Bayerisches Landesamt für Steuern

Fraunhofer FIT
Institutsteil Wirtschaftsinformatik, Fraunhofer-Institut für Angewandte Informationstechnik FIT

mgm

FAU Friedrich-Alexander-Universität Erlangen-Nürnberg

secunet

NESSI

Nachweisplattform ELSTER Self-Sovereign Identities

Gefördert durch

Bayerisches Staatsministerium für Digitales

Kooperationspartner

Finanzgruppe Deutscher Sparkassen- und Giroverband

BStBK BUNDES STEUERBERATER KAMMER

NESSI – NACHWEISPLATTFORM ELSTER SELF-SOVEREIGN IDENTITIES

Autoren

Bayerisches Landesamt für Steuern:

Dr. Tatiana Gossen, Roland Krebs, Dr. Daniela Kühne, Dr. Christoph Maier, Simone Zehetmeir

Institutsteil Wirtschaftsinformatik, Fraunhofer FIT:

Tobias Guggenberger, Dr. Nils Urbach, Fabiane Völter

Friedrich-Alexander-Universität Erlangen-Nürnberg:

Dr. Roland Ismer, Quirin Jackl, Dr. Klaus Meßerschmidt

mgm technology partners:

Stefan Hauffe, Dr. Hans Huber, Ansgar Knipschild, Guido Wischrop

secunet security networks AG:

Martin Fechtelhoff

Der Institutsteil Wirtschaftsinformatik des Fraunhofer FIT bündelt die Abteilungen »Digital Business« und »Information Systems Engineering«. Unsere Ambition ist es, Themen der Wirtschaftsinformatik inhaltlich wie methodisch umfassend abzudecken. Charakteristisch für unsere Arbeit ist unsere Fähigkeit, methodisches Know-how auf höchstem wissenschaftlichem Niveau mit einer kunden-, ziel- und lösungsorientierten Arbeitsweise zu verbinden.

Fraunhofer-Institut für Angewandte Informationstechnik FIT
Institutsteil Wirtschaftsinformatik
Wittelsbacherring 10
95444 Bayreuth

Das Bayerische Landesamt für Steuern (BayLfSt) ist eine Landesbehörde des Freistaats Bayern im Geschäftsbereich des Bayerischen Staatsministeriums der Finanzen und für Heimat.

Bayerisches Landesamt für Steuern
Sophienstr. 6
80333 München

Danksagungen

Die Autoren danken dem Bayerischen Staatsministerium für Digitales für die Förderung des Projekts sowie den Kooperationspartnern S–Finanzgruppe Deutscher Sparkassen- und Giroverband und der Bundessteuerberaterkammer für die wertvollen Beiträge. Zudem gilt der Dank Jens-Christian Stoetzer und Anton Bilchinski des Institutsteils Wirtschaftsinformatik des Fraunhofer FIT für die Unterstützung bei der Anfertigung des White Papers.

Empfohlene Zitierweise

Gossen, T., Guggenberger, T., Fechtelhoff, M., Hauffe, S., Huber, H., Ismer, R., Jackl, Q., Knipschild, A., Krebs, R., Kühne, D., Maier, C., Meßerschmidt, K., Urbach, N., Völter, F., Wischrop, G., Zehetmeir, S., 2022. NESSI – Nachweisplattform ELSTER Self-Sovereign Identities. Institutsteil Wirtschaftsinformatik des Fraunhofer-Instituts für Angewandte Informationstechnik FIT.

NESSI

Nachweisplattform ELSTER Self-Sovereign Identities

White Paper des Institutsteil Wirtschaftsinformatik des Fraunhofer FIT

Bayerisches Landesamt für Steuern 2022

Kurzfassung

Die fortschreitende Digitalisierung stellt die Steuerverwaltung vor die Herausforderung, mit den technologischen Entwicklungen Schritt zu halten und die sich hieraus ergebenden Chancen für eine weitere Modernisierung des Besteuerungsverfahrens zu nutzen. Vor diesem Hintergrund wurde im Rahmen der Machbarkeitsstudie SSI@LfSt im Jahr 2020 ein Konzept und ein erster Prototyp zur Self-Sovereign Identity (SSI)-basierten Bescheinigung der steuerlichen Erfassung von Marktteilnehmern im Bereich E-Commerce erstellt. Nach der erfolgreichen ersten Projektphase sollte das Potential von SSI im Rahmen des Projekts „Nachweisplattform ELSTER Self-Sovereign Identities“ (kurz: NESSI) durch eine tiefere Anbindung an ELSTER sowie die Einbeziehung von Kooperationspartnern entscheidend erweitert werden. Fokus lag auf der Entwicklung einer digitalen Lösung, um papierbasierte Bescheinigungsverfahren zu ersetzen. Dabei wurden folgende Ziele verfolgt:

- Effiziente Ausstellung und Nutzung vollständig digital abbildbarer Bescheinigungen auf Seiten der Steuerverwaltung und des Steuerpflichtigen ohne Medienbrüche
- Reduktion von Manipulationsmöglichkeiten
- Flexibles Gültigkeitsmanagement für die Steuerverwaltung

Im Rahmen des Projekts wurde ein detailliertes technisches Konzept entwickelt und ein Prototyp in der ELSTER-Umgebung gemeinsam mit der Sparkassen-Finanzgruppe implementiert. Dabei können Steuerpflichtige einen sicheren digitalen Nachweis (Verifiable Credential) über ihre Einkommensdaten mithilfe der Plattform *Mein ELSTER* beantragen. Dieser Nachweis kann dann bei der Kreditbeantragung als Bonitätsnachweis über eine Plattform der Sparkassen-Finanzgruppe vorgelegt werden. Auch wurde durch eine Projektbeteiligung der Bundessteuerberaterkammer die Bevollmächtigtenrolle der Steuerberatung bei NESSI konzeptionell untersucht.

Das Projekt zeigt, dass die Steuerverwaltung insbesondere von der Hoheit über die Gültigkeit von SSI-basierten Nachweisen profitiert, da ein Widerruf von Bescheinigungen mit sofortiger (Außen-)Wirkung nun technisch möglich wird. Da die Gültigkeitsprüfung des Nachweises durch die Sparkassen über ein abstraktes Register auf Basis der Blockchain-Technologie erfolgt, ist kein direkter Zugriff auf die Systeme der Steuerverwaltung notwendig. Hierbei wird auf die im Rahmen des Schaufensterprojekts IDunion betriebene Blockchain-Infrastruktur zurückgegriffen. Die sensiblen Daten aus den Nachweisen selbst werden nicht auf die Blockchain geschrieben, sondern durch die Steuerpflichtigen eigenständig verwaltet. Durch diese Selbstständigkeit werden prozessuale Komplexitäten seitens der Steuerverwaltung reduziert und die Souveränität der Bürgerinnen und Bürger gefördert. Auch bieten SSI-basierte Nachweise den Steuerpflichtigen potenziell einen erhöhten Nutzerkomfort, Selbstkontrolle und Privatsphäre. Zudem kann die überprüfende Partei – hier die Sparkassen-Finanzgruppe – voll digitale Workflows verwenden sowie von einer hohen Datenqualität profitieren. Bezüglich der Bevollmächtigtenrolle der Steuerberatung liefert die Delegierung von Nachweisen einen Ansatzpunkt für technische Lösungen.
Die Ergebnisse des Projekts NESSI bieten die Perspektive für einen Produktivbetrieb bei ELSTER in den nächsten Jahren, wenn sich die noch in Entwicklung befindliche SSI-Technologie weiter etabliert. Denn neben den großen Vorteilen von SSI-basierten Systemen in der Steuerverwaltung hat die Evaluation auch gezeigt, dass einige Rahmenbedingungen, insbesondere aufgrund der Neuartigkeit des Konzepts, vor einem Produktivbetrieb noch sichergestellt werden müssen. Jedoch ist auch eindeutig das Potenzial für eine strategische und tragende Rolle der Steuerverwaltung in einem SSI-Ökosystem erkennbar. Insbesondere die Ausstellung von Unternehmensidentitäten scheint hierbei prädestiniert für weitere Entwicklungsschritte.

Inhaltsverzeichnis

1. Einleitung 8
2. Zielvorstellung und Motivation 11
3. Grundlagen zu Self-Sovereign Identity 15
4. Projektbeschreibung 17
5. Rechtliche Einordnung 22
6. Mehrwertanalyse 27
7. Notwendige Schritte zum Produktivsystem 31
8. Einbindung der Steuerberatung in NESSI 39
9. Strategische Relevanz von SSI für die Steuerverwaltung 48
10. Fazit 52
11. Literaturverzeichnis 53

Abbildungsverzeichnis

Abbildung 1: Rollen in einem SSI-System 15
Abbildung 2: Gesamtprozess 19
Abbildung 3: Benutzeroberfläche zur Ausstellung von Credentials über Mein ELSTER 19
Abbildung 4: Benutzeroberfläche von dem Nachweisportal der Sparkassen-Finanzgruppe 20
Abbildung 5: Erweiterung des Trust Triangles 40
Abbildung 6: Weitergabe des Abholungsbescheids 41
Abbildung 7: Delegation durch Mandantinnen und Mandanten 42
Abbildung 8: Direkte Ausgabe an die Steuerberatung 43
Abbildung 9: Direkte Ausgabe an die Steuerberatung mit anschließender Delegation 44

1. Einleitung

1. Einleitung

Bereits im Jahr 2020 hat das Bayerische Landesamt für Steuern, gefördert durch das Bayerische Staatsministerium für Digitales, eine erste Machbarkeitsstudie zum Einsatz des SSI-Konzepts in der (Steuer-)Verwaltung durchgeführt. Das Projekt zielte darauf ab, Onlinehändlern den einfachen und sicheren Nachweis über ihre steuerliche Erfassung in elektronischer Form zu ermöglichen. Im Ergebnis wurden sowohl das große Potenzial für die Steuerverwaltung als auch weitere Herausforderungen für eine Umsetzung im Realbetrieb deutlich.

Aufbauend auf den vielversprechenden Ergebnissen der ersten Projektphase wurde im Jahr 2021 eine weitere Projektphase zur Erforschung von SSI in der (Steuer-)Verwaltung gestartet. In dieser wurde eine Plattformlösung pilotiert, die in Zukunft den Finanzbehörden gestatten soll, Bescheinigungen in Form eines SSI-Credentials ausstellen zu lassen. Die Vision des Bayerischen Landesamtes für Steuern sieht damit einen Beitrag der Steuerverwaltung zu einem anwendungsübergreifenden SSI-Ökosystem vor.

Der gewählte Projekttitel „Nachweisplattform ELSTER Self-Sovereign Identities“ (NESSI) zeigt das Bestreben, Bürgerinnen und Bürgern perspektivisch über die bereits bestehende Plattform Mein ELSTER Zugang zu Bescheinigungen in Form von Verifiable Credentials zu geben. Als Fallbeispiel wurde der Einsatz von SSI für die Nachweiserstellung über Einkommensdaten im Kontext eines Kreditantrags Selbständiger gewählt. So können Nutzerinnen und Nutzer der Plattform Mein ELSTER elektronische Nachweise über ihre Einkommensdaten zur Verfügung gestellt bekommen und diese Nachweise bei Dritten, bspw. Banken, vorlegen. Die Sparkassen-Finanzgruppe stand hier als Projektpartner für einen ersten Testbetrieb zur Verfügung. Auch die Rolle der Steuerberatung in SSI-basierten Systemen der Steuerverwaltung wurde durch eine Beteiligung der Bundessteuerberaterkammer im Projekt konzeptionell analysiert.

Die Ergebnisse dieser zweiten Projektphase stellen einen wichtigen Meilenstein in der langfristigen Vision des Freistaates Bayern und des Bayerischen Landesamts für Steuern dar. Mit der Pilotierung von NESSI wurden Grundlagen geschaffen, die Digitalisierung in der Steuerverwaltung vor dem Hintergrund entsprechender Initiativen der Bundesregierung und auf europäischer Ebene voranzutreiben. In Verbindung mit der bestehenden ELSTER-Infrastruktur könnten zukünftig alle 28 Millionen Nutzerinnen und Nutzer ihre steuerlichen Bescheinigungen einfach und sicher über eine Wallet App verwalten.

Neben der Nutzung der ELSTER-Infrastruktur zielt das Projekt darauf ab, ex ante die Interoperabilität der technischen Entwicklungen der Steuerverwaltung sicherzustellen. Deshalb wurde während der Entwicklung die bereits implementierte Blockchain-Infrastruktur des durch die Bundesregierung initiierten Schaufensterprojekts IDunion[1] verwendet. In den Schaufensterprojekten liegt ein Schwerpunkt auf Kompatibilität, die dem langfristigen Ziel dient, einen Beitrag zur Entstehung eines Ökosystems für digitale Identitäten zu leisten. Neben Identitäten für natürliche Personen werden diese auch Unternehmensidentitäten beinhalten.

Dieser Projektbericht beschreibt zunächst die Entwicklungen auf europäischer, deutscher und bayerischer Ebene, die gemeinsam ein zukünftiges Identitätsmanagement-Ökosystem fördern. Anschließend werden die Inhalte, Umsetzung und Ergebnisse des NESSI-Projekts beschrieben

[1] https://idunion.org/

und aus rechtlicher Sicht eingeordnet sowie die Mehrwerte, die strategische Relevanz, die mögliche Einbindung der Steuerberatung und bestehende Herausforderungen für einen Produktivbetrieb des Systems analysiert.

2. Zielvorstellung und Motivation

2. Zielvorstellung und Motivation

2.1. Ziele auf europäischer Ebene

Um einen einheitlichen Rechtsrahmen für die elektronische Identifizierung und Vertrauensdienste zu schaffen, wurde im Jahr 2014 die EU-Verordnung eIDAS (kurz für: ***e****lectronic* ***ID****entification,* ***A****uthentication and Trust* ***S****ervices*) eingeführt. Diese dient der EU-weiten Vereinheitlichung elektronischer Mittel zur Identifikation, die auf Ebene der Mitgliedsstaaten ausgestellt werden. Somit werden elektronische Identifikationsmittel grenzüberschreitend nutzbar gemacht. Zudem soll ein Rechtsrahmen für Vertrauensdienstleistungen geschaffen werden, zu welchem elektronische Signaturen und Siegel, Zeitstempel, elektronische Übermittlung und Website-Authentifizierungszertifikate gehören.

eIDAS
eIDAS (electronic IDentification, Authentication and trust Services) ist eine EU-Verordnung über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Europäischen Binnenmarkt.

Zur Erfolgsmessung von eIDAS wurde 2021 eine umfassende Evaluation durchgeführt, die die weitgehenden Schwächen der Verordnung und ihrer bisherigen Umsetzung identifizieren konnte.[2] Dazu gehört unter anderem die Beschränkung auf den öffentlichen Sektor. Während der Bedarf an vertrauenswürdiger und sicherer Identifikation auf privaten Märkten steigt, fokussiert sich die eIDAS-Verordnung fast ausschließlich auf die öffentliche Verwaltung. Darüber hinaus ist die Umsetzung eines nationalen Schemas für eIDs für die Mitgliedsstaaten bisher nicht verpflichtend, sodass nur rund 60% aller EU-Bürger Zugriff auf die Nutzung grenzübergreifender eIDs haben.

eID-Funktion des Personalausweises
In Deutschland ist eIDAS vor allem Anhand der elektronischen Ausweisfunktion des deutschen Personalausweises bekannt.

Auch vor dem Hintergrund neuer technologischer Entwicklungen, wie dem SSI-Konzept, das hohe Privatsphäre, Kontrolle und Nutzerfreundlichkeit verspricht, steigt der Bedarf an einer überarbeiteten Regulierung, welche die Nutzung solcher und ähnlicher Konzepte fördert. Zudem steigt neben der Relevanz von Basisidentitätsdaten (wie Name oder Geburtsdatum) die Bedeutung von Nachweisen von Merkmalen, die an eine bestimmte Identität geknüpft sind (bspw. Hochschulzeugnisse).

Aufbauend auf diesen Erkenntnissen hat die Europäische Kommission im Sommer 2021 einen Vorschlag für eine überarbeitete Version, eIDAS 2.0, erstellt, der aktuell das Gesetzgebungsverfahren durchläuft. Mit eIDAS2.0 soll ein einheitliches, EU-weit verpflichtendes Ökosystem für sichere und vertrauenswürdige Identitätsdienstleistungen geschaffen werden, sodass sowohl der öffentliche als auch der private Sektor auf elektronische Identitätslösungen zurückgreifen kann. Die Nutzergruppe von Identitätsdienstleistungen beinhaltet neben natürliche Personen auch juristische Personen. Dabei umfassen Identitätsdienstleistungen nicht nur Basisidentitätsdaten, sondern auch damit verknüpfte Merkmale, die mit besonderem Fokus auf den Datenschutz der Nutzerinnen und Nutzer Dritten vorgezeigt werden können. Weiterhin schlägt die Europäische Kommission vor, dass jeder Staat innerhalb der EU mindestens ein Identitätsschema und auch

[2] Die eIDAS-Verordnung ist unter folgendem Link abrufbar: https://op.europa.eu/en/publication-detail/-/publication/9ce0f9e5-03bb-11ec-8f47-01aa75ed71a1/language-en/format-PDF/source-225913375

mindestens eine Identitäts-Wallet bereitstellen muss. Größere Plattformen sollen solche Identitätsnachweise zukünftig akzeptieren müssen. Besonders erwähnenswert hierbei ist, dass in dem Gesetzesvorschlag der Europäische Kommission sowohl Blockchain bzw. Distributed Ledger Services als auch das SSI Konzept als mögliche Lösungen genannt werden.

Für eine erfolgreiche Umsetzung dieser europäischen Vision werden Leuchtturmprojekte benötigt, welche die Implementierung und Nutzung von elektronischen Identitätsnachweisen demonstrieren.

2.2. Ziele auf Bundesebene

Nicht nur auf europäischer Ebene besteht ein intensiver Diskurs zum Identitätsmanagement der Zukunft. Mit dem Wettbewerb „Schaufenster Sichere Digitale Identitäten“ wurde 2020 der Grundstein zur Entwicklung emergenter Technologien und Geschäftsmodelle für zukünftige digitale Identitäten geschaffen. Insgesamt elf Konsortien haben sich mit Konzeptideen und Entwicklungsroadmaps für den Aufbau eines Identitätsmanagement-Ökosystems befasst. Die vier vielversprechendsten Projekte gingen anschließend im April 2021 als Schaufensterprojekte in die Umsetzungsphase, die vom Bundesministerium für Wirtschaft und Klimaschutz mit insgesamt über 50 Millionen Euro gefördert wird. Neben Grundlagenforschung zu Themen wie der Governance eines zukünftigen Identitätsmanagementökosystems werden im Rahmen der Projekte auch verschiedenste Anwendungsfälle umgesetzt. Diese umfassen sowohl Anwendungen in der Privatwirtschaft, wie z.B. im Bankwesen oder in der Logistik, als auch einzelne Tätigkeiten in der öffentlichen Verwaltung. Drei der vier geförderten Projekte der Umsetzungsphase setzen bei ihren Anwendungen dabei auf den vielversprechenden Einsatz von SSI. Diese Wahl geht vor allem mit dem Wunsch einher, ein breites Ökosystem mit möglichst vielfältigen Anwendungsbereichen aufzubauen.

Die langfristig angelegten Schaufensterprojekte sollen gleichzeitig durch das Projekt „Schaufenster Sichere Digitale Identitäten“, welches durch das Bundeskanzleramt initiiert wurde, komplementiert werden.[3] In diesem wird besonders hoher Wert auf kurze Entwicklungszyklen und die Umsetzung unterschiedlicher Anwendungsfälle gelegt. Die erste Veröffentlichung eines Anwendungspiloten erfolgte dabei im Mai 2021. Anhand eines Hotel Check-Ins wurde die Übertragung und Prüfung von Personalausweis- und Rechnungsdaten mittels SSI demonstriert. Dabei wurde das SSI Framework Hyperledger Indy erprobt, um mittels einer (teil-)staatlichen Blockchain eine Infrastruktur für die Bereitstellung von Schemata und Informationen zu Signaturverfahren zu ermöglichen.

Neben dem Anwendungsfall des Hotel Check-Ins sollen weitere Anwendungen zeitnah folgen. Zu diesen zukünftigen Anwendungen gehört auch der Verifizierungsprozess bei Banken zur Kontoeröffnung. Aus den Ergebnissen des Pilotprojekts geht ebenfalls hervor, dass persönliche Daten (die sog. „Basis-ID“) langfristig durch Daten aus der Steuerverwaltung ergänzt werden sollten, um Prozesse durchgängig digital durchführen zu können. Dabei kann die bereits aufgebaute Blockchain-Infrastruktur, wie beispielsweise im Rahmen des Projekts NESSI, für weitere Anwendungsfälle genutzt werden. Um diese Einbettung zu ermöglichen, ist das Bayerische Landesamt

[3] Eine Übersicht über das Projekt „Sichere Digitale Identitäten ist unter folgendem Link abrufbar: https://www.bundesregierung.de/resource/blob/992814/1898280/d9819a40553a9543b9e8f3acb620b0c2/digitale-identitaet-neu-download-bundeskanzleramt-data.pdf

für Steuern dem Schaufensterprojekt IDunion beigetreten. Durch die Nutzung der bereits bestehenden Infrastruktur können Synergien in der Entwicklung geschaffen und die Kompatibilität sichergestellt werden.

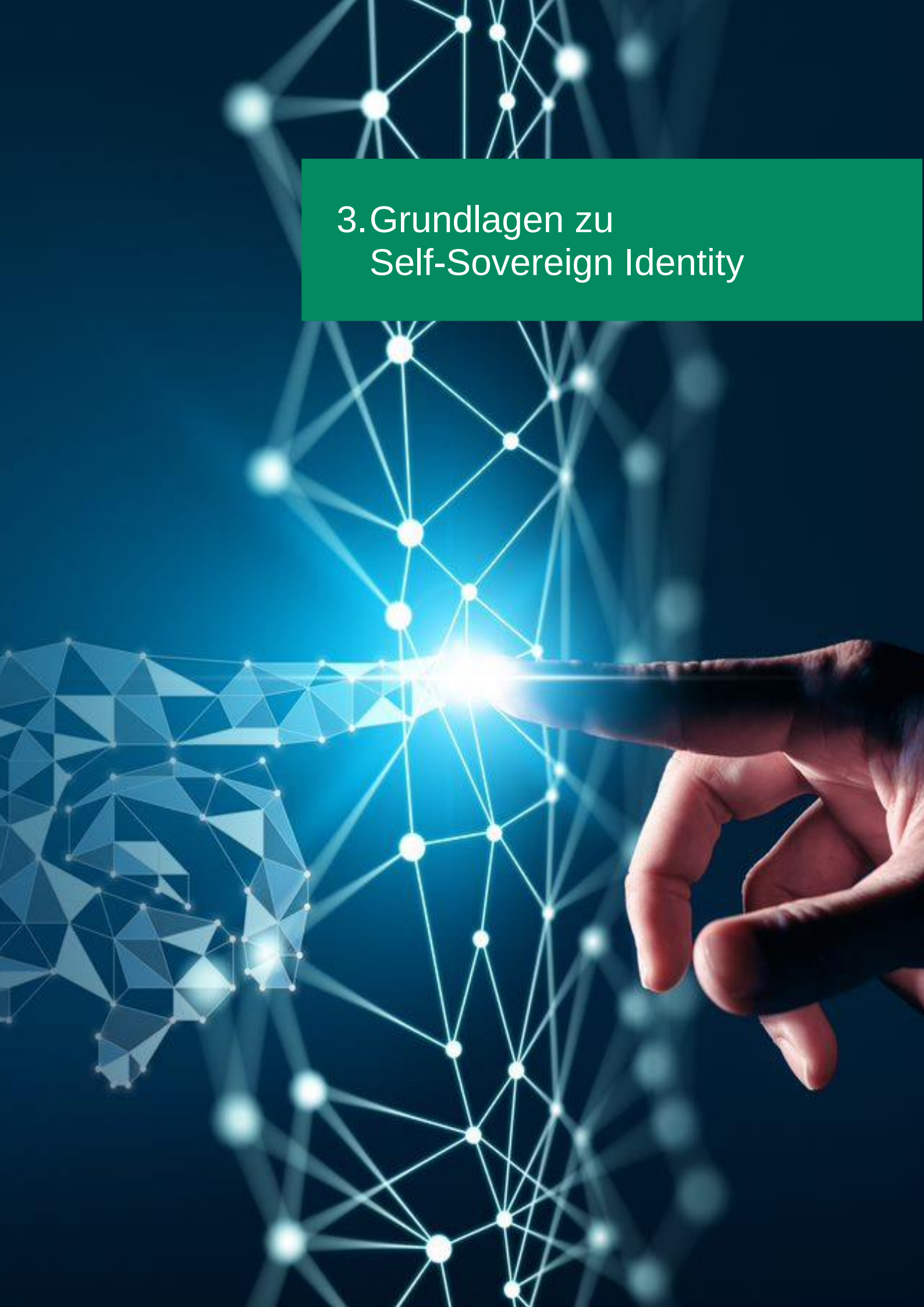
2.3. Ziele der bayerischen Steuerverwaltung

Die bayerische Steuerverwaltung verfolgt das Ziel, Bescheinigungs- und Nachweisprozesse durch die Digitalisierung der Verwaltung für die Steuerpflichtigen effizient zu gestalten. Dies bietet sich insbesondere an, da das Finanzamt in vielen Fällen die Rolle als Aussteller oder Überprüfer von Bescheinigungen bzw. Nachweisen einnimmt. Als Aussteller sind beispielsweise Bescheinigungen über die steuerliche Erfassung, die steuerliche Unbedenklichkeit, die Höhe des zu versteuernden Einkommens, die Nichtveranlagung oder die Art der Leistungen, die der Unternehmer erbringt, von Bedeutung. Spätestens seit der Diskussion um das Registermodernisierungsgesetz sind auch steuerliche Identifikationsmerkmale in den Fokus gerückt. Die Steueridentifikationsnummer soll demnach auch von anderen Behörden zur Identifizierung des Bürgers genutzt werden und stellt damit die Grundlage zur eindeutigen Identifikation im Rahmen von digitalen Behördengängen dar.

Aktuell werden diese Bescheinigungen standardmäßig in Papierform ausgegeben. Die Nachteile papierbasierter Bescheinigungen liegen dabei auf der Hand. So bringt die Entgegennahme von papierbasierten Bescheinigungen in der Steuerverwaltung oftmals einen händischen Abgleich von Daten mit sich, was zu Prozessen mit hohem Aufwand führt. In der Rolle des Ausstellers wiederum steht die Steuerverwaltung vor der Herausforderung, dass ein effektiver Mechanismus, die Gültigkeit papierbasierter Bescheinigungen mit sofortiger Außenwirkung widerrufen zu können, fehlt. So muss die Validität von Bescheinigungen meist zeitlich begrenzt werden. Dies führt dazu, dass Bescheinigungen nach Ablauf der Gültigkeit in der Regel erneut beantragt und ausgestellt werden müssen. Zudem besteht Manipulationsgefahr, da papierbasierte Bescheinigungen mit geringem Aufwand gefälscht und kopiert werden können.

Um diese Herausforderungen meistern zu können, bietet sich der Einsatz von SSI an. Neben Synergien in der Entwicklung können durch eine Einbettung in das derzeit entstehende Ökosystem Nachweise aus der Steuerverwaltung in Kombination mit weiteren Identitätsnachweisen genutzt werden. Durch die Kombination einer großen Anzahl von digitalen Nachweisen kann langfristig der effektive Zugang zu digitalen Nachweisprozessen der Verwaltung ermöglicht werden. Somit leistet die bayerische Steuerverwaltung mit dem Projekt NESSI einen grundlegenden Beitrag zum Aufbau eines digitalen Identitätsökosystems und somit zur Digitalisierung der öffentlichen Verwaltung.

3. Grundlagen zu Self-Sovereign Identity



3. Grundlagen zu Self-Sovereign Identity

Eine SSI-Architektur besteht aus fünf essenziellen Bausteinen: Verifiable Credentials und Verifiable Presentations, Rollen (Issuer, Holder und Verifier), Dezentrale Identifier (DIDs), Digital Wallets sowie Agents und Hubs.

Verifiable Credential
Digital signierte Sammlung von Attributen (Zertifikat), welche als Nachweis dienen kann.

Den Hauptbestandteil jeder SSI-Lösung bilden digitale Zertifikate (folgend engl. Credentials). Sofern diese durch Dritte attestiert werden, wie beispielsweise durch eine öffentliche Behörde, spricht man von Verifiable Credentials (1). Diese entsprechen signierten Zertifikaten und erlauben Holdern ihre Identitätsattribute gegenüber Verifiern nachzuweisen. Ein aus einem Verifiable Credential abgeleiteter Nachweis wird Verifiable Presentation (VP) genannt. Die Rollen (2) bilden im Rahmen des sogenannten Trust Triangle ein Grundgerüst für Interaktionen: Nachdem ein Issuer ein Verifiable Credential erstellt hat, kann dieses an den Holder übertragen werden. Dabei kommunizieren Issuer, Holder und Verifier mithilfe eines bilateralen, verschlüsselten Kanals. Der DID-Standard (3) erlaubt, einen solchen Kommunikationskanal zwischen zwei Parteien aufzubauen. So wird Nutzerinnen und Nutzern auch ermöglicht, unter wechselnden Identifiern aufzutreten, was die Ansammlung von Informationen und Erstellung von Nutzungsprofilen erschwert. Das notwendige kryptografische Schlüsselmaterial sowie die Verifiable Credentials werden in sog. Digital Wallets (4), die das Äquivalent von Geldbörsen darstellen, aufbewahrt. Digital Wallets beinhalten neben einem Speicher auch Agents (5), welche die technischen Endpoints für die bilaterale Kommunikation bereitstellen. Diese fünf Grundbausteine stellen die Kernarchitektur eines SSI-basierten Systems dar.

Verifiable Presentation
Nachweis (Claim) von Identitätsinformationen bzw. Attributen sowie ein Beweis von deren Korrektheit. Der Verifier bestimmt die Anforderungen des Claims.

SSI-basierte Systeme bieten zudem die Möglichkeit für einen datensparsamen Widerruf von Credentials. Hierfür wird meist ein Blockchain-basiertes Register verwendet, auf dem selbst keine sensiblen Daten über Credentials gespeichert werden. Für weiterführende Informationen zum Konzept verweisen wir auf Strüker et al. (2021). Abbildung 1 zeigt die Beziehungen zwischen den einzelnen Teilnehmenden auf.

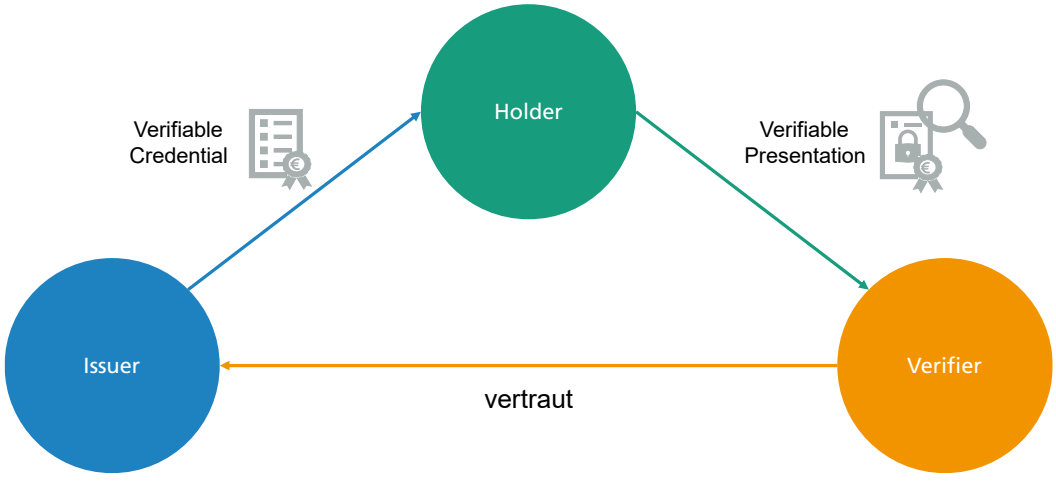


Abbildung 1: Rollen in einem SSI-System

4. Projektbeschreibung

4. Projektbeschreibung

4.1. Status quo

Für Bürgerinnen und Bürger sind Nachweise über das steuerliche Einkommen in vielen Fällen von Relevanz. Als Bonitätsnachweis, insbesondere für Selbstständige, erlauben sie die Beurteilung wirtschaftlicher Verhältnisse bei der Beantragung von Krediten oder im Kontext eines Mietverhältnisses. Auch für die Beitragsmessung bzw. -befreiung, wie beispielsweise im Rahmen der Bemessung der Zweitwohnsitzsteuer durch die Gemeinde, spielen sie eine wichtige Rolle. Zudem wird die Höhe des Einkommens bei der Beantragung von Sozialleistungen, wie z.B. bei der Beantragung von BAföG-Leistungen, abgefragt.

In den oben genannten Fällen dienen oftmals Einkommensteuerbescheide zur Erfüllung von Nachweisanforderungen, da diese durch die Ausstellung über die Steuerverwaltung eine verlässliche Auskunft über die Einkommensverhältnisse darstellen. Zudem verfügt ein Großteil der Bürgerinnen und Bürger über diesen Nachweis, was eine Prozessstandardisierung seitens der überprüfenden Partei vereinfacht: Im Jahr 2017 waren in Deutschland ca. 44 Mio. Bürgerinnen und Bürger lohn- und einkommensteuerpflichtig, wovon rund 28 Mio. eine Einkommensteuererklärung abgegeben und somit einen Einkommensteuerbescheid erhalten haben.

Der Einkommensteuerbescheid wird aktuell in Form eines elektronischen PDFs oder papierbasierten Dokuments ausgestellt. Durch dieses Format ergeben sich Nachteile im Zusammenhang mit dem Nachweis des Einkommens. Wie papierbasierte Nachweise können auch elektronische Dokumente in Form von PDFs oftmals nicht automatisiert weiterverarbeitet werden, da die Daten meist nicht strukturiert vorliegen. Zudem enthält der Einkommensteuerbescheid viele Datenfelder, die nicht allumfänglich für jeden Anwendungsfall von Relevanz sind. Allerdings sind weder elektronische PDFs noch Papier-basierte Dokumente anpassbar. Dies führt dazu, dass Dokumente umständlich manuell geschwärzt werden müssen, um lediglich relevante Datenfelder preiszugeben. Abschließend besteht die Herausforderung, dass Einkommensteuerbescheide im zeitlichen Verlauf Änderungen unterliegen können. So kann der Bescheid beispielsweise aufgrund eines Einspruchs geändert und neu ausgestellt werden. Der ursprüngliche, nun ungültige Bescheid könnte dabei weiterhin zum Nachweis des Einkommens genutzt werden, ohne dass der anfragenden Partei der aktualisierte Einkommensteuerbescheid bekannt ist.

Um eine Verbesserung zum Status quo zu erzielen, kann die Steuerverwaltung in Zukunft als Emittent eines *Elektronischen Einkommensnachweis-Credentials* fungieren. Hierzu soll die bereits bestehende Plattform Mein ELSTER genutzt werden, die bereits rund 28 Mio. Nutzerinnen und Nutzern direkten Zugriff auf Verifiable Credential-basierte Einkommensnachweise bieten würde.

Mein ELSTER
„Mein ELSTER" ist eine browserbasiere Plattform mit Hauptzweck der papierlosen Erstellung der Steuererklärung.

4.2. Use Case Kreditantrag mit Projektpartner Sparkassen-Finanzgruppe

Ein Nutzungsbeispiel des elektronischen Einkommensnachweises stellt die Kreditbeantragung dar. Dieser Anwendungsfall wurde gemeinsam mit der Sparkassen-Finanzgruppe demonstriert. Für die Sparkassen-Finanzgruppe sind Einkommensnachweise, die Sparkassen bei der Kreditvergabe zur Bonitätsprüfung benötigen, ein wichtiger Baustein für ihr Kerngeschäft. Dabei stellt ein Einkommensteuerbescheid ein sehr aussagekräftiges Indiz über die wirtschaftliche Lage von natürlichen Personen dar. Mangels Gehaltsnachweisen sind insbesondere Selbstständige auf diesen Nachweis angewiesen. Die Sparkasse zählt bei der Kreditprüfung auf die Vertrauenswürdigkeit der Steuerverwaltung als Aussteller des Bescheids. Darüber hinaus sind mit einem Einkommensteuerbescheid auch Rückschlüsse auf die privaten Verhältnisse von Selbständigen möglich, welche ihre Zahlungsfähigkeit beeinflussen können. Neben Informationen zur Fähigkeit, einen Kredit zurückzahlen zu können, enthalten Einkommensteuerbescheide auch steuerliche Stammdaten wie die Steueridentifikationsnummer. Banken und Sparkassen müssen diese Information bei einer Kontoneueröffnung zwingend aufgrund der Vorschriften zur Kontenwahrheit festhalten.

Allerdings gehen mit der Prüfung von Einkommensteuerbescheiden einige Schwierigkeiten einher. Die dokumentenbasierte Einreichung von Einkommensteuerbescheiden in Papierform oder als PDF erschwert die elektronische Datenverarbeitung. Die dadurch oftmals notwendige manuelle Datenverarbeitung verringert die Datenqualität und führt zu Medienbrüchen. Eine automatisierte Überführung von quantitativen Informationen in ein Rating-Modell wird dadurch beispielsweise unnötig erschwert oder verlangsamt. Zudem besteht bei Einkommensteuerbescheiden in aktueller Form die Problematik, dass die Gültigkeit dieser nicht ohne Weiteres überprüft werden kann. Selbst Bescheide, die nicht manipuliert wurden, können durch einen späteren Änderungssteuerbescheid überholt sein und dennoch weiterhin einem Kreditinstitut vorgelegt werden.

Um die Integration von elektronischen Einkommensnachweisen zu demonstrieren, wurde im Rahmen des Projekts NESSI idealtypisch das Anwendungsbeispiel eines Investitionskredits gewählt. So können selbstständig Tätige bei der elektronischen Beantragung eines Kredits über die durch die Steuerverwaltung ausgestellten SSI-Credentials einen elektronischen Einkommensnachweis führen sowie steuerliche Stammdaten liefern. Im Vergleich zu den heutigen papierbasierten Nachweisen bietet die Integration von elektronischen Nachweisen den Vorteil, dass Medienbrüche vermieden werden und die Datenqualität erhöht wird. Zudem kann das Elektronische Einkommensnachweis-Credential jederzeit durch die Steuerverwaltung zurückgezogen werden, sofern beispielsweise ein Änderungsbescheid erlassen wurde. Die Gültigkeit des Nachweises überprüft das Kreditinstitut mittels eines Blockchain-basierten Registers (siehe auch Kapitel 3). Schließlich kann die jeweilige Sparkasse selbst entscheiden, welche Informationen aus dem Einkommensnachweis für deren individuellen Kreditprozess notwendig sind. Entsprechend muss die Sparkasse eine Proof-Anfrage definieren. Hierbei ist eine Bandbereite möglich, die von einer Abfrage der gesamten Informationen (Full Disclosure) bis hin zu nur einzelnen Kennziffern (Selective Disclosure) reicht. Technisch sind auch sogenannte Range-Proofs möglich, bei denen eine Sparkasse z.B. abfragen könnte, ob ein bestimmtes Mindesteinkommen erreicht wird. Abbildung 2 veranschaulicht dieses Nutzungsbeispiel.

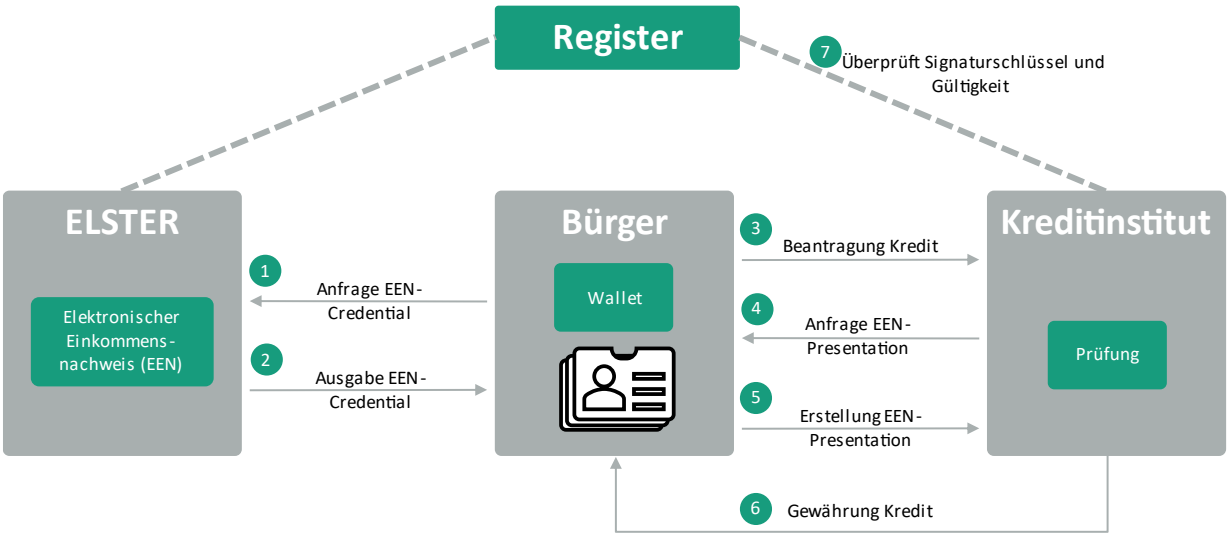


Abbildung 2: Gesamtprozess

Bis auf ein Web-fähiges Endgerät sowie einem Smartphone inkl. Wallet brauchen Nutzerinnen und Nutzer der entwickelten Lösung keine weitere Hardware. Über Mein ELSTER wird ein Dokument mit einem QR-Code erzeugt, welcher mithilfe der Wallet eingelesen wird (siehe Abbildung 3).

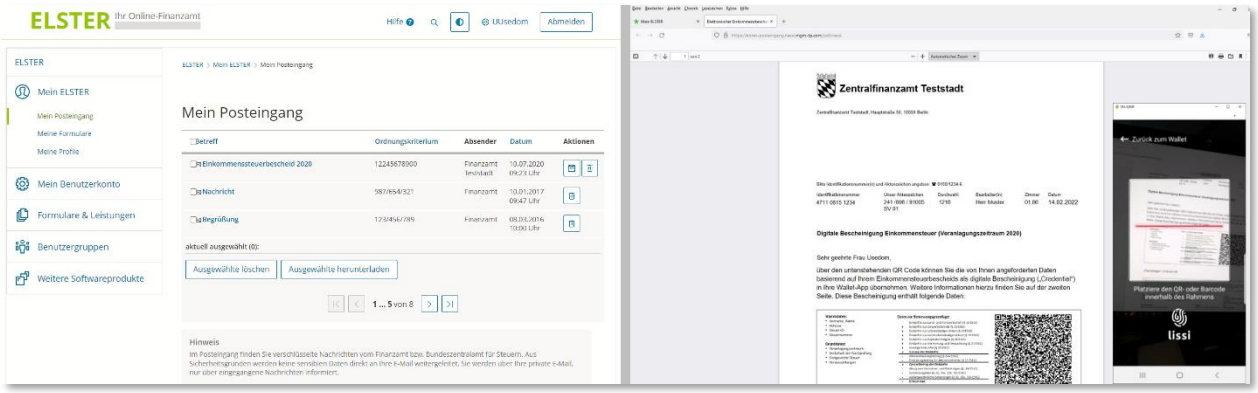


Abbildung 3: Benutzeroberfläche zur Ausstellung von Credentials über Mein ELSTER

Der QR-Code dient zur Verbindungsanfrage mit dem ELSTER Agent, sodass nachfolgend der Nachweis von der Steuerverwaltung erstellt wird und von den Nutzerinnen und Nutzern entgegengenommen werden kann. Die Web-basierten Benutzeroberflächen sind den Steuerpflichtigen bzw. Kundinnen und Kunden aus ihrer bestehenden Interaktion mit Mein ELSTER und den Online-Auftritten der Sparkassen-Finanzgruppe bereits bekannt.[4]

[4] Die entwickelte Plattformlösung zum Austausch von Einkommensnachweis-Credentials wird durch ein veröffentlichtes Video im Detail veranschaulicht.

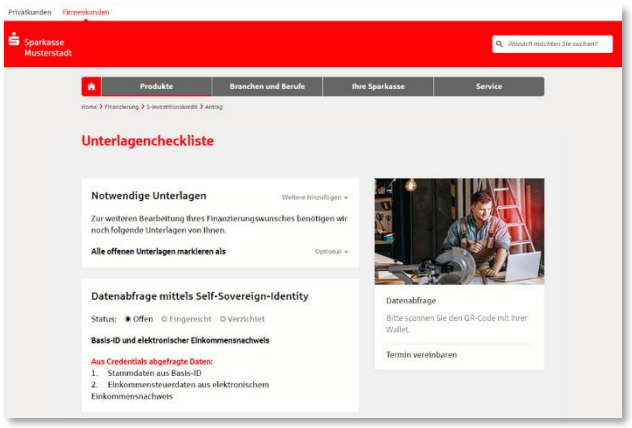


Abbildung 4: Benutzeroberfläche von dem Nachweisportal der Sparkassen-Finanzgruppe

Selbstverständlich kann der Einkommensnachweis allein für eine tief gehende Kreditprüfung nicht ausreichen. Gerade bei hohen Kreditsummen sind Banken und Sparkassen gesetzlich verpflichtet, sich weitere Nachweise vorlegen zu lassen. Daher wird im Projekt gezeigt, dass der elektronische Einkommensnachweis mit der von der Sparkassen-Finanzgruppe pilotierten Plattform „prozessintegrierter Dokumentenupload“ grundsätzlich verbunden werden könnte (siehe Abbildung 4), welchen den Kunden zum elektronischen Upload von weiteren Dokumenten dienen soll.

Durch den Einsatz von SSI-basierten Nachweisen und deren Integration in die Plattform prozessintegrierter Dokumentenupload wäre auch eine Erweiterung um weitere Nachweisarten denkbar. Beispielsweise wäre auch die Nachweiserbringung einer SSI-basierten Unternehmens-ID bzw. Unternehmensstammdaten möglich. Die Plattform an sich ist auch nicht an den Kontext eines Investitionskredits gebunden, sondern kann für weitere Beantragungsprozesse bei Sparkassen verwendet werden.

5. Rechtliche Einordnung

5. Rechtliche Einordnung

Der innovative Prototyp im Projekt antizipiert die Umsetzung der digitalen Identitäten über eine breite SSI-Infrastruktur und zeigt die Umsetzbarkeit sowie den möglichen Mehrwert eines Beitrags der Steuerverwaltung in einem derartigen Umfeld auf. Zum momentanen Zeitpunkt existieren allerdings weder diese Infrastruktur noch eine gesetzliche Grundlage, die eine Umsetzung konkret regeln könnte. Deshalb kann noch keine abschließende Bewertung abgegeben werden. Es ist davon auszugehen, dass sich bei der Entwicklung hin zu neuen Anwendungsfällen und mit einer weiteren Etablierung des SSI-Umfeldes viele Fragen der technischen Ausgestaltung und der Datensicherheit klären werden und dass der Gesetzgeber mit entsprechenden Normen den Rahmen für Projekte wie dieses klar definieren wird.

Unabhängig von diesen Erwartungen und vom Einsatz eines Prototyps im Projekt mit Testdaten (keine Echtdaten von Steuerpflichtigen) werden im Folgenden zentrale Aspekte des Projektes bewertet, die sich auf den Schutz der Steuerpflichtigen und deren Daten konzentrieren. Es handelt sich bei diesen Einschätzungen um eine Verdichtung der wichtigsten Punkte, die bei der wissenschaftlichen Begleitung dieses und des vorangegangenen SSI-Projektes mit großer Ausführlichkeit analysiert und bewertet wurden.

Da das Pilotprojekt bei einer Umsetzung die Daten aus dem Steuerbescheid bescheinigen will, ist ein zentraler Punkt für die Umsetzbarkeit die Wahrung des Steuergeheimnisses. Die Informationen im Credential sind klar personenbezogene Daten (Name, Informationen über die finanziellen Verhältnisse des Steuerpflichtigen) und in manchen Fällen möglicherweise auch Betriebs- und Geschäftsgeheimnisse,[5] die im Rahmen des Besteuerungsverfahrens bekannt geworden sind. Damit wäre jedes unbefugte Offenbaren oder Verwerten eine Verletzung des Steuergeheimnisses. Dazu kommt es aber im Rahmen des vorgestellten Konzeptes auch nicht: Der Begriff Verwertung ist von der datenschutzrechtlichen Verarbeitung abzugrenzen und setzt ein „Ausnutzen“ voraus, also einen Vorteil ziehen zu wollen[6], was hier nicht gegeben ist. Auch eine Offenbarung liegt nicht vor, da die Steuerverwaltung das Credential mit Informationen der steuerpflichtigen Person direkt an diese überträgt, woraufhin nur sie selbst diese Informationen nutzen kann. Die Informationen werden von der Verwaltung also an keinen Dritten gegeben, eine Offenbarung als Verletzung des Steuergeheimnisses bei der Übermittlung der Informationen aus seinem eigenen Steuerbescheid an den Steuerpflichtigen selbst ist nicht möglich.[7]

Der zweite wichtige Aspekt ist die datenschutzrechtliche Bewertung. Grundlage ist hier die aktuelle technische Konzeption nach den Standards, die bei den Schaufensterprojekten der Bundesregierung angewendet werden. Besonderes Augenmerk gilt der Distributed Ledger Technologie bzw. Blockchain, die gewählt wurde, um die Verwaltung der Gültigkeit von Credentials zu ermöglichen und damit grundsätzlich von Dritten (Verifiern) einsehbar sein muss. Der Einsatz der Blockchain Technologie ist vergleichsweise neu und deren Datenschutzkonformität wird regelmäßig

---

[5] Unter Betriebs- und Geschäftsgeheimnis können auch Finanzdaten des Unternehmens, wie Bilanzen und Kalkulationen fallen (Pätz in König AO, 4. Auflage 2021, § 30 Rz. 68; Tormöhlen in Gosch AO/FGO Stand April 2021, § 30 Rz. 69) soweit diese nicht bereits von § 30 Abs. 2 Nr. 1, also den personenbezogenen Daten, erfasst sind (Pätz in König AO, 4. Auflage 2021, § 30 Rz. 66). Dies liegen umso wahrscheinlicher vor, je detaillierter das Credential ist. Aber auch allein der Betrag der Einkünfte kann unter Umständen als Betriebs- und Geschäftsgeheimnis gewertet werden, wenn sie Z.B. für die Konkurrenz von Interesse sein könnten (Rüsken in Klein AO 15. Auflage 2020, § 30 Rz. 57), etwa, um Vergleiche anzustellen.

[6] Pätz in König AO, 4. Auflage 2021, § 30 Rz. 99; Tormöhlen in Gosch, AO April 2021 § 30 Rz. 74

[7] Rüsken in Klein, AO 15. Auflage 2020, § 30 Rz. 59.

diskutiert (siehe u.a. Fridgen et al. 2019, Finck 2018; Marnau 2017; Quiel 2018; Tönnissen und Teuteberg 2020; Lyons et al. 2018). Es ist wichtig, an dieser Stelle den Einsatz der Blockchain Technologie im SSI-Konzept als öffentliches Gültigkeitsregister abzugrenzen von Ansätzen, die das Schreiben steuersensibler Daten, wie z.B. Rechnungsinformationen, in verschlüsselter oder auch nur gehashter Form auf die Blockchain vorsehen. Als Kernelement bei SSI werden die kritischen Informationen nur peer-to-peer ausgetauscht. Entsprechend werden im konkreten Anwendungsfall schon durch die originäre Ausgestaltung viele der diskutierten Probleme vermieden, da nur technisch notwendige Aspekte auf die Blockchain geschrieben werden, während die bescheinigten Informationen in Form eines Credentials nur bei dem Credential-Haltenden liegen.

Die Distributed Ledger Technologie wird verwendet, um folgende Informationen auf der Blockchain zu erfassen: Daten über den Credential-Aussteller (Public Key und Public DID), über die Schemata der Credentials und die verschiedenen Versionen des Revocation Registries. Die Informationen zu den Ausstellern sind notwendig, um einen sicheren Austauschkanal zu diesen herstellen zu können und um die Authentizität der Credentials bestätigen zu können. Die Authentifizierung erfolgt über den Public Key des Ausstellers, zu keinem Zeitpunkt ist es notwendig, einen Hash des Credentials in der Blockchain zu speichern, um dessen Echtheit prüfen zu können. Der Aussteller ist hier die Steuerverwaltung, und damit keine natürliche Person. Das bedeutet, der Anwendungsbereich der Datenschutz-Grundverordnung ist nicht eröffnet. Die Schemata der Credentials sind technische Definitionen, wie ein auszustellendes Credential auszusehen hat, d.h. sie enthalten neben Namen und Version auch sogenannte Attribute. Dabei handelt es sich um abstrakte Datenfelder aus dem Einkommensteuerbescheid, die im Einkommensnachweis-Credential enthalten sein sollen. Wird das Schema entsprechend gestaltet, kann hier kein Personenbezug vorliegen. Es handelt sich um eine rein technische Formvorgabe. In der analogen Welt ließe sich dies gut mit einem leeren, keiner speziellen Person zuordenbarem Formular vergleichen.

Das Revocation Registry, um technisch ein Zurückziehen des Credentials ad hoc zu ermöglichen, bedarf jedoch genauerer Betrachtung. Die wichtigsten Inhalte im Revocation Registry sind die jeweils zur Veröffentlichung gültige Version des Accumulators sowie ein Link zum Tails File und ein Hash des zugehörigen Tails Files. Im Tails File findet sich eine Liste mit randomisierten Zahlen für theoretisch zu vergebenden Credentials, es enthält keine Information, die man auf eine Person beziehen könnte. Ein Hash des Tails Files oder ein Link zu diesem ist folglich ebenso kein personenbezogenes Datum. Die Zahlen aus dem Tails File ergeben durch eine unmöglich schwer rückrechenbare mathematische Operation den Accumulator. Wenn ein Credential ausgestellt wird, erhält es eine der Zahlen aus dem Tails File zugeteilt. Der Credential-Halter erhält dazu die Informationen, die er braucht, um mit der Zahl aus seinem Credential so lange den Accumulator herstellen zu können, solange diese Zahl ein Teil des Accumulators ist. Durch das erfolgreiche Herstellen des Accumulators beweist er die Gültigkeit seines Credentials. Wird ein Credential auf ungültig gesetzt, wird eine aktualisierte Version des Accumulators auf die Blockchain geschrieben, die die Zahl des entsprechenden Credentials in seiner Berechnung nicht mehr enthält. Der Accumulator ist also kein Hash eines Wertes und enthält für sich keine Information. Nur durch die Kenntnis der Zahl des Credentials und der Information, die notwendig ist, um den Accumulator herzustellen, kann die singuläre Aussage getroffen werden, dass das besagte Credential zu dem Zeitpunkt der Registrierung des Accumulators nicht widerrufen wurde. Selbst wenn es technisch möglich wäre, den Accumulator „zurückzurechnen“, wäre das einzig denkbare Ergebnis eine Liste mit allen Zahlen theoretischer Credentials, die nicht zurückgerufen wurden. Man könnte daraus trotzdem nicht erkennen, ob diese Credentials schon ausgestellt wurden (oder noch ausgestellt werden können), an wen diese Credentials ausgestellt wurden oder welche Werte in den Credentials stehen. Auch ist es innerhalb des SSI-Umfeldes nie notwendig, die Zahl des Credentials

offenzulegen, sodass diese nur dem Aussteller und dem Halter selbst bekannt sind. Die Informationen auf der Blockchain können für sich also nie, selbst wenn sie kompromittiert werden, direkt Informationen über eine natürliche Person preisgeben. Dieser mangelnde Informationsgehalt spricht sehr stark dafür, dass kein personenbezogenes Datum auf der Blockchain liegt.[8]

Trotzdem wäre es bei maximalweiter Auslegung des Personenbezugs[9] nicht vollständig auszuschließen, im Accumulator ein personenbezogenes Datum zu sehen. Auch wenn er für sich keinerlei Information enthält, ermöglicht er zusammen mit anderen Informationen eine Aussage über die Gültigkeit eines personenbezogenen Datums, was ein indirekter Personenbezug darstellen könnte. Diesen Personenbezug kann nur herstellen, wer die beiden anderen Elemente aus dem Credential kennt, also Credential-Aussteller und -Halter. Für alle anderen liegt auch bei einem verschärften Maßstab für relativen Personenbezug kein personenbezogenes Datum vor, was bedeutet, dass es zu keiner Offenlegung kommt (auch das Steuergeheimnis wäre in diesem Fall weiterhin nicht verletzt, da genauso keine Offenbarung vorliegen würde). Für die Steuerverwaltung wäre der Anwendungsbereich der Datenschutz-Grundverordnung an dieser Stelle allerdings eröffnet. Aufgrund der speziellen Eigenschaften des Accumulators dürfte es aber möglich sein, diese Verarbeitung DS-GVO konform zu gestalten. Vor allem das Löschen wäre hier trotz Blockchain kein Problem, da eine Löschung der Credential-Informationen dem Accumulator jeden Personenbezug nehmen würde, was de facto eine Löschung ist.[10]

Auch abseits der Blockchain verdienen einige Aspekte, wie die Ausstellung der Credentials selbst, einer genaueren Betrachtung. Hervorzuheben ist hier einerseits generell das Aktivwerden der Steuerverwaltung, und andererseits die Schutzbedürftigkeit des Steuerpflichtigen bezüglich der Informationen in den Credentials. Wie schon erwähnt, wird davon ausgegangen, dass in Zukunft ein gesetzlicher Rahmen für die vorgestellte Lösung bestehen wird. Fragen zur Gesetzmäßigkeit der Verwaltungshandlung und der Ermächtigungsgrundlage eines potenziellen Eingriffs in das allgemeine Persönlichkeitsrecht des Bürgers sind deshalb vergleichsweise unproblematisch. Es handelt sich bei dem Ausstellen des Credentials auch um keinen Verwaltungsakt. Der Verwaltungsakt ist der Steuerbescheid selbst, das Credential ist nichts weiter als das Zurverfügungstellen der darin enthaltenen Informationen.[11] Es handelt sich um keine Maßnahme zur Regelung eines Einzelfalls und es besteht keine Rechtsfolge für den Steuerpflichtigen.

Wenn es um den Schutz der Daten des Bürgers geht, stehen die Informationen in den Credentials im Vordergrund. Es handelt sich dabei in erster Linie um personenbezogene Daten derselben Person, die auch das Credential hält. Im Einkommensteuerbescheid finden sich aber auch Daten Dritter, die je nach Gestaltung in verschiedenem Maße auch in dem Credential Einzug halten können. Ein typischer Fall dürfte die Zusammenveranlagung sein. Im Steuerbescheid finden sich dann durch die gemeinsame Steuerfestsetzung auch die Informationen des Partners. Wenn das in ein Credential übertragen wird, und ein vollständiges Ausklammern ist schwer möglich, hat das zur Folge, dass der Credential-Halter zum Verantwortlichen für die Verarbeitung der Daten des

---

[8] Ähnliche Schlussfolgerung für einen nicht rückrechenbaren Hash: Erbguth, Datenschutzkonforme Verwendung von Hashwerten auf Blockchains, MMR 2019, S. 654 (659).

[9] Zur Auslegung von Personenbezug siehe auch Art 29 Datenschutzgruppe Stellungnahme WP 136, S. 7; Martin Eßer in: Eßer/Kramer/von Lewinski *Auernhammer DSGVO/BDSG,* 7. Auflage 2020, Art. 4 DS-GVO Rz. 7; Stefan Ernst in: Paal/Pauly DS-GVO BDSG, 2. Auflage 2018, Art. 4 DS-GVO Rz. 3.

[10] Der Bundesbeauftragte für Datenschutz und die Informationsfreiheit, Positionspapier zur Anonymisierung unter der DSGVO unter besonderer Berücksichtigung der TK-Branche, 29.06.2020, S. 8 f.; Mario Martini, Quirin Weinzierl, Die Blockchain-Technologie und das Recht auf Vergessenwerden, NVwZ 17/2017, S. 1251 (1256).

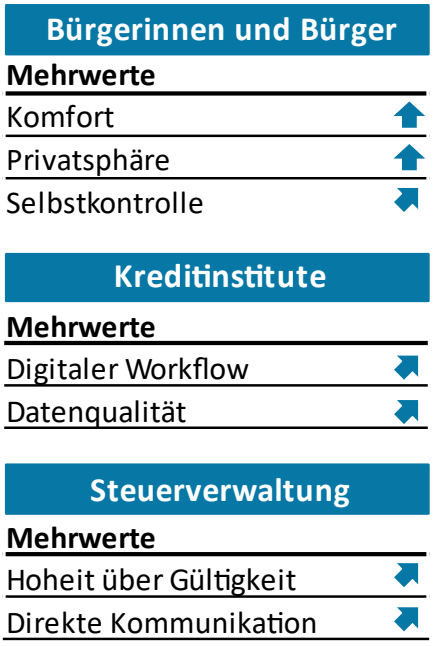
[11] Siehe analog: Seer in Tipke/Kruso AO/FGO, §118 Rz 27 für Ansässigkeitsbescheinigungen.

Partners wird. Der Anwendungsbereich der Datenschutz-Grundverordnung kann dann neben der Steuerverwaltung auch für den Credential-Halter eröffnet sein, da hier von natürlichen Personen als Steuerpflichtigen ausgegangen wird, und das Ausstellen und Speichern der Credentials Verarbeitungen sind, für die die in Deutschland sitzende Steuerverwaltung oder der in Deutschland Steuerpflichtige Verantwortlicher ist. Auch eine Nutzung des Steuerpflichtigen zu rein persönlichen Zwecken (Haushaltsausnahme) kann nicht generell angenommen werden.

Während eine datenschutzkonforme Lösung auf Seiten der Verwaltung wenig problematisch herzustellen ist, befindet man sich beim Credential-Halter in einem Bereich, auf den man schwer zugreifen kann. Die SSI-Struktur schränkt die Möglichkeiten der Verarbeitung ein, der normale Verbraucher kann das Credential nur speichern und vorzeigen, aber auch diese Schritte müssen DS-GVO konform erfolgen. Das ist grundsätzlich möglich, hier sollte schon in der Gestaltung des Systems dafür gesorgt werden, dass der unter Umständen datenschutzrechtlich unerfahrene Steuerpflichtige diese Grundsätze im Zweifel möglichst leicht erfüllen kann und dass seine Daten (und die Informationen des Partners) trotz Souveränität, was ja auch Eigenverantwortung bedeutet, ausreichend geschützt sind. Das ist gewährleistet: wenn erstens technisch sichergestellt wird, dass der Steuerpflichtige die Credentials nur im SSI-Umfeld und dem SSI-Umfeld entsprechend nutzen kann; wenn zweitens eine Grundlage für die (Weiter-)Verarbeitung geschaffen wird, sodass er nicht die Zustimmung des Partners erhalten und nachweisen können muss; und drittens, wenn man die Informationen im Credential schon so einschränkt, dass nicht die vollen Daten des Partners enthalten sind. Dadurch wird der Partner zum einen vor Credential-Empfängern geschützt, die ohne rechtmäßige Grundlage zu viele Daten erhalten möchten und zum anderen können die vollständigen Informationen nur empfangen werden, wenn beide ihre Credentials übermitteln, was nicht nur eine Weitergabe des vollständigen Inhalts ohne Zustimmung verhindert, sondern auch den Grundsatz der Transparenz umsetzt.

6. Mehrwertanalyse

6. Mehrwertanalyse



Die Evaluation des SSI Systems erfolgt dreigeteilt und soll die identifizierten Mehrwerte des Systems für Bürgerinnen und Bürger, Kreditinstitute und die Steuerverwaltung aufzeigen. Hierbei wird erörtert, inwiefern das neue System bestehende Prozesse unterstützen oder verbessern kann und somit Mehrwerte für die einzelnen Stakeholder schafft.

6.1. Mehrwerte für Bürgerinnen und Bürger

Komfort

Die Vorteile bezüglich des Nutzerkomforts resultieren in erster Linie aus der Digitalisierung der vorhandenen Papierdokumente. Gerade für Bürgerinnen und Bürger stellen Papierdokumente einen zusätzlichen Aufwand bei der Beantragung eines Kredits dar. Oftmals müssen bei der Beantragung eine Vielzahl von verschiedenen Dokumenten gesammelt und vorgelegt werden. Mit dem SSI-System wird hier ein deutlicher Komfortgewinn erzielt. Dank der Smartphone-Wallet können Bürgerinnen und Bürger nun alle auf ihrem Smartphone gespeicherten Bescheinigungen und Nachweise jederzeit mit sich führen. Bei der Kreditbeantragung können die entsprechenden Dokumente durch die Wallet bereitgestellt werden. Bürgerinnen und Bürger können dann schließlich sehen, welche Daten aus welchem Dokument benötigt werden und diese bequem freigeben. Allerdings geht dieser Komfort, bedingt durch die zentrale Speicherung von Nachweisen, bei Nutzerinnen und Nutzer auch mit gewissen Risiken einher. So führen Zugriffsschwierigkeiten auf das Smartphone, beispielsweise im Falle des Verlusts, dazu, dass auf alle gespeicherten Nachweise nicht mehr zugegriffen werden kann. Um weitreichende negative Konsequenzen für die Nutzerinnen und Nutzer zu vermeiden, wird aktuell an Lösungen gearbeitet (siehe auch Kapitel 7.3).

Privatsphäre

Dokumente wie der Einkommensteuerbescheid enthalten eine Vielzahl persönlicher Daten. Ein Teil dieser Daten könnte jedoch für den Kreditantrag gar nicht benötigt werden. Um einen unnötigen Informationsabfluss zu verhindern, ist es aktuell notwendig, einzelne Felder des Einkommensteuerbescheides zu schwärzen. Dies wiederum ist mit erhöhtem Aufwand verbunden und oft nicht möglich, da die Kreditinstitute selten genau kommunizieren, welche Felder tatsächlich für die weitere Bearbeitung verwendet werden. Im Gegensatz zu analogen Dokumenten können in einem SSI-System auch nur einzelne Datenfelder aus einem Verifiable Credential für eine Transaktion angefragt werden. Allerdings obliegt die Auswahl der für eine Transaktion benötigten Datenfelder dem Verifier, welcher bereits bei der Implementierung der technischen Prozesse dazu gezwungen wird, die benötigten Datenfelder genau zu spezifizieren. Anschließend können auch nur diese Datenfelder von Nutzerinnen und Nutzern abgefragt werden. Somit bietet das SSI System die Möglichkeit, das oft geforderte Privacy-by-Design bzw. den Grundsatz der Datenminimierung umzusetzen und stellt somit eine wichtige Grundlage dar, um Bürgerinnen und Bürgern zu mehr Datenschutz zu verhelfen. Dabei gilt weiterhin, dass Nutzerinnen und Nutzer sich aktiv entscheiden sollten, ob und welche Daten sie für die Inanspruchnahme von Services teilen möchten.

Selbstkontrolle

Der Einsatz von SSI steht in starkem Gegensatz zu zentralisierten Datenplattformen, bei denen beispielsweise verschiedene Unternehmen ohne Beteiligung der Betroffenen Daten austauschen. Damit stellt SSI eine Alternative im Rahmen der fortschreitenden Digitalisierung dar, ohne jedoch die Souveränität der Bürgerinnen und Bürger einzuschränken. Genau wie bei analogen Papierdokumenten bleibt die Kontrolle und Entscheidung über die Weitergabe der Daten bei den Betroffenen erhalten.

6.2. Mehrwerte für die Kreditinstitute

Voll digitaler Workflow

Ähnlich zum gesteigerten Komfort für Endnutzerinnen und Endnutzer zeigt die Digitalisierung von Nachweisen auch für die beteiligten Kreditinstitute deutliche Vorteile. Dank eines elektronischen Einkommensnachweises wird nun ein voll digitaler Workflow ermöglicht. Es ist nun nicht mehr notwendig, einzelne Daten aus einem Papierdokument manuell zu übertragen. Stattdessen werden Informationen direkt digital aus dem entsprechenden Elektronischen Einkommensnachweis-Credential erhoben und können anschließend einfach und sicher durch das Kreditinstitut verarbeitet werden.

Datenqualität

Dank des voll digitalen Prozesses, von der Ausstellung des elektronischen Einkommensnachweises bis zur Prüfung durch das Kreditinstitut, können Inkonsistenzen von Informationen vermieden werden. Der Einsatz von kryptographischen Mechanismen stellt sicher, dass alle Informationen, exakt wie von der Steuerverwaltung ausgestellt, auch bei dem Kreditinstitut ankommen. Dies sorgt für eine hohe Datenqualität bei allen Beteiligten. Für Banken bedeutet dies verringerte Kosten der Datenprüfung und vermeidet Prozesse zur nachträglichen Klärung bei Ungereimtheiten.

6.3. Mehrwerte für die (Steuer-) Verwaltung

Hoheit über Gültigkeit von Nachweisen

Während Papierdokumente durch den Einsatz von Wasserzeichen und Siegeln zumindest sehr grundlegende Mechanismen besitzen können, um diese vor Fälschung zu schützen, ist es damit jedoch nicht möglich, eine (temporäre) Gültigkeit abzubilden. Beim Einkommensnachweis kann es der Fall sein, dass die zugrundeliegenden Informationen im Nachhinein angepasst werden müssen und der ursprüngliche Einkommensnachweis somit die steuerlichen Verhältnisse nicht mehr zutreffend abbildet. Im Rahmen einer Nachprüfung können die zu entrichtenden Steuern beispielsweise höher oder niedriger als ursprünglich erklärt ausfallen. Infolgedessen wird ein geänderter Einkommensnachweis erlassen. Das alte Papierdokument bleibt währenddessen jedoch weiterhin im Umlauf. Mit SSI hat die Steuerverwaltung nun die Möglichkeit, ausgegebene Verifiable Credentials unter bestimmten Umständen, bspw. bei Erlass eines geänderten Einkommensnachweises, ungültig zu setzen und ein neues Einkommensnachweis-Credential auszugeben.

Direkte Kommunikation mit Bürgerinnen und Bürgern

Für die Verwaltung bleibt, ähnlich zum Papierbescheid, der direkte Kontakt zu den Bürgerinnen und Bürgern für die Weitergabe von Daten, was mehrere Vorteile mit sich bringt. Einerseits bleibt dadurch die Souveränität der Steuerpflichtigen erhalten. Es findet kein weiterer Datenaustausch zwischen der Steuerverwaltung und dritten Parteien statt. Zusätzlich bedeutet dies auch, dass der Implementierungsaufwand für Schnittstellen gering ist. Einzig und allein eine Standardschnittstelle zwischen dem Agenten der Steuerverwaltung und den Wallets der Bürgerinnen und Bürger muss entwickelt werden.

7. Notwendige Schritte zum Produktivsystem

7. Notwendige Schritte zum Produktivsystem

Das Projekt NESSI soll die Umsetzbarkeit von SSI-basierten Nachweisen im Produktiveinsatz bei ELSTER erproben. Dabei zeigen sowohl interne Untersuchungen im Rahmen des Projekts als auch eine aktuelle Bewertung des *Bundesamtes für Sicherheit in der Informationstechnik* (BSI, siehe Bundesamt für Sicherheit in der Informationstechnik 2021a), dass hinsichtlich der Sicherheit und der Governance weiterführende Konzepte noch fehlen. Auch müssen für einen Produktiveinsatz in Mein ELSTER Architekturkomponenten um Funktionen erweitert werden. Dies wird im Folgenden diskutiert und in Tabelle 1 dargestellt.

Regulatorik und Betrieb
Europäische Regulatorik (finale Verabschiedung von eIDAS 2.0)
Entscheidung über Weiterentwicklung der Basis-ID
Betrieb von Infrastruktur
IT-Sicherheit und technische Weiterentwicklung
Eindeutige Identifizierung von Nutzern und Verifiern
Hardwareseitige Verwaltung von Schlüsselmaterialien
BSI-seitige Einschätzung zu kryptografischen Verfahren
Bindung zwischen Wallet und Verifiable Credential sowie Nutzerinnen und Nutzern
Performanz, Skalierbarkeit und Stabilität
Funktionale Weiterentwicklung
Delegation
Credential Revocation
Wallet Revocation and Recovery
Nutzerakzeptanz

Tabelle 1: Überblick über notwendige Schritte zum Produktivsystem

7.1. Regulatorik und Betrieb

Aktuell verbleiben Unsicherheiten bezüglich des regulatorischen Rahmens, innerhalb dessen SSI-Anwendungen entwickelt werden. Auch muss die Governance von SSI-basierten Ökosystemen in ihrer Gesamtheit geklärt werden, um die eindeutige Zuteilung von Verantwortlichkeiten sicherzustellen. Hierzu zählt beispielsweise die Verantwortlichkeit für das langfristige Betreiben der zugrundliegenden Infrastruktur, um eine Ausfallsicherheit zu gewährleisten.

Europäische Regulatorik

Auf europäischer Ebene ist insbesondere der Gesetzesentwurf eIDAS 2.0 von großer Relevanz. Wie bereits in Kapitel 2.1 beschrieben, fördert der Entwurf die Entwicklung eines Identitätsökosystems innerhalb Europas und verpflichtet die Mitgliedsstaaten zur Bereitstellung von umfassenden Wallet-Applikationen. Eine finale Verabschiedung dieses Entwurfs würde demnach die Grundlage für ein zügiges Weiterentwickeln des zum Teil bereits erarbeiteten Identitätsökosystems innerhalb Deutschlands darstellen.

Weiterentwicklung der Basis-ID

Bereits im Jahr 2020 hat die Bundesregierung neben den öffentlich geförderten Schaufensterprojekten ein weiteres Projekt zur Entwicklung einer Basis-ID ins Leben gerufen, welches das SSI-basierte Pendant zum analogen Personalausweis bzw. der eID darstellen soll. Die Überprüfung der Identität des Holders stellt eine Voraussetzung für viele Anwendungsfälle dar, sodass das Verifiable Credential nur durch den tatsächlichen Nutzer erlangt werden kann. Auch im vorliegenden Anwendungsfall wurde diese Funktionsweise prototypisch umgesetzt. Allerdings sollte perspektivisch die Basis-ID durch Behörden auf Bundesebene ausgeben werden. Vor diesem Hintergrund ist die Fortführung der bereits bestehenden Projekte von großer Relevanz für die produktive Einführung von Bescheinigungen im steuerlichen Kontext. Eine Alternative, um die Stammdaten des Empfängers zu prüfen, stellt neben der Basis-ID die eID dar. Allerdings sind bei der Nutzung der eID höhere Aufwände für die Herstellung von Interoperabilität und Systemschnittstellen zu erwarten.

Infrastruktur-Betrieb

Die Entscheidung über die Weiterentwicklung der SSI-Tätigkeiten auf Bundesebene beeinflusst auch die Höhe der Aufwände und Komplexität für die Weiterentwicklung seitens der Steuerverwaltung. Die Möglichkeit, auf eine bestehende Infrastruktur (bspw. für das Veröffentlichen von Daten über die Issuer, Credential-Schemata, Widerruf-Listen) aufzubauen, würde die Weiterentwicklung der Vorhaben deutlich erleichtern.

Zudem ist anzumerken, dass im Rahmen des Prototypenbetriebes für das Verifiable Data Registry auf eine Blockchain gesetzt wurde. Für SSI wird jedoch nicht zwangsweise eine Blockchain benötigt. Auch eine Vielzahl anderer Infrastrukturen könnten genutzt werden. Beispielsweise wäre auch die Nutzung eines zentralen Serversystems für die Speicherung von Public DIDs, Schemas und Revocation-Lists möglich. Für den operativen Einsatz sollten entsprechend weitere Möglichkeiten analysiert und bewertet werden. Je nach Gewichtung der Anforderungen in Bezug auf Governance und IT-Sicherheit könnten sich unterschiedliche Empfehlungen für die grundlegende Infrastruktur ergeben. Zudem muss die genutzte Infrastruktur vor dem Einsatz in produktiver Umgebung geprüft werden, da sie nicht von der Steuerverwaltung (alleine) betrieben wird. Beispielsweise müsste das im Rahmen des Pilotprojekts genutzte IDunion-Netzwerk die Anforderungen in Bezug auf IT-Sicherheit, Interoperabilität mit anderen Netzwerken und eIDAS-Kompabilität erfüllen. Zudem bleibt bislang ungeklärt, welche Kosten bei der Nutzung des Netzwerks entstehen und welche Partei diese tragen wird. Auch müssen bei der Nutzung von Services durch IDunion Ausschreibungsvorgaben erfüllt werden.

7.2. IT-Sicherheit und technische Weiterentwicklung

In einer Untersuchung im vorliegenden Projekt wurden weitere sicherheitsrelevante Aspekte für den Betrieb eines Produktivsystems im Kontext von sowohl der ELSTER-Infrastruktur als auch der Plattform Mein ELSTER identifiziert. Auch das BSI hat Verbesserungspotentiale hinsichtlich der Sicherheit von SSI-basierten Systemen festgestellt (Bargstädt-Franke 2021; Bundesamt für Sicherheit in der Informationstechnik 2021a). So sei die Basis-ID, welche im Projekt des Bundeskanzleramts entwickelt wurde, bis dato noch nicht vergleichbar mit heutigen Alternativen wie der eID-Funktion des Personalausweises. Demzufolge kann die Sicherheit von SSI-basierten Identitätsnachweisen aktuell nicht als „substantiell“ oder „hoch“ entsprechend der eIDAS-Verordnung eingeschätzt werden.

Eindeutige Identifizierung von Nutzern

Aktuell bestehen fünf verschiedene Login-Möglichkeiten für die eindeutige Identifizierung und Anmeldung von Steuerpflichtigen bei Mein ELSTER. Darunter gehört neben einem ELSTER-Zertifikat auch die Anmeldung via der eID-Funktion des Personalausweises. Um ein geschlossenes Ökosystem anbieten zu können, sollten in Zukunft SSI-basierte Identifizierungsmöglichkeiten für die Anmeldung bei Mein ELSTER genutzt werden können. So arbeitet das Bundeskanzleramt gemeinsam mit der Bundesdruckerei an der Bereitstellung der Basis-ID. Daher würde eine zusätzliche Einbindung der Basis-ID eine nahtlose Nutzung von SSI von der Anmeldung bei Mein ELSTER bis zur Ausstellung von Dokumenten ermöglichen. Nicht zuletzt könnte mit der Basis-ID somit auch das entsprechende Gerät, auf dem dieses Verifiable Credential gespeichert wird, als zu der entsprechenden Person zugehörig registriert werden. Nachweise in Form von Verifiable Credentials werden anschließend nur auf Geräte übertragen, über die zuvor ein Identitätsnachweis bereitgestellt worden ist.

Identifizierung von Verifiern

Neben den Teilnehmenden müssen auch die Verifier identifizierbar sein. Dies ist insbesondere aus sicherheitstechnischen Gründen von großer Relevanz. Denn es sollten nur authentifizierte Parteien entsprechende Nachweise abfragen können. Beispielsweise könnte sich eine böswillige Partei als Kreditinstitut ausgeben und die Daten des Elektronischen Einkommensnachweis-Credentials abfragen (sog. „Man-in-the-Middle-Angriff“), während die Nutzerinnen und Nutzer davon ausgehen, ihre Daten mit der Sparkasse zu teilen. Daher muss sichergestellt werden, dass Nutzer und Nutzerinnen sich darauf verlassen können, dass der Verifier die Partei ist, die sie vorgibt zu sein. Die Authentifizierung der Partei kann dabei mithilfe unterschiedlicher Lösungsmöglichkeiten durchgeführt werden. Einerseits könnten die Holder vor der Freigabe ihrer Daten die Identität des Verifiers mittels einer Verifiable Presentations abfragen. Somit würden sie im ersten Schritt selbst als Verifier auftreten. Andererseits kann auch ein Register verwendet werden, welches vertrauenswürdige Verifier auflistet. Dies würde Holdern erlauben, bei der Anfrage nach einer Verifiable Presentation durch einen Verifier die Registrierung dieser und somit ihre Vertrauenswürdigkeit zu überprüfen.

Diese beiden Möglichkeiten bedeuten zwar einen zusätzlichen Schritt zum Verbindungsaufbau und der Freigabe einer Verifiable Presentation des Elektronischen Einkommensnachweis-Credentials, können allerdings Man-in-the-Middle-Angriff deutlich erschweren.

Hardwareseitige Verwaltung von Schlüsselmaterialien

Aktuell wird das kryptografische Schlüsselmaterial von Verbrauchern durch Wallet-Software auf deren Endgeräten erstellt. Dies birgt allerdings die Gefahr, dass durch softwareseitige Angriffe das Schlüsselmaterial kompromittiert werden kann. Um dies zu verhindern, sollte kryptografisches Schlüsselmaterial idealerweise innerhalb von sicherer Hardware, sog. Secure Elements, verwaltet werden. Dies sind besonders gesicherte Chips, bspw. in Smartphones, welche vor unautorisierten Zugriffen durch unbefugte Anwendungen und Viren geschützt sind.

Neben dem Vorteil, dass die kryptografischen Schlüssel geschützt werden, birgt der Einsatz von Secure Elements auch eine konkrete Herausforderung. Eine hardwareseitige Bindung kann auch eine Abhängigkeit von Hardware-Anbietern bedeuten, da diese die im System verwendeten Signaturmechanismen unterstützten müssen. Bürgerinnen und Bürger könnten dann die entsprechenden Sicherheitsfunktionen nur mit einem kompatiblen Smartphone nutzen, was der schnellen Verbreitung des SSI-Ökosystems allerdings zuwiderlaufen dürfte.

BSI-seitige Einschätzung zu kryptografischen Verfahren

Bisher sind noch keine Einschätzungen von neuartigen kryptografischen Verfahren durch das BSI erfolgt. Zu diesen neuartigen Verfahren gehört beispielsweise das Camenisch-Lysyanskaya-Signaturverfahren (Bundesamt für Sicherheit in der Informationstechnik 2021b; Hühnlein und Korte 2006), welches u.a. beim Einsatz von Zero-Knowledge-Proofs für die selektive Freigabe von Daten verwendet wird. Eine abschließende, positive Einschätzung durch das BSI hinsichtlich der Sicherheit der kryptografischen Mechanismen ist für die Nutzung dieser im Betrieb von Produktivsystemen notwendig.

Binding zwischen Wallet und Verifiable Credential sowie Nutzerinnen und Nutzern

Der aktuelle Prozess sieht vor, dass der elektronische Einkommensnachweis nur nach Vorzeigen der Basis-ID mittels eines QR-Codes abgeholt werden kann. Nichtdestotrotz besteht in SSI-basierten Systemen grundsätzlich die Herausforderung, die Bindung zwischen Nutzenden und der Wallet herzustellen, sodass nur rechtmäßige Nutzerinnen und Nutzer Zugriff auf die gespeicherten Nachweise haben.

Performanz, Skalierbarkeit und Stabilität

Im Produktiveinsatz müssen, verglichen mit der Testumgebung, erheblich höhere Anforderungen hinsichtlich der Performanz, Skalierbarkeit und insgesamten Stabilität des Systems erfüllt werden. Bislang ist unklar, inwieweit diese Anforderungen eingehalten werden können. Erste Ergebnisse des Projekts „Schaufenster Sichere Digitale Identitäten“ zeigen, dass die Anzahl der ausgestellten Verifiable Credentials pro Sekunde durch Agents eine Limitation SSI-basierter Systeme darstellen kann.[12] Bislang ist noch offen, wann mit einer Verbesserung der Performanz von Agents gerechnet werden kann.

Neben der Performanz von Agents muss auch die Performanz der Verifiable Data Registries sichergestellt werden. Bisherige Forschungsergebnisse haben grundsätzlich Limitationen hinsichtlich der Performanz und Skalierbarkeit von Blockchains aufgezeigt (siehe auch Sedlmeir et al. 2021). Im vorliegenden System ist allerdings von Vorteil, dass lediglich Datenpunkte mit geringer Größe sowie in limitierter Menge auf einer Blockchain festgehalten werden (u.a. öffentliche Sig-

[12] Die Ergebnisse bisher durchgeführter Performanz-Tests sind unter folgendem Link abrufbar: https://github.com/lissi-id/acapy-load-test-results

naturinformationen des Issuers, Verifiable Credential Definitions sowie Schemas und Gültigkeiten). Eine Last könnte durch das regelmäßige Veröffentlichen des Akkumulators für den Rückruf von Verifiable Credentials entstehen. Dies ist unter anderem von den rechtlichen Anforderungen an den Widerruf von Verifiable Credentials, welche an ein bestimmtes Vertrauensniveau geknüpft sind, abhängig. Im Fall von relevanten Limitationen der Performanz und Skalierbarkeit kann auch auf zentrale Serversysteme als Alternative zur Blockchain-Technologie als zugrundeliegende Infrastruktur zurückgegriffen werden (siehe auch Bundesamt für Sicherheit in der Informationstechnik 2021a).

7.3. Funktionale Weiterentwicklung

Delegation

Aus fachlicher Sicht gehören zu den funktionalen Erweiterungen einer SSI-basierten Nachweisplattform Stellvertreterregelungen bzw. Bevollmächtigungen, da diese im Umfeld der Steuerverwaltung von großer Relevanz sind. Regelmäßig erteilen Steuerpflichtige Vollmachten in Steuersachen. In diesem Fall müsste zumindest ein an Steuerberaterinnen und Steuerberater übermitteltes Verifiable Credential an die Steuerpflichtigen weiterübermittelt werden können (siehe auch Kapitel 8). Dieses Problem betrifft auch grundsätzlich die gesetzliche Vertretung von Minderjährigen sowie von juristischen Personen wie Kapitalgesellschaften. Während auf noch keine ausgereifte technische Lösung gesetzt werden kann, wird aktuell in SSI Konsortien an Stellvertreterregelungen gearbeitet, da sie für eine Vielzahl von Anwendungsfällen von Relevanz sind.

Revocation von Credentials

Für den produktiven Einsatz von SSI-basierten steuerlichen Nachweisdokumenten sind Mechanismen zur Revocation unerlässlich. Im vorliegenden Beispielanwendungsfall können diese beispielsweise zum Einsatz kommen, wenn ein Steuerbescheid geändert wird. Dabei sollte das Zurückrufen von Verifiable Credentials auch durch Nutzer ausgelöst werden können, beispielsweise im Fall des Missbrauchsverdachts (siehe auch nachfolgend Verlust der Wallet). Während das Zurückrufen von Verifiable Credentials mit den im Projekt verwendeten Protokollen bereits möglich ist, sollte dies auch bei einer Weiterentwicklung dieser bedacht werden.

Recovery bei Verlust der Wallet

Der Verlust von Wallets und dem damit assoziierten Schlüsselmaterial kann unterschiedliche Ursachen haben: Ein verlorenes Smartphone, Diebstahl oder auch physische Einflüsse wie beispielsweise ein Brand können dazu führen, dass eine Wallet nicht mehr nutzbar ist und eine andere (bereits bestehend oder neu generierte) Wallet genutzt werden muss. Im Fall von Diebstahl besteht zudem die Gefahr, dass ein böswilliger Nutzer die Wallet bzw. die Verifiable Credentials missbraucht. Um dies zu verhindern, müssen Mechanismen geschaffen werden, eine Wallet zurückzuziehen und anschließend mit geringem Aufwand eine neue Wallet nutzbar zu machen.

7.4. Nutzerakzeptanz

Zukünftige Umsetzungen sollten sich gezielt an den Bedürfnissen der Bürgerinnen und Bürger orientieren, um somit auch eine Grundlage für eine rasche Massenadoption zu schaffen. Hierzu wurden bereits während des Projektes NESSI fünf semi-strukturierte, qualitative Interviews mit Teilnehmerinnen und Teilnehmern durchgeführt, die nicht an dem Projekt NESSI beteiligt waren. Diese Interviews beinhalteten einführenden Fragen, offene Fragen zum Prozess des SSI-basierten Systems sowie eine Einordnung von Akzeptanzfaktoren. Die Ergebnisse der Studie erlauben eine positive Einordnung des Prozesses bzgl. der Verbesserung zum Status quo sowie der Nutzerfreundlichkeit.

Dabei haben die Teilnehmerinnen und Teilnehmer der Studie oftmals betont, dass eine allumfänglich positive Nutzererfahrung von großer Relevanz für die Nutzung des Systems ist. Diese beinhaltet die Akzeptanzfaktoren des intuitiven Designs des Systems, der Schnelligkeit der Anwendung, der Unabhängigkeit von genutzten Geräten sowie der Abwesenheit von Medienbrüchen. Tabelle 2 gibt einen Überblick über die Einflussfaktoren der Nutzerakzeptanz.

Bezüglich der Schnelligkeit des Systems weist der Prototyp noch Verbesserungspotentiale auf. Durch die Teilnehmerinnen und Teilnehmer wurde auch durchweg betont, dass der Nutzen des entwickelten Systems mit der Anzahl der Anwendungsmöglichkeiten für den elektronischen Einkommensnachweis erheblich steigt und dies als relevanter Akzeptanzfaktor einzuordnen ist.

Um die langfristige Nutzerakzeptanz des Systems zu maximieren, sollten aus Sicht der Teilnehmerinnen und Teilnehmer insbesondere die Vorteile der Lösung an Gruppen mit unterschiedlicher Affinität für technische Lösungen kommuniziert werden. Auch weitere Informationen in Form von FAQs und Demonstrationsvideos wurden für zukünftige Systeme als sinnvoll eingestuft.

Während die Untersuchung erste Erkenntnisse bezüglich der Nutzerakzeptanz des Systems aufzeigt, sind ihre Ergebnisse aufgrund der kleinen Stichprobe limitiert. Daher sollten weitere Untersuchungen vor der Einführung eines produktiven Systems angestellt werden.

Faktor	Erklärung
Empfundene Nützlichkeit	Die Software wird als nützlich wahrgenommen.
Wahrgenommene Nützlichkeit	Nutzerinnen und Nutzer empfinden den Aufwand, die Nutzung der Anwendung zu erlernen, als gering sowie die Benutzung als einfach.
Vertrauen	Nutzerinnen und Nutzer haben Vertrauen in die Anwendung und die involvierten Parteien.
Regulierung und Betrieb	Die Anwendung wird in angemessener Weise implementiert, betrieben sowie vermarktet.
Privatsphäre und Datenschutz	Nur erforderliche Daten werden angefragt und gespeichert. Diese Daten werden ausreichend geschützt.
Unterstützung	Der entsprechende Anwendungsfall wird nachvollziehbar erläutert. Alle Prozessschritte werden dem Benutzer transparent kommuniziert und er hat die Möglichkeit, Unterstützung zu erhalten.
Nachvollziehbarkeit	Die übertragenen Daten können anschließend überprüft werden.
Verständlichkeit	Der Einsatz und Vorteil der Anwendung sind für Nutzerinnen und Nutzer vor, während und nach der Nutzung nachvollziehbar.
Ergebnisqualität	Technische Funktionalitäten, Verfügbarkeit der Anwendung und korrekte Übertragung der Daten sind gegeben.
Anzahl der Anwendungsmöglichkeiten	Es bestehen vielfache Möglichkeiten zur Nutzung der Anwendung.
Nutzererfahrung	Nutzerinnen und Nutzer empfinden die Anwendung als intuitiv und benutzerfreundlich.
Bisherige Erfahrung	Nutzerinnen und Nutzer konnten in der Vergangenheit Erfahrungen mit der Anwendung sammeln.
Technische Affinität	Nutzerinnen und Nutzer haben eine positive Einstellung zu neuen Technologien und empfindet es als einfach, neue Software zu nutzen.

Tabelle 2: Faktoren mit Einfluss auf die Nutzerakzeptanz

8. Einbindung der Steuerberatung in NESSI

8. Einbindung der Steuerberatung in NESSI

Verifiable Credentials sollen Nutzerinnen und Nutzern ermöglichen, ihre Daten selbst zu verwalten und zu verwenden. Allerdings ist dies nicht immer möglich. So sind regelmäßig insbesondere Minderjährige oder juristische Personen nicht eigenständig handlungsfähig und werden gesetzlich vertreten. Für die Steuerverwaltung sind darüber hinaus Steuerberaterinnen und Steuerberater als Bevollmächtigte der Steuerpflichtigen Ansprechpartner, Übermittler und Empfänger steuerlicher Daten. Auch liegt im Fall einer Mandatierung der Zugang zur Plattform Mein ELSTER in erster Linie bei der Steuerberatung. Deshalb ist die Einbindung von Steuerberaterinnen und Steuerberatern nicht nur bei dem Einkommensnachweis, sondern auch bei (allen) weiteren Bescheinigungen der Steuerverwaltung von zentraler Bedeutung. Zur grundsätzlichen Berücksichtigung der (praxis-)relevanten Aspekte trägt die Bundessteuerberaterkammer als Kooperationspartner in diesem Teil wesentlich zum Projekt NESSI bei.

Unbestritten müssen Lösungen geschaffen werden, um auch in SSI-basierten Systemen der Steuerverwaltung die Möglichkeit der Steuerberaterinnen und Steuerberater zum Handeln für ihre Mandanten sicherzustellen. Eine der vier betrachteten konzeptionellen Möglichkeiten zur Umsetzung in SSI-basierten Systemen stellt die Weitergabe (Delegation) von Credentials dar. Im Folgenden werden unterschiedliche Ausgestaltungsmöglichkeiten für die Interaktion zwischen der Steuerverwaltung, Steuerberaterinnen bzw. Steuerberater und ihrer Mandantschaft konzeptionell betrachtet.

Ein denkbarer Nachweis in Credential-Form, der die (Steuerberatungs-)Vollmacht zum Handeln in Steuersachen gegenüber der Steuerverwaltung verkörpert, wird hier nicht untersucht. Denn diese Bevollmächtigung stellt aus Sicht der Steuerverwaltung ein Massenverfahren dar und unterliegt den Besonderheiten der gesetzlichen Vollmachtsvermutung. Dementsprechend wurde bereits mit dem Abruf der Vollmachtsdatenbank der Steuerberaterkammern ein effektives System etabliert.

8.1. Technische Grundlagen der Credential Delegation

Delegated Credentials (oder auch Chained Credentials) beschreiben Credentials, die durch den ursprünglichen Holder an einen weiteren Empfänger weitergegeben (delegiert) werden. So wird dieser Empfänger auch zum Holder eines Credentials und kann die Daten des „originären“ Credentials verwenden. In diesem Fall verweisen die Daten des delegierten Credentials auf die Quelle des originären Credentials, d.h. auf den Issuer.

Die Kette von delegierten Credentials startet, analog wie in Kapitel 3 beschrieben, bei dem Issuer, hier „Root Attester“ genannt. Dieser erstellt das originäre Credential. Im vorliegenden Anwendungsfall entspricht dies der Steuerverwaltung, welche Credentials über Einkommensdaten erstellt. Die Signatur des Root Attesters kann durch öffentlich zugängliche Informationen (z.B. öffentliche Signaturinformationen) überprüft werden. Nun kann der originäre Holder ein Credential delegieren, indem dieser ein weiteres Credential mit den Inhalten des ursprünglichen Credentials ausstellt. Dieses enthält weiterhin Informationen über die ursprüngliche Quelle der enthaltenen Daten, in diesem Beispiel der Steuerverwaltung. Ziel einer Credential Chain ist, dass die Vertrauenswürdigkeit der Credentials in der nachfolgenden Kette auf der Vertrauenswürdigkeit des originären Credentials beruht. Die Vertrauensbeziehungen im Vergleich zu dem ursprünglichen

Trust Triangle (siehe Kapitel 3) bleiben im Grundsatz weiterhin bestehen: Die Nutzbarkeit des delegierten Credentials hängt somit nicht vom delegierenden Holder, sondern weiterhin von dem ursprünglichen Issuer (Root Attester) ab (siehe Abbildung 5).

Im Vergleich zu dem originären Credential beinhaltet ein delegiertes Credential daher ein zusätzliches Feld, das die Herkunft von Daten, also den Root Attester als Ursprung, beschreibt sowie einen Beweis über die Gültigkeit des Credentials enthält. Somit beinhaltet das delegierte Credential durch dieses Feld eine Verifiable Presentation über die Datenfelder, die aus dem originären Credential stammen.

Dies bedeutet, dass der Root Attester weiterhin das originäre Credential zurückrufen kann, nicht jedoch delegierte Credentials. Diese können nur über ihre jeweiligen Issuer, die Delegierenden, zurückgerufen werden. Daher ist besonders wichtig, dass Verifier immer eine Verifiable Presentation über die Gültigkeit des originären Credentials anfordern. Entsprechende Governance-Mechanismen müssen somit geschaffen werden.

Während die theoretischen Konzepte zur technischen Umsetzung der Credential Delegation existieren, wurden die entsprechenden technischen Bausteine noch nicht entwickelt bzw. umgesetzt.

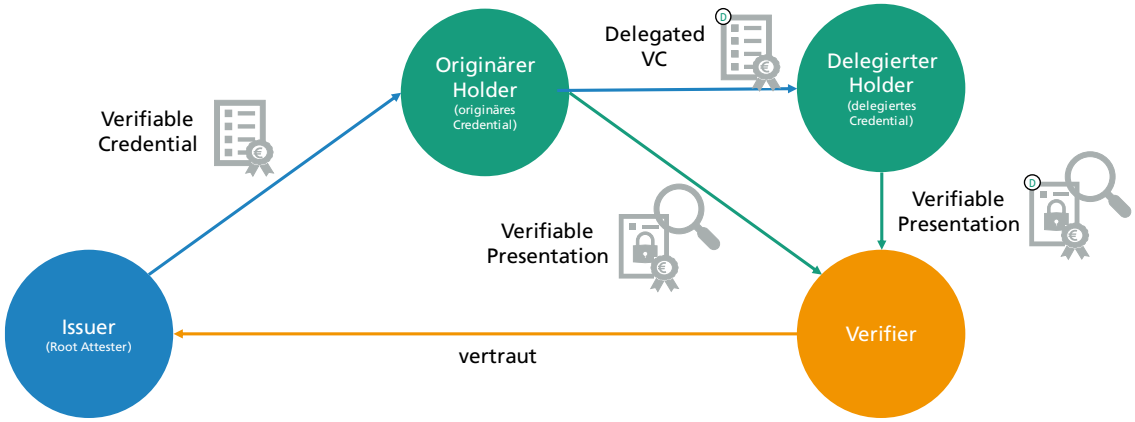


Abbildung 5: Erweiterung des Trust Triangles

8.2. Konzeptionelle Ausgestaltungsmöglichkeiten

Im Fokus der weiteren Ausarbeitung sollen die verschiedenen Möglichkeiten der technischen Einbettung der Steuerberatung in das Projekt NESSI stehen. Hierbei wurden vier Konzepte entwickelt, die sich in ihrem Entwicklungsaufwand, der Integrationstiefe und der zugrundeliegenden Prozesse unterscheiden.

8.2.1. Konzept 1: Weitergabe des Abholungsbescheids

Die erste Alternative zur Einbindung der Steuerberatung stellt nur eine kleine Veränderung zu der in NESSI entwickelten Architektur dar. In dem dortigen Standardprozess wird den Steuerpflichtigen ein Dokument ausgestellt, um das Credential zu erhalten. Alternativ zu diesem Prozessablauf können Steuerberaterinnen und Steuerberater für ihre Mandantschaft das Credential beantragen und das empfangene Abholungsdokument anschließend an die Mandantinnen und Mandanten weiterleiten. Dieses Dokument ermöglicht den Steuerpflichtigen, sich das Credential in die eigene Wallet ausstellen zu lassen (siehe Abbildung 6). Die Berechtigung zu diesem Handeln kann weiterhin über etablierte Kanäle erfolgen.

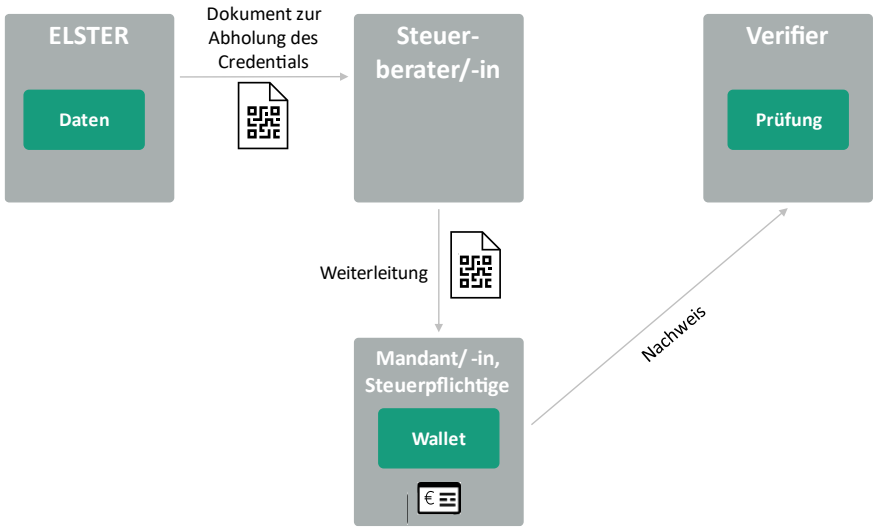


Abbildung 6: Weitergabe des Abholungsbescheids

Denkbar wäre dieser Ansatz insbesondere in solchen Fällen, in denen die Steuerberatung lediglich den Zugang zur ELSTER-Plattform sicherstellt, die jeweiligen Mandantinnen und Mandanten aber gegenüber Dritten autonom auftreten möchten. Vor allem Nachweise, die nicht originär Bescheinigungen aufgrund eines bestimmten steuerlichen Zwecks oder auch steuerliche Stammdatennachweise als Ergänzung von Basisdaten darstellen, könnten als Anwendungsfälle für diese Lösung dienen. Die Übertragung des Credentials in die eigene Wallet sowie die Nutzung liegen allein bei den Steuerpflichtigen selbst, da das Credential weiterhin lediglich auf diese ausgestellt wird. Da die Voraussetzung der Übermittlung des Credentials, der Nachweis einer Basis-ID mit entsprechendem Namen darstellt, können Steuerberaterinnen und Steuerberater das Credential nicht in ihre Wallet laden und damit auch nicht Dritten vorlegen. Dieser Lösungsansatz entspricht daher nicht einer Credential Delegation, dennoch können Steuerberaterinnen und Steuerberater in die Nutzung von SSI-basierten Systemen unkompliziert eingebunden werden.

Der größte Vorteil dieses Konzepts liegt darin, dass im Vergleich zu der bestehenden Architektur keine Änderungen an der entwickelten technischen Infrastruktur vorgenommen werden müssen.

Lediglich eine elektronische Weiterleitung des Dokumentes über einen sicheren Kanal muss ermöglicht werden. Alternativ wäre hier jedoch auch eine persönliche Übergabe eines Ausdrucks möglich.

8.2.2. Konzept 2: Delegation durch Mandantinnen und Mandanten

Der oben beschriebene Ansatz kann durch eine Delegation erweitert werden, sodass auch die Steuerberaterin oder der Steuerberater das durch die Steuerverwaltung ausgestellte Credential nutzen kann. So würde, wie in Konzept 1 beschrieben, der steuerliche Berater bzw. die Beraterin der Mandantschaft ein Dokument zur Abholung des Credentials weitergeben. Nach Erhalt des Credentials können die Steuerpflichtigen dieses an den Steuerberater oder die Steuerberaterin delegieren, d.h. ein eigenes Credential mit denselben, zertifizieren Daten (oder einer Teilmenge) aus dem originären Credential liegt vor und kann im Auftrag der Mandantschaft bei Dritten vorgelegt werden (siehe Abbildung 7). So kann Steuerberaterinnen und Steuerberatern ermöglicht werden, von der Steuerverwaltung attestierte Daten zu nutzen. Denkbar wäre die Nutzung insbesondere dann, wenn das Handeln für die Mandantschaft über Steuersachen hinausgehend erfolgt.

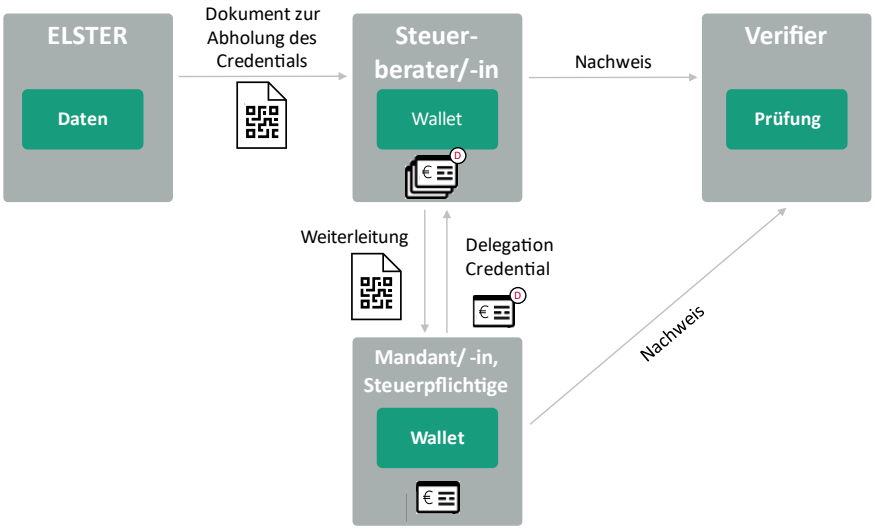


Abbildung 7: Delegation durch Mandantinnen und Mandanten

Durch die explizite Delegation an den Steuerberater oder die Steuerberaterin wird der Nutzung des Credentials grundsätzlich konkludent zugestimmt. Diese Zustimmung könnte von Verifiern im delegierten Credential nachvollzogen werden. Allerdings dürfte die Steuerberatung mit ihrer Mandantschaft explizite Vereinbarungen treffen, in welchen Fällen die Nachweise Dritten vorgelegt werden dürfen. Eine solche Vollmacht könnte wiederum auch in Credential-Form oder in konventioneller Form erfolgen. Die Steuerverwaltung selbst ist nicht mehr in den Delegationsprozess involviert. Wenn diese das Credential zurückzieht, fällt die Gültigkeitsprüfung der im delegierten Credential mitgegebenen Verifiable Presentation nicht mehr positiv aus.

Trotz der grundsätzlich freien Nutzung des Credentials durch den Steuerberater oder die Steuerberaterin besteht eine Abhängigkeit von dem Mandanten oder der Mandantin: Diese können jederzeit das Credential zurückziehen, wodurch es seine Gültigkeit verliert. Die Souveränität und Kontrolle über die Nutzung bleiben somit in der Hand des Mandanten bzw. der Mandantin.

8.2.3. Konzept 3: Direkte Ausgabe an den Steuerberater bzw. die Steuerberaterin

Eine Alternative stellt die Verwaltung des Credentials ausschließlich durch den Steuerberater bzw. die Steuerberaterin dar. Hierbei kann der Steuerberater bzw. die Steuerberaterin das Abholungsdokument beantragen und anschließend selbst zur Ausstellung eines Credentials nutzen (siehe Abbildung 8). Im Gegensatz zu Konzept 1 würde keine Weitergabe des Abholungsdokuments erfolgen. Nun könnte der Steuerberater bzw. die Steuerberaterin für seinen Mandanten bzw. seine Mandantin das Credential für verschiedene Aktivitäten nutzen. Eine solche Ausgestaltung kann insbesondere in den Anwendungsfällen von Relevanz sein, in denen der Mandant oder die Mandantin eine allumfängliche Vollmacht erteilen möchte. Dies ist beispielsweise der Fall, wenn Mandantinnen und Mandanten Kompetenzen weitreichend abtreten oder keine eigene Wallet verwalten möchten. Ähnlich wie in Konzept 1 und 2 aufgezeigt, ist auch hier eine Vollmacht gegenüber der Steuerverwaltung bei Beantragung oder Dritten bei der Nutzung des Verifiable Credentials notwendig.

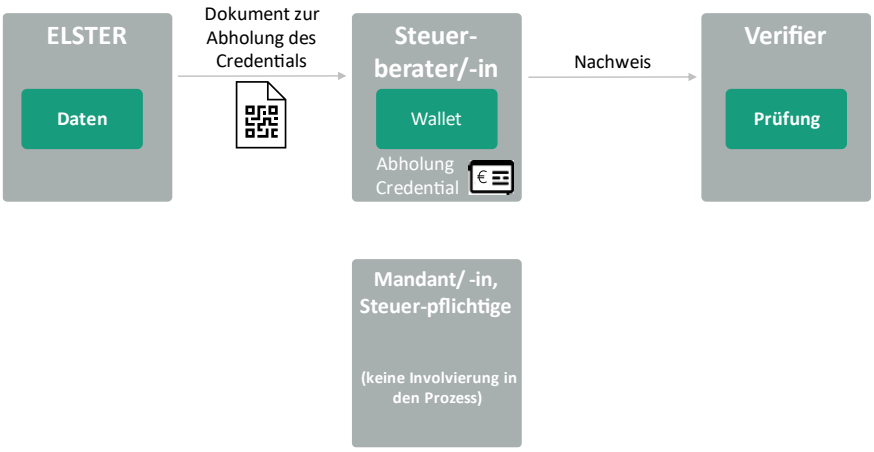


Abbildung 8: Direkte Ausgabe an die Steuerberatung

Nachteilig an diesem Konzept ist allerdings, dass die Mandantin oder Mandant keine Möglichkeit besitzt, das ausgestellte Credential selbst zu nutzen. Auch eine Revocation des Credentials durch die vollmachtgebende Person wäre nur mittelbar möglich, indem diese eine Anfrage bei der ausstellenden Behörde stellt. Das Konzept der Selbstsouveränität ist hier am schwächsten ausgeprägt.

8.2.4. Konzept 4: Direkte Ausgabe an den Steuerberater bzw. die Steuerberaterin mit anschließender Delegation

Eine ergänzende Lösung, die den Herausforderungen von Konzept 3 teilweise entgegenwirkt, wäre die Erweiterung um eine Delegation des Credentials durch den Steuerberater bzw. die Steuerberaterin an den Mandanten bzw. die Mandantin. Hierbei fragt die Steuerberatung weiterhin das Credential direkt ab und überträgt es zunächst zur Verwaltung in die eigene Wallet. Im nächsten Schritt könnte bei Bedarf dieses Credential an den Mandanten bzw. die Mandantin delegiert werden (siehe Abbildung 9). Damit wäre das Credential weiterhin nur mittelbar durch die Mandantschaft zurückziehbar, diese wäre jedoch in der Lage, eine Bescheinigung bzw. ein Nachweis in Form eines delegierten Credentials auch selbst zu nutzen.

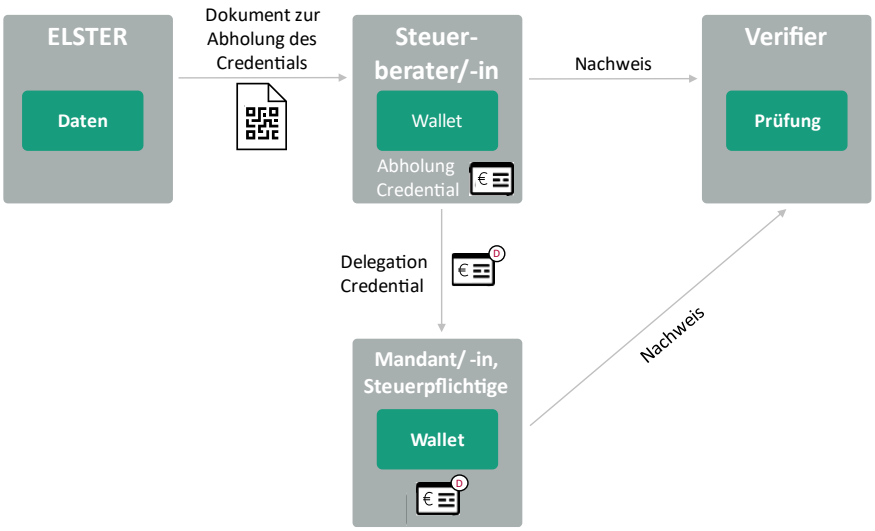


Abbildung 9: Direkte Ausgabe an die Steuerberatung mit anschließender Delegation

8.3. Einordnung der Ausgestaltungsmöglichkeiten

Die Ausgestaltungsmöglichkeiten können anhand unterschiedlicher Kriterien eingeordnet werden.

Erstens variiert der technische Aufwand der Ausgestaltungsmöglichkeiten erheblich. Konzept 1 kann mit geringfügigen Änderungen an der entwickelten Infrastruktur umgesetzt werden, da lediglich das Dokument zur Ausstellung des Credentials über einen sicheren Kanal weitergeleitet werden muss. Auch bei Konzept 3 müssen keine zusätzlichen Funktionalitäten der SSI-bezogenen Komponenten geschaffen werden, da der vorhandene Reifegrad der Technik eine Umsetzung erlauben würde. Allerdings müssten hier solche Prozesse überarbeitet werden, die der Ausstellung des Credentials vorgeschaltet sind: Während aktuell die Basis-ID des Steuerpflichtigen oder der Steuerpflichtigen überprüft wird, müsste nun die Basis-ID des Steuerberaters oder der Steuerberaterin überprüft werden. Somit muss in diesem Prozess zwischen dem Empfänger der Daten und dem Betroffenen unterschieden werden. Dahingegen erfordern die Konzepte 2 und 4 voraussichtlich größere Infrastrukturaufwendungen. So müssen für Konzept 2 die Wallets von Steuerpflichtigen um neue Funktionalitäten erweitert werden, sodass diese ihre Credentials delegieren können. Bis dato besteht die Möglichkeit, Credentials zu delegieren, nicht. Zwar existieren konzeptionelle Entwürfe für diese Funktionalitäten, diese wurden allerdings noch nicht nutzbar implementiert. Ähnlich verhält es sich bei Konzept 4. Auch hier sind erhebliche Entwicklungsaufwände zu erwarten. Allerdings würden im Vergleich zu Konzept 2 nicht die Wallets für Privatpersonen um Funktionen erweitert werden, sondern Enterprise Wallets der Steuerberatung.

Zweitens können die durch die Steuerverwaltung attestierten Daten nicht in allen Anwendungsmöglichkeiten durch den Steuerberater oder die Steuerberaterin genutzt werden. In Konzept 1 besitzt ausschließlich der Mandant bzw. die Mandantin Zugriff auf das Credential. Die Abhängigkeiten gestalten sich entsprechend der Delegation. Während in Konzept 2 eine Abhängigkeit der Steuerberaterinnen und Steuerberater von der Delegation durch Mandantinnen und Mandanten besteht, gilt dies in den Konzepten 3 und 4 vice versa.

Drittens muss bei den aufgezeigten Anwendungsfällen der Einsatz von Vollmachten berücksichtigt werden. Dies gilt insbesondere für die Konzepte 2, 3 und 4, da in diesen Fällen der Steuerberater oder die Steuerberaterin für die Mandantschaft gegenüber Dritten auftritt. Eine solche

Vollmacht könnte wiederum ebenfalls in Form eines Credentials ausgestellt werden. Hier finden sich Ansatzpunkte seitens des Berufstands der Steuerberatung für Projekte im Rahmen der Steuerberaterplattform. Für die Vollmacht gegenüber der Steuerverwaltung erscheint jedoch weiterhin die Nutzung der bestehenden Systeme, wie der Vollmachtsdatenbank der Steuerberaterkammern empfehlenswert, die sich in diesem Bereich bereits als Massenverfahren etabliert haben und durch ein System mit jeweiligen Freigaben der Mandantschaft unnötig verkompliziert werden könnten.

Neben Nachweisen über Einkommensdaten eignen sich viele weitere Bescheinigungen (siehe auch Kapitel 9) für die Ausstellung in Credential-Form, die auch im Bevollmächtigungsfall relevant sein könnten. Hierzu gehören unter anderem Freistellungsbescheinigungen über die Bauabzugsteuer sowie die Bescheinigung über durch Bauunternehmer nachhaltig erbrachte Bauleistungen, die für die Rechnungsstellung gegenüber Leistungsempfängern benötigt werden. Sofern die Steuerberatung zusätzliche Buchführungshilfe übernimmt und somit für die Rechnungsstellung mitverantwortlich ist, kann eine Abwicklung nach Konzepten 3 oder 4 sinnvoll sein. So wären die Bescheinigungen in Form eines Credentials auf die jeweiligen Steuerberaterinnen und Steuerberater ausgestellt und können für die Rechnungsstellung verwendet werden. Die Nichtveranlagungsbescheinigung betrifft insbesondere Privatpersonen. Sofern die Steuerberatung nicht umfassend gegenüber weiteren Parteien neben der Steuerverwaltung (z.B. Banken) auftritt, wäre in diesem Fall Konzept 1 auf Grund seines geringen Umsetzungsaufwandes sinnvoll. So kann der Mandant oder die Mandantin eigenständig die Nichtveranlagungsbescheinigung in Form eines Credentials gegenüber Kreditinstituten vorzeigen. Ähnlich verhält es sich mit der Bescheinigung in Steuersachen, für die Steuerberaterinnen und Steuerberater viele notwendige Informationen liefern können. Da die Mandantschaft die Bescheinigung in Steuersachen in unterschiedlichen Anwendungsfällen (z.B. Eröffnung Gewerbe, Taxikonzession) benötigt, wäre es sinnvoll, wenn diese über das entsprechende Credential verfügen (Konzept 1). In ausgewählten Fällen kann eine Weiterleitung des Credentials an Steuerberaterinnen und Steuerberater sinnvoll sein (Konzept 2), sofern diese für sie weitreichende Handlungsaufträge übernehmen. Ein weiteres Anwendungsbeispiel stellt die erbschaftssteuerliche Unbedenklichkeitsbescheinigung dar. Diese wird durch die Steuerverwaltung ausgestellt, sobald die festgesetzte Erbschaftsteuer bezahlt ist. Da es sich um eine einmalig ausgestellte Bescheinigung handelt, welche die Mandantschaft nur gegenüber der Bank benötigt, wäre es denkbar, dass diese im Rahmen einer umfassenden Mandatierung hinsichtlich des Erbfalls auf die steuerlich Beratenden ausgestellt würden (Konzepte 3 oder 4).

8.4. Ausblick zur Einbindung der Steuerberatung

Die skizzierten technischen Konzepte zeigen eine Reihe von möglichen Ansätzen auf, um Bevollmächtigungen in SSI-basierten Systemen der Steuerverwaltung abzubilden. Dabei hängt der Nutzen der Möglichkeiten maßgeblich von den Anwendungsszenarien ab und es lässt sich nicht allgemein eine überlegene Lösung identifizieren. Durch technisch aufwendigere Delegation erzielen Steuerberaterinnen und Steuerberater insbesondere dann Vorteile, wenn Mandantinnen bzw. Mandanten nicht in den Kontext der Steuerverwaltung eingebunden werden und weitere Geschäftsbesorgungen übertragen möchten. Zudem zeigte die Untersuchung, dass bei einer zukünftigen Umsetzung des Konzepts einige Aspekte beachtet werden müssen.

Erstens sollten kommende Ansätze bestehende Lösungen, wie die Vollmachtsdatenbank, ergänzen und nicht mit bereits in der Umsetzung befindlichen Verfahren und Schnittstellen konkurrie-

ren. Auch in SSI-basierten Systemen wird der Vollmachtsdatenbank eine bedeutende Rolle zukommen, da die Beantragung von Credentials für die Mandantschaft bei der Steuerverwaltung über Vollmachten abgedeckt werden muss.

Zudem bestehen neben Einkommensteuerdaten viele weitere Anwendungsfälle, bei denen SSI-basierte Systeme im Kontext der Einschaltung einer Steuerberaterin oder eines Steuerberaters gegenüber der Steuerverwaltung in Zukunft noch individuell und eingehend betrachtet werden sollten. Hierzu zählt insbesondere auch das Potenzial der Ausstellung von Unternehmensidentitäten über das ESLTER Unternehmenskonto.

Zuletzt sollte auch für Situationen in denen eine Bevollmächtigung nötig ist, die Nutzerfreundlichkeit aus Perspektive der Anwenderinnen und Anwender mitgedacht werden. Denn entscheidend für den Erfolg von SSI-basierten Systemen ist deren breite Akzeptanz, die sich insbesondere um das Thema Interoperabilität dreht. Dies gilt sowohl für die Anbindung an die Plattformen der Steuerverwaltung und die Plattformen der Steuerberatung als auch für eine Kompatibilität der Wallets. Das Projekt NESSI demonstriert dieses Bestreben bereits durch die konsequente Nutzung aktuell verfügbarer Standards bei der Implementierung von SSI-basierten Anwendungen. Diese sollten auch von weiteren Akteuren adaptiert werden, um ein interoperables Ökosystem und medienbruchfreie Prozesse mit einfachen Sign-On-Verfahren zu schaffen. Die Interoperabilität ermöglicht schließlich auch Wettbewerb um die nutzerfreundlichsten Wallets, sodass sich weitere Handlungsfelder und Geschäftsmodelle von privatwirtschaftlichen Organisationen bilden können. Hierzu könnte beispielsweise die Bereitstellung von weiteren Daten in Form von Credentials als Ergänzung zum elektronischen Einkommensnachweis der Steuerverwaltung zählen.

9. Strategische Relevanz von SSI für die Steuerverwaltung

9. Strategische Relevanz von SSI für die Steuerverwaltung

Neben den aufgezeigten Mehrwerten in dem speziellen Anwendungsfall zeigt sich eine starke strategische Relevanz von SSI für die Steuerverwaltung. Diese wird insbesondere im Kontext von Steueridentifikationsnummer, Unternehmensidentitäten und weiteren steuerlichen Nachweisen deutlich.

9.1. Übertragbarkeit auf weitere Nachweisdokumente

Der Nachweis von Identitätsmerkmalen und Eigenschaften ist an vielen Stellen des öffentlichen und privaten Lebens erforderlich. Die Steuerverwaltung dient dabei in vielen Fällen als Aussteller von Bescheinigungen und Nachweisen. Im Unterschied zu bisherigen Papierbescheinigungen bietet die SSI-Technologie für die Steuerverwaltung den Nutzen, dass die Bescheinigungen bei Bedarf elektronisch ungültig gesetzt werden können. Dies führt zu einer erheblichen Verbesserung bei der Prävention von Steuerausfällen und Steuerhinterziehung. Im Folgenden wird ein Auszug dieser Nachweise im Detail erläutert.

9.1.1. Freibestellungsbescheinigung über die Bauabzugsteuer (§ 48ff. EStG)

Bestimmte Leistungsempfänger (Auftraggeber) haben für inländische Bauleistungen einen Steuerabzug in Höhe von 15 % der Gegenleistung einzubehalten. Es muss jedoch kein Steuerabzug erfolgen, wenn im Zeitpunkt der Gegenleistung (Regelfall: Zahlung) eine gültige Freistellungsbescheinigung des Leistenden vorliegt. Der Leistende erhält eine Freistellungsbescheinigung auf formlosen Antrag bei dem zuständigen Finanzamt.

9.1.2. Bescheinigung nachhaltiger Bauunternehmer (§ 13b Abs. 5 S. 2 UStG)

Aufgrund der möglichen Anwendbarkeit des Reverse-Charge-Verfahrens bei Bauleistungen stellt sich für den leistenden Unternehmer in einem Bauvorhaben bei Ausstellung der Rechnung die Frage, wer Schuldner der Umsatzsteuer ist – der Leistende oder der Leistungsempfänger. Grundsätzlich kann davon ausgegangen werden, dass der Leistende der Schuldner der Umsatzsteuer ist. Dies gilt jedoch dann nicht, wenn der Leistungsempfänger ein Unternehmer ist, der nachhaltig Bauleistungen erbringt. Der Leistende kann davon ausgehen, dass der Leistungsempfänger nachhaltig Bauleistungen erbringt, wenn ihm dieser die im Zeitpunkt des Umsatzes gültige Bescheinigung vorlegt. Der Leistungsempfänger kann diese Bescheinigung bei seinem zuständigen Finanzamt beantragen.

9.1.3. Nichtveranlagungsbescheinigung (§ 44a Abs. 2 Nr. 2 EStG)

Die Nichtveranlagungsbescheinigung wird vom zuständigen Finanzamt ausgestellt und bestätigt dem Inhaber, dass dessen künftigen Einkünfte voraussichtlich so niedrig sind, dass keine Einkommensteuer anfällt. Die Grenze, ab welcher eine Nichtveranlagungsbescheinigung ausgestellt wird, bemisst sich am Grundfreibetrag. Der Inhaber kann die Nichtveranlagungsbescheinigung seinem Kreditinstitut vorlegen und diese ermöglicht dann die Auszahlung der Kapitalerträge ohne Abzug der Kapitalertragsteuer. In den genannten Anwendungsfällen könnte SSI einen deutlichen Mehrwert durch verbesserte Nutzererfahrung, höhere Sicherheit und schnellere Prozesse gegenüber den aktuell noch papierbasierten Verfahren ermöglichen. Sollte das Finanzamt Erkenntnisse erlangen, dass der Steuerpflichtige höhere Einkünfte erzielt als ursprünglich angenommen, kann das Verifiable Credential umgehend zurückgezogen werden.

9.1.4. Erbschaftsteuerliche Unbedenklichkeitsbescheinigung (§2 ErbStG)

Ist an einem Erbfall eine ausländische erwerbende Person beteiligt, haften die Banken für die Erbschaftsteuer, wenn sie das von ihnen verwaltete oder verwahrte Vermögen vor Entrichtung der Erbschaftsteuer an ausländische Berechtigte auszahlen oder zur Verfügung stellen. Zur Vermeidung der Haftung fordern die Banken in diesen Fällen eine erbschaftsteuerliche Unbedenklichkeitsbescheinigung an. Die Unbedenklichkeitsbescheinigung erteilt das für die Erbschaftsteuer zuständige Finanzamt, sobald nach Prüfung der Unterlagen, die gegen die ausländische erwerbende Person festgesetzte Erbschaftsteuer bezahlt ist oder festgestellt wird, dass keine Erbschaftsteuer anfällt.

9.1.5. Bescheinigung in Steuersachen

Die Bescheinigung in Steuersachen wird Steuerpflichtigen auf Antrag vom zuständigen Finanzamt ausgestellt und gibt Auskunft über das Verhalten einer Person in Steuersachen. Geprüft werden insbesondere Angaben über Steuerrückstände, das Zahlungsverhalten sowie Informationen über die Erfüllung der Steuererklärungspflichten. Die Bescheinigung kann für die Anmeldung eines Gewerbes erforderlich sein, wenn das Gewerbe der Genehmigungspflicht unterliegt. Dies gilt bspw. für die Ausübung eines Gaststättengewerbes oder die Erteilung einer Taxikonzession.

9.2. Eindeutige Identifizierung bei Unternehmensidentitäten

Für ein umfassendes SSI-Ökosystem ist nicht nur die Identifizierung von natürlichen Personen, sondern auch von Unternehmen notwendig. Eine derartige Basis-ID für Unternehmen stünde im Zentrum eines SSI-Ökosystems. Die Steuerverwaltung erfüllt im Grundsatz strukturell die Voraussetzung, Unternehmensidentitäten zu bescheinigen, da ab der steuerlichen Registrierung entsprechende Daten vorliegen und mit dem ELSTER Unternehmenskonto bereits ein Anknüpfungspunkt für eine digitale Ausstellung besteht. Dementsprechend liegt gerade in dieser Anwendung eine Chance für eine strategische Positionierung der Steuerverwaltung.

Eine Ausstattung mit SSI-basierten Unternehmensidentitäten würde Unternehmen erlauben, (potenzielle) Geschäftspartner vor Abschluss von Geschäften eindeutig zu identifizieren und die Gültigkeit derer Identitäten zu überprüfen. Langfristig würde das Stammdatenmanagement in der Lieferkette deutlich durch qualitativ hochwertige bereitgestellte Daten profitieren und direkte Einsparungen für Unternehmen bedeuten. Eine Ergänzung des Ökosystems um weitere Nachweise ist dabei denkbar und kann zusätzlichen Mehrwert liefern: Beispielsweise können Banken eben-

falls Verifiable Credentials für Unternehmen ausstellen. Diese Unternehmen könnten dann mithilfe jener Verifiable Credentials Zahlungsinformationen mit ihren Kunden teilen. Ein Verifiable Credential-basierter Datenaustausch schafft so einerseits die Möglichkeit, Medienbrüche zu vermeiden und die Datenqualität zu erhöhen. Anderseits erlauben die Eigenschaften von SSI-basierten Unternehmensidentitäten, Geschäfte mit betrügerischen Unternehmen zu vermeiden. Betrügern würde es durch den Einsatz von sicheren digitalen Unternehmensidentitäten erschwert, sich fälschlicherweise als ein anderes Unternehmen auszugeben. Somit könnte ein SSI-Ökosystem die Steuerverwaltung und andere Behörden in der (Steuer-)Betrugsbekämpfung unterstützen.

9.3. Relevanz der Steueridentifikationsnummer

Die Steueridentifikationsnummer wird künftig in der öffentlichen Verwaltung eine immer größer werdende Rolle spielen. Schon heute nutzen Bürgerinnen und Bürger diese nicht nur für die direkte Kommunikation mit der Steuerverwaltung, sondern müssen diese auch bei Kreditinstituten zur Kontoeröffnung oder auch bei der Beantragung von Sozialleistungen vorlegen. Im Kontext des Onlinezugangsgesetzes (OZGs) mit dem Ziel, bis Ende 2022 eine Großzahl von Verwaltungsleistungen digital anbieten zu können, spielt die Steueridentifikationsnummer eine tragende Rolle. Denn die Umsetzung des OZGs soll mithilfe des beschlossenen Registermodernisierungsgesetzes erfolgen, das eine eindeutige Identifizierung der Bürger mithilfe der Steueridentifikationsnummer vorsieht. Deshalb sollte die Steueridentifikationsnummer im Rahmen von digitalen Verwaltungsleistungen deutlich öfter als bisher abgefragt werden. SSI könnte hierbei eine Schlüsselrolle spielen, da durch die Nutzung von Verifiable Credentials die Steueridentifikationsnummer mit einer hohen Datenqualität bereitgestellt werden kann. Zudem können Bürgerinnen und Bürger diese zur Authentifizierung verwenden. Um auf die kommenden Entwicklungen und den Bedarf der Verwaltung in Deutschland vorbereitet zu sein, bietet es sich dementsprechend an, die Kompetenzen für Ausstellung und Empfang von Verifiable Credentials bereits jetzt aufzubauen.

10. Fazit

10. Fazit

Die Notwendigkeit von digitalem Identitätsmanagement und der Möglichkeit, elektronische Nachweise verlässlich einsetzen zu können, wurde politisch erkannt und durch den Vorschlag eIDAS 2.0 der EU-Kommission sowie die Förderung von Schaufensterprojekten auf Bundesebene adressiert. Vor diesem Hintergrund leistet das Projekt NESSI des Bayerischen Landesamts für Steuern wichtige Pionierarbeit mittels einer Plattformlösung zum Einsatz von SSI für den Nachweis von Einkommensdaten. Dabei zeigen die Ergebnisse, dass immer noch technische Herausforderungen für den Produktiveinsatz bestehen. Hierzu zählt eine relativ geringe Skalierbarkeit, da sich die zum Einsatz kommenden Softwarekomponenten noch in einem vergleichsweise jungen Entwicklungsstadium befinden. Auch konnten Fragen zur IT-Sicherheit bislang noch nicht abschließend geklärt werden, wobei eine Bewertung durch das Bundesamt für Sicherheit in der Informationstechnik in Zukunft erwartet wird. Die großen (ökonomischen) Chancen eines zukünftigen SSI-basierten Ökosystems stehen aktuell noch im Kontrast zu diesen ungeklärten Herausforderungen. Auf der einen Seite bringen elektronische Einkommensnachweise die Digitalisierung entscheidend voran und lassen entscheidende Komfort- und Effizienzgewinne erwarten, ohne im Widerspruch zu einem europäischen Verständnis von selbstbestimmter Datennutzung zu stehen. Auf der anderen Seite verdeutlicht dies auch die notwendige Sorgfalt, die in die Implementierung und spätere Nutzung solcher Systeme fließen muss. So kann der ungeschützte Zugang zu einem Smartphone in Zweifelsfall bedeuten, dass Unbefugte Zugriff auf alle Identitätsinformationen einer Person bekommen. Auch weitere Angriffsszenarien sind denkbar. Deshalb sollte mit Blick auf die Zukunft der Adressierung dieser Schwachstellen und möglicher Angriffsszenarien ein hoher Stellenwert eingeräumt werden.

Der Einsatz von SSI in der Steuerverwaltung lässt sich nicht durch einen einzelnen Anwendungsfall rechtfertigen. Daher soll sich die im Projekt NESSI entwickelte Plattform zukünftig nicht auf elektronische Einkommensnachweise beschränken. Entsprechend wurde mit einer generischen Eingabeoberfläche bereits eine technische Basis für weitere Anwendungsfälle geschaffen, sodass unterschiedlichste Informationen den Nutzerinnen und Nutzern als Verifiable Credential ausgegeben werden können. In der Bescheinigung von Unternehmensidentitäten mit dem SSI-Konzept liegt erhebliches strategisches Potenzial für die Steuerverwaltung.

11. Literaturverzeichnis

- Bargstädt-Franke, Silke (2021): Bewertung Hotel Check-in Pilot. Hg. v. Bundesamt für Sicherheit in der Informationstechnik. Online verfügbar unter https://fragdenstaat.de/dokumente/141932-bmi_idwallet/, zuletzt geprüft am 15.02.2022.
- Bundesamt für Sicherheit in der Informationstechnik (2021a): Eckpunktepapier für Self-sovereign Identities (SSI). unter besonderer Berücksichtigung der Distributed-Ledger-Technologie (DLT). Online verfügbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Krypto/Eckpunkte_SSI_DLT.html, zuletzt geprüft am 15.02.2022.
- Bundesamt für Sicherheit in der Informationstechnik (2021b): Kryptographische Verfahren: Empfehlungen und Schlüssellängen. BSI TR-02102-1, 21.03.2021. Online verfügbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102.pdf?__blob=publicationFile, zuletzt geprüft am 16.11.2021.
- Finck, M. (2018): Blockchains and Data Protection in the European Union. In: *European Data Protection Law Review* 4 (1), S. 17–35. DOI: 10.21552/edpl/2018/1/6.
- Fridgen, G.; Guggenmos, F.; Lockl, J.; Rieger, A.; Urbach, N.; Wenninger, A. (2019): Entwicklung einer datenschutzkonformen Blockchain-Lösung im deutschen Asylprozess – Pilotierung im Kontext der AnkER- Einrichtung Dresden. Hg. v. Projektgruppe Wirtschaftsinformatik des Fraunhofer-Instituts für Angewandte Informationstechnik FIT, Bundesamt für Migration und Flüchtlinge (Nürnberg).
- Hühnlein, Detlef; Korte, Ulrike (2006): Grundlagen der elektronischen Signatur. Recht Technik Anwendung. Hg. v. Bundesamt für Sicherheit in der Informationstechnik. Online verfügbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ElekSignatur/e-sig_pdf.pdf?__blob=publicationFile, zuletzt geprüft am 16.11.2021.
- Lyons, Tom; Courcelas, Ludovic; Timsit, Ken (2018): Blockchain and the GDPR. A thematic report prepared by the European Union Blockchain Observatory and Forum. Online verfügbar unter https://www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf, zuletzt geprüft am 26.04.2022.
- Marnau, Ninja (2017): Die Blockchain im Spannungsfeld der Grundsätze der Datenschutzgrundverordnung. In: M. Eibl und M. Gaedke (Hg.): INFORMATIK 2017. Bonn: Gesellschaft für Informatik, S. 1025–1036.
- Quiel, Philipp (2018): Blockchain-Technologie im Fokus von Art. 8 GRC und DS-GVO. In: *Datenschutz und Datensicherheit - DuD* (9), S. 566–573.
- Sedlmeir, Johannes; Ross, Philipp; Luckow, André; Lockl, Jannik; Miehle, Daniel; Fridgen, Gilbert (2021): The DLPS: A New Framework for Benchmarking Blockchains. In: *Hawaii International Conference on System Sciences 2021 (HICSS-54)*. Online verfügbar unter https://aisel.aisnet.org/hicss-54/st/blockchain_engineering/4.
- Strüker, Jens; Urbach, Nils; Guggenberger, Tobias; Lautenschlager, Jonathan; Ruhland, Nicolas; Schlatt, Vincent et al. (2021): Self-Sovereign Identity: Grundlagen, Anwendungen und Potenziale portabler digitaler Identitäten. Bayreuth (White paper / Fraunhofer Institute for Applied Information Technology FIT). Online verfügbar unter https://www.fit.fraunhofer.de/content/dam/fit/de/documents/Fraunhofer%20FIT_SSI_Whitepaper.pdf.

- Tönnissen, Stefan; Teuteberg, Frank (2020): DSGVO und die Blockchain. In: *Datenschutz und Datensicherheit - DuD* 44 (5), S. 322–327. DOI: 10.1007/s11623-020-1276-2.