



Digitalisierung der Armee: Anwendung Blockchain-basierter Self-Sovereign Identity

Bachelor Thesis

Bern, 19. August 2022



Studenten

Luca Dietiker

Ralf Winkelmann

Experte

Konrad Durrer

Fachbetreuer

Markus Knecht

Auftraggeberin

Eidgenössisches Departement für Verteidigung,
Bevölkerungsschutz und Sport VBS

Fachhochschule Nordwestschweiz, Hochschule für Technik

Abstract

Die Schweiz wird den elektronischen Identifikationsnachweis (E-ID) mit Self-Sovereign Identity (SSI) aufbauen. Das Eidgenössische Departement für Verteidigung, Bevölkerungsschutz und Sport (VBS) möchte die E-ID für die Digitalisierung der Miliz nutzen und Wissen in diesem Bereich aufbauen. Das Ziel der vorliegenden Bachelorarbeit ist es, die Blockchain-Technologie als Basis für das Verifiable Data Registry (VDR) in einem staatlichen SSI-Ökosystem zu evaluieren. Aufgrund bestehender Literatur wurde die Eignung unterschiedlicher Blockchain-Ausprägungen unter anderem in zuvor definierten Szenarien (auch im Kontext der Schweizerischen Armee) evaluiert. Diese Arbeit kommt zum Schluss, dass sich Public Blockchains – insbesondere die Ausprägung Permissioned – für ein staatliches Ökosystem eignen und den Anforderungen des VBSs gerecht werden.

In einem Proof of Concept (PoC) wurde ein SSI-Ökosystem auf Basis der Blockchain-Technologie mit dem Jolocom-Framework umgesetzt. Als Anwendungsfall dient die Ausbildungsgutschrift, die abhängig von Dienstgrad und Ausbildungsdauer dem Milizkader der Schweizerischen Armee gewährt wird. Der umgesetzte PoC beweist, dass vorliegender Anwendungsfall mit einer SSI-Lösung signifikant effizienter und benutzerfreundlicher umgesetzt werden könnte.

Keywords: Self-Sovereign Identity (SSI), Verifiable Data Registry (VDR), Blockchain, Digitalisierung, Jolocom, E-ID, Armee

Inhaltsverzeichnis

1 Einleitung	1
2 Theoretischer Teil	3
2.1 Related Work	4
2.2 Blockchain	5
2.2.1 Arten der Blockchain	6
2.2.2 Konsensusmechanismen	7
2.2.3 Smart Contracts	8
2.3 Kryptografie	9
2.3.1 Hashing	9
2.3.2 Asymmetrische Schlüssel-Verfahren	9
2.3.3 Verschlüsselung	9
2.3.4 Digitales Signieren	10
2.3.5 Challenge-Response-Verfahren	10
2.4 Self-Sovereign Identity	12
2.4.1 Teilnehmer/innen	12
2.4.2 Decentralized Identifier (DID)	13
2.4.3 DID-Methoden	13
2.4.4 Verifiable Credential (VC)	14
2.4.5 Verifiable Presentation (VP)	14
2.4.6 Certificate Authority (CA) und Trusted List (TL)	14
2.4.7 Digitales Wallet	15
2.4.8 Verifiable Data Registry (VDR)	15
2.4.9 Zero-Knowledge-Proofs	15
2.4.10 Predicate Proofs	16
2.4.11 Selective Disclosure	16
2.4.12 Prinzipien	16
2.5 Aktuelle Anwendungen	17
2.5.1 IDunion	17
2.5.2 Estland	17
2.5.3 Blockcerts Caribe	18
2.5.4 SSI+ (Procivis)	18
2.5.5 OrgBook BC	18

2.5.6	Findy	19
2.5.7	Kiva	19
2.5.8	Building Blocks	19
2.5.9	truu	20
2.5.10	BCdiploma	20
2.5.11	Übersicht	21
2.5.12	Fazit	22
2.6	Szenarien	23
2.6.1	Naturgefahren	23
2.6.2	Stromausfall	23
2.6.3	Cyber-Angriff	23
2.6.4	Bewaffneter Konflikt	23
2.6.5	Terrorismus	24
2.6.6	Übersicht	24
2.7	Anforderungen an VDR	25
2.7.1	Anforderungen aus SSI-Architektur	25
2.7.1.1	Dezentralität	25
2.7.1.2	Zugänglichkeit, Portabilität und Interoperabilität	25
2.7.1.3	Persistenz	25
2.7.2	Anforderungen aus Szenarien	26
2.7.2.1	Ausfallsicherheit	26
2.7.2.2	Unstoppbarkeit	26
2.7.2.3	Zensurresistenz	26
2.7.2.4	Transnationalität	26
2.7.3	Anforderungen des VBS	26
2.7.3.1	Performance	27
2.7.3.2	Kosten	27
2.7.3.3	Nachhaltigkeit	27
2.7.3.4	Regulationskonformität	27
2.7.3.5	Datenschutz	28
2.7.4	Gewichtungsmatrix	28
2.8	Evaluation Blockchain als VDR	30
2.8.1	Einordnung und Vergleich anderer Systeme	30
2.8.1.1	Zentrales System	30

2.8.1.2	Verteiltes System	31
2.8.1.3	Dezentrales System	31
2.8.2	Private Blockchain	31
2.8.3	Public Blockchain	32
2.8.3.1	Dezentralität	32
2.8.3.2	Persistenz	32
2.8.3.3	Zugänglichkeit, Portabilität und Interoperabilität	33
2.8.3.4	Regulation	33
2.8.3.5	Datenschutz	33
2.8.3.6	Performanz	34
2.8.3.7	Nachhaltigkeit	34
2.8.3.8	Sicherheit	35
2.8.3.9	Kosten	35
2.8.4	Evaluation	37
2.8.5	Fazit	39
2.9	Empfehlungen	40
2.9.1	Architektur	40
2.9.1.1	Grundarchitektur	40
2.9.1.2	Knoten	40
2.9.1.3	Transnationalität	41
2.9.1.4	Technologie	41
2.9.2	Standards	41
2.9.2.1	DID-Methode	41
2.9.2.2	Internationale Standards	41
2.9.2.3	Nationale Standards	42
2.9.3	Sicherheit	42
2.9.3.1	Algorithmen	42
2.9.3.2	Anpassungsfähigkeit	42
2.9.4	Wallet	42
3	Praktischer Teil	43
3.1	Anwendungsfall	44
3.1.1	Ausgangslage	44
3.1.2	Zielbild	45

3.2	Evaluation Technologien	46
3.2.1	Kriterien	46
3.2.2	Technologien	47
3.2.2.1	Jolocom	47
3.2.2.2	Veramo	47
3.2.2.3	Evernym	48
3.2.3	Entscheid	48
3.3	Übersicht des umgesetzten Ökosystems	49
3.4	Systemarchitektur	50
3.4.1	Google Cloud Run	51
3.4.2	CockroachDB	51
3.4.3	InterPlanetary File System	51
3.4.4	Ethereum Rinkeby	51
3.4.4.1	Registry Contract	51
3.4.5	SSI Credential Generator	52
3.4.6	myArmy Portal	53
3.4.7	Jolocom SmartWallet	55
3.4.8	Callback Logger	55
3.5	Interaktionen	56
3.5.1	Registrierung einer DID	56
3.5.2	Auflösung einer DID	57
3.5.3	Credential ausstellen	58
3.5.4	Credential verifizieren	59
3.6	Schwierigkeiten	61
3.6.1	Dokumentation	61
3.6.2	Source Code des Framework	61
3.6.3	Fehlersuche mit Jolocom SmartWallet	63
3.6.4	Jolocom Fueling Service	64
3.7	Erweiterungen	65
3.7.1	Zertifikate widerrufen	65
3.7.2	Wiederherstellung	65
3.7.3	Eigene Infrastruktur	65
3.7.4	Unterstützung von Verifiable Presentations	66
3.7.5	Trusted Lists	66
3.7.6	Integration an VBS-Anwendungen	66
3.8	Fazit	67

4 Schlussbemerkungen	68
4.1 Blockchain als VDR	68
4.2 SSI-Ökosystem mit Jolocom	68
Quellenverzeichnis	69
Abbildungsverzeichnis	75
Tabellenverzeichnis	77
Ehrlichkeitserklärung	78
A Anhang	79
A.1 Meeting Protokoll – 03.05.2022	79
A.2 Überblick Frameworks/Technologien	81
A.3 Plausibilitätsklassen	84
A.4 myArmy Portal - Prototype	85
A.5 JSON Web Token – Credential Offer	89
A.6 JSON Web Token – Credential Request	90

Glossar

Bitcoin Public Permissionless Blockchain, die Transaktionen der Kryptowährung «Bitcoin» speichert.

Brute Force Methode Methode bei der mit «roher Gewalt» (durch wahlloses Ausprobieren unterschiedlicher Buchstaben- und/oder Zahlenkombinationen) versucht wird, der zur Verschlüsselung/Signierung verwendeten Schlüssel herauszufinden, ohne diesen zu kennen[1].

Container Registry Eine Container Registry ist ein zentraler Ort, an dem Images für die containerbasierte Anwendungsentwicklung gespeichert werden.

Docker Software zur Isolierung von Anwendungen mittels Containervirtualisierung. Ein Image bündelt eine Anwendung inklusive aller nötigen Abhängigkeiten und Dateien und wird zur Laufzeit in einem Container gestartet. Dieses Image/Container wird nicht mehr auf dem Zielsystem installiert und gestartet, sondern durch eine Container-Plattform verwaltet. Dadurch kann eine Anwendung unabhängig von Betriebssystem und Umgebung ausgeführt werden.

DPKI PKI-Infrastrukturen beruhen für die Erstellung von Zertifikaten und die Bereitstellung entsprechender (asymmetrischer) Schlüsselpaare auf das Vertrauen in zentrale Instanzen. DPKI steht für Decentral Public Key Infrastructure. Wie der Name impliziert, wird auf eine zentrale Instanz verzichtet und stattdessen auf einen dezentralen Ansatz gesetzt. (vgl. [2])

Ethereum Public Permissionless Blockchain, die das Betreiben von dezentralen Applikationen bzw. Smart Contracts erlaubt und eine eigene Kryptowährung «Ether» besitzt.

IPFS Das Interplanetary File System (IPFS) ist ein verteiltes System für die Speicherung von und den Zugriff auf Dateien, Websites, Anwendungen und Daten. Als Adresse für die Datei im Netz wird ein Hash des Inhalts der Datei generiert. Damit kontrastiert IPFS mit den «ortsbasierten» Adressen wie z.B. URLs.

Quantencomputer Neuartige Prozessoren, die anstelle elektrischer Zustände sog. quantenmechanische Zustände verwenden. Theoretisches Konstrukt, das verspricht viele mathematische und physikalische Probleme in Bruchteilen der heute benötigten Zeit zu lösen bzw. zu berechnen.

Verteiltes System Eine Sammlung unabhängiger Computer, die physisch oder virtuell voneinander getrennt sind und an einem gemeinsamen Ziel arbeiten. In dieser Arbeit wird davon ausgegangen, dass das System einer zentralen Instanz unterliegt.

Akronyme

AdA Angehörige/r der Armee

ASTRA Bundesamt für Strassen

BABS Bundesamt für Bevölkerungsschutz

BIT Bundesamt für Informatik und Telekommunikation

BJ Bundesamt für Justiz

BMWK Bundesministerium für Wirtschaft und Klimaschutz

BSI Bundesamt für Sicherheit in der Informationstechnik (Deutschland)

CA Certificate Authority

DDoS Distributed-Denial-of-Service

DID Decentralized Identifier

DIF Decentralized Identity Foundation

DLT Distributed Ledger Technology

DNS Domain Name System

DSG Bundesgesetz über den Datenschutz

DSGVO Datenschutz-Grundverordnung

DTI Digitale Transformation und IKT-Lenkung

E-ID Elektronische Identität

EBSI European Blockchain Services Infrastructure

eIDAS Verordnung über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt

EJPD Eidgenössisches Justiz- und Polizeidepartement

eSSIF European Self-Sovereign Identity Framework

EU Europäische Union

FHNW Fachhochschule Nordwestschweiz

GAU Grösster Anzunehmender Unfall

IKT Informations- und Kommunikationstechnik

ISO International Organization for Standardization

JWT JSON Web Token

NGO Nichtregierungsorganisation

NHS National Health Service

P2P Peer-to-Peer

PKI Public Key Infrastructure

PoA Proof of Authority

PoC Proof of Concept

PoS Proof of Stake

PoW Proof of Work

SSI Self-Sovereign Identity

TL Trusted List

UNHCR Hoher Flüchtlingskommissar der Vereinten Nationen

UNO Vereinte Nationen

VBS Eidgenössische Departement für Verteidigung, Bevölkerungsschutz und Sport

VC Verifiable Credential

VDR Verifiable Data Registry

VP Verifiable Presentation

W3C World Wide Web Consortium

WFP World Food Programme

ZKP Zero Knowledge Proof

1 Einleitung

Die Behörden in der Schweiz wollen in den kommenden Jahren die Digitalisierung in verschiedenen Bereichen vorantreiben. Zu diesem Zweck nahm 2021 der Bereich «Digitale Transformation und IKT-Lenkung» (DTI) seine Arbeit auf. Das Bundesamt für Informatik und Telekommunikation (BIT) erarbeitet unter der Federführung des DTI die elektronische Identität (E-ID) für die Schweizer Bevölkerung. Die Einbindung der E-ID in bestehende Prozesse liegt in der Verantwortung aller Departemente und Bundesämter.

Das Eidgenössische Departement für Verteidigung, Bevölkerungsschutz und Sport (VBS) hat dazu bereits Schritte geplant. Die Vision «Armee 2030» sieht unter anderem die Digitalisierung der Miliz vor. Ein zentraler Teil davon ist die Schaffung eines Bürgerportals. In einem ersten Schritt sollen Use-Cases realisiert werden, die vor allem junge Bürgerinnen und Bürger ansprechen. Das VBS ist aktuell daran, mögliche Use-Cases und eine Kunden-Erlebnis-Kette aufzubauen. Diese wiederum werden die Basis für den Aufbau des Bürgerportals sein.

Zudem hat der Bundesrat an seiner Sitzung vom 17. Dezember 2021 die Stossrichtung für einen künftigen digitalen staatlichen Identitätsnachweis festgelegt. Nutzerinnen und Nutzer der E-ID sollen durch die Anwendung von Self-Sovereign Identity (SSI) grösstmögliche Kontrolle über ihre Daten haben. Wie eingangs erwähnt, sind alle Departemente in der Pflicht, die E-ID künftig in eigene Prozesse zu integrieren. Das VBS möchte deshalb im Rahmen des laufenden Digitalisierungs-Projektes (Bürgerportal) auch Erfahrungen mit der E-ID sammeln¹.

Eignung Blockchain-Technologie für SSI Im theoretischen Teil der Arbeit werden die Themen SSI, Blockchain und Kryptografie eingeleitet. Die Eignung der Blockchain-Technologie als Verifiable Data Registry (VDR) der SSI-Infrastruktur wird untersucht. Verschiedene Blockchain-Ausprägungen werden einander gegenübergestellt und hinsichtlich Faktoren wie Nachhaltigkeit, Performance, Sicherheit und Resilienz in verschiedenen Szenarien verglichen.

Die Eignung der Blockchain-Technologie als VDR wurde methodisch als Literaturarbeit aufgearbeitet. Dazu wurde Literatur zu unterschiedlichen Bereichen und isolierten Fragestellungen (z.B. Datenschutzkonformität der Blockchain) herangezogen. Die Erkenntnisse werden konsolidiert bzw. kombiniert, um anschliessend eine übergreifende Einschätzung abgeben zu können.

Umsetzung der Ausbildungsgutschrift mit SSI Der praktische Teil der Arbeit dokumentiert die Umsetzung eines SSI-Ökosystems auf Basis der Blockchain-Technologie mit dem Jolocom-Framework. Als Proof of Concept (PoC) dient die Ausbildungsgutschrift für das Milizkader der Schweizerischen Armee, die je nach Dienstgrad und Ausbildungsdauer ausgezahlt wird.

Für die Interaktion mit dem Ökosystem wurde die Jolocom SmartWallet App verwendet und zwei Webanwendungen umgesetzt:

- Die Anwendung «SSI Credential Generator» ermöglicht das Ausstellen digitaler Zertifikate (E-ID und Bildungszertifikate), die für die Ausbildungsgutschrift nötig sind.
- Das «myArmy Portal» bietet die Möglichkeit Militärzertifikate auszustellen und ein Anspruch auf Ausbildungsgutschrift automatisiert zu prüfen.

¹vgl. <https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-86465.html>

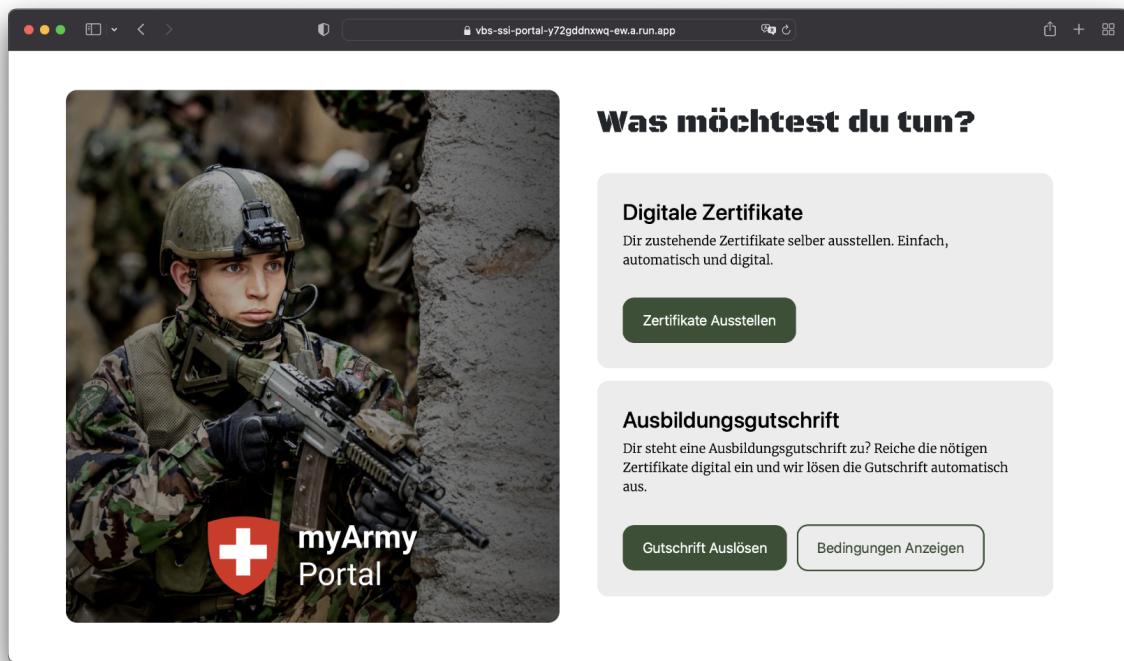


Abbildung 1.1: Startseite der umgesetzten Webanwendung «myArmy Portal» für die Interaktionen des VBSs mit dem SSI-Ökosystem.

Leseführung: Zu Beginn des theoretischen (Kapitel 2) und praktischen (Kapitel 3) Teils gibt es eine Leseführung zum jeweiligen Kapitel. Eine Zusammenfassung der Ergebnisse findet sich für die Evaluation der Blockchain als VDR im Abschnitt 2.8.5 auf Seite 39 und für den Proof of Concept im Abschnitt 3.8 auf Seite 67. Schlussbemerkungen und Ausblick sind im Kapitel 4 auf Seite 68 zu finden.

Kapitel

2 Theoretischer Teil

Leseführerung: Der theoretische Teil leitet in die Thematik ein und beschäftigt sich mit der Frage, ob die Blockchain als Verifiable Data Registry (VDR) geeignet ist.

Zu Beginn werden ähnliche Arbeiten und Literatur (Abschnitt 2.1) analysiert und die Grundlagen der Blockchain (Abschnitt 2.2), Kryptografie (Abschnitt 2.3) und SSI (Abschnitt 2.4) eingeführt. Im Abschnitt 2.5 werden aktuelle Anwendungen von SSI und deren VDR analysiert.

Zur Evaluation der VDR-Technologie werden Anforderungen (Abschnitt 2.7) an ein VDR für eine Schweizer SSI-Lösung unter Einbezug verschiedener Szenarien (Abschnitt 2.6) hergeleitet. Unter Anwendung dieser Anforderungen werden in Abschnitt 2.8 verschiedene Architekturen und Blockchain-Ausprägungen analysiert. Geeignete Ansätze werden im Abschnitt 2.8.4 evaluiert und im Abschnitt 2.8.5 wird ein Fazit gezogen.

Abschliessend werden im Abschnitt 2.9 Empfehlungen für eine Implementierung eines VDR auf Basis der Blockchain-Technologie aggregiert.

2.1 Related Work

In vielen wissenschaftlichen Arbeiten basiert das SSI-Register auf der Distributed Ledger Technology (DLT) — oft wird spezifisch von der Blockchain-Technologie gesprochen. Die Autoren des Papers «A survey on essential components of a self-sovereign identity»[3] identifizieren die Blockchain-Technologie als eine der vier essenziellen Bausteine für die Architektur.

Die Mehrheit der aktuellen Anwendungen von SSI (siehe auch Abschnitt 2.5 auf Seite 17) basieren auf der Blockchain-Technologie. Das hängt unter anderem damit zusammen, dass bestehende technische Lösungen bzw. Frameworks oft Blockchain-basiert sind. Das Paper «Self-Sovereign Identity Solution for Blockchain-Based Land Registry System: A Comparison»[4] evaluiert neun Blockchain-basierte SSI-Lösungen, unter anderem auf Basis der zehn SSI-Prinzipien von C. Allen[5]. Laut dem Paper erfüllt das Sovrin Netzwerk die meisten Prinzipien und wird von den Autoren empfohlen. Keine der Lösungen erfüllt alle Prinzipien.

Ein Paper[6] der University of Texas at Austin vergleicht 31 existierende SSI-Lösungen anhand von mehreren funktionalen und nicht-funktionalen Anforderungen. Sie konkludieren, dass Blockchain-basierte Lösungen besser abschliessen als jene ohne Blockchain.

Das Paper «Self-Sovereign Identity Solutions: The Necessity of Blockchain Technology»[7] untersucht die generelle Notwendigkeit der Blockchain-Technologie für SSI. Die Autoren kommen zum Schluss, dass die Blockchain-Technologie nicht zwingend nötig ist, jedoch aufgrund diverser technischer Vorteile eine gute Grundlage für SSI bietet.

Das deutsche Bundesamt für Sicherheit in der Informationstechnik (Deutschland) (BSI) schreibt in seinem Eckpunktepapier[8] zu SSI: «*Self-sovereign Identities müssen nicht zwingend auf einem DLT-basierten Register beruhen. Die Dezentralität und hohe Verfügbarkeit eines Distributed Ledgers werden zwar oft als Vorteil genannt, sind aber kein Alleinstellungsmerkmal dieser Technologie. Auch andere Systeme, wie beispielsweise verteilte Datenbanken oder Verzeichnisdienste, können für das Datenregister in Betracht kommen.*»[8] Durch fehlende Standards und ein Mangel an Sicherheitsempfehlungen sieht das Bundesamt eine erhöhte Komplexität des Systems bei Verwendung von Distributed-Ledger-Technologien.

Marcos Allende López bezeichnet in seinem Buch «Self-Sovereign Identity: The Future of Identity: Self-Sovereignty, Digital Wallets, and Blockchain» Blockchain und SSI als perfekte Symbiose – die beiden Ideen würden sich perfekt ergänzen[9, p. 36]. López sieht in der Ausprägung Public Permissioned Blockchain das grösste Potential und schreibt: «*The self-sovereign identity model can leverage different types of blockchain networks in addition to other decentralized ledgers. However, permissioned public networks are most suitable. Permissionless networks are designed to be anonymous and permissioned private networks are designed to be small and limited to specific use cases. Alternatively, permissioned public networks often have zero transaction fees, are compliant with regulations, and are designed to be multipurpose, making them a perfect fit for the decentralized ledger that self-sovereign identity demands.*»[9, p. 84-85]

2.2 Blockchain

Digitale Daten können beliebig vervielfältigt und manipuliert werden. Änderungen sind nur nachvollziehbar, wenn darüber Buch geführt wird. Werden Rohdaten und Logs über deren Manipulation/Veränderung durch dieselbe Partei gespeichert, entsteht ein Abhängigkeitsverhältnis. Die Integrität der Daten kann nicht unabhängig verifiziert werden – das System basiert auf Vertrauen.

1991 schlugen Stuart Haber und W. Scott Stornetta «[...] praktische Rechenverfahren für das digitale Zeitstempeln von Dokumenten vor, so dass es für einen Benutzer, eine Benutzerin nicht möglich ist ein Dokument zurück- oder vorzudatieren, selbst wenn der Zeitstempeldienst seine Integrität verliert.»[10, S. 99–111].

Die vorgeschlagene Lösung sieht vor, dass die Daten selbst zur Generierung eines Hash-Wertes verwendet und mit einem Zeitstempel digital signiert werden. Verwendet werden Einweg-Hash-Funktionen. Daraus resultieren digitale Zertifikate. Um zu verhindern, dass zu einem späteren Zeitpunkt mit veränderten Daten (aber gleichbleibendem Zeitstempel) derselbe Hash generiert wird, schlugen Haber und Stornetta folgende Lösungen vor:

Verkettung Neue Hash-Werte sollen zusätzlich zu den Daten und dem Zeitstempel auch Teile des Hash-Wertes vorheriger Zertifikate enthalten. Das erschwert eine Vor- oder Rückdatierung erheblich, da die ganze Kette an verlinkten Hash-Werten neu berechnet werden müsste[10, S. 99–111].

Dezentralisierung Die Zertifikate zur Signierung werden durch pseudozufällig ausgewählte Teilnehmende in einem offenen Netzwerk erzeugt. Das erschwert Manipulationen durch betrügerische Parteien so lange genügend vertrauenswürdige Teilnehmende im Netzwerk vorhanden sind[10, S. 99–111].

Die vorgestellten Konzepte bilden in wesentlichen Teilen die Grundlage der heute bekannten Blockchain-Technologie. Daten bzw. die aktuellen Zustände von Datenstrukturen werden in «Blöcken» konzentriert. Von den im Block enthaltenen Daten/Zustände wird ein Hash-Wert im Kopf des Blocks gespeichert. Neue Blöcke sind mit vorherigen Blöcken verknüpft, in dem der Hash-Wert des gesamten vorherigen Blocks gespeichert wird. In Abbildung 2.1 wird die daraus resultierende Kette an Blöcken (vereinfacht) dargestellt. Diese Kette bildet die Blockchain. Die Blockchain selbst ist nicht nur auf einem Knoten gespeichert, sondern verteilt auf viele Knoten in einem dezentralen Netzwerk. Knoten sind Rechner (Computer, Smartphone etc.) die sich mit der Blockchain verbinden und unterschiedliche Aufgaben (z.B. Transaktionen validieren) übernehmen.

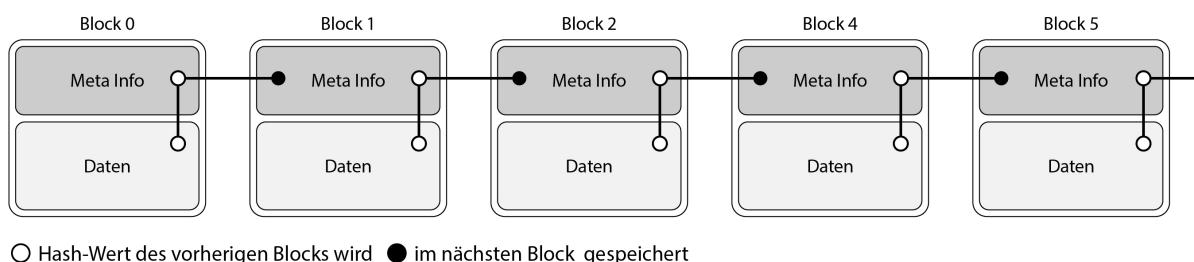


Abbildung 2.1: Vereinfachter, visueller Aufbau einer Blockchain-Kette mit verlinkten «Blöcken». Nachträgliche Manipulation würde eine komplette Neuberechnung der gesamten Kette bedingen.

Von Stuart Haber und W. Scott Stornetta erwähnte Verkettung und Dezentralisierung bringt folgende Vorteile[11, S. 4]:

- **Betrugssicherheit / Vertrauen** – Es gibt keine zentrale Partei, der vertraut werden muss und somit keinen Single Point of Failure.
- **Transparenz** – Alle Teilnehmenden haben Zugriff auf die Kette von Datenblöcken.
- **Unveränderlichkeit** und **Rückverfolgbarkeit** – Durch die Verlinkung mit vorherigen Blöcken ist die nachträgliche Manipulation erschwert und die Rückverfolgbarkeit sichergestellt.

Die Blockchain eignet sich damit als Alternative für Systeme, die heute auf das Vertrauen in eine dritte Partei angewiesen sind. Die Blockchain ist eine Distributed Ledger Technology (DLT). 2008 wurde mit Bitcoin die Idee eines Finanz-Transaktionssystem auf Basis der Blockchain lanciert[12]. In einem 2013 veröffentlichten White Paper zeigt Vitalik Buterin auf, dass auch automatisierte Prozesse (bzw. Applikationen) direkt von der Blockchain ausgeführt werden können sobald definierte Bedingungen erfüllt sind[13, S. 22–23].

2.2.1 Arten der Blockchain

Es gibt verschiedene Ausprägungen der Blockchain-Technologie, die sich unter anderem im Grad der Dezentralität, des Zugriffs und des Berechtigungsmodells unterscheiden. Oft werden Blockchains in Public und Private kategorisiert[11, S. 8]:

Public Der Zugriff auf eine Public Blockchain ist prinzipiell für alle offen. Die Teilnehmenden können dabei anonym bleiben. Die Historie der Blockchain mit allen Transaktionen/Blöcken ist öffentlich einsehbar.

Private Für den Zugriff auf das Netzwerk ist eine Einladung/Erlaubnis nötig. Der Zugriff wird oft von einer zentralen Stelle vergeben und durch Authentifizierung mit Identitätsmanagementsystemen geprüft, wodurch die Anonymität der Teilnehmenden entfällt. Eine Private Blockchain kann auch als isoliertes Netzwerk betrachtet werden[14].

Weiter wird zwischen Permissioned und Permissionless Blockchains unterschieden.

Permissioned Ausgewählte Teilnehmende erhalten Rechte und andere werden eingeschränkt. Die Einschränkungen können auf verschiedene Aspekte der Blockchain angewendet werden. Beispielsweise kann das Verifizieren oder Ausführen von Transaktionen eingeschränkt werden[11, S. 8].

Permissionless Alle Teilnehmenden einer Permissionless Blockchain sind gleichgestellt und können innerhalb der Blockchain die gleichen Aktionen ausführen. Es gibt keine Knoten mit besonderen Berechtigungen bzw. Instanzen, die Berechtigungen vergeben können.

Die internationale Organisation für Standardisierung ISO unterscheidet zwischen drei Haupt-Ausprägungen. Abbildung 2.2 auf der nächsten Seite visualisiert diese drei Ausprägungen (Public Permissionless, Public Permissioned und Private) sowie deren Eigenschaften[15].



Abbildung 2.2: Überblick unterschiedlicher Blockchain-Ausprägungen. Private und Public unterscheidet die Offenheit der Blockchain: Wer kann teilnehmen? Permissioned und Permissionless bestimmen, ob Gruppen innerhalb des Netzwerks besondere Rechte oder Einschränkungen haben oder ob alle gleichgestellt sind. In der Theorie ist auch eine Private Permissionless Blockchain möglich – macht aber in der Praxis i.d.R. keinen Sinn und wurde deshalb aus dieser Illustration ausgeklammert.

Wird von einer Blockchain gesprochen, ist damit oft eine Public Permissionless Blockchain gemeint. Viele populäre Kryptowährungen wie Bitcoin oder Ethereum basieren auf Public Permissionless Blockchains. Auf dem Markt finden sich aber auch zahlreiche Projekte mit anderen Kategoriekombinationen[16].

Hinweis

Von einigen Blockchain-Technologien existiert ein Hauptnetz, das als Public Permissionless Blockchain betrieben wird (z.B. Ethereum Mainnet). Gleichzeitig kann die zugrundeliegende Technologie auch für den Betrieb einer eigenen (Private oder Public Permissioned) Blockchain verwendet werden. Wenn nicht anders vermerkt, ist in dieser Arbeit jeweils das entsprechende Hauptnetz gemeint.

2.2.2 Konsensusmechanismen

Die Blockchain ist auf verschiedenen Knoten im dezentralen Netzwerk gespeichert. Mittels Konsensusmechanismen wird zwischen den Knoten eine Einigung über den Status der Blockchain erzielt. Sie legen fest, wie neue Blöcke entstehen und an die bestehende Blockchain angefügt werden. Es gibt verschiedene Ansätze, wie dieser Konsens erreicht werden kann.² Zu den bekanntesten gehören Proof of Work (PoW) und Proof of Stake (PoS).

Proof of Work Um einen neuen Block zu generieren, muss ein Arbeitsnachweis geliefert werden. Dieser wird in Form von Rechenleistung durch das Lösen komplexer kryptografischer Rätsel erbracht. Wer das Rätsel am schnellsten löst, erhält eine Prämie. Ist die Lösung des Rätsels gefunden, wird diese von den anderen Teilnehmenden verifiziert und ein Konsens erreicht (und damit die Lösung durch das Netzwerk akzeptiert). Die Schwierigkeit des Rätsels passt sich dynamisch der Rechenleistung im Netzwerk an, damit eine konstante Erstellung neuer Blöcke garantiert werden kann. Dieser Mechanismus wird von Bitcoin und diversen anderen Blockchain-Systemen verwendet.[11, S. 117]

Proof of Stake Ein Nachteil des Proof of Work Mechanismus ist der hohe Energieverbrauch für die Sicherheit des Netzwerks. Um dem entgegenzuwirken setzt Proof of Stake auf einen

²Es gibt bereits mehr als 30 verschiedene Konsensusmechanismen[17].

Anteilsbeweis statt Rechenleistung. Berechtigt zum Erstellen neuer Blöcke sind nur Knoten, die genügend Einheiten einer bestimmten Kryptowährung besitzen. Die Einheiten der Kryptowährung müssen hinterlegt (blockiert) werden, um neue Blöcke erstellen zu können[11, S. 118].

Jeder Konsensusmechanismus hat seine eigenen Vor- und Nachteile, die je nach Anforderung an Dezentralität, Sicherheit und Effizienz stärker oder schwächer ins Gewicht fallen. Eine allgemeingültige Empfehlung kann nicht gemacht werden.

2.2.3 Smart Contracts

Ein Smart Contract ist eine Art digitaler Vertrag, der auf einer Blockchain basiert. Die Vereinbarungen des Vertrags werden vom Ersteller des Smart Contracts als Programmcode auf der Blockchain festgehalten – oft in einfachen «Wenn-Dann»-Anweisungen. Der Code wird automatisch ausgeführt, wenn gewisse Bedingungen erfüllt sind. Die Idee eines Smart Contracts wurde vom Kryptografen Nick Szabo bereits im Jahr 1994 vorgestellt[18]. Mit Ethereum wurden Smart Contracts im Jahr 2015 in die Blockchain-Welt eingeführt[11, S. 13].

Beispiel: Eine Reiseversicherung, die eine Entschädigung bei Flugausfällen bietet. Der Smart Contract kann die Flugdaten automatisch überwachen und bei einem Ausfall die Entschädigung direkt überweisen.

2.3 Kryptografie

Kryptografie ist die Wissenschaft der Verschlüsselung. Sie ist essenziell für die Wahrung von Vertraulichkeit, Integrität und Authentizität digitaler Informationen[19]. Die Kryptografie einen wichtigen Baustein für die Blockchain-Technologie und Self-Sovereign Identity.

2.3.1 Hashing

Eine Hashfunktion wandelt eine beliebig lange Zeichenfolge in eine Prüfsumme (Hashwert) mit vordefinierter Länge um. Eine kryptografische Hashfunktion sollte unumkehrbar³ sein und einen einzigartigen Hashwert der Eingabe generieren. Eine kleine Änderung am Ausgangstext (z.B. einen Buchstaben ändern) sollte zu einem komplett anderen Resultat führen. Hashfunktionen werden unter anderem in Mechanismen zur Verschlüsselung, Integritätsprüfung von Daten und für das Erstellen digitaler Signaturen verwendet[20].

2.3.2 Asymmetrische Schlüssel-Verfahren

Asymmetrische Schlüssel-Verfahren erstellen ein Schlüsselpaar, bestehend aus einem privaten und einem öffentlichen Schlüssel. Privat und öffentlich deshalb, weil nur der private Schlüssel «geheim» bleiben muss. Der öffentliche Schlüssel kann (und soll) öffentlich zugänglich sein. Diese Schlüssel sind logisch/mathematisch miteinander verbunden, können aber nicht voneinander abgeleitet werden[20].

Symmetrische Schlüssel-Verfahren

Neben den asymmetrischen Schlüssel-Verfahren gibt es auch symmetrische Verfahren. Der Unterschied: Es wird nur ein Schlüssel erstellt. Die sendende wie die empfangende Partei haben eine Kopie desselben Schlüssels.

2.3.3 Verschlüsselung

Beim Verschlüsseln von Daten handelt es sich um kryptografische Mechanismen. Eine mathematische Funktion nimmt als Eingabe die zu verschlüsselnden Daten sowie einen entsprechenden Schlüssel entgegen und gibt eine für den Menschen nicht interpretierbare («kryptische») Abfolge von Zahlen und Buchstaben aus. So ist sichergestellt, dass nur Personen mit dem entsprechenden Schlüssel die Daten wieder entschlüsseln können. Je nach Verfahren ist dieser Schlüssel nicht identisch mit dem zur Verschlüsselung verwendeten Schlüssel⁴. Ziel der Verschlüsselung ist es, die Daten (z.B. bei Übermittlung via Internet) vor unbefugtem Zugriff zu schützen[21].

Abbildung 2.3 auf der nächsten Seite illustriert beispielhaft die Verschlüsselung mit einem asymmetrischen Schlüsselpaar.

³Unumkehrbar heisst: Aus dem Resultat (Hashwert) sollte nicht wieder auf den Ausgangstext geschlossen werden können.

⁴vgl. Abschnitt 2.3.2

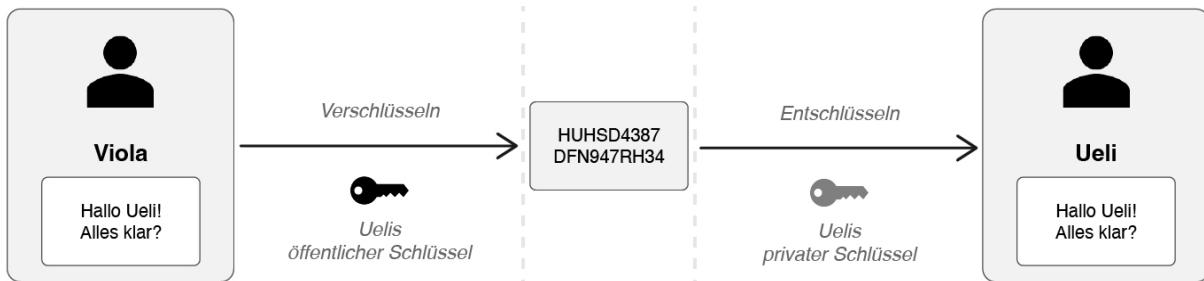


Abbildung 2.3: Beispiel asymmetrische Verschlüsselung: Viola nutzt den öffentlichen Schlüssel von Ueli, um eine Nachricht zu verschlüsseln. Die Nachricht wird via Internet übertragen und Ueli kann die Nachricht mit seinem privaten Schlüssel wieder entschlüsseln.

2.3.4 Digitales Signieren

Dokumente/Daten können mit digitalen Signaturen versehen werden. Die Signatur ersetzt dabei im digitalen Raum die physische Unterschrift. Unter Anwendung kryptografischer Funktionen wird mit einem Schlüssel ein digitales Zertifikat erstellt. Die Funktion nimmt neben einem Schlüssel auch die im Dokument enthaltenen Informationen als Eingabe entgegen. Eine Änderung des Inhalts ergibt ein verändertes Zertifikat. So können zwei Dinge jederzeit geprüft werden:

- Wurde das Dokument von einer bestimmten Partei signiert?
- Wurde der Inhalt des Dokuments seit der Signierung verändert?

Je nach verwendetem Verfahren sind zur Generierung und Prüfung einer Signatur unterschiedliche Schlüssel nötig⁵. Ziel des digitalen Signierens ist die Wahrung der Datenintegrität[21][22].

Abbildung 2.4 illustriert beispielhaft die Signierung einer Nachricht mit einem asymmetrischen Schlüsselpaar.

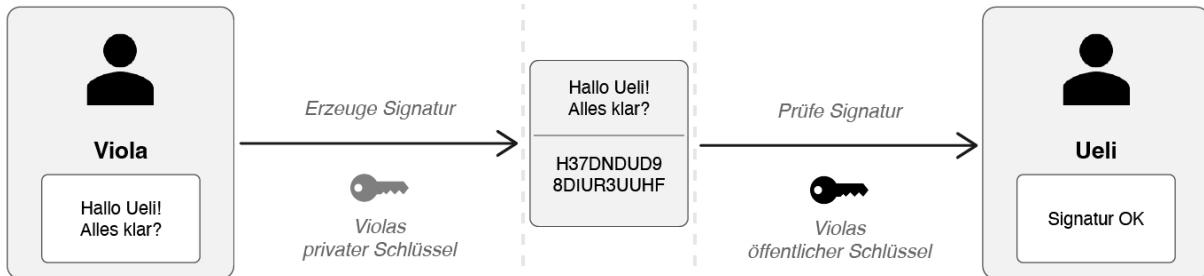


Abbildung 2.4: Beispiel asymmetrische Signierung: Viola nutzt ihren privaten Schlüssel, um eine Nachricht zu signieren. Die Nachricht wird zusammen mit der Signatur via Internet übertragen. Ueli prüft die Signatur mit dem öffentlichen Schlüssel von Viola.

2.3.5 Challenge-Response-Verfahren

Das Challenge-Response-Verfahren ermöglicht die Prüfung, ob eine Entität tatsächlich im Besitz eines konkreten Schlüssels ist, ohne dass die Entität diesen offenlegen muss. Es kann sich dabei (je nach Verfahren) um einen gemeinsamen oder um einen privaten Schlüssel aus einem Schlüsselpaar handeln⁶. Die prüfende Instanz sendet eine Anfrage (Challenge) an den Besitzer, die Besitzerin des Schlüssels. Je nach verwendetem Verfahren verschlüsselt nun der Besitzer, die Besitzerin die Nachricht oder erstellt eine digitale Signatur. Die prüfende Instanz kann nun mit

⁵vgl. Abschnitt 2.3.2 auf der vorherigen Seite

⁶vgl. Abschnitt 2.3.2 auf der vorherigen Seite

dem zugehörigen (öffentlichen oder gemeinsamen) Schlüssel die Nachricht entschlüsseln bzw. die Signatur lesen und weiss damit, dass die andere Partei im Besitz des entsprechenden (privaten oder gemeinsamen) Schlüssels ist[23].

2.4 Self-Sovereign Identity

Wie der Name impliziert, steht im Zentrum der SSI die Souveränität persönlicher Identitäten im digitalen Umfeld. Damit kontrastiert SSI mit heute gängigen (zentralistischen oder federierten) Systemen wo in der Regel eine Organisation (z.B. Google, Apple oder Microsoft) Identitäten auf ihren Servern speichert und damit die volle Kontrolle darüber hat. Identitäten dieser Provider können oft für verschiedene Services verwendet werden (z.B. «Login with Google Account»). Das funktioniert aber nur für zugelassene Services. Zudem können Besitzerinnen und Besitzer nicht autonom darüber verfügen – der Provider hat in letzter Instanz die volle Kontrolle[5].

Im SSI-Ökosystem bin ich als Subjekt meiner Identität im Besitz über alle Informationen zu meiner Person und kann autonom darüber verfügen. Informationen sind in speziellen digitalen Zertifikanten enthalten, die nur beim Subjekt gespeichert sind. Die Besitzerin, der Besitzer hat damit (anstelle zentraler Organisationen) die volle Kontrolle darüber, wem sie oder er diese Zertifikate weitergibt. Andere Teilnehmende im SSI-Ökosystem können unter Einsatz kryptografischer Mechanismen die Integrität und Zugehörigkeit der Zertifikate eindeutig verifizieren – ohne auf eine dritte Partei angewiesen zu sein[24]. Diese digitalen Zertifikate werden auch Verifiable Credential (VC) genannt (siehe Abschnitt 2.4.4 auf Seite 14).

2.4.1 Teilnehmer/innen

Es gibt drei teilnehmende Instanzen, die mit dem SSI-Ökosystem interagieren und unterschiedliche Rollen übernehmen — man spricht auch vom Trust Triangle[24].

Aussteller/in Erstellen VCs und stellen sie an einen Besitzer, eine Besitzerin aus. VCs werden durch die Ausstellerin, den Aussteller digital signiert, um später deren Echtheit zu bestätigen. Es handelt sich dabei oft um Unternehmen oder Organisationen wie staatliche Ämter, Universitäten oder andere.

Besitzer/in Speichern digitale Zertifikate in einem SSI-Wallet (siehe Abschnitt 2.4.7 auf Seite 15). Sie können ausgewählte Informationen selbstbestimmt an entsprechende Anwendungen in Form einer Verifiable Presentation (VP) (siehe Abschnitt 2.4.5 auf Seite 14) weitergeben.

Verifizierer/in Nutzen die digitalen Zertifikate für ihre Prozesse und Anwendungen. Dazu fordern sie bei der Besitzerin, dem Besitzer die nötigen Informationen an und verifizieren diese automatisiert auf ihre Gültigkeit, Authentizität, Integrität und Herkunft[24].

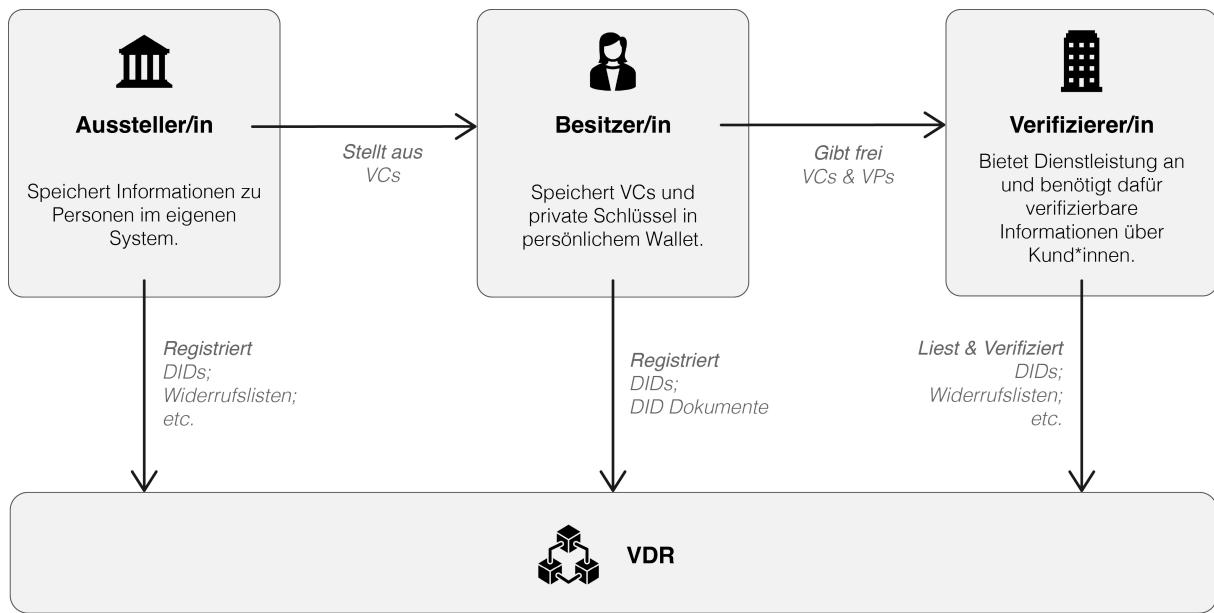


Abbildung 2.5: Überblick SSI-Schema mit teilnehmenden Instanzen und Abläufen

2.4.2 Decentralized Identifier (DID)

DIDs sind durch das World Wide Web Consortium (W3C) definierte, global einzigartige, digitale Kennungen. Sie identifizieren ein DID-Subjekt und referenzieren ein DID-Dokument. DID-Subjekte sind beliebige Entitäten im SSI-Ökosystem (z.B. Personen, Organisationen, Verträge oder Maschinen). DID-Dokumente enthalten Informationen zu den zugehörigen DIDs — darunter auch öffentliche Schlüssel⁷. Eine Entität kann mehrere DIDs erzeugen und so für jeden Service eine separate Kennung verwenden[23][25][26].

UUIDs⁸ und URNs⁹ erfüllen ähnliche Anforderungen. Diese Lösungen sind aber entweder nicht global auflösbar (UUIDs) oder bedingen dazu eine zentrale Instanz (URNs). Würden einzelnen Personen UUIDs oder URNs als Identität zugewiesen, wäre der Besitz einer entsprechenden Adresse (konkrete UUID oder URN) nicht kryptografisch beweisbar. Alle drei Punkte werden durch DIDs gelöst[23].

Drummond Reed misst dem Potenzial von DIDs eine ähnlich grosse Bedeutung für Sicherheit und Schutz bzw. Wahrung der Privatsphäre im digitalen Raum zu, wie der Etablierung des SSL/TLS Standards[23].

Beispiel did:example:123456789abcdefgijk¹⁰

2.4.3 DID-Methoden

Damit DIDs universell (über die Grenzen unterschiedlicher dezentraler Netzwerke hinweg) einsetzbar sind, wird anstelle eines Namespaces wie bei URNs eine sogenannte DID-Methode angegeben. Die Methode muss gemäss W3C-Spezifikation direkt nach dem Schlüsselwort «did» folgen. Die DID-Methode für Ethereum lautet zum Beispiel: «did:ethr:»[23]. In der Abbildung 2.6 auf der nächsten Seite ist die Unterteilung einer DID zu entnehmen.

⁷vgl. Abschnitt 2.3 auf Seite 9

⁸Weitere Informationen zu UUIDs: https://de.wikipedia.org/wiki/Universally_Unique_Identifier

⁹Weitere Informationen zu URNs: https://de.wikipedia.org/wiki/Uniform_Resource_Name

¹⁰vgl. Definition durch W3C: <https://www.w3.org/TR/did-core/>

DID-Methoden bzw. deren Spezifikation definieren, wie die entsprechende Methode funktioniert. Dazu gehört[23]:

- Wie werden neue DIDs erzeugt?
- Wie werden bestehende DIDs aufgelöst?
- Wie wird das zur DID gehörende DID-Dokument abgerufen?

Die definierten Spezifikationen werden für die Implementierung eines Resolvers bzw. Registrars verwendet. Ein Resolver löst das DID-Dokument zu einer DID auf. Ein Registrar ist für die Erstellung einer DID bzw. der Verankerung des entsprechenden DID-Dokuments auf dem Verifiable Data Registry (VDR) verantwortlich.

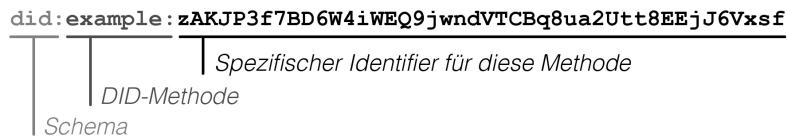


Abbildung 2.6: Beispiel einer DID, unterteilt in Schema, Methode und Identifier.

2.4.4 Verifiable Credential (VC)

Verifiable Credentials beinhalten Informationen über ein Subjekt. Sie können z.B. Zeugnisse, Bestätigungen von Behörden, Ausweise oder Mitgliedschaften ausweisen. Im Vergleich zu physischen Ausweisen haben sie den Vorteil, dass ihre Gültigkeit jederzeit digital verifizierbar ist. Es gibt unterschiedliche Datenstrukturen, im Wesentlichen sind nachfolgende Komponenten¹¹[27] enthalten.

- Subjekt – *Auf wen (welche DID) beziehen sich die Informationen.*
- Claims – *Behauptungen über ein oder mehrere Subjekte z.B. «Hat Hochschulabschluss».*
- Meta-Informationen – *z.B. Ausstellerin, Aussteller oder Datum der Ausstellung.*
- Proofs – *Digitale Signatur zur Wahrung bzw. Verifizierbarkeit der Datenintegrität.*

2.4.5 Verifiable Presentation (VP)

Je nach Anwendungsfall sind nicht alle Informationen aus einem VC nötig. Oder es sind Informationen aus unterschiedlichen VCs nötig. Verifiable Presentations enthalten Informationen aus einem oder mehreren VCs. Im Sinne der Datensparsamkeit enthalten VPs nur die für den spezifischen Anwendungsfall nötigen Informationen aus dem/den VCs. Die Besitzerin, der Besitzer kann entscheiden, welche Informationen in der VP geteilt werden¹²[27].

Siehe dazu auch Abschnitt 2.4.9 auf der nächsten Seite

2.4.6 Certificate Authority (CA) und Trusted List (TL)

Certificate Authorities (CAs) sind Entitäten, die von den Teilnehmerinnen und Teilnehmern¹³ anerkannte Identitätszertifikate ausstellen. CAs werden von einer vertrauenswürdigen Stelle, wie dem Staat, in einer sogenannten Trusted List (TL) aufgeführt. In einer weiteren TL werden alle

¹¹vgl. Definition durch W3C: <https://www.w3.org/TR/vc-data-model/>

¹²vgl. Definition durch W3C: <https://www.w3.org/TR/vc-data-model/>

¹³vgl. Abschnitt 2.4.1 auf Seite 12

von den CAs ausgestellten Zertifikate und deren Status festgehalten. So kann geprüft werden, ob eine Ausstellerin, ein Aussteller von einer CA zertifiziert wurde¹⁴ [9, S. 83].

2.4.7 Digitales Wallet

Das virtuelle Portemonnaie bietet Besitzerinnen und Besitzern einen privaten Aufbewahrungs-ort für digitale Elemente. Ein Digital Wallet wird oft für den elektronischen Zahlungsverkehr verwendet. Im Umfeld von SSI wird ein Wallet für das Speichern, Verwalten und Präsentieren von Schlüsseln und digitalen Zertifikaten verwendet — man spricht auch von einem SSI-Wallet. Oft handelt es sich um mobile Wallets — also um eine App auf dem Smartphone. Es gibt weitere Arten von Wallets, die auf Computern, in der Cloud oder auf anderen Medien gespeichert werden[9].

2.4.8 Verifiable Data Registry (VDR)

Im Wesentlichen dient das VDR als Anker für die DPKI-Infrastruktur. Via VDR werden DID-Dokumente und die darin enthaltenen öffentlichen Schlüssel zugänglich gemacht. Zudem kann das VDR als Register für folgende Daten verwendet werden[9, p. 84]:

- DID-Dokumente (u.A. mit öffentlichen Schlüsseln)
- Schemas für VCs
- Trusted Lists¹⁵
- DNS¹⁶
- Revocation Registries

Werden neben den öffentlichen Schlüssel / DID-Dokumenten noch andere Informationen auf dem VDR gespeichert, geht dessen Anwendungsfall über die Definition einer DPKI hinaus.

Die VCs, die personenbezogene Daten enthalten können, werden nicht auf dem VDR gespeichert. VCs sind nur bei der Besitzerin, dem Besitzer gespeichert. Allerdings kann deren Integrität (bzw. der Besitz des privaten Schlüssels der entsprechenden DID) anhand von Informationen (öffentlicher Schlüssel) auf dem VDR bestätigt werden. In einer «Widerrufsliste» können in der Vergangenheit ausgestellte VCs als «Widerrufen» markiert werden — z.B. weil einer Autofahrerin, einem Autofahrer als Strafe der Führerschein entzogen wird. Wegen ihrer zentralen Rolle müssen VDR-Lösungen hohen Ansprüchen hinsichtlich Manipulierbarkeit, Transparenz, und Ausfallsicherheit gerecht werden. Die Blockchain bietet sich deshalb als Lösung an[24].

2.4.9 Zero-Knowledge-Proofs

Grob vereinfacht ermöglichen Zero Knowledge Proofs (ZKP) mittels kryptografischen Funktionen etwas zu beweisen, ohne die dazu verwendeten Informationen preiszugeben. Dies ermöglicht im Kontext von SSI einen datenschutzkonformen (und damit minimalen) Austausch von digitalen Zertifikaten[24]. Verwendet werden kryptografische Funktionen wie Predicate Proofs und Selective Disclosure¹⁷.

¹⁴Siehe auch Kapitel 7.6 «Certificate Authorities (CAs) and Trusted Lists (TLs)» im Buch von Marcos Allende López[9]

¹⁵Beispiel: Liste der CAs

¹⁶DNS wird verwendet um z.B. die Hierarchie von CAs bis zum Wurzel-Zertifikat zu folgen

¹⁷Detailliertere Beschreibung und weitere kryptografische Funktionen zu finden in [24]

2.4.10 Predicate Proofs

Ermöglicht die Prüfung eines Wertes gegen eine Bedingung, die wahr oder falsch sein kann. Beispielsweise kann kalkuliert werden, ob der Wert kleiner, grösser oder gleich gross wie ein bestimmter Wert ist.

Beispiel: Beim Kauf eines alkoholischen Getränks kann die Volljährigkeit (Alter ≥ 18) bewiesen werden ohne dabei das Alter, den Namen oder andere persönliche Daten zu zeigen, wie das bei der Identitätskarte der Fall ist.

2.4.11 Selective Disclosure

Jeder Claim in einem VC wird von der Ausstellerin, dem Aussteller einzeln signiert. Dies ermöglicht die Weitergabe einer Teilmenge an Claims in einer VP, die sich aus einer oder mehreren VCs zusammensetzt.

Beispiel: Beim Anmelden für einen Kurs werden selektiv Name und Geburtsdatum geteilt, ohne weitere Informationen wie Nationalität oder Körpergrösse preiszugeben.

2.4.12 Prinzipien

Mit den eingeführten Komponenten von SSI ergeben sich Prinzipien, die ein SSI-Ökosystem auszeichnen. Es gibt unterschiedliche Übersichten. Häufig zitiert werden die zehn SSI-Prinzipien von Christopher Allen[5]:

1. **Existenz** – Nutzer/innen müssen eine unabhängige Existenz haben.
2. **Kontrolle** – Nutzer/innen müssen ihre Identitäten kontrollieren.
3. **Zugang** – Nutzer/innen müssen Zugang zu ihren eigenen Daten haben.
4. **Transparenz** – Systeme und Algorithmen müssen transparent sein.
5. **Persistenz** – Identitäten müssen langlebig sein.
6. **Portabilität** – Informationen und Dienste zur Identität müssen portabel sein (z.B. bei einem Umzug).
7. **Interoperabilität** – Identitäten sollten so weit wie möglich (für unterschiedliche Applikationen/Services/Anwendungsfälle) nutzbar sein.
8. **Einverständnis** – Nutzer/innen müssen der Verwendung ihrer Identität zustimmen.
9. **Minimale Offenlegung** – Offenlegung von Informationen muss auf ein Mindestmass beschränkt werden.
10. **Sicherheit** – Rechte der Nutzer/innen müssen geschützt werden.

2.5 Aktuelle Anwendungen

Self-Sovereign Identity wird bereits an diversen Orten eingesetzt oder erprobt. Dieses Kapitel beschreibt einige der aktuellen Anwendungen und analysiert sie bezüglich der verwendeten VDR-Technologie.

2.5.1 IDunion

Das Konsortium «IDunion», bestehend aus privaten und öffentlichen europäischen Institutionen, hat zum Ziel, ein offenes Ökosystem für dezentrale, selbstbestimmte Identitäten zu schaffen. Gefördert durch das Deutsche Bundesministerium für Wirtschaft und Klimaschutz (BMWK) wird eine SSI-Infrastruktur aufgebaut und verschiedene Anwendungsfälle¹⁸ wie digitale Studierendausweise oder online Bestellvorgänge erprobt[28].

Das IDunion Netzwerk baut auf dem Trust over IP (ToIP)¹⁹ Modell auf und verwendet internationale Standards wie die VC- und DID-Definitionen von W3C. Als VDR wird ein DLT-Netzwerk verwendet, das auf dem Open Source-Framework Hyperledger Indy aufbaut. Hyperledger Indy ist die Grundlage für eine Public Permissioned Blockchain und wurde speziell für digitale Identitäten konzipiert[29][28].

2.5.2 Estland

Seit 1994 setzen die estnischen Behörden 1% des BIP zweckgebunden für den Aufbau eines digitalen Staates (e-Estonia) ein. Heute bietet Estland umfassende Services²⁰ für die Interaktion zwischen Behörden, privaten Institutionen und Bürgern an. Beispiele sind: e-Voting, e-Health, e-Police, e-Banking, e-Tax[30].

Als Basis für die Identifikation im digitalen Raum dient die staatliche Identitätskarte mit Chip oder das Smartphone. Auf dem Chip der Identitätskarte, der SIM-Karte oder direkt auf dem Smartphone wird die eindeutige Identifikationsnummer und ein privater Schlüssel der Bürgerin, des Bürgers gespeichert[31].

Verschiedene estnische Behörden setzten für die Verarbeitung von Daten der Bevölkerung auf die Keyless Signature Infrastructure (KSI) von Guardtime²¹. Diese Blockchain-ähnlichen Lösungen der verschiedenen Behörden werden mit der Open Source Software-Lösung «X-Road»²² verbunden. So entsteht ein P2P-Ökosystem für den Austausch von Informationen. Das von Estland aufgebaute Konstrukt ermöglicht digitale Prozesse zwischen Behörden, Bevölkerung und Privaten, die den Prinzipien von SSI sehr nahe kommen[32].

Es gibt unterschiedliche Positionen darüber, ob Estland tatsächlich Blockchain-Technologie einsetzt oder nicht. In ihrem Paper «Blockchain-based application at a governmental level: disruption or illusion? The case of Estonia» analysieren Silvia Semenzin, David Rozas und Samer Hassan unter anderem Ansichten und Einschätzungen unterschiedlicher (teils anonymer) Akteure. Klar ist: Wenn Blockchain-Technologien zum Einsatz kommen, dann nur Private Permissioned Blockchains[33].

¹⁸ Beschreibung und weitere Anwendungsfälle der IDunion unter https://www.digitale-technologien.de/DT/Redaktion/DE/Standardartikel/sdi_use_case_2

¹⁹ Mehr zum ToIP-Modell unter <https://trustoverip.org/>

²⁰ Liste mit Beispielen unter <https://e-estonia.com/solutions/>

²¹ Weitere Informationen zur KSI-Lösung und Ämtern, die die Lösung verwenden unter https://e-estonia.com/wp-content/uploads/2019sept_faq-ksi-blockchain-1-1.pdf

²² Weitere Informationen zu X-Road unter <https://e-estonia.com/wp-content/uploads/2020mar-facts-a4-v02-x-road.pdf>

2.5.3 Blockcerts Caribe

Mit dem Ziel die Digitalisierung und das Ausstellen und Verifizieren von akademischen Zertifikaten in karibischen Ländern voranzutreiben, wurde Blockcerts Caribe ins Leben gerufen[34]. Die SSI-Lösung basiert auf der LACChain – eine Public Permissioned Blockchain. Die LACChain Allianz wird durch Private (und nicht durch Behörden) geführt. Die Infrastruktur steht sowohl privaten wie auch öffentlichen Entitäten offen. LACChain ist die führende Blockchain-Initiative im lateinamerikanischen und karibischen Raum[35].

Neben der Sicherstellung eines funktionierenden Systems steht auch die regulatorische Konformität im Fokus. So sind spezifische «Validator»-Knoten für den Konsensus und die Generation von neuen Blöcken zuständig. Diese Knoten interagieren mit «Boot»-Knoten in verschiedenen regionalen Subnetzwerken, die dann wiederum mit «Writer»-Knoten interagieren. Nur die «Writer»-Knoten in den regionalen Netzwerken erstellen Transaktionen. Die «Writer»-Knoten sind für die Einhaltung gesetzlicher Vorgaben in ihrer Region zuständig[36, p. 25].

Das LACChain-Framework definiert Prinzipien für die Orchestrierung, den Betrieb und die Steuerung (Governance) des Netzwerks von Netzwerken[36, p. 13]. Auf der technologischen Ebene definiert das Framework verschiedene Komponenten wie die Netzwerk-Topologie, den Konsensusmechanismus²³ oder die Etablierung privater Kanäle[36, p. 23].

2.5.4 SSI+ (Procivis)

Die 2016 in Zürich gegründete Procivis AG erarbeitet technologische Lösungen für die Digitalisierung von Schweizer Behörden. Inspiriert durch die Digitalisierung der estnischen Behörden (e-Estonia) will die Firma laut Website «die Erfolgsfaktoren des estnischen Modells mit modernster Technologie und den einzigartigen demokratischen Werten der Schweiz vereinen»[37].

Das Kernprodukt eID+ wird bereits von den Schweizer Kantonen Schaffhausen und Zug für das Erstellen einer digitalen Identität für die Bevölkerung, digitales Signieren von Dokumenten und weiteren Interaktionen²⁴ zwischen Behörden und Bevölkerung verwendet. eID+ basiert nicht auf SSI[38].

Auf dem Know-How von eID+ aufbauend hat Procivis 2021 einen SSI-Prototypen für den Staat Luxemburg umgesetzt. Anfang 2022 lancierte das Unternehmen mit SSI+ eine SSI-Lösung für ein Ökosystem mit Komponenten für Aussteller/in, Besitzer/in und Verifizierer/in. SSI+ setzt auf die Standards von W3C²⁵ und verwendet Hyperledger Indy²⁶ als Blockchain-Lösung für das VDR. Für die Kommunikation zwischen verschiedenen Agents setzt SSI+ auf Protokolle von Hyperledger Aries²⁷. Das eigene Wallet wurde als Smartphone-App umgesetzt[39]. Procivis weist auf ihrer Website (<https://procivis.ch>) aktuell keine operativen SSI+ Projekte aus.

2.5.5 OrgBook BC

OrgBook BC ist ein öffentliches Verzeichnis der Regierung von Britisch-Kolumbien (Provinz in Kanada) mit verifizierbaren Daten zu Unternehmen. Auf Basis von SSI und dem W3C-Standard werden Daten²⁸ wie Adressen und Registrierungen aber beispielsweise auch Lizenzen zum Kabinettverkauf geführt. OrgBook BC läuft auf der Sovrin-Plattform, einer Public Permissioned Blockchain auf Basis von Hyperledger Indy[40].

²³LACChain verwendet Practical Byzantine Fault Tolerance als Konsensusmechanismus[36, p. 27].

²⁴Weitere Services und Anwendungsfälle unter: <https://www.procivis.ch/eid>

²⁵vgl. Abschnitt 2.4.4 und Abschnitt 2.4.5 auf Seite 14

²⁶Weitere Informationen zu Hyperledger Indy unter <https://www.hyperledger.org/use/hyperledger-indy>

²⁷Weitere Informationen zu Hyperledger Aries unter <https://www.hyperledger.org/use/aries>

²⁸Auflistung aller VC-Typen von «OrgBook BC» unter <https://orgbook.gov.bc.ca/about/orgbook-data>

2.5.6 Findy

Findy ist ein dezentrales Netzwerk zum Teilen digital verifizierbarer Daten, das von der Findy Kooperative betrieben wird. Die Kooperative wurde 2018 gegründet um eine «ethische, wirtschaftliche und sozial-nachhaltige Daten-Ökonomie» für Finnland und interessierte (internationale) Partner zu schaffen[41].

Die Kooperative bezeichnet sich selber als gemeinnützige Organisation. Jede private oder öffentliche Entität darf beitreten. Sie finanziert sich durch Beiträge der Mitgliedschaft sowie Nutzungsgebühren. Ein Gremium aus sieben Personen leitet die Kooperative. Sowohl öffentliche wie private Institutionen - darunter die finnische Post, Steuerbehörde, Krankenkassen und Banken²⁹[42] sind Teil der Mitgliedschaft. Zugehörige Institutionen betreiben einen verifizierten Knoten in der Blockchain[43].

Das Findy-Netzwerk strebt für 2022 einen Prototypen und für 2023 eine breite Implementierung in Finnland an. Findy nutzt Hyperledger Indy und setzt auf Standards der W3C, ISO und DIF[43][41].

2.5.7 Kiva

Das Kiva-Protokoll ist ein Open-Source-System zur Ausstellung und Verifikation digitaler Credentials und Identitäten. Es wurde von der Kiva Organisation entwickelt. Ziel der Lösung ist es, auf Basis von SSI Bürgerinnen und Bürgern ohne überprüfbare Bonität sogenannte Mikrofinanzierung³⁰ zu ermöglichen[44][45].

Das Kiva-Protokoll ist insbesondere für wirtschaftlich schwache Länder mit einer hohen Quote an Personen ohne reguläre Bankkonten relevant. Die erste nationale Anwendung fand das Kiva Protokoll 2019 in Sierra Leone[46]. Teilnehmende am dezentralen Netzwerk für das SSI-Ökosystem sind die Nationalbank, der Staat, die Kiva Organisation und Entitäten für Mikrofinanzierungen. Sie alle betreiben Knoten im Netzwerk. Neue Entitäten müssen einen Antrag zur Teilnahme stellen[47].

Eine Besonderheit im SSI-Konstrukt des Kiva-Protokolls: In Sierra Leone verfügt nicht die gesamte Bevölkerung über ein eigenes Smartphone um die privaten Schlüssel zu speichern. Deshalb speichert die Kiva-Cloud in diesen Fällen die privaten Schlüssel für die entsprechenden Personen. Diese können sich in Banken mittels biometrischer Identifikation (z.B. Fingerabdruck) am Kiva-Server anmelden und so den privaten Schlüssel beziehen[47].

Das Kiva-Protokoll basiert auf den Standards der W3C und nutzt Teile von Hyperledger Indy als Basis für das VDR. Aktuelle Implementierungen sind als Private Permissioned Blockchain konzipiert[47].

2.5.8 Building Blocks

Building Blocks ist ein dezentrales Netzwerk zur Identifikation von Geflüchteten. In Lagern von Geflüchteten haben die die Betroffenen mit vielen Organisationen/Parteien zu tun. Building Blocks soll es den Geflüchteten ermöglichen, sich mit einer digitalen Identität bei verschiedenen NGO's, dem UNHCR³¹ und anderen Entitäten (z.B. Lebensmittelläden) auszuweisen und Einkäufe zu tätigen[48].

²⁹Vollständige Liste unter <https://findy.fi/en/>

³⁰Bezeichnet die Vergabe kleiner Kredite an Parteien, die keinen Zugang zu regulären Bankdienstleistungen haben. Weitere Informationen unter <https://www.kiva.global/kiva-org/>

³¹Abkürzung für United Nations High Commissioner for Refugees – Weitere Informationen: <https://www.unhcr.org/dach/ch-de/ueber-uns>

Das Projekt wurde 2017 vom World Food Programme (WFP) des UNHCR gestartet und wird heute operativ in Bangladesch und Jordanien eingesetzt. Nach einem Pilotprojekt auf dem Hauptnetz von Ethereum (Public Permissionless Blockchain) hat Building Blocks für die operative Implementierung ein eigenes privates Netz mit dem Parity Client³² aufgebaut. Als Grund für den Wechsel auf eine Private Blockchain werden Transaktionsgebühren und der tiefere Durchsatz von Public Blockchains aufgrund des vorherrschenden PoW Konsensusmechanismus angegeben. Building Block setzt auf einen Proof of Authority Konsensusmechanismus[47].

Wie bei Kiva³³ gibt es auch bei Building Block eine Besonderheit: Auch hier können die Besitzerinnen und Besitzer der Identitäten (Geflüchtete) mangels nötiger Infrastruktur den privaten Schlüssel oft nicht selber speichern. Das WFP speichert die privaten Schlüssel – außer die geflüchtete Person kann den Schlüssel selber speichern. Speichert das WFP den Schlüssel, so kann dieser mittels biometrischer Identifikation (Iris-Scan) abgerufen werden[47].

2.5.9 truu

Truu stellt «digitale Pässe» für Mitarbeitende des Gesundheitssektors aus. Ziel ist es, administrative Arbeiten zu vereinfachen: Medizinisches Fachpersonal soll mit Verifiable Credentials einfach belegen können, dass Ausbildungen, Zulassungen, Impfungen und mehr vorliegen[49].

Truu wird vom European Self-Sovereign Identity Framework-Lab (eSSIF-Lab) unterstützt und mitfinanziert. eSSIF-Lab ist eine von der Europäischen Kommission gegründete und durch Horizon Europe finanzierte Initiative. Sie hat zum Ziel, ein europäisches Netzwerk und Framework für SSI-Projekte aufzubauen. Die Initiative finanziert Projekte mit Fokus auf technologische Weiterentwicklung des SSI-Frameworks, aber auch konkrete Implementierungen verschiedener Anwendungsfälle[50].

Truu arbeitet mit nationalen britischen Akteuren wie dem National Health Service (NHS) und der nationalen Post zusammen. Als VDR wird Hyperledger Indy (Sovrin) eingesetzt[49].

2.5.10 BCdiploma

BCdiploma stellt einen Service zur Verfügung, der das Ausstellen und Verifizieren von Diplomen nach SSI-Prinzipien ermöglicht. Laut eigener Website arbeiten bereits über 100 Universitäten mit dem System – oder haben zumindest Interesse bekundet[51].

BCdiploma wird (wie truu) vom eSSIF-Lab unterstützt³⁴ und nutzt die European Blockchain Services Infrastructure (EBSI). EBSI ist eine Public Permissioned Blockchain, die durch die Europäische Kommission finanziert wird[52]. Neben den EU-Staaten gehören auch Finnland und Liechtenstein zur EBSI-Initiative und betreiben Knoten. EBSI verwendet verschiedene technologische Bausteine unterschiedlicher Anbieter bzw. Blockchains. In der Version 2.1 werden zwei Blockchain-Protokolle verwendet; Hyperledger Besu (Ethereum Client) sowie Hyperledger Fabric. Der Besu-Ledger verwendet Proof of Authority und der Fabric-Ledger Raft³⁵ als Konsensusmechanismus[53][54][55].

³²Weitere Informationen zu Parity: <https://www.parity.io>

³³vgl. Abschnitt 2.5.7 auf der vorherigen Seite

³⁴vgl. Abschnitt 2.5.9

³⁵Weitere Informationen zu Raft: <https://raft.github.io>

2.5.11 Übersicht

Tabelle 2.1 fasst die vorgestellten Initiativen zusammen und vergleicht eingesetzte Technologien. Nicht öffentlich einsehbare Daten sind mit einem Bindestrich gekennzeichnet.

Projekt	VDR	Technologie	Konsensus	Im Einsatz seit
IDunion	Public Permissoned Blockchain	Hyperledger Indy	RBFT ³⁶	2021 ³⁷
OrgBook BC	Public Permissoned Blockchain	Sovrin (Hyperledger Indy)	RBFT ³⁶	2019
Estland	Private Permissioned Blockchain ³⁸	KSI Blockchain ³⁹	-	Unklar
Blockcerts Caribe	Public Permissioned Blockchain	LACChain (Hyperledger Besu ³⁹)	PBFT ⁴⁰	Unklar
SSI+ (Procivis)	Public Permissoned Blockchain	Hyperledger Indy	-	Noch nicht im Einsatz
Findy	Public Permissioned Blockchain ⁴¹	Hyperledger Indy	RBFT ³⁶	Ab 2023
Kiva	Private Permissioned Blockchain	Hyperledger Indy	RBFT ³⁶	2019
Building Blocks	Private Permissioned Blockchain	Parity Ethereum ⁴²	PoA ⁴³	2017
truu	Public Permissioned Blockchain	Sovrin (Hyperledger Indy)	RBFT ³⁶	Unklar
BCdiploma	Public Permissioned Blockchain	EBSI (EU-Entwicklung)	PoA ⁴³	Noch nicht im Einsatz

Tabelle 2.1: Übersicht ausgewählter SSI-Projekte und eingesetzte Technologien

³⁶Redundant Byzantine Fault Tolerance <https://lig-membres.imag.fr/aublin/rbft/report.pdf>

³⁷Gemäss Roadmap «Start 2021», aktueller Stand unbekannt – vgl. <https://idunion.org/projekt/>

³⁸Ob Blockchain-Techologien zum Einsatz kommen werden, wird kontrovers diskutiert – vgl. Abschnitt 2.5.2 auf Seite 17

³⁹Weitere Informationen zu Hyperledger Besu: <https://www.hyperledger.org/use/besu>

⁴⁰Practical Byzantine Fault-Tolerant (PoA)

⁴¹Fokus auf Region Latein-Amerika und Karibik

⁴²Weitere Informationen: <https://www.parity.io/technologies/ethereum/>

⁴³Proof of Authority – vgl. Abschnitt 2.2.2 auf Seite 7

2.5.12 Fazit

Es gibt in allen Regionen der Welt und in verschiedenen Branchen Initiativen zu SSI. Die Initiativen arbeiten auf die Schaffung von Grundlagen für die Etablierung von SSI-Ökosystemen hin. Gleichzeitig arbeiten Behörden an der Schaffung regulatorischer Grundlagen (z.B. DSGVO oder eIDAS in Europa).

Die technologischen Lösungen (Open-Source wie auch lizenziert) gibt es bereits, sind aber noch nicht breit adaptiert. Weit fortgeschrittene technologische Frameworks sind IDUnion, eSSIF und LACChain. Zwei erfolgsversprechende Anwendungen zeigen zudem das Potential für sozioökonomisch tiefere Schichten und Menschen in Not (Kiva und Building Blocks). Tabelle 2.1 auf der vorherigen Seite ist zu entnehmen, dass ein Grossteil der vorgestellten Anwendungen auf Public Permissioned Blockchains als Lösung für das VDR setzen. Aufgrund der geografischen, kulturellen und regulatorischen Nähe besonders erwähnenswert ist der Aufbau einer europäischen Blockchain mit Knoten in allen EU-Staaten (EBSI) – explizit auch für SSI.

Kein Land und keine Region kennt bis heute den breiten Einsatz eines SSI-Ökosystems, das allen Prinzipien⁴⁴ von SSI gerecht wird. Durch die fortschreitende Etablierung regulatorischer und technologischer Grundlagen dürfte ein solcher Schritt zeitnah möglich sein.

⁴⁴vgl. Abschnitt 2.4.12 auf Seite 16

2.6 Szenarien

Um Anforderungen an die Netzwerkarchitektur des VDR zu eruieren, wurden diverse Szenarien definiert. Aufgrund der Definition kann im Anschluss verglichen werden, wie sich unterschiedliche Lösungen in den verschiedenen Szenarien verhalten würden. Im Optimalfall hält eine Lösung allen Szenarien stand. Als Grundlage dient die nationale Risikoanalyse[56] von Katastrophen und Notlagen des Bundesamt für Bevölkerungsschutz (BABS) und der Austausch mit dem VBS.

2.6.1 Naturgefahren

Naturgefahren wie Hochwasser, Sturm und Erdbeben, die je nach Ausmass Infrastrukturen regional oder national gefährden. Die nationale Risikoanalyse sieht bei Naturgefahren vor allem in der Häufigkeit ein Risiko.

Überschwemmung Nach mehreren Tagen mit heftigem Regenfall bricht ein Flussdamm und führt zu starken Überschwemmungen. Das Hochwasser verursacht schwere Schäden in der Region und beschädigt kritische Infrastrukturen, die nicht mehr erreichbar sind.

Erdbeben Ein starkes Erdbeben erschüttert die Schweiz. Im näheren Umkreis des Epizentrum wird ein Grossteil der Infrastruktur stark beschädigt. Im Umkreis von 150km werden diverse Schäden gemeldet. Mehrere Regionen sind vom Netz abgeschnitten oder komplett zerstört.

2.6.2 Stromausfall

Ausfall der Versorgung elektrischer Energie für einzelne Gebäude oder Regionen. Dabei wird zwischen einem Stromausfall und einem Blackout unterschieden:

Stromausfall Auf der Baustelle einer Tiefgarage wurde versehentlich ein wichtiges Stromkabel durchtrennt, welches ein grosses Stadtgebiet mit Strom versorgt hat. Alle Gebäude in der Region sind über mehrere Tage ohne Strom.

Blackout Ein Systemfehler in einem Stromkraftwerk führt zu einer Überlastung des Schweizer Stromnetzes. In Kombination mit einer knappen Gaslieferung bricht die Energieversorgung in der Schweiz zusammen. Es kommt zum Blackout und die Schweiz hat über mehrere Tage keinen Strom.

2.6.3 Cyber-Angriff

Angriff auf IT-Systeme um beispielsweise vertrauliche Daten zu stehlen oder die Funktionsweise der Systeme zu stören.

DDoS Eine anonyme Gruppierung ist mit der staatlichen E-ID der Schweiz nicht einverstanden. Sie startet einen DDoS-Angriff auf kritische Infrastruktur.

Infiltration Eine Angreiferin, ein Angreifer verschafft sich über eine Sicherheitslücke im Netzwerk Zugriff auf einen Server kritischer Infrastruktur.

2.6.4 Bewaffneter Konflikt

Ein bewaffneter Konflikt gegen feindliche Gruppierungen oder Staaten. Der militärische Konflikt zwischen der Ukraine und Russland zeigt, dass sich auch in Europa ein Krieg nicht ausschliessen lässt.

Krieg Ein grossräumiger Krieg tobt in der Peripherie Europas und zieht auch die Schweiz in kriegerische Handlungen ein. Feindliche Truppen sabotieren kritische Infrastrukturen und führen Raketenangriffe auf diverse Ziele aus.

Besetzung Nach einem bewaffneten Konflikt wird die Schweiz besetzt. Die Regierung operiert auch weiterhin aus dem Exil im Ausland und versucht den Staat funktionsfähig zu halten.

2.6.5 Terrorismus

Terroranschläge von nicht-militärischer Täterschaft, die sich gezielt oder zufällig gegen Personen oder Infrastruktur richtet.

Bombenanschlag Eine Terrororganisation verübt einen Bombenanschlag auf eine kritische Infrastruktur. Die Explosion beschädigt das Gebäude stark. Der Wiederaufbau wird mehrere Monate dauern.

2.6.6 Übersicht

Tabelle 2.2 zeigt Auswirkungen und Plausibilitäten der definierten Szenarien. Die Auswirkung bezieht sich auf Beeinträchtigungen der Infrastruktur in geografischen Regionen. Die Plausibilitätsklassen⁴⁵ basieren auf der nationalen Risikoanalyse[56].

Szenario	Auswirkung	Plausibilität
Stromausfall	Regional	plausibel
Überschwemmung	Regional	ziemlich plausibel
Cyber-Angriff	International	teilweise plausibel
Bombenanschlag	Regional	teilweise plausibel
Erdbeben	National	wenig plausibel
Blackout	National	wenig plausibel
Besetzung	National	- ⁴⁶
Krieg	International	- ⁴⁶

Tabelle 2.2: Übersicht möglicher Szenarien von denen die Schweiz gemäss Risikalanalyse des BABS betroffen sein könnte. Von den definierten Szenarien sind jene plausibler, die geografisch eine kleinere Auswirkung haben. Nationale und transnationale Szenarien sind zwar wenig plausibel, können jedoch nicht ausgeschlossen werden. Detaillierte Informationen zu den Plausibilitätsklassen sind im Bericht des BABS zu finden[56] — Auszug davon in Anhang A.3

⁴⁵Detaillierte Informationen zu den Plausibilitätsklassen sind in Anhang A.3 zu finden.

⁴⁶Auf die Plausibilitätsschätzung der Szenarien eines bewaffneten Konfliktes wurde wie bei der nationalen Risikoanalyse[56] verzichtet.

2.7 Anforderungen an VDR

Aus den im Abschnitt 2.4 vorgestellten Komponenten und den im Abschnitt 2.6 erläuterten Szenarien ergeben sich Anforderungen an ein VDR für das VBS. Als Grundlage dienen die im Abschnitt 2.4.12 vorgestellten SSI-Prinzipien.

2.7.1 Anforderungen aus SSI-Architektur

2.7.1.1 Dezentralität

Das Kernziel von SSI ist es, den Menschen auch im digitalen Raum die volle Souveränität über ihre Identität zu geben. Per Definition soll damit die Abhängigkeit von zentralen Instanzen auf ein Minimum reduziert werden. Die Identitäten liegen dezentral bei den jeweiligen Subjekten. Auch für das Bereitstellen kryptografischer Beweise sollte auf zentrale Lösungen verzichtet werden. Sie wirken sich negativ auf Zugänglichkeit, Skalierbarkeit und Angreifbarkeit aus. Zentrale Lösungen stehen im Widerspruch zu den Grundfesten von SSI.

Das «Diskussionspapier zum Zielbild E-ID» des Bundesamt für Justiz (BJ) referenziert sechs Motionen die vom Parlament zur E-ID eingereicht wurden. Sie alle fordern «Dezentrale Datenspeicherung» als wichtigen Punkt der zukünftigen E-ID[57].

Das Prinzip der Dezentralität kann unterschiedlich ausgelegt werden:

- A: Dezentralität ist bereits durch Verteilung der Zertifikate auf die Wallets der Bevölkerung gegeben.
- B: Dezentralität muss im Aufbau des ganzen Systems berücksichtigt werden (auch im VDR).

Hinweis

Wir interpretieren Dezentralität als Prinzip, das für alle Komponenten von SSI (also auch für das VDR) gelten soll. Siehe dazu [9, p. 36]

2.7.1.2 Zugänglichkeit, Portabilität und Interoperabilität

Um die Funktionsweise des SSI-Systems zu gewährleisten, müssen unterschiedliche Akteure zuverlässig und einfach Zugang zu Daten im VDR⁴⁷ haben. Entitäten müssen zudem die Möglichkeit haben, neue DIDs auf dem VDR zu registrieren. Eine offene und zugängliche Architektur des VDR ist nötig, um eine möglichst hohe Portabilität⁴⁸ und Interoperabilität⁴⁹ gewährleisten zu können. Von einer DID ausgehend muss mit einem entsprechenden Resolver⁵⁰ eindeutig das zugehörige DID-Dokument abgefragt werden.

2.7.1.3 Persistenz

Die digitale Identität eines Subjekts muss über die Zeit bestehen bleiben. Namentlich darf die Identität nicht gelöscht (z.B. durch staatliche Willkür), verändert oder nachträglich mit einem früheren Zeitstempel erstellt werden können. Eine Person verändert ihr Wesen über die Zeit – es handelt sich aber immer noch um dieselbe Person. Einträge im VDR müssen unveränderbar,

⁴⁷z.B. Referenzen oder vertrauenswürdige Listen – vgl. Abschnitt 2.4.8 auf Seite 15

⁴⁸Für die Portabilität spielt insbesondere auch das Zusammenspiel zwischen VC, VDR und Wallet eine Rolle

⁴⁹Interoperabilität zwischen verschiedenen Behörden, Ämter oder privaten Unternehmen

⁵⁰vgl. Abschnitt 2.4.3 auf Seite 13

rückverfolgbar und deren Integrität jederzeit verifizierbar sein. Persistenz bezieht sich in diesem Kontext auf die Identität – nicht auf ihr zugehörigen Behauptungen⁵¹.

2.7.2 Anforderungen aus Szenarien

2.7.2.1 Ausfallsicherheit

Im Falle eines Ereignisses, das zu einem regionalen Ausfall kritischer Infrastruktur führt⁵², muss die VDR-Infrastruktur nahtlos weiter betrieben werden können. Das VDR muss für alle Akteure erreichbar bleiben. Das Amerikanische Krisenmanagement Amt «US Federal Emergency Management Agency (FEMA)» nutzt seit 2019 DLT-Technologie um in Krisensituationen Identitäten von Betroffenen eindeutig und rückverfolgbar zuordnen zu können⁵³[58]. Das setzt voraus, dass die zugrundeliegende Infrastruktur erreichbar ist.

Dasselbe gilt auch für den Versuch, das System durch einen Cyber-Angriff⁵⁴ (z.B. DDoS-Attacke) stillzulegen.

2.7.2.2 Unstoppbarkeit

Neben einer approximativ vollständigen Ausfallsicherheit muss die VDR-Architektur verhindern, dass einzelne (oder Gruppen von) Entitäten das VDR unzugänglich⁵⁵ machen können.

2.7.2.3 Zensurresistenz

Keinem Akteur darf es möglich sein, Einträge im VDR aus Partikularinteressen (z.B. behördliche Willkür) zu verhindern.

2.7.2.4 Transnationalität

Zur Sicherstellung der Handlungsfähigkeit der Schweiz als souveräner Staat im Falle eines nationalen GAUs oder der Einnahme von Schweizer Staatsgebiet durch eine feindliche Partei⁵⁶ kann die VDR-Architektur transnational abgestützt werden. Konkret heisst das: Selbst bei feindlicher Einnahme von Schweizer Staatsgebiet könnte das System durch im Ausland betriebene Knoten weiter funktionieren.

2.7.3 Anforderungen des VBS

Hinweis

Die Etablierung eines VDR für die Staatliche E-ID der Schweiz liegt nicht in der Verantwortung des VBS. Die in diesem Abschnitt erörterten Anforderungen haben möglicherweise für eine Lösung die durch das Bundesamt für Informatik und Telekommunikation betrieben wird, keine Gültigkeit.

⁵¹vgl. Abschnitt 2.4.4 auf Seite 14

⁵²vgl. Abschnitt 2.6 auf Seite 23, Abschnitt 2.6.1 und Abschnitt 2.6.2

⁵³In Krisensituationen haben Menschen u.U. keinen Zugriff mehr auf physische Vermögenswerte

⁵⁴vgl. Abschnitt 2.6.3 auf Seite 23

⁵⁵VDR ist für andere Entitäten nicht mehr erreichbar

⁵⁶vgl. Abschnitt 2.6 auf Seite 23, Abschnitt 2.6.2 und Abschnitt 2.6.4

2.7.3.1 Performance

In Abschnitt 2.4.8 auf Seite 15 wurden essentielle Elemente eingeführt, die auf dem VDR registriert werden. Einige – aber nicht alle – dieser Elemente müssen mit sofortiger Wirkung (innerhalb von Sekunden) für andere Entitäten sichtbar sein. Die Anzahl Verarbeitungen pro Zeiteinheit variieren je nach Monat und Tageszeit stark – z.B. finden Rekrutierungen zeitlich konzentriert statt und in der Nacht ist weniger Aktivität zu erwarten.

Gemäss Absprachen mit dem VBS ist die sofortige Sichtbarkeit im System zu relativieren: In den meisten Fällen muss ein Eintrag nicht sofort für alle sichtbar sein. So kann sich das VBS beispielsweise vorstellen, Wochen vor der Rekrutierung einen Brief zu versenden, der den Auftrag zur Erstellung einer persönlichen DID beinhaltet.

2.7.3.2 Kosten

Die Kosten für den Betrieb des VDR dürfen nicht signifikant über den Betriebskosten bestehender Verarbeitungssysteme liegen. Das VDR ist als komplementärer (und nicht als substituierender) Kostenpunkt zu verstehen – weite Teile der bestehenden VBS-Infrastruktur wird zentral bestehen bleiben. Insbesondere ist darauf zu achten, dass der variable Kostenanteil⁵⁷ minimal ausfällt.

2.7.3.3 Nachhaltigkeit

Die Schweiz hat sich als UNO-Mitglied den 17 Zielen für nachhaltige Entwicklung (SDG) verpflichtet[59]. Zudem sind verschiedene parlamentarische Motionen⁵⁸ für mehr Nachhaltigkeit bei den Bundesbehörden hängig. 2022 kommt die interne Revision des VBS zudem zum Schluss, Faktoren der Nachhaltigkeit müsste vonseiten VBS mehr Beachtung geschenkt werden[60]. Nachhaltigkeit wird damit zu einem Qualitätskriterium.

2.7.3.4 Regulationskonformität

Die Ausarbeitung regulatorischer Grundlagen für die E-ID liegt in der Verantwortung des Bundesamt für Justiz (BJ). Der gesetzliche Rahmen soll Technologie-neutral gehalten werden. Das BJ strebt eine möglichst hohe Kompatibilität mit Lösungen der EU an[57, p. 10]. Rechtliche Basis für die E-ID in der EU ist die eIDAS-Verordnung die aktuell gerade überarbeitet wird. Die neue Verordnung soll im September 2022 durch die EU-Staaten verabschiedet werden[61]. eIDAS hat zum Ziel, Standards für die digitale Signatur, Verifikation und weitere sog. Vertrauensdienste über die EU-Mitgliedstaaten hinweg zu etablieren. Bis Mitte 2022 soll zudem die Architektur für EUid-Wallets konzipiert sein[62].

Der Paradigmenwechsel weg von zentralen Instanzen bringt Herausforderungen für die Regulationskonformität mit sich. Wenn das System nicht mehr in alleiniger Kontrolle einer Partei ist und Einträge persistent im System gespeichert sind, stellt sich die Frage der rechtlichen Verantwortlichkeit und Haftbarkeit für falsche oder widerrechtliche Einträge[9, p.56]. Um die Frage der Haftbarkeit zu klären dürfen gewisse Entitäten nicht anonym bleiben.

⁵⁷Kosten pro Transaktion – z.B. Registrieren einer DID

⁵⁸z.B. Motion 07.3910 für ein nachhaltiges Beschaffungswesen – <https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaef?AffairId=20073910>

2.7.3.5 Datenschutz

Die Lösung muss sich mit dem Bundesgesetz über den Datenschutz (DSG) vereinbaren lassen. Zwecks möglichst hoher Kompatibilität mit Lösungen der EU⁵⁹ ist ausserdem auf die Konformität mit der Datenschutz-Grundverordnung (DSGVO) zu achten.

Ein wichtiger Punkt ist das «Recht auf Vergessenwerden»⁶⁰. Zwar nennt das DSG (anders als die DSGVO) das «Recht auf Vergessenwerden» nicht konkret, sieht aber die Löschung von Einträgen in gewissen Fällen (z.B. falsche Informationen gespeichert) vor[63]. Christopher Allen schreibt in seinen Prinzipien für SSI⁶¹ dazu:

«Dies [die persistente Speicherung, *Anm. der Autoren*] darf nicht im Widerspruch zu einem „Recht auf Vergessenwerden“ stehen; ein Nutzer sollte in der Lage sein, über eine Identität zu verfügen, wenn er dies wünscht, und Ansprüche sollten im Laufe der Zeit gegebenenfalls geändert oder entfernt werden. Dies erfordert eine strikte Trennung zwischen einer Identität und ihren Ansprüchen: Sie können nicht für immer miteinander verbunden sein.»[5]

Die Anforderungen bezüglich Datenschutz überschneiden sich teilweise mit Anforderungen, die bereits in Abschnitt 2.7.3.4 auf der vorherigen Seite erörtert wurden. Auch die Datenschutzrechtlichen Anforderungen bedingen: Die VDR-Architektur muss die Identifizierbarkeit gewisser Entitäten und das Widerrufen registrierter Daten im VDR zulassen.

2.7.4 Gewichtungsmatrix

Tabelle 2.3 auf der nächsten Seite zeigt die Gewichtung der Anforderungen. Bewertet wurde anhand einer an MoSCoW⁶² angelehnten Bewertungsskala:

- 3 – Muss: Zwingend zu erfüllende Anforderung.
- 2 – Soll: Zu erfüllen, wenn dadurch kein Muss-Kriterium nicht mehr erfüllt ist.
- 1 – Kann: Optionale, aber wünschenswerte Anforderung.

⁵⁹vgl. Abschnitt 2.7.3.4 auf der vorherigen Seite

⁶⁰Art. 17 DSGVO

⁶¹vgl. Abschnitt 2.4.12 auf Seite 16

⁶²Weitere Informationen zu MoSCoW: <https://www.projektmagazin.de/glossarterm/moscow>

Kategorie	Anforderung	Gewichtung	Begründung
Anforderungen aus SSI-Architektur	Dezentralität	3 – Muss	SSI-Prinzipien sonst nicht erfüllt ⁶³
	Zugänglichkeit, Portabilität und Interoperabilität	3 – Muss	SSI-Prinzipien sonst nicht erfüllt.
	Persistenz	3 – Muss	SSI-Prinzipien sonst nicht erfüllt.
Anforderungen aus Szenarien	Ausfallsicherheit	3 – Muss	Hohe Plausibilität für Eintritt Szenario.
	Unstoppbarkeit	2 – Soll	Mittlere Plausibilität für Eintritt Szenario.
	Zensurresistenz	2 – Soll	Mittlere Plausibilität für Eintritt Szenario.
	Transnationalität	1 – Kann	Geringe Plausibilität für Eintritt Szenario.
Anforderungen des VBS	Performance	3 – Muss	Gem. Absprache mit VBS.
	Kosten	3 – Muss	Gem. Absprache mit VBS.
	Nachhaltigkeit	2 – Soll	Gem. Absprache mit VBS.
	Regulationskonformität	3 – Muss	Einhaltung gesetzlicher Vorgaben zwingend.
	Datenschutz	3 – Muss	Zentrale Anforderung gem. Diskussionspapier.

Tabelle 2.3: Gewichtungsmatrix für die Anforderungen an ein VDR.

⁶³Dezentralität ist je nach Auslegung der Prinzipien durch die Verteilung der VC's in den Wallets der Besitzer/innen bereits erfüllt.

2.8 Evaluation Blockchain als VDR

Auf Basis der definierten Anforderungen im Abschnitt 2.7 wird die Eignung der Blockchain-Technologie als VDR geprüft. Neben möglichen Blockchain-Ansätzen werden auch andere technologische Ansätze kurz thematisiert und deren Eignung eingeschätzt.

2.8.1 Einordnung und Vergleich anderer Systeme

Die Mehrheit der aktuellen Anwendungen⁶⁴ verwendet für das VDR eine Blockchain-basierte Lösung. Die Verwendung einer solchen Lösung ist indes keine zwingende Anforderung an die SSI-Infrastruktur[7]. Im Schnitt erfüllen Blockchain-basierte Lösungen die SSI-Prinzipien jedoch besser als nicht Blockchain-basierte[6].

Zur Einordnung und zum Vergleich werden nachfolgend Vorteile und Herausforderungen unterschiedlicher Architekturen aufgezeigt. Die Evaluation von Technologien ohne Blockchain ist nicht Fokus dieser Arbeit. Deren Eignung könnte in weiterführenden Arbeiten vertieft untersucht werden.

2.8.1.1 Zentrales System

Ein zentraler Ansatz wird für das VDR verwendet - beispielsweise eine Datenbank oder ein Verzeichnisregister. Ein zentraler Ansatz ist explizit nicht dezentral und kann entsprechend auch die Anforderung der Dezentralität bzw. Transnationalität nicht erfüllen. Da die Daten nicht zwischen mehreren Knoten verteilt und synchronisiert werden müssen, ist dieser Ansatz grundsätzlich performant und kostengünstig. Gleichzeitig erschwert aber die zentrale Kontrolle die Sicherstellung der Persistenz. Hohe Last kann für eine zentrale Lösung zum Problem werden, da vertikale Skalierung⁶⁵ nur begrenzt möglich und teuer ist. Regulationen und Gesetze können von zentralen Stellen gut eingehalten werden. Die zentrale Stelle ist ein Single Point of Failure und ein Single Point of Control. Das wirkt sich negativ auf die Sicherheit, Manipulierbarkeit und Zensurresistenz aus: die Kontrolle (und damit auch Macht und Ziel für Angriffe) konzentriert sich auf einen Punkt[64].

Folgende Anforderungen könnten mit einem zentralen Ansatz nicht oder nur schwierig umgesetzt werden:

- Dezentralität – Abschnitt 2.7.1.1 auf Seite 25
- Persistenz – Abschnitt 2.7.1.3 auf Seite 25
- Ausfallsicherheit – Abschnitt 2.7.2.1 auf Seite 26
- Unstoppbarkeit – Abschnitt 2.7.2.2 auf Seite 26
- Zensurresistenz – Abschnitt 2.7.2.3 auf Seite 26
- Transnationalität – Abschnitt 2.7.2.4 auf Seite 26

Erkenntnis

Zentrale Systeme eignen sich nicht für die Umsetzung des VDR.

⁶⁴vgl. Abschnitt 2.5 auf Seite 17

⁶⁵z.B. durch Erhöhung der CPU und RAM

2.8.1.2 Verteiltes System

Das System wird weiterhin von einer zentralen Instanz kontrolliert, die Systemarchitektur ist jedoch verteilt. Ein Beispiel für einen solchen Ansatz ist eine verteilte Datenbank. Nachteile einer rein zentralen Lösung wie Ausfallsicherheit und Skalierbarkeit können damit gelöst werden. Zudem ist auch eine geografisch verteilte Architektur möglich[64]. Durch die zentrale Kontrolle ist das System weiterhin anfällig für Angriffe⁶⁶, zentraler Abschaltung und Zensur. Auch die Erfüllbarkeit der Persistenz unterscheidet sich nicht von einem zentralen System.

Nachfolgende Anforderungen könnten weiterhin nicht oder nur schwierig umgesetzt werden:

- Dezentralität – Abschnitt 2.7.1.1 auf Seite 25
- Persistenz – Abschnitt 2.7.1.3 auf Seite 25
- Unstoppbarkeit – Abschnitt 2.7.2.2 auf Seite 26
- Zensurresistenz – Abschnitt 2.7.2.3 auf Seite 26

Erkenntnis

Verteilte Systeme eignen sich nicht für die Umsetzung des VDRs.

2.8.1.3 Dezentrales System

Die Kontrolle des Systems liegt nicht mehr bei einer zentralen Instanz und die Architektur ist dezentral aufgebaut. Dazu zählen dezentrale und verteilte Lösungen wie dezentrale Dateisysteme, das GNU Name System⁶⁷ oder die Blockchain.

Dezentrale Systeme können je nach Ausprägung alle Anforderungen an ein VDR erfüllen[4][6]. Blockchain-Lösungen fallen in diese Kategorie und werden in den folgenden Abschnitten im Detail auf Erfüllbarkeit der Kriterien analysiert[65, S. 1].

2.8.2 Private Blockchain

Private Blockchain-Implementierungen haben Vorteile hinsichtlich Kosten (keine oder tiefe Transaktionsgebühren), Datenschutz/Regulationskonformität (geschlossenes System, Verantwortlichkeiten klar) und Nachhaltigkeit (Rechenintensiver Konsensusmechanismus PoW kommt nicht zum Einsatz)[9, p. 84]. Ein wesentlicher Nachteil liegt in der Offenheit: Die Einsicht in eine Private Blockchain bedingt die Erlaubnis durch deren Betreiberinnen, deren Betreiber⁶⁸. Diese Abhängigkeit steht in direktem Widerspruch zu mehreren Anforderungen an eine VDR-Lösung für SSI. Der geschlossene Ansatz verhindert die Zugänglichkeit und schränkt die Dezentralität ein. Zudem hat die betreibende Instanz die Macht, das Netz unzugänglich zu machen (Unstoppbarkeit).

- Unstoppbarkeit – Abschnitt 2.7.2.2 auf Seite 26
- Dezentralität – Abschnitt 2.7.1.1 auf Seite 25
- Zugänglichkeit, Portabilität und Interoperabilität – Abschnitt 2.7.1.2 auf Seite 25

⁶⁶z.B. durch eine Infiltration wie im Szenario Cyber-Angriff in Abschnitt 2.6.3 auf Seite 23 beschrieben.

⁶⁷GNU Name System (GNS) ist eine dezentrale Datenbank zur Namensauflösung <https://www.gnunet.org/>

⁶⁸vgl. Abschnitt 2.2.1 auf Seite 6

Erkenntnis

Private Blockchain eignet sich nicht für die Umsetzung des VDR^a.

^aSiehe dazu auch [9, p.84] und [36, p. 9]

2.8.3 Public Blockchain

Die in Abschnitt 2.8.2 beschriebenen Nachteile einer Private Blockchain werden durch die Öffnung der Blockchain (Public Blockchain) gelöst (Dezentralität, Zugänglichkeit, Portabilität und Interoperabilität) oder gemindert (Unstoppbarkeit).

Wesentlichster Unterschied zur Private Blockchain: Zu einer Public Blockchain haben alle Akteure Zugriff – ohne zentrale Autorität(en) die den (Lese-)Zugang kontrollieren⁶⁹. In Public Permissioned Blockchains können Teilnehmenden unterschiedliche Berechtigungen zugewiesen werden. Damit können Public Blockchains je nach Ausprägung viele oder alle Anforderungen an ein VDR für SSI erfüllen. Nachfolgend werden die Ausprägungen Permissionless und Permissioning hinsichtlich der Erfüllbarkeit vorher erwähnter Anforderungen im Detail analysiert.

Hinweis

Im Bereich der Public Blockchain wird viel geforscht und aktiv weiterentwickelt. Ansätze wie Sharding oder Rollups^a versprechen, die Skalierbarkeit und Performanz einer Blockchain zu erhöhen und Kosten zu senken. Für die Evaluation wurden solche Ansätze nicht berücksichtigt, da sie oft noch in Entwicklung und schwierig einzuordnen sind.

^aMehr zu Skalierungsansätzen unter <https://ethereum.org/en/developers/docs/scaling/>

2.8.3.1 Dezentralität

Public Permissionless Blockchains gewährleisten durch ihre offene Natur einen hohen Grad an Dezentralität. Es gibt keine zentrale Autorität(en), die das Netzwerk und den Zugang kontrollieren - Wer will, kann teilnehmen. Bei Public Permissioned Blockchains haben Teilnehmende unterschiedliche Berechtigungen. Der Grad der Dezentralität wird durch die Art und Weise der Berechtigungsvergabe beeinflusst. Liegt die Kontrolle bei einer oder mehreren Autoritäten, leidet darunter zwangsläufig die Dezentralität – Je mehr Hürden es für eine Teilnahme gibt, desto tiefer die Wahrscheinlichkeit für viele unabhängige Teilnehmende[66]. Ein höherer Grad an Dezentralität hat einen positiven Einfluss auf die Sicherheit einer Blockchain[67, S. 18–20].

2.8.3.2 Persistenz

Im Abschnitt 2.2 wurden die generellen Vorteile der Blockchain-Technologie vorgestellt. Die Manipulationssicherheit, Transparenz, Unveränderlichkeit und Rückverfolgbarkeit von Public Blockchains eignen sich sehr gut für die Anforderung an die Persistenz des VDRs. Nachträgliche Änderungen bedingen durch die Architektur einer Blockchain eine Neuberechnung der betroffenen und nachfolgenden Blöcke. Je nach Konsensusmechanismus und Netzwerkgröße ist dies kaum möglich und/oder bedarf einer hohen Investition (zum Beispiel in Hardware). Andere Teilnehmende können die Änderung schnell identifizieren und als ungültig markieren. Das gilt sowohl für Public Permissioned wie auch Public Permissionless Blockchains[68, S. 51].

⁶⁹vgl. Abschnitt 2.2.1 auf Seite 6

2.8.3.3 Zugänglichkeit, Portabilität und Interoperabilität

Die Zugänglichkeit zu den VDR-Daten wird durch den offenen Lesezugang von Public Blockchains ermöglicht. In Kombination mit etablierten Standards (z.B. der W3C) kann die Interoperabilität und der Austausch mit anderen SSI-Ökosystemen gewährleistet werden. Wesentlicher Einfluss auf die Portabilität hat indes nicht der Aufbau des VDRs selber, sondern die Spezifikation der verwendeten DID-Methode, VCs und anderen Komponenten im System. Die dem VDR zugrundeliegende Technologie spielt eine untergeordnete Rolle[69].

2.8.3.4 Regulation

Da die rechtliche Grundlage aktuell beim Bundesamt für Justiz (BJ) noch in Arbeit ist, kann die Regulationskonformität nicht abschliessend beurteilt werden. Grundsätzlich lässt sich festhalten, dass Entitäten in einer Public Permissionless Blockchain anonym bleiben können (vgl. Abschnitt 2.2.1 auf Seite 6 und die Frage der Haftbarkeit damit nur sehr schwer bis gar nicht klarbar ist. Dieses Problem wird mit der Definition von Anforderungen für Schreibvorgänge gelöst (Permissioned Blockchain).

Für die Kompatibilität mit der EU gilt: Als nicht EU-Mitglied erfährt die Schweiz erst nach der Veröffentlichung der finalen EUid-Architektur deren Inhalte. Bekannt ist, dass die Europäische Kommission seit 2020 eine EU-Weite Blockchain (EBSI) aufbaut, die auf ihrer Website⁷⁰ den Use-Case SSI prominent bewirbt[52]. EBSI ist eine Public Permissioned Blockchain[70]. Zudem gibt es Initiativen einzelner EU-Staaten⁷¹ im Bereich Public Permissioned Blockchain. Daraus lässt sich schliessen, dass eine solche Architektur für ein VDR regularitätskonform betrieben werden kann.

2.8.3.5 Datenschutz

Der Datenschutz soll durch das System selber (Privacy by Design), durch die Minimierung der nötigen Datenflüsse (Prinzip der Datensparsamkeit) und einer dezentralen Datenspeicherung gewährleistet werden. Dies hält der Bund in seinem Richtungsentscheid zur E-ID fest[71]. Das Datenschutzgesetz der Schweiz wird aktuell überarbeitet und soll sich der DSGVO der EU annähern[72]. Dies ist eine wichtige Grundvoraussetzung, damit das SSI-Ökosystem interoperabel mit der EU ist.

Ein Paper «Your Identity is Yours: Take Back Control of Your Identity Using GDPR Compatible Self-Sovereign Identity»[73] analysierte die Kompatibilität von Public Permissioned und Public Permissionless Blockchains mit den Grundsätzen⁷² der DSGVO. Die Autoren kommen zum Schluss, dass SSI-Systeme auf Basis einer Public Permissionless Blockchain vor grösseren Herausforderungen stehen, da alle Teilnehmenden die gleichen Rechte haben. Public Permissioned Blockchain hingegen erfüllen einen Grossteil der Grundsätze, da sie über ein Governance-Modell verfügen und oft von einem Konsortium von vertrauenswürdigen Organisationen betrieben werden.

⁷⁰Website EBSI: <https://ec.europa.eu/digital-building-blocks/wikis/display/EBSI/Home>

⁷¹z.B. Finny in Finnland – vgl. Abschnitt 2.5.6 auf Seite 19

⁷²Die Grundsätze der DSGVO sind im Artikel 5 festgehalten. Mehr unter <https://dsgvo-gesetz.de>

Hinweis

Was im digitalen Raum alles unter die sog. «personenbezogenen Daten» fällt, ist nicht in jedem Fall klar. Zum Beispiel wurde von offizieller Stelle noch nicht definiert, ob eine DID bereits unter personenbezogene Daten fällt. Die Behörden (nicht nur in der Schweiz) sind in der Pflicht, solche datenschutzrechtlichen Fragen zu klären.

2.8.3.6 Performanz

Der Grossteil des Datenverkehrs (z.B. die Übermittlung von persönlichen Daten wie der Name und das Alter) findet ausserhalb des VDRs statt⁷³. Viele zeikritische Aktionen wie das Verifizieren von VCs greifen nur lesend auf das VDR zu. Das Lesen der Blockchain ist grundsätzlich schnell und lässt sich vertikal skalieren. Schreibende Aktivitäten wie das Registrieren von DIDs sind oft nicht zeikritisch. Beispielsweise könnten junge Personen vor der Rekrutierung mit einem Brief zur Registrierung einer DID aufgefordert werden - der Prozess der Registrierung muss nicht unmittelbar erledigt sein. Die Performanzeinschränkung der Blockchain-Technologie bei Schreiboperationen stellt deshalb für SSI kein nennenswertes Problem dar[74, S. 26].

Generell wird davon ausgegangen, dass Permissioned Blockchains besser skalieren und effizienter sind. Im Gegensatz zu einer Permissionless Blockchain kann das Netz an Validatoren in einer Permissioned Blockchain bezüglich Latenz und Durchsatz optimiert und erweitert werden[75, S. 25][11, S. 91].

2.8.3.7 Nachhaltigkeit

Das «EU Blockchain Observatory and Forum» veröffentlichte eine umfangreiche Analyse⁷⁴ zum Energieverbrauch von Blockchain-Technologien. Der Bericht teilt den Stromverbrauch in drei Hauptkategorien ein:

- Konsensusmechanismus
- Operationen auf der Blockchain
- Energieverbrauch von Knoten im Leerlauf

Einen hohen Energieverbrauch ergibt sich vor allem aus der Verwendung des Konsensusmechanismus Proof of Work (PoW). In Permissioned und Permissionless Blockchains, die nicht PoW verwenden, liegt der größte Teil des Energieverbrauchs im Leerlauf der Knoten und steigt damit linear mit der Anzahl Knoten. Der Bericht sieht den Energieverbrauch jedoch so deutlich geringer als bei Blockchains die PoW verwenden, dass sie einen weiteren Vergleich des Energieverbrauchs dieser Lösungen hinterfragen[76, p. 13-17]. Das VDR kann grundsätzlich sowohl mit Permissionless als auch Permissioned Blockchains nachhaltig betrieben werden, solange auf den Konsensusmechanismus Proof of Work verzichtet wird. Bei der Knotenanzahl gilt es den Aspekt der Nachhaltigkeit mit dem der Sicherheit auszubalancieren.

Ein Grossteil der Permissionless Blockchains wie Bitcoin und Ethereum setzen noch⁷⁵ auf den Konsensusmechanismus PoW[78, S. 1]. Ein Ethereum Netz kann auch als Permissioned oder Private Blockchain betrieben werden, das andere Konsensusmechanismen (z.B. PoA)) verwendet⁷⁶. Die Einhaltung der Nachhaltigkeitsanforderungen ist damit aktuell mit Permissioned Blockchains einfacher.

⁷³vgl. Abschnitt 2.4 auf Seite 12

⁷⁴Der Bericht «Energy Efficiency of Blockchain Technologies» und weitere unter <https://www.eublockchainforum.eu/reports>

⁷⁵Dies kann und wird sich vermutlich in Zukunft ändern. Beispielsweise wird Ethereum in einem zukünftigen Update auf Proof of Stake wechseln[77]

⁷⁶vgl. Abschnitt 2.2.1 auf Seite 6

2.8.3.8 Sicherheit

Die Sicherheit eines Blockchain-Netzwerks ist abhängig von verschiedenen Faktoren wie dem Konsensusmechanismus, den kryptografischen Algorithmen, der Anzahl an Knoten und dem Grad an Dezentralität. Generell gilt, dass ein IT-System höchstens so sicher ist wie die schwächste Stelle. Die Blockchain löst dieses Problem teilweise: Einzelne Knoten, die ausfallen oder kompromittiert sind, werden von den anderen Knoten einfach ignoriert. Das «schwächste Glied» ist in diesem Kontext der schwächste Mechanismus (der dann wiederum bei allen Knoten zum Einsatz kommt). Eine Herausforderung in der Sicherheitsbestimmung liegt beim Konsensusmechanismus. Da neben kryptografischen Mechanismen auch ökonomische Aspekte⁷⁷ eine Rolle spielen, die schwer verglichen und eingeordnet werden können[79, p. 40-41].

Die Blockchain-Technologie ist durch die dezentrale Architektur und die Anwendung kryptografischer Verfahren grundsätzlich sehr robust gegen Manipulation und Angriffe — vor allem im Vergleich zu zentralen Ansätzen[11, S. 16]. Wie bereits im Abschnitt 2.8.3.1 erwähnt, hat ein höherer Grad an Dezentralität einen positiven Einfluss auf die Sicherheit einer Blockchain[67, S. 18–20]. Public Permissionless Blockchains ermöglichen es einen hohen Grad an Dezentralität zu erreichen, da keine Entität zusätzliche Rechte⁷⁸ besitzt. Dadurch können die Sicherheitsanforderungen Ausfallsicherheit, Zensurresistenz und Unstoppbarkeit mit Public Permissionless Blockchains gut erfüllt werden.

Grundsätzlich wird davon ausgegangen, dass Permissioned Blockchains kostengünstiger und effizienter sind, dies jedoch zu Lasten der Transaktionssicherheit. Ein Paper[75] hat diesen Tradeoff untersucht, der laut den Autoren hauptsächlich in einem komplett vertrauenslosen Umfeld existiert. Sobald aber ein gewisses Vertrauen gegenüber einer Permissioned Blockchain etabliert ist, kann die Transaktionssicherheit sogar höher sein. In einer Permissioned Blockchain können Validatoren auch mit externen Massnahmen wie rechtlichen Verträgen bzw. drohendem Reputationsschaden zur korrekten Teilnahme gezwungen werden[75, p. 24-25].

2.8.3.9 Kosten

Die zugrundeliegenden Kosten können in dieser Arbeit nicht abschliessend dargelegt werden. Ein Vergleich unterschiedlicher Blockchain-Varianten lässt eine Einschätzung zu. Beim Betrieb eines VDR entstehen verschiedene Aufwände. Wir unterscheiden drei Kostentreiber:

- Infrastruktur für den Betrieb von Knoten
- Transaktionsgebühren
- Einbindung bestehender Software-Lösungen

Infrastrukturstkosten Die Kosten für den Betrieb eines dezentralen Netzwerks hängen stark von Art und Menge der betriebenen Knoten ab. Public Permissionless Blockchain bieten bereits ein umfangreiches dezentrales Netz an Knoten. Dadurch müssen deutlich weniger (bzw. keine) Knoten selbst betrieben werden, um den Anforderungen der Dezentralität zu entsprechen. Wie alle anderen kann auch die Schweiz bei Public Blockchains ein oder mehrere Knoten selber betreiben. Die Kosten dafür sind abhängig von den aktuellen Anforderungen der entsprechenden Blockchain. Die Anschaffungskosten für die Hardware zum Betrieb eines Ethereum Full-Node⁷⁹ belaufen sich heute (Stand Juni 2022) auf mehrere hundert Franken[80]. Auch bei den meisten bestehenden Permissioned Blockchains kann ein eigener Knoten betrieben werden. Hier variieren

⁷⁷Damit Transaktionen valide ausgeführt werden, braucht es einen ökonomischen Anreiz. Dies betrifft vor allem Public Permissionless Blockchains.

⁷⁸vgl. Abschnitt 2.2.1 auf Seite 6

⁷⁹Informationen zu den unterschiedlichen Knoten-Typen unter: <https://ethereum.org/en/developers/docs/Knotens-and-clients/>

die Kosten sehr stark zwischen den Blockchains, deren Anforderungen und ggf. Lizenzkosten. Werden die Lizenzkosten ausgeklammert, bewegen sich die Kosten in einem ähnlichen Rahmen wie für das Betreiben eines Knotens einer Public Permissionless Blockchain. So sind z.B. die Anforderungen zum Betreiben eines Knotens der LACChain und Sovrin ähnlich wie die bei Ethereum[80][81][82].

Werden blockgenerierende Knoten betrieben, können die Anforderungen je nach Blockchain höher sein. Blockchains wie Ethereum bieten dafür eine Kompensation (Transaktionsgebühren) für den Aufwand an. Auf Transaktionsgebühren wird im nächsten Abschnitt genauer eingegangen.

Alternativ kann ein eigenes Netzwerk aufgebaut werden. Die effektiven Kosten für Aufbau und Betrieb eines eigenen Blockchain-Netzwerks können im Rahmen dieser Arbeit nicht geschätzt werden.

Transaktionsgebühren Der Betrieb eines Knotens der Transaktionen ausführt, verursacht Kosten (vgl. Punkt Infrastrukturkosten). Diese Kosten werden oft durch Transaktionsgebühren kompensiert. Wer eine Transaktion in das Blockchain-Netzwerk sendet, muss diese Gebühr entrichten.

Die Höhe der Gebühr variiert je nach Blockchain stark. Bei einigen Public Permissionless Blockchains wie Ethereum und Bitcoin wird der Preis durch den Markt bestimmt. Je höher die angebotene Gebühr, desto schneller wird die Transaktion verarbeitet. Public Permissioned sowie Private Blockchains können fixe oder keine Gebühren⁸⁰ verlangen[83, p. 49]. Allerdings bedeutet dies, dass die Kosten blockgenerierender Knoten nicht mehr gedeckt sind.

Es lässt sich festhalten, dass Transaktionsgebühren bei Public Permissionless Blockchains stark variieren und somit eine genaue Vorhersage schwierig ist. Public Permissioned und Private Blockchains hingegen erlauben es den betreibenden Instanzen die Kosten selber zu definieren. Die Kosten variieren je nach Anbieter auch hier stark. Insbesondere wenn eigene (blockgenerierende) Knoten betrieben werden, darf der Aspekt der Transaktionsgebühren nicht isoliert betrachtet werden. Werden keine Transaktionsgebühren bezahlt, bedeutet dies auch, dass der Aufwand blockgenerierender Knoten nicht kompensiert und somit bei den Infrastrukturkosten stärker ins Gewicht fallen wird.

Einbindung in bestehende Systeme Für die Einbindung bestehender Software-Lösungen gibt es keine offensichtlichen und signifikanten Unterschiede bei den Kosten. Egal in welcher Form das VDR betrieben wird, es braucht Dienste zur Validierung und Ausstellung von Credentials, DIDs und TLs, die mit den entsprechenden Kern-Systemen verbunden werden müssen.

Zusammenfassung Insgesamt lässt sich festhalten, dass die Kosten sowohl für Public Permissionless wie auch für Public Permissioned Blockchains stark variieren. Zudem muss dem Aspekt der Blockgeneration Rechnung getragen werden: Werden eigene blockgenerierende Knoten betrieben und wie hoch ist die Entschädigung dafür? Für eine sinnvolle Einschätzung ist zudem die Frage essentiell, was auf der Blockchain gespeichert wird. Sind nur wenige Transaktionen nötig, fällt der Aspekt der Transaktionskosten viel weniger ins Gewicht. Die Ethereum DID-Methode «did:ethr:» beispielsweise erlaubt es aus jedem Ethereum Schlüssel-Paar eine Ethereum DID zu generieren. Der öffentliche Schlüssel bzw. die Ethereum Adresse dient als DID. Für die Erstellung dieser DID ist keine Transaktion auf der Blockchain nötig und die Erstellung ist damit kostenlos. Dieses Beispiel zeigt, dass die effektiven Kosten stark davon abhängen, was genau im VDR gespeichert wird[84].

⁸⁰Beispiel Gebühren von Sovrin: <https://sovrin.org/sovrin-price-plan/>

2.8.4 Evaluation

Tabelle 2.4 auf der nächsten Seite vergleicht die VDR-Ansätze aus Abschnitt 2.8, welche die definierten Muss-Anforderungen aus Abschnitt 2.7 erfüllen können. Dabei handelt es sich um die Public Blockchain Ausprägungen Permissionless und Permissioned. Bewertet wurden die Ansätze mit folgender Skala:

- 3 — Gut erfüllbar: Der Ansatz eignet sich gut, um die Anforderung zu erfüllen.
- 2 — Erfüllbar: Die Anforderung ist erfüllbar.
- 1 — Schwer erfüllbar: Die Anforderung ist erfüllbar, jedoch mit erhöhtem Aufwand und Vorsicht verbunden.

	Gewichtung	Public Permissioned Blockchain	Public Permissionless Blockchain	Begründung
Dezentralität	3	2	3	Siehe Abschnitt 2.8.3.1
Zugänglichkeit, Portabilität und Interoperabilität	3	3	3	Siehe Abschnitte 2.8.3 und 2.8.3.3
Persistenz	3	3	3	Siehe Abschnitt 2.8.3.2
Ausfallsicherheit	3	3	3	Siehe Abschnitt 2.8.3.8
Unstoppbarkeit	2	2	3	Siehe Abschnitte 2.8.3.8
Zensurresistenz	2	2	3	Siehe Abschnitt 2.8.3.8
Transnationalität	1	3	3	Siehe Abschnitte 2.8.1.3 und 2.8.3
Performanz	3	3	2	Siehe Abschnitt 2.8.3.6
Kosten	3	2	2	Siehe Abschnitt 2.8.3.9
Nachhaltigkeit	2	3	2	Siehe Abschnitt 2.8.3.7
Regulationskonformität	3	3	1	Siehe Abschnitt 2.8.3.4
Datenschutz	3	3	2	Siehe Abschnitt 2.8.3.5
Total	83	76		

Tabelle 2.4: Bewertung der Public Blockchain Ausprägungen Permissionless und Permissioned. Der Permissioned-Ansatz erfüllt im Schnitt die Anforderungen besser, obwohl beide Ansätze gut abschliessen. Einen deutlichen Unterschied gibt es bei der Einhaltung der Regulationskonformität.

2.8.5 Fazit

Ein dezentraler Ansatz bietet sich als VDR-Grundlage an und lässt sich gut mit den SSI-Prinzipien und den definierten Anforderungen aus Abschnitt 2.7 vereinbaren. Eine genauere Analyse der Blockchain-Technologie zeigt, dass viele Anforderungen durch die Grundsätze der Technologie bereits erfüllbar sind. Alle Anforderungen sind mit Public Blockchains erfüllbar - dies gilt sowohl für Public Permissionless und Public Permissioned Blockchains. Beide Ausprägungen können als VDR in Betracht gezogen werden.

Eine Einordnung der beiden Ansätze wurde im Abschnitt 2.8.3 durchgeführt und schlussendlich in der Tabelle 2.4 bewertet. Alle Teilnehmenden in einer Public Permissionless Blockchain sind gleichberechtigt, wodurch eine höhere Dezentralität erreicht werden kann. Dies wirkt sich positiv auf die Unstoppbarkeit und Zensurresistenz aus. Public Permissioned Blockchain hingegen schliessen bzgl. Performanz, Nachhaltigkeit, Datenschutz und Regulationkonformität besser ab.

In der Bewertung schliesst der Ansatz Public Permissioned Blockchain insgesamt besser ab. Ausschlaggebender Faktor ist die Regulationskonformität⁸¹. Dieser Entscheid sollte erneut hinterfragt werden, wenn die rechtlichen Grundlagen durch das BJ geschaffen wurden.

Die Erkenntnisse der Evaluation stimmen mit den generellen Aussagen in der Literatur⁸² überein[3][6][9, p. 84-85]. Das im Abschnitt 2.1 erwähnte Eckpunktepapier[8] des BSI sieht auch andere nicht-dezentrale Systeme als Ansatz für das VDR. Diese Aussage trifft für die definierten Anforderungen dieser Arbeit nicht zu (siehe Abschnitt 2.8.1). Das Paper[4] fand in den untersuchten 31 Lösungen keine, die alle SSI-Prinzipien erfüllt. Die vorliegende Arbeit widerlegt diese Aussage nicht, da keine spezifischen Lösungen sondern technologische Ausprägungen untersucht wurden. Die von den SSI-Prinzipien abgeleiteten Anforderungen⁸³ können mit einer Public Blockchain erfüllt werden.

Auch bei den analysierten Anwendungen im Abschnitt 2.5 zeigt sich, dass der Ansatz Public Permissioned Blockchain bevorzugt wird.

Erkenntnis

Public Blockchains können die definierten Anforderungen aus Abschnitt 2.7 erfüllen. Gemäss Evaluation im Abschnitt 2.8 eignet sich Public Permissioned Blockchain am besten.

⁸¹vgl. Abschnitt 2.8.3.4 auf Seite 33

⁸²vgl. Abschnitt 2.1

⁸³vgl. Abschnitt 2.7.1

2.9 Empfehlungen

In den vorangehenden Kapiteln wurde die Eignung unterschiedlicher Blockchain-Ausprägungen für das VDR einer SSI-Lösung analysiert. Nachfolgend sind Empfehlungen für eine Implementierung eines VDR auf Basis der Blockchain-Technologie aggregiert. Diese Empfehlungen erheben nicht Anspruch auf Vollständigkeit. Die unterschiedlichen Bereiche können als Basis für weitere Forschungsfragen dienen.

2.9.1 Architektur

2.9.1.1 Grundarchitektur

Wie im Abschnitt 2.8 ausgeführt, eignet sich eine Public Permissioned Blockchain gemäss Anforderungen am besten als VDR der SSI-Lösung⁸⁴.

2.9.1.2 Knoten

Ein umfangreiches und geografisch verteiltes Knotennetz ist wichtig für die Erfüllung der definierten Anforderungen Dezentralität, Persistenz, Ausfallsicherheit, Unstoppbarkeit und Zensurresistenz im Abschnitt 2.7. Die empfohlene Anzahl an Knoten ist abhängig von diversen Faktoren (z.B. Konsensusmechanismus) und sollte je nach Lösung im Detail analysiert werden. Generell kann gesagt werden, dass sich eine höhere Anzahl an unabhängigen Knoten positiv auf die erwähnten Anforderungen auswirkt.

Nur geringe Datenmengen werden auf dem VDR gespeichert. Der benötigte Speicherplatz für eine DID bzw. deren DID-Dokument liegt im Bereich von wenigen Kilobytes. Mit solch geringen Datenmengen sind die Betriebskosten eines Nodes inkl. Rechenleistung (angenommen kein PoW) für die Validierung relativ tief. Beispielsweise kann ein Ethereum-Archivknoten⁸⁵ für die Blockchain-Synchronisation laut Anforderungen mit einem handelsüblichen Computer⁸⁶ betrieben werden — trotz sehr hohem Datenverkehr auf der Ethereum-Blockchain[80]. Der Aufbau eines verteilten und umfangreichen Knotennetzes im Besitz der Schweizer Eidgenossenschaft ist somit finanziell machbar und ist laut dem Austausch⁸⁷ mit dem BIT auch gefordert.

In der Schweiz kann unter anderem der Föderalismus für die Knotenverteilung verwendet werden. Dank des Konstrukts als föderale Republik bzw. Bundesstaat besitzen die 26 Kantone in der Schweiz weitgehende Eigenständigkeit bzw. Staatlichkeit. Betreibt jeder Kanton einen Knoten der eidgenössischen Blockchain kommen so bereits 26 voneinander unabhängige Knoten zusammen. Neben Kantonen und Botschaften könnten auch Bundesämter oder vertrauenswürdige juristische Personen einen Knoten stellen.

Wird zusätzlich in jeder dritten der rund 100 Botschaften im Ausland⁸⁸ ein Knoten betrieben, ergeben sich bereits fast 60 aktive Knoten – global verteilt[85]. Dieser Verteilschlüssel stellt den Weiterbetrieb auch dann sicher, wenn der Fall einer feindlichen Besetzung der Schweiz eintreten sollte: Selbst wenn alle 26 Kantonsknoten von einer feindlichen Partei übernommen werden, sind die verbleibenden (über 30) Knoten im Ausland ausreichend, um Attacken abzuwehren⁸⁹. Werden in der Schweiz mehr als 26 Knoten betrieben, müsste der Anteil Knoten im Ausland entsprechend erhöht werden.

⁸⁴vgl. Abschnitt 2.7 auf Seite 25 und Abschnitt 2.8 auf Seite 30

⁸⁵Knoten, die den gesamten historischen Verlauf der Blockchain speichern.

⁸⁶z.B. Mac mini, 8-Core-CPU, 16 GB RAM, 2 TB SSD — 1 989.– CHF (Juli 2022)

⁸⁷vgl. Meeting Protokoll – 03.05.2022 im Anhang A.1

⁸⁸vgl. Abschnitt 2.9.1.3 auf der nächsten Seite

⁸⁹Verhindert wird damit eine sogenannte 51%-Attacke - mehr dazu: <https://www.investopedia.com/terms/1/51-attack.asp>

2.9.1.3 Transnationalität

Wie im vorherigen Abschnitt erwähnt, eignen sich staatliche Vertretungen im Ausland (Botschaften) sehr gut, um Knoten zu betreiben. Daraus resultiert ein internationales und geografisch verteiltes Netzwerk, das auch bei einem Ausfall oder Kompromittierung aller Knoten in der Schweiz funktionsfähig bleiben kann. Vertretungen im Ausland unterstehen besonderen Rechten: Nach internationalem Recht dürfen staatliche Vollzugsbehörden (z.B. Polizei) ohne Erlaubnis des Botschafters das Botschaftsgelände nicht betreten⁹⁰. Nicht jedes Land wird sich für den Betrieb eines Knotens eignen (z.B. wegen unsicherer Rechtslage oder schlechter Breitbandversorgung). Entsprechende Analysen müssten durchgeführt werden.

2.9.1.4 Technologie

In den nachfolgenden Kapiteln werden Technologien für die Implementierung eines PoCs für das VBS analysiert. Die Ergebnisse verstehen sich im Kontext des PoCs und sind für eine produktive Umsetzung nicht ausreichend geprüft worden. Es wird empfohlen, die unterschiedlichen Technologien jeweils im Rahmen eines separaten PoCs zu evaluieren. Dafür reichen die im Rahmen dieser Arbeit zur Verfügung stehenden Ressourcen nicht.

2.9.2 Standards

2.9.2.1 DID-Methode

Die European Blockchain Services Infrastructure (EBSI) hat für die EU-Blockchain bereits eine DID-Methode «did:ebsi:» nach der DID-Spezifikation der W3C erstellt⁹¹. Eine entsprechende DID-Methode ist auch für eine Schweizer VDR-Lösung zentral. Diese sollte sich an die Spezifikationen der W3C halten.

2.9.2.2 Internationale Standards

Das W3C-Konsortium – eine Community aus Entwicklerinnen, Entwicklern aus der ganzen Welt – geniesst global Anerkennung für die durch Arbeitsgruppen definierten und etablierten Standards. Dezentrales Identitätsmanagement verspricht die Zukunft im digitalen Raum nachhaltig zu gestalten. Es ist für den Erfolg wichtig, dass nationale Lösungen einen hohen Grad an Interoperabilität ermöglichen. Dies kann vor allem mit der Einhaltung der durch die W3C und DIF definierten Standards erreicht werden.

Aktuell sind folgende W3C-Spezifikationen in Kraft:

- DID-Methoden Spezifikation: <https://www.w3.org/TR/did-core>
- VC-Spezifikation: <https://www.w3.org/TR/vc-data-model/>

Die Schweiz ist umgeben von EU-Ländern. Ein Austausch von digitalen Zertifikaten (z.B. Passkontrollen) ist sehr wahrscheinlich. Deshalb sollten die europäischen Initiativen zur Etablierung einer EU-Blockchain (EBSI) bzw. eines Frameworks für SSI (eSSIF) begleitet bzw. aktiv beobachtet werden. Zudem ist die Konformität mit den regulatorischen Grundlagen einer EU-SSI, namentlich die DSGVO sowie die eIDAS anzustreben. Der Aufbau eines engen Kontaktes mit den entsprechenden EU-Partnern ist empfehlenswert.

⁹⁰vgl. Wiener Übereinkommen: https://www.fedlex.admin.ch/eli/cc/1968/887_927_843/de

⁹¹Spezifikation der EBSI-DID: <https://github.com/validatedid/ebsi-did-resolver>

2.9.2.3 Nationale Standards

Zusätzlich zu den internationalen Standards sollten auch für VCs in der Schweiz Standards etabliert werden. Es bietet sich an, für ähnliche Credentials einheitliche Schemas zu definieren. So könnte z.B. ein Schema für Hochschuldiplome definiert werden, an das sich alle Hochschulen halten müssen. Dazu können – ähnlich dem Aufbau von W3C – Arbeitsgruppen eingesetzt werden, die entsprechende Spezifikationen ausarbeiten.

2.9.3 Sicherheit

2.9.3.1 Algorithmen

Es sollten grundsätzlich nur Algorithmen und (Hash-)Funktionen verwendet werden, die aktuellen und zukunftsgerichteten Sicherheitsempfehlungen entsprechen. Im Gegensatz zu anderen Staaten⁹² wurden keine entsprechenden Empfehlungen für IT-Systeme in der Schweiz gefunden.

2.9.3.2 Anpassungsfähigkeit

Technologischer Fortschritt ist fortwährend. Heute bekannte kryptografische Mechanismen schützen Informationen (z.B. durch Verschlüsselung oder Signierung). Die Informationen sind geschützt, bis Unbefugte den zugehörigen Schlüssel herausfinden. Heute gängige Methoden sind sicher, weil es mathematisch berechenbar viel zu lange dauern würde, den Schlüssel durch Ausprobieren (Brute Force Methode) herauszufinden. Zukünftige technologische Möglichkeiten könnten aktuelle Verfahren unsicher machen und eine Anpassung der SSI-Lösung erfordern (z.B. die Migration zu Post-Quanten-Kryptografie⁹³). Dies sollte im Voraus beachtet werden und ist vor allem bei einem Blockchain-Ansatz fürs VDR relevant. Ein Upgrade der Blockchain-Software ist je nach Ausprägung nicht einfach möglich, da die Mehrheit der Netzwerk-Teilnehmenden das Upgrade akzeptieren müssen[86].

2.9.4 Wallet

Die Abstimmung zum E-ID-Gesetz und der darauf folgende Diskurs in der Bevölkerung haben gezeigt, dass eine nationale Lösung wichtig ist. Gemäss einer Nachwahlbefragung haben die meisten Personen das Gesetz wegen der Rolle von Privaten abgelehnt[87]. Um den Erwartungen der Schweizer Bevölkerung gerecht zu werden und möglicher Ablehnung entgegenzuwirken, ist eine eigene nationale Wallet App empfehlenswert. Herausgeberin sollte die Bundesverwaltung sein – der visuelle Auftritt entsprechend gewählt werden. Mit der Swiss Covid Cert App kennt die Bevölkerung bereits eine Schweizer⁹⁴ Lösung zur lokalen Speicherung eines Zertifikats.

⁹²Beispiel BSI: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102.pdf?__blob=publicationFile

⁹³vgl. Empfehlungen des BSI: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Krypto/Post-Quanten-Kryptografie.pdf?__blob=publicationFile&v=2

⁹⁴Die Swiss Covid Cert App wurde durch das BIT herausgegeben.

Kapitel

3 Praktischer Teil

Leseführerung: Im praktischen Teil wird die Umsetzung des Proof of Concept dokumentiert. Der Anwendungsfall der Ausbildungsgutschrift wird im Abschnitt 3.1 mit der Ausgangslage und dem Zielbild beschrieben. Die Technologienwahl für den PoC ist in Abschnitt 3.2 beschrieben.

Abschnitt 3.3 gibt eine Übersicht der Umsetzung. Daraufhin werden im Abschnitt 3.4 die Systemarchitektur und die technischen Komponenten im Detail beschrieben. Im Anschluss werden die wichtigsten Interaktionen (Abschnitt 3.5) im SSI-Ökosystem erläutert.

Nachfolgend werden Schwierigkeiten (Abschnitt 3.6), die während der Umsetzung aufgetreten sind und mögliche Erweiterungen (Abschnitt 3.7) der Lösung aufgezeigt. Abschliessend wird im Abschnitt 3.8 ein Fazit gezogen.

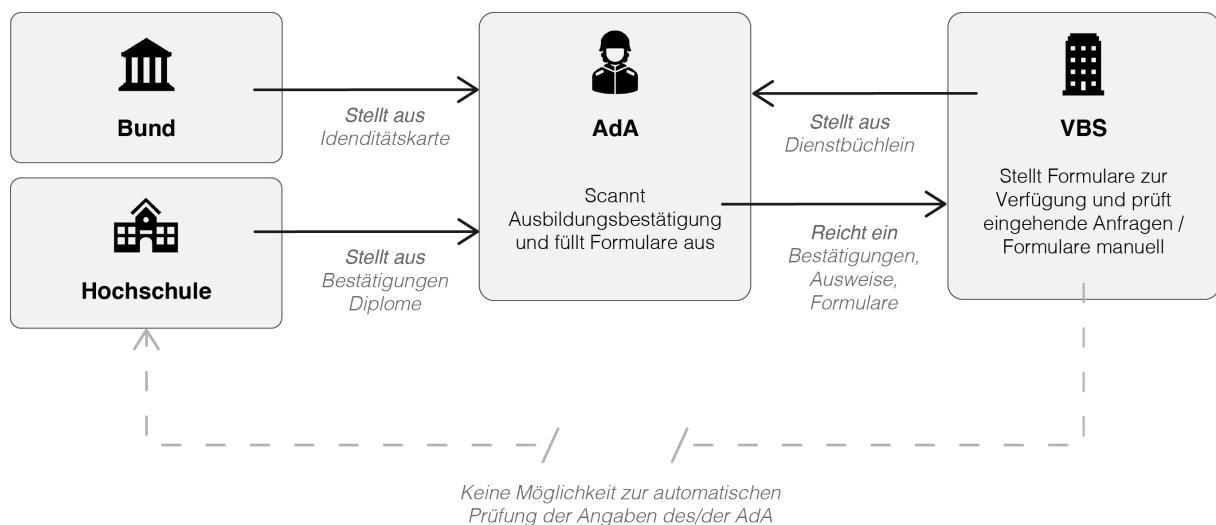
3.1 Anwendungsfall

Die Schweizerische Armee möchte ambitionierte AdA dazu animieren, nach der Rekrutenschule zusätzliche militärische Weiterbildungen zu absolvieren und so in höhere Militärgrade aufzusteigen. Zu diesem Zweck macht die Armee den AdA ein Angebot: Erreicht ein AdA gewisse militärische Grade, bezahlt die Armee dem AdA einen finanziellen Beitrag an zivile Ausbildungen. Je nach Höhe der militärischen Gradkategorie können diese Ausbildungsgutschriften bis zu 11'300.- CHF betragen⁹⁵.

3.1.1 Ausgangslage

Der Prozess von der Erreichung des entsprechenden militärischen Grades bis hin zur Auszahlung der Ausbildungsgutschrift zieht sich heute über einen längeren Zeitraum hinweg. Zudem ist der Prozess gezeichnet von vielen manuellen Schritten durch verschiedene Stellen der Armee, der zivilen Ausbildungsinstitution (z.B. Hochschule) und der/des AdA.

Abbildung 3.1 zeigt den prozeduralen Ablauf einer Anfrage im heutigen (manuellen) System. Der analoge Austausch verschiedener Dokumente und Formulare setzt voraus, dass die unterschiedlichen Akteure sich gegenseitig vertrauen. Eine unabhängige und vor allem automatisierte Prüfung ist nicht möglich. Der Prozess ist sowohl für die/den AdA wie auch die Armee nicht zufriedenstellend[88].



3.1.2 Zielbild

Die Schaffung einer SSI-Infrastruktur für die E-ID eröffnet auch den Bundesämtern und anderen Institutionen neue Möglichkeiten. Abbildung 3.2 illustriert wie der Use-Case «Ausbildungsgutschrift» in einem solchen System ablaufen könnte.

Initial registrieren alle Parteien ihre eigene DID (und das zugehörige DID-Dokument) auf dem VDR. Die staatliche Stelle «Bund» stellt der/dem AdA VCs zur Identifikation als Schweizer Bürgerin, Bürger aus. Die Hochschule wiederum stellt der/dem AdA Ausbildungsbestätigungen als VCs aus. Sowohl Bund als auch Hochschule signieren die VCs mit ihrem privaten Schlüssel. Der/die AdA speichert diese VCs bei sich im digitalen Wallet.

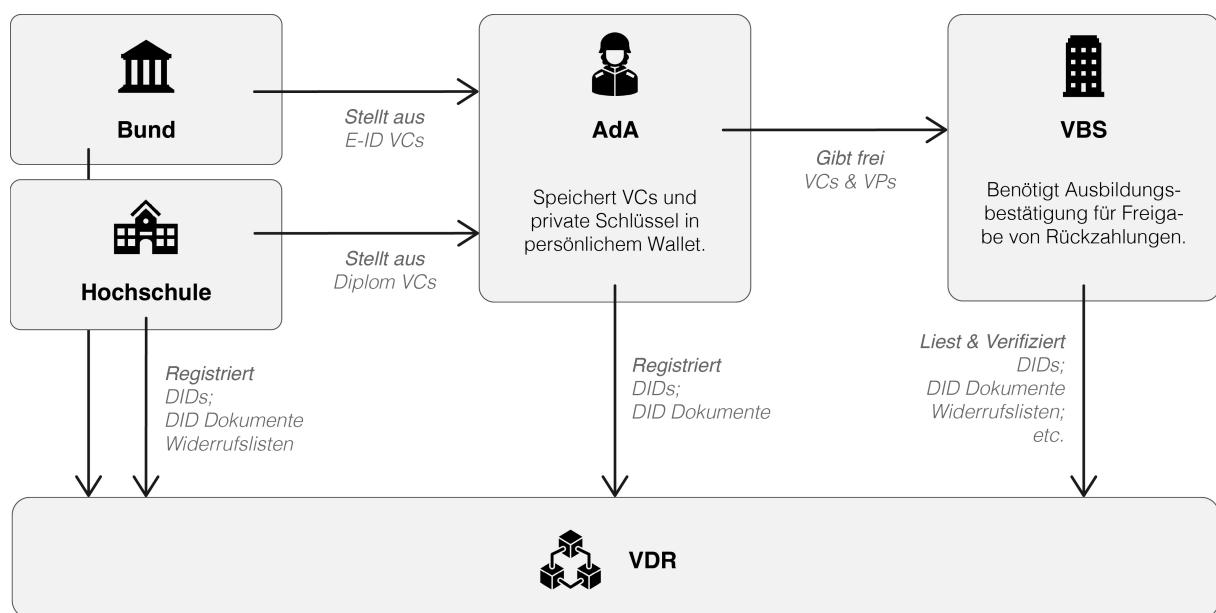


Abbildung 3.2: Überblick SSI Use-Case VBS mit E-ID — Unterschiedliche Entitäten stellen VCs aus. So erhält der/die AdA VCs für die E-ID und eine Ausbildung an einer Hochschule. Diese VCs speichert die/der AdA im eigenen Wallet und gibt entsprechende VCs bzw. VPs an das VBS weiter.

Statt Formulare auszufüllen, Dokumente zu scannen und dem VBS zur Verfügung zu stellen, kann die/der AdA im SSI-System VPs erstellen, die ihre/seine Ausbildung bestätigen. Diese stellt sie/er dem VBS zur Verfügung. Das VBS wiederum kann dank den öffentlichen Schlüsseln auf dem VDR und den digitalen Signaturen in den VPs den Anspruch automatisiert prüfen und das Geld sofort freigeben.

3.2 Evaluation Technologien

Basierend auf der Evaluation im Abschnitt 2.8 soll das VDR auf einer Public Permissioned Blockchain aufbauen. Zum Zeitpunkt dieser Arbeit steht das BIT bezüglich einer Umsetzung des nationalen SSI-Ökosystems noch in der Planungsphase. Deshalb kann keine bestehende Komponente der Bundesverwaltung verwendet werden. Stattdessen muss das SSI-Ökosystem für den Anwendungsfall isoliert aufgebaut werden. In Abschnitt 3.2.1 werden Kriterien zur Evaluierung möglicher Technologien für die Umsetzung des Anwendungsfalls definiert. In den darauffolgenden Abschnitten werden unterschiedliche Lösungen evaluiert.

3.2.1 Kriterien

Nachfolgende Kriterien beziehen sich auf den Proof of Concept des im Abschnitt 3.1 definierten Anwendungsfalls. Tabelle 3.1 listet die Kriterien und deren Gewichtung auf.

- 3 – Muss: Zwingend zur erfüllen Kriterium.
- 2 – Soll: Zu erfüllen wenn dadurch kein Muss-Kriterium nicht mehr erfüllt ist.
- 1 – Kann: Optionales, aber wünschenswertes Kriterium.

Kriterium	Gewichtung	Beschreibung
SSI-Komponenten	3 – Muss	Alle SSI-Komponenten (Verifier, Issuer, Wallet) sind verfügbar/implementierbar.
Lizenzenfrei		Die nötigen Komponenten für den PoC des Anwendungsfalls sind lizenzenfrei nutzbar.
Unterstützung von Standards	2 – Soll	Etablierte Standards wie die Credentials von W3C werden unterstützt.
Aktive Entwicklung		Die Lösung wird aktiv weiterentwickelt bzw. Abhängigkeiten aktuell gehalten.
Dokumentation	1 – Kann	Die Lösung ist gut dokumentiert und/oder es gibt eine aktive Gemeinschaft für Fragen.
Eigene Nodes		Eigene Knoten für das Netzwerk können gestellt werden.
Public Permissioned Blockchain	1 – Kann	Die Lösung erlaubt die Nutzung einer Public Permissioned Blockchain als VDR.
Open-Source		Der Quellcode der Technologie ist Open-Source.
Wissen im Team		Eingesetzte Sprachen und/oder Tools sind dem Entwicklungsteam bekannt.

Tabelle 3.1: Übersicht der Kriterien und entsprechender Gewichtung zur Evaluierung möglicher Technologien für die Umsetzung des PoC für den Anwendungsfall «Ausbildungsgutschrift».

3.2.2 Technologien

Zur Eingrenzung möglicher Technologien wurde eine Voranalyse durchgeführt. Bemerkungen bzw. Einschätzungen zu den Technologien sind in Anhang A.2 zu finden. Die vielversprechendsten Technologien für die Erfüllung der definierten Kriterien werden nachfolgend im Detail analysiert und bewertet.

In der initialen Vorauswahl wurden auch Hyperledger Indy und die Lösung BC-Gov als möglicherweise vielversprechend eingestuft. Für Hyperledger Indy wird als VDR ein eigenes Netzwerk aufgebaut und die Interaktion läuft über das Protokoll Hyperledger Aries[89]. Beide Aspekte müssen konfiguriert und umgesetzt werden, was aufgrund der limitierten zeitlichen Ressourcen neben der Umsetzung des Anwendungsfalls als nicht realistisch eingestuft wurde. Auch BC-Gov⁹⁶ macht einen vielversprechenden Eindruck – allerdings ist die Dokumentation veraltet (tote Links). Aus genannten Gründen wurden diese beiden Lösungen in der engeren Auswahl nicht mehr berücksichtigt.

3.2.2.1 Jolocom

Allgemein — Jolocom bietet eine in Typescript geschriebene Open-Source SDK («Jolocom SDK») zur Implementierung unterschiedlicher Akteure im SSI-Ökosystem an. Das VDR wurde bewusst Technologie-Agnostisch aber explizit DLT- bzw. Blockchain-kompatibel gehalten. Auf der Website wird angegeben, dass verschiedene Blockchains getestet werden und eine Verwendung von EBSI angestrebt wird[90].

DID-Methode — Jolocom stellt eine eigene DID-Methode («did:jolo:») zur Verfügung. Die Standard-Implementierung schreibt auf Rinkeby (Ethereum Testnetzwerk). Jolocom verfügt über einen Smart Contract, der die DID und IPFS-Hash zum DID-Dokument speichert. Aus Kostenüberlegungen werden keine weiteren Daten auf der Blockchain gespeichert[91][92].

Wallet — Digital Wallet für iOS und Android-Geräte steht zur Verfügung («Jolocom Smart-Wallet»)[93].

Standards — Wurde für DSGVO-, eIDAS und eSSIF-Konformität gebaut und hält sich an W3C-Standards. VC's werden unterstützt, VP's noch nicht — soll aber noch folgen[90][94].

3.2.2.2 Veramo

Allgemein — Veramo ist eine Javascript Library für verifiable Data. Die Library entstammt wie Serto.id⁹⁷ von uPort und ist noch in der Beta-Phase. Die Library ist gut dokumentiert und aktiv in Weiterentwicklung[95].

DID-Methode — Veramo bietet keine eigene DID-Methode an. Die Library bietet aktuell folgende DID-Methoden an: «did:ether:», «did:web:» und «did:key:»⁹⁸.

Wallet — Veramo bietet aktuell kein eigenes Wallet an. Eine Kompatibilität mit anderen bestehenden Wallets müsste geprüft werden.

Standards — Veramo arbeitet für die Einhaltung und Etablierung von Standards eng mit der W3C und der Decentralized Identity Foundation (DIF) zusammen. Die Library unterstützt die oben erwähnten DID-Methoden – weitere Methoden müssen über einen Fork selbst implementiert werden. Neben Ethereum sind damit keine weitere Blockchain-Lösungen direkt unterstützt[95].

⁹⁶Aktuelle Anwendung von BC-Gov vgl. Abschnitt 2.5.10 auf Seite 20

⁹⁷vgl. Anhang A.2

⁹⁸Weitere Infromationen zu den angebotenen Methoden: https://veramo.io/docs/veramo_agent/did_methods/

3.2.2.3 Evernym

Allgemein — Evernym ist eine im 2013 gegründete SSI-Plattform und damit schon lange auf dem Markt. Mit über 1000 Organisationen auf der Plattform wirkt sie sehr ausgereift. Evernym hat Code für das Sovrin Netzwerk gespendet und mitgeholfen, die Plattform zu etablieren. Dies wiederum führte zur Gründung von Hyperledger Indy. Im Gegensatz zu Jolocom speichert Evernym auch die DID-Dokumente auf dem VDR. Evernym bietet SDKs für Java, Python und Node.js und ist gut dokumentiert[96][97].

Standards Unterstützt aktuell nur das Sovrin Netzwerk - weitere Plattformen mit W3C-Standard sind geplant[96][97].

DID-Methode — Everny verwendet heute die DID-Methode von Sovrin «did:sov»[96].

Wallet — Eine Wallet ist auf Android und iOS verfügbar («Connect.Me»). Auf die Wallet SDK für eine eigene Implementierung einer Wallet-App ist nur mit bezahlten Plänen zugänglich[98].

3.2.3 Entscheid

Die drei in diesem Kapitel vorgestellten Technologien erfüllen die definierten Kriterien für den Proof of Concept. Bei Evernym gilt es die Abhängigkeit zu Sovrin zu beachten. Sovrin wurde nicht in die engere Auswahl aufgenommen⁹⁹ und Evernym deshalb nicht weiterverfolgt. Jolocom und Veramo wird hinsichtlich der definierten Kriterien als gleichwertig bewertet. Jolocom ist mit einem ansprechenden Wallet für iOS und Android, guter Dokumentation, einer eigenen DID-Methode und Beispielen positiv herausgestochen. Zudem wird Jolocom in Deutschland mit Fokus auf den europäischen Markt entwickelt. Diese Punkte waren ausschlaggebend für den Entscheid, eine Implementierung mit Jolocom anzustreben.

Entscheid

Von den drei Favoriten aus der Vorauswahl (Siehe Anhang A.2) erfüllen sowohl Jolocom als auch Veramo die im Abschnitt 3.2.1 definierten Kriterien für die Umsetzung. Jolocom wird vom Projektteam präferiert. Die Umsetzung des Proof of Concepts wird mit Jolocom durchgeführt.

⁹⁹vgl. Anhang A.2

3.3 Übersicht des umgesetzten Ökosystems

Ziel des praktischen Teils ist die Umsetzung eines Proof of Concept des definierten Zielbilds im Abschnitt 3.1.2. Der Fokus liegt auf dem VBS, welches die Ausbildungsgutschrift anhand digitaler Zertifikate der/des AdA verifiziert und selbst digitale Zertifikate (z.B. für den Militärgrad) ausstellt. Da es noch kein bestehendes SSI-Ökosystem für die Schweizer E-ID gibt, wurden alle Teilnehmende des Zielbilds umgesetzt.

Abbildung 3.3 zeigt die Anwendungslandschaft des Proof of Concepts. Ein Service «SSI Credential Generator» wurde umgesetzt, um die für die Validierung der Ausbildungsgutschrift benötigten digitalen Zertifikate der FHNW und des Bundes auszustellen. Die/der AdA als Besitzer/in verwendet die bestehende Jolocom SmartWallet, die für Android und iOS als App zur Verfügung steht. Im «myArmy Portal» kann sich die/der AdA den benötigten digitalen Zertifikate für den Militärgrad ausstellen lassen und eine Anfrage für eine mögliche Ausbildungsgutschrift an das VBS stellen.

Im Abschnitt 3.4 auf der nächsten Seite wird die Systemarchitektur detaillierter dargestellt und die einzelnen Komponenten technisch beschrieben.

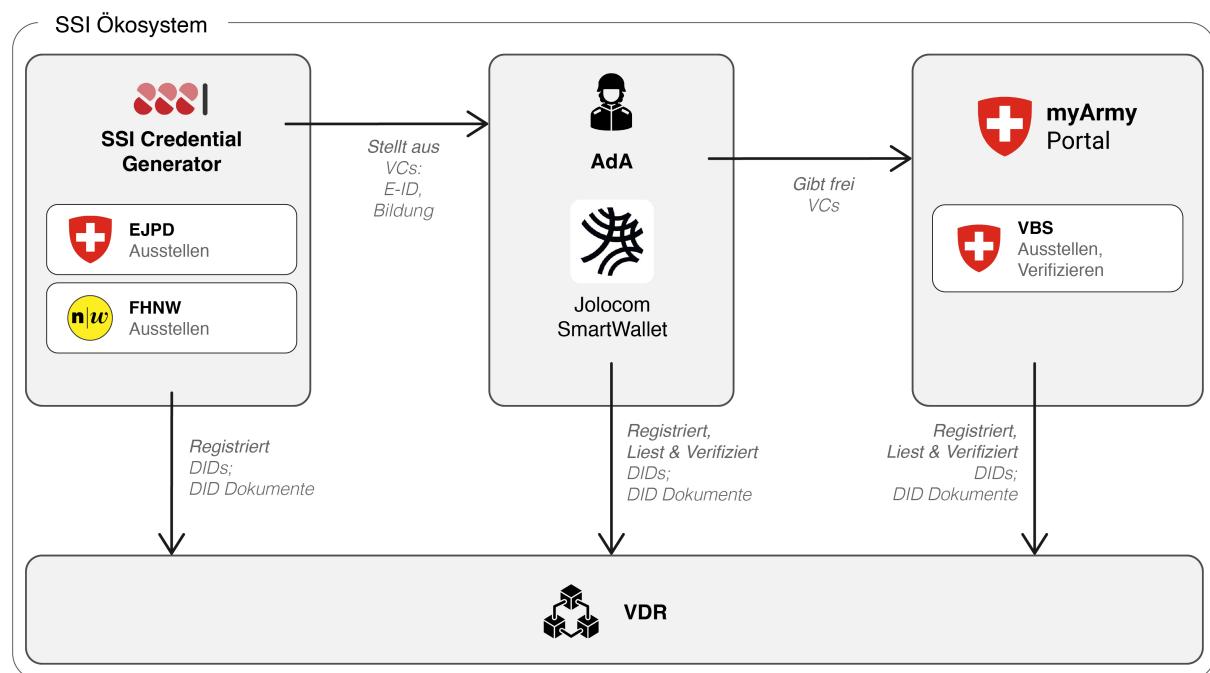


Abbildung 3.3: Anwendungslandschaft des Proof of Concepts: «SSI Credential Generator» zum Ausstellen der E-ID und Ausbildungsbestätigung der FHNW, «myArmy Portal» zum Ausstellen von Militärgrad-Zertifikaten bzw. Anfordern von Ausbildungsgutschriften, VDR und persönlichem SmartWallet der/des AdA.

3.4 Systemarchitektur

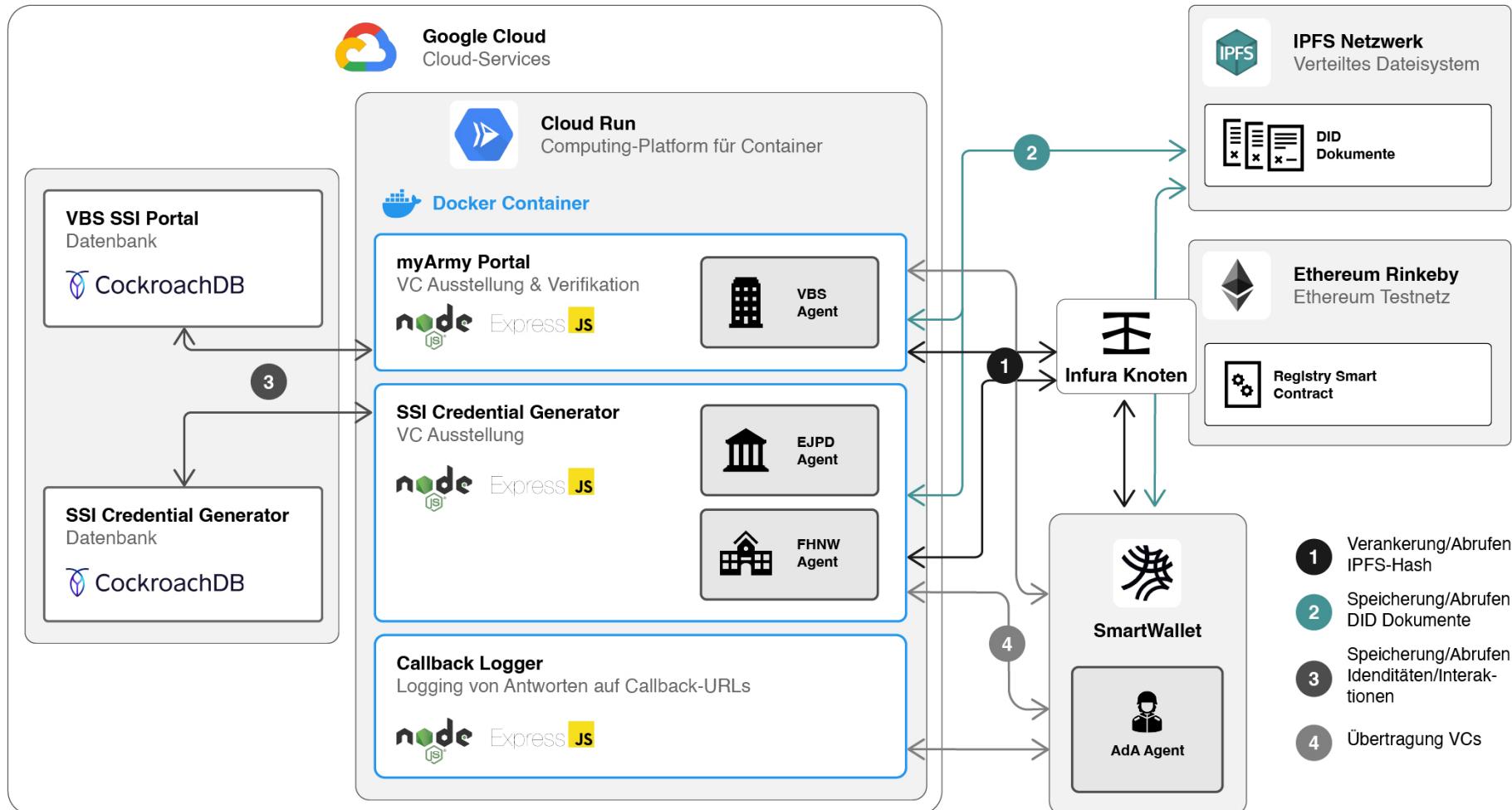


Abbildung 3.4: Architektur SSI-Ökosystem für PoC: Jolocom SmartWallet (iOS/Android) mit entsprechendem Jolocom Agent, zwei Portale (in Docker Container auf Google Cloud Run) die wiederum Agents zur Ausstellung und Verifikation von VCs enthalten, ein Infura-Knoten für den Zugriff auf Rinkeby und das IPFS-Netzwerk zur Speicherung der DID-Dokumente.

3.4.1 Google Cloud Run

Google bietet mit ihrem Service «Cloud Run» eine serverlose Plattform an und ermöglicht ein einfaches Deployment der containerisierten Anwendungen, ohne eine eigene Infrastruktur aufzubauen und zu verwalten. Die umgesetzten Anwendungen des PoCs verwenden eine Cloud Build Konfiguration, um das Docker Image zu bauen, in die Container Registry hochzuladen und einen Container auf Google Cloud Run zu deployen¹⁰⁰.

3.4.2 CockroachDB

Jede, Jeder Teilnehmende benötigt im Jolocom-Framework ein Speichermedium um Daten (DID-Dokumente, Schlüsselpaare, Verifiable Credentials etc.) zu speichern, die während unterschiedlichen Interaktionen gesammelt oder generiert wurden. Das Jolocom-Framework unterstützt diverse Speichermedien, solange das bereitgestellte Interface `IStorage`¹⁰¹ implementiert wird.

Die Jolocom SmartWallet speichert ihre Daten auf dem lokalen Speicher des Gerätes[90]. Als Speicher für die weiteren Teilnehmenden (FHNW, EJPD und VBS) wurde CockroachDB¹⁰² verwendet. Für die Anwendungen wurde jeweils ein Cluster erstellt, welcher in der Google Cloud läuft. CockroachDB wurde gewählt, da die Datenbank für den PoC kostenlos betrieben werden kann und die Google Cloud unterstützt wird.

3.4.3 InterPlanetary File System

DID-Dokumente von Jolocom werden auf dem verteilten Dateisystem IPFS gespeichert. Für die Interaktion mit IPFS verwendet Jolocom einen eigenen IPFS Gateway (`ipfs.jolocom.com`).

IPFS behandelt gespeicherte Daten wie ein Cache, wodurch nicht garantiert wird, dass die Daten weiterhin gespeichert werden. Um ein Verlust der Daten zu verhindern, werden die gespeicherten Daten von Jolocom standardmäßig gepinnt[99]. Dieser Pinn-Mechanismus verhindert, dass wichtige Dateien automatisch aus dem Speicher entfernt werden¹⁰³.

3.4.4 Ethereum Rinkeby

Jolocom verwendet neben IPFS das Ethereum Rinkeby Testnet als Vertrauensebene für die DID-Methode «did:jolo». Testnets bieten Entwickler/innen die Möglichkeit, die Ethereum Blockchain auszutesten bevor auf das Mainnet von Ethereum deployed wird. Rinkeby verwendet den Proof of Authority (PoA) Konsensmechanismus «Clique» und fällt in die Ausprägung Public Permisioned Blockchain¹⁰⁴.

3.4.4.1 Registry Contract

Die Jolocom DID-Methode verwendet einen Smart Contract für das Mapping einer DID auf eine IPFS Hash-Adresse. Dadurch können auf IPFS gespeicherte DID-Dokument mit einer DID adressiert werden[91]. Die Verwendung des Smart Contracts für die Registrierung und Auflösung einer DID ist im Abschnitt 3.5 beschrieben. Der Registrar und der Resolver können mit einem

¹⁰⁰Informationen zum Cloud Build Deployment: <https://cloud.google.com/build/docs/deploying-builds/deploy-cloud-run>

¹⁰¹IStorage Interface: https://jolocom.github.io/jolocom-sdk/1.0.0/api/interfaces/_src_storage_index_.istorage.html

¹⁰²Informationen zu CockroachDB: <https://www.cockroachlabs.com/>

¹⁰³Informationen zum Pinn-Mechanismus: <https://docs.ipfs.tech/how-to/pin-files>

¹⁰⁴Informationen zum Clique PoA: <https://eips.ethereum.org/EIPS/eip-225>

eigenen Smart Contract konfiguriert werden. Standardmässig und auch im PoC wird der Registry Smart Contract¹⁰⁵ von Jolocom verwendet.

3.4.5 SSI Credential Generator

Der «SSI Credential Generator» ist eine Webanwendung, die mit dem Node.js-Framework Express umgesetzt wurde. Das Frontend wird serverseitig mittels Templating und der View Engine Embedded Javascript (EJS) bereitgestellt. Als CSS-Framework wurde Bootstrap 5 verwendet. Die Kommunikation zwischen Client und Server läuft synchron über eine REST-Schnittstelle. Die Endpunkte wurden mit der OpenAPI Spezifikation dokumentiert und über ein Swagger-UI bereitgestellt.

Für die Integration von Jolocom wurde das Jolocom SDK verwendet, die als SSI-Agent Factory fungiert. Ein Agent repräsentiert einen Teilnehmenden des SSI-Ökosystems mit einer DID. Die SDK selbst verwendet die Jolocom Library und abstrahiert einen Teil der Komplexität. Für gewisse Funktionalität (z.B. Ausstellen von öffentlichen Profilen) muss trotzdem auf die Jolocom-Lib zurückgegriffen werden.

Der «SSI Credential Generator» stellt zwei Agents für das EJPD und die FHNW zur Verfügung. Die Agents werden nach ihrer Erstellung in CockroachDB gespeichert und können später wieder daraus geladen werden. Für die Agents wird zudem ein öffentliches Profil erstellt, welches dem DID-Dokument angehängt wird. Das öffentliche Profil ist ein selbstausgestelltes VC, welches die DID identifiziert und z.B. in der Jolocom SmartWallet angezeigt wird. Abbildung 3.5 zeigt den Startbildschirm des «SSI Credential Generators» mit den zwei Agents. Nach der Auswahl eines Agents erscheint eine Übersichtsseite der Ausstellerin, des Ausstellers (Abbildung Abbildung 3.6 auf der nächsten Seite). Die Seite enthält Informationen wie das öffentliche Profil und die angebotenen Zertifikate zum Ausstellen. Wie das Ausstellen eines Credentials funktioniert, wird im Abschnitt 3.5.3 auf Seite 58 erläutert.

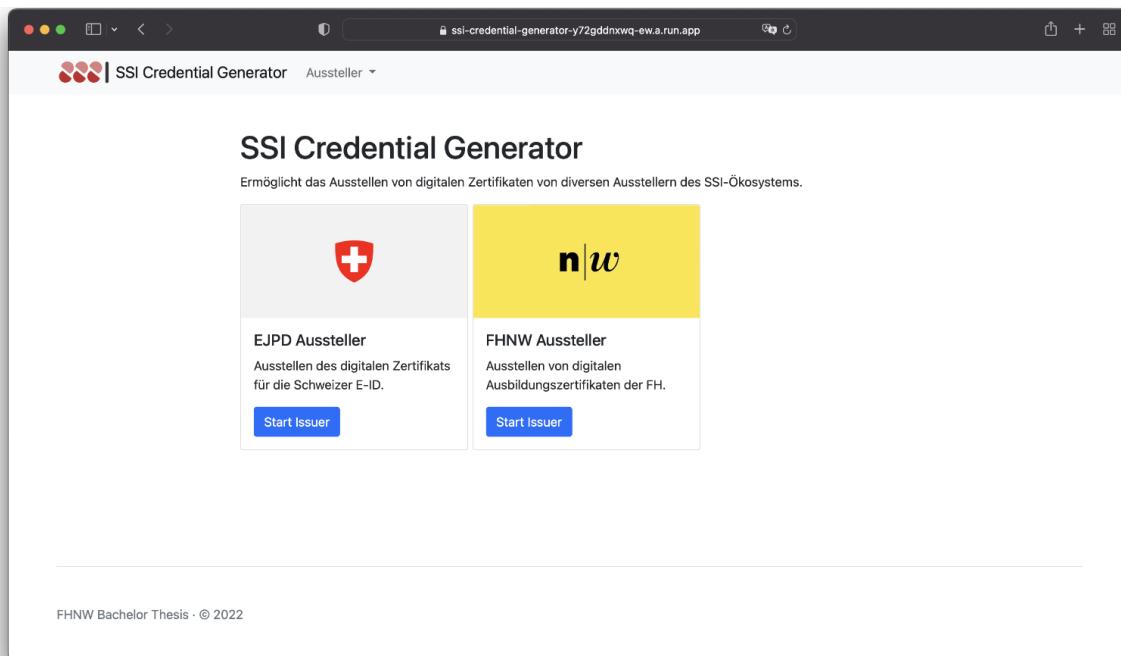


Abbildung 3.5: Startseite der umgesetzten Webanwendung «SSI Credential Generator».

¹⁰⁵Jolocom Smart Contract: <https://rinkeby.etherscan.io/address/0xd4351c3f383d79ba378ed1875275b1e7b960f120>

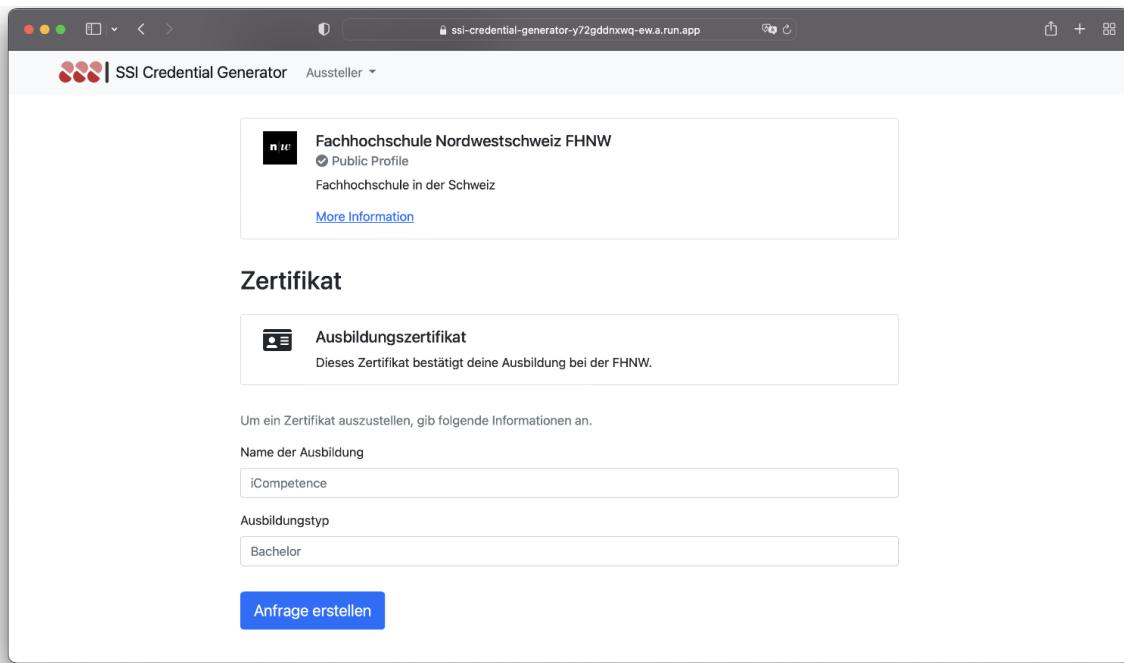


Abbildung 3.6: Seite zum Ausstellen eines Ausbildungszertifikat der FHNW in der Anwendung «SSI Credential Generator».

3.4.6 myArmy Portal

Das «myArmy Portal» ist eine mit dem Node.js-Framework Express umgesetzte Webanwendung und technologisch gleich aufgebaut wie der «SSI Credential Generator». Es gibt einen Agent für das VBS, der digitale Zertifikate ausstellt und verifiziert. Beide Interaktionen sind im Abschnitt 3.5 auf Seite 56 genauer beschrieben.

Die Webanwendung wurde visuell im Stil der Schweizer Armee umgesetzt. Der Prototyp wurde mit dem Tool Figma erstellt und befindet sich im Anhang A.4.

Abbildung 3.7 auf der nächsten Seite zeigt ein Prozessschritt für das Anfordern einer Ausbildungsgutschrift: Die/der AdA muss bestätigen, im Besitz aller relevanten Zertifikate zu sein. Nach der Bestätigung wird wie in Abbildung 3.8 auf der nächsten Seite dargestellt ein QR-Code angezeigt, den die/der AdA mit der SmartWallet App scannen kann. Daraufhin werden die nötigen Zertifikate zur Prüfung übermittelt.

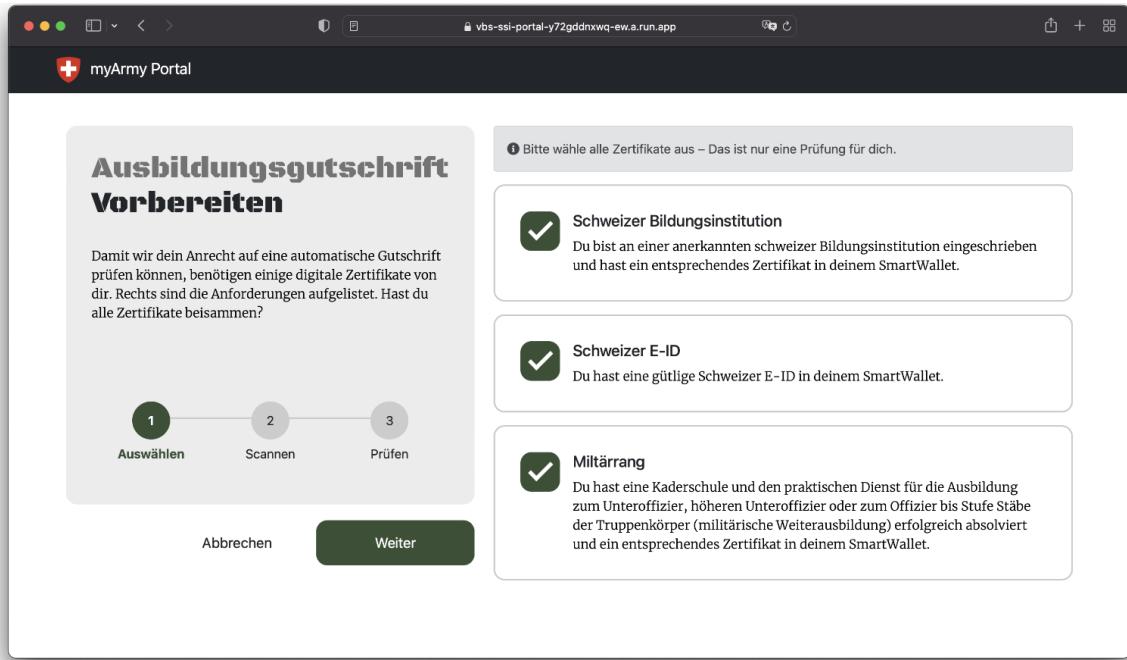


Abbildung 3.7: Seite mit Auflistung der nötigen digitalen Zertifikaten im Ausbildungsgutschrift-Prozess im «myArmy Portal».

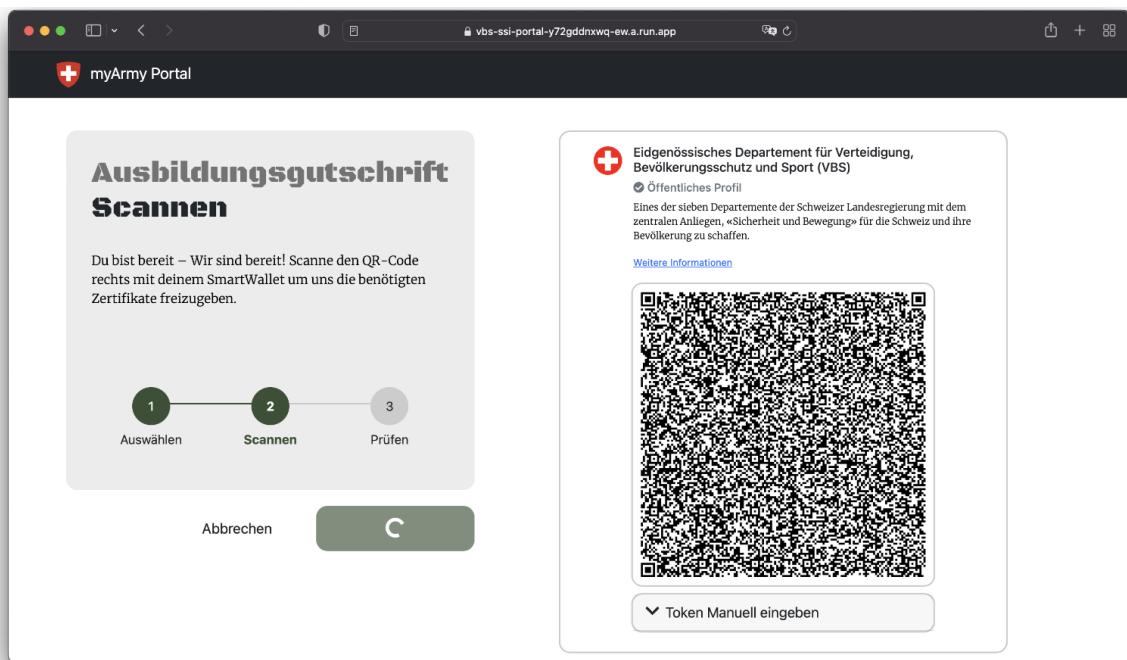


Abbildung 3.8: Seite mit QR-Code zur Anforderung der nötigen Zertifikate für die Ausbildungsgutschrift im «myArmy Portal».

3.4.7 Jolocom SmartWallet

Jolocom stellt eine eigene Wallet zur Verfügung, die von der/dem AdA für den Proof of Concept verwendet wird. Die Jolocom SmartWallet ermöglicht das Verwalten und Teilen von digitalen Zertifikaten. Die React Native App ist Open-Source und auf Android und iOS verfügbar[100].

3.4.8 Callback Logger

Bei der Interaktion (Kapitel 3.5) zum Ausstellen und Verifizieren von Credentials wird eine Callback-URL angegeben. Die Callback-URL wird verwendet, um z.B. ein Credential zu akzeptieren und erhalten. Dieser Austausch funktioniert mit der Jolocom SmartWallet nur über eine öffentliche HTTPS-Adresse, wofür die Anwendungen veröffentlicht werden müssen. Um im Entwicklungsprozess effizienter zu sein, wurde eine REST-Schnittstelle mit dem Node.js-Framework Express umgesetzt, welche die Antwort des Jolocom SmartWallets loggt. Die Antwort kann anschliessend in der lokalen Entwicklungsumgebung weiterverwendet werden. Der Service «Callback Logger» ist nicht produktionsrelevant.

3.5 Interaktionen

Nachfolgend werden die wichtigsten Interaktionen im umgesetzten PoC erklärt.

3.5.1 Registrierung einer DID

Die Art der Erstellung und Verankerung einer DID wird durch die gewählte DID-Methode definiert. In der Jolocom SDK wird standardmäßig die DID-Methode «did:jolo:» verwendet. Die SDK ist so konzipiert, dass auch andere DID-Methoden (z.B. «did:ebsi:») verwendet werden könnten. In der Implementierung des PoCs wurde die Standard-Methode («did:jolo:») verwendet [90][101].

Jolocom bietet bei der Registrierung einer neuen DID zudem die Publizierung eines öffentlichen Profils an. Das öffentliche Profil kann Name, Beschreibung, URL und ein Bild enthalten. Es kann von allen anderen Entitäten abgerufen und angezeigt werden. Diese Funktion ist DID-Methoden-Spezifisch – neue Methoden können das Interface `publishPublicProfile` ebenfalls implementieren. Die Veröffentlichung erfolgt auf IPFS.

Erstellung und Verankerung mit der Jolocom DID-Methode («did:jolo:») erfolgt in vier Schritten und wird in Abbildung 3.9 auf der nächsten Seite illustriert:

1. Erzeuge DID
 - (a) Registrar (in diesem Fall «did:jolo:»): Erstelle neue Schlüsselpaare für die Signierung, Verschlüsselung und Verankerung.
 - (b) Speichere private Schlüssel lokal im SmartWallet.
 - (c) Nimm öffentlichen Schlüssel des Signierungs-Paares
 - (d) Erzeuge keccak256-Hash¹⁰⁶ von Schlüssel
 - (e) Füge «did:jolo:» als Präfix hinzu
2. Erzeuge, publiziere (und pinne¹⁰⁷) DID-Dokument mit DID und öffentlichen Schlüsseln (+ ggf. Öffentliches Profil) in IPFS.
3. IPFS liefert Hash auf publiziertes DID-Dokument zurück.
4. Erzeuge, signiere und verteile Transaktion zur Verankerung des IPFS-Hashs
 - Während des Prozesses wird die Ethereum-Adresse¹⁰⁸ mit Ether befüllt.
 - Zur Verankerung wird `.setRecord()` mit DID und IPFS-Hash als Parameter auf dem Registry Smart Contract aufgerufen
 - `setRecord` ist eine Schreib-Methode und verursacht Transaktionskosten auf der Blockchain
 - Zugriff auf Blockchain erfolgt via Infura-Knoten (<https://rinkeby.infura.io/v3/64fa85ca0b28483ea90919a83630d5d8>)

Hinweis

Jolocom speichert das DID-Dokument auf IPFS und verankert nur den IPFS-Hash auf der Blockchain. Theoretisch könnte auch das DID-Dokument direkt auf der Blockchain gespeichert werden. Als Grund für das Vorgehen nennt Jolocom die hohen Kosten^a.

^avgl. Abschnitt 3.2.2.1 auf Seite 47

¹⁰⁶Weitere Informationen zu keccak256: <https://keccak.team/keccak.html>

¹⁰⁷IPFS-Pinning: <https://docs.ipfs.tech/concepts/persistence/#persistence-versus-permanence>

¹⁰⁸Wird aus öffentlichem Verankerungsschlüssel erzeugt, welcher neben dem Schlüssel für Signaturen und Verschlüsselung separat erzeugt wird

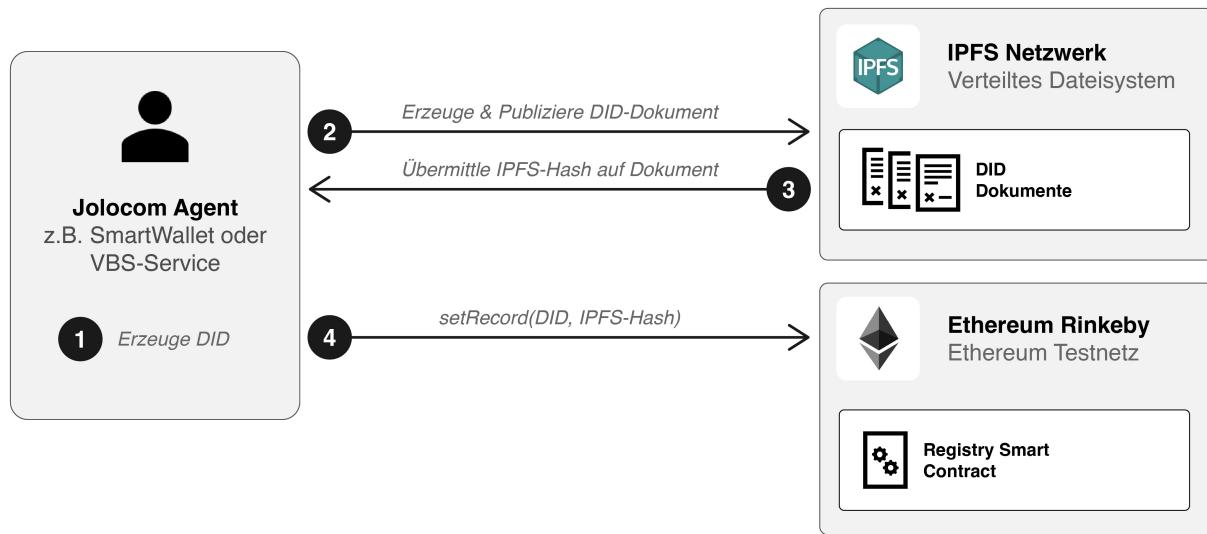


Abbildung 3.9: Interaktion zwischen einem Jolocom Agent (Person oder Service), dem IPFS-Netzwerk und dem Registry Smart Contract auf Ethereum Rinkeby. Der Jolocom Agent erzeugt eine neue DID mit den zugehörigen Schlüsselpaaren und generiert daraus ein DID-Dokument, das anschliessend auf IPFS gespeichert und im Smart Contract (als IPFS-Hash) referenziert/verankert wird.

3.5.2 Auflösung einer DID

Die Art der Auflösung einer DID (bzw. deren DID-Dokument) wird durch die gewählte DID-Methode definiert. Wie im Abschnitt 3.5.1 beschrieben, wurde in der Implementierung des PoCs die Standard-Methode («did:jolo:») verwendet[90][101].

Auflösung einer DID mit der Jolocom DID-Methode («did:jolo:») erfolgt in vier Schritten und wird in Abbildung 3.10 auf der nächsten Seite illustriert:

1. Rufe `.getRecord()` mit DID als Parameter auf Registry Smart Contract¹⁰⁹ auf.
 - Zugriff auf Blockchain erfolgt via Infura-Knoten (<https://rinkeby.infura.io/v3/64fa85ca0b28483ea90919a83630d5d8>)
 - `getRecord` ist eine read-only (View)-Methode und verursacht keine Transaktionskosten auf der Blockchain
2. Smart Contract gibt IPFS-Hash zurück, falls diese DID im Contract-eigenen Mapping enthalten ist.
3. Lade DID-Dokument aus IPFS
 - Verwendet eigenes Jolocom IPFS-Gateway (<https://ipfs.jolocom.com:443>)
4. IPFS liefert DID-Dokument zurück

¹⁰⁹vgl. Abschnitt 3.4.4.1 auf Seite 51

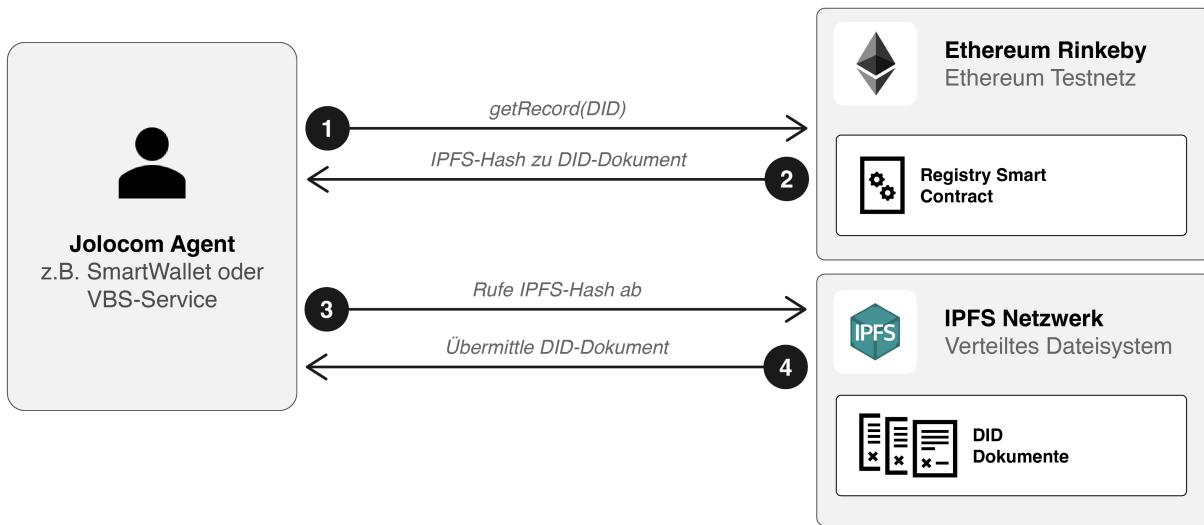


Abbildung 3.10: Interaktion zwischen einem Jolocom Agent (Person oder Service), dem IPFS-Netzwerk und dem Registry Smart Contract auf Ethereum Rinkeby. Der Jolocom Agent ruft auf dem Registry Smart Contract den IPFS-Hash zum DID-Dokument einer DID ab und löst anschliessend den IPFS-Hash auf, um das DID-Dokument zu laden.

3.5.3 Credential ausstellen

Der Prozess zum Ausstellen von Verifiable Credentials involviert eine ausstellende und empfängende Partei. Der Austausch der Daten findet via sogenannte JSON Web Token (JWT) statt. JWTs bestehen aus einem Header, Payload (Credentials) und der Signatur[102][103]. Ein Beispiel eines JWTs dieser Interaktion ist im Anhang A.5 zu finden.

Das Ausstellen von Verifiable Credentials erfolgt in sechs Schritten und wird in Abbildung 3.11 auf der nächsten Seite illustriert:

1. [Aussteller/in] Erstelle und übermittle Credential Offer Token JWT
 - Credential-Typ
 - Claim-Typen
 - Claims
 - Callback-URL
 - Ablaufdatum
 - Signatur (Aussteller/in)
2. [Empfänger/in] Verarbeite JWT (Offer akzeptieren / ablehnen).
 - (a) Validiere Signatur (via DID-Dokument Aussteller/in).
 - (b) Validiere Ablaufdatum.
 - (c) Validiere Audienz (Empfänger/in).
3. [Empfänger/in] Übermittle Antwort an Callback-Adresse.
4. [Aussteller/in] Verarbeite JWT-Antwort.
 - (a) Validiere Signatur (via DID-Dokument Empfänger/in).
 - (b) Validiere Ablaufdatum.
 - (c) Validiere Audienz (Aussteller/in).
 - (d) Validiere ob alle ausgewählten Credentials vorher angeboten wurden.
5. [Aussteller/in] Erstelle und übermittle Credential Issuance Token JWT basierend auf Offer.
 - Credential-Typ
 - Claim-Typen

- Signierte Claims (mit Subjekt)
 - Callback-URL
 - Ablaufdatum
 - Signatur (Aussteller/in)
 - Audienz (Empfänger/in)
6. [Empfänger/in] Verarbeite JWT (Credentials speichern).
- Validiere Signatur (via DID-Dokument Aussteller/in).
 - Validiere Ablaufdatum.
 - Validiere Audienz (Empfänger/in).
 - Validiere, ob alle und nur ausgewählte Credentials ausgestellt wurden.
 - Validiere, ob Aussteller/in und Subjekt mit Informationen aus Offer übereinstimmen.

Hinweis: Audienz und Subjekt müssen nicht dieselben natürlichen oder juristischen Personen sein: So kann z.B. eine Mutter (Audienz/Empfängerin) ein VC für ihren Sohn (Subjekt) anfordern/empfangen.

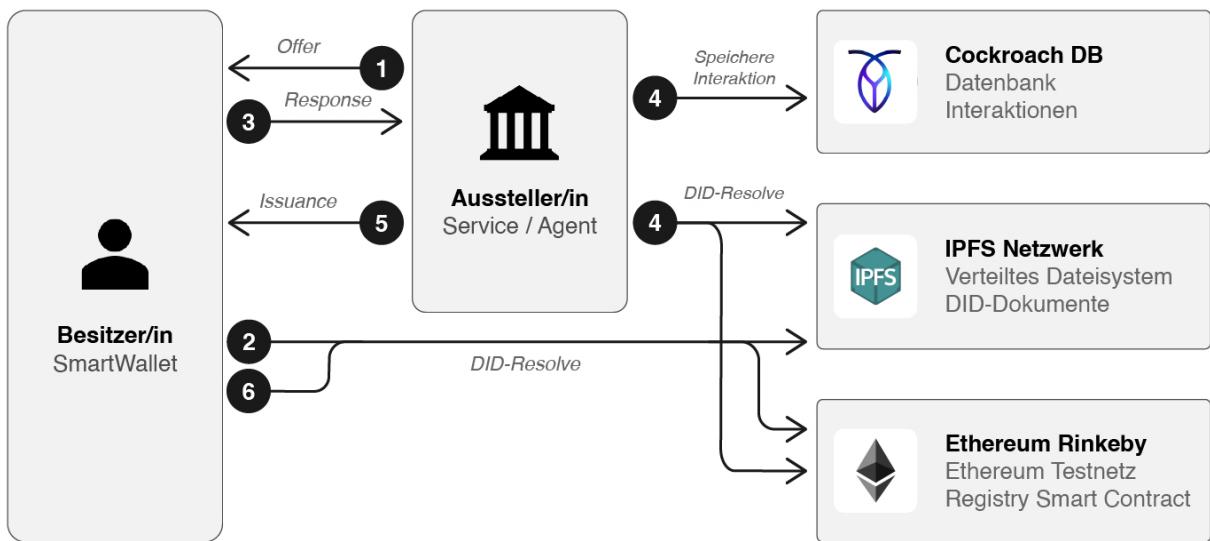


Abbildung 3.11: Interaktion zwischen zwei Jolocom-Agents (Besitzer/in und Aussteller/in von Credentials) sowie Datenbank, IPFS-Netzwerk und Ethereum Smart Contract. Die Ausstellerin, der Aussteller erzeugt eine Token Offer, die von der Besitzerin, dem Besitzer akzeptiert oder abgelehnt werden kann. Bei einer Annahme der Offer stellt die Ausstellerin, der Aussteller die entsprechenden Credentials aus. Beide Parteien greifen jeweils auf IPFS und Ethereum zu, um DID-Dokumente zur Validierung der Signaturen zu laden (DID-Resolve). Die Ausstellerin, der Aussteller persistiert die Interaktion in der Datenbank.

3.5.4 Credential verifizieren

Der Prozess zum Anfordern und Verifizieren von VCs involviert die Besitzerin, den Besitzer und die Verifiziererin, den Verifizierer der VCs. Der Austausch der Daten findet via JSON Web Token (JWT)s statt. Ein Beispiel eines JWTs dieser Interaktion ist im Anhang A.6 zu finden.

Das Verifizieren von Verifiable Credentials erfolgt in vier Schritten und wird in Abbildung 3.12 auf der nächsten Seite illustriert:

- [Verifizierer/in] Erstelle und übermittle Credential Request Token JWT.
 - Angeforderte Credential-Typen
 - Einschränkungen / Anforderungen an Claims (z.B. «Alter grösser als x»)

- Zugelassene Ausssteller/innen für Credentials (DIDs)
 - Callback-URL
 - Ablaufzeitpunkt (Standard-Gültigkeit: 1 Stunde)
 - Signatur (Verifizierer/in)
2. [Besitzer/in] Verarbeite JWT.
 3. [Besitzer/in] Erstelle und übermittle Credential Response Token JWT.
 - Callback-URL
 - Signierte VCs
 - Verifizierer/in (Audienz)
 - Nonce (Identisch mit Nonce aus Credential Request)
 - Ablaufzeitpunkt (Standard-Gültigkeit: 1 Stunde)
 - Signatur (Besitzer/in)
 4. [Verifizierer/in] Verarbeite JWT.
 - (a) Prüfe, ob ein Credential Request offen ist.
 - (b) Validiere Signatur (via DID-Dokument Besitzer/in).
 - (c) Validiere Ablaufdatum.
 - (d) Validiere Audienz (Verifizierer/in).
 - (e) Für jedes übermittelte VC: Prüfe ob Einschränkungen / Anforderungen erfüllt.

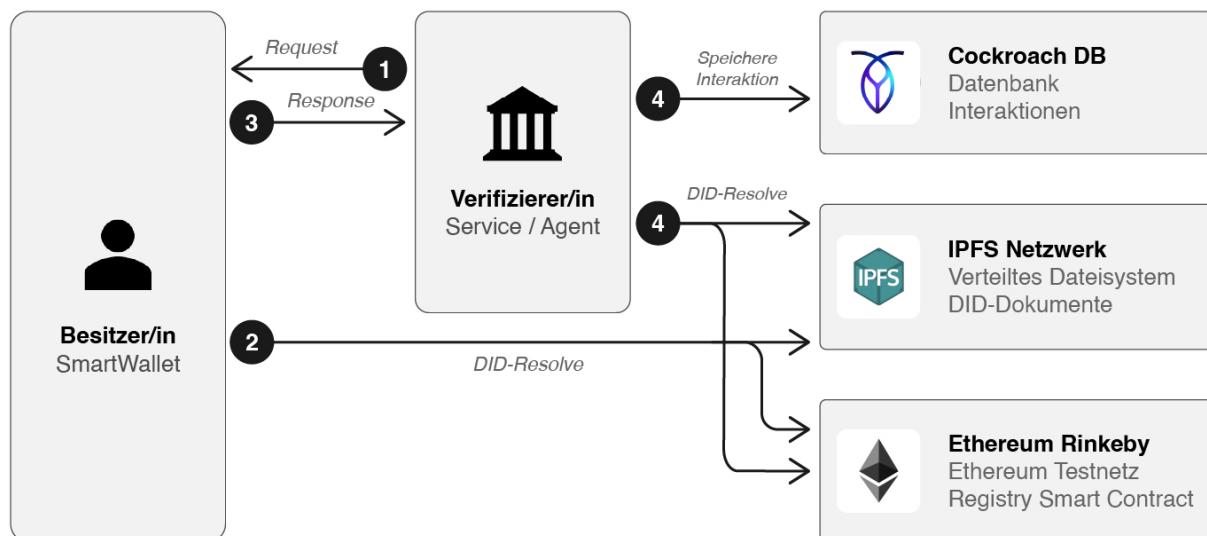


Abbildung 3.12: Interaktion zwischen zwei Jolocom-Agents (Besitzer/in und Verifizierer/in von Credentials) sowie Datenbank, IPFS-Netzwerk und Ethereum Smart Contract. Die Verifiziererin, der Verifizierer erzeugt ein Credential Request Token, der von der Besitzerin, dem Besitzer beantwortet werden kann (Übermittlung der angeforderten Credentials). Beide Parteien greifen jeweils auf IPFS und Ethereum zu, um DID-Dokumente zur Validierung der Signaturen zu laden (DID-Resolve). Die Verifiziererin, der Verifizierer persistiert die Interaktion in der Datenbank.

Hinweis zur Validierung

Die Jolocom SDK validiert die Einschränkungen / Anforderungen zwar, ein Fehlschlagen der Validierung hat aber keine Konsequenzen. Weitere Informationen im Abschnitt 3.6 auf der nächsten Seite.

3.6 Schwierigkeiten

Folgender Abschnitt geht auf Schwierigkeiten ein, die während der Umsetzung mit dem Jolocom Framework aufgetreten sind.

3.6.1 Dokumentation

Die Dokumentationen der Jolocom SDK und Jolocom Library eignen sich für den Einstieg sehr gut. Sie geben eine gute Einführung zu SSI. Der Aufbau eines Ökosystems und die Interaktionen sind verständlich anhand von Beispielen erklärt.

Allerdings bleibt die Dokumentation oberflächlich. Genaue Erklärungen was im Hintergrund geschieht, sowie eine Spezifikation welche Parameter in welcher Form übermittelt werden müssen, fehlen.

Um Fehler zu beheben musste deshalb oft manuell rekonstruiert werden, welche Methoden im Hintergrund aufgerufen werden, was diese genau ausführen und welche Parameter erwartet werden.

3.6.2 Source Code des Framework

Der Source Code ist teilweise intuitiv verständlich, enthält sinnvolle Kommentare und ist durchdacht. In gewissen Bereichen sind aber Mängel aufgefallen.

Veralteter Code Gewisse Methoden wurden als «deprecated» (= Veraltet) gekennzeichnet, ohne dabei eine Alternative anzugeben. Die entsprechenden neuen Methoden müssen manuell gesucht werden.

Beispiel: Die Methode `Agent.signedCredential` der Jolocom SDK.

Verletzlichkeiten Einige Abhängigkeiten in der Jolocom SDK, werden als potenzielles Sicherheitsrisiko eingestuft. Von den 17 Verletzlichkeiten stuft der Javascript-Paketmanager «npm» 14 als schwach/moderat, 1 als hoch und 2 als kritisch ein.

Auf GitHub¹¹⁰ hat Jolocom dazu zuletzt im September 2021 geschrieben, dass an einer Version 2 gearbeitet werde, die diese Verletzlichkeiten beheben soll. Seit diesem Zeitpunkt gibt es kein Update mehr.

Unfertige Komponenten Während der Umsetzung sind einige Code-Stellen aufgefallen, die noch unfertig wirken. Dies betrifft nur einen kleinen Teil des Frameworks - der Grossteil ist gut dokumentiert und getestet. Aufgefallen ist dies vor allem bei der Interaktion zum Anfordern von Credentials. Das Jolocom Framework ermöglicht bei der Anforderung die Angabe sogenannter Constraints (Bedingungen), die die Credentials erfüllen müssen.

Constraints werden zwar im Prozess validiert, das Resultat der Validierung wird allerdings nicht gespeichert bzw. weiterverwendet. Teilweise wird auf diesen Umstand mit TODOs (Dinge zu erledigen) hingewiesen, wie im Code-Ausschnitt 1 ersichtlich ist.

¹¹⁰vgl. <https://github.com/jolocom/jolocom-sdk/issues/126>

```

async _processToken(token, fromStorage = false) {
    // [...] Code weggelassen wegen Lesbarkeit
    try {
        // > TODO what happens if the signer isnt resolvable
        const requester = await this.ctx.ctx.resolve(token.signer.did);
        // [...]
    } catch (err) { console.error('error resolving requester', err); }
    // [...]
    const onMessage = async (msg) => {
        // > TODO throw on failure? processInteractionToken returns bool
        await this.ctx.ctx.processJWT(msg);
    };
    // [...]
    // > TODO if handling fails, should we still be pushing the token??
    const res = await this.flow.handleInteractionToken(...);
    // [...]
    return res;
}

```

Code-Ausschnitt 1: Diverse TODOs sind z.B. in der Funktion Interaction._processToken() offen, die unter anderem beim Anfordern von Credentials aufgerufen wird.

Für den PoC ist es wichtig, dass der/dem AdA mitgeteilt werden kann, ob die Bedingungen für eine Ausbildungsgutschrift erfüllt sind. Aus diesem Grund werden die Constraints in unserer Implementierung durch den VBS-Agent erneut geprüft und das Ergebnis anschliessend gespeichert. Code-Ausschnitt 2 zeigt die entsprechende Implementierung.

```

verifyAusbildungsgutschriftCredentials = async (requestId, credentialReponseToken) => {
    // [...] Code weggelassen wegen Lesbarkeit
    const interaction = await this.agent.processJWT(credentialReponseToken);

    // Check for constraint satisfaction is already done by SDK on processJWT
    // but they don't return the validation result
    const providedCredentials = getProvidedCredentials(interaction);
    > const constraintsSatisfied = providedCredentials.satisfiesRequest(...);

    // check if provided credentials are valid
    if (!constraintsSatisfied ...) {
        request.status = STATUS.DENIED;
        // [...]
        return;
    }

    request.status = STATUS.APPROVED;
    // [...]
};

```

Code-Ausschnitt 2: Ausschnitt aus der Funktion VBS-Agent.verifyAusbildungsgutschriftCredentials() des «myArmy Portals». Die Funktion Agent.processJWT() (Jolocom SDK) ruft intern bereits CredentialRequest.satisfiesRequest() auf. Da keine Fehlermeldung oder Resultat zurückgeliefert wird, muss die Funktion nochmals aufgerufen werden.

3.6.3 Fehlersuche mit Jolocom SmartWallet

Tritt ein Fehler auf, zeigt die Jolocom SmartWallet App oft nur eine generelle bzw. nicht aussagekräftige Fehlermeldung. Um Probleme bzw. deren Ursache zu verstehen, musste teilweise der Quellcode von der SmartWallet und des Jolocom Frameworks analysiert werden. In Kombination mit der wie oben beschrieben Problematik bzgl. Dokumentation, war das Finden von Fehlern sehr zeitintensiv.

Beispiel: Beim Scannen des QR-Codes zur Validierung der Ausbildungsgutschrift wurde folgende Fehlermeldung angezeigt:

Hoppla ... Damit haben wir auch nicht gerechnet. Bitte helfen Sie uns, indem Sie uns den Fehler mitteilen, auf den Sie gestoßen sind.

In den Beispielen der Dokumentation (siehe Code-Ausschnitt 3) wird beim Ausstellen und Anfordern von Zertifikaten nur ein Zertifikatstyp angegeben. In der Definition der Constraints wird zudem nur der Attributname angegeben. Die Wallet konnte das Token so bei der Zertifikatsanfrage nicht verarbeiten.

```
import { JolocomLib } from '@jolocom/sdk'

const aliceCredRequest = await alice.credRequestToken({
  callbackURL: 'https://example.com/request',
  credentialRequirements: [
    {
      type: ['SimpleExampleCredential'],
      constraints: [
        JolocomLib.util.constraintFunctions.greater('age', 18),
        JolocomLib.util.constraintFunctions.is('name', 'Bob'),
      ],
    },
  ],
})
```

Code-Ausschnitt 3: Code-Beispiel aus der Jolocom SDK-Dokumentation, wie ein Credential verifiziert werden kann. https://jolocom.github.io/jolocom-sdk/1.0.0/guides/interaction_flaws/#credential-verification

Es stellte sich heraus, dass beim Ausstellen und Anfordern von Zertifikaten ein zusätzlicher Typ angegeben werden muss und die Constraints den Präfix `claim.` erfordern (siehe Code-Ausschnitt 4).

```

const qualifiedForPaymentCredRequest = await this.agent.credRequestToken({
  callbackURL: `${callbackURL}/${requestId}`,
  credentialRequirements: [
    {
      type: [>'VerifiableCredential', 'SwissMilitaryRankCert'],
      constraints: [
        JolocomLib.util.constraintFunctions.greater(>'claim.level', 0),
        JolocomLib.util.constraintFunctions.is('issuer', process.env.AGENT_DID),
      ],
    },
    // [...] Weitere Constraints
  ],
});

```

Code-Ausschnitt 4: Umgesetzter Code des Request-Tokens zur Validierung der Ausbildungsgutschrift. Abweichende Stellen zur Dokumentation sind markiert.

Es besteht die Möglichkeit, die Jolocom SmartWallet zu Debugging-Zwecken lokal zu installieren. Trotz Bemühungen konnte die App auf den Geräten der Autoren aufgrund Kompatibilitätsproblemen nicht installiert werden.

3.6.4 Jolocom Fueling Service

Wie im Abschnitt 3.5.1 beschrieben, werden bei der Registrierung einer DID mit der DID-Methode «did:jolo» die erstellten ETH-Adressen mit ETH befüllt¹¹¹. Nur so kann eine kostenpflichtige Schreib-Methoden auf dem Smart Contract aufgerufen werden. Das sogenannte Fueling wird von einem Service von Jolocom ausgeführt – was zu einer Abhängigkeit führt. Fällt dieser Service aus oder hat selbst kein ETH-Guthaben mehr, so werden die erstellten Ethereum-Adressen nicht mehr automatisch befüllt und können keine DIDs mehr verankern. Diese Situation ist während der Umsetzung mehrmals eingetreten, wurde jedoch innerhalb von einigen Tagen behoben.

Eine Option wäre die ETH-Adresse des Agent auszulesen und selbst mit ETH zu befüllen. Folgender Ansatz aus dem Internet lieferte jedoch eine ungültige ETH-Adresse:

```

const { publicKeyHex } = await agent.keyProvider.getPubKeyByController(
  password, `${agent.keyProvider.id}#keys-2`);
const ethPublicKey = `0x${publicKeyHex}`;

```

Code-Ausschnitt 5: Ansatz zum Auslesen der ETH-Adresse eines Agents gemäss User chunningham auf <https://gitter.im/jolocom/jolocom-sdk>

Generell ist zu hinterfragen, wie Jolocom diesen Prozess auf dem Hauptnetz von Ethereum umsetzen würde. Im Hauptnetz entstehen effektive Kosten für Transaktionen, die Jolocom vermutlich nicht tragen wird.

¹¹¹Ethereum-Adresse wird Ether (ETH) gutgeschrieben, das zum Bezahlen innerhalb des Testnetzwerks verwendet werden kann.

3.7 Erweiterungen

Dieser Abschnitt zeigt mögliche Erweiterungen für nachfolgende Iterationen und Ansatzpunkte für weiterführende Untersuchungen auf.

3.7.1 Zertifikate widerrufen

Ausgestellte VCs werden lokal auf den Geräten der Besitzerinnen und Besitzer gespeichert. Zentrale Instanzen wie z.B. Behörden haben entsprechend keine Möglichkeit, bereits ausgestellte Zertifikate zu widerrufen. In gewissen Fällen ist das aber nötig¹¹².

Beispiel: Ein/e AdA wird gemäss Artikel 22a des Militärgesetz (MG) infolge eines Strafurteils degradiert. Die aktuelle Implementierung lässt in diesem Fall kein Widerrufen des bereits ausgestellten Militärgrad-VCs zu.

Es gibt Konzepte, um bereits ausgestellte Credentials zu widerrufen. So können zum Beispiel «Widerrufslisten» auf der Blockchain (in Smart Contracts) geführt werden. Widerrufslisten könnten von Certificate Authority (CA) – bzw. durch von CA berechtigte Ausstellerinnen, Aussteller geführt werden[9, S. 83].

3.7.2 Wiederherstellung

Die Jolocom SDK bietet zwei Ansätze, eine Identität (bzw. einen Agent) wiederherzustellen:

- Die Identität aus dem Speicher (der Datenbank) wiederherstellen. Dazu muss das bei der Erstellung verwendete Passwort bekannt und der Eintrag in der Datenbank vorhanden sein.
- Die Identität deterministisch mit einem Mnemonic¹¹³ wiederherstellen. Dazu muss bei der Erstellung bereits diese Methode gewählt worden und das Mnemonic noch bekannt sein.

In der aktuellen Implementierung werden die Agents aus dem Speicher geladen. Wird der Speicher gelöscht oder das Passwort vergessen, hat z.B. das VBS keinen Zugriff mehr auf ihren Agent. Eben so wichtig ist die Wiederherstellung einer Identität für den/die AdA. Diese Thematik sollte deshalb weiter untersucht werden.

3.7.3 Eigene Infrastruktur

Die verwendete DID-Methode («did:jolo:») verwendet für die Verankerung des IPFS-Hashes das Rinkeby-Testnetz. Für eine produktive Implementierung gilt es folgende Punkte zu beachten:

- Aktuell werden die Ethereum-Adressen durch den Jolocom Fueling Service¹¹⁴ mit ETH versorgt. Was ist wenn der Service nicht funktioniert?
- Das Rinkeby-Testnetz wird Ende 2023 abgeschaltet[104].
- Die Verwendung eines Netzes wie Ethereum verursacht Transaktionskosten – Wer übernimmt diese?
- Der Betrieb eines eigenen Public Permissioned Netzwerks sollte geprüft werden.

¹¹²vgl. Abschnitt 2.7.3.4 und Abschnitt 2.7.3.5 auf Seite 28

¹¹³Weitere Infos zu Mnemonics: <https://0-100.io/glossar/mnemonics>

¹¹⁴vgl. Abschnitt 3.6.4

Die Jolocom SDK ist DID-Methoden-agnostisch gehalten. Jolocom plant wie im Abschnitt 3.2.2.1 beschrieben die Anbindung der DID-Methode der EBSI. Erste Analysen des Codes zeigen, dass andere DID-Methoden möglicherweise mit wenig Aufwand implementiert bzw. integriert werden könnten. VBS und BIT streben bereits eine eigene Lösung an¹¹⁵. Entsprechend sind weitere Anstrengungen/Untersuchungen zum Aufbau eines eigenen (Public Permissioned Blockchain) Netzwerks und einer eigenen DID-Methode (Registrar/Resolver) zu unternehmen.

3.7.4 Unterstützung von Verifiable Presentations

Im Sinne der Datensparsamkeit sollten VPs¹¹⁶ unterstützt werden. So könnte die/der AdA lediglich die für den Beweis für die Ausbildungsgutschrift relevanten Angaben erbringen – ohne den kompletten Inhalt ganzer VCs zu teilen.

Das Jolocom Framework bietet aktuell keine Möglichkeit, aus einem oder mehreren VCs ein VP zu erzeugen[94]. Einzelne Behauptungen/Attribute müssten als separate VCs ausgestellt werden, damit sie isoliert geteilt werden können. Es sollten Möglichkeiten untersucht bzw. implementiert werden, die das Erstellen von VPs ermöglichen.

3.7.5 Trusted Lists

Auch im SSI-Umfeld sind einige Instanzen darauf angewiesen, gewissen Entitäten besondere Rechte einzuräumen.

Beispiel: Nicht alle Ausbildungen werden für die Ausbildungsgutschrift von der Schweizerischen Armee akzeptiert.

In der aktuellen Implementierung wurde eine Liste mit DIDs zugelassener Institutionen direkt im Code verankert. Diese Lösung ist für einen produktiven Betrieb nicht sinnvoll. Stattdessen könnten Trusted List (TL) eingeführt werden, die auf dem VDR gespeichert werden. Die Einführung von TL oder andere Möglichkeiten sollten weiter untersucht werden.

3.7.6 Integration an VBS-Anwendungen

Im umgesetzten PoC bezieht das «myArmy Portal» keine Daten von der bestehenden Infrastruktur des VBS.

Für eine produktive Implementierung könnte folgendes Szenario evaluiert werden: Die/Der AdA könnte sich initial im Portal anmelden (z.B. mit der E-ID). Dadurch können Angaben wie z.B. der Militärgrad von einem VBS-System bezogen und als VC ausgestellt werden.

Die Anbindung an VBS-Kernsysteme sowie erwähnter Vorgang zum Anmelden auf dem Portal sollte analysiert werden.

¹¹⁵vgl. Anhang A.1

¹¹⁶vgl. Abschnitt 2.4.5 auf Seite 14

3.8 Fazit

Der definierte Anwendungsfall (Abschnitt 3.1) konnte erfolgreich mit einem Proof of Concept umgesetzt werden. Das VBS übernimmt im SSI-Ökosystem die Rolle als verifizierende und ausstellende Entität von VCs. Der Prozess der Ausbildungsgutschrift konnte mit SSI digitalisiert und automatisiert werden.

Jolocom Framework Das gewählte Framework von Jolocom hat sich als guter Einstieg mit einfacher Handhabung erwiesen. Alle geplanten Komponenten des Zielbilds (Abschnitt 3.1.2) konnten mit dem Framework umgesetzt werden. Eine Ausnahme sind VPs, die initial in der Implementierung vorgesehen waren. Aufgrund der fehlenden Unterstützung durch Jolocom wurde deren Einsatz für den PoC exkludiert.

Trotz des insgesamt guten Eindrucks gilt es einige Einschränkungen zu beachten. Abschnitt 3.6 zeigt auf, dass der Quellcode in gewissen Bereichen überarbeitet bzw. weiterentwickelt werden muss, damit das Framework produktiv eingesetzt werden kann. Jolocom schreibt dazu auf Github dass an einer Version 2 gearbeitet wird – ohne Termine zu nennen.

Der Aufbau und die Informationen der Website (<https://jolocom.io>) legen die Vermutung nahe, dass Jolocom den Fokus vor allem in die Zusammenarbeit mit europäischen Initiativen (z.B. EBSI, eSSIF) zur Schaffung von SSI-Ökosystemen – und weniger in die Weiterentwicklung der eigenen SDK legt. Die SDK könnte dabei als «Werbung» verstanden werden um aufzuzeigen, was mit SSI möglich ist. Für diese Argumentation spricht auch, dass sich die Deutsche Regierung während der Implementierung dieses PoCs entschieden hat, Jolocom Fördergelder für einen Test-Case zur Deutschen eID zur Verfügung zu stellen[105].

Es ist wichtig anzumerken, dass es sich bei der umgesetzten Lösung um einen Proof of Concept handelt und sich diese in der vorliegenden Form nicht für einen produktiven Betrieb eignet. Es gibt diverse Punkte aus den vorherigen Abschnitten 3.6 und 3.7, die zuerst analysiert und bearbeitet werden müssten.

4 Schlussbemerkungen

4.1 Blockchain als VDR

Fazit Unter Einbezug definierter Szenarien (vgl. Abschnitt 2.6) wurden verschiedene Ansätze untersucht. Die Evaluation kam zum Ergebnis, dass sich eine Blockchain-basierte VDR-Lösung für ein Schweizer SSI-System eignet. Die definierten Anforderungen (vgl. Abschnitt 2.7) können mit einer Public Blockchain-Lösung erfüllt werden. Von den untersuchten Blockchain-Ausprägungen eignet sich Public Permissioned am besten (vgl. Abschnitt 2.8.5).

Weiterführende Untersuchungen Verschiedene Aspekte einer Umsetzung des VDRs mit Blockchain-Technologien können erst nach Vorliegen einer konkreten Architektur detailliert analysiert werden. So sind z.B. die Kosten und die Performance stark von verschiedenen Faktoren abhängig (vgl. Abschnitt 2.8.3.9 und 2.8.3.6). Diese Punkte könnten in weiterführenden Untersuchungen konkreter Technologien und/oder Frameworks detailliert beleuchtet werden.

Empfehlungen Neben der Bestimmung konkreter Technologien sind in der Schweiz (und auch international) noch Fragen der Governance zu klären. Zu Architektur, Etablierung von Standards/Governance, Sicherheit und dem Wallet hält Abschnitt 2.9 konkrete Empfehlungen fest.

Ausblick Das Etablieren von SSI zeichnet einen Paradigmenwechsel im Identitätsmanagement. Die Roadmap sieht 2023 noch Pilotprojekte bei der Bundesverwaltung und ein Aufbau des gesamten Ökosystems bis 2025 vor.

4.2 SSI-Ökosystem mit Jolocom

Fazit Für den PoC zum Use-Case «Ausbildungsgutschrift» (vgl. Abschnitt 3.1) wurden verschiedene Frameworks evaluiert (vgl. Abschnitt 3.2) und schliesslich ein SSI-Ökosystem mit dem Framework Jolocom erfolgreich umgesetzt (vgl. Abschnitt 3.8).

Im Vergleich zum heutigen Prozess ist der automatisierte Ablauf sowohl für AdAs, wie auch für das VBS effizienter:

- AdAs können selbständig und zeitunabhängig digitale Zertifikate ausstellen.
- AdAs können zeitunabhängig und digital eine Ausbildungsgutschrift beantragen.
- Anträge auf Ausbildungsgutschriften können automatisch und digital geprüft und abgewickelt werden. Die Durchlaufzeit reduziert sich damit von Wochen auf Minuten (ausgenommen Auszahlung des Geldes).

Erweiterungen und nächste Schritte Der umgesetzte PoC zeigt, dass ein SSI-Ökosystem basierend auf Jolocom aufgebaut werden kann. Abschnitt 3.6 dokumentiert Schwierigkeiten/-Probleme, die während der Umsetzung des PoCs aufgetreten und für eine Weiterentwicklung relevant sind. Abschnitt 3.7 fasst mögliche nächste Schritte bzw. Erweiterungen zusammen.

Ausblick SSI kann im Rahmen der Vision «Armee 2030» bei der Digitalisierung der Miliz und der Schaffung eines Bürgerportals des VBS einen wichtigen Beitrag leisten und sollte weiterverfolgt werden. Wird das Framework Jolocom aktuell gehalten, kann es vom BIT als möglichen Ansatz für die Schweizer E-ID evaluiert werden.

Quellenverzeichnis

- [1] P. S. Stefan Luber. „Was ist ein Brute-Force-Angriff?“ (2018), [Online]. Adresse: <https://www.security-insider.de/was-ist-ein-brute-force-angriff-a-677192/>. (Aufgerufen: 08.07.2022).
- [2] C. A. et. al. „Decentralized Public Key Infrastructure“. (2015), [Online]. Adresse: <https://danubetech.com/download/dpki.pdf?ref=hackernoon.com>. (Aufgerufen: 08.07.2022).
- [3] A. Mühle, A. Grüner, T. Gayvoronskaya und C. Meinel, „A survey on essential components of a self-sovereign identity“, *Computer Science Review*, S. 80–86, 2018. [Online]. Adresse: <https://www.sciencedirect.com/science/article/pii/S1574013718301217>.
- [4] M. Shuaib, N. H. Hassan, S. Usman *et al.*, „Self-Sovereign Identity Solution for Blockchain-Based Land Registry System: A Comparison“, *Mobile Information Systems*, 2022. [Online]. Adresse: <https://doi.org/10.1155/2022/8930472>.
- [5] C. Allen. „The Path to Self-Sovereign Identity“. (2016), [Online]. Adresse: <http://www.lifewithalacrity.com/2016/04/the-path-to-self-sovereign-identity.html>. (Aufgerufen: 15.03.2022).
- [6] N. Z. Razieh, C. K. Chih, H. Teng-Chieh *et al.*, „Blockchain-Based Self-Sovereign Identity: Survey, Requirements, Use-Cases and Comparative Study“, 2021. [Online]. Adresse: <https://doi.org/10.1145/3486622.3493917>.
- [7] D. van Bokkem, R. Hageman, G. Koning, L. Nguyen und N. Zarin, „Self-Sovereign Identity Solutions: The Necessity of Blockchain Technology“, *CoRR*, 2019. [Online]. Adresse: <http://arxiv.org/abs/1904.12816>.
- [8] B. für Sicherheit in der Informationstechnik. „Eckpunktepapier für Self-Sovereign Identities (SSI)“. (2021), [Online]. Adresse: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Krypto/Eckpunkte_SSI_DLT.pdf?__blob=publicationFile&v=2. (Aufgerufen: 18.04.2022).
- [9] M. Allende López, *Self-Sovereign Identity: The Future of Identity: Self-Sovereignty, Digital Wallets, and Blockchain*. Inter-American Development Bank, 2020.
- [10] S. H. und W. Scott Stornetta, „How to time-stamp a digital document“, *J. Cryptology*, Jg. 3, S. 99–111, 1991. DOI: <https://doi.org/10.1007/BF00196791>.
- [11] E. Ganne, *Can Blockchain Revolutionize International Trade?* World Trade Organization, 2018.
- [12] S. Nakamoto, „Bitcoin: A peer-to-peer electronic cash system“, *Decentralized Business Review*, S. 21 260, 2008.
- [13] V. Buterin *et al.*, „Ethereum white paper“, *GitHub repository*, Jg. 1, S. 22–23, 2013.
- [14] M. Schurtenberger. „Öffentliche vs. private Blockchains: Warum öffentliche Blockchains die Zukunft sind“. (2020), [Online]. Adresse: <https://www.bitcoinsuisse.com/de/outlook/why-public-blockchains-are-the-future-2>. (Aufgerufen: 04.03.2022).
- [15] International Organization for Standardization. „Governance of blockchain and distributed ledger technology systems (ISO/TC 307/SG/6)“. (2016), [Online]. Adresse: <https://www.iso.org/committee/6266604.html>. (Aufgerufen: 17.05.2022).
- [16] Z. Vardai. „What are public, private and permissioned blockchains?“ (2022), [Online]. Adresse: <https://forkast.news/what-are-public-private-permissioned-blockchains/#public-chain>. (Aufgerufen: 15.08.2022).
- [17] V. Saini. „ConsensusPedia: An Encyclopedia of 30+ Consensus Algorithms“. (2018), [Online]. Adresse: <https://hackernoon.com/consensuspedia-an-encyclopedia-of-29-consensus-algorithms-e9c4b4b7d08f>. (Aufgerufen: 07.03.2022).

- [18] N. Szabo. „Smart Contracts“. (1994), [Online]. Adresse: <https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smарт.contracts.html>. (Aufgerufen: 06.03.2022).
- [19] M. Bender. „Schutzziele der Kryptographie“. (2019), [Online]. Adresse: <https://www.mbitomatik.com/schutzziele-der-kryptographie-2>. (Aufgerufen: 21.03.2022).
- [20] A. Bode. „Schutzziele in der Informationssicherheit und ihre Umsetzung in der Praxis“. (2020), [Online]. Adresse: <https://blog.netwrix.de/2020/07/25/schutzziele-in-der-informationssicherheit-und-ihre-umsetzung-in-der-praxis>. (Aufgerufen: 22.03.2022).
- [21] Preveil. „Public – private key pairs & how they work“. (2021), [Online]. Adresse: <https://www.preveil.com/blog/public-and-private-key/>. (Aufgerufen: 26.07.2022).
- [22] Bundesamt für Sicherheit in der Informationstechnik. „Arten der Verschlüsselung“. (), [Online]. Adresse: <https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Onlinekommunikation/Verschlüsselt-kommunizieren/Arten-der-Verschlüsselung/arten-der-verschlüsselung.html>. (Aufgerufen: 04.07.2022).
- [23] D. Reed. „DID Primer“. (2017), [Online]. Adresse: <https://github.com/WebOfTrustInfo/rwot5-boston/blob/master/topics-and-advance-readings/did-primer.md>. (Aufgerufen: 02.07.2022).
- [24] N. Pohlmann. „Self-Sovereign Identity (SSI)“. (), [Online]. Adresse: <https://norbert-pohlmann.com/glossar-cyber-sicherheit/self-sovereign-identity-ssi/>. (Aufgerufen: 13.03.2022).
- [25] W3C. „Decentralized Identifiers (DIDs) v1.0“. (2022), [Online]. Adresse: <https://www.w3.org/TR/did-core>. (Aufgerufen: 14.03.2022).
- [26] M. Sasdi. „Digitale Freiheit durch SSI“. (2021), [Online]. Adresse: <https://csoonline.com/de/a/digitale-freiheit-durch-ssi,3673692>. (Aufgerufen: 15.03.2022).
- [27] W3C. „Verifiable Credentials Data Model v1.1“. (2022), [Online]. Adresse: <https://www.w3.org/TR/vc-data-model/>. (Aufgerufen: 14.03.2022).
- [28] Idunion. „IDunion - Über das Projekt“. (), [Online]. Adresse: <https://idunion.org/projekt>. (Aufgerufen: 03.04.2022).
- [29] „Hyperledger“. (2018), [Online]. Adresse: <https://hyperledger-indy.readthedocs.io/>. (Aufgerufen: 03.04.2022).
- [30] E-Estonia. „e-Estonia“. (2022), [Online]. Adresse: <https://e-estonia.com/story/>. (Aufgerufen: 09.04.2022).
- [31] —, „e-Identity“. (2022), [Online]. Adresse: <https://e-estonia.com/solutions/e-identity/id-card/>. (Aufgerufen: 09.04.2022).
- [32] P. Noro. „What is Self-Sovereign Identity and should states be afraid or fit?“ (2020), [Online]. Adresse: <https://www.sciencespo.fr/public/chaire-numerique/en/2020/12/21/what-is-self-sovereign-identity-should-states-be-afraid/>. (Aufgerufen: 09.04.2022).
- [33] S. H. Silvia Semenzin David Rozas, „Blockchain-based application at a governmental level: disruption or illusion? The case of Estonia“, *Policy and Society*, 2022. DOI: 10.3389/fbloc.2019.00028. [Online]. Adresse: <https://www.frontiersin.org/article/10.3389/fbloc.2019.00028>.
- [34] LACChain. „Blockcerts Caribe“. (), [Online]. Adresse: <https://www.lacchain.net/projects/Blockcerts-Caribe>. (Aufgerufen: 26.04.2022).
- [35] Innovation Laboratory of the Inter-American Development Bank Group. „LAC-Chain.net“. (), [Online]. Adresse: <https://www.lacchain.net/home?lang=en>. (Aufgerufen: 18.04.2022).

- [36] M. Allende López, *LACCchain Framework for permissioned public blockchain networks*. Inter-American Development Bank, 2021.
- [37] Procivis. „Procivis – Über uns“. (), [Online]. Adresse: <https://www.procivis.ch/about-us>. (Aufgerufen: 12.04.2022).
- [38] ——, „Die Smart-Government-Lösung für digitale Behördendienstleistungen“. (), [Online]. Adresse: <https://www.procivis.ch/eid>. (Aufgerufen: 12.04.2022).
- [39] ——, „One step closer to self-sovereign identity - Procivis launches SSI+“. (2022), [Online]. Adresse: <https://www.procivis.ch/post/one-step-closer-to-self-sovereign-identity-procivis-launches-ssi>. (Aufgerufen: 12.04.2022).
- [40] Sovrin. „Use case spotlight: The Government of British Columbia uses the Sovrin Network to take strides towards a fully digital economy“. (2019), [Online]. Adresse: <https://sovrin.org/use-case-spotlight-the-government-of-british-columbia-uses-the-sovrin-network-to-take-strides-towards-a-fully-digital-economy/>. (Aufgerufen: 04.04.2022).
- [41] Findy. „FINDY - VERIFIABLE DATA NETWORK“. (), [Online]. Adresse: <https://findy.fi/en/>. (Aufgerufen: 01.05.2022).
- [42] M. Hautala. „Findy – a visionary initiative by the public and private sectors in Finland – develops a new type of verifiable data network that strengthens Finland’s position in building digital trust“. (2021), [Online]. Adresse: <https://www.tietoevry.com/en/newsroom/all-news-and-releases/press-releases/2021/05/findy-a-visionary-initiative-by-the-public-and-private-sectors-in-finland--develops-a-new-type-of-verifiable-data-net/>. (Aufgerufen: 01.05.2022).
- [43] Nordea. „Leading the way to a verifiable data network with Findy“. (2021), [Online]. Adresse: <https://www.nordea.com/en/news/leading-the-way-to-a-verifiable-data-network-with-findy>. (Aufgerufen: 01.05.2022).
- [44] Kiva Organization. „The Kiva Organization“. (), [Online]. Adresse: <https://www.kiva.global/kiva-org/>. (Aufgerufen: 1.05.2022).
- [45] ——, „Kiva Protocol“. (), [Online]. Adresse: www.kiva.global/protocol/technology. (Aufgerufen: 01.05.2022).
- [46] ——, „The Kiva Protocol“. (), [Online]. Adresse: <https://www.kiva.global/protocol/>. (Aufgerufen: 01.05.2022).
- [47] D. F. P. Wang Fennie, „Self-Sovereign Identity in a Globalized World: Credentials-Based Identity Systems as a Driver for Economic Inclusion“, *Frontiers in Blockchain*, 2020. DOI: 10.3389/fbloc.2019.00028. [Online]. Adresse: <https://www.frontiersin.org/article/10.3389/fbloc.2019.00028>.
- [48] World Food Programme WFP. „Building Blocks“. (), [Online]. Adresse: <https://innovation.wfp.org/project/building-blocks>. (Aufgerufen: 01.05.2022).
- [49] Truu Ltd. „Trusted Digital Passports for Healthcare Professionals“. (), [Online]. Adresse: <https://truu.id>. (Aufgerufen: 15.05.2022).
- [50] Europäische Kommission. „The EU Project 'eSSIF-Lab'“. (), [Online]. Adresse: <https://essif-lab.github.io/framework/docs/essifLab-project>. (Aufgerufen: 15.05.2022).
- [51] ——, „Academic Verifiable Credentials (Academic VC)s by Blockchain Certified Data“. (2021), [Online]. Adresse: <https://essif-lab.eu/academic-verifiable-credentials-academic-vcs-by-blockchain-certified-data/>. (Aufgerufen: 15.05.2022).
- [52] ——, „Experience cross-borders services with EBSI — The first public sector blockchain services in Europe“. (), [Online]. Adresse: <https://ec.europa.eu/digital-building-blocks/wikis/display/EBSI/Home>. (Aufgerufen: 07.05.2022).

- [53] ——, „Academic Verifiable Credentials (Academic VCs) by Blockchain Certified Data“. (2022), [Online]. Adresse: https://ec.europa.eu/digital-building-blocks/wikis/download/attachments/447687044/%C2%8210610%C2%29%C2%82EBSI_Architecture_Explained%C2%29%C2%82v1.02%C2%29.pdf. (Aufgerufen: 15.05.2022).
- [54] The Linux Foundation. „Hyperledger Besu“. (), [Online]. Adresse: <https://www.hyperledger.org/use/besu>. (Aufgerufen: 24.07.2022).
- [55] ——, „Hyperledger Fabric“. (), [Online]. Adresse: <https://www.hyperledger.org/use/fabric>. (Aufgerufen: 24.07.2022).
- [56] Bundesamt für Bevölkerungsschutz BABS. „Nationale Risikoanalyse von Katastrophen und Notlagen“. (2020), [Online]. Adresse: <https://www.babs.admin.ch/de/aufgabenbabs/gefaehrdrisiken/natgefaehrdanalyse.html>. (Aufgerufen: 03.05.2022).
- [57] B. für Justiz BJ, „Diskussionspapier zum «Zielbild E-ID»“, 2021. [Online]. Adresse: <https://www.bj.admin.ch/dam/bj/de/data/staat/gesetzgebung/staatliche-e-id/diskussionspapier-zielbild-e-id.pdf.download.pdf/diskussionspapier-zielbild-e-id-d.pdf>.
- [58] Deloitte United States. „Deloitte Announces Strategic Alliance With Ava Labs to Use Blockchain to Improve State and Local Governments’ Recovery From Natural Disasters and Public Health Emergencies“. (2019), [Online]. Adresse: <https://www2.deloitte.com/us/en/pages/about-deloitte/articles/press-releases/deloitte-ava-labs-blockchain-state-local-government-natural-disaster-recovery.html>. (Aufgerufen: 24.04.2022).
- [59] UNO – Vereinte Nationen. „Resolution der Generalversammlung, verabschiedet am 25. September 2015“. (2015), [Online]. Adresse: <https://www.un.org/Depts/german/gv-70/band1/ar70001.pdf>. (Aufgerufen: 24.04.2022).
- [60] A. Schmid, „Kauf von Rüstungsgütern: Die Armee soll nachhaltiger werden“, 2022. [Online]. Adresse: <https://www.srf.ch/news/schweiz/interner-vbs-bericht-kauf-von-ruestungsguetern-die-armee-soll-nachhaltiger-werden>, (Aufgerufen: 24.04.2022).
- [61] U. Kampffmeyer. „eIDAS 2.0 und das European Digital Identity Wallet“. (2022), [Online]. Adresse: <https://www.project-consult.com/news/eidas-and-the-european-digital-identity-wallet/>. (Aufgerufen: 15.08.2022).
- [62] D. K. Nguyen. „Digitale Identitäten: EU setzt auf “elektronische Brieftasche”“. (2022), [Online]. Adresse: <https://www.it-daily.net/it-management/digitalisierung/digitale-identitaeten-eu-setzt-auf-elektronische-brieftasche>. (Aufgerufen: 07.05.2022).
- [63] D. M. R. Lukas Bühlmann. „DSG Revision: Vergleich zum geltendem Recht und zur EU-DSGVO“. (2020), [Online]. Adresse: https://www.mll-news.com/wp-content/uploads/2020/11/DSG_Revision_Gegen%C3%BCberstellung_30112020.pdf. (Aufgerufen: 24.04.2022).
- [64] Shivang, „Difference Between Centralized, Decentralized & Distributed Systems Over-simplified“, [Online]. Adresse: <https://www.scaleyourapp.com/difference-between-centralized-decentralized-distributed-systems-explained>, (Aufgerufen: 08.05.2022).
- [65] P. Tasatanattakool und C. Techapanupreeda, „Blockchain: Challenges and applications“, S. 473–475, 2018. DOI: 10.1109/ICOIN.2018.8343163.
- [66] 1. Blockchains, „Permissioned Vs Permissionless Blockchains“, [Online]. Adresse: <https://101blockchains.com/permissioned-vs-permissionless-blockchains/>, (Aufgerufen: 30.05.2022).
- [67] C. Li und B. Palanisamy, „Comparison of Decentralization in DPoS and PoW Blockchains“, Z. Chen, L. Cui, B. Palanisamy und L.-J. Zhang, Hrsg., S. 18–32, 2020.

- [68] R. Zhang, R. Xue und L. Liu, „Security and Privacy on Blockchain“, *ACM Comput. Surv.*, Jg. 52, Nr. 3, 2019, ISSN: 0360-0300. DOI: 10.1145/3316481. [Online]. Adresse: <https://doi.org/10.1145/3316481>.
- [69] A. Grüner, A. Mühle und C. Meinel, „Analyzing Interoperability and Portability Concepts for Self-Sovereign Identity“, S. 587–597, 2021. DOI: 10.1109/TrustCom53373.2021.00089.
- [70] Europäische Kommission. „European Commission adopts decision to license European Blockchain Services Infrastructure software as open-source“. (), [Online]. Adresse: <https://ec.europa.eu/digital-building-blocks/wikis/display/EBSI/European+Commission+adopts+decision+to+license+European+Blockchain+Services+Infrastructure+software+as+open+source>. (Aufgerufen: 7.05.2022).
- [71] Schweizer Bundesrat. „Bundesrat trifft Richtungsentscheid zur E ID“. (2021), [Online]. Adresse: <https://www.admin.ch/de/start/dokumentation/medienmitteilungen.msg-id-86465.html>. (Aufgerufen: 18.05.2022).
- [72] Bundesamt für Justiz (BJ). „Stärkung des Datenschutzes“. (2022), [Online]. Adresse: <https://www.bj.admin.ch/bj/de/home/staat/gesetzgebung/datenschutzstaerkung.html>. (Aufgerufen: 24.04.2022).
- [73] N. Nitin und J. Paul, „Your Identity is Yours: Take Back Control of Your Identity Using GDPR Compatible Self-Sovereign Identity“, 2020. [Online]. Adresse: <https://ieeexplore.ieee.org/document/9348298>.
- [74] B. Schellinger, J. Sedlmeir, L. Willburger, P. D. J. Strüker und P. D. N. Urbach, „Mythbusting Self-Sovereign Identity (SSI)“, 2022. [Online]. Adresse: https://www.fit.fraunhofer.de/content/dam/fit/de/documents/Whitepaper_Mythbusting_Self-Sovereign_Identity.pdf.
- [75] Y. Bakos und H. Halaburda, „Tradeoffs in Permissioned vs Permissionless Blockchains: Trust and Performance“, 2021. [Online]. Adresse: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3789425.
- [76] I. Vlachos, N. Kostopoulos, T. Damvakaraki *et al.*, „Energy Efficiency of Blockchain Technologies“, 2021. [Online]. Adresse: https://www.eublockchainforum.eu/sites/default/files/reports/Energy%20Efficiency%20of%20Blockchain%20Technologies_1.pdf.
- [77] Ethereum Foundation. „The Merge“. (2022), [Online]. Adresse: <https://ethereum.org/en/upgrades/merge/>. (Aufgerufen: 29.05.2022).
- [78] K. Koštál, T. Krupa, M. Gembec, I. Vereš, M. Ries und I. Kotuliak, „On Transition between PoW and PoS“, S. 207–210, 2018. DOI: 10.23919/ELMAR.2018.8534642.
- [79] D. C. Berghoff, D. U. Gebhardt, D. M. Lochter *et al.*, „Blockchain sicher gestalten“, 2019. [Online]. Adresse: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Krypto/Blockchain_Analyse.pdf?__blob=publicationFile&v=3.
- [80] Ethereum Docs. „NODES AND CLIENTS“. (2022), [Online]. Adresse: <https://ethereum.org/en/developers/docs/nodes-and-clients/#requirements>. (Aufgerufen: 02.07.2022).
- [81] LACChain Docs. „Node Requirements“. (2021), [Online]. Adresse: https://github.com/lacchain/besu-pro-testnet/blob/master/DEPLOY_NODE.md. (Aufgerufen: 02.07.2022).
- [82] Sovrin Docs. „Node Requirements“. (2018), [Online]. Adresse: <https://sovrin.org/wp-content/uploads/2019/03/Sovrin-Steward-Technical-Policies-V1.pdf>. (Aufgerufen: 02.07.2022).
- [83] E. J. Scheid, B. Rodrigues und B. Stiller, „Policy-Based Blockchain Selection“, *IEEE Communications Magazine*, Jg. 59, Nr. 10, S. 48–54, 2021. DOI: 10.1109/MCOM.100.2100120.

- [84] Veramo. „Veramo: DID-Methods“. (), [Online]. Adresse: https://veramo.io/docs/veramo_agent/did_methods/. (Aufgerufen: 21.06.2022).
- [85] Eidgenössisches Departement für auswärtige Angelegenheiten EDA. „Verzeichnis der offiziellen Vertretungen der Schweiz im Ausland“. (2022), [Online]. Adresse: https://www.eda.admin.ch/content/dam/eda/de/documents/vertretungen-reisehinweise/vertretungsverzeichnis_DE.pdf. (Aufgerufen: 04.07.2022).
- [86] N. Karagiannidis. „How decentralized are your software updates?“ (2020), [Online]. Adresse: <https://priviledge-project.eu/news/how-decentralized-are-your-software-updates>. (Aufgerufen: 17.08.2022).
- [87] Schweizer Radio und Fernsehen SRF. „Das E-ID-Gesetz wird deutlich abgelehnt“. (2021), [Online]. Adresse: <https://www.srf.ch/news/abstimmungen/elektronische-identitaet/eidgenoessische-abstimmung-das-e-id-gesetz-wird-deutlich-abgelehnt>. (Aufgerufen: 18.08.2022).
- [88] Schweizer Armee. „Ausbildungsgutschrift“. (), [Online]. Adresse: <https://www.vtg.admin.ch/de/karriere/bildungslandschaft-und-armee/ausbildungsgutschrift.html>. (Aufgerufen: 17.04.2022).
- [89] D. Reed. „Hyperledger Aries: The Next Major Step Towards Interoperable SSI“. (2019), [Online]. Adresse: <https://www.evernym.com/blog/hyperledger-aries/>. (Aufgerufen: 18.08.2022).
- [90] Jolocom. „A Decentralized, Open Source Solution for Digital Identity and Access Management“. (2019), [Online]. Adresse: <https://jolocom.io/wp-content/uploads/2019/12/Jolocom-Whitepaper-v2.1-A-Decentralized-Open-Source-Solution-for-Digital-Identity-and-Access-Management.pdf>. (Aufgerufen: 24.04.2022).
- [91] ——, „Github Repository: Jolocom DID Method“. (), [Online]. Adresse: <https://github.com/jolocom/jolo-did-method>. (Aufgerufen: 21.06.2022).
- [92] L. Cristian. „Gitter Chat: Jolocom SDK“. (), [Online]. Adresse: <https://gitter.im/jolocom/jolocom-sdk>. (Aufgerufen: 21.06.2022).
- [93] Jolocom. „Github Repository: Jolocom SmartWallet - An application to manage your digital identity.“ (), [Online]. Adresse: <https://github.com/jolocom/smartwallet-app>. (Aufgerufen: 21.06.2022).
- [94] ——, „4.2. Credential issuance“. (2018), [Online]. Adresse: <https://jolocom-lib.readthedocs.io/en/latest/interactionFlows.html#credential-issuance>. (Aufgerufen: 14.08.2022).
- [95] Veramo. „Github Repository: Veramo“. (), [Online]. Adresse: <https://github.com/uport-project/veramo>. (Aufgerufen: 21.06.2022).
- [96] Evernym Inc. „Evernym Docs“. (), [Online]. Adresse: <https://www.evernym.com/docs/>. (Aufgerufen: 21.06.2022).
- [97] A. Tobin. „Sovrin: What Goes on the Ledger?“ (2018), [Online]. Adresse: <https://www.evernym.com/wp-content/uploads/2017/07/What-Goess-On-The-Ledger.pdf>. (Aufgerufen: 21.06.2022).
- [98] Evernym Inc. „Connect.Me“. (), [Online]. Adresse: <https://www.evernym.com/connectme/>. (Aufgerufen: 21.06.2022).
- [99] Jolocom. „IPFS Pinning Code“. (2020), [Online]. Adresse: <https://github.com/jolocom/jolo-did-method/blob/1302227410d7aa91262e3da9ecafaaa89779b68e/packages/jolo-did-registrar/ts/ipfs.ts#L40>. (Aufgerufen: 10.08.2022).
- [100] ——, „Github Repository: Jolocom SmartWallet“. (), [Online]. Adresse: <https://github.com/jolocom/smartwallet-app>. (Aufgerufen: 10.08.2022).
- [101] ——, „Jolocom DID Method Specification“. (2020), [Online]. Adresse: <https://github.com/jolocom/jolo-did-method/blob/master/jolocom-did-method-specification.md>. (Aufgerufen: 11.08.2022).

- [102] ——, „The Jolocom Protocol - Own Your Digital Self“. (2018), [Online]. Adresse: <https://jolocom-lib.readthedocs.io/en/latest/>. (Aufgerufen: 11.08.2022).
- [103] ——, „RFC 7519 — Jason Web Token (JWT)“. (2015), [Online]. Adresse: <https://www.rfc-editor.org/rfc/rfc7519>. (Aufgerufen: 11.08.2022).
- [104] Ethereum. „Ropsten, Rinkeby and Kiln Deprecation Announcement“. (2022), [Online]. Adresse: <https://blog.ethereum.org/2022/06/21/testnet-deprecation/>. (Aufgerufen: 12.08.2022).
- [105] Jolocom. „Gemeinsam auf dem Weg zu einer eIDAS Wallet“. (2021), [Online]. Adresse: <https://jolocom.io/blog/once-eidas-de/>. (Aufgerufen: 12.08.2022).

Abbildungsverzeichnis

1.1	Startseite der umgesetzten Webanwendung «myArmy Portal» für die Interaktionen des VBSs mit dem SSI-Ökosystem.	2
2.1	Vereinfachter, visueller Aufbau einer Blockchain-Kette mit verlinkten «Blöcken». Nachträgliche Manipulation würde eine komplette Neuberechnung der gesamten Kette bedingen.	5
2.2	Überblick unterschiedlicher Blockchain-Ausprägungen. Private und Public unterscheidet die Offenheit der Blockchain: Wer kann teilnehmen? Permissioned und Permissionless bestimmen, ob Gruppen innerhalb des Netzwerks besondere Rechte oder Einschränkungen haben oder ob alle gleichgestellt sind. In der Theorie ist auch eine Private Permissionless Blockchain möglich – macht aber in der Praxis i.d.R. keinen Sinn und wurde deshalb aus dieser Illustration ausgeklammert.	7
2.3	Beispiel asymmetrische Verschlüsselung: Viola nutzt den öffentlichen Schlüssel von Ueli, um eine Nachricht zu verschlüsseln. Die Nachricht wird via Internet übertragen und Ueli kann die Nachricht mit seinem privaten Schlüssel wieder entschlüsseln.	10
2.4	Beispiel asymmetrische Signierung: Viola nutzt ihren privaten Schlüssel, um eine Nachricht zu signieren. Die Nachricht wird zusammen mit der Signatur via Internet übertragen. Ueli prüft die Signatur mit dem öffentlichen Schlüssel von Viola.	10
2.5	Überblick SSI-Schema mit teilnehmenden Instanzen und Abläufen	13
2.6	Beispiel einer DID, unterteilt in Schema, Methode und Identifier.	14
3.1	Ablauf Prozess «Ausbildungsgutschrift» heute: Die Parteien tauschen verschiedene Dokumente untereinander aus. Die Prüfung eingereichter Dokumente läuft manuell über verschiedene Stellen beim VBS. Eine automatisierte Prüfung ist nicht möglich.	44
3.2	Überblick SSI Use-Case VBS mit E-ID — Unterschiedliche Entitäten stellen VCs aus. So erhält der/die AdA VCs für die E-ID und eine Ausbildung an einer Hochschule. Diese VCs speichert die/der AdA im eigenen Wallet und gibt entsprechende VCs bzw. VPs an das VBS weiter.	45
3.3	Anwendungslandschaft des Proof of Concepts: «SSI Credential Generator» zum Ausstellen der E-ID und Ausbildungsbestätigung der FHNW, «myArmy Portal» zum Ausstellen von Militärgrad-Zertifikaten bzw. Anfordern von Ausbildungsgutschriften, VDR und persönlichem SmartWallet der/des Ada.	49

3.4 Architektur SSI-Ökosystem für PoC: Jolocom SmartWallet (iOS/Android) mit entsprechendem Jolocom Agent, zwei Portale (in Docker Container auf Google Cloud Run) die wiederum Agents zur Ausstellung und Verifikation von VCs enthalten, ein Infura-Knoten für den Zugriff auf Rinkeby und das IPFS-Netzwerk zur Speicherung der DID-Dokumente.	50
3.5 Startseite der umgesetzten Webanwendung «SSI Credential Generator».	52
3.6 Seite zum Ausstellen eines Ausbildungszertifikat der FHNW in der Anwendung «SSI Credential Generator».	53
3.7 Seite mit Auflistung der nötigen digitalen Zertifikaten im Ausbildungsgutschrift-Prozess im «myArmy Portal».	54
3.8 Seite mit QR-Code zur Anforderung der nötigen Zertifikate für die Ausbildungsgutschrift im «myArmy Portal».	54
3.9 Interaktion zwischen einem Jolocom Agent (Person oder Service), dem IPFS-Netzwerk und dem Registry Smart Contract auf Ethereum Rinkeby. Der Jolocom Agent erzeugt eine neue DID mit den zugehörigen Schlüsselpaaren und generiert daraus ein DID-Dokument, das anschliessend auf IPFS gespeichert und im Smart Contract (als IPFS-Hash) referenziert/verankert wird.	57
3.10 Interaktion zwischen einem Jolocom Agent (Person oder Service), dem IPFS-Netzwerk und dem Registry Smart Contract auf Ethereum Rinkeby. Der Jolocom Agent ruft auf dem Registry Smart Contract den IPFS-Hash zum DID-Dokument einer DID ab und löst anschliessend den IPFS-Hash auf, um das DID-Dokument zu laden.	58
3.11 Interaktion zwischen zwei Jolocom-Agents (Besitzer/in und Aussteller/in von Credentials) sowie Datenbank, IPFS-Netzwerk und Ethereum Smart Contract. Die Ausstellerin, der Aussteller erzeugt eine Token Offer, die von der Besitzerin, dem Besitzer akzeptiert oder abgelehnt werden kann. Bei einer Annahme der Offer stellt die Ausstellerin, der Aussteller die entsprechenden Credentials aus. Beide Parteien greifen jeweils auf IPFS und Ethereum zu, um DID-Dokumente zur Validierung der Signaturen zu laden (DID-Resolve). Die Ausstellerin, der Aussteller persistiert die Interaktion in der Datenbank.	59
3.12 Interaktion zwischen zwei Jolocom-Agents (Besitzer/in und Verifizierer/in von Credentials) sowie Datenbank, IPFS-Netzwerk und Ethereum Smart Contract. Die Verifiziererin, der Verifizierer erzeugt ein Credential Request Token, der von der Besitzerin, dem Besitzer beantwortet werden kann (Übermittlung der angeforderten Credentials). Beide Parteien greifen jeweils auf IPFS und Ethereum zu, um DID-Dokumente zur Validierung der Signaturen zu laden (DID-Resolve). Die Verifiziererin, der Verifizierer persistiert die Interaktion in der Datenbank.	60
A.1 Komponenten die für die Erstellung des User Interface konzipiert wurden.	85
A.2 UI-Prototyp: Startseite	85
A.3 UI-Prototyp: Instruktionen	86
A.4 UI-Prototyp: Zertifikate auswählen	86
A.5 UI-Prototyp: Formular	87
A.6 UI-Prototyp: QR Code	87

A.7 UI-Prototyp: Erfolgreiche Prüfung	88
A.8 UI-Prototyp: Footer	88

Tabellenverzeichnis

2.1 Übersicht ausgewählter SSI-Projekte und eingesetzte Technologien	21
2.2 Übersicht möglicher Szenarien von denen die Schweiz gemäss Risikonalalyse des BABS betroffen sein könnte. Von den definierten Szenarien sind jene plausibler, die geografisch eine kleinere Auswirkung haben. Nationale und transnationale Szenarien sind zwar wenig plausibel, können jedoch nicht ausgeschlossen werden. Detaillierte Informationen zu den Plausibilitätsklassen sind im Bericht des BABS zu finden[56] — Auszug davon in Anhang A.3	24
2.3 Gewichtungsmatrix für die Anforderungen an ein VDR.	29
2.4 Bewertung der Public Blockchain Ausprägungen Permissionless und Permissioned. Der Permissioned-Ansatz erfüllt im Schnitt die Anforderungen besser, obwohl beide Ansätze gut abschliessen. Einen deutlichen Unterschied gibt es bei der Einhaltung der Regulationskonformität.	38
3.1 Übersicht der Kriterien und entsprechender Gewichtung zur Evaluierung möglicher Technologien für die Umsetzung des PoC für den Anwendungsfall «Ausbildungsgutschrift».	46
A.1 Analyse möglicher Frameworks für die Umsetzung des Anwendungsfalls.	83

Codeverzeichnis

1 Diverse TODOs sind z.B. in der Funktion Interaction._processToken() offen, die unter anderem beim Anfordern von Credentials aufgerufen wird.	62
2 Ausschnitt aus der Funktion VBSAgent.verifyAusbildungsgutschriftCredentials() des «myArmy Portals». Die Funktion Agent.processJWT() (Jolocom SDK) ruft intern bereits CredentialRequest.satisfiesRequest() auf. Da keine Fehlermeldung oder Resultat zurückgeliefert wird, muss die Funktion nochmals aufgerufen werden.	62
3 Code-Beispiel aus der Jolocom SDK-Dokumentation, wie ein Credential verifiziert werden kann. https://jolocom.github.io/jolocom-sdk/1.0.0/guides/interaction_flows/#credential-verification	63
4 Umgesetzter Code des Request-Tokens zur Validierung der Ausbildungsgutschrift. Abweichende Stellen zur Dokumentation sind markiert.	64
5 Ansatz zum Auslesen der ETH-Adresse eines Agents gemäss User chunningham auf https://gitter.im/jolocom/jolocom-sdk	64

Ehrlichkeitserklärung

Hiermit erklären wir, die vorliegende Bachelorarbeit selbstständig und nur unter Benutzung der angegebenen Quellen verfasst zu haben. Die wörtlich oder inhaltlich aus den aufgeführten Quellen entnommenen Stellen sind in der Arbeit als Zitat bzw. Paraphrase kenntlich gemacht. Diese Bachelor Thesis ist noch nicht veröffentlicht worden. Sie ist somit weder anderen Interessierten zugänglich gemacht noch einer anderen Prüfungsbehörde vorgelegt worden.

Bern, 19. August 2022

Name: Luca Dietiker

Unterschrift:



Name: Ralf Winkelmann

Unterschrift:



A Anhang

A.1 Meeting Protokoll – 03.05.2022

Dieses Dokument protokolliert die besprochenen Themen des Meetings vom 03.05.2022.

Eckdaten

Teilnehmer*innen	Datum, Zeit	Ort
<ul style="list-style-type: none"> • Carlo Dietiker (Auftraggeber, VBS) • Carsten Plum (BIT) • Andreas Frey Sang (BIT) • Ralf Winkelmann (Projektteam) • Luca Dietiker (Projektteam) 	03.05.2022 16:00 - 17:30	Bundesamt für Informatik und Telekommunikation (BIT), Bern

Agenda

- Einführung, Vorstellung Personen
- Vorstellung Projektstand Studenten
- Vorstellung Projektstand BIT/VBS/DTI
- Weiteres Vorgehen / Synergien

Protokoll

Aktuelle Planung von DTI/BIT:

- Pilotenphase — Q3/4 2022
 - PoC Bundesausweis
 - PoC Lernfahrausweis (Astra)
 - Produktentwicklung
- Aufbau Schweizer Ökosystem — 2025
- Gesetzgebung schaffen — 2025

Proof of Concepts (PoC) und E-ID In einem ersten Schritt sollen zwei PoC's erstellt werden. (Siehe Auflistung oben) Ziel dieser PoC's soll es sein, dass den Parlamentarier*innen «etwas handfestes gezeigt» werden kann. Primäres Ziel der PoC's ist also nicht (nur) die Definition der Architektur, sondern das Schaffen von Awareness.

Für den konkreten Fall der E-ID ist bereits vorgesehen, dass eine persönliche Vorsprache nicht mehr nötig sein soll.

Kompatibilität mit der EU Das Gesetz sieht keine Verpflichtung zur Kompatibilität einer Schweizer E-ID-Lösung mit der EU (eIDAS) vor. Allerdings wird diese aus praktischen Gründen unumgänglich sein und deshalb angestrebt. Die genauen Spezifikationen der EU werden aber für die Schweiz als Drittstaat erst nach deren Veröffentlichung zugänglich.

Standards (u.A. für Credentials) Für die PoC's in den Bundesämtern (z.B. Lernfahrausweis Astra) werden Architekturen unter Einhaltung der durch die W3C definierten Standards angestrebt und die eIDAS Regulation verfolgt. Die Verantwortung für die Credentials liegt bei den einzelnen Bundesämtern/Ausstellern.

Es gibt Unterschiede zwischen den Standards die von der W3C (jsonld) definiert sind, und den Schemas, die bei Hyperledger Indy.

VDR Im PoC für den Bundesausweis setzt das BIT auf Hyperledger Indy und verfolgt die Entwicklungen in Finnland bzw. der EU genau. Es zeichnet sich ein offenes auf Blockchain-basiertes System ab. Sovrin wird sich in den Augen des BIT nicht durchsetzen. Es wird auf die Entwicklungen in der EU referenziert. Fest steht: Die Schweizer Regierung (Eidgenossenschaft) muss Besitzerin des Register sein! Wie das genau definiert wird und wie die Verteilung innerhalb des Bundes aufgeleist wird, ist noch nicht klar.

Das BIT wird Verifizierer-Lösungen für die Bundesämter bereitstellen. (Offizielles App und dann API-Schnittstelle für Verifizierer)

Wallet Als Wallet kommt für den PoC ein bereits bestehendes Wallet zum Einsatz. (erwähnt wird „Esatus“)

Für den Produktiven Launch wird das BIT ein eigenes Wallet entwickeln. Stand heute ist die Lancierung von verschiedenen Wallets nicht vorgesehen, wird allerdings durch die offene Definition der Standards kaum verhindert werden können.

Erkenntnis für weitere Kooperation

Die Roadmap des BIT und der zeitliche Rahmen dieser Arbeit lassen eine vertiefte Kooperation für die praktische Umsetzung leider nicht zu. Das Gespräch hat dennoch viele wichtige Stossrichtungen und Eckdaten für die SSI-Architektur offenbart. Erkenntnisse und Fragen aus dem Gespräch fliessen in die wissenschaftliche Arbeit und die praktische Umsetzung des Studenten-PoC ein.

A.2 Überblick Frameworks/Technologien

Das Projektteam hat diverse SSI-Lösungen analysiert und eine mögliche Eignung für die Umsetzung des Anwendungsfalls geprüft. Die Erkenntnisse sind in der Tabelle A.1 zusammengefasst.

Name	Geeignet	Notizen
Jolocom	Ja	<p>Allgemein — Bietet Open-Source SDK zur Implementierung unterschiedlicher Akteure im SSI-Ökosystem ("Jolocom SDK"). Baut auf Node.js auf. VDR: Technologie-Agnostisch aber explizit DLT- bzw. Blockchain-ready. Auf der Website wird angegeben, dass verschiedene Blockchains getestet werden und eine Verwendung von EBSI angestrebt wird. Dokumentation macht guten Eindruck. Chat für Fragen steht offen.</p> <p>DID-Methode — Stellt eigene DID-Methode ("DID:jolo") zur Verfügung. Schreibt auf Rinkeby (Ethereum Testnet). Jolocom verfügt über Smart Contract, der DID und IPFS-Hash zum DID-Dokument speichert. Mehr wird aus Kostengründen aktuell nicht auf Blockchain geschrieben.¹¹⁷</p> <p>Wallet — Digital Wallet für iOS und Android-Geräte steht zur Verfügung ("Jolocom SmartWallet").¹¹⁸</p> <p>Standards — Wurde für DSGVO-, eIDAS und ESSIF-Konformität gebaut, hält sich an W3C-Standards und wird aktiv weiterentwickelt. VS'c werden unterstützt. VP's noch nicht.</p>
Hyperledger Indy	Ja	<p>Allgemein — Open-Source Code-Basis für die Etablierung eines Public Permissioned Blockchain Netzwerks. Bietet umfassende Dokumentation. Zur Vollständigen Implementierung eines SSI-Ökosystems werden weitere Hyperledger-Komponenten benötigt (z.B. Aries) – Technischer Durchstich sehr komplex.</p> <p>Standards — Wurde mit Fokus SSI entwickelt und unterstützt DID, VC's, ZKP's nach W3C Standards und wird von verschiedenen europäischen Behörden evaluiert bzw. verwendet.</p>
Hyperledger Besu	Nein	Ethereum Client zur Erstellung eines private oder public (permissioned) Blockchain-Netzwerks unter Verwendung der Ethereum Spezifikationen. Wurde nicht speziell für SSI entwickelt und bedarf deshalb signifikanter Erweiterung. Wenn Hyperledger für SSI, dann Indy in Kombination mit weiteren Hyperledger-Komponenten verwenden.

¹¹⁷DID:jolo Methode: <https://github.com/jolocom/jolo-did-method>

¹¹⁸Jolocom Smart Wallet: <https://github.com/jolocom/smartzwallet-app>

Sovrin	Nein	<p>Open-Source Projekt basierend auf Hyperledger Indy. (Public Permissioned Blockchain) Im Whitepaper wird DSGVO-Kompatibilität erwähnt. Schreibzugang haben durch das Governance-Board zugelassene Entitäten (sog. «Stewards») Steward wird, wer vordefinierte und transparente Kriterien einhält. Trotzdem wohl eher schwierig im Vergleich zu anderen Lösungen Schweiz stellt mit Swisscom bereits einen Steward. Kostenlose Test-Umgebung kann genutzt werden. Dokumentation schwierig interpretierbar. (Es ist nicht klar, wie gestartet werden müsste..) Für PoC eher nicht geeignet.</p> <p>Im Gespräch mit dem BIT wurde Sovrin eher negativ erwähnt. Sovrin habe sich in Europa nicht durchgesetzt.</p>
BCGov	Ja	Bietet Kit für Issuing und Verifying von VC's. Wird aktiv weiterentwickelt. Basiert auf Hyperledger Indy (Indy-Netz out of the box mitgeliefert) und Hyperledger Aries. Bieten diverse Developer Tools, Node Browser die von Nutzen sein könnten. Dokumentation scheint veraltet – viele Links funktionieren nicht mehr. Aufwand zum Finden der Dokumentation hoch.
Alastria	Nein	Man muss Member sein um Nodes zu stellen. Kann kein eigenes Netz bauen, baut auf Quorum auf. Mitgliedschaft wird von einem Board geprüft und ist nur für Unternehmen zugänglich. Kostenpflichtig.
Blockcerts	Nein	Bietet Library für UI-Integration, Hat alle SSI-Komponenten inkl. Wallet, ist ein Open-Standard, hält sich an die Standards der W3C. Open-Source Projekt das aktiv weiterentwickelt wird. Proofs für Zertifikate werden auf Bitcoin und Ethereum Blockchain gespeichert. DID-Methode und Kompatibilität mit anderen Blockchain-Lösungen in Arbeit. (Kein aktuelles Update) Dokumentation dürftig.
Cordentity	Nein	Integriert Hyperledger Indy und damit SSI-Funktionalität in die Corda Plattform. Corda ist eine permissioned Blockchain Plattform. Das Corda Netzwerk besteht, man kann aber eigene Nodes hinzufügen und sogenannte Business Networks bauen. Corda ist eher für komplexere dezentrale Applikationen geeignet und würde vermutlich den Rahmen des Anwendungsfall sprengen - Hyperledger Indy könnte einfach direkt verwendet werden.
Evernym	Ja (X)	<p>Algemein, Standards — Eine im 2013 gegründete SSI-Plattform und sehr ausgereift. Hat Code für das Sovrin Netzwerk gespendet und die Plattform etabliert. Dies wiederum führte zur Gründung von Hyperledger Indy. Unterstützt aktuell nur das Sovrin Netzwerk - weitere Plattformen mit W3C-Standard sind geplant. Bietet SDK für Java, Python und Node und hat eine gute Dokumentation.</p> <p>Wallte — Wallet verfügbar, Wallet SDK für eigene Implementation nur mit bezahlten Plänen möglich.</p>

IDChainZ	Nein	Basiert auf der Blockchain ChainZy, die mehrere Applikationstypen bietet. IDChainZ ist für SSI gedacht. Keine Informationen, ob Permissioned oder Permissionless Blockchain. Auf der Webseite wird von "Working Proof-of-Concept" gesprochen. Die Dokumentation ist knapp und Informationen schwierig zu finden. Sieht nicht so aus, als wird aktiv entwickelt. Aus diesen Gründen vermutlich nicht geeignet.
Identity.com	Nein	Ist ein Open-Source getriebenes Ökosystem für SSI. Basiert auf der Ethereum Plattform und verwendet einen eigenen Token (CVC) um eine Art Marktplatz zu betreiben. Auf der Webseite sind diverse Libraries noch nicht verfügbar oder als "Work-in-Progress" gekennzeichnet. Für die Umsetzung deshalb noch nicht geeignet.
Serto.id	Nein	Bietet die Serto Suite, womit über eine grafische Oberfläche DIDs und VCs bearbeitet werden können - also ohne Code. Ist noch in der Beta-Phase. Bietet einen Agent für die Integration ins Ökosystem, der auf AWS deployed wird und bis zu einer gewissen Laufzeit im Free-Tier von AWS betreibbar ist. Entstand ursprünglich aus uPort und basiert auf Ethereum. Verwendet den W3C Standard. Ist mehr ein fertiges Produkt und kein technisches Framework für den Anwendungsfall.
Veramo	Ja	Allgemein — Ist eine Javascript Library für verifiable Data. Entstammt wie Serto.id von uPort und ist noch in der Beta-Phase. Ist gut dokumentiert und wird aktiv weiterentwickelt. Standards — Arbeitet eng mit W3C and DIF zusammen für die Standards. Unterstützt die DID-Methoden ethr, web und key - weitere Methoden müssten über einen Fork selbst implementiert werden. Neben Ethereum sind damit keine weiteren Blockchain-Lösungen direkt unterstützt.
SOWL / Esatus	Nein	Unterstützt alle Hyperledger Indy DLT-Netzwerke, wie z.B. Sovrin und IDUnion. Bietet alle Komponenten, jedoch als Fertiglösung über eine grafische Oberfläche. Zugriff nur auf Anfrage möglich und wahrscheinlich kostenpflichtig.
Trinsic	Nein	Bietet eine umfangreiche API aber auch eine grafische Oberfläche. Alle SSI-Komponenten sind verfügbar. Das SDK ist in diversen Sprachen erhältlich. Basiert auf Hyperledger-Stack und setzt auf diverse Open Standards wie W3C. Die Dokumentation ist sehr ausführlich und es wird aktiv entwickelt. Bis zu 50 Credential-Austausche (Ausstellen, Verifizieren) pro Monat sind gratis - dies ist für den Anwendungsfall zu wenig.

Tabelle A.1: Analyse möglicher Frameworks für die Umsetzung des Anwendungsfalls.

A.3 Plausibilitätsklassen

Quelle: [56]

Katastrophen und Notlagen Schweiz 2020 – Risikobericht

3.1.3 Plausibilität

Für mutwillig herbeigeführte Ereignisse – z. B. im Zusammenhang mit politischen Entwicklungen, Terrorismus oder Cyber-Angriffen – lassen sich aufgrund teils rasch ändernder Bedrohungslagen nur schwer eine Häufigkeit bzw. eine Wahrscheinlichkeit abschätzen. Außerdem bestehen für diese Arten von Ereignissen nur wenig Erfahrungswerte. Deshalb wird für diese Gefährdungen die Plausibilität eines möglichen Eintritts abgeschätzt.

Für KNS 2020 wurde die bisher durchgeführte expertenbasierte Delphi-Methode zur Plausibilitätseinschätzung durch einen indikatorbasierten Ansatz ergänzt.

Die Plausibilitätseinschätzung beruht neu auf zwei massgeblichen Leitindikatoren, welche die «Absicht und Fähigkeiten der Täterschaft» und die «Realisierbarkeit bzw.

Machbarkeit des Szenarios» bewerten. Den Leitindikatoren sind Subindikatoren mit definierten Bewertungskriterien zugeordnet. Diese werden im Rahmen der Workshops von Fachleuten erfasst. Mit dieser indikatorbasierten Methode werden für die einzelnen Szenarien Plausibilitätsindizes ermittelt und fünf Plausibilitätsklassen (P-Klassen) zugeordnet (siehe Tab. 3). Das Vorgehen ist detaillierter im KNS-Methodenbericht (BABS, 2020b) dokumentiert.

Die Einschätzung der Plausibilität ist wie die der Eintrittswahrscheinlichkeit szenariopezifisch. Sie ermöglichen einen relativen Vergleich der Plausibilität zwischen den verschiedenen Szenarien.

Tabelle 3: Plausibilitätsklassen (P-Klassen) für mutwillig herbeigeführte Ereignisse. Die in den Umbeschreibungen gemachten Angaben zu Hinweisen auf die Absicht einer Täterschaft und die Realisierbarkeit des Szenarios beziehen sich auf die Leitindikatoren der Methode.

P-Klasse	P-Index	Plausibilität	Umschreibung
P5	5,0	sehr plausibel	<p>Die Möglichkeit des Eintretens des Ereignisses in der Schweiz ist im Vergleich zu anderen Szenarien sehr gut vorstellbar. Es gibt eindeutige Hinweise auf die Absicht einer Täterschaft. Die Realisierbarkeit des Szenarios insgesamt ist einfach.</p>
	4,5	plausibel	<p>Die Möglichkeit des Eintretens des Ereignisses in der Schweiz ist im Vergleich zu anderen Szenarien gut vorstellbar. Es gibt eindeutige bis deutliche Hinweise auf die Absicht einer Täterschaft. Die Realisierbarkeit des Szenarios insgesamt ist einfach bis anspruchsvoll.</p>
P4	4,0	ziemlich plausibel	<p>Die Möglichkeit des Eintretens des Ereignisses in der Schweiz ist im Vergleich zu anderen Szenarien vorstellbar. Die Hinweise auf die Absicht einer Täterschaft reichen von deutlich bis nicht vorhanden / erkennbar. Die Realisierbarkeit des Szenarios insgesamt reicht von einfach bis komplex.</p>
	3,5	teilweise plausibel	<p>Die Möglichkeit des Eintretens des Ereignisses in der Schweiz ist im Vergleich zu anderen Szenarien wenig vorstellbar. Die Hinweise auf die Absicht einer Täterschaft reichen von deutlich vorhanden bis nicht vorhanden / erkennbar. Die Realisierbarkeit des Szenarios insgesamt reicht von anspruchsvoll bis komplex.</p>
P2	2,5	wenig plausibel	<p>Die Möglichkeit des Eintretens des Ereignisses in der Schweiz ist im Vergleich zu anderen Szenarien kaum vorstellbar, aber nicht ganz auszuschliessen. Es gibt keine Hinweise auf die Absicht einer Täterschaft. Die Realisierbarkeit des Szenarios insgesamt ist komplex.</p>
	2,0		
P1	1,5		
	1,0		

A.4 myArmy Portal - Prototype

Das User Interface für das «myArmy Portal» wurde zuerst als klickbarer Prototyp in Figma umgesetzt. Nachfolgend sind die erstellten Artboards als Referenz einsehbar.

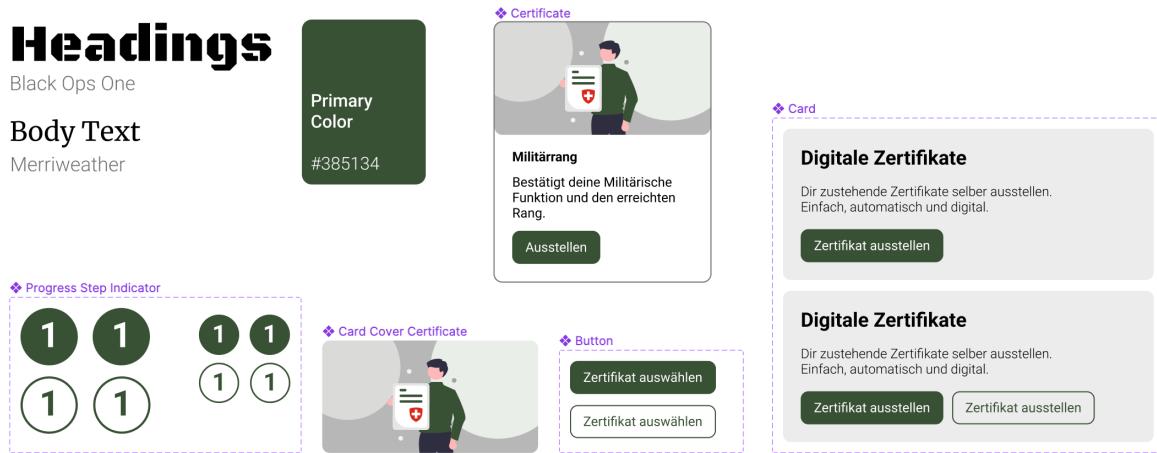


Abbildung A.1: Komponenten die für die Erstellung des User Interface konzipiert wurden.

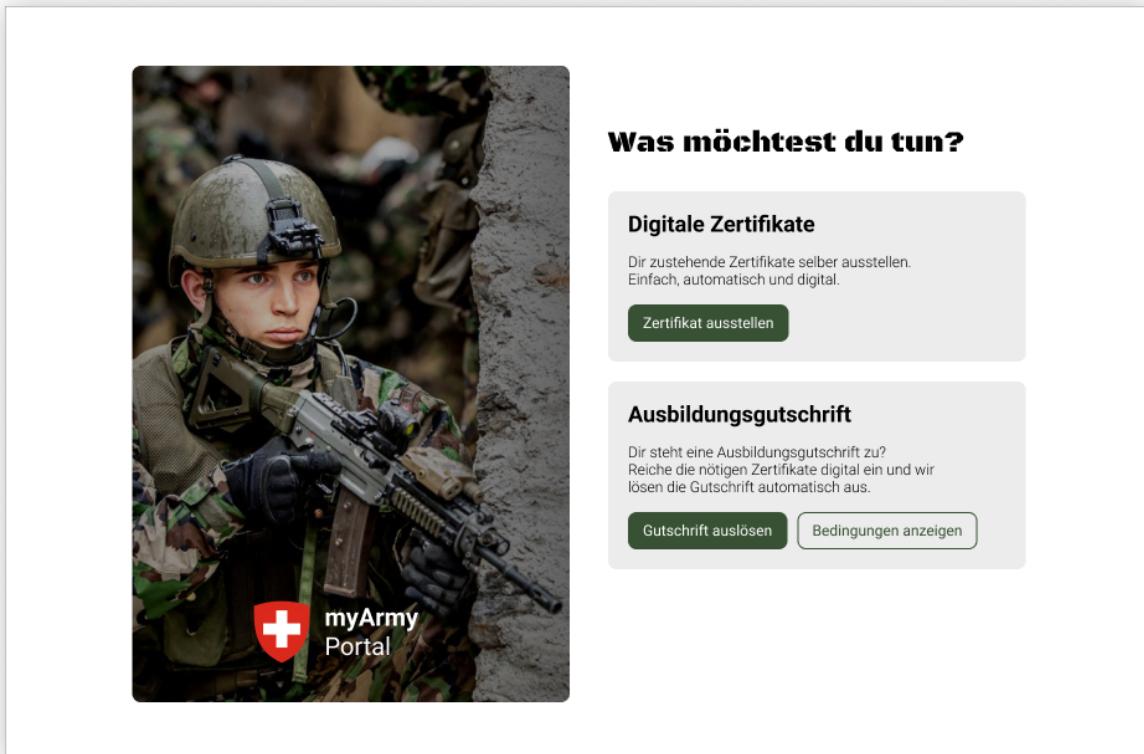


Abbildung A.2: UI-Prototyp: Startseite

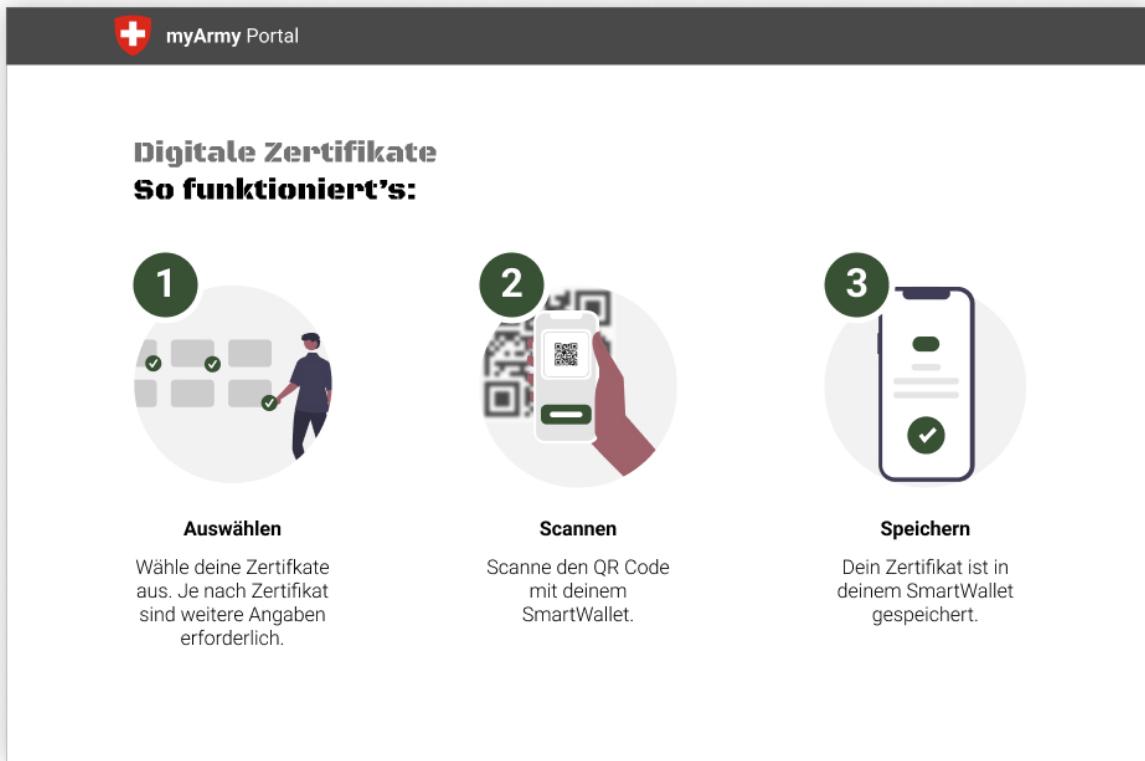


Abbildung A.3: UI-Prototyp: Instruktionen

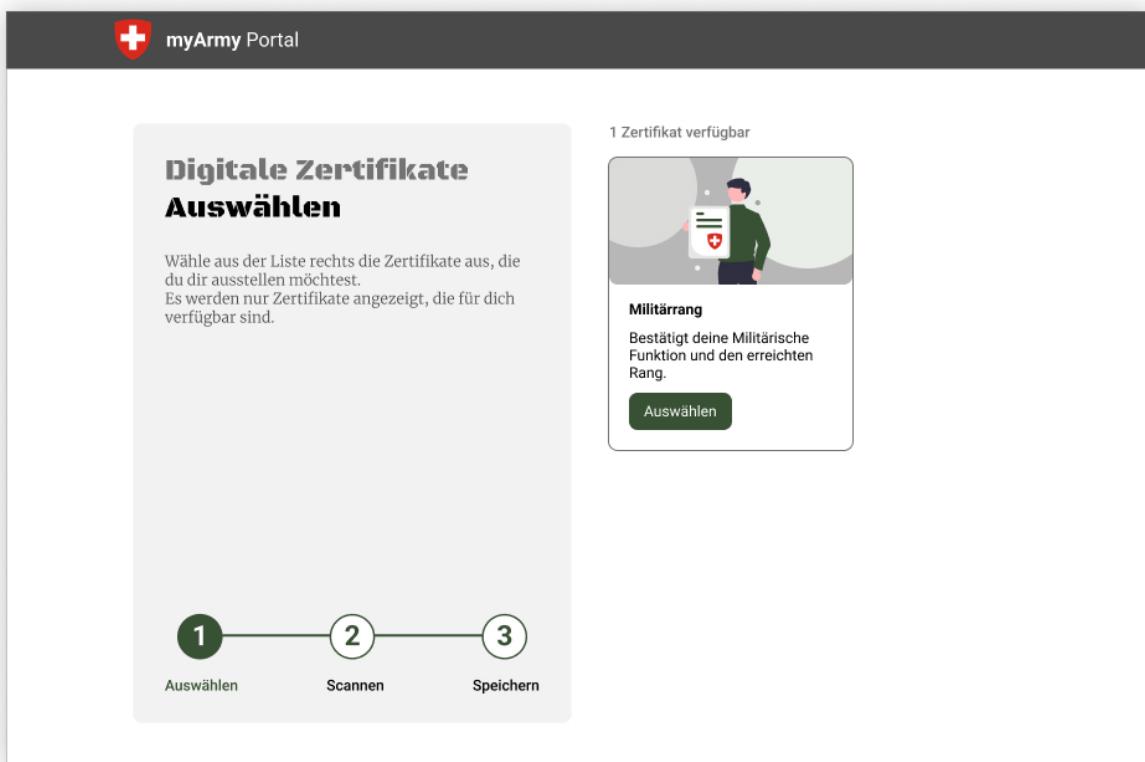


Abbildung A.4: UI-Prototyp: Zertifikate auswählen

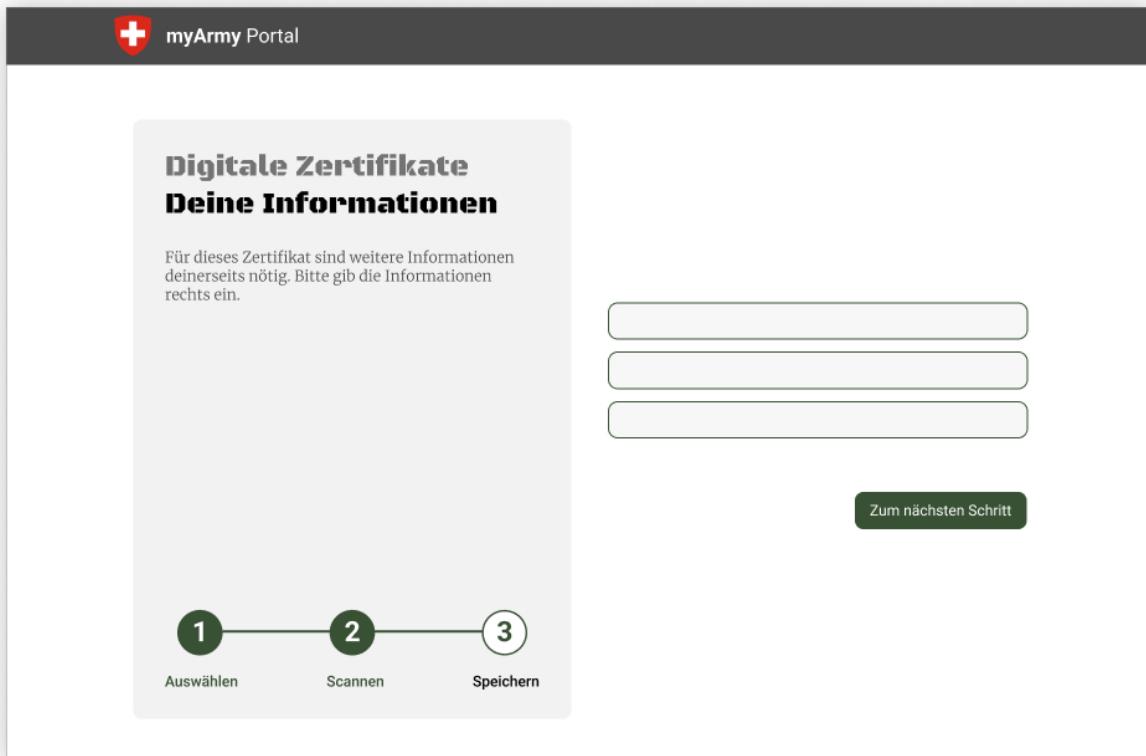


Abbildung A.5: UI-Prototyp: Formular

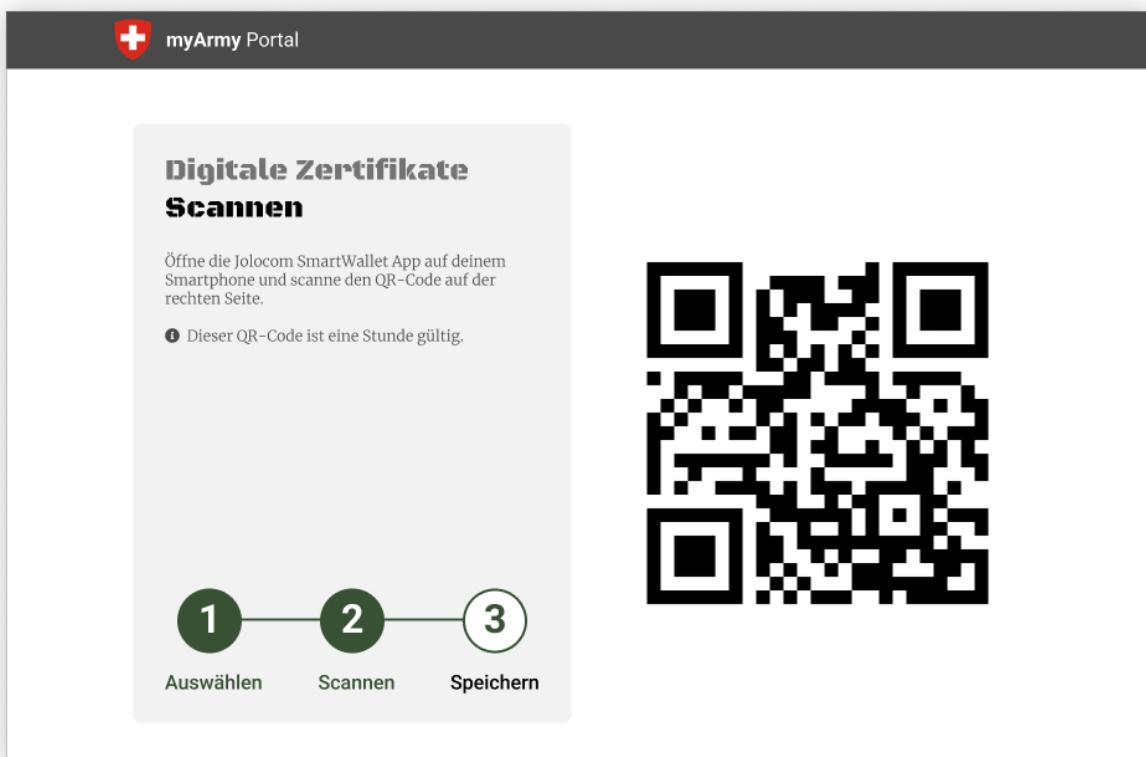


Abbildung A.6: UI-Prototyp: QR Code

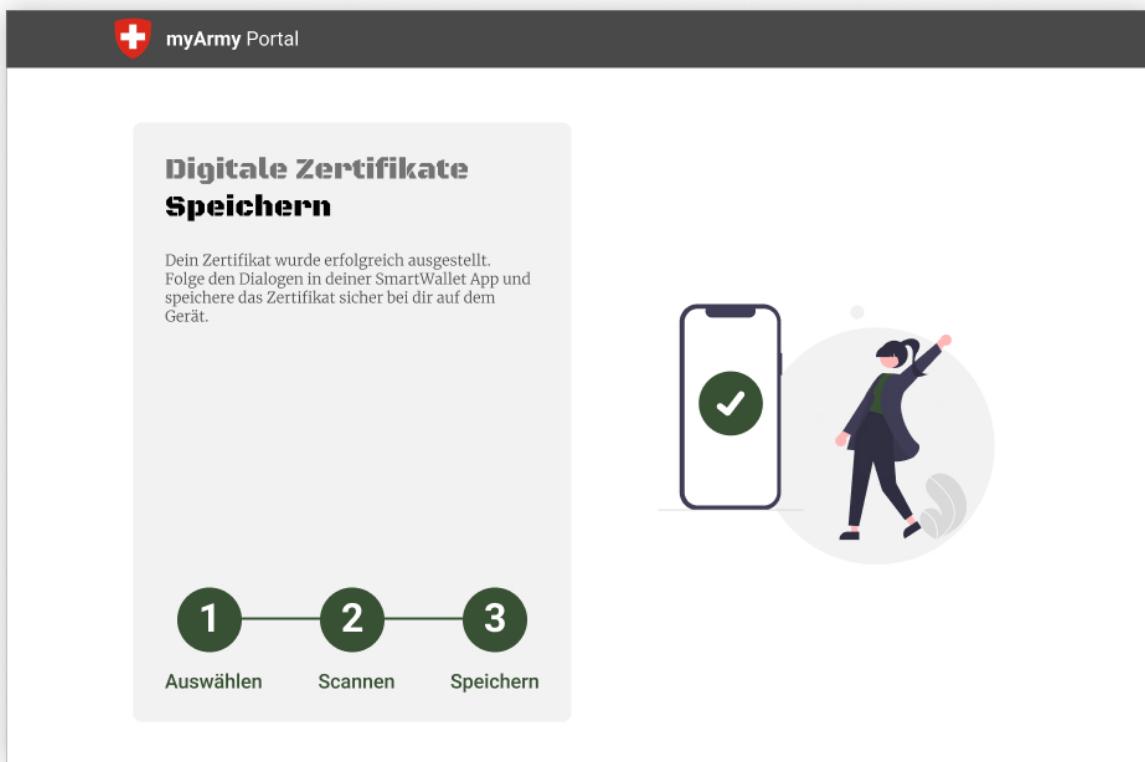


Abbildung A.7: UI-Prototyp: Erfolgreiche Prüfung

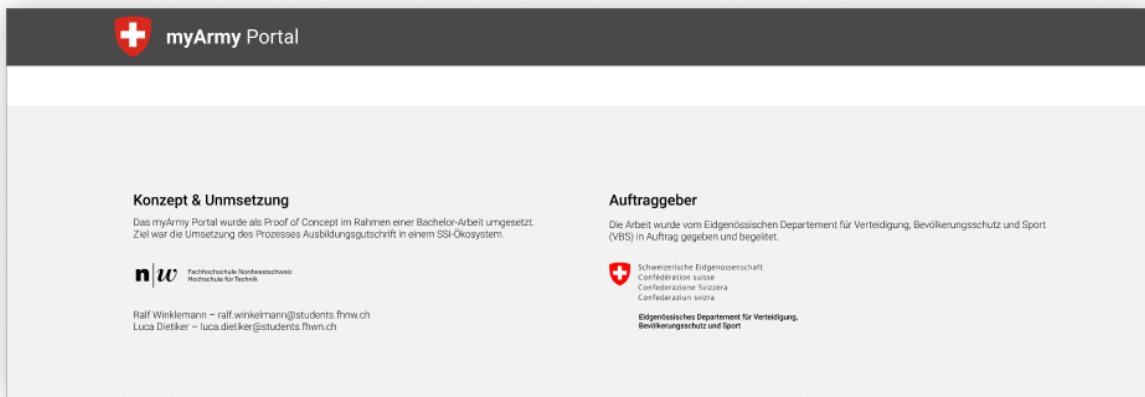


Abbildung A.8: UI-Prototyp: Footer

A.5 JSON Web Token – Credential Offer

```
{
  "typ": "JWT",
  "alg": "ES256K"
},
{
  "interactionToken": {
    "callbackURL": "https://vbs-ssi-portal-... ",
    "offeredCredentials": [
      {
        "type": "SwissMilitaryRankCert",
        "renderInfo": {
          "renderAs": "document"
        },
        "credential": {
          "schema": "https://schema.org/MilitaryRankCredential",
          "name": "Swiss Military Rank Certificate",
          "display": {
            "properties": [
              {
                "path": [
                  "$.rank"
                ],
                "label": "Grad",
                "value": "Mannschaft"
              }
            ]
          },
          "issuer": {
            "id": "did:jolo:606f0515bc4281d27b9882a1b3a59d253d3063ee52e645daff60aebdfb4dbd78"
          }
        }
      }
    ],
    "typ": "credentialOfferRequest",
    "iat": 1660375899249,
    "exp": 1660379499249,
    "jti": "c9fdad6eddc0ea2d",
    "iss": "did:jolo:606f0515bc4281d27b9882a1b3a59d253d3063ee52e645daff60aebdfb4dbd78#keys-1"
  },
  HMACSHA256(
    base64UrlEncode(header) + "." +
    base64UrlEncode(payload),
    secret
  )
}
```

A.6 JSON Web Token – Credential Request

```
{
  "typ": "JWT",
  "alg": "ES256K"
},
{
  "interactionToken": {
    "credentialRequirements": [
      {
        "type": [
          "VerifiableCredential",
          "SwissMilitaryRankCert"
        ],
        "constraints": [
          {
            ">": [
              {
                "var": "claim.level"
              },
              2
            ]
          },
          {
            "===": [
              {
                "var": "issuer"
              },
              "did:jolo:606f0515bc4281d27b9882a1b3a59d253d3063ee52e645daff60aebdfb4dbd78"
            ]
          }
        ]
      },
      "callbackURL": "https://vbs-ssi-portal-y72gddnxwq-ew.a.run.app/..."
    ],
    "typ": "credentialRequest",
    "iat": 1660377729617,
    "exp": 1660381329617,
    "jti": "288de0218b5c41a2",
    "iss": "did:jolo:606f0515bc4281d27b9882a1b3a59d253d3063ee52e645daff60aebdfb4dbd78#keys-1"
  },
  HMACSHA256(
    base64UrlEncode(header) + "." +
    base64UrlEncode(payload),
    secret
  )
}
```