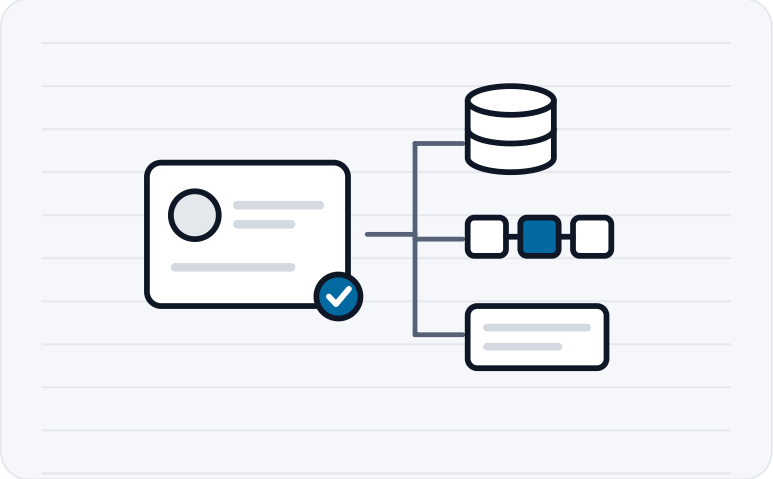
A-SIT Technology

E-Government Innovationszentrum

3. Juni 2024 Überblick · Transparenz · Digitale Identität · 24 Min. Lesezeit

Die Rolle von Vertrauensregistern im Ökosystem für verifizierbare Anmeldeinformationen

Edona Fasllija



Autorinnen und Autoren	Edona Fasllija
Quelle	https://technology2.a-sit.at/veroeffentlichungen/vertrauensregister-fuer-verifizierbare-anmeldeinformationen/
Hinweis	Maschinell übersetzt.

Kernaussagen

- Die VC-Standards schreiben keine Implementierung der Verifiable Data Registry vor; eine sichere, manipulationserkennbare Datenbank kann genügen.
- Vertrauenswürdige Datenbanken sind schnell und skalierbar, aber ein zentraler Ausfallpunkt und weniger transparent als manche dezentrale Optionen.
- Distributed Ledgers und Blockchains bieten robuste Sicherheit und Transparenz, können wegen des Konsensprozesses aber weniger effizient sein.
- Die Wahl der Speicherlösung hängt vom Anwendungsfall ab: Bedarf an Dezentralisierung, Geschwindigkeit und Vertrauen in die Betreiber der Registry.

- Widerruf birgt Privatsphäre-Risiken wie Nachverfolgbarkeit und Verknüpfbarkeit; eine Universallösung ist schwer zu finden.

Überprüfbare Datenregister werden im W3C-VC-Datenmodell definiert und verwalten alle Daten im Zusammenhang mit der Erstellung und Überprüfung überprüfbarer Anmeldeinformationen, wie z. B. vertrauenswürdige Anmeldeinformationsschemata, öffentliche Schlüssel vertrauenswürdiger Aussteller, Sperrregister usw. Einer der Vorteile dieser Definition ist, dass es umfassend und flexibel genug ist, um passgenaue überprüfbare Datenregister zur Verwaltung von VC-Daten zu ermöglichen und eine ganze Reihe unterschiedlicher Optionen zu berücksichtigen; von vertrauenswürdigen zentralisierten Datenbanken bis hin zu verteilten Datenbanken, Ledgers oder Blockchains.

Im Rahmen dieses Projekts untersuchen wir die verschiedenen Trust-Registry-Optionen zur Verwaltung von VC-Daten und identifizieren die Vorteile und Einschränkungen der alternativen Speichersysteme für verschiedene Trust-Frameworks.

1. Einleitung

Auf der Suche nach mehr Sicherheit, Benutzerfreundlichkeit und Privatsphäre haben sich digitale Identitätslösungen deutlich gewandelt. Vom klassischen Ansatz mit Benutzername und Passwort über Federated-Identity-Systeme [1] bis hin zu nutzerzentrierten Modellen wie Verifiable Credentials hat sich der Schwerpunkt verschoben: Nutzende erhalten mehr Kontrolle, Privatsphäre und Flexibilität über ihre Identitätsinformationen.

Der Verifiable-Credentials-Ansatz ermöglicht es Einzelpersonen, ihre digitalen Bestätigungen von Identitätsattributen selbst zu verwalten und zu kontrollieren. Ein Verifiable Credential (VC) ist ein manipulationssicherer Nachweis, dessen Urheberschaft kryptografisch überprüfbar ist [2]. Dieses Modell wird typischerweise über eine persönliche und sichere „Wallet"-Anwendung [3] umgesetzt, die Verifiable Credentials und Schlüsselmaterial der Nutzerin bzw. des Nutzers empfängt, speichert, präsentiert und verwaltet. Diese Wallet lässt sich bequem auf persönlichen Geräten wie Smartphones installieren und bietet so einen einfachen Zugang für die Einzelperson.

Ein VC-Ökosystem umfasst drei unterschiedliche Entitäten:

- Die Nutzerin bzw. der Nutzer (User), also die Entität, die ihre Identitätsaussagen authentifizieren möchte, manchmal auch als Identity Holder oder Credential Subject bezeichnet.
- Der Verifier, also die Entität, die von der Nutzerin bzw. vom Nutzer den Nachweis bestimmter Identitätsaussagen verlangt (auch als Service Provider oder Relying Party bekannt).
- Der Issuer, also die Entität, die der Nutzerin bzw. dem Nutzer den Nachweis der Gültigkeit der Aussagen ausstellt (auch als Identity Provider bekannt).

Konkret stellt der Issuer der Nutzerin bzw. dem Nutzer ein Verifiable Credential (VC) aus. Dieser digitale Nachweis enthält eine Reihe von Aussagen oder Attributen über die Nutzerin bzw. den Nutzer sowie einen kryptografischen Integritätsnachweis in Form der digitalen Signatur des Issuers. Das Verifiable Credential

kann dann über eine Verifiable Presentation (VP) jedem Verifier präsentiert werden, der bestimmte Attribute aus einem oder mehreren der Nachweise verlangt. Verifiable Presentations werden so aus dem Verifiable Credential abgeleitet, dass über Selective-Disclosure-Mechanismen nur die für den jeweiligen Zweck erforderliche Mindestmenge an Informationen offengelegt wird.

Neben der Überprüfung einer Aussage über das Subjekt des Verifiable Credential (VC) sollte der Verifier anhand des vorgelegten VC Folgendes feststellen, um zu entscheiden, ob er diese Nachweise akzeptiert:

(i) den Issuer des Nachweises, (ii) die Integrität des VC seit seiner Ausstellung und (iii) die Gültigkeit des VC, also dass er weder abgelaufen ist noch widerrufen wurde.

Der Verifier nutzt dann öffentlich zugängliche Informationen, die in Verifiable Data Registries [2] (VDRs) gespeichert sind, um die Gültigkeit des Nachweises des Verifiable Credential zu bestätigen, ohne den Issuer kontaktieren zu müssen. Nach erfolgreicher Überprüfung kann der Verifier die Richtigkeit der Aussagen im Verifiable Credential bestätigen.

Das Verifiable Credentials Data Model v2.0 [2] ist ein offener Standard für das Format digitaler Nachweise, der kryptografische Sicherheit, Wahrung der Privatsphäre und maschinelle Überprüfbarkeit gewährleistet. Verifiable Credentials gehen jedoch über das W3C VC Data Model hinaus und umfassen auch Nachweise, die über andere Datenmodelle ausgedrückt werden, etwa die Mobile Driver's License (mDL) [4].

Nutzerzentrierte Identitätsparadigmen stützen sich stark auf das Konzept der Verifiable Data Registries. Sie dienen als robuste und verlässliche Datenquelle, die dem System ein Element des Vertrauens verleiht. Diese Registries erleichtern die Erstellung und Validierung von Nachweisen im VC-Ökosystem, indem sie Zugang zu einem Aufzeichnungssystem bieten, das einer Partei hilft zu entscheiden, dass eine Entität vertrauenswürdig ist. Dieser Prozess ermöglicht sicherere und vertrauenswürdigere Informationsaustausche, die einen grundlegenden Aspekt des VC-Identitätsparadigmas darstellen.

1.1. Vertrauensmodell

Die Architektur des Verifiable-Credentials-Ökosystems stellt einen bedeutenden Paradigmenwechsel dar: Die Nutzerin bzw. der Nutzer steht im Zentrum der Interaktionen zwischen dem Verifier und dem Credential Issuer. Dieser Paradigmenwechsel bringt auch neue Trust-Frameworks hervor.

Es bietet Nutzenden mehr Privatsphäre, Portabilität und Kontrolle, indem es ihnen erlaubt:

i. Nachweise gegenüber Verifiern zu präsentieren, ohne dass die Verifier den Credential Issuer kontaktieren müssen.

ii. Identifikatoren zu verwenden, die nicht von einem bestimmten Drittanbieter vergeben werden.

iii. Vertrauensbeziehungen zu Verifiern unabhängig von Credential Issuern zu verwalten [5].

Es ist wichtig zu erkennen, dass der volle Nutzen von Verifiable Credentials davon abhängt, im Ökosystem wirksam Vertrauen aufzubauen. Die bloße Überprüfung der Signatur des Credential Issuers auf einem Nachweis genügt möglicherweise nicht, damit Verifier den Nachweis akzeptieren und Nutzenden Zugang zu Diensten gewähren. Der Verifier muss feststellen, dass dem Issuer des Nachweises vertraut wird, den jeweiligen Nachweistyp in dem betreffenden Bereich auszustellen. Die Nutzerin bzw. der Nutzer (oder die Wallet-Anwendung) muss beurteilen, ob dem Verifier vertraut wird, im Rahmen der Verifiable Presentation

bestimmte Attribute anzufordern. Eine weitere Vertrauensfrage ist, ob Nutzende beliebige Wallet-Anwendungen zur Verwaltung ihrer Verifiable Credentials verwenden dürfen. Trust Frameworks stellen Mechanismen bereit, die diese Vertrauensentscheidungen erleichtern. Sie beruhen auf der Vertrauensbeziehung zwischen Nutzenden und Verifier (oder Relying Party) sowie zwischen Verifiern und Wallets.

Der Aufbau dieser Vertrauensbeziehungen erfordert neben der technischen Interoperabilität auch regulatorische oder vertragliche Vereinbarungen. Verifiable Data Registries dienen dazu, diese Vereinbarungen zu erfassen und bereitzustellen.

VDRs, alternativ auch Trust Registries genannt, bieten den Entitäten im System eine sichere und verlässliche Grundlage, um Vertrauen aufzubauen und miteinander zu interagieren. Sie speichern vor allem die Trust Anchors der relevanten Entitäten des Ökosystems. Der Trust Anchor ist im Allgemeinen der Entitätsidentifikator mit dem zugehörigen öffentlichen Schlüssel, der zur Überprüfung der von dieser Entität erstellten Signaturen dient. Darüber hinaus speichern sie Daten zu Nachweisvorlagen und Verifizierungsrichtlinien sowie eine Liste der Entitäten, die im Ökosystem zur Ausstellung und Überprüfung von Nachweisen berechtigt sind. Außerdem können diese Registries Einträge enthalten, die festlegen, welche Issuer welche Arten von Verifiable Credentials ausstellen dürfen, aber auch welche Verifier welche Arten von Verifiable Presentations anfordern dürfen.

Das W3C VC Data Model beschreibt das Vertrauensmodell eines VC-Ökosystems anhand eines Vertrauensdreiecks (dargestellt in Abbildung 1), das die Interaktionen zwischen Issuer, Nutzerin bzw. Nutzer und Verifier beschreibt. In diesem Modell vertraut der Verifier darauf, dass der Issuer den erhaltenen Nachweis ausgestellt hat. Dies wird durch einen Nachweis begründet, dass der Issuer den Nachweis erzeugt hat. Nutzende und Verifier vertrauen darauf, dass der Issuer wahrheitsgemäße Nachweise über das Subjekt ausstellt und sie bei Bedarf rasch widerruft. Alle Entitäten vertrauen darauf, dass die Verifiable Data Registry manipulationssicher ist und korrekt abbildet, welche Daten von welchen Entitäten kontrolliert werden [2].

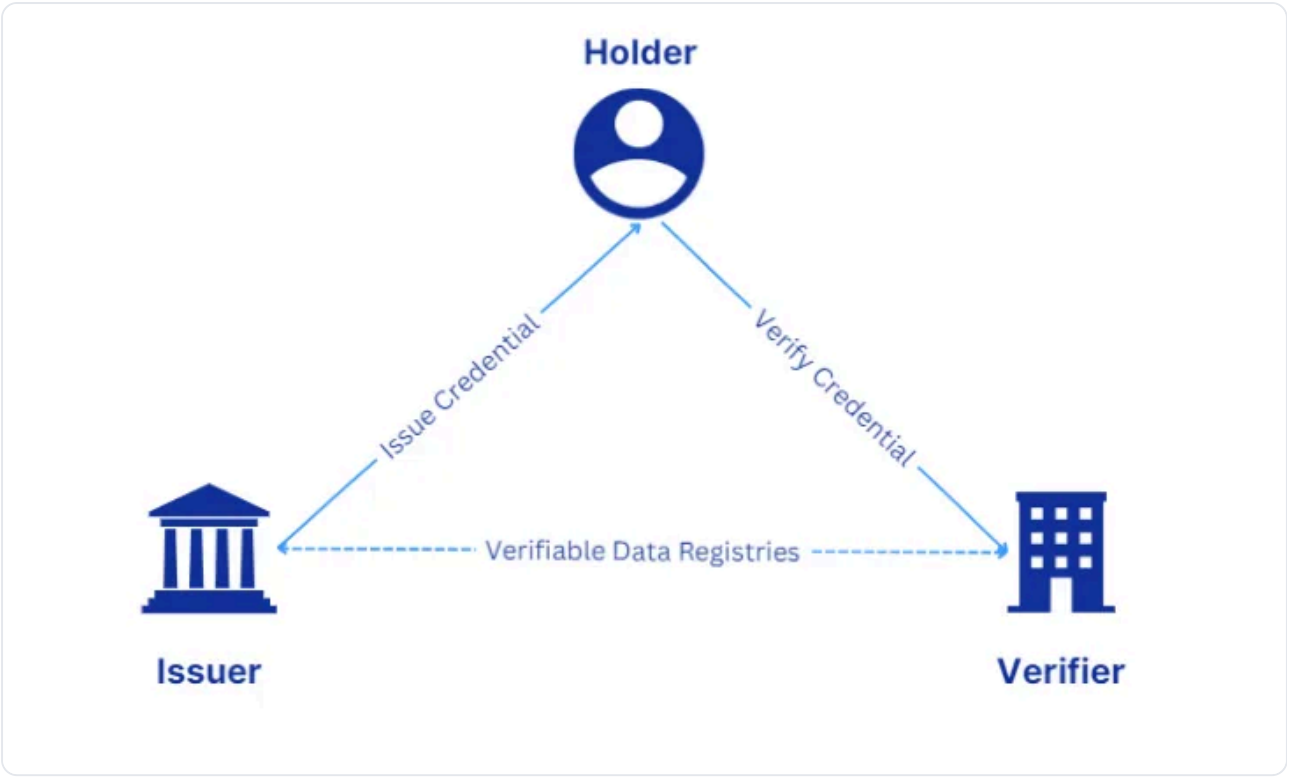


Abbildung 1: Vertrauensdreieck im Verifiable-Credential-Ökosystem

VDRs ermöglichen das technische Vertrauen, das für die Interaktionen zwischen den Entitäten erforderlich ist. Damit Verifier den Ursprung des Verifiable Credential feststellen können, müssen sie prüfen, ob der Issuer des VC im jeweiligen Bereich als vertrauenswürdig anerkannt ist und woher diese Anerkennung stammt. In diesem Zusammenhang hat der Verifier eine indirekte Vertrauensbeziehung zum Issuer. Statt direkt mit dem Verifier zu kommunizieren, hinterlegt der Issuer Informationen zu seinen öffentlichen Schlüsseln in den Trust Registries, auf die der Verifier ohne Weiteres zugreifen kann. Bei der Überprüfung kann der Nachweis im Verifiable Credential mit dem in den Registries gespeicherten öffentlichen Schlüssel authentifiziert werden. Da die VDR manipulationsresistent ist, vertraut der Verifier auf die Integrität der gespeicherten Informationen des Issuers und stellt sicher, dass der öffentliche Schlüssel unverändert bleibt. Damit schließt sich das Vertrauensdreieck, wie in Abbildung 1 dargestellt.

1.2. Trust Frameworks

Im VC-Ökosystem benötigen Credential Issuer, Nutzende und Verifier Identifikatoren. Typischerweise dienen diese Identifikatoren auch dazu, auf einen kryptografischen öffentlichen Schlüssel zuzugreifen, der zur Überprüfung der Signatur des Nachweises nötig ist. Verifiable Credentials geben Nutzenden mehr Kontrolle, da sie Identifikatoren verwenden können, die nicht zwingend von einer bestimmten Drittstelle (Identity Provider) vergeben werden. Das Konzept dezentraler Identifikatoren, häufig mit den W3C Decentralized Identifiers (DIDs) verbunden, steht im Vordergrund, wobei neben DIDs auch andere Arten von Identifikatoren anwendbar sind. Mögliche Optionen sind HTTPS-URLs, JWKs, X.509-Zertifikate und weitere.

Die Überprüfung der Gültigkeit eines Verifiable Credential setzt das Verständnis des zugrunde liegenden Trust Frameworks voraus. Das Trust Framework wird benötigt, um die Vertrauenswürdigkeit der verschiedenen im VC-Ökosystem beteiligten Parteien zu adressieren. Je nach Vertrauensmodell und der

Art des verwendeten Entitätsidentifikators lassen sich Verifiable-Credential-Ökosysteme in zwei Hauptgruppen einteilen: dezentral oder zentral.

Systeme der ersten Kategorie nutzen eine dezentrale Public-Key-Infrastruktur (DPKI) [6] und können Technologien wie Distributed Ledgers oder Blockchains einsetzen, um Decentralized Identifiers (DIDs) dezentral zu erzeugen und zu verwalten. In diesen Systemen sind die Identifikatoren global eindeutig und in einer Verifiable Data Registry verankert, die den Auffindungs- und Überprüfungsprozess unterstützt. DIDs sind so konzipiert, dass sie unabhängig von zentralen Identity Providern und Zertifizierungsstellen funktionieren. Die Inhaberin bzw. der Inhaber der DID kann daher die Kontrolle darüber nachweisen, ohne die Autorisierung einer anderen Entität zu benötigen.

Zentrale Systeme dagegen stützen sich auf eine zentrale Public-Key-Infrastruktur (PKI) und sind zur Validierung von einer Hierarchie vertrauenswürdiger Zertifizierungsstellen (CAs) abhängig. Dabei stellt eine Vertrauenswurzel Zertifikate für Zertifizierungsstellen aus, die wiederum Zertifikate für Nutzende ausstellen. So entsteht eine Vertrauenskette von der Wurzel bis zu den Endzertifikaten.

Damit Nutzende Nachweise direkt von Issuern erhalten und direkt an Verifier präsentieren können, muss ein Mechanismus geschaffen werden, über den Verifier auf die von den Issuern verwalteten öffentlichen Schlüssel zugreifen können. Genau hier kommen VDRs ins Spiel. Über die VDRs können die Verifier auf vertrauenswürdige Weise auf die öffentlichen Schlüssel der Credential Issuer zugreifen.

1.3. Die Rolle von VDRs

Verifiable Data Registries spielen in Verifiable-Credential-Ökosystemen aus mehreren Gründen eine entscheidende Rolle:

i. Vertrauenswürdiger Vermittler: Eine VDR fungiert als vertrauenswürdiger Vermittler (Mediator) im VC-Ökosystem. Sie ist ein Repository bzw. eine Datenbank, die kritische Informationen zu VCs speichert und den Zugriff darauf bereitstellt. Dazu gehören kryptografische öffentliche Schlüssel, Service-Endpunkte, Authentifizierungsparameter, Zeitstempel und Metadaten. Die VDR stellt sicher, dass diese Informationen verfügbar und zugänglich sind, um Auflösungs- und Überprüfungsprozesse zu unterstützen.

ii. Lebenszyklusmanagement: Die VDR verwaltet und pflegt den Lebenszyklus von VCs. Sie unterstützt die Erstellung, Registrierung und den Widerruf von VCs, indem sie als zentrale Kontroll- oder Koordinationsstelle dient. Eine Entität, die ein neues VC ausstellt, kann beispielsweise die VDR nutzen, um die ordnungsgemäße Registrierung und Verwaltung der zugehörigen Informationen sicherzustellen. Ebenso verarbeitet die VDR Aktualisierungen oder Widerrufe von VCs und bildet diese Änderungen im System ab.

iii. Interoperabilität: Die VDRs verbessern auch die Interoperabilität und Standardisierung im Ökosystem. Sie erzwingen einheitliche Datenformate, Validierungsregeln und Datenaustauschprotokolle und stellen so sicher, dass die gespeicherten Informationen den etablierten Standards und Spezifikationen entsprechen. Das fördert Kompatibilität und nahtlose Integration über verschiedene VC-Issuer und Verifier hinweg.

iv. Nachvollziehbarkeit: VDRs tragen dazu bei, die Interaktionen zwischen den Entitäten des Ökosystems transparenter und nachvollziehbarer zu machen. Sie unterstützen die Einhaltung von Vorschriften, indem sie die Nachvollziehbarkeit (Auditability) der Ausstellungs- und Überprüfungsprozesse von Nachweisen ermöglichen.

2. Analyse von Verifiable Data Registries

2.1. Anforderungen

Die Anforderungen an Speicherlösungen für Verifiable Data Registries im Verifiable-Credential-Ökosystem drehen sich vor allem um Sicherheit, Transparenz und die spezifischen Bedürfnisse des jeweiligen Anwendungsfalls. Die Anforderungen ergeben sich aus verschiedenen Quellen, darunter Standards und Richtlinien, technische Spezifikationen, regulatorische Anforderungen, Best Practices und Anforderungen aus Anwendungsfällen. Nachfolgend wird eine nicht abschließende Liste einiger zentraler Anforderungen angeführt:

1. Sicherheit: Die Speicherlösung muss sicher sein, um unbefugten Zugriff oder Manipulation zu verhindern. Das ist entscheidend, wenn sensible Daten wie Identitätsnachweise gespeichert werden.
2. Transparenz: Die Lösung sollte transparent sein und eine einfache Überprüfung der Daten ermöglichen. Das ist besonders bei Distributed Ledgers oder Blockchains wichtig, bei denen Daten öffentlich überprüfbar sein müssen.
3. Verfügbarkeit: Die Speicherlösung sollte hochverfügbar sein, damit jederzeit auf die Daten zugegriffen werden kann, wenn sie benötigt werden.
4. Eignung für den Anwendungsfall: Die Wahl zwischen einer vertrauenswürdigen Datenbank, einem zentralisierten Ledger oder einem Distributed Ledger hängt weitgehend von den spezifischen Anforderungen des Anwendungsfalls ab. Zu berücksichtigen sind unter anderem der Bedarf an Zentralisierung oder Dezentralisierung, die erforderliche Geschwindigkeit und Effizienz sowie das Maß an Vertrauen in die Betreiberin bzw. den Betreiber der Registry.
5. Skalierbarkeit: Mit wachsendem Volumen an Identitätsdaten sollte die Speicherlösung effizient mitwachsen können.
6. Datenintegrität: Die Lösung sollte die Datenintegrität sicherstellen, sodass die Daten über ihren gesamten Lebenszyklus korrekt und konsistent bleiben.
7. Manipulationserkennung (Tamper-evident): Die Speicherlösung sollte Manipulationen erkennbar machen, das heißt, jede Veränderung der Daten sollte leicht feststellbar sein.
8. Unveränderlichkeit (Immutability): Für manche Anwendungsfälle kann es nötig sein, dass die gespeicherten Daten manipulationssicher sind. Das ist ein zentrales Merkmal von Ledgers: Sobald eine Transaktion aufgezeichnet ist, kann sie nicht mehr verändert werden. Dieses Merkmal ist grundlegend für den sicheren Austausch von Informationen wie DID Documents.
9. Dezentralisierung: In manchen Fällen kann eine dezentrale Lösung erforderlich sein, um einen Single Point of Failure zu vermeiden und sicherzustellen, dass keine einzelne Entität die Kontrolle über alle Daten hat.
10. Interoperabilität: Die Lösung sollte mit anderen Systemen im VC-Ökosystem interoperabel sein. Dazu gehört die Kompatibilität mit verschiedenen Nachweisformaten, Issuer- und Verifier-Systemen und anderen Datenregistern.

Es ist wichtig zu beachten, dass diese Anforderungen weder abschließend noch verpflichtend sind und an die spezifischen Bedürfnisse der Anwendung angepasst werden sollten.

2.2. Funktionalität

Verifiable-Credential-Ökosysteme können sich in ihrer Offenheit für eine Teilnahme unterscheiden. Je nach Ökosystem können für Entitäten wie Anbieter von Wallet-Anwendungen, Credential Issuer und Verifier bestimmte Berechtigungen oder Zertifizierungen erforderlich sein, um beizutreten. Andere Ökosysteme stehen dagegen möglicherweise allen Entitäten uneingeschränkt zur Teilnahme offen. Um diese Zertifizierungen abzubilden, können Verifiable Data Registries die folgenden Funktionalitäten übernehmen:

Trusted Issuer Registry: Eine Trusted Issuer Registry ist eine Art von Verifiable Data Registry, die die öffentlichen Schlüssel von Issuern enthält. Sie dient als verlässliche Quelle, um die Echtheit der von diesen Entitäten ausgestellten Nachweise zu überprüfen. Die Registry stellt sicher, dass der Issuer im Ökosystem anerkannt ist und ihm vertraut wird, und trägt so zur Sicherheit und Integrität des VC-Frameworks bei. Beispiele für Trusted Issuer Registries finden sich in der European Blockchain Service Infrastructure (EBSI) [7] oder in der Trust-service Status List (TSL) nach dem Format ETSI TS 119 612, die über eine Well-Known-URL oder Domain Name System PTR Records (DNS PTR Records) bereitgestellt werden kann, wie im TRAIN-Modell [8].

Trusted Verifier Registry: Verifier spielen im VC-Ökosystem eine zentrale Rolle, da sie für die Überprüfung der in einem Nachweis getroffenen Aussagen verantwortlich sind. Eine Trusted Verifier Registry ist eine Art von Verifiable Data Registry, die die öffentlichen Schlüssel von Verifiern enthält. Damit lässt sich die Identität eines Verifiers während der Überprüfung von Nachweisen verifizieren. So ist sichergestellt, dass auch die Entität, die die Nachweise überprüft, vertrauenswürdig und im Ökosystem anerkannt ist.

Trusted Wallet Provider Registry: Diese Registry führt eine Liste verifizierter und vertrauenswürdiger Wallet-Anbieter. Die Registry stellt sicher, dass diese Wallet-Anbieter bestimmte Standards und Protokolle für Sicherheit, Privatsphäre und Interoperabilität einhalten.

Credential Schema Registry: Die Credential Schema Registry ist eine Art von Verifiable Data Registry, die die verschiedenen Schemata für Verifiable Credentials speichert. Diese Schemata definieren Struktur und Format der Nachweise, einschließlich der Arten von Aussagen, die getroffen werden können, und der Datentypen dieser Aussagen. Die Credential Schema Registry ist für die Standardisierung im VC-Ökosystem unverzichtbar, da sie es verschiedenen Parteien ermöglicht, Nachweise einheitlich auszustellen, zu überprüfen und zu verstehen.

Revocation Registry: Die Revocation Registry ist eine Art von Verifiable Data Registry, die nachverfolgt, welche Nachweise vom Issuer widerrufen wurden. Das ist entscheidend, weil Verifier so prüfen können, ob ein vorgelegter Nachweis noch gültig ist oder vom Issuer widerrufen wurde. Dadurch bleiben die Nachweise aktuell und relevant, was zum Gesamtvertrauen im VC-Ökosystem beiträgt.

Trusted Accreditation Organization Registry: Diese Registry speichert die Liste der Organisationen, die berechtigt sind, die Trusted Issuer und die Trusted Verifier des Ökosystems zu akkreditieren.

Public Keys Registry: Registry, die die öffentlichen Schlüssel von Entitäten in Verifiable-Credential-Systemen speichert und verwaltet. In dezentralen, nutzerzentrierten Identitätssystemen. Beispielsweise erlaubt die Issuer Public Key Registry den Verifiern, die Echtheit des Nachweises zu prüfen, indem sie die

Signatur auf dem Nachweis mit dem gespeicherten öffentlichen Schlüssel des Issuers vergleichen.

Jedes Mal, wenn eine Nutzerin bzw. ein Nutzer einem Verifier einen Nachweis präsentiert, konsultiert der Verifier diese Trust Registries. Je nach anwendungsspezifischen Anforderungen können die folgenden Prüfungen ausgeführt werden, damit der Nachweis als erfolgreich validiert gilt [9] :

- Das Format des Nachweises entspricht einem Schema, das in der Credential Schema Registry gelistet ist.
- Der Nachweis wurde von einem Issuer ausgestellt, der in der Trusted Issuers Registry enthalten ist.
- Die im Nachweis enthaltene Signatur des Issuers kann mit dem zugehörigen öffentlichen Schlüssel des Issuers überprüft werden, der in der Public Keys Registry gelistet ist.
- Der Nachweis wurde nicht widerrufen und ist in der *Revocation Registry* als gültig gelistet.
- Der Nachweis ist in einer zertifizierten und sicheren Wallet gespeichert, die die erforderlichen Sicherheitsstandards erfüllt.
- Der Issuer ist von einer Accreditation Organization berechtigt, Nachweise mit dem entsprechenden Schema auszustellen.

2.3. Lösungen zur Speicherimplementierung

Die Verifiable-Credentials-Standards enthalten keine expliziten Vorgaben, wie die VDR zu implementieren ist. Die meisten vorgeschlagenen Methoden stützen sich auf Distributed-Ledger-Technologien (DLTs), da diese durch ihr Design Manipulationssicherheit und Nachverfolgbarkeit gewährleisten. Es wurden jedoch auch alternative Ansätze eingesetzt. Lösungen zur Speicherimplementierung für VDRs lassen sich allgemein in zentrale und dezentrale Lösungen einteilen. Nachfolgend werden einige Beispiele für jede Kategorie vorgestellt:

2.3.1. Vertrauenswürdige Datenbanken

Vertrauenswürdige Datenbanken sind mit ihren starken Sicherheitsprotokollen und Authentifizierungsmechanismen eine klassische Option zur Speicherung sensibler Daten wie Identitätsnachweisen. Sie können zentral verwaltet werden, das heißt, eine oder mehrere Organisationen kontrollieren, wie auf die Daten der Registry zugegriffen wird, wie sie gepflegt und verteilt werden. Vertrauenswürdige Datenbanken können jedoch auch über mehrere Systeme hinweg betrieben werden oder in einer Cloud laufen. Das Vertrauensmodell für Verifiable Credentials verlangt von der Verifiable Data Registry lediglich, manipulationserkennbar zu sein und korrekt abzubilden, welche Daten von welchen Entitäten kontrolliert werden. Erfüllt daher eine sichere, zentrale oder verteilte Datenbank diese Kriterien, kann sie im VC-Ökosystem als Verifiable Data Registry dienen.

Vertrauenswürdige Datenbanken bieten in der Regel schnelle Datenabrufe und können große Datenmengen verarbeiten, wodurch sie hoch skalierbar sind. Sie nutzen starke Sicherheitsprotokolle, um die Datenintegrität zu wahren. Aufgrund ihrer zentralen Natur können sie jedoch anfällig für Angriffe auf ihren zentralen Ausfallpunkt sein. Außerdem bieten sie möglicherweise nicht dieselbe Transparenz wie manche dezentralen Optionen, was für einige Anwendungsfälle von Bedeutung sein kann.

2.3.2. Zentralisierte Ledgers

Zentralisierte Ledgers, wie Amazon QLDB [10], werden von einer zentralen Instanz verwaltet und betrieben. Nutzende dieser Ledgers vertrauen darauf, dass die Inhalte nicht manipuliert wurden, indem sie der Betreiberin bzw. dem Betreiber des Ledgers vertrauen. Diese Ledgers haben einige wesentliche Eigenschaften, die sie für Verifiable-Credentials-Dienste im Unternehmensumfeld besser geeignet machen. Zentralisierte Ledgers wie QLDB benötigen beispielsweise keinen Konsensmechanismus wie Distributed Ledgers, was sie als Verifiable Data Registry schneller, effizienter und oft kostengünstiger macht.

2.3.3. Distributed Ledgers

Distributed Ledgers hingegen enthalten Daten, die über mehrere Systeme oder Entitäten hinweg repliziert, geteilt und synchronisiert werden. Die Blockchain ist ein bekanntes Beispiel für einen Distributed Ledger. Die Inhalte des Ledgers werden gemeinsam von allen Entitäten überprüft, die einen Node betreiben, was eine Manipulation der Daten erschwert. Je nach verwendeter Distributed-Ledger-Technologie können Einträge öffentlich überprüft werden, sodass sich leicht feststellen lässt, ob ein Nachweis verändert wurde. Diese Eigenschaft ist besonders wichtig für den sicheren Austausch von Informationen im Zusammenhang mit DIDs [11].

2.3.4. Distributed Hash Tables (DHT)

Eine DHT ist ein dezentrales verteiltes System, das einen Lookup-Dienst ähnlich einer Hash-Tabelle bereitstellt. Beispiele sind das BitTorrent-Protokoll oder das Distributed-Hash-Table-Netzwerk, das vom IPFS (InterPlanetary File System) verwendet wird. DHTs sind dezentrale Systeme, die große Datenmengen effizient verarbeiten und Daten im Netzwerk schnell auffinden können. Sie können jedoch langsamer sein als zentrale Datenbanken, da über mehrere Nodes hinweg gesucht werden muss. Das kann ein Zielkonflikt zur höheren Widerstandsfähigkeit gegenüber Fehlern und Ausfällen sein, die diese verteilten Systeme bieten.

2.3.5. Verteilte Dateisysteme

Verteilte Dateisysteme wie das Hadoop Distributed File System (HDFS) [12] sind auf hohe Skalierbarkeit und Zuverlässigkeit ausgelegt. Sie verteilen Daten über mehrere Nodes, was die Datenredundanz und die Fehlertoleranz erhöhen kann. Aufgrund der verteilten Natur dieser Systeme kann der Datenabruf jedoch langsamer sein als bei zentralen Systemen.

2.3.6. Content Delivery Networks (CDNs)

CDNs [13] wie Akamai oder Cloudflare können große Datenmengen verarbeiten und Inhalte schnell ausliefern. Ihr globales Netzwerk aus Servern arbeitet zusammen, um hohe Verfügbarkeit und Leistung zu bieten. Sie können jedoch ebenfalls anfällig für zentralisierte Angriffe sein und bieten möglicherweise nicht dieselbe Kontrolle über die Daten wie manche anderen Optionen.

Zusammenfassend bieten Distributed Ledgers und Blockchains zwar robuste Sicherheit und Transparenz, können aber wegen des für die Datenüberprüfung nötigen Konsensprozesses weniger effizient sein. Sie werden daher typischerweise für Anwendungsfälle gewählt, in denen Daten öffentlich verfügbar sein

müssen und eine dezentrale Instanz gefordert ist.

Die Wahl zwischen einer zentralen oder dezentralen Speicherlösung als Trust Registry im VC-Ökosystem hängt weitgehend von den spezifischen Anforderungen des jeweiligen Anwendungsfalls ab. Jede hat ihre eigenen Stärken und möglichen Nachteile. Die Entscheidung sollte anhand von Faktoren wie dem Bedarf an Zentralisierung oder Dezentralisierung, der erforderlichen Geschwindigkeit und Effizienz sowie dem Maß an Vertrauen in die Betreiberin bzw. den Betreiber der Registry getroffen werden.

3. Widerruf von Verifiable Credentials

Trotz der zahlreichen Vorteile von VCs sind noch mehrere technische Herausforderungen zu bewältigen. Eine Herausforderung ist die Gestaltung von Widerrufsmechanismen für VCs. Der Widerruf ist ein wesentlicher Prozess, mit dem Issuer einen zuvor ausgestellten Nachweis für ungültig erklären können. Das kann in bestimmten Fällen nötig sein, etwa wenn die in einem Nachweis enthaltenen Identitätsinformationen einer Person nicht mehr zutreffen oder wenn der Nachweis irrtümlich oder betrügerisch ausgestellt wurde.

Verifier müssen sowohl den Status als auch die Gültigkeit der VCs bestätigen, um das Vertrauen zwischen Issuer, Nutzenden und Verifier zu wahren. Ohne ein solches Widerrufsframework steigt die Wahrscheinlichkeit betrügerischen Verhaltens, was Vertrauen und Glaubwürdigkeit im gesamten VC-Ökosystem untergräbt. Trotz des wachsenden Interesses an VCs befinden sich effiziente Widerrufsmethoden noch in einem frühen Entwicklungsstadium, wie auch das Fehlen eines eigenen W3C-Standards zeigt.

In der W3C-Spezifikation wird der Widerrufsstatus eines Nachweises in der Credential-Status-Eigenschaft eines VC ausgedrückt. Bei der Ausstellung des Nachweises kann der Issuer einen Verweis auf eine externe (öffentlich zugängliche) Revocation Registry aufnehmen.

Der Widerruf von Verifiable Credentials kann jedoch bestimmte Risiken für die Privatsphäre mit sich bringen. Dazu zählen Nachverfolgbarkeit, Verknüpfbarkeit, Offenlegung personenbezogener Informationen und unbefugte Widerrufe. Um diese potenziellen Risiken zu verringern, ist es entscheidend, Widerrufsprozesse so zu gestalten, dass die Privatsphäre Vorrang hat. Das lässt sich erreichen, indem eine Revocation Registry gestaltet wird, die es den Credential Issuern erlaubt, die von ihnen ausgestellten Nachweise zu verwalten und dabei zugleich die Anonymität der VC-Inhaberinnen und -Inhaber zu wahren.

3.1. Designüberlegungen zum Widerruf von Verifiable Credentials

Der Widerruf von Verifiable Credentials ist zwar wesentlich für die Integrität und Vertrauenswürdigkeit eines Systems, kann aber bei unsorgfältiger Handhabung ebenfalls Risiken für die Privatsphäre mit sich bringen. Mögliche Risiken für die Privatsphäre sind:

Nachverfolgbarkeit (Traceability): Wenn der Widerrufsprozess die Prüfung eines Nachweises gegen eine öffentlich zugängliche Widerrufsliste umfasst, kann dies möglicherweise die Verfolgung der Aktivitäten der Nachweisinhaberin bzw. des Nachweisinhabers ermöglichen und dadurch deren bzw. dessen Privatsphäre verletzen. Das Abfragen oder der Zugriff auf die Widerrufsstatus-Einträge in den Revocation Registries darf es anderen Entitäten nicht ermöglichen, die Verwendung des VC nachzuverfolgen.

Verknüpfbarkeit (Linkability): Wenn zur Widerrufung eines Nachweises ein eindeutiger Identifikator verwendet wird, könnte dies verschiedenen Parteien ermöglichen, getrennte Aktivitäten oder Transaktionen der Nachweisinhaberin bzw. des Nachweisinhabers miteinander zu verknüpfen. Der in den Revocation Registries gespeicherte Widerrufsstatus-Eintrag darf nicht als global eindeutiger Identifikator oder Korrelator der Nutzerin bzw. des Nutzers dienen.

Offenlegung personenbezogener Informationen: Bei manchen Widerrufsmethoden können personenbezogene Informationen gegenüber dem Verifier oder anderen am Überprüfungsprozess beteiligten Parteien offengelegt werden. Der Zugriff auf den Widerrufs- oder Statuseintrag eines VC darf keine weiteren Informationen über die Nutzerin bzw. den Nutzer preisgeben.

Unbefugte Widerrufe: In nutzerzentrierten Modellen, in denen die Nachweisinhaberin bzw. der Nachweisinhaber die Möglichkeit hat, die eigenen Nachweise zu widerrufen, besteht das Risiko unbefugter oder betrügerischer Widerrufe, wenn keine robusten Sicherheitsmaßnahmen vorhanden sind.

Auch Leistungsaspekte sind beim Entwurf eines Widerrufsmechanismus von größter Bedeutung. Ein wesentlicher Faktor ist die Bandbreite und die Verarbeitungslast, die er sowohl auf der Client-Seite, die die Widerrufsinformationen abruft, als auch auf der Server-Seite verursacht.

3.2. Bestehende Widerrufsmechanismen

Widerrufsmechanismen lassen sich als zentral oder dezentral einteilen, je nachdem, ob eine zentrale Instanz beteiligt ist, die die Revocation Registries verwaltet, oder nicht.

Zentraler Widerruf: Bei diesem Ansatz verwaltet eine zentrale Instanz den Widerrufsprozess und führt eine Liste ungültig gemachter Nachweise. Verifier prüfen diese Liste, bevor sie einen Nachweis akzeptieren, um sicherzustellen, dass er nicht widerrufen wurde. Ein Beispiel für diese Methode ist Let's Revoke [14]. Solche Lösungen können jedoch wegen eindeutiger Nachweisidentifikatoren Datenschutzbedenken aufwerfen, da sie es Verifiern ermöglichen können, die Inhaberin bzw. den Inhaber mit dem konkreten Nachweis zu verknüpfen.

Dezentraler Widerruf: Dezentrale Widerrufsmechanismen nutzen häufig Distributed-Ledger-Technologien (DLTs) oder Smart Contracts und speichern typischerweise eine Widerrufsliste auf einer Blockchain. Zu dieser Kategorie gehören auch Peer-to-Peer-Netzwerke (P2P). Da Ledgers nur Anhängen erlauben (append-only), ist es stets möglich, den Status eines Nachweises zu einem bestimmten Zeitpunkt zu validieren. Im Gegensatz zu einer zentralen Widerrufsliste ist es schwierig, eine Statusänderung rückzudatieren. Auch diese Ansätze können jedoch Datenschutzbedenken aufwerfen.

Die Komplexität des Widerrufs für VCs führt dazu, dass sich schwer eine Universallösung finden lässt. Wie bei den Lösungen zur Speicherimplementierung muss die Widerrufsstrategie entsprechend den Anforderungen des Anwendungsfalls gewählt werden. Nachfolgend werden alternative Implementierungen von Widerrufsmechanismen für VCs angeführt.

3.2.1. Listenbasierter Widerruf

Listenbasierte Widerrufsmethoden verwenden einfache Allow- oder Blocklists. Diese Listen sind öffentlich zugänglich oder können über eine Schnittstelle uneingeschränkt abgefragt werden. Ein Beispiel ist die Certificate Revocation List (CRL), die in der Web PKI verwendet wird.

Andere listenbasierte Widerrufsmechanismen verbergen die Allow- oder Blocklists. Eine vertrauenswürdige Partei verwaltet die Liste und kontrolliert den Zugriff. Dabei können Gruppensignaturen eingesetzt werden, wobei eine Gruppenverwalterin bzw. ein Gruppenverwalter die Liste überwacht und die Anonymität sicherstellt.

Eine weitere Option für listenbasierte Revocation Registries sind komprimierte Listen. Komprimierte Listen verringern die Größe der Informationen und machen Speicherung, Download und Abfrage effizienter. Zur Umsetzung dieser Methoden können Techniken wie Bloom-Filter oder Bit-Arrays verwendet werden. Bitstring Status List 1.0 [15] des W3C (World Wide Web Consortium) ist eine Spezifikation zur kompakten und effizienten Verwaltung und Übermittlung des Status von Entitäten mithilfe von Bitstrings.

Da diese Listen Widerrufsstatus für viele Nachweise enthalten, können die Nachweissubjekte gegenüber der Entität, die die Revocation Registry führt, „Herdenschutz“ (herd privacy) erreichen. Manche Anwendungsfälle erfordern jedoch Widerrufsmechanismen mit einem höheren Maß an Privatsphäre für die Nachweissubjekte.

3.2.2. Akkumulatorbasierter Widerruf

Manche Widerrufsmechanismen nutzen kryptografische Techniken wie akkumulatorbasierten Widerruf oder Zero-Knowledge-Proofs, um den Nicht-Widerrufsstatus eines Nachweises zu belegen, ohne den konkreten Nachweis selbst preiszugeben. Das ermöglicht eine effiziente Widerrufsprüfung, ohne die Privatsphäre zu beeinträchtigen.

Ein Akkumulator ist eine Einwegfunktion, die eine große Menge von Elementen zu einem einzigen Wert zusammenfasst. Akkumulatoren können symmetrisch oder asymmetrisch sein. Asymmetrische Akkumulatoren benötigen für die Mitgliedschaftsprüfung zusätzliche Informationen (den sogenannten Witness). Beispiele sind RSA-basierte, Bilinear-Pairing-basierte und Merkle-Tree-basierte Akkumulatoren. Symmetrische Akkumulatoren wie Bloom-Filter benötigen keine Witness-Informationen.

Darüber hinaus lassen sich Akkumulatoren nach den Nachweisen unterscheiden, die sie unterstützen. Positive Akkumulatoren unterstützen Mitgliedschaftsnachweise, die zeigen, dass ein Element in der Menge enthalten ist. Negative Akkumulatoren unterstützen Nicht-Mitgliedschaftsnachweise, die zeigen, dass ein Element nicht enthalten ist. Universelle Akkumulatoren unterstützen schließlich sowohl Mitgliedschafts- als auch Nicht-Mitgliedschaftsnachweise.

4. Fazit

Zusammenfassend sind Verifiable Data Registries ein Grundpfeiler des Verifiable-Credential-Ökosystems und ermöglichen sichere und vertrauenswürdige Informationsaustausche. Sie bieten eine verlässliche Methode, die Richtigkeit von Identitätsaussagen zu überprüfen, und tragen so zur Gesamtintegrität und zum Vertrauen im System bei.

Einer der herausragenden Vorteile der W3C-Definition von Verifiable Data Registries ist ihr umfassender Charakter und ihre Flexibilität. Sie ist so angelegt, dass sich maßgeschneiderte Verifiable Data Registries schaffen lassen, die Verifiable-Credential-Daten wirksam verwalten. Zudem ist sie anpassungsfähig genug, um eine breite Palette unterschiedlicher Optionen zur Datenspeicherung zu berücksichtigen. Diese Optionen reichen von vertrauenswürdigen zentralen Datenbanken, die von einer einzelnen Instanz

verwaltet werden, über verteilte Datenbanken, die die Daten für mehr Sicherheit und Zuverlässigkeit auf mehrere Standorte verteilen. Weitere Optionen sind Ledgers oder Blockchains, die kryptografische Methoden nutzen, um Datentransaktionen zu sichern und unbefugte Änderungen zu verhindern.

Außerdem kann die Bedeutung gut umgesetzter Widerrufsmechanismen nicht hoch genug eingeschätzt werden. Diese Mechanismen stellen sicher, dass Integrität und Vertrauenswürdigkeit des VC-Systems erhalten bleiben, auch wenn ein VC aus verschiedenen Gründen für ungültig erklärt werden muss. Die Implementierung dieser Mechanismen sollte jedoch mit Sorgfalt erfolgen, um mögliche Risiken für die Privatsphäre wie Nachverfolgbarkeit, Verknüpfbarkeit und die Offenlegung personenbezogener Informationen zu vermeiden.

Letztlich ist es das Ziel eines VC-Systems, ein sicheres, effizientes und nutzerzentriertes Mittel zur Verwaltung und Überprüfung von Nachweisen bereitzustellen. Die Wahl des Vertrauensmodells und der Widerrufsmechanismen sollte sich daher an diesen Prinzipien orientieren.

Im Rahmen dieses Projekts wurden verschiedene Trust-Registry-Optionen untersucht, die sich für die Verwaltung von VC-Daten eignen. Diese Untersuchung erlaubt es, die Vorteile und Einschränkungen jedes dieser alternativen Speichersysteme in verschiedenen Trust Frameworks zu identifizieren. Das Verständnis dieser Aspekte ist entscheidend für die Entscheidungsfindung bei der Wahl eines geeigneten Speichersystems für Verifiable Credentials, abhängig von den spezifischen Anforderungen und Rahmenbedingungen unterschiedlicher Trust Frameworks.

Referenzen

[1] J. Camenisch and B. Pfitzmann, “Federated Identity Management,” *Security, Privacy, and Trust in Modern Data Management*, pp. 213–238, Jun. 2007, doi: 10.1007/978-3-540-69861-6_15.

[2] “Verifiable Credentials Data Model v2.0.” Accessed: Apr. 02, 2024. [Online]. Available: https://www.w3.org/TR/vc-data-model-2.0/

[3] B. Podgorelec, L. Alber, and T. Zefferer, “What is a (Digital) Identity Wallet? A Systematic Literature Review”, doi: 10.1109/COMPSAC54236.2022.00131.

[4] “ISO/IEC 18013-5:2021 - Personal identification — ISO-compliant driving licence — Part 5: Mobile driving licence (mDL) application.” Accessed: Apr. 22, 2024. [Online]. Available: https://www.iso.org/standard/69084.html

[5] K. Yasuda, T. Lodderstedt, D. Chadwick, K. Nakamura, and J. Vercammen, “OpenID for Verifiable Credentials,” 2022, Accessed: May 27, 2024. [Online]. Available: https://www.iso.org/committee/45144.html

[6] A. Papageorgiou, A. Mygiakis, K. Loupos, and T. Krousarlis, “DPKI: A Blockchain-Based Decentralized Public Key Infrastructure System,” *GIoTS 2020 - Global Internet of Things Summit, Proceedings*, Jun. 2020, doi: 10.1109/GIOTS49054.2020.9119673.

[7] “Home - EBSI -.” Accessed: May 27, 2024. [Online]. Available: https://ec.europa.eu/digitalbuilding-blocks/sites/display/EBSI/Home

[8] “A novel approach to establish trust in verifiable credential issuers in Self-sovereign identity ecosystems using TRAIN.” Accessed: May 27, 2024. [Online]. Available: https://dl.gi.de/items/ae2dd3f9-d34b-48a1-9d67-2ee5db2e8df3

[9] “The Role of Trust Registries in an SSI Ecosystem | Gataca.” Accessed: Apr. 02, 2024. [Online]. Available: https://gataca.io/blog/the-role-of-trust-registries-in-an-ssi-ecosystem/

[10] “CRUD Database - Amazon Quantum Ledger Database (QLDB) - AWS.” Accessed: Apr. 02, 2024. [Online]. Available: https://aws.amazon.com/qldb/

[11] P. Dunphy and F. A. P. Petitcolas, “A First Look at Identity Management Schemes on the Blockchain *,” 2018.

[12] “HDFS Architecture Guide.” Accessed: May 27, 2024. [Online]. Available: https://hadoop.apache.org/docs/r1.2.1/hdfs_design.html

[13] “What Is a CDN (Content Delivery Network)? | How Do CDNs Work? | Akamai.” Accessed: May 27, 2024. [Online]. Available: https://www.akamai.com/glossary/what-is-a-cdn

[14] “Let’s Revoke: Scalable Global Certificate Revocation - NDSS Symposium.” Accessed: May 27, 2024. [Online]. Available: https://www.ndss-symposium.org/ndss-paper/lets-revoke-scalableglobal-certificate-revocation/

[15] “Bitstring Status List v1.0.” Accessed: May 27, 2024. [Online]. Available: https://www.w3.org/TR/vc-bitstring-status-list/