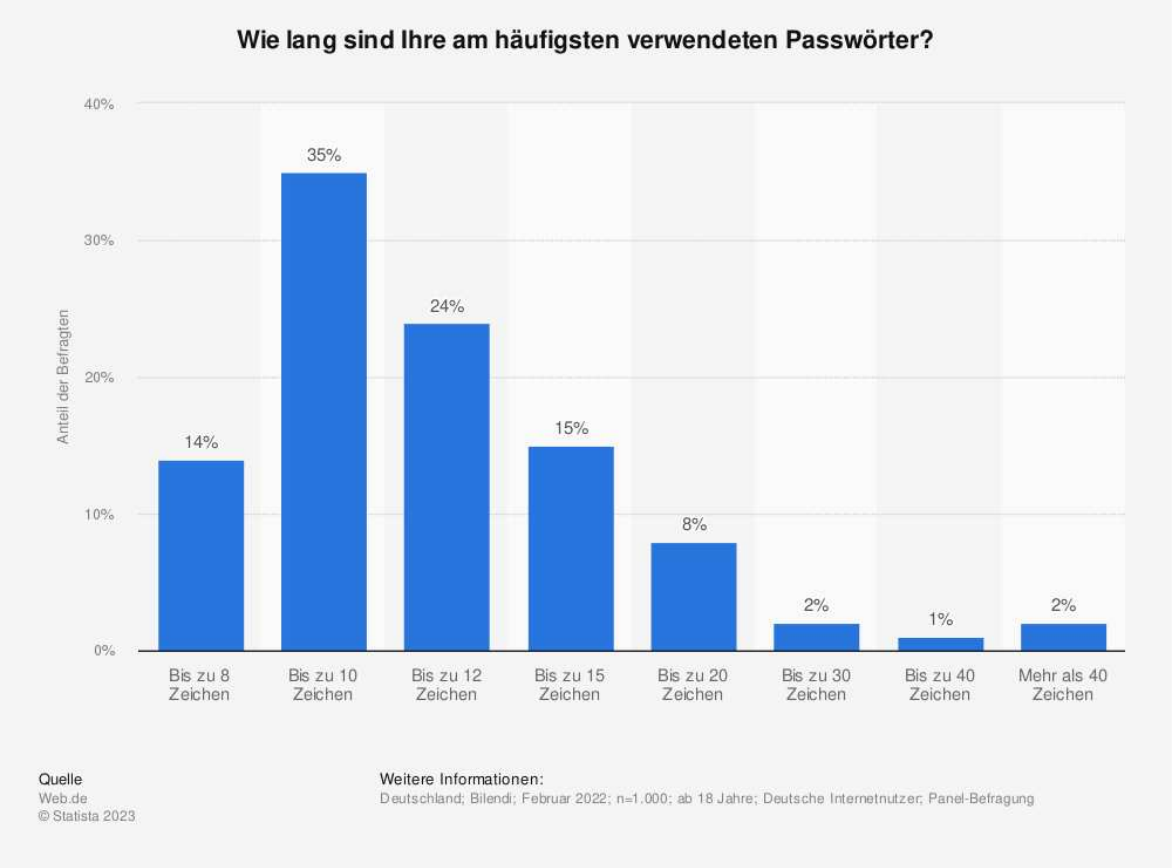


Abbildung 1: Umfrage zur Länge von Passwörtern in Deutschland 2022

Quelle: [14]

Einer weiteren Statistik aus dem April 2023 (Abbildung 2) zufolge, welche sich mit der Nutzung von Passwörtern für unterschiedliche Online-Dienste in Deutschland beschäftigte, nutzen die Mehrheit von 51 % der Befragten zumindest teilweise dieselben Passwörter für unterschiedliche Online-Dienste und 6 % benutzen für alle Online-Dienste dasselbe Passwort. Dem entgegen stehen 38 % der Befragten, welche für jeden Online-Dienst ein individuelles Passwort nutzen. Mehrfachnutzung von Passwörtern stellt ein Sicherheitsrisiko dar. Erlangt ein unbefugter Dritter dieses eine oder eines der genutzten Passwörter, erlangt er damit Zugriff auf mehrere Konten und nicht nur auf eines. [25]

Beide Statistiken zeichnen ein Bild von weit verbreiteter, unsicherer Erstellung und Nutzung von Passwörtern. Passwörter werden selten komplex zusammengesetzt und mehrfach wiederverwendet, sodass bei einem potenziellen Entschlüsseln der Passwörter direkt mehrere Zugriffe von unbefugten Dritten erlangt werden würden. Ein möglicher Grund für die, z. T. auch mehrfache, Verwendung wenig komplexer Passwörter ist die aufwendige Verwaltung und die Anzahl benötigter Passwörter. Laut [7] besitzt ein Mensch durchschnittlich 70 digitale Identitäten. Im Idealfall sollte jede digitale Identität einen eigenen Identitätsnachweis, in diesem Fall also ein eigenes Passwort besitzen. Hinzukommt ein wachsender Mehraufwand beim Speichern von Passwörtern bei steigender Komplexität.

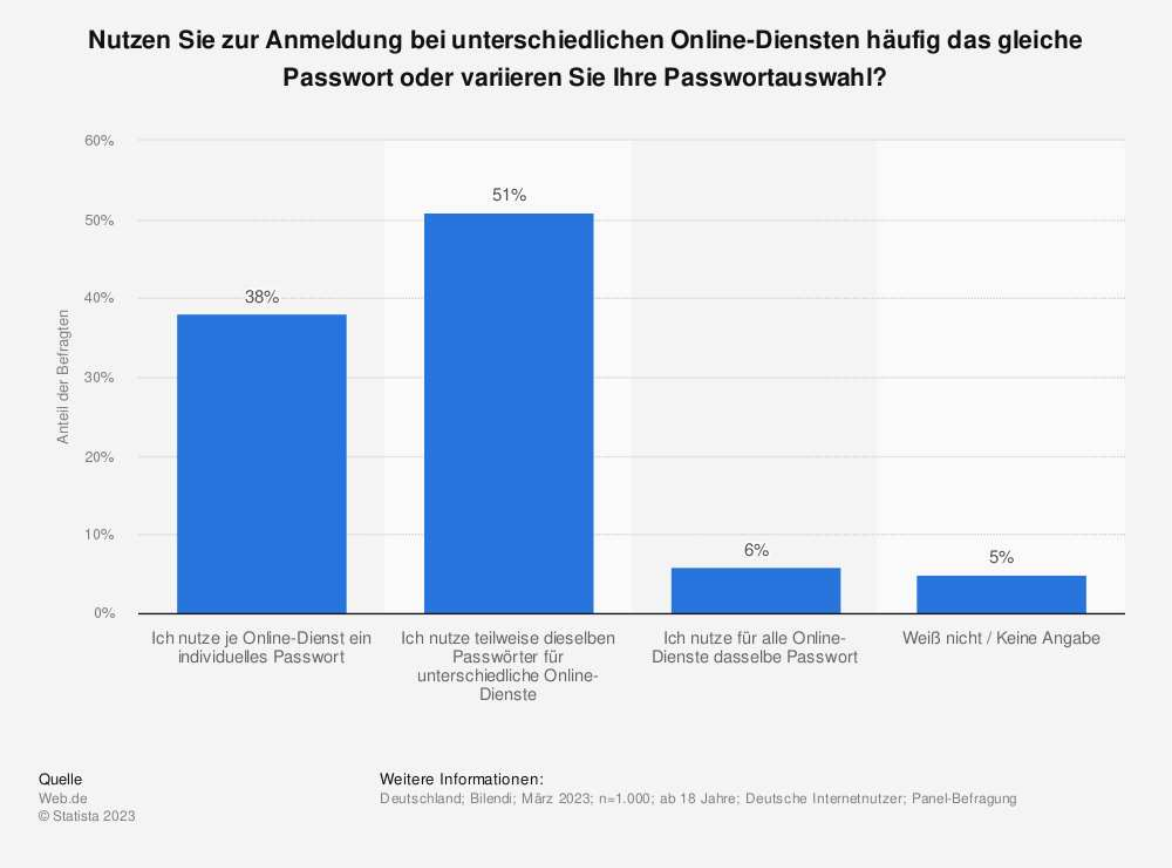


Abbildung 2: Statistik über die Nutzung von unterschiedlichen Passwörtern für unterschiedliche Online-Dienste 2023

Quelle: [25]

Einer Umfrage aus Deutschland aus dem Jahr 2021 (Abbildung 3) nach merken sich 33 % der Befragten ihre Passwörter und schreiben sie nirgendwo nieder bzw. verwenden sonstige Verwaltungsmethoden. Mit 12 % benutzen ein Achtel der befragten Personen einen Passwort-Manager, weitere 27 % benutzen einen Zettel und 8 % speichern ihre Passwörter im Browser. Einige wenige Befragte verwenden ein Dokument auf einem Computer (4 %) oder ein Dokument in einer Cloud (2 %). [26]

Möglicherweise dürfte es für die meisten Menschen eine große Herausforderung darstellen, sich 70 komplexe Passwörter zu merken. Moderne Passwort-Manager sind u. a. in der Lage, lange, komplexe und kontextunabhängige Passwörter zu generieren und zu verwalten. Jedoch sind Passwort-Manager nicht weit verbreitet, wie [26] gezeigt hat. Das Abspeichern von Passwörtern auf Computern, in der Cloud oder im Browser birgt Sicherheitsrisiken, die mit unbefugtem Zugriff auf diese Speichermedien verbunden sind. Dies könnte dazu führen, dass sämtliche gespeicherten Konten gefährdet sind, falls Unbefugte Zugang zu diesen Medien erlangen. Einem Report über Cybersecurity aus dem Jahr 2018 zufolge waren von 1000 Befragten 207 schon einmal Opfer eines Hacking-Angriffs geworden. Zudem droht bei einem möglichen Verlust des Dokuments oder des Gerätes der Verlust aller Passwörter. [46]

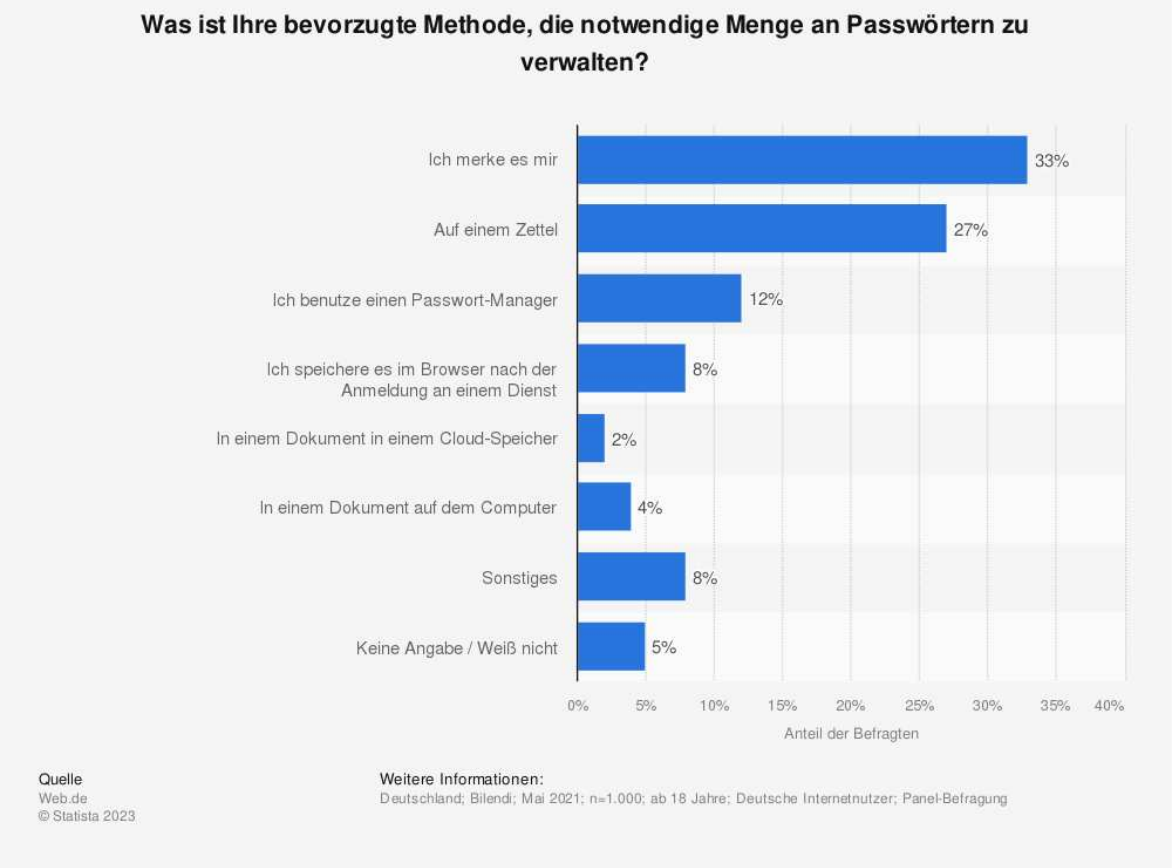


Abbildung 3: Umfrage zur Ablage von Passwörtern in Deutschland 2021

Quelle: [26]

Ein weiteres Problem ergibt sich, falls E-Mail-Konten gehackt wurden. Nicht nur fällt dann die Kontrolle über dieses Konto in die Hände unbefugter Dritter, sondern möglicherweise lassen sich über diese E-Mail-Adresse Passwörter anderer Konten zurücksetzen. Dadurch können die Angreifer Zugriff auf gleich mehrere Konten erlangen.

Durch bestimmte Mechanismen wird das Erraten, Hacken und Zurücksetzen von Passwörtern bereits erschwert oder unterbunden. Bspw. durch das Sperren des Logins nach mehreren fehlerhaften Versuchen oder eine Zwei-Faktor-Authentifizierung, die den Zugriff auf eine Authentifizierungsapp, eine Telefonnummer oder ein weiteres E-Mail-Konto erfordert. Letzteres ist durch die Eingabe eines Passwortes und das Verifizieren des Logins mittels Zwei-Faktor-Authentifizierung für Nutzer jedoch weniger komfortabel.

Damit Passwörter zur Zugriffsfreigabe auf bestimmte Inhalte verwendet werden können, müssen diese zusammen mit bestimmten Nutzerdaten seitens der Online-Plattform, die den freizugebenden Inhalt bereitstellt, gespeichert werden. Nur so kann ein Abgleich der bei der Registrierung angegebenen mit den zur Zugriffsfreigabe angegebenen Daten und eine Zugriffsfreigabe erfolgen. Daraus ergibt sich das zweite Problem von Passwörtern: sog. Datenlecks und Datenschutzverletzungen.

Datenschutzverletzungen stellen die absichtliche und gezielte Verletzung von Datenschutzrichtlinien dar und können den Diebstahl, Verlust oder unbefugten Zugriff durch Dritte auf sensible Daten umfassen. Ugs. werden sie häufig als „Hacker-Angriff“ bezeichnet. Bei Datenlecks, auch genannt Datenpanne, handelt es sich um keine mutwillige Verletzung des Datenschutzes, dennoch wird dieser durch das versehentliche Weitergeben sensibler Daten an Unbefugte durch den Eigentümer oder aufgrund von Fahrlässigkeit des Eigentümers verletzt. In beiden Fällen werden Nutzerdaten, die auch Passwörter sein können, unbefugten Personen zugänglich bzw. zugänglich gemacht. Der Nutzer hat darauf keinen Einfluss, da die Sicherheit und Souveränität der Infrastruktur dem Plattformbetreiber obliegen. [47]

Im September 2023 bspw. informierte die Verbraucherzentrale darüber, wie Nutzer des sozialen Netzwerks Facebook prüfen können, ob ihre bei Facebook gespeicherten Daten bei Datenlecks betroffen sind. In dem Artikel wurde ein Datenleck aus dem Frühjahr 2021 erwähnt, bei dem weltweit persönliche Daten von ca. 530 Mio. Facebook-Nutzern veröffentlicht worden waren. Dieses Datenleck basierte vermutlich auf einer Sicherheitslücke, die nach Angaben von Facebook bereits im Sommer 2019 geschlossen worden sei. [48]

Eine Statistik aus dem Jahr 2022 (Abbildung 4) zeigt die Anzahl an Datenlecks und geklauten Datensätze in den USA in den Jahren 2005 bis 2019. Ihr zufolge wurden 2019 bei 1.473 Datenlecks etwa 164,68 Mio. Datensätze gestohlen. 2005 wurden bei 157 Datenlecks etwa 66,9 Mio. Datensätze gestohlen. Daraus ergeben sich Anstiege von ca. 840% bei der Anzahl an Datenlecks und etwa 150% bei der Anzahl gestohlener Datensätze. Im Anstieg der aufgetretenen Datenlecks stellte das Jahr 2017 mit 1579 Datenlecks den Höhepunkt dar. Im Jahr 2018 wurden mit 471,22 Mio. die meisten Datensätze im angegebenen Zeitraum gestohlen. [49]

Wie auch bei Datendiebstahl aus privaten Dokumenten und Geräten hilft gegen das Veröffentlichen von Passwörtern und sonstigen Login-Daten bei Datenlecks und Datenschutzverletzungen vor allem die Zwei-Faktor-Authentifizierung. Wird diese Methode angewendet, reichen das Passwort und dazugehörige Login-Daten, wie ein Nutzername oder eine E-Mail-Adresse, nicht für den Login auf einem Portal aus.

Es gibt zahlreiche Alternativen zu Passwörtern. Die PIN, welche nur aus Zahlen besteht, steht hinsichtlich seiner Komplexität dem Passwort nach. Dasselbe trifft auf den Login via Smartphone oder Tablet zu. Login mit sog. Single Sign-on-Diensten wie Google, Facebook oder Apple stellt u. a. aus Datenschutzgründen für viele Nutzer keine valide Alternative dar. Passkey-Verfahren, wie sie u.a. Google nun ausrollt, sollen diese Alternative zu Passwörtern bieten (siehe Abschnitte 2.1.1 und 2.1.2).

Der Login über biometrische Daten, wie etwa Fingerabdruck, Augen- oder Gesichtsscan, ist im Smartphone-Login bereits seit Jahren ein Standard. Anders als bei einem Passwort, welches Nutzer selbst erstellen und eingeben müssen, werden bei der biometrischen Authentifizierung bspw. das Gesicht oder der Fingerabdruck des Nutzers erfasst und daraus

numerische Daten gezogen, die als Passwortersatz dienen. Durch die Individualität eines jeden Menschen und abhängig vom Detailgrad der Erfassung der biometrischen Daten sind die numerischen Daten sehr komplex und individuell. Ein manuelles Entschlüsseln scheint kaum denkbar. Laut [58] können jedoch moderne KI-Algorithmen zur Fälschung biometrischer Daten verwendet werden. Dafür könnten bspw. Fotos der entsprechenden Person verwendet werden. Des Weiteren können diese Verfahren fehleranfällig sein. Z. B. beim Fingerabdruckscan einiger Smartphones reichen zum Entsperren teilweise Übereinstimmungen verschiedener Fingerabdrücke aus. Ebenfalls können Fehler beim Erkennen des gültigen Benutzers auftreten, wenn dessen biometrische Daten durch äußere Einflüsse verändert wurden. Dies können bereits das Tragen einer Bille oder bestimmten Make-up sein. Im Falle des Verlusts oder einer sonstigen Veränderung der Fingerkuppe des für die biometrische Authentifizierung registrierten Fingers besteht die Gefahr, dass der Fingerabdruck beim Scannen nicht mehr identifiziert werden kann. [57], [58]

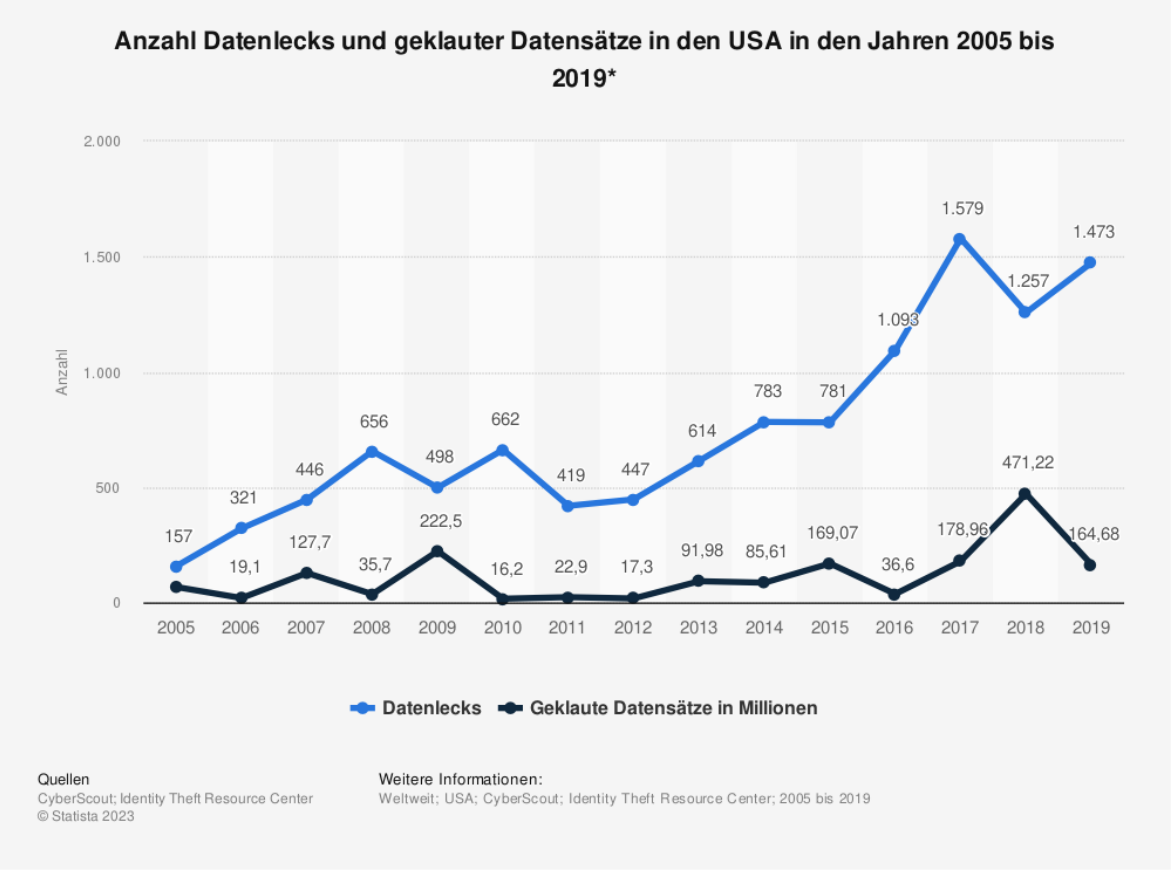


Abbildung 4: Anzahl Datenlecks und geklauter Datensätze in den USA von 2005 bis 2019

Quelle: [49]

Von Datenlecks können neben Login-Daten jedoch auch sonstige private und personenbeziehbare Daten betroffen sein, die von Onlineplattformen gespeichert und verwaltet werden. Nach Artikel 4 Abs. 1 der DS-GVO umfassen „personenbezogene Daten“ alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person […] beziehen [50]. Identifizierbar sind dabei natürliche Personen. D. h. sämtliche Daten, die

einer natürliche Person zugeordnet werden, sind personenbezogen. Daten, die einer natürlichen Person zugeordnet werden können, werden als personenbeziehbar bezeichnet. Sie können nicht unmittelbar und ohne weitere Auskünfte einer natürlichen Person zugeordnet werden, dennoch stellen sie persönliche Daten dar, die den Richtlinien der DS-GVO gemäß zu verwalten und zu schützen sind. Daraus ergibt sich weiterführend ein erhebliches Problem durch das mittlerweile weit verbreitete umfangreiche Erheben von Nutzerdaten, die weit über die von Nutzern selbstständig angegebenen Daten hinausgehen (siehe Abschnitte 2.1.1 und 2.1.2). [50], [51]

1.2 Motivation und Problemstellung

Die anhaltende Evolution des digitalen Zeitalters geht mit einem stetig wachsenden Bewusstsein für Datenschutz einher. Mit der fortschreitenden Digitalisierung gewinnt die Datenerhebung und -verarbeitung an signifikanter Bedeutung, wodurch der Wert persönlicher Informationen zunehmend steigt. Große Konzerne mit monopolähnlicher Stellung verstärken diesen Trend noch weiter.

Vor diesem Hintergrund entsteht ein Bedürfnis nach dezentralisierten Lösungen und ein Streben nach Unabhängigkeit von diesen Konzernen. Menschen wollen wieder mehr Kontrolle über ihre eigenen Daten und Konten haben. Gleichzeitig suchen sie nach sicheren Alternativen zu Passwörtern, um die Sicherheit ihrer Benutzerkonten und der damit verbundenen personenbeziehbaren Daten zu erhöhen und gleichzeitig den Verwaltungsaufwand dieser zu reduzieren.

Die Motivation für diese Arbeit ist die Schaffung eines innovativen Verfahrens, basierend auf der SSI-Softwarelösung Hidy Wallet, das Nutzern ermöglicht, selbstbestimmt über ihre Daten und Konten zu verfügen. Diese Lösung soll nicht nur Sicherheit bieten, sondern auch benutzerfreundlich sein und die Verwaltung digitaler Identitäten erleichtern.

1.3 Zielsetzung

Ziel dieser Arbeit ist die Konzeptionierung und prototypische Umsetzung eines WordPress-Plugins, welches „Verifiable Credentials“, z. Dt. verifizierbare Berechtigungsnachweise, validieren kann. Nach der Validierung kann der Nutzer authentifiziert werden, um ihm bspw. bestimmte Inhalte zugänglich zu machen und bei Nichterbringen des geforderten Nachweises zu bestimmten Inhalten den Zugang verweigern zu können. Zudem sollen Anwendungsmöglichkeiten aufgezeigt werden und insbesondere ein Vergleich dieser Verifizierungsmethode mit Passkey-Technologien erfolgen.

2 Grundlagen

Um die Funktionsweise des Plugins selbst sowie die zugrundeliegende Technologie, auf die das Plugin aufbaut, vollumfänglich verstehen und mögliche Anwendungsbereiche dieses Zusammenspiels ableiten zu können, werden im folgenden Kapitel alle benötigten Grundlagen zusammengefasst und erklärt.

2.1 Identitätsmanagement im digitalen Zeitalter

Im digitalen Zeitalter gewinnt das Identitätsmanagement zunehmend an Bedeutung, insbesondere vor dem Hintergrund einer sich ständig weiterentwickelnden Online-Welt, denn laut [52] bringt die Digitalisierung immer mehr Logins, Authentifizierungs- und Identifizierungsvorgänge mit sich. Die digitale Identität eines Individuums, bestehend aus persönlichen Informationen und Authentifizierungsdaten, ist ein wesentliches Element im täglichen Leben. Vor diesem Hintergrund haben sich nach [60] im Wesentlichen drei Methoden der Authentifikation entwickelt:

- Authentifikation durch Wissen
- Authentifikation durch Biometrie
- Authentifikation durch Besitz

Bei der **Authentifizierung durch Wissen** muss ein Nutzer zeigen, dass er ein bestimmtes vorher vereinbartes Geheimnis kennt. Ein solches Geheimnis kann u. a. ein Passwort oder eine PIN sein. Passwörter sind laut [60] dabei am weitesten verbreitet im Internet. Ein Nutzer zeigt, dass er dieses Passwort kennt, durch die Eingabe in ein Login-Formular. Anschließend wird die Nutzereingabe mit dem üblicherweise bei der Einrichtung des Kontos vereinbarten Passwort verglichen. Bei einer Übereinstimmung in allen Zeichen hat der Nutzer erfolgreich gezeigt, dass er das Passwort kennt, und erhält Zugriff auf die gesperrten Inhalte. Vorteile von Wissen-basierter Authentifikation sind laut [60], dass sie bereits weit verbreitet und einfach zu implementieren ist. Nutzer kennen diese Methode bereits von zahlreichen Diensten und sie hat die geringsten (systemischen) Anforderungen. Benötigt wird ein Eingabeformular, ein Speichermedium, auf dem das vereinbarte Geheimnis gespeichert wird, meistens eine Datenbank, und ein System, das die Eingabe mit der Datenbank-Variable vergleicht, sowie das Wissen über das Geheimnis. Zudem kann das Geheimnis über bestimmte Methoden nachträglich geändert werden, sollte das Passwort in die Hände von unbefugten Dritten gelangt sein. Das benötigte Wissen für die Authentifizierung kann jedoch vergessen, denn „vor allem textbasierte Passwörter sind schwer zu merken“ [60], oder von Unbefugten erraten werden (siehe Abschnitt 1.1). Sollte das Wis-

sen schriftlich festgehalten sein, können Dritte das Geheimnis ausfindig machen (siehe Abschnitt 1.1). [60]

Für die **Authentifizierung mittels Biometrie** werden biometrische Daten eines Menschen bzw. von seinem Körper benötigt. Neben statischen Merkmalen eines Menschen, wie Fingerabdruck, Iris und Gesichtsform, gibt es auch dynamische, wie bestimmte Gesten und Mimik oder den Gang. Zur Nutzbarmachung als Authentifizierungsmittel werden bestimmte Merkmale erfasst, z. B. gescannt, und in numerische Daten überführt (siehe Abschnitt 1.1). Im Vergleich zu Passwörtern bietet diese Methode für Nutzer mehr Komfort. Die benötigten Merkmale müssen nicht gemerkt oder anderweitig verwaltet werden. Allerdings sind bereits die systemischen Anforderungen höher als bspw. bei einer Passwort-Eingabe. Die meisten Smartphones und Tablets sowie viele moderne Laptops und Notebooks besitzen bereits Scanner für Fingerabdruck oder Gesichtserkennung. Bei Desktop-PCs hingegen wird allerdings externe Hardware benötigt, die nicht zur Grundausstattung gehört und extra besorgt werden muss. Zudem kann diese Methode, sollte sie kompromittiert sein, nicht oder nur begrenzt oft geändert werden. Sollten etwa Unbefugte an den hinterlegten Fingerabdruck gelangt sein oder dieser aus diversen Gründen nicht mehr für eine Authentifizierung verwendet werden können, kann er nur noch neun Mal geändert werden. [60]

Die **Besitz-basierte Authentifizierung** verwendet als Geheimnis zur Verifikation des Nutzers einen Gegenstand. Ein solcher Gegenstand ist ein Ausweis und muss daher eindeutig sein. D. h. der Ausweis und damit auch sein Besitzer können eindeutig identifiziert und von anderen Ausweisen und Nutzern unterschieden werden. Beispiele für physikalische Ausweise zur eindeutigen Verifikation sind Chipkarten und Smartphones. Ein solcher Gegenstand kann jedoch auch von digitaler Natur sein. Etwa Zertifikation und private Schlüssel, sog. Private Keys, können Gegenstände zur Authentifizierung sein (siehe Kapitel 2.1.2 Abschnitt Passkey-Technologie und Kapitel 2.1.3 Abschnitt Verifiable Credentials). Bei dieser Methode muss der Nutzer sich kein Geheimnis merken, sondern den Besitz eines bestimmten Gegenstands vorzeigen. Dieser kann jedoch verloren gehen oder gestohlen werden. [60]

Wie eine Statistik (Abbildung 5) zeigt, steigt die Bedrohung durch Cyberkriminalität und Datenmissbrauch und unterstreicht damit die Notwendigkeit, sich intensiver mit der Sicherheit digitaler Identitäten auseinanderzusetzen. Im Jahr 2021 ist die Cyberkriminalität insgesamt um 12,2 % im Vergleich zum Vorjahr angestiegen. Dabei besonders stark betroffen sind das Ausspähen und Abfangen von Daten mit einem Anstieg von 38,6 % auf etwa 15.000 registrierte Straftaten und die Datenfälschung sowie Täuschung im Rechtsverkehr bei Datenverarbeitung mit einem Anstieg von 22,9 % auf ca. 13.400 registrierte Straftaten. [27]

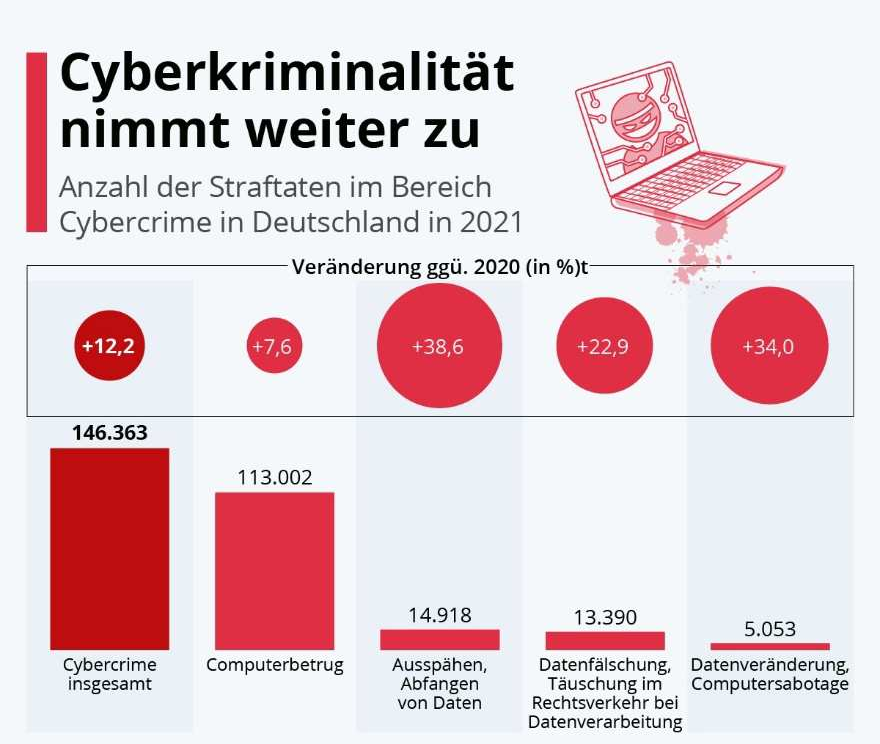


Abbildung 5: Statistik über Zunahme der Cyberkriminalität von 2020 zu 2021

Quelle: [27]

Im Folgenden werden die Begriffe digitale Identitäten, Self-Sovereign Identity und ID-Provider genauer erklärt sowie ein Vergleich der beiden Konzepte zur Verwaltung digitaler Identitäten miteinander durchgeführt.

2.1.1 Digitale Identitäten

„Der moderne Mensch besitzt im Durchschnitt ca. 70 digitale Identitäten.“ [7]

Als digitale Identität wird die Teilmenge von Attributen einer Entität bezeichnet, welche diese Entität im Cyber-Raum eindeutig von anderen Entitäten unterscheidbar und sie selbst bestimmbar macht. Eine Entität stellt in diesem Kontext eine identifizierbare reale Person oder ein IT-System dar, welches bestimmte Attribute, bzw. Eigenschaften besitzt. Diese Arbeit begrenzt sich hierbei auf Personen. Personen besitzen ebenfalls eine reale Identität, die alle Eigenschaften dieser Person umfasst. Eine digitale Identität einer Person muss nicht alle Eigenschaften dieser Person besitzen. Einige der folgenden Eigenschaften reichen in den meisten Fällen bereits aus, um eine digitale Identität bei bspw. einem beliebigen Onlineshop zu bilden: Name, Vorname, Geburtsdatum oder Alter im Allgemeinen, Email-Adresse, Wohnadresse und ggf. eine Bezahlmethode. Daher kann eine Person auch mehrere digitale Identitäten besitzen. Schließlich muss für die meisten unabhängigen Onlineshop und andere Plattformen ein eigenes Konto angelegt werden. [2]

Mittlerweile gibt es mit dem eID-Verfahren des elektronischen Personalausweises, Video-Ident bzw. Videoidentifikation und PostIdent bereits einige Verfahren, die eine Möglichkeit für Nutzer darstellen, sich über das Internet rechtskräftig auszuweisen. Jedoch begrenzt sich dies bisher nur auf einige wenige Dokumente, wie den Personalausweis, und der Einsatz wird bisher nur von bestimmten Dienstanbietern unterstützt. [2]

Datenerhebung und Cookies

Bei der Benutzung des Internets werden durch verschiedene Dienste Daten erhoben, die digitalen Identitäten zugeschrieben werden. Dafür können Benutzerkonten auf Webseiten dienen. Aber auch ohne solche Benutzerkonten können Webseiten Daten erheben und sie anhand anderer Parameter, wie der IP-Adresse oder der CPU-ID, eindeutig Benutzern zuordnen, ohne dass diese selbst aktiv Eigenschaften ihrer realen Identität mit den Webseitenbetreibern teilen. Dies funktioniert u. a. über sog. Cookies. Gemäß Artikel 5 Abs. 3 der EU-Richtlinie 2002/58/EG (Stand 30.09.2023) [5] sind Webseitenbetreiber dazu verpflichtet, im Falle einer Erhebung, Speicherung oder Verarbeitung von personenbeziehbaren Daten Besuchern ihrer Webseite dies in Form des „Cookie-Banners“ zu kommunizieren (Abbildung 6). Cookies sind Datenpakete, die im Browser gespeichert werden. Sie werden in den Kontext mit bestimmten Webseiten gestellt und beim Aufruf dieser Webseiten automatisch an eben diese gesendet. So funktionieren bspw. „Angemeldet bleiben“-Optionen bei Login-Formularen. Die Login-Daten werden im Browser gespeichert und beim Aufruf der Website automatisch an die Webseite gesendet.

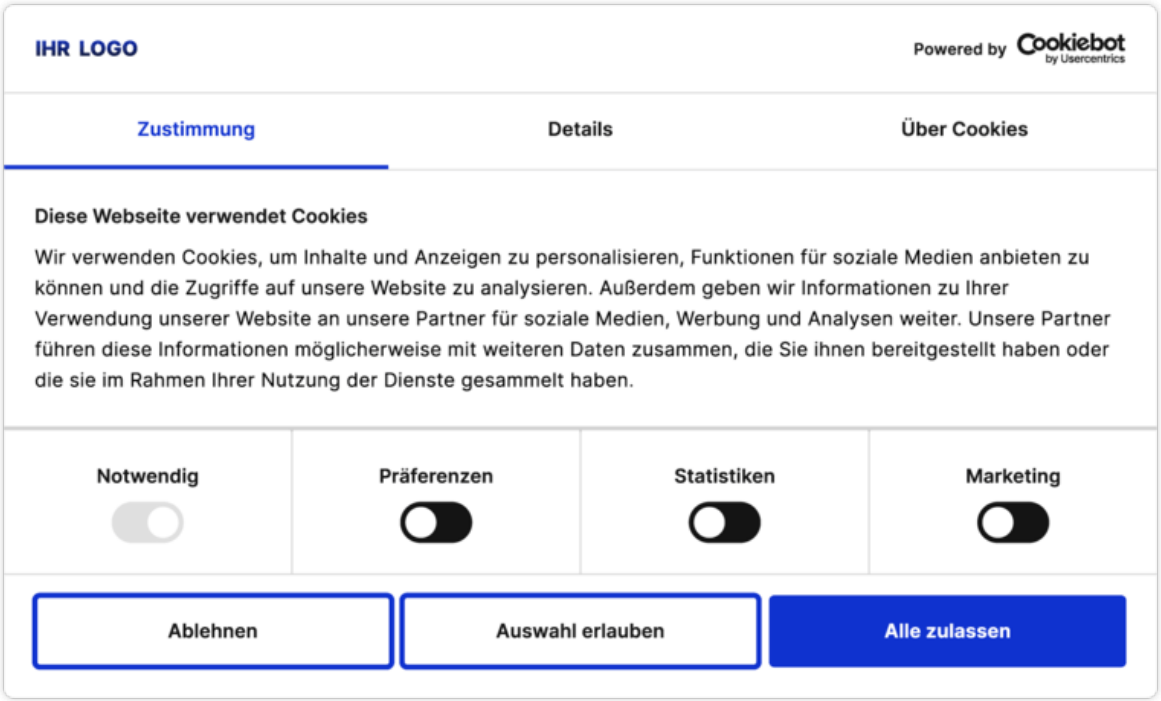


Abbildung 6: Beispielbild für ein Cookie-Banner auf einer beliebigen Webseite.
Quelle: URL: https://www.cookiebot.com/de/dsgvo-cookies/, verfügbar am 30.09.2023

Dieses Cookie-Banner muss den Webseitenbesucher darüber informieren, welche Daten erhoben werden und was mit ihnen passiert. Oft wird dabei in notwendige und verschiedene optionale Daten unterschieden, wobei die optionalen vom Webseitenbesucher abgelehnt werden können. Notwendige hingegen werden in jedem Fall beim Benutzer der Webseite erhoben. Sollte der Nutzer auch dies nicht akzeptieren, kann er die Seite nicht benutzen.

Targeting – ein Werkzeug des Online-Marketings

Wie umfangreich und weitreichend diese erhobenen Daten sein können, zeigt Tabelle 1. Über verschiedene **Targeting- und Tracking-Methoden**, die Teil von Online-Marketing sind, können der Ort und die Zeit des Internetzugriffs erfasst werden. Tracking beschreibt dabei das Erfassen von nutzerbezogenen Daten. Das Targeting stellt das gezielte Ansprechen von Nutzern nach Auswertung der erhobenen Daten in Form von personalisierter Werbung dar. Es können Schlüsselwörter aus dem Suchverlauf sowie der Browserverlauf hinsichtlich zuletzt besuchter Webseiten und Hard- bzw. Software-Spezifikationen, wie der Gerätetyp oder das verwendete Betriebssystem, verarbeitet werden. Ebenfalls fließen in das bisherige Suchverhalten viele weitere Daten, wie bspw. Profil- und Interessendaten aus sozialen Netzwerken, häufig verwendete Suchbegriffe und die Länge des Aufenthalts auf bestimmten Webseiten. Webseitenspezifisch können zudem Daten über das spezifische Verhalten auf dieser Webseite getrackt werden, und Benutzern, die eine bestimmte Webseite besucht haben, kann eben diese oder ähnliche Webseiten nach Verlassen der Webseite angezeigt werden. [59], [60]

Tracking-Methode	**Daten die erhoben werden / Beschreibung**
Geo-Tracking	Ort des Internetzugriffs (Stadt, Land, Adresse)
Time-Tracking	Zeit des Internetzugriffs (Uhrzeit, tags/nachts)
Contextual-Tracking	Schlüsselwörter, die auf häufig od. zuletzt besuchten Webseiten verwendet werden
Technical-Tracking	Hard- und Software-Spezifikationen (Gerätetyp, Betriebssystem)
Demografic-Tracking	User-Daten aus Webseiten und Internet
Behavioral-Tracking	Informationen über das Suchverhalten von Nutzern (besuchte Webseiten, aktuelle u. vergangene Suchverläufe, häufig verwendete Suchbegriffe, Profil- u. Interessendaten aus sozialen Netzwerken)
Retracking	Kürzliche besuchte Webseiten od. Profile, gekaufte Produkte od. Dienstleistungen werden erneut angezeigt

Tabelle 1: Übersicht aller üblichen Tracking-Methoden im Online-Marketing

Quelle: [60]

All diese Daten werden digitalen Identitäten bzw. Profilen zugeordnet, welche durch bestimmte Attribute eindeutig bestimmbar sind, auch wenn die reale Identität der Person hinter der digitalen Identität nicht immer eindeutig bestimmbar ist. Bei Datenlecks und Datenschutzverletzungen können diese Daten ebenfalls betroffen sein und unbefugten Personen zugänglich gemacht werden (siehe Abschnitt 1.1).

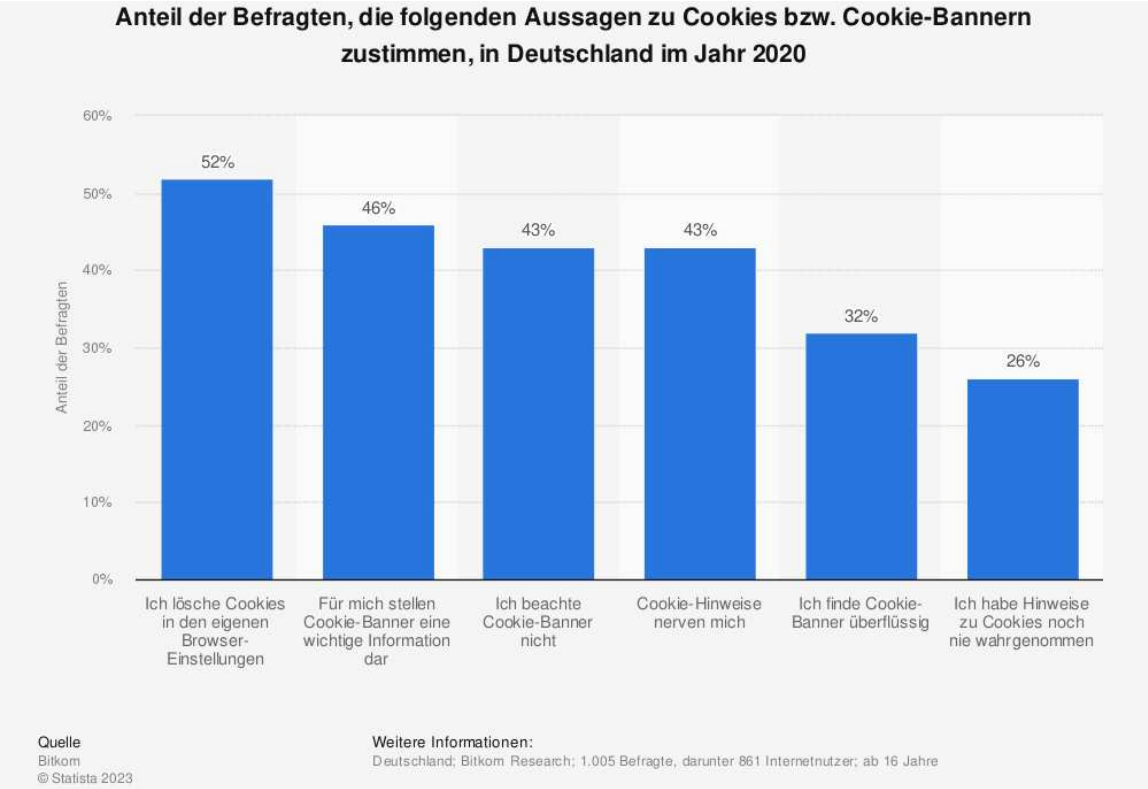


Abbildung 7: Umfrage zu Cookies und Cookie-Bannern auf Webseiten in Deutschland 2020

Quelle: [28]

Dies stellt für einen Großteil der Internetbenutzer ein Problem dar. Einer Statistik (Abbildung 7) aus dem Jahr 2020 zufolge löschen 52 % der befragten Personen Cookies in den eigenen Browsereinstellungen und für 46 % stellen die Cookie-Banner eine wichtige Informationsquelle dar. Jedoch sagen jeweils 43 % der Befragten ebenfalls aus, Cookie-Banner gar nicht zu beachten oder dass sie von Cookie-Bannern genervt seien. Eine mögliche Erklärung hierfür könnte sein, dass auf nahezu jeder modernen Webseite Cookie-Banner auf die Erhebung von Daten hinweisen und dass auf den meisten Webseiten diese Einstellungen nicht gespeichert, sondern bei jedem Aufruf der Webseite erneut abgefragt werden. Es ist daher denkbar, dass diese Personen nicht desinteressiert daran sind, was mit ihren Daten geschieht, sondern eher keine Zeit oder Lust haben, sich mit den Details von Cookies und den Auswirkungen der Erfassung personenbezogener Daten auseinanderzusetzen. Deshalb akzeptieren sie womöglich kollektiv alle Cookie-Banner, um die Webseite schnellstmöglich in vollem Umfang nutzen zu können. [28]

Die Erhebung ist vor allem dann ein Problem, wenn Benutzer sog. **ID-Provider** zur Verwaltung ihrer digitalen Identitäten verwenden. Sie haben oftmals die Möglichkeit, aus verschiedenen Quellen Daten zu erheben und zudem Zugriff auf mehrere digitale Identitäten von realen Personen. Benutzern ist meistens nicht ersichtlich, welche Daten und in welchem Umfang diese letztendlich erhoben und anschließend weiterverarbeitet werden.

2.1.2 ID-Provider

ID-Provider, auch Identitätsanbieter genannt oder kurz IdP, bieten zentrale Zugangssysteme für Service-Provider-Dienste, bei denen Nutzer sich anmelden können, sowie wichtige Cyber-Sicherheitsdienste für Service-Provider, wie die Authentifizierung eines Nutzers für SSO und die Autorisierung eines Zugriffs auf die Ressourcen der Identität über spezielle APIs [3]. Die wohl bekanntesten ID-Provider sind Google, Microsoft, Facebook und Apple – es gibt jedoch auch kleinere, wie bspw. das 2017 in Deutschland gegründete Unternehmen Verimi. Grundlegend funktionieren sie alle gleich. Nutzer richten bei einem ID-Provider ihrer Wahl ein Benutzerkonto ein, welches bestimmte Attribute der realen Identität einer Person benötigt, um eine digitale Identität der Person zu erstellen. [3], [19]

Google bspw. erfasst folgende Attribute, welche zur Erstellung eines Google-Kontos teilweise notwendig und optional sind: Vor- und Nachnamen, Geburtsdatum, Geschlecht, (mehrere) private oder Arbeitsadressen sowie eine Telefonnummer. Zusätzlich wird die Erstellung einer E-Mail-Adresse und das Festlegen einer Möglichkeit zur Identitätsbestätigung via Passwort oder Passkey-Verfahren benötigt. Die Verwendung eines Passwortes stellt eine Wissen-basierte Authentifizierung dar, während das Passkey-Verfahren Besitz-basiert ist. Benutzer können ebenfalls mehrere digitale Identitäten bzw. Google-Konten miteinander verknüpfen. Zum einen dient dies dem Schutz der miteinander verbundenen Konten, da beim Verlust der Identitätsbestätigung für eines der beiden Konten der Zugriff über das andere Konto weiterhin bestehen bleibt. Zum anderen kann Google nun sämtliche erhobenen Daten beider Konten miteinander vergleichen und bei bestimmten Voraussetzungen erhobene Daten beiden Konten zuweisen. Ebenfalls ist es möglich, das Google-Konto mit Konten anderer Google-Dienste, anderer ID-Provider und generell mit anderen digitalen Identitäten zu verknüpfen. Dem Nutzer bringt dies Komfort, da die Verknüpfung von Konten oft Vorteile hinsichtlich Bedienungsfreundlichkeit, Belohnungen oder Vorteile in einer anderen Form bringt. Gleichzeitig können die Service-Provider erhobene Daten nun unter Umständen untereinander teilen, was der Privatsphäre im Internet zu Schaden kommen kann. [53], [54]

Funktionsweise von ID-Providern

Diese Funktionen verleihen jedoch nicht die Charakteristik eines Identitätsproviders. Erst durch die Funktion, das Google-Konto als Login-Methode bei Dritten zu nutzen, macht Google zu einem Identitätsprovider (Abbildung 8).

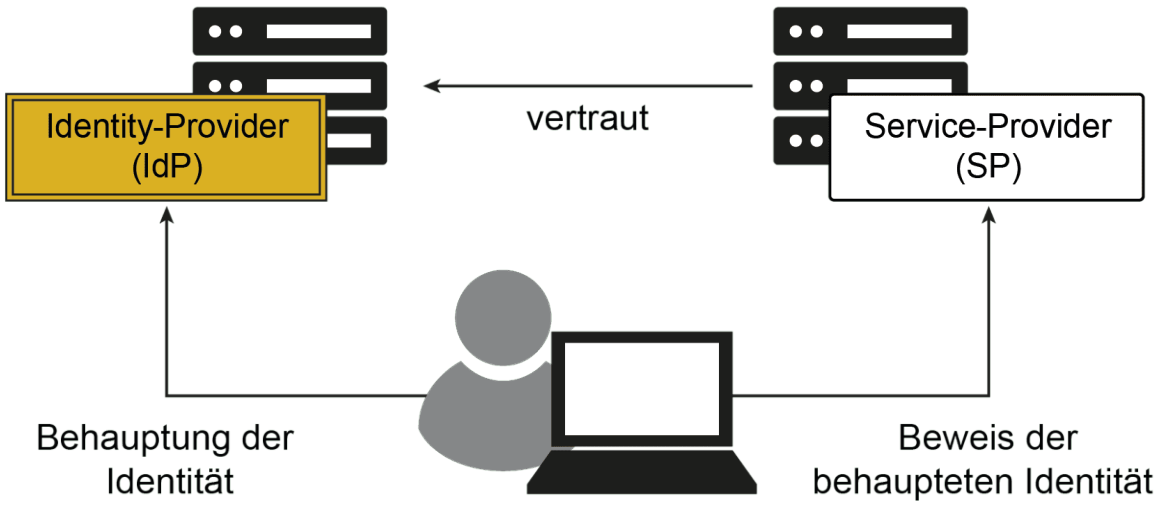


Abbildung 8: Modell Identity Provider

Quelle: [3]

Das Beispiel Google ausführend könnte ein möglicher Service-Provider ein Onlineshop wie Instant Gaming sein. Eine Person, welche bei Google ein Konto mit bestimmten Attributen erstellt hat, kann dieses Konto beim Service-Provider ebenfalls als Konto nutzen. Der Benutzer muss bei dem Service-Provider kein eigenes Konto einrichten, welches erneut bestimmte Attribute seiner realen Identität zur Erstellung der digitalen Identität sowie eine Identifikationsmöglichkeit wie E-Mail-Adresse und Passwort benötigt. Der Login ist für den Benutzer in erster Linie komfortabel, weil er unkompliziert und schnell ist, und weil er kein weiteres, möglichst sicheres Passwort erstellen und in Zukunft verwalten muss. Der Service-Provider verlässt sich dabei auf das Vertrauen zum ID-Provider, dass die vorgegebene Identität der Person korrekt ist, da das Google-Konto in diesem Fall über eine umfassende Sammlung von Informationen zur realen Identität verfügt. Es gibt mehrere Login-Möglichkeiten. Zum einen via E-Mail-Adresse und Passwort für das hauseigene Konto, zum anderen befinden sich über den Eingabefeldern für den Login im hauseigenen Konto gleich mehrere ID-Provider – neben Google ist hier ebenfalls ein Login über Facebook, Apple und Discord möglich (Abbildung 9). Ebenfalls ist zu beachten, dass beim erstmaligen Besuchen einer Webseite ein hauseigenes Konto erst eingerichtet werden muss, bevor die Webseite vollumfänglich benutzt werden kann. Der Login über einen ID-Provider benötigt diesen Arbeitsschritt nicht und bietet damit dem Benutzer noch mehr Komfort.

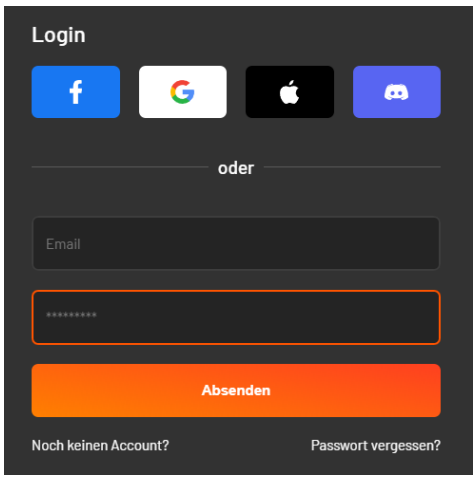


Abbildung 9: Screenshot des Login-Formulars des Online-Shops Instant-Gaming
Quelle: URL: https://www.instant-gaming.com/de/, verfügbar am 02.10.2023

Die Nutzung von ID-Providern beim Login auf beliebigen Webseiten führt dazu, dass der verwendete ID-Provider über bspw. das Demografic- oder das Behavioral-Tracking Daten erheben kann, auf die der IdP ohne den Login auf der Webseite keinen Zugriff hätte. Die Sammlung an personenbeziehbaren Daten wird daher noch größer und umfangreicher, und für den Benutzer wird unübersichtlicher, welche Daten große Firmen tatsächlich über die eigene Person besitzen.

Hinzukommt, dass je mehr digitale Identitäten unter einem Konto vereint werden, der Wert des Kontos und damit verbunden auch der Schaden bei Verlust des Kontos steigt. Google-Konten bspw. können mittlerweile über diverse Möglichkeiten, wie Passwort, 2-Faktor-Authentifizierung und Passkey, sowie durch Back-Ups in Form von eingeloggten Geräten oder anderen verknüpften E-Mail-Adressen, geschützt werden. Unangreifbar sind sie jedoch weiterhin nicht.

Datenökonomie

Der Begriff der Datenökonomie kann weit gefasst werden. Sie beschreibt die umfassende wirtschaftliche Nutzung und das Management von Daten. Dabei umfasst sie die Erfassung, Speicherung, Analyse, Nutzung und den Austausch von Daten zur Generierung von Werten. Bei diesen Werten handelt es sich oftmals um Geld. [31]

ID-Provider, wie Facebook bzw. der Mutterkonzern Meta, Google und Apple, erwirtschaften einen Großteil ihres Umsatzes durch Online-Werbung und -Marketing. Eine Statistik aus dem Oktober 2023 (Abbildung 10) besagt, dass der weltweite Umsatz von Meta im gesamten Jahr 2022 knapp 116,6 Mrd. US-Dollar betrug. Einer anderen, im Februar 2023 veröffentlichter Statistik (Abbildung 11) zufolge hat Meta im Jahr 2022 ca. 113 Mrd. US-Dollar Umsatz mit Werbung generiert, was rund 97 % des Gesamtumsatzes des Unternehmens darstellt. Zudem kann der Statistik ein Anstieg der Werbeumsätze um knapp 250 % in den letzten zehn Jahren von etwa vier Mrd. US-Dollar auf 113 Mrd. US-Dollar entnommen werden. [32], [33]

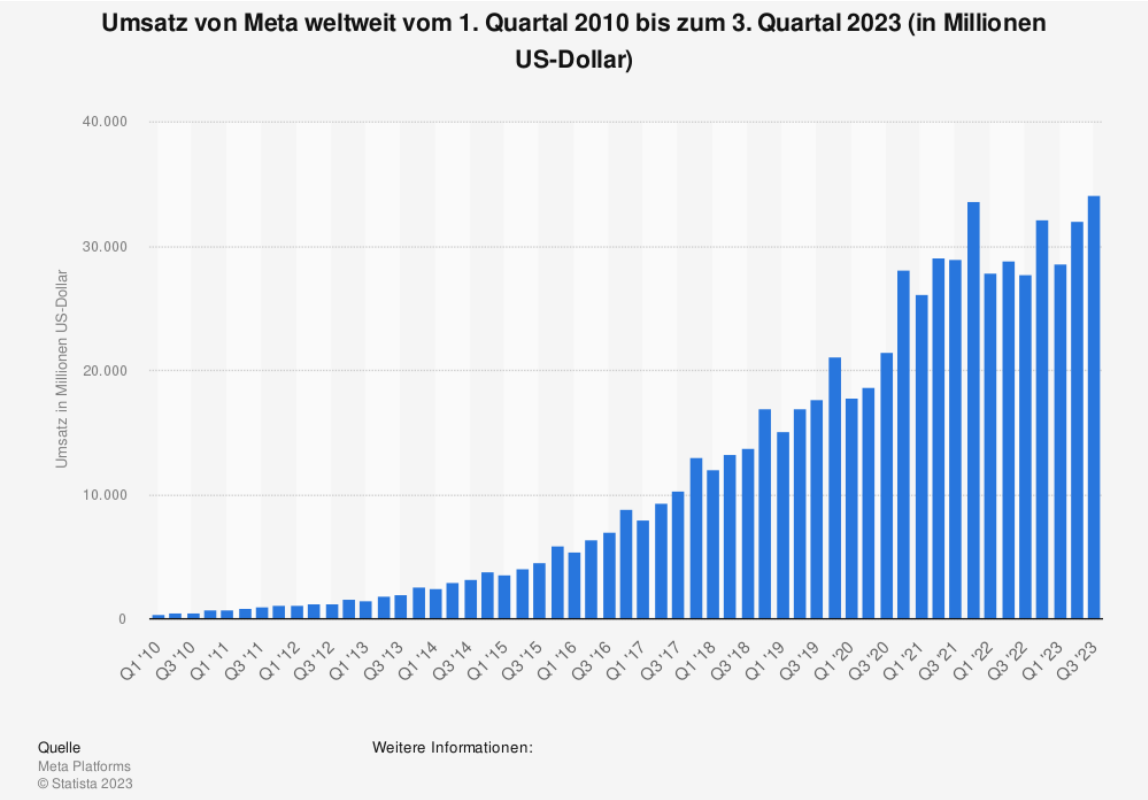


Abbildung 10: Umsatz von Meta weltweit bis zum 3. Quartal 2023

Quelle: [32]

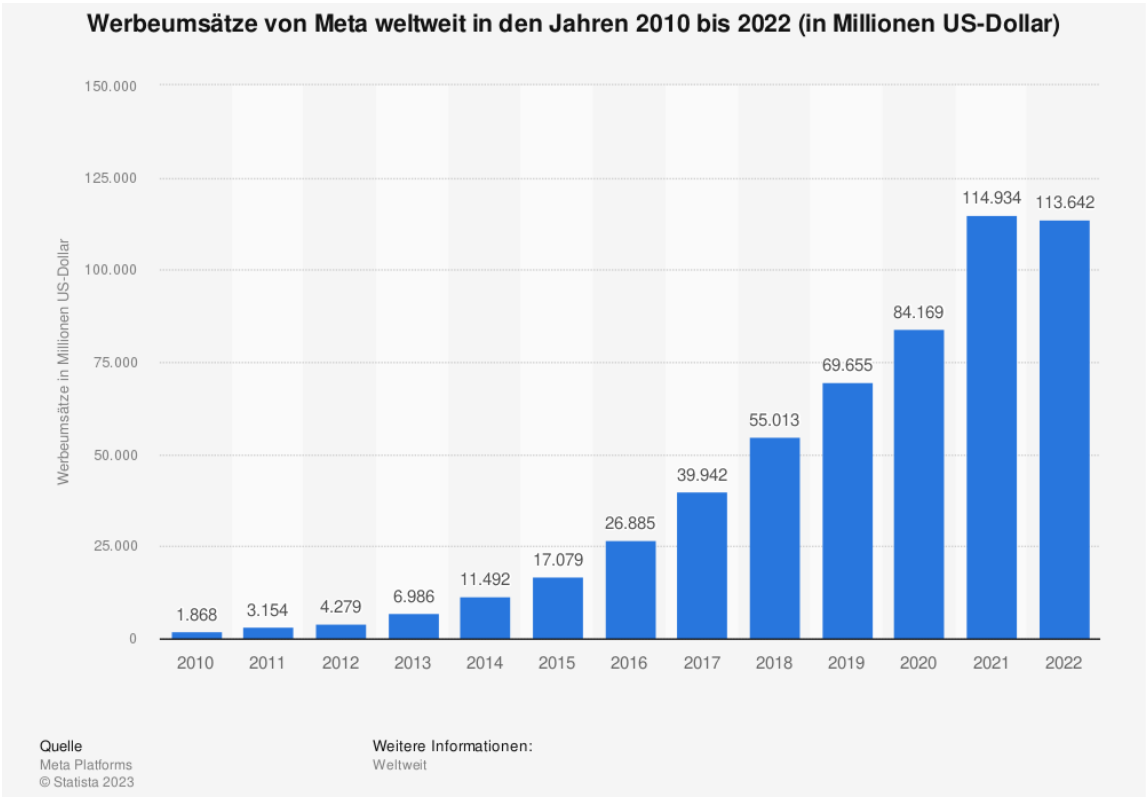


Abbildung 11: Werbeumsätze von Meta weltweit bis 2022

Quelle: [33]

Bei Google zeichnet sich ein ähnliches Bild. Eine Statistik aus dem Februar 2023 (Abbildung 12) zeigt einen weltweiten Jahresumsatz von etwa 280 Mrd. US-Dollar im Jahr 2022 und von knapp 256 Mrd. US-Dollar im Jahr 2021. Mit der Suchmaschine sowie YouTube-Werbung wurden 2021 ca. 191 Mrd. US-Dollar Umsatz generiert. Dadurch werden ca. 75 % des Gesamtumsatzes im Jahr 2021 erwirtschaftet. In einer weiteren Statistik (Abbildung 13), veröffentlicht im Februar 2023, wird der gesamte Werbeumsatz von Google 2021 mit etwa 209 Mrd. und 2023 mit etwa 224 Mrd. US-Dollar angegeben. Neben Meta erwirtschaftete Google ebenfalls mit ca. 80 % den Großteil des Umsatzes mit Werbung. [34], [35]

Für die Effizienzerhöhung von Werbemaßnahmen wird oftmals Werbung personalisiert. D. h. sie wird auf Basis von erhobenen Nutzerdaten an die Interessen, Ausgangssituationen und Suchverläufe von Nutzern angepasst und individualisiert (siehe Kapitel 2.1.1 Abschnitte Datenerhebung und Cookies sowie Targeting). Personalisierung von Werbung ist ein Aspekt von Datenökonomie. Einige Nutzer sehen darin Vorteile, da sie keine irrelevante Werbung erhalten, sondern für sie potenziell interessante Produkte und Dienstleistungen vorgeschlagen bekommen. Andere Nutzer können sich in ihrer Privatsphäre gestört fühlen, da diese Daten schließlich in einer Cloud gespeichert werden und theoretisch andere Menschen darauf zugreifen können, bspw. bei Hackerangriffen.

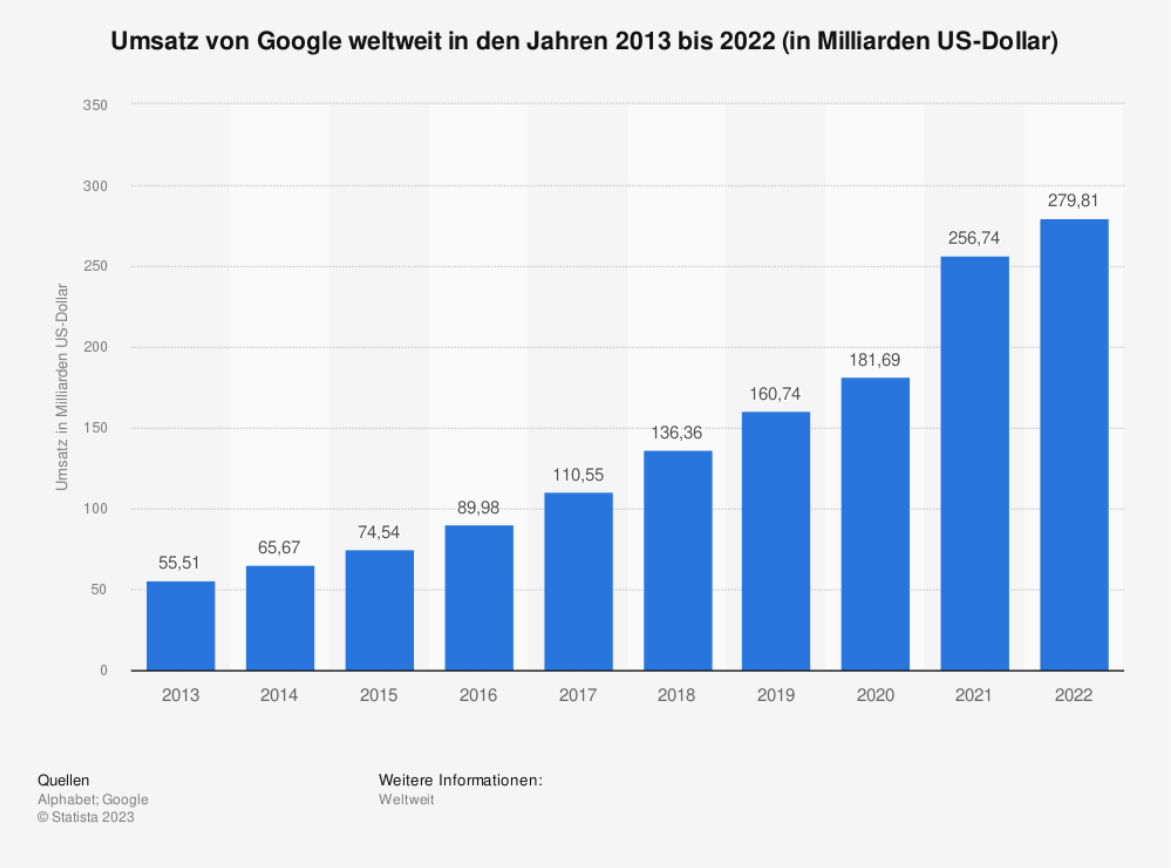


Abbildung 12: Umsatz von Google weltweit bis 2022

Quelle: [34]

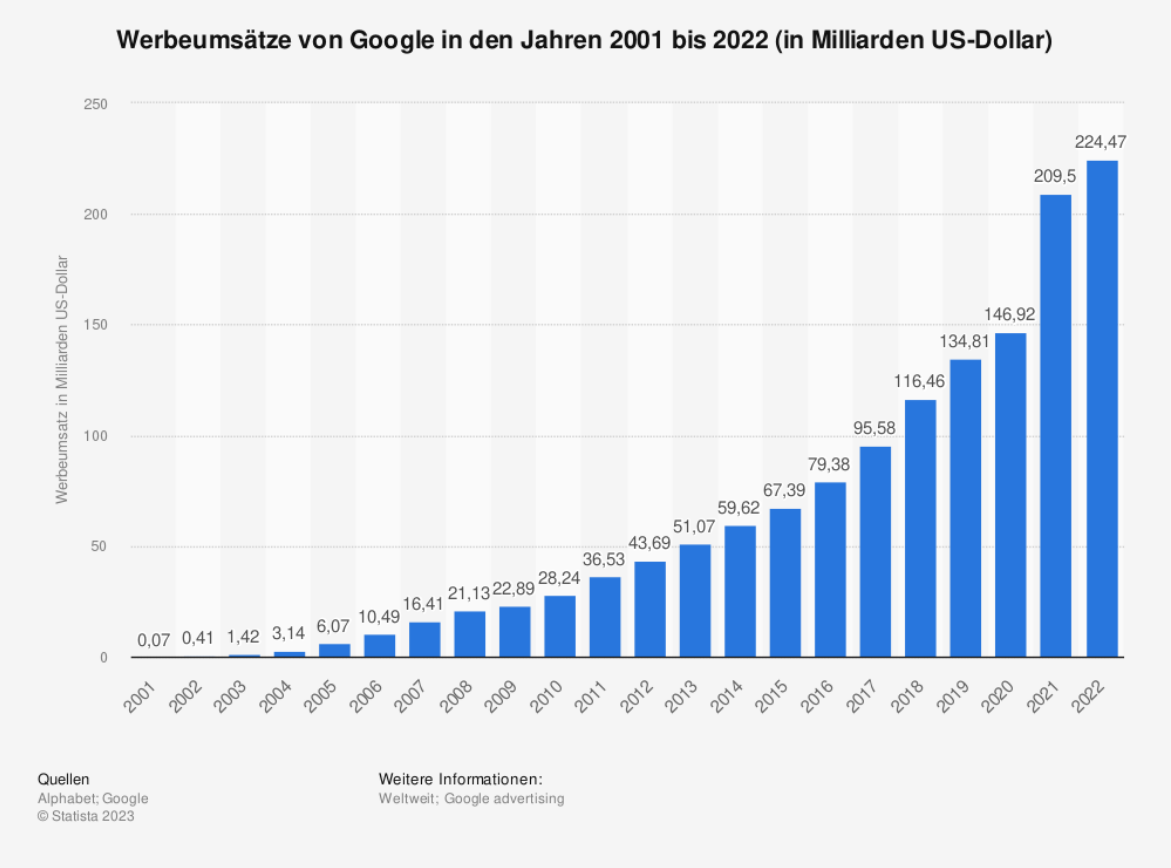


Abbildung 13: Umsatz mit Werbung von Google bis 2022

Quelle: [35]

Passkey-Technologie

Die Passkey-Technologie ist ein asymmetrisches Verschlüsselungsprinzip, bestehend aus zwei Schlüsseln: einem sog. **Private Key** und einem sog. **Public Key**. Der *Public Key* ist öffentlich zugänglich. Er wird verwendet, um Inhalte zu verschlüsseln und die Echtheit von digitalen Signaturen zu prüfen. Der *Private Key* hingegen ist nicht öffentlich zugänglich und wird ausschließlich auf dem Endgerät des Benutzers gespeichert. Er wird zum Entschlüsseln von Inhalten benötigt, die vorher mit dem *Public Key* verschlüsselt wurden. Im Fall der Passkey-Technologie von Google wird der Benutzer beim Login-Versuch auf einer beliebigen Plattform aufgefordert, ein Gerät, auf dem das entsprechende Google-Konto angemeldet ist, mit der gewählten Sicherheitssperre (Fingerabdruck, Gesichtsscan oder sonstiger Sperrbildschirmtyp) freizugeben. Sobald das Gerät entsperrt wurde, wird der Benutzer auf der entsprechenden Plattform eingeloggt. Passkey-Technologie ist daher eine Authentifizierung durch Besitz. [15]

2.1.3 Self-Sovereign Identity

Self-Sovereign Identity stellt den Gegenpol zu sog. ID-Providern dar. Während Identitätsprovider als IT-Dienstleister digitale Identitäten auf zentralisierten Cloud-Servern speichern und Personen den Zugang zu diesen Daten über spezielle APIs mit entsprechenden Identitätsnachweisen ermöglichen, zielt SSI auf eine dezentrale Verwaltung von Nutzerdaten durch die Nutzer selbst auf entsprechenden Endgeräten ab. Dadurch sollen Souveränität und der Schutz der Privatsphäre von Nutzern im Internet wachsen. Dies wird unter dem neuen Identitätsparadigma „User-Centric-Identity“ zusammengefasst. Es steht im klaren Gegensatz zur aktuell vorherrschenden „Enterprise-Centric-Identity“. [4]

SSI, auch selbstbestimmte Identitätskontrolle genannt, ermöglicht Nutzern, vollkommen unabhängig von Drittinstanzen wie ID-Providern, ihre digitalen Identitäten und weitere verifizierbare digitale Nachweise, auch genannt Verifiable Credentials, kurz VC, zu kontrollieren und zu verwalten. Allein die Nutzer bestimmen, wem und in welchem Umfang sie ihre Identitäts- und Nutzerdaten zur Verfügung stellen. VCs können beliebige Datenstrukturen aufweisen, weshalb sie für viele verschiedene Szenarien Anwendung finden können. Zur Realisierung dieses Konzepts werden laut [63] drei wichtige Elemente benötigt: dezentrale Identifikatoren, kryptografisch gesicherte Datenformate und Protokoll zur Peer-to-Peer-Kommunikation zwischen den beteiligten Akteuren. Dadurch zählt SSI zu Besitzbasierter Authentifizierung. [4], [63]

Verifiable Credentials sind kryptografisch gesicherte Datenformate, die Aussagen über eine bestimmte Entität abbilden. Diese werden genutzt, um verschiedene Identitätsattribute zu beschreiben, und können beliebige Datenstrukturen unterstützen. Ähnlich zu den Nachweisdokumenten im physischen Leben, wie Personalausweisen oder Zeugnissen, gliedern sich Verifiable Credentials in drei Hauptkomponenten: Sie enthalten Behauptungen über das Subjekt des Credentials, Metadaten wie Herausgeber, Typ und Datum sowie einen digitalen Beweis, der die Authentizität der Behauptungen sichert. Dieser Beweis kann eine digitale Signatur sein. Die Verifizierung dieser Behauptungen erfolgt über ein Kommunikationsprotokoll namens DIDcomm, welches auf dezentralen Identifikatoren basiert und von der Decentralized Identity Foundation entwickelt wird. [4], [63], [66]

Eine **digitale Signatur** ist ein asymmetrisches Kryptographie-Verfahren und verwendet Public Key Infrastrukturen, kurz PKI. Mit Hilfe eines geheimen Signaturschlüssels, dem *Privat Key*, wird zu einer digitalen Nachricht ein Wert berechnet, welcher Dritten ermöglicht, zusammen mit dem öffentlichen Verifikationsschlüssel, dem *Public Key*, die nicht abstreitbare Urheberschaft der Nachricht zu überprüfen (Abbildung 14). Der Public Key wird über eine PKI verfügbar gemacht. Durch dieses Verfahren werden digitale Signaturen und auch Inhalte, die mit einer digitalen Signatur versehen sind, manipulations- und fälschungssicher. Manipulationssicher heißt, dass bereits ausgestellte Dokumente mit einer digitalen Signatur nachträglich nicht bearbeitet oder verändert werden können. Da zum Erstellen von VCs bestimmte digitale Signaturen benötigt werden, können sie nicht ohne Weiteres gefälscht, also von unbefugten Dritten ausgestellt werden. Diese digitalen

Nachweise ermöglichen es, dass Subjekte ihre Identität nachweisen können, ohne sensible Daten preiszugeben. [11], [65]

Eine **Public Key Infrastruktur** ist ein hierarchisches System, das digitale Zertifikate für sicheres Kommunizieren bereitstellt. Basierend auf asymmetrischer Verschlüsselung werden Schlüsselpaare erzeugt, bestehend aus einem *Private* und einem *Public Key*. Um den Austausch zu erleichtern, werden Public Key Infrastrukturen gebildet, wo ein Root-Zertifikat bei einer vertrauenswürdigen Stelle erstellt wird und weitere Zertifikate daran geknüpft werden. [66]

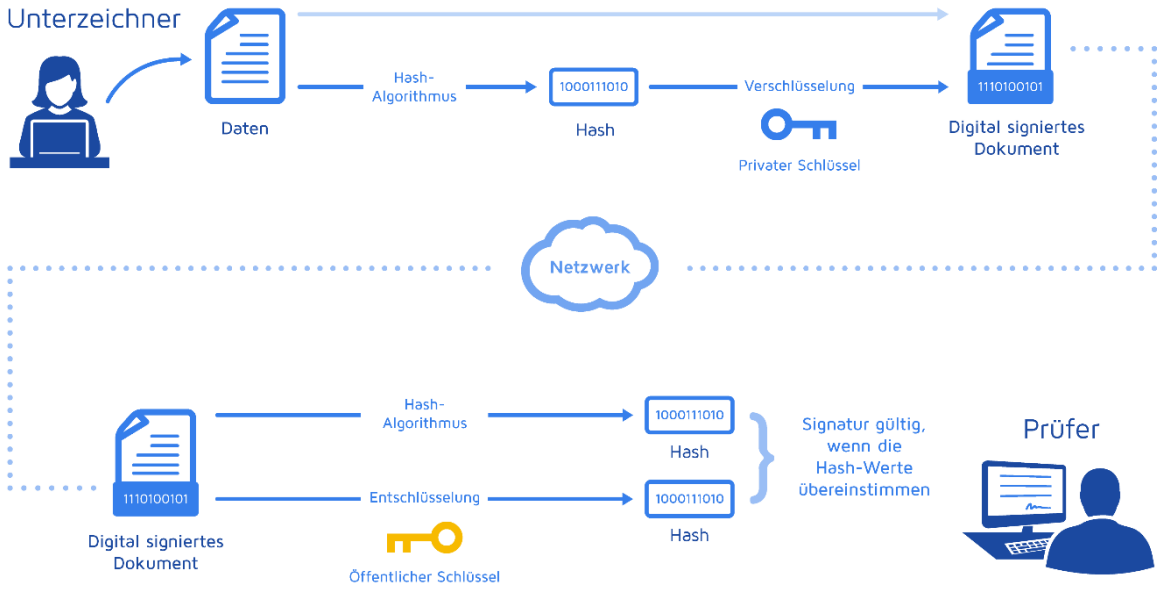


Abbildung 14: Schema der Funktionsweise von digitalen Signaturen

Quelle: [11]

Decentralized Identifiers, kurz DIDs, sind einzigartige URIs, die eine bestimmte Entität identifizieren und nach einem festgelegten Schema strukturiert sind. Sie ermöglichen eine dezentrale und unabhängige Verwaltung von Identifikatoren ohne eine zentrale Kontrollinstanz. DIDs bestehen aus einem Schema, einer Methode und einem methodenspezifischen Identifikator und haben das Ziel, eine weltweite Standardisierung für verifizierbare Identifikatoren zu etablieren. Diese Identifikatoren können für verschiedene Zwecke genutzt werden, etwa für die Ausstellung und Verifikation von Verifiable Credentials, wie z. B. Studentenausweisen. [4], [63]

DIDcomm ist ein Kommunikationsprotokoll, das auf DIDs basiert und in Zusammenarbeit mit dem Hyperledger-Projekt Aries von der DIF entwickelt wird. Es ermöglicht die sichere und vertrauenswürdige Kommunikation zwischen verschiedenen Identitäten und bildet eine wesentliche Komponente in der Architektur von Agenten, welche die Identitätsinhaber bei der Verwaltung und Nutzung ihrer Identität unterstützen. DIDcomm-Nachrichten basieren auf Asynchronität und Simplexbetrieb, wodurch Nachrichtenaustausch auch über beschränkte Netzwerkverbindungen wie Smartphones möglich ist. [4], [63]

Ein **Verifiable Data Registry**, kurz VDR, wird genutzt, um Informationen über Decentralized Identifiers und Verifiable Credentials zu speichern, zu aktualisieren und zu beschreiben. Es dient als Speicher für die öffentlichen DIDs der Herausgeber, Verifizierungsmechanismen von VCs und VC-Schemata zur Beschreibung von Attributen. Obwohl DTLs, wie Blockchains, oft als Technologie für solche Register genutzt werden, sind sie nicht zwingend erforderlich, besonders bei reinen Peer-to-Peer-Verbindungen. Diese Register müssen jedoch hohe Verfügbarkeit, Skalierbarkeit und Manipulationssicherheit aufweisen, um ein hohes Vertrauensniveau zu gewährleisten. [4], [63]

SSI-Ökosystem

Das **SSI-Ökosystem** besteht im Wesentlichen aus drei Akteuren und einer Infrastruktur zur Kommunikation der Akteure miteinander. Die drei Akteure, der Aussteller, der Besitzer und der Verifizierer digitaler Identitäten und Nachweise, bilden ein sog. **Trust Triangle** und tragen mit ihren definierten Aufgaben zur erfolgreichen Umsetzung des SSI-Ökosystems (Abbildung 15) bei. Als Infrastruktur werden VDRs verwendet. [4], [63]

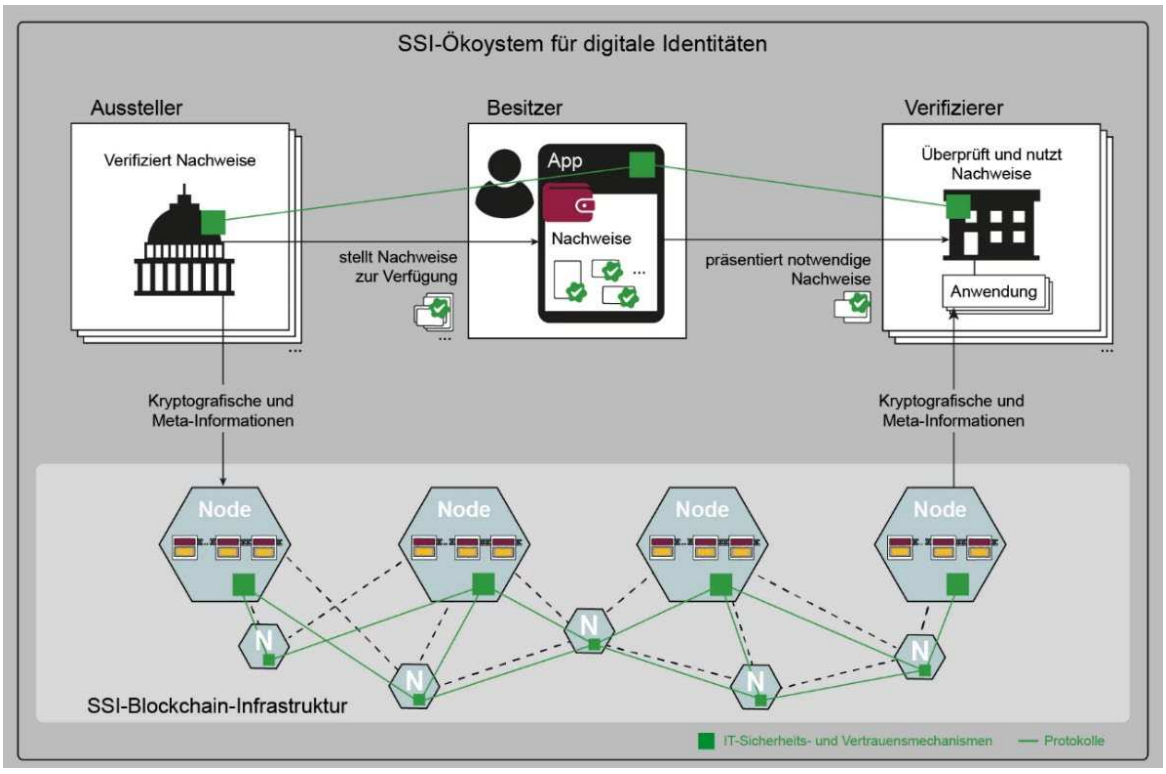


Abbildung 15: SSI-Ökosystem für digitale Identitäten und Nachweise

Quelle: [4]

Aussteller sind u. a. Unternehmen oder Organisationen mit entsprechender Berechtigung zur Ausstellung digitaler Nachweise, wie bspw. Einwohnermeldeämter, Hochschulen, sonstige Behörden oder Qualifizierungs- und Prüfungsorganisationen. Sie können folgende verifizierbare digitale Nachweise ausstellen:

- Bescheinigungen der Identität (z. B. eID-Verfahren des Personalausweises)
- Bestätigungen
- Befähigungen
- Befugnisse
- Qualifikationen
- Mitgliedsausweise [4]

Verifizierer stellen Akzeptanzstellen oder Anwendungen dar, welche das Vorzeigen bestimmter digitaler Nachweise erfordern, um dem Benutzer den Zugriff auf bestimmte Ressourcen oder Inhalte zu gewähren. Für die Verifizierung des Benutzers benötigt der *Verifizierer* Inhalte, Teilinhalte oder auch nur bestimmte Attribute der digitalen Nachweise. Dieser Vorgang wird **Presentation** (des VCs) genannt. Idealerweise passiert die Presentation vollkommen automatisch und ist durch die digitale Signatur sicher. Diese Voraussetzungen sind bspw. bestimmte Markierungen, die zur Ausstellung bestimmter digitaler Nachweise autorisierte Aussteller eindeutig verifizierbar machen. [4]

Besitzer sind im Kontext dieser Arbeit Personen, die ihre digitalen Identitäten und Nachweise unabhängig von Dritten selbstständig verwalten. Besitzer können jedoch ebenfalls Organisationen, Unternehmen oder Objekte sein. Zur Verwaltung von VCs benötigen sie eine Software, in der Regel auf einem mobilen Endgerät, um ihre digitalen Identitäten und Nachweise speichern und verwalten zu können. Dies ist in der Regel eine SSI-fähige App, eine sog. SSI-Wallet, wie z. B.: Lissi ID-Wallet, Trinsic Wallet, SWOL oder Hidy Wallet. *Besitzer* können digitale Nachweise von entsprechenden *Ausstellern* anfordern und in der SSI-Wallet abspeichern. *Verifizieren* können *Besitzer* bei Bedarf die benötigten digitalen Nachweise oder nur einige Informationen aus digitalen Nachweisen übermitteln. [4], [12], [13], [55], [61], [62]

Die Übermittlung der DIDs und VCs zwischen den drei Akteuren funktioniert über P2P ohne zentrale Übermittlungsstellen. In der Regel wird dafür DIDcomm verwendet. Zur Verifikation der Echtheit des übermittelten VCs seitens des Verifizierers wird das VDR benötigt (Abbildung 16). Es muss eine Dezentralisierung und Datensouveränität bieten. In VDRs werden laut [63] die öffentliche DID des Herausgebers, Informationen zum Verifizierungsmechanismen für VC-Überprüfung und VC-Schemata zur Beschreibung von VC-Attributen sowie Gültigkeitsdefinitionen gespeichert. Darüber hinaus werden Public Keys hinterlegt und über eine PKI bereitgestellt, um die Authentizität von VCs zu gewährleisten. Diese Public Keys dienen dazu, digitale Signaturen zu überprüfen, welche die Echtheit der VCs sicherstellen. Mithilfe der PKI können Prüfer die von Herausgebern signierten Daten verifizieren, wodurch die Integrität und Authentizität der bereitgestellten Identitätsinformationen sichergestellt werden. VDRs müssen daher eine hohe Verfügbarkeit und Skalierbarkeit vorzeigen können. [63], [67]

Es gibt einige Möglichkeiten, eine VDR umzusetzen. Laut [68] können eben DTLs wie Blockchain ebenfalls Web-Domänen, sog. Sidetrees und Key Event Receipt Infrastructure, kurz KERI, mögliche Alternativen sein. Auf einer Webdomäne könnte ein öffentlicher

DID gespeichert werden, auf dessen Bearbeitung nur die Administratoren der Webseite Zugriff haben. Diese Methode bietet ein gewisses Maß an Sicherheit, ist aber nicht so widerstandsfähig wie eine Blockchain, da zum Beispiel der Hosting-Anbieter die Website abschalten könnte. Sidetree ist eine Technologie, die DIDs und DID-Dokumente in einer temporären Layer-2-Speicherschicht namens Sidetree ablegt. Die Daten werden in Inter-Planetary File Systems, kurz IPFS, gespeichert, gebündelt und in Rollups an Blockchains verankert. Dies reduziert die Anzahl der erforderlichen Transaktionen zur Layer-1-Blockchain erheblich. Key Event Receipt Infrastructure ist eine weitere aufstrebende Innovation in der dezentralen Identität. Im Gegensatz zur Verankerung eines DIDs an einem bestimmten Ort oder Block innerhalb einer Kette vertraut KERI darauf, dass Knoten Key Event Logs, kurz KELs, bezeugen. Diese KELs können als verlässliche Quelle über die neuesten Schlüssel im Zusammenhang mit einer DID und deren Besitzer dienen. KERI-Protokolle sind im Gegensatz zu einer Blockchain nicht unveränderlich, sondern beruhen darauf, dass KERI-Zeugen vertrauenswürdig handeln und stets aktuelle KELs mit den richtigen Schlüsselereignissen bereitstellen. Das bedeutet, dass die Sicherheit des Systems nicht von einer unveränderlichen Blockchain-Struktur abhängt, sondern auf der Annahme beruht, dass bei ausreichend vielen und vertrauenswürdigen KERI-Zeugen die Gesamtheit ihrer Aktivitäten und Zeugnisse ein vertrauenswürdiges Maß an Sicherheit bieten können. [68], [69]

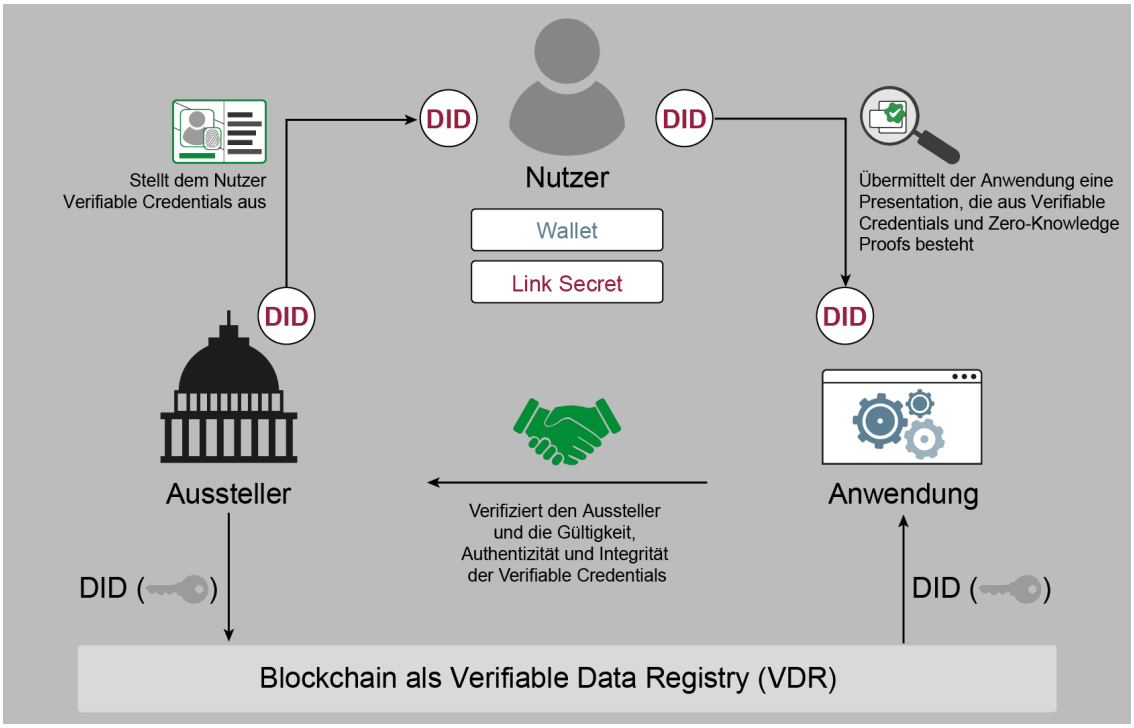


Abbildung 16: Architektur von Self-Sovereign Identity

Quelle: [4]

Passkey-Technologien funktionieren ähnlich. Abhängig vom Anbieter der Passkey-Verfahren kommt jedoch keine VDR als Infrastruktur zum Einsatz, sondern bereits bestehende Infrastruktur. Dadurch besitzen klassische SSI-Verfahren, unabhängig von sonsti-

gen Datenschutzrisiken und Eingriffen in die Privatsphäre von Nutzern durch einige Passkey-Anbieter, ein natürlich höheres Sicherheitsniveau.

2.1.4 Gegenüberstellung von IdP und SSI

Abschließend lässt sich feststellen, dass das Konzept IdP durch die weitreichende Verbreitung und Vernetzung großer Konzerne wie Google für den Endnutzer komfortabler sind. Sie sind bereits etabliert, bieten einen zentralen Zugang zu verschiedenen Diensten und vereinfachen die Anmeldung. Im Gegensatz dazu erfordern SSI-Lösungen möglicherweise mehr Selbstverantwortung bei der Verwaltung von Identitäten und könnten anfänglich komplexer erscheinen, da sie auf dezentralen, selbstverwalteten Daten basieren. Sie sind noch nicht weit verbreitet. Nutzer müssten daher von einem bekannten System auf ein neues unbekanntes System umsteigen. Viele digitale Identitäten auf einem Konto eines IdP zu vereinen birgt jedoch auch Sicherheitsrisiken. Viele ID-Provider bieten daher neben dem klassischen Passwort, welches, wie in 1.1 bereits analysiert, nur mit viel Aufwand sicher ist, auch Sicherheitsmaßnahmen wie 2-Faktor-Authentifizierung oder Back-up-Email-Adressen an. Mit der Passkey-Technologie werden diese Accounts zukünftig vermutlich noch sicherer.

Für Personen, die viel Wert auf Privatsphäre und Datenschutz im Internet legen, gab es jedoch bisher kaum komfortable Alternativen. Passwort-Manager sind eben doch auch nur Verwaltungssoftware für entschlüsselbare Passwörter. An dieser Stelle setzen SSI-Wallets an – eine unabhängige und Cloud-freie SSI-Lösung zur Verwaltung digitaler Identitäten und Nachweise.

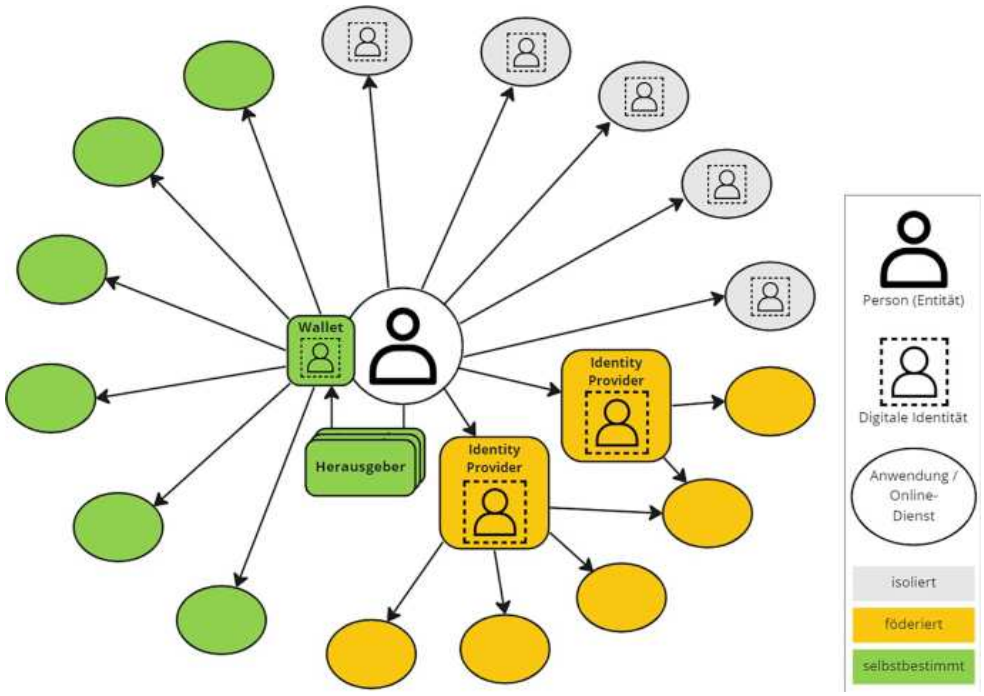


Abbildung 17: Grundmodell des Identitätsmanagements

Quelle: [55]

In Tabelle 2 werden die wichtigsten Merkmale beider Konzepte zusammengefasst und einander gegenübergestellt. Es ist wichtig anzumerken, dass beide Konzepte ihre Rechtfertigung haben. Sie agieren in gegensätzlicher Weise und bieten somit eine Alternative für Benutzer (Abbildung 17). Die Entscheidung darüber, welches Konzept das vermeintlich bessere ist, obliegt dem individuellen Ermessen jeder Person. Gegenwärtig dominieren ID-Provider das Feld. SSI-Lösungen befinden sich noch am Anfang, und es bedarf noch erheblicher Anstrengungen, um diese Lösungen für eine breite Nutzerschaft komfortabel zu gestalten.

Merkmal	**ID-Provider (IdP)**	**Self-Sovereign Identity (SSI)**
Datenverwaltung	Zentralisierte Speicherung auf Cloud-Servern	Dezentrale Verwaltung durch Benutzer auf eigenen Endgeräten
Benutzeranmeldung	Zentrale Anmeldung bei verschiedenen Diensten	Unabhängige Verwaltung ohne Drittanbieter
Datenschutz	Sammlung und möglicher Austausch von Benutzerdaten zwischen Service-Providern	Zusammenführung von Daten und Zuordnung einer bestimmten digitalen Identität schwieriger
Identitätsausstellung	Ausstellung digitaler Nachweise durch ID-Provider	Aussteller können Unternehmen oder Organisationen sein
Verifikation	ID-Provider bestätigen die Identität der Person basierend auf den bereitgestellten Daten	Verifizierung durch Prüfung digitaler Nachweise, die vom Besitzer vorgelegt werden können
Sicherheit	Sicherheitsmaßnahmen wie Passwörter, 2-Faktor-Authentifizierung	Verwendung von digitalen Signaturen und VDR für höhere Sicherheit
Komfort	Einfacher, schneller Zugang zu verschiedenen Diensten durch zentrale Anmeldung	Umstieg auf neue Technologie notwendig, nicht weit verbreitet, kaum Implementierungen auf bekannten Plattformen
Souveränität	Benutzer vertrauen ID-Providern, ihre Identität zu bestätigen	Benutzer haben die volle Kontrolle über ihre digitalen Identitäten und Nachweise

Tabelle 2: Zusammenfassung und Gegenüberstellung der wichtigsten Merkmale der beiden Konzepte zur Verwaltung von digitalen Identitäten ID-Providern und Self-Sovereign Identity

2.2 Hidy Wallet

Die **Hidy Wallet** ist eine, im Rahmen des Verbundprojektes ID-Ideal vom Blockchain Competence Center Mittweida entwickelte, SSI-Wallet.

ID-Ideal ist ein Forschungsprojekt des BMWK, welches im Rahmen des Innovationswettbewerbs „Schaufenster Sichere digitale Identitäten“ im Mai 2021 ins Leben gerufen wurde und sich einer Lösung der Problematik der Verwaltung und Sicherheit digitaler Identitäten sowie der damit verbundenen benutzerbezogenen Daten widmet. Aus allen digitalen Identitäten soll eine rechtssichere Identität, basierend auf staatlichen Dokumenten wie Personalausweis oder Reisepass, entstehen, deren sämtliche personenbezogenen Daten beim Nutzer, statt bei Unternehmen, gespeichert werden. Der Nutzer soll die vollständige Kon-

trolle über die eigenen Daten und deren Verwendung erhalten. Die übergeordnete Vision des Forschungsprojektes ist ein rechtssicherer Raum im Internet, genannt TrustNet. „Im TrustNet sind die Akteure eindeutig identifizierbar, die ausgetauschten Information verifizierbar und Transaktionen rechtssicher. Gleichzeitig soll die Datensouveränität für alle Akteure sichergestellt werden.“ [8]

TRUSTnet – Vertrauenswürdige Netzwerke in der Industrie 4.0 ist ein Forschungsprojekt des BMBF, welches dieses sichere Netzwerk aufbauen soll. Nach [9] soll dieses Overlay-Netzwerk sichere, dezentrale Prozessnetze ermöglichen, auch wenn dafür verwendete Netzinfrastrukturen, wie das Internet, grundsätzlich als nicht vertrauenswürdig einzustufen sind. Es soll als Gegenpol zum sog. Darknet fungieren, wo der Fokus auf maximaler Anonymität liegt, und eine Plattform etablieren, auf der Personen aufgrund der gewährleisteten Identifizierbarkeit keine illegalen Aktivitäten ausführen, Straftaten begehen oder irreführende Informationen sowie Hass verbreiten können. In erster Linie geht es dem Projekt um berufliche Seriosität. Bei Erfolg des TRUSTnets besteht jedoch die Möglichkeit, das Netzwerk auf viele weitere Aspekte auszurollen und eine „sichere Version des Internets“ aufzubauen. [9]

Die **Hidy Wallet** wird als App für mobile Endgeräte umgesetzt und soll zur Verwaltung digitaler Identitäten dienen. Darunter zählen sowohl amtliche und offizielle Nachweise wie Personalausweis, Reisepass und Studierendenausweis, als auch nicht amtliche Anwendungsbereiche, wie das Speichern und Verwalten von Tickets für Konzerte und Shows. Sie kann VCs von Ausstellern entgegennehmen, diese abspeichern und an Verifizierer übermitteln. Derzeit können bereits zu Demonstrationszwecken Mitarbeiter- und Studierendenausweise von der HSMW sowie Handelsregisterauszüge ausgestellt und abgespeichert werden. Zudem können auch verschiedene Formen von Kunden- und Treuepunktkarten in der App gesammelt werden, sofern diese auf einem Barcode basieren. Ebenso ist es möglich, direkt über die App mit Bitcoin Lightning zu bezahlen.

2.3 WordPress

WordPress ist ein kostenloses quellenoffenes Content-Management-System, kurz CMS, mit dem Webseiten erstellt und verwaltet werden können. Weitere Funktionen können mit Hilfe von Plug-ins, Add-ons und Themes hinzugefügt sowie bereits implementierte Funktionen erweitert werden. [6], [23]

2.3.1 Content-Management-Systeme

Als **Content-Management-System**, kurz CMS, z. Dt. Inhaltsverwaltungssystem, werden Softwarelösungen bezeichnet, mit deren Hilfe Inhalte wie Bilder, Texte und Videos vorwiegend auf Webseiten, aber auch auf anderen Medienkanälen zentral verwaltet werden können. Neben WordPress sind weitere bekannte CMS Joomla, TYPO3, Shopify und Wix. [36]-[38], [56]

Das bekannteste und am häufigsten genutzte CMS ist WordPress. Einer Statistik (Abbildung 18) aus dem Oktober 2023 zufolge benutzen 43,1 % aller untersuchten Webseiten weltweit WordPress als CMS. Dahinter folgen Shopify mit 4,1 % und Wix mit 2,5 %. Joomla wird von nur 1,8 % der untersuchten Webseiten verwendet und TYPO3 kommt in den Top 10 gar nicht vor. Aus einer weiteren Statistik geht ebenfalls hervor, dass WordPress im Oktober 2023 unter den Content-Management-Systemen einen Marktanteil von 63 % besitzt, gefolgt von Shopify mit 5,9 % Marktanteil und Wix mit 3,7 %. Subdomains wurden nicht berücksichtigt. [29]

Um dem Plug-in die größtmögliche Verbreitung und den größtmöglichen Anwendungsbereich zu geben, fiel daher die Entscheidung auf ein Plug-in für das CMS WordPress.

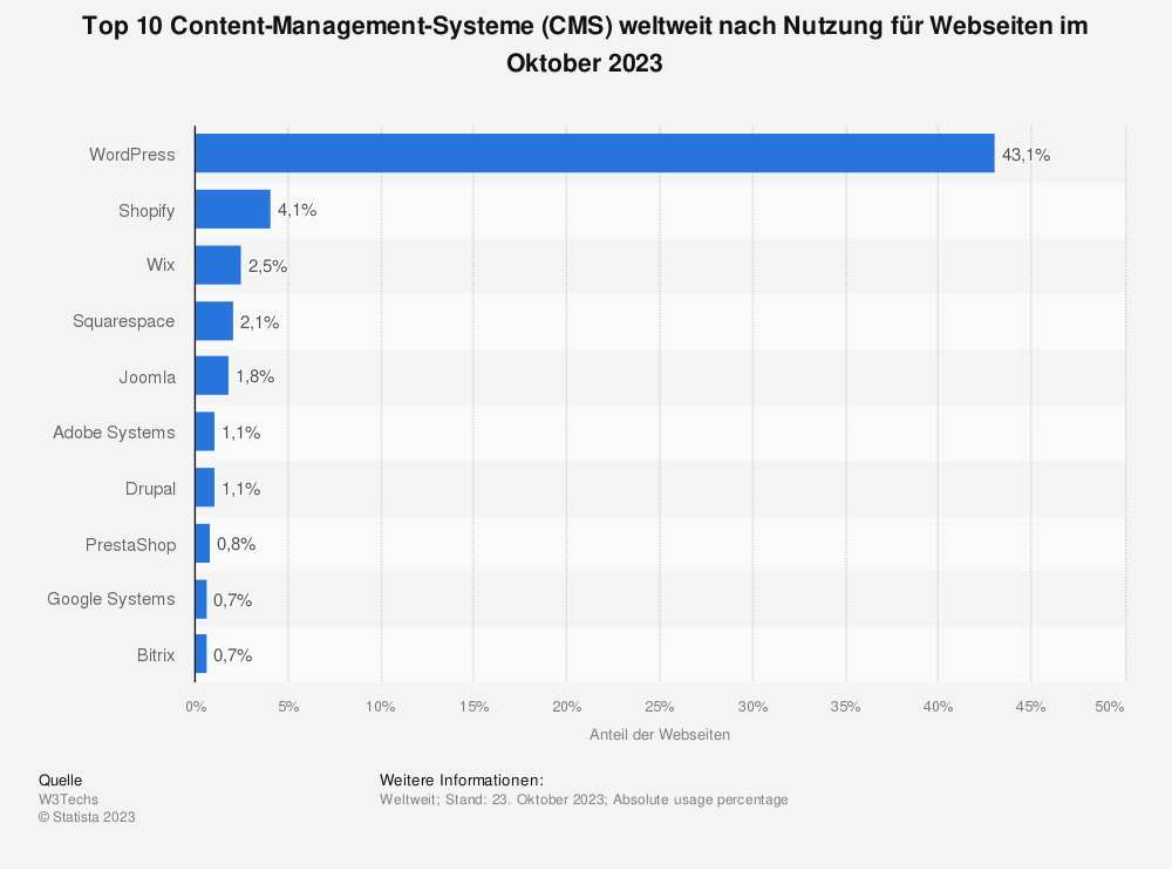


Abbildung 18: Nutzungsanteil der Content-Management-Systeme (CMS) weltweit im Oktober 2023

Quelle: [29]

2.3.2 Gutenberg Editor ein Pagebuilder

Damit keine Programmierkenntnisse zum Erstellen der Webseiten-Frontends notwendig sind, wurden sog. **Pagebuilder**, ugs. Baukasten-Systeme oder Block-Editor, entwickelt. Diese Werkzeuge operieren häufig auf Grundlage eines visuellen „Drag & Drop“-Editors, der es gestattet, Design-Elemente mühelos mit der Maus zu bearbeiten und zu platzieren. Zahlreiche Pagebuilder stellen vorgefertigte Vorlagen und Elemente bereit, die als Aus-

gangspunkt für individuelle Designs dienen können. Diese Vorlagen und Elemente werden Gutenberg Editor-Blöcke, kurz GEB, genannt.

Der Gutenberg Editor, kurz GE, ist in drei Hauptmenüs strukturiert: das Seitenmenü, das Schnellauswahlmenü und das Block-Editor-Menü. Das Seitenmenü (Abbildung 19) dient der übersichtlichen Verwaltung von allen installierten Blöcken und ermöglicht das Hinzufügen, Bearbeiten und Löschen dieser innerhalb des Editor-Fensters. Das Schnellauswahlmenü (Abbildung 20) bietet eine praktische Auswahl an Blöcken und Funktionen, die häufig oder zuletzt verwendet wurden. Es ermöglicht einen schnellen Zugriff auf gängige Bearbeitungsfunktionen und erleichtert somit die Gestaltung des Inhalts. Das Block-Editor-Menü (Abbildung 21) enthält alle Steuerelemente und Einstellungen, die zur Bearbeitung und Anpassung einzelner Blöcke vorhanden sind.

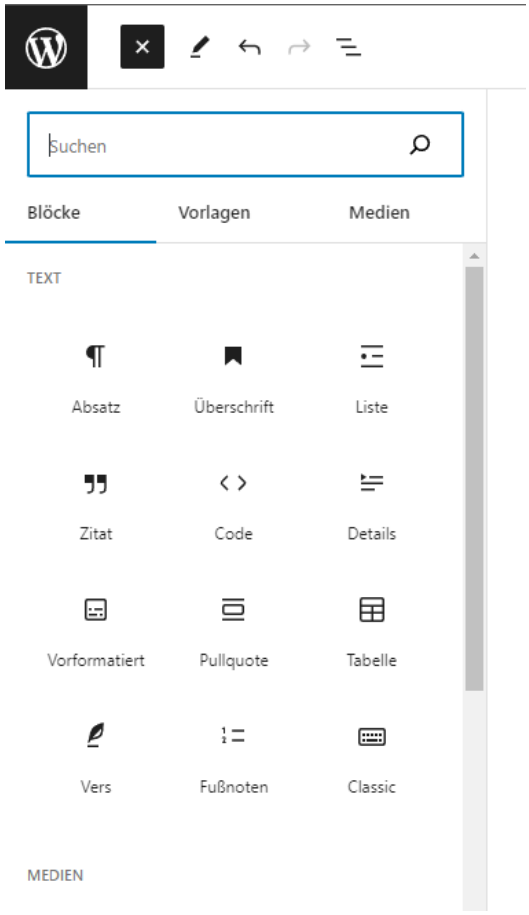


Abbildung 19: Screenshot des Gutenberg Editor-Seitenmenüs zum Einfügen von Gutenberg Editor-Blöcken

Quelle: WordPress-Testumgebung

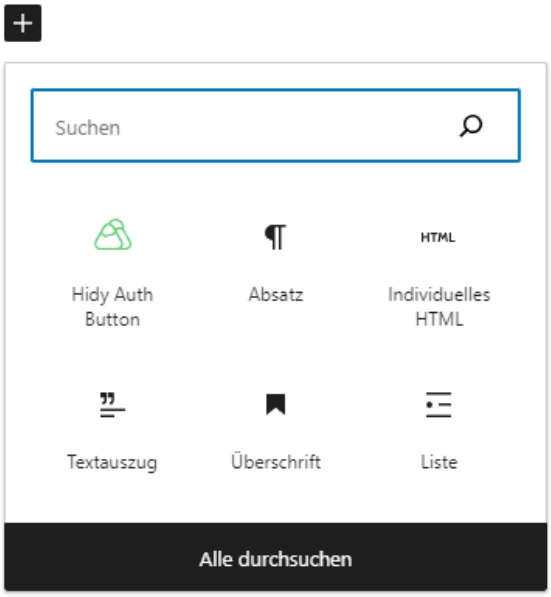


Abbildung 20: Screenshot des Gutenberg Editor-Schnellmenüs zum Einfügen von Gutenberg Editor-Blöcken

Quelle: WordPress-Testumgebung

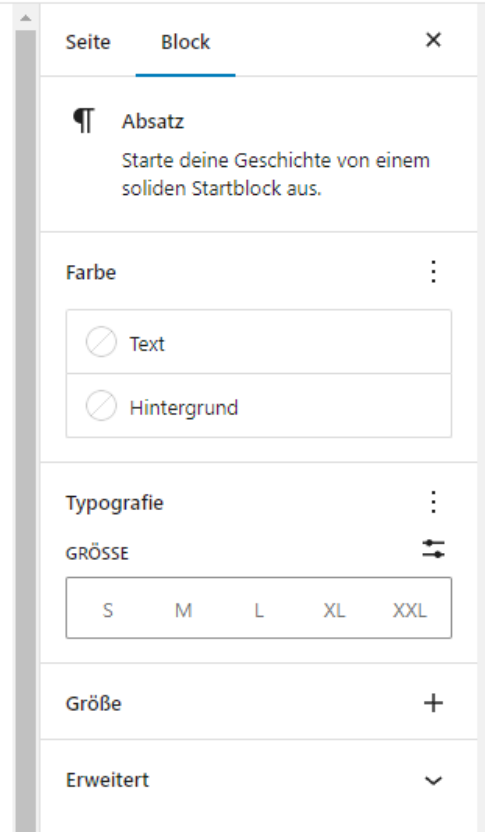


Abbildung 21: Screenshot des Gutenberg Editor-Blockmenüs individuellen Anpassen bestimmter Blöcke nach vorgegebenen Richtlinien

Quelle: WordPress-Testumgebung

Eine standardmäßige WordPress-Installation umfasst bereits den Open-Source-Pagebuilder **Gutenberg Editor**. Einer Statistik (Abbildung 22) aus dem August 2023 zufolge ergibt sich daraus ein Marktanteil von ca. 65,6 % auf WordPress-Seiten. Nutzern von WordPress steht es jedoch offen, einen anderen Pagebuilder als Plug-in zu installieren und damit den Gutenberg Editor zu ersetzen. Mit 20,5 % stellt Elementor den größten Konkurrenten des GE dar, gefolgt von WPBakery mit 12,5 %. [17]

Page Builder	Marktanteil
Gutenberg	ca. 65,6 %
Elementor	20,5 %
WPBakery	12,5 %
Beaver Builder	1,1 %
Oxygen	0,3 %

Abbildung 22: Ranking der beliebtesten WordPress Pagebuilder nach Marktanteilen (Stand: 11.08.2023)

Quelle: [17]

Neben der Installation von anderen Pagebuildern als Plug-in für WordPress können auch Add-ons für einige Pagebuilder-Plug-ins in WordPress installiert werden. So ist es möglich, für bestimmte Pagebuilder eigene Elemente mit individuellen Funktionen zu entwickeln, welche anschließend per „Drag-and-Drop“-Prinzip von Nutzern auf ihrer Webseite platziert werden können, ohne dass diese manuell konfiguriert werden müssen. [10]

Aufgrund der Marktdominanz des Gutenberg Editors mit knapp zwei Drittel der Marktanteile und der Verfügbarkeit in jeder standardmäßigen WordPress-Installation bietet sich der GE sehr gut an, wenn eine möglichst weitreichende Verbreitung der Software angestrebt wird.

3 Konzept

Wie in 2.3 und 2.3.2 beschrieben, bietet WordPress Softwareentwicklern die Möglichkeit, neue Funktionalitäten via Plug-in, Add-on oder Add-in einzubinden. Für eine schnelle und großflächige Verbreitung einer Softwarelösung sollten für Endbenutzer der Installationsaufwand und die Handhabung möglichst unkompliziert sein. Der Gutenberg Editor ermöglicht das programmierfreie „Zusammen-Klicken“ von Webseiten aus vorgefertigten Blöcken. Solche Blöcke können über ein Add-on dem Gutenberg Editor hinzugefügt und mit Backend-Logik versehen werden. Daher fiel die Entscheidung, die Schnittstelle zwischen Webseiten und der Hidy Wallet über einen Gutenberg Editor-Block zu realisieren. Das grundlegende Konzept des Validierungsprozesses kann jedoch auch ohne die Nutzung des GE weiterverwendet werden. Das nachfolgend erklärte Konzept umfasst die Plug-in-Registrierung in WP, die Block-Einbindung in den GE sowie den Validierungsprozess, um VCs, die in der Hidy Wallet bereits gespeichert sind, auf einer Webseite zu validieren. Wie dieses Konzept um weitere, z. T. komfortbringende, Funktionen erweitert werden kann, wird in Kapitel 8 ausgeführt.

Bei der Software-Lösung handelt es sich um ein WordPress-Plug-in aufgrund weitreichender Backend-Komponenten, aber auch um ein Gutenberg-Editor-Add-on, da der GE mit dem Block um eine neue Funktion erweitert wird und dabei die Bibliothek als Grundlage dient.

WordPress bietet Entwicklern grundsätzlich zwei Möglichkeiten, ein Gutenberg Editor-Add-on zu entwickeln. Einerseits stellt WP ein Werkzeug namens „Create-Block“ bereit, welches mit dem Befehl „@wordpress/create-block pluginName“ aufgerufen wird und einen funktionslosen GEB erzeugt. Andererseits kann ein GEB auch „from scratch“, also vollkommen selbstständig, ohne Nutzung vorgefertigter Bibliotheken und Vorlagen, entwickelt werden. Letzte Variante bietet Entwicklern mehr Freiheiten und die Einarbeitung ist leichter. Daher wurde das Validierungs-Plug-in „from scratch“ entwickelt. Dabei werden jedoch trotzdem WP- und GE-Funktionen verwendet. [10]

3.1 Plug-in-Registrierung und Integration in WordPress

WordPress ist größtenteils in PHP programmiert. Zur Implementierung von Plug-ins stellt WordPress einige PHP-Funktionen bereit. Im Verzeichnis einer WordPress-Installation gibt es einen eigenen Ordner, in dem Plug-ins in ihren eigenen Verzeichnissen mit allen benötigten Dateien in separaten Ordnern gespeichert werden. Jedes Plug-in benötigt für die Registrierung und Integration eine Hauptdatei im Verzeichnis, welche wiederum eine Kopfzeile mit Informationen zum Plug-in (siehe Quellcode 1).

```
/*
 * Plugin Name:       My Basics Plugin
 * Plugin URI:        https://example.com/plugins/the-basics/
 * Description:       Handle the basics with this plugin.
 * Version:           1.10.3
 * Requires at least: 5.2
 * Requires PHP:      7.2
 * Author:            John Smith
 * Author URI:        https://author.example.com/
 * License:           GPL v2 or later
 * License URI:       https://www.gnu.org/licenses/gpl-2.0.html
 * Update URI:        https://example.com/my-plugin/
 * Text Domain:       my-basics-plugin
 * Domain Path:       /languages
 */
```

Quellcode 1: Kopfzeile einer WordPress-Plug-in-Hauptdatei

Quelle: [10]

Die Hauptdatei trägt normalerweise den Namen des Plug-ins und ist für die Implementierung aller wichtigen PHP-Funktionen und Plug-in-Dateien sowie für weitere Plug-in-Einstellungen zuständig. Folgende Funktionen werden benötigt, um Plug-in-Dateien in WordPress zu integrieren:

- *wp_enqueue_script()* für die Pfadbestimmung von JavaScript-Dateien
- *wp_enqueue_style()* für die Pfadbestimmung von CSS-Dateien
- *add_action()* für die Integration von neuen PHP-Funktionen
- *add_filter()* für die Veränderung von PHP-Funktionen
- *add_menu_page()* für das Erzeugen einer Administrationsseite mit Einstellungen für das Plug-in
- *update_option()* überschreibt den Wert einer Variable in der WP-Datenbank

Bei Benutzung des Create-Block-Befehls werden die Hauptdatei mit allen benötigen Funktionen und Klassen sowie alle weiteren Dateien und Verzeichnisse automatisch erzeugt. Beim Entwickeln eines GEB from scratch müssen alle benötigten Dateien selbst angelegt werden. [10]

3.2 Block-Einbindung in Gutenberg Editor

Der Gutenberg Editor ist primär in JS geschrieben und bietet einige JS-Funktionen zur Einbindung von Add-ons. Der Pagebuilder bedient sich zudem der JS-Bibliothek React zum Erstellen von Benutzeroberflächen aus interaktiven Komponenten.

Für die Einbindung eines neuen Blocks in den Gutenberg Editor mittels des Create-Block-Befehls wird in der Hauptdatei eine PHP-Funktion, die die WordPress-Methode register_block_type() verwendet, generiert. Diese WP-Funktion verweist auf einen Unter-

ordner im Plug-in-Verzeichnis, welcher alle Informationen beinhaltet, die für das Einbinden und Rendern des GEBs benötigt werden. Dieses Vorgehen kann ebenfalls beim From-Scratch-Entwickeln angewendet werden. Auf diese Art und Weise können vergleichsweise einfach viele GEBs in das Plugin eingebunden werden, die größtenteils Frontend-Komponenten darstellen sollen. Die Verwendung des JavaScript-Objekts registerBlockType() bietet mehr Freiheiten und eine einfachere Implementierung. Ein JavaScript-Objekt ist ein Datentyp, welcher aus Schlüssel-Wert-Paaren besteht und mehrere dieser Paare abspeichern kann, wie ein Array. Einem Schlüssel, wie z. B. „Title“, wird immer ein Wert, z. B. „Hidy Validation Plug-in“, zugeordnet. Das JS-Objekt registerBlockType() ist folgendermaßen aufgebaut:

- **Title:** Name des Blocks
- **Description:** Beschreibung des Blocks
- **Category:** GE-Kategorie im Seitenmenü
- **Icon (optional):** Icon des GEB in Seiten- und Schnellmenü
- Keywords (optional): Aliasname des Blocks zum besseren Auffinden
- Styles (optional): Alternative Stile des Blocks (Blockmenü)
- **Attributes (optional):** Im Block gespeicherte und übergebene Variablen
- Example (optional): Strukturierte Beispieldaten
- Variantions (optional): Alternative Variationen des Blocks (Blockmenü)
- Support (optional): Steuerung der im GE verwendeten Funktionen
- Transforms (optional): Transformationsregeln für den Block
- Parent (optional): Regelt Abhängigkeiten zu und „Verschachtelungen“ in anderen Blöcken
- Ancestor (optional): Regelt Abhängigkeiten zu und „Verschachtelungen“ in anderen Blöcken (speziell übergeordnete Blöcke)
- Block Hooks (optional): Regelt Abhängigkeiten zu anderen Blöcken (speziell Blöcke, an die der Block angefügt werden kann)
- **Edit:** Beschreibt die Struktur des Blocks im Editor (Frontend-Komponenten, die im Editor zu sehen sind)
- **Save:** Beschreibt die Struktur des Blocks in der Live-Ansicht der Webseite (Frontend-Komponenten, die in der Live-Ansicht der Webseite gerendert werden)

Die fett geschriebenen Keys „title“, „description“, „category“, „icon“, „attributes“, „edit“ und „save“ sind für das Validierungs-Plug-in besonders wichtig. Die weiteren Keys können für diese Arbeit vernachlässigt werden. [10]

3.3 Validierungsprozess

Der Validierungsprozess beschreibt die Abfolge bestimmter Handlungen durch Benutzer der Hidy Wallet, dem Validierungs-Plug-in und maschineller Verarbeitungsprozesse, die zur Validierung eines Verifiable Credentials erfolgen müssen (Abbildung 23).

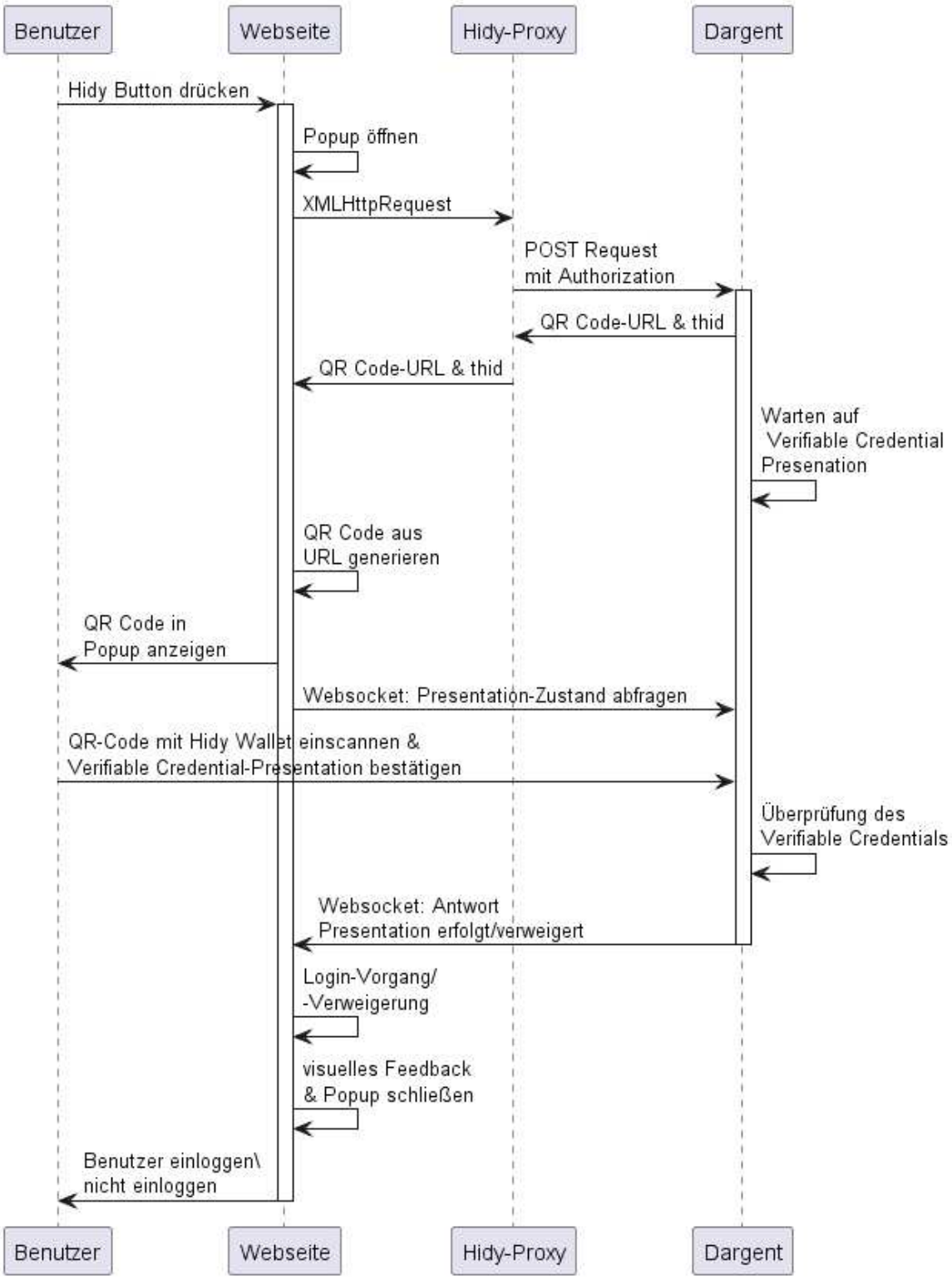


Abbildung 23: Sequenzdiagramm des Validierungsprozesses

Quelle: Eigenkreation mit PlantUML [24]

Der Benutzer betätigt einen Knopf auf der Webseite. Dadurch wird eine automatische Abfolge bestimmter Funktionen gestartet. Zuerst wird ein Pop-up mit einem Ladesymbol und weiteren Informationen geöffnet.

Die Webseite sendet mittels XHR über einen Proxy, den Hidy-Proxy, um die CORS-Richtlinien zu umgehen, eine POST-Anfrage zur VC-Validierung an einen derzeit zentralen Validierungsserver, den sog. „Dargent“. Der Dargent antwortet mit einer einmaligen URL und einer dazugehörigen, einmaligen ID, namens thid.

Auf der Webseite wird aus der URL ein QR-Code, unter Nutzung der Open Source-JavaScript-Bibliothek QRious, generiert. Anschließend wird der QR-Code mit der Bezeichnung des geforderten digitalen Nachweises im Pop-up angezeigt. [18]

Der Nutzer muss den QR-Code mit einem Endgerät, auf dem die Hidy Wallet installiert ist, scannen. Dabei ist es egal, ob dies in der App oder einer anderen Kamera-Anwendung geschieht. Sollte der QR-Code nicht mit dem QR-Code-Scanner der Hidy Wallet eingescannt werden, die App jedoch installiert sein, öffnet sie sich automatisch und zeigt ein Pop-up mit dem geforderten digitalen Nachweis sowie weitere Informationen. Sofern der geforderte Nachweis in der Hidy Wallet gespeichert ist, kann der Benutzer nun der Presentation an die Webseite zustimmen oder diese ablehnen. Sollte der geforderte Nachweis nicht in der Wallet gespeichert sein, kann keine Presentation erfolgen und der Vorgang muss abgebrochen werden.

Der Dargent wartet unterdessen, dass eine Presentation des VC erfolgt. Ist der digitale Nachweis in der Wallet gespeichert und der Nutzer hat der Presentation zugestimmt, überprüft der Dargent die Validität des gesendeten Nachweises. Bei erfolgreicher Prüfung wird der Status der Presentation-Anfrage der entsprechenden thid auf „verifiziert“ geändert. Sollte die Validitätsprüfung nicht erfolgreich oder der geforderte Nachweis nicht in der Hidy Wallet des Nutzers gespeichert sein und muss der Vorgang abgebrochen werden. Dies erfolgt derzeit über einen Timeout bei einer Zeitüberschreitung von einer Minute.

Die Webseite startet nach dem Generieren des QR-Codes aus der URL einen Websocket, welcher den Status der Presentation-Anfrage beim Dargent für eine Minute abfragt. So lange hat der Nutzer Zeit, die VC-Presentation durchzuführen.

Abhängig vom Wert, auf den der Status der Presentation-Anfrage geändert wird, gibt die Webseite unterschiedliche Rückmeldungen an den Nutzer. Diese können sinngemäß folgende sein (Anlage 2, Abbildungen 4, 5, 6 und 7):

- Presentation erfolgreich: Login-Vorgang wird gestartet.
- Presentation nicht erfolgreich: kein Login möglich.
- Zeitüberschreitung: Presentation hat zu lange gedauert, bitte erneut versuchen.
- Fehler bei der Verarbeitung, bitte erneut versuchen.

Im Idealfall verlief die Presentation des VCs reibungslos und erfolgreich, sodass weiterführend ein Login-Vorgang gestartet werden kann.

4 Implementierung

Das folgende Kapitel bietet einen detaillierten Einblick in die technische Umsetzung des Hidy-Validierungs-Plug-ins hinsichtlich des verwendeten Technologie-Stacks, der Softwarearchitektur, der aktuellen Funktionalitäten sowie der derzeitigen Benutzeroberfläche.

4.1 Technologie-Stack

Der Technologie-Stack für die Entwicklung des Plugins ist vielschichtig und umfasst verschiedene Sprachen und Bibliotheken. Das Backend des Plugins, das die Einbindung in WordPress und die Nutzung von dessen Funktionen sowie der WordPress-Datenbank ermöglicht, ist vollständig in PHP programmiert. Ebenfalls ist die VC-Presentation Backend-seitig in PHP umgesetzt und verwendet zusätzlich für die POST-Anfrage an den Dargent cURL. Die Integration des Plugins in den Gutenberg Editor erfordert JavaScript, da dieser Editor in dieser Sprache programmiert ist. Speziell nutzt der Gutenberg Editor die JavaScript-Bibliothek React, welche auch für die Realisierung dieses Plugins benötigt wird. Sie ermöglicht eine effiziente Implementierung dynamischer Komponenten. Ebenfalls wird für die Verarbeitung von Nutzerinteraktionen und die Aktualisierung des User Interfaces JS verwendet. Für die Generierung des QR-Codes, eine zentrale Funktion des Plugins, kommt die freie JavaScript-Bibliothek QRious.js zum Einsatz. Diese Bibliothek wandelt einen eingegebenen Text in einen QR-Code um und rendert diesen in einem Canvas-Element, welches zuvor auf der Seite platziert wurde. Die Gestaltung der Benutzeroberfläche der Einstellungsseite erfolgt mittels HTML-Elementen, während für die Stilisierung sämtlicher Frontend-Komponenten CSS verwendet wird. [18]

4.2 Softwarearchitektur

Model-View-ViewModel

Das Model-View-ViewModel, kurz MVVM, ist ein Architekturmuster in der Softwareentwicklung, das zur Strukturierung von Anwendungen verwendet wird. Es gliedert sich in drei Hauptkomponenten:

- **Model** (z. Dt. Modell): Das Modell repräsentiert die Daten und die Geschäftslogik der Anwendung, das sog. Backend. Hier werden Daten verwaltet und verarbeitet, unabhängig von der Benutzeroberfläche.
- **View** (z. Dt. Ansicht): Die Ansicht ist die Benutzeroberfläche, die dem Benutzer angezeigt wird, das sog. Frontend. Sie stellt die visuelle Darstellung der Daten dar und reagiert auf Benutzerinteraktionen.

- **ViewModel**: Das ViewModel agiert als Bindeglied, auch Middleware genannt, zwischen Modell (Backend) und Ansicht (Frontend). Es bereitet die Daten aus dem Modell so auf, dass sie für die Ansicht optimal dargestellt werden können. Das ViewModel enthält Logik, die für die Präsentation der Daten benötigt wird, aber nicht direkt zur Datenverarbeitung gehört.

MVVM dient dazu, die Trennung von Daten, Geschäftslogik und Benutzeroberfläche zu erleichtern. Durch diese Struktur können Änderungen an einem Bereich (z. B. Daten) durchgeführt werden, ohne die anderen Bereiche (z. B. UI) stark zu beeinflussen. Es ermöglicht auch eine bessere Testbarkeit und Wartbarkeit der Anwendung, da jeder Bereich unabhängig voneinander behandelt werden kann. Insgesamt unterstützt MVVM eine klare und saubere Strukturierung von Anwendungen. Die Aufteilung in diese drei Komponenten fördert einen modularen Aufbau, der die Anwendung dynamisch anpassbar und erweiterbar macht, da jede Komponente unabhängig voneinander entwickelt, getestet und gewartet werden kann. [41], [42]

Umsetzung des Validierungs-Plug-ins nach MVVM (Abbildung 24)

Das **Modell** wird durch die PHP-Dateien admin-page.php und hidy-auth-plugin.php sowie hidy-proxy.php repräsentiert. Sie stellen das Backend dar. Die Datei hidy-auth-plugin.php ist die Hauptdatei des Plug-ins. Sie wird für die Registrierung aller wichtigen Dateien in WordPress benötigt (siehe Abschnitt 3.1). Die admin-page.php erzeugt die Einstellungsseite des Plug-ins, wo Webseitenbetreiber das Plug-in an ihre Anforderungen anpassen können. Sie übernimmt CRUD-Operationen in der WordPress-Datenbank. Über die hidy-proxy.php wird die Presentation-Anfrage an den Dargent gesendet (siehe Abschnitt 3.3).

Die JavaScript-Dateien hidy-block-functions.js und hidy-block-register.js sind für die Präsentation (**Ansicht**) der Benutzeroberfläche verantwortlich und bilden das Frontend. In der Datei hidy-block-register.js wird mit dem JS-Objekt registerBlockType() der Gutenberg Editor-Block erzeugt, sämtliche Frontend-Komponenten gerendert und der Block im Gutenberg Editor registriert (siehe Abschnitt 3.2). Die Datei hidy-block-functions.js umfasst alle wichtigen Funktionen zur Aktualisierung des UIs. Zusätzlich definiert hidy-block-style.css alle stilistischen Regeln.

Als **Bindeglied** (ViewModel) sorgt die Datei hidy-block-functions.js für die Verarbeitung von Nutzereingaben, verarbeitet Datenmanipulationen, nimmt Daten aus dem Backend entgegen, verarbeitet diese und koordiniert die Aktualisierung des Frontends. Es übernimmt die logische Schicht des Architekturmusters, ohne direkt die Datenbankinteraktionen zu steuern. Diese JS-Datei dient als Middleware.

Zudem sind weitere Dateien notwendig, die hier als „**Ressourcen**“ bezeichnet werden. Dazu gehören Bilder, Grafiken und Icons, zusammengefasst unter dem Begriff „Assets“, die aus Designgründen und für visualisiertes Feedback notwendig sind. Visuelles Feedback im UI bezieht sich auf die grafische Reaktion des Benutzerinterfaces auf Aktionen

des Nutzers oder auf den Fortschritt von Prozessen. Dieses Feedback dient dazu, dem Benutzer ein Verständnis für seine Handlungen zu vermitteln oder den Status von Prozessen anzuzeigen. Weiter werden die Konfigurationsdateien vcs.json und config.json für Modularität und eine dynamische Anpassbarkeit des Plug-ins benötigt. Konkret beinhaltet die Datei vcs.json Informationen über VCs, welche für die Presentation benötigt werden. Die Datei config.json enthält Informationen und Daten, die die Konfiguration der VC-Presentation betreffen. Fast alle Komponenten benötigen Informationen aus diesen Dateien, um Prozesse durchführen zu können. Für die Softwarearchitektur nicht benötigte Dateien sind die readme.txt und die licence.txt. Diese Dateien dienen der Erläuterung des Plugins und bieten Anweisungen zur Installation und Verwendung sowie zur Festlegung rechtlicher Rahmenbedingungen und Nutzungsbestimmungen für das Plug-in. Die Verzeichnisstruktur mit allen Dateien befindet sich in Anlage 1.

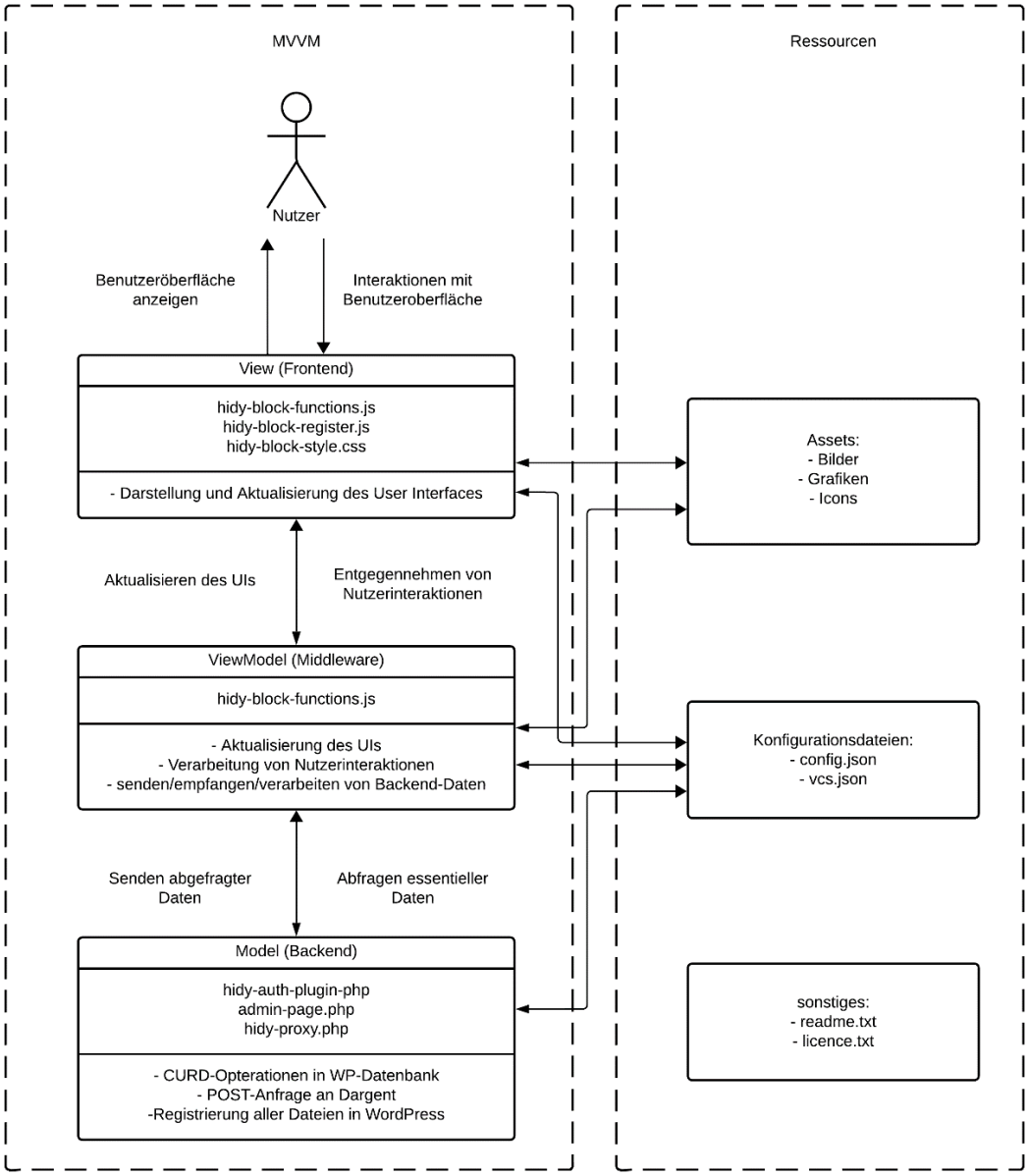


Abbildung 24: Softwarearchitektur des Validierungs-Plug-ins nach MVVM-Muster

Quelle: Eigenkreation mit LucidChart [30]

4.3 Funktionalitäten

Die derzeitigen Funktionen des Plugins umfassen alle wichtigen Abläufe und Funktionen, die für die **Validierung von Verifiable Credentials im Hidy-Ökosystem** notwendig sind.

Über die vcs.json-Datei kann der Pool digitaler Nachweise mit Angaben zu Namen, Verwendung und einem eindeutigen Identifikationstoken sowie weiteren Informationen, die für die Presentation benötigt werden, dynamisch und in beliebigem Ausmaß erweitert werden. Aus diesem Pool können Webseitenbetreiber über die Einstellungsseite des Plug-ins einen Nachweis für die Verifikation festlegen. Anschließend kann in der Editoransicht des GE der Block, welcher den Validierungsprozess (siehe Abschnitt 3.3) startet, beliebig oft und an verschiedenen Stellen auf der Webseite einfügen werden. Nutzer können durch Interaktion mit dem entsprechenden Knopf, welcher durch den Gutenberg Editor-Block auf der Webseite hinzugefügt wird, den Validierungsprozess starten.

Das Backend initiiert dann eine VC-Presentation-Anfrage an den Verifizierer „Dargent“. Dieser stellt eine URL und eine thid aus, die auf der Webseite angezeigt werden. Durch einen QR-Code wird diese Information Nutzern verfügbar gemacht. Diese können nun den QR-Code mit einem Endgerät, auf dem die Hidy Wallet installiert ist, scannen und bei Vorhandensein des geforderten Verifiable Credentials dieses vorzeigen.

Das UI aktualisiert sich entsprechend dem Fortschritt des Validierungsprozesses und dem jeweiligen Status und gibt wichtige Informationen an Nutzer weiter. Nach einer erfolgreichen Präsentation wird das Pop-up geschlossen, jedoch erfolgt zu diesem Zeitpunkt noch kein automatischer Login. Der **Validierungsprozess** ist damit abgeschlossen.

Zur Vollendung des **Verifizierungsprozesses** muss das Plug-in um eine Login-Mechanik, die bei einer erfolgreichen VC-Presentation aufgerufen wird, erweitert werden. Ansätze dafür werden in Abschnitt 8.1.1 vorgestellt.

4.4 Benutzeroberfläche

Die Benutzeroberfläche des Hidy-Validierungs-Plug-ins besteht im Wesentlichen aus zwei Elementen. Beim Einfügen des Gutenberg Editor-Blocks auf die Seite wird das erste Element sichtbar. Ein sog. „Button“ (Abbildung 25), z. Dt. Knopf, ein HTML-Element, startet durch Interaktion von Nutzern der Webseite durch Anklicken den Validierungsprozess.

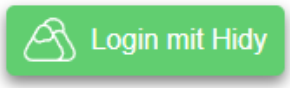


Abbildung 25: „Hidy-Button“ – ein UI-Element des Gutenberg Editor-Blocks
Quelle: WordPress-Testumgebung

Nach dem Start des Validierungsprozesses wird das zweite Element sichtbar. Ein Pop-up öffnet sich, welches in drei Bereiche unterteilt werden kann (Abbildung 26):

- Header (Kopfbereich)
- Body (Hauptbereich)
- Footer (Fußzeile)

Der **Header** ist der obere Bereich des Pop-ups. Er beinhaltet Navigationselemente, hier einen Knopf zum Schließen des Pop-ups, den Titel des Pop-ups, in diesem Fall prototypisch „Authenticator“ sowie das Logo von Hidy.

Der **Body** stellt den Hauptteil des Pop-ups dar. Er enthält den sog. „Feedback-Block“. Dieser zeigt Nutzern neben dem QR-Code auch Rückmeldungen auf ihre Handlungen oder Informationen über den Status von Prozessen an. In Abschnitt 8.4 wird mit einem Checkboxen-Formular zur Auflistung übermittelter Daten ein weiteres Element präsentiert, welches zukünftig im Body des Hidy-Pop-ups angezeigt werden könnte.

Im **Footer** werden Nutzern weitere Informationen oder Handlungsempfehlungen vermittelt. Im Beispiel des angezeigten QR-Codes wird Nutzern die Handlungsempfehlung, den QR-Code einzuscannen, gegeben. Über einen Link, der zur Webseite von Hidy führt, können Nutzer zudem mehr über Hidy erfahren.

Im **Hintergrund** verdeckt ein blaues, transparentes Element den Inhalt der Webseite.

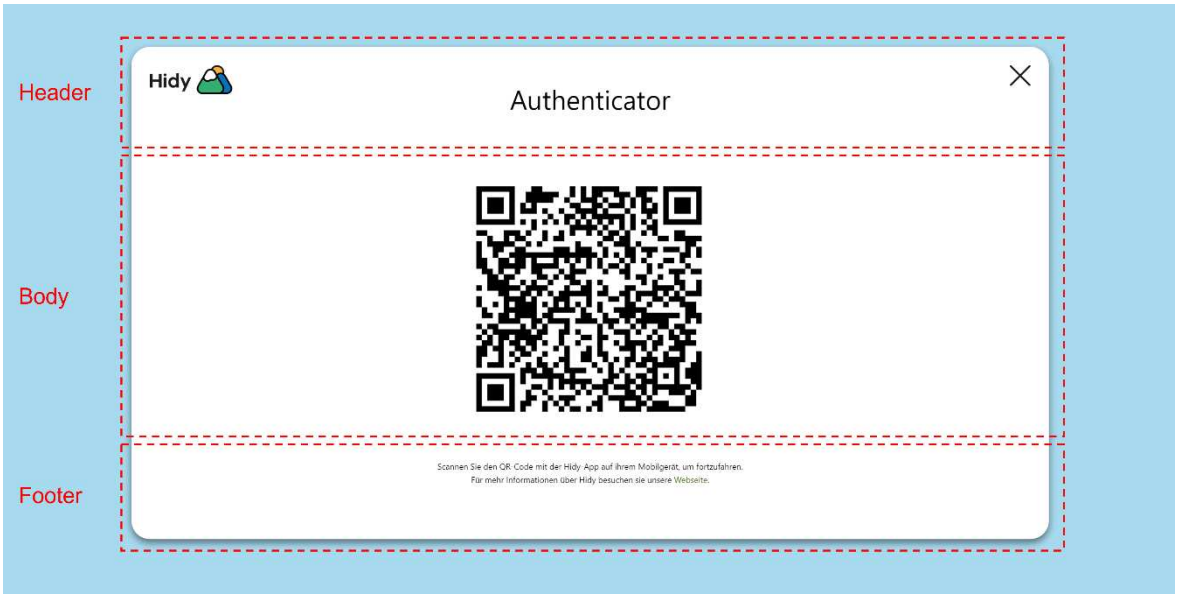


Abbildung 26: „Hidy-Pop-up" – ein UI-Element des Gutenberg Editor-Blocks

Quelle: WordPress-Testumgebung

In Anlage 2 befinden sich Screenshots aller UI-Elemente sowie die verschiedenen Zustände und Anzeigen des Hidy-Pop-up-Bodys.

5 Demonstration

Das folgende Kapitel gliedert sich in zwei Perspektiven. Zuerst wird die Installation, Einrichtung und Einbindung des Plug-ins aus Sicht eines Webseitenbetreibers demonstriert. Im darauffolgenden Abschnitt wird der typische Ablauf einer VC-Presentation aus Nutzersicht skizziert.

Es ist zu berücksichtigen, dass die Plug-in-Version derzeit nicht für eine Veröffentlichung geeignet ist und die Abläufe, vor allem aus der Perspektive des Webseitenbetreibers, sich möglicherweise noch ändern können. Abläufe, bei denen eine Änderung bei Fertigstellung der Software absehbar ist, sind mit entsprechenden Verweisen auf Abschnitte in Kapitel 8 gekennzeichnet.

5.1 Einrichtung und Integration des Plugins auf der Webseite

Installation und Einrichtung

Die Installation und Einrichtung werden sich im weiteren Entwicklungsverlauf vermutlich stark verändern. WordPress stellt Webseitenbetreibern ein öffentliches Plug-in-Verzeichnis zur Verfügung, welches im Administrations-Dashboard einer WordPress-Installation integriert ist (siehe Abschnitt 8.1.4). Die prototypische Umsetzung kann derzeit nicht über diesen üblichen Weg installiert werden. Es muss manuell als ZIP-Datei hochgeladen und kann dann installiert werden (Abbildung 27).

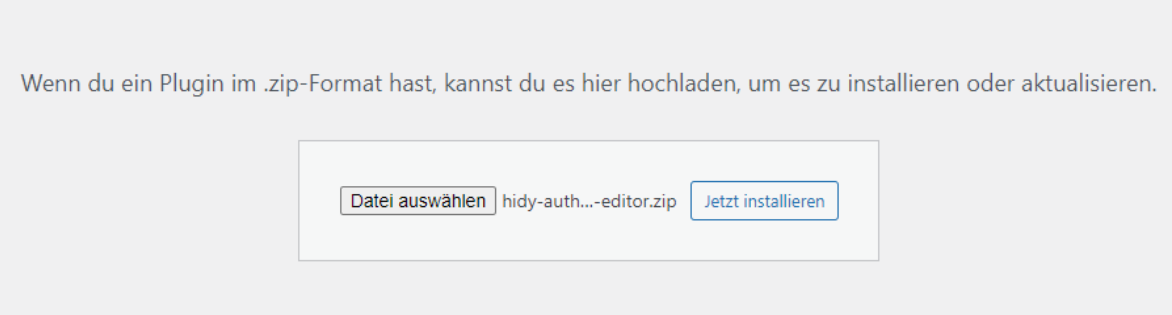


Abbildung 27: Installation des Hidy-Validierungs-Plug-ins in ZIP-Dateiformat

Quelle: WordPress-Testumgebung

Anschließend wird das Plug-in in der Übersicht von installierten Plug-ins im Administrator-Dashboard der Webseite aufgelistet und muss aktiviert werden. Über den Link „Einstellungen“ (Abbildung 28), neben der Option von Aktivieren und Deaktivieren des Plug-ins, oder den Menüpunkt im Seitenmenü des Dashboards (Abbildung 29) gelangt der Webseitenbetreibet auf die Einstellungsseite.

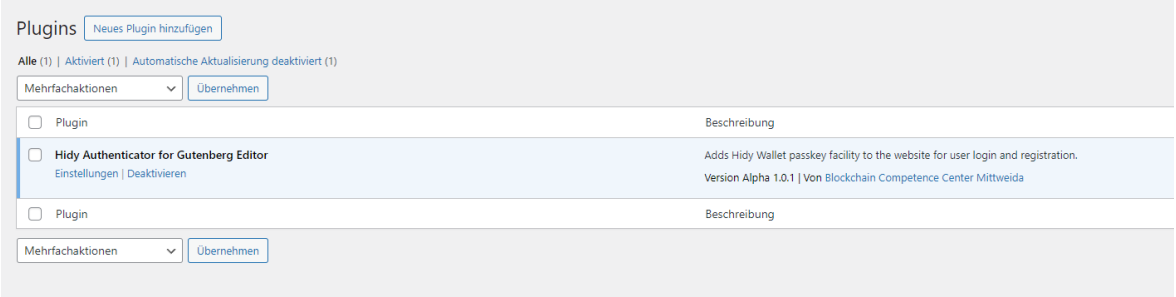


Abbildung 28: Hidy-Validierungs-Plug-in in der Plug-in-Übersicht von WordPress

Quelle: WordPress-Testumgebung

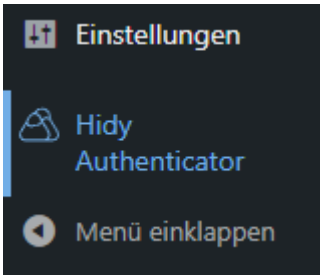


Abbildung 29: Link zur Einstellungsseite des Plug-ins im Administrationsmenü

Quelle: WordPress-Testumgebung

Die Einstellungsseite bietet Webseitenbetreibern, in bisher einem Formular (siehe Anlage 2, Abbildung 8), die Möglichkeit, aus einem Pool an digitalen Nachweisen einen auszuwählen, der für die Presentation von Nutzern gefordert wird. Es ist zu erwarten, dass die Einstellungsseite zukünftig um weitere Formulare und Einstellungen zur individuellen Anpassung bestimmter Aspekte erweitert wird. Möglicherweise könnten Formulare dynamisch erzeugt werden, Optionen, Gutenberg Editor-Blöcke dynamisch zu generieren, und die Auswahl mehrerer verschiedener digitaler Nachweise hinzugefügt werden (siehe Abschnitte 8.1.2, 8.2, 8.3 und 8.4). Entsprechend der möglicherweise ergänzten Optionen können Seiteninhaber weitere Anpassungen in Formularen und Menüs vornehmen.

Einbindung auf Seiten

Das Plug-in definiert eine eigene Kategorie namens „Hidy Authenticator“ im Seitenmenü des Editors (Abbildung 30). Darin befindet sich der zurzeit statisch generierte GEB namens „Hidy Auth Button“. Sollten zukünftig dynamisch mehr GEBs erzeugt werden können, würden diese ebenfalls mit entsprechend angepasster Bezeichnung in dieser Kategorie aufgelistet werden. Ebenfalls kann der Hidy Auth Button über das Schnellmenü (Abbildung 31) gesucht und ausgewählt werden. Aus diesen beiden Menüs kann der Webseitenbesitzer per Drag-and-Drop-Prinzip (siehe Abschnitt 2.3.2) auf die Seite ziehen und anschließend weiter verschieben (siehe Anlage 2, Abbildungen 1 bis 7). Im Einstellungsmenü des Blocks (Abbildung 32) können derzeit noch keine Anpassungen vorgenommen werden. Dass eine Anpassbarkeit zu einem späteren Zeitpunkt hinzugefügt wird, ist jedoch nicht auszuschließen.

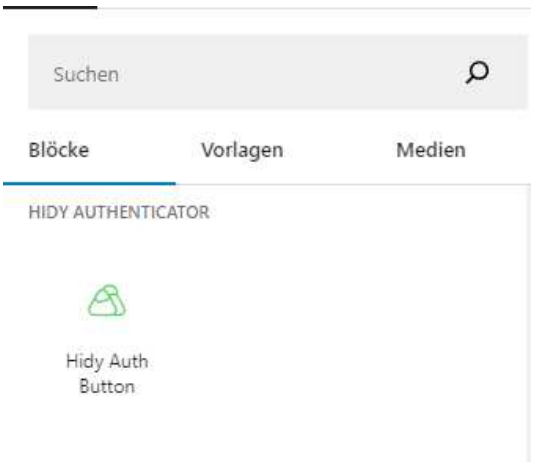


Abbildung 30: Hidy Authenticator-Kategorie und Hidy Auth Button im Seitenmenü des Gutenberg Editors

Quelle: WordPress-Testumgebung

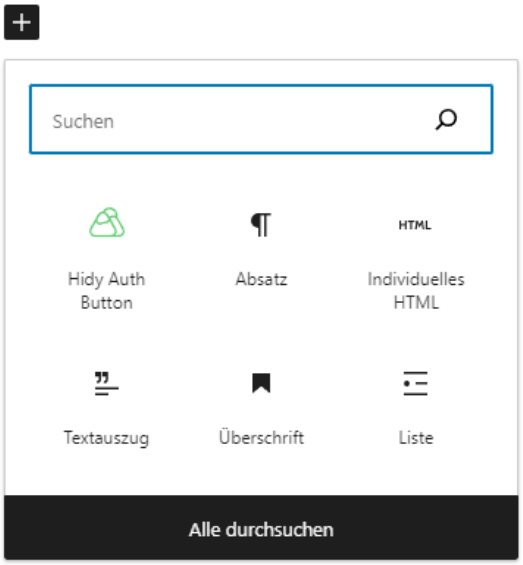


Abbildung 31: Hidy Auth Button im Schnellmenü des Gutenberg Editors

Quelle: WordPress-Testumgebung

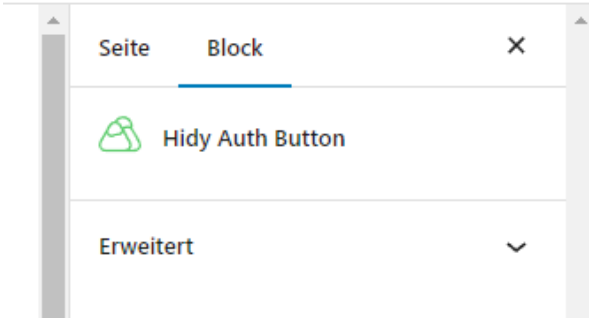


Abbildung 32: Einstellungsmenü des Gutenberg Blocks im Gutenberg Editor

Quelle: WordPress-Testumgebung

5.2 Ablauf einer VC-Presentation aus Nutzersicht

Im Ablauf einer VCP muss ein Nutzer zwei Interaktionen durchführen. Der Nutzer muss beim Besuch der Webseite den Hidy Auth Button anklicken. Die Validierungsanfrage wird automatisch an den Dargent gesendet. Aus der Antwort wird ein QR-Code generiert und ausgegeben. Nun muss der Nutzer den QR-Code mit einem Endgerät einscannen, auf dem die Hidy Wallet installiert ist, und anschließend die Presentation bestätigen, falls das geforderte VC in der Wallet gespeichert ist. Beim Webseiten-Aufruf von einem Endgerät, auf dem die Wallet installiert ist, könnte zukünftig auch eine VC-Presentation ohne das Einscannen eines QR-Codes umgesetzt werden, indem die Wallet auf dem Endgerät geöffnet wird. Dann müsste nur noch die Presentation bestätigt werden (siehe Abschnitt 8.1.3). Die Validierung des VCs erfolgt anschließend wieder automatisch. Abhängig vom Ausgang der Presentation wird visuelles Feedback gegeben und bei einer erfolgreichen Presentation sollte ein Login-Mechanismus, welcher noch entwickelt werden muss, das Einloggen auf der Webseite übernehmen (Abbildung 33).

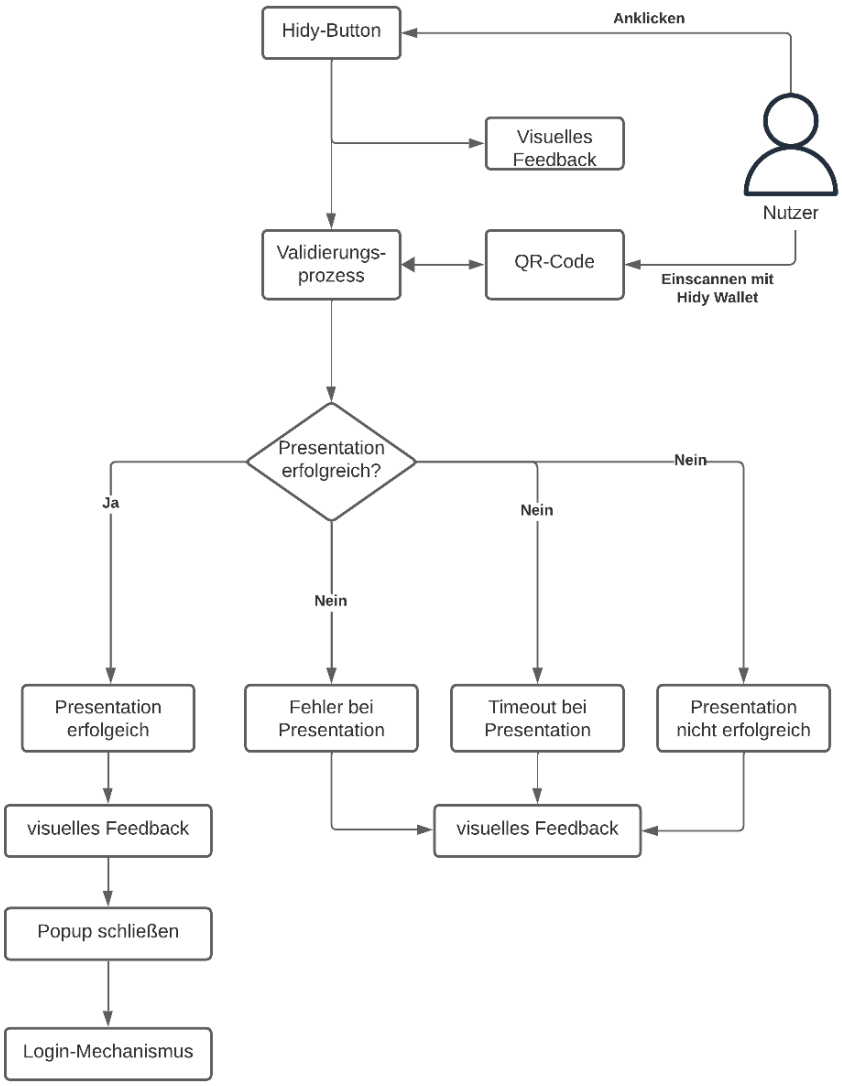


Abbildung 33: Typischer Ablauf einer Verifiable Credential-Presentation aus Nutzersicht

Quelle: Eigenkreation mit LucidChart [30]

6 Anwendungsmöglichkeiten

Die folgenden Anwendungsmöglichkeiten sind Gedankenspiele des Autors und unabhängig von Plänen und Vorstellung des Forschungsprojektes ID-Ideal zu betrachten. Sie stellen theoretische Überlegungen dar, wofür SSI-Technologie und die entwickelte, prototypische Schnittstelle zwischen Besitzern und Verifizieren von digitalen Identitäten und Nachweisen genutzt werden könnten. Im Fokus stehen dabei die digitale Verifikation der ausstellbaren, verifizierbaren digitalen Nachweise, wie in Abschnitt 2.1.3 erwähnt, und die Schaffung einer Alternative zu Passkey-Technologien von IdPs. Wichtig ist ebenfalls zu erwähnen, dass die entwickelte Schnittstelle bisher nur prototypisch umgesetzt ist. Für eine freie Einbindung und Nutzung durch Dritte auf ihren Webseiten sind noch einige Aspekte auszubauen. In Kapitel 8 werden die Aspekte, die zu einer Fertigstellung der Anwendung erforderlich sind, sowie mögliche Lösungsansätze behandelt.

6.1 Digitale Identitätsverifikation

In erster Linie könnten SSI-Wallets selbst die physische Brieftasche ersetzen. Digitale Bezahlmethoden, basierend auf NFC-Technologie, sind auf Smartphones, Tablets und Smartwatches bereits weit verbreitet. Von Kunden- und Treuepunktkarten, die auf einem Barcode basieren, können ebenfalls mit Apps, wie bspw. Stocard oder Catima, digitale Replikate erstellt werden, sodass die physischen Exemplare nicht mehr mitgeführt werden müssen. Für das Abspeichern und Verwalten amtlicher Ausweisdokumente, wie bspw. Personalausweis, Reisepass oder Führerschein, und weitere Identifikationsdokumente, wie z. B. Krankenkassenkarte, Studenten- oder Mitgliederausweise, gibt es bisher wenig unabhängige Anwendungen. An dieser Stelle setzt die Hidy Wallet an und könnte letztendlich die physische Brieftasche vollständig ersetzen. [20]-[22]

Das entwickelte Plug-in könnte zukünftig als API-Schnittstelle zwischen einer SSI-Wallet und damit dem *Besitzer* der digitalen Identitäten und Nachweise, wie in Abschnitt 2.1.3 bereits erklärt, und den *Verifizierern* in Form von amtlichen Behörden und sonstigen offiziellen Stellen zur Verifikation der realen Identität oder bspw. der aktiven Mitgliedschaft in einem Verein oder einer Institution bilden.

Auf diese Weise können zahlreiche Amtsbesuche, die eine persönliche Anwesenheit zur Identitätsbestätigung oder aus Datenschutz-Gründen erfordern, digitalisiert werden. Dies könnten u. a. das Ummelden des Wohnortes beim Einwohnermeldeamt, das Zulassen eines Fahrzeugs bei der Kfz-Zulassungsbehörde oder die Beantragung und Ausstellung bestimmter Ausweise, wie z. B. dem Reisepass oder dem Führerschein, sein. Ebenso sind weitere Anwendungsfelder denkbar, die die Digitalisierung weiter vorantreiben wie

das Gewähren von Studierendenrabatt in Onlineshops, die Ermöglichung von Online-Sprechstunden oder die vereinfachte Rezeptabwicklung für verschriebene Medikamente, die teilweise von der Krankenkasse gedeckt sind.

Zusammenfassend könnte das Authentifikations-Plug-in dazu beitragen, mit SSI-Lösungen die Digitalisierung zahlreicher, teilweise komplexer analoger Prozesse und in einigen Bereichen die Automatisierung manueller Abläufe, welche die rechtssichere Presentation eines der in Abschnitt 2.1.3 vorgestellten Nachweise erfordern, zu fördern.

6.2 Alternative zu Passkey-Technologien

Moderne Passkey-Technologien von IdPs und SSI besitzen Parallelen. Prinzipiell funktionieren sie ähnlich. Ein Endgerät speichert eine Information, welche den Besitzer des Endgerätes als den Inhaber eines bestimmten Kontos oder einer bestimmten digitalen Identität bzw. digitaler Nachweise verifiziert. Die beiden Konzepte unterscheiden sich jedoch hinsichtlich der Umsetzung dieser Verifizierung sowie in Datenschutz und Privatsphäre der Nutzer. Im Folgenden werden die beiden Konzepte gegenübergestellt und Potenziale von SSI mit dem WordPress-Plugin zur Validierung von VCs skizziert.

6.2.1 Vergleich von Passkey-Technologien und SSI

Passkey-Technologien, wie sie Google und Co. zurzeit in ihre Systeme implementieren, benötigen einen sicheren Nachweis davon, dass das zur Passkey-Verifizierung verwendete Gerät dem Inhaber des anzumeldenden Kontos gehört. Dies wird durch eine Registrierung des Gerätes in entsprechendem IdP-Konto oder durch die Anmeldung dieses Kontos auf dem Endgerät erreicht. Die Authentifizierung des Nutzers erfolgt innerhalb des Ökosystems des ID-Providers. Daher können potenziell alle Nutzerdaten, Logins und das allgemeine Nutzerverhalten von diesem gespeichert und weiterverarbeitet werden.

Die Sicherstellung der Nutzeridentität bei SSI-Lösungen erfolgt auf eine andere Weise. Die Verifikation des Nutzers geschieht durch kryptografische Signaturen und dezentrale Identitätsnachweise, die auf einem Endgerät in einer SSI-fähigen Software-Anwendung gespeichert werden. Anstelle einer Geräteverbindung zu einem zentralen Konto, wie es bei Passkey-Technologien üblich ist, nutzt SSI eine verteilte Verifikation der Identität. „Verteilt“ steht in diesem Kontext für die Nutzung von verteilten Systemen als Datenverarbeitungsumgebung. Dies wird durch die digitalen Signaturen und Zertifikate, die von verschiedenen unabhängigen Instanzen, den Ausstellern, ausgestellt werden und dezentral von Nutzern bzw. Besitzern selbst gespeichert werden, realisiert. Diese dezentrale Art der Identitätsverifikation bei SSI-Lösungen schützt die Privatsphäre der Nutzer besser, da keine zentrale Datenbank mit Nutzerinformationen existiert, die von Dritten angegriffen und „ausgeraubt“ werden kann. Durch die Nutzung einer VDR statt Firmen-Ökosystemen können zudem von keiner Instanz personenbeziehbare Daten erhoben und verarbeitet werden. Selbst die Anwendungen oder auch Verifizierer, bei denen sich Nutzer verifizie-

ren, können keine personenbeziehbaren Daten erheben, da sie lediglich eine Bestätigung der Übereinstimmung der vorgezeigten mit der angeforderten Identität erhalten, nicht jedoch tiefergreifende Informationen aus den vorgezeigten Nachweisen. Tabelle 3 fasst alle wichtigen Merkmale der beiden Konzepte zusammen und stellt sie einander gegenüber.

Grundsätzlich sind beide Verfahren per se nicht sehr verschieden. Sie sind beide Besitzbasierte Authentifikationsmethoden und verwenden asymmetrische Verschlüsselungsverfahren zur Sicherung des zur Authentifizierung benötigten Besitzes. Der wesentliche Unterschied besteht im Ökosystem, in dem die Technologie verwendet wird. Passkey-Technologien von ID-Providern sind in bestehende zentrale Systeme eingebunden, während SSI weitestgehend unabhängig und dezentralisiert ist.

Merkmal	**Passkey-Technologie**	**Self-Sovereign Identity (SSI)**
Authentifizierungsmethode	Geräteverbindung zu einem zentralen Konto	Kryptografische Signaturen und dezentrale Identitätsnachweise
Sicherung der Nutzeridentität	Registrierung des Gerätes in einem IdP-Konto oder Anmeldung des Kontos auf dem Endgerät	Kryptografische Signaturen und Zertifikate, die dezentral von Nutzern gespeichert werden
Datenverarbeitung und Speicherung	Potenzielle Speicherung und Verarbeitung von Nutzerdaten, Logins und Nutzerverhalten durch den ID-Provider	Dezentralisierte Datenverarbeitung, keine zentrale Datenbank mit Nutzerinformationen
Datenschutz	Potenzielles Risiko für die Privatsphäre, da alle Daten im ID-Provider-Ökosystem gespeichert sind	Bessere Privatsphäre, keine zentrale Datenbank, die von Dritten angegriffen werden kann
Datenzugriff durch Anwendungen	Zugriff auf Nutzerdaten und allgemeines Nutzerverhalten möglich	Verifizierung der Übereinstimmung der vorgezeigten Identität, ohne Zugriff auf tiefergreifende Informationen
Infrastruktur	Nutzung von Firmen-Ökosystemen	Nutzung von Blockchain-Infrastruktur

Tabelle 3: Zusammenfassung und Gegenüberstellung der wichtigsten Merkmale der beiden Identitätsbestätigungsmethoden Passkey und Self-Sovereign Identity

6.2.2 Potential von SSI-Lösungen

SSI besitzt ein riesiges Potenzial, als unabhängige Softwarelösung für das Management digitaler Identitäten die physische Brieftasche zu ersetzen und sie zu digitalisieren. Nicht nur können amtliche und offizielle Nachweise und Dokumente rechtssicher gespeichert und an entsprechenden Akzeptanzstellen vorgezeigt werden, was für sich bereits eine Innovation darstellt. Auch nicht amtliche Dokumente können dadurch digitalisiert werden. Zudem könnten SSI-Lösungen sich zu einer Alternative zu modernen Passkey-Technologien entwickeln.

Digitale Identitäten und Nachweise wurden in dieser Arbeit bisher und werden auch außerhalb derzeit vor allem als digitale Exemplare realer Dokumente angesehen (siehe Abschnitt 2.1.3). Künftig könnten ebenso Nutzerkonten von inoffiziellen Stellen wie E-Commerce-Seiten, sozialen Netzwerken, Bank- und Finanzseiten und sonstigen Webdiensten in Form von digitalen Nachweisen, basierend auf SSI-Technologie, ausgestellt werden. Auf diese Art und Weise würden Nutzer keine Benutzerkonten mit bspw. E-Mail-Adresse, Passwort oder einer anderen Sicherheitsmaßnahme und sonstigen persönlichen Daten eröffnen, sondern vom entsprechenden Webseiten-Betreiber ein VC ausgestellt bekommen, welches in einer SSI-Wallet abgespeichert wird. Diese VCs könnten das Login-Verfahren zu einem möglicherweise weiterhin bestehenbleibenden Konto, statt Passwort und Passkey, darstellen. Der einzelne Webseiten-Betreiber würde so zum *Aussteller* von VCs und somit ein weiteres Mitglied des „verteilten Systeme“-Komplexes werden. Anwendungs- und dienstabhängig könnte ebenfalls das komplette Entfallen von Nutzerkonten und lediglich die Nutzung bestimmter amtlicher oder offizieller VCs, wie bspw. dem Personal- oder Studentenausweis, für eine Anmeldung als sog. „Verifizierter Nutzer“, vorstellbar sein. Webseitenbetreibern könnte eine Liste von amtlichen und offiziellen Nachweisen zur Verfügung gestellt werden, aus welcher sie auswählen können, welche sie akzeptieren. Bei mehreren akzeptierten Nachweisen könnte dem Nutzer ebenfalls die Wahl gegeben werden, welcher dieser Nachweise vorgezeigt werden soll, sofern er mehrere dieser geforderten Nachweise besitzt.

Ein Ansatz, um dieses Verfahren im Verifiable Credential-Validierungs-Plug-in einzubinden, sowie weitere Möglichkeiten, die Software-Lösung mit Hilfe der geschaffenen Schnittstelle um innovative und nutzerorientierte Funktionen zu erweitern, werden in Kapitel 8 vorgestellt.

7 Fazit

Der im Rahmen dieser Arbeit entwickelte Prototyp demonstriert, wie in der möglicherweise passwortlosen Zukunft Online-Logins und -Verifikationen verschiedener digitaler Nachweise aussehen könnten. Dabei trägt dieser Prototyp als Teil eines SSI-Ökosystems zur Entwicklung einer Alternative zu Passkey-Technologien bei.

Durch die Integration in WordPress und den Gutenberg Editor bietet die Softwarelösung eine schnelle und unkomplizierte Einrichtung für Webseitenbetreiber sowie eine komfortable Bedienung für Nutzer. Sie können mit zwei Interaktionen ihre Verifiable Credentials aus der Hidy Wallet auf der entsprechenden Webseite validieren lassen. Durch einen modularen Aufbau ist das Plug-in erweiterbar und kann zu einem dynamisch anpassbaren Werkzeug weiterentwickelt werden. Zur Nutzbarmachung des Plug-ins sind Weiterentwicklungen zwingend notwendig. Derzeit gibt es keinen Login-Mechanismus, der Nutzer auf Webseiten nach erfolgreicher Presentation des geforderten Nachweises als „verifiziert“ kennzeichnet und den Zugriff auf bestimmte Inhalte gewährt. Der Validierungsprozess ist jedoch vollständig umgesetzt und kann auf andere Systeme übertragen werden. Einige Ansätze für notwendige und sonstige Erweiterungsmöglichkeiten werden in Kapitel 8 präsentiert.

Letztendlich sind die Kernfunktionen des Plug-ins, die den Validierungsprozess betreffen (siehe 3.3), jedoch nicht auf WordPress oder den Gutenberg Editor angewiesen. Mit Anpassungen an der Integration auf einer Webseite kann der Mechanismus auf andere Systeme übertragen werden. Die Integration auf WordPress und im Gutenberg Editor soll zu einer schnellen Verbreitung beitragen.

Die Softwarelösung ist Teil der Infrastruktur eines SSI-Ökosystems und sollte daher weniger als Hidy-Lösung, sondern vielmehr als ID-Ideal-Lösung betrachtet werden. Die derzeitige Umsetzung basiert auf dem Hidy-Ökosystem. Eine Umsetzung für andere SSI-Ökosysteme ist jedoch mit gewissen Anpassungen ebenfalls möglich. Notwendig sind dafür die drei Akteure des Trust Triangles: Aussteller, Besitzer und Verifizierer. Das Plug-in bzw. seine Kernfunktionen stellen eine Kommunikationsschnittstelle zwischen Besitzer und Verifizierer dar.

8 Ausblick

Das Validierungs-Plug-in wurde im Rahmen dieser Arbeit prototypisch für die Demonstration einer möglichen VC-Validierung auf WordPress-Webseiten mit der Hidy Wallet entwickelt. Damit dieser Prototyp Teil einer marktreifen SSI-Softwarelösung zum Speichern, Verwalten und Verifizieren auf einer breiten Anzahl an Webseiten werden kann, benötigt das Plug-in weitere Kernfunktionen. Insbesondere für das Verifizieren auf Webseiten muss das Plug-in anpassungsfähiger und dynamischer gestaltet sowie eine Login-Mechanik nach erfolgreicher VC-Presentation eingebunden werden, wenn dieses Konzept eine Alternative zu Passkey-Technologien darstellen soll.

Im Folgenden werden einige Möglichkeiten, den Prototypen zu erweitern, und mögliche Lösungsansätze vorgestellt. Zu beachten ist, dass lediglich Abschnitt 8.1 sich auf die unabhängige Weiterentwicklung des Validierungs-Plug-ins bezieht, sodass der Prototyp für die Öffentlichkeit nutzbar wird. Die Realisierbarkeit von Erweiterungsansätzen, die darüber hinausgehen, ist von der Umsetzung und dem Aufbau, bzw. der Anpassbarkeit und Erweiterbarkeit, des Ökosystems der jeweiligen SSI-Lösung abhängig und kann nur in enger Zusammenarbeit konzeptioniert und entwickelt werden.

8.1 Fertigstellung des Prototyps zu einer kompletten Softwarelösung

Das Validierungs-Plug-in bietet derzeit die Möglichkeit, einen digitalen Nachweis bei der Presentation anzufordern und zu überprüfen. Der Webseitenbetreiber kann den geforderten digitalen Nachweis in den Einstellungen des Plug-ins selbst aus einer vorgegebenen Liste amtlicher oder offizieller Nachweise auswählen. Daraus erschließen sich zwei Funktionen und weitere Anpassungen, die vor dem Veröffentlichen des Plug-ins noch bearbeitet werden sollten. Zum einen der Login-Vorgang bei einer erfolgreichen VC-Presentation und zusätzliche Optionen in den Plug-in-Einstellungen für Webseitenbetreiber, die die Abfrage von mehreren verschiedenen digitalen Nachweisen und an verschiedenen Stellen ermöglichen.

8.1.1 Login-Vorgang

Damit das Plug-in weiterhin an Webseitenbetreiber möglichst geringe Anforderungen stellt, empfiehlt es sich, das WordPress-eigene Nutzerverwaltungssystem für den Login-Vorgang zu verwenden. Es bietet zahlreiche Funktionen, wie Benutzerrollen, Benutzerprofile, anpassbare Benutzerberechtigungen, Benutzerregistrierung und -anmeldung sowie Benutzeraktivität und Protokollierung. Zudem ähnelt die Benutzerfreundlichkeit des Nut-

zerverwaltungssystems der von WordPress selbst und weist keine signifikante Komplexität auf. Darüber hinaus ist es durch benutzerdefinierte Entwicklung mittels Plug-ins erweiterbar und anpassbar. Für die Implementierung eines Login-Vorgangs nach erfolgreicher VC-Presentation über das WordPress-Nutzerverwaltungssystem bieten sich zwei Optionen an. [10]

Option 1: Verwendung von WordPress-Funktionen

Die WordPress-Funktionen „wp_set_current_user“ und „wp_set_auth_cookie“ ermöglichen das manuelle Initiieren eines Login-Vorgangs im Nutzerverwaltungssystem von WP. Dabei setzt die Funktion „wp_set_current_user“ für den aktuellen Benutzer den Login-Status, während die Funktion „wp_set_auth_cookie“ Authentifizierungs-Cookies verwendet. Im Sinne des Datenschutzes ist von letzterer Funktion abzuraten. Cookies selbst stellen kein Sicherheitsrisiko dar, jedoch können sie zu Sicherheitsproblemen führen, wenn die Verwaltung unsachgemäß ist oder das betroffene Endgerät durch bspw. XSS oder CSRF angegriffen wird. Eine Implementierung von beiden Möglichkeiten ist dennoch denkbar. Dem Benutzer könnte die Wahl der zu verwendenden Option inkl. sicherheitsrelevanter Informationen und Hinweise überlassen werden. [10]

Option 2: Manuelle Datenbankoperationen

Alternativ besteht die Möglichkeit, manuelle Datenbankoperationen durchzuführen, indem direkt auf die WordPress-Datenbank zugegriffen wird, um die Benutzerdaten zu aktualisieren und den Nutzer als eingeloggt zu markieren. Dafür könnten folgende WordPress-Methoden zum Einsatz:

- wpdb: WordPress-Datenbankklasse, mit der benutzerdefinierte SQL-Abfragen ausführen kannst.
- wp_insert_user(): Ermöglicht das Hinzufügen eines Benutzers zur Datenbank.
- wp_update_user(): Ermöglicht das Aktualisieren vorhandener Benutzerdaten.
- wp_set_auth_cookie(): Erlaubt das Setzen von Authentifizierungs-Cookies, um einen Benutzer einzuloggen.
- wp_signon(): Erlaubt das Anmelden eines Benutzers programmgesteuert.

Diese Vorgehensweise bietet mehr Flexibilität bei der Umsetzung, birgt jedoch das Risiko von Problemen bei Änderungen in der Datenbankstruktur oder bei unsachgemäßer Durchführung der VC-Validierungs- und des Login-Prozesses. Die Wartung dieses Systems wäre daher aufwendiger. [10]

Zu beachten ist, dass die in beiden Optionen verwendeten Funktionen serverseitig in PHP ausgeführt werden. Die VCV wird im Client in JS umgesetzt. Am Ende des VC-Validierungsprozesses müsste eine JS-Funktion aufgerufen werden, über welche eine

Methode zur Kommunikation zwischen Frontend und Backend bzw. Client und Server aufgebaut wird. Dies könnte bspw. mit Ajax umgesetzt werden.

Weiterführend könnte ein Nutzer durch die Verwendung des WordPress-Hooks „wp_login“ bestimmten, z. T. vorgegebenen Nutzerrollen zugewiesen werden, abhängig vom vorgezeigten Nachweis. So könnten mögliche Nutzerrollen bspw. „deutscher Staatsbürger“, „Studierender“ oder die Mitgliedschaft und Rang in einer offiziellen oder inoffiziellen Organisation, Verein o. ä. sein. [10]

8.1.2 dynamische Skalierbarkeit

Derzeit ist die Nutzung des Validierungs-Plug-ins auf die Validierung **eines** aus einem vorgegebenen Pool an VCs frei wählbaren, digitalen Nachweises beschränkt. Es ist jedoch denkbar, dass auf bestimmten Webseiten mehrere Nachweise für dieselbe Verifizierung nutzbar gemacht werden sollen oder, dass für verschiedene Kontexte unterschiedliche Nachweise benötigt werden. Bspw. könnte für die Verifikation als deutscher Staatsbürger neben dem Personalausweis ebenso der Reisepass oder der Führerschein verwendet werden. An anderer Stelle, unabhängig von der Verifikation als deutscher Staatsbürger, könnte die Verifikation als Student, z. B. für die Gewährung von Studierenden-Rabatt, benötigt werden. Solche Szenarien sind derzeit noch nicht umsetzbar. Daher sind weitere Optionen notwendig, die Webseitenbetreibern ermöglichen, dynamisch Gutenberg Editor-Blöcke nach ihren Anforderungen zu generieren und die Abfrage mehrerer VCs zu ermöglichen.

Dynamische Generierung von Gutenberg Editor-Blöcken

Derzeit wird ein Gutenberg Editor-Block statisch erzeugt. Mit Nutzung der WordPress-Datenbank kann diese Generierung modifiziert werden. Webseitenbetreibern könnte die Möglichkeit gegeben werden, auf der Einstellungsseite des Plug-ins im Administrations-Dashboard der WordPress-Webseite eine bestimmte Anzahl an GEBs zu erzeugen. Abhängig von dieser Zahl, welche in die WP-Datenbank geschrieben wird, würde die JS-Funktion, die den GEB erzeugt, mehrfach ausgeführt werden. Dafür bedarf es einiger Anpassungen in dieser Funktion bzgl. Vergebung von IDs, Bezeichnungen und weiterführenden Funktionsaufrufen. Alle dynamisch erzeugten GEBs könnten mit eindeutiger Bezeichnung in der, vom Plug-in registrierten, Kategorie in der Editoransicht des GEs eingegliedert werden (siehe 5.1).

Des Weiteren könnten abhängig von dieser Zahl auf der Einstellungsseite des Plug-ins Formulare für jeden einzelnen GEB erzeugt werden, welche den entsprechenden GEB an die Anforderungen des Webseitenbetreibers anpasst. Zu diesen dynamischen Anpassungen könnten Name, Beschreibung, Informationstexte für Benutzer und angeforderte VCs sowie weitere Daten gehören. Was diese „weiteren Daten“ umfassen könnte, wird in den Abschnitten 8.3 und 8.4 vorgestellt.

Verwendung mehrere Verifiable Credentials

In den Formularen auf der Einstellungsseite des Plug-ins könnten Optionen eingebaut werden, beliebig oder bestimmt viele digitale Nachweise als Alternative oder zusätzlich anzufordern. So könnten verschiedene VCs für die Verifizierung verwendet werden oder die Verifikation durch mehrere VCs gleichzeitig möglich sein, bspw. als deutscher Staatsbürger und Studierender.

Bei Verwendung eines VCs von mehreren möglichen, könnte erneut dem Benutzer die Wahl gegeben werden. Entsprechend würde vor der Presentation-Anfrage der Nutzer gefragt werden, welches der möglichen VCs er vorzeigen kann bzw. möchte. Im Anschluss erfolgt die Presentation-Anfrage.

Die Verwendung mehrerer VCs gleichzeitig könnte mit mehreren aufeinanderfolgenden Presentation-Anfragen und dem damit verbundenen mehrfachen Einscannen unterschiedlicher QR-Codes durch den Nutzer mit einer SSI-Wallet umgesetzt werden. Besser wäre es, wenn mehrere VCs in einer Presentation-Anfrage verifiziert werden könnten. Die Umsetzung dieser Variante hängt jedoch von anderen Faktoren des jeweiligen SSI-Ökosystems ab und kann im Rahmen dieser Arbeit nicht weiter beleuchtet werden.

Für beide Optionen, die Verwendung eines VCs von mehreren Möglichen und die Verwendung mehrerer VCs gleichzeitig, könnten nach erfolgreicher VC-Presentation und erfolgtem Login für die Session dynamisch WordPress-Hooks (siehe 8.1.1) für die vorgezeigten VCs gesetzt werden.

8.1.3 Anpassungsfähige UI und Integration der SSI-Wallet

In der bisherigen Entwicklungsphase wurde die Benutzeroberfläche lediglich als Prototyp für Desktopformate umgesetzt. Für eine Fertigstellung zu einer kompletten Softwarelösung erfordert es eine höhere Anpassungsfähigkeit des UIs, insbesondere auf mobilen Endgeräten, wie Smartphones und Tablets. Die aktuelle Designkonzeption repräsentiert lediglich einen Prototyp und befindet sich noch nicht in seiner endgültigen Ausführung. Ggf. sind Anpassungen erforderlich, um den Vorgaben des Hidy Style Guides, sofern vorhanden, gerecht zu werden.

Bei der Nutzung eines Endgerätes mit installierter SSI-Wallet des verwendeten SSI-Ökosystems besteht die Option, anstatt den QR-Code auf der Webseite anzeigen zu lassen, die direkte Öffnung der App und des Fensters für die Bestätigung des digitalen Nachweises. Wichtig hierbei ist, dass die App keinesfalls ohne die ausdrückliche Zustimmung des Nutzers geöffnet werden sollte. Es sollte eine Benachrichtigung angezeigt werden, die um die Erlaubnis zur Öffnung der SSI-Wallet bittet. Bei Bestätigung durch den Nutzer öffnet sich die App und zeigt die Bestätigung des erforderlichen digitalen Nachweises an. Falls die Zustimmung des Nutzers verweigert wird, wird der gesamte Verifizierungsprozess abgebrochen.

Um dies realisieren zu können, könnten spezielle APIs wie die Deeplink-Intent-API für Android und Univeral Links für iOS verwendet werden. Diese ermöglichen nicht nur das bloße Öffnen von Anwendungen, sondern auch gezielte Verweise auf spezifische Seiten oder Funktionalitäten innerhalb der Anwendung. [43], [44]

Die Verwendung von Deeplinks könnte jedoch ausreichen, um diese Funktion umzusetzen. Die URL, aus welcher der QR-Code generiert wird, könnte alternativ als Deeplink an das Endgerät des Nutzers übergeben werden. Die SSI-Wallet sollte den Deeplink erkennen und automatisch die App und die Bestätigung für die VC-Presentation anzeigen.

Zusätzlich könnten für ein verbessertes Feedback dem Nutzer Rückmeldungen gegeben werden, wenn während des Validierungsprozesses ein Fehler aufgetreten ist oder das benötigte VC nicht in der Wallet des Nutzers gespeichert ist. Dafür müsste der Dargent bei entsprechenden Ereignissen eine andere Antwort als „verifiziert“ ausgeben, die vom Websocket des Plug-ins entgegengenommen werden würde. Abhängig vom Inhalt der Antwort kann das UI anschließend Feedback ausgeben. Das visuelle Feedback ist bereits vorhanden, es fehlt jedoch die Initialisierung durch differenzierte Antworten vom Dargent.

8.1.4 Veröffentlichen auf WordPress.org

Nachdem der Prototyp vollendet und optimiert wurde, stellt die Veröffentlichung auf WordPress.org den nächsten logischen Schritt dar. Um das Validierungsplugin auf WordPress.org zu veröffentlichen, sind mehrere Schritte erforderlich. Zunächst sollte eine sorgfältige Dokumentation mit allen neuen Mechaniken und Funktionen erstellt werden, die detaillierte Anweisungen zur Installation, Konfiguration und Verwendung des Plugins bereitstellt. Die WordPress-Coding-Standards, welche bei der initialen Entwicklung des Plugins bereits beachtet wurden, sollten erneut überprüft werden. Die Lizenzierung des Plugins ist ein weiterer wichtiger Schritt, um die rechtlichen Anforderungen zu erfüllen. Nach Fertigstellung und umfassenden Tests des Plug-ins wird es über das WordPress.org-Entwicklerportal eingereicht, wo es einer gründlichen Prüfung auf Qualität, Sicherheit und Einhaltung der Richtlinien unterzogen wird. Es sollte zudem eine langfristige Wartung und Aktualisierung des Plug-ins organisiert werden, damit auch in neueren WordPress-Versionen alle Prozesse reibungslos funktionieren. Eine, von WordPress unabhängige, Veröffentlichung der Software, bspw. auf der Webseite von Hidy, könnte ebenfalls als zusätzliche Option in Betracht gezogen werden. [45]

8.2 Verifizierungsstelle in Plug-in integrieren

Im Ökosystem von Hidy fungiert der Dargent als Verifizierer (siehe Kapitel 2.1.3, Abschnitt SSI-Ökosystem). Derzeit ist dieser ein zentraler Webserver. Um VCs zu bestätigen, müssen Webseiten POST-Anfragen an diesen Server senden. Zunächst scheint das unproblematisch zu sein. Es gibt keine funktionalen Unterschiede zwischen einem SSI-Ökosystem mit einem einzelnen oder mehreren Verifizieren, sofern alle Verifizierer gleich

aufgebaut sind und dieselben Nachweise akzeptieren. Allerdings könnten logistische Probleme entstehen, wenn dieser einzige Verifizierer nicht erreichbar sein sollte.

Um diesem Risiko vorzubeugen, könnte eine Verifizierungsstelle, ähnlich dem Dargent im Hidy-Ökosystem, in das Validierungs-Plug-in integriert werden. Dadurch würde jede Webseite zu dem Verifizierer für ihre eigenen VC-Presentation-Anfragen werden. Das SSI-Ökosystem wäre dann nicht mehr von einer einzelnen Instanz abhängig. Um dies realisieren zu können, müsste sichergestellt sein, dass diese Verifizierungsstelle auf Webseiten vor Manipulation geschützt ist. Eine detaillierte Beschreibung eines Lösungsansatzes für dieses Vorhaben übersteigt jedoch den Rahmen dieser Arbeit, und ein mögliches Gelingen ist abhängig von äußeren Faktoren.

8.3 Ausstellen „privater“ Nachweise

Für die Weiterentwicklung dieses Konzeptes zu einer Alternative zu bestehenden Passkey-Technologien müssten Webseitenbetreiber befähigt werden, eigene Verifiable Credentials als Authentifizierungsmethode für die Benutzerkonten auf ihren Webseiten ausstellen zu können. Dadurch würden Webseiten, neben ihrer Rolle als Verifizierer für amtliche und offizielle VCs, zu Ausstellern und Verifizierern für ihre eigenen VCs werden (siehe Kapitel 2.1.3, Abschnitt SSI-Ökosystem).

Die genaue technische Umsetzung dieses Zukunftsmodells liegt außerhalb des Rahmens dieser Arbeit, jedoch werden im Folgenden einige wichtige Aspekte betrachtet, die bei der Entwicklung eines solchen Modells zu beachten sind.

VCs, die von privaten Websites oder Unternehmen ausgestellt werden, sollten klar als solche gekennzeichnet sein, um sie von amtlichen und offiziellen Nachweisen unterscheiden zu können. Bspw. könnten sie als „inoffizielle“ oder „private“ VCs bezeichnet werden. Sie sollten nur von Verifizierern akzeptiert werden, die mit der ausstellenden Instanz verbunden sind. Für unabhängige Verifizierer sollten diese VCs nicht erkennbar oder zugänglich sein. Insbesondere bei der Auswahl geforderter Nachweise dürften diese inoffiziellen VCs nicht sichtbar oder mindestens nicht auswählbar sein.

Dennoch müssten unbeteiligte Webseiten Informationen über die Existenz anderer inoffizieller VCs erhalten. Zur Vermeidung von Konflikten bei der Ausstellung von privaten VCs in der Hidy Wallet und zur eindeutigen Erkennung auf Webseiten könnten diese VCs mit einer eigenen ID gekennzeichnet werden. Diese ID würde bei der Erstellung eines Ausstelldienstes einmalig vergeben und anschließend für alle anderen privaten Aussteller gesperrt werden. So würden Dopplungen vermieden werden und der Nachweis bleibt eindeutig erkennbar. Auf diese Weise würden ebenfalls sonstige Informationen über das Credential nicht mit fremden Anbietern geteilt werden.

Webseiten, die eigene private Verifiable Credentials ausstellen möchten, sollten ebenfalls als Aussteller gekennzeichnet sein, um eine Rückverfolgung ausgestellter Nachweise zu ermöglichen. Da nicht alle Webseiten eigene Nutzerverwaltungssysteme besitzen, sollten Webseiten nicht automatisch mit dem Installieren des Validierungs-Plug-ins als Aussteller inoffizieller Nachweise gekennzeichnet werden. Eine entsprechende Option zur Aktivierung und Autorisierung als ein solcher Aussteller könnte auf der Einstellungsseite des Plug-ins untergebracht werden. Ebenfalls könnte ein Autorisierungsprozess in Erwägung bezogen werden, bei dem Webseitenbetreiber eine Autorisierung beantragen können und unter gewissen Voraussetzungen durch einen Mechanismus oder durch eine offizielle Stelle zum Ausstellen privater VCs autorisiert werden.

Möglichkeiten einer erstmaligen Registrierung und der damit verbundenen Eröffnung eines neuen Nutzerkontos auf einer Webseite sowie des Migrierens eines vorhandenen Kontos zu einem VC oder das Hinterlegen eines VCs als Autorisierungsmethode beim Login müssten ebenfalls mitbedacht werden. Dafür könnten ähnliche Ansätze wie beim Login-Mechanismus (siehe Abschnitt 8.1.1) gewählt und WordPress-Funktionen zum Hinzufügen und Bearbeiten von Werten in die Datenbank des Nutzerverwaltungssystems von WordPress mittels Ajax genutzt werden.

Wie bereits in Abschnitt 8.2 der Integration einer Verifizierungsstelle in das Plug-in erwähnt, müsste sichergestellt werden können, dass der Vorgang des VC-Ausstellens sicher vor Manipulation ist. Zudem müsste das Ausstellen von VCs vor der Benutzung von unbefugten Dritten bspw. für Zwecke der VC-Fälschung geschützt werden können. Dabei könnte die Kennzeichnung von zum Ausstellen privater VCs autorisierter Webseiten hilfreich sein. Allgemein ist die Realisierbarkeit eines solchen Modells im Rahmen dieser Arbeit jedoch schwer abzuschätzen.

8.4 Datenökonomie und Transparenz

Datenökonomie

SSI-Lösungen wirken konträr zu zentralisierten ID-Providern, welche durch die Erhebung und die Weiterverarbeitung von Nutzerdaten aus u. a. Marketingzwecken einen Großteil ihres Umsatzes generieren (siehe Kapitel 2.1.2, Abschnitt Datenökonomie). Durch die Nutzung von SSI-Technologie mit einem Mechanismus zur VCV auf Webseiten würde keine oder nur eine beschränkte Erhebung nutzerbeziehbarer Daten für IdPs und andere Dienstleister möglich sein. Die Hoheit der eigenen Daten bleibt beim Nutzer.

Durch diese geschaffene Eigenverantwortung und Selbstständigkeit der Nutzer könnte ihnen die Möglichkeit gegeben werden, ihre eigenen Daten gezielt an Dienstleister im Austausch für einen bestimmten Wert weiterzugeben und somit eine eigene Datenökonomie zu betreiben. Dieser Wert könnte bspw. ein Rabattcode oder Gutschein im Falle

einer E-Commerce-Seite oder ein Geldbetrag sein, der im Austausch für bestimmte Nutzerdaten auf die SSI-Wallet des Nutzers überwiesen wird.

Ein möglicher Ansatz zur Umsetzung könnte folgendermaßen aussehen. Webseitenbetreibern könnte ein Pool von Daten, die Nutzer in der App speichern können, zur Verfügung gestellt werden. Aus diesem Pool können sie bestimmte Daten festlegen, die sie von Nutzern erheben wollen, und einen entsprechenden Gegenwert im Tausch für diese Daten festlegen. Sofern eine Webseite personenbeziehbare Daten erheben möchte, würde ein Banner, ähnlich dem Cookie-Banner (siehe Kapitel 2.1.2, Abschnitt Datenerhebung und Cookies), auf der Webseite zu sehen sein und darauf hinweisen. An dieser Stelle könnte ein weiterer Informationstext den Ablauf eines solchen Daten-Werte-Austausches aus Nutzersicht erklären. Beim Anklicken des Buttons durch den Nutzer wird vor dem Senden der Presentation-Anfrage eine Einwilligung zum Daten-Werte-Austausch erfragt. Bei Einwilligung wird von der Webseite abgefragt, welche Daten der Nutzer in seiner Wallet gespeichert hat, ohne die Werte dieser Daten zu erfahren. Dies könnte über eine Presentation via QR-Code erfolgen. Anschließend könnte ein Formular mit allen Nutzerdaten, die die Webseite erheben möchte, und der angebotene Gegenwert angezeigt werden. Dieses Formular könnte mit Checkboxen umgesetzt werden (Abbildung 34). Dabei könnte der Nutzer die Daten, die getauscht werden sollen, an-, bzw. die Daten, die nicht getauscht werden sollen, abwählen. Mit der Bestätigung des Formulars wird entweder eine weitere Presentation-Anfrage gesendet, die alle ausgewählten Nutzerdaten an die Webseite, ggf. Gegenwerte zurück an die SSI-Wallet sendet sowie die Login- oder Verifizierungsdaten für den Login- oder Registrierungsvorgang enthält, oder es müssten mehrere Presentation-Anfragen für die einzelne Übertragung der Nutzerdaten, ggf. Gegenwerte und den Login- oder Registrierungsvorgang via QR-Code-Scan gestellt werden. Welche der beiden Optionen umgesetzt werden würde, ist abhängig von der Umsetzung der Skalierbarkeit hinsichtlich der Verwendung mehrerer Verifiable Credentials (siehe Abschnitt 8.1.2). Bei Ablehnen des Daten-Werte-Austausches würde dieser Vorgang entsprechend übersprungen, keine gespeicherten Nutzerdaten abgefragt und die VCV sowie der weiterführende Login- oder Registrierungsvorgang fortgesetzt werden.

Transparenz

Generell könnten über ein solches Formular alle zu übermittelnden Informationen dem Nutzer gezeigt werden. Dies würde zu mehr Transparenz und zur Erhöhung der Privatsphäre führen. Dabei könnte in vier Kategorien unterschieden werden:

- Nicht abwählbare Daten (vorausgewählt)
- Abwählbare, (stark) priorisierte Daten (vorausgewählt)
- Anwählbare, weniger stark priorisierte Daten
- Nicht anwählbare Daten

Nicht abwählbare Daten könnten in etwa das Vorhandensein und die Echtheit eines für den Login oder die Registrierung benötigten digitalen Nachweises sein. Dazu würden kei-

ne weiteren personenbeziehbaren Daten zählen. Die Checkbox im Formular wäre bereits ausgewählt und könnte vom Nutzer nicht abgewählt werden. Abwählbare, aber priorisierte Daten könnten vorausgewählt, aber für den Nutzer abwählbar sein. Dies könnte Daten umfassen, die der Webseitenbetreiber gerne erheben und verarbeiten möchte. Für diese Daten könnten zudem höhere Gegenwerte geboten werden. Anwählbare, weniger stark priorisierte Daten könnten Daten sein, die der Webseitenbetreiber ebenfalls erheben und verarbeiten kann, die jedoch nur einen untergeordneten Wert haben und deren Gegenwert für einen Datenaustausch dementsprechend geringer ausfällt. Für mehr Transparenz könnten ebenfalls Daten angezeigt werden, die im geforderten VC enthalten sind, vom Webseitenbetreiber jedoch nicht verarbeitet werden und daher auch nicht anwählbar und nicht vorausgewählt sind. Das Formular könnte im Body des Pop-ups neben dem Feedback-Block (siehe Kapitel 4.4) aufgelistet werden (Abbildung 34). Das Formular würde abhängig von den Einstellungen des Seiteninhabers dynamisch generiert werden.

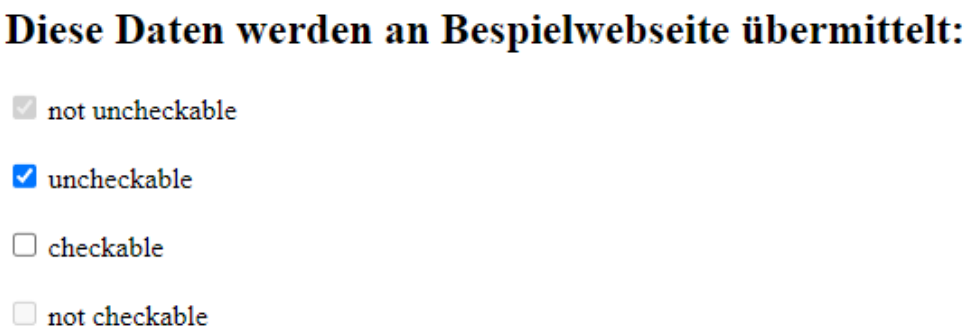


Abbildung 34: Konzept des Checkboxen-Formulars zur Auflistung übermittelter Informationen zwischen Hidy Wallet und Webseite

Quelle: WordPress-Testumgebung

8.5 Verfügbarmachung auf weiteren Systemen

Sobald das Validierungs-Plug-in durch Weiterentwicklungen den Prototyp-Status verlassen hat und veröffentlicht wird, könnte begonnen werden, die Softwarelösung auf weiteren Systemen verfügbar zu machen. Das CMS WordPress und der Pagebuilder Gutenberg Editor sind die weitest verbreiteten Systeme ihrer Art (siehe Abschnitte 2.3.1 und 2.3.2).

Der Kernprozess des Plug-ins, der Validierungsprozess (siehe Kapitel 3.3), dürfte im Kern auf jedem System gleichbleiben. Lediglich die Einbindung auf die Seite sowie der Login-Mechanismus müssten an entsprechende Systeme angepasst werden.

Ausbreitung auf weitere Content-Management-Systeme

Eine Ausbreitung auf weitere CMS, wie Shopify, Wix oder Joomla, wäre denkbar. Während die Umsetzung in Joomla als Open Source-CMS grundsätzlich einfacher und flexib-

ler sein dürfte, könnte eine Umsetzung für Shopify und Wix jedoch komplizierter sein, da dies proprietäre Plattformen und nicht Open Source sind. Shopify-Apps, wie Plug-ins für Shopify bezeichnet werden, können unter Verwendung der Shopify-API und from scratch entwickelt werden. Bei Wix ist die Entwicklung von Plug-ins nur über eine vorgegebene REST-API möglich. In beiden Fällen ist schwer abzuschätzen, ob eine Konvertierung des WordPress-Plug-ins möglich ist. Denkbar ist jedoch, eine Partnerschaft mit Shopify und Wix anzufragen. Dadurch könnte unter Umständen eine flexiblere Entwicklung möglich gemacht werden. [29], [36]-[38]

Ausbreitung auf weitere Pagebuilder

Für eine Umsetzung in anderen Pagebuildern würden sich Elementor und WPBakery anbieten. Elementor ist nicht Open Source, verfügt jedoch über ein umfangreiches Plug-in-System und ein detailliertes Entwicklerhandbuch. WPBakery bietet keine Möglichkeiten der freien Entwicklung von Plug-ins oder Add-ons an. Add-ons können ausschließlich durch Nutzung der kostenpflichtigen „Addon Creators“-Software erstellt werden. Dieses Werkzeug beherbergt zahlreiche vorgefertigte Elemente und Optionen, eigenen Quellcode einzubinden. Es ist schwierig einzuschätzen, ob genug Flexibilität in den beiden Pagebuildern für die Umsetzung des Validierungs-Plugins vorhanden ist. [17], [39], [40]

Die vorgestellten Plattformen stellen eine erste Auswahl dar. Eine tiefergreifende Analyse, welche Plattformen für eine Umsetzung des Plug-ins geeignet sind und ob eine Umsetzung möglich wäre, bzw. welche Anpassungen für eine erfolgreiche Umsetzung erforderlich wären, übersteigt den Rahmen dieser Arbeit.

Des Weiteren könnte ebenfalls das Anbieten einer **Individuallösung** in Betracht gezogen werden. Es könnte, ausgehend vom entwickelten Prototyp, ein anpassbares Grundgerüst geschaffen werden, welches auf Kunden-Anfrage, auf Webseiten ohne CMS oder Pagebuilder oder auf Webseiten mit CMS oder Pagebuilder, für die kein Plug-in oder Add-on existiert, individuell angepasst und implementiert werden würde.

Literaturverzeichnis

[1] Christiaan Brand: Google Blog: The beginning of the end oft the password
URL: https://blog.google/technology/safety-security/the-beginning-of-the-end-of-the-password/, verfügbar am 25.09.2023

[2] Norbert Pohlmann: Digitale Identitäten
URL: https://norbert-pohlmann.com/glossar-cyber-sicherheit/digitale-identitaet/, verfügbar am 29.09.2023

[3] Norbert Pohlmann: Identity Provider
URL: https://norbert-pohlmann.com/glossar-cyber-sicherheit/identity-provider/, verfügbar am 29.09.2023

[4] Norbert Pohlmann: Self-Sovereign Identity (SSI)
URL: https://norbert-pohlmann.com/glossar-cyber-sicherheit/self-sovereign-identity-ssi/, verfügbar am 30.09.2023

[5] EU-Richtlinie 2002/58/EG
URL: https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX%3A32002L0058,
verfügbar am 30.09.2023

[6] Ionos: Was ist WordPress?
URL: https://www.ionos.de/digitalguide/hosting/blogs/was-ist-wordpress/,
verfügbar am 29.09.2023

[7] ID-Ideal: Was ist ID-Ideal?
URL: https://id-ideal.de/about/, verfügbar am 29.09.2023

[8] Bundesministerium für Wirtschaft und Klimaschutz: ID-Ideal
URL: https://www.digitale-technologien.de/DT/Navigation/DE/ProgrammeProjekte/AktuelleTechnologieprogramme/Sichere_Digitale_Identitaeten/Projekte_Umsetzungsphase/IDideal/IDideal.html,
verfügbar am 30.09.2023

[9] Bundesministerium für Bildung und Forschung: TRUSTnet
URL: https://www.forschung-it-sicherheit-kommunikationssysteme.de/projekte/trustnet/,
verfügbar am 30.09.2023

[10] WordPress: Developer Resources
URL: https://developer.wordpress.org/,
verfügbar von 01.09.2023 bis 27.11.2023

[11] Docusign.com: Details zur digitalen Signatur
URL: https://www.docusign.com/de-de/wie-es-funktioniert/elektronische-signatur/digitale-signatur/digitale-signatur-faq/, verfügbar am 02.10.2023

[12] Lissi.id: Interact with ID-Wallets
URL: https://www.lissi.id/, verfügbar am 24.11.2023

[13] Trinsic.id: Build the future of identity
URL: https://trinsic.id/, verfügbar am 24.11.2023

[14] Statista: Wie lang sind Ihre am häufigsten verwendeten Passwörter?URL: https://de.statista.com/statistik/daten/studie/988439/umfrage/laenge-von-passwoertern-in-deutschland/, verfügbar am 25.09.2023

[15] Andreas Tuerk: Google Blog: Passkeys Einmaleins: Das steckt hinter der Passwort-Alternative
URL: https://blog.google/intl/de-de/unternehmen/technologie/passkeys-101/, verfügbar am 13.10.2023

[16] Christian Tietz, Chris Pelchen, Christoph Meinel, Maxim Schnjakin: Management Digitaler Identitäten: Aktueller Status und zukünftige Trends URL: https://publishup.uni-potsdam.de/opus4-ubp/frontdoor/deliver/index/docId/10316/file/tbhpi114.pdf, verfügbar am 23.11.2023

[17] Martktiefe: Marktanteile WordPress Page Builder URL: https://markentiefe.de/marktanteile-beliebteste-wordpress-page-builder/, verfügbar am 03.11.2023

[18] GitHub: Neocotic: QRious URL: https://github.com/neocotic/qrious/, verfügbar am 05.11.2023

[19] Verimi: Ihr digitaler Ausweis URL: https://verimi.de/, verfügbar am 06.11.2023

[20] Stocard: Deine Mobile Wallet URL: https://stocardapp.com/, verfügbar am 06.11.2023

[21] Catima: A Loyalty Card & Ticket Manager for Android URL: https://catima.app/, verfügbar am 06.11.2023

[22] Test.de: Kontaktlos mit Karte oder Handy zahlen – so funktionierts URL: https://www.test.de/Kontaktlos-bezahlen-per-Funk-mit-Karte-zahlen-so-funktionierts-5082480-0/, verfügbar am 06.11.2023

[23] MySpartester.de: Plugin, Add-on und Add-in was ist das? URL: https://www.myspartester.de/tutorial/webhosting/plugins/, verfügbar am 14.11.2023

[24] PlantUML: Softwarepaket zur codebasierten Erstellung von UML-Diagrammen URL: https://plantuml.com/, verfügbar am 16.11.2023

[25] Statista: Nutzen Sie zur Anmeldung bei unterschiedlichen Online-Diensten häufig das gleiche Passwort oder variieren Sie Ihre Passwortauswahl?
URL: https://de.statista.com/statistik/daten/studie/818713/umfrage/nutzung-von-unterschiedlichen-passwoertern-fuer-unterschiedliche-dienste-in-deutschland/, verfügbar am 25.09.2023

[26] Statista: Was ist Ihre bevorzugte Methode, die notwendige Menge an Passwörtern zu verwalten?
URL: https://de.statista.com/statistik/daten/studie/818850/umfrage/ablage-von-passwoertern-in-deutschland/, verfügbar am 25.09.2023

[27] Statista: Cyberkriminalität nimmt weiter zu
URL: https://de.statista.com/infografik/23077/anzahl-der-straftaten-im-bereich-cybercrime/, verfügbar am 30.09.2023

[28] Statista: Anteil der Befragten, die folgenden Aussagen zu Cookies bzw. Cookie-Bannern zustimmen, in Deutschland im Jahr 2020
URL: https://de.statista.com/statistik/daten/studie/884689/umfrage/meinung-zu-cookies-und-cookie-bannern-auf-webseiten-in-deutschland/, verfügbar am 30.09.2023

[29] Statista: Top 10 Content-Management-Systeme (CMS) weltweit nach Nutzung für Webseiten im Oktober 2023
URL: https://de.statista.com/statistik/daten/studie/320685/umfrage/nutzungsantei
l-der-content-management-systeme-cms-weltweit/,
verfügbar am 02.11.2023

[30] Lucidchart: Where seeing becomes doing.
URL: https://www.lucidchart.com/pages/landing/, verfügbar am 19.11.2023

[31] Bundesnetzagentur: Datenökonomie
URL: https://www.bundesnetzagentur.de/DE/Fachthemen/Digitalisierung/Daten/Datenoekonomie/start.html, verfügbar am 18.11.2023

[32] Statista: Umsatz von Meta weltweit vom 1. Quartal 2010 bis zum 3. Quartal 2023
URL: https://de.statista.com/statistik/daten/studie/237434/umfrage/umsatz-von-facebook-weltweit-quartalszahlen/, verfügbar am 18.11.2023

[33] Statista: Werbeumsätze von Meta weltweit in den Jahren 2010 bis 2022
URL: https://de.statista.com/statistik/daten/studie/458825/umfrage/werbeeinnah men-von-facebook/, verfügbar am 18.11.2023

[34] Statista: Umsatz von Google weltweit in den Jahren 2013 bis 2022
URL: https://de.statista.com/statistik/daten/studie/541785/umfrage/umsatz-von-google-weltweit/, verfügbar am 18.11.2023

[35] Statista: Werbeumsätze von Google in den Jahren 2001 bis 2022
URL: https://de.statista.com/statistik/daten/studie/75188/umfrage/werbeumsatz-von-google-seit-2001/, verfügbar am 18.11.2023

[36] Shopify: Erstellung von Shopify-Apps
URL: https://help.shopify.com/de/partners/making-apps/, verfügbar am 18.11.2023

[37] Wix: Eine Drittanbieter-App für den App-Markt von Wix erstellen
URL: https://support.wix.com/de/article/eine-drittanbieter-app-f%C3%BCr-den-app-markt-von-wix-erstellen/, verfügbar am 18.11.2023

[38] Joomla: Erste Schritte in der Plugin-Entwicklung
URL: https://docs.joomla.org/J3.x:Creating_a_Plugin_for_Joomla/de,
verfügbar am 18.11.2023

[39] Elementor: Creating Your First Addon
URL: https://developers.elementor.com/docs/getting-started/first-addon/,
verfügbar am 18.11.2023

[40] WPBakery: Addon Creator
URL: https://wpbakery.com/addons/addon-creator/,
verfügbar am 18.11.2023

[41] Matthew Martin: Guru99: MVC vc MVVM – Difference Between Them
URL: https://www.guru99.com/mvc-vs-mvvm.html,
verfügbar am 19.11.2023

[42] Chrissikraus: Dev-Insider: Was bedeutet MVVM?
URL: https://www.dev-insider.de/was-bedeutet-mvvm-a-51b659a606adfa077ed2e637bc189dee/, verfügbar am 19.11.2023

[43] Android Developers: Create Deep Links to App Content
URL: https://developer.android.com/training/app-links/deep-linking/,
verfügbar am 19.11.2023

[44] Apple Developer: Universal Links for Developers
URL: https://developer.apple.com/ios/universal-links/,
verfügbar am 19.11.2023

[45] Bernhard Kau: Krautpress: Ein Plugin im WordPress.org-Plugin-Verzeichnis veröffentlichen
URL: https://krautpress.de/2017/plugins-veroeffentlichen/,
verfügbar am 19.11.2023

[46] Statista: Report über Cybersecurity 2018
URL: https://de.statista.com/statistik/studie/id/58204/dokument/cybersecurity-und-cloud/, verfügbar am 21.11.2023

[47] Box.com: Was ist ein Datenleck oder eine Datenschutzverletzung?URL: https://www.box.com/de-de/resources/was-ist-ein-datenleck-oder-eine-datenschutzverletzung/, verfügbar am 21.11.2023

[48] Verbraucherzentrale: Datenlecks bei Facebook: So prüfen Sie, ob Sie betroffen sind
URL: https://www.verbraucherzentrale.de/wissen/digitale-welt/datenschutz/datenlecks-bei-facebook-so-pruefen-sie-ob-sie-betroffen-sind-25013/, verfügbar am 21.11.2023

[49] Statista: Anzahl Datenlecks und geklauter Datensätze in den USA in den Jahren 2005 bis 2019*
URL: https://de.statista.com/statistik/daten/studie/865084/umfrage/anzahl-datenlecks-und-geklauter-datensaetze-in-den-usa/,
verfügbar am 21.11.2023

[50] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)
URL: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=celex%3A32016R0679, verfügbar am 21.11.2023

[51] Etracker.com: Personenbezogene, personenbeziehbare und persönliche Daten
URL: https://www.etracker.com/personenbezogene-personenbeziehbare-und-persoenliche-daten/, verfügbar am 21.11.2023

[52] Dr. Hansjörg Leichsenring: Der Bank Blog: Digitales Identitätsmanagement gewinnt an Bedeutung
URL: https://www.der-bank-blog.de/digitales-identitaetsmanagement-bedeutung/digital-banking/37676992/, verfügbar am 23.11.2023

[53] Google: Google optimal nutzen
URL: https://www.google.com/intl/de/account/about/,
verfügbar am 23.11.2023

[54] Google Support: Google-Konto anlegen
URL: https://support.google.com/accounts/answer/27441/,
verfügbar am 23.11.2023

[55] Jürgen Anke, Daniel Richter: Springer Link: Digitale Identitäten: Status Quo und Perspektiven
URL: https://link.springer.com/article/10.1365/s40702-023-00965-1/,
verfügbar am 23.11.2023

[56] TYPO3 – the Professional, Flexible Content Management System
URL: https://typo3.org/, verfügbar am 23.11.2023

[57] Onelogin.com: Wie funktionieren Single Sign-on?
URL: https://www.onelogin.com/de-de/learn/how-single-sign-on-works/,
verfügbar am 23.11.2023

[58] Onelogin.com: Biometrische Authentifizierung: Vorteile, Nachteile und Probleme
URL: https://www.onelogin.com/de-de/learn/how-single-sign-on-works/,
verfügbar am 23.11.2023

[59] Annasleben.de: Tracking und Targeting im Dienste der Werbung
URL: https://www.annasleben.de/snippet/tracking-und-targeting-im-dienste-der-werbung/, verfügbar am 23.11.2023

[60] Daniel Wolter: HubSpot: Die wichtigsten Targeting-Techniken im Überblick
URL: https://blog.hubspot.de/marketing/targeting/, verfügbar am 30.09.2023

[61] Esatus.com: Identitfikationsprozess effizient digitalisieren mit SOWL
URL: https://esatus.com/digitale-identitaet/, verfügbar am 24.11.2023

[62] Hidy: Say goodbye to plastic cards and endless passwords. Say Hi, ID Security.
URL: https://hidy.eu/, verfügbar am 24.11.2023

[63] Tobias Ehrlich, Daniel Richter, Michael Meisel, Jürgen Anke: Springer Link: Self-Sovereign Identity als Grundlage für universell einsetzbare digitale Identitäten
URL: https://link.springer.com/article/10.1365/s40702-021-00711-5/, verfügbar am 24.11.2023

[64] Xovi.de: Was bedeutet Peer-to-Peer?
URL: https://www.xovi.de/was-bedeutet-peer-to-peer/, verfügbar am 24.11.2023

[65] Schellinger, B., Sedlmeir, J., Willburger, L., Strüker, J. und Urbach, N.: Mythbusting Self-Sovereign Identity (SSI). Diskussionspapier zu selbstbestimmten digitalen Identitäten.
URL: https://www.fit.fraunhofer.de/content/dam/fit/de/documents/Whitepaper_Mythbusting_Self-Sovereign_Identity.pdf, verfügbar am 24.11.2023

[66] Bundesamt für Sicherheit in der Informationstechnik: Public Key Infrastrukturen (PKIen)
URL: https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Elektronische-Identitaeten/Public-Key-Infrastrukturen/public-key-infrastrukturen.html, verfügbar am 24.11.2023

[67] Bundesamt für Sicherheit in der Informationstechnik: Eckpunktepapier für Self-Sovereign-Identities (SSI)
URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Krypto/Eckpunkte_SSI_DLT.pdf, verfügbar am 24.11.2023

[68] Chepd.io: What is a Verifiable Data Registry
URL: https://learn.cheqd.io/overview/introduction-to-decentralised-identity/what-is-a-decentralised-identifier-did/what-is-a-verifiable-data-registry/, verfügbar am 24.11.2023

[69] Keri.one: Welcome to KERI
URL: https://keri.one/, verfügbar am 24.11.2023

Anlagenverzeichnis

Anlage 1: Verzeichnisstruktur des Hidy-Validierungs-Plug-ins ..... A-I

Anlage 2: Screenshots der Benutzeroberfläche des Hidy-Validierungs-Plug-ins

…….. A-II

Anlage 1: Verzeichnisstruktur des Hidy-Validierungs-Plug-ins

```
hidy-auth-plugin-for-gutenberg-editor
│
├── config.json
├── hidy-auth-plugin.php
├── licence.txt
├── readme.txt
├── vcs.json
│
├── admin
│     └── admin-page.php
│
├── assets
│     ├── Hidy_close_icon.svg
│     ├── Hidy_Logo_menuIcon.svg
│     ├── Hidy_Logo_schwarzeKontur_15.svg
│     ├── Hidy_Logo_schwarzeKontur.svg
│     ├── Hidy_Logo_weißeKontur.svg
│     ├── Hidy_Logo_farbig.svg
│     ├── Hidy_qr_deny.png
│     ├── Hidy_qr_error.png
│     ├── Hidy_qr_loading.gif
│     ├── Hidy_qr_login.png
│     └── Hidy_qr_timeout.png
│
├── css
│     └── hidy-block-style.css
│
├── js
│     ├── hidy-block-functions.js
│     ├── hidy-block-register.js
│     └── qrious.js
│
└── proxy
      └── hidy-proxy.php
```

Anlage 2: Screenshots der Benutzeroberfläche des Hidy-Validierungs-Plug-ins

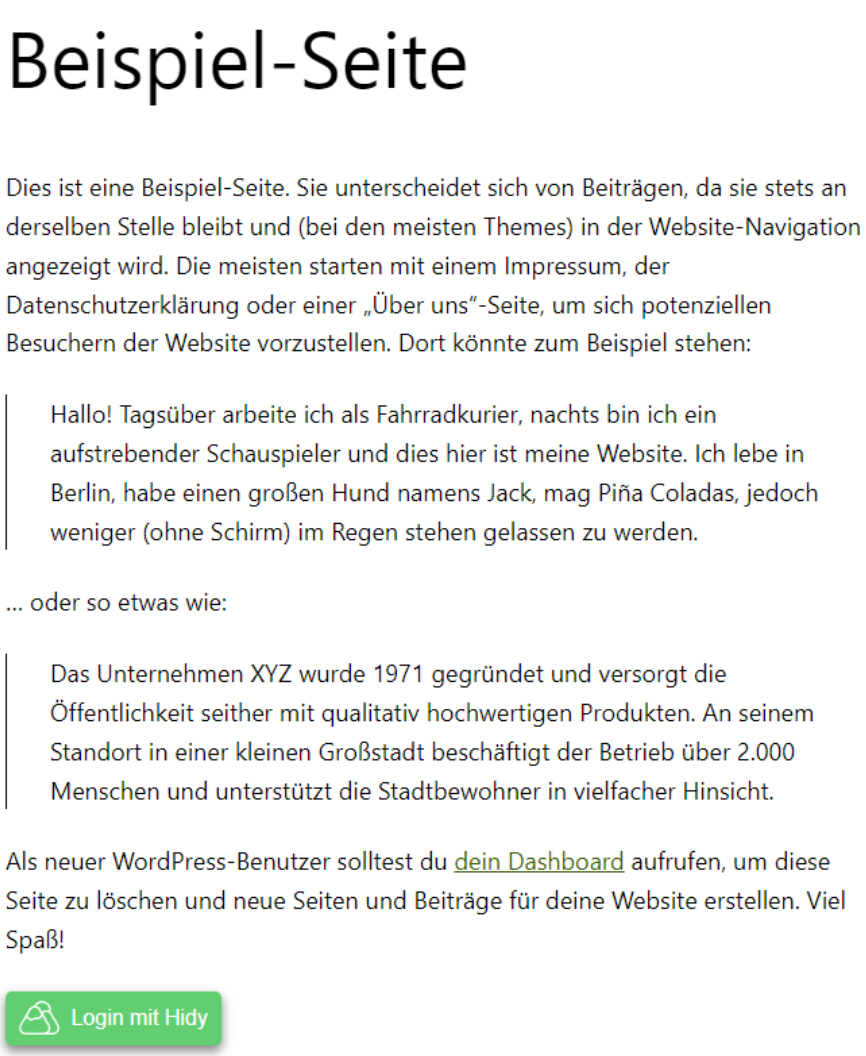


Abbildung 1: Screenshot einer, von WordPress generierten, Beispiel-Seite mit dem Hidy-Button
Quelle: Eigenkreation in Entwicklungsumgebung

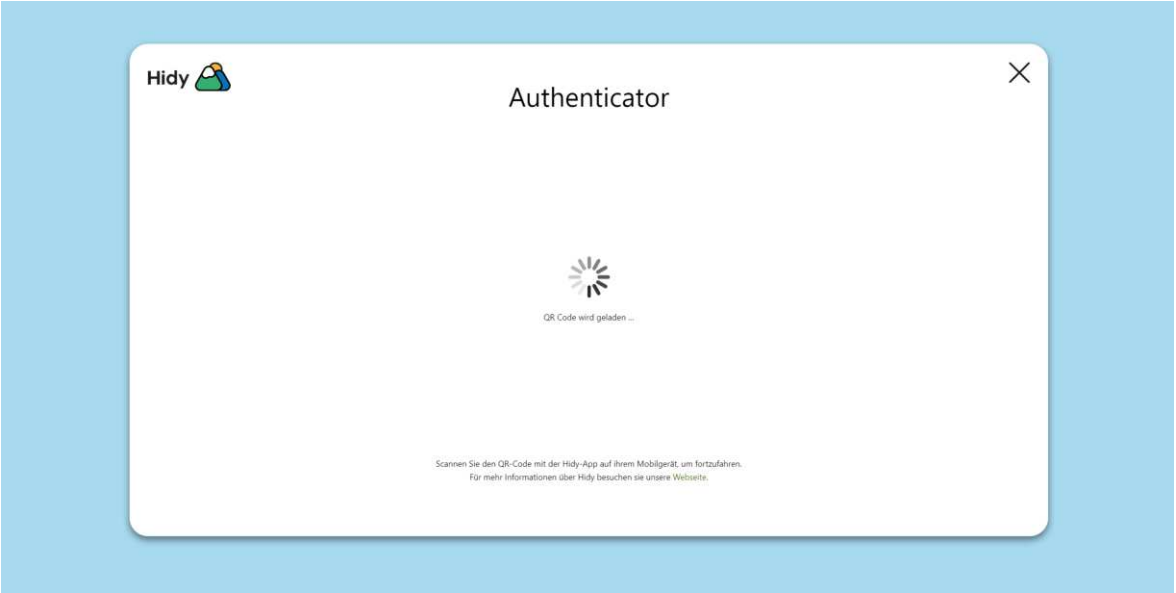


Abbildung 2: Screenshot des Hidy Pop-ups mit Ladebildschirm
Quelle: Eigenkreation in Entwicklungsumgebung

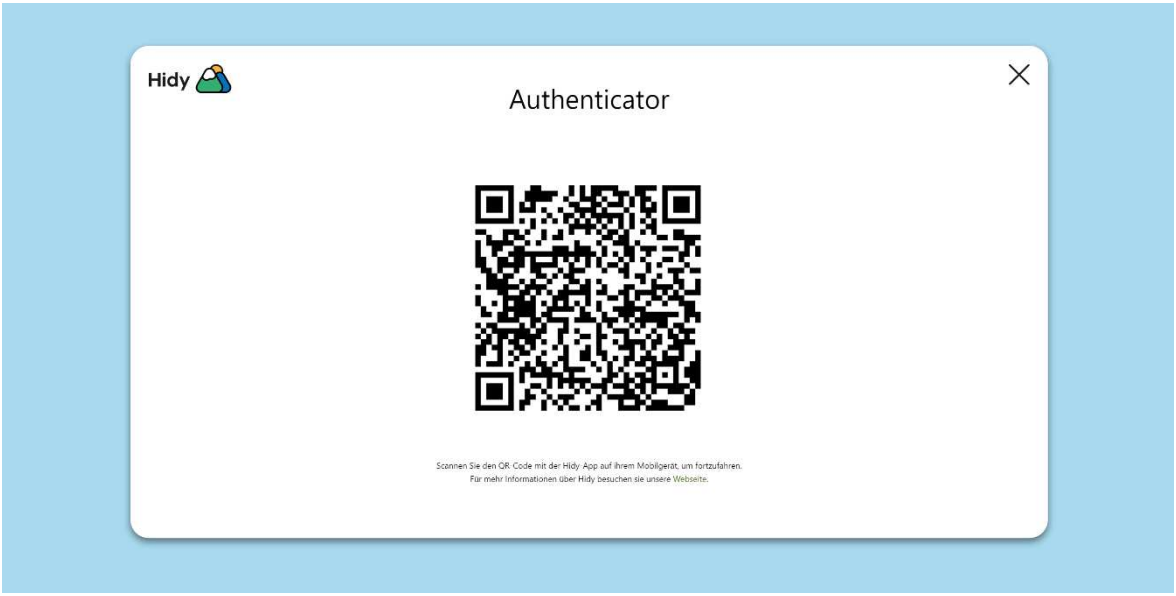


Abbildung 3: Screenshot des Hidy Pop-ups mit Beispiel-QR-Code
Quelle: Eigenkreation in Entwicklungsumgebung

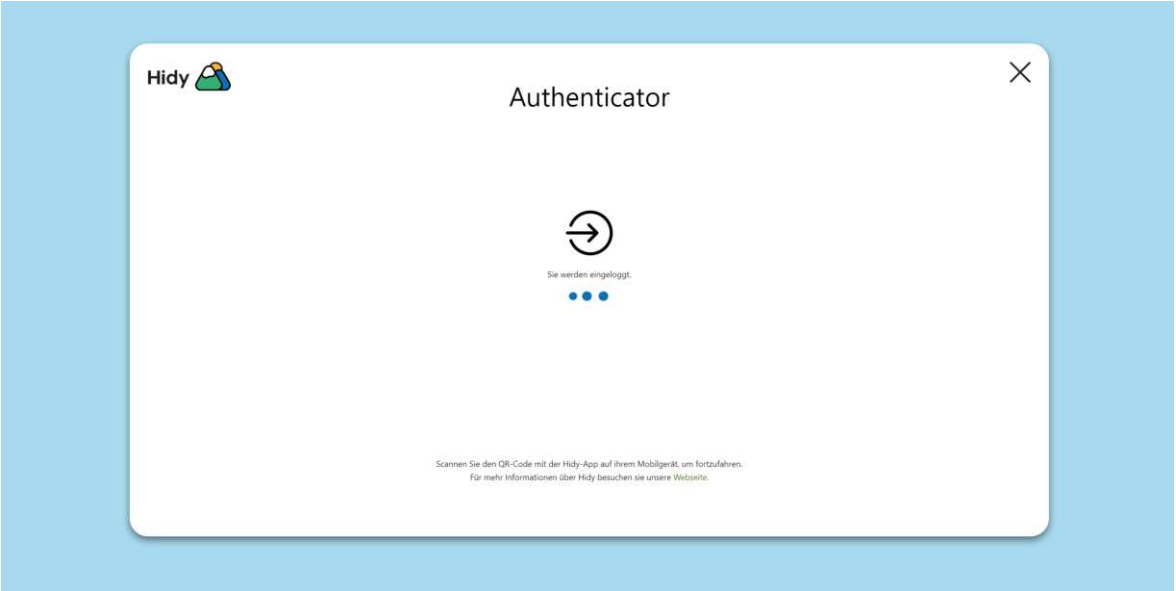


Abbildung 4: Screenshot des Hidy Pop-ups mit Login-Animation
Quelle: Eigenkreation in Entwicklungsumgebung

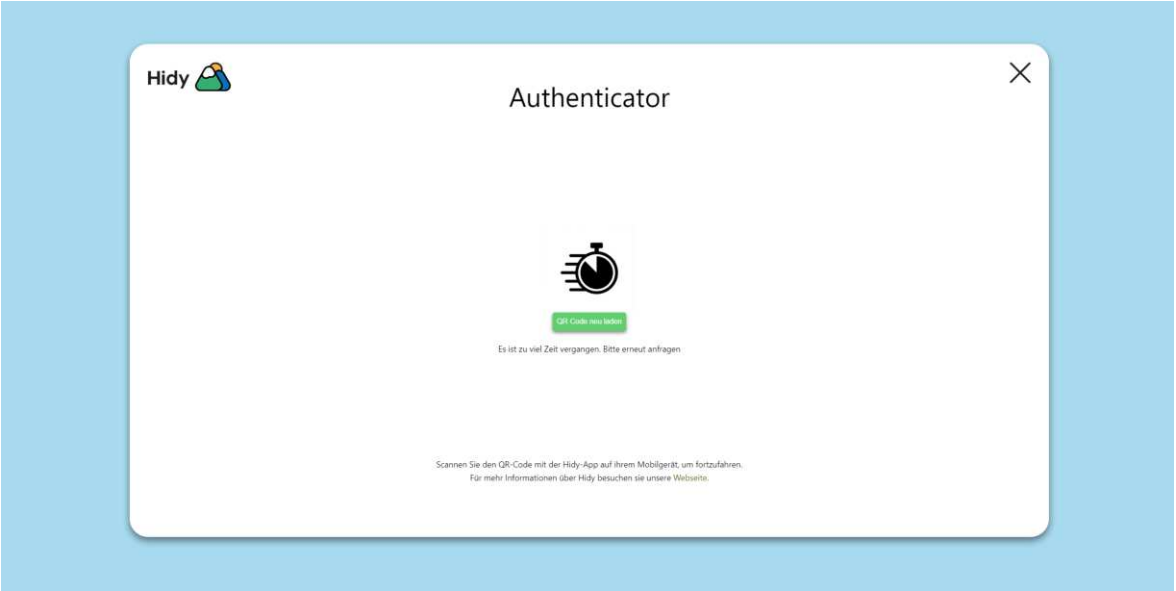


Abbildung 5: Screenshot des Hidy Pop-ups mit Zeitüberschreitungsanzeige
Quelle: Eigenkreation in Entwicklungsumgebung

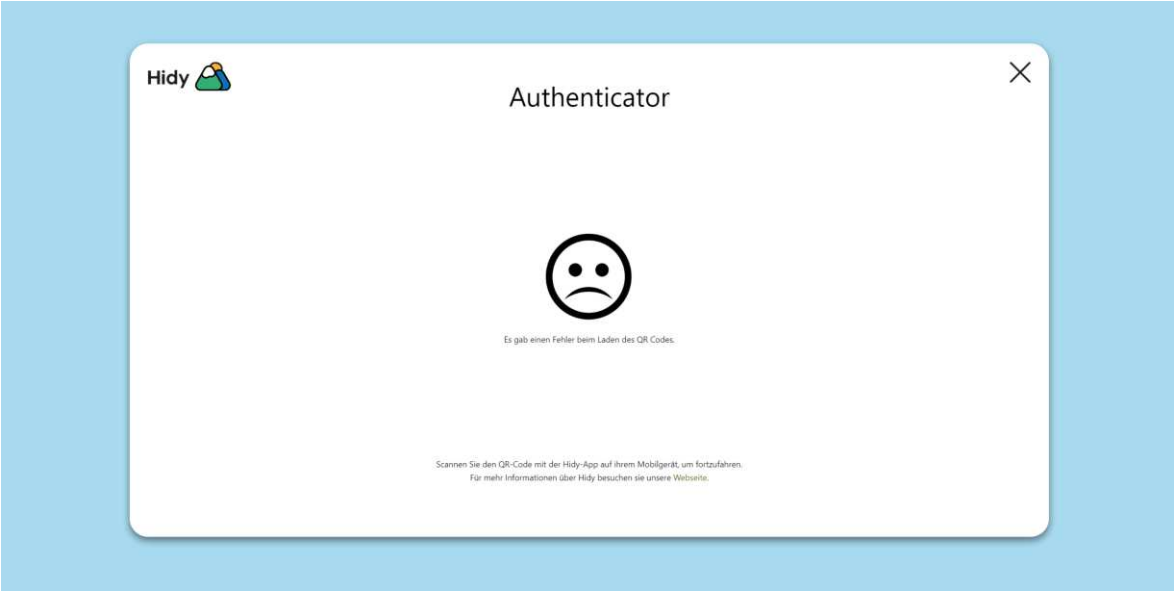


Abbildung 6: Screenshot des Hidy Pop-ups mit Fehlermeldung
Quelle: Eigenkreation in Entwicklungsumgebung

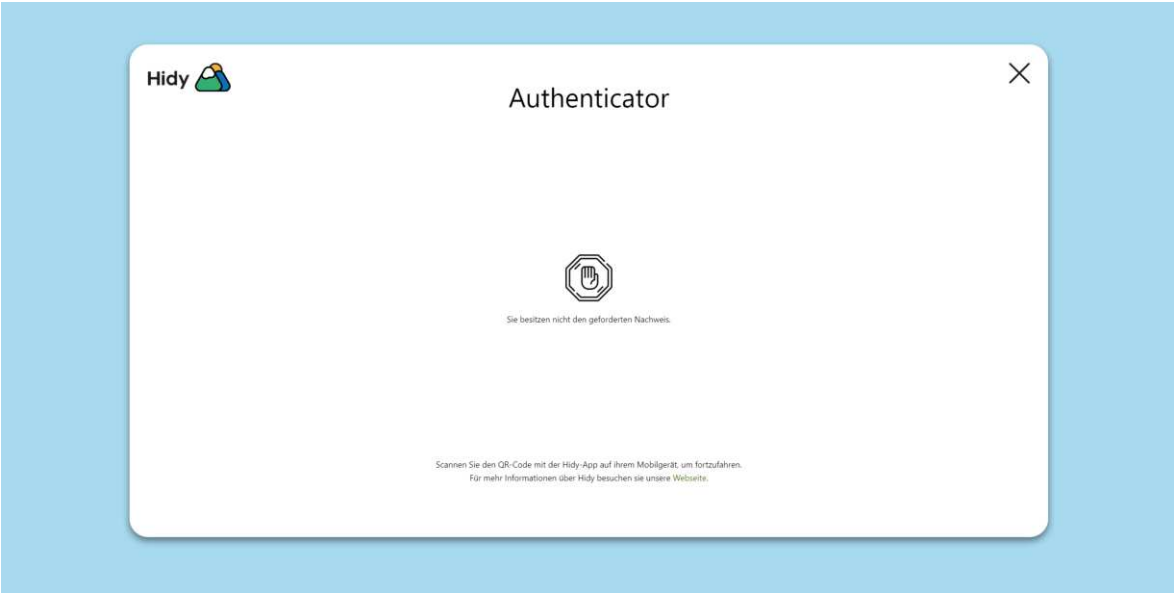


Abbildung 7: Screenshot des Hidy Pop-ups mit Information über Verweigerung des Logins
Quelle: Eigenkreation in Entwicklungsumgebung

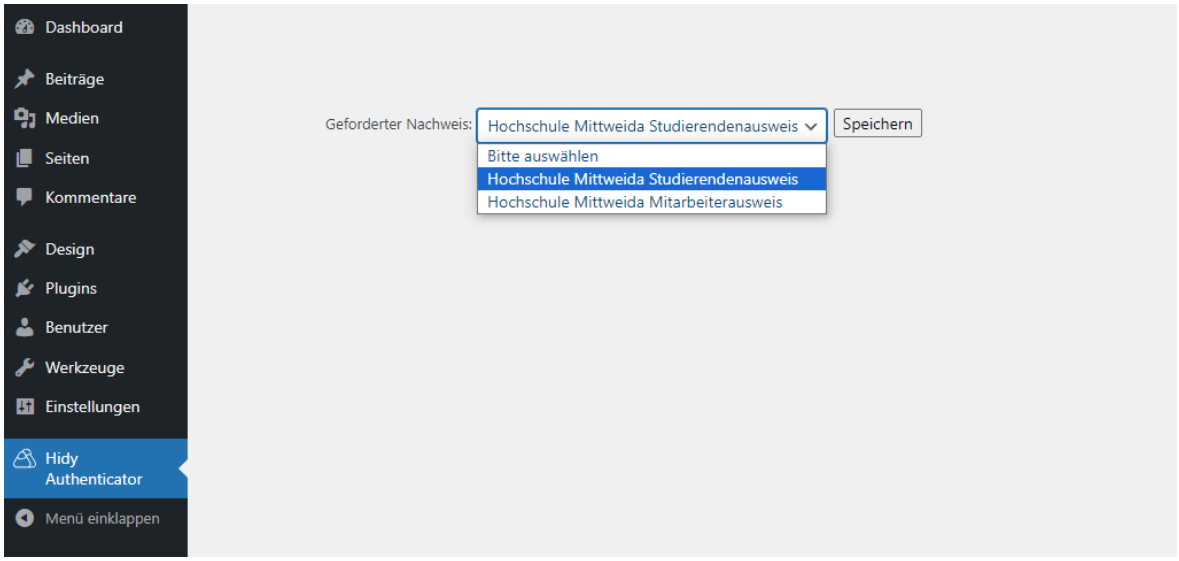


Abbildung 8: Screenshot des Einstellungsmenüs des Hidy-Validierungs-Plug-ins im Administrator-Dashboard einer WordPress-Webseite

Quelle: Eigenkreation in Entwicklungsumgebung

Selbstständigkeitserklärung

Hiermit erkläre ich, dass ich die vorliegende Arbeit selbstständig und nur unter Verwendung der angegebenen Literatur und Hilfsmittel angefertigt habe.

Stellen, die wörtlich oder sinngemäß aus Quellen entnommen wurden, sind als solche kenntlich gemacht.

Diese Arbeit wurde in gleicher oder ähnlicher Form noch keiner anderen Prüfungsbehörde vorgelegt.

Mittweida, den 27.11.2023



Paul Werner Anton Petzold