Bundesamt
für Migration
und Flüchtlinge

Fraunhofer
FIT

uni.lu | SnT

Digitalisierung der Bescheinigungsprozesse im Asylverfahren mittels digitaler Identitäten

Eine Machbarkeitsstudie des Bundesamtes für Migration und Flüchtlinge

Informationstechnologie

FLORA
Föderale Blockchain-Infrastruktur Asyl
Zusammenarbeit | Kommunikation | Flexibilität | Sicherheit

Digitalisierung der Bescheinigungsprozesse im Asylverfahren mittels digitaler Identitäten

Eine Machbarkeitsstudie des Bundesamtes für Migration und Flüchtlinge

Whitepaper der Projektgruppe Wirtschaftsinformatik des Fraunhofer-Instituts für Angewandte Informationstechnik FIT, des Interdisciplinary Centre for Security, Reliability and Trust der Universität Luxemburg sowie von Mitarbeitenden des Bundesamtes für Migration und Flüchtlinge

Bundesamt für Migration und Flüchtlinge 2021

Kurzfassung

Im Rahmen des Asylverfahrens werden sequenziell verschiedene Bescheinigungen in papierbasierten Prozessen an Asylsuchende und Antragstellende ausgestellt. Zur Erörterung der Verbesserungspotenziale in den aktuellen Verfahren durch den Einsatz innovativer Technologien wurde eine Machbarkeitsstudie durchgeführt. In diesem Rahmen entstand ein Prototyp, der die Blockchain-Technologie und Ansätze des digitalen Identitätsmanagements nutzt, um Bescheinigungsprozesse für Asylsuchende digital abzubilden.

Die aktuellen Prozessabläufe umfassen verschiedene Bescheinigungen, die Asylsuchenden im Laufe des Asylprozesses jeweils auf Papier ausgestellt werden. Dazu zählen die Anlaufbescheinigung, der Ankunftsnachweis, die Aufenthaltsgestattung sowie die Verlassenserlaubnis. Im aktuellen Verfahren zur Ausstellung und Überprüfung der Bescheinigungen bestehen jedoch Ineffizienzen und Sicherheitsrisiken. Insbesondere die Prüfung der Echtheit und Gültigkeit der Papierbescheinigungen stellt eine große Herausforderung dar. Digitales Identitätsmanagement, mittels dessen Bescheinigungen digitalisiert und im Kontext einer Identität manipulationsresistent und effizient genutzt werden können, erscheint als ein möglicher Lösungsansatz. In diesem Rahmen spielt auch die Blockchain-Infrastruktur FLORA als neutrale und organisationsübergreifende Infrastruktur zur Überprüfung der Gültigkeit sowie zur Abbildung von Rechten im Umgang mit einer digitalen Bescheinigung eine Rolle.

Daher wurde durch das Bundesamt für Migration und Flüchtlinge (BAMF) ein Prototyp entwickelt, der es Mitarbeitenden verschiedener am Asylprozess beteiligter Behörden erlaubt, relevante Bescheinigungen an Asylsuchende digital auszustellen, diese auf ihre Gültigkeit zu überprüfen sowie deren Gültigkeitsstatus zu bearbeiten. Asylsuchende können die digitalen Bescheinigungen in einer Smartphone-Anwendung und/ oder in einem Papierausdruck als Nachweis mit sich führen. Der Prototyp nutzt eine Instanz einer Hyperledger-Fabric-Blockchain, die es erlaubt, die ausstellende Behörde einer spezifischen Bescheinigung sowie deren aktuelle Gültigkeit zu überprüfen. Die Bescheinigungen werden als QR-Code, der ein standardisiertes Bescheinigungsdokument repräsentiert, an die Asylsuchenden übermittelt.

Die Lösung bietet auf fachlicher Ebene vielversprechende Mehrwerte. So könnte der Aufwand seitens der involvierten Behörden deutlich reduziert und eine zuverlässige Prüfung der Integrität der Bescheinigungen ermöglicht werden. Die Lösung nutzt die Vorteile einer dezentralen Infrastruktur, die eine isolierte Datenhaltung zur Überprüfung von Bescheinigungen obsolet werden lässt. Zudem greift der Prototyp bereits auf Elemente neuartiger Konzepte zum Identitätsmanagement zurück. Diese werden bisher allerdings nicht in den üblichen Abläufen genutzt, weshalb eine Interoperabilität mit bestehenden Lösungen nach neuen Ansätzen zum digitalen Identitätsmanagement noch nicht gegeben ist. Aufgrund der Neuartigkeit des Lösungsansatzes gibt es derzeit außerdem noch rechtliche Hürden. Beispielsweise müssen einige Bescheinigungen gemäß der aktuellen Rechtslage physisch erstellt werden.

Das Bundesamt möchte sich nun mit dem gewonnenen Wissen zielgerichtet mit anderen Behörden und Organisationen austauschen und Weiterentwicklungspotenziale hin zu interoperablen Ansätzen des digitalen Identitätsmanagements prüfen. Dazu ist das BAMF bereits in der Vorbereitung entsprechender Rahmenbedingungen und Testumgebungen. Das nachfolgende Begleitdokument und der entwickelte Prototyp sind Teil einer Machbarkeitsstudie, die einen ersten Schritt in Richtung vollständig digitaler und interoperabler Bescheinigungsprozesse und Identitäten für Asylsuchende darstellt.

Inhalt

Abbildungsverzeichnis

1. Motivation

Im Rahmen des Asylverfahrens werden aktuell verschiedene Bescheinigungen in papierbasierten Prozessen an Asylsuchende und Antragstellende ausgegeben. Teile des Prozesses sind dabei nicht fälschungssicher. Zudem sind die Prozesse mit hohem Aufwand verbunden. Um Lösungen für diese Herausforderungen zu finden, führte das Bundesamt für Migration und Flüchtlinge (BAMF) nun eine Machbarkeitsstudie durch. Dabei wurden insbesondere die Potenziale von Blockchain-basierten Anwendungen zur digitalen Abbildung von Bescheinigungen im Asylprozess analysiert. In diesem Rahmen wurde ein Prototyp für einen technischen Lösungsansatz entwickelt.

Bescheinigungen für Asylsuchende bzw. Antragstellende weisen zum Beispiel den Aufenthalt (per Ankunftsnachweis, AKN und Aufenthaltsgestattung, AG), den Weg zur genannten Aufnahmeeinrichtung (Anlaufbescheinigung) oder eine Genehmigung zum vorübergehenden Verlassen einer räumlichen Beschränkung (Verlassenserlaubnis, VE) nach. Diese Bescheinigungen müssen bei Bedarf verlängert oder geändert werden. Teilweise erlöschen mit dem Fortschreiten des Asylprozesses die Gültigkeiten der Bescheinigungen und Folgebescheinigungen werden ausgestellt.

Aktuell findet die Bearbeitung der Bescheinigungen im Asylprozess papierbasiert statt, wodurch drei wesentliche Herausforderungen entstehen. (1) Zunächst gestaltet es sich bisweilen schwierig, die Gültigkeit von Bescheinigungen nachzuvollziehen und deren Rückruf zeitnah durchzuführen. Diese Herausforderung impliziert wiederum einen erhöhten Aufwand seitens der Behördenmitarbeitenden. (2) Eine weitere Herausforderung ist die teilweise eingeschränkte Fälschungssicherheit, die besonders bei den Anlaufbescheinigungen und Verlassenserlaubnissen besteht. Diese werden nicht auf Hochsicherheitspapier erstellt und lassen somit Raum für Fälschung und Manipulation. (3) Ferner besteht ein hoher administrativer Aufwand für die Verwaltung einiger Bescheinigungen aufgrund deren Erstellung auf Sicherheitspapier. Dieses erfordert einen entsprechenden Umgang, sichere Lagerung und Vernichtung sowie umfangreiche Dokumentationen.

Diese Herausforderungen können insbesondere durch den Einsatz innovativer digitaler Technologien adressiert werden. Besonders vielversprechend erscheint dabei ein Ansatz, welcher Bescheinigung gemäß einem neuen Standard des World Wide Web Consortiums (W3C) digital abbildet und die Blockchain-Technologie als Basis eines gemeinsamen und behördenübergreifenden Gültigkeitsregisters einsetzt.

Das BAMF hat diesen Ansatz aufgegriffen und im Rahmen der beschriebenen Machbarkeitsstudie für den dargestellten Anwendungsbereich erprobt. Die Studie wurde unter Betrachtung der folgenden Fragestellungen durchgeführt: Welche Digitalisierungspotentiale bestehen im aktuellen Bescheinigungsprozess? Wie könnte eine Lösung zur Umsetzung digitaler Bescheinigungen technisch ausgestaltet sein? Dabei wurde sichergestellt, dass neben einer digitalen Abbildung der Bescheinigungen auch eine analoge Option bestehen bleibt. Weiterhin galt es, das mögliche Zusammenspiel zwischen des sich gerade in der Pilotierungsphase befindlichen Blockchain-basierten Assistenzsystems für das Asylverfahren und einer neuen Lösung für digitale Bescheinigungen und digitales Identitätsmanagement zu untersuchen. Details zum Blockchain-basierten Assistenzsystem für das Asylverfahren können bei Fridgen et al. (2019) nachgelesen werden. Darüber hinaus werden die potenziellen Rahmenbedingungen auf Basis bestehender Rechtsvorschriften identifiziert.

Das vorliegende Begleitdokument zum Prototyp legt zunächst den aktuellen, papierbasierten Prozess dar und stellt die konzeptionellen Grundlagen zum digitalen sowie dezentralen Identitätsmanagement vor. Es fokussiert sich ferner auf den Standardablauf einer üblichen Fallkonstellation als Beispiel. Aufbauend auf

diesen Grundlagen wird das Lösungskonzept auf Basis Blockchain-basierter digitaler Bescheinigungen dargelegt und anschließend evaluiert. Das Dokument schließt mit einem zusammenfassenden Fazit.

2. Grundlagen

2.1. Der aktuelle Bescheinigungsprozess

Der Bescheinigungsprozess zu Beginn eines Asylverfahrens beinhaltet in einer typischen Fallkonstellation drei wesentliche Bescheinigungen, die sequenziell ausgestellt werden und einander der Reihe nach ablösen. Der aktuelle Prozess beinhaltet folglich mehrere sequenzielle Prozessschritte, die jeweils unterschiedliche Arten von Bescheinigungen für die Asylsuchenden bzw. Antragstellenden mit sich bringen. Der aktuelle Prozess ist grafisch veranschaulicht der Abbildung 1 zu entnehmen.

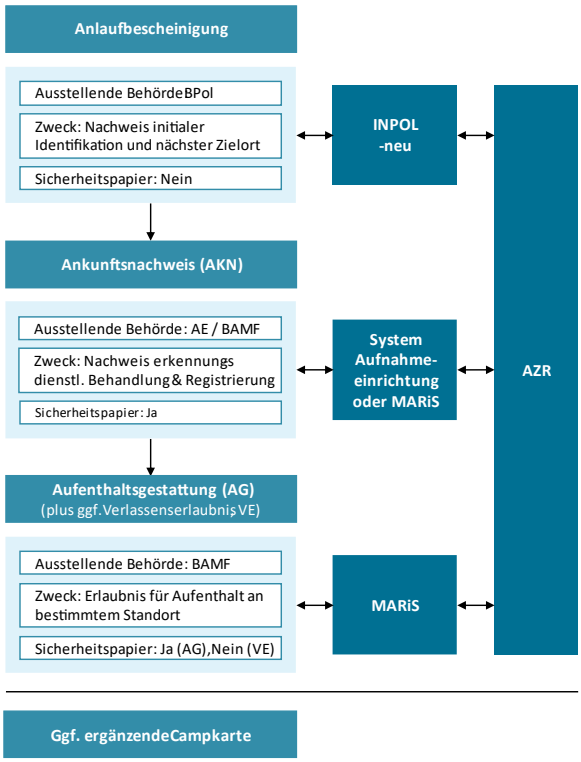

Abbildung 1: Aktueller, papierbasierter Bescheinigungsprozess im Asylprozess

2.1.1. Die Anlaufbescheinigung

Die Anlaufbescheinigung verweist im Falle der Asylgesuchstellung auf die zuständige bzw. die nächstgelegene Aufnahmeeinrichtung (AE), bei der sich eine asylsuchende Person zu melden hat. Hierfür wird die asylsuchende Person zunächst durch die Bundespolizei (BPol) registriert und erkennungsdienstlich behandelt. Über das IT-System der BPol erfolgt dabei auch eine erste Meldung an das Ausländerzentralregister (AZR). Die Anlaufbescheinigung bescheinigt somit eine initiale Identifizierung sowie Identifikationsmerkmale und einen festgelegten Zielort für Asylsuchende. Sie ist nicht auf Sicherheitspapier gedruckt. Sollte kein Asylgesuch gestellt werden und eine Zurückweisung nicht möglich sein, so verweist die Anlaufbescheinigung auf die nächste örtliche Ausländerbehörde (ABH).

Die Anlaufbescheinigung kann durch die BPol ausgestellt werden, wenn diese z.B. nach § 18 Asylgesetz (AsylG) als Grenzbehörde agiert. Darüber hinaus kann die Anlaufbescheinigung im Rahmen der Aufgaben nach § 19 AsylG auch von einer ABH oder der Landespolizei ausgestellt werden. Für die folgende Prozessbeschreibung wird von einer Ausstellung durch die BPol ausgegangen.

2.1.2. Der Ankunftsnachweis

Der Ankunftsnachweis (AKN) bescheinigt die Meldung als asylsuchende Person vor der förmlichen Stellung eines Asylantrags. Der AKN wird von der zuständigen Aufnahmeeinrichtung oder einer zugeordneten Außenstelle des BAMF auf Sicherheitspaper ausgestellt (§ 63a AsylG). Bei Ausstellung des AKN wird die Anlaufbescheinigung eingezogen. Der AKN weist eine erkennungsdienstliche Behandlung und eine formelle Registrierung einer asylsuchenden Person nach. Über das jeweilige System der ausstellenden Behörden erfolgt auch hier eine Meldung der relevanten Daten an das AZR. Die AZR-Nummer des Asylsuchenden wird auf dem AKN abgedruckt.

2.1.3. Die Aufenthaltsgestattung

Die Aufenthaltsgestattung (AG) gewährt Antragstellenden das Recht, sich für die Durchführung eines Asylverfahrens in Deutschland aufzuhalten und unter bestimmten Bedingungen zu arbeiten. Die AG wird vom BAMF bei förmlicher Asylantragsstellung ausgehändigt und ersetzt den AKN. Sie dient als Erlaubnis für den Aufenthalt an einem festgelegten Standort und ist auf Sicherheitspapier gedruckt. Bei der Ausstellung werden wiederum Daten im zentralen System des BAMF (MARiS) gespeichert und an das AZR gemeldet.

2.1.4. Die Verlassenserlaubnis

Sollte es notwendig sein, dass Antragstellende, noch während sie verpflichtet sind, in einer AE zu wohnen, den Geltungsbereich der AG aus bestimmten Gründen verlassen, kann das BAMF eine sog. Verlassenserlaubnis (VE) ausstellen (§ 57 AsylG). Eine VE wird bspw. häufig im Zusammenhang mit der Ermöglichung von Terminen bei Bevollmächtigten oder Flüchtlingsorganisationen erteilt. Die VE gilt parallel zur AG und ersetzt teilweise die hierin festgelegten Regelungen. Sie wird mit Ausnahme von Gerichts- und Behördenterminen beim BAMF beantragt. Eine Meldung an das AZR erfolgt nicht.

2.1.5. Die Campkarte

Um Personen im Asylverfahren Zugang zu ihrer zugewiesenen Unterkunft (Camp) und bestimmten Leistungen (z. B. Verpflegung, Hygieneartikel und Kleidung) zu gewähren, stellen die Betreiber – behördlich oder privat – häufig sog. Campkarten aus. Diese Campkarten existieren parallel sowie unabhängig zu anderen Bescheinigungen und folgen keinem bestimmten Muster, d. h. sie können inhaltlich beliebig ausgestaltet werden. Das vorliegende Whitepaper fokussiert sich zunächst auf den behördlichen Bescheinigungsprozess. Daher wird in den nachfolgenden Prozessbeschreibungen von der Ausstellung durch eine zuständige Behörde ausgegangen.

Zusammenfassend bleibt festzuhalten, dass die zu Beginn eines Asylverfahrens ausgestellten Bescheinigungen unterschiedliche Formate sowie Sicherheitsniveaus aufweisen und durch unterschiedliche Behörden ausgestellt werden. Hieraus ergeben sich Herausforderungen hinsichtlich der Überprüfung der Integrität und Gültigkeit der Bescheinigungen. Infolgedessen entsteht ein hoher administrativer Aufwand.

2.2. Digitale Identitäten

Mit der zunehmenden Verlagerung analoger Prozesse in den digitalen Raum gewinnen auch die digitale Abbildung sowie das Management von Identitätsdokumenten zunehmend an Bedeutung. Identitäten setzen sich allgemein aus Teil-Identitäten zusammen, die kontextabhängig sind. Teil-Identitäten bestehen aus verschiedenen Attributen, welche die Identitätsinhabenden beschreiben (Clauß und Köhntopp 2001).

2.2.1. Die Entwicklung digitaler Identitäten

Über die vergangenen Jahrzehnte haben sich unterschiedliche Ansätze zur Abbildung digitaler Identitäten entwickelt, die individuelle Eigenschaften mit sich bringen (Allen 2016). Dabei sind heute vor allem zwei wesentliche Paradigmen hervorzuheben, die jedoch jeweils Schwachstellen aufzeigen. Um zu verstehen, warum neuartige Ansätze notwendig sind und in dieser Machbarkeitsstudie betrachtet werden, werden nachfolgend die Entwicklungsstufen dargelegt.

Zum einen gibt es Ansätze, bei denen die Nutzenden selbst für die Verwaltung von Zugängen zu ihren jeweiligen identitätsbezogenen Daten verantwortlich sind. Für jeden Dienst besteht ein eigener Account, in dem gewisse Identitätsdaten hinterlegt sind. So entsteht ein erhöhter Aufwand für die Nutzenden, da die jeweiligen Identitätsdaten nur schwer zwischen den Diensten transferiert werden können. In der Folge ist die Nutzerfreundlichkeit niedrig. Zudem können z. B. durch die

häufige Verwendung ähnlicher Passwörter Sicherheitsrisiken entstehen. Zur Verwaltung dieser Daten, zum Beispiel von Zugängen zu Diensten, wird häufig auf lokale Anwendungen zurückgegriffen. Ein Beispiel dafür sind sog. Passwort-Manager. Diese ermöglichen es, die Zugangsdaten zu verschiedenen Diensten und digitalen Identitäten mit einem einzigen Passwort bzw. Authentifizierungsschritt zu nutzen.

Des Weiteren gibt es föderierte Identitäten, die es ermöglichen, in einem Interaktionsschritt Identitäten zwischen verschiedenen Diensten zu transferieren, wobei die entsprechenden Daten immer über einen zentralen Log-In-Dienst weitergeben werden. Nachteilig ist dabei, dass durch die Zentralisierung eine hohe Abhängigkeit und Transparenz gegenüber dem zentralen Log-In-Dienst entsteht. Ebenfalls geht damit ein hohes Missbrauchsrisiko einher.

Als dritter Ansatz, der zunehmend an Bedeutung gewinnt, ist das Konzept der selbst-souveränen Identität (SSI) zu nennen. Dabei treten Nutzende als die zentralen Verwaltenden ihrer Identitäten auf und besitzen dadurch die volle Kontrolle sowie Autonomie in der Verwaltung dieser Identitäten. Bescheinigungen über Identitätsattribute werden mit kryptographischen Mitteln digital und fälschungssicher durch die ausstellenden Organisationen signiert und von den Nutzenden aufbewahrt. Durch standardisierte Schnittstellen und Datenmodelle lassen sich die Identitätsattribute der Nutzenden in verschiedenen Kontexten einsetzen. Eine anschauliche Analogie ist durch einen Geldbeutel gegeben. In diesem werden Ausweise, die durch vertrauenswürdige Institutionen bescheinigte und fälschungssicher dokumentierte Attribute ihrer Inhabenden enthalten, gesammelt. Diese Ausweise können in bilateralen Interaktionen hervorgezeigt und geprüft werden.

Unter Berücksichtigung dieser Ansätze und vor dem Hintergrund der Vielzahl an zu verwaltenden Bescheinigungen, die Asylsuchenden bzw. Antragstellenden während ihres Asylprozesses ausgestellt werden, ist ein moderner technischer Ansatz notwendig. Dabei sollen sowohl die technischen Entwicklungen hinsichtlich digitaler Identitäten als auch fachliche Anforderungen berücksichtigt werden. Die Grundbausteine von modernen digitalen Identitäten werden nachfolgend dargelegt.

2.2.2. Die Grundbausteine digitaler Identitäten

Technisch bauen einige wesentliche Grundbausteine eines modernen und nutzerfreundlichen Identitätsmanagements auf Elementen aus dem SSI-Konzept auf, die nachfolgend knapp erläutert werden. Dabei ist wichtig zu beachten, dass diese auch unabhängig von SSI genutzt werden können.

Verifiable Credentials (VCs): VCs sind digitale Dokumente, die Eigenschaften ihrer Inhabenden enthalten und durch eine ausstellende Institution digital signiert wurden. Ihre Gültigkeit kann durch die ausstellende Institution mittels öffentlicher kryptographischer Register entzogen werden. Die Gültigkeit kann dritten Parteien durch die Inhabenden direkt bewiesen werden, ohne dass eine Interaktion der dritten Partei mit der ausstellenden Institution erforderlich ist. Ihr Format wird in einem Standard des W3C definiert (W3C 2020). Konzeptionell lassen sich VCs also mit analogen Identitätsdokumenten vergleichen, die durch vertrauenswürdige Stellen ausgestellt und fälschungssicher gestaltet werden (z. B. Personalausweis).

Digital Wallets: Digital Wallets sind Softwareprogramme, die Interaktionen im Kontext einer Nutzeridentität ermöglichen. Sie dienen dem Signieren von Nachrichten, der Authentifizierung von Identitätsinhabenden und der Verwaltung von VCs. Zudem werden kryptographische Schlüssel, welche digitale Signaturen für Interaktionen einer Identität ermöglichen, in Digital Wallets gespeichert. Ein Beispiel hierfür wäre eine Smartphone-Anwendung, deren ausschließliche Funktion die domänenunabhängige Authentifizierung und Erstellung digitaler Signaturen ist.

Rollen: Im Kontext von SSI und verwandten Ansätzen digitaler Identitäten sind drei Rollen von zentraler Bedeutung (Mühle et al. 2018): (1) *Holder* als Besitzende der Bescheinigungen über Identitätsattribute. Im Falle des Asylprozesses sind das die Asylsuchen-

den bzw. Antragstellenden. In manchen Fällen kann das Subjekt der Bescheinigungen jedoch vom Holder abweichen, z. B. falls Asylsuchende bzw. Antragstellende Bescheinigungen für ihre Kinder verwalten. Zur Vereinfachung wird in der Machbarkeitsstudie von Holdern ausgegangen, die gleichzeitig das Subjekt der Bescheinigungen sind. (2) *Issuer* als vertrauenswürdige Aussteller der Bescheinigungen. Im Falle des Asylprozesses könnten diese Rolle das BAMF, die BPol, die AE oder die ABH einnehmen. (3) *Verifier* als Prüfende der Bescheinigungen. Im Falle des Asylprozesses sind dies etwa die Mitarbeitenden der am Asylprozess beteiligten Behörden, die mit den Asylsuchenden in Kontakt treten.

2.2.3. Die Rolle der Blockchain-Technologie für digitale Identitäten

Die Blockchain-Technologie bietet einige wesentliche Vorteile zur Umsetzung effizienter digitaler Identitäten. Diese lassen sich vor allem auf die Eigenschaften der Blockchain als transparentes Register mit rückwirkend nur schwer und nicht unbemerkt veränderbaren Einträgen zurückführen. Konkret kann ein Blockchain-System genutzt werden, um Informationen von öffentlichen Institutionen abzuspeichern. Dies kann zum Beispiel den aktuell durch die entsprechende Institution verwendeten kryptografischen Signaturschlüssel umfassen. Außerdem können so Standards über die Inhalte von VCs eines bestimmten Typs (zum Beispiel AKN) definiert und veröffentlicht werden, was die Verifizierung der Authentizität vereinfacht. Zudem können Gültigkeitsregister für VCs, die öffentlich verifizierbar sein müssen, auf entsprechenden Infrastrukturen abgespeichert und bereitgestellt werden.

Die Wahl der optimalen Blockchain-Ausgestaltung für eine Identitätsanwendung ist jedoch abhängig vom konkreten Anwendungsfall und den Anforderungen an die digitalen Identitäten selbst. Zunächst ist dabei entscheidend, wie weitreichend das angedachte Ökosystem zur Nutzung der digitalen Identitäten ist. Sind die beteiligten Parteien bekannt und in ihrer Anzahl begrenzt (zum Beispiel für behördenübergreifende Anwendungen), eignen sich Ausgestaltungen, die exakt auf die Bedürfnisse der beteiligten Parteien anpassbar sind. Ist jedoch Interoperabilität mit verschiedenen Anwendungen und Parteien, die nicht vorhersehbar sind, gewünscht, sollten standardisierte und auf digitales Identitätsmanagement optimierte sowie öffentlich einsehbare Blockchain-Ausgestaltungen genutzt werden. Dies ist beispielsweise im Kontext einer zusätzlichen außerbehördlichen Nutzung von Bescheinigungen der Asylsuchenden bzw. Antragstellenden denkbar.

Für das erste Szenario eignen sich insbesondere Blockchain-Systeme, für die sich mittels Smart Contracts Logiken zur Interaktion mit den entsprechenden digitalen Identitäten definieren lassen. Smart Contracts sind Computerprogramme, die dezentral auf den Knoten eines Blockchain-Netzwerkes ausgeführt werden; beispielsweise um Transaktionen nach festgelegten Regeln automatisch auszuführen. Um Effizienz und Kontrolle über die Ausgestaltung des entsprechenden Ökosystems zu gewährleisten, eignen sich private Blockchain-Netzwerke. Ein Beispiel für ein entsprechendes Blockchain-Framework ist *Hyperledger Fabric* (Hyperledger 2020a). Um Risiken hinsichtlich der Privatsphäre zu minimieren, muss gegebenenfalls mit Instrumenten wie Zero-Knowledge-Proofs (ZKPs) gearbeitet werden, wodurch erhöhte Komplexität entstehen kann, wenn diese nicht bereits inhärent vorhanden sind (Zhang et al. 2019).

Falls eine Anwendung entsprechend des zweiten, oben beschriebenen Szenarios mit gewünschter Interoperabilität konstruiert werden soll, so sollte eine Kompatibilität mit führenden Standards des Identitätsmanagements mit der Blockchain-Technologie sichergestellt werden. Das Framework rund um *Hyperledger Indy* (Hyperledger 2020b) stellt entsprechende Komponenten bereit, die auch auf den zuvor bereits referenzierten *W3C*-Standards aufbauen und beispielsweise ZKPs ermöglichen. Allerdings ist zu beachten, dass dieses Framework nur eine enge Auswahl von Funktionalitäten zur Verfügung stellt, die stark auf das SSI-Konzept ausgelegt sind und etwa keine Speicherung von VCs auf der Blockchain oder Verwaltung von Gültigkeitsregistern von VCs eines Typs durch mehrere Institutionen vorsieht. Einmal ausgestellte Nachweisdokumente in Form von VCs sind unter der Kontrolle und Verwaltung ihrer Besitzenden und somit auch auf deren techni-

scher Infrastruktur, zum Beispiel Smartphones, gespeichert. Diese VCs können nachträglich lediglich noch als ungültig markiert, d.h. widerrufen, werden. Dieses Privileg ist zudem den ausstellenden Parteien der jeweiligen VCs vorbehalten und lässt sich für Dritte nur durch technische Umgehungslösungen umsetzen. Dies könnte beispielsweise bedeuten, dass eine dazu berechtigte Partei bilateral mit dem Aussteller kommuniziert und diesem gegenüber den Widerruf fordert.

3. Lösungskonzept

3.1. Architektur des Prototyps

Um den spezifischen Anforderungen an digitale Identitätsbescheinigungen im Kontext des Asylprozesses zu entsprechen und dabei innovative sowie zukunftsfähige technische Elemente zu nutzen, hat das BAMF eine umfassende prototypische Lösung entwickelt. Diese berücksichtigt bereits im Aufbau befindliche technische Infrastrukturen wie FLORA sowie fachliche Anforderungen und technische Elemente aus dem Kontext von SSI.

Die Architektur des Prototyps setzt sich dabei aus drei Ebenen zusammen und ist schematisch in Abbildung 2 dargestellt.

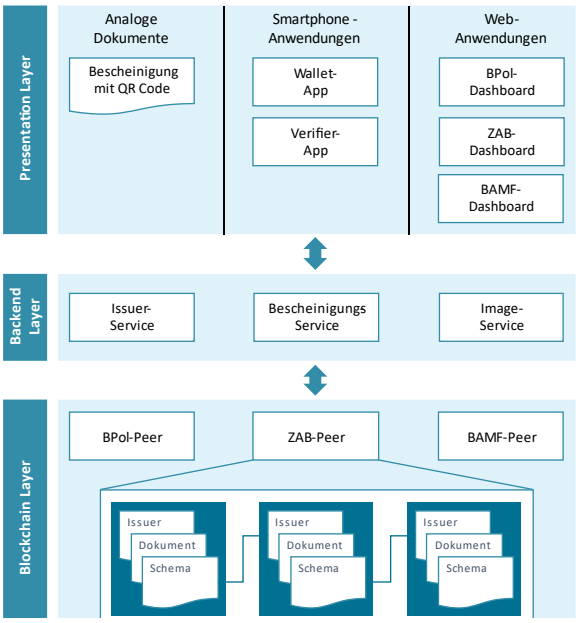

Abbildung 2: Architektur des Prototyps

3.1.1. Presentation Layer

Der *Presentation Layer* enthält Komponenten zur Interaktion natürlicher Personen im Asylprozess mit den digitalen Identitäten bzw. digitalen Identitätsdokumenten der Asylsuchenden bzw. Antragstellenden. Diese Ebene umfasst zwei Smartphone-Anwendungen. Eine Anwendung erlaubt es Asylsuchenden bzw. Antragstellenden, die ihnen ausgestellten Bescheinigungen zu speichern und diese bei Bedarf zu präsentieren (*Wallet-App*). Die zweite Anwendung (*Verifier-App*) erlaubt die Überprüfung der Bescheinigungen. Die mobilen Anwendungen sind multi-plattform-kompatibel (Android und iOS) und basieren technisch auf dem Ionic-Framework.

In der *Wallet-App* werden Bescheinigungen in Form von VCs als JSON-Dateien abgespeichert. Ein QR-Code zum Abruf der JSON-Datei wird bei jeder Anfrage erneut generiert. Grundlegende Daten (inkl. Foto) können im Klartext vorgezeigt sowie der aktuelle und vorangegangene QR-Code abgerufen werden. Die VCs können darüber hinaus auch gelöscht werden. Da nicht allen Asylsuchenden bzw. Antragstellenden ein Smartphone zur Verfügung steht, wird hierzu auch eine analoge, d. h. papierbasierte, Alternative angeboten. Die QR-Codes werden bei dieser analogen Alternative auf Papier gedruckt, bieten jedoch dieselben digitalen Möglichkeiten zur Überprüfung mittels der Behörden-Dashboards wie die digitale Alternative. Die *Verifier-App* ermöglicht die Gültigkeitsprüfung der VCs über den Scan der angezeigten QR-Codes mit den potenziellen Status „gültig“, „abgelaufen“ und „ungültig“. Dazu wird die /api/bescheinigung/verify Schnittstelle zu dem Backend verwendet und die Informationen als JSON übergeben - entweder als encodierte oder decodierte Version. Das Backend überprüft dann, die Gültigkeit der Bescheinigungen. Des Weiteren können die in einem überprüften VC enthaltenen Informationen angezeigt werden.

Zusätzlich zu den Smartphone-Anwendungen wurden auf dieser Ebene drei Web-Anwendungen konzipiert, die es Mitarbeitenden berechtigter Behörden erlauben, die Korrektheit

der jeweils präsentierten Informationen der Bescheinigung zu überprüfen oder neue Bescheinigungen zu erstellen und auszugeben. Die Webanwendungen sind browserbasiert und damit auf verschiedenen Betriebssystemen nutzbar. Für das BAMF, die zentrale Ausländerbehörde (ZAB)[1] und die BPol existiert jeweils ein Dashboard: Das *BPol-Dashboard* unterstützt das Erstellen sowie Widerrufen der Anlaufbescheinigungen; das *ZAB-Dashboard* wird für das Erstellen und Widerrufen eines AKN genutzt und das *BAMF-Dashboard* wird für das Erstellen der Aufenthaltsgestattung sowie das Widerrufen von Bescheinigungen genutzt. Zudem soll das BAMF-Dashboard eine Möglichkeit bieten, eine VE zu erfassen. Zu diesem Zweck sind Interaktionen mit der Blockchain notwendig, wozu eine Zwischenschicht, das Backend Layer, eingeführt wurde.

3.1.2. Backend Layer

Der *Backend Layer* umfasst wesentliche Dienste, die für die zwei Hauptaktivitäten im Zusammenhang mit digitalen Bescheinigungen asylsuchender bzw. Antragstellender Personen genutzt werden. Zum einen ist dies die Ausstellung digitaler Bescheinigungen wie zum Beispiel der AKN, und zum anderen die Verifikation der Authentizität von Bescheinigungen. Diese Services sind technisch dreigeteilt: (1) *Issuer-Service* zum Anlegen neuer Organisationen im System, die Bescheinigungen ausstellen können; (2) *Bescheinigungs-Service* zum Anlegen, Verifizieren und Widerrufen neuer Bescheinigungen in Form von VCs sowie (3) *Image-Service* zum Hochladen und Abrufen von Fotos, die zu den Identitäten der Asylsuchenden bzw. Antragstellenden gehören. Die Web-Anwendungen wurden in Java geschrieben und die Schnittstellen sind als REST APIs konzipiert.

3.1.3. Blockchain Layer

Auf der *Blockchain Layer* findet der Betrieb einer Blockchain für Aktivitäten im Kontext der digitalen Identitäten statt. Dies umfasst einerseits die Speicherung von Informationen über ausgestellte Bescheinigungen, andererseits aber auch Berechtigungen für deren Widerruf. Dazu werden drei Peers, also Netzknoten in einem Peer-to-Peer-Netzwerk, betrieben. Diese repräsentieren jeweils eine der Organisationen BPol, ZAB und BAMF. Auf diesen Peers ist der aktuelle Stand der Blockchain gespeichert. Die Peers senden Transaktionen, beispielsweise zur Ausstellung neuer Bescheinigungen im Asylprozess, an das übrige Netzwerk und nehmen außerdem aktiv an dem Konsensmechanismus des Netzwerks teil. So kann dezentral über den korrekten Status des Systems entschieden werden. Im vorliegenden Prototyp wurde eine Instanz von *Hyperledger Fabric* verwendet, die auf den Konsensmechanismus RAFT zurückgreift und neben den drei Peers einen Ordering Service verwendet. Dieser Ordering Service ordnet Transaktionen innerhalb des Netzwerks final zu und pflegt Listen von Netzwerkteilnehmern sowie deren Rechte. Details können bei Hyperledger (2020) nachgelesen werden. Ein weiterer Grund für die Wahl dieses Blockchain-Systems liegt in der Integrierbarkeit mit der bestehende Pilot-Lösung für das Assistenzsystem im Asylverfahren für die Verwaltung von Asylprozessen mittels Blockchain. Diese baut ebenfalls auf Hyperledger Fabric auf, wodurch eine gemeinsame Nutzung der bereits bestehenden Infrastruktur ermöglicht wird.

Die auf der Blockchain zu speichernden Informationen hängen grundsätzlich vom Dokumententyp ab. Dabei wird zwischen drei Arten von Dokumenten unterschieden, die im Prototyp auf der Blockchain gespeichert werden: Es gibt Dokumente vom Typ (1) *Issuer*, welche Informationen über ausstellende Organisationen enthalten, (2) *Document*, die eine ausgestellte Bescheinigung beschreiben und (3) *Schema*, welche ein Schema für eine Bescheinigung abbilden. Bei allen wird das Erstellungs- und Änderungsdatum sowie eine

[1] Je nach landesgesetzlicher Regelung können verschiedene Behörden die Rolle einer AE wahrnehmen. In Sachsen ist dies die ZAB.

zufällige und einzigartige ID gespeichert. Zusätzlich können weitere Informationen wie die ausstellende Behörde oder – im Falle der Issuer-Dokumente – auch öffentliche Schlüssel zur Signatur von ausgestellten VCs gespeichert werden.

3.2. Prozessabläufe

Der Prototyp bildet drei Anwendungsfälle im Kontext digitaler Bescheinigungen von Asylsuchenden bzw. Antragstellenden ab: die Ausstellung, die Einziehung einer abgelaufenen und die Kontrolle von Bescheinigungen. Die Datenflüsse und Abläufe entlang der zuvor bereits präsentierten Systemarchitektur werden nachfolgend jeweils ausführlich beschrieben.

Allgemein sind drei wesentliche Rollen an den jeweiligen Prozessen beteiligt, die auf ein behördenübergreifend genutztes Blockchain-System zugreifen. Zum einen gibt es die Asylsuchenden bzw. Antragstellenden als zentrale Entitäten und Bescheinigungsinhabende (Holder). Zum anderen gibt es die ausstellenden Institutionen von Bescheinigungen wie das BAMF, die BPol, die AE und die ABH (Issuer). Diese können darüber hinaus auch als prüfende Institutionen von Bescheinigungen hinsichtlich der Integrität und Gültigkeit auftreten (Verifier). Die Blockchain dient als gemeinsam genutzte Infrastruktur, wobei lediglich die ausstellenden sowie prüfenden Behörden direkt mit dieser interagieren. Die jeweiligen Akteure und ihre Hauptaktivitäten sind in Abbildung 3 schematisch dargestellt.

3.2.1. Ausstellung einer Bescheinigung

Sobald eine Bescheinigung für Asylsuchende bzw. Antragstellende im Rahmen bestimmter Prozessschritte im Asylprozess ausgestellt werden soll, werden zunächst ggf. Stammdaten und Fingerabdrücke aufgenommen (1). Die Behörde gibt diese Daten schließlich in einer standardisierten Web-Anwendung (*Dashboard* der jeweiligen Behörde) ein (2) und verifiziert dann formal das Datenschema mittels einer Abfrage auf dem Blockchain-System (3), wo dieses unter dem Dokumententyp *Schema* abgespeichert ist. Zur Kommunikation mit der Blockchain werden standardisierte

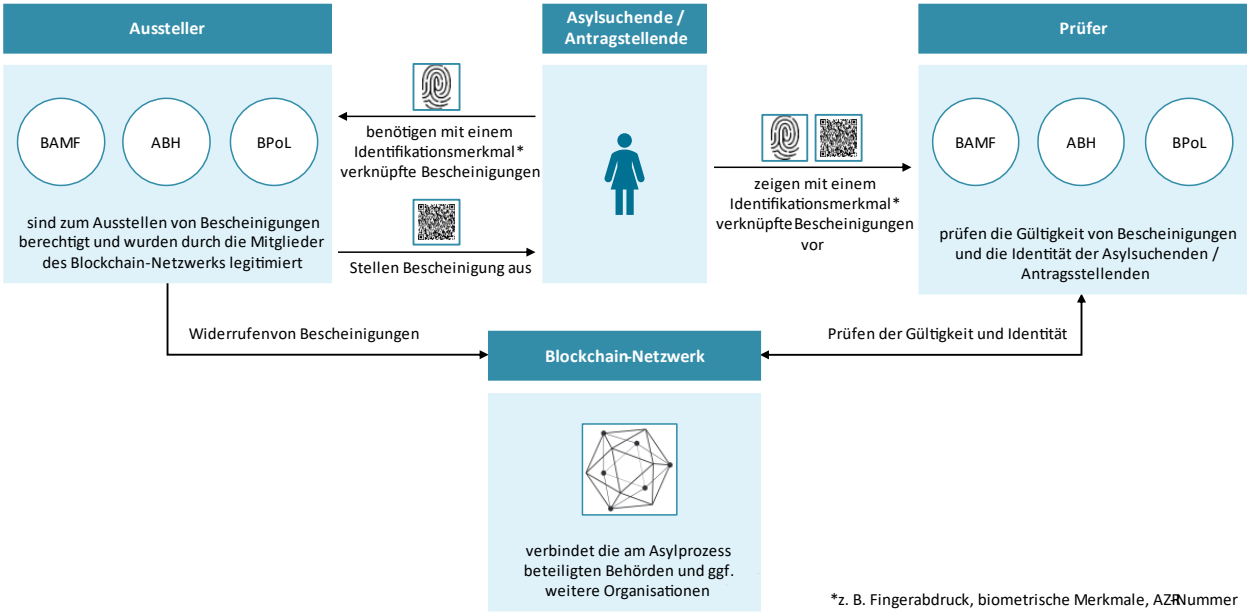

Abbildung 3: Akteure und Aktivitäten in der Blockchain-Lösung für digitale Bescheinigungen im Asylprozess

Schnittstellen über das Backend (*Issuer Service*) verwendet. Bei Bedarf werden die entsprechenden Schemata durch die zuständigen Behörden auf dem Blockchain-System aktualisiert. Schließlich wird die jeweilige Bescheinigung nach dem Datenschema erstellt und

durch die jeweilige Behörde digital signiert (4). Die Bescheinigungen sind als VCs nach dem W3C-Standard gestaltet und werden zunächst als JSON-Dateien erstellt. Diese JSON-Dateien werden anschließend an die entsprechenden Asylsuchenden bzw. Antragstellenden ausgegeben, indem sie an ihre *Wallet-App* gesendet und dort gespeichert werden. Die Dateien werden alternativ komprimiert und als QR-Code abgebildet auf Papier gedruckt, welches dann als Bescheinigung an die Asylsuchenden ausgegeben wird (5). Der Grund für diese analoge Option besteht darin, dass nicht allen asylsuchenden bzw. antragstellende Personen ein den Anforderungen entsprechendes mobiles Endgerät zur Verfügung steht oder sie dieses nutzen möchten.

3.2.2. Widerruf der Gültigkeit einer Bescheinigung

Unter gegebenen Umständen, beispielsweise wenn prozessual eine Folgebescheinigung ausgestellt werden soll, müssen Bescheinigungen als ungültig markiert und damit widerrufen werden. Dazu müssen zunächst die Asylsuchenden bzw. Antragstellenden ihre Bescheinigung digital in ihrer App oder auf dem Papier mittels eines QR-Codes einer berechtigten Behörde vorzeigen, sodass diese im Blockchain-System gefunden werden kann (1). Die Daten werden durch die Behörde in einer Web-Anwendung (*Dashboard* der jeweiligen Behörde) folglich mit dem Scannen des QR-Codes eingegeben (2) und durch die Blockchain im Hinblick auf Gültigkeit und Korrektheit des Schemas sowie der Inhalte mittels definierter Schnittstellen (*Verifier Service*) verifiziert (3). Hierbei wird die in dem VC enthaltene Signatur überprüft, indem der öffentliche Signaturschlüssel über das referenzierte *Issuer*-Profil auf der Blockchain abgefragt wird. Der Widerruf findet ebenfalls auf der Blockchain statt, indem entweder Behördenmitarbeitende direkt über ihre Web-Anwendung einen Widerruf setzen oder indem automatisiert ein Widerruf hervorgerufen wird, sobald eine neue Bescheinigung für eine asylsuchende bzw. antragstellende Person ausgestellt wird (5). Der Widerruf einer Bescheinigung in Form eines VC wird in der Machbarkeitsstudie abgebildet, indem ein Parameter des den VC beschreibenden *Document* auf der Blockchain auf „false“ gesetzt wird. Dabei können die Behörden entweder eine Bescheinigung widerrufen, die sie selbst ausstellen, oder aber auch eine im Prozess vorangegangene Bescheinigung, z. B. kann die BPol lediglich die Anlaufbescheinigung widerrufen, wohingegen die ZAB die Anlaufbescheinigung sowie den AKN widerrufen kann.

3.2.3. Kontrolle einer Bescheinigung

In unterschiedlichen Situationen kann eine Überprüfung der Gültigkeit sowie inhaltlichen und objektbezogenen Integrität der digitalen bzw. analogen Bescheinigungen erforderlich sein. In diesem Fall zeigen die Asylsuchenden bzw. Antragstellenden entweder in der App oder auf ihrem Papierdokument den QR-Code vor, der die transformierte Version des VCs referenziert (1). Zusätzlich wird ein Identifikationsmerkmal, welches der Fingerabdruck, ein biometrisches Merkmal oder eine AZR-Nummer sein kann, von der prüfenden Behörde festgestellt. Anschließend wird die digitale Signatur durch den *Verifier Service* mittels einer Abfrage der Blockchain verifiziert (2). Hierbei wird die Signatur des VCs, welche beim Anlegen der Bescheinigung erstellt und deren Inhalt durch den privaten Schlüssel der ausstellenden Behörde verschlüsselt wurde, mittels des öffentlichen Schlüssels der ausstellenden Behörde entschlüsselt und der Inhalt mit dem VC abgeglichen. In diesem Zug wird auch der Widerruf und somit die Gültigkeit durch das Datenfeld „revoked“ (deutsch: „widerrufen“) des Dokumentes auf der Blockchain geprüft (3). Das Verifizierungsergebnis wird nachfolgend in einem Web-Dashboard mittels eines Service im Backend (*Verifier Service*) direkt an die prüfende Behörde zurückgegeben (4), sodass durch diese die physische Identitätsprüfung erfolgen kann (5).

4. Einordnung & initiale Evaluation

4.1. Fachliche Einschätzung

Die Entwicklung des Machbarkeitsstudie diente primär der Überprüfung möglicher fachlicher Vorteile durch die Einführung einer digitalen und Blockchain-basierten Abbildung der Bescheinigungsprozesse im Asylverfahren. Die erwarteten fachlichen Mehrwerte sind dabei wie folgt definiert worden:

(1) Erleichterte Prüfung von Gültigkeit und Integrität der Bescheinigungen

(2) Höhere Fälschungssicherheit

(3) Reduzierter Administrationsaufwand

4.1.1. Erleichterte Prüfung von Gültigkeit und Integrität der Bescheinigungen

Besondere Vorteile sind hinsichtlich der Unterstützung von Behördenmitarbeitenden durch eine erleichterte Prüfung von Gültigkeit und Integrität der verschiedenen Bescheinigungen festzustellen. Während im zuvor angewendeten Prozess die Integrität von Papierbescheinigungen überprüft werden musste, findet nun eine Prüfung durch technische Infrastruktur statt. Dabei werden sowohl die Struktur als auch die Gültigkeit der Bescheinigung und die Signatur der ausstellenden Behörde überprüft. Die entsprechende Prüfung findet über auf dem Blockchain-System gespeicherte Daten statt. Für die prüfenden Behördenmitarbeitenden umfasst die Überprüfung nur einen einzelnen Interaktionsschritt, der mit dem Scan des QR-Codes auf der Papierbescheinigung oder der Smartphone-App abgeschlossen ist.

4.1.2. Höhere Fälschungssicherheit

Eine erhöhte Sicherheit der Bescheinigungen soll vor allem durch die Verwendung digitaler Signaturen und ein Blockchain-System als geteilte Infrastruktur erreicht werden. Die QR-Codes, die in den Bescheinigungen abgebildet sind, zeigen auf ein digitales Dokument, das auf dem Blockchain-System gespeichert ist. Dieses enthält den Signaturschlüssel der ausstellenden Behörde. Digitale Signaturen ermöglichen so eine erhöhte Sicherheit hinsichtlich der Verifizierung der ausstellenden Behörden einer Bescheinigung. Die notwendigen Daten zur Überprüfung liegen zudem nicht auf einem einzelnen System, sondern sind dezentral auf der Blockchain-Infrastruktur gespeichert. So kann durch die zwischen Behörden geteilte Infrastruktur auch eine Manipulation oder rückwirkende Veränderung der Daten nachvollzogen werden. Hierbei würden nicht nur der AKN und die AG von einer höhten Fälschungssicherheit profitieren, sondern es könnten auch erste wegweisende Fortschritte hin zur Fälschungssicherheit der VE und der Anlaufbescheinigung erzielt werden. Eine mögliche Sicherheitslücke besteht jedoch auf der physischen Ebene, da die Identitäten der Asylsuchenden bzw. Antragstellenden und somit der Nachweis, dass sie tatsächlich Besitzer der Bescheinigungen sind, nach wie vor durch physische Überprüfung der Identifikationsmerkmale geschehen muss.

4.1.3. Reduzierter Administrationsaufwand

Die Lösung könnte den Administrationsaufwand seitens der Behörden durch den Wegfall des Sicherheitspapiermanagements für AKN und AG reduzieren. Während die initiale Aufnahme und Verifikation der Identitäten von Asylsuchenden bzw. Antragstellenden nach wie vor manuell vonstattengeht, ist die Ausstellung und Speicherung der entsprechenden Bescheinigungen weitgehend digitalisiert und kann sofort nach den initialen Prüfprozessen durchgeführt werden. Insbesondere entfällt die aufwändige Verwaltung von Sicherheitspapier. Solange die Asylsuchenden bzw. Antragstellenden eine Bescheinigung vorzeigen können, sind durch den Zugriff auf die geteilte Infrastruktur zur Verifikation von Inhalten der Bescheinigungen behördenübergreifende Nachforschungspro-

zesse über die Urheberschaft einer Bescheinigung bei Zweifeln oder Unregelmäßigkeiten weitgehend zu vernachlässigen. Durch digitale Signaturen kann die ausstellende Behörde einer Bescheinigung festgestellt werden, indem ihre Signaturschlüssel auf der Blockchain überprüft werden. Allerdings muss die Überprüfung, ob die jeweiligen Asylsuchenden bzw. Antragstellenden tatsächlich die Besitzenden der entsprechenden Bescheinigungen sind, weiterhin manuell durchgeführt werden.

Fazit: Die Lösung bietet große Vorteile bei der Prüfung der Gültigkeit und Integrität von Bescheinigungen. Ebenfalls ist eine insgesamt höhere Fälschungssicherheit zu erwarten. Möglich ist auch ein reduzierter Administrationsaufwand.

4.2. Juristische Einschätzung

Der nachfolgende Abschnitt dient einer initialen juristischen Bewertung des vorgestellten Prototyps. Die wesentlichen rechtlichen Herausforderungen für die Digitalisierung des Bescheinigungsprozesses liegen in der aktuell geltenden Schriftformerfordernis für den AKN und die AG sowie in bestimmten Vorgaben für die inhaltliche Ausgestaltung der Bescheinigung. Ferner könnten zusätzliche Anforderungen an die Bescheinigungen bestehen, insofern sie als Verwaltungsakt und somit mit unmittelbarer Rechtswirkung nach außen zu sehen sind.

4.2.1. Form der Bescheinigungen

Nach derzeitiger Rechtslage dürfte ein Ersetzen der Schriftform durch eine elektronische Form i.S.v. § 3a Abs. 2 S. 1 Verwaltungsverfahrensgesetz (VwVfG) für den AKN und die AG zweifelhaft sein. Laut gesetzlichen Vorgaben ist das jeweilige Dokumentenmuster aktuell körperlich zu erstellen. Das Asylgesetz (AsylG) spricht dabei jeweils von den einer asylsuchenden Person zu erteilenden "Bescheinigungen" und lässt durch die vergleichbaren Begrifflichkeiten auch nicht erkennen, dass diese unterschiedlich auszulegen wären.

Für den AKN findet ferner die Ankunftsnachweisverordnung (AKNV) Anwendung, in welcher nach §5 eine ausschließliche elektronische Version nicht zulässig ist. Eine Koexistenz von elektronischer und körperlicher Version ist weder in der AKNV noch im AsylG vorgesehen. Darüber hinaus wird nach § 78a Abs. 5 Aufenthaltsgesetz (AufenthG) ein einheitliches Vordruckmuster für Bescheinigungen gefordert.

Für Anlaufbescheinigung, VE und Campkarte existieren nach gegenwärtigem Stand keine entsprechenden Formvorschriften. Daher dürfte für diese Bescheinigungen ein Ersetzen der Schriftform durch eine elektronische Form zumindest in diesem Punkt als unkritisch erachtet werden.

4.2.2. Inhalt der Bescheinigungen

Gesetzliche Vorgaben bestehen nicht nur bezüglich der Form der Bescheinigung, sondern auch bezüglich deren Inhalt. Für einige Bescheinigungen gelten sehr genaue Regelungen bezüglich des Inhalts (z.B. AKN), wohingegen für andere Bescheinigungen kaum bis keine Vorgaben existieren (z.B. Anlaufbescheinigung).

Dies gilt insbesondere für den AKN, dessen Inhalt in § 63a AsylG geregelt wird. § 63a AsylG regelt nicht nur die Angaben, die der AKN enthalten muss, sondern schreibt auch vor, dass diese „sichtbar“ aufgebracht sein müssen. Es wird also nicht unterschieden, wer das Dokument in Augenschein nimmt. Außerdem schreibt § 63a Abs. 1 AsylG vor, welche Daten in einem automatisch erzeugten, maschinenlesbaren QR-Code enthalten sein müssen.

Die AG wird in § 63 AsylG geregelt. § 63 AsylG schreibt für die AG lediglich vor, dass diese das Datum der Ausstellung des AKN und der Antragsstellung sowie die AZR-Nummer enthält. Darüber hinaus beinhaltet § 63 AsylG keine genaueren Regelungen des Inhaltes, allerdings soll an dieser Stelle auf die Verweisung in § 63 Abs. 5 AsylG auf weitere inhaltliche Regelungen im AufenthG und der AufenthV hingewiesen werden

Für die Anlaufbescheinigung bestehen bisher keine vergleichbaren Regelungen und die rechtliche Lage gestaltet sich diffus. Ein Hinweis kann dem Aufsatz von J. Rosenstein in ZAR 2017, 73, "Die Entwicklung und die praktische Bedeutung der Bescheinigung über die Meldung als Asylsuchender (BüMA und Ankunftsnachweis) im Verlauf der letzten Jahre und heute", unter dem Abschnitt 4.1 „Die BüMA als Anlaufbescheinigung“ entnommen werden. Darin heißt es, dass es für diese Bescheinigung kein amtliches Muster gäbe und jede Behörde das Dokument nach eigenen Mustern ausstellen könne. Ferner hätten lediglich einige Bundesländer (wie Niedersachsen) in der Vergangenheit entsprechende Muster geschaffen. Gegenwärtig seien damit keine Mindestinhalte für die BüMA bzw. Anlaufbescheinigung festgelegt. Nichtsdestotrotz könne den Behörden empfohlen werden, die BüMA bzw. Anlaufbescheinigung mit einem Foto zu versehen, um Missbrauch vorzubeugen. Von der Verordnungsermächtigung des § 88 AsylG sei zu dieser Bescheinigung kein Gebrauch gemacht worden.

Mangels recherchierbarer Regelungen bezüglich der VE und der Campkarte sind zwingend einzuhaltende Inhalte nicht ersichtlich. Gleichwohl muss sich nach Sinn und Zweck der jeweiligen Bescheinigungen gerichtet werden und ggf. Regularien der Betreiber berücksichtigt werden.

Letztlich lässt sich festhalten, dass eine digitale Abbildung der Bescheinigungen unter Berücksichtigung der bestehenden Inhaltsvorgaben möglich sein dürfte.

4.2.3. Bescheinigungen als Verwaltungsakt

Ein weiterer zu betrachtender Aspekt ist die Frage, ob Bescheinigungen als Verwaltungsakt zu bewerten sind. Hierzu existieren vielfältige, teils widersprüchliche Positionen.

§ 35 Verwaltungsverfahrensgesetz (VwVfG) bezeichnet einen Verwaltungsakt als „Verfügung, Entscheidung oder andere hoheitliche Maßnahme, die eine Behörde zur Regelung eines Einzelfalls auf dem Gebiet des öffentlichen Rechts trifft und die auf unmittelbare Rechtswirkung nach außen gerichtet ist“. Diese unmittelbare Rechtswirkung könnte erhöhte Anforderungen an die Bescheinigungen und deren Digitalisierung stellen.

Ob Anlaufbescheinigung, AKN und AG jedoch als Verwaltungsakt zu bewerten sind, ist in der Literatur und Rechtsprechung umstritten. So geht etwa das Verwaltungsgericht (VG) Trier (Urteil vom 05.03.2020, 10 K 5062/19.TR) davon aus, dass es sich bei der Weiterleitungsverfügung nach § 22 Abs. 1 Satz 2, 1. Halbsatz, 2. Alt. AsylG um einen Verwaltungsakt handelt. Dieser Verwaltungsakt sei in der "Wichtigen Mitteilung" der Aufsichts- und Dienstleistungsdirektion des Landes Rheinland-Pfalz (ADD) - EAE Trier - zu sehen. Zwar finde sich die Bezeichnung der zuständigen Aufnahmeeinrichtung auch in der ausgehändigten BüMA (heute ersetzt durch den AKN), allerdings handele es sich laut VG Trier (so auch VG Gelsenkirchen, Beschluss vom 20.11.2013 - 11 L 1505/13) dabei lediglich um die Mitteilung der Verteilungsentscheidung des Bundesamtes, nicht um die originäre Entscheidung der ADD Rheinland-Pfalz, durch welche die Weiterleitungsanordnung getroffen werde.

Anderer Ansicht ist dazu das Verwaltungsgericht Berlin in seinem Urteil vom 04.07.2014, VG 10 K 289.13, das den Verwaltungsakt in der BüMA (also dem AKN) sieht. Diese unterschiedlichen Ansichten dürften sich auf alle hier zu betrachtenden Bescheinigungen übertragen lassen, zumal Kommentierungen zum AsylG mit Verweis auf die Rechtsprechung des Bundesverwaltungsgerichts (BVerwG) ebenfalls einen entsprechenden Meinungsstreit erkennen lassen.

Unabhängig von der Klärung oder Nicht-Klärung dieser Frage ist allerdings die Notwendigkeit zur Anwendung des § 37 Abs. 3 VwVfg beim schriftlichen oder elektronischen Verwaltungsakt. Darin ist festgeschrieben, dass die ausstellende Behörde und die Unterschrift oder der Name des Behördenleiters, seines Vertreters oder seines Beauftragten enthalten sein muss. Letzteres wird in elektronischer

Form durch eine qualifizierte Signatur ersetzt. Ferner sollte ein Zugangsnachweis berücksichtigt werden, da im § 41 Abs. 2 VwVfG festgelegt ist, dass die Behörde den Zugang eines Verwaltungsaktes und den Zeitpunkt des Zugangs im Zweifel nachzuweisen hat.

Hinsichtlich der VE kann davon ausgegangen werden, dass es sich um einen Verwaltungsakt i. S. v. § 35 VwVfG handelt. Das Gesetz sieht in § 57 AsylG grundsätzlich eine Ermessensentscheidung vor (Ausnahmen sind bestimmte Termine z. B. bei Behörden und Gerichten). Laut Kommentierung Funke-Kaiser; Fritz; Vormeier – Gemeinschaftskommentar zum Asylgesetz zu § 57 AsylG RN 54 ist im Falle des Nichterteilens einer VE die Verpflichtungsklage statthaft. Gemäß § 42 Abs. 1 Alt. 2 VwGO kann mit der Verpflichtungsklage die Verurteilung zum Erlass eines abgelehnten oder unterlassenen Verwaltungsaktes begehrt werden. Auch wenn sich die bisher geprüften Kommentierungen (auch Marx; Kommentar zum Asylgesetz zu § 57 AsylG) über die Rechtsnatur der VE nicht äußerten, kann davon ausgegangen werden, dass die Verwaltungsaktqualität unstreitig vorliegen dürfte.

Zwecks der Campkarte wäre diese Frage nur zu diskutieren, falls es sich um einen hoheitlichen Betreiber handelt. Hier wäre dann anhand des jeweiligen Inhaltes zu prüfen, inwiefern ein Einzelfall regelnder Charakter mit unmittelbarer rechtlicher Außenwirkung vorliegen könnte, was nur dann für einen Verwaltungsakt sprechen könnte. Sofern es sich um einen privaten Betreiber handelt, sollte sich die Frage nach dem Verwaltungsakt nicht stellen.

Ebenso unabhängig von den bisher zutage getretenen unterschiedlichen Ansichten zur Einordnung der Bescheinigungen als Verwaltungsakt – und eventuell damit verbundener Form- und Bekanntgabevorschriften – sollten sich die Beteiligten zukünftig auf eine gemeinsame Verfahrensweise einigen (z. B. auf das Zugrundelegen der Verwaltungsaktqualität) und eine entsprechende klarstellende Regelung einfordern. Bezüglich des Inhalts sind keine Konsequenzen zu erwarten.

Fazit: Während eine digitale Abbildung von Anlaufbescheinigung, VE und Campkarte unproblematisch scheint, so bedarf es für die Digitalisierung des AKN sowie der AG gesetzlicher Änderungen.

4.3. Technologische Einschätzung

Die durch die Machbarkeitsstudie abgebildete Lösung soll nicht nur fachlich, sondern auch auf technologischer Ebene Mehrwerte generieren und den Umgang mit neuen Technologien erproben. Der für den Prototyp gewählte Ansatz ist ein hybrider Ansatz aus Elementen des SSI-Umfelds und der bereits im Aufbau befindlichen Blockchain-Lösung des BAMF. Nachfolgend werden für den hier untersuchten Anwendungsfall besonders relevante technische Aspekte diskutiert.

4.3.1. Erhöhte Datenverfügbarkeit und -integrität

Um eine durchgängige Bereitstellung der Dienstleistungen im Kontext digitaler Bescheinigungen von Personen im Asylverfahren zu gewährleisten, müssen notwendige Daten zur Überprüfung von Bescheinigungen und Interaktionen durchgängig verfügbar sein. Diese Daten dürfen zudem nur durch berechtigte Parteien verändert werden und Änderungen müssen nachvollziehbar sein.

Durch die Verwendung eines Blockchain-Netzwerks, dessen Knoten über mehrere Behörden verteilt sind, kann eine hohe Datenverfügbarkeit gewährleistet werden. Die Blockchain speichert dabei für die Überprüfung der Integrität und Gültigkeit von Bescheinigungen relevante Daten. Die Verwendung digitaler Signaturen für die Bescheinigungen, die sich über diese Infrastruktur überprüfen lassen, ermöglicht zudem eine hohe Datenintegrität im Vergleich zu ausschließlich auf Papier ausgestellten Bescheinigungen und in zentralen Systemen gespeicherten Daten zur Überprüfung der Signaturen. Berechtigungen zur Änderung der Daten sind zudem in der Blockchain dokumentiert und verwaltet. Durch die nachvollziehbare Datenhistorie in Blockchains lassen sich Veränderungen zudem nachvollziehen.

4.3.2. Verwendung von Elementen aus dem Kontext von SSI

SSI gilt aufgrund der ermöglichten Interoperabilität und Sicherheit als ein vielversprechendes Konzept für digitales Identitätsmanagement. Um diese Mehrwerte zu nutzen und generelle Digitalisierungspotenziale zu verstehen, wird nachfolgend eine Kompatibilität mit dem Prototyp evaluiert. Dabei müssen jedoch stets fachliche Anforderungen berücksichtigt werden.

Typische, bisher verfügbare SSI-Konzepte weisen einige Herausforderungen auf, die eine Verwendung vor dem Hintergrund der konkreten Anforderungen des Use Cases in Frage stellen. Aus diesem Grund wurde für den Prototyp kein reiner SSI-Ansatz verfolgt. So sind analoge Teilprozesse in klassischen SSI-Systemen schwierig einzubinden. Ein reiner SSI-Ansatz baut vollständig auf digitalen Dokumenten bzw. Bescheinigungen in Form von VCs auf. Zudem ist in aktuellen technischen Rahmenwerken für SSI ein Widerruf der Gültigkeit von Bescheinigungen (z. B. VCs) zunächst nur für die ausstellenden Organisationen möglich. In der Folge könnte beispielsweise das BAMF keine durch die BPol ausgestellten VCs widerrufen, was zu erheblichen Prozessineffizienzen führen könnte.

Um eine gute Vereinbarkeit des Prototyps mit analogen Teilprozessen zu gewährleisten, ermöglicht der Prototyp eine analoge Abbildung digitaler Bescheinigungen durch den QR-Code als Papierausdruck. Zudem ist der Gültigkeitswiderruf für verschiedene Organisationen über die ausstellende Organisation einer Bescheinigung hinaus möglich. Die entsprechenden Berechtigungen werden über die Blockchain gewährt und auch auf dieser für die beteiligten Behörden transparent abgebildet.

4.3.3. Eingeschränkte Interoperabilität

Mit dem Prototyp können ausschließlich Bescheinigungen im Behördenkontext verwaltet werden. Damit die Bescheinigungsinhabenden ihre Bescheinigungen auch in außerbehördlichen Kontexten nutzen können, muss eine Überprüfung der Integrität und Gültigkeit auch für Dritte möglich sein. Dazu bietet es sich an, standardisierte Komponenten und Interoperabilität mit bestehenden Systemen zu gewährleisten. Auch die Privatsphäre der Asylsuchenden bzw. Antragstellenden muss dabei gewährleistet werden.

Der größte Nachteil der Prototyp-Lösung ist die Tatsache, dass aktuell keine Interoperabilität mit anderen SSI-Systemen und Komponenten, wie Digital Wallets, gewährleistet ist. Im Vergleich zu einem klassischen SSI-Ansatz wird beim vorliegenden Prototyp die Informationen in den Bescheinigungen nicht, wie im SSI-Kontext üblich, direkt bilateral mittels Beweise, die aus VCs erstellt werden, nachgewiesen. Sofern die im Asylprozess ausgestellten Bescheinigungen auch in anderen Kontexten verwendet und überprüft werden sollen, zum Beispiel durch Mitarbeitende in Verkehrsbetrieben, so sollte eine Standardisierung ermöglicht werden. Dritte Parteien, die Bescheinigungen überprüfen, können derzeit nicht auf das private Blockchain-System zugreifen. Dies ist nötig, um Probleme hinsichtlich des Datenschutzes zu vermeiden. Durch Verwendung eines SSI-Ansatzes mit minimaler Menge auf der Blockchain gespeicherter Daten könnte eine direkte Prüfung der Integrität und Gültigkeit jedoch auch für Dritte ermöglicht werden.

Fazit: Die für den Prototyp gewählte hybride Lösung stellt einen initialen Denkansatz dar, der die spezifischen fachlichen Anforderungen der Ausstellung von Bescheinigungen im Asylprozess berücksichtigt und zugleich zur Sammlung von Erfahrungen mit neuen Technologien beiträgt. Die Lösung ist aktuell ohne standardisierte Elemente ein auf bestimmte Behörden limitierter Ansatz, hebt aber dabei wichtige Digitalisierungs- und Innovationspotentiale hervor, deren Weiterentwicklung vielversprechend erscheint.

5. Zusammenfassung & Ausblick

Im Rahmen dieser Machbarkeitsstudie wurde eine digitale Lösung zur Abbildung von Bescheinigungen im Asylprozess vorgestellt und initial evaluiert. Die betrachtete Lösung nutzt eine Blockchain und Elemente des SSI-Konzeptes, um Bescheinigungen für Asylsuchende bzw. Antragstellende digital abzubilden. Mittels verschiedener webbasierter und Smartphone-Anwendungen können das Ausstellen und Ändern von Nachweisen über Bescheinigungen von Asylsuchenden bzw. Antragstellenden und deren Kontrolle durch unterschiedliche Behörden umgesetzt werden.

Der vorgestellte Lösungsansatz des BAMF weist zahlreiche Stärken auf. Dennoch bleiben auch einige Klärungspunkte offen. Nach derzeitiger Rechtslage ist ein Ersetzen der Schriftform durch eine elektronische Form für den AKN und die AG nicht möglich, denn aktuell ist das Bescheinigungsdokument physisch zu erstellen. Ebenfalls ist eine Koexistenz von physischen und elektronischen Bescheinigungen zumindest beim AKN nicht zulässig. Dies ist jedoch kein spezifisches Problem der umgesetzten Lösung, sondern ein grundlegendes Hindernis für die Digitalisierung der Bescheinigungen im Asylprozess. Hier bestehen entsprechende rechtliche Anpassungsbedarfe. Darüber hinaus muss noch geklärt werden, inwieweit es erforderlich ist, dass die digitalen Bescheinigungen nicht kopierbar sind.

Es lässt sich zudem festhalten, dass die Lösung den drei erwarteten fachlichen Zielsetzungen gerecht wird. Die Behördenmitarbeitenden werden bei der Prüfung der Gültigkeit und Integrität der verschiedenen Bescheinigungen unterstützt und die Lösung trägt zu einer höheren Fälschungssicherheit im Bescheinigungsprozess bei. Ebenfalls kann der Administrationsaufwand reduziert werden. Lediglich die physische Identifizierung von Asylsuchenden bzw. Antragstellenden muss (analog zum aktuellen Verfahren) systemextern bzw. durch Nutzung von anderen Systemen (z. B. Fast-ID) ablaufen.

Neben der Erreichung der fachlichen Ziele konnte gezeigt werden, dass der Prototyp die grundsätzliche technische Machbarkeit eines innovativen, zukunftsfähigen und digitalen Ansatzes erfüllt. Dieser nutzt die Vorteile einer dezentralen Infrastruktur, die eine unabhängige Datenhaltung zur Überprüfung von Bescheinigungen Asylsuchender bzw. Antragstellender obsolet macht. Die Anwendungen für Endnutzende, also Asylsuchende bzw. Antragstellende sowie Behördenmitarbeitende, sind mit mehreren gängigen Betriebssystemen nutzbar. Um Fälschungssicherheit für die digitalen Bescheinigungen herzustellen, werden kryptographische Signaturverfahren genutzt, die Industriestandards entsprechen. Vorbereitend werden zudem Elemente aus dem Kontext des neuartigen SSI-Konzepts für die Bescheinigungen genutzt.

Vor dem Hintergrund, dass im Prototyp nicht alle Elemente so genutzt werden, wie es das klassische SSI-Konzept vorsehen würde, ist derzeit noch keine Interoperabilität mit bestehenden, organisationsübergreifenden SSI-Lösungen gegeben. Standardisierte technische Komponenten aus dem SSI-Umfeld, wie zum Beispiel Wallet-Applikationen, können nicht genutzt werden. Der Grund für die Entwicklung einer Lösung, die noch nicht in allen Ebenen konform mit klassischen SSI-Konzepten ist, liegt in fachlichen und rechtlichen Anforderungen.

Die vorgestellte Lösung orientiert sich jedoch an Best Practices der Industrie und wirkt gezielt an der Weiterentwicklung der Technologie mit, in welcher vielversprechenden Anknüpfungspunkte zu den diversen Initiativen und technologische Entwicklungen berücksichtigt werden. Zu den neueren technologischen Entwicklungen zählen u. a. die Bemühungen rund um SSI, die in den vergangenen Jahren zunehmend an Relevanz gewonnen haben. Das nutzerzentrierte Konzept, welches sich vor allem die Interoperabilität und Autonomie der Anwendenden fokussiert, wird mittlerweile in verschiedenen Initiativen auf

regionaler, nationaler, sowie europäischer und internationaler Ebene untersucht und weiterentwickelt. Mit dem European Self-Sovereign Identity Framework (ESSIF) werden auf europäischer Ebene konzeptionelle und technische Rahmenbedingungen entwickelt, um das Konzept für EU-Staatszugehörige nutzbar und zugänglich zu machen. Auf deutscher Ebene ist vor allem das industriegetriebene IDunion-Konsortium hervorzuheben, das die Entwicklung eines Identitätsökosystems für Deutschland anstrebt. Organisationen wie das W3C und die Decentralized Identity Foundation sind um die Entwicklung technischer Standards für interoperable SSI-Lösungen bemüht.

Mit der vorliegenden Machbarkeitsstudie ist das BAMF einen wichtigen und erkenntnisreichen Schritt hin zu einer Digitalisierung des Bescheinigungsprozesses für asylsuchende bzw. antragstellende Personen gegangen. In zukünftigen Iterationen soll eine Einbindung und Weiterentwicklung der Lösung in bereits bestehende Initiativen im Kontext von SSI erfolgen. In diesem Rahmen soll erörtert werden, welche Schritte erforderlich sind, um standardisierte SSI-Infrastrukturen nutzen zu können und welchen Einfluss dies auf die Bescheinigungsprozesse im Asylverfahren hat. Durch die Entwicklung einer entsprechenden Lösung könnten digitale Bescheinigungen in Zukunft selbstbestimmt, sicher und interoperabel in unterschiedlichsten Kontexten nutzbar sein.

6. Literaturverzeichnis

Allen, Christopher (2016): The Path to Self-Sovereign Identity. Online verfügbar unter https://www.lifewithalacrity.com/2016/04/the-path-to-self-sovereign-identity.html, zuletzt aktualisiert am 01.07.2019.000Z, zuletzt geprüft am 28.10.2020.344Z.

Clauß, Sebastian; Köhntopp, Marit (2001): Identity management and its support of multilateral security. In: *Computer Networks* 37 (2), S. 205–219. DOI: 10.1016/S1389-1286(01)00217-1.

Ethereum (2020). Online verfügbar unter https://ethereum.org/de/, zuletzt aktualisiert am 28.10.2020.000Z, zuletzt geprüft am 28.10.2020.502Z.

Fridgen, Gilbert; Guggenmos, Florian; Lockl, Jannik; Rieger, Alexander; Urbach, Nils; Wenninger, Annette (2019): Entwicklung einer datenschutzkonformen Blockchain-Lösung im deutschen Asylprozess. Pilotierung im Kontext der AnkER-Einrichtung Dresden. Unter Mitarbeit von Projektgruppe Wirtschaftsinformatik des Fraunhofer-Instituts für Angewandte Informationstechnik FIT. Hg. v. Bundesamt für Migration und Flüchtlinge. Online verfügbar unter https://www.bamf.de/SharedDocs/Anlagen/DE/Digitalisierung/blockchain-whitepaper.htmlblob=publicationFile, zuletzt geprüft am 28.10.2020.

Hyperledger (2020a): Hyperledger Fabric – Hyperledger. Online verfügbar unter https://www.hyperledger.org/use/fabric, zuletzt aktualisiert am 29.06.2020+00:00, zuletzt geprüft am 28.10.2020.452Z.

Hyperledger (2020b): Hyperledger Indy – Hyperledger. Online verfügbar unter https://www.hyperledger.org/use/hyperledger-indy, zuletzt aktualisiert am 23.04.2020+00:00, zuletzt geprüft am 28.10.2020.047Z.

Hyperledger (Hg.) (2020c): The Ordering Service. Hyperledger-fabricdocs master documentation. Online verfügbar unter https://hyperledger-fabric.readthedocs.io/en/release-2.2/orderer/ordering_service.html, zuletzt aktualisiert am 23.10.2020.000Z, zuletzt geprüft am 28.10.2020.880Z.

Mühle, Alexander; Grüner, Andreas; Gayvoronskaya, Tatiana; Meinel, Christoph (2018): A survey on essential components of a self-sovereign identity. In: *Computer Science Review* 30, S. 80–86. DOI: 10.1016/j.cosrev.2018.10.002.

Oded Goldreich; Yair Oren (1994): Definitions and properties of zero-knowledge proof systems. In: *J. Cryptology* 7 (1), S. 1–32. DOI: 10.1007/BF00195207.

W3C (2020): Decentralized Identifiers (DIDs) v1.0. Online verfügbar unter https://www.w3.org/TR/did-core/, zuletzt aktualisiert am 27.10.2020.000Z, zuletzt geprüft am 28.10.2020.979Z.

Disclaimer

Dieses Whitepaper wurde von der Projektgruppe Wirtschaftsinformatik des Fraunhofer-Instituts für Angewandte Informationstechnik FIT, dem Interdisciplinary Centre for Security, Reliability and Trust der Universität Luxemburg und Mitarbeitenden des Bundesamtes für Migration und Flüchtlinge nach bestem Wissen und unter Einhaltung der nötigen Sorgfalt erstellt.

Fraunhofer FIT, das Interdisciplinary Centre for Security, Reliability and Trust der Universität Luxemburg, das Bundesamt für Migration und Flüchtlinge, deren gesetzlichen Vertreter und/oder Erfüllungsgehilfen übernehmen keinerlei Garantie dafür, dass die Inhalte dieses Whitepapers gesichert, vollständig für bestimmte Zwecke brauchbar oder in sonstiger Weise frei von Fehlern sind. Die Nutzung dieses Whitepapers geschieht ausschließlich auf eigene Verantwortung.

In keinem Fall haften Fraunhofer FIT, das Interdisciplinary Centre for Security, Reliability and Trust der Universität Luxemburg und das Bundesamt für Migration und Flüchtlinge, ihre gesetzlichen Vertreter und/oder Erfüllungsgehilfen für jegliche Schäden, seien sie mittelbar oder unmittelbar, die aus der Nutzung des Whitepapers resultieren.

Die Ausführungen geben allein die Sicht der beteiligten Mitarbeitenden des BAMF wider und entsprechen nicht notwendigerweise der Sicht des Bundesamtes für Migration und Flüchtlinge.

Impressum

Herausgeber:
Bundesamt für Migration und Flüchtlinge
90461 Nürnberg

Autoren:
Projektgruppe Wirtschaftsinformatik des Fraunhofer-Instituts für Angewandte Informationstechnik FIT, Interdisciplinary Centre for Security, Reliability and Trust der Universität Luxemburg und Mitarbeitende des Bundesamts für Migration und Flüchtlinge

Stand:
April 2021

Druck:
Bundesamt für Migration und Flüchtlinge
90461 Nürnberg

Gestaltung:
Projektgruppe Wirtschaftsinformatik des Fraunhofer-Instituts für Angewandte Informationstechnik FIT und das Interdisciplinary Centre for Security, Reliability and Trust der Universität Luxemburg

Bildnachweis:
Titelbild: ©iStock matejmo; Abbildung 1-3: ©Fraunhofer FIT

Empfohlene Zitierweise:
Amend, J., Federbusch, M., Fridgen, G., Köhler, F., Rieger, A., Schlatt, V., Sedlmeier, J., Stohr, A. und Van Dun, C. 2021. Digitalisierung der Bescheinigungsprozesse im Asylverfahren mittels digitaler Identitäten – Eine Machbarkeitsstudie des Bundesamts für Migration und Flüchtlinge. Projektgruppe Wirtschaftsinformatik des Fraunhofer-Instituts für Angewandte Informationstechnik FIT, Interdisciplinary Centre for Security, Reliability and Trust der Universität Luxemburg und Bundesamt für Migration und Flüchtlinge, Hrsg.: Bundesamt für Migration und Flüchtlinge (Nürnberg)

Bestellmöglichkeit:
Publikationsstelle des BAMF

www.bamf.de/publikationen

Diese Publikation wird vom Bundesamt für Migration und Flüchtlinge im Rahmen seiner Öffentlichkeitsarbeit herausgegeben. Die Publikation wird kostenlos abgegeben und ist nicht zum Verkauf bestimmt.

Besuchen Sie uns auf
www.facebook.com/bamf.socialmedia
@BAMF_Dialog
www.bamf.de/blockchain