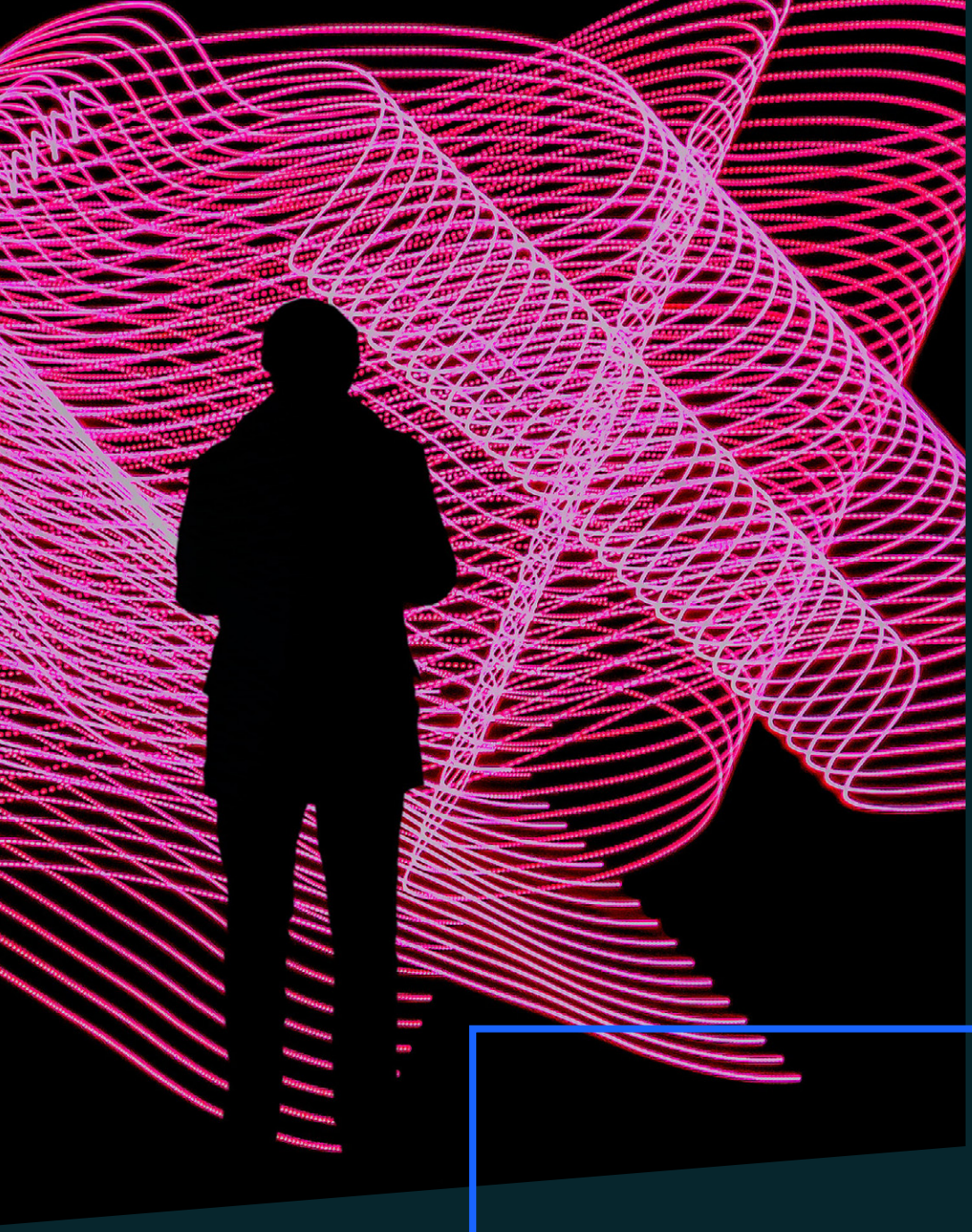


bitkom

Vertrauen stärken

Praktischer Leitfaden zu digitalen Identitäten, SSI & DLT

Herausgeber
Bitkom e. V.
Albrechtstraße 10
10117 Berlin
T 030 27576-0
bitkom@bitkom.org
www.bitkom.org

Ansprechpartner
Benedikt Faupel | Bereichsleiter Blockchain
T 030 27576-410 | b.faupel@bitkom.org

Clemens Schleupner | Referent Digitale Identitäten
T 030 27576-424 | b.faupel@bitkom.org

Verantwortliches Bitkom-Gremium
AK Blockchain & AK Digitale Identitäten

Autorinnen und Autoren
Rayissa Armata | IDnow GmbH
Max Beinke | SVA System Vertrieb Alexander GmbH
Dr. Marc Henniges | d-fine GmbH
Frank Hornbach | BWI GmbH
Lennart Kalwa | SVA System Vertrieb Alexander GmbH
Dr. Christoph Krück | SKW Schwarz Rechtsanwälte
Michael Mundt | Esri Deutschland GmbH
Christian Stengel | Deutsche Telekom Security GmbH
Nicklas Urban | Accenture GmbH
Kamal Vaid | SVA System Vertrieb Alexander GmbH

Layout
Katrin Krause | Bitkom e. V.

Titelbild
Fernand De Canne – unsplash.com

Inhalt

1 Einleitung

Aktuelle Identifikationsverfahren im digitalen Raum sind oft umständlich und finden geringe Akzeptanz. Digitale Identitäten bieten Möglichkeiten, diese Prozesse zu vereinfachen und Dienste weiterzuentwickeln. Eine gestärkte Selbstbestimmung sowie die volle Kontrolle über die eigenen Daten passen gut in das übergeordnete, europäische Wertegerüst und zeigen Wege auf, digitale Identifikation für eine Vielzahl von Diensten, Produkten und Plattformen zu nutzen.

Die (Weiter-)entwicklung digitaler Identitäten bringt jedoch für die Nutzenden viele reale Vorteile mit sich, um sich im digitalen Raum sicherer, selbstbestimmter und effizienter bewegen zu können. Die Zeitersparnis in der Kommunikation mit Behörden, beim Eröffnen eines Bankkontos, oder die bessere Übersicht darüber, welche Daten für welchen Identifizierungsprozess online weitergegeben werden, sind nur einige Beispiele. Digitale Dokumente können beispielsweise durch Verschlüsselung gesichert und ortsunabhängig bearbeitet und verarbeitet werden. Durch die Nutzung weiterentwickelter digitaler Identitäten wird hierbei die Komplexität reduziert, da die Bürgerinnen und Bürger keine Kennungen und Passwörter für mehrere Systeme erstellen und verwalten müssen, was den Authentifizierungsprozess vereinfachen kann. Digitale Identitäten können außerdem z. B. auf Basis von Self-Sovereign Identities (SSI) mit starken Sicherheitsmerkmalen wie Multi-Faktor-Authentifizierung und Verschlüsselung ausgestattet werden, die dazu beitragen, die persönlichen Daten der Menschen zu schützen und das Risiko eines Identitätsdiebstahls zu verringern. Mehr noch: Die bereits eingangs erwähnten SSIs selbst sind so konzipiert, dass sie jeder einzelnen Person die Kontrolle über die eigenen Daten geben. Das kann zur Einhaltung der Datenschutz-Grundverordnung (DSGVO) und anderer Datenschutzvorschriften beitragen.

Gleichwohl ist es wichtig, dieses Thema mit Fingerspitzengefühl anzugehen und sicherzustellen, dass das Feedback der Nutzerinnen und Nutzer berücksichtigt wird, um Bedenken hinsichtlich des Datenschutzes und der Sicherheit auszuräumen. Der Einsatz von Sicherheitsmaßnahmen wie Verschlüsselung und Signaturverfahren ist elementar, um das Vertrauen der Menschen in Digitale Identitäten zu stärken und die Einhaltung internationaler Anforderungen wie der neuen Verordnung über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt, kurz eIDAS-Verordnung[1] zu gewährleisten. Das führt letztlich zu mehr Vertrauen und Sicherheit bei der digitalen Identifizierung und Dokumentation.

Das folgende Papier soll einen Überblick über Digitale Identitäten und mögliche Umsetzungskonzepte geben. Dazu werden zunächst die verschiedenen Arten Digitaler Identitäten definiert und verschiedene technische Ansätze zu deren Entwicklung diskutiert. Im Anschluss werden verschiedene Umsetzungskonzepte vorgestellt und bewertet. In einem abschließenden Statement werden mögliche aktuelle Entwicklungen zum Einsatz Digitaler Identitäten skizziert.

1 »Neue eIDAS Verordnung schafft praktische Werkzeuge für die Digitalisierung«. Bitkom e. V.. 20. Juli 2023. ↗https://www.bitkom.org/Themen/Datenschutz-Sicherheit/Oeffentliche-Sicherheit-Wirtschaftsschutz/eIDAS

2 Digitale Identitäten und Nachweise

In der digitalen Welt von heute werden sowohl für kostenfreie als auch kostenpflichtige Services Benutzerkonten angelegt, die zu Identifikationszwecken der Nutzenden dienen. Somit ergibt sich eine (digitale) Identität, welche durch die Kombination verschiedener Merkmale wie beispielsweise E-Mail-Adresse und Alter charakterisiert wird. Oft werden diese Konten mit weiteren personenbezogenen Informationen wie zum Beispiel der Adresse und dem Geschlecht angereichert. Bestimmte Geschäfte setzen die Echtheit der von den Nutzenden eingetragenen Informationen voraus. So muss eine Altersverifikation vom Dienstleister durchgeführt werden, wenn die Kundin oder der Kunde ein altersbegrenztes Produkt oder Dienstleistung erwerben möchte. Als Legitimationsmittel kann dann bspw. eine videobasierte Legitimation durchgeführt werden. Somit erhält der Dienstleister nicht nur Zugriff auf das Geburtsdatum zur Altersverifikation, sondern auch auf weitere sensible Informationen zum Geburtsort oder der Personalausweisnummer, welche nicht zur Verifikation benötigt werden. Zahlreiche Internetunternehmen bieten das Verwalten von Identitätsdaten als Geschäftsmodell an. Oft sind hier aber zum einen die für das jeweilige Geschäft benötigten Informationen mit diversen anderen Informationen zur Person verknüpft. Zum anderen können, diese Anbieter in vielen Fällen die mitgeteilten Informationen für eigene geschäftliche Zwecke, zum Beispiel zur Werbung, nutzen.

Digitale Identitäten betreffen allerdings nicht nur natürliche Personen, sondern auch Identitäten von Maschinen oder juristische Personen. Diese spielen im Geschäftsleben eine wichtige Rolle. Durch die virtuelle Abbildung der Identität einer Maschine können Wartungsarbeiten beauftragt werden oder Materialien selbstständig bestellt werden. Mit der virtuellen Abbildung einer juristischen Person kann diese online rechtskräftig agieren.

2.1 Typen Digitaler Identitäten

Es gibt verschiedene Arten digitaler Identitäten, die sich prinzipiell in hoheitliche und nicht-hoheitliche Identitäten unterteilen lassen.

Hoheitliche Digitale Identitäten am Beispiel Deutschlands

Der 2010 eingeführte deutsche Personalausweis (PA), der darauf aufbauende »elektronische Aufenthaltstitel« (eAT, eingeführt 2011) und die ebenfalls aus dem PA abgeleitete »eID-Karte für Unionsbürger und Angehörige des Europäischen Wirtschaftsraums« (eID-UB, eingeführt 2020) bieten eID-Funktionen. Diese erlauben es der Anwenderin oder dem Anwender, sich bei eBusiness- oder eGovernment-Dienstleistern über eine Internetverbindung sicher und auf hohem Vertrauensniveau zu identifizieren.

Herausragendes Sicherheitsmerkmal des PA ist ein integrierter Sicherheitschip zur Speicherung des Schlüsselmaterials und biometrischer Daten sowie zur Durchführung kryptografischer Funktionen.

Das Gesamtsystem der verschiedenen hoheitlichen Identitäten wird derzeit um die Smart-eID erweitert. In der Smart-eID liegen die kryptografischen Funktionen des Ausweises nicht auf einer dedizierten physischen Chipkarte vor, sondern werden durch in Mobiltelefone eingebettete Sicherheitselemente in verschiedenen Ausprägungen erbracht.

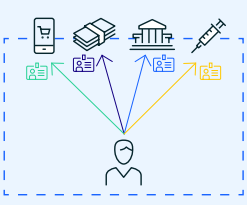
Die oben genannten hoheitlichen eIDs sind technisch weitestgehend identisch gestaltet. Dies ermöglicht die Verwendung einer gemeinsamen eID-Infrastruktur sowohl für die hoheitlichen Anwendungen wie den PA oder den eAT als auch für Anwendungen aus dem eGovernment oder dem eBusiness.

Heute verfügbare sichere Identifizierungslösungen haben bei der Umsetzung entscheidende Nachteile. Sie sind oft schwer zu integrieren, lassen sich mit Bezug auf die verfügbaren technischen Begebenheiten auf den jeweiligen Endgeräten nicht diskriminierungsfrei umsetzen, oder sie scheitern aufgrund der Notwendigkeit zur Geheimhaltung personenbezogener Daten an den hohen Hürden der DSGVO. Verfahren auf Basis von SSI können hier Abhilfe schaffen und die Idee der EU-Brieftasche für digitale Identitäten (EUDI-Wallet) stärken. So unterstützt das Konzept von SSI die Nutzenden dabei, die volle Kontrolle über ihre Identität und Anmeldedaten innerhalb der Wallet zu behalten. Dadurch können sie sowohl frei wählen, welche Attribute an welche vertrauende Partei weitergegeben werden, als auch eine authentifizierte Zustimmung zur Weitergabe der Anmeldedaten geben.

Nicht-hoheitliche Identitäten

Nicht-hoheitliche Identitäten können in drei Arten unterteilt werden:

1. isolierte elektronische Identitäten
2. zentrale und föderierte Identitäten
3. dezentrale Identitäten



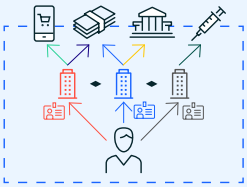
Jede Anwendung hat eine eigene ID, die i.d.R. nicht kompatibel zu den IDs anderer Anwendungen ist.

Anwenderinnen und Anwender müssen sich jede ID merken.

Isolierte Identitäten

In isolierten Systemen mit isolierten elektronischen Identitäten (isolierten eIDs) hat jede Anwendung eine eigene, in der Regel zu anderen Anwendungen nicht kompatible, eID. Die anwendende Person muss für jede einzelne Anwendung eine isolierte eID anlegen. Dies führt zu einer Vielzahl von verschiedenen isolierten eIDs und nicht kompatiblen Insellösungen. Bekannte Beispiele isolierter eIDs sind Name-Passwort-Kombinationen bei Onlineshop oder anderen Online-Anwendungen. Hier müssen sich Nutzende sämtliche Kombinationen merken, sie (offline) hinterlegen oder durch einen Passwortmanager verwalten. Da derartige Passwortmanager oft online zum Beispiel in zentralen eID-Systemen geführt werden, sind alle dort hinterlegten Passwörter in vielen Fällen mit nur einer zentralen Name-Passwort-Kombination gesichert. Zudem lassen sich Passwörter meistens über E-Mail zurücksetzen, sodass ihre Sicherheit darüber hinaus von der Sicherheit des E-Mail-Passwortes abhängt.

Zentrale und föderierte Identitäten



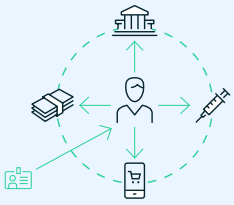
Die ID(s) werden durch einen **zentralen** oder mehrere **föderierte IDPs** bereitgestellt.

Der jeweilige IDP verfügt über sämtliche ID-Daten, mit denen er die Identität **bei jeder Verwendung** gegenüber dem Serviceanbieter bestätigen kann.

Zentrale und föderierte elektronische Identitäten

Ein System mit zentraler elektronischer Identität (zentraler eID) bindet einen Identity Provider (IDP) in die Kommunikation zwischen Anwendenden auf der einen und dem Service Provider (SP) auf der anderen Seite ein. Der IDP verfügt über einen Satz von Zugangsdaten, mit dem er die Identität bei jeder Verwendung gegenüber SPs bestätigen kann. Er steht hier im Zentrum sämtlicher eID-Vorgänge und hat die Möglichkeit, die Verwendung der eIDs zu überwachen und hierauf ein Geschäftsmodell aufzubauen (Stichwort: Big Data). Der Ansatz ist durch verschiedene Kommunikationsstandards wie OpenID-Connect und OAUTH2.0 weitestgehend standardisiert und etabliert. Beispiele für zentrale eIDs sind die Identitäten der großen Plattformbetreiber im Web2.0. Ein Spezialfall der zentralen eIDs sind föderierte elektronische Identitäten (föderierte eIDs). Hierbei handelt es sich um zusammengefasste Identitäten, die sich über verschiedene, sich gegenseitig vertrauende Systeme erstrecken.

Dezentrale Identitäten



Identität wird durch einen Herausgeber bereitgestellt/bestätigt.

Anwender/-innen können die Identität selbst verwalten.

ID-Daten werden **ohne Einbindung** des Herausgebers digital präsentiert.

Dezentrale elektronische Identitäten und SSI

Bei dezentralen elektronischen Identitäten (dezentralen eIDs) wird – einfach ausgedrückt – die eID nicht durch eine zentrale Instanz, sondern durch die anwendende Person verwaltet und kontrolliert. Aus diesem Grund werden dezentrale eIDs als SSI bezeichnet.

Um bestätigte bzw. zertifizierte eID-Informationen von Anwenderinnen und Anwendern in das System zu integrieren, kann eine herausgebende Instanz (Issuer) eingebunden werden, der die Identität entweder über ein Zertifikat in einer Public Key Infrastruktur (PKI) oder über einen dezentralen Identifikator z. B. in einem Blockchain-Netzwerk auf Basis von Distributed Ledger Technologie (DLT) bereitstellt. Eine externe Entität kann die eID-Information dann direkt von der Inhaberin oder dem Inhaber erhalten und über das Zertifikat oder das Blockchain-Netzwerk prüfen.

Ein Ansatz zur Umsetzung dezentraler eIDs sind die sogenannten Verifiable Credentials (VC). Hierbei werden eID-Informationen als »Verifiable Presentations« über eine verteilte Datenquelle (Verifiable Data Registry; VDR) bereitgestellt. Hervorzuheben ist, dass diese ohne den Kontakt zu einem möglichen Herausgeber der eID durch eine externe Instanz (Verifier) prüfbar sind, sodass eine Profilbildung bei einer zentralen Instanz wie dem IDP verhindert oder zumindest erschwert wird.

Für die Umsetzung dezentraler eIDs werden derzeit verschiedene Ansätze wie SSI-Verfahren auf Basis von Blockchains oder zertifikatsbasierte Verfahren auf Basis von PKIs angewendet. SSI werden dabei oft als Synonym für dezentrale Identitäten gebraucht. Nach Herausgabe des Nachweises erlauben SSI es Personen, Organisationen, oder Maschinen, Digitale Identitäten vollständig zu kontrollieren, ohne dass es der Erlaubnis eines Vermittlers oder einer zentralen Partei bedarf. Zudem erlaubt sie die Kontrolle darüber, wie die persönlichen Daten geteilt und verwendet werden.

Der SSI-Begriff wird für verschiedene Dinge verwendet, was eine einheitliche Definition erschwert:

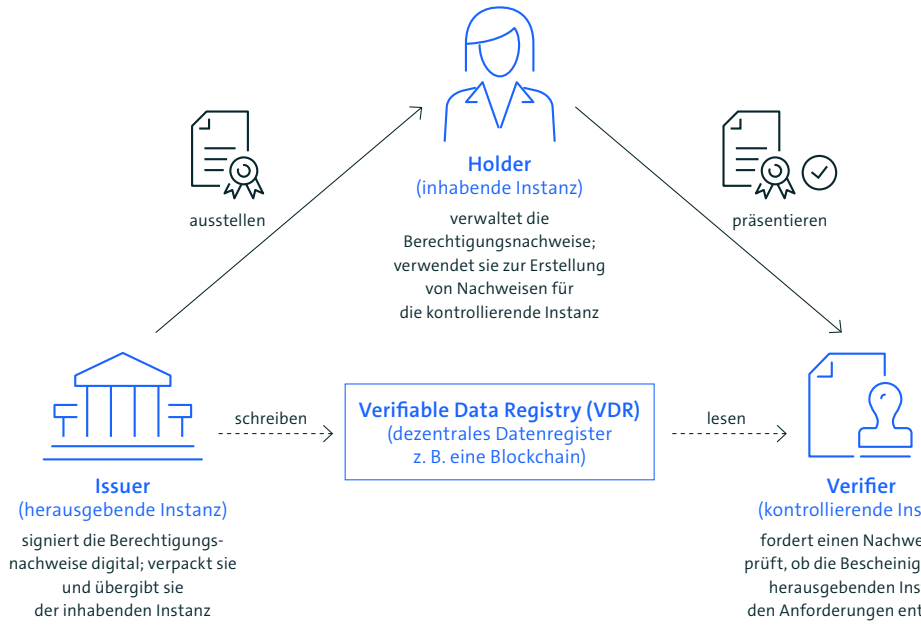
- SSI definiert ein Konzept, bei dem Daten, die eine Entität beschreiben, in der Kontrolle dieser Entität liegen. Eine Analogie aus der physischen Welt beschreibt der Personalausweis, der sich in einer Brieftasche befindet und über dessen Verwendung die Besitzerin oder der Besitzer

selbst entscheiden kann. Das SSI-Konzept greift dies für die digitale Welt auf und beschreibt die Ablage von »Credentials« (Nachweisen) und »Claims« (einzelnen durch Nachweise belegte Behauptungen) in digitalen Wallets.

- SSI definiert darüber hinaus ein Framework, das weitestgehend vom World Wide Web Consortium (W3C), standardisiert wurde und das verschiedene Konzepte und Standards sowie Vorschläge für deren Implementierung einführt, so z. B.:
  - Decentralized Identifiers (DIDs): Identifier, die mithilfe dezentraler, sogenannter »DID Methoden« vergeben werden und die innerhalb eines bestimmten Netzwerkes eindeutig sind. Diese verweisen auf ein DID Document, welches Aufschluss darüber gibt, wie man mit der Entität kommunizieren kann, welche eine solche DID kontrolliert oder durch sie repräsentiert wird.
  - Verifiable Credentials: Nachweise, die mehrere Claims beinhalten können und durch kryptografische Signaturen verifizierbar sind. Eine Überprüfung der Signatur kann dabei Aufschluss darüber geben, ob die Halterin oder der Halter die Daten verändert hat (Authentizität), wer den Nachweis ausgestellt hat (Issuer), ob der Nachweis abgelaufen ist (Gültigkeit) und ob der Nachweis wirklich an die vermeintliche Inhaberin oder den vermeintlichen Inhaber des Nachweises ausgestellt wurde (Zuordnung).
  - Weitere Elemente, z. B. DIDcomm (Kommunikation basierend auf DIDs), wie von der Decentralized Identity Foundation (DIF) spezifiziert, erweitern den W3C-Standard, um z. B. kryptografisch abgesicherte Peer-to-Peer Kommunikationen zwischen DIDs zu ermöglichen.

Das Framework folgt dabei dem Konzept. Der Begriff wird daher oft synonym für beides verwendet.

Ein wichtiger Grundsatz für SSI ist das »Trust Triangle«, welches die drei wichtigen Rollen in SSI kennzeichnet: die herausgebende Instanz (Issuer) von Nachweisen, die inhabende Instanz (Holder) und die kontrollierende Instanz (Verifier):



Während zwischen dem Verifier und dem Holder in diesem Bild in der Regel kein Vertrauensverhältnis besteht, muss der Verifier dem Issuer vertrauen, dass dieser nur rechtmäßige Nachweise ausgestellt hat. Um die Korrektheit des erhaltenen Nachweises zu überprüfen, liest er dafür eine zuvor vom Issuer auf ein VDR geschriebene Signatur, die den Nachweis kryptografisch absichert. Wichtig ist zu erwähnen, dass diese Signatur unabhängig vom ausgestellten Nachweis ist und auch keine Teile des Nachweises auf der VDR gespeichert werden – diese liegen in der Wallet des Holders, wobei je nach Use Case und legalen Anforderungen auch der Aussteller aufbewahren kann.

Damit erreicht SSI, dass

1. persönliche Daten ausschließlich bei den nutzenden Personen liegen,
2. diese selbst entscheiden können, welche Daten sie an Verifier freigeben und mit ihnen teilen,
3. im Falle einer dezentralen SSI, die Infrastruktur des Issuers zum Zeitpunkt der Überprüfung nicht zur Verfügung stehen muss und
4. der Verifier die erhaltenen Daten nach Überprüfung auf Korrektheit nach zusätzlichen eigenen Kriterien validieren kann (z. B., ob das Alter einem geforderten Mindestalter entspricht).

SSI lässt sich damit abgrenzen von anderen digitalen Nachweis- und Identitätsmethoden wie den eingangs erwähnten föderierten Identitäten, der klassischen Nutzer-Passwort-Methode oder auch blockchainbasierten nicht übertragbaren sogenannten »Soulbound Tokens«.

3 Verwendete Technologien

3.1 Distributed Ledger Technologie (DLT)

Der DLT-Begriff beschreibt eine Form von verteilten Datenbanken mit bestimmten Eigenschaften:

Verteiltheit	Dezentralität	Transaktionen	Validierungs-Regeln	Kryptographie	Immutabilität
					
Alle Knoten im Netzwerk enthalten entweder einen Teil oder die Gesamtheit aller Daten (lokale Kopien); eine zentrale Instanz existiert nicht	Die Knoten kommunizieren direkt miteinander, tauschen auf diesen Kanälen Daten aus und sorgen so auf dezentrale Weise für deren Verteilung über das gesamte Netzwerk	Änderungen am Datenstand werden anhand von zustandsverändernden Transaktionen ins Netzwerk eingetragen	Änderungen an den Daten können nur nach bestimmten, vorab fest-gelegten Regeln vorgenommen und über das Netzwerk verteilt werden	In der Regel erfolgt die Absicherung der Daten, Prozesse und Berechtigungen in Form von kryptographischen Signaturen oder Schlüsseln	Sind Daten einmal im Netzwerk gespeichert, können diese nicht mehr verändert werden; damit existiert eine vollständige Protokollierung aller Änderungen (auch Rückbuchungen); man spricht vom »immutable audit trail«

Eine Blockchain beschreibt eine Unterform von DLT, bei der bestimmte Arten der dezentralen Konsensfindung zum Einsatz kommen, die zur Sammlung von gültigen Transaktionen in aneinandergereihten Blöcken führen. Bekannte Beispiele sind hier die Bitcoin- oder die Ethereum-Blockchain.

Gleichermaßen gibt es weniger dezentrale Formen von DLT, bei denen bestimmte zusätzliche Rollen die Gültigkeit von Transaktionen bestätigen müssen, damit sie ins Netzwerk übernommen werden. Beispiele für solche Blockchain-Protokolle sind Hyperledger Indy, R3 Corda oder in gewissen Konfigurationen auch die Ethereum-Software. Der Einsatz einer Blockchain oder zentraler organisierter Versionen von DLT zur Verwaltung digitaler Identitäten ist jedoch nicht zwingend notwendig.

3.2 Public Key Infrastrukturen (PKI)

Eine Public Key Infrastruktur (PKI) ist ein kryptografisches System, das zur sicheren Verwaltung digitaler Identitäten verwendet wird. Sie spielt eine wesentliche Rolle bei der Authentifizierung, Integritätssicherung und Vertraulichkeit von elektronischen Kommunikationen und Transaktionen.

PKIs sind komplexe Systeme mit verschiedenen Komponenten wie Zertifizierungsstellen (Certificate Authorities, CAs), Registrierungsstellen, Zertifikaten, Zertifikatssperrlisten und Benutzerzertifikaten. Die Zertifizierungsstellen sind darin vertrauenswürdige Entitäten, die digitale Zertifikate ausstellen, die die Verbindung zwischen einem öffentlichen Schlüssel und der Identität einer Person oder Organisation herstellen. Die Registrierungsstelle validiert die Identität der antragstellenden Person und überprüft die Informationen, die in das Zertifikat aufgenommen werden sollen. Zertifikate können besonders gut als Träger digitaler Identitäten dienen. Sie ermöglichen ggf. eine pseudonymisierte Speicherung der Identitätsdaten, die nach einer hinreichenden Legitimation an eine kontrollierende Instanz weitergegeben werden.

Hardwaresicherheitsanker sind eine wichtige Grundlage digitaler Identitäten. Wallet-Apps zur Speicherung von SSI und weiterer Daten, die in der Regel als mobile Anwendungen konzipiert sind, benötigen einen sicheren Vertrauensanker für ihre Schlüssel. Bei der Konstruktion dezentraler Identitätssysteme ist daher darauf zu achten, dass die Schlüssel zur Identifizierung auf sichere Hardwarekomponenten der Endgeräte zurückgreifen und Identitätsdaten je nach technischer Ausprägung sicher lokal speichern. Ein Beispiel einer solchen Hardwarekomponente ist das auf Smartphones weit verbreitete Secure Element. Dies ist ein Chip, der auch vom Gerätehersteller nicht einsehbar ist. So kann ein unerlaubtes Kopieren der Daten und damit Datenpiraterie oder Identitätsdiebstahl sicher verhindert werden. Zudem ist eine Absicherung der Daten über ein biometrisches Merkmal wie einen Fingerabdruck und die Sicherung durch eine PIN möglich.

4 Vor- und Nachteile der Typen Digitaler Identitäten

4.1 Die Erwartungshaltung an digitale Identitäten

Die Erwartungshaltung an Digitale Identitäten hängt in erster Linie damit zusammen, was Bürgerinnen und Bürger sowie Unternehmen und Organisationen auf der einen und die Anbieter digitaler Dienste auf der anderen Seite von dem System erwarten. Klar ist, dass für beide Seiten Digitale Identitäten ein Mittel sind, sich sicher in der echten Welt oder im Internet zu identifizieren. So erwarten Bürgerinnen und Bürger in erster Linie eine einfache Installation und eine noch einfachere und intuitive Verwendung Digitaler Identitäten. Jeder weitere Komplexitätsschritt kann dazu führen, dass Digitale Identitäten nicht angenommen werden und damit das Ziel einer flächendeckenden Einführung konterkarieren. Digitale Identitäten wie die deutsche eID müssen auf Smartphones nutzbar sein, da diese Geräte immer mehr das erste Mittel der Wahl beim Zugang zu mobilen Diensten darstellen.
Weitere Anforderungen von Bürgerinnen und Bürgern liegen in einem effektiven Datenschutz sowie dem Schutz der Identität gegen verschiedene Attacken wie unerlaubter Verwendung oder Identitätsdiebstahl. Ein hinreichend hohes Sicherheits- und Datenschutzniveau wird jedoch von den meisten Menschen als notwendig und erfüllt vorausgesetzt, d. h. man möchte sich hierüber keine Gedanken machen müssen. Sicherheit und Datenschutz dürfen die Verwendbarkeit nicht spürbar einschränken, da viele Personen sonst auf einfachere und unter Umständen unsicherere eIDs zurückgreifen.

Seitens der Anbieter digitaler Dienstleistungen besteht die wesentliche Anforderung in einer einfachen Integrierbarkeit in bestehende Anwendungen sowie in der Interoperabilität. eIDs sollen nach Möglichkeit konform zu internationalen Standards sein, langfristig eine Kostenreduktion ermöglichen und den Weg zu neuen digitalen Diensten ebnen.

Aus Sicherheitssicht erwarten die Anbieter IT-Security-by-Design mit ausreichenden Sicherheitsmaßnahmen sowie eine Kryptoagilität. Eine schnelle, möglichst automatisierte Anpassung der Krypto-Systeme soll möglich werden, um eine Migration des Systems bei neuen Anforderungen, z. B. aus der Postquantenkryptografie[2], zu vereinfachen. Zusammenfassend kann festgestellt werden, dass sowohl Bürgerinnen und Bürger als auch die Anbieter digitaler Dienste kryptografische Sicherheit und Datenschutz fordern, die genauen Umsetzungen in vielen Fällen jedoch vielfältige Herausforderungen mit sich bringen. Vor- und Nachteile werden im Folgenden an diesen Erwartungshaltungen gespiegelt.

Unter **Post-Quanten-Kryptografie** versteht man kryptografische Verfahren, von denen angenommen wird, dass sie auch mit Hilfe eines Quantencomputers nicht zu brechen sind.

2 »Post-Quanten-Kryptografie«. Bundesamt für Sicherheit in der Informationstechnik (BSI). 19. Juli 2023. ↗https://www.bsi.bund.de/DE/Service/Impressum/impressum_node.html.

4.2 Vor- und Nachteile föderierter und zentraler Identitäten

In Systemen mit föderierten und zentralen Identitäten wird die eID an zentraler Stelle durch einen IDP oder einen ID-Broker bereitgestellt. Die eIDs in diesen Systemen sind i. d. R. einfach integrierbar, standardkonform zu den jeweiligen IDP-Standards wie OpenID-Connect[3] oder OAuth 2.0[4], universal und modular einsetzbar und komfortabel nutzbar. Über Identifizierungsmaßnahmen, wie zum Beispiel Single Sign-on, können Nutzerinnen und Nutzer leicht mit ihrem Account verknüpfte Daten auf verschiedene Plattformen übertragen.

In der Regel sind zentrale Identitäten nur in Broker- oder in föderierten eID-System Multi ID-fähig und lassen sich aufgrund der Aufstellung der großen, weltweit operierenden IDPs nicht oder nur schwer in Wallet-Systeme integrieren.
Die Sicherheit föderierter und zentraler Systeme hängt entscheidend von ihrem Design ab; sofern die Anmeldung zu den Systemen über eine Softwarelösung oder z. B. über eine Nutzername-Passwort-Kombination erfolgt, kann das Niveau nicht mit hardwarebasierter Sicherheit verglichen werden.

Besonders problematisch ist der Verzicht auf einen großen Teil der digitalen Souveränität jedes bzw. jeder Einzelnen in den meisten zentralen oder föderierten eID-Systemen, da die Anwenderinnen und Anwender ihre Souveränität hier an den IDP abgeben. Zudem ist dieser als zentrale Rolle in sämtliche Vorgänge der Verwendung der eID eingebunden, kann Profile erstellen oder das Verhalten der Anwenderinnen und Anwender im Detail überwachen. Das Geschäftsmodell vieler IDPs basiert daher oft auf Big Data und der Nutzung von Daten, was den Aufbau von unerwünschten Datenoligopolen fördern kann. Hier können Hybridlösungen entgegenwirken.

4.3 Vor- und Nachteile dezentraler Identitäten

Schwieriger werden generelle Aussagen zu dezentralen eID-Systemen. Diese befinden sich derzeit in der Konzeptions-, Spezifikations- und der ersten Umsetzungsphase, vgl. hierzu z. B. das derzeit als W3C-Recommendation vorliegende VC Data Model. Gleiches gilt für die Sicherheit der Systeme, den Datenschutz und nicht zuletzt auch die möglichen Geschäftsmodelle für die Anbieter der eID-Services.
Zentrale Probleme dezentraler Systeme und gerade der Systeme auf Basis von DLT bestehen im Ursprung der digitalen ID bzw. den notwendigen Aushandlungsverfahren, der fehlenden Berücksichtigung etablierter Standards im eID-Umfeld, den derzeit immer noch vorhandenen großen Datenschutzlücken sowie der Umsetzung des Rechts auf Vergessen. Dies beinhaltet die Problematik, dass Relying Parties bei einer Blockchain nicht überprüft werden können, theoretisch also einfacher auf die Identitäten zugegriffen werden kann.

3 »What is OpenID Connect«. OpenID Foundation. 11. May 2023. ↗https://openid.net/developers/how-connect-works/.
4 »Was ist OAuth?«. Digital Guide IONOS. 2022. IONOS SE. 11. May 2023. ↗https://www.ionos.de/digitalguide/server/sicherheit/was-ist-oauth/.

Zu den Problemen einer DLT-basierten eID formuliert das Bundesamt für Sicherheit und Informationstechnik (BSI) in seinem Eckpunktepapier für SSIs die folgenden Kernaussagen:

- SSIs müssen nicht zwingend auf einem DLT-basierten Register beruhen.
- Die Verwendung eines Distributed Ledgers erhöht die Komplexität des Gesamtsystems um Protokolle und Verfahren, für die es bislang keine belastbaren Sicherheitsaussagen gibt.
- Die Sicherheit des Gesamtsystems ist über alle Ebenen sicherzustellen.
- Auch bei der Verwendung von SSI hat die Datensouveränität praktische Grenzen.

Der besondere Vorteil dezentraler Verfahren zeichnet sich jedoch bereits heute ab: Es existiert keine zentrale Rolle des ID-Providers mehr, d. h. Anwenderinnen und Anwender werden in den Mittelpunkt gestellt und behalten Kontrolle über ihre Daten. Beim Design des jeweiligen Verfahrens ist jedoch wie bereits erwähnt darauf zu achten, dass es ein digitales »Recht-auf-Vergessen« gibt und es daher möglich sein muss, Identitäten zu löschen. Dies ist wichtig um dem Fall vorzubeugen, dass aufgrund technischer Fehler oder Cyber-Angriffe personenbezogene Daten auf den VDR geschrieben werden.

Ein weiterer entscheidender Vorteil dezentraler Verfahren ist die Möglichkeit, nur für einen Service relevante Ausprägungen einer Identität weiterzugeben. Dabei werden Identitätsdaten in sog. Claims (z. B. »ich bin als Studierende eingeschrieben« oder »ich bin volljährig«) gespeichert und bereitgestellt.

Abschließend ist festzustellen, dass die SSI-Technologie einen ergänzenden Ansatz zu anderen technologischen und hoheitlichen Standards wie eID und mobilem Führerschein darstellen kann. So könnte eine Form der SSI-Funktion für Anwendungsfälle und vorschriftenübergreifend eingesetzt werden, bei denen ein höheres Sicherheitsniveau nicht erforderlich ist. Die Nutzenden könnten dann je nach Anwendungsfall entscheiden, wann und welche Anmeldedaten sie an wen weitergeben möchten und ob diese lieber in hoheitlicher oder privater Hand liegen sollten.

5 Regulatorische Herausforderungen

Je nach Ausgestaltung des Konzepts und/oder der Technologie können auch regulatorische Anforderungen eine Herausforderung darstellen. So sind etwa bei der Verarbeitung von personenbezogenen Daten die Rahmenbedingungen der EU- DSGVO einzuhalten. Personenbezogenen Daten sind Daten, die einer natürlichen Person zugeordnet werden können, bspw. Name, Adresse, E-Mail-Adresse, Telefonnummer, Kontonummer oder auch die IP-Adresse.
Keine Anwendung findet die DSGVO hingegen grundsätzlich in Fällen der Verarbeitung von Informationen juristischer Personen, also z. B. von Geschäftsbezeichnungen oder -adressen. Ähnliches gilt für Information, die ausschließlichen Maschinen zugeordnet werden können. Auch hier wird man in der Regel keinen Bezug zu einer natürlichen Person herstellen können, sodass z. B. Identifikationsnummer von Maschinen nicht in den Anwendungsbereich der DSGVO fallen.

Wenn die DSGVO auf das jeweilige Konzept Anwendung findet, kann sich etwa das Problem ergeben, dass die betroffene Person grundsätzlich einen Anspruch auf jederzeitige Löschung der verarbeiteten personenbezogenen Daten hat. So kann es unter Umständen schwieriger sein, diesen Anspruch mit dem Konzept der Blockchain-Technologie in Einklang zu bringen.

Der Digital Markets Act (DMA) der Europäischen Kommission ist ein weiterer wichtiger Aspekt, der die Verbreitung Digitaler Identitäten deutlich erleichtern kann. Der DMA, d. h., »das Gesetz über digitale Märkte«, dient zur Regulierung großer Plattformbetreiber, die als Gatekeeper im Internet fungieren und ihre Dienste sowohl Endkunden als auch Dritten bereitstellen. Der DMA soll z. B. gewährleisten, dass Dritte in bestimmten Situationen mit den eigenen Diensten des Gatekeepers zusammenarbeiten und auf Daten des Gatekeepers zuzugreifen können. Außerdem soll der DMA die Nutzung der Plattformfunktionen für Dritte ermöglichen. Mit dem DMA soll u. a. einer weiteren Monopolbildung im Bereich Digitaler Identitäten vorgebeugt werden.

6 Use Cases

6.1 Fahrzeugbezogene Nachweise

Der Lebenszyklus von Kraftfahrzeugen (Kfz) wird von einer Vielzahl verschiedener Nachweise wie z. B. dem Fahrzeugbrief und -schein, dem Scheckheft oder dem Nachweis von Haupt- und Abgasuntersuchung begleitet. In den meisten Fällen sind diese Nachweise papierbasiert und verfügen über stark unterschiedliche Level an eingesetzten Sicherheitsmerkmalen. Während hoheitliche Nachweise wie der Fahrzeugschein auf speziellem Papier gedruckt und gesiegelt ist, verfügen Scheckhefte oder der Bericht der Haupt- und Abgasuntersuchung über keine derartigen Sicherheitsmerkmale. Diese werden mittels Unterschrift und Stempel »abgesichert« und zumeist im IT-System des jeweiligen Ausstellers (z. B. der Werkstatt) erfasst. Im Falle des späteren Verkaufs des Kfz ist es der Käuferin oder dem Käufer jedoch nur schwer möglich, die Echtheit und Originalität dieser zu validieren. Diese können jedoch einen erheblichen Einfluss auf den Kauf und Wert des Fahrzeuges haben.

Während die Nachweisdokumente zumeist mehrere Arten von Daten beinhalten, lassen sich die einzelnen Nachweise ihrer Natur nach grob in drei Kategorien unterteilen:

- Dauerhafte Nachweise von Kfz-spezifischen Eigenschaften entlang des gesamten Lebenszyklus, wie z. B. Fahrzeuggewicht, Antriebsart, Achsabstand – gegenwärtig Teil des Fahrzeugscheines.
- Temporäre Nachweise wie der aktuelle Halter eines Kfz, die sich entlang des Lebenszyklus beliebig oft ändern können.
- Zustands- bzw. ereignisbasierte Nachweise wie eine Haupt- und Abgasuntersuchung oder Inspektion, die u. U. gleichzeitig auch den Kilometerstand miterfassen.

Vor diesem Hintergrund bietet sich die Ausstellung dieser Nachweise nativ, verifizierbar und digital an.
Für die hoheitlichen Nachweise wie der Fahrzeugbrief ließe sich damit die weitere Digitalisierung der öffentlichen Verwaltung fördern. Ein Teil der Kfz-bezogenen Verwaltungsdienstleistungen sind bereits online möglich. Berlin bietet u. a. die Fahrzeugumschreibung als Onlineantrag an. Der neue Fahrzeugschein wird im Anschluss per Post versendet. Eine Ausstellung als VC in die Wallet der Fahrzeughalterin bzw. des Fahrzeughalters würde den Medienbruch eliminieren und die Grundlage für die vollständige Digitalisierung weiterer Folgeprozesse ermöglichen.

In diesem Kontext lässt sich die Brücke zum Large Scale Pilots (LSPs) Programm für Digitale Identitäten der Europäischen Union (EU) schlagen. Ziel der EU ist der Aufbau einer europaweiten, interoperablen Lösung für Digitale Identitäten. Als Teil der LSPs arbeiten derzeit vier Konsortien aus staatlichen sowie privatwirtschaftlichen Akteuren an der Umsetzung und Erprobung verschiedener Anwendungsfälle. Einer davon ist die

Nutzung des »Personal Identifier«. Dieser ist vergleichbar mit einem digitalen Personalausweis, für die Identifizierung und Authentifizierung von Bürgerinnen und Bürgern für Onlineservices der öffentlichen Verwaltung. Sobald ein »Personal Identifier« implementiert ist, wäre eine Erweiterung der Lösung um die Ausstellung und Speicherung weiterer Nachweise denkbar. Die technischen Grundlagen in Form von QEAA (Qualified Electronic Attestation of Attributes)-basierten Nachweisen wird in der Umsetzung bereits mitberücksichtigt.

Parallel zu den oben beschriebenen hoheitlichen Nachweisen können VC zudem einen großen Mehrwert in der Privatwirtschaft in den Bereichen der Zustands- bzw. Ereignisbasierten Nachweise erbringen. So würde die Durchführung einer Fahrzeuginspektion inkl. Kilometerstand nicht auf Papier im Fahrzeugscheckheft festgehalten, sondern (zusätzlich) ein VC von der Werkstatt direkt in die Wallet der Fahrzeughaltenden ausgestellt. Wird das Fahrzeug später verkauft, kann die potenzielle Käuferin oder der Käufer bspw. mittels einer »Check-App« die Nachweise über die Inspektion validieren (der Prozessablauf ist vergleichbar mit der Validierung der Corona-Impfzertifikate). Fälschungen der Daten bei scheckheftgepflegten Fahrzeugen oder die Manipulation des Kilometerstandes sind dadurch deutlich schwieriger.

Für die Zukunft ist zudem denkbar, dass Fahrzeuge über eine eigene Wallet verfügen und somit eigene Nachweise halten können, um sich gegenüber dritten Diensteanbietern wie Mautstellen oder Ladesäulen selbst ausweisen zu können. Gleiches gilt für das Halten der oben beschriebenen Nachweise für Inspektionen oder dauerhafte, hoheitliche Nachweise. Da diese aufgrund ihrer Eigenschaften inhaltlich an das Fahrzeug und nicht die Halterin oder den Halter gebunden sind, ließen sich diese zusätzlich leicht an eine neue Besitzerin oder einen neuen Besitzer »übertragen«.
Weitere Beispiele sind der EU Battery Passport oder CarPass, womit Daten und Dokumente eines Fahrzeugs zentral aufbewahrt werden sollen.

6.2 DLT-basiertes Zutrittsmanagement in gesicherten Liegenschaften

In abgesicherten Liegenschaften wie Industrieanlagen, Produktionsstätten, Bürokomplexen oder auch militärischen Sicherheitsbereichen wie Kasernen der Bundeswehr gibt es meist aufwändige Regelungen zur Absicherung und Zutrittskontrolle der entsprechenden Infrastrukturen. Der tägliche Personen- und Kfz-Verkehr von Handwerkerinnen und Handwerkern, Dienstleistenden, Geschäftsreisenden oder auch den eigenen Mitarbeitenden des Unternehmens erfordert umfassende und teilweise differenzierte Regelungen. Diese sind durch das Wachpersonal und die Besucherinnen und Besucher zu befolgen. Da papierbehaftete Zugangskontrollen für externe Besucherinnen und Besucher immer noch weit verbreitet sind, werden den verschiedenen Besuchergruppen zweck- und anlassbezogen personalisierte Zutrittsausweise ausgehändigt. Externe Besucherinnen und Besucher einer militärischen Liegenschaft müssen sich auf Basis der gültigen Dienstvorschriften über ein staatliches Ausweisdokument mit Lichtbild identifizieren. Dieser Ausweis ist das zentrale Element einer Personenidentifikation, die am Zugangspunkt jeder Kaserne durchgeführt wird.

Die Konzepte und die Technologien selbstbestimmter, verifizierbarer digitaler Identitätsnachweise können in diesem Anwendungsfall signifikante Mehrwerte liefern und zudem vielfältige Potenziale in weiteren Prozessen und Anwendungsfällen eröffnen. Das betrifft zum einen die effektive Prüfbarkeit der durch eine Besucherin oder einen Besucher vorgelegten Ausweisdokumente, zum anderen den mit der Administration verbundene Arbeitsaufwand, einschließlich der resultierenden Wartezeiten bei den Besuchenden.

Die Möglichkeit einer digitalen Abbildung der heutigen analogen Ausweis- und Zutrittsdokumente durch Identitätsnachweise wie VC und einem VDR auf Basis von DLT wurde bereits in dem Innovationsexperiment »Smart Digital Badge« untersucht. Dieses Experiment war anfänglich auch in das Pilotprojekt »Ökosystem Digitale Identitäten« der Bundesregierung mit eingebettet und wurde nachfolgend eigenständig umgesetzt. Die aktuelle Weiterentwicklung in Richtung einer Pilot-Erprobung mit Echtdaten erfolgt mit Abstützung auf das Förderprojekt IDunion.

Es darf angenommen werden, dass zumindest bei überregional agierenden Unternehmen der Industrie und insbesondere bei Organisationen der öffentlichen Verwaltung teilweise ähnliche Anforderungen bestehen. Vor diesem Hintergrund ist eine vergleichbare technische Umsetzung auf Basis einer gemeinsamen Plattform sinnvoll. Gerade im Verbund auf Ebene B2B (analog auch B2G oder G2G) kann ein Zusammenwirken gleichartiger Lösungen zielführend sein. Das würde eine organisationsübergreifende Wiederverwendung von Identitätsnachweisen, die durch Verbundpartner ausgestellt wurden, erlauben. Plakativ wird dieser Umstand am Beispiel formaler Vertragsparteien deutlich. Die handelnden Personen eines Auftragnehmers benötigen zur Vertragserfüllung oft einen direkten Zugang zu den Liegenschaften des Auftraggebers. Das Anerkennen von verifizierbaren digitalen Ausweisen von Mitarbeitenden des Auftragnehmers durch den jeweiligen Auftraggeber kann beispielsweise Onboarding-Prozesse beschleunigen. Die Verwendung dezentraler Lösungen auf Basis von z. B. DID, VC und DLT könnte hierzu ein belastbarerer Brückenschlag sein.

PKI-basiertes ID- und Zutrittsmanagement in Unternehmen

Das ID- und Zutrittsmanagements kann bei Firmen oder Konzernen auch über eine eigene PKI realisiert werden. Hierzu ist eine PKI-Infrastruktur erforderlich, die unterschiedliche Zertifikatstypen auf Basis des weltweit etablierten X.509-Standards generiert, bereitstellt und verwaltet. Die Zertifikate können unter anderem zur E-Mail-Sicherheit, zum Zutritts- und Arbeitszeitmanagement, bei verschiedenen Druckerdienstleistungen, bei der starken Authentifizierung (Client-Server), bei Remote-VPN oder bei aktiven Netzkomponenten (z. B. Router, Gateways) eingesetzt werden.
Um die Sicherheit der PKI zu gewährleisten, sollte diese in einem sicheren Trust Center betrieben werden und Chipkarten oder vergleichbare hardwarebasierte Token als sicheres Identifikationsmittel unterstützten.

6.3 Know Your Customer (KYC) Online-Kredite

KYC ist die gesetzliche Grundlage für die Identitätsüberprüfung in regulierten Marktsektoren: von Bank- und Finanzdienstleistungen bis hin zur Altersüberprüfung im Einzelhandel, in den Medien oder bei Vertragsabschlüssen. Im Bankwesen erfüllt der KYC-Onboarding-Prozess eine der ersten Anforderungen an die Sorgfaltspflicht gegenüber Kundschaft gemäß den Geldwäsche-Gesetzen auf Bundes- und nationaler Ebene. Eine KYC-Überprüfung ermöglicht es Organisationen, natürliche oder juristische Personen auf Anzeichen von Geldwäsche, oder anderen illegalen Aktivitäten zu überwachen.

Bei einem KYC-Prozess zur Identifizierung und Verifizierung von Kundinnen und Kunden werden persönliche Daten der Nutzenden erfasst. Eine Verifizierung stellt sicher, dass die Informationen der Endnutzenden mit den Daten im offiziellen Ausweisdokument übereinstimmen. In der Regel werden mindestens folgende Informationen erfasst:

- Vollständiger Name
- Geburtsdatum
- Adresse
- Nationalität
- Ausweisnummer
- Ausstellungsdatum und Ablaufdatum des Ausweisdokuments

Je nach Art des Dienstleisters und des Landes können auch weitere Informationen wie Steuernummer, Telefonnummer, E-Mail-Adresse, Beruf, Bankdaten oder andere Identitätsnachweise erforderlich sein. Die erfassten Informationen werden dann überprüft, um sicherzustellen, dass die Kundin oder der Kunde tatsächlich existiert und legitim ist.

Innovationen bei der Fernüberprüfung von Identitäten und fragmentierte Vorschriften

Die Online-Identitätsprüfung in Deutschland, ganz Europa und im Vereinigten Königreich hat sich im Laufe der Zeit von der persönlichen Identifizierung über die Post-Identifizierung und videobasierte Identifizierungen in Begleitung eines spezialisierten Agenten bis hin zum elektronischen Identitätsnachweis über chipbasierte nationale Ausweisdokumente oder die qualifizierte elektronische Signatur entwickelt. Es ist wichtig zu beachten, dass es in verschiedenen Mitgliedstaaten und im Vereinigten Königreich sowie in den einzelnen Marktsektoren unterschiedliche Vorschriften für die Fernidentifizierung von Kundinnen und Kunden gibt. Dies hat zu einer fragmentierten KYC-Landschaft sowohl für Dienstleister als auch für deren Kundschaft geführt. Die Unterschiede bei der Fernidentitätsprüfung (IDV) haben in einigen Fällen zu Einschränkungen bei grenzüberschreitenden Dienstleistungen und regulatorischer Arbitrage geführt.

Eine positive Entwicklung ist, dass Regulierungsbehörden in verschiedenen Mitgliedstaaten sich dazu verpflichtet haben, Innovationen im Bereich der Identitätsprüfung

aus der Ferne zu evaluieren. In Deutschland wurden kürzlich Änderungen des Vertrauensdienstegesetzes (VDG) umgesetzt, welche zertifizierte automatisierte Lösungen im Rahmen der Bundesnetzagentur erlauben. Dies wird sich auch auf das deutsche Telekommunikationsgesetz erstrecken, welches ein neues Zertifizierungssystem für KYC-Anwendungen anbieten wird. Andere Mitgliedstaaten, wie Spanien, erlauben automatisierte Lösungen Geldwäscheprävention mit zusätzlichen Sicherheitsmerkmalen (z. B. mit Video-Streaming der ID-Dokumente und Lebenderkennung). In Frankreich sieht das französische Währungs- und Finanzgesetzbuch vor, dass ein IDV-Fernüberwachungsdienst mit ausdrücklicher Zertifizierung und Genehmigung der französischen Agentur für Cybersicherheit (ANSSI) zulässig ist. ANSSI verlangt ein neues Zertifizierungs- und Genehmigungsverfahren nach ihrem Fernidentitätsstandard, bekannt als Prestataires de verification d'identité à distance (PVID). Die Akzeptanz neuer Innovationen durch die Regulierungsbehörden mittels Zertifizierung, um robuste Sicherheitsanforderungen innerhalb der IDV-KYC-Dienste aufrechtzuerhalten, ist eine willkommene Entwicklung, die eine weitere Harmonisierung der digitalen Dienste ermöglicht.

7 Fazit

In der Debatte um die flächendeckende Ausrollung Digitaler Identitäten, ihrer Vor- und Nachteile, sowie möglicher Anwendungsfälle, kann das SSI-Konzept einen ergänzenden Ansatz zu anderen technologischen und hoheitlichen Standards wie eID und dem mobilen Führerschein darstellen. So gibt es, wie in diesem Leitfaden herausgearbeitet wurde, eine Reihe von Anwendungsbeispielen, bei denen der Einsatz von SSI sinnhaft sein kann. Diese Anwendungen sind bereits zum Teil in die Praxis umgesetzt und kommen in verschiedenen Strukturen erfolgreich zum Einsatz. Die Effizienzsteigerung einzelner Prozesse sowie die stärkere individuelle Kontrolle über die eigenen (personenbezogenen) Daten sind die stärksten Argumente für die anwendungsbasierte Einführung von SSI-basierten Digitalen Identitäten.

Der Herausforderung der punktuellen Weitergabe von Anmeldedaten kann begegnet werden, indem zunächst kontext- oder ökosystemspezifische Anwendungsfälle entwickelt werden. Diese werden erst später und bei Bedarf mit staatlichen IDs kombiniert oder aus staatlichen IDs mit bewährten und neuen Verfahren abgeleitet. Ziele sollten sein,

- dass Bürgerin und Bürger selbst entscheiden können, welche Daten sie oder er an eine verifizierende Instanz weitergeben möchten,
- dass die entsprechenden Verfahren eine unberechtigte Verwendung effektiv verhindern,
- dass keine Personen aus ID-Systemen ausgeschlossen werden können und
- dass ID-Systeme interoperabel funktionieren und auf einem einheitlichen Standard beruhen.

Um das volle Potenzial und den Vorteil dezentraler Identitäten und SSI-basierter Systeme gegenüber föderierten und zentralen Identitäten auszuschöpfen, ist ein hohes Maß an Standardisierung erforderlich. Dies wird derzeit unter anderem durch geförderte Projekte und private Initiativen vorangetrieben. So kann der Bildung von Datenoligopolen wirksam begegnet werden. Der Schlüssel zu einer benutzerfreundlichen und sicheren digitalen Identität sollte flexible Optionen und Benutzerautonomie beinhalten. Hierfür ist auch eine staatliche Regulierung notwendig, welche u. a. die Bürgerinnen und Bürger sowie Organisationen und Unternehmen in die Lage versetzt, individuell über den Umfang an Daten und Informationen, die geteilt werden, zu entscheiden. Die Gefahr einer durch Services erzwungenen Überidentifikation besteht generell bei der Verwendung Digitaler Identitäten. Sie kann jedoch durch gesetzliche Vorgaben minimiert werden.

In Deutschland spielt die SSI-Technologie auf Bundesebene bei der Entwicklung digitaler Identitäten bisher noch keine bedeutende Rolle. Auf europäischer Ebene hingegen wird SSI bereits als mögliche Lösung für die Gestaltung EUDI-Wallet betrachtet. Die EU-Toolbox, das technische Grundgerüst für zukünftige Wallets, ermöglicht derzeit den Einsatz von SSI. Dies wird durch das EWC-Konsortium im LSP-Programm auf Funktionalität und Skalierbarkeit getestet.

SSI wird also auf europäischer Ebene aktiv getestet und kann auch in Deutschland für spezifische Anwendungsfälle genutzt werden. Es ist wichtig, dass Deutschland hier Schritt hält und sich den Entwicklungen anderer europäischer Länder anschließt, um eine Architektur zu vermeiden, die mit

einem Großteil der EU-Länder nicht kompatibel wäre. Indem Deutschland die Nutzung von SSI in der Entwicklung digitaler Identitäten berücksichtigt, kann eine effiziente und kohärente digitale Identitätsstruktur geschaffen werden, die sich nahtlos in den europäischen Rahmen einfügt.

Bitkom vertritt mehr als 2.200 Mitgliedsunternehmen aus der digitalen Wirtschaft. Sie erzielen allein mit IT- und Telekommunikationsleistungen jährlich Umsätze von 190 Milliarden Euro, darunter Exporte in Höhe von 50 Milliarden Euro. Die Bitkom-Mitglieder beschäftigen in Deutschland mehr als 2 Millionen Mitarbeiterinnen und Mitarbeiter. Zu den Mitgliedern zählen mehr als 1.000 Mittelständler, über 500 Startups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Geräte und Bauteile her, sind im Bereich der digitalen Medien tätig oder in anderer Weise Teil der digitalen Wirtschaft. 80 Prozent der Unternehmen haben ihren Hauptsitz in Deutschland, jeweils 8 Prozent kommen aus Europa und den USA, 4 Prozent aus anderen Regionen. Bitkom fördert und treibt die digitale Transformation der deutschen Wirtschaft und setzt sich für eine breite gesellschaftliche Teilhabe an den digitalen Entwicklungen ein. Ziel ist es, Deutschland zu einem weltweit führenden Digitalstandort zu machen.

Bitkom e.V.

Albrechtstraße 10
10117 Berlin
T 030 27576-0
bitkom@bitkom.org

bitkom.org

bitkom