Schlussbericht

Teil II

MANDAT

Methoden zum Austausch von unternehmensbezogenen Daten in treuhänderbasierten Datenökosystemen



Projektzeitraum: 01.01.2022 – 31.12.2024

Andreas Harth, Sebastian Schmid, Daniel Schraudner
Friedrich-Alexander-Universität Erlangen-Nürnberg

Tobias Käfer, Christoph Braun
Karlsruher Institut für Technologie

Andreas Both, Thorsten Kastner, Dustin Yeboah
DATEV eG

Das diesem Bericht zugrunde liegende Vorhaben wurde mit Mitteln des Bundesministeriums für Bildung und Forschung unter den Förderkennzeichen 16DTM107A-C gefördert. Die Verantwortung für den Inhalt dieser Veröffentlichung liegt bei den Autor*innen.

Inhaltsverzeichnis

1 Zusammenfassung **III**

2 Durchgeführte Arbeiten und erzielte Ergebnisse **1**
2.1 AP 1: Anwendungsfall, Datenquellen und Infrastruktur 1
2.2 AP 2: Identitäten, Freigabeprozesse und Rechte 6
2.3 AP 3: Verarbeitungstransparenz 16
2.4 AP 4: Integrität von Daten und Analysen 24
2.5 AP 5: Demonstrator, Evaluation und Verbreitung 34
2.6 AP 6: Rechte- und Datenmanagement 39
2.7 AP 7: Projektmanagement und Dissemination 42

3 Wichtigste Positionen des zahlenmäßigen Verwendungsnachweises **45**
3.1 Friedrich-Alexander-Universität Erlangen-Nürnberg 45
3.2 Karlsruher Institut für Technologie (KIT) 46
3.3 DATEV eG 47

4 Notwendigkeit und Angemessenheit der geleisteten Arbeit **48**

5 Verwertbarkeit der Ergebnisse **49**
5.1 Wissenschaftlich-technische Erfolge 49
5.2 Voraussichtlicher Nutzen und Verwertungsplan 50

6 Relevante Ergebnisse Dritter **52**

7 Erfolgte und geplante Veröffentlichungen **54**

KAPITEL 1

Zusammenfassung

Im Projekt MANDAT erforschten wir **M**ethoden zum **A**ustausch von unter**n**ehmensbezogenen **Da**ten in **t**reuhänderbasierten Datenökosystemen. Das Ergebnis von MANDAT ist eine methodischen Grundlage für offene, datengetriebene Ökosysteme im Web, insbesondere für Datentreuhänder. Im Rahmen von Datentreuhandmodellen ermöglichen diese Methoden einen breiten und flexiblen Datenaustausch (Portabilität), während gleichzeitig die Kontrolle über die Daten beim Eigentümer verbleibt (Souveränität). Entsprechende Lösungskomponenten bieten eine hohe Wiederverwendbarkeit für die Etablierung von Datentreuhändern sowie für das Einbinden von Systemteilnehmern, insbesondere kleinen und mittelständischen Unternehmen (KMUs). Die entwickelten Methoden nehmen sich der technischen, rechtlichen und ablauforganisatorischen Anforderungen und Herausforderungen, welche bei dem Datenaustausch zwischen Unternehmen (B2B) auftreten, an.

Im Projekt MANDAT entwickeln wir wiederverwendbare Methoden anhand des Anwendungsfalles (AP 1), sich um die Kreditvergabe für ein KMU durch ein Kreditinstitut unter Mitwirkung eines Steuerberaters dreht. Wir adressieren die Fragen von Datenspeichers und -schnittstellen, der Datenfreigabe im Außenverhältnis (AP 3), der Rechtedelegation im Innenverhältnis (AP 2) sowie der Authentizität von geteilten Daten (AP 4) in souveränen Datenteilungsketten. In MANDAT wurden nicht nur Konzepte entwickelt, sondern auch die Praktikabilität der Methoden durch die Implementierung entsprechender wiederverwendbarer Softwarekomponenten (AP 5) sichergestellt und demonstriert.

Als konkrete, wiederverwendbare Lösungen entwickeln wir für MANDAT unter anderem den Rights Delegation Proxy (RPD) zur Verwaltung und Ausübungen von Rechten in Delegationen, den Data Provision Proxy (DPP) zum anonymen Teilen von Daten durch Dritte, die semantisch interoperable Self-Sovereign Identity (SISSI) Architektur um verschiedene Web-basierte Zertifikate interoperable zu machen, und die Authorization App (AuthApp) um den Zugriff und das Teilen von Daten basierend auf Nachfragen zu verwalten.

KAPITEL 2

Durchgeführte Arbeiten und erzielte Ergebnisse

2.1 AP 1: Anwendungsfall, Datenquellen und Infrastruktur

Im Rahmen des Arbeitspaketes 1 wurde der Anwendungsfall konkretisiert, die benötigten Beispieldaten zur Verfügung gestellt sowie die notwendige Infrastruktur für die Entwicklung des Demonstrators und die Evaluierung der Forschungsergebnisse konfektioniert und bereitgestellt.

2.1.1 AP 1.1 Ausarbeitung des Anwendungsfalls

Zielsetzung des Arbeitspakets. Ziel dieses Arbeitspakets war die detaillierte Ausarbeitung des Anwendungsfalls, benötigte Beispieldaten zu identifizieren und datenschutzkonform aufzubereiten sowie in geeigneter Form bereitzustellen.

Durchgeführte Arbeiten und Ergebnisse. Im Austausch mit mehreren Fachabteilungen innerhalb der DATEV eG wurde für den Anwendungsfall „Eröffnung, Durchführung, Überwachung und Beendigung einer Geschäftsbeziehung zwischen Unternehmen unter Berücksichtigung der Datenhoheit“ die Kreditvergabe einer Bank an ein KMU als konkretes, praxisnahes und repräsentatives Anwendungsszenario identifiziert und ausgearbeitet. Der Anwendungsfall fokussiert sich auf die Geschäftsbeziehung zwischen Bank, Unternehmer und Steuerberater am Beispiel eines Kreditvergabeverfahrens mit den Phasen „Anbahnung der Partnerschaft“, „Durchführung und Überwachung der Partnerschaft“ sowie „Beendigung der Partnerschaft“ und bildet typische Datenflüsse sowie Abstimmungsprozesse in einem hochregulierten Umfeld ab. Damit dient er als konkrete, verallgemeinerbare Grundlage zur Erprobung und Weiterentwicklung der im Projekt verfolgten Konzepte und technischen Lösungen. Im Projektverlauf wurde die initial definierte Phase der Anbahnung der Partnerschaft um den Vorgang der Findung von Geschäftspartnern mittels

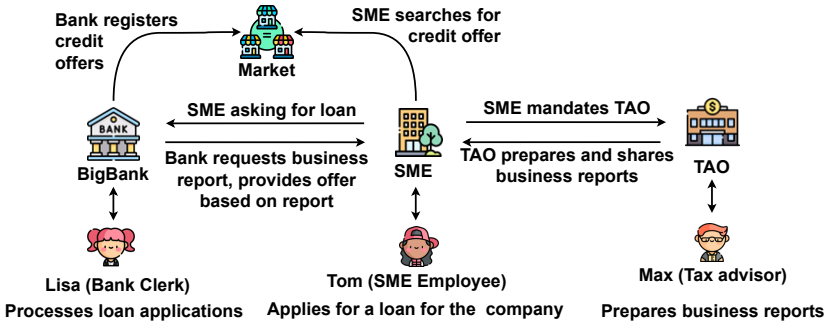


Abbildung 2.1: Finden der Vertragspartner und Anbahnung der Vergabe eines Unternehmenskredits an ein mittelständisches Unternehmen (SME) mit den beteiligten Personen Lisa (Kreditbeauftrage der BigBank), Tom (Unternehmer und Eigentümer des SME), Max (Angestellter des Steuerbüros (TAO), beauftragt von Tom) sowie dem Marktplatz für die Präsentation von und Suche nach Kreditangeboten

eines Marktplatzes erweitert. Abbildung 2.1 zeigt exemplarisch die Phase der Anbahnung der Partnerschaft am Anwendungsfall.

Identifizierte vertragliche und rechtliche Rahmenbedingungen des Anwendungsfalls für die technische Realisierung Im Rahmen des untersuchten Anwendungsfalls der digitalen Kreditvergabe zwischen Bank, Unternehmer und Steuerberater ergeben sich komplexe vertragliche Konstellationen sowie datenschutz- und berufsrechtliche Herausforderungen, die bei der Modellierung eines Datentreuhändersystems zu berücksichtigen sind.

- Zwischen Unternehmer und Bank besteht ein anzubahnendes schuldrechtliches Vertragsverhältnis.
- Zwischen der Bank und dem Steuerberater besteht keine direkte Vertragsbeziehung.
- Der Steuerberater steht in einem berufsrechtlich geregelten Mandatsverhältnis mit dem Unternehmer, das sowohl zivilrechtlich (§ 611 ff. BGB) als auch datenschutzrechtlich als besonders schutzwürdig einzustufen ist.
- Das Mandatsverhältnis unterliegt einem hohen Schutzniveau für sämtliche im Rahmen des Mandats verarbeiteten personenbezogenen und mandatsbezogenen Daten. Es gelten dabei insbesondere die berufsrechtlichen Verschwiegenheitspflichten (§ 203 StGB) sowie die Regelungen der Datenschutz-Grundverordnung (DSGVO), wonach der Steuerberater als eigenständig Verantwortlicher i. S. d. Art. 4 Nr. 7 DSGVO einzustufen ist.
- Für die operative Umsetzung des Anwendungsfalls ist eine klar definierte Trennung von Innen- und Außenverhältnis erforderlich: Natürliche Personen, etwa Bankmitarbeitende, agieren als Erfüllungsgehilfen juristischer Personen (z. B. Banken) und treten gegenüber den anderen Akteuren im Namen der Organisation auf. Daraus

ergibt sich eine differenzierte Betrachtung von Zugriffsrechten, Willenszurechnung und Verantwortlichkeiten.
- Der Steuerberater ist in den Kreditvergabeprozess einzubinden, da er wirtschaftlich relevante Steuerdaten beisteuert. Diese Daten dürfen ausschließlich lesend verwendet und auf Grundlage expliziter Autorisierung weitergegeben, jedoch nicht verändert oder überschrieben werden.
- Zur Wahrung seiner datenschutzrechtlichen Rechenschafts- und Kontrollpflichten muss dem Steuerberater eine vollständige Sichtbarkeit darüber ermöglicht werden, welche durch ihn bereitgestellten Daten verwendet und an Dritte (z. B. Banken) übermittelt wurden. Dies ist erforderlich, um die Anforderungen aus Art. 5 Abs. 2 DSGVO („Rechenschaftspflicht“) sowie berufsrechtliche Dokumentationspflichten zu erfüllen.
- Der Unternehmer verfügt über autarke Zugriffsrechte auf seine Datenbestände. Soweit Daten weitergegeben werden, die vom Steuerberater stammen, ist dieser vor oder zeitgleich zur Weitergabe zu benachrichtigen, um dessen datenschutzrechtliche und berufsrechtliche Stellung zu wahren. Auch in diesem Fall bleibt der Steuerberater Verantwortlicher im Sinne der DSGVO.

Weiterhin wurden auf Grundlage der in AP 1.1 identifizierten Anforderungen für die verschiedenen Phasen einer Geschäftsbeziehung (Eröffnung, Durchführung, Überwachung und Beendigung) die relevanten betriebswirtschaftlichen Prozesse im Kontext der Kreditvergabe analysiert und formal modelliert. Hierfür kamen insbesondere UML-Diagramme zum Einsatz, um Abläufe und Rollen klar strukturiert abzubilden.

Weitere Ergebnisdokumente. Die im Projekt abgeleiteten Anforderungen aus dem Anwendungsszenario wurden in unseren wissenschaftlichen Publikationen genutzt, um die entwickelten methodischen Konzepte zu untermauern und deren Relevanz an einem realitätsnahen Beispiel zu evaluieren, unter anderem in:
- Andreas Both, Thorsten Kastner, Dustin Yeboah, Christoph Braun, Daniel Schraudner, Sebastian Schmid, Tobias Käfer und Andreas Harth. AuthApp - Portable, Reusable Solid App for GDPR-Compliant Access Granting“. ICWE 2024 [6]
- Thorsten Kastner, Christoph Braun, Andreas Both, Dustin Yeboah, Sebastian Josef Schmid, Daniel Schraudner, Tobias Kaefer, Andreas Harth. Data-Sovereign Enterprise Collaboration using the Solid Protocol. SEMANTiCS (Posters & Demos) 2024 [27]
- Andreas Both, Thorsten Kastner, Dustin Yeboah, Christoph Braun, Daniel Schraudner, Sebastian Schmid, Tobias Käfer und Andreas Harth. „Foundational Components for B2B Data Sharing Using the Solid Protocol“. In: Journal of Web Engineering. 2025.(akzeptiert) [7]

Erfüllung der Zielsetzung. Die Zielsetzung des Arbeitspakets wurde erfolgreich erfüllt. Der zentrale Anwendungsfall wurde praxisnah ausgearbeitet und bildete die belastbare Grundlage für die Entwicklung und Evaluation der entwickelten Konzepte. Dabei wur-

den zentrale Rollen, Prozesse und Datenflüsse formal beschrieben und technische Anforderungen an das Rechte- und Datenmanagement abgeleitet. Die hierfür benötigten Beispieldaten wurden datenschutzkonform ausgewählt, aufbereitet und bereitgestellt.

2.1.2 AP 1.2 Konzeptionierung und Bereitstellung von Infrastruktur, Daten und Schnittstellen

Zielsetzung des Arbeitspakets. Das Ziel dieses Arbeitspakets bestand in der Konzeption und initialen Bereitstellung der infrastrukturellen und datentechnischen Grundlage für das Gesamtprojekt. Dabei sollten sowohl beispielhafte Daten als auch eine technische Infrastruktur geschaffen werden, die eine prototypische Umsetzung und Evaluierung des datensouveränen Ansatzes auf Basis der Solid-Technologie ermöglichen: das Solid Protokoll bündelt verschiedene, etablierte Web Standards und ermöglicht unter anderem die eindeutige Authentifizierung von Nutzern im Web und die Autorisierung zur Manipulation von Datenressourcen. Solid zielt darauf ab, einfach zu integrieren zu sein, indem es leichtgewichtige und technisch offene Spezifikationen nutzt und eine dezentralisierte Architektur unterstützt.

Durchgeführte Arbeiten und Ergebnisse. Im Rahmen des Projekts wurde ein technisches Infrastrukturkonzept entwickelt, das die Anforderungen an Wiederverwendbarkeit, Skalierbarkeit, Sicherheit und organisationsübergreifende Zusammenarbeit systematisch adressiert. Die Ausgestaltung erfolgte unter Berücksichtigung folgender Leitlinien:

Konzeptionelle Leitlinien

- Die Entwicklung der Konzepte und Komponenten orientiert sich an offene Standards, um eine hohe Übertragbarkeit, Interoperabilität und Anschlussfähigkeit an bestehende sowie zukünftige Datenökosysteme zu gewährleisten.
- Es wurde ein Fokus auf die Nutzung von Managed Services bzw. *-as-a-Service-Angeboten gelegt, um den operativen Aufwand und Wartungslasten signifikant zu reduzieren.
- Die Architektur unterstützt eine unternehmens- und institutsübergreifende Kollaboration, u. a. durch standardisierte Schnittstellen, eine containerbasierte Infrastruktur und mandantenfähige Zugriffskonzepte.
- Zur Reduzierung des operativen Betriebsaufwands und zur Nutzung etablierter Sicherheitsmechanismen wurde auf Public-Cloud-Infrastrukturen gesetzt. Amazon AWS wurde in Abstimmung mit Projektpartnern – insbesondere DATEV – als Anbieter gewählt.
- Infrastructure-as-Code (IaC) ist als zentrales Entwicklungs- und Betriebsprinzip verankert. Dies gewährleistet eine automatisierte Bereitstellung, versionierbare Änderungsprozesse und eine verbesserte Nachvollziehbarkeit im Lebenszyklus der Infrastrukturkomponenten.
- Als übergeordnete Zielgröße wurde Datensouveränität adressiert.

Umsetzungsschritte und Technologien Die initiale Umsetzung der Infrastruktur orientierte sich an modernen Cloud-nativen Prinzipien und beinhaltete folgende zentrale Elemente:

- Eine containerbasierte Entwicklung mit Docker, um eine hohe Portabilität, Skalierbarkeit und Wartbarkeit sicherzustellen. Für lokale Entwicklungs- und Integrationsprozesse wurde Docker Compose eingesetzt
- Versionsverwaltung sowie die kollaborative Entwicklung der im Projekt entstandenen Softwareartefakte mit GitHub[1]
- Implementierung eines Security-by-Design-Ansatzes, insbesondere durch:
  - Die Verwendung einer Virtual Private Cloud (VPC) Zur Isolierung der Workload.
  - Die Sicherstellung der Vertraulichkeit und Integrität der Container-Artefakte erfolgt mit einer privaten Container Registry (AWS ECR).
  - Die standardmäßige Verschlüsselung von Daten im Ruhezustand (Encryption-at-Rest) sowie optionaler clientseitiger Verschlüsselung mit selbstverwalteten Schlüsseln
  - Verwenden von TLS 1.3 zur Verschlüsselung aller Kommunikationsflüsse (Encryption-in-Transit)
  - Zentralisierte Auditierung aller Zugriffe auf Laufzeitumgebungen der Container (Pods) zur Sicherstellung der Nachvollziehbarkeit und Compliance

Des Weiteren wurden synthetische Beispieldaten für ein Beispielunternehmen bereitgestellt. Diese sollten sowohl zur Validierung der entwickelten Konzepte als auch zur Anbindung an den Demonstrator dienen. Die bereitgestellten Datensätze umfassten unter anderem:

- Betriebswirtschaftliche Unternehmensdaten: Kontobuchungen, Kreditoren und Debitoren, Steuerveranlagungsdaten, Hauptbuchungsdaten aus der Finanzbuchhaltung
- Stammdaten / Unternehmensprofile Informationen zur Organisation, Rechtsform, Kontaktdaten und Branchenzugehörigkeit

Basierend auf den zur Verfügung gestellten Datenschemata wurden Ontologien zur semantischen Beschreibung sowohl von Stammdaten als auch betriebswirtschaftlichen Kennzahlen abgeleitet und weiterentwickelt. Ziel war eine standardisierte und maschinenlesbare Beschreibung, die Interoperabilität und Wiederverwendbarkeit der Daten im Rahmen von Solid gewährleistet.

Die technische Anbindung der Daten erfolgte über Solid-basierte Schnittstellen [19], welche die Verwaltung und den Zugriff auf die Daten dezentral und nutzerzentriert ermöglichen. Damit konnte eine erste prototypische Umsetzung von datensouveräner Zusammenarbeit auf technischer Ebene realisiert werden (AP 5).

Insgesamt bildete AP 1.2 somit die datentechnische und infrastrukturelle Grundlage für die folgenden Arbeitspakete und den Demonstrator. Die verwendeten Modelle und Schnittstellen sind übertragbar und können künftig für weitere betriebswirtschaftliche Anwendungsfälle im Unternehmenskontext genutzt werden.

[1] `https://github.com/mandat-project`

Die gewählte Infrastruktur ist anschlussfähig an föderierte Datenräume, z. B. International Data Spaces (IDS), wie im Rahmen von [12] gezeigt.

Zugehöriges Ergebnisdokument und Artefakte

- Bereitgestellte Infrastruktur (siehe Kap. 2.5.1, AP 5.1 Deploymentsicht)
- Exemplarische Daten (e.g. Beispielunternehmen, Unternehmensdaten)[2,3]

Erfüllung der Zielsetzung. Die Ziele des Arbeitspakets wurden erfolgreich erfüllt. Die geschaffene Infrastruktur und bereitgestellten Daten bildeten die datentechnische und infrastrukturelle Grundlage für die folgenden Arbeitspakete und den Demonstrator.

2.2 AP 2: Identitäten, Freigabeprozesse und Rechte

Im Rahmen des Arbeitspaketes 2 wurde eine systematische Untersuchung und Entwicklung von Konzepten, Technologien und Prozessen im Bereich Identitäten, Rechtevergabe und Nachvollziehbarkeit von Freigaben durchgeführt. Dies umfasste etwa die Analyse und Auswahl geeigneter Technologien zur Verwaltung der Identitäten einzelner Akteure, sowohl natürliche als auch juristische, die Entwicklung von Methoden zur Delegation von Berechtigungen im Innenverhältnis einer Organisation sowie die Spezifikation und Dokumentation von Freigabeprozessen für ebenjene Berechtigungen. Dabei wurde sowohl technische als auch rechtliche Perspektiven berücksichtigt, um den Anforderungen an die Verwaltung von Identitäten und Berechtigungen sowohl im Innen- als auch Außenverhältnis gerecht zu werden. Ziel war es somit, eine robuste, überprüfbare und skalierbare Lösung zu schaffen, die sowohl natürliche als auch juristische Personen einbezieht und Interaktionen effizient und nachvollziehbar gestaltet.

2.2.1 AP 2.1 Identitäten und Delegation von Berechtigungen

Zielsetzung des Arbeitspakets. Ziel von AP 2.1 war die Auswahl von Technologien zur Repräsentation und Verwaltung von Identitäten und Methoden zur Delegation von Berechtigungen im Datenaustausch. Während wir auf der einen Seite natürliche Personen und deren Identität beschreiben müssen, mussten wir ebenfalls juristische Personen, wie Unternehmen, mit ihren teilweise großen und komplexen Strukturen beschreiben. Gleichzeitig galt es zu klären, wie die Verbindung zwischen natürlichen und juristischen Personen aussehen kann, etwa welche Rollen eingenommen werden und wo sich diese im Unternehmen befinden, oder wie die Prozesse zur Erlangung jener aussehen.

Durchgeführte Arbeiten und Ergebnisse. Zur Auswahl von passenden Technologien zur Identitätsverwaltung und Datenaustausch führten wir eine Analyse zum Stand der Technik durch. Hierzu analysierten wir unter anderem die drei Architekturvarianten zur Verwaltung von Identitäten, zentralisiert, föderiert und dezentralisiert, und untersuchten,

[2] `https://github.com/mandat-project/mandat-organization`
[3] `https://github.com/mandat-project/musterkanzlei-lifted`

welche im Rahmen des Anwendungsfalles von AP 1 infrage kommen und von Datentreuhändern genutzt werden können [16, 24].

Zentralisierte Architekturen zeichnen sich dadurch aus, dass Identität, zugehörige Daten und Anwendungen an einer einzigen Stelle verwaltet werden können. Weit verbreitete Dienste wie Google oder Facebook benutzen diese Art der Architektur bereits, indem sie neben der Identitätsverwaltung auch eine Vielzahl an Anwendungen und Diensten anbieten, welche auch das Verwalten und Speichern der zugehörigen Daten beinhaltet. Diese Struktur birgt Risiken hinsichtlich des Datenschutzes und der Abhängigkeit von einem zentralen Anbieter.

In föderierten Architekturen wird lediglich die Identitätsverwaltung von großen Anbietern übernommen, sogenannten Identity Providern. Anwendungen werden hierbei von externen Drittanbietern bereitgestellt und werden über die Anmeldung mittels der verwalteten Identität genutzt. Hierbei ist der Identity Provider erneut für die Verwaltung der Identitätsdaten zuständig und behält einen Überblick über die verknüpften Anwendungen. Diese Architektur ermöglicht eine hohe Interoperabilität, jedoch bleibt erneut eine Abhängigkeit der Nutzenden gegenüber der zentralen Kontrolle der Identitätsdaten durch den Provider vorhanden.

In dezentralisierte Architekturen werden schlussendlich Identität, Anwendungen und Daten komplett voneinander entkoppelt, so dass keinerlei Abhängigkeit zwischen diesen entsteht. Als klassische dezentralisierte Ansätze kommen hierbei vor allem Architekturen rund um das Web infrage. Vor allem Solid stellt hier im Umfeld web-basierter Ansätze einen dezentralen Ansatz dar. Solid basiert auf offenen Web-Standards und ermöglicht Nutzern ihre Daten in sogenannten Pods selbst zu verwalten. Zugriffsrechte zu den jeweiligen können dabei individuell für verschiedene Anwendungen und andere Nutzende definiert werden, was eine flexible und datenschutzfreundliche Verwaltung ermöglicht.

Weiterhin anaylsierten wir, mit welchen existierenden Methoden Identitäten von natürlichen und juristischen Personen und deren Rechten beschrieben werden können.

PROV Ontology Die PROV Ontology (PROV-O)[4] ist eine Ontologie, welche Klassen, Prädikate und Prozesse definiert, mit welcher Veränderungen an Daten nachvollzogen werden können. Hieraus ergeben sich die drei grundlegenden Klassen in PROV-O, Entity, Agent und Activity, welche die Beziehung der Aspekte der Veränderungen (bspw. Wer hat wann was wie verändert?) definieren.

Zusätzlich existieren in PROV-O sogenannte „qualified Terms", welche die grundlegenden und erweiterten Klassen mit zusätzlichen Details versehen können, um Vorgänge genauer zu beschreiben. Neben den zeitlichen Aspekten, welche Activities mit sich bringen, werden auch statische Beziehungen abgebildet, bspw. welcher Agent (bspw. Angestelle einer Organisation) ist statisch Teil welcher Organisation (bspw. eine Firma). In diesem Fall kann auch eine Kette nachvollzogen werden, wer im Namen welches anderen Agenten oder welcher Organisation am Ende gehandelt hat (Delegation) und woraus sich entsprechende Rechte speisen. PROV eignet sich in MANDAT zur Beschreibung von durchgeführten Prozessen, etwa zum Gewähren und Entziehen von rollenspezifischen Rechten in Unternehmen oder der Änderung von Dokumenten im Namen anderer. Im MANDAT

[4] `https://www.w3.org/TR/prov-o/`

Anwendungsfall betrifft das insbesondere die Nachvollziehbarkeit von Änderungen im Geschäftsgebaren, so etwa im Rahmen von Activites als Schnittstelle zwischen Entities und Agenten.

Organization Ontology Die Organization Ontology (ORG)[5] ist eine Ontologie zur Beschreibung von organisatorischen Strukturen und Hierarchien. Im Zentrum der Ontologie steht die `org:Organisation`, welche als übergeordnete Gruppierung das gemeinschaftliche, zielgerichtete Agieren von Personen darin beschreibt. Sie kann selbst als Agent auftreten. In der Organisation enthaltene `org:OrganizationalUnit` sind Unterabteilungen, welche innerhalb definierter Teilbereiche agieren, aber auch eine eigene `org:Organisation` sein können. Die Beziehung zur enthaltenden Organisation ist `org:unitOf` bzw. von dieser zur enthaltenen `org:hasUnit` für Suborganisationen und Abteilungen. Agenten, für ORG Personen oder andere Organisationen, treten als `foaf:Agent`[6] auf und definieren ihre Zugehörigkeit zur Organisation über `org:memberOf`. Die Beziehung zu Leitung der Organisation ist durch `org:headOf` definiert, weitere Rollen durch `org:role` auf eine `org:Role`.

ORG eignet sich daher in MANDAT in erster Linie zur Beschreibung einer statischen Unternehmens-Struktur, aus welcher sich die Hierarchie eines Unternehmens ableiten lässt. Damit kann man nachvollziehen, welcher Akteur welche Rechte im Rahmen der eigenen Rolle innehat und wie weit diese reichen.

Verifiable Credentials Verifiable Credentials (VC)[7] sind ein dezentralisierter Ansatz für Identitätsverwaltung, wobei der Inhaber die volle Kontrolle darüber hat, welche Informationen gegenüber Dritten präsentiert werden. VCs definieren drei verschiedene Rollen, Issuer, Holder und Verifier, wobei diese Rollen sowohl von Personen, Institutionen oder Geräten eingenommen werden können.

Ein Verifiable Credential (VC) ist nach der W3C-Empfehlung ein RDF-Datensatz, der aus zwei RDF-Graphen besteht: dem Credential-Graphen mit Claims und Attributen, der mit einem Beweisgraphen verknüpft ist, welcher die digitale Signatur des des Berechtigungsnachweises und Metadaten zu seiner Interpretation enthält. Die Claims des Credential-Graphs sind die Aussagen über das CredentialSubject, die vom die vom Aussteller angegeben werden (z. B. das Geburtsdatum). Claims enthalten Metadaten wie wie eine DID, die den Aussteller identifiziert, der das Credential signiert, sein expirationDate und das Ausgabedatum.

Im Rahmen von MANDAT sind Verifiable Credentials insbesondere zum Nachweis einer bestimmten Rolle im Unternehmen durch Mitarbeitende interessant.

Self Sovereign Identities und Identity Wallets Die Idee der souveränen Identität (Self-Sovereign Identity, SSI), die in Christopher Allens Blogpost[8] popularisiert wurde, soll Nutzern oder allgemein Agenten die Kontrolle über ihre digitale Identität übertragen. Das heißt, dass Agenten in der Lage sein sollten, digitale IDs zu erstellen und im Web

[5] `https://www.w3.org/TR/vocab-org`
[6] `foaf: http://xmlns.com/foaf/0.1/`
[7] `https://www.w3.org/TR/vc-data-model/`
[8] `https://www.lifewithalacrity.com/article/the-path-to-self-soverereign-identity/`

zu verwenden, ohne eine dritte Partei einzubeziehen, wenn die IDs angefordert, präsentiert oder überprüft werden. SSI findet international und bereichsübergreifend, z. B. im Finanzsektor, im öffentlichen Sektor und im Gesundheitswesen, Beachtung und Akzeptanz. Bei der SSI stehen Sicherheit und Datenschutz an erster Stelle, um den Benutzer zu schützen: Die Benutzer müssen die Kontrolle haben, die Datenminimierung und Maßnahmen zum Schutz der Privatsphäre sind erwünscht.

Um ein Identitäts- und Zugriffsmanagementsystem zu realisieren, sind folgende Bausteine erforderlich: Identifizierung des Agenten, Attribute für die Autorisierung und Protokolle für die Authentifizierung. In der SSI sind die Spezifikationen für diese Bausteine Gegenstand laufender und meist getrennter Standardisierungsbemühungen des World Wide Web Consortium (W3C), der Decentralised Identity Foundation (DIF) und der Hyperledger Community. Die erste relevante W3C-Empfehlung spezifiziert dezentrale Identifikatoren (DIDs), die standardisiert, wie Agenten identifiziert werden können, ohne sich notwendigerweise auf eine zentrale Autorität zu verlassen. Die zweite Empfehlung zum Verifiable Credentials Data Model verbessert die Interoperabilität digitaler Ausweise, indem sie definiert, wie diese als Wissensgraphen beschrieben werden und wie Signaturen in Bezug auf eine kanonische Darstellung dieses Wissensgraphen geltend gemacht werden können, im Gegensatz zu einer anwendungsspezifischen Serialisierung.

Eine Identity Wallet ist eine Anwendung, die ein Benutzer zum Speichern, Verwalten und Präsentieren von VCs verwendet. SSIs dienen im Rahmen von MANDAT als eindeutiger, dezentraler Identifikator für natürliche und jursitische Personen, der zur Zuordnung von VCs genutzt wird.

Open Digital Rights Language Open Digital Rights Language (ODRL)[9] ist ein Standard für die Beschreibung von Rechten und Richtlinien für den Austausch digitaler Inhalte. ODRL bietet Definitionen für eine interoperable Methode zur Darstellung von Rechten, Berechtigungen und Beschränkungen für digitale Inhalte. ODRL verwendet strukturierte Beschreibungen zur Darstellung von Rechten und Richtlinien und ermöglicht die Definition von Rechteinhabern, welche die Kontrolle über die Nutzung der von ihnen bereitgestellten Inhalte haben. Es werden `odrl:Actions` und `odrl:Rules` in sogenannten `odrl:Policies` definiert, die auf digitale Inhalte angewandt werden können, z. B. Zugriff, Änderung, Verteilung. Parteien und Gruppen von Parteien, die an der Umsetzung von Rechten und Richtlinien beteiligt sind, werden identifiziert, darunter Nutzer und Dienstanbieter. Es können flexible `odrl:Constraints` für die Ausübung von Rechten festgelegt werden, z. B. zeitliche und geografische Beschränkungen, Zahlungsbedingungen. Bislang wird ODRL häufig für die Lizenzierung digitaler Inhalte, den Schutz digitaler Werke vor unbefugter Nutzung und die Festlegung von Nutzungsrichtlinien auf digitalen Plattformen verwendet.

Im Hinblick auf die Datensouveränität und die Datentreuhänderschaft im Kontext von MANDAT kann ODRL verwendet werden, um Rechte und Beschränkungen von Agenten im Zusammenhang mit der Nutzung, Weitergabe und Verarbeitung von Daten festzulegen.

[9] `https://www.w3.org/TR/odrl-model/`

Erfüllung der Zielsetzung. Mittels der Analyse zum Stand der Technik und der daraus resultierenden Übersicht über mögliche Architekturen und existierenden Möglichkeiten, konnten wir die oben erklärten Methoden wählen, um damit unter Nutzung von Solid, Identitäten von Unternehmen und Personen zu repräsentieren und diese bei der Delegation und Nachvollziehbarkeit von Berechtigungen (siehe AP 2.2 und 2.3) zu nutzen. Die derzeitigen Möglichkeiten, in Solid natürliche Personen zu beschreiben, wurde auf juristische Personen erweitert. Außerdem bilden wir die Rollen, welche natürliche Personen im Zusammenhang mit juristischen Personen haben können (z.B. Rollen im Außenverhältnis wie Prokura, Rollen im Innenverhältnis wie Einkaufsberechtigungen) explizit ab.

2.2.2 AP 2.2 Freigabeprozesse und Rechtevergabe

Zielsetzung des Arbeitspakets. Das Ziel von AP 2.2 war die Auswahl von Technologien und Methoden zur Darstellung von Freigabeprozessen. Dies basierte auf den gewählten Technologien von AP 2.1, welche sich vor allem um die Repräsentation von Identitäten von natürlichen und juristischen Personen und deren damit verknüpften Attributen wie Hierarchien und Rollen drehte. Damit konnten wir nun in AP 2.2 Prozesse, welche etwa für die tatsächliche Vergabe von Rollen in einem Unternehmen notwendig sind, etwa zur Vertretung im Außenverhältnis oder nur temporär als Vertretung bei Krankheit des eigentlichen Rechteinhabers. Hierzu unterscheiden wir auch das Innenverhältnis und Außenverhältnis eines Unternehmens, basierend auf definierten Rechten, welche den Rollen eingeräumt werden.

Durchgeführte Arbeiten und Ergebnisse. Mit den Kernprinzipien von Solid, die Verwaltung von Identität, Daten und Anwendungen zu trennen, können die Benutzer die Anwendungen auswählen, die ihren spezifischen Bedürfnissen entsprechen, und diese Anwendungen mit ihrer WebID [35] (eindeutige Identität innerhalb des Solid-Ökosystems) verwenden. Folglich können verschiedene Anwendungen für den Zugriff auf verschiedene Datentypen mit unterschiedlichen Zwecken und Bedürfnissen verwendet werden. Read-Write Linked Data ermöglicht grundsätzlich schon einen gegenseitigen Austausch entweder von statischen Daten oder von dynamischen Datenströmen [41]. Da jedoch ein Datenanbieter in Geschäftsumgebungen bei komplexeren Prozessen, z. B. über Organisationsgrenzen hinweg, eine fundierte Entscheidung darüber treffen muss, welche Daten er mit wem und zu welchem Zweck austauschen möchte, ist hierzu eine Nutzung des Solid-Protokolls notwendig, das auf Read-Write Linked-Data basiert.

In unserem Anwendungsfall findet eine gemeinsame Datennutzung statt, z. B. zwischen dem Agenten SME und BigBank als einem weiteren Agenten, wobei SME Daten mit Geschäftsberichten bereitstellt und BigBank Zugang zu den Geschäftsberichten beantragt. Außerdem stellt BigBank Daten über ein Kreditangebot zur Verfügung, auf die SME Zugriff wünscht.

Da es sich bei SME und BigBank jedoch nur um juristische Personen handelt, benötigen sie Bevollmächtigte, die in ihrem Namen handeln. Dies ist insbesondere im Geschäftsleben ein häufiger Anwendungsfall, z. B. handelt ein Arbeitnehmer im Namen seines Arbeitgebers. In unserem Anwendungsfall handelt Tom als natürliche Person im Namen

des Arbeitgebers SME, einer Organisation, um den Darlehensvertrag für SME zu unterzeichnen. Die Übertragung von Rechten von einem Vertreter auf einen anderen ist eine sogenannte Delegation oder Vollmacht.

Bei einer Delegation legt der Delegierende Policies fest, welche die Rechte und Transaktionen bestimmen, die im Namen des Delegierenden gegenüber einem Partner, bspw. einem verbundenen Unternehmen, ausgeübt werden können. Ein Delegierter kann dann gegenüber dem verbundenen Unternehmen so handeln, wie es in einer entsprechenden Policy festgelegt ist. Aktuelle Lösungen für die gemeinsame Nutzung von Daten mit Solid basieren auf Zugriffskontrolllisten (ACLs) oder, wenn eine größere Gruppe betrachtet wird, auf der Mitgliedschaft eines Agenten in vCard-Gruppen[10].

Bei Verwendung dieser Lösungen in einer Delegationsumgebung werden die Identität des Delegierten und die Delegation selbst notwendigerweise einem Partner offenbart, der die entsprechenden ACLs setzen muss, um den Zugang zu ermöglichen. Wenn man bedenkt, dass der Delegierte ein Interesse daran hat, anonym zu bleiben, ergeben sich schnell Probleme. Außerdem verliert der Delegierende nach der Gewährung einer Delegation die Kontrolle darüber, ob der Delegierte nur legitime Handlungen im Rahmen der festgelegten Policies vornimmt.

Da Delegationen häufig vorkommen (insbesondere in Geschäftsumgebungen entlang von Hierarchien), Delegationen von Rechten weitreichende Konsequenzen in Bezug auf die Macht des Delegierten haben und Delegationsprozesse in Bezug auf die abstrakten Rollen des Delegierenden, des Delegierten und des Partners in allen Geschäftsanwendungen ähnlich sind, haben wir den Rights Delegation Proxy (RDP) [39] entwickelt, eine wiederverwendbare Komponente, die in verschiedenen Organisationen eingesetzt werden kann (siehe Abbildung 2.2).

Bevor eine Delegation beginnt, gehen wir davon aus, dass das angeschlossene Unternehmen bereits Zugriffsrechte für den Delegierenden definiert hat, z. B. Leserechte für SME auf dem Solid Pod der BigBank. Um eine Delegation vom Delegierenden an den Delegierten zu definieren, erstellt der Delegierende eine Richtlinie, welche die Rechte des Delegierten festlegt, z. B. gebunden an eine bestimmte WebID oder an eine Mitarbeiterrolle in einer Organisation. Die Richtlinie definiert auch die Bedingungen, unter denen der Delegierte handeln darf.

Die Bedingungen werden vom RDP ausgewertet und können definieren, wie eine Ressource aussehen muss, bevor ein Delegierter auf sie zugreifen darf (Vorbedingung), oder wie die Ressource aussehen muss, nachdem der Delegierte auf sie zugegriffen hat (Nachbedingung). Zu beachten ist, dass der Delegierende zwar im Prinzip so viele Rechte an den Delegierten delegieren kann, wie er möchte, dass der Delegierte aber niemals die Rechte übersteigen kann, die der Partner des Delegierenden dem Delegierenden ursprünglich zugestanden hat. Wenn der Delegierende zum Beispiel Leserechte hat, können einem Delegierten nur Leserechte gewährt werden, aber keine Schreibrechte, da ein fehlendes

[10] `https://www.w3.org/2006/vcard/ns#Group`

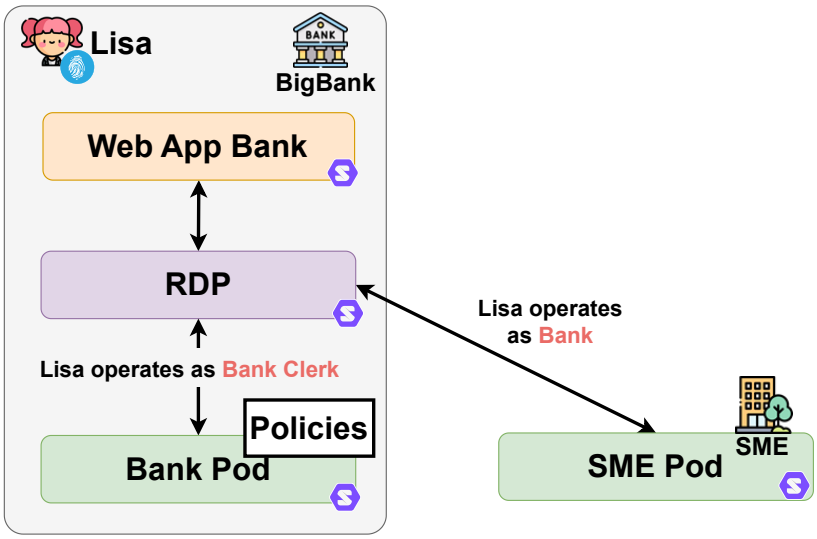


Abbildung 2.2: Komponentendiagramm Rights Delegation Proxy (RDP). Lisa nutzt ihre Rolle als Sachbearbeiterin in der Web-App der Bank. Wenn sie auf den SME-Pod zugreift, prüft der RDP, ob ihre Aktion mit den Richtlinien der Bank übereinstimmt. Wenn ja, führt der RDP ihre Aktion mit der Identität der Bank aus. SME erkennt nur, dass Bank gehandelt hat.

Schreibrecht vom Partner gegenüber dem Delegierenden fehlen würde. Policies können komplexer sein und z.B. als Shape Expressions (ShEx)[11] oder SPARQL[12]-ASK-Abfragen.

Da der RDP darauf abzielt Rechte von einem Agenten an einen anderen in Bezug auf eine bekannte Ressource eines verbundenen Unternehmens zu delegieren, kommt der RDP hauptsächlich der zugreifenden Partei, dem Delegierten, zugute, der seine Identität vor dem verbundenen Unternehmen schützt. In einem ähnlichen Fall soll die Identität der Partei, auf deren Daten zugegriffen wird, geschützt und nicht offengelegt werden. Wir haben deshalb außerdem den Data Provisioning Proxy (DPP) [8] entwickelt. Der Prozess ähnelt der Funktionsweise des RDP unterscheidet sich aber hauptsächlich in der Art und Weise, wie Richtlinien und der Datenfluss gehandhabt werden.

In diesem Fall befindet sich der DPP bei einer weiterleitenden Partei (z. B. SME), die Datenanforderungen von einer externen Partei (z. B. von Lisa im Namen der Bank) erhält, wobei die angeforderten Daten von einer externen, verborgenen Quelle abgerufen werden könnten. Der DPP prüft, ob sich die angeforderte Ressource auf dem aktuellen Pod befindet (z. B. für die eigenen Daten von SME) oder ob die Ressource von einer externen Datenquelle abgerufen und weitergegeben werden muss (z. B. von einer dritten Partei wie dem Steuerberater, die den Zugriff mit SME geteilt hat). Auch hier kann der

[11] https://shex.io/
[12] https://www.w3.org/TR/sparql11-overview/

Eigentümer der externen Datenquelle eine Richtlinie festlegen, unter welchen Bedingungen die gemeinsame Nutzung von Daten akzeptabel ist.

Der DPP überprüft zunächst die geltende Richtlinie im Hinblick auf die angeforderten Daten, und sofern die Weitergabe gemäß dieser Regelung zulässig ist, fordert der DPP anschließend die entsprechende Ressource an. Im Prozess nimmt der DPP, ähnlich zum RDP, wieder die Identität der weitergebenden Partei an; im Beispiel etwa ist der DPP als SME authentifiziert. Aus der Sicht der anfragenden Partei sehen die bereitgestellten Daten damit so aus, als ob sie direkt von der weitergebenden Partei stammen, während die ursprüngliche Datenquelle verborgen bleibt.

Software-Artefakte. Die Implementierungen des RDP und DPP sind im GitHub-Repository des MANDAT-Projekts[13] zu finden.

Zugehörige Ergebnisdokumente. Die Ergebnisse dieser Untersuchung sind in den folgenden wissenschaftlichen Publikationen dokumentiert:

- Andreas Both, Dustin Yeboah, Thorsten Kastner, Daniel Schraudner, Sebastian Schmid, Christoph Braun, Andreas Harth und Tobias Käfer. „Towards Solid-based B2B Data Value Chains“. In: 21st Extended Semantic Web Conference (ESWC 2024) (Hersonissos, Crete). 26.–30. Mai 2024. [8]
- Andreas Both, Thorsten Kastner, Dustin Yeboah, Christoph Braun, Daniel Schraudner, Sebastian Schmid, Tobias Käfer und Andreas Harth. „Foundational Components for B2B Data Sharing Using the Solid Protocol“. In: Journal of Web Engineering. 2025. (akzeptiert) [7]
- Sebastian Schmid, Daniel Schraudner und Andreas Harth. „The Rights Delegation Proxy: An Approach for Delegations in the Solid Dataspace“. In: Proceedings of the Second International Workshop on Semantics in Dataspaces (SDS 2024) co-located with the 21st Extended Semantic Web Conference (ESWC 2024) (Hersonissos). 26. Mai 2024. [39]
- Andreas Both, Thorsten Kastner, Dustin Yeboah, Christoph Braun, Daniel Schraudner, Sebastian Schmid, Tobias Käfer und Andreas Harth. „AuthApp - Portable, Reusable Solid App for GDPR-Compliant Access Granting“. In: Web Engineering - 24th International Conference, ICWE 2024, Tampere, Finland, June 17-20, 2024, Proceedings. Springer, 2024, S. 199–214. [6]
- Daniel Schraudner, Sebastian Schmid, Christoph H.-J. Braun und Andreas Harth. „Delegation of Access Rights to Web Resources between Agents“. (eingereicht). 2025. [40]

Erfüllung der Zielsetzung. Mit einer Definition zur Vergabe von Rechten durch Rollen in einem Unternehmen an natürliche Personen, erhalten diese sowohl im Innen- als auch im Außenverhältnis die Möglichkeit zu handeln. Da die Vergabe von Rechten mit einer großen Tragweite einhergeht, soll eine Ausübung der Rechte allerdings nur in einem wohldefinierten Rahmen geschehen, so dass ein Delegierender sich sicher sein kann, dass

[13] `https://github.com/mandat-project/delegation-proxy`

Bevollmächtigte die gewährten Rechte nicht unsachgemäß gebrauchen. Daher legten wir unser Augenmerk vor allem auf eine gesicherte Vergabe anhand definierter Policies, welche die Möglichkeit zur Nachvollziehbarkeit (siehe AP 2.3) gibt. Der RDP und der DPP sind hier maßgebliche Artefakte, welche die Verwaltung, Vergabe und Ausübung von Rechten zum Schreiben und Lesen externer Daten bei Dritten ermöglichen und überwachen. Dabei haben wir erneut darauf geachtet, dass unsere geschaffenen Lösungen wiederverwendbar sind und somit ohne tiefgreifende Maßnahmen in das System eines Unternehmens eingebracht werden können.

2.2.3 AP 2.3 Nachvollziehbarkeit

Zielsetzung des Arbeitspakets. Das Ziel von AP 2.3 war die Erarbeitung von Methoden zur Nachvollziehbarkeit der Freigaben auf Basis der gewonnenen Erkenntnisse aus AP 2.1 und AP 2.2: Nachdem wir in AP 2.1 definierten, wie die Identitäten von natürlichen und juristischen Personen für MANDAT festzulegen sind, und in AP 2.2 erarbeiteten, wie die Delegation von Rechten vonstattengeht, stellten wir in AP 2.3 sicher, dass die Ausübung der Rechte einer Delegation über die Zeit hinweg aufgezeichnet, abfragbar und nachvollziehbar ist. Weiterhin prüfen wir die Richtigkeit unserer geschaffenen Architektur zur Delegation mittels formaler Methoden.

Durchgeführte Arbeiten und Ergebnisse. Die Nachvollziehbarkeit von Delegationen kann durch den RDP-Ansatz ebenfalls gelöst werden. Da alle Requests, die im Namen des Delegierenden nach außen gehen, vorher zwangsläufig einen RDP passiert haben müssen, ist der RDP in der Lage, ein Log über alle ausgehenden Requests zu erstellen. Weiterhin können in diesem Zusammenhang nicht nur die ausgehenden Requests geloggt werden, sondern auch die WebId des Delegierten sowie die konkreten Policies, durch die die Delegation gewährt wurde.

Bei der Nutzung eines RDP sendet ein Delegierter einer Organisation HTTP-Anfragen direkt an den RDP, wobei der Zugriffspfad die Ressource des Partners ist und die Anfrage den Host des URI des Partners enthält. Nach dem Empfang einer Anfrage sucht der RDP nach einer passenden Policy in Abhängigkeit von der WebID und der angeforderten Webressource. Der RDP prüft die Vorbedingungen mit einem „Preflight GET“ an die angeforderte Ressource und wertet aus, ob die Antwort mit der Vorbedingung übereinstimmt. Um eine Nachbedingung zu prüfen, wertet der RDP den Nachrichtentext aus, welcher den zu erwartenden Zustand der Ressource enthält. In jedem Fall protokolliert der RDP die Prüfergebnisse einschließlich der Zeit, des Inhalts, der aufgerufenen Ressource und der anfragenden WebID an einem vom Delegierenden festgelegten Ort. Wenn der Delegierte die Richtlinie erfüllt, authentifiziert sich das RDP als Delegierter, so dass eine Trennung zwischen dem Delegierten und dem Partner erfolgt, und leitet die Anfrage des Delegierten an die Ressource des Partners weiter und sendet die entsprechende Antwort an den Delegierten zurück.

Der RDP verhindert, dass Aktionen außerhalb der definierten Kontrolle des Delegierenden stattfinden und ist daher für geschäftliche Anwendungsfälle besonders interessant. Als eine Komponente im Gesamtprozess hat das RDP eine zentrale Rolle, da es alle einge-

henden Anfragen von potenziellen Delegierten verwalten, bewerten und ausführen muss. Seine hohe Verantwortung stellt somit einen Engpass und einen potenziellen Single Point of Failure dar. Die Möglichkeit einer Verteilung der Daten zur Delegation ist allerdings gegeben, da verteilte Daten mit begrenzter Verfügbarkeit selbst im dynamischen Umfeld, ähnlich zum Web, zum Erfolg führen können, wenn die nutzenden Agenten sich untereinander austauschen [38], hier etwa unternehmensintern zum Delegationsprozess. Darüber hinaus ist die Verantwortung für die Definition von Richtlinien, welche die Absicht des Delegierenden widerspiegeln, ein heikler Schritt, der sorgfältig gehandhabt werden sollte, da ein Delegierter direkt im Namen des Delegierenden handeln kann, wie es bereits heute der Fall ist.

Neben dem RDP haben wir noch andere Delegationsarchitekturen, namentlich die registerbasierte Delegationsarchitektur und die rollenbasierte Delegationsarchitektur untersucht. Wir erstellen außerdem ein formales Modell, um verschiedene Eigenschaften und Anforderungen an die Architekturen mittels des automatischen kryptografischen Beweissystems *ProVerif* zu prüfen [40].

Während sich der RDP hauptsächlich mit der Durchführung von Aktionen befasst und daher eine effiziente Auswertung der Policies des Delegierenden vor Ort benötigt, muss sich der DPP auf eine effiziente Datenlokalisierung konzentrieren, um festzustellen, ob sich die angeforderten Daten auf dem Pod der übergebenden Partei oder auf einem externen Pod befinden. Ein zusätzlicher Bonus des DPP ist die Möglichkeit für die weitergebende Partei, sowohl die angeforderten Daten in einem letzten Schritt zu verarbeiten, bevor diese schließlich mit der anfordernden Partei geteilt werden, als auch alle Zugriffe auf die angeforderten Daten mitzuloggen. Dies ist besonders wichtig, wenn die weiterzugebenden Daten in erster Linie die weitergebende Partei betreffen oder besonders sensibel sind. Beispielsweise können die Berichte des Steuerberaters von SME anonymisiert werden, bevor sie an BigBank weitergegeben werden. Die Schritte zu solchen Bearbeitungen können unter Zuhilfenahme von Laufzeitinformationen effizient geplant werden, wobei nicht notwendigerweise alle Informationen statisch vorliegen müssen, da die Agenten verschiedener Parteien Prozesse auch mit dynamischen Informationen erfüllen können [37]. In jedem Fall stellt die weitergebende Partei die Datenquelle für solche Daten dar, während die ursprüngliche Quelle immer noch unter der Kontrolle der externen Partei steht und versteckt ist.

Software-Artefakte. Die Implementierungen des RDP und DPP sind im GitHub-Repository des MANDAT-Projekts[14] zu finden.

Zugehörige Ergebnisdokumente. Die Ergebnisse dieser Untersuchung sind in den folgenden wissenschaftlichen Publikationen dokumentiert:

- Andreas Both, Dustin Yeboah, Thorsten Kastner, Daniel Schraudner, Sebastian Schmid, Christoph Braun, Andreas Harth und Tobias Käfer. „Towards Solid-based B2B Data Value Chains“. In: 21st Extended Semantic Web Conference (ESWC 2024) (Hersonissos, Crete). 26.–30. Mai 2024. [8]

[14] `https://github.com/mandat-project/delegation-proxy`

- Andreas Both, Thorsten Kastner, Dustin Yeboah, Christoph Braun, Daniel Schraudner, Sebastian Schmid, Tobias Käfer und Andreas Harth. „Foundational Components for B2B Data Sharing Using the Solid Protocol“. In: Journal of Web Engineering. 2025. (akzeptiert) [7]
- Sebastian Schmid, Daniel Schraudner und Andreas Harth. „The Rights Delegation Proxy: An Approach for Delegations in the Solid Dataspace“. In: Proceedings of the Second International Workshop on Semantics in Dataspaces (SDS 2024) co-located with the 21st Extended Semantic Web Conference (ESWC 2024) (Hersonissos). 26. Mai 2024. [39]
- Andreas Both, Thorsten Kastner, Dustin Yeboah, Christoph Braun, Daniel Schraudner, Sebastian Schmid, Tobias Käfer und Andreas Harth. „AuthApp - Portable, Reusable Solid App for GDPR-Compliant Access Granting“. In: Web Engineering - 24th International Conference, ICWE 2024, Tampere, Finland, June 17-20, 2024, Bd. 14629. Lecture Notes in Computer Science. Springer, 2024, S. 199–214. [6]
- Daniel Schraudner, Sebastian Schmid, Christoph H.-J. Braun und Andreas Harth. „Delegation of Access Rights to Web Resources between Agents“. (eingereicht). 2025. [40]

Erfüllung der Zielsetzung. Mit AP 2.3 bekommen Delegierende auch langfristig die Sicherheit, mit den Möglichkeiten zur sicheren Delegation mittels Policies aus AP 2.2, die Vergabe und Ausübung gewährter Rechte aufzuzeichnen und diese vollständig und abfragbar zu sichern. Der RDP steht als Komponente zwischen den Bevollmächtigten und einer dritten Partei, daher werden sowohl versuchte als auch durchgeführte Interaktionen im Namen des Delegierenden konsequent nachvollzogen, wie in der Analyse der RDP Architektur ebenfalls gezeigt. Gleichfalls hat der DPP als zwischengeschaltete Komponente die Möglichkeit, umfassende Aufzeichnungen über Datenabrufe zu erstellen und somit die Nachvollziehbarkeit zu sichern.

2.3 AP 3: Verarbeitungstransparenz

Im Rahmen des Arbeitspaketes 3 wurden Methoden zur Beschreibung von Daten und deren Verarbeitung untersucht. Dabei wurde ein Fokus auf die Modellierung und Durchführung von souveränen, zweckgebundenen Datenfreigaben sowie deren Protokollierung gelegt. Die entwickelten Methoden ermöglichen insbesondere die Transparentmachung der Datenverarbeitung gegenüber Datengebenden für einen “Informed Consent” (eine Einwilligung nach erfolgter Aufklärung) und die Protokollierung von zweckgebundenen Datenfreigaben und angestrebter Verarbeitung für Compliance-Untersuchungen.

Datennutzende, also Anwendungen und ihre Nutzer, müssen den Zugriff auf Daten bei dem potentiellen Datengebenden anfragen, bevor die App die gewünschten Daten verarbeiten kann. Datenanfragen beinhalten daher eine formale Beschreibung des Zwecks der Datenverarbeitung. Auf diese Weise wird potentiellen Datengebenden eine informierte Entscheidung ermöglicht. Durch die formale Modellierung des Zwecks und der Datenanfrage selbst können auch automatisierte Freigabeentscheidungen durchgeführt werden.

Um eine spätere Auditierbarkeit von solchen Datenfreigaben zu gewährleisten, werden Autorisierungen und Entscheidungen nachvollziehbar protokolliert. Eine Zusammenfassung der in MANDAT erfolgten Arbeiten wurde in [6], [7] und [28] präsentiert, und eine Implementierung im Rahmen von AP 5 in den Demonstrator eingebunden.

Weitere Arbeiten befassten sich damit, die tatsächlich ausgeführten Datenverarbeitung transparent zu machen, um die Lücke zwischen der im Zuge der Datenfreigabe angestrebten Datenverarbeitungsschritten und deren Ausführung zu schließen. Bei diesen Arbeiten existiert eine große Schnittstelle zu den in AP 4 bearbeiteten Themen der Integrität und Authentizität von Daten und Analysen.

Nachfolgend werden die durchgeführten Arbeiten detaillierter beschrieben.

2.3.1 AP 3.1 Architektur für Verarbeitungstransparenz in Apps

Zielsetzung des Arbeitspakets. Im Solid-Ökosystem, das auf der Trennung von Identität, Daten und Anwendungen basiert, müssen Anwendungen bei Dateneigentümern um Zugriff auf deren Datenspeicher (Pods) ersuchen. Standardmäßig umfassen diese Anfragen primär technische Zugriffsrechte (z. B. Lesen, Schreiben). Die Zielsetzung des Arbeitspakets 3.1 war es, diesen Prozess zu erweitern, um eine umfassende Transparentmachung der Datenverarbeitung durch die anfragende Anwendung zu erreichen. Hierfür sollte eine technische Architektur für die Ausführung der Datenverarbeitung im Kontext von Anwendungen, die Daten aus Solid Pods nutzen, untersucht werden. Ein besonderer Fokus der Untersuchung lag auf der Analyse des Zielkonflikts (Trade-Offs) zwischen der Last auf dem System des Dateneigentümers und der notwendigen Offenlegung von Daten. Die zu entwickelnde Architektur sollte sich nahtlos in dezentrale, auf dem Solid-Protokoll basierende Systemlandschaften integrieren lassen und dabei die Prinzipien von Datensouveränität und Interoperabilität wahren.

Durchgeführte Arbeiten und Ergebnisse. Im Rahmen des Projekts wurde die Architektur für eine als „Authorization App“ (AuthApp) bezeichnete Komponente entworfen. Hierbei handelt es sich um eine eigenständige, wiederverwendbare Solid-Anwendung, deren primäre Funktion die Verwaltung von Datenfreigaben ist.

Die Kernidee der Architektur besteht darin, die komplexe Logik der Zugriffsverwaltung aus den einzelnen Fachanwendungen auszulagern. Anstatt dass jede Anwendung den Prozess zur Anforderung, Gewährung und zum Widerruf von Datenzugriffen selbst implementieren muss, kann sie auf die standardisierte Funktionalität der AuthApp zurückgreifen. Dies geschieht durch eine dynamische Weiterleitung des Nutzers von der Fachanwendung zur AuthApp, sobald eine Interaktion bezüglich einer Datenfreigabe erforderlich ist. Die Architektur wurde als reine Solid-Anwendung konzipiert. Abbildung 2.3 illustriert, wie die Autorisierungsapplikation mit den unterschiedlichen Komponenten einer Solid-basierten Systemlandschaft zusammenhängt. Diese architektonische Entkopplung stellt die Portabilität und Wiederverwendbarkeit der Komponente sicher und senkt die Entwicklungskosten für komplexe, datensouveräne Ökosysteme. Wir fassen die technischen Eigenschaften der entworfenen Architektur zusammen:

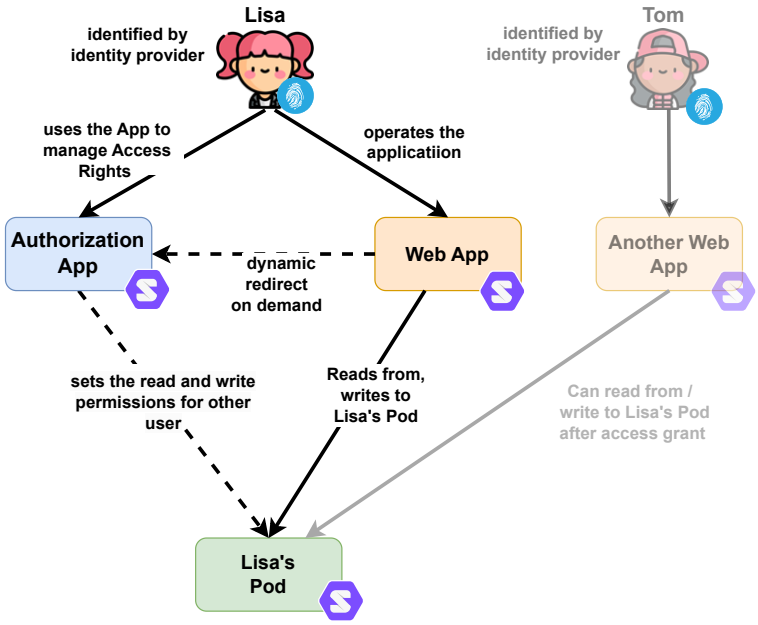


Abbildung 2.3: Komponentendiagramm Autorisierungsarchitektur. Lisa betreibt ihre Webanwendung unabhängig von der Autorisierungsapplikation. Wenn Tom auf bestimmte Daten in Lisas Pod zugreifen möchte, sendet er eine Datenzugriffsanfrage an Lisas Pod, wobei er zusätzliche Informationen wie Datentyp und Bedarf angibt. Lisa kann dann in der Autorisierungsapplikation über Toms Anfrage entscheiden und sie verwalten.

- Standardkonformität: Die Interaktion mit der AuthApp erfolgt ausschließlich über etablierte Webstandards (HTTP, REST, LDP, Solid).
- Minimierung der Last beim Datengeber: Die AuthApp führt keine geschäftslogische Datenverarbeitung durch. Fachanwendungen leiten den Nutzer zur AuthApp weiter, um eine Zugriffsgenehmigung einzuholen. Die eigentliche Verarbeitungslast verbleibt bei der Fachanwendung des Datennehmers, was die Infrastruktur des Datengebers schont.
- Datenspeicherung im Nutzerkontext: Alle für den Freigabeprozess relevanten Daten, wie Anfragen, erteilte Genehmigungen und deren Zwecke, werden direkt im Solid Pod des Nutzers gespeichert. Es werden keine Daten außerhalb des direkten Kontrollbereichs des Nutzers oder der Organisation abgelegt.
- Zero-Trust-Prinzip: Da die Komponente keine eigenen Daten speichert und vollständig im Kontext des Nutzers agiert, werden keine Spuren außerhalb des Geltungsbereichs des Nutzers hinterlassen und es muss keiner zusätzlichen Komponente vertraut werden.

- Portabilität und Wiederverwendbarkeit: Durch die Auslagerung der komplexen Logik der Zugriffsverwaltung in die AuthApp müssen diese Prozesse nicht von jeder Fachanwendung neu implementiert werden. Dies senkt die Entwicklungskosten und fördert einheitliche Sicherheitsstandards im Ökosystem.

Software-Artefakte. Die Referenzimplementierung der AuthApp, die auf dieser Architektur basiert, ist im zentralen GitHub-Repository des MANDAT-Projekts[15] öffentlich zugänglich.

Zugehöriges Ergebnisdokumente. Die detaillierte Beschreibung der Architektur, der Anforderungen und der konzeptionellen Einbettung in das Solid-Ökosystem sind in folgenden wissenschaftlichen Publikationen dokumentiert:

- Andreas Both, Thorsten Kastner, Dustin Yeboah, Christoph Braun, Daniel Schraudner, Sebastian Schmid, Tobias Käfer, Andreas Harth: Foundational Com- ponents for B2B Data Sharing Using the Solid Protocol. In: Journal of Web Engineering (2025), (akzeptiert). [7]
- Andreas Both, Thorsten Kastner, Dustin Yeboah, Christoph Braun, Daniel Schraudner, Sebastian Schmid, Tobias Käfer, Andreas Harth: AuthApp - Portable, Reusable Solid App for GDPR-Compliant Access Granting. ICWE 2024: 199-214 [6]
- Thorsten Kastner, Dustin Yeboah, Andreas Both, Sebastian Schmid, Daniel Schraudner, Christoph H.-J. Braun, Andreas Harth, Tobias Käfer: Cornerstones of a Future Solid B2B Ecosystem: Authorization App and Rights Delegation Proxy. SoSy 2024: 51-57 [28]

Erfüllung der Zielsetzung. Durch den Entwurf der AuthApp als eine entkoppelte, standardbasierte und reine Solid-Anwendung wurde das Ziel des Arbeitspakets vollständig erreicht. Die geschaffene Architektur für Verarbeitungstransparenz ermöglicht es, die Datenzugriffsverwaltung aus den Fachanwendungen auszulagern. Die entworfene Architektur löst den zentralen Trade-Off zwischen Systemlast und Datenkontrolle effektiv auf. Sie ermöglicht eine zweckgebundene, transparente und DSGVO-konforme Datenfreigabe, ohne die Systeminfrastruktur des Datengebers zu belasten. Die geschaffene Lösung ist portabel, wiederverwendbar und legt einen entscheidenden Grundstein für sichere und datensouveräne Verarbeitungsschritte im Solid-Ökosystem.

2.3.2 AP 3.2 Transparentmachung der Datenverarbeitungs- und -weitergabeschritte

Zielsetzung des Arbeitspakets. Aufbauend auf der in AP 3.1 entworfenen Architektur war das Ziel dieses Arbeitspakets, die konkreten Schritte der Datenverarbeitung und -weitergabe für den Nutzer transparent und nachvollziehbar zu gestalten. Diese Transparenz sollte direkt bei der Anfrage (dem Ersuchen) für den Zugriff auf Daten in einem Solid Pod zum Tragen kommen. Dabei sollten sowohl fachliche Aspekte (z. B. der

[15] `https://github.com/mandat-project/hackathon-demo`

Verwendungszweck wie „Bilanzdatenmonitoring“) als auch technische Aspekte (z. B. welche Datenfelder werden für eine Durchschnittsberechnung benötigt) eine Rolle spielen. Ein zentraler Aspekt war somit die Schaffung von Mechanismen, die es Dateneigentümern ermöglichen, informierte, granulare und DSGVO-konforme Entscheidungen über Zugriffsanfragen zu treffen und diese zu jeder Zeit zu überwachen. Die Lösung sollte Nutzern die volle Kontrolle darüber geben, welche Daten mit wem und zu welchem Zweck geteilt werden. Eine formale Modellierung sollte zudem die Grundlage für zukünftige, automatisierte Freigabeentscheidungen schaffen.

Durchgeführte Arbeiten und Ergebnisse. Zur Erreichung der Zielsetzung wurde die in AP 3.1 entworfene Authorization App (AuthApp) hinsichtlich der benötigten Daten und Informationen weiter spezifiziert:

- Modellierung der fachlichen Aspekte: Der fachliche Verwendungszweck („Warum werden die Daten benötigt?“) wurde als zentrale Komponente für eine informierte Entscheidung identifiziert. Dieser Zweck wird mithilfe von Linked-Data-Vokabularien formal und maschinenlesbar beschrieben. Dies erlaubt es, einen klaren Grund wie Kreditwürdigkeitsprüfung oder Vertragserfüllung anzugeben, der für den Nutzer verständlich und gleichzeitig systemisch auswertbar ist.
- Modellierung der technischen Aspekte: Die technischen Verarbeitungsschritte („Welche Daten werden wie verarbeitet?“) werden durch die Spezifikation der benötigten Datenstruktur modelliert. Anstatt vage Finanzdatenänzufragen, wird mittels Shape Trees eine präzise, maschinenlesbare Definition der Daten-Schemata angefordert. Diese legt exakt fest, welche Datenfelder und -typen die Anwendung für ihre Funktion (z.B. eine Durchschnittsberechnung) benötigt. Damit wird die Datennutzung auf das technisch erforderliche Minimum (Prinzip der Datenminimierung) beschränkt und transparent gemacht.

Für den Nutzer stellt die AuthApp eine webbasierte Benutzeroberfläche bereit, die den Nutzer durch den gesamten Prozess der Zugriffsverwaltung führt. Die Transparenz wird durch folgende implementierte Kernfunktionen sichergestellt:

- Verwaltung von Zugriffsanfragen: Die AuthApp empfängt und visualisiert neue Datenfreigabeanfragen. Der Nutzer kann diese Anfragen gezielt annehmen oder ablehnen.
- Überwachung von Berechtigungen: Es wird eine umfassende Übersicht über alle erteilten, abgelehnten und widerrufenen Berechtigungen geboten. Dies ermöglicht dem Dateneigentümer die lückenlose Nachvollziehbarkeit aller Datenflüsse.
- Widerruf von Zugriffen: Bestehende Berechtigungen können jederzeit mit sofortiger Wirkung widerrufen werden, um die Einhaltung von DSGVO-Vorgaben zu gewährleisten.

Ein wesentliches Merkmal für die Transparenz ist die detaillierte und maschinenlesbare Aufbereitung der Zugriffsanfragen. Wie in Abbildung 2.4 dargestellt, werden dem Nutzer alle entscheidungsrelevanten Informationen angezeigt:

- Anfragesteller: Wer (Person oder Organisation) fragt den Datenzugriff an.

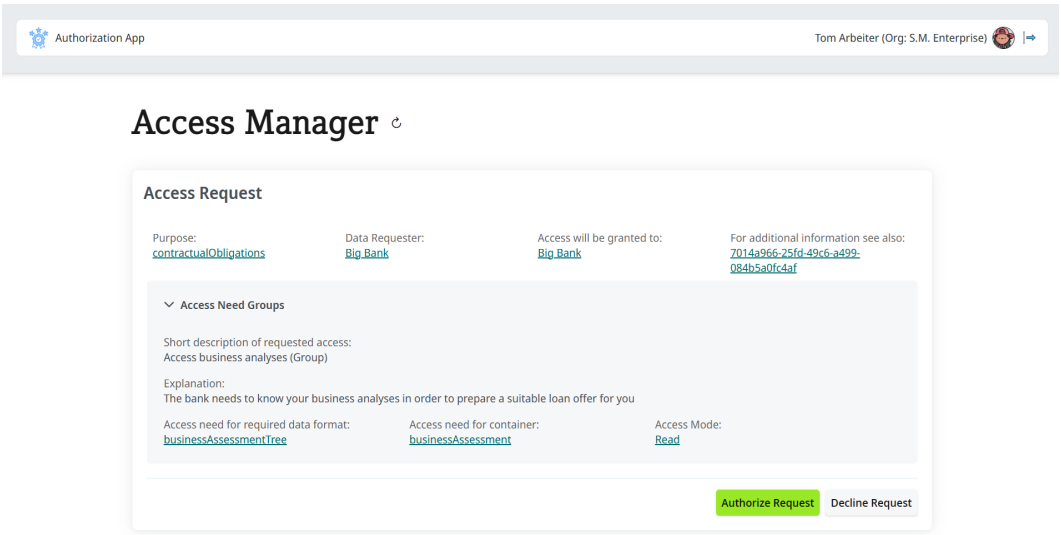


Abbildung 2.4: Benutzeroberfläche der AuthApp. Dargestellt ist eine Zugriffsanfrage der „BigBank“ auf Geschäftsberichte des „SME“ zum Zweck der Vertragserfüllung. Alle relevanten Informationen sind klar ersichtlich und über Links weiterführend abrufbar.

- Anfragegegenstand: Auf welche konkreten Daten oder Daten-Typen wird der Zugriff erbeten.
- Zweck der Verarbeitung: Für welchen spezifischen, vom Anfragesteller deklarierten Zweck werden die Daten benötigt (z. B. zur Erfüllung einer vertraglichen Verpflichtung).

Diese Informationen basieren auf standardisierten Vokabularien und sind über Links abrufbar und maschinenlesbar, was die Grundlage für zukünftige automatisierte Konformitätsprüfungen legt. Der gesamte Prozess der Rechtevergabe und die zugehörigen Metadaten werden revisionssicher im Solid Pod des Nutzers protokolliert.

Software-Artefakte. Die Referenzimplementierung der AuthApp, die auf dieser Architektur basiert, ist im zentralen GitHub-Repository des MANDAT-Projekts[16] öffentlich zugänglich.

Zugehöriges Ergebnisdokumente. Die detaillierte Beschreibung der Architektur, der zugrundeliegenden Anforderungen und der konzeptionellen Einbettung in das Solid-Ökosystem sind in folgenden wissenschaftlichen Publikationen dokumentiert:

- Andreas Both, Thorsten Kastner, Dustin Yeboah, Christoph Braun, Daniel Schraudner, Sebastian Schmid, Tobias Käfer, Andreas Harth: Foundational Com- ponents for B2B Data Sharing Using the Solid Protocol. In: Journal of Web Engineering (2025), (akzeptiert). [7]

[16] `https://github.com/mandat-project/hackathon-demo`

- Andreas Both, Thorsten Kastner, Dustin Yeboah, Christoph Braun, Daniel Schraudner, Sebastian Schmid, Tobias Käfer, Andreas Harth: AuthApp - Portable, Reusable Solid App for GDPR-Compliant Access Granting. ICWE 2024: 199-214 [6]
- Thorsten Kastner, Dustin Yeboah, Andreas Both, Sebastian Schmid, Daniel Schraudner, Christoph H.-J. Braun, Andreas Harth, Tobias Käfer: Cornerstones of a Future Solid B2B Ecosystem: Authorization App and Rights Delegation Proxy. SoSy 2024: 51-57 [28]

Erfüllung der Zielsetzung. Die Ziele des Arbeitspakets wurden vollständig erfüllt. Es wurde eine Modellierung zur Beschreibung der Datenverarbeitung erfolgreich untersucht und spezifiziert. Das entwickelte zweistufige Modell trennt fachliche und technische Aspekte und macht sie für den Dateneigentümer transparent, was eine informierte Entscheidung ermöglicht. Durch die Verwendung formaler, maschinenlesbarer Beschreibungen (Shape Trees, Linked-Data-Vokabularien) wurde zudem die Voraussetzung für eine zukünftige Automatisierung von Freigabeprozessen geschaffen und damit die Zielsetzung vollumfänglich erreicht.

2.3.3 AP 3.3 Protokollierung der Datenverarbeitungsschritte

Zielsetzung des Arbeitspakets. Ziel dieses Arbeitspakets war die Untersuchung von Methoden zur Protokollierung von Datenverarbeitungsschritten während ihrer Ausführung (in processus). Sobald Daten den Kontrollbereich eines Nutzers verlassen (dem Paradigma data-to-compute folgend), ist deren weitere Verarbeitung ohne eine vertrauenswürdige Ausführungsumgebung nicht mehr nachvollziehbar. Eine Alternative ist das compute-to-data-Paradigma, bei dem die Verarbeitungslogik zu den Daten gesendet wird. Hierbei besteht jedoch die Herausforderung, dass die Verarbeitungslogik selbst ein schützenswertes Geschäftsgeheimnis sein kann. Unabhängig vom gewählten Paradigma war es das Ziel, einen Ansatz zu entwickeln, mit dem die durchgeführten Verarbeitungsschritte nachvollziehbar beschrieben, dokumentiert und auf ihre Integrität hin überprüft werden können.

Durchgeführte Arbeiten und Ergebnisse. Die Arbeiten konzentrierten sich auf die Datenverarbeitung im Umfeld semantischer Technologien, in dem die Abfragesprache SPARQL eine zentrale Rolle spielt. Es wurde ein Ansatz zur Übermittlung, Beschreibung und Dokumentation von SPARQL-basierter Datenverarbeitung konzipiert.

Das Ergebnis ist der Ansatz HaVaRi, der eine Methode zur lückenlosen Dokumentation der Datenverarbeitung in einem Wissensgraphen unter Verwendung der PROV-Ontologie (PROV-O) darstellt. Darüber hinaus wird die Integrität der Verarbeitungsergebnisse durch den Einsatz digitaler Signaturen sichergestellt. Abbildung 2.5 illustriert den konzeptionellen Ansatz von HaVaRi.

Das für HaVaRi entwickelte Datenmodell (siehe Abbildung 2.6) wird als RDF-Graph beschrieben und besteht aus drei aufeinanderfolgenden Schichten, die jeweils eine neue Facette der Dokumentation und Sicherstellung der Datengenauigkeit hinzufügen. Für

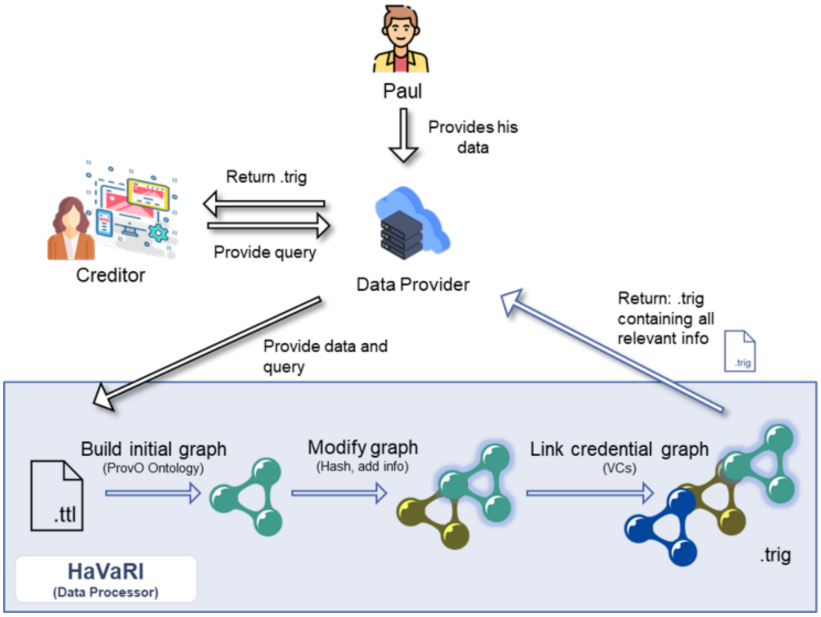


Abbildung 2.5: Der konzeptionelle HaVaRi-Ansatz zur nachvollziehbaren Protokollierung und Integritätssicherung von Datenverarbeitungsschritten.

die Modellierung wurde die etablierte PROV-Ontologie um eine projektspezifische Erweiterung namens PROV-X ergänzt. PROV-X dient der verbesserten Dokumentation der spezifischen Verarbeitungsschritte, die im Projektkontext relevant sind.

Software-Artefakte. Der HaVaRi-Ansatz stellt ein konzeptionelles Ergebnis dar. Prototypische Implementierungen befinden sich in einem internen Projektstadium und sind zum aktuellen Zeitpunkt nicht öffentlich verfügbar.

Zugehöriges Ergebnisdokument. Die Ergebnisse der Untersuchung sind in internen Projektdokumenten festgehalten und werden für eine zukünftige wissenschaftliche Publikation aufbereitet.

Erfüllung der Zielsetzung. Die Ziele des Arbeitspakets wurden erreicht. Mit HaVaRi wurde eine Methode zur Protokollierung von Datenverarbeitungsschritten erfolgreich konzipiert. Der Ansatz liefert ein konkretes Modell zur Dokumentation von SPARQL-basierter Verarbeitung und berücksichtigt dabei sowohl die Nachvollziehbarkeit des Prozesses (mittels PROV-O und PROV-X) als auch die Integrität der Ergebnisse (mittels digitaler Signaturen). Damit wurde eine wichtige Grundlage für die Schaffung von auditierbaren und vertrauenswürdigen Datenverarbeitungsketten in datensouveränen Ökosystemen gelegt.

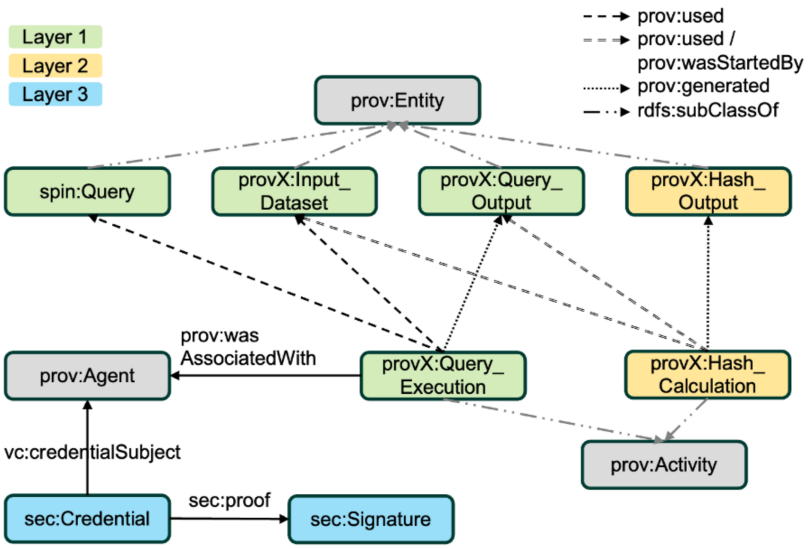


Abbildung 2.6: Das für HaVaRi entwickelte Modellierungsschema zur Beschreibung von Datenverarbeitung mittels SPARQL unter Nutzung von PROV-O und der Erweiterung PROV-X.

2.4 AP 4: Integrität von Daten und Analysen

Im Rahmen des Arbeitspakets 4 wurden Methoden für die Integrität und Authentizität von Daten und Analysen untersucht. Dabei wurde ein Fokus auf Technologien für das Signieren von RDF Graphen sowie für die Beschreibung von zugehörigen Metadaten gelegt. Auf diese Weise können Daten, die über das Solid Protokoll verwaltet werden, zusätzlich zertifiziert werden, sodass ihre Integrität und Authentizität im Datenaustausch sichergestellt ist.

Dafür wurden zum einen Signaturen und Zertifikate hinsichtlich fachlicher Anforderungen (Verordnung Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG) untersucht. Zum anderen wurden Technologien für Signaturen und Zertifikate, beispielsweise qualifizierte elektronische Signaturen und Signaturen über RDF Graphen, auf ihre Anwendbarkeit geprüft. Im Rahmen der technischen Arbeit zu Signaturen und Zertifikaten ist insbesondere das Feld der neu entstehenden Web Standards zu Verifiable Credentials (VCs) durch das World Wide Web Consortium (W3C) untersucht worden. Dort ergaben sich Probleme bei der Interoperabilität unterschiedlicher Lösungen für Zertifikate. Für dieses Problem präsentiert MANDAT eine Architektur für die semantische Interoperabilität von Web-basierten Zertifikaten als Lösung [15].

Zur Sicherstellung der Integrität und Authentizität von Daten im Web, die unter einer URI [5] und mithilfe des Resource Description Frameworks (RDF) [22] beschrieben sind,

wurde insbesondere für ortsfeste Daten eine neue Methode entwickelt [14]. Für den Umzug von Daten, während gleichzeitig deren Integrität und Authentizität erhalten bleiben soll, wurden kleinere Arbeiten durchgeführt.

Zur Sicherstellung der Integrität von Verarbeitungsschritten wird sich auf die in AP 3 stattgefundene Arbeit hinsichtlich der Beschreibung und Protokollierung von Verarbeitungsschritten bezogen. Insbesondere ergänzen die im Rahmen des AP 4 stattgefundenen kleineren Arbeiten die Protokollierung der Verarbeitungsschritte um Signaturen für entsprechende Verarbeitungszertifikate.

Um den Einsatz in der Praxis unter relevanten Bestimmungen, Praktiken und Regularien zu prüfen, wurde die Praktikabilität der im AP 4 entwickelten Methoden teilweise anhand fachlicher Szenarien und teilweise formal untersucht. Dabei wurden insbesondere der Aspekt der Datenminimierung im Rahmen von Zertifikaten und Signaturen geprüft [9], sowie die Sicherheit von Authentifizierungsprotokollen, die auf den Web Standards rund um Verifiable Credentials basieren, formal überpüft [13].

Nachfolgend werden die durchgeführten Arbeiten detaillierter beschrieben.

2.4.1 AP 4.1 Signaturen und Zertifikate

Zielsetzung des Arbeitspakets. In diesem Arbeitspaket sollten Technologien für Signaturen und Zertifikate aus zweierlei Perspektiven untersucht werden. Zum einen aus einer fachlichen Perspektive, die sich auf rechtliche Rahmenbedingungen wie die eIDAS-Verordnung (EU) Nr. 910/2014 sowie auf Praktiken rund um rechtsverbindliche Unterschriften im Unternehmenskontext konzentriert. Zum anderen aus einer technischen Perspektive, die Technologien für qualifizierte elektronische Signaturen sowie für das Signieren von semantischen Daten (Linked Data) beleuchtet, deren Standardisierung beim W3C aktiv vorangetrieben wird.

Durchgeführte Arbeiten und Ergebnisse. Diese Übersicht basiert u.a. auf unseren publizierten Arbeiten [9, 13, 14, 15] im Rahmen des Projektes.

1. Stand der Technik - Fachliche Perspektive: Eine Analyse der rechtlichen Rahmenbedingungen für elektronische Signaturen bildete die Grundlage der Arbeiten. Die EU-Verordnung Nr. 910/2014 (eIDAS) definiert drei Stufen elektronischer Signaturen:

- Einfache Elektronische Signatur (EES): Die niedrigste Stufe ohne rechtliche Garantien bezüglich des Ursprungs oder der Validität (z.B. eine eingescannte Unterschrift).
- Fortgeschrittene Elektronische Signatur (FES): Ein höheres Sicherheitsniveau, das die eindeutige Zuordnung zum Unterzeichner ermöglicht und die nachträgliche Manipulation der Daten erkennbar macht.
- Qualifizierte Elektronische Signatur (QES): Die höchste Stufe, die rechtlich der handschriftlichen Unterschrift gleichgestellt ist und von einem qualifizierten Vertrauensdiensteanbieter (VDA) ausgestellt werden muss.

Anwendung im deutschen Recht: Nach deutschem Zivilrecht (§ 126a BGB) kann nur die QES die gesetzlich vorgeschriebene Schriftform ersetzen.

Relevanz für den Anwendungsfall: Für die im Projekt betrachteten Dokumente (z.B. Kreditverträge) besteht keine generelle gesetzliche Pflicht zur Verwendung einer bestimmten Signaturstufe. Die Wahl des Niveaus (EES, FES oder QES) richtet sich nach dem Sicherheitsbedürfnis und der von den Geschäftspartnern angestrebten Beweiskraft und Rechtssicherheit.

2. Stand der Technik - Technische Perspektive: Es muss klar getrennt werden zwischen der fachlichen Definition einer QES und der technischen Erstellung: Eine QES kann per Definition nur von einem VDA ausgestellt werden. Eine technisch äquivalente Signatur kann jedoch erstellt werden, wenn den entsprechenden technischen Standards entsprochen wird. Die technische Untersuchung umfasste sowohl traditionelle als auch moderne Signaturtechnologien.

- Traditionelle Signaturformate: Analysiert wurden etablierte Standards wie PAdES (für PDF), XAdES (für XML) und CAdES (für beliebige Datenformate). Gemeinsam ist diesen, dass sie vom konkreten Dateiformat (Serialisierung) der signierten Daten abhängen.
- Zertifikate: X.509-Zertifikate [21] wurden als etablierter Standard zur Verknüpfung kryptografischer Schlüssel mit Identitäten (Personen, Organisationen) betrachtet.
- Linked Data Signatures (LDS): Als zukunftsweisender Ansatz für die im Projekt verwendeten RDF-Daten wurden LDS identifiziert. Ihr entscheidender Vorteil ist die Unabhängigkeit von der Syntax (dem Datenformat), was die Verifikation über verschiedene Systeme hinweg vereinfacht.
- Verifiable Credentials (VCs) [43] und Self-Sovereign Identity (SSI) [1]: VCs wurden als flexibles Datenmodell zur Zertifizierung beliebiger Daten (sog. „Claims") im Kontext von SSI analysiert.
- Signaturen mit selektiver Offenlegung: Weiterhin wurden datenschutzfreundliche Signaturalgorithmen wie BBS+ [4], Camenisch-Lysyanskaya (CL) [17] und Pointcheval-Sanders (PS) [34] untersucht, die es ermöglichen, nur Teile eines zertifizierten Nachweises offenzulegen.

Durch die Verwendung des VC Datenmodells [43], können unterschiedlichste Daten zertifiziert werden. Zum Vergleich: Ein X.509-Zertifikat enthält eine Identität (einen Hostnamen, eine Organisation oder eine Einzelperson) und einen öffentlichen Schlüssel (RSA, DSA usw.) und wird entweder von einer Zertifizierungsstelle signiert oder ist selbstsigniert. In VCs können beliebige Daten mit einer breiten Auswahl an Signaturalgorithmen attestiert werden – sowohl von Zertifizierungsstellen als auch selbst.

Die Standardisierung dieser Technologien rund um VCs, welche in dem Bereich der Selbstverwalteten Identitäten (Self-Sovereign Identities, SSI) [1] anzusiedeln sind, ist noch nicht abgeschlossen und in stetem Wandel.

3. Methoden und Werkzeuge zur Signatur von Daten und Berechtigungen. Methoden und Werkzeuge zur Signatur von Daten und Berechtigungen sind weit verbreitet und gehören in der Praxis zum Alltag. Jedoch entstehen im Bereich der Selbstverwalteten Identitäten (Self-Sovereign Identity, SSI) [1] neue Standards und Spezifikationen, wie solche Berechtigungszertifikate zu modellieren und einzusetzen sind. Durch die hohe Heterogenität und Fragmentierung der sich noch in Entwicklung befindlichen Standards ist eine Adaption

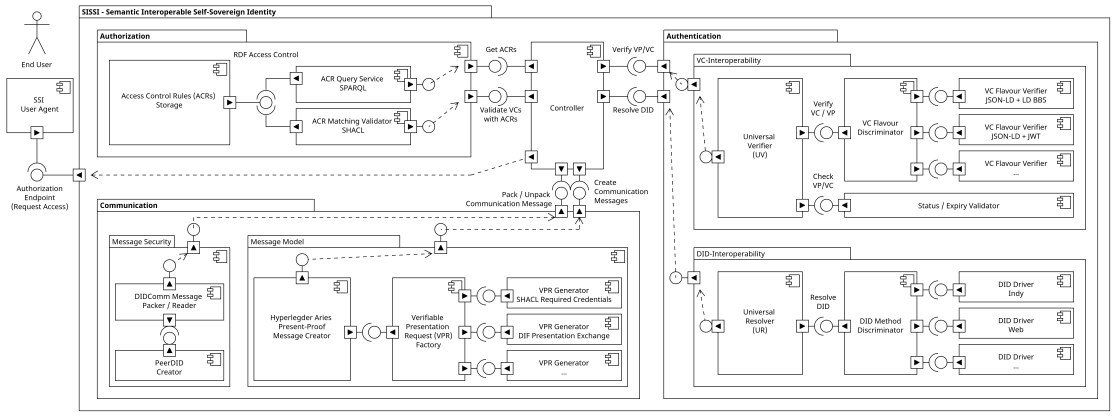


Abbildung 2.7: Die Komponenten der SISSI-Architektur.

über Unternehmensgrenzen hinweg zum jetzigen Zeitpunkt nicht trivial. Um Verständnis und Interoperabilität zu fördern, stellten wir mit SISSI [15] eine Architektur für eine semantische, interoperable, selbstverwaltete und identitätsbasierte Zugangskontrolle vor.

Übersicht: Die SISSI-Architektur basiert auf dem SSI Paradigma [1] und erreicht die semantische Interoperabilität der entsprechenden Konzepte unter Verwendung bestehender Web-Standards: Wir bauen auf dem semantischen Datenmodell auf, welches den Empfehlungen des W3C für dezentrale Identifikatoren (DIDs) [42] und dem Datenmodell für überprüfbare Berechtigungen (VC) [43] zugrunde liegt. Da ihr Datenmodell dem Resource Description Framework (RDF) [22] entspricht, modellieren wir nahtlos Zugangskontrollregeln (ACRs) unter Verwendung der Web Access Control (WAC) Ontologie [18], welche in der Solid-Community [19] genutzt wird.

Architektonische Innovation: Unsere Architektur, dargestellt in Abbildung 2.7, ermöglicht eine flexible und inkrementelle Erweiterbarkeit hinsichtlich neuer Dienste oder den Austausch bestehender Komponenten. Die unabhängige Weiterentwickelbarkeit ist ein wichtiger Vorteil, da aufgrund der dezentralen Natur und der schnellen Entwicklung des SSI-Paradigmas Aktualisierungen in den Kerntechnologien von SSI zu erwarten sind. Der Kern der Architektur sind der Universal DID Resolver und der Universal VC Verifier. Diese Komponenten ermöglichen es, verschiedene DID-Methoden und VC-Formate über eine einheitliche, erweiterbare Schnittstelle anzusprechen und zu überprüfen. Die SISSI-Architektur erreicht somit die gewünschte Interoperabilität zwischen SSI-Technologien.

Evaluation: Selbst ein einfaches Proof-of-Concept der SISSI-Architektur erbringt eine angemessene Leistung: Abhängig von den DID-Methoden dauert ein Autorisierungsprozess zwischen 1,5 und 3,1 Sekunden. Ein webbasiertes Vorgehen ist in Bezug auf die Ausführungszeit deutlich performanter als blockchain-basierte Ansätze. Mit unserer Architektur haben wir eine Lösungsmethode für die Probleme geschaffen, die durch die umstrittenen W3C Standards für VCs [43] und DIDs [42] verursacht werden.

Zugehörige Ergebnisdokumente. Die Ergebnisse dieser Arbeiten, insbesondere zum Stand der Technik sowie der Konzeption und Evaluation der SISSI-Architektur, wurden in der folgenden wissenschaftlichen Publikation detailliert beschrieben:

- Christoph H.-J. Braun, Ross Horne, Tobias Käfer, Sjouke Mauw: SSI, from Specifications to Protocol? Formally Verify Security! WWW 2024: 1620-1631 [13]
- Christoph H.-J. Braun, Vasil Papanchev, Tobias Käfer: SISSI: An Architecture for Semantic Interoperable Self-Sovereign Identity-based Access Control on the Web. WWW 2023: 3011-3021 [15]
- Christoph Braun, Tobias Käfer: Attribute-based Access Control on Solid Pods using Privacy-friendly Credentials. SEMANTiCS (Posters & Demos) 2022 [9]
- Christoph H.-J. Braun, Tobias Käfer: Self-verifying Web Resource Representations Using Solid, RDF-Star and Signed URIs. ESWC (Satellite Events) 2022: 138-142 [14]

Erfüllung der Zielsetzung. Die Ziele des Arbeitspakets wurden vollständig erfüllt. Es wurde eine umfassende Untersuchung von Signaturen und Zertifikaten aus fachlicher und technischer Perspektive durchgeführt. Darauf aufbauend wurde mit der SISSI-Architektur nicht nur ein theoretisches Konzept, sondern eine konkrete, evaluierte Lösungsmethode für die identifizierten Interoperabilitätsprobleme im zukunftsweisenden Bereich der SSI entwickelt. Die Ergebnisse liefern einen praxisnahen Ansatz für den Einsatz von überprüfbaren digitalen Zertifikaten in der im Projekt entwickelten Gesamtarchitektur.

2.4.2 AP 4.2 Integrität von ortsfesten und umgezogenen Daten

Zielsetzung des Arbeitspakets. In diesem Arbeitspaket sollten Methoden zur Sicherstellung der Integrität von RDF-basierten Repräsentationsbeschreibungen von Web-Ressourcen untersucht werden. Der Fokus lag dabei auf zentralen technischen Fragen wie der Äquivalenz von RDF-Graphen (Isomorphismus, kanonische Formen) und Hashing-Methoden. Eine besondere Herausforderung stellte der Vergleich von Graphen dar, die ihre Web-Adresse ändern („umgezogene Daten“). Weiterhin sollte die Möglichkeit untersucht werden, Hashes von RDF-Graphen mit Zeitstempeln zu versehen, um die Entwicklung von Daten über die Zeit nachvollziehbar zu machen.

Durchgeführte Arbeiten und Ergebnisse.

1. Analyse des Stands der Technik und bestehender Methoden: Im Rahmen des Projekts wurden Methoden zur Sicherstellung der Integrität von vernetzten Daten (Linked Data) untersucht. Die Integrität von Linked Data wird in der Regel durch die Berechnung und den Vergleich von kryptografischen Hashes der zugrunde liegenden RDF-Graphen überprüft. Eine wichtige Entwicklung während der Projektlaufzeit war die Finalisierung eines W3C-Standards für die Kanonisierung von RDF-Graphen [32], was eine Voraussetzung für vergleichbare Hashes ist. Unterschiedliche Algorithmen zur Erzeugung kryptografischer Hashes von RDF Graphen existieren schon seit langem [3, 20, 26, 31, 36, 44].

Die Analyse umfasste unter anderem die folgenden Ansätze:

- Trusty URIs [30, 31]: Diese erweitern eine URI um einen kryptografischen Hash des Ressourceninhalts. Dies macht Ressourcen überprüfbar und unveränderlich.
- Nanopublikationen [29]: Dieser Ansatz nutzt Trusty URIs, um Daten als überprüfbare und dauerhafte digitale Artefakte zu veröffentlichen. Da hierbei nur Hash-Werte verwendet werden, bleibt die Urheberschaft der Veröffentlichungen jedoch ungeschützt.
- Hashlinks[17]: Ein Entwurf der IETF, der kryptografisch gesicherte Hyperlinks vorschlägt, um unerwartete Änderungen an Ressourcen zu erkennen. Eine Schwäche dieses Ansatzes ist, dass die Hash-Berechnung vom Serialisierungsformat der Daten abhängt, was für RDF-Daten ungeeignet ist.
- Resource Integrity Proofs [2]: Eine hashbasierte Integritätsprüfung digitaler Ressourcen soll in Kombination mit Distributed-Ledger-Technologie einen dauerhafte Existenznachweise von Ressourcen zu schaffen. Ansätze, die einer solchen Strategie folgen, werden in [23, 45] untersucht und beispielsweise in einem einfachen Anwendungsfall der Lieferkette in [10, 11] angewendet.
- Linked Data Signatures (LDS): Im Kontext von Verifiable Credentials (VCs) [43] hat das W3C das Konzept der LDS als mögliches Signaturschema vorgeschlagen. Im Gegensatz zu VCs, die auf die Modellierung von Berechtigungsnachweisen spezialisiert sind, sind LDS breiter anwendbar, um beliebige Linked-Data-Inhalte zu signieren. Zum Zeitpunkt der Untersuchung war LDS noch nicht standardisiert.

2. Konzeption und Entwicklung neuer Methoden: Im Rahmen des Projektes wurde eine neue Methode entwickelt und demonstriert – Signierte URIs [14]. Als zentrales Ergebnis wurde im Projekt die neuartige Methode der Signierten URIs entwickelt. Diese Methode adressiert die festgestellte Lücke, dass bestehende Ansätze oft nur die Integrität, aber nicht die Urheberschaft von Daten sichern. Die Funktionsweise der Signierten URIs lässt sich wie folgt zusammenfassen:

- Grundlage: Der Ansatz baut auf dem Solid-Protokoll [19] auf, bei dem RDF-Daten in den persönlichen Online-Datenspeichern (Pods) der Nutzer gespeichert werden.
- Mechanismus: Eine Datenressource wird vom Nutzer mit einer Linked Data Signature (LDS) signiert. Für die Modellierung dieser Signatur wird RDF-star [25] verwendet.
- Innovation: Inspiriert von Trusty URIs [30] wird der URI ein Suffix hinzugefügt. Dieses Suffix enthält jedoch nicht den Hash des Inhalts, sondern den Wert der digitalen Signatur.
- Nutzen: Eine Signierte URI referenziert eine Ressource in einem spezifischen, vom Autor überprüften Zustand. Dies sichert sowohl die Integrität als auch die Authentizität der Daten.
- Demonstration: Die Erstellung und Verifizierung von Signierten URIs wurde im Rahmen einer Solid-Anwendung demonstriert.

3. Methode zur Sicherstellung der Integrität umgezogener Daten: Kleinere Arbeiten befassten sich mit der Integrität von umgezogenen Daten. Es wurde ein Algorithmus entworfen, der die strukturelle Gleichheit (Isomorphismus) von Linked-Data-Graphen relativ zu

[17] `https://tools.ietf.org/html/draft-sporny-hashlink-06`

einer neuen Basis-URI sicherstellt. Dies gewährleistet, dass Daten auch nach einer Änderung ihrer Web-Adresse als unverändert verifiziert werden können, solange ihre interne Struktur und Aussage gleich geblieben ist.

Software-Artefakt. Ein Prototyp zur Demonstration der Erstellung und Verifizierung von „Signierten URIs“ wurde im Rahmen einer Solid-Anwendung entwickelt. Der Quellcode ist öffentlich verfügbar[18] und die Funktionsweise ist im zugehörigen Ergebnisdokument detailliert beschrieben.

Zugehörige Ergebnisdokumente. Die Ergebnisse dieser Arbeiten, insbesondere die Konzeption und Umsetzung der „Signierten URIs“, wurde in der folgenden wissenschaftlichen Publikation detailliert beschrieben:

- Christoph H.-J. Braun, Tobias Käfer: Self-verifying Web Resource Representations Using Solid, RDF-Star and Signed URIs. ESWC (Satellite Events) 2022: 138-142 [14]

Erfüllung der Zielsetzung. Die Ziele des Arbeitspakets wurden vollständig erfüllt. Es wurden Methoden zur Sicherstellung der Datenintegrität untersucht und darauf aufbauend mit den „Signierten URIs“ eine neuartige Methode entwickelt, die über bestehende Ansätze hinausgeht, indem sie sowohl Integrität als auch Authentizität gewährleistet. Die spezifischen Herausforderungen der Nachverfolgung von Daten über die Zeit sowie der Integritätsprüfung von „umgezogenen Daten“ wurden durch die Konzeption der „Signierten URIs“ bzw. die Entwicklung eines dedizierten Isomorphismus-Algorithmus adressiert und gelöst.

2.4.3 AP 4.3 Integrität der Beschreibung von Verarbeitungsschritten

Zielsetzung des Arbeitspakets. Die in AP 3.3 untersuchte Beschreibung der Datenverarbeitung sollte in Arbeitspaket 4.3 mit Verfahren zur Sicherstellung ihrer Integrität angereichert werden. Ziel war es, nachzuweisen, dass eine Beschreibung eines Verarbeitungsschrittes (z. B. eine SPARQL-Anfrage) authentisch ist und nicht manipuliert wurde. Dabei sollten Methoden wie die Erzeugung kanonischer Formen von Anfragen und deren Hashing eine zentrale Rolle spielen. Die Untersuchung sollte im Hinblick auf die in AP 3 festgelegten architektonischen Entscheidungen erfolgen.

Durchgeführte Arbeiten und Ergebnisse. Um die Integrität der Beschreibungen von Verarbeitungsschritten zu gewährleisten, wurde der in AP 3.3 eingeführte HaVaRi-Ansatz angewendet und weiter ausgebaut. Die Kernidee besteht darin, für jede einzelne Datenverarbeitung eine in sich geschlossene, kryptografisch gesicherte und überprüfbare Protokolldatei zu erzeugen.

Dieser Prozess lässt sich wie folgt zusammenfassen:

[18] `https://github.com/uvdsl/solid-web-ldsig`

1. Bündelung der Evidenz: Zunächst werden alle für die Nachvollziehbarkeit relevanten Informationen in einem RDF-Graphen zusammengefasst. Dieser enthält:
   - Einen kryptografischen Hash der als Eingabe genutzten Daten.
   - Die exakte SPARQL-Anfrage, die den Verarbeitungsschritt darstellt.
   - Das Ergebnis, das durch die Ausführung der Anfrage erzeugt wurde.
2. Sicherstellung der Integrität: Dieser „Evidenz-Graph“ wird anschließend unter Verwendung des W3C-Standards zur RDF-Kanonikalisierung in eine eindeutige, serialisierte Form gebracht und gehasht. Über diesen finalen Hash wird eine digitale Signatur durch das verarbeitende System (HaVaRi) erstellt.
3. Erzeugung des Beweisdokuments: Die Signatur wird zusammen mit dem öffentlichen Schlüssel des Systems in einem separaten „Beweisgraphen“ (Proof Graph) gespeichert, der in Anlehnung an das W3C-Datenmodell für Verifiable Credentials (VCs) modelliert ist.

Das Endergebnis ist ein RDF-Datensatz, der sowohl das Ergebnis der Datenverarbeitung als auch den signierten Beweis für dessen korrekte und unveränderte Entstehung enthält. Dieser Datensatz wird zur Überprüfung an den Datengeber zurückgesandt, bevor eine Freigabe an die ursprünglich anfragende Partei erfolgt. Durch diesen Mechanismus wird die Integrität des gesamten Verarbeitungsschrittes gesichert. Es kann im Nachgang jederzeit von Dritten (z. B. im Rahmen eines Audits) überprüft werden, welche Anfrage auf Basis welcher Daten zu welchem Ergebnis geführt hat und dass dieses Protokoll seit seiner Erstellung nicht manipuliert wurde.

Software-Artefakte. Die beschriebene Methode ist Teil des konzeptionellen HaVaRi-Ansatzes. Prototypische Implementierungen befinden sich in einem internen Projektstadium und sind zum aktuellen Zeitpunkt nicht öffentlich verfügbar.

Zugehöriges Ergebnisdokument. Die Ergebnisse dieser Untersuchung sind in internen Projektdokumenten festgehalten und werden für eine zukünftige wissenschaftliche Publikation aufbereitet.

Erfüllung der Zielsetzung. Die Ziele des Arbeitspakets wurden vollständig erfüllt. Es wurde eine Methode entwickelt und konzeptionell umgesetzt, um die in AP 3.2 definierten Beschreibungen von Verarbeitungsschritten mit einem robusten Integritätsschutz zu versehen. Durch den Einsatz von kanonischen Hashes und digitalen Signaturen im Rahmen des HaVaRi-Ansatzes wurde ein Verfahren geschaffen, das die Authentizität und Unveränderbarkeit der Verarbeitungsprotokolle sicherstellt. Dies fügt sich nahtlos in die Gesamtarchitektur aus AP 3 ein und leistet einen wesentlichen Beitrag zur geforderten Auditierbarkeit und Vertrauenswürdigkeit des Systems.

2.4.4 AP 4.4 Zertifizierung und Auditierung der Integrität von Daten und Verarbeitungsschritten sowie Rechten

Zielsetzung des Arbeitspakets. Während das Projekt technisch funktionsfähige Technologien vorschlagen kann, ist für den Praxiseinsatz ein Abgleich mit relevanten Bestim-

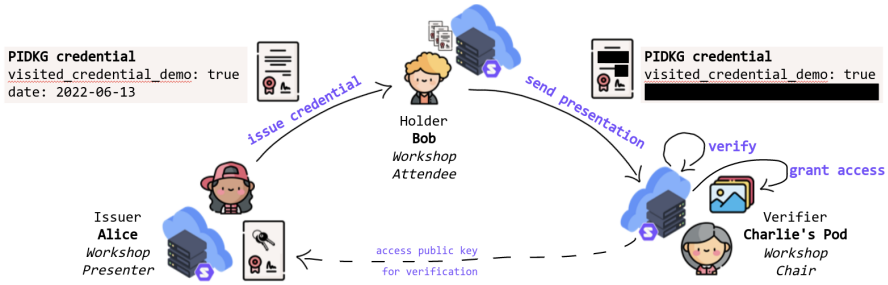


Abbildung 2.8: Zugriff auf Daten in einem Solid Pod mittels Verifiable Credential.

mungen, Gesetzen und Regularien erforderlich. Ziel dieses Arbeitspakets war es daher, die Praktikabilität der in den vorangegangenen Arbeitspaketen untersuchten Technologien (insbesondere Trusty URIs, Linked Data Signatures, Verifiable Credentials) zu untersuchen. Hierfür sollten die Technologien bestehenden und diskutierten Regularien auf nationaler und europäischer Ebene gegenübergestellt werden, um eine Validierung zu erzielen und Lücken für zukünftige Forschung und Entwicklung aufzuzeigen.

Durchgeführte Arbeiten und Ergebnisse. Im Rahmen des Arbeitspakets wurden die im Projekt entwickelten und analysierten Technologien vor dem Hintergrund zentraler europäischer Verordnungen – insbesondere der DSGVO und der neuen eIDAS-Verordnung (EU) 2024/1183 – bewertet. Die Technologien bieten eine tragfähige Grundlage für vertrauenswürdige, regulierungskonforme Datenverarbeitung, erfordern jedoch noch standardisierte Zertifizierungsverfahren und rechtliche Klärungen zur breiten Umsetzung.

1. Validierung der technologischen Ansätze: Die im Projekt fokussierten Technologien passen konzeptionell zu den Zielen der europäischen Gesetzgebung.

- Integrität und Nachvollziehbarkeit: Methoden wie die in AP 4.2 entwickelten „Signierten URIs“ erfüllen grundlegende Anforderungen an die Sicherstellung der Datenintegrität und die Nachvollziehbarkeit von Änderungen, wie sie von Compliance-Frameworks und Regulatorien (DSGVO, eIDAS und ISO 27001) gefordert werden.
- Datensparsamkeit und zweckgebundene Zugriffskontrolle: Die in AP 4.1 untersuchten Verifiable Credentials (VCs) ermöglichen in Kombination mit der Solid-Architektur eine datensparsame Rechte- und Rollenvergabe. Wie in einer explorativen Arbeit im Rahmen des Projektes [9] gezeigt wurde, kann ein Nutzer selektiv nur die für einen Vorgang notwendigen Attribute eines digitalen Nachweises offenlegen (siehe Abbildung 2.8). Dies adressiert Kernanforderungen der DSGVO an Datenminimierung und Zweckbindung.
- Datensouveränität: Die Solid-Architektur überzeugte insbesondere durch die Trennung von Datenhaltung und -verarbeitung sowie durch ihre dezentrale Rechteverwaltung im Sinne der DSGVO. Die dezentrale Architektur von Solid in Verbindung mit VCs unterstützt das in der eIDAS-Verordnung formulierte Ziel der Nutzerkontrolle über die eigene digitale Identität im Rahmen der neuen „European Digital Identity Wallets“ (EuID Wallets).

2. Aufgedeckte Lücken für Forschung und Entwicklung: Die detaillierte Analyse deckte jedoch auch erhebliche Lücken zwischen dem technologisch Möglichen und den Anforderungen für einen rechtssicheren, zertifizierbaren Praxiseinsatz auf:

- Lücke 1: Schwächen in den zugrundeliegenden SSI-Standards: Eine im Projekt durchgeführte formale Sicherheitsanalyse von Protokollen [13], die auf VCs und Decentralised Identifiers (DIDs) basieren, deckte kritische Schwachstellen auf. Es wurde nachgewiesen, dass als „optional" deklarierte Parameter in den Spezifikationen für die Sicherheit zwingend erforderlich sind. Ihr Weglassen ermöglicht Angriffe, bei denen sich unberechtigte Personen mit den Nachweisen ehrlicher Nutzer authentifizieren können. Diese Unschärfe in den Basis-Spezifikationen stellt ein erhebliches Hindernis für die Entwicklung nachweislich sicherer Systeme dar.
- Lücke 2: Fehlende Zertifizierungs- und Audit-Standards: Die Untersuchung ergab, dass aktuelle Audit-Frameworks (z. B. nach ISO 27001) nicht auf die Besonderheiten von dezentralen, semantischen Datenräumen ausgelegt sind. Es fehlen etablierte, rechtlich belastbare Bewertungs- und Zertifizierungsverfahren für dynamisch referenzierte, dezentral gespeicherte Daten.
- Lücke 3: Paradigmen-Unterschied zwischen Solid und EuID Wallets: Obwohl Solid die geforderte Datensouveränität ermöglicht, folgt die Architektur nicht zwangsläufig dem „Wallet"-App-Paradigma, das die EU-Gesetzgebung vorsieht. Die explorativen Arbeiten im Rahmen des Projektes [9] zeigten zwar einen Weg zur Überbrückung dieser Lücke auf, verdeutlichten aber auch den Bedarf an weiterer Forschung, um eine nahtlose und standardkonforme Integration zu gewährleisten.

Besonders hervorzuhebender Beitrag zur Schließung von Lücke 1:
Formale Sicherheitsanalyse von SSI-basierten Authentifizierungsprotokollen [13].

Methodik: Zunächst wurden die zugrundeliegenden Annahmen aus den Standard-Vertrauens-Modellen explizit gemacht. Anschließend wurde ein symbolisches Modell des Authentifizierungsprotokolls systematisch aus den entsprechenden Standards konstruiert, sodass eine direkte Verbindung zwischen Protokoll, Modell und Standard geschaffen wurde. Mithilfe symbolischer Sicherheitstools wurde dann das Model formal auf sicherheits- und datenschutzrelevante Merkmale wie Geheimhaltung, Authentifizierung und Unverknüpfbarkeit hin überprüft. Diese Methodik erlaubt es, die Lücke zwischen den theoretischen Spezifikationen und den Anforderungen an eine sichere, praktische Implementierung zu schließen.

Zentrale Erkenntnisse: Bestimmte, in den Spezifikationen als optional gekennzeichnete Parameter sind für die Sicherheit des Protokolls faktisch zwingend erforderlich. Das Weglassen dieser Parameter führt zu schwerwiegenden, praktisch durchführbaren Angriffen. Insbesondere wurde eine Schwachstelle nachgewiesen, bei der sich Angreifer mit den digitalen Nachweisen (Credentials) ehrlicher Nutzer authentifizieren und somit deren Identität annehmen können.

Schlussfolgerung und Empfehlung: Aufgrund der aufgedeckten Schwachstellen in den zugrundeliegenden Standards kann zum jetzigen Zeitpunkt keine uneingeschränkte Empfehlung für den breiten Einsatz von DIDs und VCs in sicherheitskritischen Systemen

ausgesprochen werden. Die durchgeführte Arbeit liefert eine formale Begründung und konkrete Ansatzpunkte, welche zusätzliche Präzision von den Standardisierungsgremien und Implementierern gefordert werden muss, um Sicherheitslücken zu schließen.

Software-Artefakte. Die formalen Analysen aus [13] sind online öffentlich verfügbar[19]. Auch die prototypische Implementierung aus [9] ist öffentlich verfügbar[20].

Zugehörige Ergebnisdokumente. Die Ergebnisse dieser Untersuchung sind in den folgenden wissenschaftlichen Publikationen dokumentiert:

- Christoph H.-J. Braun, Ross Horne, Tobias Käfer, Sjouke Mauw: SSI, from Specifications to Protocol? Formally Verify Security! WWW 2024: 1620-1631 [13]
- Christoph Braun, Tobias Käfer: Attribute-based Access Control on Solid Pods using Privacy-friendly Credentials. SEMANTiCS (Posters & Demos) 2022 [9]

Erfüllung der Zielsetzung. Die Ziele des Arbeitspakets wurden vollständig erfüllt. Es wurde eine Gegenüberstellung der im Projekt untersuchten Technologien mit den relevanten rechtlichen Rahmenbedingungen durchgeführt. Die Ergebnisse validieren, dass die Ansätze prinzipiell geeignet sind, die Ziele von DSGVO und eIDAS 2.0 zu unterstützen. Gleichzeitig wurden durch die Analyse klare Lücken für die zukünftige Forschung und Entwicklung identifiziert, insbesondere im Bereich der Standard-Spezifikationen und der fehlenden Audit-Verfahren. Das Projekt liefert somit die geforderte, wohlfundierte Bewertung der Praktikabilität der untersuchten Technologien.

2.5 AP 5: Demonstrator, Evaluation und Verbreitung

Im Rahmen des Arbeitspakets 5 wurde ein nutz- und vorzeigbarer Demonstrator als prototypische Umsetzung des Anwendungsfalls realisiert und mit den Anforderungen aus AP1.1 abgeglichen. Die folgende Beschreibung fasst unsere diesbezüglichen gemeinsamen Forschungsergebnisse zusammen, die in [6] und [7] veröffentlicht wurden.

2.5.1 AP 5.1 Implementierung des Demonstrators

Zielsetzung des Arbeitspakets. Ziel des Arbeitspakets 5.1 war die Umsetzung eines nutz- und vorzeigbaren Demonstrators zur prototypischen Umsetzung des Anwendungsfalls.

Komponenten

Die Komponenten des Demonstrators sind in Abbildung 2.9 dargestellt. Die Architektur besteht aus folgenden Komponenten:

- Solid Pod

[19] `https://github.com/uvdsl/ssi-protocol-verify`
[20] `https://github.com/uvdsl/solid-vc-pwa`

- Rights Delegation Proxy (RDP)
- Data Provisioning Proxy (DPP)
- Authorization App (AuthApp)
- Company Web App

Die Bausteine AuthApp, RDP und DPP wurden dabei konzeptionell derart gestaltet, dass sie eine einfache Wiederverwendung ermöglichen.

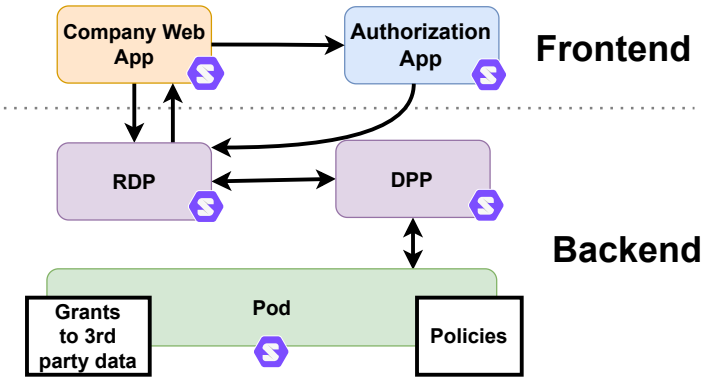


Abbildung 2.9: Übersicht Systemkomponenten

Der Solid Pod eines Unternehmens speichert die Geschäftsdaten des Unternehmens und stellt sie unter Zugriffskontrolle zur Verfügung. Er enthält außerdem Regeln für die Rechtedelegation an die Mitarbeitenden des Unternehmens sowie bestehende Rechte zur Weitergabe von Daten Dritter an weitere Dritte für die Realisierung von Datenteilungsketten.

Die AuthApp ermöglicht es Nutzern, Daten auf Anfrage zu teilen. Mit ihr werden Zugriffsanfragen auf den Solid Pod des Unternehmens verwaltet und entsprechend berechtigten Mitarbeitenden ermöglicht, empfangene, bestehende, abgelehnte und widerrufene Anfragen zur Datenfreigabe von Unternehmensdaten zu überwachen und zu bearbeiten.

Der Rights Delegation Proxy (RDP) empfängt und protokolliert Anfragen, die von Mitarbeitenden des Unternehmens (z.B. Tom, Lisa, Max) über die UnternehmenswebApp gestellt werden. Der Mitarbeitende wird über seine WebID authentifiziert und es wird anhand der im Unternehmens-Pod hinterlegten Richtlinien geprüft, ob dieser die erforderlichen Bevollmächtigungen / Rechte besitzt (bspw. für Datenfreigabe). Sind alle Voraussetzungen erfüllt, wird die Anfrage im Namen der delegierenden anstatt der bevollmächtigten Person ausgeführt. Empfangene Antworten werden protokolliert und an die delegierende Person weitergeleitet.

Der Data Provisioning Proxy (DPP) empfängt alle Datenanfragen, z.B. Anfragen von Lisa im Namen der Bank. Dabei wird überprüft, ob es sich bei der Datenanfrage um unternehmenseigene Daten (des KMU) im Unternehmens-Pod handelt oder um externe Daten eines Dritten. Stammen die angeforderten Daten von einem Dritten, wird die Freigaberichtlinie des Drittanbieters durch den DPP geprüft. Sofern der Zugriff erlaubt

ist, wird die Ressource abgerufen, der Datenursprung dabei versteckt und die Daten so bereitgestellt, als stammen sie vom Unternehmen selbst.

Für jede der beteiligten Unternehmen im Use Case wurde als einzige spezifische Anwendung eine Solid-kompatible Company Web App entwickelt. Sie ermöglicht den Mitarbeitenden ihre Geschäftstätigkeiten. In unserem Use-Case beispielsweise die Initiierung einer Kreditanfrage vom KMU an die BigBank, die Bereitstellung der von der BigBank angeforderten Geschäftsberichte oder die Genehmigung des Kreditangebots der BigBank.

Kontextdiagramm

Abbildung 2.10 stellt ein umfassendes Kontextdiagramm dar, das die wichtigsten Elemente und Akteure im Rahmen des Projekts visualisiert. Es zeigt die beteiligten Unternehmen sowie die relevanten Rollen und Personen innerhalb dieser Unternehmen, die aktiv in die dargestellten Prozesse eingebunden sind. Darüber hinaus beinhaltet das Diagramm sowohl die im Projekt prototypisch entwickelten unternehmensspezifischen Anwendungen als auch die generisch einsetzbaren, auf Solid basierenden, wiederverwendbaren Komponenten AuthApp, RDP und DPP, welche zentrale Funktionen im Umgang mit datenbasierten Interaktionen erfüllen: Das Zusammenspiel dieser Elemente im dargestellten Kontext bildet die Grundlage für eine vertrauenswürdige, nachvollziehbare und datenschutzkonforme Datenverarbeitung und -weitergabe im Rahmen des Projektansatzes.

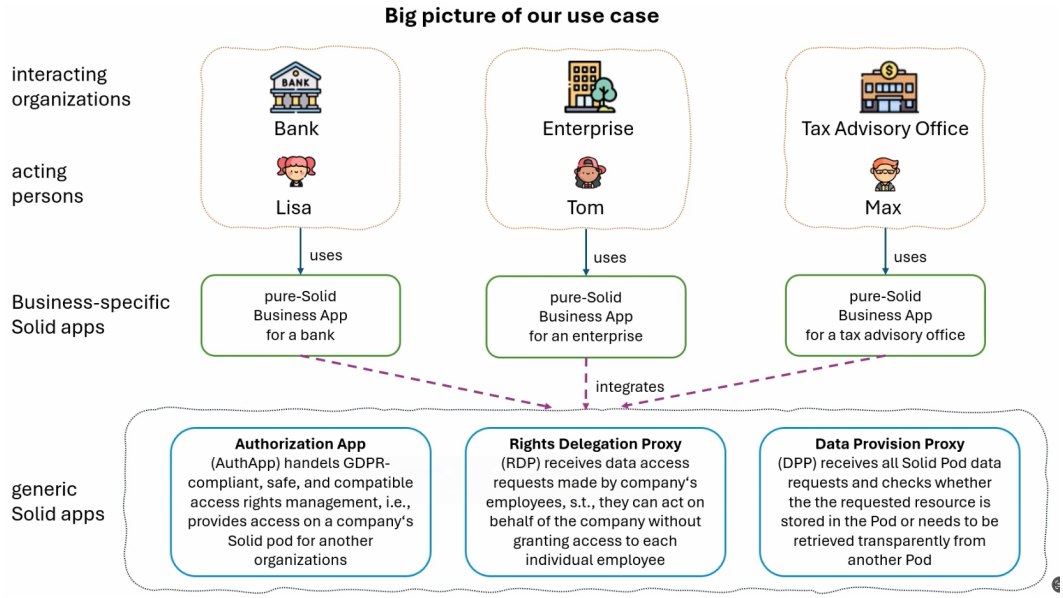


Abbildung 2.10: Kontextdiagramm mit den beteiligten Unternehmen, den handelnden Personen im Auftrag des Unternehmens und den entwickelten Anwendungen

Zugehörige Artefakte.

- Öffentliche verfügbare Sourcen der AuthApp, des Rights Delegation Proxy und des Data Provisioning Proxy[21,22]
- Öffentlich verfügbarer Screencast des Anwendungsszenario[23].

Erfüllung der Zielsetzung. Die Ziele des Arbeitspakets wurden vollständig erfüllt. Ein finaler nutz- und vorzeigbarer Demonstrator als prototypische Umsetzung des Anwendungsfalls wurde realisiert.

2.5.2 AP 5.2 Evaluierung der Solid-Architekturkonzepte und des Demonstrators an dem Anwendungsfall und Prüfung der Übertragbarkeit

Zielsetzung des Arbeitspakets. Im Rahmen des Arbeitspakets 5.2 sollte die Solid-Archi-tektur in Verbindung mit dem entwickelten Demonstrator hinsichtlich ihrer technischen und rechtlichen Eignung für die im Arbeitspaket 1.1 formulierten Anforderungen evaluiert werden.

Durchgeführte Arbeiten und Ergebnisse. Durch die prototypische Umsetzung konnten zentrale Anforderungen aus AP 1.1 wie die Wahrung der Datenautonomie, das Zugriffsrechtemanagement auf Datenebene sowie Benachrichtigungen bei Datenweitergabe systemseitig umgesetzt und demonstriert werden. Folgende Liste spiegelt das Ergebnis des Abgleichs der in AP 1.1 identifizierten Rahmenbedingungen und Anforderungen mit dem umgesetzten Demonstrator wider:

- Zwischen Unternehmer und Bank besteht ein anzubahnendes schuldrechtliches Vertragsverhältnis. Sich anbahnende Vertragsverhältnisse werden durch explizite Datenfreigaben in der AuthApp technisch unterstützt. Der Unternehmer kann via AuthApp gezielt steuern, welche Daten auf Anfrage der Bank offengelegt werden.
- Zwischen der Bank und dem Steuerberater besteht keine direkte Vertragsbeziehung. Es besteht im Demonstrator keine direkte Verbindung zwischen Bank und Steuerberaterbüro. Die Datenweitergabe erfolgt ausschließlich über den Unternehmer als Vermittler mittels DPP. Das Vertragsverhältnis zwischen KMU und Steuerberaterbüro ist für die Bank dadurch nicht erkennbar und bleibt geschützt.
- Der Steuerberater steht in einem berufsrechtlich geregelten Mandatsverhältnis mit dem Unternehmer, das zivil- und datenschutzrechtlich als besonders schutzwürdig einzustufen ist. Dieses Schutzverhältnis wird durch eine isolierte Datenbereitstellung via DPP und Rechtevergabe über den RDP umgesetzt. Der Steuerberater agiert als eigenständig Verantwortlicher und gibt nur solche Daten frei, die zur Einsicht bestimmt sind. Die Datenhoheit verbleibt beim Steuerberater (bei von ihm bereitgestellten Daten) und jede Weitergabe erfolgt nur auf Grundlage klarer Autorisierung über der AuthApp und dem RDP.

[21] `https://github.com/mandat-project/hackathon-demo`
[22] `https://github.com/DATEV-Research`
[23] `https://purl.archive.org/mandatb2b/JWE2024`

- Das Mandatsverhältnis unterliegt einem hohen Schutzniveau für sämtliche im Rahmen des Mandats verarbeiteten personenbezogenen und mandatsbezogenen Daten. Die Datenhoheit verbleibt beim Steuerberater, der über dedizierte Zugriffsrechte im Solid-Pod kontrolliert, welche Daten freigegeben werden. Protokollierungsfunktionen in der Infrastruktur (DPP und RDP) unterstützen die Dokumentationspflichten. Der DPP sorgt zusätzlich dafür, dass Datenzugriffe revisionssicher nachvollziehbar sind.
- Für die operative Umsetzung des Anwendungsfalls ist eine klar definierte Trennung von Innen- und Außenverhältnis erforderlich. Der RDP ermöglicht eine feingranulare Modellierung von Innen- und Außenverhältnissen der handelnden Personen und der Unternehmen.
- Der Steuerberater ist in den Kreditvergabeprozess einzubinden. Daten vom Steuerberater dürfen ausschließlich lesend verwendet und nur auf Grundlage expliziter Autorisierung weitergegeben werden. Geschäftsberichte vom KMU werden vom Steuerberater im eigenen Pod des Steuerberaterbüros schreibeschützt bereitgestellt. Über den DPP des KMU kann die Bank ausschließlich lesend auf die Daten im Pod des Steuerberaterbüros zugreifen.
- Dem Steuerberater muss eine vollständige Sichtbarkeit darüber ermöglicht werden, welche durch ihn bereitgestellten Daten verwendet und an Dritte übermittelt werden. Die AuthApp bietet eine Übersicht über alle aktiven, abgelehnten und widerrufenen Zugriffe. Zusätzlich protokolliert der DPP jede tatsächliche Datenabfrage, sodass ein vollständiger Audit-Trail zur Verfügung steht.
- Der Unternehmer verfügt über autarke Zugriffsrechte auf seine Datenbestände. Die Solid Architektur ermöglicht für alle beteiligten Unternehmen eine autonome Haltung ihrer eigenen Daten. Gewährung und Entzug von Datenfreigaben an externe Dritte können feingranular über die AuthApp durchgeführt werden.

Weiterhin wurde zusammen mit DATEV-Fachexperten der Nutzen des Ansatzes entlang realer Geschäftsszenarien bewertet. Bereits der Bereich Kanzleiprozessmanagement identifizierte dabei zusätzliche Potenziale für eine effizientere Gestaltung von Geschäftsvorgängen, wie in folgenden Anwendungsfällen:

- Mandatsübernahmeprozesse im steuerberatenden Umfeld,
- Zusammenarbeit mit Wirtschaftsprüfern bei der gezielten Freigabe prüfungsrelevanter Daten,
- Zusammenarbeit mit Notaren und Rechtsanwälten, etwa im Kontext von Unternehmensgründungen oder -übernahmen.

Die entwickelten und am Demonstrator realisierten Konzepte adressieren wiederkehrende Herausforderungen, die sich auch auf andere Kontexte übertragen lassen – beispielsweise im Umgang mit regulatorischen Anforderungen wie dem Lieferkettengesetz: Hier gilt es, firmensensible Informationen (z.B. Zulieferer) zu schützen, ohne die Nachweispflicht hinsichtlich verwendeter Materialien zu verletzen. Die im Projekt erarbeiteten Lösungen bieten hierfür einen konzeptionellen Ordnungsrahmen.

Das eingeholte Feedback von fachlichen Experten war durchweg positiv, sowohl hinsichtlich der rechtlichen und vertraglichen Abbildbarkeit der Anforderungen als auch

in Bezug auf die Wiederverwendbarkeit der Konzepte in anderen Geschäftskontexten. Gleichzeitig wurde auf potenzielle Herausforderungen hingewiesen: Der organisatorische Aufwand zur Integration der entwickelten Konzepte in bestehende IT-Infrastrukturen und Softwarearchitekturen wurde als potenzielle Hürde benannt. Dies verdeutlicht die Notwendigkeit einer anschlussfähigen und pragmatischen Implementierungsstrategie für die Weiterentwicklung im Unternehmenskontext.

Insgesamt konnte nicht nur der Nutzen, sondern auch dessen Übertragbarkeit auf eine Vielzahl weiterer Anwendungsfälle bestätigt werden. Die Projektergebnisse stehen damit auf einer tragfähigen konzeptionellen Basis für eine zukünftige Verwertung in Forschung und Praxis.

Zugehöriges Ergebnisdokument. Die Ergebnisse dieser Evaluation sind in der folgenden wissenschaftlichen Publikation dokumentiert:

- Andreas Both, Thorsten Kastner, Dustin Yeboah, Christoph Braun, Daniel Schraudner, Sebastian Schmid, Tobias Käfer und Andreas Harth. „Foundational Components for B2B Data Sharing Using the Solid Protocol“. In: Journal of Web Engineering. 2025.(akzeptiert)[7]

2.6 AP 6: Rechte- und Datenmanagement

Im Rahmen von Arbeitspaket 6 wurde ein umfassendes Konzept für das Rechte- und Datenmanagement entwickelt, mit dem Ziel, einen datenschutzkonformen, sicheren und nachvollziehbaren Umgang mit sensiblen Daten im Projekt sicherzustellen. Hierzu wurden zunächst Anforderungen aus relevanten Datenschutzinitiativen systematisch erfasst, bewertet und auf ihre Anwendbarkeit im Projektkontext geprüft. Die Ergebnisse flossen in ein technisches und organisatorisches Maßnahmenkonzept ein, das insbesondere die Regelung des Datenzugriffs im Innen- und Außenverhältnis sowie die sichere Weitergabe über Datenteilungsketten berücksichtigt.

Im weiteren Projektverlauf wurde das Rechte- und Datenmanagement kontinuierlich fortgeschrieben, wobei neue Erkenntnisse, regulatorische Anforderungen und technische Entwicklungen berücksichtigt wurden. Ein besonderes Augenmerk lag auf der dokumentierten Umsetzung datenschutzrelevanter Anforderungen und der Anpassung der Systemarchitektur, um langfristige Nachvollziehbarkeit und Rechtssicherheit zu gewährleisten.

2.6.1 AP 6.1 Erhebung von Anforderungen für das Rechte- und Datenmanagement

Zielsetzung des Arbeitspakets. Das Arbeitspaket AP 6.1 bildete die Grundlage für die Entwicklung eines rechtssicheren und datenschutzkonformen Rechte- und Datenmanagements im Projektkontext. Ziel des Arbeitspakets war die Ableitung, Bewertung und strukturelle Integration von Anforderungen aus relevanten Datenschutzinitiativen (DSGVO, Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz (TTDDG), bereichsspezifischen Vorschriften), gesetzlichen Verschwiegenheitspflichten (§203 StGB) sowie von Prinzipien

des Forschungsdatenmanagements nach FAIR (Findable, Accessible, Interoperable, Reusable).

Durchgeführte Arbeiten und Ergebnisse. Ein Anforderungskatalog wurde erstellt, der zentrale rechtliche und technische Rahmenbedingungen systematisch erfasst. Dieser wurde mit den bestehenden Projektkonzepten abgeglichen und diente als Grundlage für die Anpassung von Rollenmodellen, Datenflüssen und Servicearchitekturen. Parallel wurde ein strukturierter Ansatz zur fortlaufenden Evaluation und Dokumentation der Anforderungen in Form eines Journals erarbeitet.

In enger Abstimmung mit Fachexperten der DATEV aus den Bereichen Datenschutz, IT-Architektur und Steuerberatungspraxis wurden konkrete Architekturanforderungen, Leitplanken und Eckpfeiler für das Rechte- und Datenmanagement erarbeitet. Dabei flossen sowohl regulatorische Vorgaben als auch die praktischen Anforderungen realer B2B-Szenarien wie im untersuchten Kreditvergabeszenario als exemplarisches Beispiel für Anbahnung, Durchführung und Beendigung einer Partnerschaft in die Konzeption ein. Ein zentrales Resultat war die Ausarbeitung eines Metamodells, das vier grundlegende Teilnehmertypen im DATEV Ökosystem unterscheidet (Kanzlei, Unternehmen, Partner, Privatperson) und deren Rollen sowie Rechte im Ökosystem modelliert. Die Teilnehmertypen spiegeln sich auch in den im Arbeitspaket 1 identifizierten Teilnehmern wider (Steuerkanzlei, KMU, Bank) wodurch sich eine enge Verzahnung zwischen Metamodell und Anwendungsszenario ergibt. Die Rolle eines Identitätsankers wurde im Projekt durch Solid-konforme Mechanismen abgebildet. In Kombination mit ergänzenden Solid-Komponenten, wie der entwickelten Authorization-App, wird so eine flexible und sichere Zugriffssteuerung realisiert ohne auf eine proprietäre Kontostruktur angewiesen zu sein.

Zur Veranschaulichung wurden praxisnahe Szenarien erarbeitet, in denen das Zusammenspiel von Teilnehmern, Identitäten und handelnden Personen analysiert und mit dem Metamodell gespiegelt wurde. Daraus ergaben sich u.a. folgende konzeptionelle Festlegungen:

- Geschäftsbeziehungen erfolgen zwischen zwei eigenständigen Teilnehmern (bspw. Kanzlei und Unternehmen), wobei jeder Teilnehmer seine eigene Kundenstruktur verwaltet. Datentreuhänder können in solchen Beziehungen eine begleitende und unterstützende Rolle einnehmen, etwa durch die Bereitstellung sicherer Infrastrukturen und die Wahrung datenschutzrechtlicher Vorgaben. Diese würde sowohl den technischen Betrieb einer Plattform zur Datenfreigabe und -verarbeitung als auch die aktive Bereitstellung von Leistungen im Rahmen der jeweiligen Geschäftsbeziehung umfassen. Der Datentreuhänder fungiert dabei als eigenständiger, vertrauenswürdiger Teilnehmer, der insbesondere für die Einhaltung datenschutzrechtlicher und organisatorischer Anforderungen verantwortlich ist. DATEV würde hier in einer Doppelrolle als Plattformbetreiber und Leistungsgeber agieren, jeweils als eigenständiger Teilnehmer.
- Die Organisationsstruktur eines Teilnehmers ist flexibel gestaltbar und bildet die Basis für die Zuweisung von Rollen, Aufträgen und Mandanten. Anwendungen müssen diese Strukturen in ihrem Ablauf berücksichtigen.

- Ein durchgängiges Rechtemanagement wurde spezifiziert, das durch differenzierte Zugriffsrechte die Datensicherheit erhöht und Risiken wie unautorisierte Zugriffe oder Datenmanipulation minimiert.
- Für föderierte Ökosysteme wurde die Möglichkeit zur Föderation von Identitäten und Berechtigungen berücksichtigt. Dabei kann ein Teilnehmer Rollen und Rechte von externen Identitäten abbilden (Federation of Authorization). Dies schafft die Grundlage für standardisierte, interoperable Authentifizierungs- und Autorisierungsverfahren.

Hinsichtlich des Zugriffs auf Daten und Services wurde ein Scope-basiertes Konzept verfolgt. Scopes im Kontext Zugriffssteuerung definieren den Bereich (Daten, Funktionen, Services), auf den ein Benutzer oder eine Anwendung Zugriff erhalten soll. Öffentlich deklarierte Scopes können beispielsweise ohne gesonderte Zustimmung verwendet werden, während andere einer expliziten Freigabe bedürfen.

Abschließend wurde eine erste Dokumentation von technisch-organisatorischen Maßnahmen (TOMs) erstellt, welche zentrale Schutzmaßnahmen gemäß DSGVO (Art. 32) umfasst, u. a. Zugriffskontrollen, Protokollierung, Datenminimierung und organisatorische Trennung sensibler Daten. Diese Maßnahmen spiegeln sich konkret in der Umsetzung der im Projekt entwickelten Konzepte und Komponenten wider, insbesondere in den Arbeitspaketen AP 2, AP 3 und AP 4: Der Rights Delegation Proxy übernimmt unter anderem rollenbasierte Zugriffskontrollen und Rechtevergabe; der Data Provision Proxy (DPP) unterstützt die kontrollierte Weitergabe und Protokollierung von Datenflüssen; und die Authorization App ermöglicht eine gezielte Datenfreigabe durch die betroffenen Personen selbst. Darüber hinaus tragen die Grundprinzipien der verwendeten Solid-Architektur, wie etwa die dateninhaberzentrierte Zugriffskontrolle auf Pod-Ebene, wesentlich zur Umsetzung der TOMs bei.

2.6.2 AP 6.2 Fortschreibung des Rechte- und Datenmanagements

Zielsetzung des Arbeitspakets. Ziel des Arbeitspakets war die Entwicklung von Konzepten zur Einhaltung der identifizierten Anforderungen aus AP 1.2 sowie zum Monitoren und Rückführen von weiteren Anforderungen aus ausgewählten Datenschutzinitiativen in AP 1.2 entlang des Projektverlaufs.

Durchgeführte Arbeiten und Ergebnisse. Im Arbeitspaket AP 6.2 wurde ein kontinuierlicher Evaluationsprozess etabliert, der datenschutzrelevante Anforderungen aus Initiativen wie der DSGVO, dem TTDDG sowie projektspezifischen Rahmenbedingungen fortlaufend analysiert, bewertet und dokumentiert. Dabei lag der Fokus auf den abgeleiteten Anforderungen für die Arbeitspakete AP 2-5 aus AP 6.1. In enger Zusammenarbeit mit DATEV-Fachexperten (e.g. aus den Bereichen Rechnungswesen und Vertragswesen) und den Forschungspartnern von KIT und FAU wurden hierfür in gemeinsamen Workshops Lösungsansätze regelmäßig überprüft und architekturprägende Anforderungen identifiziert und adressiert. In wiederkehrenden, gemeinsamen Vor-Ort Hackathons (siehe AP 7) wurden unter anderem diese auf ihre technische Umsetzbarkeit analysiert. Die architek-

tonischen Konzepte wurden dabei iterativ angepasst, um die Einhaltung der rechtlichen und datenschutzbezogenen Vorgaben zu gewährleisten.

Beispielhafte Anforderungen, welche Auswirkungen auf die gesamte Architektur von MANDAT hatten, sind:

- Das Mandatsverhältnis zwischen Steuerberater und Mandant unterliegt einem besonderen Schutzbedarf, Daten und Informationen über ein Mandatsverhältnis sind streng vertraulich. Eine Einsicht durch Dritte, insbesondere Banken, ist auszuschließen.
- Aufgrund gesetzlicher Aufbewahrungspflichten verbleiben Daten sowohl beim Steuerberater als auch beim Unternehmen. Eine potenzielle Vermeidung redundanter Datenhaltung zur Erhöhung der Wartbarkeit wurde diskutiert.
- Um Haftungsrisiken zu minimieren, werden vom Steuerberater erstellte Daten nicht direkt an Dritte weitergegeben. Die Übergabe erfolgt stattdessen durch den Mandanten selbst.

Die technischen Anforderungen, insbesondere zu Anonymisierung, Zugriffsbeschränkung und Datenverantwortlichkeiten, wurden dokumentiert und in die architektonischen Entwürfe sowie in das Rechte- und Datenmanagement integriert. Die Ergebnisse wurden zudem systematisch in AP 1.2 rückgespiegelt. Im Hinblick auf das Forschungsdatenmanagement wurden eingesetzte Technologien im Kontext der FAIR-Prinzipien bewertet.

2.7 AP 7: Projektmanagement und Dissemination

Zielsetzung des Arbeitspakets. Im Rahmen des Arbeitspakets 7 wurde festgelegt, wie Kommunikation und Projektkoordination in MANDAT durchzuführen sind, und wie durch Treffen und Austausch alle Partner eingebunden werden. Hierdurch sollte sichergestellt werden, dass einerseits alle Aufgaben der Partner fertiggestellt und bearbeitet werden und andererseits auftretende Probleme frühzeitig erkannt und behoben werden können. Als Konsortialführer übernahm die Friedrich-Alexander-Universität Erlangen-Nürnberg das Projektmanagement von MANDAT.

Durchgeführte Arbeiten und Ergebnisse. Während der gesamten Projektlaufzeit von MANDAT war eine Koordination des Projekts und seiner Partner notwendig, um die Zusammenarbeit zwischen den einzelnen Partnern zu fördern und zu lenken. In diesem Rahmen wurde vereinbart, mindestens halbjährlich ein Projekttreffen in Präsenz abzuhalten. Dabei wechselten sich die Veranstaltungsorte ab, damit jeder Projektpartner einmal Gastgeber eines Treffens war. Vor den Treffen wurde gemeinschaftlich eine Agenda ausgearbeitet, welche einen Überblick über die zu bearbeitenden Themen lieferte.

Sinn und Zweck dieser Projekttreffen war einerseits das Teilen und gegenseitige Vorstellen von Ergebnissen und andererseits das Klären offener Fragen sowie das Aufdecken von Abstimmungsbedarf. Als zeitlicher Rahmen wurde hierfür immer eine zweitägige Veranstaltung gewählt: ein Tag wurde der Planung, Koordination und Reflexion des Projektverlaufs gewidmet, der andere diente der Bündelung der Arbeitskräfte im Rahmen eines gemeinsamen Arbeitseinsatzes.

Während der Treffen wurde der weitere Arbeitsverlauf der einzelnen Partner geplant und festgelegt, wobei die entsprechenden Punkte im nachfolgenden Projekttreffen erneut aufgegriffen wurden. Besonderer Wert wurde hierbei auf den Abgleich zwischen MANDAT Arbeitsplan laut Antrag, Zeitplanung und präsentierten Inhalten gelegt. Entsprechend wurde auch die Erreichung der Meilensteine abgeglichen.

Insgesamt wurde das Projekt von zweiwöchentlich stattfindenden Telefonkonferenzen als Jour fixe durchgängig begleitet. Die Teilnehmenden konnten hier ihre aktuellen Arbeiten diskutieren und anliegende Themen ansprechen. In diesem Rahmen wurden auch gemeinschaftliche Aktionen koordiniert, etwa bevorstehende Veröffentlichungen, anstehende Veranstaltungen oder die kurzfristige Planung von gemeinsamen Arbeitstreffen. Die Treffen folgten einem geordneten und zuvor festgelegten Ablauf: Eine editierbare Agenda wurde im Vorfeld über Filesharing-Software den Teilnehmenden zur Verfügung gestellt, um anliegende Themen notieren zu können. Die Konferenzen wurden von einem der Anwesenden moderiert, welcher auch als Schriftführer zum Protokollieren fungierte und die Ergebnisse stichpunktartig dokumentierte. Je nach Ergebnis wurden kleinere Aufgabenpakete verfasst. In nachfolgenden Jour fixe wurde der Erfüllungsgrad der Aufgaben jeweils abgeglichen.

Insgesamt fanden mehrtägige Statustreffen zu folgenden Terminen in Übereinstimmung mit den entsprechenden Meilensteinen statt:

- Nürnberg, Oktober 2022
- Karlsruhe, Juni 2023
- Nürnberg, März 2024
- Nürnberg, November 2024

Zusätzlich zu den Planungs- und Abstimmungstreffen wurde auch die Möglichkeit geschaffen, arbeitsintensive Hackathons zu ausgewählten Themen abzuhalten und dadurch auch die Zusammenarbeit im Projekt gezielt zu stärken. In den Hackathons konnte der Austausch und die Zusammenarbeit zu offenen Fragen des Technologieverständnisses und der Anwendungsfälle auf direkter Ebene intensiv gefördert werden. Teilweise fanden diese Treffen mit virtueller Teilnahme statt. Hackathons wurden an folgenden Terminen durchgeführt:

- Nürnberg, Oktober 2022
- Berlin, März 2023
- Nürnberg, Oktober 2023
- Nürnberg, Januar 2024
- Nürnberg, Juni 2024
- Nürnberg, August 2024

Der Projektstart von MANDAT erfolgte im Januar 2022, der Projektabschluss nach 36 Monaten zum Dezember 2024. Der ursprüngliche Zeitplan ergab sich hierbei aus der Planung und Abfolge der Arbeitspakete. Zur Außendarstellung und Dissemination von MANDAT wurden, wie in AP 7 geplant, Fachkonferenzen und -veranstaltungen für potenzielle Anwender identifiziert und als Plattformen genutzt. Im Rahmen von MANDAT entstanden somit 14 wissenschaftliche Veröffentlichungen, welche unter anderem auf der *Extended Semantic Web Conference*, der *International World Wide Web Conference*, dem

Solid Symposium, der *International Conference on Semantic Systems* sowie der *International Conference on Web Engineering* präsentiert wurden.

Neben Auftritten und Präsentationen im öffentlichen Rahmen nutzten die einzelnen Partner ebenfalls Gelegenheiten, die Projektziele und -methoden von MANDAT in internen Veranstaltungen vorzustellen, bspw. die DATEV auf sogenannten Inhouse-Messen.

KAPITEL 3

Wichtigste Positionen des zahlenmäßigen Verwendungsnachweises

3.1 Friedrich-Alexander-Universität Erlangen-Nürnberg

	Bewilligung gesamt	Ausgaben gesamt	Differenz
0812 WiMi	209.899,08 €	218.388,74 €	-8.489,66 €
0822 HiWi	10.754,52 €	5.301,40 €	5.453,12 €
0846 Reisekosten	7.522,00 €	8.173,44 €	-651,44 €
Summe	228.175,60 €	231.863,58 €	-3.687,98 €
Projektpauschale	45.635,12 €		
Bundesanteil	273.810,72 €		

Tabelle 3.1: Wichtigste Positionen des zahlenmäßigen Verwendungsnachweises der FAU

Personalkosten Die FAU beschäftigte während der Projektlaufzeit zwei wissenschaftliche Mitarbeiter, wobei beide Stellen durchgehend von Projektbeginn bis jeweils zum Projektende besetzt wurden. Über die Projektlaufzeit hinweg beschäftigte die FAU eine wissenschaftliche Hilfskraft zur Unterstützung.

Reisekosten Die Wissenschaftler der FAU nahmen an verschiedenen, internationalen Konferenzen teil, um die Ergebnisse ihrer Arbeit vor Fachpublikum im wissenschaftlichen Rahmen zu präsentieren. Weiterhin wurden über die Projektlaufzeit hinweg Statusmeetings, Meilensteinmeetings und Hackathons bei den einzelnen Projektpartnern veranstaltet und besucht.

3.2 Karlsruher Institut für Technologie (KIT)

	gekürzte Bewilligung	Ausgaben gesamt	Differenz
0812 WiMi	128.007,67 €	119.432,74 €	8.574,93 €
0822 HiWi	17.316,31 €	19.091,65 €	-1.775,34 €
0843 SAV	1.111,42 €	1.622,67 €	-511,25 €
0846 Reisekosten	9.008,05 €	9.426,89 €	-418,84 €
Summe	155.443,45 €	149.573,95 €	5.869,50 €
Projektpauschale		29.914,79 €	
Bundesanteil		179.488,74 €	

Anmerkung: SAV → Sonstige Allgemeine Verwaltungsausgaben → Open-Access-Publikationskosten.

Tabelle 3.2: Wichtigste Positionen des zahlenmäßigen Verwendungsnachweises des KIT

Personalkosten Das KIT beschäftigte während der Projektlaufzeit zwei wissenschaftliche Mitarbeiter. Zu Projektbeginn war der Mitarbeiter, der an den Themen von MANDAT forschte grundfinanziert, daher wurden vom Projektträger anteilig die Mittel gekürzt. Über die Projektlaufzeit hinweg beschäftigte das KIT mehrere wissenschaftliche Hilfskräfte zur Unterstützung.

Reisekosten Die Wissenschaftler des KIT nahmen an führenden internationalen Konferenzen wie der World Wide Web Conference, ESWC, und SEMANTiCS sowie dem Solid Symposium teil, um die Ergebnisse ihrer Arbeit vor Fachpublikum im wissenschaftlichen Rahmen zu präsentieren. Weiterhin wurden über die Projektlaufzeit hinweg Statusmeetings, Meilensteinmeetings und Hackathons bei den einzelnen Projektpartnern veranstaltet und besucht.

3.3 DATEV eG

	Bewilligung gesamt	Ausgaben gesamt	Differenz
0837 Personal	530.112,10 €	485.192,05 €	44.920,05 €
0838 Reisekosten	3157,00 €	4429,43 €	-1.272,43 €
Summe	533.269,10 €	489.621,48 €	43.647,62 €
Bundesanteil	195.848,59 €		

Tabelle 3.3: Wichtigste Positionen des zahlenmäßigen Verwendungsnachweises der DATEV eG

Personalkosten Die DATEV eG beschäftigte während der Projektlaufzeit hauptsächlich 2 Mitarbeiter. Während der Projektlaufzeit wurden temporär weitere Mitarbeiter anforderungsbezogen hinzugezogen.

Reisekosten Die Mitarbeiter nahmen an führenden internationalen Konferenzen wie der ESWC, SEMANTiCS sowie dem Solid Symposium teil, um sowohl die Ergebnisse ihrer Arbeit vor Fachpublikum zu präsentieren als auch zur inhaltlichen Vernetzung mit Fachexperten.

KAPITEL 4

Notwendigkeit und Angemessenheit der geleisteten Arbeit

Die durchgeführten Forschungsarbeiten im MANDAT-Projekt sowie die dafür aufgewandten Ressourcen waren notwendig und angemessen, da sie der im Projektantrag formulierten Planung entsprachen und alle wesentlichen im Arbeitsplan formulierten Aufgaben erfolgreich bearbeitet wurden. Darüber hinaus waren keine zusätzlichen Ressourcen notwendig, um das Vorhaben erfolgreich durchzuführen.

KAPITEL 5

Verwertbarkeit der Ergebnisse

5.1 Wissenschaftlich-technische Erfolge

Im Rahmen von MANDAT adressierten wir den Austausch von sensiblen, unternehmensbezogenen Daten mittels dezentral organisierten treuhänderbasierten Datenökosystemen. Unternehmensdaten sollten portabel werden und datensouverän geteilt werden können, wie im Anwendungsfall von AP 1 gezeigt. Im Rahmen unserer Arbeiten, haben wir in den Schwerpunkten Identität, Verarbeitung von Daten und wiederverwendbarer, datendurchgängiger Anwendungen wissenschaftliche und technische Erfolge vorzuweisen. Hierzu setzen wir technisch auf offene Web-Standards, speziell auf das Solid-Protokoll, welches verschiedene, etablierte Web Standards bündelt. Solid ermöglicht somit unter anderem die eindeutige Authentifizierung von Nutzern im Web und die Autorisierung zur Manipulation von Datenressourcen. Solid zielt darauf ab, einfach zu integrieren zu sein, indem es leichtgewichtige Spezifikationen nutzt und eine dezentralisierte Architektur unterstützt.

Zur Verknüpfung der Identitäten von natürlichen und juristischen Personen haben wir ein System zur Delegation von Rechten entwickelt. Mit dem Konzept des Rights Delegation Proxy können wir einerseits das Verhältnis zwischen Mitarbeiter und Unternehmen beschreiben, etwa eingeräumte Vertretungsrechte, Zugehörigkeit zu Abteilungen und Verantwortungsbereiche im Unternehmen. Andererseits kann damit ein Mitarbeiter im Außenverhältnis für sein Unternehmen tätig sein, ohne dass ein Unternehmen Kontrolle über die gewährten Rechte aufgeben muss, noch dass die beauftragten Mitarbeiter ein Teilen ihrer Identität gegenüber Dritten in Kauf nehmen müssen. Sowohl die Definition des Innenverhältnisses als auch des Außenverhältnisses waren vorher auf technischer Ebene nur unzureichend beschrieben und spezifiziert.

Durch die semantisch interoperable Self-Sovereign Identity Architektur (SISSI) kommt eine allgemeingültige Architektur für selbstverwaltete und identitätsbasierte Zugangs-

kontrolle über Unternehmensgrenzen hinweg hinzu. Mit beiden Technologien schaffen wir einen vertrauenswürdigen Ansatz, welcher Solid-basierte Datentreuhändersysteme und Datenverarbeitung fit für den Einsatz im Unternehmensbereich macht.

Die Schaffung eines Demonstrators war für uns nicht nur die Möglichkeit, unsere Ergebnisse von einer konzeptionellen Stufe auf die der gezeigten Machbarkeit zu heben, sondern gleichzeitig ein Motivator Softwareartefakte zu schaffen, welche die Ergebnisse von MANDAT über die Projektdauer hinaus verfügbar machen. Hierbei haben wir insbesondere drei Artefakte, deren Einsatz eines datentreuhänderbasierten Systems für Unternehmen erleichtern kann: der Rights Delegation Proxy (RDP), der Data Provisioning Proxy (DPP), und die Authorization App (AuthApp). Während RDP und DPP in ihrer Funktion ähnlich sind und den geregelten Zugriff auf Daten ermöglichen, entweder direkt im eigenen Namen oder indirekt auf externe Datenquellen, schafft die AuthApp einen neuen Ansatz zur zweckgebundenen Freigabe von Daten. Mit unseren wiederverwendbaren Implementierung, die im Solid-Ökosystem für die Verwaltung von Datenanforderungen und die Überwachung von Datenfreigaben eines Solid Servers verwendet werden kann, benötigen wir keine zusätzlichen Komponenten, denen vertraut werden muss, da die Anwendung vollständig auf Nutzerseite läuft.

5.2 Voraussichtlicher Nutzen und Verwertungsplan

Die im Projekt MANDAT erzielten Forschungsergebnisse wurden gezielt der wissenschaftlichen und fachlichen Öffentlichkeit zugänglich gemacht. Veröffentlichungen auf renommierten, vorzugsweise Open-Access-Konferenzen (siehe Kapitel 7) gewährleisten die nachhaltige Sichtbarkeit und Nachnutzbarkeit der Resultate. Ein erheblicher Teil der im Projekt entwickelten Software wurde zudem als Open-Source bereitgestellt[1]. Diese offene Lizenzierung fördert die Weiterentwicklung und Integration der Lösungen durch externe Akteure aus Wissenschaft und Wirtschaft. Die beteiligten Forschungseinrichtungen verfolgen dabei grundsätzlich keine direkte wirtschaftliche Verwertung der Ergebnisse. Stattdessen wurde durch die Maßnahmen in Arbeitspaket 7 sichergestellt, dass die Projektergebnisse aktiv verbreitet, kommuniziert und für Folgeprojekte aufbereitet wurden.

Ein besonderer Nutzen ergibt sich in der Verwendbarkeit der Projektergebnisse als Grundlage für zukünftige Forschungsprojekte der beteiligten Partnerinstitutionen. Die erzielten Ergebnisse stärken somit die wissenschaftliche Kompetenz und das thematische Profil der Partner und erhöhen ihre Sichtbarkeit in relevanten Forschungsgemeinschaften.

Darüber hinaus fließen die im Projekt gewonnenen Erkenntnisse unmittelbar in die akademische Lehre der beteiligten Hochschulen ein. Die Themen werden auch nach Projektende, z. B. in Lehrveranstaltungen, Bachelor- und Masterarbeiten, weiterhin bearbeitet.

Durch die Ausrichtung an einem verallgemeinerbaren und praxisrelevanten Anwendungsszenario wird gewährleistet, dass die Projektergebnisse über den Forschungskontext hinaus auch in der Wirtschaft Anwendung finden können. Ein zentraler Aspekt zur Sicherstellung der nachhaltigen Verwertung der Projektergebnisse war bei DATEV der

[1] `https://github.com/mandat-project`

offene Austausch mit internen und externen Fachexperten. Die kontinuierliche Diskussion von Erkenntnissen förderte nicht nur den Wissenstransfer über den Projektzeitraum hinaus, sondern ermöglichte auch die frühzeitige Einbindung relevanter Praxisperspektiven.

Die prototypische Umsetzung in Form eines Demonstrators spielte und spielt weiterhin dabei eine zentrale Rolle. Sie ermöglicht es, die entwickelten Konzepte greifbar zu machen, im realitätsnahen Kontext zu evaluieren und so Rückmeldungen aus der Praxis zielgerichtet in die Weiterentwicklung einfließen zu lassen.

Ein besonderer Mehrwert ergibt sich aus der Integration des Solid-Ansatzes: Er schafft eine klare Trennung zwischen Datenhaltung, Authentifizierung und Applikationslogik durch den Einsatz offener, standardisierter Protokolle. Dies bietet Unternehmen eine hohe Gestaltungsfreiheit bei der Wahl ihrer Daten- und Identitätsanbieter und fördert gleichzeitig Interoperabilität sowie digitale Souveränität. Zudem steigert die Entkopplung die Effizienz in der Softwareentwicklung durch klare Schnittstellen und Wiederverwendbarkeit von Komponenten.

Diese Erkenntnisse fließen direkt in die Weiterentwicklung der cloud-basierten DATEV Geschäftsplattform ein. Ziel dieser Plattform ist es, einen zentralen digitalen Ort für die Vernetzung des steuerberatenden Berufsstands, des Mittelstands und weiterer Akteure zu schaffen. Sie bildet den technischen Rahmen für vertrauensvolle und wertschöpfende Zusammenarbeit, indem sie klare Regeln und Strukturen für Daten- und Serviceaustausch bereitstellt – entlang von Geschäftsprozessen, Produkten und Interaktionen.

Mit den im Projekt MANDAT entwickelten Verfahren kann DATEV künftig innerhalb eines offenen digitalen Ökosystems agieren, neue Kundengruppen erschließen und ihren Mitgliedern eine breitere Palette an Services einfacher zugänglich machen. Gleichzeitig unterstützt die Plattform datenbasierte Innovationen wie Datenmarktplätze und Datenteilungsnetzwerke – insbesondere im Kontext von Steuerberatern, Mandanten und deren Geschäftsumfeld.

Die im Projekt berücksichtigten FAIR-Prinzipien (Findable, Accessible, Interoperable, Reusable) wurden inzwischen als Leitlinien in die DATEV Cloud-Strategie übernommen. Sie fördern eine nachhaltige Dateninfrastruktur und stärken die Position von DATEV als vertrauenswürdiger Enabler im Bereich datengetriebener Geschäftsmodelle.

Insgesamt zeigen die Projektergebnisse großes Potenzial für Effizienzsteigerungen in datengetriebenen Geschäftsprozessen im Steuer- und KMU-Umfeld, sowohl durch technische Innovation als auch durch strukturelle Veränderungen im Datenmanagement.

Insgesamt tragen die im Projekt gewonnenen Erkenntnisse und entwickelten Konzepte dazu bei, den Datenmarktplatz, Datenteilungsnetzwerke und das entstehende datengetriebene Ökosystem rund um Steuerberater, Mandanten und deren Geschäftsumfeld entscheidend mitzugestalten und damit einen bedeutenden Beitrag zur digitalen Transformation des Mittelstands zu leisten.

KAPITEL 6

Relevante Ergebnisse Dritter

Während der Laufzeit von MANDAT wurden international weitere Projekte verfolgt, die sich vor allem dem unternehmensübergreifenden Datenaustausch widmen:

International Data Spaces (IDS)[1] sind ein in der Entwicklung befindlicher Standard, der einer Referenzarchitektur folgt, mit dem angepeilten Ziel eines sicheren Datenaustauschs über Unternehmensökosysteme hinweg, unter der Beibehaltung von Datensouveränität mittels sicherer und vertrauenswürdiger Data Spaces. Datensouveränität wird hierbei als eine bindende Regelung zum Umgang mit Daten eines Eigners definiert, etwa zur Verarbeitung, Verlinkung, Analyse oder Weitergabe an Dritte. Die jeweils vertraglich vereinbarte Datensouveränität soll durch geeignete technische Infrastruktur und Schnittstellen gewährleistet werden. Die Hauptkomponente, die den Austausch ermöglichen soll, ist der IDS-Konnektor, welcher für die Weiterleitung der Daten vom Datenanbieter an den Datenverbraucher zuständig ist. Der Konnektor soll vom Broker unterstützt werden, einem Vermittler, der Metadaten über die verfügbaren Datenprodukte im Datenraum empfängt, speichert und bereitstellt. Ein App Store soll ein weiterer Vermittler werden, der wiederverwendbare Datenanwendungen verwaltet und bereitstellt, die innerhalb des Konnektors eingesetzt werden könnten, um Datenverarbeitungsabläufe zu erleichtern.

GAIA-X[2] entwickelt hierbei ein Framework, in dessen Zentrum der IDS steht: hierbei sollen bestehende Cloud-Systeme als Dateninfrastrukturökosysteme föderiert und dezentral zusammenarbeiten können, wobei Konzepte wie Offenheit und Durchgängigkeit durch gegenseitigem Trust ermöglicht werden sollen. GAIA-X soll als Verknüpfung zwischen diesen angestrebten Lösungen auftreten und die Zusammenarbeit ermöglichen. Data Spaces definieren die Bereiche in welchen Partner anhand definierter Regeln in einem vertrauenswürdigen Umfeld ihre jeweiligen Daten teilen können (anh. der IDS Architektur).

[1] `https://internationaldataspaces.org/`
[2] `https://www.gaia-x.eu/`

IDS und GAIA-X verfolgen ähnliche Ziele wie MANDAT, jedoch stehen vor allem abstrakte Zielsetzungen zu Governance und Datendurchgängigkeit in Datenräumen im Vordergrund. Eine Rolle eines Datentreuhänders, wie im Rahmen eines Datentreuhandmodells angedacht, wird nur implizit definiert, so etwa beim IDS durch die Zugriffs- und Nutzungskontrolle. Die technische Umsetzung in GAIA-X und IDS folgte den zuvor gesetzten abstrakten Zielsetzungen, während die Dokumente der Standardisierung bisweilen losgelöst von technischen Umsetzungen erscheinen. In MANDAT fokussierten wir uns hingegen auf konzeptionell durchdachte und konkrete Implementierungsarbeiten rund um den tatsächlichen Datenaustausch, welcher auf der Solid-Erweiterungen etablierter und standardisierter Web-Protokolle basieren. Dabei ging die konzeptionelle Arbeit Hand in Hand mit der technischen Umsetzung. Dies ermöglichte uns, bei einem im Vergleich zu Initiativen wie GAIA-X und IDS geringen Projektumfang, schnell Methoden für das Datenteilen in treuhänderbasierten Datenökosystemen zu etablieren und in einem lauffähigen Demonstrator umzusetzen. Die Methoden aus MANDAT genügen obendrein den höchsten Anforderungen nach Datensouveränität und wurden teilweise sogar formal verifiziert. GAIA-X und IDS sind teilweise komplementär zu Solid, siehe z. B. Arbeiten aus dem MANDAT-Kontext wie [12], teilweise können Bausteine von GAIA-X und IDS einfach mit Solid implementiert werden, was ebenfalls in Arbeiten aus den Forschungsgruppen, die an MANDAT beteiligt sind gezeigt wurde [33]. Ebenfalls implementieren Komponenten aus MANDAT, wie die AuthApp [7], Aspekte eines sogenannten Clearing Houses aus der IDS-Governance und schaffen eine nachvollziehbare, kontrollierte und vertrauensbasierte Umgebung zum Datenaustausch. Während GAIA-X und IDS auf den Austausch zwischen den Identitäten ganzer Unternehmen, d. h. juristischer Personen, fokussiert sind (top-down), folgt MANDAT einem dem Ansatz, der von natürlichen Personen ausgeht und auf juristische Personen erweitert wurde (bottom-up). Dadurch können etwa Delegationen näher am deutschen Recht realisiert werden, wie bspw. dass natürliche Personen sowohl Unternehmen oder andere Personen vertreten können, was sich auch in der Flexibilität des Rights Delegation Proxy [39] aus MANDAT widerspiegelt.

KAPITEL 7

Erfolgte und geplante Veröffentlichungen

[6] Andreas Both, Thorsten Kastner, Dustin Yeboah, Christoph Braun, Daniel Schraudner, Sebastian Schmid, Tobias Käfer und Andreas Harth. „AuthApp - Portable, Reusable Solid App for GDPR-Compliant Access Granting“. In: *Web Engineering - 24th International Conference, ICWE 2024, Tampere, Finland, June 17-20, 2024, Proceedings*. Bd. 14629. Lecture Notes in Computer Science. Springer, 2024, S. 199–214. DOI: 10.1007/978-3-031-62362-2_14. URL: https://doi.org/10.1007/978-3-031-62362-2%5C_14.

[7] Andreas Both, Thorsten Kastner, Dustin Yeboah, Christoph Braun, Daniel Schraudner, Sebastian Schmid, Tobias Käfer und Andreas Harth. „Foundational Components for B2B Data Sharing Using the Solid Protocol (akzeptiert)“. In: *Journal of Web Engineering* (2025).

[8] Andreas Both, Dustin Yeboah, Thorsten Kastner, Daniel Schraudner, Sebastian Schmid, Christoph Braun, Andreas Harth und Tobias Käfer. „Towards Solid-based B2B Data Value Chains“. In: *21st Extended Semantic Web Conference (ESWC 2024)* (Hersonissos, Crete). Hrsg. von Albert Meroño Peñuela, Oscar Corcho, Paul Groth, Elena Simperl, Valentina Tamma, Andrea Giovanni Nuzzolese, Maria Poveda-Villalón, Marta Sabou, Valentina Presutti, Irene Celino, Artem Revenko, Joe Raad, Bruno Sartini und Pasquale Lisena. 26.–30. Mai 2024.

[9] Christoph Braun und Tobias Käfer. „Attribute-based Access Control on Solid Pods using Privacy-friendly Credentials“. In: *Proceedings of Poster and Demo Track and Workshop Track of the 18th International Conference on Semantic Systems co-located with 18th International Conference on Semantic Systems (SEMANTiCS 2022), Vienna, Austria, September 13th to 15th, 2022*. Hrsg. von Umutcan Simsek, David Chaves-Fraga, Tassilo Pellegrini und Sahar Vahdat. Bd. 3235. CEUR Workshop Proceedings. CEUR-WS.org, 2022. URL: https://ceur-ws.org/Vol-3235/paper1.pdf.

[12] Christoph Braun, Yanxiu Wuwang, Zhi Wang, Xuyang Hou und Tobias Kaefer. „Towards using the Solid Protocol for Data Transport in International Data Spaces (IDS)“. In: *Proceedings of the Third International Workshop on Semantics in Dataspaces (SDS 2025) co-located with the 22nd Extended Semantic Web Conference (ESWC 2025)*. to be published. 1. Juni 2025.

[13] Christoph H.-J. Braun, Ross Horne, Tobias Käfer und Sjouke Mauw. „SSI, from Specifications to Protocol? Formally Verify Security!“ In: *Proceedings of the ACM on Web Conference 2024, WWW 2024, Singapore, May 13-17, 2024*. Hrsg. von Tat-Seng Chua, Chong-Wah Ngo, Ravi Kumar, Hady W. Lauw und Roy Ka-Wei Lee. ACM, 2024, S. 1620–1631. DOI: 10.1145/3589334.3645426. URL: https://doi.org/10.1145/3589334.3645426.

[14] Christoph H.-J. Braun und Tobias Käfer. „Self-verifying Web Resource Representations Using Solid, RDF-Star and Signed URIs“. In: *The Semantic Web: ESWC 2022 Satellite Events - Hersonissos, Crete, Greece, May 29 - June 2, 2022, Proceedings*. Hrsg. von Paul Groth, Anisa Rula, Jodi Schneider, Ilaria Tiddi, Elena Simperl, Panos Alexopoulos, Rinke Hoekstra, Mehwish Alam, Anastasia Dimou und Minna Tamper. Bd. 13384. Lecture Notes in Computer Science. Springer, 2022, S. 138–142. DOI: 10.1007/978-3-031-11609-4_26. URL: https://doi.org/10.1007/978-3-031-11609-4%5C_26.

[15] Christoph H.-J. Braun, Vasil Papanchev und Tobias Käfer. „SISSI: An Architecture for Semantic Interoperable Self-Sovereign Identity-based Access Control on the Web“. In: *Proceedings of the ACM Web Conference 2023, WWW 2023, Austin, TX, USA, 30 April 2023 - 4 May 2023*. Hrsg. von Ying Ding, Jie Tang, Juan F. Sequeda, Lora Aroyo, Carlos Castillo und Geert-Jan Houben. ACM, 2023, S. 3011–3021. DOI: 10.1145/3543507.3583409. URL: https://doi.org/10.1145/3543507.3583409.

[27] Thorsten Kastner, Christoph Braun, Andreas Both, Dustin Yeboah, Sebastian Josef Schmid, Daniel Schraudner, Tobias Kaefer und Andreas Harth. „Data-Sovereign Enterprise Collaboration using the Solid Protocol“. In: *20th International Conference on Semantic Systems (SEMANTICS'24)* (Amsterdam). Hrsg. von Daniel Garijo, Anna Lisa Gentile, Anelia Kurteva, Andrea Mannocci, Francesco Osborne und Sahar Vahdati. CEUR-WS, 17.–19. Sep. 2024. DOI: 10.5445/IR/1000174700.

[28] Thorsten Kastner, Dustin Yeboah, Andreas Both, Sebastian Schmid, Daniel Schraudner, Christoph H.-J. Braun, Andreas Harth und Tobias Käfer. „Cornerstones of a Future Solid B2B Ecosystem: Authorization App and Rights Delegation Proxy“. In: *Proceedings of the Posters and Privacy Session of the Solid Symposium 2024, Leuven, Belgium, May 2-3, 2024*. Hrsg. von Beatriz Esteves, Jan Hofmann und Sebastian Schmid. Bd. 3947. CEUR Workshop Proceedings. CEUR-WS.org, 2024, S. 51–57. URL: https://ceur-ws.org/Vol-3947/short8.pdf.

[37] Sebastian Schmid, Michael Freund und Andreas Harth. „Adaptive Planning on the Web: Using LLMs and Affordances for Web Agents“. In: *Knowledge Graphs and Semantic Web*. Hrsg. von Sanju Tiwari, Boris Villazón-Terrazas, Fernando Ortiz-

Rodríguez und Soror Sahri. Cham: Springer Nature Switzerland, 2025, S. 93–108. ISBN: 978-3-031-81221-7.

[38] Sebastian Schmid und Andreas Harth. „Enabling Adaptation in Dynamic Manufacturing Environments with Decentralized Agent-Based Systems and Local Perception“. In: *Proceedings of the 39th ACM/SIGAPP Symposium on Applied Computing*. SAC '24. Avila, Spain: Association for Computing Machinery, 2024, S. 235–242. ISBN: 9798400702433. DOI: 10.1145/3605098.3635967. URL: https://doi.org/10.1145/3605098.3635967.

[39] Sebastian Schmid, Daniel Schraudner und Andreas Harth. „The Rights Delegation Proxy: An Approach for Delegations in the Solid Dataspace“. In: *Proceedings of the Second International Workshop on Semantics in Dataspaces (SDS 2024) co-located with the 21st Extended Semantic Web Conference (ESWC 2024)* (Hersonissos). 26. Mai 2024. URL: https://ceur-ws.org/Vol-3705/paper02.pdf.

[40] Daniel Schraudner, Sebastian Schmid, Christoph H.-J. Braun Braun und Andreas Harth. *Delegation of Access Rights to Web Resources between Agents (eingereicht)*.

[41] Daniel Schraudner, Sebastian Schmid und Andreas Harth. „Distributed Detection of Complex Events on Streams of Linked Data (akzeptiert)“. In: *Web Engineering: 25th International Conference (ICWE 2025)* (Delft, Netherlands). 2025.

Literatur

[1] Christopher Allen. *The Path to Self-Sovereign Identity*. 2016. URL: http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html.

[2] Ganesh Annan und Kim Hamilton Dufy. *Resource Integrity Proofs*. Rebooting Web Of Trust VII Design Workshop, Toronto. 2018. URL: https://nbviewer.jupyter.org/github/WebOfTrustInfo/rwot7/blob/master/final-documents/resource-integrity-proofs.pdf (besucht am 20. 11. 2020). Online.

[3] Jesús Arias-Fisteus, Norberto Fernández García, Luis Sánchez Fernández und Carlos Delgado Kloos. „Hashing and Canonicalizing Notation 3 Graphs“. In: *Journal of Computer and System Sciences* 76.7 (2010), S. 663–685.

[4] Man Ho Au, Willy Susilo und Yi Mu. „Constant-Size Dynamic k-TAA“. In: *Proc. of the 5th SCN*. 2006.

[5] Tim Berners-Lee, Roy Fielding und Larry Masinter. *Uniform Resource Identifier (URI): Generic Syntax*. Internet Standards Track document. https://www.ietf.org/rfc/rfc3986.txt. IETF, Jan. 2005.

[10] Christoph Braun und Tobias Käfer. „Verifying the Integrity of Hyperlinked Information Using Linked Data and Smart Contracts“. In: *Proceedings of the 15th International Conference on Semantic Systems (SEMANTiCS)*. Bd. 11702. Lecture Notes in Computer Science. Springer, 2019, S. 376–390.

[11] Christoph Braun und Tobias Käfer. „Verifying the Integrity of Information along a Supply Chain using Linked Data and Smart Contracts“. In: *Proceedings of the Posters and Demo Track at the 15th International Conference on Semantic Systems (SEMANTiCS)*. Bd. 2451. CEUR Workshop Proceedings. CEUR-WS.org, 2019.

[16] Buyle, Raf and Taelman, Ruben and Mostaert, Katrien and Joris, Geroen and Mannens, Erik and Verborgh, Ruben and Berners-Lee, Tim. „Streamlining Governmental Processes by Putting Citizens in Control of their Personal Data“. eng. In: *Electronic Governance and Open Society : Challenges in Eurasia*. Bd. 1135. St-Petersburg, Russia: Springer, 2020, 346–359. ISBN: 9783030392956. URL: http://doi.org/10.1007/978-3-030-39296-3_26.

[17] Jan Camenisch und Anna Lysyanskaya. „An Efficient System for Non-transferable Anonymous Credentials with Optional Anonymity Revocation“. In: *Proc. of EUROCRYPT 2001*. Bd. 2045. LNCS. Springer, 2001, S. 93–118.

[18] Sarven Capadisli. *„Web Access Control“*. Editor's Draft. W3C Solid Community Group, März 2022. URL: https://solid.github.io/web-access-control-spec/.

[19] Sarven Capadisli, Tim Berners-Lee, Ruben Verborgh und Kjetil Kjernsmo. *„Solid Protocol“*. Version 0.9.0. W3C Solid Community Group, Dez. 2021. URL: https://solidproject.org/TR/protocol.

[20] Jeremy J. Carroll. „Signing RDF Graphs“. In: *Proceedings of the 2nd International Semantic Web Conference (ISWC)*. Bd. 2870. Lecture Notes in Computer Science. Springer, 2003, S. 369–384.

[21] D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley und W. Polk. *„Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile“*. Internet Standards Track document. https://www.ietf.org/rfc/rfc5280.txt. IETF, Mai 2008.

[22] Richard Cyganiak, David Wood und Markus Lanthaler. *RDF 1.1 Concepts and Abstract Syntax*. W3C Recommendation. https://www.w3.org/TR/rdf11-concepts/. W3C, Feb. 2014.

[24] Yoshiaki Fukami, Takumi Shimizu und Hiroyasu Matsushima. „The Impact of Decentralized Identity Architecture on Data Exchange“. In: *2021 IEEE International Conference on Big Data (Big Data)*. 2021, S. 3461–3465. DOI: 10.1109/BigData52589.2021.9671674.

[25] Olaf Hartig, Pierre-Antoine Champin, Gregg Kellogg und Andy Seaborne. *RDF-star and SPARQL-star*. W3C Draft Community Group Report. https://w3c.github.io/rdf-star/cg-spec/editors_draft.html. W3C, Feb. 2022.

[26] Aidan Hogan. „Canonical Forms for Isomorphic and Equivalent RDF Graphs: Algorithms for Leaning and Labelling Blank Nodes“. In: *ACM Trans. Web* 11.4 (2017), 22:1–22:62. DOI: 10.1145/3068333.

[29] Tobias Kuhn, Christine Chichester, Michael Krauthammer, Núria Queralt-Rosinach, Ruben Verborgh, George Giannakopoulos, Axel-Cyrille Ngonga Ngomo, Raffaele Viglianti und Michel Dumontier. „Decentralized Provenance-aware Publishing with Nanopublications“. In: *PeerJ Comput. Sci.* 2 (2016), e78.

[30] Tobias Kuhn und Michel Dumontier. „Making Digital Artifacts on the Web Verifiable and Reliable“. In: *IEEE Trans. Knowl. Data Eng.* 27.9 (2015), S. 2390–2400.

[31] Tobias Kuhn und Michel Dumontier. „Trusty URIs: Verifiable, Immutable, and Permanent Digital Artifacts for Linked Data“. In: *Proceedings of the 11th European Semantic Web Conference (ESWC)*. Hrsg. von Valentina Presutti, Claudia d'Amato, Fabien Gandon, Mathieu d'Aquin, Steffen Staab und Anna Tordai. Bd. 8465. Lecture Notes in Computer Science. Springer, 2014, S. 395–410.

[32] Dave Longley. *RDF Dataset Canonicalization*. W3C Recommendation. W3C, 2024. URL: https://www.w3.org/TR/rdf-canon/.

[33] Sascha Meckler, Rene Dorsch, Daniel Henselmann und Andreas Harth. „The Web and Linked Data as a Solid Foundation for Dataspaces“. In: *Companion Proceedings of the ACM Web Conference 2023*. WWW '23 Companion. Austin, TX, USA: Association for Computing Machinery, 2023, S. 1440–1446. ISBN: 9781450394192. DOI: 10.1145/3543873.3587616. URL: https://doi.org/10.1145/3543873.3587616.

[34] David Pointcheval und Olivier Sanders. *Short Randomizable Signatures*. Cryptology ePrint Archive, Paper 2015/525. https://eprint.iacr.org/2015/525. 2015.

[35] Andrei Sambra, Henry Story und Tim Berners-Lee. *WebID 1.0 - Web Identity and Discovery*. W3C Editor's Draft. W3C, März 2014. URL: https://www.w3.org/2005/Incubator/webid/spec/identity/.

[36] Craig Sayers und Alan H. Karp. *Computing the Digest of an RDF Graph*. Techn. Ber. HP, 2004. URL: http://www.hpl.hp.com/techreports/2003/HPL-2003-235R1.pdf.

[42] Manu Sporny, Amy Guy, Markus Sabadello und Drummond Reed. *Decentralized Identifiers (DIDs)*. W3C Recommendation. W3C, Juli 2022. URL: https://www.w3.org/TR/did-core/.

[44] Andrew Sutton und Reza Samavi. „Integrity Proofs for RDF Graphs“. In: *Open Journal of Semantic Web (OJSW)* 6.1 (2019), S. 1–18.