

Digitale Identitäten für digitale Kommunen und Unternehmen

Europäischer Rechtsrahmen für Vertrauensdienste

„Einmal den Ausweis bitte“ heißt es bislang meist, wenn wir ein Bankkonto eröffnen oder einen Reisepass beantragen möchten. Immer mehr Dienstleistungen und Prozesse finden mittlerweile jedoch online statt und durch die zunehmende Vernetzung von Menschen, Daten, Informationen, Geräten und Ressourcen sind Konzepte und Technologien erforderlich, die eine sichere und effiziente Kommunikation im virtuellen Raum ermöglichen.

Sichere, interoperable und nutzerfreundliche digitale Identitäten sind in diesem Zusammenhang ein **zentraler Baustein für die Digitalisierung der öffentlichen Verwaltung und kommunaler Unternehmen** und sind bereits heute – bewusst oder unbewusst – integraler Bestandteil unseres Alltags. Der Einsatz digitaler Identifikationsdienste bietet neben vielen weiteren Sektoren (Finanzwesen, Social-Media, Gesundheitswesen) auch für zahlreiche Anwendungsfelder im kommunalen Umfeld (E-Government, IoT, Smart City, E-Commerce) großes Potenzial, die Effizienz, Transparenz, Nutzerfreundlichkeit und Sicherheit von Prozessen, Dienstleistungen und Infrastrukturen zu steigern.

Für Kommunen und kommunale Unternehmen ist die aktive Auseinandersetzung mit Digitalen Identitäten nicht nur aufgrund der wachsenden praktischen Relevanz von wichtiger Bedeutung, sondern in Anbetracht des europäischen und nationalen Rechtsrahmens zwingend notwendig.

Was sind digitale Identitäten?

Grundsätzlich beschreibt der Begriff „Identität“ die Summe spezifischer Merkmale (Attribute), die einer Entität (Person, Organisation oder Objekt oder Gerät) in einem bestimmten Anwendungskontext zugeordnet werden. Attribute können bspw. Name, Geburtsdatum oder biometrische Merkmale sein, aber auch digitale Attribute wie z. B. Benutzernamen oder Zertifikate.

Das BSI beschreibt den Identitätsbegriff in der Technischen Richtlinie „BSI TR-03107“ wie folgt: *„Die Identität einer natürlichen oder juristischen Person wird durch verschiedene Eigenschaften beschrieben, wie beispielsweise Name, Anschrift, Geburtsdatum, E-Mail-Adressen oder auch Pseudonyme. Identitäten benennen und charakterisieren aber nicht nur Personen, sondern auch Dinge, Ressourcen, Dienste und andere Objekte. In der virtuellen Welt werden Namen und Eigenschaften durch Attribute einer elektronischen Identität abgebildet.“*

Während sich (analoge) Identitäten in der physischen Welt auf physische Merkmale und Dokumente (z. B. Personalausweis oder Reisepass) beziehen, die zur Identifikation in analogen Kontexten genutzt werden können, beschreibt eine Digitale Identität die elektronische Repräsentation einer Entität, die in digitalen Umgebungen genutzt werden kann, um die Entität eindeutig zu identifizieren.

Im Kontext der digitalen Identitäten kann zwischen Personen-, Maschinen-, Software- und Unternehmensidentitäten unterschieden werden, je nachdem welche Entität durch die jeweilige digitale Identität repräsentiert wird.

Eine digitale Identität besteht aus digital erfassten Attributen (z. B. Name, Geburtsdatum, Geschlecht) einer Entität kombiniert mit Berechtigungsnachweisen, den sog. Credentials, die eine Person, eine Organisation oder ein Objekt bzw. Gerät online eindeutig identifizieren. Dies können Benutzernamen, digitale Zertifikate, Passwörter, biometrische Daten und andere spezifische, verifizierbare Informationen sein, aber auch physische Geräte wie Smartcards oder Token.

Zu einer Entität können mehrere digitale Identitäten existieren, die unterschiedliche Rollen einer Entität repräsentieren oder aber für verschiedene Anwendungen, Plattformen oder Netzwerke genutzt werden können. So kann bspw. ein und dieselbe Person als Mitarbeitender, Privatperson oder Unternehmen im digitalen Raum agieren sowie unabhängige Identitäten auf verschiedenen Social-Media-Plattformen besitzen. Gleiches gilt bspw. für IoT Geräte, die einerseits eine Identität zur Kommunikation mit dem Hersteller verfügen und andererseits Zugriff auf ein isoliertes Smart-Home-System haben.

Wie werden digitale Identitäten erzeugt, verwaltet und eingesetzt?

Für die Erzeugung, Verwaltung und den Einsatz digitaler Identitäten existieren unterschiedliche Modelle:

- **Isolierte Identitäten (auch „Silo-Identitäten“)** sind aufgrund der Unabhängigkeit von anderen Diensten und der höheren Kontrolle durch den Dienst gerade in Online-Shops und anderen Web-Diensten weit verbreitet. Jede Plattform oder jeder Dienst verwaltet die Identitäten ihrer Benutzerinnen und Benutzer dabei selbst, sodass Benutzerinnen und Benutzer für jeden Dienst eine separate Identität (z. B. Benutzername und Passwort) erstellen müssen. Da jede Identität getrennt verwaltet wird ist i. d. R. kein einfacher Austausch zwischen den Diensten möglich.
- **Föderierte Identitäten** werden z. B. in Teil II der eIDAS 1.0 (s. Kap. III a) als zwischenstaatliche Lösung definiert, aber auch bspw. in Form von Google- oder Facebook-Log-Ins umgesetzt. Ein oder mehrere zentrale Identitätsanbieter (Identity Provider, IdP) stellen sicher, dass Benutzerinnen und Benutzer sich mit einer einzigen Identität bei verschiedenen Diensten anmelden können, indem sie sich einmal bei einem zentralen Anbieter (z. B. per Single Sign-On, SSO) authentifizieren. Nutzende können sich mit einer einzigen Identität bei verschiedenen Diensten anmelden.
- **Staatliche Identitäten** werden von Regierungsbehörden ausgestellt und verwaltet und dienen der sicheren Authentifizierung und Verifikation von Bürgeridentitäten in digitalen und physischen Kontexten. In der EU wird dies etwa durch eID-Karten oder Bürger-IDs ermöglicht, die als vertrauenswürdige Identitäten für Behörden und bestimmte private Dienste verwendet werden. Staatliche Identitäten basieren meist auf staatlich überprüften Dokumenten wie Personalausweis oder Reisepass. Staatliche Identitäten weisen eine hohe Vertrauenswürdigkeit und Sicherheitsstandards auf und können so auch für sensible offizielle Dokumente und öffentliche Dienste verwendet werden. Die starke Abhängigkeit von staatlicher Infrastruktur und Verwaltung kann sowohl technisch als auch datenschutzrechtlich kritisch betrachtet werden.
- **Self-Sovereign Identities („selbstbestimmte Identitäten“)** basieren auf der dezentralen Organisation von Identitätsdaten und damit der Unabhängigkeit des Nutzenden von einem zentralen Identity-Provider. Die Nutzenden verwalten ihre eigenen Identitätsdaten, d. h. Identitätsmerkmale und Berechtigungen in Form von kryptografisch gesicherten digitalen Nachweisen („Verifiable Credentials“) mittels einer digitalen Brieftasche („Wallet“) selbständig und können selektiv entscheiden, welche Informationen sie mit welchen Diensten teilen. Um sich gegenüber einer Akzeptanzstelle auszuweisen, legen die Nutzenden sog. „Verifiable Presentations“ (VPs) vor, die ohne direkten Kontakt zum Herausgeber überprüfbar sind. Die Kontrolle über die Self-Sovereign-Identities liegt vollständig beim Benutzenden. Dieser entscheidet, welche Informationen mit welchem Dienst geteilt werden. In der Umsetzung sind SSIs komplex. Derzeit arbeiten mehrere Initiativen und Unternehmen daran, das Konzept an den Markt zu bringen.

eIDAS – Ein europäischer Rechtsrahmen für digitale Identitäten

Die **eIDAS-Verordnung** (englisch: electronic IDentification, Authentication and trust Services), in Deutschland auch IVT (elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen) schafft seit ihrem Inkrafttreten am 17. September 2014 (Verordnung 910/2014 (EU)) erstmals einen **einheitlichen Rechtsrahmen für die elektronische Identifikation und Vertrauensdienste in der EU**. In **Kombination mit dem dazugehörigen technischen Rahmenwerk** fördert sie die grenzüberschreitende Anerkennung elektronischer Identitäten und unterstützt sichere digitale Transaktionen. Dabei legt die Verordnung die Voraussetzungen fest, damit elektronische Vertrauensdienste – wie elektronische Signaturen, Siegel, Zeitstempel, Zustelldienste oder Website-Authentifizierung – grenzüberschreitend denselben Rechtsstatus wie traditionelle papierbasierte Verfahren erhalten.

Die Bilanz der ersten eIDAS Verordnung fällt jedoch gemischt aus: Einerseits hat sich zwar ein funktionierender europäischer Binnenmarkt für digitale Dienste entwickelt und auch in Deutschland konnten sich in den vergangenen Jahren einige erfolgreiche Anbieter aus dem Ausland etablieren. Andererseits haben zahlreiche EU-Länder noch kein System für elektronische Identitäten entwickelt. Andere wiederum kämpfen – wie Deutschland – seit Jahren mit einer niedrigen Akzeptanz ihrer Systeme durch die Bevölkerung. Zusätzlich haben die komplexe technische Architektur der eIDAS-Verordnung sowie das Fehlen einer klaren Ausrichtung auf den Privatsektor die umfassende Umsetzung behindert.

Die Verordnung von 2014 basiert noch auf nationalen eID-Systemen, die unterschiedlichen Standards folgen. Sie fokussiert sich damit nur auf einen kleinen Teil des Bedarfs an elektronischer Identifizierung – den öffentlichen Sektor. Sie enthält keinerlei Verpflichtungen für die Mitgliedstaaten, nationale Verfahren für die elektronische Identität zu entwickeln und mit denen anderer Mitgliedstaaten interoperabel zu machen, weshalb es große Unterschiede in der Bewertung der Konformität von Lösungen zur digitalen Identitätsprüfung gibt.

Am 20. Mai 2024 trat die **Novellierung der eIDAS-Verordnung**, kurz **eIDAS 2.0**, in Kraft. Sie baut auf der ursprünglichen Verordnung auf und aktualisiert diese angesichts der fortschreitenden digitalen Transformation. Ziel ist es, Diskrepanzen zwischen Mitgliedsstaaten auszugleichen und die Interoperabilität nationaler Identifizierungssysteme zu verbessern.

Zentrale Inhalte der eIDAS 2.0 sind:

- **Einführung der Europäischen Digitalen Identität (EUID):**
Die EUID ermöglicht Bürgern und Unternehmen in der EU eine sichere Identifizierung sowohl online als auch offline. Neben persönlichen Identitäten (PID) umfasst die EUID auch Identitäten für Organisationen (ODI). Dies soll insbesondere die Einhaltung regulatorischer Verpflichtungen erleichtern und den strukturierten Datenaustausch fördern.
- **Verifizierung von Person zu Person (P2P):**
Mit eIDAS 2.0 wird die Verifizierung nicht nur zwischen Person und Organisation, sondern auch zwischen Personen möglich. Dies eröffnet neue Anwendungsfelder, z. B. die Identitätsprüfung von Dienstleistern wie Zählerablesern.
- **Erweiterung der Vertrauensdienste:**
Die Verordnung erweitert die Regelungen für elektronische Vertrauensdienste und macht sie EU-weit interoperabel und sicherer. Neben elektronischen Unterschriften, Siegeln und Zeitstempeln werden auch Zustelldienste, Authentifizierungszertifikate und Siegel für elektronische Dokumente aufgenommen.

- **Einführung digitaler Nachweise:**
eIDAS 2.0 führt qualifizierte, attestierte Attribute (QEAs) ein, die spezifische Informationen (z. B. Führerscheinklassen) digital bereitstellen, ohne vollständige Dokumente teilen zu müssen. Dies fördert Datensparsamkeit und erhöht die Sicherheit im Umgang mit personenbezogenen Daten.
- **European Digital Identity Wallets (EUDI-Wallets):**
Die EUDI-Wallet ist eine digitale Brieftasche in Form einer mobilen App, die allen Bürger:innen und Unternehmen in der EU ein harmonisiertes Identifizierungsmittel bereitstellt. **Mitgliedsstaaten sind verpflichtet, mindestens eine Wallet bereitzustellen**, die sowohl für private als auch öffentliche digitale Dienste genutzt werden kann. Die EUDI-Wallet greift damit das **Konzept der Self-Sovereign Identity (SSI)** auf und übersetzt es in einen staatlich regulierten Rahmen, um Bürger:innen der EU eine sichere, flexible und benutzerzentrierte Verwaltung digitaler Identitäten zu ermöglichen.

Zur Sicherstellung einheitlicher Standards und Interoperabilität zwischen den Mitgliedsstaaten konkretisieren **Durchführungsrechtsakte die eIDAS-Verordnung**. Sie legen technische und betriebliche Mindestanforderungen, Normen für Wallet-Zertifizierungen sowie Anforderungen an qualifizierte Vertrauensdiensteanbieter fest.

Umsetzungsstand in Deutschland

Seit der Einführung des neuen elektronischen Personalausweises (nPA) am 1. November 2010 steht in Deutschland eines der technisch fortschrittlichsten und sichersten eID-Systeme Europas zur Verfügung. Der nPA kombiniert den herkömmlichen Sichtausweis mit neuen elektronischen Funktionen im Scheckkartenformat (eID-Karte), darunter biometrische Funktionen (ein digitales Lichtbild, Fingerabdrücke), elektronischer Identitätsnachweis (eID-/ Onlineausweis-Funktion).

Über den integrierten RFID-Chip (13,56 MHz) ermöglicht der nPA verschiedene Formen der elektronischen Authentifizierung. Er speichert sowohl Personaldaten als auch biometrische Daten (Lichtbild, Fingerabdrücke) und bietet „hoheitliche“ sowie „nicht hoheitliche“ Funktionen mit unterschiedlichen Vertrauensniveaus. Neben öffentlichen Stellen können auch Unternehmen den elektronischen Identitätsnachweis freiwillig anerkennen.

Trotz dieser technischen Fortschritte leidet die deutsche eID auch nach 14 Jahren unter geringer Akzeptanz und einer begrenzten Anzahl an Nutzungsmöglichkeiten. Große Technologiekonzerne bieten zunehmend benutzerfreundlichere Alternativen, die die eID insbesondere bei nicht hoheitlichen Anwendungen verdrängen könnten.

Das Thema digitale Identitäten spielt in Deutschland eine **zentrale Rolle bei der Umsetzung des Onlinezugangsgesetzes (OZG)**. Das 2017 eingeführte Gesetz verpflichtete Bund, Länder und Kommunen, Verwaltungsleistungen bis 2022 digital bereitzustellen und über einen Portalverbund zu verknüpfen. Nach Verfehlen der Zielvorgaben wurde am 14. Juni 2024 das **OZG 2.0** beschlossen. Zentrales Ziel ist die **Einführung einer einheitlichen digitalen Identität**, um bürokratische Hürden abzubauen und die Nutzerfreundlichkeit zu steigern. Die **BundID soll zur DeutschlandID weiterentwickelt werden** und eine zentrale Lösung für Verwaltungsdienstleistungen auf Bundes-, Länder- und Kommunalebene bieten. Unternehmen erhalten ein digitales Organisationskonto als Pendant.

Umsetzung der EUDI-Wallet in Deutschland

Am 30. September 2024 beschloss die Bundesregierung zur Umsetzung der eIDAS 2.0 eine staatliche digitale Briefftasche für Smartphones zu entwickeln. Diese soll Bürger:innen ermöglichen, sich EU-weit digital auszuweisen und wird schrittweise bis 2027 um zusätzliche Funktionen erweitert.

Neben der staatlichen Wallet sollen auch private Anbieter zugelassen werden, um Wahlfreiheit und Innovation zu fördern. So können Unternehmen, Stiftungen oder Forschungseinrichtungen eigene Wallets entwickeln und anerkennen lassen.

Unter der Federführung des Bundesministeriums des Innern und für Heimat (BMI) arbeiten die Bundesagentur für Sprunginnovationen (SPRIND) und das Bundesamt für Sicherheit in der Informationstechnik (BSI) gemeinsam an der Umsetzung. Am 7. Juni 2023 wurde zu diesem Zweck ein transparenter und partizipativer Architektur- und Konsultationsprozess für EUDI-Wallets unter kontinuierlicher Einbindung von Bürger:innen, Privatwirtschaft, Verbänden und Wissenschaft initiiert.

Unter der Federführung des Bundesministeriums des Innern (BMI) arbeiten die Bundesagentur für Sprunginnovationen (SPRIND) und das Bundesamt für Sicherheit in der Informationstechnik (BSI) an der Umsetzung. **Am 7. Juni 2023 wurde ein transparenter Architektur- und Konsultationsprozess initiiert**, der Bürger:innen, Privatwirtschaft, Verbände und Wissenschaft einbezieht. Die Ergebnisse wurden in sechs Architekturvarianten zusammengefasst und in ein finales Konzept integriert, das als Grundlage für die nationale Umsetzung von eIDAS 2.0 dient.¹

Ein weiterer Schritt ist der 13-monatige **SPRIND-Innovationswettbewerb „EUDI Wallet Prototypes“**, der im April 2024 startete. Elf Teams entwickeln in drei Phasen Prototypen für nutzerfreundliche und universelle Wallets, die in verschiedenen Szenarien erprobt werden.²

Weitere spannende Impulse konnten im Rahmen des Innovationswettbewerbs **„Schaufenster Sichere Digitale Identitäten“**³ des Bundesministeriums für Wirtschaft und Klimaschutz (BMWK) entwickelt werden. Ziel war die Förderung nutzerfreundlicher und interoperabler digitaler Identitäten für den Alltag. Hierfür wurden bis Ende 2024 innovative Ansätze für neue offenem interoperable und einfach nutzbare ID-Ökosysteme in Modellregionen anwendungsnah erprobt.

Das Besondere dabei: Der Wettbewerb adressierte nicht nur notwendige Technologien zur Umsetzung vom Onlinezugangsgesetz (OZG) oder generell die digitale Nutzung behördlicher Dienstleistungen, sondern fokussierte auch sämtliche andere Dienstleistungen aus dem Alltag der Bürger:innen. Im Gegensatz zu vergleichbaren Projekten konnten somit alle relevanten Stakeholder an einen Tisch gebracht werden: Privatwirtschaft, Identitätsdienstleister, Kommunen und nicht zuletzt die Bürger:innen. Dabei wurden auch erste eIDAS-konforme Anwendungen entwickelt, die teilweise bereits heute genutzt werden können.

Fazit und Ausblick

¹ Aufzeichnungen des Konsultationsprozesses können auf OpenCode abgerufen werden: https://gitlab.opencode.de/bmi/eudi-wallet/eidas2/-/tree/main/02_Workshops?ref_type=heads; Aufzeichnungen der öffentlichen Sprechstunden finden Sie hier: https://gitlab.opencode.de/bmi/eudi-wallet/eidas2/-/tree/main/03_Open_Online_Consultations?ref_type=heads. Die jeweils aktuelle Version des Architekturkonzepts ist hier abrufbar: <https://gitlab.opencode.de/bmi/eudi-wallet/eidas-2.0-architekturkonzept>.

² Weitere Informationen zum SPRIND-Innovationswettbewerb und die teilnehmenden Teams finden Sie hier: <https://www.sprind.org/de/challenges/eudi-wallet-prototypes/>

³ Weitere Informationen zu den „Schaufensterprojekten Sichere Digitale Identitäten“, den Projektkonsortien und Lösungen unter: <https://digitale-identitaeten.de/>

Digitale Identitäten bieten Kommunen, Unternehmen und Organisationen nicht nur Vorteile im Hinblick auf die Nutzung von Identitätslösungen für sichere und effiziente digitale Transaktionen, sondern bieten auch für Marktakteure interessante Möglichkeiten, um eigene eIDAS-konforme Lösungen anzubieten. Dabei sind staatliche Lösungen wie die DeutschlandID oder die EUDI-Wallet zentrale und vielversprechende Bausteine für eine standardisierte und zukunftssichere digitale Identitätsinfrastruktur.

Allerdings wird ihre vollständige Verfügbarkeit und Funktionalität noch einige Zeit in Anspruch nehmen. Kommunen und kommunale Unternehmen sollten daher nicht untätig bleiben, sondern die Zeit aktiv nutzen, um sich auf die kommenden Veränderungen vorzubereiten und erste Schritte zu unternehmen.

Proaktives Handeln und Austausch

So gibt es bspw. schon erste eIDAS-konforme Implementierungen von digitalen Identitätslösungen auf dem Markt, die sich für spezifische Anwendungsfälle in der öffentlichen Verwaltung und bei kommunalen Unternehmen eignen. Kommunen und kommunale Unternehmen können durch die frühzeitige Einführung und Erprobung marktreifer Lösungen wichtige Erfahrungen sammeln und ihre digitalen Angebote bereits heute verbessern.

Dabei sollte bei der Zusammenarbeit mit externen Anbietern stets die Bewahrung eines Höchstmaßes an Souveränität im Mittelpunkt stehen. Bei der Auswahl von Identitätslösungen sollte zudem auf die eIDAS-Kompatibilität und Interoperabilität, um einen nahtlosen Übergang zu staatlichen Standards wie der EUDI-Wallet oder DeutschlandID zu gewährleisten.

Eine Recherche zu Pilotprojekten und bewährten Anwendungen in anderen Kommunen sowie der Austausch mit anderen kommunalen Akteuren kann helfen, Herausforderungen zu identifizieren und Erkenntnisse für die Auswahl eigener Identitätslösungen zu nutzen.

Von der Funktions- zur Datenorientierung

Digitale Identitäten und Prozessdigitalisierung gehen Hand in Hand. Um sich auf die Einführung moderner Identitätslösungen vorzubereiten, sollten kommunale Prozesse und Abläufe bereits heute darauf abgestimmt und vollständig digitalisiert werden.

Digitale Identitäten sind Werkzeuge, die eine sichere Authentifizierung per Datenübermittlung ermöglichen. Traditionell sind kommunale Prozesse jedoch stark funktionsorientiert organisiert: Jede Abteilung arbeitet unabhängig voneinander und verfolgt eigene Ziele und Abläufe. Der Übergang von der Funktions- zur Datenorientierung – sprich Die systematische Nutzung und den Austausch von Daten mit anderen Bereichen ist entscheidend für die nachhaltige Implementierung von digitalen Identitäten. Insellösungen und isolierte Arbeitsweisen in den verschiedenen Fachbereichen, die fehlende Interoperabilität von IT-Systemen und nicht standardisierte Prozesse stehen heute noch einer Einführung einheitlicher digitaler Prozesse und damit auch der Nutzung digitaler Identitäten im Wege.

Kommunen und kommunale Unternehmen sollten daher ihre Digitalisierungsstrategien ganzheitlich ausrichten und sicherstellen, dass digitale Identitäten nicht isoliert betrachtet, sondern als integraler Bestandteil umfassender Prozessdigitalisierung implementiert werden.

Im Rahmen von Civitas Connect e. V. möchten wir in den nächsten Monaten den Erfahrungsaustausch zum Thema begleiten. Mitglieder und Partner von Civitas Connect e. V. sind herzlich dazu eingeladen, Fragen, Anregungen und Ideen zum Thema an uns heranzutragen.

