Evaluation einer Methode zur Entwicklung von Anforderungen im Bereich der digitalen Souveränität am Beispiel digitaler Identitäten

Masterarbeit

von

Manuel Brazel

Studiengang: Wirtschaftsinformatik

Matrikelnummer: 1750849

Institut für Angewandte Informatik und Formale Beschreibungsverfahren (AIFB)

KIT-Fakultät für Wirtschaftswissenschaften

Prüfer:	Prof. Dr. Andreas Oberweis
Zweiter Prüfer:	Prof. Dr. Johann Marius Zöllner
Betreuer:	Dr. Sascha Alpers
Eingereicht am:	31. Juli 2023

Hinweis

Die in dieser Arbeit gewählte männliche Form bezieht sich immer zugleich auf weibliche, männliche und diverse Personen. Auf eine Mehrfachbezeichnung wird in der Regel zugunsten einer besseren Lesbarkeit verzichtet.

Zusammenfassung

Die vorliegende Arbeit evaluiert und diskutiert eine am FZI Forschungszentrum Informatik entwickelte Methode zur Entwicklung von Anforderungen im Bereich der digitalen Souveränität. Die Methode wurde im Rahmen des Projekts SDIKA durchgeführt. Das Ziel des Software-Projekts ist die Entwicklung einer Lösung für digitale Identitäten.

Die Evaluation erfolgte mithilfe der Bewertungskriterien „Durchführbarkeit der Methode“ und „Qualität der Ergebnisse“. Besonders die ersten vier Schritte von MEADigS waren relativ effektiv, effizient und wurden von den Beteiligten Akteuren akzeptiert. Der fünfte und sechste Schritt konnte nicht vollständig durchgeführt werden.

Die Durchführung von fokusgruppenähnlichen Workshops und die anschließende Analyse führte zu guten Ergebnissen. Die Qualität der Ergebnisse wurde anhand der Kriterien Vollständigkeit, Korrektheit, Sachdienlichkeit, Konsistenz, Nachvollziehbarkeit und Eindeutigkeit beurteilt. Insgesamt wurden 33 elementare Anforderungen entwickelt. Die Anforderungen konnten 81% der Themenfelder digitaler Souveränität abdecken.
Auf eine zusätzliche Validierung der Anforderungen in Form von Interviews oder quantitativer Erfassung musste aus Zeitgründen verzichtet werden. Die Qualität der Anforderungen war aber insgesamt sehr gut.

MEADigS kann mit Einschränkungen als eine geeignete Methode betrachtet werden, wobei die Schritte fünf und sechs teilweise als optional betrachtet werden können.

Inhaltsverzeichnis

Abkürzungsverzeichnis

BDSG Bundesdatenschutzgesetz.

BMWK Bundesministerium für Wirtschaft und Klimaschutz.

eID digitale/elektronische Identität.

eIDAS-Verordnung Verordnung Nr. 910/2014 des Europäischen Parlaments und des Europäischen Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG.

EU Europäische Union.

EU-DS-GVO Datenschutz-Grundverordnung.

FZI FZI Forschungszentrum Informatik.

MEADigS Methode zur Entwicklung von Anforderungen im Bereich der digitalen Souveränität.

RE Requirements Engineering.

REO Requirements Engineering Objectives.

SDIKA Schaufenster Sichere Digitale Identitäten Karlsruhe.

SSI Self Sovereign Identity.

SSO Single-Sign-on.

UX User Experience.

Abbildungsverzeichnis

Tabellenverzeichnis

1 Einleitung

Dieses Kapitel stellt eine Einführung in das Thema dieser Arbeit dar. Dafür wird auf den Hintergrund, die Motivation und die Zielsetzung eingegangen. Außerdem wird ein Überblick über den Aufbau der Arbeit gegeben.

1.1 Motivation

Die großen Technologiekonzerne aus den Vereinigten Staaten haben einen immensen Einfluss auf das Leben der Menschen überall auf der Welt. Eine Vielzahl digitaler Anwendungen von Google, Apple, Facebook, Amazon und Microsoft erleichtern auch den Alltag vieler Europäer.

Gleichzeitig besteht eine immer größer werdende Sorge vor der Marktmacht dieser Internet-Giganten. Die Gefahr, dass diese Marktmacht missbraucht wird scheint allgegenwärtig (Petropoulos 2021, S. 1, Floridi 2020).

Angesichts dieser Gegebenheiten ist es nicht verwunderlich, dass im öffentlichen Diskurs der Wunsch nach mehr Souveränität im digitalen Raum, sowohl auf individueller als auch auf politischer Ebene, immer stärker zum Ausdruck kommt (Beyerer et al. 2018).

Eine grundlegende Voraussetzung, um souverän im digitalen Raum agieren zu können, ist das Vertrauen in die Sicherheit von Identitäten. Ohne sichere digitale Identitäten lässt sich ein Schutz vor Cyber-Kriminalität, Missbrauch von Daten und Industriespionage nicht gewährleisten (Beyerer et al. 2018).

Unter anderem aus diesen Gründen wird eine Lösung für digitale Identitäten dringend benötigt.

1.2 Fragestellung

Im Rahmen des regionalen Schaufensterprojekts Schaufenster Sichere Digitale Identitäten Karlsruhe (SDIKA) soll eine Lösung für sichere digitale Identitäten entwickelt werden (SDIKA 2023).

Für das Gelingen großer Software-Projekte ist eine systematische Erhebung von Anforderungen im Vorfeld eine entscheidende Aktivität (Pohl 2008, S. 1-7).

Am FZI Forschungszentrum Informatik (FZI) wurde eine Methode zur Entwicklung von Anforderungen im Bereich der digitalen Souveränität (MEADigS) entwickelt, die für die Entwicklung von Anforderungen im Bereich der digitalen Souveränität besonders geeignet sein soll (Weinreuter 2022; Weinreuter et al. 2023). Diese Methode soll im Rahmen dieser Arbeit durchgeführt werden.

Mit der Durchführung von MEADigS sollen die Anforderungen der Stakeholder an eine digitale Identitätslösung erhoben und dem Projekt zur Verfügung gestellt werden. Dabei soll die Methode MEADigS evaluiert und kritisch betrachtet werden.

1.3 Aufbau dieser Arbeit

Diese Arbeit gliedert sich in vier Teile. Zunächst werden die theoretischen Grundlagen erläutert und auf die wesentlichen Begriffe eingegangen. Außerdem wird das Projekt SDIKA kurz vorgestellt.

Das darauffolgende Kapitel definiert und erklärt die Bewertungskriterien, anhand derer später die Evaluation durchgeführt werden soll.

Danach wird die Methode MEADigS vorgestellt. Außerdem wird ein Methodenplan erstellt, mit dessen Hilfe MEADigS auf das Projekt SDIKA angewandt wird.

Es folgt die Beschreibung der Durchführung der Methode. Außerdem werden die Ergebnisse dargestellt.

Anschließend wird die Methode evaluiert, kritisch diskutiert und ein Fazit gezogen.

2 Theoretische Grundlagen

Im Folgenden wird auf die theoretischen Grundlagen eingegangen. Dabei werden die wesentlichen Definitionen vorgestellt und Grundbegriffe erläutert, die für das Verständnis der Arbeit benötigt werden. Hierdurch wird auch der Kontext, in dem die Arbeit angefertigt wurde, genauer erklärt.

2.1 Digitale Souveränität

Unter digitaler Souveränität versteht man „die Fähigkeit zu selbstbestimmtem Handeln und Entscheiden im Digitalen Raum“ (Beyerer et al. 2018, S. 278).

Diese Fähigkeit kann von Individuen und Institutionen wie natürlichen Personen, Unternehmen, Vereinen oder Körperschaften des öffentlichen Rechtes sowie sonstige juristische Personen ausgeübt werden. Auch Staaten oder Staatenbunde wie die Europäische Union (EU) haben ein Interesse daran, ihre eigene digitale Souveränität sowie die ihrer Bürger zu stärken (Beyerer et al. 2018; Goldacker 2017).

2.1.1 Bedeutung digitaler Souveränität

Mit fortschreitender Digitalisierung und Vernetzung wird das Thema digitale Souveränität immer relevanter. Aus diesem Grund wird diese in der Öffentlichkeit immer häufiger diskutiert.

Die Globalisierung führt dazu, dass Datenströme über Ländergrenzen hinweg fließen. Dies führt unweigerlich zu Abhängigkeiten von ausländischen Akteuren.

Insbesondere große US-amerikanische Technologiekonzerne dominieren den Markt der digitalen Infrastruktur und der Cloud-Dienste. Die Abhängigkeit von Unternehmen aus dem Ausland deutet auf einen Kontrollverlust und damit einer Schwächung der digitalen Souveränität eines Staates hin (Couture und Toupin 2019).

Dies spielt auch aus sicherheitspolitischer Sicht eine bedeutende Rolle, da die Gefahr besteht, dass ausländische Geheimdienste sich Zugang zu Daten von Bürgern, Unternehmen und staatlichen Institutionen der EU verschaffen und diese auswerten (vgl. Pohle 2020, S. 3-5). Je kritischer die Systeme desto relevanter wird Souveränität. Dementsprechend wird schon seit einiger Zeit von IT Spezialisten gefordert, die europäische Wettbewerbsfähigkeit in Bezug auf Schlüsseltechnologien zu verbessern. Das könne gelingen, wenn Alternativen zu den etablierten Systemen anderer Akteure geschaffen würden (vgl. Beyerer et al. 2018, Kranich et al. 2017, S. 62-72, Bitkom 2019, S. 7-11).

2.1.2 Dimensionen digitaler Souveränität

Man kann vier Dimensionen der digitalen Souveränität voneinander abgrenzen (Krupka 2020):

1. Kompetenzen
2. Daten
3. Soft-/Hardwaretechnologien und
4. Governance-Systeme.

Kompetenzen
Um selbstständig und selbstbestimmt im digitalen Raum agieren zu können, benötigt es Kompetenzen im Umgang mit den entsprechenden Systemen und Technologien.

Die Fähigkeit der Nutzenden, beispielsweise eine Technologie eigenständig verwenden zu können setzt voraus, dass der Mensch diese versteht und ebenso in der Lage ist, die Konsequenzen seiner Handlungen einzuschätzen. Medienkompetenz und IT-Grundkenntnisse können Personen ermächtigen, sich selbst vor Angriffen wie Phishing, Schadsoftware oder Kostenfallen zu schützen.

Ein weiterer Aspekt ist nicht nur die Freiheit, zwischen Alternativen wählen zu können sondern auch, diese auf ihre Sicherheit zu prüfen. Die Verfügbarkeit quellcodeoffener (engl. Open-Source) Systeme, welche die Überprüfung durch IT-Spezialisten ermöglichen, kann unter anderem dazu beitragen, gesamtgesellschaftliche digitale Souveränität zu erreichen (vgl. Goldacker 2017).

Daten
Hierbei hat sich der Begriff *Datensouveränität* etabliert. In Zeiten von Big Data und Cloudspeichern gilt sie als gefährdet. Unter *Datensouveränität* versteht man die Fähigkeit, informiert und selbstbestimmt zu entscheiden, wie und von wem Daten über die eigene Person erhoben, verarbeitet und weitergegeben werden (Beyerer et al. 2018).

Mit der Datenschutz-Grundverordnung (EU-DS-GVO) hat die EU einheitliche umfassende Regelungen zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten aufgestellt. Diese werden im Rahmen existierender Öffnungsklauseln durch nationale Gesetzgebung wie dem Bundesdatenschutzgesetz (BDSG) ergänzt. Der Schutz des Grundrechts auf informationelle Selbstbestimmung (Garstka 2003) steht dabei im Vordergrund.

Einerseits wird die Umsetzung der rechtlichen Rahmenbedingungen als Voraussetzung für *Datensouveränität* betrachtet (Beyerer et al. 2018, S. 278), andererseits gilt digitale

Souveränität auch als notwendig, um effektiven Datenschutz zu gewährleisten (Roßnagel 2023).

Soft-/Hardwaretechnologien

Die technologische Souveränität stellt einen weiteren Teilaspekt digitaler Souveränität dar. Wenn die EU das Ziel verfolgt, sich unabhängiger von ausländischen Technologie-Konzernen zu machen, benötigt sie eigene Soft- bzw. Hardwarelösungen wie unter anderem eine eigene europäische Cloud-Architektur als praktikable und vertrauenswürdige Alternative.

Insbesondere kritische Infrastrukturen wie Energieversorgung, Gesundheitswesen und Verkehrsinfrastruktur haben einen besonders hohen Schutzbedarf. Die Gewährleistung, vor Angriffen und Spionage geschützt zu sein, steht hierbei im Vordergrund.

Dementsprechend haben Deutschland und die EU ein großes Interesse daran, diese Schlüsseltechnologien autark entwickeln und kontrollieren zu können (Abbildung 1) (Krupka 2020; Beyerer et al. 2018).

Governance-Systeme

Mit der zunehmenden Digitalisierung rücken die Herausforderungen auf dem Gebiet der Governance-Strukturen immer stärker in den Vordergrund. Regulatorische Rahmenbedingungen können dazu beitragen, die digitale Souveränität zu stärken. Einerseits können Governance-Strukturen dabei unterstützen, den Schutz der personenbezogenen Daten der Bürger zu gewährleisten. Dafür müssen die Systeme einen hohen Grad an Sicherheit bieten. Mittels kryptografischer Verfahren können Daten verschlüsselt werden und durch geeignete Schutzmaßnahmen das Risiko von Cyberangriffen reduziert werden. Gleichzeitig sollten die Systeme leistungsfähig und funktional sein.

Ein weiterer wesentlicher Aspekt im Bereich der IT-Sicherheit in Governance-Systemen ist der Schutz vor Identitätsdiebstahl. Digitale Verwaltungssysteme erfordern daher auch sichere technologische Lösungen für digitale Identitäten (Krupka 2020; Stemmer 2016).

2.1.3 Ziele digitaler Souveränität

Die Forderung zur Entwicklung europäischer Alternativen zu den etablierten Technologien führt zu der Frage, wie hoch der Grad der Autarkie der EU sein soll. Maximale digitale Autarkie würde bedeuten, dass Schlüsseltechnologien grundsätzlich selbst entwickelt und benutzt werden. Der Vorteil wäre Unabhängigkeit von ausländischen Akteuren. Andererseits könnten dadurch erhebliche wirtschaftliche Nachteile entstehen, falls andere Lösungen leistungsfähiger oder kostengünstiger sind als die Eigenen.

Das Gegenteil von Autarkie wäre vollständige digitale Abhängigkeit. Das würde bedeuten, dass die EU über keine eigenen Fähigkeiten verfügt und die Gestaltung der Technologien Akteuren aus anderen Teilen der Welt überlässt. Digitale Souveränität bedeutet ein Abwägen zwischen Autarkie und Abhängigkeit wie in Abbildung 1 dargestellt (Bitkom 2019, S. 9-10).

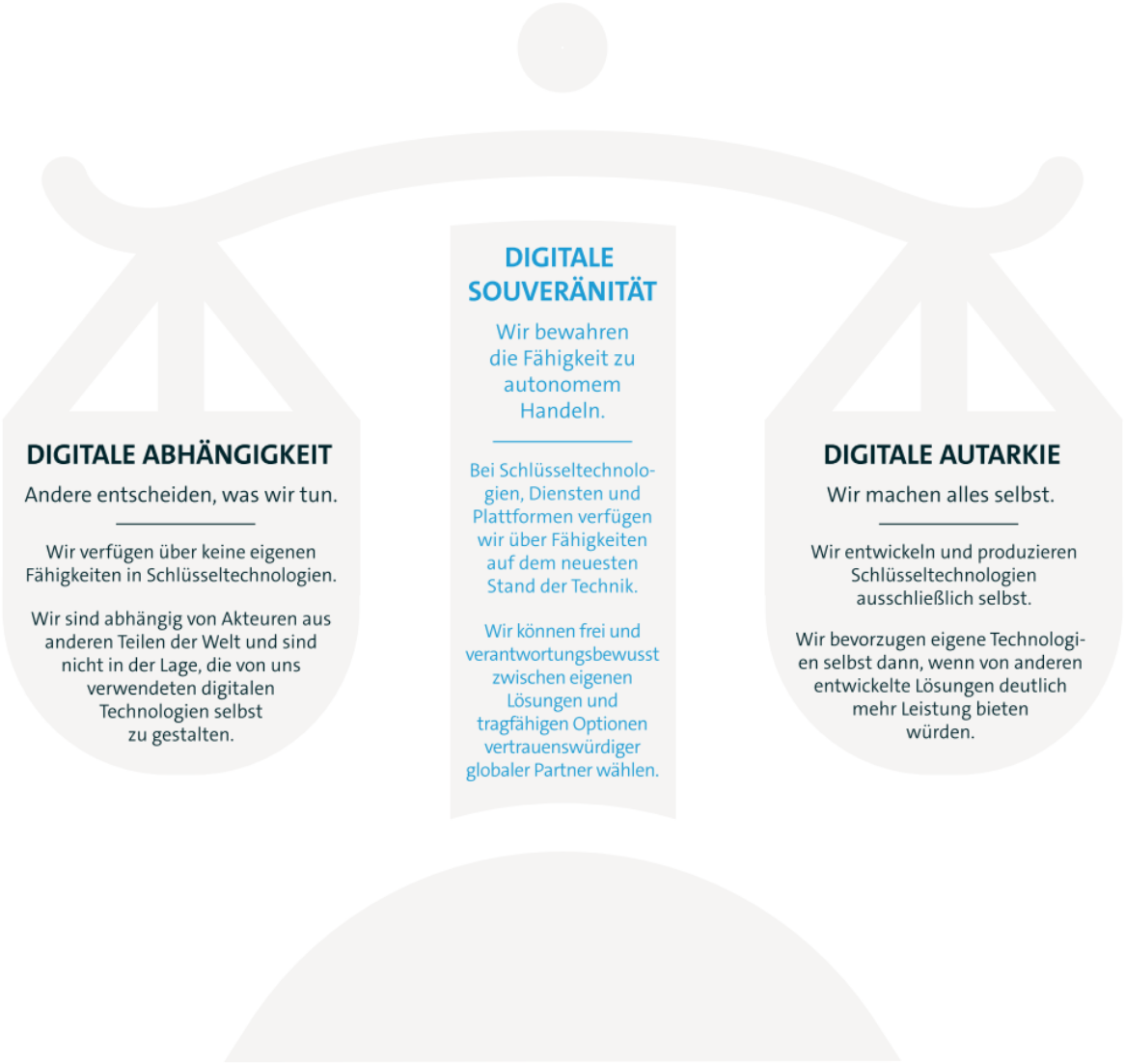


Abbildung 1: Digitale Souveränität (Bitkom 2019).

2.2 Digitale Identitäten

Eine digitale Identität beschreibt den Satz von dauerhaften oder langfristigen Attributen, die mit einer Entität verbunden sind. Zur Identifizierung einer Entität benötigt es eindeutige Identitätsmerkmale (Camp 2004, S. 36).

Um im digitalen Raum sicher und souverän handeln zu können, benötigt es Verfahren zur

eindeutigen Identifizierung von Identitäten. Das bedeutet, dass ein Anbieter von Diensten die Gewissheit hat, dass ein Subjekt auch das ist, was es vorgibt zu sein. Ohne sichere digitale Identitäten ist digitale Souveränität nicht erreichbar.

Bürger haben ein Interesse daran, sich und ihre Daten vor unerlaubter Nutzung oder Identitätsdiebstahl zu schützen. Unternehmen wollen beispielsweise verhindern, dass Betriebs- und Geschäftsgeheimnisse offengelegt werden und Systeme müssen vor unbefugtem Zugriff geschützt werden, damit unter anderem die Sicherheit der kritischen Infrastruktur gewährleistet ist.

Es gibt verschiedene Ansätze für digitales Identitätsmanagement von denen im Folgenden einige kurz vorgestellt werden.

2.2.1 Elektronischer Personalausweis

Die Verordnung Nr. 910/2014 des Europäischen Parlaments und des Europäischen Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG (eIDAS-Verordnung) regelt den Einsatz elektronischer Vertrauensdienste und Identifizierung. Die Online-Ausweisfunktion, mit der sich die digitale/elektronische Identität (eID) in Deutschland nachweisen lässt, ist seit Juli 2017 in jedem neu ausgestellten Personalausweis aktiviert.[1] Damit können unter anderem Dienste der öffentlichen Verwaltung teilweise digital genutzt werden.

2.2.2 Rolle privater Unternehmen

Internationale IT-Dienstleister wie Google oder Apple bieten seit einiger Zeit eigene Dienste zum digitalen Identitätsmanagement an (Identity-as-a-Service). Mit *Cloud Identity* von Google und der sign-in API können Nutzende sich mit ihrem Google Konto per Single-Sign-on (SSO), also ohne für den Dienst einen eigenen Nutzernamen und ein Passwort eingeben zu müssen, bei Drittanbietern mit der entsprechenden Schnittstelle über ihr Google Konto authentifizieren. Mit den APIs von Google lassen sich auch digitale Personalausweise und Bankverbindungen in der Wallet auf dem Smartphone speichern. Das ist eine komfortable Option, die zwar häufig genutzt wird, allerdings zu Abhängigkeiten von diesen Konzernen und deren Infrastruktur führt (van Bokkem et al. 2019). Darüber hinaus bestehen datenschutzrechtliche Bedenken in Bezug auf US-amerikanische Anbieter sowie

[1] Digitale Identifizierung mit dem deutschen Online-Ausweis. Bundesministerium des Innern, für Bau und Heimat. 2009. `https://www.personalausweisportal.de/SharedDocs/downloads/Webs/PA/EN/anwenderhandbuch.pdf`.

die Sorge vor einer marktbeherrschenden Stellung dieser Konzerne (Borges und Werners 2018, S. 1-5, Beyerer et al. 2018, S. 279).

2.2.3 Self-Sovereign-Identity (SSI)

Self Sovereign Identity (SSI) ist ein technologieneutraler Ansatz, bei dem Nutzende ihre Identität selbst verwalten. Hierbei gibt es keinen zentralen Identitätsdienstleister. Die Identitäten liegen in einem digitalen Wallet, zum Beispiel lokal auf einem Endgerät des Nutzenden. Ein Vertrauensdienst kann einzelne Attribute des Identitätssubjekts verifizieren und somit die Echtzeit bestätigen. Diese durch den Vertrauensdienst ausgestellte Identität kann daraufhin zur Authentisierung genutzt werden (vgl. Pohlmann 2022, S. 645-649).

Die Sicherheit von SSI wird durch kryptografische Verfahren erreicht. Um die Echtheit und Vertrauenswürdigkeit der SSI-Infrastruktur zu gewährleisten kann auch Blockchain-Technologie zum Einsatz kommen (Pöhn et al. 2021; Schwalm et al. 2022).

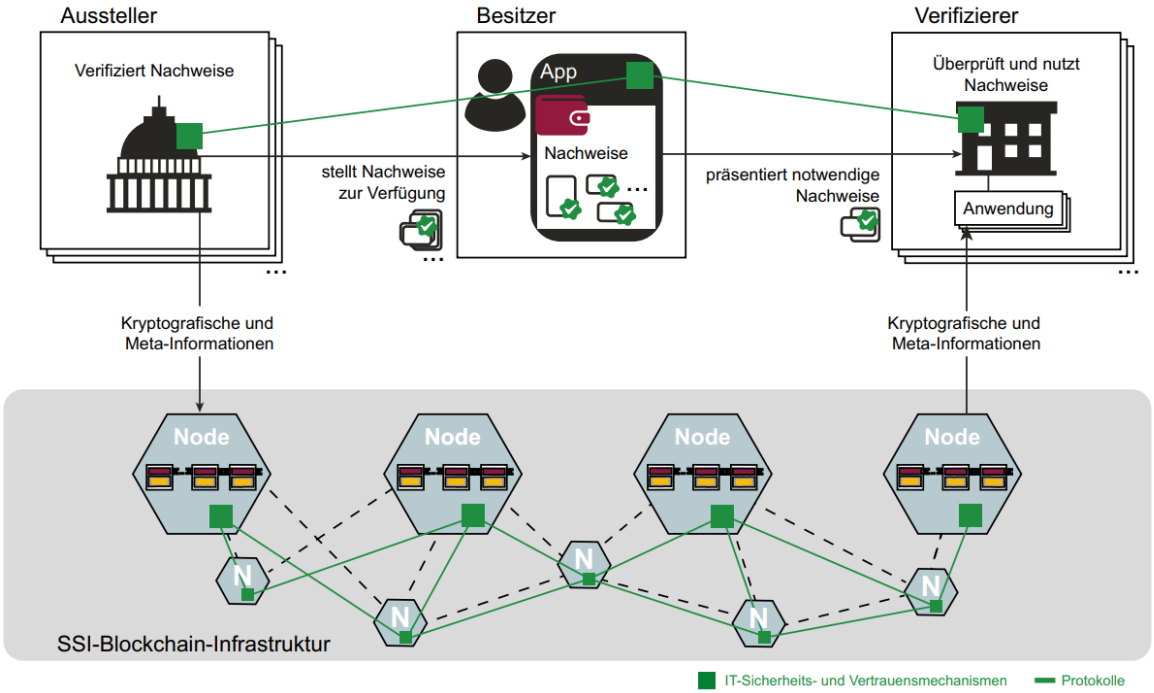


Abbildung 2: SSI-Ökosystem für digitale Identitäten und Nachweise (Pohlmann 2022, S. 647).

2.2.4 Cloud-based Identity

Neben der lokalen Selbstverwaltung existieren Ansätze, die Identität in der Cloud verwalten zu lassen und die Vertrauenswürdigkeit durch Garantien des Anbieters gewährleisten zu lassen. Die Identitätsmerkmale der Benutzer sind dann bei einem Cloud-Anbieter gespeichert. Der *Identity Provider (IdP)* übernimmt in diesem Fall die Authentifizierung der Identitätsmerkmale. Bei einem Anmeldevorgang werden die Identitätsmerkmale über standardisierte Schnittstellen an die entsprechende Anwendung weitergegeben (Spencer 2012; Zou et al. 2012).

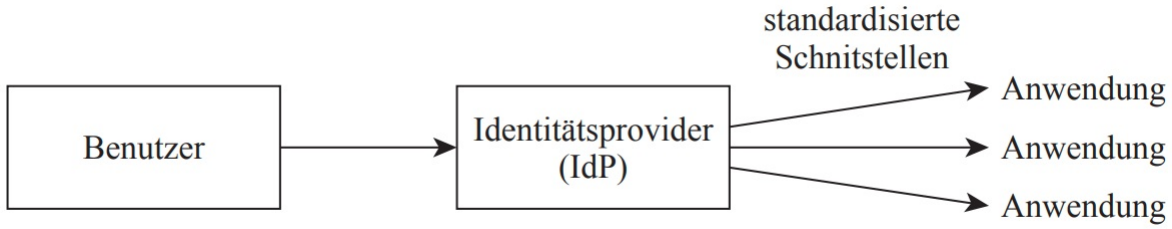


Abbildung 3: Cloud-basierte Authentifizierung über einen Identitätsprovider (IDP) (Borges und Werners 2018, S. 20, Abb. 2.1).

2.3 SDIKA

Das SDIKA ist ein Schaufensterprojekt in der Stadt Karlsruhe und der Metropolregion Rhein-Neckar. Es ist eines von vier vom Bundesministerium für Wirtschaft und Klimaschutz (BMWK) im Rahmen eines Innovationswettbewerbs geförderten Projekten mit dem Thema „Sichere Digitale Identitäten“ (BMWK 2023). Der Hintergrund des Wettbewerbs ist der Mangel an nutzerfreundlichen, vertrauenswürdigen und gleichzeitig wirtschaftlichen Lösungen für digitale Identitäten (BMWi 2019, S. 1-2).

Ziel des Projekts SDIKA ist die Entwicklung einer interoperablen software-basierten Lösung für digitale Identitäten. Das Projekt wird von der Stadt Karlsruhe koordiniert und in Kooperation mit diversen Partnern wie unter anderem dem FZI und Unternehmen aus dem Bereich der Software-Entwicklung sowie verschiedene Dienststellen der öffentlichen Verwaltung entwickelt (SDIKA 2023).[2]

[2]FZIchannel (05.07.2023). SDIKA - Schaufenster Sichere Digitale Identitäten Karlsruhe [Video]. Youtube. `https://www.youtube.com/watch?v=qM7zwwwKCDU`. Abgerufen am 28.07.2023.

2.3.1 Akteure

Das Projekt SDIKA definiert drei Rollen, die sich in drei verschiedenen Sphären befinden. Vertrauensdienste (Issuer-Sphäre), Akzeptanzstellen (Verifier-Sphäre) und Identitätsinhaber (Holder-Sphäre). Die Akteure und ihre Rollen sind in Tabelle 1 dargestellt.

Tabelle 1: Akteure in SDIKA (Projektpräsentation SDIKA 2021)

Akteur	**Sphäre**	**Aufgabe**
Vertrauensdienst	Issuer-Sphäre	Ausgabe von Identitäten
Identitätsubjekt	Holder-Sphäre	Entscheidet über Verwendung der eigenen Identität
Akzeptanzstelle	Verifier-Sphäre	Verifiziert und akzeptiert Identitäten

2.3.2 Technologie

Die technologische Kernkomponente des Schaufensterprojekts SDIKA ist das SDI-X System mit Open-Source Adapter. Mithilfe des Open-Source Adapters sollen Akzeptanzstellen die digitale Identitäten die von verschiedenen Ausgabestellen ausgegeben wurden überprüfen können. Interoperabilität ist ein wesentlicher Faktor, um ein offenes digitales Ökosystem zu gewährleisten. Der Open-Source Ansatz soll Vertrauen schaffen und die digitale Souveränität der Nutzer stärken (BMWK 2023).

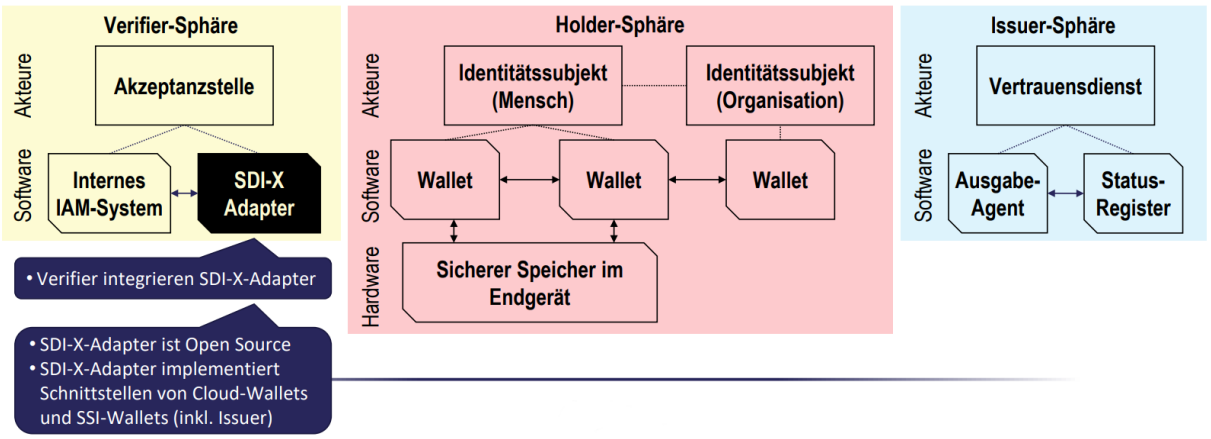


Abbildung 4: Darstellung des SDI-X Systems mit Open-Source Adapter (Projektpräsentation SDIKA 2021).

2.3.3 Use Cases

Im Umsetzungskonzept des Projekts SDIKA wurden unterschiedliche Use Cases beschrieben. Die Anwendungsbereiche der Identitätslösung umfassen E-Governance, Mobilität, Gesundheit, Digitales Planen und Bauen und Digitale Stadtgesellschaft.

Ein Vertrauensdienst wie beispielsweise eine Ausweisstelle stellt die digitale Identität an den berechtigten Anwender aus. Die verschiedenen Identitäten eines Anwenders können in einer digitalen Brieftasche (engl. Wallet) entweder lokal auf dem Smartphone oder in der Cloud gespeichert werden. Der Anwender kann dann mithilfe einer Wallet Applikation auf dem Smartphone frei entscheiden, welche Berechtigungsnachweise (engl. Credentials) er der Akzeptanzstelle zur Verfügung stellt.

Die Software-Hersteller Jolocom (Smartwallet) und CAS (SmartWe Network) waren ebenfalls (assoziierte) Partner im Projekt (SDIKA 2023).

Beispiel 1: Carsharing im Anwendungsbereich Mobilität
Der Carsharing-Dienst Stadtmobil Karlsruhe prüft bei jeder Neuanmeldung grundsätzlich, ob eine gültige Fahrerlaubnis vorliegt. Dafür muss der Nutzer persönlich in einem Kundenbüro erscheinen und seinen Führerschein und Personalausweis vorzeigen. Alternativ gibt es auch die Möglichkeit, seine Fahrerlaubnis über ein Video-Ident Verfahren zu verifizieren.[3]

Mithilfe der Identitätslösung von SDIKA soll dieser Prozess ersetzt werden. In der Wallet-Anwendung können Ausweisdokumente und andere Identitäten gespeichert werden, indem sich der Nutzer einem Vertrauensdienst gegenüber identifiziert. Der Benutzer gelangt in der App von Stadtmobil über einen Absprung zum Wallet und kann sich dort authentifizieren. Danach kann er auswählen, welche Identitätsdaten er zur Verfügung stellt und diese dann freigeben. Stadtmobil Karlsruhe kann die Freigaben verifizieren und der Benutzer kann, wenn die notwendigen Daten (Personalausweis, Fahrerlaubnis und Bankverbindung) geteilt wurden mit der Buchung eines Fahrzeuges fortfahren. (vgl. Auswahl Use Cases in BMWK 2023)

Beispiel 2: Karlsruher Pass
Der Karlsruher Pass ist ein Angebot der Stadt Karlsruhe für Einwohner mit geringem Einkommen bzw. Empfänger von Sozialleistungen. Inhaber des Karlsruher Passes sind in verschiedenen Einrichtungen des öffentlichen Lebens (z.B. Schwimmbäder, Theater oder im öffentlichen Nahverkehr) rabattberechtigt. Der Karlsruher Pass muss aktuell vor Ort bei einem von der Stadt Karlsruhe beauftragten Büro beantragt, persönlich abgeholt und

[3]Stadtmobil Karlsruhe. `https://karlsruhe.stadtmobil.de/privatkunden/so-funktionierts/`. Abgerufen am 24.03.2023.

nach zwölf Monaten verlängert werden.[4]

Mithilfe der Identitätslösung von SDIKA soll der Pass digital ausgestellt werden. Die Credentials können in die Wallet App exportiert werden. Mit der Wallet kann dann der Karlsruher Pass digital vorgezeigt werden um zum Beispiel Online eine Fahrkarte zu kaufen. Außerdem könnte die Verlängerung des Passes ebenfalls per App beantragt werden. (vgl. Auswahl Use Cases in BMWK 2023)

2.4 Requirements Engineering

Anforderungsmanagement (engl. Requirements Engineering, kurz RE) umfasst sowohl die Erhebung, Definition und Dokumentation von Anforderungen der Stakeholder als auch die Analyse, das Verifizieren, die Validierung und das systematische Verwalten sowie Kommunizieren dieser Anforderungen (Pohl 2008).

2.4.1 Hintergrund

Besonders im Bereich der Software-Entwicklung spielt das Anforderungsmanagement eine entscheidende Rolle. Je größer ein Software-Entwicklungsprojekt ist desto heterogener können die Anforderungen der Stakeholder an die Software sein. Wenn Anforderungen nicht vollständig erhoben werden, ist die Wahrscheinlichkeit, dass ein Software-Projekt scheitert, sehr hoch (vgl. Pohl 2008). Aus diesen Gründen gilt ein gutes Anforderungsmanagement als Voraussetzung für den Erfolg eines Software-Entwicklungsprojekts (vgl. Fuentes-Fernandez et al. 2009).

2.4.2 Anforderungstypen

Stakeholder haben unterschiedliche Arten von Anforderungen an ein Projekt. Um diese zu kategorisieren gibt es einen weit verbreiteten Ansatz. Typischerweise unterscheidet man die folgenden drei Anforderungstypen voneinander (Pohl 2008):

Funktionale Anforderungen
Ein Ergebnis oder ein Verhalten, das durch eine Funktion des Systems erfüllt werden soll, bezeichnet man als funktionale Anforderung. Ein System soll beispielsweise den Zweck erfüllen, für den es entwickelt wurde.

[4] Karlsruher Pass. `https://karlsruher-pass.de/karlsruher-pass`. Abgerufen am 24.03.2023.

Nicht-funktionale Anforderungen
Eine qualitative Anforderung, die nicht durch funktionale Anforderungen abgedeckt wird sondern sich auf einen Qualitätsaspekt beziehen, wird als nicht-funktionale Anforderung bezeichnet. Zum Beispiel könnte man Anforderungen bezogen auf die Nutzerfreundlichkeit, das Design oder die Performance eines Systems als nicht-funktionale Anforderungen bezeichnen.

Randbedingungen
Solche Bedingungen, die den Lösungsraum einschränken und die notwendig sind, um die funktionalen und nicht-funktionalen Anforderungen zu erfüllen. Randbedingungen lassen sich im Rahmen des Requirements Engineering (RE) nicht beeinflussen. Das können zum Beispiel externe Einschränkungen wie ökonomische und gesetzliche Rahmenbedingungen sein oder auch intern vorgegebene Restriktionen, die eingehalten werden müssen.

2.4.3 Kommunizierte und nicht-kommunizierte Anforderungen

Gerade bei großen Projekten mit heterogenen Stakeholdergruppen kann es passieren, dass nicht jede Anforderung durch die Stakeholder artikuliert wird. Eine nicht-kommunizierte Anforderung kann unterbewusst bei einem Stakeholder vorhanden sein, wird aber in einem Interview nicht geäußert, weil der Stakeholder die Anforderung zum Beispiel für selbstverständlich oder trivial hält, dass er sie gar nicht äußert (Kametani et al. 2010, S. 39-44.). Da in sozialen Situationen wie Interviews in natürlicher Sprache kommuniziert wird, besteht immer die Möglichkeit, dass Aussagen des Interviewpartners anders interpretiert werden, als sie gemeint waren (Ferrari et al. 2016; Sutcliffe und Sawyer 2013).

Aus diesen Gründen ist es wichtig, wenn sowohl die kommunizierten Anforderungen als auch die nicht-kommunizierten Anforderungen vollständig erheben werden sollen, vorab eine Stakeholderanalyse durchzuführen (Sutcliffe und Sawyer 2013).

3 Evaluationskriterien

Im Folgenden wird auf die Rahmenbedingungen der Evaluation eingegangen. Dabei werden zunächst die Ziele der Evaluation definiert. Danach werden die Kriterien für die Bewertung der Methode präzisiert. Anschließend werden die Kriterien für die Bewertung der Qualität der Ergebnisse definiert.

3.1 Ziele der Evaluation

Ziel dieser Arbeit ist die empirisch-wissenschaftliche Evaluation zu Kontrollzwecken. Einerseits soll überprüft werden, inwiefern die Methode MEADigS geeignet ist, die Zielvorgaben zu erreichen. Andererseits werden die Ergebnisse, die durch den Einsatz der Methode entwickelt werden, auf ihre Qualität geprüft werden. Ein quasi-experimenteller Ansatz bietet sich hierbei an (Kromrey 2001).

3.2 Durchführbarkeit der Methode

Für die Beurteilung der Durchführbarkeit der Methode wird die Art und Weise betrachtet, wie die definierten Ziele mit der Durchführung erreicht werden. Dabei sollen Rahmenbedingungen sowie Umgebungseinflüsse, die die Methode während der Durchführung beeinflussen, berücksichtigt werden (Kromrey 2001, S. 116-117). Außerdem sollen im Rahmen der Erfolgskontrolle die Effekte, die einzelne Maßnahmen der Methode bewirken und deren Auswirkung auf das angestrebte Ziel analysiert werden.

Klassische Erfolgskriterien für empirische Methoden aus anderen Fachgebieten sind Effektivität, Effizienz und Akzeptanz (Kromrey 2001, S. 114-115).

Auch speziell in Bezug auf Methoden für die Entwicklung von Anforderungen sind diese Kriterien anwendbar. Die Effektivität einer Methode wird im Requirements Engineering als maßgeblicher Faktor betrachtet (Davis et al. 2006; Gupta und Deraman 2019). Ebenso gilt der effiziente Einsatz von Zeit und Ressourcen im RE als entscheidend (Kanwal 2019). Auch die Akzeptanz der Teilnehmenden wird im RE als wichtig erachtet (Ribeiro et al. 2014).

Dementsprechend werden die drei Erfolgskriterien nachfolgend definiert.

3.2.1 Effektivität

Der Begriff der Effektivität beschreibt im Allgemeinen das „Ausmaß, in dem geplante Tätigkeiten verwirklicht und geplante Ergebnisse erreicht werden“ (DIN EN ISO 9000 2015, Nr. 3.7.11). Effektivität im Kontext des RE bezeichnet die Wirksamkeit einer Erhebungsmethode in Bezug auf die beabsichtigten Ziele. Die Frage nach dem Zielerreichungsgrad ist dabei zentral (Davis et al. 2006).

Man kann davon ausgehen, dass eine effektive Methode schlussendlich zu wünschenswerten und wertvollen Ergebnissen führt (Al-subaie und Maibaum 2006).

3.2.2 Effizienz

Im Gegensatz zur Effektivität bezieht sich der Begriff der Effizienz auf das „Verhältnis zwischen dem erzielten Ergebnis und den eingesetzten Mitteln“ (DIN EN ISO 9000 2015, Nr. 3.7.10).

Bei der Durchführung einer Methode können Faktoren wie Kosten-, Zeit- und Ressourcenaufwand betrachtet werden. Mit diesen Faktoren sollte stets effizient umgegangen werden, da sie nur begrenzt zur Verfügung stehen (Naeem et al. 2017; Weinreuter et al. 2023).

3.2.3 Akzeptanz

Ein weiteres Erfolgskriterium in Bezug auf die Durchführung einer Methode ist die Akzeptanz. Alle Akteure, die an der Durchführung beteiligt sind einschließlich der Stakeholder sollten die Methode annehmen (Kromrey 2001, S. 114-115).

Dazu gehört, dass sowohl die Teilnehmenden als auch die Akteure, die an der Durchführung beteiligt sind die Aktivitäten als angemessen und nutzbringend wahrnehmen (Weinreuter 2022, S. 31).

3.3 Qualität der Ergebnisse

Um eine Methode mit klar definierten Zielen zu evaluieren, muss die Qualität der Zielerreichung geprüft werden. Hierfür werden Kriterien aufgestellt, die nachvollziehbar und überprüfbar sind (Kromrey 2001, S. 107-112).

Da es sich bei MEADigS um eine Methode des RE handelt, werden die im Rahmen der Durchführung entwickelten Anforderungen mithilfe von Requirements Engineering Ob-

jectives (REO) bewertet. Die Bewertungskriterien Vollständigkeit, Korrektheit, Sachdienlichkeit, Konsistenz, Nachvollziehbarkeit und Eindeutigkeit werden festgelegt (Al-subaie und Maibaum 2006, S. 4-7). Im Folgenden werden diese REOs definiert und erläutert.

3.3.1 Vollständigkeit

Anforderungen können aus verschiedenen Gründen unvollständig sein. Entweder weil einzelne Aspekte schlicht vergessen werden oder ein Stakeholder annimmt, dass jemand anderes für die Dokumentation einer bestimmten Anforderung verantwortlich ist. Gerade bei größeren Projekten ist daher auf die Vollständigkeit (engl. completeness) der Anforderungen zu achten. Das Überprüfen der Vollständigkeit der erhobenen Anforderungen stellt sich allerdings als komplex dar (Sinha und Popken 1996, S. 263).

Im Kontext von MEADigS ist insbesondere die Vollständigkeit in Bezug auf die Dimensionen digitaler Souveränität (Abschnitt 2.1.2 und auf die Arten der Anforderungen (kommunizierbare als auch nicht-kommunizierbare Anforderungen) von Bedeutung (Weinreuter 2022, S. 30).

3.3.2 Korrektheit

Das Konzept der Korrektheit (engl. correctness) stellt ein schwer zu fassendes Konzept dar. Es beschreibt die Übereinstimmung mit den tatsächlichen Bedürfnissen der Stakeholder (Zowghi und Gervasi 2003, S. 997).

Formal lässt sich feststellen, dass unter Korrektheit eine Kombination aus Vollständigkeit und Konsistenz verstanden werden kann. In der Praxis dient die Erfüllung von Anforderungen dazu, dass bestimmte Geschäftsziele erreicht werden können. Der Beweis der Eigenschaft der Korrektheit von Anforderungen ist eine schwierige Aufgabe.

Um sicherzustellen, dass Fehler erkannt und als solche gekennzeichnet werden, existieren verschiedene Arten der Validierungsprüfung, die eingesetzt werden können (Zowghi und Gervasi 2003, S.993-994). Beispielsweise können Software-Werkzeuge zur automatischen Erkennung von semantischen Fehlern, Tippfehlern oder Inkonsistenzen eingesetzt werden (Heitmeyer et al. 1996).

3.3.3 Sachdienlichkeit

Anforderungen sollten auf Sachdienlichkeit oder auch Relevanz (engl. pertinence) geprüft werden. Gerade wenn bei der Anforderungserhebung mit Szenarien oder User Storys gearbeitet wird, kann es schnell passieren, dass Anforderungen formuliert werden, die für das Projekt nicht relevant sind. Szenarien beinhalten häufig Details, die dazu da sind, das Verständnis für das Projekt zu verbessern. Das kann wiederum dazu führen, dass gerade durch potentielle Nutzer formulierte Anforderungen eine Menge Details beinhalten können, die nicht relevant für das Projekt sind.

Um die Sachdienlichkeit von Anforderungen sicherzustellen, können Anforderungen beispielsweise eine Validierungsprozess durchlaufen (Sabatucci et al. 2015, S. 124-126).

3.3.4 Konsistenz

Unter Konsistenz (engl. consistency) versteht man die Widerspruchsfreiheit der Anforderungen. Unstimmigkeiten können viele verschiedene Ursachen haben. Beispielsweise kann es passieren, dass zwei durch verschiedene Stakeholder geäußerte Anforderungen miteinander in Konflikt stehen oder sich sogar widersprechen. In diesem Fall wäre es nicht möglich, eine praktikable Lösung zu finden.

Außerdem kann es vorkommen, dass eine Anforderung durch das System gar nicht erfüllt werden kann. Darüber hinaus kann es zu Inkonsistenzen kommen, wenn mehrere Stakeholder die gleiche Anforderung formuliert haben.

Eine weitere Form der Inkonsistenz kann auftreten, wenn ein und derselbe Begriff für unterschiedliche Dinge verwendet wird oder wenn unterschiedliche Begriffe dieselbe Sache bezeichnen (Sinha und Popken 1996, S. 263-264).

3.3.5 Nachvollziehbarkeit

Unter Nachvollziehbarkeit (engl. tracability) versteht man die Fähigkeit, den Lebenszyklus einer Anforderung zu verfolgen. Diese Art der Rückverfolgung sollte sowohl in die direkt als auch in die entgegengesetzte Richtung möglich sein.

Rückverfolgbare Anforderungen ermöglichen es, Zeit zu sparen und Kosten zu senken. Dadurch kann die Qualität der Ergebnisse verbessert werden (Murtazina und Avdeenko 2019, S. 628-629).

3.3.6 Eindeutigkeit

Die Verwendung von mehrdeutigen Begriffen stellt eine potentielle Quelle für Unstimmigkeiten zwischen den Erwartungen der Stakeholder und der Lösung dar. Durch Personen geäußerte mehrdeutige Aussagen können dazu führen, dass nachträglich im Rahmen der Entwicklung ein Produkt oder ein Artefakt nachbearbeitet werden muss, weil die Anforderung bereits zu Beginn des Erhebungsprozesses missverständlich beschrieben wurde. Daher gilt Eindeutigkeit (engl. unambiguity) als ein wichtiges Kriterium im RE (Fantechi et al. 2023).

Anforderungen werden im Allgemeinen in natürlicher Sprache verfasst. Damit Software auch auf die Anforderungen der Stakeholder erfüllen kann ist es essentiell, die Mehrdeutigkeiten aus diesen Texten zu entfernen und Anforderungen eindeutig zu beschreiben. Dieser Prozess stellt sich häufig als recht komplex dar (Kato und Tsuda 2022, S. 1483).

4 Adaption der Methode

Im Rahmen dieser Arbeit soll MEADigS im Projekt SDIKA angewendet werden. Dafür wurden spezifische Modifikationen an einzelnen Aspekten der Methode vorgenommen. In den nachfolgenden Abschnitten wird zunächst die Methode MEADigS vorgestellt. Anschließend werden die vorgenommenen Anpassungen der Methode erläutert und begründet.

4.1 MEADigS

Die Methode zur Entwicklung von Anforderungen im Bereich der digitalen Souveränität (MEADigs bzw. engl. MERDigS) wurde am FZI entwickelt (Weinreuter 2022; Weinreuter et al. 2023).

Die MEADigS adaptiert verschiedene bestehende Verfahren auf dem Gebiet des RE mit dem Ziel, eine Methode speziell auf die Anforderungserhebung im Kontext der digitalen Souveränität auszurichten.

Der daraus entstandene Methodenleitfaden skizziert eine schrittweise Vorgehensweise, mit der Anforderungen der verschiedenen Stakeholder ermittelt werden können.

Da die Methode im Rahmen des Projekts SDIKA entstanden ist, sollte sie auch mindestens in diesem Kontext anwendbar sein.

Ziel von MERDigS ist die Erhebung der Anforderungen auf dem Gebiet der digitalen Souveränität möglichst aller Stakeholder an ein Software-Entwicklungsprojekt.

Dabei sollten idealerweise auch solche Anforderungen vollständig erhoben werden, die nicht direkt durch Stakeholder kommuniziert werden (siehe Abschnitt 2.4.3).

Eine erste Evaluation fand mithilfe von drei Experteninterviews statt, bei denen Projektmitarbeiter des Projekts SDIKA befragt wurden. Hierbei wurden die Kriterien Durchführbarkeit, Akzeptanz und Zeitplan betrachtet.

Die erste Einschätzung der Experten war, dass die Methode grundsätzlich plausibel sei. Je nach Größe des Software-Entwicklungsprojekts könne die vollständige Durchführung Methode aber in ihrer Gesamtheit etwas zu aufwändig und komplex sein (Weinreuter 2022, S. 68-78).

Es folgt eine kurze Darstellung der Rollen in MEADigS, der einzelnen Schritte der Durchführung und des Ziels der Evaluation.

4.1.1 Wichtige Rollen in MERDigS

Analytiker
Der Analytiker trägt die Verantwortung für Aktivitäten innerhalb des Software-Entwicklungsprojekts (z.B. Entwickler oder Projektmanager). Er sollte über umfassendes Wissen über das Projekt verfügen.

Diese Rolle kann auch durch mehrere Personen besetzt werden.

Moderator
Der Moderator führt Workshops aus MERDigS Schritt 4 durch und ist für die Sicherung der Ergebnisse verantwortlich. Da er zwischen Stakeholdervertretern und Analytikern vermittelt, sollte ebenfalls die Rolle des Analytikers haben.

Stakeholdervertreter
Stakeholder im Kontext der Softwareentwicklung bezeichnet jemanden, der ein Interesse am Gelingen eines Vorhabens oder Projekts hat (Miles 2017).

Ein Stakeholdervertreter im Sinne von MEADigS unterstützt bei den Erhebungsaktivitäten und lässt sich dazu befragen. Er ist bereit, seine Bedürfnisse und Wünsche zu äußern und zu diskutieren. Er vertritt einen Stakeholdertyp.

Fokusgruppenteam
Das Fokusgruppenteam besteht bestenfalls aus vier bis neun Stakeholdervertretern. Diese sollten möglichst heterogen die verschiedenen Standpunkte der Stakeholder abbilden. Sie nehmen an fokusgruppenähnlichen Workshops teil und repräsentieren dabei eine Stakeholdergruppe.

4.1.2 Ablauf

MERDigS gliedert sich in sechs Schritte. Mit jedem Schritt soll der Informationsgehalt größer werden. Der Ablauf und der relative Informationsgehalt im Laufe der Durchführung wird in Abbildung 5 dargestellt. Die einzelnen Schritte werden im Folgenden kurz beschrieben.

Schritt 1: Verständnisaufbau und Registrierung der Themenfelder
Im ersten Schritt baut der Analytiker durch intensive Recherche ein umfassendes Verständnis für das Thema digitale Souveränität auf. Mit diesem Wissen wird ein Themenfeldregister erstellt.

Mit dem Themenfeldregister werden Anforderungen in Kategorien eingeteilt. Die Themenfelder werden eingegrenzt damit der Fokus auf noch nicht erhobene Anforderungen im Bereich der digitalen Souveränität bleibt.

Schritt 2: Analyse der Stakeholder
Nachdem im ersten Schritt das Themenfeldregister erstellt wurde, kann mit der Analyse der Stakeholder begonnen werden. Dabei werden die Stakeholder durch den Analytiker identifiziert, gegebenenfalls in Gruppen eingeteilt oder Typen zugeordnet.

Hierdurch soll ein Verständnis aufgebaut werden, in welcher Beziehung die Stakeholder zu dem Projekt stehen und welche Ziele sie verfolgen. Ein Stakeholderregister soll erstellt werden, welches die Stakeholdertypen, ihre Eigenschaften und die deren Anforderungen erfasst.

Schritt 3: Analyse von Dokumenten
Anschließend können das Themenfeld- und das Stakeholderregister verwendet werden, um Dokumente zu identifizieren, die analysiert werden sollten. Das Ziel der Analyse von Dokumenten ist, ein tieferes Verständnis für die Eigenschaften, Bedürfnisse und Wünsche der unterschiedlichen Stakeholdertypen zu entwickeln und daraus Grundanforderungen abzuleiten, die in den ersten beiden Schritten noch nicht entdeckt worden sind. Hierbei soll insbesondere auf möglicherweise nicht-kommunizierte Anforderungen (siehe Abschnitt 2.4.3) geachtet werden.

Die aus den Schritten 1 bis 3 abgeleiteten Grundanforderungen werden in einem Anforderungsdokument festgehalten.

Schritt 4: Durchführung fokusgruppenähnlicher Workshops
Mit den Stakeholdergruppen werden dann fokusgruppenähnliche Workshops durchgeführt. Aus jeder Gruppe werden mehrere Personen eingeladen, die alle zu einer Stakeholdergruppe zugeordnet werden können.

Zu Beginn des Workshops werden die Grundanforderungen, aus den Schritten 1-3 validiert. Dies erfolgt in elektronischer Form durch Ja/Nein Fragen. Im weiteren Verlauf bekommen die Teilnehmenden Zeit für ein individuelles Brainstorming.

Anschließend werden die Ergebnisse des Brainstorming diskutiert, gruppiert und als Anforderungen festgehalten („KJ-ähnliche Session“ (Scupin 2008,Weinreuter 2022, S. 104-

111)). Diese beiden Schritten können gegebenenfalls wiederholt werden.

Danach folgt, falls möglich, eine Use-Case-Betrachtung. Hierbei werden Szenarien anhand von Prototypen vorgestellt, sofern bereits Prototypen existieren. Die Betrachtung der Use-Cases veranschaulicht das Projekt und regt zur weiteren Diskussion an, bei der ebenfalls Anforderungen erfasst werden können.

Schlussendlich erhalten die Teilnehmenden noch die Möglichkeit, Anforderungen nachzureichen, falls ihnen in den Tagen nach dem Workshop während der Selbstbeobachtung noch weitere Anforderungen einfallen.

Für jede Stakeholdergruppe wird ein separater Workshop veranstaltet.

Ziel der Workshops ist es, die Grundanforderungen zu validieren und neue Anforderungen zu erheben.

Schritt 5: Durchführung von Interviews mit Stakeholdervertretern
Nachdem die Grundanforderungen erhoben sind, werden Interviews mit einzelnen Stakeholdervertretern durchgeführt.

Die persönlichen Gespräche sollen dabei helfen, Qualitätsanforderungen zu identifizieren. Insbesondere für die Erfassung von nicht-kommunizierten Anforderungen soll die Form des semi-strukturierten Interviews ein zielführendes Verfahren darstellen. Das Ergebnis des fünften Schrittes ist eine möglichst vollständige Erhebung aller Anforderungen.

Schritt 6: Quantitative Erfassung und Validierung der Anforderungen
Im letzten Schritt werden die Anforderungen aus dem Anforderungsdokument zunächst quantitativ erfasst. Die Validierung erfolgt mittels Fragebögen, die an eine repräsentative Stichprobe der Stakeholder verteilt werden. Das Ziel der Befragung ist, offene Fragen zu klären und die Anforderungen zu priorisieren.

Das Ergebnis des sechsten Schritts soll ein vollständiges Anforderungsdokument sein.

4.1.3 Erprobung und Evaluation der Methode

MERDigS wurde auf theoretischer Ebene entwickelt und auf Plausibilität geprüft, allerdings noch nicht in der Praxis angewendet. Die Evaluation durch Experteninterviews gibt erste Anhaltspunkte. Im Rahmen dieser Arbeit soll die Methode praktisch erprobt und anschließend evaluiert werden. Die Anwendung erfolgt am Beispiel digitaler Identitätslösungen im Rahmen des Projekts SDIKA.

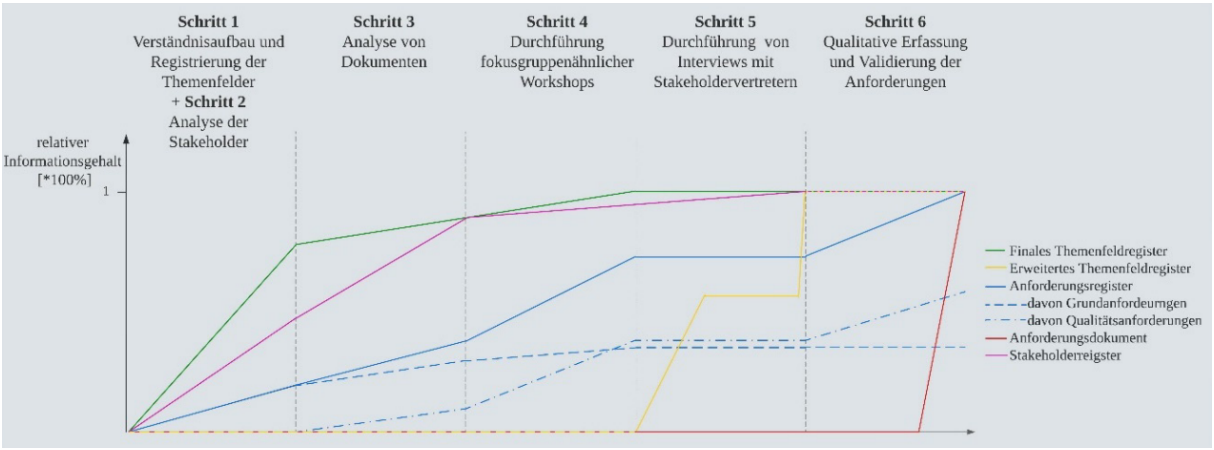


Abbildung 5: Ablauf von MERDigS und relativer Informationsgehalt (Weinreuter 2022, Abb. 12).

4.2 Einschränkung der Stakeholdergruppen

Da diese Arbeit einen begrenzten Umfang hat, wird die Zahl der zu betrachtenden Stakeholdergruppen reduziert. Da die Stadt Karlsruhe und die Metropolregion Rhein-Neckar bereits Veranstaltungen zur Bürgerbeteiligung organisiert haben, sollte in dieser Arbeit der Fokus auf Unternehmen und anderen Organisationen liegen. Dabei wurde sich auf zwei Gruppen beschränkt. MEADigS wurde im Rahmen dieser Arbeit für die folgenden Stakeholder durchgeführt:

1. **Unternehmen und Organisationen als Identitätsinhaber**
2. **Akzeptanzstellen für digitale Identitäten**

Da über das FZI der Kontakt zu diversen Vertretern der Projektpartner besteht, die zu einer oder mehreren der genannten Rollen zugeordnet werden können, bot es sich an, die einzelnen Schritte von MEADigS mit diesen Vertretern durchzuführen. Die Einteilung der Stakeholder in Stakeholdergruppen und Stakeholdertypen erfolgt in der Analyse der Stakeholder in Abschnitt 4.4.

4.3 Verständnisaufbau und Registrierung der Themenfelder

Der erste Schritt in MEADigS wurde wie in der Methode beschrieben durchgeführt. Die Rolle des Analytikers wurde vom Verfasser dieser Arbeit übernommen. Die Liste mit möglichen Themenfeldern (Weinreuter 2022, Tabelle 10 in Anhang F) wurde als Vorlage verwendet und angepasst, wobei zwei Themenfelder aus dem Register entfernt wurden, die als nicht relevant betrachtet werden können.

Gesundheit Ziel des Projekts SDIKA ist es, eine sichere, wirtschaftliche, nutzerfreundliche Lösung für digitale Identitäten zu entwickeln, die die Privatsphäre der Personen schützt (BMWi 2019; Projektpräsentation SDIKA 2021). Eine direkte Auswirkung auf die Gesundheit besteht nicht.

Selbstverwirklichung Eine Lösung für digitale Identitäten kann die digitale Souveränität stärken und den Alltag erleichtern. Die Möglichkeiten zur Selbstverwirklichung werden dadurch nicht unmittelbar beeinflusst.

Da es sich bei beiden untersuchten Stakeholdergruppen um Unternehmen oder Organisationen handelt (siehe Abschnitt 4.2), kann bei beiden Gruppen das gleiche Themenfeldregister verwendet werden. Das Themenfeldregister befindet sich in Tabelle 10 in Anhang A. Bereits erhobene Anforderungen lagen zum Zeitpunkt der Durchführung nicht als Eingabe vor.

4.4 Analyse der Stakeholder

Mithilfe der Projektpräsentation (SDIKA 2023) und den Informationen zu den (assoziierten) Partnern und Use-Cases im Projekt (Abbildung 6) kann ein Überblick gewonnen und mögliche Stakeholder identifiziert werden. Entsprechend werden Vertreter von Unternehmen und Organisationen als Teilnehmende für die Workshops in Schritt 4 eingeladen.

Über die Webseiten dieser Unternehmen und Organisationen lassen sich Informationen gewinnen, die in das Stakeholderregister (Anhang B) mit aufgenommen werden.

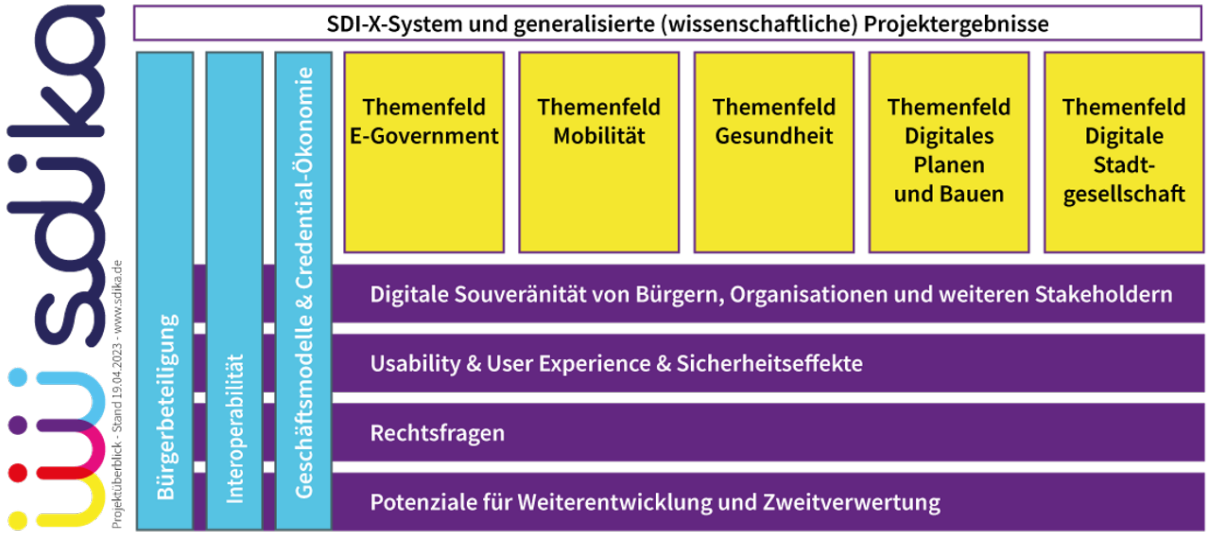


Abbildung 6: Projektübersicht SDIKA (Brazel et al. 2023).

Die Stakeholder werden aufgelistet und einer Stakeholdergruppe zugeordnet. Die Einteilung in die Stakeholdergruppen Natürliche Personen, Staat, Öffentliche Verwaltung und Organisationen ist angelehnt an Weinreuter 2022, Tabelle 6. Die Unterteilung der Stakeholder in verschiedene Stakeholdertypen ergibt sich aus den Rollen der Akteure in SDIKA (Abschnitt 2.3.1), wobei als zusätzliche Rolle noch der Betreiber der digitalen Wallet hinzukommt. Anhand der möglichen Kombinationen aus Stakeholdergruppe und möglicher Rolle ergeben sich acht Stakeholdertypen (siehe Tabelle 2).

Tabelle 2: Stakeholdergruppen und mögliche Rollen in SDIKA

Stakeholdergruppe	**mögliche Rollen in SDIKA**
Natürliche Personen	Identitätsinhaber
Öffentliche Verwaltung	**Akzeptanzstelle**, **Identitätsinhaber**, Vertrauensdienst
Organisationen aus der Zivilgesellschaft, Wissenschaft und Wirtschaft	**Akzeptanzstelle**, **Identitätsinhaber**, Vertrauensdienst, Wallet-Betreiber

Die im Folgenden mithilfe von MEADigS betrachteten Stakeholdertypen sind in der Tabelle fett markiert. Der Staat (Bund, Länder und Landkreise) ist zwar prinzipiell auch ein Stakeholder sicherer digitaler Identitäten, tritt aber in der Lösung von SDIKA nicht als Akteur auf. Handelnder Akteur im Namen des Staates sind Organisationen der öffentlichen Verwaltung wie beispielsweise Behörden. Somit wird der Staat im Folgenden nicht als Stakeholdergruppe aufgeführt.

4.5 Analyse von Dokumenten

Um ein umfassendes Bild der Themenfelder, Stakeholder und des Projekts SDIKA zu erarbeiten, wurde eine Literaturrecherche zu dem Themenkomplex digitale Identitäten durchgeführt. Bestehende Lösungen zu digitalen Identitäten von privaten Anbietern wurden gesichtet. Zusätzliche Informationen zu den Hintergründen und der Entstehung des Innovationswettbewerbs Sichere Digitale Identitäten konnten aus den entsprechenden Webseiten gewonnen werden.[5]

Des Weiteren wurden die verfügbaren klickbaren Prototypen, die bereits entwickelt wurden, gesichtet. Die Publikationen, die im Rahmen des Projekts SDIKA veröffentlicht wurden, wurden studiert (Rotthaus 2022; Alpers et al. 2020). Ein Glossar wurde angelegt und im Laufe der weiteren Durchführung von MEADigS iterativ mit Inhalten befüllt (Tabelle 12).

4.6 Ablauf der fokusgruppenähnlichen Workshops

MEADigS sieht vor, dass Workshops online durchgeführt werden. (Weinreuter 2022, S. 63) Aufgrund der Tatsache, dass es sich bei SDIKA um ein regionales Schaufensterprojekt handelt und sich die Tätigkeitsstätten vieler potentieller Teilnehmender in der Region befinden, war es möglich, beide Workshops in Präsenz durchzuführen. Da die Teilnehmenden selbst als Partner in das Projekt eingebunden waren, sind die Hintergründe und die Ziele von SDIKA den Teilnehmenden bereits bekannt. Daraus ergeben sich einige Anpassungen der Aktivitäten in der Methode.

Die Präsentationsfolien für die Workshops wurden im Nachgang um die Dokumentation der Ergebnisse ergänzt und veröffentlicht (Brazel et al. 2023).

[5] BMWK: Schaufenster Sichere Digitale Identitäten. Programm. `https://www.digitale-technologien.de/DT/Navigation/DE/ProgrammeProjekte/AktuelleTechnologieprogramme/Sichere_Digitale_Identitaeten/Programm/programm.html`. Abgerufen am 16.02.2023.

4.6.1 Fokus auf digitale Souveränität

Bereits in der Vorstellungsrunde bekommen die Teilnehmenden die Frage gestellt: „Was verstehen Sie unter digitaler Souveränität?“. Im Anschluss werden Definitionen digitaler Souveränität vorgestellt (siehe Abschnitt 2.1). Dadurch soll ein gemeinsames Verständnis der Teilnehmenden für digitale Souveränität erreicht werden. Darüber hinaus können die Aussagen in der Vorstellungsrunde ggf. Rückschlüsse darauf geben, welche Aspekte den Teilnehmenden besonders wichtig sind.

4.6.2 Vorstellung des Software-Entwicklungsprojektes

Die Vorstellung fällt kurz aus. Eine detaillierte Erörterung des Projekts ist nicht notwendig, da das Projekt SDIKA allen Teilnehmenden bekannt ist. Es wird zu Beginn des Workshops nur ein kurzer Überblick über das Projekt gegeben.

4.6.3 Einschränkung auf die zu betrachtende Rolle

Da Unternehmen und Organisationen in unterschiedlichen Rollen mit digitalen Identitäten zu tun haben, im Rahmen der Workshops aber nicht davon ausgegangen werden kann, dass jeder Workshopteilnehmende auch tatsächlich Teil der betrachteten Stakeholdergruppe ist, werden zu Beginn die verschiedenen Rollen aus Tabelle 1 besprochen und die Teilnehmenden darauf Aufmerksam gemacht, dass die Fragestellungen aus der Perspektive der entsprechenden Rolle (Unternehmensidentitäten bzw. Akzeptanzstellen) betrachtet werden sollen.

Aufgrund der Tatsache, dass die Teilnehmenden in das Projekt SDIKA involviert sind, kann davon ausgegangen werden, dass sie sich in die entsprechende Rolle hinein versetzen können.

4.6.4 Validierung der Grundanforderungen

Die Teilnehmenden sind (assoziierte) Partner des Projekts SDIKA und damit Experten für das Projekt. Die Ziele des Projekts sind bereits definiert, eine Liste mit bereits bestehenden Anforderungen liegt allerdings nicht vor. Die Validierung von Grundanforderungen als Bestandteil der Workshops entfällt daher.
Der Fokus der Workshops liegt stärker auf der Erhebung der qualitativen Anforderungen und dem gegenseitigen Austausch der Teilnehmenden über diese Anforderungen.

4.6.5 Individuelles Brainstorming

Zu Beginn des individuellen Brainstormings bekommen die Teilnehmenden nur die Frage („Was erwarten Sie von einer Lösung für digitale Identitäten?“) gestellt und können frei ihre Anforderungen aufschreiben. Nach zehn Minuten bekommen die Teilnehmenden mögliche Themenfelder stichpunktartig auf einer Powerpoint-Folie präsentiert. Die Themenfelder stammen aus dem *Themenfeldregister* (Tabelle 10) und dienen als Anregung für weitere Ideen für Anforderungen.

4.6.6 KJ-ähnliche Session

Da die Workshops in Präsenz stattfinden, ist es nicht notwendig, ein digitales Brainstorming-Werkzeug zu verwenden. Stattdessen kann das Brainstorming in Form einer Karten-Abfrage (angelehnt an Seifert 2020, S. 120) analog stattfinden. Auf eine Gruppierung von ähnlichen Karten in Themenfelder wird im Rahmen der Workshops verzichtet. Dadurch bleibt mehr Zeit für Diskussion unter den Teilnehmenden.

Durch die Erläuterung der Anforderungen im Teilnehmendenkreis wird sichergestellt, dass alle das gleiche Verständnis für die jeweilige Anforderung haben. Eine Gruppierung kann im Nachgang durch den Analytiker durchgeführt werden.

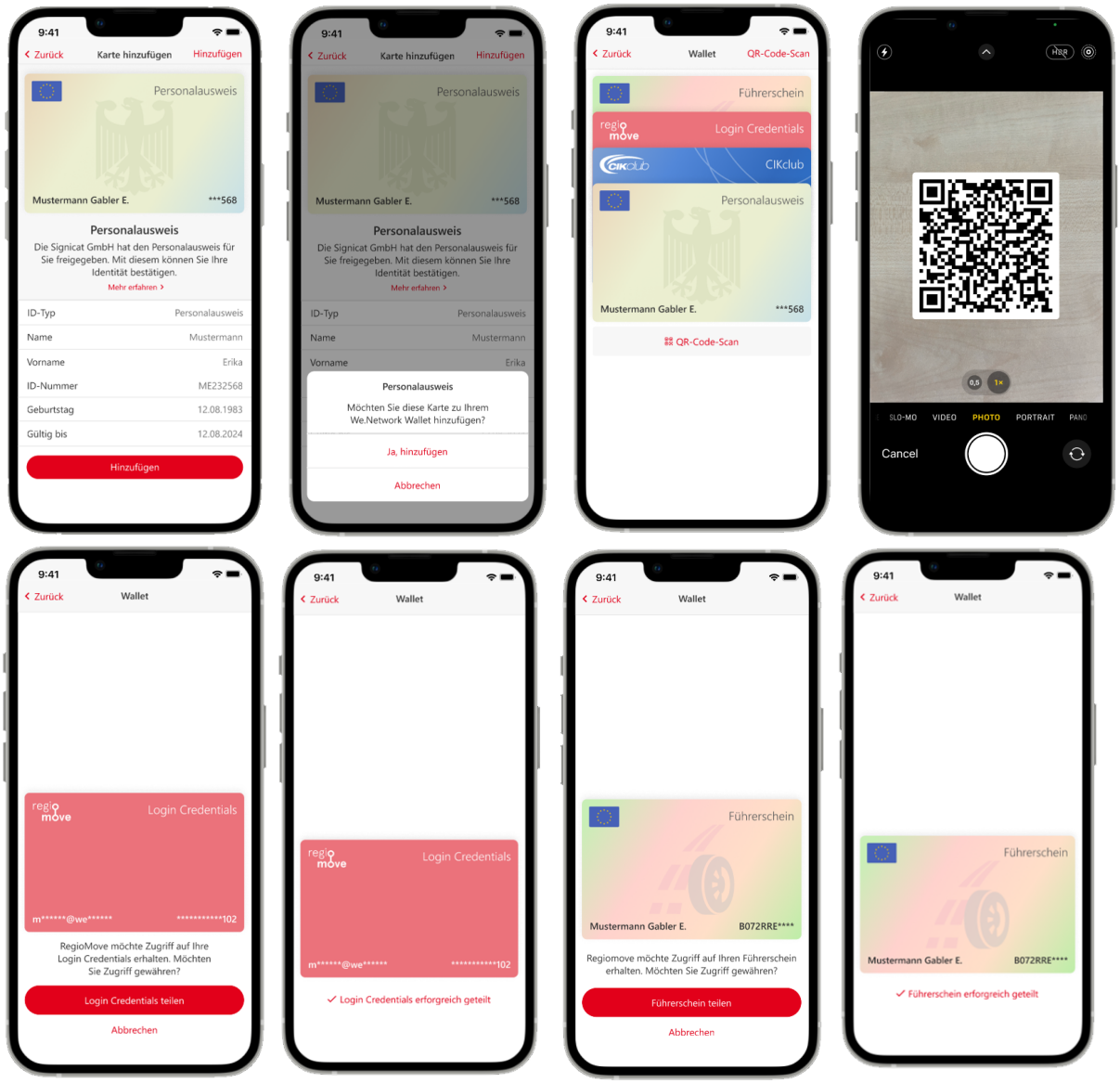
4.6.7 Aufzeichnung der Anforderungserhebung

Aus datenschutzrechtlichen Gründen werden die Workshops nicht auf Video oder Ton aufgezeichnet. Stattdessen erfolgt die Dokumentation der Ergebnisse zunächst durch ein Protokoll.

4.6.8 Use-Case Betrachtung

Zum Zeitpunkt der Durchführung der Workshops waren mehrere Prototypen („Mockups“) zur Demonstration verfügbar. In beiden Workshops wurden die Mockups *Buchung eines Carsharing-Fahrzeuges* und *Karlsruher Pass* (siehe Abschnitt 2.3.3) vorgeführt. Im Workshop zu Unternehmensidentitäten wurde der Protoyp zur Buchung eines Carsharing-Fahrzeuges in modifizierter Form aus Unternehmenssicht vorgeführt (Abbildung 7). Zusätzlich wurden die Mockups auch auf Tablets bereitgestellt, damit interessierte Teilnehmende auch die Gelegenheit haben, interaktiv die Mockups zu begutachten.

Abbildung 7: Auszug aus den SDIKA Prototypen.[6]



[6]Screenshots aus: FZIchannel (05.07.2023). SDIKA - Schaufenster Sichere Digitale Identitäten Karlsruhe [Video]. Youtube. `https://www.youtube.com/watch?v=qM7zwwwKCDU`. Abgerufen am 28.07.2023.

4.6.9 Weitere Use-Cases und Fragestellungen

Für den Fall, dass in einer Diskussion nach der Use-Case Betrachtung weitere Fragestellungen oder Ideen für weitere Use-Cases für Unternehmensidentitäten aufkommen, wird ein Flipchart bereitgestellt, auf denen diese Gedanken festgehalten werden können. Mit der Frage nach weiteren Anwendungsfällen aus Sicht der Unternehmen werden diese abgefragt.

4.6.10 Zweites Brainstorming und Diskussion

Sofern in den Workshops eine produktive Diskussion entsteht, kann das zweite Brainstorming auch als offene Runde durchgeführt werden. In diesem Fall können die Teilnehmenden gemeinsam im Dialog weitere Anforderungen formulieren. Der Fokus sollte dann noch einmal auf das Thema digitale Souveränität gelenkt werden. Dafür wird die Frage gestellt: „Welche zusätzlichen Anforderungen ergeben sich aus dem Anspruch der digitalen Souveränität?“

4.6.11 Vorbereitung der angepassten Workshops

Für die Vorbereitung auf die Workshops wurde eine Materialliste und ein Plan erstellt (Abbildung 8). Die Moderation der beiden Workshops wird mithilfe des Methodenplans der fokusgruppenähnlichen Workshops in Tabelle 3 durchgeführt.

Abbildung 8: Materialliste und Vorbereitung der Workshops

Materialliste

- Beamer, Laptop (ggf. Tablets)
- 3 Pinnwände oder Magnetwände
- 1 Flipchart
- Bunte Karteikarten
- Pins bzw. Magneten
- Weißes DIN A4-Papier
- Stifte

Vorbereitung

- Stühle im Halbkreis anordnen
- Tische beiseite stellen
- Flipchart bereitstellen, um Ideen zu sammeln
- Prototypen in Adobe XD öffnen
- Verpflegung bereitstellen

Tabelle 3: Methodenplan der fokusgruppenähnlichen Workshops

	Zeitaufwand	Inhalt	Ziel	Methodik	Hilfsmittel
1.Begrüßung/ Einführung	30 Minuten	Begrüßung, Vorstellung des Themas und der Ziele des Workshops, Präsentation der Agenda, Vorstellung des Moderators, Vorstellungsrunde Teilnehmende, Definitionen digitaler Souveränität, Kurze Vorstellung des Projekts SDIKA, der Akteure und der Perspektive (Unternehmensidentitäten bzw. Akzeptanzstellen).	Kennenlernen, gemeinsames Verständnis der Zielsetzung schaffen	-	Powerpoint-Präsentation, Namensschilder, Stifte
2.Individuelles Brainstorming	15 Minuten	Teilnehmende bekommen Zettel und Stifte ausgeteilt, Zeit für individuelles Brainstorming. Fragestellung: „Was erwarten Sie von einer Lösung für digitale Identitäten?“, Nach 10 Minuten werden als Anregung die möglichen Themenfelder aus dem Themenfeldregister gezeigt	Erhebung der Anforderungen	individuelles Brainstorming, KJ-ähnliche Session	Powerpoint-Präsentation, Karteikarten, Stifte
3.Diskussion	45 Minuten	Anforderungen werden einzeln vom Moderator vorgelesen. Jeder Teilnehmende hat die Möglichkeit, seine Anforderungen zu erklären und Rückfragen zu den Anforderungen der anderen Teilnehmenden zu stellen.	Sammlung und Erörterung der Anforderungen	KJ-ähnliche Session, Dialog	Stellwände, Karteikarten, Stifte
4.Use-Case Betrachtung	45 Minuten	Prototypen werden auf dem Beamer vorgeführt, Teilnehmende bekommen die Möglichkeit, Fragen zu stellen und Feedback zu den Prototypen zu geben. Prototypen können auch auf Mobilgeräten präsentiert werden. Frage: „Welche Anwendungsfälle ergeben sich aus Sicht der Unternehmensidentität?“. Moderator nimmt die vorgeschlagenen Anwendungsfälle schriftlich auf Flipchart auf	Gemeinsames Verständnis für die Use-Cases schaffen	(interaktive) Vorführung der Prototypen	Adobe XD
5.Brainstorming und Diskussion	30 Minuten	Teilnehmende können mit den Anregungen aus der Use-Case Betrachtungen weitere Anforderungen formulieren und diskutieren. Fragestellungen: „Welche zusätzlichen Anforderungen ergeben sich aus dem Anspruch der digitalen Souveränität?“ und „Welche Anforderungen ergeben sich aus den Use-Cases?“	Ideen für weitere Use-Cases sammeln, Erhebung weiterer Anforderungen	KJ-Ähnliche Session, Dialog	Stellwände, Karteikarten, Stifte
6.Feedback/ Verabschiedung	30 Minuten	Teilnehmende bekommen die Möglichkeit, Feedback zum Workshopformat zu geben. Teilnehmende werden angeregt, Anforderungen nachzureichen, falls ihnen im Nachgang noch weitere Ideen kommen. Danksagung und Verabschiedung durch den Moderator	Abschluss der Moderation	Dialog	-

5 Durchführung und Ergebnisse

In diesem Kapitel werden die Ergebnisse der Anforderungserhebung präsentiert. Zunächst wird die Durchführung der fokusgruppenähnlichen Workshops beschrieben. Anschließend werden die erzielten Ergebnisse dargestellt und analysiert.

5.1 Durchführung der fokusgruppenähnlichen Workshops

Die beiden Workshops wurden im April 2023 in den Räumlichkeiten des FZI in Karlsruhe durchgeführt. Hierfür wurde eine größere Menge an potentiellen Teilnehmenden aus dem Projekt angefragt, um auch bei kurzfristigen Absagen noch hinreichend viele Teilnehmende zu haben. Die Teilnehmenden waren projektinterne Stakeholder. Die Präsentationsgrundlage wurde mit Microsoft Powerpoint erstellt. Die Folien und die schriftlich dokumentierten Ergebnisse wurden veröffentlicht (Brazel et al. 2023). Die Rolle des Moderators und des Analytikers wurde von der gleichen Person übernommen. Das Protokoll wurde von zwei FZI-Projektkollegen erstellt. Der Workshop wurde entsprechend dem Ablaufplans aus Tabelle 3 durchgeführt.

5.1.1 Workshop: Unternehmensidentitäten

Der fokusgruppenähnliche Workshop zu den Unternehmensidentitäten fand am 18. April 2023 statt. Das Fokusgruppenteam umfasste sieben projektinterne Stakeholder aus den Bereichen E-Government, Wallet-Betrieb und Forschung. Die Atmosphäre unter den Teilnehmenden war insgesamt angenehm und ergebnisorientiert.

Fragen, die in der Gruppe diskutiert wurden waren häufig auf die Rolle der Unternehmensidentität an sich bezogen, da diese sich wesentlich von der Identität einer natürlichen Person unterscheidet. Die Schwierigkeit der Abgrenzung von Personen- und Unternehmensidentität wurde festgestellt, da hinter jeder Handlung einer Unternehmensidentität auch eine Person stehen muss, die im Namen des Unternehmens agiert. Daraus ergibt sich die Frage, wie einzelne Personen berechtigt werden können, mit der Unternehmensidentität bestimmte Aktionen durchführen zu können und wie das technisch implementiert werden könnte.

Eine weitere Frage, die diskutiert wurde, war der Unterschied zwischen Unternehmen und sonstigen Organisationen. Unternehmen stellen eine spezielle Form von Organisation dar, die bestimmte Ziele und Bedürfnisse hat (z.B. Gewinnabsicht, Schutz von Geschäftsgeheimnissen etc.). Sonstige Organisationen können beispielsweise Forschungseinrichtun-

gen oder Stellen der öffentlichen Verwaltung sein. Die Anforderungen von Unternehmen könnten teilweise andere sein als die Anforderungen von sonstigen Organisationen, daher können Unternehmen und andere Organisationen auch als zwei verschiedene Stakeholdertypen betrachtet werden. Im Rahmen des Workshops wurden beide Gruppen gemeinsam betrachtet betrachtet.

Eine Anmerkung aus dem Teilnehmendenkreis wies darauf hin, dass anders als in der Projektpräsentation (z.B. in Abbildung 4) dargestellt, nicht nur die Rollen Akzeptanzstelle, Identitätssubjekt und Vertrauensdienst in SDIKA auftreten sondern zusätzlich noch der Betreiber der Wallet als Akteur aufgeführt sein müsste. Die Rolle des Wallet-Betreibers wurde daraufhin in das Stakeholderregister und ebenfalls als Stakeholdertyp (siehe Tabelle 2) mit aufgenommen.

Neue Anwendungsfälle, die sich aus diesen Fragestellungen ergeben, wurden zum Ende des Workshops erfasst. Die Ideen wurden separat zu den Anforderungen auf einem Flipchart erfasst. Im Fokus des Workshops stand allerdings die Erhebung von Anforderungen.

Verständnis digitaler Souveränität

Die Teilnehmenden hatten allgemein ein gutes Verständnis vom Begriff der Digitalen Souveränität. Selbstständigkeit, Sicherheit und Datensouveränität (siehe Abschnitt 2.1.2) wurden besonders häufig genannt. Alle Aussagen der Teilnehmenden sind in Anhang C dargestellt.

Abfrage der Anforderungen

Die Aussagen aus der Karten-Abfrage im Anforderungsworkshop Unternehmensidentitäten sind in Tabelle 6 dargestellt. Die Einordnung in Themenfelder erfolgte im Nachgang durch den Analytiker.

Use-Cases und weitere Fragestellungen

Im Anschluss an die Demonstration der klickbaren Prototypen (Abbildung 7) wurden unter den Teilnehmenden weitere Anwendungsfälle für die Unternehmensidentität diskutiert. Die Beiträge der Teilnehmenden, die erfasst werden sollten, aber nicht als Anforderungen zu kategorisieren sind, wurden separat zunächst auf einem Flipchart erfasst. Die Frage, bei welchen Aktivitäten die Identität eines Unternehmens oder einer Organisation selbst so im Vordergrund steht, dass die Identität der ausführenden Person in den Hintergrund tritt, führte zu einer Sammlung an Use-Cases. Beispielsweise kann es den Fall geben, dass einzelne Mitarbeitende berechtigt sind, im Namen des Unternehmens Vertragsabschlüs-

se oder Zahlungen durchzuführen. Dies ist unter anderem bei Hotelbuchungen der Fall, wenn Hotelzimmer im Namen eines Unternehmens gebucht werden. In diesem Fall ist es möglicherweise noch nicht klar, welche Person das Zimmer später belegen wird. Die Buchung erfolgt vorab nur auf den Namen des Unternehmens. Die gesammelten Use-Cases und weitere aufkommende Fragestellungen sind in Anhang C aufgeführt.

5.1.2 Workshop: Akzeptanzstellen

Der fokusgruppenähnliche Workshop zu Akzeptanzstellen fand am 20. April 2023 statt. Das Fokusgruppenteam umfasste ebenfalls sieben Teilnehmende aus den Bereichen E-Government, Mobilität, Wallet-Betrieb und Forschung. Vier Teilnehmende waren bereits im Workshop zu Unternehmensidentitäten anwesend. Die Stimmung war kollegial und es entstanden angeregte fachliche Diskussionen über die Anforderungen von Akzeptanzstellen. Insbesondere die Anforderungen von kleinen Betrieben (z.B. Eisdielen, 1-Personen Betriebe, siehe Tabelle 8) wurden diskutiert.

Verständnis digitaler Souveränität

Wie bereits im Workshop zu Unternehmensidentitäten wurde bei der Abfrage zum Verständnis digitaler Souveränität vor allem die Dimension Daten genannt. Auch das Recht auf informationelle Selbstbestimmung (Garstka 2003) und die Dimension Kompetenzen wurde angesprochen (siehe Abschnitt 2.1.2). Die Aussagen der Teilnehmenden sind in der Liste in Anhang C.1 aufgeführt.

Abfrage der Anforderungen

Die Abfrage der Anforderungen im Workshop zu Akzeptanzstellen erfolgte analog zum vorherigen Workshop. Die Aussagen aus der Karten-Abfrage im Anforderungsworkshop Akzeptanzstellen sind in Tabelle 8 dargestellt.

Use-Cases und weitere Fragestellungen

Wie bereits im Workshop zu Unternehmensidentitäten diskutierten die Teilnehmenden nicht nur über Anforderungen aus der Sicht der Stakeholder sondern auch über weitere Herausforderungen und Fragestellungen, die sich aus den Anwendungsfällen für Akzeptanzstellen ergeben. Die Use-Cases, Fragestellungen und Herausforderungen finden sich in Anhang D.

5.2 Auswertung der Workshops

Die Ergebnisse der fokusgruppenähnlichen Workshops wurden protokolliert und veröffentlicht (Brazel et al. 2023). Die Aussagen der Teilnehmenden aus dem Ergebnisprotokoll wurden in einer Liste festgehalten und durch den Analytiker den Themenfeldern aus dem Themenfeldregister zugeordnet, wobei einige Aussagen auch mehreren Themenfeldern zugeordnet werden konnten. Falls eine Aussage zu keinem der Themenfelder passte, wurde ein neues Themenfeld identifiziert und in das Themenfeldregister mit aufgenommen. Hierbei wurde das Themenfeld **Berechtigungen** identifiziert, das nicht Bestandteil des initialen Themenfeldregisters war. Das neue Themenfeld ist in Tabelle 4 beschrieben.

Tabelle 4: Neu identifiziertes Themenfeld: Berechtigungen

Themenfeld und Beschreibung	**untergeordnete Themenfelder**	**Anforderungsart**
Berechtigungen befasst sich mit der Frage, wer innerhalb eines Unternehmens oder einer Organisation zu bestimmten Handlungen (Vertragsabschlüsse, Käufe, Buchungen) berechtigt ist.	Kompetenzeinsatz	Funktionale Anforderungen, Qualitätsanforderungen

5.2.1 Mapping der Anforderungen

Die Ergebnisse wurden entsprechend MEADigS auf Anforderungen gemappt und auf redundante Inhalte untersucht. Bei doppelten Aussagen wurden mehrere Aussagen auf eine Anforderung gemappt. Wenn sich in einer Karte mehrere Anforderungen ableiten lassen, wurden diese in mehrere Anforderungen geteilt (Tabelle 6 und Tabelle 8).

Für eine bessere Übersichtlichkeit bekommt jede Anforderung eine ID zugewiesen. Diese setzt sich aus einem Buchstaben für die Quelle, aus der die Anforderung erhoben wurde (siehe Tabelle 5) und einer fortlaufenden Nummerierung zusammen.

Tabelle 5: Indexierung der Anforderungen

ID	**Quelle**
U.#	Anforderung stammt aus dem Workshop Unternehmenidentitäten
A.#	Anforderung stammt aus dem Workshop Akzeptanzstellen
B.#	Anforderung wurde sowohl im Workshop Unternehmensidentitäten als auch im Workshop Akzeptanzstellen genannt.

Tabelle 6: Mapping der Anforderungen aus dem Workshop „Unternehmensidentitäten“

Aussage	**Themenfeld(er)**	**Gemappt auf Anforderung**
Unternehmens-ID (ohne Personenbezug) fällt nicht unter EU-DS-GVO. - Datenschutz für identifizierbare oder identifizierte natürliche Personen VERSUS Schutz von Geschäftsgeheimnissen → sind unterschiedliche Aspekte - Evtl. sind wir dadurch bei Unternehmensidentitäten freier	Betriebs- und Geschäftsgeheimnisse, IT-Sicherheit	U.1
Flexibel (benötigte Nachweise lassen sich abbilden)	Flexibilität	U.4
Anpassungsfähig – nicht statisch. Auch Unternehmen verändern sich und die Identität und ihr betreffenden Regeln müssen angepasst werden	Flexibilität	U.4
Übertragbarkeit von Vollmachten (wie z.B. Prokura) (Admin/Verwalter)	Funktionalität (Berechtigungen)	U.6
Einfache Arbeitsvertretung (bei Ausfall eines Kollegen)	Funktionalität (Berechtigungen)	U.6
Rechteverwaltung für mögliche Vertragsabschlüsse	Funktionalität (Berechtigungen)	U.6
These: Unternehmensidentitäten sind immer mit handelnden natürlichen Personen und ihren Identitäten verknüpft. Beispiel: Außendarstellung von einem Unternehmen, ohne dass die handelnde Person sichtbar ist, Credential von Produkten (Zusicherung von Produkteigenschaften) Auch Analogie: Ich habe in einer Personenidentität das Vertretungsrecht für ein Unternehmen und gebe in einem Fall nur das Unternehmen raus (wie aus dem Personalausweis nur die Eigenschaft der Volljährigkeit)	Funktionalität (Berechtigungen)	U.6
Selbstverwaltung der Daten: Aufnahme, Speicherung, Löschung und Dauer der Datenverarbeitung	Funktionalität, Entscheidungsträger	U.2
Aktuelle und nicht veraltete Daten	Funktionalität, Identität	U.7
Sowohl selbst- als auch fremdverwaltete Identitätslösungen und Austausch von Credentials	Funktionalität, Interoperabilität, Infrastruktur	U.3

Aussage	**Themenfeld(er)**	**Gemappt auf Anforderung**
Internationale Verfügbarkeit (weil ich Geschäftspartner/Kunden weltweit habe)	Funktionalität, Leistung	U.5
Verifikationsprozess	Identität	U.8
Identität wird von öffentlicher Stelle bestätigt, keine Abhängigkeit zu privaten Akteuren (Ggf. Bestätigung durch öffentliche Stelle aus gesetzlicher Pflicht und nicht freiwillig)	Identität, Unabhängigkeit, Neutralität	U.8
Integration in bestehende Anwendungen (z.B. betriebliche Software/WorkflowManagement-Systeme)	Interoperabilität, Flexibilität	U.10
Modular und Transparent	Interoperabilität, Flexibilität, Transparenz	U.9
Interoperabilität und keine Lock-In-Effekte zu einzelnen Anbietern, selbst- als auch fremdverwaltete Identitätslösungen mit gegenseitigem Credential-Austausch	Interoperabilität, Unabhängigkeit	U.9
Sicherer Zugang/fälschungssicher	IT-Sicherheit	U.11
Manipulationssicher	IT-Sicherheit	U.12
Sicherstellung von Datensicherheit	IT-Sicherheit	U.12
Sichere Schnittstellen ohne Aufwand	IT-Sicherheit	U.12
Sicherer Datenaustausch	IT-Sicherheit, Datenschutz	U.12
Transaktionssicherheit	IT-Sicherheit, Datenschutz	U.12
Sicheres und schnelles Handeln mit Unternehmensdaten	IT-Sicherheit, Leistung	U.12
Verständlichkeit, z.B. Für Endnutzende (auch Mitarbeitende in Betrieben und Unternehmen) besser zu verstehen als SSL Webseiten-Schlosssymbol	Kompetenzeinsatz, Transparenz, Usability	U.13
Ich als Organisation/Unternehmen kann nachvollziehen, welche Berechtigten in einem konkreten Fall mit meiner Identität gehandelt haben – andere können dies nicht	Kontrolle, Transparenz, Privatsphäre	U.15
Rechtssicherheit: Nachvollziehbar & nicht abstreitbar & rechtlich durchsetzbar (in der wirklichen Welt & vor Gericht anerkannt . . .)	Kontrolle, Transparenz, Vertrauen	U.14

Aussage	**Themenfeld(er)**	**Gemappt auf Anforderung**
Das Verfahren ist nachvollziehbar (als Beteiligter kann ich es, wenn nötig, so offen legen, dass es bspw. vor Gericht anerkannt wird)	Kontrolle, Transparenz, Vertrauen	U.15
Auswahl der Endgeräte sollte für alle Unternehmen eine Machbarkeit bieten (Vom 1-Personen-Betrieb bis zum Großkonzern)	Leistung	U.16
Effizientere und reduzierte Papier-basierte Prozesse, dafür mehr digitale Nachweise, da für Menschen leichter auffindbar/durchschaubar	Leistung	U.17
Schnellere Arbeitsprozesse	Leistung	U.18
Weite Verbreitung	Leistung	U.19
Geringe Einstiegshürden (Kosten, andere Aufwände, technische Komplexität)	Leistung	U.20
Digitaler Nachweis wird anerkannt (vgl. S/MIME Zertifikat Class x und die mangelnde Anerkennung)	Leistung	U.19
Wirtschaftlich (nicht zu teuer bspw. bzgl. Transaktionskosten,...)	Leistung	U.20
Genügend Akzeptanzstellen	Leistung	U.19
Notwendigkeit und Aufwand: Aus der Sicht von kleineren Unternehmen muss der Vorteil größer sein als der Aufwand zu einer Identität zu kommen	Leistung	U.17, U.18, U.20
Kostengünstig	Leistung	U.20
Prozessvereinfachungen	Leistung	U.17
Nutzung mit viel Partnern im Kontext B2B/B2C/B2Gov	Leistung	U.19
Änderungen müssen schnell und einfach sein	Leistung	U.4
Verwaltung von sicheren Digitalen Identitäten sollte „Grundbedürfnis“ von Unternehmen sein (ohne eine digitale Identität zu sein, sollte für Unternehmen undenkbar sein)	Leistung	U.19
Nachvollziehbar / Replizierbarkeit	Transparenz	U.15
Einsehbarer Quellcode	Transparenz, Unabhängigkeit, Vertrauen	U.21

Aussage	**Themenfeld(er)**	**Gemappt auf Anforderung**
Keine Vendor-Lock-In-Effekte, z.B. leichter Wechsel zwischen Mobilitätsplattformen	Unabhängigkeit, Interoperabilität, Plattformen	U.9
Das System wird nicht von „einem“ kontrolliert (aktuell und in Zukunft)	Unabhängigkeit, Plattformen	U.22
Einfache Verwaltung und Steuerung (UX)	Usability	U.23
Strukturierte Datensammlung (das Wallet ist für den Holder übersichtlich)	Usability	U.23
Identitäten dürfen nicht „für Entscheidungsfindungen missbraucht“ werden	Vertrauen	U.24
Dritte vertrauen meiner digitalen Identität	Vertrauen	U.24
Identitätslösung ist so vertrauensvoll wie das Handelsregister. Dieses genießt z.B. „öffentlichen Glauben“[7], d.h. andere dürfen davon ausgehen, dass die Informationen darin richtig und aktuell sind	Vertrauen	U.24
Gewährleistung der Mindestverfügbarkeit, z.B. bei Netzausfall, Spannungsfeld Datenschutz und Speicherung für die Offline-Verfügbarkeit	Zuverlässigkeit	U.25
Verlässliches, nachhaltiges, digital souveränes Gesamtsystem	Zuverlässigkeit	U.22
Garantierte Mindestverfügbarkeit (Service-Level)	Zuverlässigkeit	U.25

Die Anforderungen werden zunächst nach Stakeholdertypen getrennt in zwei verschiedenen Anforderungsregistern gesammelt (Anhänge C und D). Anschließend werden die beiden Anforderungsregister zusammengeführt, indem redundante Anforderungen vereint werden. Die Anforderungen, die zu einer einzigen Anforderung zusammengefasst werden, erhalten eine neue ID (siehe Tabelle 7).

[7] „Öffentlicher Glaube“: Hopt und Merkt 2023, Rn. 1-3.

Tabelle 7: Zusammenführung redundanter Anforderungen

Anforderungen	**Zusammengeführt in neuer Anforderung**
U.2, A.2	B.1
U.8, A.4	B.2
U.12, A.5	B.3
U.13, A.6	B.4
U.14, A.7	B.5
U.19, A.8	B.6
U.20, A.9	B.7
U.18, A.12	B.8
U.22, A.15	B.9
U.23, A.17	B.10
U.24, A.18	B.11
U.25, A.21	B.12

Das Anforderungsregister mit allen Anforderungen aus beiden Workshops befindet sich im Anforderungsdokument in Anhang F. Die Begründungen und weitere Anmerkungen zu den Anforderungen ergeben sich aus den Aussagen der Workshop-Teilnehmenden.

Tabelle 8: Mapping der Anforderungen aus dem Workshop „Akzeptanzstellen“

Aussage	**Themenfeld(er)**	**Gemappt auf Anforderung**
Hohe Nutzerzahlen, kritische Masse erreichen, klarer Mehrwert (damit sich Akzeptanzstelle überhaupt am System beteiligt und die richtigen Nutzer angesprochen werden)	Leistung	A.8
Transparente Kosten und kostengünstig	Leistung, Transparenz	A.9, A.10
Unkomplizierte Anbindung der digitalen Lösung und Betrieb	Usability, Infrastruktur, Kompetenzeinsatz	A.16
Sicherstellung der Gültigkeit von Credentials (z.B. Führerschein und Personalausweis)	Funktionalität, Identität	A.3
Aufwand muss sich lohnen	Leistung	A.8, A.9, A.10, A.16
Sichere Datenübertragung, Vertrauensaufbau	IT-Sicherheit, Vertrauen	A.5
Verifizierte Daten sind sichtbar	Funktionalität	A.4
Keine Abhängigkeiten, damit Prozesse zukünftig auch ohne die eingeführte Lösung laufen (keine Lock-In-Effekte)	Unabhängigkeit, Interoperabilität, Plattformen	A.14
Unterstützt alle notwendigen Nachweismöglichkeiten (Wallets, Credential-Typen, ..)	Leistung	A.8
Vertrauenswürdig (Worst case wäre, wenn System immer alles kontrolliert, was ich mache)	Vertrauen, Neutralität	A.18
Hohe UX/Usability für Nutzende	Usability	A.17
Nutzer und ihre Daten werden durch das System oder Betreiber nicht ausgenutzt	Datenschutz, Vertrauen	A.1
Nachhaltig, souverän und zukunftssicher (z.B. wenn IT-System umgestellt wurde und es folgt ein Aufkauf, muss nicht wieder erneut mühselig umgestellt werden)	Zuverlässigkeit	A.20
Hohe Verfügbarkeit	Leistung	A.8
Menschenlesbare Nachrichten (nicht zu technisch, sondern nachvollziehbar)	Usability	A.17

Aussage	**Themenfeld(er)**	**Gemappt auf Anforderung**
Rechtssicherheit und Nachvollziehbarkeit, Transkationen müssen be-/nachweisbar und nicht mehr im Nachhinein änderbar sein, Wallet kann die Anfrage als Beweis speichern	Kontrolle	A.7
System muss den Datenschutzregelungen entsprechen (welche Daten wohin ausgetauscht werden, könnten kompakt für Nutzende zusammenfasst werden, zusätzlich zu den unübersichtlichen AGB)	Datenschutz	A.1
Die übertragenen Daten sind sicher und zuverlässig	IT-Sicherheit	A.5
Leicht und günstig nutzbar → Keine hohen Kosten für IT-System, z.B. bei der Eisdiele	Leistung	A.11
Einfache Integration in die Geschäftsprozesse (Beispiel: Eisdiele will sich nicht verändern, um digitale Identität nutzen zu können)	Leistung	A.11
Überprüfung der Echtheit erübrigt sich	Identität	A.4
Zuverlässiger Betrieb	Zuverlässigkeit	A.21
Zeit- und Ressourcen-sparend	Leistung	A.12
Vertretbare Transkations- und Betriebskosten	Leistung	A.9
Keine Einstiegshürden für die digitale Lösung (Personalschulen, Hardware)	Leistung	A.11
Standards und Vereinheitlichung (1. Unabhängigkeit von einer einzigen Lösung, 2. Gültige Credential-Standards)	Unabhängigkeit	A.15
Berücksichtigung von (komplexen) Anforderungen der Anwendung (Nutzer verständlich nahebringen, welche Nachweise er liefern muss und was bei der Akzeptanzstelle damit passiert)	Kompetenzeinsatz	A.6
Signifikate Anzahl an vertrauenswürdige Kunden	Leistung	A.8
Keine eigene IT bei kleineren Organisationen nötig (z.B. bei Disko, der Disko-Einlass), Positivbeispiel: Digitales Corona-Konzept bei Festen	Leistung	A.11
Vermittelt Informationen, wie z.B. Vertrauensniveau	Kompetenzeinsatz	A.6

Aussage	**Themenfeld(er)**	**Gemappt auf Anforderung**
Daten vorzugsweise beim Nutzer (Wallet) speichern, dadurch weniger Datenschutzprobleme (z.B. nur Prüfung auf Volljährigkeit, ohne Datum zu speichern → es gibt aber Fälle, bei denen gewisse Daten gespeichert werden müssen)	Entscheidungs-träger	A.2
Nur weil es technisch möglich ist, digital sicherer zu sein als analog, muss das nicht umgesetzt werden	IT-Sicherheit	A.5
Akzeptanzstelle will sicher sein, dass der Prozess valide ist	Vertrauen	A.19
Welche Daten an wen gehen, könnte kompakt zusammenfasst und dem Nutzer präsentiert werden (anstatt 30 Seiten AGBs lesen)	Kompetenzeinsatz	A.6
Transparenter Umgang mit integrierten Zahlungsdiensten (wie bspw. Log Pay, Nutzer sieht im Bankkonto die Abbuchung von Log Pay und kann diese nicht zu Regiomove zuordnen)	Transparenz	A.13

5.2.2 Zuordnung der Artefakt-Inhalte zu Themenfeldern

Die Anforderungen wurden den Themenfeldern aus dem Themenfeldregister (Anhang A) zugeordnet und in das erweiterte Themenfeldregister (Tabelle 11) überführt (Weinreuter 2022, S. 112). Die Anforderungen mit Beschreibung, Begründung, Anforderungsart und weiteren Anmerkungen befinden sich im Anforderungsregister (Tabelle 14 in Anhang F.4).

Tabelle 9: Zuordnung der Anforderungen aus den Workshops zu Themenfeldern

ID	Anforderung	Themenfeld
U.1	Schutz von Unternehmensdaten	Betriebs- und Geschäftsgeheimnisse
U.4	Anpassungsfähigkeit	Flexibilität
U.5	Internationale Verfügbarkeit	Funktionalität
U.6	Rechteverwaltung	Funktionalität
U.7	Aktualität der Daten	Funktionalität
U.9	Interoperabilität	Interoperabilität
U.10	Integration	Interoperabilität
U.11	Sicherer Zugang	IT-Sicherheit
U.15	Nachvollziehbarkeit	Kontrolle
U.16	Technische Machbarkeit	Leistung
U.17	Digitale Prozesse	Leistung
U.21	Open-Source	Transparenz
A.1	Datenschutz	Datenschutz
A.3	Gültigkeit	Funktionalität
A.10	Transparente Kosten	Leistung
A.11	Geringe Einstiegshürden	Leistung
A.13	Transparenz mit Dienstleistern	Transparenz
A.14	Unabhängigkeit	Unabhängigkeit
A.16	Unkomplizierte Anbindung	Usability
A.19	Validität der Prozesse	Vertrauen
A.20	Zukunftssicher	Zuverlässigkeit
B.1	Selbstverwaltung	Entscheidungsträger
B.2	Verifikationsprozess	Identität
B.3	Sichere Datenübertragung	IT-Sicherheit
B.4	Verständlichkeit	Kompetenzeinsatz
B.5	Rechtssicherheit	Kontrolle
B.6	Weite Verbreitung	Leistung
B.7	Geringe Kosten	Leistung
B.8	Schnellere Prozesse	Leistung
B.9	Standardisierung	Unabhängigkeit
B.10	Einfache UX	Usability
B.11	Vertrauenswürdigkeit	Vertrauen
B.12	Verfügbarkeit	Zuverlässigkeit

6 Evaluation

Im Folgenden werden die Ergebnisse MEADigS der Evaluation zusammengefasst und diskutiert. Die Evaluation erfolgt anhand der Bewertungskriterien, die in Kapitel 3 aufgestellt wurden. Zunächst wird die Durchführbarkeit der Methode bewertet. Darauf folgt eine Beurteilung der Ergebnisqualität. Anschließend wird die Methode und ihre Durchführung kritisch betrachtet und diskutiert.

6.1 Durchführbarkeit der Methode

Um die Durchführbarkeit der Methode zu bewerten werden die Aktivitäten innerhalb der einzelnen Schritte der Methode in Hinblick auf die Evaluationskriterien aus Abschnitt 3.2 beleuchtet.

6.1.1 Schritt 1: Verständnisaufbau und Registrierung der Themenfelder

Effektivität
Der Aufbau eines Verständnisses für digitale Souveränität ist unerlässlich und bildet die Grundlage für alle darauf folgenden Aktivitäten. Das Aufstellen eines Themenfeldregisters hat sich als effektiv erwiesen. Die Vorlage (Weinreuter 2022, Tabelle 10 in Anhang F) hilft dabei, einen Überblick für die relevanten Themenfelder digitaler Souveränität zu erlangen. Eine Literaturrecherche zu dem übergeordneten Thema ist prinzipiell sehr sinnvoll.

In Weinreuter 2022, S. 98 werden bereits erhobene Anforderungen als notwendige Eingabe im ersten Schritt genannt. Dies setzt voraus, dass bereits Anforderungen vorliegen. Da davon nicht ausgegangen werden kann, sollten bereits erhobene Anforderungen eher als optionale Eingabe des ersten Schrittes aufgeführt sein. Sofern keine Anforderungen vorliegen, kann das Anforderungsregister erst später angelegt werden. In diesem Fall muss eine Adaption erfolgen (wie beispielsweise in Kapitel 4 beschrieben), damit die Methode mit Einschränkungen durchgeführt werden kann.

Effizienz
Die Aktivitäten im ersten Schritt werden ausschließlich durch den Analytiker ausgeübt. Der Bedarf an personellen Ressourcen ist in diesem Schritt demnach im Rahmen.

Der Zeitaufwand für die Recherche und die Registrierung der Themenfelder hat sich insbesondere aufgrund der Nützlichkeit des Themenfeldregisters als angemessen erwiesen.

Da ein umfassendes Wissen des Analytikers über digitale Souveränität unabdingbar ist, kann der Aufwand gerechtfertigt sein.

Akzeptanz
Eine Komplexität im ersten Schritt entsteht durch die Aktivität „Themenfelder einschränken“. Ob ein oder mehrere Themenfelder in der Vorlage (Weinreuter 2022, Tabelle 10 in Anhang F) für das entsprechende Projekt relevant sind oder nicht, kann sich möglicherweise erst später herausstellen. Die Vorgabe, zu Beginn bereits Einschränkungen der Themenfelder vorzunehmen, wurde durch den Analytiker kritisch betrachtet. Es ist zu empfehlen, diese Aktivität zu einem späteren Zeitpunkt, wie in Schritt 3 oder sogar Schritt 4, durchzuführen.

Da Schritt 1 durch den Analytiker als ausführenden Akteur bereits während der Durchführung für nützlich empfunden wurde, kann die Akzeptanz dennoch als sehr hoch eingeschätzt werden.

6.1.2 Schritt 2: Analyse der Stakeholder

Effektivität
Eine Analyse der Stakeholder dient dem Verständnisaufbau und ist grundsätzlich zu empfehlen. Allerdings liegen nicht bei jedem Projekt bereits Informationen über Stakeholder in großer Menge vor oder sind ungleichmäßig verteilt. Es ist möglich, dass beispielsweise viele Informationen zu Unternehmen aus einer bestimmten Branche vorliegen, dafür aber nur wenig über die Bedürfnisse und Wünsche von Bürgern bekannt ist. Das Anfertigen eines Stakeholderregisters dient dem grundlegenden Verständnis für das Software-Projekt und dient der erfolgreichen Durchführung der weiteren Schritte.

MEADigS sieht vor, dass in diesem Schritt bereits Anforderungen erfasst werden, die sich den Bedürfnissen der Stakeholder ergeben. Dieses Ziel konnte im Rahmen der Durchführung nicht erreicht werden. Vorab Telefonate mit einzelnen Stakeholdern zu führen war ebenfalls nicht möglich.

Es konnten lediglich Hinweise auf mögliche Anforderungen gefunden werden. Diese Informationen dienten als Hintergrundwissen für den Analytiker. Die Analyse der Stakeholder diente in diesem Fall jedoch ausschließlich zu einem besseren Überblick über die am Projekt beteiligten Stakeholder und nicht der Erhebung von Grundanforderungen.

Effizienz

Für Analyse der Stakeholder gibt MEADigS kein systematisches Verfahren vor. Auch gibt es keine Vorgaben, wie diese Analyse durchgeführt werden könnte. Wie bereits in der kurzen Evaluation in Weinreuter 2022, S. 74 durch Experten angesprochen, gibt es keine Werkzeuge, die eine strukturierte Analyse von Stakeholdern ermöglichen. Viele Stakeholder im Projekt SDIKA waren bereits bekannt. Eine Stakeholderliste liegt aber nicht zwangsläufig bei jedem Projekt bereits vor. Dieser Schritt kann, je nachdem wie viel Zeit investiert wird und wie viele Stakeholder beteiligt sind, sehr aufwändig sein.

Man könnte beispielsweise die Analyse der Stakeholder entsprechend des „Stakeholder Analysis Process Model“ (Celar et al. 2010) durchführen. Dabei werden die Stakeholder entsprechend der Eigenschaften „Macht“, „Einfluss“, „Wissen“ und „Bereitschaft zur Zusammenarbeit“ bewertet und in einem Diagramm grafisch dargestellt, um die Analyse zu erleichtern.

Das Stakeholderregister, das im Rahmen dieser Arbeit angefertigt wurde, beinhaltet lediglich die wichtigsten Informationen zu den Stakeholdern für deren Kategorisierung.

Akzeptanz

Für die Bildung der Fokusgruppen für Schritt 4 ist eine Einteilung der Stakeholder in Stakeholdertypen notwendig. Um die weiteren Schritte zu planen, muss der Analytiker einen Überblick über die Stakeholder haben.

Es ist fraglich, ob es sinnvoll ist, bereits in diesem Schritt Anforderungen zu erheben, bevor eine Interaktion mit den Stakeholdern selbst stattgefunden hat.

Die Akzeptanz dieser Aktivität war trotzdem hoch.

6.1.3 Schritt 3: Analyse von Dokumenten

Effektivität

Das Sammeln von sämtlichen Informationen über Stakeholder und das Projekt ist sinnvoll, könnte aber auch Bestandteil der ersten beiden Schritte von MEADigS sein. Allerdings ist es denkbar, dass zu einem Software-Projekt noch keine große Menge an Dokumenten vorhanden ist oder diese nicht ohne Weiteres zugänglich sind.

Ein Glossar dient der Klärung von Begriffen und kann im späteren Verlauf helfen, Inkonsistenzen zu finden und zu beseitigen. Auch bei der Arbeit mit Stakeholdervertretern könnte ein Glossar eingesetzt werden. Dementsprechend ist die Erstellung eines Glossars nützlich.

Wie im Rahmen der Experten-Interviews zu MEADigS in Weinreuter 2022, S.76 bereits angemerkt, sind die Aktivitäten „Mehrdeutige Aussagen festhalten“ sowie „Fragen zu mehrdeutigen Aussagen aufstellen“ in der Praxis sehr komplex. Mehrdeutige Aussagen konnten in diesem Schritt nicht identifiziert werden.

Auch in Schritt 3 konnten aus den Dokumenten keine Anforderungen abgeleitet werden. Für das reine Sammeln von Informationen war dieser Schritt effektiv.

Effizienz

Der Aufwand, der im dritten Schritt entsteht, ist abhängig von der Zahl der verfügbaren Dokumente über die Stakeholder. Je nachdem, wie viele Dokumente vorliegen, kann dieser Schritt sowohl sehr aufwändig oder aber relativ simpel sein. In jedem Fall sollte darauf geachtet werden, dass dieser Schritt nicht unverhältnismäßig viel Zeit in Anspruch nimmt. Wenn viele Dokumente vorliegen, ist es empfehlenswert, eine zeitliche Grenze zu setzen, damit nur wirklich relevante Dokumente analysiert werden.

Auch das Aufstellen eines Glossars kann, je nachdem wie umfangreich es sein soll, einen hohen Aufwand erzeugen. Es liegt im Ermessen der Akteure, wie viel Aufwand in diese Aktivität fließen sollte. Im Rahmen dieser Arbeit wurde ein kurzes Glossar mit den wichtigsten (Fach-)begriffen und Definitionen angefertigt. Dieses diente dem Analytiker und Moderator zur Orientierung, wurde aber in der späteren Durchführung nicht mehr weiter benötigt.

Akzeptanz

Es ist fraglich, ob es sinnvoll ist, bereits in diesem Schritt Anforderungen zu erheben, bevor eine Interaktion mit den Stakeholdern selbst stattgefunden hat.

Anforderungen aus den Dokumenten abzuleiten war in diesem Fall nicht möglich.

Das Aufstellen von Fragen zu mehrdeutigen Aussagen der Stakeholder wurde als zu komplex wahrgenommen.

Die Analyse von Dokumenten zur Informationsbeschaffung stellt eine Aktivität dar, deren Durchführung durch den Analytiker als notwendig empfunden wird.

6.1.4 Schritt 4: Durchführung fokusgruppenähnlicher Workshops

Effektivität

Das Format des Anforderungsworkshops ist im Requirements Engineering eine bewährte Methode (Kanwal 2019). Dementsprechend ist ein Workshop auch gut geeignet, Anforderungen im Bereich der digitalen Souveränität zu erheben. MEADigS gibt vor, dass das primäre Ziel des fokusgruppenähnlichen Workshops ist, Grundanforderungen zu validieren und nennt die Erhebung neuer Qualitäts- und Grundanforderungen als sekundäres Ziel (Weinreuter 2022, S. 104). Da bei den im Rahmen dieser Arbeit durchgeführten Workshops im Vorfeld keine Grundanforderungen vorlagen, konnte das primäre Ziel nicht verfolgt werden. Es ist nicht davon auszugehen, dass zu Beginn eines Software-Projekts bereits Grundanforderungen formuliert wurden, die mithilfe von Ja/Nein-Fragen validiert werden könnten. In den durchgeführten Workshops wurde deshalb der Fokus auf die Erhebung von Qualitäts- und Grundanforderungen der Stakeholder gelegt.

MEADigS empfiehlt, die fokusgruppenähnlichen Workshops virtuell durchzuführen. Falls die Möglichkeit besteht, ist ein Workshop-Format in Präsenz aber grundsätzlich zu bevorzugen. Daraus folgte auch eine Abwandlung der Methode, wie sie in Abschnitt 4.6 beschrieben ist. Aus Gründen des Datenschutzes wurde keine Videoaufnahme der Workshop-Sessions erstellt. Als Datengrundlage dient das textuelle Ergebnisprotokoll (Brazel et al. 2023).

Darüber hinaus sieht MEADigS vor, bereits in der Einladung Impulse zum Thema digitale Souveränität zu setzen. MEADigS präzisiert nicht genau, wie so ein Impuls aussehen könnte. Es ist allerdings naheliegend, dass das Thema digitale Souveränität bereits frühzeitig gegenüber den Teilnehmenden mitgeteilt werden sollte.

Für die Erhebung von Anforderungen allgemein waren die Workshops hingegen effektiv. Die Themenfelder aus dem Themenfeldregister konnten genutzt werden, um während des individuellen Brainstormings Impulse zu setzen.

Nicht-kommunizierte Aussagen von Teilnehmenden der Workshops waren schwer zu identifizieren. Aufgrund der Tatsache, dass es sich bei den Teilnehmenden um Experten für das Projekt SDIKA handelte, kann davon ausgegangen werden, dass sie sich vorab bereits ausführlich Gedanken gemacht haben und ihre Anforderungen gut in Worte fassen konnten. Nichtsdestotrotz ist es empfehlenswert, auf nicht-kommunizierte Aussagen zu achten, insbesondere wenn Bürger befragt werden, die keine Experten sind.

Die Aussagen über Anforderungen, die durch die Teilnehmenden genannt wurden, waren jedoch in einer guten Qualität und wurden ausführlich begründet.

Effizienz

Grundsätzlich ist das Planen, Vorbereiten und Durchführen von Workshops eine zeitintensive Aktivität. Alleine für die Validierung von Grundanforderungen einen Termin mit einer Gruppe von Personen zu organisieren, ist nicht effizient. Außerdem sieht MEADigS vor, dass für jeden Stakeholdertypen eine eigene Fokusgruppe gebildet und ein Workshop veranstaltet wird. Der Zeitaufwand für die Organisation, Terminfindung und nicht zuletzt die Durchführung ist in der Regel sehr hoch. Die Durchführung solcher Veranstaltungen kann dennoch lohnenswert sein, wenn sie dazu genutzt wird, um möglichst viele Anforderungen der Stakeholder zu erheben. Wenn eine größere Menge an Anforderungen erfasst werden können und durch gute Moderation ein straffer Ablauf gewährleistet wird, kann ein Workshop effizient sein.

Laut MEADigS sollen die in Workshops genannten Anforderungen zunächst gesammelt und als „vorgeschlagen“ gekennzeichnet werden. Eine Validierung soll dann im nächsten Schritt stattfinden. Fraglich ist, ob diese Vorgehensweise effizient ist. Die Anforderungen wurden bereits innerhalb der Fokusgruppe gegenseitig erklärt und diskutiert. Damit wurden sie bereits durch die anderen Teilnehmenden validiert, sofern es sich bei der Gruppe um Experten handelt. Eine erneute Validierung in Form von Interviews wäre sehr aufwendig. Es ist unwahrscheinlich, dass ein Stakeholdervertreter im Interview eine vorgeschlagene Anforderung ablehnt, die vorher von einer ganzen Fokusgruppe für valide befunden wurde.

Dabei ist jedoch anzumerken, dass sich die Durchführung eines Workshops mit projektinternen Experten nur schwer mit einem Workshop mit anderen Stakeholdertypen wie Bürgerinnen und Bürgern vergleichen lässt. Diese müssten eine viel intensivere Einführung in das Thema und die Hintergründe und Ziele der Veranstaltung bekommen, um ein Verständnis für digitale Souveränität und das entsprechende Projekt zu erhalten.

Aus diesen Gründen kann eine umfassende Antwort zur Effizienz von fokusgruppenähnlichen Workshops im Allgemeinen daraus nicht abgeleitet werden. Workshops mit projektinternen Experten als Fokusgruppe waren allerdings sehr effizient. Innerhalb von zwei jeweils vierstündigen Veranstaltungen wurden 33 elementare Anforderungen entwickelt.

Akzeptanz

MEADigS gibt vor, dass die Zahl der Mitglieder eines Fokusgruppenteams zwischen vier und neun liegen sollte (Weinreuter 2022, S. 56-57). Beide Workshops wurden mit jeweils sieben Teilnehmenden durchgeführt. Damit lag die Größe der Gruppe im empfohlenen Bereich. Die Größe der Gruppe wurde sowohl vom Moderator als auch von den Teilnehmenden als praktikabel empfunden. Alle Teilnehmenden hatten dadurch Zeit, ihre Gedanken auszuführen. Der vorab festgelegte Zeitrahmen von ca. 4 Stunden für die Veranstaltungen

konnte eingehalten werden.

Eine Voraussetzung für diesen Schritt ist die Zuverlässigkeit der Stakeholder und die Bereitschaft zur Teilnahme.

Die Einordnung der Anforderungen in Themenfelder während des Workshops durchzuführen stieß bei den Teilnehmenden auf wenig Akzeptanz, da der Mehrwert als gering eingeschätzt wurde. Diesem Problem könnte unter Umständen durch eine weitere Anpassung des Moderationsplans entgegengewirkt werden, bei dem die Anforderungen bereits bei der Nennung in Themenfelder gruppiert werden. Im Rahmen dieser Arbeit konnte die Kategorisierung jedoch auch im Nachgang durch den Analytiker erfolgen.

Grundsätzlich war die Bereitschaft der Stakeholder, gemeinsam die Anforderungen zu diskutieren sehr hoch. Der Moderator konnte mit dem adaptierten Ablaufplan (Tabelle 3) ebenfalls gut arbeiten.

6.1.5 Schritt 5: Durchführung von Interviews mit Stakeholdervertretern

Effektivität
Das Mapping der Anforderungen konnte erfolgreich durchgeführt werden. Es hat dazu geführt, dass die Anforderungen in einer strukturierten Form und ohne Redundanzen vorliegen. Dieser Schritt ist entscheidend für die Qualität der Anforderungen, da aus Aussagen von Stakeholdern ausformulierte und begründete Anforderungen werden müssen. Hierbei ist anzumerken, dass die Ergebnisse dieser Schritte stark abhängig von der Arbeit des Analytikers sind. Dies kann eine potentielle Fehlerquelle sein.

Die entwickelten Anforderungen sollen gemäß MEADigS im Anforderungsregister gespeichert werden. Dieses enthält einen Eintrag für „Technische Möglichkeiten der Implementierung“. Im Rahmen der Durchführung konnten keine Informationen zu technischen Möglichkeiten der Implementierung gesammelt werden. Es ist insgesamt fraglich, ob die Sammlung von Möglichkeiten zur Implementierung ein Teil der Methode sein sollte. Stakeholdervertreter sind oft nicht an der technischen Entwicklung beteiligt und können in der Regel hierzu keine Aussagen treffen. Es ist zu empfehlen, dass die Erhebung von Anforderungen unabhängig von der Implementierung stattfindet. Eine Einschätzung zur technischen Machbarkeit sollte erst im Nachgang erfolgen.

Die Aufstellung eines erweiterten Themenfeldregisters führt dazu, dass Anforderungen zu Themenfeldern zugeordnet werden. Dies verbessert die Übersichtlichkeit und vereinfacht später eine Beurteilung der Qualität der Ergebnisse. Diese Form des Clustering ist grundsätzlich empfehlenswert. Allerdings ist die Zuordnung der Anforderungen zu Themenfeldern nicht immer eindeutig möglich. Anforderungen passen häufig in mehrere The-

menfelder. MEADigS macht keine Angaben, inwieweit es zulässig ist, eine Anforderung auch mehreren Themenfeldern gleichzeitig zuzuordnen und wie im weiteren Verlauf damit umgegangen werden sollte.

Insgesamt können die Aktivitäten „Artefakt-Inhalte mappen“ und „Artefakt-Inhalte Themenfeldern zuordnen“ als sehr effektiv betrachtet werden.

Zu der Effektivität von Interviews kann allerdings keine Aussage getroffen werden, da diese nicht durchgeführt werden konnten.

Effizienz

Mappen und kategorisieren hat sich als eine effiziente Methode erwiesen, mit der aus einer Menge an Aussagen Anforderungen erzeugt werden können.

Das Planen, Durchführen und Auswerten von Interviews mit Stakeholdervertretern ist eine sehr zeitaufwändige Aktivität. Ob dieser Zeitaufwand gerechtfertigt ist, nachdem bereits Workshops durchgeführt wurden, ist zu bezweifeln. Da dieser Schritt nicht vollständig durchgeführt wurde, kann allerdings keine eindeutige Aussage über die Effizienz von Schritt 5 getroffen werden.

Akzeptanz

Zu der Akzeptanz von Schritt 5 kann im Rahmen dieser Arbeit nicht beurteilt werden, da nicht alle Aktivitäten durchgeführt werden konnten.

6.1.6 Schritt 6: Quantitative Erfassung und Validierung der Anforderungen

Effektivität

Zu der Effektivität von Schritt 6 kann keine eindeutige Aussage getroffen werden, da eine Durchführung aus Zeitgründen nicht möglich war.

Ob eine zusätzliche Validierung in Form einer quantitativen Erfassung den gewünschten Mehrwert bringt, lässt sich im Rahmen dieser Arbeit nicht eindeutig feststellen. Dies ist auch abhängig von der Qualität der bis zu diesem Zeitpunkt erfassten Anforderungen.

Effizienz

Die Konzeption eines Fragebogens sowie das aufstellen einer repräsentativen Stichprobe von Stakeholdern ist eine zeitintensive Aufgabe. Es ist zu bezweifeln, ob in Projekten so viel Zeit und Ressourcen zur Verfügung steht. Aus diesem Grund ist zu empfehlen, Schritt 6 als optional zu betrachten.

Akzeptanz

MEADigS gibt vor, dass der Fragebogen von mindestens 30 Stakeholdern ausgefüllt werden sollte (Weinreuter 2022, S. 110). Ob es in Projekten möglich ist, so viele Stakeholder zu motivieren, teilzunehmen ist fraglich. Da der sechste Schritt nicht durchgeführt wurde, kann zu der Akzeptanz der Stakeholder im Rahmen dieser Arbeit keine Aussage getroffen werden.

6.2 Qualität der Ergebnisse

Es folgt ein Abgleich der REOs aus Abschnitt 3.3 mit den Ergebnissen aus dem finalen Anforderungsdokument (Anhang F) unter Berücksichtigung der einzelnen Schritte von MEADigS.

6.2.1 Vollständigkeit

a) Zunächst wird geprüft, ob Anforderungen in allen **Dimensionen digitaler Souveränität** erhoben werden konnten. Für die Abdeckung der Dimensionen digitaler Souveränität wurde das Themenfeldregister angelegt.

   Im erweiterten Themenfeldregister (Tabelle 11 in Anhang E) findet sich eine Aufstellung der Themenfelder und der zugeordneten Anforderungen. Hierbei fällt auf, dass die Themenfelder Infrastruktur, Neutralität, Plattformen und Privatsphäre nicht durch Anforderungen abgedeckt wurden. Damit wurden 17 von 21 Themenfeldern abgedeckt, was einem Abdeckungsgrad von ca. 81 % entspricht.

   MEADigS gibt keine Vorgehensweise für den Fall vor, dass Themenfelder nicht abgedeckt werden. Eine weitere Schwierigkeit entsteht dadurch, dass MEADigS nicht vorgibt, ob eine Anforderung nur einem oder auch mehereren Themenfeldern zugeordnet werden kann. Die Zuordnung zu Themenfeldern war nicht immer eindeutig möglich. Eine Anforderung wie **U.21 Open-Source** könnte beispielsweise sowohl zum Themenfeld „Transparenz“ als auch zu „Infrastruktur“ zugeordnet werden. Gerade technische Fragen zur Implementierung lassen sich, insbesondere wenn das Projekt sich noch in einem frühen Stadium befindet, durch Stakeholder nur schwer beurteilen.

   Durch die Einschränkung der Stakeholdergruppen (siehe Abschnitt 4.2) wurden außerdem nur die Anforderungen der Unternehmensidentitäten sowie der Akzeptanzstellen erhoben. Es ist nicht ausgeschlossen, dass eine vollständige Durchführung unter Einbeziehung von Vertrauensdiensten und Bürgern zu einer vollständigen Abdeckung der Themenfelder digitaler Souveränität führen könnte. Auch muss angemerkt werden, dass MEADigS in der gegebenen Zeit nicht vollständig durchgeführt werden konnte.

b) Die Vollständigkeit in Bezug auf die **Arten der Anforderungen** lässt sich in den Ergebnissen nicht feststellen. Ein Ziel von MEADigS ist es, sowohl kommunizierte als auch nicht-kommunizierte Anforderungen der Stakeholder zu erheben (Weinreuter 2022, S. 30). Die erhobenen Anforderungen wurden alle durch Stakeholder kommuniziert. Es konnten keine nicht-kommunizierten Anforderungen identifiziert werden.

Auch ist es möglich, dass bei einer Ausweitung der Stakeholdergruppen nicht-kommunizierte Anforderungen erhoben werden könnten. Die Teilnehmenden der Workshops (Abschnitt 5.1) waren Experten für das Projekt und somit in der Lage, ihre Wünsche und Bedürfnisse klar zu äußern. Es ist denkbar, dass es bei einer Beteiligung von Bürgern häufiger zu mehrdeutigen Aussagen oder nicht-kommunizierten Anforderungen kommen kann. Hierbei muss angemerkt werden, dass die Erfassung von nicht-kommunizierten Anforderungen, wie bereits im Rahmen der Experten-Interviews (Weinreuter 2022, S. 76) angemerkt wurde, in der Praxis ein sehr komplexes Vorhaben ist. MEADigS beschreibt zwar, dass auch Anforderungen identifiziert werden sollen, die nicht ausgesprochen werden, gibt aber keine Anleitung für eine konkrete Durchführung.

6.2.2 Korrektheit

Die Korrektheit der Anforderungen lässt sich nicht eindeutig bestimmen. MEADigS sieht vor, dass jede Anforderung durch Stakeholder validiert wird, bevor sie in das Anforderungsregister gelangt. Somit wird sichergestellt, dass keine der Anforderungen nur durch eine einzelne Person (z.B. den Analytiker) festgehalten wird. Es finden immer wieder Überprüfungen statt.

Im Zuge dieser Arbeit wurden alle Anforderungen während der fokusgruppenähnlichen Workshops (MEADigS Schritt 4) erhoben. Diese wurden unter den Teilnehmenden gegenseitig vorgestellt und diskutiert. Das Risiko, dass eine oder mehrere Anforderungen nicht korrekt sind, kann deswegen als sehr gering eingeschätzt werden.

Dennoch kann nicht vollständig ausgeschlossen werden, dass bei dem Mapping der Anforderungen durch den Analytiker (Abschnitt 5.2.1) aufgrund von Verständnisproblemen Fehler unterlaufen sind. Falls Fehler unterlaufen sein sollten, hätte es im Rahmen der Interviews (MEADigS Schritt 5) die Möglichkeit gegeben, diese aufzudecken.

6.2.3 Sachdienlichkeit

Um zu prüfen, ob die entwickelten Anforderungen sachdienlich bzw. relevant sind, wird zunächst das Themenfeldregister betrachtet. Wenn es möglich ist, eine Anforderung zu einem der Themenfelder digitaler Souveränität zuzuordnen, dann ist davon auszugehen, dass die Anforderung auch **relevant in Bezug auf digitale Souveränität** ist. Alle erhobenen Anforderungen konnten Themenfeldern zugeordnet werden (siehe Tabelle 9). Eine Sachdienlichkeit in Bezug auf digitale Souveränität liegt demnach vor.

Fraglich ist, ob auch die Sachdienlichkeit in Bezug auf das Projekt SDIKA vorliegt. Diese

Frage lässt sich nicht eindeutig beantworten. Es ist denkbar, dass durch die Demonstration von Prototypen im Rahmen der Workshops, der Fokus von Teilnehmenden auf weniger relevante Details verschoben wird und daraus Anforderungen abgeleitet werden, die nicht relevante Inhalte enthalten. Da die Teilnehmenden der Workshops, die im Kontext dieser Arbeit durchgeführt wurden, projektinterne Experten waren, kann dieses Risiko als gering eingestuft werden.

Insbesondere falls MEADigS mit Bürgern durchgeführt wird, sollten die Anforderungen auf Sachdienlichkeit überprüft werden.

6.2.4 Konsistenz

Für das Kriterium der Konsistenz nimmt MEADigS eine Abgrenzung vor.

a) Die Existenz von Widersprüchen zwischen und innerhalb der elementaren Anforderungen soll im Anforderungsdokument festgehalten werden, da eine Behebung von Widersprüchen nicht immer möglich sei. Ein Widerspruch in den Anforderungen lässt sich zwischen den Anforderungen **Selbstverwaltung** und **Fremdverwaltung** erkennen. Dieser Widerspruch könnte dadurch aufgelöst werden, wenn eine Wahlmöglichkeit zwischen Selbst- und Fremdverwaltung angeboten würde (**B.1 Selbstbestimmung**.

b) Widerspruchsfreiheit in Bezug auf die verwendeten Begriffe soll gewährleistet werden. Auf diese wird in Abschnitt 6.2.6 genauer eingegangen.

6.2.5 Nachvollziehbarkeit

Die Nachvollziehbarkeit oder Rückverfolgbarkeit wird durch MEADigS sichergestellt, indem der Prozess von der Quelle bis hin zur elementaren Anforderung klar dokumentiert wird. Die Quelle jeder Anforderung lässt sich aus dem Anforderungsdokument ablesen und zu jeder Äußerung der Teilnehmenden lässt sich die Anforderung, die daraus abgeleitet wurde, erkennen. Mithilfe von Tabelle 6, Tabelle 8 und Tabelle 7 lässt sich der vollständige Prozess von der Quelle bis zur Anforderung nachvollziehen.

Die Nummerierung der Anforderungen mit IDs wie in Abschnitt 5.2.1 beschrieben, wird in dieser Form in MEADigS nicht beschrieben, hat sich aber aus Gründen der Übersichtlichkeit als nützlich erwiesen.

Das Kriterium der Nachvollziehbarkeit kann daher als voll erfüllt betrachtet werden.

6.2.6 Eindeutigkeit

Eine Übersicht über Begriffsbestimmungen und Wortverwendungen gibt das Glossar, dessen Erstellung MEADigS vorgibt. Unter Zuhilfenahme des Glossars ist es die Aufgabe des Analytikers, die Anforderungen so zu formulieren, dass keine Inkonsistenzen in der Verwendung der Begriffe auftreten. Diese Aufgabe kann sich als komplex darstellen.

Eine Überprüfung der Eindeutigkeit der verwendeten Begriffe findet in MEADigS nicht statt. Die Qualität der Anforderungen in Bezug auf dieses Kriterium ist demnach stark abhängig von den Fähigkeiten des Analytikers.

6.3 Weitere Anmerkungen

Da MEADigS nicht vollständig durchgeführt werden konnte, kann diese Evaluation nicht als vollumfänglich betrachtet werden. Die wesentlichen Aspekte der Methode und deren Ergebnisse wurden allerdings ausführlich beleuchtet und bewertet. Ein abschließendes Urteil wäre möglich, wenn alle Schritte der Methode vollständig durchgeführt wurden.

Aufgrund des Umfangs dieser Arbeit wurde, wie in Abschnitt 4.2 beschrieben, eine Einschränkung auf zwei Stakeholdertypen vorgenommen: Unternehmen als Identitätssubjekte und Akzeptanzstellen

Aufgrund der Charakteristik dieser Arbeit konnten die verschiedenen Rollen (Analytiker, Moderator) nicht von mehreren Personen übernommen werden. Die Rollen wurden nicht von einem Projektmanager sondern von einer projektexternen Person übernommen. Auch bei zukünftigen Software-Projekten kann nicht davon ausgegangen werden, dass ein mehrköpfiges Team für die Anforderungserhebung verfügbar ist.

Auch die Erhebung von nicht-kommunizierten Anforderungen konnte mit den Aktivitäten aus MEADigS nicht erfolgen.

Insgesamt macht MEADigS viele Vorschläge für mögliche Werkzeuge und Vorgehensweisen, aber wenig feste Vorgaben. Die Methode lässt viel Freiheit, die auch genutzt werden sollte.

Ob die vollständige Durchführung der Schritte 5 und 6 einen Mehrwert bietet, ist noch nicht abschließend geklärt. Es fällt jedoch auf, dass die Anforderungen im Anforderungsregister (Tabelle 14) bereits in einer guten Qualität sind.

7 Abschlussbetrachtung

In diesem Kapitel werden die wichtigsten Erkenntnisse dieser Arbeit zusammengetragen und ein Fazit gezogen. Abschließend wird ein Ausblick auf mögliche weiterführende Forschungsarbeiten gegeben.

7.1 Fazit

Die Evaluation zeigt, dass MEADigS in der Durchführung der Schritte 1 bis 4 effektiv und effizient ist. Auch die Akzeptanz der beteiligten Akteure war bei den Aktivitäten der genannten Schritte hoch. Der fünfte Schritt konnte nur teilweise durchgeführt werden, während Schritt 6 vollständig ausgelassen wurde. Eine Beurteilung der Effektivität dieser Schritte ist daher nur eingeschränkt möglich. Es ist fraglich, ob der Aufwand der Aktivitäten „Interviews mit Stakeholdervertretern“ und „Quantitative Erfassung“ in keinem angemessenen Verhältnis zum Nutzen steht.

Die Vollständigkeit der Anforderungen lässt sich nicht eindeutig feststellen. Es zeigt sich jedoch, dass die Themenfelder digitaler Souveränität zu 81% durch die entwickelten Anforderungen abgedeckt werden, was einen hohen Grad der Vollständigkeit impliziert.

Einschränkend muss erwähnt werden, dass die Zielsetzung von MEADigS, auch nichtkommunizierte Anforderungen zu erheben (Abschnitt 2.4.3) nicht erreicht werden konnte. Es ist zu bezweifeln, ob dies überhaupt in einer strukturierten Art und Weise möglich ist.

Die Anforderungen wurden im Rahmen der fokusgruppenähnlichen Workshops in Schritt 4 durch die Gruppe der Teilnehmenden validiert. Damit lässt sich die Korrektheit der Anforderungen feststellen.

Eine widersprüchliche Verwendung von Begriffen lässt sich in den Anforderungen nicht erkennen.

Die Nachvollziehbarkeit und Rückverfolgbarkeit der Anforderungen ist durch die klare Dokumentation der Herkunft und Ableitung jeder Anforderung sichergestellt.

Insgesamt zeigt die Evaluation, dass MEADigS ein vielversprechender Ansatz zur Entwicklung von Anforderungen im Bereich der digitalen Souveränität ist. Die Methode bietet einen weitestgehend strukturierten und gut durchdachten Prozess, um qualitativ hochwertige Anforderungen zu erheben.

Dennoch wäre es empfehlenswert, einzelne Aktivitäten der Methode zu präzisieren, wie den genauen Umfang mit dem erweiterten Themenfeldregister oder ein strukturiertes Verfahren bei der Analyse der Stakeholder.

Eine kritische Betrachtung der Methode ergibt, dass es in der Praxis nicht immer möglich ist, alle Aktivitäten der Methode vollständig umzusetzen. Es wird daher empfohlen, die Aktivität „Interviews mit Stakeholdervertretern“ sowie Schritt 6 als optional zu betrachten, um den Zeit- und Ressourcenaufwand entsprechend anzupassen. Darüber hinaus sollten Aktivitäten, die dringend notwendig sind, auch als solche markiert werden.

Wenn einem Projekt sehr viel Zeit und Ressourcen zur Verfügung stehen, würde eine vollständige Durchführung aller Aktivitäten relativ sicher zur sehr guten Ergebnissen führen. Es können aber auch schon mit deutlich weniger Aufwand sehr hochwertige Ergebnisse erzeugt werden.

7.2 Ausblick

Da diese Arbeit einen Teil der Methode, wie Interviews und die quantitative Erfassung, nicht durchgeführt hat, ist diese Evaluation nicht als abgeschlossen zu betrachten. Um festzustellen, wie Anforderungen im Bereich der digitalen Souveränität am besten entwickelt werden können, ist weitere Forschung notwendig.

Denkbar wäre, MEADigS im Kontext SDIKA exemplarisch anhand weiterer Stakeholdertypen wie natürlicher Personen und Vertrauensdiensten durchzuführen. Auch eine Betrachtung der Anforderungen der Wallet-Betreiber steht noch aus.

Eine weitere Frage, mit der sich zukünftige Arbeiten befassen könnten ist, wie Stakeholder systematisch analysiert werden können. Ein passendes Werkzeug für die Analyse könnte dazu führen, dass in Schritt 2 bereits einige Anforderungen erhoben werden könnten.

Auch ist denkbar, dass die Themenfelder im Themenfeldregister noch nicht alle Aspekte digitaler Souveränität abdecken. Da es sich um ein komplexes Thema handelt, das in der letzten Zeit immer mehr an Bedeutung gewonnen hat, lässt sich nicht ausschließen, dass in Zukunft weitere relevante Aspekte identifiziert werden.

In jedem Fall sollte sich die Wissenschaft weiterhin intensiv mit digitaler Souveränität befassen, um dazu beizutragen, dass Menschen souverän und selbstbestimmt im digitalen Raum handeln können.

Anhang

A Initiales Themenfeldregister

Tabelle 10: Initiales Themenfeldregister (Angelehnt an Weinreuter 2022, Tabelle 10 in Anhang F)

Themenfeld und Beschreibung	**untergeordnete Themenfelder**	**Anforderungsart**
Betriebs- und Geschäftsgeheimnisse befasst sich mit der Frage, wer organisationsspezifische Informationen, die sich aus kaufmännisch-geschäftlichen oder technischen Sphären ergeben und „erhebliche Unternehmenswerte“ (Alpers 2019, S. 88) darstellen können, autorisiert gewinnen darf.	Autorisierung, Informationsvertraulichkeit	Funktionale Anforderungen, Qualitätsanforderungen
Datenschutz umfasst rechtliche Rahmenbedingungen, die während der Verarbeitung personenbezogener Daten beachtet werden müssen und darüber hinaus weitere Bedingungen, die zum Schutz personenbezogener Daten erfüllt sein müssen.	Datenspeicher, Datenhoheit, Datenverarbeitung, Informationsvertraulichkeit	Funktionale Anforderungen, Qualitätsanforderungen
Entscheidungsträger befasst sich mit der Frage, wofür, beziehungsweise in welchen Gebieten, die Software dem Menschen Entscheidungen abnehmen darf und sollte.	Verantwortung, Substitution	Qualitätsanforderungen
Flexibilität befasst sich mit den Möglichkeiten, die die Software anbieten sollte, um die Software eigenständig zu erweitern, und auf den Stakeholder anzupassen	Skalierbarkeit, Vernetzbarkeit, Anpassbarkeit	Funktionale Anforderungen, Qualitätsanforderungen
Funktionalität umfasst die Vollständigkeit hinsichtlich der Softwarefunktionen und insbesondere den erwarteten Funktionsumfang durch die Stakeholder.	Angemessenheit, Richtigkeit	Funktionale Anforderungen
Identität befasst sich mit dem Management, der Speicherung, dem Schutz und der Authentizität von Identitätsdaten.	Identitätsmanagement, Autorisierung, Authentifizierung, Datenschutz	Funktionale Anforderungen, Qualitätsanforderungen
Infrastruktur befasst sich mit der Frage, auf welcher Basis, die Software aufgebaut werden sollte.	Ursprung der Infrastruktur, Integrität, Sicherheit	Qualitätsanforderungen, Begeisterungsanforderungen

Themenfeld und Beschreibung	untergeordnete Themenfelder	Anforderungsart
Interoperabilität umfasst die Vereinbarkeit der Software mit bereits existierenden digitalen Technologien, wodurch ein Wechsel zwischen verschiedenen Technologieanbietern vereinfacht wird.	Vernetzbarkeit, Integrität, Zugänglichkeit, Portabilität, Wechselmöglichkeit	Funktionale Anforderungen, Qualitätsanforderungen
IT-Sicherheit befasst sich mit der Frage, wie und wie weit der Stakeholder vor Gefahren und externen Angriffen geschützt werden möchte, beziehungsweise wie und wie viel Sicherheit gewährleistet werden soll.	Resilienz, Manipulationsfreiheit, Stabilität, Nachweisbarkeit, Rechtedelegation	Funktionale Anforderungen, Qualitätsanforderungen
Kompetenzeinsatz umfasst den erforderlichen und gewünschten Einsatz an Kompetenzen und Wissen des Stakeholders, der die Software anwendet, beziehungsweise den Einsatz an Unterstützungsangeboten und Assistenz, den die Software dem Stakeholder zur Verfügung stellen sollte.	Grundwissen, Selbstständigkeit, Assistenz	Qualitätsanforderungen
Kontrolle befasst sich mit der Frage, wie viel und wie der Stakeholder die Kontrolle über die Software und darin enthaltenen Prozesse ausüben soll.	Kontrollabgabe, Verantwortung	Funktionale Anforderungen, Qualitätsanforderungen
Leistung umfasst die Fähigkeit der Software, dem Stakeholder so zu dienen, dass der Einsatz einen Nutzen, auch in Relation zu vergleichbarer Software, bewirkt.	Zeitverhalten, Kosten, Nutzen Effektivität, Effizienz	Funktionale Anforderungen, Qualitätsanforderungen
Neutralität befasst sich mit der Frage, inwieweit die Software neutral von Gesetzen und Einschränkungen bleiben soll, und bis zu welchem Grad sie den Stakeholder beeinflussen sollte.	Einfluss, Limitationen	Funktionale Anforderungen, Qualitätsanforderungen
Plattformen befasst sich mit der Frage, wie und von dem die Plattformen gestaltet werden sollen.	Marktfragmentierung, Vertrauen	Qualitätsanforderungen
Privatsphäre befasst sich mit der Freigabe der Identität des Stakeholders und der den Stakeholder umgebenden Identitäten, beziehungsweise der Möglichkeit, die Software ohne Rückschluss auf den Identitätsinhaber zu nutzen.	Anonymität, Nichtverbindbarkeit, Kommunikation, Identität	Funktionale Anforderungen, Qualitätsanforderungen
Transparenz umfasst das Abstraktionslevel und das Ausmaß, mit der eine Software ihren Stakeholdern ihre algorithmische Entscheidungsprozesse, Nutzungsimplikationen und im Hintergrund ablaufenden Prozesse kommuniziert.	Information, Verständlichkeit, Offenheit, Rückverfolgbarkeit	Funktionale Anforderungen, Qualitätsanforderungen

Themenfeld und Beschreibung	untergeordnete Themenfelder	Anforderungsart
Unabhängigkeit umfasst den Abhängigkeitsgrad des Software-Anbieters zu seinen Stakeholdern sowie den Abhängigkeitsgrad der Software-Stakeholder, die die Software betreiben und nutzen, zu dem Software-Anbieter.	Kontrolle, Vertrauen, ausländische Unternehmen	Funktionale Anforderungen, Qualitätsanforderungen
Usability umfasst die Fähigkeit einer Software, in schneller Zeit verstanden, erlernbar und durchführbar zu sein.	Bedienbarkeit, Verständlichkeit, Einfachheit, Lernfähigkeit, Attraktivität	Funktionale Anforderungen, Qualitätsanforderungen
Vertrauen befasst sich mit der Frage, wie Vertrauen gewährt und Unsicherheiten beseitigt werden können.	Sicherheit, Schutz, Kontrolle	Funktionale Anforderungen, Qualitätsanforderungen
Zuverlässigkeit beschreibt die Fähigkeit einer Software, ein Leistungsniveau unter bestimmten Bedingungen über einen bestimmten Zeitraum aufrechtzuerhalten.	Fehlertoleranz, Haltbarkeit	Funktionale Anforderungen

B Stakeholderregister

Stakeholder	Beschreibung	Bereich	Rolle(n)	Stakeholdergruppe
Atruvia AG (früher: Fiducia)	IT-Dienstleister für Banken	Banking	Akzeptanzstelle, Vertrauensdienst	Unternehmen
Bitmi (e.V.)	Interessensverband IT-Mittelstand	IT		Organisation
brain-SCC GmbH	Softwareentwickler, E-Government, Portale für öffentliche Verwaltung	E-Government	Akzeptanzstelle	Unternehmen
Bund	Elektronischer Personalausweis	E-Government	Vertrauensdienst	Öffentliche Verwaltung
Bund	Führerschein	E-Government	Vertrauensdienst	Öffentliche Verwaltung
cantamen GmbH	Softwareentwickler für Car-sharing z.B. Stadtmobil, Bike-sharing, Fuhrparkverwaltung	Mobilität	Vertrauensdienst	Unternehmen
CAS Software AG	Softwareentwickler für CRM Systeme, WeNetwork (Wallet)	Digitale Identiäten	Betreiber digitale Wallet	Unternehmen
CIK	Karlsruher Pass	E-Government	Akzeptanzstelle, Vertrauensdienst	Organisation
CyberForum e.V.	Netzwerk	IT		Organisation
DIN e. V.	Normungsorganisation			Organisation
DPS Innovations GmbH	E-Government Lösungen, Digitalisierung von Verwaltung	E-Government	Vertrauensdienst	Unternehmen
First Cash Solution GmbH (Volksbank)	Zahlungsabwicklung	Banking	Akzeptanzstelle	Unternehmen
FZI Forschungs-zentrum Informatik	Forschungseinrichtung	Wissenschaft		Organisation

Stakeholder	Beschreibung	Bereich	Rolle(n)	Stakeholdergruppe
INIT GmbH	Software für ÖPNV z.B. Regiomove App (Buchungs- und Bezahlplattform)	Mobilität	Akzeptanzstelle	Unternehmen
Jolocom	SmartWallet App	Digitale Identiäten	Betreiber digitale Wallet	Unternehmen
KA-IT-Si	Sicherheitsinitiative	IT-Sicherheit		Organisation
KVV	Regiomove App	Mobilität	Akzeptanzstelle	Unternehmen
Metropolregion Rhein-Neckar GmbH	Öffentlichkeitsarbeit	Marketing		Organisation
raumobil GmbH	Softwareentwickler, Regiomove, Smart Mobility Map	Mobilität	Akzeptanzstelle	Unternehmen
Signicat GmbH	Identitätslösungen, Mobile Identität, Digitale Signaturen	Digitale Identiäten	Vertrauensdienst	Unternehmen
Stadt Karlsruhe	Gewerbeanmeldung, Baugenehmigungsverfahren	E-Government	Akzeptanzstelle, Vertrauensdienst	Öffentliche Verwaltung
Stadtmobil	Carsharing	Mobilität	Akzeptanzstelle	Unternehmen
Urban Software Institute GmbH	Strategische Beratung für Kommunen, Softwarehersteller	Mobilität, Energie	Akzeptanzstelle	Unternehmen
WIDAS ID GmbH	Softwarehersteller Identitätslösungen	Digitale Identiäten	Akzeptanzstelle, Vertrauensdienst	Unternehmen
YellowMap AG	Karten-Software	Mobilität	Akzeptanzstelle	Unternehmen
YES Payment Services GmbH	Zahlungsabwicklung	Banking	Akzeptanzstelle	Unternehmen
ZKRD	Knochenmarkspenderregister	Gesundheit	Akzeptanzstelle, Vertrauensdienst	Organisation

C Ergebnisse aus dem Workshop Unternehmensidentitäten

C.1 Was verstehen Sie unter digitaler Souveränität?

Sicher und souverän mit den persönlichen Daten im Internet und in Netzwerken bewegen können.

Sicherheit, bewegen im Digitalen Umfeld, Accounts unter einem sicheren und verifizierten Dach zu versammeln.

Sicherheit im Internet, Umgang mit eigenen Daten, persönliche Datenhoheit.

Digitale Souveränität als Teil der unternehmerischen Zielvision einiger SDIKA Partner. Grund ist die Frage der Nachhaltigkeit von Unternehmen und Nutzern. „Ich mag dauerhaft glücklich mein Leben leben." → Unternehmerische Ziele dauerhaft verfolgen können, Gefahren: Abhängigkeit, gläserner Mensch.

Selbstständiges Handeln in der digitalen Welt, ohne dass daraus Probleme für die echte Souveränität (in der normalen Welt) resultieren.

Reale und digitale Identitäten sind immer gekoppelt und beeinflussen sich gegenseitig.

Möglichkeit und Freiheit selbst zu bestimmen, was mit meinen Daten passieren soll (z.B. Löschen von Daten).

C.2 Use-Cases für Unternehmensidentitäten

Vertragsabschlüsse und/oder Zahlungen (z.B. Hotelbuchungen)

Mobilitätsguthaben für Mitarbeitende

Webseite auf Echtheit prüfen, z.B. mit einer Handelsregisterprüfung

Zeugnisse (Unternehmen bezeugt, dass Person X bei Unternehmen Y angestellt ist)

Zertifizierungen (z.B. ISO 27001) für Unternehmen, Produkte oder Prozesse

Fusionierung, Splittung oder Aufkauf von Unternehmen

Vertretungsberechtigungen (z.B. an Anwälte)

Übergeordnet: Identitätsnachweis, Beispiel: Unternehmen beantragt Stand auf dem Weihnachtsmarkt bei der Stadt KA, Insolvenzverfahren oder Förderungsantrag

Bio Siegel, Umweltsiegel

Nutzung mit viel Partnern im Kontext B2B/B2C/B2Gov

C.3 Weitere Fragestellungen für Unternehmensidentitäten

Was unterscheidet die Unternehmens-ID von anderen IDs (auch Organisationen wie GbR ohne staatliche Bestätigungen/Instanzen)? Wie ist die Unternehmens-ID an eine Personen-ID gekoppelt? Wer darf diese beantragen/vorzeigen/löschen/verwalten, nur ein Vorstand, auch ein Prokurist?

Wann nutze ich Unternehmens-ID, Vorstands-ID, Mitarbeiter-ID?

Wer ist der Vertrauensdienst? Wer stellt Unternehmens-ID aus? Das Handelsregister beim Registergericht (Amtsgericht)?

Ist eine Unternehmensidentität überhaupt nötig? Unternehmen besteht aus Mitarbeitern, die dann ein Zertifikat haben könnten, dass sie mit bestimmten Rechten wie Vorstand oder Prokurist für ein Unternehmen handeln. Beispiel: Car-Sharing-Angebot. Ist der Führschein und Personalausweis nicht obsolet, da man generell als Unternehmen handelt? Beispiel: Unternehmen mietet ein Auto für 20 Mitarbeitende. Was kann ich im „Außenverhältnis“ an Vertretungsmacht wirksam abbilden und rechtlich durchsetzen? (4 Augen Prinzip, Wertgrenzen,...). Was kann ich nur im Innenverhältnis regeln?

Kann eine Firma anonym handeln, ohne die Identität aufzudecken? Beispiele: Wird dem Staat ein Vertrag zwischen zwei Unternehmen offengelegt? Quellsteuer in der Schweiz: Schweiz meldet nicht DE, was der Mitarbeiter in der Schweiz gearbeitet hat.

Umgang mit rechtlich korrekten Bezeichnungen wie „XYZ GmbH & Co KG“ und Marke „XYZ“ klären. Kann es in der Identität beides geben? Weil der rechtlich korrekte Namen ist notwendig der andere aber vielleicht als „Alias“ oder so auch gewünscht

Wie wird sichergestellt, dass Daten aktuell sind und nicht veraltet? Stichwort: Handelsregister, neuen Auszug abholen

D Ergebnisse aus dem Workshop Akzeptanzstellen

D.1 Was verstehen Sie unter digitaler Souveränität?

Gefahr: Wenn ich zu viele Daten angebe, werde ich zu gläsern. Ich entscheide selbst, wo meine Daten hingehen

Informelle Selbstbestimmung, Informationen und deren Vertrauenswürdigkeit vernünftig einordnen können

Nutzende wissen, wohin, wann und warum ihre Daten verarbeitet werden

Datensparsamkeit, nur so viele Daten wie nötig übertragen und auch erhalten

These: Schwierig überhaupt noch souverän zu handeln

D.2 Use-Cases für Akzeptanzstellen

Self-issued Credentials, um Nutzer-Präferenzen zu hinterlegen, Beispiel: Nutzer bestellt online ein Kaffee und dieser ist beim Abholen fertig gerichtet und zwar mit Hafermilch

Kreative Bonus-/Rabattsysteme (Nutzer kauft 10 Fahrkarten und erhält im Urlaub Rabatt auf den E-Scooter zur Erkundung der Stadt)

D.3 Weitere Fragestellungen für Akzeptanzstellen

Aktualität von Credentials: Regiomove könnte Interesse haben, jedes Mal den Führerschein abzufragen, da sonst mehr bei Versicherungsfällen gezahlt werden muss → Holder kann Credential und ein Nachweis der Gültigkeit von diesem Credential vorzeigen: Möglich oder gewollt? Variante: Nach X Jahren muss der Nachweis neu gezeigt werden: Ist das von SSIPrinzip gewollt?

Muss eine Akzeptanzstelle nachweisen, wofür sie ihre Daten braucht? → Wallet könnte die Anfrage speichern als Beweis

E Erweitertes Themenfeldregister

Tabelle 11: Erweitertes Themenfeldregister

Themenfeld und Beschreibung	ID	Anforderung(en)
Berechtigungen befasst sich mit der Frage, wer innerhalb eines Unternehmens oder einer Organisation zu bestimmten Handlungen berechtigt ist.	U.6	Rechteverwaltung
Betriebs- und Geschäftsgeheimnisse befasst sich mit der Frage, wer organisationsspezifische Informationen, die sich aus kaufmännisch-geschäftlichen oder technischen Sphären ergeben und „erhebliche Unternehmenswerte“ (Alpers 2019, S. 88) darstellen können, autorisiert gewinnen darf.	U.1	Schutz von Unternehmensdaten
Datenschutz umfasst rechtliche Rahmenbedingungen, die während der Verarbeitung personenbezogener Daten beachtet werden müssen und darüber hinaus weitere Bedingungen, die zum Schutz personenbezogener Daten erfüllt sein müssen.	A.1	Datenschutz
Entscheidungsträger befasst sich mit der Frage, wofür, beziehungsweise in welchen Gebieten, die Software dem Menschen Entscheidungen abnehmen darf und sollte.	U.3 B.1	Fremdverwaltung Selbstverwaltung
Flexibilität befasst sich mit den Möglichkeiten, die die Software anbieten sollte, um die Software eigenständig zu erweitern, und auf den Stakeholder anzupassen	U.4	Anpassungsfähigkeit
Funktionalität umfasst die Vollständigkeit hinsichtlich der Softwarefunktionen und insbesondere den erwarteten Funktionsumfang durch die Stakeholder.	U.5 U.7 A.3	Internationale Verfügbarkeit Aktualität der Daten Gültigkeit

Themenfeld und Beschreibung	ID	Anforderung(en)
Identität befasst sich mit dem Management, der Speicherung, dem Schutz und der Authentizität von Identitätsdaten.	B.2	Verifikationsprozess
Infrastruktur befasst sich mit der Frage, auf welcher Basis, die Software aufgebaut werden sollte.		
Interoperabilität umfasst die Vereinbarkeit der Software mit bereits existierenden digitalen Technologien, wodurch ein Wechsel zwischen verschiedenen Technologieanbietern vereinfacht wird.	U.9 U.10	Interoperabilität Integration
IT-Sicherheit befasst sich mit der Frage, wie und wie weit der Stakeholder vor Gefahren und externen Angriffen geschützt werden möchte, beziehungsweise wie und wie viel Sicherheit gewährleistet werden soll.	U.11 B.3	Sicherer Zugang Sichere Datenübertragung
Kompetenzeinsatz umfasst den erforderlichen und gewünschten Einsatz an Kompetenzen und Wissen des Stakeholders, der die Software anwendet, beziehungsweise den Einsatz an Unterstützungsangeboten und Assistenz, den die Software dem Stakeholder zur Verfügung stellen sollte.	B.4	Verständlichkeit
Kontrolle befasst sich mit der Frage, wie viel und wie der Stakeholder die Kontrolle über die Software und darin enthaltenen Prozesse ausüben soll.	U.15 B.5	Nachvollziehbarkeit Rechtssicherheit
Leistung umfasst die Fähigkeit der Software, dem Stakeholder so zu dienen, dass der Einsatz einen Nutzen, auch in Relation zu vergleichbarer Software, bewirkt.	U.16 U.17 A.10 A.11 B.6 B.7 B.8	Technische Machbarkeit Digitale Prozesse Transparente Kosten Geringe Einstiegshürden Weite Verbreitung Geringe Kosten Schnellere Prozesse

Themenfeld und Beschreibung	ID	Anforderung(en)
Neutralität befasst sich mit der Frage, inwieweit die Software neutral von Gesetzen und Einschränkungen bleiben soll, und bis zu welchem Grad sie den Stakeholder beeinflussen sollte.		
Plattformen befasst sich mit der Frage, wie und von dem die Plattformen gestaltet werden sollen.		
Privatsphäre befasst sich mit der Freigabe der Identität des Stakeholders und der den Stakeholder umgebenden Identitäten, beziehungsweise der Möglichkeit, die Software ohne Rückschluss auf den Identitätsinhaber zu nutzen.		
Transparenz umfasst das Abstraktionslevel und das Ausmaß, mit der eine Software ihren Stakeholdern ihre algorithmische Entscheidungsprozesse, Nutzungsimplikationen und im Hintergrund ablaufenden Prozesse kommuniziert.	U.21 A.13	Open-Source Transparenz mit Dienstleistern
Unabhängigkeit umfasst den Abhängigkeitsgrad des Software-Anbieters zu seinen Stakeholdern sowie den Abhängigkeitsgrad der Software-Stakeholder, die die Software betreiben und nutzen, zu dem Anbieter.	A.15 B.9	Standardisierung Unabhängigkeit
Usability umfasst die Fähigkeit einer Software, in schneller Zeit verstanden, erlernbar und durchführbar zu sein.	A.16 B.10	Unkomplizierte Anbindung Einfache UX
Vertrauen befasst sich mit der Frage, wie Vertrauen gewährt und Unsicherheiten beseitigt werden können.	A.19 B.11	Validität der Prozesse Vertrauenswürdigkeit
Zuverlässigkeit beschreibt die Fähigkeit einer Software, ein Leistungsniveau unter bestimmten Bedingungen über einen bestimmten Zeitraum aufrechtzuerhalten.	A.20 B.12	Zukunftssicher Verfügbarkeit

F Anforderungsdokument

F.1 Übersicht

Projektbeschreibung Das Schaufenster Sichere Digitale Identitäten Karlsruhe (SDIKA) ist ein Schaufensterprojekt in der Stadt Karlsruhe und der Metropolregion Rhein-Neckar. Es ist eines von vier vom Bundesministerium für Wirtschaft und Klimaschutz (BMWK) im Rahmen eines Innovationswettbewerbs geförderten Projekten mit dem Thema Sichere Digitale Identitäten. (BMWK 2023) Der Hintergrund des Wettbewerbs ist der Mangel an nutzerfreundlichen, vertrauenswürdigen und gleichzeitig wirtschaftlichen Lösungen für digitale Identitäten. Ziel des Projekts SDIKA ist die Entwicklung einer interoperablen software-basierten Lösung für digitale Identitäten. Das Projekt wird von der Stadt Karlsruhe koordiniert und in Kooperation mit diversen Partnern wie unter anderem dem Forschungszentrum Informatik (FZI) und Unternehmen aus dem Bereich der Software-Entwicklung sowie verschiedene Dienststellen der öffentlichen Verwaltung entwickelt.

Stakeholdergruppen Die Stakeholder sicherer digitaler Identitäten sind sowohl natürliche Personen als auch der Staat, die öffentliche Verwaltung sowie Unternehmen und Organisationen aus der Zivilgesellschaft, Wissenschaft und Wirtschaft.

Stakeholdertypen Die Rollen der Akteure in SDIKA sind: Akzeptanzstelle, Identitätsinhaber, Vertrauensdienst und Wallet-Betreiber.
In diesem Anforderungsdokument sind die Anforderungen der folgenden Stakeholdertypen abgedeckt:

1. Unternehmen als Identitätsinhaber
2. Akzeptanzstellen

Inhalte

1. Übersicht
2. Glossar
3. Themenfeldregister
4. Anforderungsregister

F.2 Glossar

Tabelle 12: Glossar

Begriff	Definition / Erklärung
Akzeptanzstelle	In SDIKA: Prüft und akzeptiert Credentials (z.B. Unternehmen oder Institution)
Cloud-based Identity	Ansatz, bei dem ein Anbieter die Identität eines Anwenders zentral in der Cloud verwaltet.
eID	digitale/elektronische Identität
Identitätsinhaber	In SDIKA: Das Subjekt, das Inhaber eine Identität ist (z.B. Natürliche Person oder Unternehmen/Institution)
Karlsruher Pass	Angebot der Stadt Karlsruhe für Einwohner mit geringem Einkommen bzw. Empfänger von Sozialleistungen. Gewährt Rabatte für diverse öffentlche Einrichtungen.
SDIKA	Schaufenster Sichere Digitale Identitäten Karlsruhe
SSI (Self-Sovereign Identity)	Technologieneutraler Ansatz, bei dem der Anwender seine Identität selbst verwaltet
UX	User Experience, Erfahrung, die Nutzende mit einem Produkt machen
Vertrauensdienst	In SDIKA: Institution, die Identitäten ausstellt
Wallet	Digitale Brieftasche, in der Identitätsnachweise aufbewahrt werden können

F.3 Themenfeldregister

Tabelle 13: Finales Themenfeldregister

Themenfeld und Beschreibung	**untergeordnete Themenfelder**	**Anforderungsart**
Berechtigungen befasst sich mit der Frage, wer innerhalb eines Unternehmens oder einer Organisation zu bestimmten Handlungen (Vertragsabschlüsse, Käufe, Buchungen) berechtigt ist.	Kompetenzeinsatz	Funktionale Anforderungen, Qualitätsanforderungen
Betriebs- und Geschäftsgeheimnisse befasst sich mit der Frage, wer organisationsspezifische Informationen, die sich aus kaufmännisch-geschäftlichen oder technischen Sphären ergeben und „erhebliche Unternehmenswerte“ (Alpers 2019, S. 88) darstellen können, autorisiert gewinnen darf.	Autorisierung, Informationsvertraulichkeit	Funktionale Anforderungen, Qualitätsanforderungen
Datenschutz umfasst rechtliche Rahmenbedingungen, die während der Verarbeitung personenbezogener Daten beachtet werden müssen und darüber hinaus weitere Bedingungen, die zum Schutz personenbezogener Daten erfüllt sein müssen.	Datenspeicher, Datenhoheit, Datenverarbeitung, Informationsvertraulichkeit	Funktionale Anforderungen, Qualitätsanforderungen
Entscheidungsträger befasst sich mit der Frage, wofür, beziehungsweise in welchen Gebieten, die Software dem Menschen Entscheidungen abnehmen darf und sollte.	Verantwortung, Substitution	Qualitätsanforderungen
Flexibilität befasst sich mit den Möglichkeiten, die die Software anbieten sollte, um die Software eigenständig zu erweitern, und auf den Stakeholder anzupassen	Skalierbarkeit, Vernetzbarkeit, Anpassbarkeit	Funktionale Anforderungen, Qualitätsanforderungen
Funktionalität umfasst die Vollständigkeit hinsichtlich der Softwarefunktionen und insbesondere den erwarteten Funktionsumfang durch die Stakeholder.	Angemessenheit, Richtigkeit	Funktionale Anforderungen
Identität befasst sich mit dem Management, der Speicherung, dem Schutz und der Authentizität von Identitätsdaten.	Identitätsmanagement, Autorisierung, Authentifizierung, Datenschutz	Funktionale Anforderungen, Qualitätsanforderungen
Infrastruktur befasst sich mit der Frage, auf welcher Basis, die Software aufgebaut werden sollte.	Ursprung der Infrastruktur, Integrität, Sicherheit	Qualitätsanforderungen, Begeisterungsanforderungen

Themenfeld und Beschreibung	untergeordnete Themenfelder	Anforderungsart
Interoperabilität umfasst die Vereinbarkeit der Software mit bereits existierenden digitalen Technologien, wodurch ein Wechsel zwischen verschiedenen Technologieanbietern vereinfacht wird.	Vernetzbarkeit, Integrität, Zugänglichkeit, Portabilität, Wechselmöglichkeit	Funktionale Anforderungen, Qualitätsanforderungen
IT-Sicherheit befasst sich mit der Frage, wie und wie weit der Stakeholder vor Gefahren und externen Angriffen geschützt werden möchte, beziehungsweise wie und wie viel Sicherheit gewährleistet werden soll.	Resilienz, Manipulationsfreiheit, Stabilität, Nachweisbarkeit, Rechtedelegation	Funktionale Anforderungen, Qualitätsanforderungen
Kompetenzeinsatz umfasst den erforderlichen und gewünschten Einsatz an Kompetenzen und Wissen des Stakeholders, der die Software anwendet, beziehungsweise den Einsatz an Unterstützungsangeboten und Assistenz, den die Software dem Stakeholder zur Verfügung stellen sollte.	Grundwissen, Selbstständigkeit, Assistenz	Qualitätsanforderungen
Kontrolle befasst sich mit der Frage, wie viel und wie der Stakeholder die Kontrolle über die Software und darin enthaltenen Prozesse ausüben soll.	Kontrollabgabe, Verantwortung	Funktionale Anforderungen, Qualitätsanforderungen
Leistung umfasst die Fähigkeit der Software, dem Stakeholder so zu dienen, dass der Einsatz einen Nutzen, auch in Relation zu vergleichbarer Software, bewirkt.	Zeitverhalten, Kosten, Nutzen Effektivität, Effizienz	Funktionale Anforderungen, Qualitätsanforderungen
Neutralität befasst sich mit der Frage, inwieweit die Software neutral von Gesetzen und Einschränkungen bleiben soll, und bis zu welchem Grad sie den Stakeholder beeinflussen sollte.	Einfluss, Limitationen	Funktionale Anforderungen, Qualitätsanforderungen
Plattformen befasst sich mit der Frage, wie und von dem die Plattformen gestaltet werden sollen.	Marktfragmentierung, Vertrauen	Qualitätsanforderungen
Privatsphäre befasst sich mit der Freigabe der Identität des Stakeholders und der den Stakeholder umgebenden Identitäten, beziehungsweise der Möglichkeit, die Software ohne Rückschluss auf den Identitätsinhaber zu nutzen.	Anonymität, Nichtverbindbarkeit, Kommunikation, Identität	Funktionale Anforderungen, Qualitätsanforderungen
Transparenz umfasst das Abstraktionslevel und das Ausmaß, mit der eine Software ihren Stakeholdern ihre algorithmische Entscheidungsprozesse, Nutzungsimplikationen und im Hintergrund ablaufenden Prozesse kommuniziert.	Information, Verständlichkeit, Offenheit, Rückverfolgbarkeit	Funktionale Anforderungen, Qualitätsanforderungen

Themenfeld und Beschreibung	untergeordnete Themenfelder	Anforderungsart
Unabhängigkeit umfasst den Abhängigkeitsgrad des Software-Anbieters zu seinen Stakeholdern sowie den Abhängigkeitsgrad der Software-Stakeholder, die die Software betreiben und nutzen, zu dem Software-Anbieter.	Kontrolle, Vertrauen, ausländische Unternehmen	Funktionale Anforderungen, Qualitätsanforderungen
Usability umfasst die Fähigkeit einer Software, in schneller Zeit verstanden, erlernbar und durchführbar zu sein.	Bedienbarkeit, Verständlichkeit, Einfachheit, Lernfähigkeit, Attraktivität	Funktionale Anforderungen, Qualitätsanforderungen
Vertrauen befasst sich mit der Frage, wie Vertrauen gewährt und Unsicherheiten beseitigt werden können.	Sicherheit, Schutz, Kontrolle	Funktionale Anforderungen, Qualitätsanforderungen
Zuverlässigkeit beschreibt die Fähigkeit einer Software, ein Leistungsniveau unter bestimmten Bedingungen über einen bestimmten Zeitraum aufrechtzuerhalten.	Fehlertoleranz, Haltbarkeit	Funktionale Anforderungen

F.4 Anforderungsregister

Tabelle 14: Anforderungsregister

Name und Beschreibung	Begründung	Art	Weitere Anmerkungen
U.1 Schutz von Unternehmensdaten[8] Der Schutz von Unternehmensdaten soll gewährleistet sein.	Unternehmensdaten (ohne Personen- bezug) fällt nicht unter die EU-DS- GVO. Unternehmen haben ein Interes- se, dass Geheimnisse geschützt sind.	Qualitätsanforderung	Datenschutz vs. Schutz von Geschäftsgeheimnissen: Personenbezogene Daten werden gesetzlich anders behandelt als Daten von Unternehmen (Alpers 2019, Abb. 2)
U.4 Anpassungsfähigkeit Die benötigten Identitätsnachweise lassen sich abbilden.	Unternehmen und ihre Daten können sich im Laufe der Zeit ändern. Bei Veränderungen soll es möglich sein, die Identität und sie betreffende Regeln anzupassen.	Grundanforderung	
U.5 Internationale Verfügbarkeit Die Lösung soll international verfügbar sein.	Unternehmen haben oft Geschäfts- partner/Kunden in der ganzen Welt. Auch im Ausland soll die Funktionali- tät der Lösung gewährleistet sein.	Grundanforderung	Mögliche Fragestellungen: Datenschutzthematik, unsichere Drittländer, Standards usw.
U.6 Rechteverwaltung Verschiedene Rollen von Anwendern Vollmachten und Arbeitsvertretung sollen abbildbar sein.	Es soll sichergestellt werden, dass die Person (z.B. Mitarbeiter), die mit der Unternehmensidentität handelt, auch für die entsprechende Handlung (z.B. Vertragsabschluss) berechtigt ist. Vollmachten wie Prokura sollen abbildbar sein. Bei Ausfall eines Kollegen soll eine einfache Arbeitsvertretung möglich sein.	Grundanforderung	Unternehmensidentitäten sind immer mit handelnden natürlichen Personen und deren Identitäten verknüpft. Bsp: Außendarstellung von einem Unternehmen, ohne dass die handelnde Person sichtbar ist, Credentials von Produkten (Zusicherung von Produkteigenschaften). Analogie: Eine Person hat das Vertretungsrecht für das Unternehmen und nur das in diesem Fall benötigte Merkmal des Unternehmens aus. (wie aus dem Personalausweis nur die Eigenschaft der Volljährigkeit)

[8] „Unternehmen“ bezeichnet hier alle Formen von Organisationen.

Name und Beschreibung	Begründung	Art	Weitere Anmerkungen
U.7 Aktualität der Daten Die Aktualität der Daten wird gewährleistet.	Identitätsdaten können abgelaufen oder veraltet sein. Die Lösung sollte sicherstellen, dass die Daten aktuell sind.	Grund-anforderung	
U.9 Interoperabilität Durch einen modularen und transparenten Aufbau soll die Lösung Interoperabel sein. Sowohl selbst- als auch fremdverwaltete Systeme sollen miteinander kompatibel sein.	Lock-in Effekt zu einzelnen Anbietern soll vermieden werden. Daher muss sowohl die Nutzung verschiedener Wallets als auch der Credential-Austausch zwischen verschiedenen Wallet-Anbietern möglich sein.	Grund-anforderung	
U.10 Integration Die Integration in bestehende Anwendungen soll möglich sein.	Betriebliche Informationssysteme, Workflow Management Systeme	Grund-anforderung	
U.11 Sicherer Zugang Der Zugang zum System soll gesichert sein.	Schutz vor Fälschung und Manipulation	Qualitäts-anforderung	
U.15 Nachvollziehbarkeit Es soll möglich sein, Vorgänge im Nachhinein offen zu legen.	Das Unternehmen muss in der Lage sein, zu überprüfen, welche Berechtigten in einem konkreten Fall mit der Unternehmensidenität gehandelt haben. Andere dürfen das nicht können.	Grund-anforderung	Nachvollziehbarkeit durch den Identitätsinhaber aus technischer Sicht
U.16 Technische Machbarkeit Die Auswahl der Endgeä- te soll für alle Unterneh- men machbar sein.	Die Notwendigkeit der Beschaffung von Hardware darf nicht zur Einstiegshürde werden.	Qualitäts-anforderung	z.B. 1-Personen Betriebe haben oft wenig Endgeräte zur Verfügung. Die Lösung sollte auch z.B. mit einem Smartphone funktionieren.
U.17 Digitale Prozesse Die Lösung und ihre Prozesse sollten möglichst digital sein.	Papier reduzieren und dadurch effizientere Prozesse.	Qualitäts-anforderung	dadurch werden die Prozesse für Menschen einfacher durchschaubar.
U.21 Open-Source Der Quellcode der Lösung sollte öffentlich einsehbar sein.	Durch Transparenz soll Vertrauen geschaffen werden.	Qualitäts-anforderung	
A.1 Datenschutz Personenbezogene Daten sollen geschützt werden	Nutzer und ihre Daten sollen durch das System nicht ausgenutzt.	Qualitäts-anforderung	z.B. Die gesetzlichen Regelungen (z.B. EU-DS-GVO u.a.) werden eingehalten, Datenaustausch muss für Nutzer kompakt zusammengefasst sein.
A.3 Gültigkeit Die Gültigkeit der Credentials soll sichergestellt sein.	Die Gültigkeit von Nachweisen kann ablaufen (z.B. Führerschein hat ein Ablaufdatum). Wenn der Nachweis abgelaufen ist, sollte er nicht mehr verwendet werden können.	Grund-anforderung	

Name und Beschreibung	Begründung	Art	Weitere Anmerkungen
A.10 Transparente Kosten Die Kosten für die Lösung sollen transparent sein.		Qualitäts-anforderung	
A.11 Geringe Einstiegshürden Die Integration in Geschäftsprozesse soll kostengünstig und einfach sein.	Bsp: Eisdiele will sich nicht verändern, um digitale Identität nutzen zu können.	Qualitäts-anforderung	
A.13 Transparenz mit Dienstleistern Der Umgang mit (Unter-)auftragnehmern wie z.B. integrierten Zahlungsdiensten muss Transparent und nutzer-verständlich sein.	z.B. Unternehmen arbeitet mit einem Zahlungsdienst zusammen. Nutzer sieht im Bankkonto die Abbuchung von LogPay und kann diese nicht Regiomove zuordnen.	Qualitäts-anforderung	
A.14 Unabhängigkeit Keine Abhängigkeiten weder zur Lösung noch zu einem Anbieter	Der Betrieb soll nicht abhängig von der Einführung der Lösung sein. Prozesse sollen auch ohne das System weiter funktionieren. Keine Lock-In Effekte	Qualitäts-anforderung	z.B. bei Ausfall oder wenn das System abgeschafft wird oder jemand es nicht nutzen möchte.
A.16 Unkomplizierte Anbindung Die Anbindung und der Betrieb der Lösung soll unkompliziert sein.		Qualitäts-anforderung	
A.19 Validität der Prozesse Die Akzeptanzstelle soll sicher sein, dass die Prozesse valide sind.		Qualitäts-anforderung	
A.20 Zukunftssicher Die Lösung sollte nachhaltig sein.	Bei Umstellung des Systems (z.B. bei Aufkauf) soll nicht wieder mühselig umgestellt werden müssen.	Qualitäts-anforderung	
B.1 Selbstbestimmung Wahlmöglichkeit zwischen SSI und Cloud-basiertem Ansatz. Nutzende müssen die Möglichkeit haben, ihre Identität/Credentials selbst und lokal verwalten zu können oder diese cloud-basiert verwalten zu lassen.	Anwender sollen die Kontrolle über Aufnahme, Speicherung, Löschung und Dauer der Datenverarbeitung haben. (SSI) Weniger Datenschutzprobleme durch lokale Speicherung. Datensparsamkeit: Es sollen nur die Merkmale übertragen werden, die auch wirklich notwendig sind (z.B. Volljährigkeit, nicht das Geburtsdatum).	Grund-anforderung	SSI vs. Cloud-based. Wahlmöglichkeit soll gegeben sein (vgl. Datensouveränität als eine Dimension digitaler Souveränität). Es gibt aber Fälle, in denen gewisse Daten gespeichert werden müssen. Evtl. Konflikt mit der Nachvollziehbarkeit/Rechtssicherheit

Name und Beschreibung	Begründung	Art	Weitere Anmerkungen
B.2 Verifikationsprozess Die Identitätsmerkmale sollen verifiziert sein. Die Echtheit der Identität soll gewährleistet gewährleistet sein.	Die Überprüfung der Echtheit von Nachweisen wird durch das System übernommen und erübrigt sich aus Sicht der Nutzenden. Eine öffentliche Stelle soll bestätigen, dass die Identität echt ist. Bei der Verifikation der Identität soll es keine Abhängigkeit zu privaten Akteuren geben.	Grund-anforderung	ggf. Frage: ist die öffentliche Stelle zur Bestätigung der Identitäten verpflichtet?
B.3 Sichere Datenübertragung Die Übertragung von Daten soll sicher vor Fälschung und Manipulation sein.	An der Schnittstelle werden Daten ausgetauscht. Diese Transaktion soll sicher sein. Vertrauen in die Lösung kann nur entstehen, wenn die Übertragung von Daten sicher ist.	Qualitäts-anforderung	Digital ist nicht zwangsläufig sicherer als analog. Die Umsetzung muss auch entsprechend Sicherheit gewährleisten. IT-Schutzziele: Vertraulichkeit und Integrität, aber auch: Datenschutz
B.4 Verständlichkeit Die Lösung soll für Endnutzende leicht zu verstehen sein.	Die Mitarbeiter in den Betrieben müssen das System verstehen, um die Konsequenzen ihrer Handlungen einschätzen zu können. Nutzer müssen verstehen, welche Nachweise sie liefern müssen und was damit passiert. Dafür müssen die Informationen kompakt zusammengefasst präsentiert werden (keine 30 Seiten AGB).	Qualitäts-anforderung	Bsp: die Bedeutung des Schloss-Symbols für SSL-verschlüsselte Webseiten ist für viele Personen nicht leicht verständlich. (vgl. Kompetenzen als eine Dimension digitaler Souveränität)
B.5 Rechtssicherheit Transaktionen sollen be-/nachweisbar und dadurch rechtssicher und nichtabstreitbar sein.	Die Freigabe eines Identitätsmerkmals darf nicht im Nachhinein abgestritten werden können. Sie muss in der wirklichen Welt und vor Gericht anerkannt werden.	Grund-anforderung	Nachvollziehbarkeit im rechtlichen Sinne
B.6 Weite Verbreitung Die Lösung soll weit verbreitet und einsetzbar sein. Viele Identitäten sollen durch die Lösung abgebildet werden können. Alle notwendigen Nachweise, Wallets, Credential-Typen sollen von der Lösung abgebildet werden können. Es sollte viele Akzeptanzstellen geben, die die Lösung anerkennen.	Nur bei vielen Nutzern hat die Lösung einen Mehrwert. Verwaltung von sicheren Digitalen Identitäten sollte „Grundbedürfnis“ von Unternehmen sein (ohne eine digitale Identität zu sein, sollte für Unternehmen undenkbar sein)	Qualitäts-anforderung	
B.7 Geringe Kosten Die Nutzung sollte wirtschaftlich (nicht zu teuer) sein.	Kosten/Nutzenverhältnis	Qualitäts-anforderung	

Name und Beschreibung	Begründung	Art	Weitere Anmerkungen
B.8 Schnellere Prozesse Die Lösung sollte Arbeitsprozesse beschleunigen und dadurch Ressourcen sparen.		Qualitäts-anforderung	
B.9 Standardisierung Unabhängigkeit von einer einzelnen Lösung, gültige Credential-Standards. Das System wird nicht von einem einzelnen Akteur kontrolliert (auch in Zukunft).	Keine Vendor Lock-in Effekte zu einem bestimmten Wallet-Betreiber. Abhängigkeit von einem einzelnen Akteur oder einer Plattform führt zu einem Verlust von Souveränität.	Qualitäts-anforderung	
B.10 Einfache User Experience (UX) Aus Nutzersicht einfache Verwaltung und Steuerung der Lösung durch übersichtliche Darstellung der Daten	Nicht zu technische Darstellung, Nachvollziehbar für Menschen.	Qualitäts-anforderung	
B.11 Vertrauenswürdigkeit Die Lösung soll vertrauenswürdig sein.	Dritte sollen der digitalen Identität vertrauen können. Die Lösung soll ebenso vertrauenswürdig sein wie z.B. das Handelsregister ("öffentlicher Glauben")	Qualitäts-anforderung	Das System darf nicht missbraucht werden und alles kontrollieren, was der Anwender macht.
B.12 Verfügbarkeit Ein zuverlässiger Betrieb des Systems soll gewährleistet werden (Mindestverfügbarkeit, Service-Level)	Frei von Störungen. IT-Schutzziel: Verfügbarkeit, auch: wirtschaftliche Interessen der Unternehmen an der Verfügbarkeit des Systems	Qualitäts-anforderung	Mindestverfügbarkeit z.B. bei Netzausfall, ggf. Offline-Verfügbarkeit (Spannungsfeld Datenschutz), Service Level

Literatur

Alpers S. (2019). *Modellbasierte Entscheidungsunterstützung für Vertraulichkeit und Datenschutz in Geschäftsprozessen.* DOI: 10.5445/KSP/1000094545.

Alpers S., Sürmeli J., Trunko R. (2020). "eID einfach einsetzen". In: *Kommune 21* 10/2020, S. 48–49. ISSN: 1618-2901.

Beyerer J., Müller-Quade J., Reussner R. (2018). "Karlsruher Thesen zur Digitalen Souveränität Europas". In: *Datenschutz und Datensicherheit - DuD* 42.5, S. 277–280. ISSN: 1614-0702. DOI: 10.1007/s11623-018-0940-2.

Bitkom e.V. (2019). *Digitale Souveränität: Anforderungen an Technologien- und Kompetenzfelder mit Schlüsselfunktion.* URL: https://www.bitkom.org/sites/main/files/2020-01/200116_stellungnahme_digitale-souveranitat.pdf.

Borges G., Werners B. (2018). *Identitätsmanagement im Cloud Computing: Evaluation ökonomischer und rechtlicher Rahmenbedingungen.* Berlin und Heidelberg: Springer. ISBN: 3662555832. DOI: 10.1007/978-3-662-55584-2.

Brazel M., Sauer M., Alpers S. (2023). *Dokumentation Workshops Digitale Souveränität aus Sicht von Unternehmen und Organisationen als Identitätsinhaber sowie Akzeptanzstellen für digitale Identitäten.* DOI: 10.13140/RG.2.2.18886.55366.

Bundesministerium für Wirtschaft und Energie (2019). *Innovationswettbewerb „Schaufenster Sichere Digitale Identitäten". Förderaufruf auf Grundlage des Förderrahmens „Entwicklung digitaler Technologien".* (BAnz 17.01.2019 B1. URL: https://www.digitale-technologien.de/DT/Redaktion/DE/Downloads/innovationswettbewerb-schaufenster-sichere-digitale-identitaeten-foerderaufruf.pdf.

Bundesministerium für Wirtschaft und Klimaschutz: Aktuelle Technologieprogramme (2023). *SDIKA.* https://www.digitale-technologien.de/DT/Navigation/DE/ProgrammeProjekte/AktuelleTechnologieprogramme/Sichere_Digitale_Identitaeten/Projekte_Umsetzungsphase/SDIKA/SDIKA.html. Abgerufen am 14.03.2023.

Camp, J. L. (2004). "Digital identity". In: *IEEE Technology and Society Magazine* 23.3, S. 34–41. DOI: 10.1109/MTAS.2004.1337889.

Celar S. Turic M., Vicković L. (2010). "Stakeholder Analysis: Process Modell". In: URL: https://api.semanticscholar.org/CorpusID:168597844.

Couture S., Toupin S. (2019). "What does the notion of "sovereignty" mean when referring to the digital?" In: *New Media & Society* 21.10, S. 2305–2322. DOI: 10.1177/1461444819865984. eprint: https://doi.org/10.1177/1461444819865984. URL: https://doi.org/10.1177/1461444819865984.

Davis, A., Dieste O., Hickey A., Juristo N., Moreno A. M. (2006). "Effectiveness of Requirements Elicitation Techniques: Empirical Results Derived from a Systematic Review". In: S. 179–188. DOI: 10.1109/RE.2006.17.

DIN e.V. (Hrsg.) (2015). *Qualitätsmanagementsysteme - Grundlagen und Begriffe (ISO 9000:2015)*. Standard. Berlin.

Fantechi A., Gnesi S., Semini L. (2023). "VIBE: Looking for Variability In amBiguous rEquirements". In: *Journal of Systems and Software* 195, S. 111540. ISSN: 0164-1212. DOI: https://doi.org/10.1016/j.jss.2022.111540. URL: https://www.sciencedirect.com/science/article/pii/S0164121222002163.

Ferrari A., Spoletini P., Gnesi S. (2016). "Ambiguity and tacit knowledge in requirements elicitation interviews". In: *Requirements Engineering* 21. DOI: 10.1007/s00766-016-0249-3.

Floridi L. (2020). "The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU". In: *Philosophy & Technology* 33. DOI: 10.1007/s13347-020-00423-6.

Fuentes-Fernandez R., Gomez-Sanz J. J., Pavon J. (2009). "Requirements Elicitation and Analysis of Multiagent Systems Using Activity Theory". In: *IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans* 39.2, S. 282–298. DOI: 10.1109/TSMCA.2008.2010747.

Garstka, H. (2003). "Informationelle Selbstbestimmung und Datenschutz". In: *Bürgerrechte im Netz*. Hrsg. von Schulzki-Haddouti C. Wiesbaden: VS Verlag für Sozialwissenschaften, S. 48–70. ISBN: 978-3-322-92400-1. DOI: 10.1007/978-3-322-92400-1_5. URL: https://doi.org/10.1007/978-3-322-92400-1_5.

Goldacker, G. (2017). *Digitale Souveränität*. 1. Auflage. Berlin: Kompetenzzentrum Öffentliche IT, Fraunhofer-Institut für Offene kommunikationssysteme FOKUS. ISBN: 9783981889222.

Gupta A. K., Deraman A. (2019). "Algorithmic Solution for Effective Selection of Elicitation Techniques". In: *2019 International Conference on Computer and Information Sciences (ICCIS)*, S. 1–7. DOI: 10.1109/ICCISci.2019.8716378.

Heitmeyer C. L., Jeffords R. D., Labaw B. G. (1996). "Automated Consistency Checking of Requirements Specifications". In: *ACM Trans. Softw. Eng. Methodol.* 5.3, S. 231–261. ISSN: 1049-331X. DOI: 10.1145/234426.234431. URL: https://doi.org/10.1145/234426.234431.

Hopt K. J., Merkt H. (2023). *Kommentar zum HGB*. Band 9. Beck'sche Kurz-Kommentare.

Kametani T., Nishina K., Suzuki K. (2010). "Attractive Quality and Must-be Quality from the Viewpoint of Environmental Lifestyle in Japan". In: *Frontiers in Statistical Quality Control 9*. Hrsg. von Lenz, H., Wilrich P., Schmid W. Heidelberg: Physica-Verlag HD, S. 315–327. ISBN: 978-3-7908-2380-6. DOI: 10.1007/978-3-7908-2380-6_20. URL: https://doi.org/10.1007/978-3-7908-2380-6_20.

Kanwal A. (2019). "Requirements Engineering: Elicitation Techniques". In: *International Journal of Scientific & Engineering Research*. Volume 10, Issue 6. ISSN: 2229-5518.

Kato, T., Tsuda, K. (2022). "A Method of Ambiguity Detection in Requirement Specifications by Using a Knowledge Dictionary". In: *Procedia Computer Science* 207, S. 1482–1489. ISSN: 18770509. DOI: 10.1016/j.procs.2022.09.205.

Kranich L., Hauth P., Pols A. (2017). *Kompetenzen für eine Digitale Souveränität. Studie im Auftrag des Bundesministeriums für Wirtschaft und Energie (BMWi).* FZI Forschungszentrum Informatik. URL: https://www.bmi.bund.de/cybersicherheitsstrategie/BMI_CyberSicherheitsStrategie.pdf.

Kromrey, H. (2001). "Evaluation–ein vielschichtiges Konzept. Begriff und Methodik von Evaluierung und Evaluationsforschung. Empfehlungen für die Praxis". In: *Sozialwissenschaften und Berufspraxis* 2.

Krupka, D. (2020). "Dimensionen digitaler Souveränität - Ein Überblick". In: *Arbeitspapier Schlüsselaspekte digitaler Souveränität.* Gesellschaft für Informatik e.V., S. 1–13.

Miles, S. (2017). "Stakeholder Theory Classification: A Theoretical and Empirical Evaluation of Definitions". In: *Journal of Business Ethics* 142.3, S. 437–459. ISSN: 0167-4544. DOI: 10.1007/s10551-015-2741-y.

Murtazina M. S., Avdeenko T. V. (2019). "An Ontology-based Approach to Support for Requirements Traceability in Agile Development". In: *Procedia Computer Science* 150, S. 628–635. ISSN: 18770509. DOI: 10.1016/j.procs.2019.02.044.

Naeem M., Ashraf R., Ali N., Ahmad M., Habib M. A. (2017). "Bottom up Approach for Better Requirements Elicitation". In: *Proceedings of the International Conference on Future Networks and Distributed Systems.* ICFNDS '17. Cambridge, United Kingdom: Association for Computing Machinery. ISBN: 9781450348447. DOI: 10.1145/3102304.3109820. URL: https://doi.org/10.1145/3102304.3109820.

Petropoulos, G. (2021). "A European Union Approach to Regulating Big Tech". In: *Commun. ACM* 64.8, S. 24–26. ISSN: 0001-0782. DOI: 10.1145/3469104. URL: https://doi.org/10.1145/3469104.

Pohl, K. (2008). *Requirements Engineering - Grundlagen, Prinzipien, Techniken (2. Aufl.).* dpunkt.Verlag. ISBN: 978-3-89864-550-8.

Pohle, J. (2020). "Digitale Souveränität". In: *Handbuch Digitalisierung in Staat und Verwaltung.* Hrsg. von Klenk, T., Nullmeier F., Wewer G. Springer Fachmedien Wiesbaden, S. 1–13. ISBN: 978-3-658-23669-4. DOI: 10.1007/978-3-658-23669-4_21-1. URL: https://doi.org/10.1007/978-3-658-23669-4_21-1.

Pohlmann, N. (2022). "Self-Sovereign Identity (SSI)". In: *Cyber-Sicherheit.* Hrsg. von Pohlmann, N. Wiesbaden: Springer Fachmedien Wiesbaden GmbH und Springer Vieweg, S. 645–671. ISBN: 978-3-658-36242-3. DOI: 10.1007/978-3-658-36243-0_18.

Pöhn, D., Grabatin M., Hommel W. (2021). "eID and Self-Sovereign Identity Usage: An Overview". In: *Electronics* 10.22, S. 2811. DOI: 10.3390/electronics10222811.

Projektpräsentation SDIKA (2021). *Projektpräsentation*. https://www.digitale-technologien.de/DT/Redaktion/DE/Downloads/sdi_SDIKA_praesentation.pdf. Abgerufen am 24.03.2023.

Ribeiro C., Farinha C., Pereira J., Mira da Silva M. (2014). "Gamifying requirement elicitation: Practical implications and outcomes in improving stakeholders collaboration". In: *Entertainment Computing* 5.4, S. 335–345. ISSN: 1875-9521. DOI: https://doi.org/10.1016/j.entcom.2014.04.002. URL: https://www.sciencedirect.com/science/article/pii/S1875952114000135.

Roßnagel, A. (2023). "Digitale Souveränität im Datenschutzrecht". In: *MMR Zeitschrift für IT-Recht und Recht der Digitalisierung* 2023, 64.

Rotthaus, T. (2022). "Mehr Akzeptanz für digitale Identitäten (Interview Alpers S, Sürmeli J, Toppazzini W.)" In: *Behörden Spiegel* März 2022, S. 44. ISSN: 1437-8337.

Sabatucci L., Ceccato M., Marchetto A., Susi A. (2015). "Ahab's legs in scenario-based requirements validation: An experiment to study communication mistakes". In: *Journal of Systems and Software* 109, S. 124–136. ISSN: 0164-1212. DOI: https://doi.org/10.1016/j.jss.2015.07.039. URL: https://www.sciencedirect.com/science/article/pii/S0164121215001648.

Schwalm S., Albrecht D., Alamillo I. (2022). *eIDAS 2.0: Challenges, perspectives and proposals to avoid contradictions between eIDAS 2.0 and SSI*. DOI: 10.18420/OID2022_05.

Scupin, R. (2008). "The KJ Method: A Technique for Analyzing Data Derived from Japanese Ethnology". In: *Human Organization* 56.2, S. 233–237. ISSN: 0018-7259. DOI: 10.17730/humo.56.2.x335923511444655. eprint: https://meridian.allenpress.com/human-organization/article-pdf/56/2/233/1726606/humo_56_2_x335923511444655.pdf. URL: https://doi.org/10.17730/humo.56.2.x335923511444655.

SDIKA (2023). *Schaufenster Sichere Digitale Identitäten Karlsruhe*. https://www.sdika.de/. Abgerufen am 14.03.2023.

Seifert, J. W. (2020). *Visualisieren, präsentieren, moderieren*. 42. Auflage. Whitebooks. Offenbach: GABAL. ISBN: 9783869362403.

Sinha A. P., Popken D. (1996). "Completeness and consistency checking of system requirements: An expert agent approach". In: *Expert Systems with Applications* 11.3, S. 263–276. ISSN: 0957-4174. DOI: https://doi.org/10.1016/S0957-4174(96)00043-7. URL: https://www.sciencedirect.com/science/article/pii/S0957417496000437.

Spencer T. (2012). "Identity in the cloud". In: *Computer Fraud & Security* 2012.7, S. 19–20. ISSN: 13613723. DOI: 10.1016/S1361-3723(12)70075-1.

Stemmer M. (2016). *Digitale Governance - Ein Diskussionspapier*. 1. Auflage. Berlin: Kompetenzzentrum Öffentliche IT, Fraunhofer-Institut für Offene kommunikationssysteme FOKUS.

Al-subaie, H. S. F., Maibaum T. S. E. (2006). "Evaluating the Effectiveness of a Goal-Oriented Requirements Engineering Method". In: *Fourth International Workshop on Comparative Evaluation in Requirements Engineering (CERE'06 - RE'06 Workshop)*, S. 8–19. DOI: 10.1109/CERE.2006.3.

Sutcliffe A., Sawyer P. (2013). "Requirements elicitation: Towards the unknown unknowns". In: *2013 21st IEEE International Requirements Engineering Conference (RE)*, S. 92–104. DOI: 10.1109/RE.2013.6636709.

van Bokkem D., Hageman R., Koning G., Nguyen L., Zarin N. (2019). *Self-Sovereign Identity Solutions: The Necessity of Blockchain Technology*. URL: https://arxiv.org/pdf/1904.12816.

Weinreuter M., Alpers S., Oberweis A. (2023). "Method for Eliciting Requirements in the area of Digital Sovereignty (MERDigS)". In: *ICICT: 8th International Congress on Information and Communication Technology*.

Weinreuter, M. (2022). "Methode zur Entwicklung von Anforderungen im Bereich der digitalen Souveränität". Abschlussarbeit - Bachelor. Karlsruher Institut für Technologie (KIT). DOI: 10.5445/IR/1000151128.

Zou, X., Chen B., Jin B. (2012). "Cloud-Based Identity Attribute Service with Privacy Protection in Cyberspace". In: *Procedia Engineering* 29, S. 1160–1164. ISSN: 18777058. DOI: 10.1016/j.proeng.2012.01.105.

Zowghi D., Gervasi V. (2003). "On the interplay between consistency, completeness, and correctness in requirements evolution". In: *Information and Software Technology* 45.14. Eighth International Workshop on Requirements Engineering: Foundation for Software Quality, S. 993–1009. ISSN: 0950-5849. DOI: https://doi.org/10.1016/S0950-5849(03)00100-9. URL: https://www.sciencedirect.com/science/article/pii/S0950584903001009.

Erklärung

Ich versichere wahrheitsgemäß, die Arbeit selbstständig verfasst, alle benutzten Hilfsmittel vollständig und genau angegeben und alles kenntlich gemacht zu haben, was aus Arbeiten anderer unverändert oder mit Abänderungen entnommen wurde sowie die Satzung des KIT zur Sicherung guter wissenschaftlicher Praxis in der jeweils gültigen Fassung beachtet zu haben.

Karlsruhe, 31. Juli 2023 Manuel Brazel