Wie kann selbstsouveränes digitales Identitätsmanagement behördenübergreifend Prozesse verbessern?

Julia Podlipensky
Matrikelnummer: 765550

Bachelorprojekt Interactive Media Design
Wintersemester 2023/24

Erstreferent: Prof. Tsunemitsu Tanaka
Zweitreferent: Prof. Andrea Krajewski

h_da
HOCHSCHULE DARMSTADT
UNIVERSITY OF APPLIED SCIENCES

Inhalt

Vorausgehende Forschungsarbeit

In der vorausgehenden Forschungsarbeit wurde sich mit der Frage nach der digitalen Unsichtbarkeit beschäftigt, was diese bedeutet und wie man diese möglicherweise erreichen könnte. Im Verlauf der Recherche wurde jedoch das Ergebnis erreicht, dass der Grund für die Frage nach der digitalen Unsichtbarkeit eigentlich den Wunsch nach Selbstbestimmung in der digitalen Welt innehat. Es geht nicht primär darum sich zurückzuziehen und jeglichen Austausch von Informationen zu unterbinden - sozusagen die absolute digitale Unsichtbarkeit damit anzustreben – wobei dies schwer zu erreichen ist und dessen Folgen für die freie Lebensgestaltung alles andere als wünschenswert wären. Es geht vor allem aus der Perspektive der Selbstbestimmung darum, die Informationen mit demjenigen Gegenüber zu teilen, für den die Informationen zu einem gewissen Zweck bestimmt sind. Man tauscht beim Teilen von Informationen deren Kontrolle gegen die starke soziale Norm des Vertrauens und die Erwartungen, wie mit diesen Informationen umgegangen werden soll und was mit ihnen passiert. Diese starke soziale Norm sollte in unserer Gesellschaft erhalten und gefördert werden. Dafür müssen sich Gedanken gemacht werden, wie Formen der Selbstbestimmung in der digitalen Welt, speziell unserem digitalen Identitätsmanagement, gefördert werden können. Wie mit den Daten umgegangen werden soll, die es in der Zukunft über uns geben wird, welche Prozesse es dafür geben sollte und wie es letztendlich allen Akteuren dabei zugutekommen kann, stellt sich als übergreifende Leitfrage und Motivation für dieses Projekt.

SSI – ein vielversprechender Ansatz von selbstsouveräner Identität im Digitalen?

Die self sovereign identity/selbstsouveräne Identität (SSI) ist ein Ansatz und eine Bewegung, die es Menschen ermöglichen möchte, ihre Identität zu besitzen, selbstbestimmt zu verwalten und kontextabhängig zu teilen. Der Ansatz entsteht aus dem Wunsch als Nutzer nicht mehr auf große Identitätsprovider angewiesen zu sein und eine Entwicklung über zentralisierte oder föderierte Identitätsmanagement-Systeme hinweg einzuschlagen.

Status Quo

Die Entwicklung des digitalen Identitätsmanagements geht über mehrere Stufen hinweg (Strüker et al., 2021 ; Allen, 2016): Existierte anfangs noch ein zentralisiertes Modell, indem bspw. Administratoren Zugriffe zu Dienste einstellen und die Daten auf dem jeweiligen Konto verwalten, wurde als Reaktion auf dessen Nachteile ein nutzerorientiertes Modell entworfen. Dabei verwalten die Nutzer über Log-ins mit Benutzernamen, E-Mail-Adressen und Passwörtern die Zugänge zu den Diensten selbst. Nicht nur entstehen durch bspw. die Mehrfachanwendung von Passwörtern Sicherheitsrisiken. Auch die mangelnde Nutzerfreundlichkeit, dass schon einmal nachgewiesene Identitätsmerkmale für jeden Dienst nochmals einzeln eingetragen werden müssen, löst Frust aus. Die eingetragenen Identitätsmerkmale - man kann dabei im Digitalen auch von einer Zusammensetzung von Teilidentitäten sprechen – bleiben auch weiterhin beim jeweiligen Anbieter gespeichert und können dementsprechend zwischen verschiedenen Webdiensten weitergegeben werden. In der nächsten Entwicklungsstufe wurden föderierte Identitätsmodelle eingeführt, welche über eine zentrale Log-in Instanz Nutzern die Möglichkeit geben, ihre Teilidentitäten einfacher mit anderen Anbietern zu teilen. Bekannt ist dieses Prinzip als Single Sign-On, wie es bspw. große Identitätsprovider wie Google, Facebook und Co. anbieten. Dabei macht man sich als Nutzer nicht nur abhängig von diesen zentralen Providern. Diese zentralen Stellen können auch sehr gut nachvollziehen, wie und welche Dienste mit den Teilidentitäten genutzt werden. Auch liegt hierbei ein hohes Missbrauchsrisiko der Identität vor, wenn beispielsweise Informationen oder sogar die Zugangsdaten an Dritte gelangen, mit denen sich dann eine große Anzahl der verbundenen digitalen Teilidentitäten extern kontrollieren lassen.

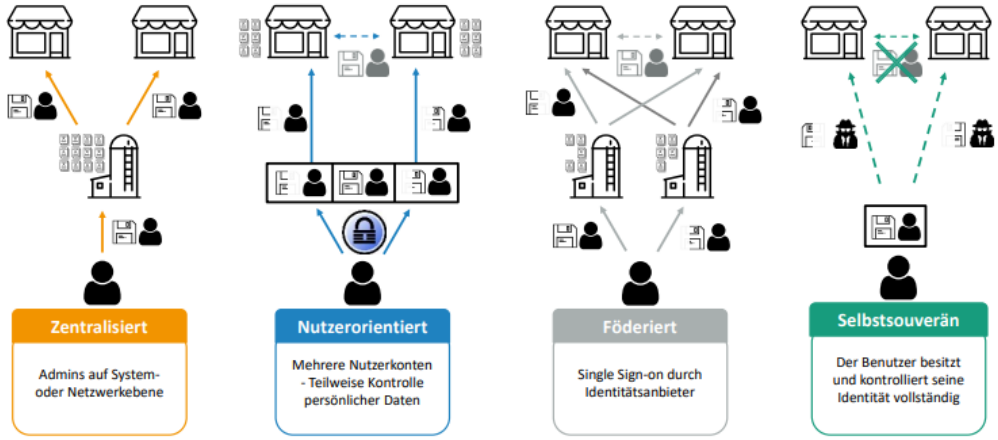


Abbildung 1: Entwicklung des Identitätsmanagements (Strüker et.al, 2021)

Es lässt sich damit erkennen, dass Identitätsmanagement-Systeme ständig im Wandel sind und auf Mängel vorhergehender Modelle aufbauen möchten. Deswegen sollten wir diese Entwicklung fördern und immer weiter nach neuen und besseren Ansätzen für die Anforderungen einer stetig digitalisierenden Gesellschaft suchen.

Die Werte von SSI

Der nächste Entwicklungspunkt wird in dem selbstsouveränen Identitätsmodell gesehen. Der Nutzer wird als zentraler Verwalter seiner Teilidentitäten gesehen und in der Lage sein, seine Identität über verschiedene Dienste hinweg zu kontrollieren. Solch eine Identität muss daher interoperabel und portabel sein, um eine autonome Verwaltung zu gewährleisten. Nutzer müssen in der Lage sein, Behauptungen über ihre Identität zu treffen, die durch die Bestätigung von Dritten zu verifizierten Attributen werden. Auch müssen Dritte in der Lage sein, Attribute zu einer Identität hinzuzufügen, die durch die Nutzer bestätigt werden können (Strüker et al., 2021).

Der Autor Christopher Allen definierte 2016 erstmals zehn Prinzipen für die selbstsouveräne Identität und prägte damit die SSI-Bewegung. Diese beschreiben damit jedoch noch keine spezifische technische Lösung und das Prinzip von SSI wird zunächst technologieneutral erklärt (Strüker et al, 2021). Die Prinzipien fungieren eher als Anforderungskatalog für eine Umsetzung einer SSI-Lösung und setzen sich zusammen aus (Allen, 2016):

Existenz: Nutzer müssen die Möglichkeit haben eine unabhängige Identität zu haben.

Kontrolle: Die Nutzer einer SSI müssen die volle Befugnis über diese haben. Dies sollte durch sichere und gut erforschte Algorithmen gewährleistet werden.

Zugriff: Nutzer sollten immer in der Lage sein, alle Aussagen und andere Daten innerhalb ihrer Identität leicht abzurufen. Sie können nicht unbedingt alle Daten ändern, sollten aber über sie informiert sein.

Transparenz: Jede SSI muss transparente Systeme und Algorithmen haben, die für alle zugänglich sind. Durch Open-Source-Code sollte die Technologie überprüfbar sein, um Vertrauen aufzubauen.

Langlebigkeit: SSI-Identitäten sollten so lange wie gewünscht nutzbar bleiben, auch wenn sich die zugrunde liegenden Algorithmen eventuell ändern. Die Identitätsinformationen sollten im Idealfall unverändert bleiben. Gleichzeitig sollte das Recht auf Vergessenwerden gewährleistet sein, sodass Benutzer ihre Identität löschen und damit die bisher erteilten Rechte ungültig machen können.

Übertragbarkeit: Die Daten einer SSI müssen immer übertragbar sein, damit die Nutzer die Kontrolle über ihre Identität behalten, auch wenn ausstellende oder verifizierende Entitäten verschwinden oder sich Regulierungen ändern.

Interoperabilität: Eine SSI sollte in vielen verschiedenen Bereichen einsetzbar sein und unabhängig von bestehenden Grenzen und Systemen arbeiten.

Einverständnis: Nutzer müssen immer zustimmen, wenn eine Entität ihre Identität verwenden möchte. Da das System darauf basiert, Informationen mit Entitäten zu teilen, ist die Zustimmung der Nutzer für jede Datenweitergabe erforderlich.

Minimisierung: Es sollte nur die minimal erforderliche Datenmenge beim Teilen offenbart werden, um die jeweilige Aufgabe zu erfüllen. Wenn beispielsweise nur ein Mindestalter benötigt wird, muss nicht das genaue Alter preisgegeben werden. Ebenso wenn nur ein Alter angefordert wird, sollte nicht das präzise Geburtsdatum preisgegeben werden müssen. Selektive Offenlegung und andere Zero-Knowledge-Techniken können dieses Prinzip unterstützen.

Schutz: Die Nutzerrechte müssen geschützt werden. Bei Konflikten zwischen den Bedürfnissen des Identitätsnetzwerks und den Rechten der Nutzer sollte das Netzwerk die individuellen Rechte priorisieren. Die Identitätsauthentifizierung sollte durch unabhängige, zensurresistente und dezentrale Algorithmen erfolgen.

Es werden sich aber auch schon Gedanken um konkrete Konzepte und technische Umsetzungen gemacht und Pilotprojekte aufgebaut, wie die European Blockchain Service Infrastructure (EBSI) und das dazugehörige European Self-Sovereign Identity Framework (eSSIF) (Europäische Kommission, 2023), als auch in Deutschland ID-Union (ID-Union, 2022). Es wurden konkrete mögliche Schlüsseltechnologien und Rollenkonzepte identifiziert, auf welche im nächsten Abschnitt näher drauf eingegangen wird.

Die Rollen bei SSI

Das Konzept eines SSI-Ökosystems sieht derzeit drei Rollen vor: Issuer, Holder und Verifier (Grytz & Kudra, 2022). Der Holder, welcher als Nutzer im Mittelpunkt steht, erhält seine digitalen Nachweise, genannte verifizierbare Credentials, von einem Credential Issuer. Dies sollte eine dazu berechtigte und anerkannte Instanz sein, die die Richtigkeit der Informationen auf dem digitalen Nachweis garantiert. Der Holder speichert den digitalen Nachweis mit den personenbezogenen Daten bei sich ab und kann sich nun gegenüber Dritten, den Verifiern, identifizieren und autorisieren. Der Verifier schickt dazu dem Holder eine Anfrage über Inhalte und Anforderungen auf geforderten Nachweisen. Der Holder kann dabei benötigte Inhalte und Aussagen aus seinen Nachweisen in einer sogenannten verifizierbaren Präsentation sammeln und als Antwort an den Verifier freigeben. Der Verifier prüft dann die Inhalte auf ihre Anforderungen, sowie deren bestätigte Gültigkeit und Richtigkeit vom Issuer (Grytz & Kudra, 2022). Dabei müssen Issuer und Verifier nicht mehr zwingend im direkten Kontakt stehen, jedoch ein Vertrauensverhältnis des Verifiers gegenüber dem Issuer existieren. So würde der Issuer dieser Nachweise nicht mitbekommen, für welche Interaktionen der Inhaber der Nachweise diese nutzt, so wie es auch derzeit mit physischen Ausweisdokumenten in der analogen Welt stattfindet.

Deswegen wird dieses Rollenverhältnis bei SSI das „Triangle of Trust“ genannt, indem diese drei Rollen in ihren jeweiligen Verhältnissen agieren (Strüker et al, 2021). Um dieses Vertrauensverhältnis zu etablieren und zu unterstützen wird empfohlen innerhalb bestehender Vertrauensverhältnisse anzusetzen und eine Bildung von skalierbaren Konsortien von Netzwerkverwaltern und unterschiedlichen Issuern als auch Verifiern gefordert. Auch soll die darunterliegende Technologie mit ihren kryptografischen Verfahren sowohl die benötigte Sicherheit für die Nachweise des Holders als auch Transparenz für das Vertrauensverhältnis bereitstellen. Eine oft vorgeschlagene Technologie für diese Vertrauensanker sind *Distributed Ledger* – Netzwerke, die wie unveränderbare und dezentral verwaltbare Hauptbücher oder Register die Infrastruktur für die Ausstellung und Verifikation von Nachweisen bereitstellen, ohne die Nachweise oder personenbezogene Daten selbst darin zu speichern (Grytz & Kudra, 2022).

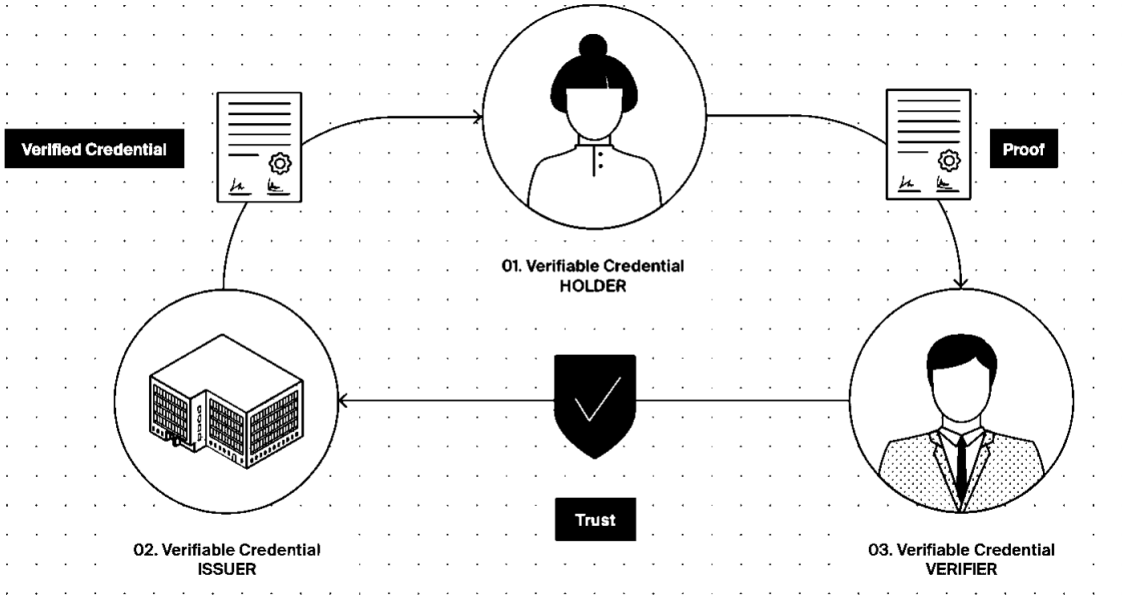


Abbildung 2: Das Triangle of Trust, das Grundkonzept von SSI (Kaumanns, 2023)

Kernelemente derzeitiger Technologien

Nun wird auf die technischen Kernelemente eingegangen, um das Verständnis von SSI zu vertiefen und den Jargon der dezentralen Identitäten näher zu bringen.

Decentralized Identifiers (DIDs)

Der W3C-Standard von ***dezentralisierten Identifiers*** spielt eine Schlüsselrolle für die Ende-zu-Ende-Kommunikation und Anonymisierung, indem sie eine persönliche Adresse (wie eine E-Mail oder Telefonnummer) darstellen, die von den jeweiligen Personen und Organisationen aber selbst kontrolliert wird (Stücker et al, 2021; W3C, 2022). Jeweils ein **DID-Dokument** mit kryptografischen Schlüsseln als auch bspw. Service-Endpunkten zur weiteren Kontaktaufnahme ist an eine DID gekoppelt und ermöglicht eine eindeutige Identifizierung der inhabenden Person, den DID-Controller, bei Bedarf und Einverständnis (Strüker et al, 2021; Pohlmann, 2019). Die DID und das dazugehörige DID-Dokument fungieren hierbei wie ein einzigartiger digitaler Fingerabdruck (Strüker et. al, 2021).

Ein Subjekt kann mehrere DIDs besitzen und diese so lange verwenden wie es möchte (W3C, 2022).

Es kann öffentliche und private DIDs geben. Issuer müssen öffentliche DIDs auf dem *Ledger* speichern, um sie zu identifizieren und deren Reputation und Signatur bei von ihnen ausgestellten Nachweisen zu überprüfen (Grytz & Kudra, 2022).

Natürliche Personen, die sich nur ausweisen möchten, können aber müssen diese nicht auf dem Ledger abspeichern, wenn sie auch anderweitig die Kontrolle des DIDs kryptografisch nachweisen können (Europäische Kommission, 2022). Bei der Kommunikation zwischen zwei Parteien werden paarweise eindeutige DIDs generiert, um Interaktionen von anderen Parteien zu isolieren (Grytz & Kudra, 2022). Obwohl bei SSI oft die Kontaktaufnahme mit einem öffentlichen DID beginnt, können die Parteien für die weitere Interaktion ihre eigenen Peer-DIDs austauschen (Strüker et al, 2021).

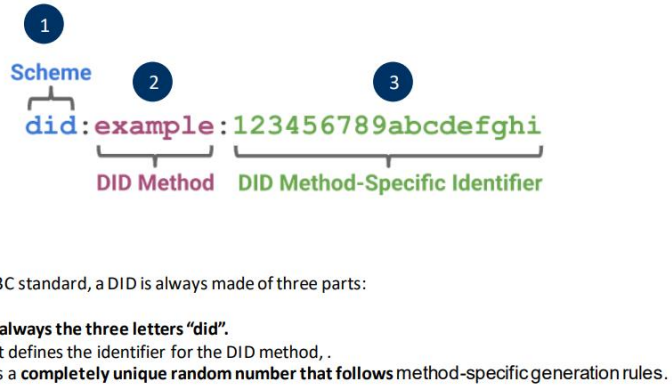


Abbildung 3: Aufbau eines decentralized Identifiers (DID) (Europäische Kommission, 2022)

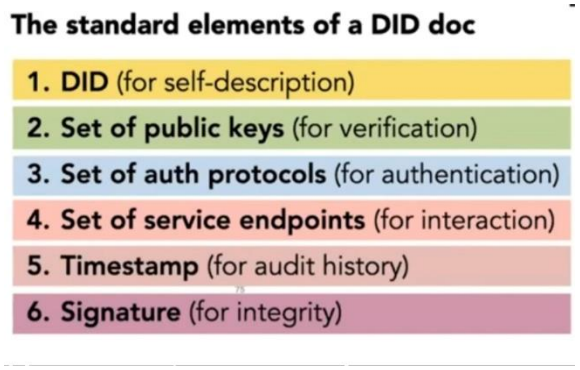


Abbildung 4: Aufbau eines DID Dokuments (Young, 2022)

Verifiable Credentials (VCs)

Verifizierbare Credentials sind dabei die digitalen Nachweise in einem kryptografischen Format, die von den Ausstellern an den Inhaber erteilt werden (Grytz & Kudra, 2022). Diese beinhalten Metadaten zu Aussteller, Credentialtyp, Gültigkeit und Nutzungsbedingungen, sowie weitere Felder, die das Credential beschreiben. Zentraler Bestandteil sind die *Claims* des VCs, also die Aussagen, die in dem Nachweis getroffen werden. Man kann sich das ähnlich wie die Daten auf dem Chip des Personalausweises oder elektronischen Aufenthaltstitels mit eID/eAT-Funktion vorstellen, wobei die Bundesdruckerei dabei als Aussteller fungierte (BDR, 2022). Der letzte wichtige Teil sind die *Proofs*, eine digitale Signatur/Siegel vom Issuer, die er mit seinem kryptografischen geheimen Schlüssel (*private key*) erstellt hat (Grytz & Kudra , 2022; Stüker et. al, 2021).

Abbildung 5: Aufbau eines Verifiable Credentials (VC) (Stüker et al, 2021)

Nun kann jeder mithilfe des öffentlichen Schlüssels des Issuers (*public key* aus dem *public DID* auf dem *Ledger*) überprüfen, dass die Signatur mittels des zugehörigen *private keys(welchen nur der Besitzer der jeweiligen digitalen Identität hat)* berechnet wurde, ohne diesen *private key* jemals gesehen zu haben [1] (Stüker et. al, 2021). Dies stellt sicher, dass die Einträge tatsächlich vom Aussteller vorgenommen und nicht nachträglich geändert wurden – die Verifikation der Nachweise würde sonst fehlschlagen. Ebenso wird die Authentizität von Aussteller und Inhaber eines Credentials bestätigt(Grytz & Kudra , 2022). Neben der Basis-ID des Personalausweises könnten als VCs jedoch auch Bonitätsnachweise, Fahrerlaubnis, Arbeitgebernachweise und Zugänge bei der Arbeit, Gesundheits- und Versicherungsnachweise, Zertifikate und Abschlüsse, Beglaubigungen, Visa und viele weitere verschiedene Aussagen zugehörig zur Identität eines Subjektes ausgestellt werden.

1: Dieses Public-Key Verfahren zählt zur sehr sicheren asymmetrischen Verschlüsselung (Pohlmann, 2020). Gängige Public Key Infrastrukturen (PKIs) benötigen derzeit global zentralisierte Zertifizierungs-Instanzen die für die jeweiligen Issuer Dokumente signieren oder die public keys aus den Signaturen zu ihnen zuordnen. Mit der Einführung von DIDs würde dies nicht mehr nötig sein und der Issuer hätte eine direkte Zuordnung seiner public keys aus Signaturen (Savill, 2022)

Distributed Ledger Technology (DLT)

Die schon erwähnten ***Distributed Ledger Technologien*** bieten dabei die Infrastruktur für die Ausstellung und Verifikation dieser digitalen Nachweise. Daten über die Authentizität und Gültigkeit von Nachweisen würden damit nicht im inhaltlichen Klartext auf einer zentralen Stelle gespeichert, sondern der kryptografische Proof des Issuers auf viele verschiedene Knoten geschrieben werden. Zudem können DLTs ein gewisses Maß an Standardisierung und Vorteile bei der Ausfallssicherheit, wie z.B im Falle von Cyberangriffen, bringen (Stücker et. al, 2021). Dabei erhält jeder Rechner, nach einem erfolgten Konsens-mechanismus über das hinzugefügte Element, eine Kopie des *Ledgers* (Grytz & Kudra , 2022; Stücker et. al, 2021). Der Zugang zu diesem Register könnte, je nach Anforderung der Anwendung, als *public oder private Ledger* gestaltet werden, abhängig davon welcher Anzahl an Identitäten veröffentliche DIDs bekannt zu machen sind (Stücker et. al, 2021). Oft werden derzeit hierfür als mögliche DLTs Blockchains [1] vorgeschlagen, da diese in den Punkten der Unveränderlichkeit, Transparenz, kryptografischen Signaturen und zeitchronologischen Anordnung in Fällen des Widerrufs und Änderungen überzeu-gen (Stücker et al. 2021; Pohlmann, 2019). Zu nennen ist aber die Einhaltung von DSGVO-Vorschriften über die Berichtigung und Löschung von personenbezogenen Daten, weshalb auch aus diesem Grund keine personenbezogenen Daten selbst auf einem manipulationsresistenten Ledger wie einer Blockchain gespeichert werden dürfen und damit beim Holder liegen sollten (Strüker et al. 2021). Die dabei sehr beliebte Open-Source Lösung *Hyperledger Aries*, *Hyperledger Ursa* und *Hyperledger Indy* von der Linux-Foundation (The Linux Foundation, 2024), hat in diesem Vorhaben eine Standardisierung von Protokollen, Prozessen und Frameworks und damit eine Interoperabilität zwischen verschiedenen möglichen SSI Blockchain-Netzwerken zum Ziel gemacht und befindet sich in vielen verschiedenen Pilotprojekten im Einsatz (Pohlmann, 2019; Grytz & Kudra , 2022).

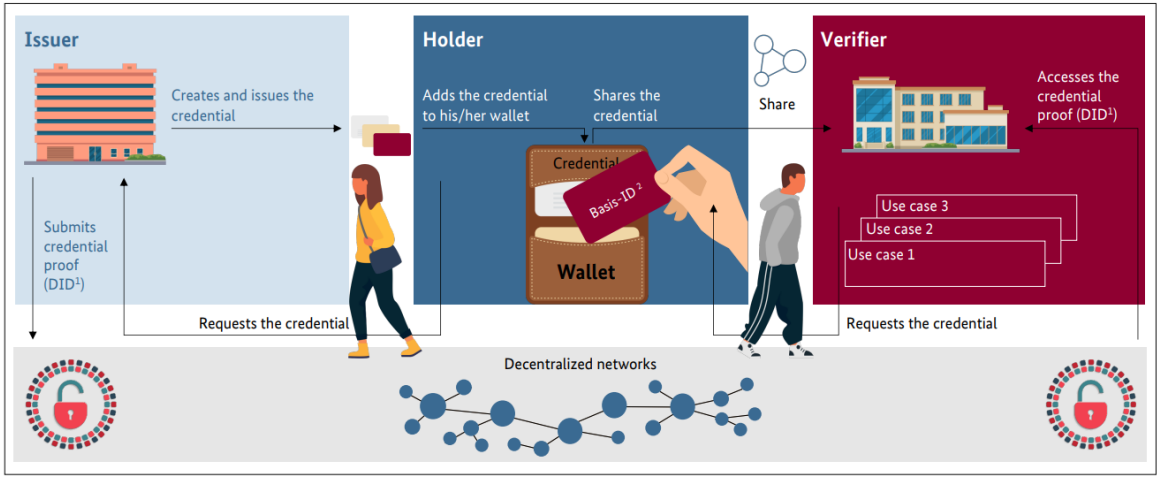


Abbildung 6: Konkretere Darstellung des Triangle of Trust (Bundeskanzleramt, 2021)

Man darf jedoch auch die derzeitigen Nachteile einer Blockchain-Infrastruktur nicht vernachlässigen. Auch wenn keine personenbezogenen Daten im Register gespeichert wer-den und die zu speichernde Datenmenge in den public DIDs für eine bessere Skalierbarkeit klein genug bleiben (Strüker et. al, 2021), ist der Energieaufwand für Konsensmechanismen einer Blockchain, vor allem eine der Methoden „Proof of Work“, mit erheblicher Rechenleistung und dementsprechend Energieauf-wand und Ressourcenverbrauch verbunden (Gourisetti et al.,

1: Eine Blockchain ist eine de-zentrale Datenbankstruktur, in der Daten in kryptographisch verketteten Blöcken unverän-derlich gespeichert werden können Die Blöcke enthalten zudem Informationen über die Verifikation der Nachbarblö-cke. Eine Manipulation in der Datenkette würde durch Ändern oder Einfügen eines Blocks damit auffliegen (Jannik et. al, 2019)

2021). Deswegen empfiehlt sich weiterhin auch weitere Konsensmechanismen als auch *DLTs* für den Aufbau einer SSI-Lösung heranzuziehen und zu untersuchen. Das Bundesamt für Sicherheit in der Informationstechnik kam sogar zum Schluss, dass SSI nicht zwingend auf einem DLT-basierten Register beruhen muss und anhand dem Anforderungskatalog eines Anwendungsfalls auch andere Strukturen denkbar wären (BSI, 2021).

Weitere technische Kernelemente

Man könnte noch auf weitere Möglichkeiten und vorgesehene Verfahren bezogen auf die Technologien eingehen, wie beispielsweise *Link Secrets*, *Selective Disclosure* , *Zero-Knowledge Proofs (ZKP)*, *Signature Blinding* und *digitale Wallets* (Pohlmann, 2019; Strüker et. al, 2021). Dies würde jedoch den Rahmen der Einleitung in die SSI sprengen. *Digitale Wallets* sind vor allem in Bezug auf den Inhaber interessant, da sie auch ohne Ablage des DIDs auf dem Ledger erlauben, den Besitz über diese Identität nachzuweisen. Die Frage entsteht, ob alle Nachweise (wie oft vorgeschlagen) im Sicherheits-Element des mobilen Endgeräts gelagert werden und über Apps verwaltet werden sollen (Strüker et. al, 2021). Wenn das Ziel der digitale Aktenschrank ist (Bundeskanzleramt, 2021), ist es im Hinblick auf die Gestaltung der Nachweisverwaltung eher weniger wünschenswert diesen anfangs jederzeit in seiner Hosentasche mitzuziehen. Formen der Anbindung über *Mobile-* und *Cloud-Agents*, die die Speicherung, Verwaltung und Austausch der Daten ermöglichen, als auch physische Speicherlösungen müssen weiterhin erforscht und auf ihre Abhängigkeit zu den Anbietern geprüft werden (Pohlmann, 2019; BSI, 2021).

Chancen und Herausforderungen von SSI

Die Einführung von SSI kann viele positive Chancen für öffentliche Institutionen, Unternehmen und Bürger beinhalten, wird aber auch mit einigen Herausforderungen begleitet.

Chancen

Viele Chancen werden sowohl bei staatlichen Institutionen und Unternehmen gesehen, wobei Prozesse der Datenprüfung als auch Datenhaltung vereinfachter und effizienter gestaltet werden können. So können beispielsweise im E-Commerce ein sicherer, passwortfreier Zugang zu Webservices realisiert werden und Altersprüfungen oder Bonitätsprüfungen mithilfe verifizierbarer Aussagen zum Mindestalter/Mindestbetrag getroffen werden, ohne die genauen Daten zu teilen und personenbezogene Dokumente im Klartext an Unternehmen zu übertragen (Strüker et al., 2021). Auch Mischungen aus hoheitlichen Nachweisen, wie der Basis-ID, als auch privaten Nachweisen von Arbeitgebern, wie Firmenzugehörigkeit und Firmenadresse, können für die schnellere Bearbeitung von Anträgen mit Dokumentprüfungen sorgen. Ein konkretes Beispiel ist der Hotel-Check-In mit der Hotelmeldebescheinigung, welche als Pilotprojekt in vielen Betrieben an den Start ging (Bundeskanzleramt, 2021). Auch für Objekte im Internet of Things (IOT) könnten Nachweise ausgestellt werden und einfacher geprüft als auch verwaltet werden, wie beispielsweise Fahrzeugschein, TÜV-Prüfungen und Mautzahlungen bei Autos (Strüker et al., 2021).

Bei öffentlichen Institutionen wird das meiste Potential für die Digitalisierung von Dokumenten in der Ausstellung als auch Prüfung gesehen, was diese Prozesse deutlich vereinfachen

würde. Neben der Erstellung von manipulationsresistenteren digitalen Versionen von Personalausweisen, Reisepässen oder Geburtsurkunden, könnten auch Zertifikate, Bescheinigungen und weitere noch im Papierformat befindlichen Nachweise von den jeweiligen Institutionen ausgestellt werden. Wenn diese heutzutage in einem digitalen Format gefordert werden, werden diese meist eingescannt oder fotografiert, welches die Bescheinigung oder das Zertifikat leicht manipulierbar macht. Aus diesem Grund wird dann vermehrt auf Echtheitsprüfungen zurückgegriffen, welche hohe Kosten und vor allem Zeit fordern (Strüker et. al, 2021). Es geht aber auch darum, Daten, die schon einmal durch eine hoheitliche Instanz geprüft wurden, wiederverwendbar zu gestalten. Man könnte im Kontext vom Staat davon sprechen, dass der Bürger nun die API [1] ist – die schon mal ausgestellten digitalen Nachweise werden vom Bürger selbst an die Stellen befördert, an denen sie benötigt und angefragt werden (Tobin, 2021).

Abbildung 7: Der Bürger ist nun die API (Tobin, 2021)

Nutzer könnten dadurch verwaltungsdienstliche Leistungen digital schnell und einfach beantragen und erhalten. Verifizierte Daten könnten aufwendige Prüfprozesse beschleunigen und Automatisierung ermöglichen, wodurch Ressourcen besser genutzt werden könnten. Darüber hinaus könnte SSI den Behörden selbst einen einfacheren Zugriff auf Verwaltungsleistungen anderer Behörden ermöglichen und würde deren Informationsabruf beschleunigen (Biedermann et al., 2023). Ein Pilotprojekt im Bereich von öffentlichen Institutionen könnte damit als Anstoß einer weiteren Digitalisierung von Verwaltungsprozessen dienen (Strüker et. al, 2021).

Herausforderungen

Neben den schon angeschnittenen technischen Herausforderungen gibt es derzeit jedoch noch weitere Bedenken im rechtlichen und Governance-Bereich. Zum einen stellt sich die Frage nach dem Umgang der geteilten Daten. Der Identitätsinhaber muss sich von der Authentizität des Prüfers überzeugen, um eine unabsichtliche Weitergabe von Daten an Unberechtigte zu verhindern (BSI, 2021), als auch die Daten zu dem Zweck verarbeiten zu lassen, zu dem sie bestimmt sind (Strüker et. al, 2021). Auch muss bei einer Umsetzung in dezentralen Netzwerken sicher gegangen werden, dass die Manipulation der Reputation eines Nachweisaussteller unterbunden wird. Ein Beispiel ist der Sybil-Angriff. indem ein Akteur viele Identitäten annimmt, um überproportional oft für die Vertrauenswürdigkeit eines speziellen Herausgebers zu votieren oder Netzwerk-Nodes lahmzulegen (BSI, 2021). In Bezug auf öffentliche Institutionen wie Behörden, sind eine besondere Herausforderung veraltete Satzungen und Rechtsauflagen. Die Einführung eines digitalen Prozesses

1: Eine Application Programming Interface (API), ist ein Zugriffspunkt, der von der Anwendung angeboten wird, um Daten oder ein Programm nutzen. Im Prinzip ist eine API eine Programmierschnittstelle, die die Interaktion und Integration mehrerer Programme erleichtert (Lautenschlag, 2022).

scheitert oft an „Unterschrift-“ oder „Schrifterfordernissen“, weswegen Dokumente immer noch ausgedruckt, unterzeichnet und vor Ort oder per Post eingereicht werden müssen (Biedermann et al., 2023). Eine Abhilfe könnte dabei die Durchsetzung der europaweiten eIDAS-Verordnung schaffen, da sie die rechtlichen Rahmenbedingungen für die Verwendung elektronischer Signaturen stellt und damit einer elektronischen Transaktion die gleiche rechtliche Stellung wie einer papierbasierten Transaktion ermöglicht (Strüker et. al, 2021). Die Governance, also die Verwaltung für die Rahmenbedingungen und Regeln im SSI-System, ist auch bezogen auf die jeweiligen Anwendungsfälle klärungsbedürftig. Um eine Skalierbarkeit von SSI-Lösungen zu gewährleisten, müssen vereinheitlichte SSI-Protokolle durchgesetzt werden, welche eine stetig breite Anzahl an möglichen Nutzern des Netzwerks benötigt (Strüker et al., 2021). Auch die Verwaltung der einzelnen Knoten im Netzwerk, von beispielsweise EU-Staaten, dem deutschen Staat als auch staatlichen Unternehmen, sowie die Bereitstellung von Identitätsverwaltungs-Apps von Unternehmen für Bürger wirft die Sorge auf, ob durch die Bemühungen Identitäten zu dezentralisieren, sich nicht wieder ein zentralisiertes System hinter einem Deckmantel einschleichen könnte.

Idee-Ansatzmöglichkeit in der Behörde - aber in welcher?

Trotz der angeschnittenen Herausforderungen bei SSI, bleibt es weiterhin interessant, wie diese in Konzepten angenommen werden können. Die Chancen und Möglichkeiten, speziell in öffentlichen Institutionen wie Behörden sind im Kontext der digitalen Transformation von Verwaltungsprozessen und der Erneuerung des Onlinezugangsgesetzes (OZG) [1] von großer Bedeutung. Es benötigt für eine ganzheitliche Digitalisierung ein behördenübergreifende Prozessoptimierung und keine Abbildung derzeitiger Prozessstrukturen in das Digitale. Aus diesem Grund ist es von Nöten, sich gestalterische Gedanken über ideale Prozesse innerhalb von verschiedenen Behörden zu machen und dann Anforderungen an technische und rechtliche Maßnahmen aufzustellen.

Für den Ansatz einer Prozessgestaltung mit dem Hintergrund von SSI, wurde nach konkreten Behörden gesucht, die möglicherweise schon zwischenbehördliche Personen- und Nachweisregister nutzen oder damit vertraut sind. Dazu hat sich das Wissen über das *Ausländerzentralregister* (AZR) mit Visadatei eröffnet, welches als Datenbank alle ausländerrechtlich relevanten Informationen über 26 Millionen ausländische Personen beinhaltet (BVA, o.D.). Damit ist es bundesweit die von dem Bundesamt für Migration und Flüchtlinge zentral verwaltete Datenquelle im Bereich des Ausländerwesens, durch die den zuständigen Verwaltungs- und Sicherheitsbehörden des Bundes, der Länder und Kommunen umfassende sowie einheitliche Informationen zur Verfügung gestellt werden sollen (BAMF, 2022). Trotz umfassender zentraler Speicherung sind jedoch noch nicht alle wichtigen Informationen und

1: Das Onlinezugangsgesetz hatte sich anfangs zum Ziel gemacht, bis Ende 2022 einen digitalen Zugang für alle behördlichen Dienstleistungen für Bürger zu gewährleisten (Bundesinnenministerium, 2019). Dieses Vorhaben ist gescheitert, aufgrund von bspw. fehlenden Standards und Basisdiensten, fehlender Planung einer Ende-zu-Ende Digitalisierung und einer geringen Unterstützung der Kommunen durch den Bund (Wölbert, 2022). Mit der Erneuerung zum OZG 2.0 wird der Druck auf die Umsetzung nun bis 2028 erhöht, ohne jedoch konkrete Zwischenschritte bis zu diesem Jahr zu definieren (Deutschlandfunk, 2024)

Verlaufsdaten in der Datenbank enthalten, und jede Erweiterung erfordert eine aufwändige und zeitintensive Prüfung des verbundenen AZR-Gesetzes (Jannik et al., 2019). Die umfassenden und perspektivisch noch wachsenden Dokumentationspflichten können jedoch seitens der Ausländerbehörden keineswegs vollumfänglich geleistet werden und werden dementsprechend kaum genutzt (Schlee et al., 2023). Ob solch ein zentrales Erfassungssystem von sensiblen Daten nicht nur effizient, sondern überhaupt normativ wünschenswert sein kann, sollte sich auch dabei gefragt werden (Schlee et al., 2023; Biselli, 2023).

Für das weitere Projekt wurde sich dementsprechend dazu entschlossen, bei der Gestaltung eines Angebots für Prozesse in öffentlichen Institutionen aus dem Blickwinkel der Ausländerbehörden anzusetzen. Nicht nur mit dem Hintergrund, das vor allem ausländerrechtliche Prozesse in Deutschland stark föderal organisiert sind und von dezentral gestalteten Technologien profitieren könnten (Amend et. al, 2023). Auch das persönliche Interesse daran, die Gründe für die Reputation und Herausforderungen innerhalb der Ausländerbehörden zu verstehen, spielten dabei eine Rolle.

Kontext Ausländerbehörde – was ist da eigentlich los?

Aufgaben und Organisation einer Ausländerbehörde

Allgemein sind Ausländerbehörden für die aufenthalts- und passrechtlichen Maßnahmen und Entscheidungen nach dem Gesetz über den Aufenthalt, die Erwerbstätigkeit und die Integration von Ausländern im Bundesgebiet (AufenthG) und nach ausländerrechtlichen Bestimmungen in anderen Gesetzen zuständig. Sie sind damit auch erste Ansprechstelle für alle Fragen zu einem konkreten Einzelfall in diesen Bereichen (BMI, o.D). Die Ausländerbehörden setzen damit das Aufenthaltsrecht als Auftragsangelegenheiten um (Schlee et al., 2023).

Praktisch alle Aufenthaltsregelungen für Ausländer - außerhalb des Asylrechts - werden von Ausländerbehörden umgesetzt. Das betrifft z.B. die Ausstellung, Verlängerung oder Verfestigung von Aufenthaltstiteln (verschiedene Formen der Aufenthaltserlaubnis, Erlaubnis zum Daueraufenthalt - EU, verschiedene Formen der Niederlassungserlaubnis, Blaue Karte EU, ICT-Karte, Mobiler-ICT-Karte, Visum (BMI, o.D.)), Visaanträge für Familienzusammenführung und Arbeitserlaubnisse sowie Einbürgerungen (Schammann & Kühn, 2016). So sind nur im Kontext der Erteilung von Aufenthaltstiteln schon allein 195 Leistungen geführt. Die Aufgaben der Ausländerbehörden variieren dabei je nach Bundesland und können die statistische Erfassung von Ausländern, die Ausstellung von Aufenthaltsdokumenten, Einbürgerungen bis hin zum Rückführungsmanagement umfassen. Die Komplexität des Arbeitsfeldes zeichnet sich auch durch die vielfältiger werdenden Migrationsformen und damit verbundenen ausdifferenzierten Anforderungen und Gesetze in den jeweiligen Aufgaben aus. Allerdings sind die Aufgaben so komplex, dass ein Überblick nicht alles in der Tiefe erfassen könnte (Schlee et al., 2023).

Die Bundesländer regeln die Zuständigkeit im Ausländerwesen jeweils selbst. Diese definieren die Architektur der Organisationen und Zuständigkeitsordnungen, die Kommunen haben eine Steuerungsfähigkeit in der Organisationsanbindung durch Schwerpunktsetzungen und interne Personalverteilungen. In einigen Bundesländern teilen sich zentrale Ausländerbehörden (als staatliche Landesmittelbehörden) und kommunale Ausländerbehörden die Aufgaben. Die kommunalen Ausländerbehörden haben prinzipiell eine örtliche Zuständigkeit für die Personen, die sich in der Kommune aufhalten.
Je nach ihrer Größe verfügen die Behörden über unterschiedliche Ressourcen und zeigen verschiedene Grade an Professionalisierung und Spezialisierung, sowie einen unterschiedlichen Arbeitsalltag und Anwendungspraxis (Schlee et. al, 2023).

Reputation der Ausländerbehörde und Wahrnehmung von Betroffenen

Das „One Stop Government“ an der Schnittstelle Ausländerbehörde dient als zentrale Anlaufstelle für alle Anträge zum Aufenthalt und zur Beschäftigungsaufnahme (Schneider, 2012). Was jedoch für Prozesse nach dem Besuch des Ausländeramtes ablaufen und was nach der Abgabe des Antrags und dazugehöriger Dokumente passiert, ist für viele Betroffene unklar. Man könnte fast von einer Blackbox sprechen. Dies führt zu einer Verwaltung, deren Handlungen und Entscheidungen von außen nur schwer nachvollziehbar sind (Schlee et. al, 2023).

Es sind Berichte in den Medien und Meldungen, die über lange Wartezeiten und schlechte Erreichbarkeit als auch deren gravierende Auswirkungen auf die Möglichkeit, einer Arbeit nachzugehen oder Sozialleistungen zu beziehen, informieren. Auch die zahlreichen Wortmeldungen aus den Behörden selbst, die einen Eindruck von der Arbeitsbelastung vermitteln, prägen das bisherige Gesamtbild der Ausländerbehörden.

Es liegen jedoch keine validen Daten zur durchschnittlichen Bearbeitungsdauer von Fallarten, Struktur von Prozessabläufen, Wartezeiten in Ausländerbehörden als auch allgemein zur Organisations- und Prozessforschung in Ausländerbehörden vor (Schlee et. al, 2023).

Auch der Kontakt zu den Ausländerbehörden des Publikums findet immer mehr über intermediäre Instanzen wie Steuerberater, Migrationsberatungen, Sozialberatungen oder Anwälte statt. Die komplexe Natur aufenthaltsrechtlicher Entscheidungen und fehlende Kontaktmöglichkeiten führen dazu, dass diese Entscheidungen und ihre schwerwiegenden Folgen oft als willkürlich empfunden werden, da sie für die Betroffenen schwer nachvollziehbar sind. Recht und Verwaltung scheinen nicht nur komplexer, sondern vor allem für die Öffentlichkeit unzugänglicher zu werden (Schlee et. al, 2023).

Die Mehrheit der Ausländerbehörden sieht sich als zentralen Akteur im Integrationsprozess, ist damit aber auch einem erheblichen Druck ausgesetzt (Bogumil et al. 2023)

Abbildung 8: Sammlung von Titeln aus Medienberichten des letzten Jahres

Ursachen für die Probleme

In einer neuen umfassenden Studie der Bertelsmann Stiftung zu der Situation in verschiedenen Ausländerbehörden, wurden anhand der Beteiligung von Leitern und Sachbearbeitern verschiedene derzeitige Problemfelder und Ursachen identifiziert, als auch Empfehlungen für Verbesserungen erarbeitet (Schlee et. al, 2023). Die Kernursachen werden im Folgenden zusammengetragen:

Personalmangel: Personalengpässe, unbesetzte Stellen und Bewerbermangel im gehobenen Dienst belasten die Ausländerbehörden, was zu vermehrtem Einsatz von Mitarbeitern im mittleren Dienst oder Verwaltungsfachangestellten führt, die oft nicht über die erforderlichen rechtlichen Kompetenzen verfügen. Es können dabei Rückstandfälle entstehen, die mehr Arbeit verursachen als neu eingetroffene Fälle, da aktuelle Nachweise über bspw. Gehalt und Wohnung von den Kunden erneut angefordert werden müssen aufgrund des Entscheidungszeitpunkts. Dieser Personalmangel wird zwar derzeit stark problematisiert, ist aber kein Alleinstellungsmerkmal, da auch andere Behörden damit zu kämpfen haben. Erkannt wurde, dass die Bearbeitungsdauer von aufenthaltsrechtlichen Angelegenheiten nicht nur vom Behördenpersonal und dem Anliegen des Antragstellers abhängt, sondern oftmals auch von der Mitwirkung anderer Behörden wie auch der antragstellenden Person beeinflusst wird.

Zentralisierung: Es gibt einen Trend zur Zentralisierung von Ausländerbehörden, der jedoch zu einem schlechteren Aufgabenvollzug geführt hat, da das vorhandene lokale Know-how und Netzwerke nicht mehr genutzt werden. Insbesondere die Diskussion über die Schaffung einer bundesweit zuständigen Stelle birgt das Risiko, die Vorteile dezentraler Strukturen zu verlieren und neue Engpässe zu schaffen.

Gesetzesanpassungen und Politik: Eine weitere Ursache für Prozessschwierigkeiten in der Ausländerverwaltung liegen in der hohen Komplexität und sehr dynamischen Änderungen des Ausländerrechts sowie in unbestimmten Rechtsbegriffen. Es wird gefordert, dass gesetzliche Neuerungen unter Berücksichtigung der praktischen Umsetzung im Ausländerrecht erfolgen und dass der Bund klare Rahmenbedingungen formuliert. Die Verwaltung fordert für die Bearbeitung der Anträge Prüfschemata und Musterschreiben vom Bund. Es wird auch ein Interessenskonflikt zwischen Verwaltung und Politik gesehen: Die Verwaltung ist dazu verpflichtet, rechtssicher zu handeln. Die Politik ist jedoch auf einen vierjährigen Zyklus für Neuerungen und Programme festgelegt und strebt in dieser Zeit politische Impulse und Erfolge an, wobei das Thema der Migration starkes Mobilisierungspotenzial besitzt.

Digitalisierung: Es besteht ein dringender Bedarf an Verfahrensinnovationen, insbesondere in der Digitalisierung und Automatisierung von Prozessen. Allerdings herrscht Skepsis aufgrund von Ressourcenmangel und fehlender Infrastruktur, was Digitalisierungsbemühungen wie leere Versprechen erscheinen lässt. Viele eingeführte Programme sind jedoch nur unvollständig aufeinander abgestimmt, was zu einem Mehraufwand führt und alles andere als eine medienbruchfreie Bearbeitung zulässt. Zu den derzeit erfolgreicheren digitalen Lösungen zählen die e-Akte, das Fachprogram X-Ausländer-Asyl, die wie ein zwischenbehördlich geteiltes Postfach für

manche Antragsdaten im standardisierten Format dient (BAMF, o.D.), und Onlineterminvergaben.

Es ist wichtig, die Digitalisierung der Ausländerbehörden ganzheitlich und koordiniert anzugehen, indem sie mit anderen kommunalen Aufgaben synchronisiert wird. Dies erfordert Zeit und Zusammenarbeit zwischen verschiedenen Behördenebenen. Die Digitalisierung ermöglicht es, Verwaltungsprozesse neu zu überdenken, einschließlich einer automatisierten Vorprüfung von Anträgen und Dokumenten für unstrittige Fälle. Probleme im Datenaustausch sind aber nicht nur technischer Natur, sondern oft auf einen Mangel an Kooperationsbereitschaft zwischen den beteiligten Behörden zurückzuführen.

Kommunikation und Datenaustausch: Die Anträge werden meist nicht nur von der Ausländerbehörde geprüft, bei der der Antrag und die Dokumente als Kunde eingereicht wurden. Bei der Erfüllung ihrer Aufgaben und abhängig vom Antragsprozess müssen Ausländerbehörden häufig individuelle Abstimmungen und Teilprüfungen mit anderen Behörden durchführen. Dies schließt Behörden ein, die für bestimmte Zielgruppen und Rechtskreise zuständig sind, wie bspw. zentrale Landesmittelbehörden, die Bundesagentur für Arbeit, Sicherheitsbehörden, Auslandvertretungen, Jobcenter, als auch Gesundheitsbehörden. Dies fordert dementsprechend einen Datenaustausch und gemeinsame Koordination bei der Antragsbearbeitung. Sachbearbeiter in Ausländerbehörden berichteten, dass landesintern die Kommunikation und der Austausch über das Behördennetz ganz in Ordnung ist. Teils werden aber ähnliche Erfahrungen gemacht, wie die Kunden mit der Erreichbarkeit der eigenen Ausländerbehörde. Deswegen ist der Ausbau der Kommunikations-Anbindung zwischen den an Prozess beteiligten Behörden von Nöten. Ausländerbehörden sollten aber auch intensive Netzwerke mit zivilgesellschaftlichen Akteuren außerhalb der Kommunalverwaltung aufbauen und pflegen, um die externe Transparenz und Nachvollziehbarkeit ihrer Handlungen und Entscheidungen zu erhöhen.

Doppelte Prüfungen: Kooperationshindernisse führen häufiger zu doppelten Prüfungen von Dokumenten und identischen Meldungen, welches zu längeren Bearbeitungszeiten führt. Das liegt daran, dass sich Ausländerbehörden und bspw. Arbeitsverwaltung unterschiedlichen Zielstellungen verpflichtet fühlen und das gegenseitige Vertrauen fehlt. Die erneute Prüfung von Dokumenten, die bereits von einer anderen Behörde – beispielsweise dem Jobcenter oder der Meldebehörde – gesichtet wurden, sollte aber vermieden werden. Eine mögliche Lösung wird in einer gesetzlichen Änderung im Verwaltungsverfahrensrechts gesehen, die die Anerkennung bereits geprüfter Dokumente vorschreibt oder zumindest empfiehlt. Bundes- und Landesbehörden sollten aber schnell gemeinsam mit Ausländerbehörden, Arbeitgebern und zivilgesellschaftlichen Akteuren nach weiteren Vereinfachungspotenzialen suchen.

Ein Teil des Endfazits der Studie beschreibt, wieso der Fokus auf die Vermeidung von doppelten Prüfaufträgen von Wichtigkeit ist:

„Richtig ist daher, dass dringend eine Reduktion von Fallzahlen erfolgen muss.

Kurzfristig ist dies aber nicht über eine Verringerung der Zuwanderungszahlen zu leisten – unabhängig davon, ob man diese mittel- bis langfristig erreichen kann und möchte. Die Belastung der Ausländerbehörden ist auch mit den aktuell in Deutschland lebenden Ausländern hoch. Der schnellste Weg zu einer Entlastung der Ausländerbehörden führt daher über eine Reduktion von unnötigen Prüfaufträgen.“ – (Schlee et. al, 2023, S.41)

Blickwinkel-Wechsel bei einem Angebotsansatz

Das vorherige Kapitel als auch die die Anforderungen an SSI wurden vor allem aus dem Blickwinkel des Bürgers betrachtet. Auch bei Forderungen nach einer Digitalisierung in öffentlichen Institutionen, wie Behörden, und Zielstellungen des E-Governments, ist der einfache und digitale Zugang des Bürgers zu Leistungen des Staates im Fokus (BMI, o.D.). In Anbetracht der Situation in den Ausländerbehörden, ist der Kunde jedoch ab der Stellung eines vollständigen Antrags nicht mehr ausschlaggebend in die behördlichen Abläufe miteinbezogen. Die derzeitigen Herausforderungen und Problemstellungen sowie Ansätze zu Digitalisierung sollten dabei auch vermehrt auf weitere Akteure in der Interaktion des staatlichen Verwaltungsprozesses eingehen – speziell auf die Sachbearbeiter in den jeweiligen Behörden. Wenn diese entsprechend bei ihren Aufgabenbewältigung unterstützt und gefördert werden, sowie deren Prozesse angemessen im Digitalen gestaltet werden können, wird es nicht nur zu Entlastungen bei den jeweiligen behördlichen Akteuren führen, sondern auch schließlich zu der Entlastung der Bürger. Aus diesem Grund ist es von Vorteil einen Blickwinkel-Wechsel bei der Digitalisierungs-Gestaltung zu tätigen, und aus der Sicht der Sachbearbeiter in der Ausländerbehörde ein Angebot für einen idealen Antragsprozess zu entwerfen.

Ein Angebot für einen idealen Antragsprozess in der Ausländerbehörde

Im Folgenden wird anhand der Erkenntnisse über SSI und die Ausländerbehörde ein Angebot für einen idealen Prozess seitens der Sachbearbeiter gestaltet. Ziel ist es, einen generischen Ablauf für mögliche Antragsprozesse in der Ausländerbehörde zu formulieren und die Rahmenbedingungen sowie die Anforderungen daran aufzustellen.

Grober Ablauf

Ein möglicher idealer Ablauf sieht hierbei drei Phasen vor: Die Antrags- und Dokumenterhebung, die Verifizierung der Nachweise und die Prüfung des Antrags. Die jeweiligen Phasen folgen dem Ziel, in die nächste Phase überzugehen oder den Prozess abzuschließen. Die Schritte in den jeweiligen Phasen könnten in fast jeder Antragsform stattfinden und beinhalten teils nochmal eigene Prozesse, die jeweils unterstützt werden sollten.

Abbildung 9: Grober idealer Ablauf der Antragsbearbeitung

Phase 3, die Prüfung des Antrags, ist dabei eine intensive Arbeitsphase und sollte wertgeschätzt werden. Die Phase kann unterstützt werden durch geforderte Prüfschemata, Musterschreiben, automatisierte Vorprüfungen und einer zwischenbehördlichen vorausschauenden Planung der Phase. Es sollte aber auch die Zeit, die für diese Phase nötig ist, geschätzt werden. Dabei könnten neu gestaltete Ansätze vorangehende Phasen beschleunigen.

Mithilfe von nutzbaren digitalen verifizierbaren Nachweisen einer beantragenden Person, als auch der entsprechenden Infrastruktur für deren Vertrauensanker, besteht das Potenzial für die Beschleunigung von Dokumentprüfprozessen. Im Weiteren wird näher darauf eingegangen welche Rollen es in einem idealen Szenario geben würde und welche Aufgaben sowie Anforderungen an diese Rolle gebunden wären.

Rollen und deren Aufgaben

Nachweisaussteller

Die Nachweisaussteller wären diejenigen Parteien, die die benötigten Dokumente für den Antrag bei der Ausländerbehörde erstmalig ausstellen oder beglaubigen. Dazu würde auch der Prozess Identitätssicherung zählen, der beispielsweise bei vorangehenden Visa- oder Asylanträgen durch Auslandsvertretungen, Sicherheitsbehörden und BAMF durchgeführt wird und biografische und biometrische Daten sichert (BAMF, 2017).

Zu weiteren Parteien könnten bspw. zählen: Ausbildungsstätten, Universitäten, Beglaubigungsstellen, Bundesdruckerei, Arbeitgeber, Banken, Versicherungen, Ärzte, Wohnungsgeber und unter Behörden die Meldebehörde, Sozialamt, Bundesagentur für Arbeit, Jobcenter, Integrationsamt, als auch die Ausländerbehörde selbst. Im Endeffekt alle Parteien, die auch derzeit anerkannte Nachweise für Anträge ausstellen, nur dass dies auch in digitaler Form ermöglicht wäre. Ziel ist es, der Person verifizierbare Nachweise über ihre Identität und deren dazugehörige Attribute auszustellen.

Zu der Aufgabe der jeweiligen Mitarbeiter oder Einzelpersonen würde gehören:

- Verantwortung dafür übernehmen, dass die ausgestellten Aussagen und Daten richtig und vollständig sind
- Bestätigen der Aussagen und Daten durch ein einzigartiges Prüfzeichen, welches beweist, dass die Nachweise von einem bestätigt wurden
- Ablage eines zugehörigen öffentlich sichtbaren Vertrauensankers
- Ausstellung der Nachweise an den Inhaber
- Bei Widerruf oder Änderung der Nachweise, Änderung dokumentieren und den vorausgehenden Vertrauensanker für ungültig erklären und/oder berichtigen

Kunde

Hierbei handelt es sich um die jeweilige Person, die einen Antrag bei der Ausländerbehörde stellt. Dies kann beispielsweise die Erteilung oder Verlängerungen von Aufenthaltstiteln, -gestattungen oder Duldungen, Arbeitserlaubnissen als auch die Einbürgerung oder Teilnahme an Integrationskursen sein (Darmstadt, o.D.). Ein Antrag beinhaltet Antragsformulare, die den geforderten Anspruch und Umstände beschreiben, als auch Dokumente und Nachweise, um die Informationen zur Identität, zum Umstand und für Voraussetzungen nachzuweisen. Ziel der Interaktion mit dem Amt ist es, schnell die Umstände der Teilhabe an der Gesellschaft zu klären und die dafür benötigten Dokumente als auch Nachweise zu beantragen.

Zu den Aufgaben der jeweiligen Person würde gehören:

- Anfordern der benötigten Nachweise für den Antrag bei den zuständigen Stellen
- Speichern und verwalten der eigenen Dokumente, Nachweise und Daten
- Den angeforderten Nachweisen oder Daten aus Nachweisen zustimmen und übermitteln
- Bei Bedarf die restlichen Angaben des Antrags wahrheitsgemäß und richtig ausfüllen, die nicht schon aus Daten der Nachweise übernommen werden können
- Bei Bedarf Beratung beantragen und Termine für persönliche Vorsprachen wahrnehmen

Sachbearbeiter in der Ausländerbehörde

Diejenigen Personen, die kommunal für die Kunden, Prüfung ihrer Nachweise und Bearbeitung ihrer Anträge nach AufenthG zuständig sind. Sie nehmen die Anträge entgegen, führen Identitätsfeststellungen durch, verwalten Kunden-Akten, prüfen die Anträge und entscheiden über das Ergebnis, informieren an Teilprozessen beteiligte Behörden, beantragen Dokumente und stellen Nachweise aus. Ziel der Interaktion mit dem Kunden ist es, ihm die Umstände für die Beteiligung an der Gesellschaft ausführlich zu prüfen und das Ergebnis sowie die nötigen Dokumente dafür schnell zukommen zu lassen.

Zu den Aufgaben der jeweiligen Personen würde gehören:

- Durchführen von Beratungen für Kunden
- Verifizieren der Identität und zugehörige Nachweise des Antrags des Kunden
- Prüfen des Antrags
- Koordinieren des Prozessablaufs und des Prozessstatus des Antrags mit beteiligten Behörden
- Bei Bedarf einholen von Vorsprachen des Kunden
- Ausstellen von Nachweisen

Sachbearbeiter in der beteiligten Behörde

Diejenigen Personen der am Antragsprozess beteiligten Behörden, die bei Teil- und Abstimmungsprüfungen herangezogen werden. Dies können bspw. Sachbearbeiter aus der Bundeagentur für Arbeit, Jobcenter, Gesundheitsbehörden, Integrationsämtern oder Sicherheitsbehörden sein. Ziel ist es, den zugewiesenen Teil des Antrags vom Kunden und die Abstimmung zu prüfen sowie das Ergebnis an die Ausländerbehörde zu übermitteln.

Zu den Aufgaben der jeweiligen Personen würde gehören:

- Koordinieren des Prozessablaufs und des Prozessstatus des Antrags mit beteiligten Behörden
- Prüfen des Teilantrags und/oder der Abstimmungsgrundlage
- Verifizieren der Identität und zugehörige Nachweise des Teil-Antrags des Kunden

Es fällt auf, dass die Beschreibung der Aufgaben auch auf die derzeitige papierbasierte Anwendung übertragbar wäre. Die Art und Weise wie diese Aufgaben mit digitalen Nachweisen ausgeführt werden würden, können sich damit an schon vorhandene und bekannte Handlungsweisen orientieren. Damit könnte man die Akteure bei der digitalen Transformation von Verwaltungsleistungen unterstützen.

Hauptanforderungen an einen idealen Ablauf

Wenn es sich um einen idealen Ablauf handelt, werden auch Erwartungen der Akteure an solch einen Prozess gestellt. Mit der Einführung von verifizierbaren digitalen Nachweisen für Personen, lassen sich folgende wesentliche Anforderungen formulieren:

Sachbearbeiter der Ausländerbehörde und beteiligter Behörden:

- „Ich muss sichergehen dass die Daten dieser Person zugehörig sind“, „Ich muss sichergehen, dass diese Institution/Person, die die Richtigkeit und Vollständigkeit der Daten bestätigt hat und dafür verantwortbar gemacht werden kann„
- „Ich muss sichergehen, dass die beteiligten Behörden mit ihren Aufgaben anfangen können, wenn der Prüfantragsstatus es erfordert“
- Ich muss medienbruchfrei arbeiten können“

Kunde:

- „Ich muss meine Nachweise und Dokumente besitzen und nutzen können, wie ich möchte“
- „Ich muss mitbekommen, wer, wann und was von meinen Daten anfragt und abruft“

Nachweisaussteller:

- „Ich muss die Angaben und Daten, die ich ausstelle gründlich überprüfen“
- „Ich muss ermöglichen, dass ich und die Nachweise für andere Prüfende vertrauenswürdig sind“

Es geht bei der Gestaltung des Ablaufs also vor allem darum, Sicherheit an die Sachbearbeiter zu vermitteln, als auch eine gewisse Transparenz für Kunden und Sachbearbeiter zu ermöglichen.

Attribute als weitere Anforderungen an das Angebot

sicher

Nur die jeweilige Person besitzt ihre Nachweisdaten und digitalen Identitäten

Die Verantwortung für die Richtigkeit und Gültigkeit der Nachweise ist manipulationsresistent dokumentiert

Informationen und Daten werden nur zwischen den Personen und Institutionen ausgetauscht, die sie benötigen

vertrauenswürdig

Die geteilten Aussagen und Informationen sind über eindeutige Vertrauensanker der Aussteller verifizierbar

Vertrauenswürdige Akteure sind als solche erkennbar

Die getroffenen Aussagen sind richtig und gültig

Es gibt eine gemeinsame Wahrheit

entgegenkommend

Die Informationen aus Nachweisen sind so aufbereitet, dass sie direkt zur Bearbeitung nutzbar sind

So wenig Schritte wie möglich, so viel rechtlich wie nötig

Die benötigte Zeit für die wesentlichen Prozessschritte wird geschätzt

rational

Die Datensouveränität wird in der föderalen Struktur respektiert

Die Systemanbindung an die Praxis folgt verständlichen Nutzungsmustern

Die Handhabung mit der gemeinsamen Basis ist über die jeweiligen Bestandsysteme möglich

kooperativ

Der Austausch von verlässlichen Informationen wird gefördert

Die Verantwortung in der jeweiligen Rolle wird übernommen

Kein Gegeneinander, sondern fördern eines Miteinanders zum gemeinsamen Ziel

zielstrebig

Der Prozess zur Klärung der Teilhabe des Menschens an der Gesellschaft ist das oberste Ziel

"Ich muss wissen was meine Aufgabe ist und wann ich anfangen kann"

In der Bedienung: Mit wenigen Schritten zum Ziel

transparent

"Das was ich mache ist richtig"

Ein offenes Ökosystem

"Ich kann deine Handlung nachvollziehen"

Abbildung 10: Attribute als weitere Anforderungen an das Angebot

Struktur des Gesamtablaufs

Um ein System für digitale verifizierbare Nachweise zu schaffen, muss sich auch Gedanken um die Struktur zwischen allen beteiligten Entitäten gemacht werden. Im Kontext von ausländerrechtlichen Anliegen läuft dies derzeit über den schon erwähnten Ansatz des „One Stop Governments“. Dabei überträgt die antragsstellende Person die Anträge und ihre Nachweise und Dokumente an den Sachbearbeiter in der Ausländerbehörde, welcher sich dann darum kümmern muss die Nachweise und Dokumente zu verifizieren, die Anträge zu prüfen und bei Beteiligung anderer Behörden den Antragsstatus mit Beschlüssen als auch die Dokumente des Kunden an die Behörden sicher weiterzugeben.

Das Rollenkonzept von SSI kann dabei unterstützen, da die Nachweisaussteller ihren Vertrauensanker der Signatur auf den Nachweisen für die Ausländerbehörde öffentlich verankern und der Kunde sein verifizierbaren Nachweisdaten mit dem Antrag zum Sachbearbeiter der Ausländerbehörde (ABH) zustellen kann. Der Sachbearbeiter kann dann über die Schlüssel im hinterlegten Vertrauensanker prüfen, ob die Daten dem Kunden zugehörig sind, richtig, vollständig und gültig sind und welcher Aussteller dafür die Verantwortung übernimmt, ohne den Aussteller zwingend kontaktieren zu müssen.

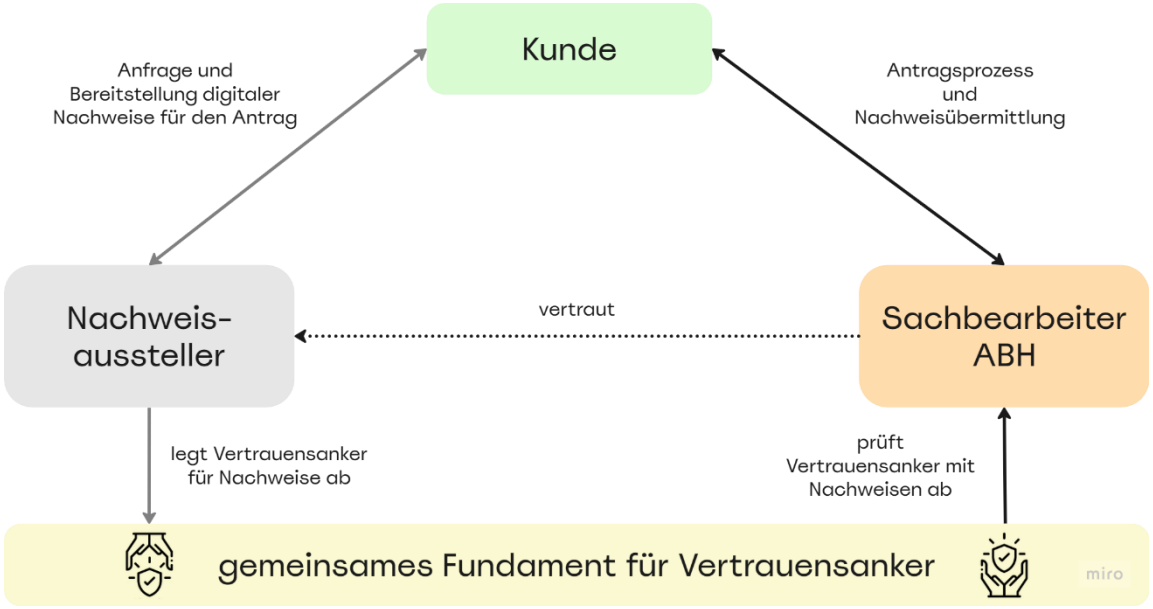


Abbildung 11: Trust Triangle innerhalb der Antragsstellung und Verifikation der Nachweise

Aber was passiert danach? Wie werden der Antrag und die Dokumente vom Kunden unter den Behörden bearbeitet? Entsteht nicht wieder die Blackbox ab der Ausländerbehörde?

Überträgt man diese Struktur des „One Stop Governments“ in das Digitale, wird dieselbe Herausforderung des Dokumentaustauschs zwischen den Behörden auch mitübertragen. Auch wenn es erstmals für den Kunden einfacher erscheint, die eigenen Daten des Antrags an eine Stelle zu übermitteln, bleibt für ihn weiterhin unklar, welche weiteren Behörden Zugriff auf diese Daten haben.

Auch entsteht das Risiko eines Medienbruchs bei der Bearbeitung der Anträge aus Seiten des Sachbearbeiters, da dieser sowohl Beschlüsse im Antrag als auch zugehörige Dokumente des Kunden an die beteiligten Behörden sicher weiterleiten muss. Und bevor dafür stetig einzelne Datenaustausch-Integrationen zwischen den Entitäten aufgebaut werden (Tobin, 2021), oder noch bei postalischem Papierversand verblieben wird [1], sollte man den Aufbau einer Struktur in Erwägung ziehen, die eine einzige verifizierbare Datenquelle benötigt – und zwar den Kunden selbst.

1: Auch wenn das Antragsverfahren bei Behörden für Kunden digitalisiert wird, muss vor allem darauf geachtet werden, wie der gesamte Ablauf behördenintern noch weitergeht. Eine geäußerte Kritik ist dabei, dass der digitale Prozess nicht etwa den gesamten analogen Prozess ablöst, sondern kurz vor dem Ziel endet (Umweltbundesamt, 2023)

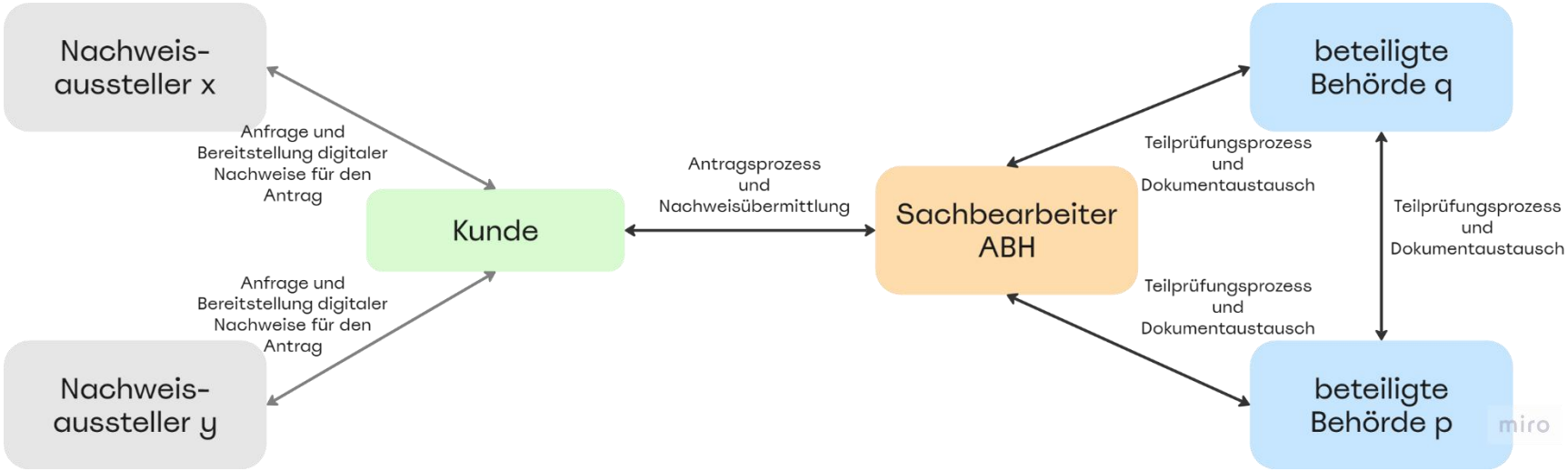


Abbildung 12: Struktur des Gesamtablaufs anhand dem „One Stop Government“-Ansatzes

Die “Citizen is now the API”-Struktur würde damit die ansprechbare Quelle für personenbezogene Daten in diesem Szenario beim Kunden selbst sehen. Jeder Abgriff von Daten zur Identität der Person müsste bei ihr selbst angefragt und von ihr zugestimmt werden. Das würde nicht nur die Transparenz für die Nutzung der eigenen Daten beim Kunden einführen, sondern auch eine gewisse Transparenz für zwischenbehördliche Vorgänge schaffen. Die jeweilige beteiligte Behörde fragt zum entsprechenden Zeitpunkt die Daten des Kunden ab, die sie auch tatsächlich für die Bearbeitung des Teil-Antrags oder Abstimmungsprüfung benötigen. Die Datensouveränität würde damit beim Kunden liegen. Sachbearbeiter der Ausländerbehörde müssten nicht nochmal die Daten des Kunden für den Dokumentaustausch aufbereiten und ausgestellte Nachweise können mehrmals genutzt werden. Zwischen den Behörden kann sich nun darauf fokussiert werden, wie der Antragsprozess koordiniert, Prüfaufgaben bestimmt und der Prozessstatus des Antrags geteilt wird.

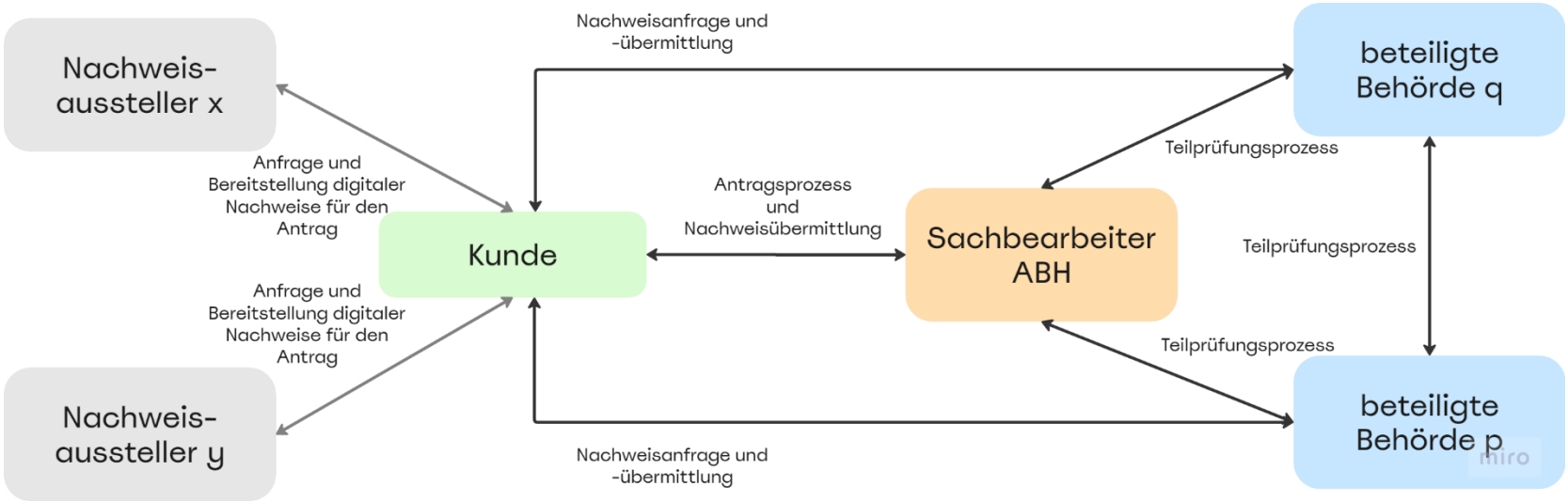


Abbildung 13: Struktur des Gesamtablaufs anhand der „Citizen is now the API“-Struktur

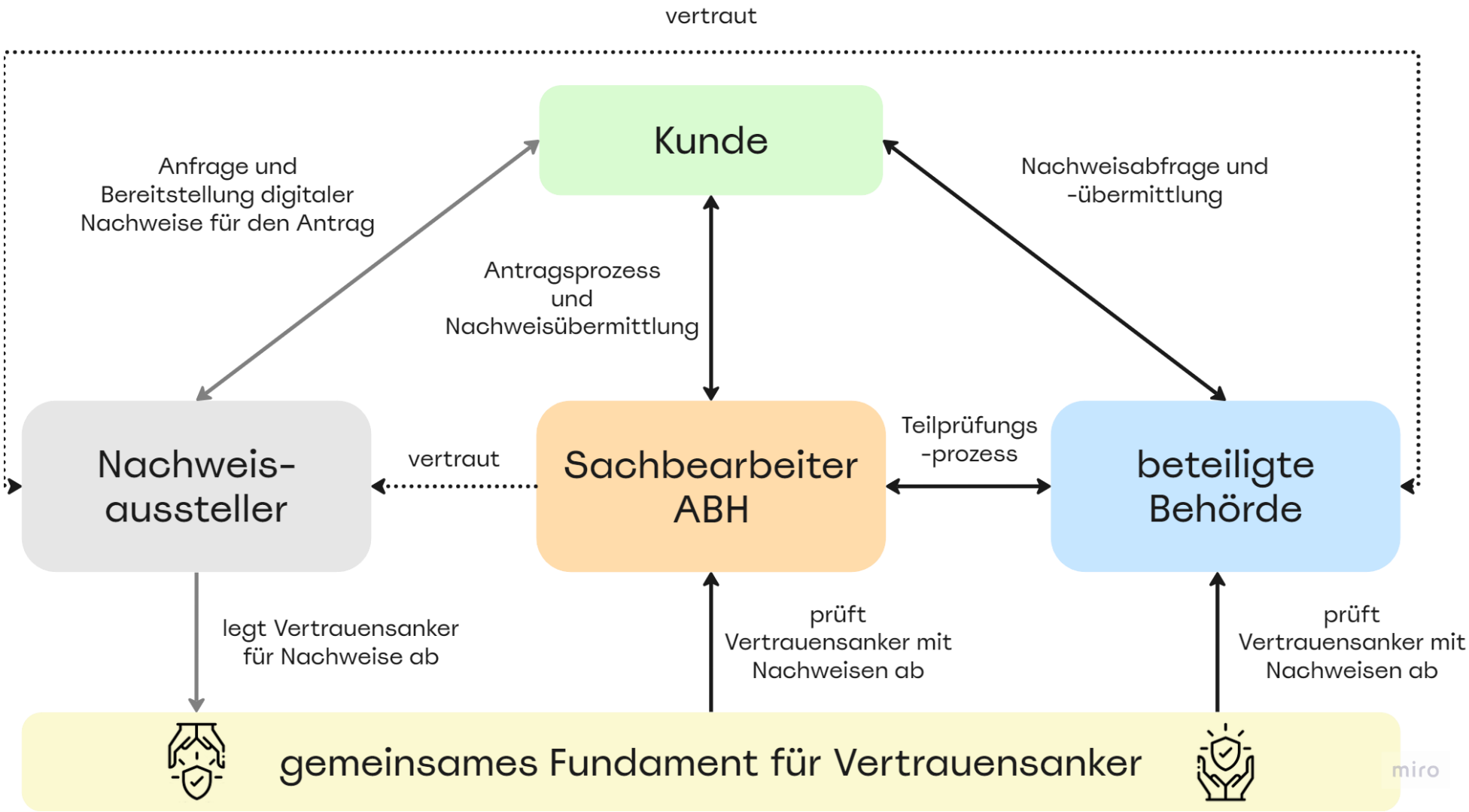


Abbildung 14: Erweitertes Trust Triangle für den gesamten Antragsprozess aus Sicht des Kunden

Eine der Erkenntnisse zu SSI war auch, dass es den Behörden selbst dabei helfen kann, Verwaltungsdienstleistungen anderer Behörden zu beantragen und den Informationsabruf zu beschleunigen (Biedermann et al., 2023). Dabei könnten die Ausländerbehörden, bzw. deren Sachbearbeiter, selbst auch als Issuer und Holder ihrer Antragsbeschlüsse und Prüfergebnisse fungieren und diese in einem verifizierbaren Prozessstatus für beteiligte Behörden zur Verfügung stellen. Die beteiligten Behörden können dann verifizieren, ob der Prozessstatus gültig ist, welche Institution für die Gültigkeit verantwortbar ist und bei welchen Service-Endpunkten sie die benötigten Dokumente und Daten für ihre Aufgabe anfragen sollen.

Damit kann auch das Bedürfnis der Behörden, die eigene Souveränität über Verfahren und die Verwaltung von Daten zu bewahren (Amend et al., 2023), unterstützt werden. Es kann aber sein, dass sich das Fundament für die Vertrauensanker zum Prozessstatus von derjenigen für die Nachweisaussteller des Kunden unterscheidet, da die Abstimmungs- und Teilprüfungen nur zwischenbehördlich ablaufen.

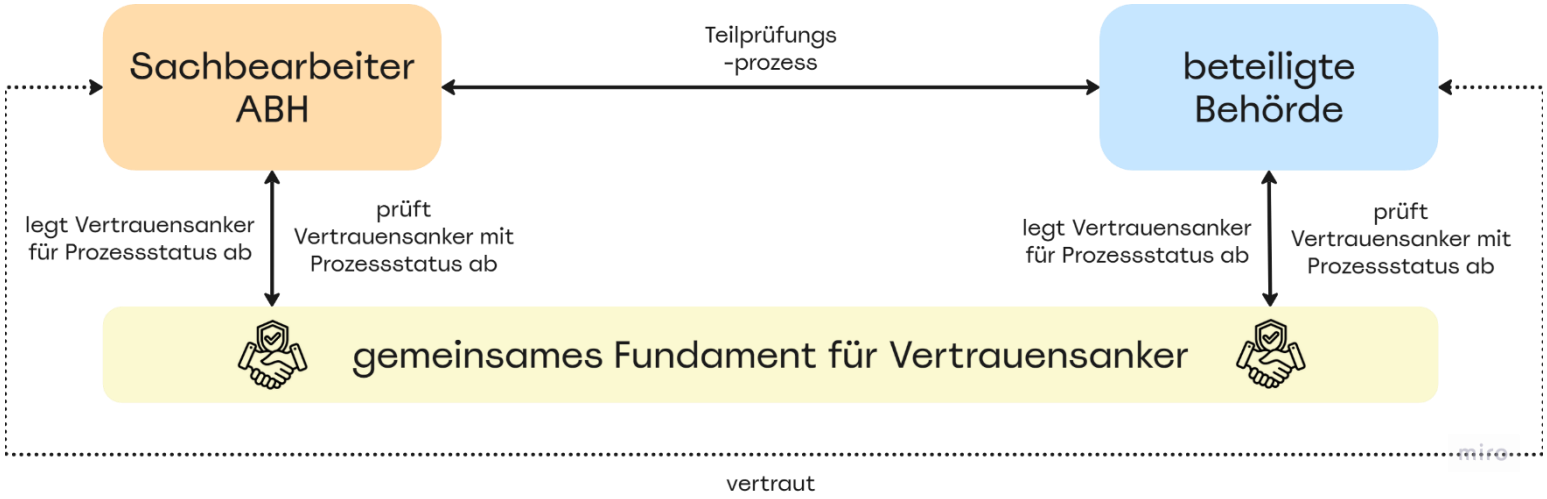


Abbildung 15: Erweitertes Vertrauensverhältnis für den Teilprüfprozess in Phase 3

Wenn der Prüfungs- und Abstimmungsprozess abgeschlossen ist und das Ergebnis des Antrags zwischenbehördlich feststeht, wird es Zeit dieses Ergebnis an den Kunden zu vermitteln. Abhängig davon, was der Inhalt des Antrags ist, wird beispielsweise ein Dokument über den Aufenthaltstitel verlängert oder neu ausgestellt. Dabei wird der Sachbearbeiter in der Ausländerbehörde (oder ggf. eine andere ausstellende Institution), nun als Vertreter der Behörde Issuer des digitalen Nachweises. Dabei wird der Kunde zur Ergebnisabfrage angefragt und erhält damit seinen digitalen Nachweis, den er nun bei sich abspeichert. Diesen kann er jetzt beliebig für sich einsetzten und verifizieren lassen: ob beim Arbeitgeber, Wohnungsgeber, für weitere behördliche Anträge oder Freizeitangebote. Der Kreislauf der Nachweis-Verifikation kann nun in vielen Bereichen von vorne beginnen.

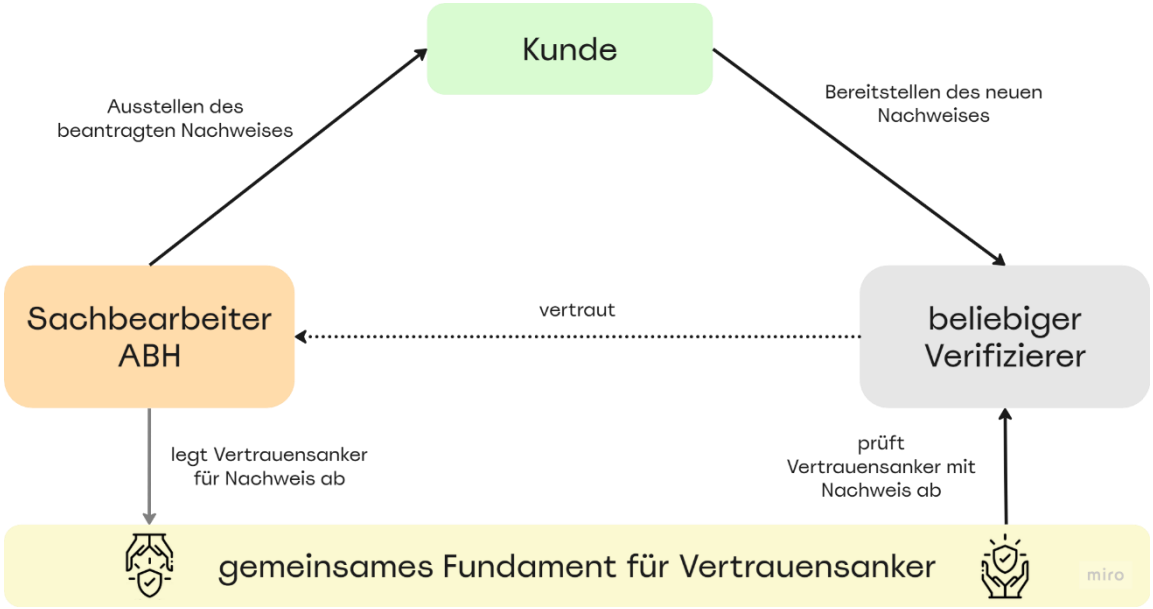


Abbildung 16: Trust Triangle nach Ausstellung der Nachweise von der Ausländerbehörde

Exkurs zu Phase 3 – ein ähnlicher konkreter Ansatz bei der BAMF

Das Ziel der Unterstützung der jeweiligen Behörden beim Überblick über den Prozessstatus von Anträgen wird derzeit vom FLORA-Projekt und deren bereits laufenden Assistenzsystem im Bereich Asyl verfolgt (Amend et. al, 2023). Diese ermöglicht eine zeitnahe und unveränderbare Verteilung von Prozessdaten und einheitlichem Informationsstand zwischen den an bestimmten Asylprozessen beteiligten Behörden (Amend et. al, 2022). Der Vertrauensanker ist dabei ein Hashwert, der wie ein Fingerabdruck den Prozessstatus kennzeichnet, und mit den Ausstellerdaten und „Zeigern“ [1] zur Datenabfrage auch auf einem geteilten unveränderbaren *Ledger* gelegt wird – beim FLORA-Projekt ist es eine Hyperledger Blockchain (Amend et. al, 2022). Bestehende behördeninterne IT-Systeme werden dabei vom Projekt nicht abgelöst, sondern im Sinne einer „technologischen Klammer“ verbunden und die föderale Struktur harmonisiert (Amend et. al, 2022). An der Oberfläche der jeweiligen Sachbearbeiter in den Behörden werden die für sie bearbeitbaren Anträge aufgelistet, die schon mit den angefragten Daten und Daten aus eigenen Bestandsystemen angereichert wurden. Eine direkte Bearbeitung der Teilanträge ist dann mit allen benötigen Dokumenten möglich (Amend et. al, 2022). Solch eine ähnliche Struktur könnte auch in der Ausländerbehörde für den behördeninternen Austausch in Phase 3 übernommen werden, wobei die „Zeiger“ aber dann auf den Endpunkt zur Datenabfrage beim Antragskunden verweisen.

Das Projekt erweist sich als erfolgreich und wurde nach einer Pilotierung in Dresden an weitere Standorte in Sachen und Brandenburg angeschlossen - ein Anschluss in Rhein-Land Pfalz und konkrete Planungen für Baden-Württemberg und Nordrhein-Westfalen stehen in Vorbereitung (Amend et. al, 2023; Biselli, 2023); Laut einer Anfrage von netzpolitik.org wurden für das Projekt seit 2018 bisher 18 Millionen Euro ausgegeben, wobei die BAMF beim jährlichen Betrieb mit etwa 100.000 Euro rechnet (Biselli, 2023). Des Weiteren wurde vom BAMF neben den Ausbaustufen des FLORA-Projektes vorantreibende Aktivitäten im Bereich von SSI angekündigt (Amend et. al, 2023). SSI wurde bei den Erkenntnissen im Proof-Of-Concept des Projektes im Ausblick angeschnitten, aber auch da wurde verwiesen, dass ein solches ganzheitliches System mit erheblichem Mehraufwand in der Konzeption und Implementierung verbunden wäre und es vermutlich aus mehrere interoperablen Blockchains bestehen würde (Jannik et. al, 2019).

1: Eine Analogie für einen Ressource Locator für Daten innerhalb der Bestandsysteme der jeweiligen Behörde. Über diesen können die Daten zum Antrag in einer Adapterschicht außerhalb der Blockchain beim Speicherort der jeweiligen Behörde angefragt und bei entsprechender Berechtigung zur Verfügung gestellt werden (Amend et. al, 2022; Jannik et. al, 2019)

Gesamtablauf des Angebots

Im Folgenden ist ein möglicher Gesamtablauf anhand des groben Ablaufs mit allen Akteuren aus dem primären Blickwinkel des Sachbearbeiters formuliert. Dieser wurde auch genutzt, um die verschiedenen benötigen digitalen Medien und Systeme an den Schnittstellen zu identifizieren (in schwarz und grau dargestellt). Als Rahmenbedingung für den Ablauf ist gegeben:

- die Nachweisaussteller haben dem Kunden die digitalen Nachweise überreicht und die Vertrauensanker für diese im Fundament gesetzt
- Nachweisausteller als auch der Sachbearbeiter in der Ausländerbehörde (ABH) und beteiligter Behörde sind gegenüber ihrer jeweiligen Institution und deren verwendeter Anwendung zum Ausstellen von Vertrauensankern und Nachweisen, persönlich authentifiziert und autorisiert worden

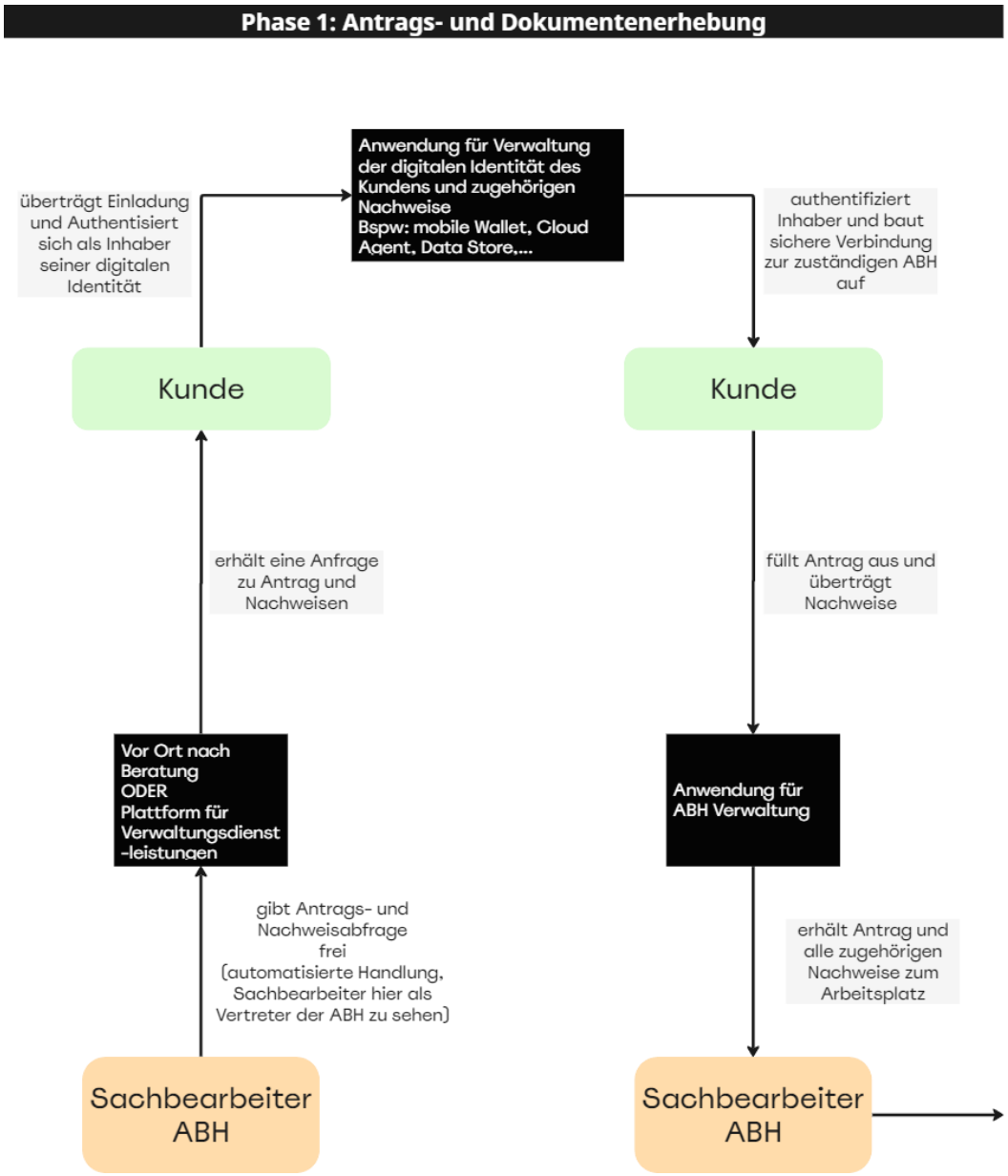
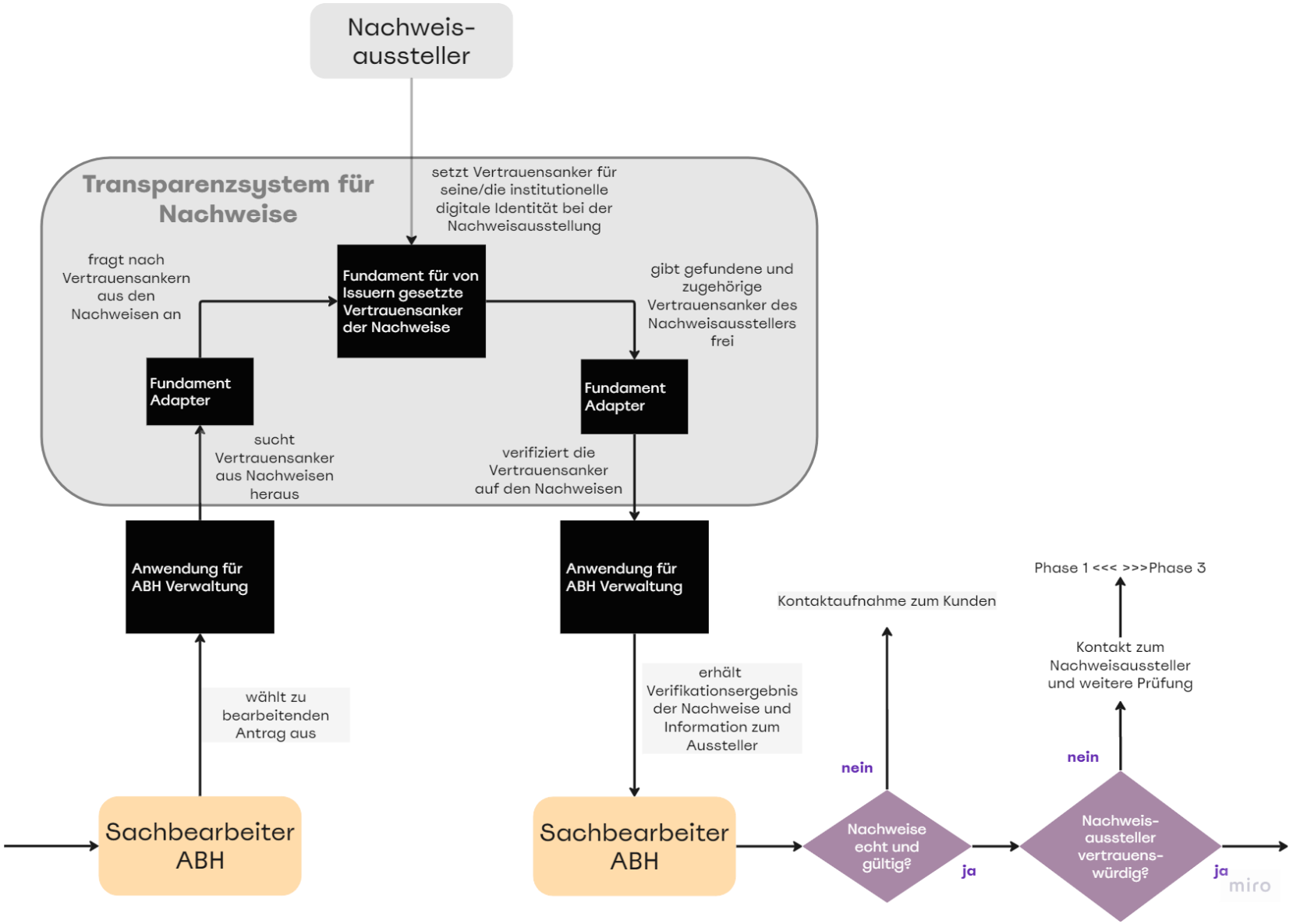
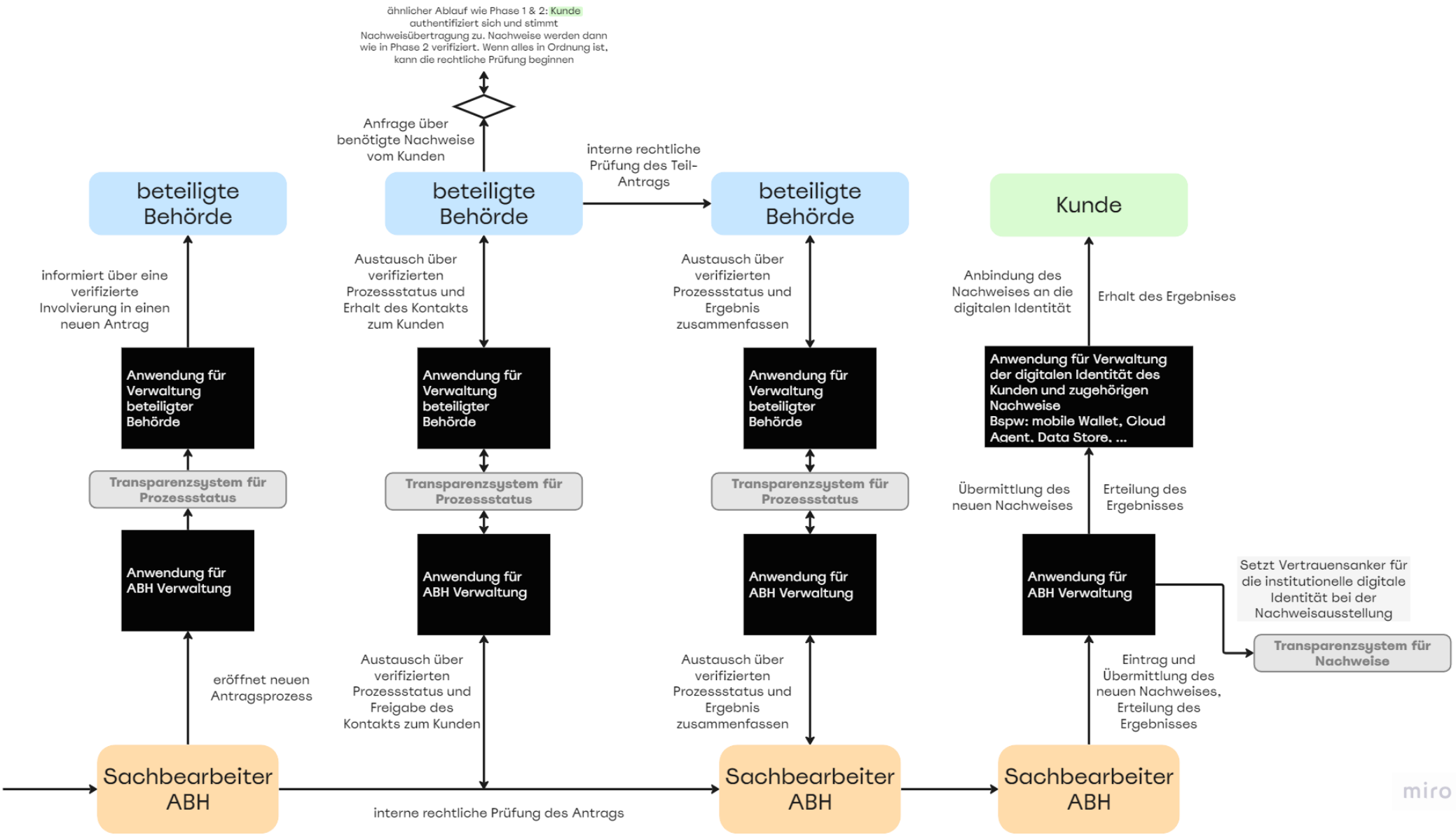


Abbildung 17: Gesamtablauf des Angebots

Phase 2: Verifikation der Dokumente



Phase 3: Prüfung des Antrags



Rahmenbedingung Sicherheit – wer wird wie verantwortbar gemacht?

Wenn es darum geht, als Sachbearbeiter digitale Nachweise zu überprüfen, muss bekannt sein, für wen diese ausgestellt wurden und vor allem wer diese Daten überprüft und ausgestellt hat. Dafür müssen für die jeweiligen Inhaber der Nachweise als auch die Aussteller der Nachweise und für deren Vertrauensanker einzigartige Identifikatoren eingesetzt werden, den nur sie besitzen können. Es muss deutlich werden, dass der Identifikator tatsächlich nur von dieser Person oder Institution kommen kann und niemand anderes sich dahinter verbirgt.

Was eine Person ein Leben lang besitzt, sind biometrisch eindeutige Merkmale, wie beispielsweise Fingerabdrücke. Diese sind unmittelbar an die Person gebunden und erlauben eine eindeutige Erkennung einer Person. So wurden diese auch über Jahrhunderte von verschiedenen Kulturen genutzt, um Verträge zu authentifizieren (BSI, o.D.). Institutionen haben aber keine Fingerabdrücke und Fingerabdrücke von Einzelpersonen oder Mitarbeitern als bildliche Signatur ohne weitere Informationen für digitale Nachweise zu verwenden ist auch nicht zielführend.

Im Digitalen benötigt man etwas anderes, was den Fingerabdruck einer Person als auch Institution repräsentieren kann. Ein allgemeingültiger Standard, der dieselbe Aussagekraft hat wie ein menschlicher Fingerabdruck. Aus dem technischen Blickwinkel kann dies der globale W3C-Standard der dezentralisierten Identifikatoren (DIDs) erfüllen, da diese einzigartig sind und kryptografisch an die jeweilige Person/Institution gebunden sind und nur diese sie besitzen.

Aber in ihrer reinen Form geben sie einem menschlichen Betrachter keine Auskunft über das jeweilige Gegenüber. Während das für nicht an der Interaktion beteiligte Parteien von großem Vorteil ist, wird das den Anforderungen des Sachbearbeiters als auch denen des Kunden bei Nachweisabfrage nicht gerecht. Wie weiß man, dass es sich tatsächlich um vertrauliche Nachweisaussteller oder die Person in den Nachweisen handelt?

Example of an Verifiable Credential – W3C Specification

```
{
 "@context": [
   "https://www.w3.org/2018/credentials/v1",
   "https://essif.europa.eu/schemas/vc/2020/v1"
 ],
 "id": "https://essif.europa.eu/tsr/53",
 "type": [
   "VerifiableCredential",
   "VerifiableAttestation",
   "VerifiableAccreditation",
   "DiplomaVerifiableAccreditation"
 ],
 "issuer": "did:ebsi:zsSgDXeYPhZ3AuKhTFneDf1",
 "issuanceDate": "2020-06-22T14:11:44Z",
 "credentialSubject": {
   "id": "did:ebsi:zDnaeSGrMFB9kCxnPYWaeMrRyun2HLVHjDNUf76ccy4ZfHU24",

   (....)
```

DID of the Issuer

DID of the Holder

Abbildung 18: Beispiele für DIDs auf der European Blockchain Infrastructure (Europäische Kommission, 2022)

Anforderung an die Governance im System

Nun ist die Frage nach der Governance im System gestellt, also unter welchen Rahmenbedingungen und Regeln dieses System Transparenz für Vertrauensaufbau schafft. Im zwischenbehördlichen Bereich existieren bereits Instanzen, die festlegen wer bspw. eine Meldebehörde, ein Sozialamt, eine Sicherheitsbehörde, ein Jobcenter, eine Auslandsvertretung oder allgemein eine staatliche Dienststelle ist. Die Verknüpfung der einzigartigen DID zu der jeweiligen Behörde oder anderen staatlichen Dienststelle müsste von diesen oberen Instanzen in einem Register geführt werden und bei der Prüfung vom System abgeglichen werden (Young, 2022). Auch die Registerführung für vertrauliche DIDs von privatwirtschaftlichen oder auch zivilgesellschaftlichen Akteuren wie Arbeitsgeber und Wohnungsgeber kann von höher gelegten prüfenden Instanzen für den jeweiligen Aufgabenbereich übernommen werden – diese Aussteller von Nachweisen müssen sich ja auch jetzt schon für ihre Rolle bei einer Stelle anmelden und ihre Vertraulichkeit bestätigen. Diese sollten anhand der bestehenden föderalen Strukturen und etablierten Vertrauensverhältnissen in Ländern und Kommunen gefunden werden und damit wesentlicher Partner für die zentral-dezentrale Koordination im System sein. Es könnten auch Voting Mechanismen für die Bestimmung der Vertrauenswürdigkeit unter Nachweisausstellern und Verifizierenden eingesetzt werden, um Wissen aus lokalen Beziehungen zu verwenden. Wie im Researchteil schon besprochen, dürfte es jedoch keine Möglichkeit zur Manipulation des Votings geben. Es werden somit Services für das Vertrauen benötigt, damit das System als gemeinsame Wahrheit genutzt werden kann. Die genauere Ausgestaltung der Governance müsste weiter anhand der eIDAS-Verordnung und des Vertrauensdienstleistergesetzes in Deutschland durchgeführt werden (BSI, o.D.).

Für den Anwendungsfall der Ausländerbehörde, die definitiv vertrauenswürdige Nachweisaussteller benötigt, wäre ein zugangsbeschränktes öffentliches System (public permissioned) (Bundestag und Beck, 2018) für das Fundament der Vertrauensanker eher geeignet. Das bedeutet, dass die Vertrauensanker der Nachweisaussteller als Beleg für ihre Verantwortung öffentlich zugänglich sind, die Nachweisaussteller die Vertrauensanker jedoch nur setzen können, wenn sie von anderen als vertrauenswürdig bestätigt wurden und dazu berechtigt sind.

Auch muss für die jeweiligen nachweisausstellenden Institutionen intern erkenntlich sein, welcher Mitarbeiter im Namen der Institution den Vertrauensanker gesetzt hat und damit die Verantwortung für die Richtigkeit der ausgestellten Nachweise übernimmt. Dies kann beispielsweise durch die Verknüpfung seiner digitalen Teilidentität für die Arbeit sein.

Anforderungen an die Authentisierung und Umstände für die digitale Identität

Zum anderen ist nun die Frage, wie sich Personen ihren digitalen Identitäten authentisieren können und sowohl den eindeutigen Besitz der DID und der Nachweise bezeugen können.

Diese Frage lässt sich im Bezug auf die Schnittstelle zum Nutzer der jeweiligen digitalen Identität einordnen – der Authentifikation mit seinem digitalen Ich. Abhängig davon, wo die Person ihre Daten speichert, verwaltet und von wo sie mit anderen in Interaktion tritt (Software, App, Cloud-Agent, eigener Server), wird ein Authentifikator benötigt. Authentisieren müsste man sich dann mit einem einzigartigen Merkmal, wie bspw. der Schnittstelle seines Körpers (Fingerabdruck, Handvenen, Gesicht oder genetischer Zusammensetzung) (BSI, o.D). Auch können eindeutige physische Nachweise mit biometrischen Daten genutzt werden, wie die e-ID und e-AT, um die Kontrolle über die digitale Identität für das Szenario Ausländerbehörde nachzuweisen. Die derzeitige AusweisApp für das mobile Endgerät ist genau solch ein Authentifikator für diese Ausweise (BSI, 2023). Jedoch verfügt nicht jeder Antragsstellende über einen elektronischen Aufenthaltstitel – diese werden ja erst bei der Ausländerbehörde beantragt. Eine mögliche Lösung wäre erstmals auf biometrische Authentisierung zu setzen, möglicherweise gekoppelt mit einem PIN, um eine digitale Identität für die Interaktion mit der Behörde zu nutzen. Andererseits könnte auch ein Model wie in Estland eingeführt werden, wobei eine Authentifizierungs-Karte im Rahmen einer E-Residency für jeden Menschen global angeboten wird. Dabei wird zunächst die Identität mit biometrischen Merkmalen gesichert und anschließend eine Chip-Karte per Post versendet, die das digitale Authentifizieren in der dazugehörigen Software für alle Leistungen innerhalb Estlands ermöglicht (e-estonia, 2024). Ob die Authentisierung nun mit seiner unmittelbaren Biometrie oder den Besitz biometrischen Chipkarten erfolgt - die Anforderung muss sein, dass diese Merkmale einzigartig sind und nur in Kombination mit Wissen, wie bspw. PINs den Zugang zur Identität ermöglichen. Auch wenn ein Angreifer eines dieser Merkmale stiehlt oder repliziert (CCC, o.D.), ist der Zugang zur digitalen Identität schwer möglich. Im Falle von behördlichen Leistungen müssen die DIDs, als auch die Nachweise auf den DIDs, nur von derjenigen Person verwendet werden, für die sie bestimmt sind. D.h auch wenn die hoheitlichen Nachweise für eine DID ausgestellt wurden, dürfen sie nur unter denjenigen DIDs verteilt werden, die im Besitz der tatsächlichen Person liegen. Deshalb muss eine starke Authentisierung als Anforderung an die Technik gestellt werden.

Eine weitere Anforderung für die technische Umsetzung ist dabei, dass diese Authentifikation nur in der eigenen Umgebung stattfindet. Die digitale Identität ist letztendlich Teil von uns, die Technologie, die wir um uns haben ist ein erweiterter Teil von uns – daher sollten wir diese Technologien im Umkehrschluss auch besitzen. Aus diesem Grund ist es wichtig, wenn Software oder Apps zur Authentifikation und dem Verbindungsaufbau für Interaktionen eingesetzt werden, sie nur in Erweiterungen von einem selbst laufen – also nur auf Endgeräten, nur auf der Cloud und nur auf Servern in eigenem Besitz. Beispielsweise auf *decentralized web nodes* (DWNs) (Decentralized Identity Foundation, 2023) oder eigenen Servern, die die EU uns zum eigenen Besitz stellt. Auch müssen diese Anwendungen Open-Source sein, damit der Quellcode transparent, frei und für alle verfügbar ist. Wenn ein Verbindungsaufbau mit dieser digitalen Identität zu einer anderen Partei stattfindet, sei es der Sachbearbeiter in der Behörde, dem Nachweisaussteller, die Universität oder die Arbeitststelle oder auch Freunde und

Familie, muss dies Peer-to-Peer stattfinden. Vor allem wenn hoheitliche Nachweise über die Identität und zum Ausweisen übertragen werden, sollten sie auch nur bei demjenigen ankommen, für den diese bestimmt sind. Die Decentralized Identity Foundation unter Linux arbeitet derzeit daran, dass das „DIDComm Messaging“ Kommunikationsprotokoll für diese Anforderung zum Standard wird (Begleitforschung, 2023).

Werden diese Anforderungen erfüllt, so kann innerhalb eines solchen Systems von einem digitalen Fingerabdruck gesprochen werden – ein eindeutiger Identifikator in der digitalen Welt, über den man beim Austausch relevante andere als auch sich selbst identifizieren.

Anforderung an das Fundament für Vertrauensanker

Es wurde bereits im Abschnitt der Anforderung an die Governance erwähnt, dass voraussichtlich ein öffentlich zugangsbeschränktes Fundament nötig wird.

Die Vertrauensanker sind dabei die öffentlichen Schlüssel der Nachweisaussteller, mit denen die Nachweise signiert werden, gemäß asymmetrischer Verschlüsselungsverfahren, wie im Researchsteil diskutiert. Nur die DIDs und DID-Dokumente mit den enthaltenen öffentlichen Signaturschlüsseln der Nachweisaussteller werden in das Fundament verankert.

Das Fundament dafür muss manipulationssicher und ausfallsicher sein, sowie Transparenz für eine breite Palette von Akteuren bieten. Die Sachbearbeiter müssen sicherstellen, dass keine Änderungen am Nachweis vorgenommen wurden und dass der Nachweisaussteller für die Ausstellung verantwortlich gemacht werden kann. Für den zwischenbehördlichen Prozess muss der Status des Antrags für alle beteiligten Sachbearbeiter gesetzt und vertrauenswürdig sein. Die Verantwortung in der Entscheidung der jeweiligen Behörde muss unveränderbar dokumentiert werden. Dies bedeutet, dass die verankerten Schlüssel weder abgeändert noch gelöscht werden dürfen, und die Verantwortung nicht abgetreten werden darf - weder durch externe Parteien noch durch die Nachweisaussteller, Behörden oder den Staat selbst.

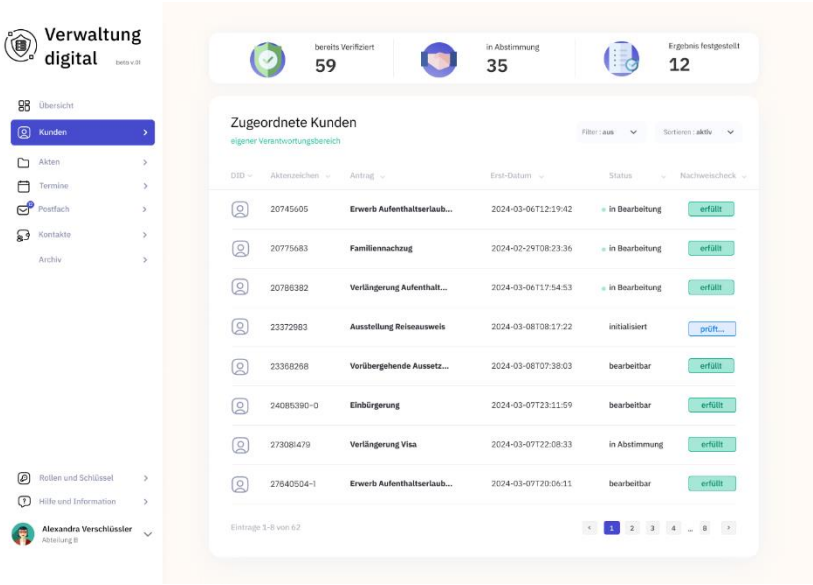
Das Fundament muss daher unveränderbar sein, verteilt existieren und nur durch dokumentierte und abgestimmte Änderungsbeschlüsse erweitert werden. Anhand dieser Anforderungen würde sich ein Datenregister auf Distributed Ledger Technologie wie eine Blockchain anbieten, um diese Schlüsseltransaktionen unveränderbar zu dokumentieren. Da das Datenregister zugangsbeschränkt wäre und die Knotenpunkte bekannt sind, könnte auch ein ökologischerer Konsensmechanismus in Form von Abstimmungen gefunden werden. Auf europäischer Ebene wird derzeit ein Ökosystem der European Blockchain Service Infrastructure (EBSI) ausgebaut (Bundesnetzagentur, 2024) und könnte für eine mögliche Anwendung in Betracht kommen. Hier muss jedoch eine ausführliche Prüfung der Governance-Anforderungen und Umstände für die digitale Identität durchgeführt werden.

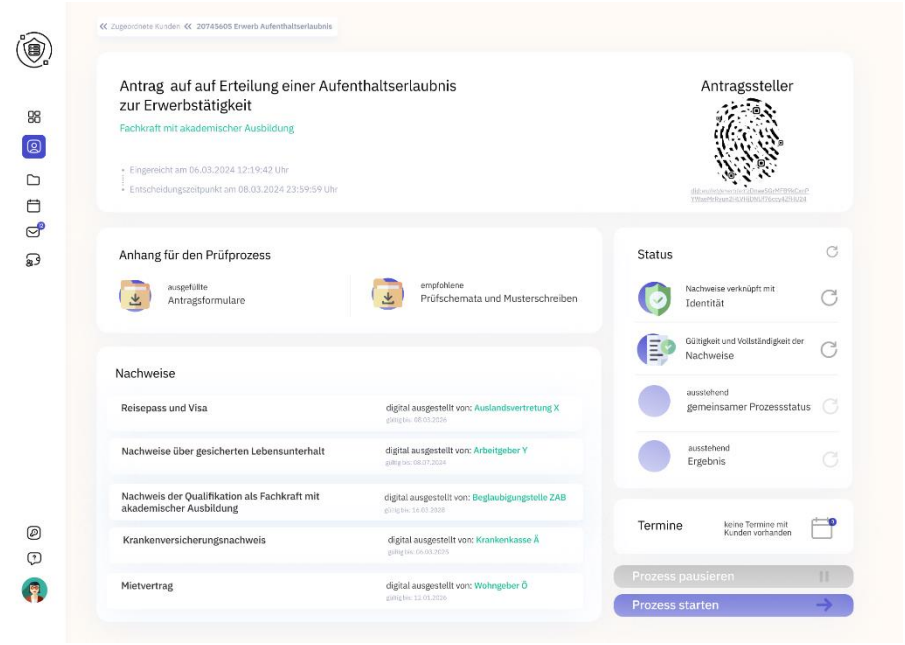
Es sollte auch eine Prüfung von Seiten wie dem Bundesamt für Sicherheit in der Informationstechnik (BSI) durchgeführt werden, um festzustellen, welche anderen unveränderbaren Datenregister für Schlüssel in diesem Anwendungsfall und seinen Anforderungen besser geeignet wären. Dabei sollte auch

geklärt werden, ob für jeden signierten Nachweis ein eigenes Schlüsselpaar erzeugt werden muss oder ob ein regelmäßiger dokumentierter Wechsel der Signaturschlüssel ausreicht.

Visualisierung der Verifikationsphase beim Sachbearbeiter

Im Folgenden wurde eine Visualisierung für das Näherbringen der Phase 2 des idealen Ablaufs angefertigt. Die Verifikation der Nachweise des Kunden läuft im Hintergrund ab und der Sachbearbeiter erhält letztendlich nur das Ergebnis. Anhand der Rahmenbedingungen für die Sicherheit muss diese dem Sachbearbeiter aber auch auf seiner Anwendungsoberfläche übermittelt werden. Wie gibt man dem Sachbearbeiter also die Sicherheit, dass das, was man tut richtig ist und die Identitätsdaten richtig sind? Wie macht man die Gestaltung der benötigten Informationen transparent, sodass es verstanden wird? Ein Vorschlag findet sich in den beiliegenden Screens einer möglichen Anwendung für die Ausländerbehörde.





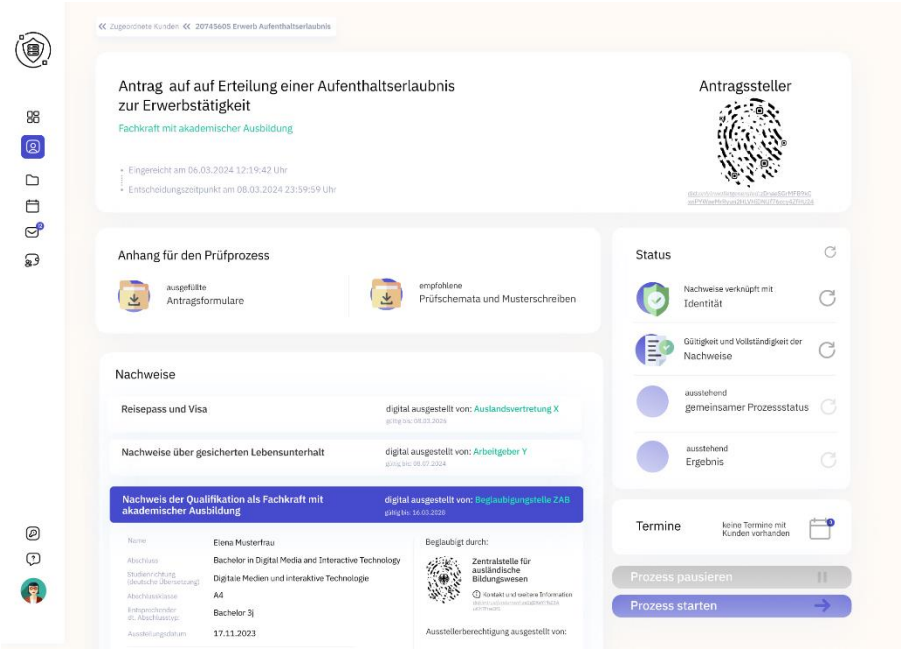


Abbildung 19: Screendesigns für die Oberfläche bei der Verifikationsphase

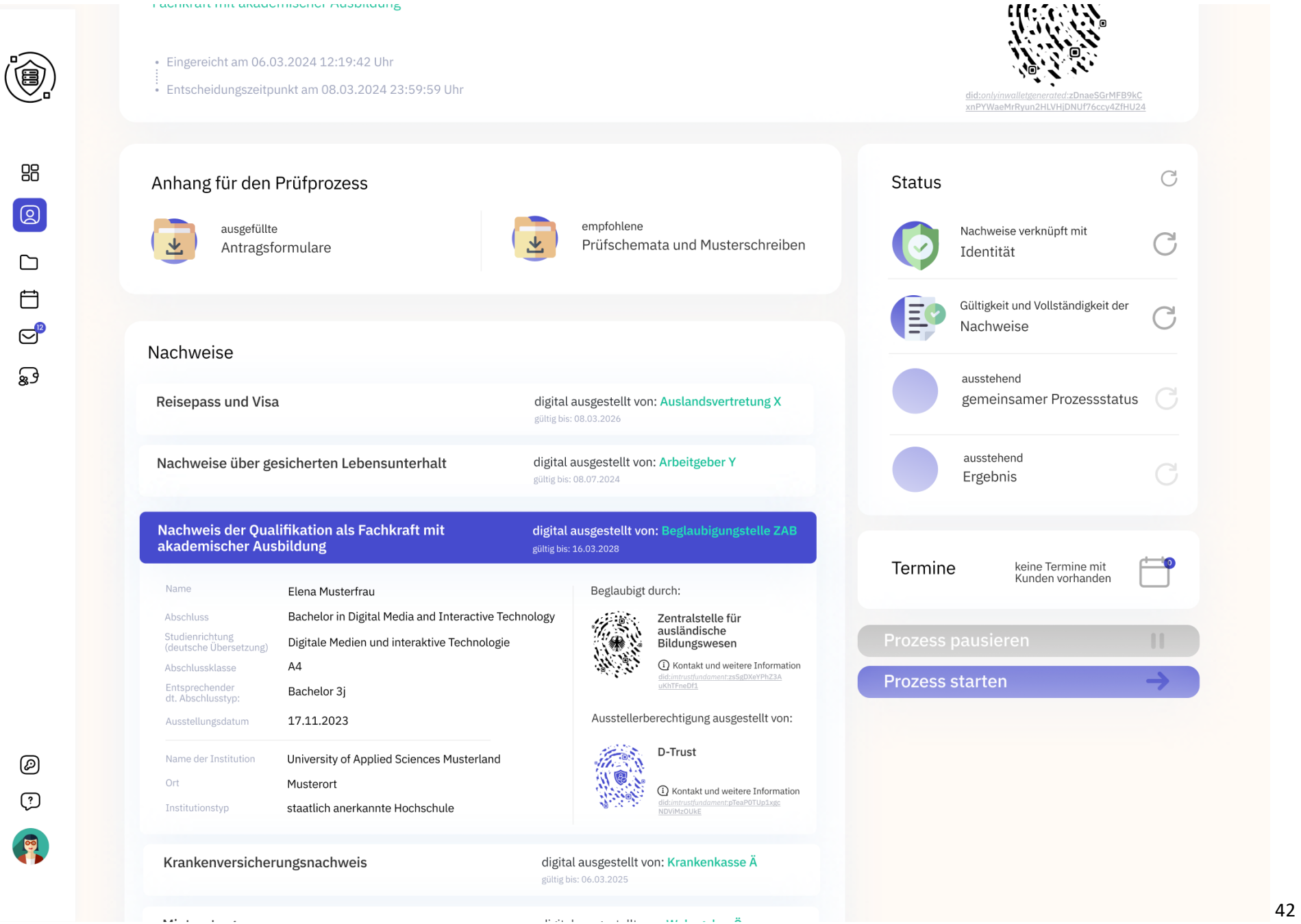


Abbildung 20: Screen bei geöffneten Nachweis des Kunden

Angelehnt an die Analogie des digitalen Fingerabdrucks werden Repräsentationen der einzigartigen DIDs angeboten. Diese fungieren wie eine bildliche Unterschrift der jeweiligen Institution oder Person im Besitz dieser DID, über die man weiteren Kontakt mit ihr aufnehmen kann – ob über die Anzeige in einem digitalen Format oder beim Verbinden vor Ort.

Angelehnt ist dieses Prinzip an QR-Codes, welche heutzutage bspw. auf Webseiten verweisen, Ticketdaten enthalten, Pakete identifizieren, Anträge kennzeichnen, Visadaten enthalten, WLAN-Zugänge herstellen und auch Menschen zueinander verbinden lassen. Dieser 1994 von der japanischen Firma Denso Wave entwickelte und patentierte Standard, ist weltweit kaum mehr wegzudenken und ist zu einem bekannten alltäglichen Artefakt geworden (Denso Wave, o.D.).

Menschen sind aber weder Tickets noch ihre Anträge. Wenn es um menschliches Identitätsmanagement geht, kann auch nach einer repräsentierenden Form dafür gesucht werden. Ein erster Vorschlag sind damit QR-Code angelehnte „Thumb Ports“, welche die persönliche oder institutionelle DID und das zugehörige DID-Document encodiert haben. Dies stellt einen Idee für einen abgeleiteten Standard dar, aber die tatsächliche Encodierungsstruktur bedarf weiterer Forschung.

Dabei können auch Thumb Ports von natürlichen Personen und der vertrauenswürdigen Rolle als Nachweisaussteller unterschieden werden. Letztere erhalten von ihrer jeweiligen Ausstellungsberechtigungsinstanz ein Emblem für ihren Bereich.

Abbildung 21: Beispiele für Thumb Ports

Fazit und weitere Schritte

Dies waren die erarbeiteten Rahmenbedingungen und Ansätze für einen idealen Ablauf in der Ausländerbehörde, anhand des dargelegten Wissens in der Arbeit. Abschließend lassen sich folgende Forderungen, Überlegungen, Bedenken und weitere Schritte für eine weitere Arbeit formulieren.

Zum Anwendungsfall Ausländerbehörde

Es ist erforderlich, dass rechtliche Anforderungen wie Schriftformerfordernisse mit eIDAS in Einklang gebracht werden, wobei elektronische Unterschriften den gleichen Stellenwert haben müssen. Es bedarf einer Aufstockung von Ressourcen und dem Ausbau von zwischenbehördlichen Netzwerken sowie einer Basisdigitalisierung in allen Kommunen. Das Angebot entspricht eher einem digitalen Rennen, obwohl noch nicht alle Kommunen digital Laufen können (Bundestag und Beck, 2018).

Das Projekt selbst kann keine konkrete Lösung darstellen, sondern einen Diskussionsansatz für ein mögliches Ideal. Um konkretere Konzepte für den Soll-Zustand in den jeweiligen Kommunen oder Bundesländern zu entwickeln, ist ein tieferer Einblick in die Praxis und Organisationsforschung erforderlich.

Trotz erkannter Hürden im zwischenbehördlichen Austausch und den doppelten Prüfungen sollten weitere Digitalisierungsansätze, insbesondere in diesem Bereich, verfolgt werden. Die Einführung und Etablierung von Verifiable Credentials könnte zu rechtlichen Änderungen bezüglich des geforderten Umfangs der Nachweise führen, da wesentliche Aussagen präziser getroffen werden können, ohne die derzeit benötigte Datenmenge anzufordern. Dies würde eine Form der Datenminimierung einführen, die sowohl den Kunden als auch den Sachbearbeitern zugutekommt. Kryptografische Zero-Knowledge Proofs, also verifizierbare Aussagen ohne Offenlegung der dazugehörigen umfassenden Nachweise, werden dabei besonders interessant.

Weitere Forderungen beinhalten die praxisnahe Verfassung und Auslegung von erneuten Änderungen und Anpassungen des Ausländerrechts sowie die Bereitstellung von Prüfschemata und Prozesslandkarten durch den Bund, um den Raum für Ermessensfehler einzuschränken. Runde Tische in Kommunen mit Sachbearbeitern, Betroffenen sowie weiteren zivilgesellschaftlichen und privatwirtschaftlichen Akteuren sollten eingerichtet werden, um Transparenz über Handlungsweisen zu ermöglichen und den Austausch über die Bewältigung von Situationen zu fördern.

Prüfungsbedarf und weitere Schritte

Neben der Prüfung für den Anwendungsfall Ausländerbehörde muss auch eine technische Umsetzungsprüfung erfolgen: Ist es realistisch, diese technische Struktur in naher Zukunft umzusetzen? Eine Prüfung muss durchgeführt werden, um die Einführung von DIDs für den Ausbau benötigter Netzwerke zu bewerten. Möglicherweise gibt es einfachere Lösungen, die die Anforderungen erfüllen und bestehende oder gerade sich aufbauende Systeme an die man anknüpfen kann.

Zu einer weiteren Ausarbeit könnte anfangs ein zweijähriges Forschungsprojekt mit einer Laufzeit angemeldet werden. Dieses Forschungsprojekt würde sich zum Ziel machen, die benötigte Governance innerhalb den Ebenen des Trust Over IP-Modells zu etablieren. Dieses aufgestellte Modell der gleichnamigen Organisation unter Linux definiert ein Framework mit vier Ebenen zur Schaffung von Vertrauen im Digitalen. Jede Ebene erfordert geeignete Regelwerke, um den Einsatz der Technologie nachvollziehbar und vertrauenswürdig zu gestalten (Anke und Richter, 2023). Vor allem in der vierten Ebene der Anwendungsökosysteme wäre als Interaktionsdesigner viel wertvolle Arbeit möglich. Hier kann das Ökosystem von der Ausländerbehörde auf die allgemeine Verwaltung erweitert und weiter erforscht und konzipiert werden. Es können Vertrauensmechanismen, Regelwerke und neue dezentrale Strukturen in verschiedenen Anwendungsfällen erarbeitet und entwickelt werden. Dabei sollten Artefakte und Prototypen erstellt werden, um die Auswirkungen auf bestehende Strukturen zu untersuchen. Parallel dazu sollte ein technischer Ausbau erfolgen und wiederholt zu den aufgestellten Anforderungen gegengeprüft werden.

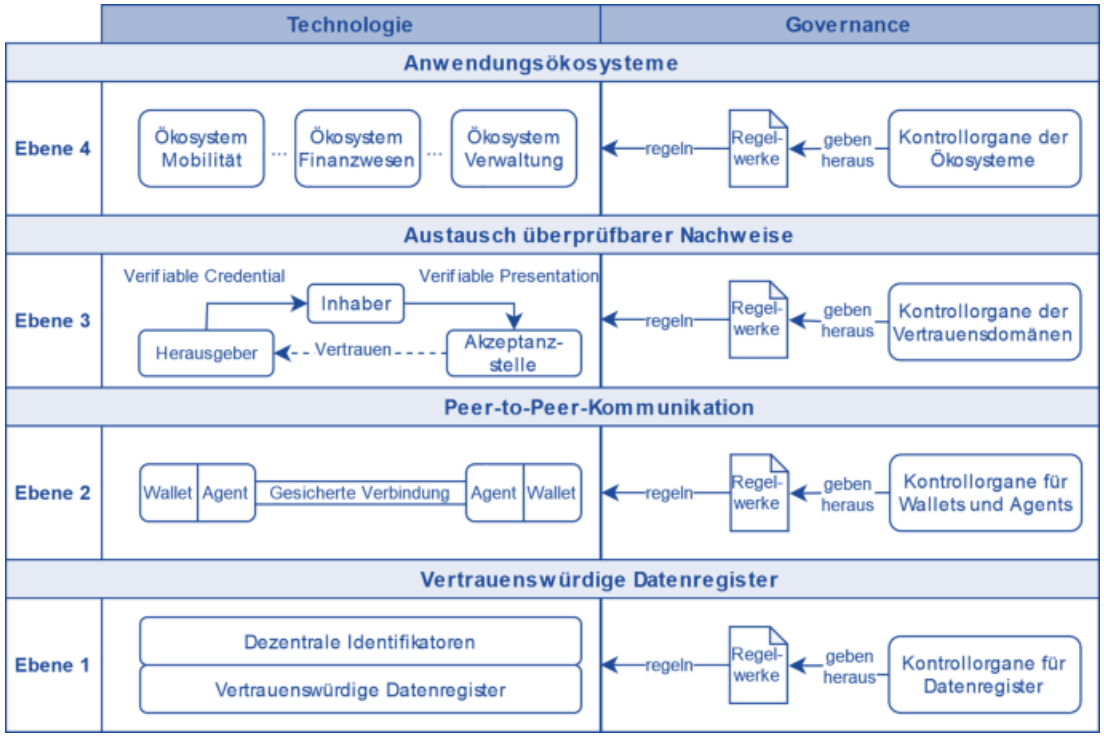


Abbildung 21: Die vier Ebenen zum Aufbauen von Vertrauen im Internet (Anke und Richter, 2023)

Abschluss

Insgesamt lässt sich festhalten, dass das Thema der selbstbestimmten Identitäten ein weites und komplexes Forschungsfeld darstellt, das unterschiedliche Disziplinen und Expertisen einbeziehen muss. Die rasante technologische Entwicklung in diesem Bereich und die Entstehung neuer Anwendungsfälle verdeutlichen die Relevanz und Aktualität dieses Feldes. Es bleibt spannend zu beobachten, wie sich diese Entwicklung in Zukunft fortsetzt und welche Auswirkungen sie auf nationaler, europäischer Ebene und globaler Ebene haben wird. Es ist anzunehmen, dass in den kommenden Jahren immer mehr Projekte und Forschungsvorhaben in diesem Bereich entstehen werden. Unsere digitalen Endgeräte sind schon längst ein erweiterter Teil von uns als Menschen. Die Technik wird uns auch nicht verlassen - sie wird sich weiterentwickeln, uns begleiten und sich mit uns vereinen.

Abschließend ist es wichtig, sich dringend mit unseren digitalen Identitäten und unserer Datensouveränität auseinanderzusetzen. Es müssen unbedingt Initiativen ergriffen werden, um eine Dezentralisierung weg von monopolistischen Identitätsprovidern voranzutreiben. Daher müssen wir sicherstellen, dass wir sie im Einklang mit menschlichen Bedürfnissen, Werten und zwischenmenschlichen Strukturen gestalten. Damit wir uns gemeinsam hin zu lebenswerten sozio-technischen Systemen entwickeln, und nicht zu dystopischen techno-soziologischen Systemen entwickeln lassen.

Quellenverzeichnis

Allen, C. (2016, April 26). *The Path to Self-Sovereign Identity*. Life With Alacrity. https://www.lifewithalacrity.com/article/the-path-to-self-soverereign-identity/

Amend, J., Arnold, L., Fabri, L., Feulner, S., Fridgen, G., Harzer, L., Karnebogen, P., Koehler, F., Ollig, P., Rieger, A., Schellinger, B. und Schmid- - bauer-Wolf (2023). *Föderale Blockchain Infrastruktur Asyl (FLORA)*. Institutsteil Wirtschaftsinformatik des Fraunhofer-Instituts für Angewandte Informationstechnik FIT, Interdisciplinary Centre for Security, Reliability and Trust of the University of Luxembourg und Bundesamt für Migration und Flüchtlinge. https://www.bamf.de/SharedDocs/Anlagen/DE/Digitalisierung/blockchain-whitepaper-2022.pdf?__blob=publicationFile&v=5

Amend, J., Arnold, L., Feulner, S., Fridgen, G., Köhler, F., Ollig, P., Rieger, A. und Roth, T. (2023). *Chancen und Herausforderungen des Einsatzes von Blockchain in der öffentlichen Verwaltung*. Institutsteil Wirtschaftsinformatik des Fraunhofer-Instituts für Angewandte Informationstechnik FIT, Interdisciplinary Centre for Security, Reliability and Trust of the University of Luxembourg und Bundesamt für Migration und Flüchtlinge. https://www.bamf.de/SharedDocs/Anlagen/DE/Digitalisierung/blockchain-whitepaper-Chancen-Herausforderungen.pdf?__blob=publicationFile&v=4

Anke, J., & Richter, D. (2023). Digitale Identitäten. *HMD Praxis der Wirtschaftsinformatik*, 60(2), 261–282. https://doi.org/10.1365/s40702-023-00965-1

BAMF. (o. J.). *Standard XAusländer*. BAMF - Bundesamt für Migration und Flüchtlinge. Abgerufen 28. Februar 2024, von https://www.BAMF.de/DE/Themen/Digitalisierung/Xauslaender/xauslaender-node.html

BAMF. (2017, September 27). *Identitätssicherung und -feststellung im Migrationsprozess*. BAMF - Bundesamt für Migration und Flüchtlinge. https://www.BAMF.de/SharedDocs/Meldungen/DE/2017/EMN/20170927-am-emn-studie-identitaetssicherung-feststellung.html?nn=282388

BAMF. (2022). *Das Ausländerzentralregister*. Bundesamt für Migration und Flüchtlinge. https://www.bamf.de/SharedDocs/Anlagen/DE/Behoerde/flyer-auslaenderzentralregister.pdf?__blob=publicationFile&v=10

BDR. (2022, Juni 21). *Warum die Self-Sovereign Identity eine Bewegung ist*. https://www.bundesdruckerei.de/de/innovation-hub/warum-die-self-sovereign-identity-eine-bewegung-ist

Begleitforschung. (2023, Januar 17). *Self-Sovereign-Identities (SSI) – Das kleine 1×1 der sicheren digitalen Identitäten*. Schaufenster Sichere Digitale Identitäten Begleitforschung. https://digitale-identitaeten.de/self-sovereign-identities-ssi-das-kleine-1x1-der-sicheren-digitalen-identitaeten/

Biedermann, B., Handke, S., Jürgenssen, O., Orta, E., Schindler, C., Schröder, R., Schroll, L., & Sonne, F. (2023). Nutzen und Grenzen von SSI für Verwaltung und öffentliche Institutionen. *HMD Praxis der Wirtschaftsinformatik*, 60(2), 437–457. https://doi.org/10.1365/s40702-023-00953-5

Biselli, A. (2023a, Juni 14). *Ausländerzentralregister: Kaum Asylentscheidungen in der Riesendatenbank*. netzpolitik.org. https://netzpolitik.org/2023/auslaenderzentralregister-kaum-asylentscheidungen-in-der-riesendatenbank/

Biselli, A. (2023b, Juni 22). *BAMF: Die Asyl-Blockchain wird immer länger*. netzpolitik.org. https://netzpolitik.org/2023/bamf-die-asyl-blockchain-wird-immer-laenger/

BMI. (o. J.-a). *Behördengänge online erledigen: E-Government*. Bundesministerium des Innern und für Heimat. Abgerufen 28. Februar 2024, von https://www.bmi.bund.de/DE/themen/moderne-verwaltung/e-government/e-government-node.html;jsessionid=7B8F7D4D1507244E973FFAAF7E3A135A.live862

BMI. (o. J.-b). *FAQ zum Aufenthaltsrecht*. Bundesministerium des Innern und für Heimat. Abgerufen 27. Februar 2024, von https://www.bmi.bund.de/SharedDocs/faqs/DE/themen/migration/aufenthaltsrecht/aufenthaltsrecht-liste.html?nn=9392780

BMI. (o. J.-c). *Was passiert bei der Ausländerbehörde?* Bundesministerium des Innern und für Heimat. Abgerufen 27. Februar 2024, von https://www.bmi.bund.de/SharedDocs/faqs/DE/themen/verfassung/brexit/neues-aufenthaltsdokument/was-passiert-bei-der-auslaenderbehoerde.html;jsessionid=FD681081AF51032A8ACDC23D2609BA71.live861?nn=9390170

BMI. (2019). *Das Onlinezugangsgesetz (OZG)*. Bundesministerium des Innern und für Heimat. https://www.bmi.bund.de/DE/themen/moderne-verwaltung/verwaltungsmodernisierung/onlinezugangsgesetz/onlinezugangsgesetz-artikel.html?nn=9391878

Bogumil, J., Kuhlmann, S., Hafner, J., Kastilan, A., Oehlert, F., & Reusch, M. C. (2023). *Lokales Integrationsmanagement in Deutschland, Schweden und Frankreich*. Nomos Verlagsgesellschaft mbH & Co. KG. https://doi.org/10.5771/9783748939115

BSI. (o. J.-a). *eIDAS-Verordnung über elektronische Identifizierung und Vertrauensdienste*. Bundesamt für Sicherheit in der Informationstechnik. Abgerufen 8. März 2024, von https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/eIDAS-Verordnung/eidas-verordnung.html?nn=129796

BSI. (o. J.-b). *Grundsätzliche Funktionsweise biometrischer Verfahren*. Bundesamt für Sicherheit in der Informationstechnik. Abgerufen 3. März 2024, von https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Technologien_sicher_gestalten/Biometrie/AllgemeineEinfuehrung/einfuehrung.html?nn=452592

BSI. (2021). *Eckpunktepapier für Self-sovereign Identities (SSI)—Unter besonderer Berücksichtigung der Distributed-Ledger-Technologie (DLT)*. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Krypto/Eckpunkte_SSI_DLT.pdf?__blob=publicationFile&v=2

BSI. (2023, Juli 13). *AusweisApp*. Bundesamt für Sicherheit in der Informationstechnik. https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Elektronische-Identitaeten/Online-Ausweisfunktion/AusweisApp/ausweisapp.html?nn=130324

Bundeskanzleramt. (2021). *Digitale Identität—Wie ein Ökosystem digitaler Identitäten zu einem selbstbestimmten und zugleich nutzerfreundlichen Umgang mit dem digitalen Ich beitragen kann*. https://www.bundesregierung.de/resource/blob/992814/1898280/d9819a40553a9543b9e8f3acb620b0c2/digitale-identitaet-neu-download-bundeskanzleramt-data.pdf?download=1

Bundesnetzagentur. (2024). *Bundesnetzagentur—European Blockchain Services Infrastructure*. https://www.bundesnetzagentur.de/DE/Fachthemen/Digitalisierung/Technologien/Blockchain/BC_European/start.html

Bundestag und Beck, R. (2018). *Fragen für das Fachgespräch zum Thema Blockchain im Ausschuss Digitale Agenda*. https://www.bundestag.de/resource/blob/580714/7327080bc4e2c6c13eb3657867fa5ff1/A-Drs-19-23-26-Beck.pdf

BVA. (o. J.). *BVA - Ausländerzentralregister*. Abgerufen 27. Februar 2024, von https://www.bva.bund.de/DE/Das-BVA/Aufgaben/A/Auslaenderzentralregister/azr_node.html

CCC. (o. J.). *CCC | Wie können Fingerabdrücke nachgebildet werden?* Abgerufen 3. März 2024, von https://www.ccc.de/de/campaigns/aktivitaeten_biometrie/fingerabdruck_kopieren

Darmstadt. (o. J.). *Ausländerbehörde Darmstadt—Hauptmenü: Darmstadt*. Abgerufen 1. März 2024, von https://www.darmstadt.de/rathaus/online-dienste/auslaenderbehoerde-darmstadt/auslaenderbehoerde-darmstadt-hauptmenue

Decentralized Identity Foundation. (2023). *DIF Decentralized Web Node*. https://identity.foundation/decentralized-web-node/spec/

Denso Wave. (o. J.). *QR Code development story ／Technologies ／DENSO WAVE*. QR Code development story,Technologies,DENSO WAVE. Abgerufen 8. März 2024, von https://www.denso-wave.com/en/technology/vol1.html

Deutschlandfunk. (2024, Februar 19). *Onlinezugangsgesetz 2.0: Behördengänge sollen digital werden*. tagesschau.de. https://www.tagesschau.de/wirtschaft/digitales/onlinezugangsgesetz-102.html

e-estonia. (2024). *Become an e-resident of Estonia | How to apply*. E-Residency. https://www.e-resident.gov.ee/become-an-e-resident/

Europäische Kommission. (2022). *EBSI Veriable Credentials explained—Chapter 3 EBSI DIDs*. https://ec.europa.eu/digital-building-blocks/sites/download/attachments/659621351/Chapter%203%20-%20EBSI%20DIDs.pdf?version=1&modificationDate=1679559952457&api=v2

Europäische Kommission. (2023, Juni 20). *European Self Sovereign Identity Framework Laboratory | eSSIF-Lab | Project | Fact sheet | H2020 | CORDIS | European Commission*. https://cordis.europa.eu/project/id/871932

Gourisetti, S. N. G., Cali, Ü., Choo, K.-K. R., Escobar, E., Gorog, C., Lee, A., Lima, C., Mylrea, M., Pasetti, M., Rahimi, F., Reddi, R., & Sani, A. S. (2021). Standardization of the Distributed Ledger Technology cybersecurity stack for power and energy applications. *Sustainable Energy, Grids and Networks*, *28*, 100553. https://doi.org/10.1016/j.segan.2021.100553

Grytz, C. M., & Kudra, A. (2022, Februar 25). *Mit Self-Sovereign Identity sicher unterwegs in die digitale Zukunft!* https://www.informatik-aktuell.de/betrieb/sicherheit/mit-self-sovereign-identity-sicher-unterwegs-in-die-digitale-zukunft.html

ID-Union. (2022). *Über uns – IDunion*. https://idunion.org/ueber-uns/

Jannik, L., Alexander, R., & Gilbert, F. (2019). *Blockchain in der öffentlichen Verwaltung—Unterstützung der Zusammenarbeit im Asylprozess*. Frauenhofer FIT, Universität Bayreuth. https://www.fim-rc.de/Paperbibliothek/Veroeffentlicht/943/wi-943.pdf

Lautenschlag, A. (2022, Januar 7). *Was ist eine API: Eine einfache Erklärung für Selbstständige*. Lautenschlager Marketing & Entwicklung. https://www.lautenschlager.de/blog/was-ist-eine-api-eine-einfache-erklaerung-fuer-selbststaendige/

Pohlmann, N. (2019, Januar 26). Self-Sovereign Identity (SSI)—Glossar—Prof. Norbert Pohlmann. *Prof. Dr. Norbert Pohlmann*. https://norbert-pohlmann.com/glossar-cyber-sicherheit/self-sovereign-identity-ssi/

Pohlmann, N. (2020, April 21). Decentralized Identifiers (DIDs)—Glossar—Prof. Pohlmann. *Prof. Dr. Norbert Pohlmann*. https://norbert-pohlmann.com/glossar-cyber-sicherheit/decentralized-identifiers/

Savill, J. (Regisseur). (2022, November 22). *Understanding and Using Verifiable Credentials*. John Savill's Technical Training. https://www.youtube.com/watch?v=BxLSSH_EHjo

Schammann, H., & Kühn, B. (2016). Kommunale Flüchtlingspolitik in Deutschland. *Friedrich-EbertStiftung, Abteilung Wirtschafts- und Sozialpolitik*. https://library.fes.de/pdf-files/wiso/12763.pdf

Schlee, T., Schammann, H., & Münch, S. (2023). *An den Grenzen?: Ausländerbehörden zwischen Anspruch und Alltag*. https://doi.org/10.11586/2023069

Schneider, J. (2012). *Die Organisation der Asyl- und Zuwanderungspolitik in Deutschland*. BAMF - Bundesamt für Migration und Flüchtlinge. https://www.BAMF.de/SharedDocs/Anlagen/DE/EMN/Studien/wp25-emn-organisation-asylpolitik.html?nn=282022

Strüker, D. J., Urbach, D. N., Guggenberger, T., Lautenschlager, J., Ruhland, N., Sedlmeir, J., Stoetzer, J.-C., & Völter, F. (2021). *Self-Sovereign Identity – Grundlagen, Anwendungen und Potenziale portabler digitaler Identitäten*. Projektgruppe Wirtschaftsinformatik des Fraunhofer-Instituts für Angewandte Informationstechnik FIT. https://www.fit.fraunhofer.de/content/dam/fit/de/documents/Fraunhofer%20FIT_SSI_Whitepaper.pdf

The Linux Foundation. (2024). *About Us | Hyperledger*. https://www.hyperledger.org/about

Tobin, A. (2021, Dezember 8). *Decentralized Identity & Government*. https://www.youtube.com/watch?v=I8pHUdjKfes

Umweltbundesamt (Regisseur). (2023, April 19). *Digitale Kommunen, Digitale Region: Prozesse sinnvoll Digitalisieren*. https://www.youtube.com/watch?v=ojIKE9O-U6A

W3C. (2022, Juli 19). *Decentralized Identifiers (DIDs) v1.0 becomes a W3C Recommendation*. W3C. https://www.w3.org/press-releases/2022/did-rec/

Wölbert, C. (2022, Dezember 30). *Warum das Gesetz zur Digitalisierung der Verwaltung scheiterte*. heise online. https://www.heise.de/news/Warum-das-Gesetz-zur-Digitalisierung-der-Verwaltung-scheiterte-7435103.html

Young, K. (2022, April 8) *Keeping Your Personal Data Personal: How Decentralized Identity Drives Data Privacy*. (2022, April 8). https://www.youtube.com/watch?v=hRBKWxAon_Y

Abbildungsverzeichnis

Abbildung 17: eigene Anfertigung

Abbildung 18: Europäische Kommission. (2022). *EBSI Veriable Credentials explained—Chapter 3 EBSI DIDs*. https://ec.europa.eu/digital-building-blocks/sites/download/attachments/659621351/Chapter%203%20-%20EBSI%20DIDs.pdf?version=1&modificationDate=1679559952457&api=v2

Abbildung 19: eigene Anfertigung

Abbildung 20: eigene Anfertigung

Abbildung 21: eigene Anfertigung

Abbildung 22: Anke, J., & Richter, D. (2023). Digitale Identitäten. *HMD Praxis der Wirtschaftsinformatik*, *60*(2), 261–282. https://doi.org/10.1365/s40702-023-00965-1

Einverständniserklärung

Eigenständigkeitserklärung

Hiermit erkläre ich, dass ich die vorliegende Arbeit selbstständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe. Alle sinngemäß und wörtlich übernommenen Textstellen aus fremden Quellen wurden kenntlich gemacht.

Darmstadt, 08.03.2024

Erklärung zur Archivierung

Hiermit erkläre ich mich mit der Archivierung dieser Forschungsarbeit einverstanden.

Darmstadt, 08.03.2024