WHITEPAPER

Gaia-X-sichere und vertrauenswürdige Ökosysteme mit souveränen Identitäten

Entwicklung eines dezentralen, benutzerzentrierten und sicheren Cloud-Ökosystems

Hinweis: Ausschließlich zum Zweck der besseren Lesbarkeit wird auf geschlechtsspezifische Sprachformen verzichtet. Sämtliche Personenbezeichnungen gelten gleichermaßen für alle Geschlechter.

Gefördert durch:

Bundesministerium
für Wirtschaft
und Klimaschutz

aufgrund eines Beschlusses
des Deutschen Bundestages

Zusammenfassung

Dieses Whitepaper erläutert die wichtigsten Anliegen, die Architektur und die Prinzipien des Konzepts der selbstbestimmten Identität (aus dem Englischen Self-Sovereign Identity, SSI), die im Gaia-X-Ökosystem angewandt werden. Die selbstbestimmte digitale Identität sorgt für eine sichere und vertrauenswürdige Digitalisierung in dem dezentralen Ökosystem, das Gaia-X anstrebt. Das SSI Konzept erlaubt allen, sei es eine Person, eine Organisation oder sogar eine Maschine, digitale Identitäten und die damit verbundenen Anmeldeinformationen wie Mitgliedsausweise, Zertifikate oder Selbstbeschreibungen selbstsouverän zu verwalten, ohne dabei auf ein konventionelles zentrales Identitätsmanagementsystem (IdM) zurückgreifen zu müssen. Kryptostandards und SSI Standards kombiniert mit Web3-konformen Technologiekomponenten ermöglichen es dem Gaia-X-Ökosystem, das erforderliche Maß an Vertrauen zu erlangen, ohne dass zentral gehostete und kontrollierte Identitätsanbieter (IDPs) hinzugezogen werden müssen.

Inhaltsverzeichnis

ZUSAMMENFASSUNG....1
WARUM EIN CLOUD-ÖKOSYSTEM MIT SSI AUFBAUEN?....2
GUTE GRÜNDE, WARUM GAIA-X SSI IMPLEMENTIERT....3
SSI AUF DEN PUNKT GEBRACHT....3
GRUNDSTRUKTUR UND PROZESS DES SSI-ÖKOSYSTEMS....4
DIE ARCHITEKTUR DES SSI-ÖKOSYSTEMS....5
ENSATZ VON SSI BEI GAIA-X FEDERATION SERVICES....9
SSI IM KONTEXT VON DATENAUSTAUSCH UND DATENSCHUTZ....11
SCHLUSSFOLGERUNG....13

Warum ein Cloud-Ökosystem mit SSI aufbauen?

Angesichts des hohen wirtschaftlichen Potenzials der nächsten Generation Web3, im Einklang mit den Anforderungen des Datenschutzes, haben viele Unternehmen und Regierungen die Bedeutung von Selbstbestimmter Identität (SSI) erkannt und bereits mit der Einführung von SSI auf globaler Ebene begonnen. Insbesondere die Apps für Covid-Tracker und Test- und Impfzertifikate haben ihre Einführung beschleunigt. Die Europäische Union investiert stark in den dezentralen Identitätsrahmen ESSIF (European Self Sovereign Identity Framework), der für die nächste Generation der Digitalisierung (Web3) im öffentlichen und privaten Bereich genutzt wird.

Das SSI-Ökosystem wird jedoch von den Nutzern nur akzeptiert und übernommen, wenn es einzigartige Datenschutzvorteile bietet und die verwendeten Technologien zukunftssicher sind. Ein weiterer wichtiger Faktor, um Vertrauen in die digitale Welt der Next Generation zu schaffen, ist die angemessene Community-Unterstützung nach Open-Source-Prinzipien und Standards und die umfassende Einführung gängiger Softwarekomponenten rund um die Cloud Native Compute Foundation (CNCF)[2].

Unternehmerische und soziale Relevanz eines SSI-Ökosystems für digitale Identitäten

Die folgenden Unterpunkte beleuchten Aspekte eines SSI und eines Cloud-Ökosystems, die für Wirtschaft und Gesellschaft relevant sind:

Digitalisierung und Akzeptanz bei den Bürgern

Die Digitalisierung ist wirtschaftlich besonders relevant, da der Einsatz innovativer Technologien dazu beiträgt, Prozesse zu vereinfachen und effizienter zu gestalten. Sie ist daher ein entscheidender Faktor für die Aufrechterhaltung der Wettbewerbsfähigkeit. Viele Nutzer wünschen sich eine Vereinfachung von Prozessen und Verfahren durch digitale Technologien. Allerdings mangelt es an Vertrauen in die Art und Weise, wie Nutzerdaten erhoben, verarbeitet und weitergegeben werden. Unter Verwendung des aktuellen Musters, indem der Benutzer vor dem Zugriff auf einen Dienst umfassende Geschäftsbedingungen akzeptieren muss, weiß der Benutzer oft nicht genau, wofür er die Erlaubnis erteilt.

Trotz dieser Skepsis möchten die Nutzer, dass Unternehmen Vertrauen aufbauen und zurückgewinnen[3]. Sie erwarten, dass Unternehmen verantwortungsvoll und vertrauenswürdig handeln, wenn sie neue Technologien bereitstellen: Nur wenn die Nutzer sich sicher sind, dass ihr Vertrauen gerechtfertigt ist, werden sie neue Technologien und IT-Dienste akzeptieren und nutzen. Der SSI Ansatz kann dazu beitragen, dieses Vertrauen aufzubauen, da er benutzerorientiert und benutzerfreundlich mit granularer Kontrolle der Berechtigungen und der Datennutzung konzipiert wurde.

Die wirtschaftliche Relevanz eines SSI-Ökosystems für digitale Identitäten

Manuell ausgeführte Prozesse und Medienbrüche[1] sind der Grund für ineffiziente Prozesse und beeinträchtigen somit die optimale Produktivität. Daraus lässt sich die wirtschaftliche und politische Relevanz der beschleunigten Digitalisierung ableiten. Anwendungsbeispiele zeigen, wie sich die Optimierung von Lieferketten durch Digitalisierung umsetzen lässt, wobei digitale und gut strukturierte nachprüfbare Anmeldeinformationen einfach, schnell, sicher und vertrauenswürdig verarbeitet werden können. Die Implementierung von digitalen Identitäten und Anmeldeinformationen hat einen außergewöhnlich hohen wirtschaftlichen Nutzen für Unternehmen, die Anwendungen entwickeln.

Der SSI-Ansatz bietet sowohl ein hohes Maß an Souveränität als auch ein enormes wirtschaftliches Potenzial.

---

1) Bei der Informationsverarbeitung tritt ein Medienbruch auf, wenn der über einen Informationsträger empfangene Inhalt in der Übertragungskette des Prozesses auf einen anderen übertragen wird und neu erstellt werden muss.

2) https://www.cncf.io/

3) https://www.dotmagazine.online/issues/building-trust/trustworthiness-creates-trust

Technologische Souveränität

Die technologische Souveränität ist ein zunehmend wichtiger Faktor, da der Mehrwert der Informationstechnologie und des Internets und damit die Daten in allen Branchen kurz- und mittelfristig enorm ansteigen werden. Damit unsere Gesellschaft frei, unabhängig und branchenübergreifend handeln kann, muss die Entwicklung von Kompetenzen und Schlüsseltechnologien in kritischen Schlüsselbereichen gezielt gefördert werden. Nur so kann potenziellen Risiken entgegengewirkt werden, die sich aufgrund von Abhängigkeiten zu den Marktführern ergeben können. Darüber hinaus ist eine frühzeitige Positionierung bei innovativen Technologien und Konzepten von entscheidender Bedeutung, um auf globaler, nationaler und europäischer Ebene wettbewerbsfähig zu bleiben. Dazu müssen Abhängigkeiten abgebaut und der Einsatz zukünftig relevanter Technologien selbstbewusst und vertrauensvoll gestaltet und auch aktiv gefördert werden. Die SSI-Technologie ist für digitale Identitäten von entscheidender Bedeutung und ermöglicht eine größere Autonomie hinsichtlich der Verwertung personenbezogener Daten.

Gute Gründe, warum Gaia-X SSI implementiert

Dem Internet fehlt ein wesentliches Konzept, das für ein dezentrales und nicht-monopolisiertes Internet mit vielen gleichzeitigen Cloud-Diensten und Knoten, so wie Gaia-X es fördern möchte, notwendig ist. Dieser fehlende Teil ist die Identitäts- und Vertrauensebene, die erforderlich ist, um Dienste in Anspruch zu nehmen und vertrauensvoll miteinander zu interagieren.

Heute fehlt es uns oft an Optionen und wir sind gezwungen, uns an einen zentralen Cloud-Identitätsanbieter zu wenden, mit allen Vor- und Nachteilen. In den letzten Jahrzehnten haben wir jedoch erlebt, wie die Welt immer digitaler wurde, und folglich sind mit den damit verbundenen Mentalitätsänderungen viele neue dezentrale Web3-Komponenten entstanden, die dazu beitragen, zum ursprünglichen dezentralen Internet zurückzukehren – so wie es ursprünglich entworfen wurde. Eines dieser Konzepte basiert auf dem Web-Of-Trust-Prinzip, das darauf abzielt, dass der Nutzer seine Identität und die Kontrolle über seine Daten zurückerhält.

SSI auf den Punkt gebracht

Eine digitale Identität ist eine Teilmenge von Inhaberattributen, die zur Identifizierung des Inhabers verwendet werden können. Ein Inhaber besitzt je nach Kontext mehrere digitale Identitäten. Die Teilmenge der Attribute einer Person wird, zusammen mit der digitalen Identität, als Datenidentität bezeichnet. In einem persönlichen Authentifizierungsfall ist der Benutzername die digitale Identität. Das Passwort wird zur Verifizierung der digitalen Identität verwendet. Bei den weiteren Daten wie vollständiger Name, Adresse und Angaben der Zahlungsart handelt es sich um weitere Identitätsdaten.

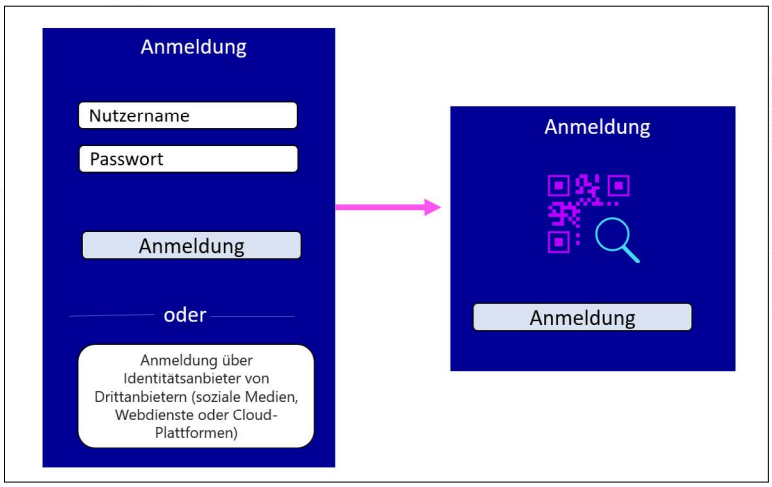

Abb. 1: Login mit dem vorliegenden monopolistischen Identitätsanbietermodell gegenüber selbstverwalteten und nicht monopolistischen Identitätsanbietern

Die in Abbildung 1 gezeigte Abhängigkeit von monopolistischen Identitätsanbietern schafft eine signifikante Abhängigkeit für Gesellschaft, Unternehmen und Nutzern bei der fortschreitenden Digitalisierung der geschäftlichen und persönlichen Lebensbereiche. Darüber hinaus verwenden die monopolistischen Identitätsanbieter, die sich nicht in Gaia-X befinden, die sensiblen personenbezogenen Daten der Nutzer für eigene Werbezwecke oder sonstige wirtschaftliche Interessen oder stellen sie anderen Unternehmen zur Verfügung. Dies geht zulasten der Privatsphäre der Nutzer und hat Konsequenzen für die Akzeptanz und Entwicklung unserer digitalen Zukunft.

Hier soll SSI helfen, da die Souveränität und der Schutz der Privatsphäre der Nutzer im Mittelpunkt des neuen Paradigmas „User-Centric Identity" stehen und viel besser und benutzerfreundlicher implementiert sind als im aktuellen Ansatz der „Enterprise-Centric Identity".

Grundstruktur und Prozess des SSI-Ökosystems

Mit SSI kontrollieren und besitzen Benutzer ihre digitalen Identitäten und andere überprüfbare digitale Anmeldeinformationen lokal. Es ist weder erforderlich, vorherrschende Cloud-Diensteanbieter zu nutzen, noch ist der Aufbau eines zentralen Gaia-X-Identitätsanbieters nötig. Die Nutzer sind somit völlig unabhängig von Dritten und entscheiden selbst, mit wem sie Identitätsdaten teilen, da alle Identitätsdaten des Nutzers sicher in der SSI-Wallet gespeichert werden.

Mit SSI benötigt ein vertrauensvoller und einfacher Peer-to-Peer-Austausch zwischen Benutzern und Anwendungen keinen Mediator.

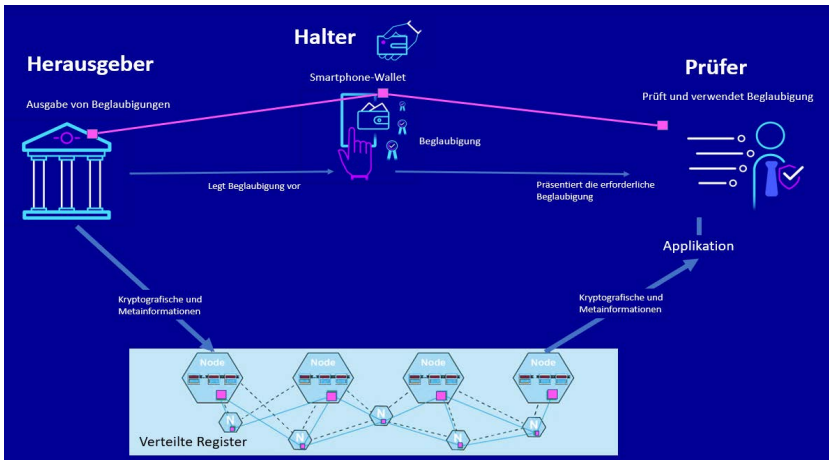

Abb. 2: SSI-Ökosystem für digitale Identitäten und Anmeldeinformationen

Im SSI-Ökosystem für digitale Identitäten spielen drei Akteure eine wesentliche Rolle, die mit der SSI-Infrastruktur interagieren (Prinzip: Vertrauensdreiecksmodell), siehe Abbildung 2. Jeder dieser Akteure hat eine definierte Aufgabe.

Ausstellende überprüfbarer Anmeldeinformationen

Im SSI-Ökosystem stellen *Ausstellende* überprüfbare digitale Anmeldeinformationen bereit, einschließlich spezifischer Ansprüche (eine Sammlung von sogenannten überprüfbaren Anmeldeinformationen), wie z. B. Zertifikatsansprüche auf Identitäten, Bestätigungen, Qualifikationen, Berechtigungen oder Mitgliedskarten. Beispiele im Gaia-X-Ökosystem sind Gaia-X-Anmeldeinformationen von Mitgliedern, ISO-27001-Zertifizierungen, BSI-C5-Bescheinigung, Servicebeschreibungen usw., die in Gaia-X als überprüfbare und bestehende Selbstbeschreibung erscheinen (W3C verifizierbare Präsentation – VP).

Inhaber (Benutzer) überprüfbarer Anmeldeinformationen

SSI bezeichnet einen *Inhaber* als Benutzer, Organisationen oder technische Geräte, die über legitimierte Anmeldeinformationen verfügen. In der Regel verwaltet der Inhaber diese Anmeldeinformationen sicher in seiner entsprechenden SSI-fähigen digitalen Brieftasche, einem sogenannten SSI-Wallet-Agent mit einer wählbaren Funktion zur Datenweitergabe.

Der Wallet-Agent ist nicht an ein mobiles Gerät gebunden. Aus den umfangreichen Angeboten, die als integrierte Browser-Erweiterungen, als selbst gehostete oder cloudgehostete Backend-Variante und natürlich in der klassischen Form einer App für mobile Endgeräte zur Verfügung stehen, kann der Inhaber selbstständig die passende Wallet auswählen. Dies ermöglicht es dem jeweiligen Inhaber, nur die überprüfbaren digitalen Anmeldeinformationen mit den entsprechenden Anwendungen zu teilen, die für den anfänglichen Prozess unerlässlich sind. Es sind keine weiteren Informationen erforderlich.

Überprüfung von Attributen der Anmeldeinformationen

Die *Verifizierer* oder Akzeptanzstellen in diesem SSI-Ökosystem – z. B. der Verbraucher in Form einer Anwendung oder einer Person – benötigen überprüfbare digitale Anmeldeinformationen, um den Inhalt des Dateninhabers, Teile davon oder sogar Aussagen über bestimmte Attribute in einem Prozess oder einer Anwendung (offline oder online) zu nutzen und weiterzuverarbeiten.

Idealerweise geschieht dies vollautomatisch in einem digitalisierten Prozess, der besonders sicher und eindeutig ist – und zwar dank der Verifizierung der digitalen Unterschrift. Bei diesem Überprüfungsprozess werden der Inhalt und der Ausstellende eindeutig kryptografisch verifiziert, ohne dass eine direkte Verbindung zum Ausstellenden erforderlich ist.

Die Architektur des SSI-Ökosystems

Die fortschrittlichen Web3-Architekturkonzepte ermöglichen im Gegensatz zu den alten Cloud-Architekturen die Etablierung eines dezentralen und selbstsouveränen Ökosystems. Dies führt dazu, dass die Zukunft des digitalen Identitätsmanagements in der Europäischen Union sicher, vertrauenswürdig und datenschutzfreundlich wird.

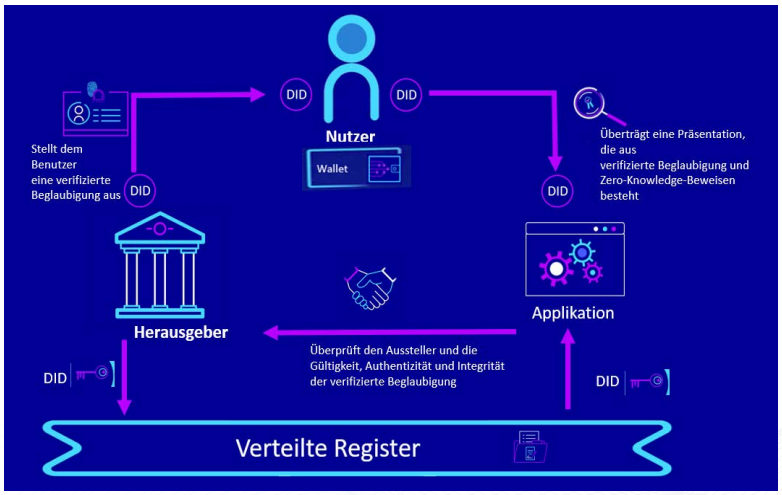

Abb. 3: Überblick über die SSI-Architektur

Der Web3-Architekturstil unterstützt das Hauptprinzip der Selbstverwaltung, bei dem Benutzer ihre digitalen Identitäten selbst erstellen und verwalten. Das gesamte Ökosystem profitiert von diesem Konzept des dezentralen Aufbaus, das sowohl einen einzigen Kontrollpunkt als auch eine einzelne Fehlerstelle im föderierten Gaia-X-Ökosystem vermeidet.

Das Ziel eines solchen Aufbaus besteht darin, die Interoperabilität zwischen verschiedenen SSI-Lösungen zu ermöglichen. Selbstbestimmte Identität (SSI) verwendet die W3C-Spezifikation, dezentrale Identifikatoren (DID), um eindeutige Kennungen für alle Arten von Objekten und Organisationen auszudrücken. Die verifizierbaren Anmeldeinformationen (VC) für den standardisierten, kryptografisch gesicherten Daten- und Identitätsaustausch basieren dagegen auf dem etablierten Format JSON (JavaScript Object Notation). Optionale Standards wie DIDComm (DIDCommunications) oder REST (Representational State Transfer) ermöglichen eine transportunabhängige Kommunikation, die über HTTPS, WebSockets, BlueTooth, AMQP (Advanced Message Queuing Protocol), SMTP (Simple Mail Transfer Protocol), NFC (Near Field Communication), Snail Mail usw. für asynchrone und synchrone Nachrichtenstile genutzt werden kann.

Das Konzept der dezentralen Identifikatoren (DIDs)

Ein wichtiges Merkmal des SSI-Konzepts sind dezentrale Identifikatoren (DIDs). Im SSI-Ökosystem sind DIDs weltweit eindeutige und auflösbare Adressen für Organisationen, Einzelpersonen, Unternehmen oder digitale Einheiten wie Gaia-X-Teilnehmer, die als spezielle W3C Uniform Resource Locators (URLs), wie HTTP-URLs, implementiert sind. Die Schaffung und die Verwaltung einer DID hängen nicht von einer zentralen Behörde ab. Sie wird vom Inhaber selbst mit voller Kontrolle über die eigenen Kennungen und das zugehörige Schlüsselmaterial erstellt. In Kombination mit W3C verifizierbaren Anmeldeinformationen (VC) gibt es dem Nutzer die Möglichkeit, sensible Informationen von der Kennung zu entkoppeln und diese öffentlich für die Verwendung von kryptografischen Proof-Systemen sichtbar zu machen. Der Eigentümer wird die DID pro Transaktion selektiv verwenden oder eine neue generieren, um eine Zuordnung zu verhindern.

Wie bei einer URL identifiziert und lokalisiert ein DID ihre entsprechende Ressource, das DID-Dokument. Bei dem DID-Dokument handelt es sich um ein JSON-Objekt (JavaScript Object Notation), in dem die zugehörigen öffentlichen Schlüssel, Lifecycle-Eigenschaften, Service-Endpunkte und Metainformationen enthalten sind. Es gibt keinen Verweis auf personenbezogene Daten im öffentlichen Schlüssel. Das Format einer DID ist in Abbildung 4 dargestellt.

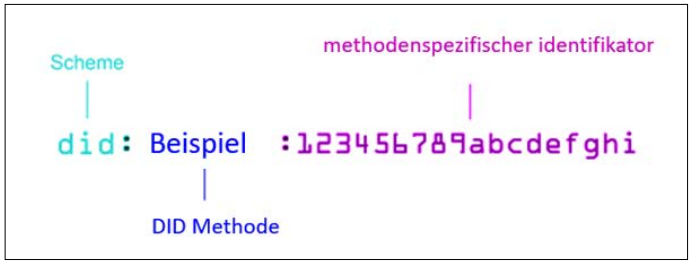

Abb. 4: Dezentrale Kennung (DID)

Das Konzept der verifizierbaren Anmeldeinformationen (VC)

Das Modell der verifizierbaren Anmeldeinformationen definiert ein standardisiertes Format des Datencontainers für kryptografisch signierte und verifizierbare Anmeldedaten und ist auch eine W3C-Spezifikation.

Das Konzept der verifizierbaren Anmeldeinformationen soll IT-Sicherheit, Vertrauen und Datenschutz, die für physische Anmeldedaten gültig sind, durch Kryptografie in den Cyberspace übertragen und diese durch zusätzliche Eigenschaften und Funktionen ergänzen.

Abb. 5: Verifizierbare Anmeldeinformationen

Beispiele für überprüfbare Anmeldeinformationen (siehe Abbildung 6):

- ***Ausweisdokumente*** wie Personalausweise, Rechtsträger-Kennung (GLEIF)
- ***Zertifikate*** wie ISO-27001-Zertifikate, BSI-Sicherheitszertifikate, ITIL- oder TOGAF-Zertifikate
- ***Bescheinigungen***, Gaia-X-Konformitätsstufe, Echtheitszertifikat, Impfbescheinigung
- ***Qualifikationen*** wie die Approbation eines Arztes, Qualifikation als Datenwissenschaftler
- ***Verträge***, die zur Festlegung ausgehandelter Cloud-Service- oder Datennutzungsrichtlinien verwendet werden
- ***Befugnisse*** wie die der Behörden (EU, Gaia-X AISBL) oder Aufenthaltsgenehmigungen
- ***Qualifikationen***, z. B. Nachweis über geschultes Personal zur Verwaltung von Cloud Services
- ***Mitgliedskarten***, z. B. Gaia-X-Mitgliedschaft, Clubkarten, Nachweis der Mitgliedschaft in einem Verein oder einer Gesellschaft
- ***Treuekarten*** wie Bonuskarten oder Vielfliegerprogramme

Diese VCs werden hauptsächlich an Einzelpersonen, juristische Personen oder Geräte ausgegeben. Ein VC bietet in der Regel den gleichen Informationsgehalt wie ein vergleichbarer physischer Nachweis (Personalausweis, Mitgliedskarte).

Im Gegensatz zu einfachen Datenformaten wie JSON (JavaScript Object Notation), XML (Extensible Markup Language), CSV (Comma-Separated Values file) oder sogar unstrukturierte PDF-(Portable Document Format)-Dokumente kombiniert das standardisierte und verifizierbare W3C-Anmeldedatenmodell:

- die Notwendigkeit der Absicherung durch digitale Unterschriften,
- gut geformte Datenstrukturen für die digitale Verarbeitung mittels JSON (JavaScript Object Notation),
- das Hinzufügen von Bedeutung und Semantik zu den Datenstrukturen pro verknüpftem Datenschema mit dem JSON-LD-Standard (JavaScript Object Notation Linked Data) und
- Nachweismechanismen

durch die Anwendung des Konzepts der dezentralen Identitäten.

Grundsätzlich bestehen VCs aus Anforderungen oder Behauptungen, die zu einem bestimmten Thema gemacht werden, z. B. dass eine Person einen Universitätsabschluss hat oder dass ein Gebäude eine bestimmte Höhe hat. Des Weiteren besteht ein VC aus Meta-Informationen, die z.B. die Art, das Ablaufdatum oder den Aussteller des VC angeben. Mit dem Ziel, die Authentizität, Integrität und Herkunft eines VC kryptografisch sicher und überprüfbar zu machen, verwenden die Ausstellenden auch die digitale Signatur-Suite, um eine digitale Unterschrift oder einen kryptografischen Nachweis für einen VC zu erstellen.

Der Nachweis belegt, dass ein VC und dessen Anforderungen zu einem Thema tatsächlich von einem bestimmten Aussteller an einen bestimmten Benutzer ausgestellt wurden. Sowohl die betreffende Person als auch der Ausstellende eines VC können über ihre jeweiligen DIDs referenziert und verifiziert werden. Da die DID des Ausstellenden in dem überprüfbaren digitalen Nachweis enthalten ist, kann das entsprechende DID-Register auch mit dem öffentlichen Schlüssel identifiziert werden, der für die Überprüfung erforderlich ist, siehe Abbildung 6.

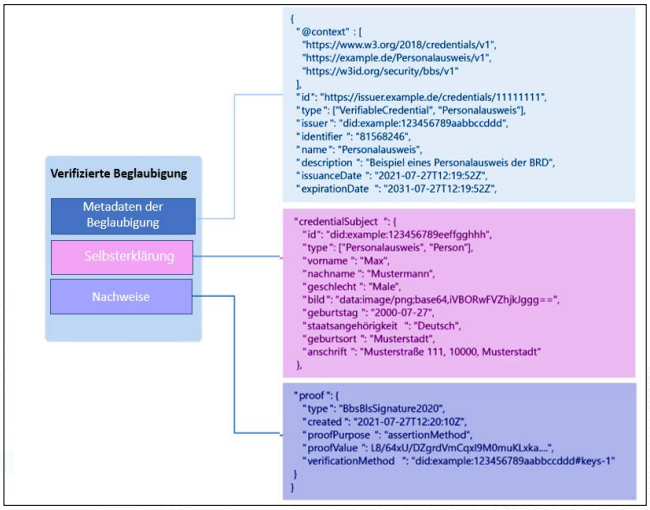

Abb. 6: Beispiel für eine verifizierbare Anmeldeinformationen

Verifizierbare Anmeldeinformationen sind die Grundlagen einer Selbstbeschreibung

Die Selbstbeschreibung (aus dem Englischen Self-Description, SD) ist ein wichtiges Element der Gaia-X-Architektur, die Dienste, Teilnehmer und Datenbestände beschreibt. Sie deckt Metadaten und genau definierte Angaben ab, auf die sich die Verbraucher verlassen können. Sie verwendet die sicheren VC-, W3C-Standards, DID und die zugehörigen Austauschprotokolle, um Daten mit deren Eigenschaften zu definieren und auszutauschen.

Grundsätzlich können Gaia-X-Selbstbeschreibungen als verifizierbare Präsentationen angesehen werden, die von VCs zusammengestellt werden, die Anforderungen oder Behauptungen zu einem bestimmten Thema ausdrücken, z. B. dass ein Teilnehmer ein Mitglied von Gaia-X oder der Besitzer eines bestimmten Datensatzes ist.

Darüber hinaus werden die Selbstbeschreibungsdaten und Anmeldeinformationen von der Gaia-X-Federation-Services-(GXFS)-Komponente, dem Organisational Credential Manager (OCM), verwaltet. Es fordert eine Schnittstelle an, die der GXFS-Katalog und die GXFS-Teilnehmer verwenden, um verifizierte Informationen für die Indexbildung und zukünftige Dienstauswahlprozesse zu sammeln.

Verifizierbare Anmeldeinformationen sind die Grundlage des Gaia-X-Trust-Frameworks und des Labelling-Konzepts

Da Gaia-X als digitale Plattform ein höheres und beispielloses Maß an Vertrauen bietet, muss Gaia-X dieses Vertrauen für alle Teilnehmer leicht verständlich und umsetzbar machen. Zu diesem Zweck ist Gaia-X dabei, ein sicheres Labelling-Framework zu entwickeln, das alle erforderlichen Tests und Verifizierungen automatisiert, um einem Dienst ein spezifisches Label zu verleihen.

Gaia-X wird das Trust Framework eines Dienstattributs gemäß den für ein bestimmtes Label bzw. eine Labelebene festgelegten Attributs überprüfen, wobei externen Behörden (Regierungs-, branchenspezifischen, Normungsgremien usw.) jedoch die Möglichkeit gegeben wird, domänenspezifische Labels zu definieren. Labels bieten ein gewisses Maß an Sicherheit, ohne langwierige und schwer auszumachende Dienst-Anmeldeinformationen prüfen zu müssen.

Ein einzelnes Label kann auf mehreren Trust Framework-Kriterien basieren, von denen jedes ein oder mehrere verifizierbare Anmeldeinformationen enthalten kann. Daher erleichtern Labels die Gruppierung von Kriterien und verbergen die Komplexität ihrer Verifizierung hinter dem Gaia-X-Trust-Framework und dem Labelling-Framework.

Die Implementierung eines Labels besteht aus der Aufteilung aller Label-Anforderungen in überprüfbare Anmeldeinformationen, die dann im Gaia-X-Trust-Frameworks und im Labelling-Framework kodiert werden, damit sie, wenn möglich, automatisch verifiziert werden können. Der Aussteller eines Labels kann Gaia-X oder ein anderer Aussteller sein, der von der Gaia-X European Association for Data and Cloud AISBL verifiziert und akzeptiert wird.

Gaia-X-Registrierung

Darüber hinaus kann zur Sicherstellung eines fälschungssicheren Prüfszenarios idealerweise ein entsprechendes Verzeichnis (Distributed Ledger Technology – DLT) als zusätzliche Vertrauensebene verwendet werden. DLT wird als überprüfbares Datenregister (VDR) für die sichere und vertrauenswürdige Freigabe öffentlicher Schlüssel verwendet, um kryptografischen Schutz aufgrund eines anonymen Widerrufsregisters zu gewähren. Dieses Konzept kann langfristig als Ersatz für die klassische Infrastruktur für öffentliche Schlüssel (PKI) mit ihren zentralisierten Nachteilen gesehen werden. Das Konzept der dezentralen Identität (DID) ermöglicht es Gaia-X, verschiedene dezentrale Register – sogar Standard-Webdomains – zu verwenden, die als weitere Vertrauenskomponente zwischen den Akteuren fungieren.

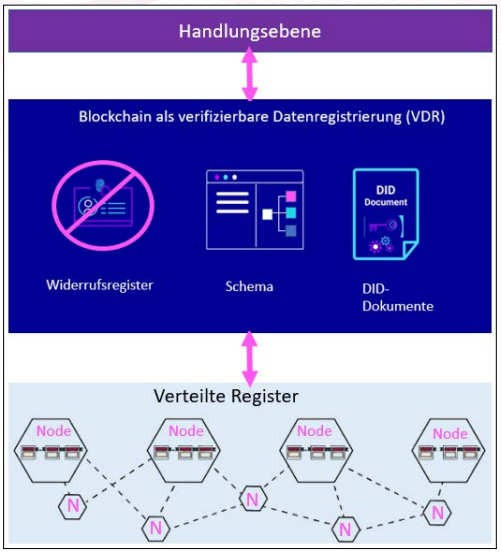

Abb. 7: Verteiltes Register als überprüfbares Datenregister

Vertrauenswürdige Kommunikation

SSI führte das Konzept der SSI-Agents vor der Wallet als Benutzeroberfläche ein, die Kommunikationsprotokolle wie DIDComm (Decentralized Identity Communication) oder OIDC (OpenID Connect) für den sicheren Agent-zu-Agent-Datenaustausch implementiert. Mit dieser Trennung versucht die Gemeinschaft eine hohe Standardisierung von Prozessen und Protokollen zu schaffen, um eine höchstmögliche Interoperabilität zwischen verschiedenen SSI-Lösungen und Anmeldesystemen zur Verfügung zu stellen.

Daher werden die Agent Rahmenwerke dazu verwendet, dass dezentrale Identitäten (DIDs) und verifizierbare Anmeldeinformationen (VCs) miteinander kommunizieren und sich untereinander austauschen können. Üblicherweise ist ein Wallet auch Teil eines Agents, in dem die ausgegebenen VCs sicher gespeichert werden können. Es gibt verschiedene Arten von Agents, aber in der Regel wird zwischen mobilen und Cloud- oder institutionellen Agents unterschieden. Während mobile Agents auf dem Smartphone in Form von Anwendungen vorhanden sein können, sind Cloud-Agents Anwendungen oder Dienste, die auf einem Server betrieben werden, siehe Abbildung 8.

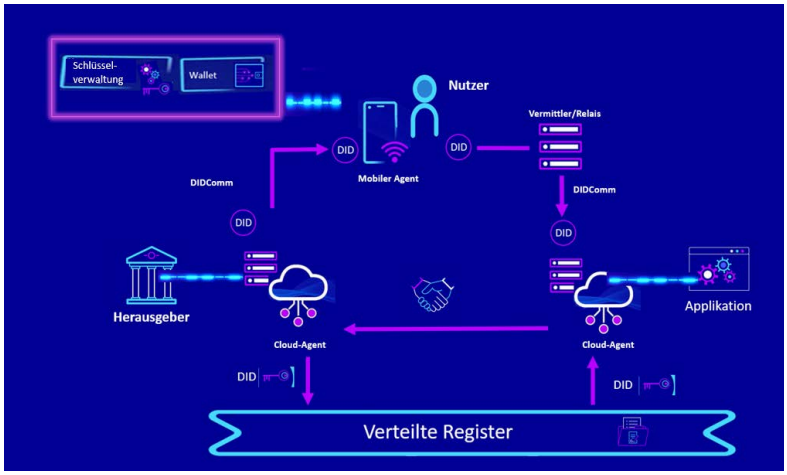

Abb. 8: Konzeptbild SSI-Agents und DIDComm

Die Standardisierungsbemühungen des Hyperledger Aries Project, der Decentralized Identity Foundation (DIF) und des W3C (World Wide Web Consortium) ermöglichen nicht nur die Interoperabilität auf der Client-Ebene, sondern reflektieren auch die zugrunde liegende Registrierungsebene. Man wird in der Zukunft weniger von Hyperledger Indy als Blockchain-basiertes Register für SSI-Rahmenwerke abhängig sein. Dies hat dazu geführt, dass die Anbieter von SSI flexiblere Register in Form von Distributed Ledger Technology (DLT) gewählt haben.

Einsatz von SSI bei Gaia-X Federation Services

In traditionellen, zentralisierten Cloud-Ökosystemen können Identitäten und zugehörige Anmeldeinformationen wie Konten, Gaia-X-Mitgliedschaften, Bescheinigungen oder ISO-Zertifizierungen (International Organization for Standardization) usw. für Verfahren nur schwer auf vertrauenswürdige und datenschutzkonforme Weise ausgetauscht werden.

Würde Gaia-X den SSI nicht nutzen, würde dies das System der zentralen Identitäts- und Vertrauensanbieter, das wir derzeit tagtäglich nutzen, aufrechterhalten. Dieses System hat sowohl Vorteile als auch Nachteile. Nicht zu wissen, wie gut unsere Daten bei diesen zentralen Identitätsanbietern aufgehoben sind und inwieweit sie vor Missbrauch geschützt sind, ist ein Grund, warum Gaia-X-Teilnehmer sie nicht nutzen sollten. Kein Teilnehmer sollte die Kontrolle und Souveränität über seine Daten verlieren oder einem Anbieter die Möglichkeit geben, diese in einigen kritischen Situationen in der Zukunft zu überwachen und einzuschränken. Ein Hauptunterscheidungsmerkmal von Gaia-X ist daher die Fähigkeit, ein vollständig dezentralisiertes und autonom verwaltetes Ökosystem aufzubauen, das im Identitäts- und Vertrauenskonzept der Gaia-X Federation Services (GXFS) verankert ist, wobei jeder Akteur direkt mit jedem anderen Teilnehmer interagieren kann. Neben dem Bereich Identität & Vertrauen wird SSI im GXFS Projekt in verschiedenen Bereichen eingesetzt:

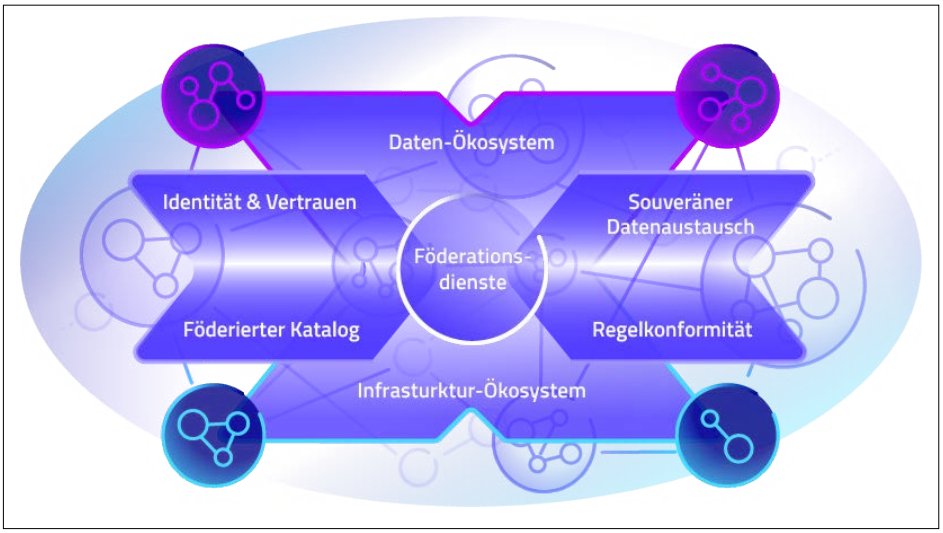

Abb. 9: Gaia-X-Ökosystem

Identität & Vertrauen:

- Selbstausstellender OpenIDProvider (SIOP) für die dezentrale Authentifizierung
- Attributbasierte Berechtigung mit Anmeldeinformationen mittels rollen-basierter Zugriffskontrolle
- Selbstverwaltung von Anmeldeinformationen durch sichere Wallets für Personen und Organisationen
- Software-Agent für selektive Selbstauskunft mit unterzeichneten und überprüfbaren Anmeldeinformationen und Selbstbeschreibungen
- Bereitstellung technischer Vertrauensmethoden und Vertrauensanker-Schnittstellen

Föderierter Katalog:

- Bereitstellung vertrauenswürdiger Daten für die Generierung von Suchindexen durch kryptografisch verifizierbare Selbstbeschreibungen und zugehörige Bescheinigungen
- Vertrauensvolle Verzahnung von Dienstangeboten und Dienstleistern
- Schutz von Selbstbeschreibungsattributen mit selektiver Datenweitergabefunktion

Regelkonformität (Compliance):

- Beglaubigungsfunktion zur Umwandlung von Zertifikaten und Bescheinigungen in Papierformat in entsprechende digitale verifizierbare Anmeldeinformationen
- Ausstellung digitaler und verifizierbarer Mitgliedsdaten mit eIDAS-konformen Unterschriften
- Verwaltung von konformen Vertrauens- und Widerrufslisten für die digitale Verifizierung
- Missbrauchskontrolle

Datensouveränitätsdienste:

- Bereitstellung einer Basis für eine fähigkeitsgestützte Zugriffskontrolle durch Anmeldeinformationen
- Verbesserung des Datenschutzes und des Schutzes durch Zero-Knowledge-Proof, einschließlich selektiver Offenlegungsfunktionen
- Sicherstellung der Authentizität des Dateneigentümers, -anbieters und -verbrauchers auf digital verifizierbare Weise
- Erstellung digitaler unanfechtbarer Datenaustauschverträge
- Aufbau vertrauenswürdiger und sicherer Datenfreigabeverbindungen

Portal:

- Authentifizierung und Zugriffskontrolle mit Bridge-Funktionalität zur Verbindung mit einer bestehenden OpenID-Connect-IAM-(Identity and Access Management)-Infrastruktur

SSI im Kontext von Datenaustausch und Datenschutz

Neben der Datenverschlüsselung ermöglicht die Anwendung von SSI-Zero-Knowledge-Proof-Konzepten und Attribute-Based Access Control (ABAC) zukünftige Null-Trust- und Datenschutzarchitekturen ohne die Nachteile der statischen rollenbasierten Zugriffskontrolle (RBAC). Zero-Knowledge-Proofs (ZKP) sind unter anderem wesentliche kryptografische Funktionen, die einen datenschutzkonformen und datenschützenden Austausch von verifizierbaren Anmeldeinformationen (VCs) im Rahmen von SSI ermöglichen. Mit diesen speziellen digitalen Signatur-Suiten werden VCs vom Ausstellenden in besonderer Weise kryptografisch bei der Erstellung gezeichnet, um die folgenden ZKP-Mechanismen implementieren zu können.

Selektive Offenlegung

Wenn ein Anwender seine VCs als digitalen Nachweis in einer Anwendung verwenden möchte, wird die Anwendung in ihrer Gesamtheit in Form einer Vorlage zur Verifizierung ohne den Einsatz von ZKPs mit den erforderlichen VCs präsentiert. Infolgedessen können Anwendungen deutlich mehr Informationen oder Ansprüche über einen Benutzer erhalten, als für den beabsichtigten Anwendungsfall tatsächlich benötigt werden. Eine selektive Offenbarung kann verwendet werden, um die Informationsübertragung feinkörniger zu gestalten und auf das absolute Minimum zu reduzieren. Mit dieser Funktion ist es möglich, nur bestimmte Ansprüche von einem oder mehreren VCs sicher und vertrauenswürdig offenzulegen und kryptografisch nachzuweisen, siehe Abbildung 10.

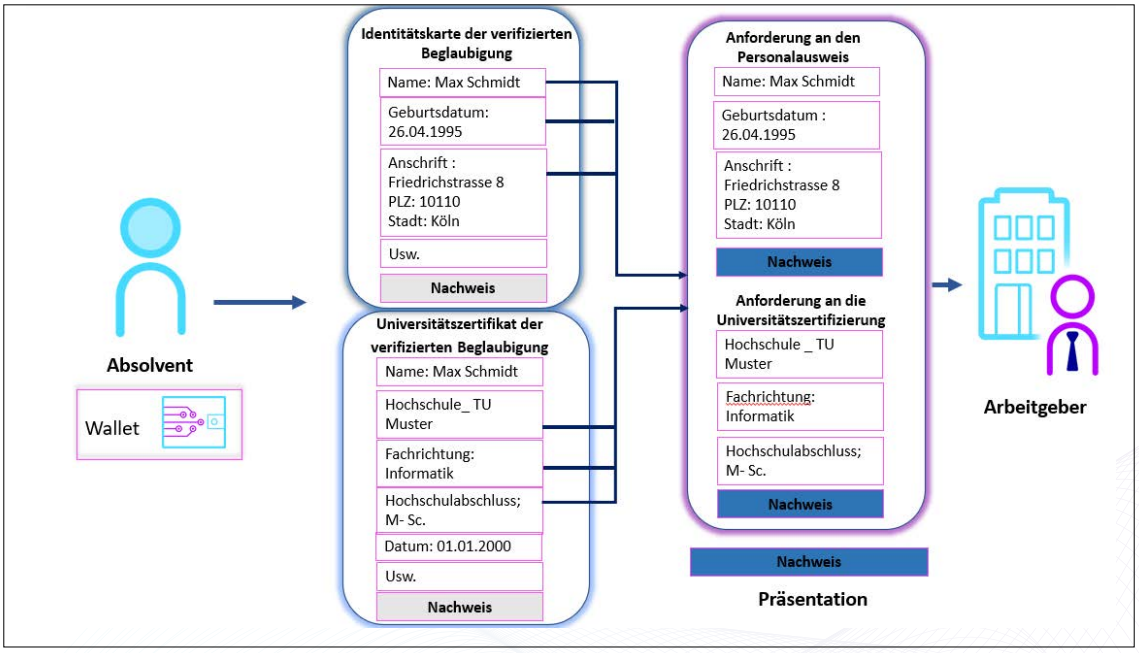

Abb. 10: Gezielte Informationsübertragung durch selektive Offenlegung

Durch die selektive Offenlegung können Informationen innerhalb eines verwendeten VCs, die von der Anwendung nicht angefordert oder benötigt werden, während der Vorlage ausgeblendet werden. Bei der Ausgabe eines VCs verwendet der Ausstellende eine spezielle Multimessage-Signatursuite, um jede Forderung innerhalb des VC einzeln zu signieren. Anstelle eines VCs kann auch eine Teilmenge der Ansprüche eines VCs dargestellt werden, ohne dass die digitale Signatur ihre Gültigkeit verliert. Zudem können bestimmte Anforderungen verschiedener VCs für eine Vorlage verwendet werden.

Ein Beispiel für eine selektive Offenlegung wäre, wenn ein Benutzer seine Adresse an eine Anwendung weitergeben oder einen Nachweis über die Adresse liefen möchte. Der Benutzer kann beispielsweise VCs seines Personalausweises, bestehend aus dem Namen der Forderung, Geburtsdatum, Adresse, Größe etc., verwenden und nur den Namen der Forderung und die Adresse für die Anwendung freigeben. Sämtliche Anforderungen der Anmeldung, die nicht erforderlich sind, werden nicht angezeigt (Geburtsdatum, Größe etc.). Dieses Beispiel zeigt deutlich den Unterschied zwischen einem verifizierbaren Ausweis und einem physischen Ausweis wie einem Pass. Während Funktionen wie die selektive Offenlegung mit überprüfbaren Anmeldeinformationen verwendet werden können, ist es nicht möglich, Informationen selektiv auszublenden, wenn ein physischer Ausweis zur Überprüfung oder Authentifizierung verwendet wird.

Prädikatsnachweise

Prädikatsnachweise sind ein weiterer wesentlicher Bestandteil der Zero-Knowledge-Proofs (ZKP) und helfen oft, die Datenschutz-Grundverordnung (DSGVO) umzusetzen und Datenschutzaspekte einfach und effektiv zu bestätigen, da Informationen kryptografisch verifiziert werden können, ohne dass die Informationswerte an einen Anfragenden weitergegeben werden müssen. Denn anstatt Informationen zu offenbaren, wird kryptografisches Material verwendet, um berechnete Prädikatsnachweise bereitzustellen, wie etwa „größer als 18“, „kleiner als 18“ oder „gleich“.

Es gibt Anwendungsfälle, in denen beispielsweise geprüft werden muss, ob eine Person zahlungsfähig ist; ein Prädikat gibt nur die verschlüsselte Information weiter, dass das betreffende Konto bis zu 10.000 € gedeckt ist, ohne den genauen Kontostand mitzuteilen.

Blinde Unterschrift

Ein Dokument, das vom Benutzer an eine Anwendung übermittelt wird, enthält eine Reihe von überprüfbaren Anmeldeinformationen, die vom jeweiligen Aussteller digital unterzeichnet wurden. Mithilfe der digitalen Unterschrift kann die Authentizität und Integrität überprüft werden, daher ist sie für das SSI-Ökosystem von elementarer Bedeutung. Trotz alledem bieten diese digitalen Unterschriften ein potenzielles Ziel für Angreifer, da digitale Unterschriften eindeutige Identifikatoren sind und folglich ein Faktor, der korreliert werden kann.

Blinde Unterschriften werden verwendet, um eine mögliche Korrelation der digitalen Signaturen zu vermeiden. Mit der blinden Unterschrift kann die digitale Unterschrift oder der entsprechende Nachweis eines Ausstellenden kryptografisch ausgeblendet werden, indem die digitale Signatur randomisiert wird, bevor sie in einer anderen Anwendung endet. Während dieses Prozesses bleiben die Gültigkeit und die Herkunft von verifizierbaren Anmeldeinformationen (VCs) und Anträgen überprüfbar.

Bindung des privaten Inhabers

Mit der privaten Inhaberbindung ist es möglich, einen VC kryptografisch an einen Benutzer zu binden und diese Verbindung später nachzuweisen, ohne die dezentrale Identität (DID) des Benutzers zu verwenden oder offenzulegen. Hierzu werden einzelne Linkgeheimnisse verwendet, mit denen VCs kryptografisch verknüpft werden können. Der Vorteil durch die indirekte Verbindung des VC mit dem Benutzer besteht darin, dass die DID nicht mehr als eindeutiger Verbindungsfaktor benötigt wird und somit eine kryptografische und datenschutzfreundliche Alternative darstellt.

Schlussfolgerung

Im Gaia-X-Ökosystem fördert die Verwendung von offenen W3C-Spezifikationen (World Wide Web Consortium) wie den dezentralen Identifikatoren (DID) und dem Datenmodell der verifizierbaren Anmeldeinformationen (VC) sowie von Open-Source-Projekten wie Hyperledger Aries, ESSIF (European Self-Sovereign Identity Framework) oder IDUnion die kontinuierliche Weiterentwicklung der Selbstbestimmten Identität (SSI). Sie ermöglicht auch die Interaktion zwischen SSI-Lösungen und anderen Anmeldeinformationssystemen. Der Einsatz von Web3-Konzepten und dezentralen Technologien ermöglicht es Gaia-X-Mitgliedern, ihre eigene autonome Gaia-X-Föderationen aufzubauen, ohne dass eine zentrale Gaia-X-Kontrollinstanz erforderlich ist.

Verteilte Ledger in Kombination mit dem SSI-Ökosystem sind nicht vorgeschrieben, können jedoch integriert werden, um zusätzliches Vertrauen, Flexibilität und Skalierbarkeit zu generieren. Agents zur Verwaltung der digitalen Identität und Nutzung von fortschrittlichen SSI-Standard-Kommunikationsprotokollen sind sinnvolle Konzepte, die Datenschutz in einer benutzerfreundlichen Anwendung von DIDs und Zero-Knowledge-Proofs-(ZKP)-fähigen VCs ermöglichen, ohne den Benutzer mit ihrer Komplexität und ihrem Verwaltungsaufwand zu überfordern. Das SSI-Ökosystem schließt die Abhängigkeit von einzelnen Marktführern aus und gibt Nutzern die Freiheit, ihre digitale Zukunft unabhängiger und erfolgreicher zu gestalten. Als Beschleuniger der Digitalisierung sorgt SSI für eine schnellere, sicherere und vertrauenswürdigere Digitalisierung. Mit SSI können die Benutzer im Gaia-X-Ökosystem selektiv auswählen, wie viel Privatsphäre sie haben und an welche Partei sie alle oder eine ausgewählte Teilmenge ihrer Identität und der zugehörigen Daten an die Cloud-Anwendungen übermitteln. Dies schafft ein hohes Maß an Privatsphäre, wertorientierte IT und Dienste und damit eine hohe Akzeptanz für die digitale Zukunft.

Autoren:

Berthold Maier (Telekom – T-Systems International), Chefarchitekt und SSI-Experte

Berthold Maier ist seit über zwei Jahrzehnten als Leiter Architektur in den Branchen Industrie, Telekommunikation und öffentlicher Bereich tätig. Er ist Chefarchitekt bei T-Systems für das Bundesamt für Migration und Flüchtlinge (BAMF) und Lead für das Gaia-X Federation Services (GXFS) Arbeitspaket Identität und Vertrauen. Zuvor bekleidete er die Position des CTO von Digital Solutions bei T-Systems.

Prof. Dr. Norbert Pohlmann (eco), Vorstand für IT-Sicherheit

Norbert Pohlmann ist Professor für Informatik auf dem Gebiet der Cybersicherheit und Leiter des Instituts für Internet-Sicherheit - if(is) an der Westfälischen Fachhochschule in Gelsenkirchen, Vorsitzender des Vorstands des Deutschen IT-Sicherheitsverbandes TeleTrusT und Vorstandsmitglied der eco – Association of the Internet Industry.

Verbandsname: Gaia-X European Association for Data and Cloud AISBL
Ansprechpartner: Dr. Vassilia Orfanou, CMO
Telefon: +306974825327
E-mail: vassilia.orfanou@gaia-x.eu
Adresse: Avenue des Arts 6-9, 1210 Brussels, Belgium
Website: www.gaia-x.eu

Name der Firma: eco – Association of the Internet Industry
Ansprechpartner: Mareike Zeisig, Marketing Manager
Telefon: +49 (0) 221 - 70 00 48 - 107
E'-mail: mareike.zeisig@eco.de
Adresse: Lichtstr. 43h, 50825 Köln, Germany
Website: www.gxfs.eu

Gefördert durch:

Bundesministerium
für Wirtschaft
und Klimaschutz

aufgrund eines Beschlusses
des Deutschen Bundestages