Organisations-identitäten

Whitepaper

bitkom

Inhalt

Autoren

Dominik Deimel | Wallet-Experts GmbH
Christian Gericke | d.velop AG
Detlef Hühnlein | ecsec GmbH
Sascha Kraus | Nortal AG
Boris Lingl | DATEV eG
Hendrik Lume | Nortal AG
Alexander Manecke | Telekom
Artur Philipp | SVA System Vertrieb Alexander GmbH
Jan Rehder-Lange | Nortal AG
Justus Schrecker | SCHUFA
Steffen Schwalm | msg systems
Christian Seegebarth | D-Trust GmbH
Carsten Stöcker | Spherity GmbH
Andreas Wand | D-Trust GmbH

Einleitung

Die Organisationsidentität (OrgID) im Sinne einer digitalen Identität für Unternehmen ist ein zentraler Baustein, um Unternehmen im digitalen Raum sicher, effizient und zukunftsorientiert zu positionieren. Sie sorgt für mehr Vertrauen im digitalen Raum sowie erhöhten Betrugsschutz durch eine sichere und eindeutige Identifikation von Geschäftspartnern, Kunden und Rechnungsstellern. Auch bei Compliance und regulatorischen Anforderungen z. B. im KYB (Know your Business) -Bereich kann eine OrgID helfen, das Einhalten zu erleichtern. Unternehmen können mit ihrer Hilfe interne Prozesse modernisieren und externe Prozesse digitaler und damit effizienter gestalten. Je mehr Interaktionen und Geschäfte online stattfinden, umso mehr wird eine OrgID zu einem notwendigen Werkzeug, um Unternehmensdaten zu verwalten, zu versenden und zu verifizieren.

Eine OrgID hat also ähnliche Charakteristika wie eine digitale Identität für Personen. Die grundlegenden Gedanken der besseren Identifizierung und Authentisierung im digitalen Raum sind für natürliche und juristische Personen gleich. Obwohl jüngste Studien zeigen, welches Potenzial einheitliche Organisationsidentitäten für Unternehmen haben, ist die Thematik insbesondere in Deutschland sowohl im privaten als auch öffentlichen Sektor noch sehr wenig bekannt. Das spiegelt sich auch darin wider, dass es kein einheitliches Bild darüber gibt, wie eine solche OrgID aussehen und wie ein digitales Ökosystem zur Identifizierung von Unternehmen ausgestaltet werden muss.

Trotz dieses Defizits müssen sich Politik und Unternehmen gleichermaßen schon heute mit der Frage befassen, wie sie eine OrgID zur Verfügung stellen und nutzbar machen können. Dieses Whitepaper soll Anhaltspunkte dazu liefern und ein schärferes Bild von Organisationsidentitäten zeichnen.

Zusammenfassung Status quo

Eine Organisationsidentität ist eine digitale, eindeutige und vertrauenswürdige Darstellung einer Organisation, die zur Authentifizierung, Autorisierung und sicheren Kommunikation in digitalen Ökosystemen dient. Die digitale OrgID ist in dieser Hinsicht ähnlich zu den Merkmalen einer analogen Identität für juristische Personen.

Ein gängiges Beispiel für eine Organisationsidentität in der analogen Welt ist der als Ausdruck vorliegende Handelsregisterauszug. Hier sind verpflichtende Eintragungen über eine juristische Person oder Personengesellschaft enthalten. In Deutschland existieren über das Handelsregister hinaus zahlreiche fragmentierte Register für unterschiedliche Organisationsformen und Verwendungszwecke, die zur Identifizierung von Organisationen dienen. Zu den wichtigsten gehören das Vereinsregister, das Genossenschaftsregister, das Stiftungsregister sowie das Basisregister, in denen Unternehmen nach verschiedenen Standards und Aktualisierungszyklen erfasst werden. Weiterhin gibt es Steuerregister, in denen

Unternehmenssteuer-IDs wie die Umsatzsteuer-Identifikationsnummer (USt-ID) und die Steueridentifikationsnummer (Steuer-ID) für betriebliche Zwecke geführt werden. Die fehlende Vernetzung der verschiedenen Register erschwert eine konsistente und verlässliche Identifizierung juristischer Personen und verhindert eine umfassende Digitalisierung und Automatisierung von Prozessen. Aus all diesen Registern ließe sich zwar ein für jedes Unternehmen individueller Identifikator ableiten, jedoch keine einheitliche digitale OrgID kreieren. Neben öffentlichen Registern oder GLEIF für internationale Unternehmen können auch aggregierte Verfahren wie auch das vom Bundesanzeiger Verlag betriebene Unternehmensregister als Quelle für die Ausstellung einer Organisationsidentität sein. Dieses wird im Industrie 4.0 Kontext bereits verwendet, kann jedoch ebenfalls zum heutigen Zeitpunkt die Herausforderungen einer OrgID nicht vollständig lösen. So sind einige Unternehmensformen, insbesondere kleinere Unternehmen und Solo-Selbstständige, auch in diesem Register nicht aufgeführt.

Für eine einheitliche OrgID müssten digitale, verifizierbare Nachweise über die Unternehmensidentität und damit verbundene Berechtigungen erstellt werden können, die ein Unternehmen vielseitig nutzen kann. Diese könnten in verschiedenen Anwendungsfällen eingesetzt werden, wie bei der Eröffnung von Bankkonten, der Ausstellung und Verwaltung von digitalen Produktpässen (DPPs) und in Industrie-4.0-Anwendungen wie Data Spaces. Auch die Automatisierung von Compliance-Prozessen würde hierdurch erleichtert, beispielsweise bei Exportkontrollen für Dual-Use-Güter oder beim sicheren Austausch von kritischen Infrastrukturdaten in Bereichen wie der Energiewirtschaft.

Die fehlende Verknüpfung der deutschen Registerlandschaft ist nicht die einzige Lücke, die einheitlichen und allgemein akzeptierten Organisationsidentitäten im Weg steht. Auch auf europäischer Ebene ist das Thema Organisationsidentität nicht einheitlich geregelt. Ebenfalls stellen verschiedene Anwendungen und Branchen unterschiedliche Anforderungen. Solche Inkonsistenzen bringen entscheidende Nachteile bei der Digitalisierung, insbesondere in Länder- und branchenübergreifenden Prozessen.

Ein solcher international verwendbarer, anerkannter, standardisierter und möglichst bereits eingeführter Identifikator ist essenziell für die Schaffung von Organisationsidentitäten. Nur so kann eine schnelle Akzeptanz hergestellt werden. Eine Möglichkeit, ein Identifikationsmerkmal zu finden, woraus sich eine Identität für eine Organisation ableitet, ist die Verwendung eines je nach Branche etablierten Identifikators, welcher gegebenenfalls mit den Registerdaten verknüpft, sowie mit einem europäischen Vertrauensanker, z. B. einem qualifizierten elektronischen Siegel, versehen werden kann. Vereinfacht werden könnte dieser Vorgang durch eine übergreifende, interoperable Plattform, die die Daten aus verschiedenen Registern integriert und regelmäßig aktualisiert.

Ein internationales Beispiel für einen hohen Digitalisierungsgrad öffentlicher Verwaltung ist Estland. Der Erfolg basiert dabei in großen Teilen auf einer stringenten digitalen Basisinfrastruktur. Das betrifft sowohl Privatpersonen als auch Unternehmen. So melden sich potenzielle Bieter für öffentliche Ausschreibungen beispielsweise in der öffentlichen Vergabeplattform Estlands mit einem der gängigen elektronischen Identifizierungsmittel an. Bei jeder Anmeldung wird gegen das Unternehmensregister und verschiedene weitere Register geprüft, für welche juristischen Personen die natürliche Person vertretungsberechtigt ist. Der Nutzer wählt

die juristische Person aus, die er in der Session vertreten will. Weiteren natürlichen Personen können dann direkt in dem Portal Rechte zugewiesen werden, um beispielsweise an Ausschreibungen teilzunehmen. Das gleiche Prinzip findet in allen anderen staatlichen Portalen Anwendung, die Onlinedienste für juristische Personen anbieten.

Auch wenn dieses Beispiel veranschaulicht, wie ein Staat Organisationsidentitäten digital abbilden und so digitale Prozesse für Unternehmen vereinfachen kann, ist es nur bedingt zukunftstauglich. Mit der Novellierung der eIDAS-Verordnung wird ein europäisch einheitlicher Rahmen für natürliche und juristische Personen geschaffen, der die Identifizierung im digitalen Raum neu regelt. Damit werden heutige analoge und digitale Modelle wie in Estland eine Reihe von Anpassungen erleben.

eIDAS 2.0 / EUDI Wallet allgemein

Überblick

Die ergänzte Fassung der eIDAS-Verordnung (EU) 2024/1183 („eIDAS 2.0“) definiert die Anforderung an jeden Mitgliedstaat, eine Europäische Brieftasche für die Digitale Identität („EU Digital Identity Wallet“, EUDIW) bereitzustellen. Die EUDIW kann vom Mitgliedstaat, den dort ansässigen oder niedergelassenen natürlichen und juristischen Personen im Mitgliedstaat, unter seiner Autorität oder unabhängig, aber von einem Mitgliedstaat anerkannt veröffentlicht werden. Dies macht auch private Wallets unter der Anerkennung eines Mitgliedstaats möglich, wie dies beispielsweise in Deutschland als Option entschieden wurde. Jedes EUDIW enthält so genannte „Personenidentifizierungsdaten“ („Person Identification Data“, PID für natürliche oder juristische Personen als Wallet-Inhaber) basierend auf einem notifizierten eID-System auf einem hohen Vertrauensniveau. Direkt korrespondierend mit dem EUDIW müssen die neuen qualifizierten Attributsbescheinigungsdienste berücksichtigt werden. (Qualifizierte) Elektronische Attributsbescheinigungen ((Q)EAA) dienen lediglich der Authentifizierung zusätzlicher Attribute, wie z.B. eine Fahrerlaubnis im Führerschein, ein Diplom, das einen erfolgreichen Studienabschluss dokumentiert, eine Handlungsberechtigung oder ein digitaler Produktpass, deren Authentizität mit einem (qualifizierten) elektronischen Siegel gewährleistet wird.

Dies bedeutet, dass die EUDIW die Kernidentität des Unternehmens, respektive der natürlichen Person enthalten wird, sowie zusätzliche mit dem Unternehmen, bzw. der Person verknüpfte Nachweise. Die in den (Q)EAAs zu bestätigenden Daten werden anhand der von den Mitgliedstaaten bereitgestellten öffentlichen Register erzeugt und geprüft. Zur Sicherstellung eines einheitlichen technischen Rahmens für die erleichterte Umsetzung in Europa enthält die eIDAS-Verordnung verbindliche Durchführungsrechtsakte, die auf internationale oder europäische Normen verweisen.

Deren Einhaltung wird durch unabhängige Konformitätsbewertungsstellen geprüft und zertifiziert, um damit ein hohes Maß an Sicherheit gewährleisten zu können.

Herausforderungen

Eine wesentliche Herausforderung bei der Umsetzung von Organisationsidentitäten ist die Definition der Organisationsidentität selbst. Es wäre regulatorisch zu klären, ob es sich dabei wie bei der natürlichen Person um eine eID oder um den Auszug beispielsweise aus dem Handelsregister handelt. Im Falle der eID wäre durch die Bundesregierung ein eigenes eID-Schema zu definieren und zu notifizieren, wie dies in einigen europäischen Mitgliedsstaaten bereits der Fall ist. Sofern es sich um einen Registerauszug beispielsweise aus dem Handelsregister handelt, wäre die Organisationsidentität eine sog. (qualifizierte) Elektronische Attributsbescheinigung und würde durch öffentliche oder private (qualifizierte) Vertrauensdiensteanbieter ausgestellt.

Eine weitere Herausforderung ist die Quelle der Organisationsidentität. Für Unternehmen liegt in Deutschland mit dem Handelsregister eine Lösung vor, für Vereine wäre das Vereinsregister nutzbar. Bei internationalen Unternehmen kommen auch nicht staatliche Quellen wie z. B. GLEIF in Frage, wohingegen es für Behörden oder GbR aufwendiger sein könnte. Eine einheitliche Regelung hierzu ist in Europa bislang nicht entschieden. Nur auf den Staat als Akteur zu hoffen, wäre jedoch zu kurz gegriffen. Es braucht ein gesamtes Ökosystem mit starkem Einbezug der Wirtschaft, um die Register für alle Organisationsformen zu verknüpfen und einheitliche Identitäten zu ermöglichen.

Identitäten für Personen oder Unternehmen: Viele Gemeinsamkeiten und wichtige Unterschiede

Die grundlegenden Funktionen digitaler Wallets sind deckungsgleich für Personen und Organisationen. Vereinfacht müssen Wallets Daten, Dokumente und Nachweise empfangen, vorzeigen, signieren, verifizieren und verwalten. Dabei sind Wallets für natürliche Personen auf den individuellen Gebrauch ausgelegt. Sie ermöglichen es Bürgerinnen und Bürgern, ihre persönlichen Identitätsdaten zu verwalten, auf Dienstleistungen im öffentlichen und privaten Sektor zuzugreifen und sicher persönliche Nachweise wie Diplome, Führerscheine oder Ausweisdokumente zu teilen. Im Gegensatz dazu dienen Wallets für juristische Personen – sogenannte Organizational Wallets – der Verwaltung von Identitätsdaten für rechtliche Einheiten, wie Unternehmen und Organisationen. Diese Wallets müssen die Verwaltung einer Vielzahl von unternehmensrelevanten Nachweisen unterstützen, darunter Geschäftslizenzen, Compliance-Zertifikate, Vollmachten und Verträge. Um den Anforderungen der Organisation gerecht zu werden, benötigen Organizational Wallets ein Nutzerverwaltungssystem, das es mehreren Mitgliedern der Organisation erlaubt, diese Nachweise zu empfangen, zu speichern und bei Bedarf vorzulegen. Dabei müssen auch Einzelpersonen ihre Wallets im Unternehmenskontext nutzen können, z. B. um innerhalb der Organisation den Besitz von Berechtigungen nachzuweisen.

Bezüglich der Ausgestaltungsmöglichkeiten von Wallets gibt es drei grundlegende Möglichkeiten.

Natürliche Personen-Wallet

Die EUDI-Wallet für natürliche Personen wird die Grundform aller EUDI-Wallets in der EU sein. Sie beruht auf der PID der natürlichen Person und kann weitere Attribute und Nachweise speichern. Sie wird sowohl Bürgern als auch Verbrauchern und Unternehmen offenstehen. Über Vertretungsnachweise als mit der PID verknüpfte Attribute werden zunächst organschaftliche Vertreter berechtigt, die juristische Person digital zu vertreten. Diese Vertretungsberechtigung kann auch mittels rechtsgeschäftlichem Vertretungsattribut an die EUDI-Wallet einer weiteren Person weitergegeben werden.

Die natürliche Personen-Wallet ist damit insbesondere als Unternehmenswallet einsetzbar für kleinere Unternehmen, die nur von einer Person vertreten werden und nur einen kleineren Geschäftsumfang und überschaubare Anzahl an Transaktionen tätigen. Die Delegation des Vertretungsrechtes über Erteilung und Widerruf über das jeweilige Attribut macht jedoch eine komplexe Vertretungsstruktur mit Gesamtvertretung und gemischten Rollen, wie sie in vielen mittelständischen und großen Unternehmen regelmäßig zu finden sind, technisch sehr schwer handhabbar. Hinzu kommt, dass die natürliche Personen-Wallet auf dem Endgerät des Vertreters betrieben wird, was eine zentrale, unternehmensweite Steuerung der Wallet unmöglich macht. Beide Aspekte erschweren die Nutzung einer natürlichen Personen-Wallet für die meisten juristischen Personen.

Juristische Personen-Wallet

Bei einer Wallet für juristische Personen hingegen liegt eine zentrale Walletinstanz vor, die eine zentrale Steuerung der Nutzung der Wallet mittels eines Rechte- und Rollenmanagements erlaubt. Die Grundidentität der juristischen Person wird dem organschaftlichen Vertreter ausgestellt. Danach managt das Unternehmen die Vertretung der juristischen Person eigenverantwortlich mittels des Rechte- und Rollenmanagements. So können ohne Weiteres komplexe, mehrstufige Vertretungsmechanismen kreiert werden. Hierbei bleiben interne Unternehmensabläufe größtenteils unangetastet. Daher ist die Juristische Personen-Wallet prädestiniert für den Einsatz bei mittelständischen und großen Unternehmen. Die Wallet ist hierbei eine echte zertifizierte EUDI-Wallet samt dem damit verbundenen Sicherheitsniveau und den rechtlichen Vorteilen. Beim Wallet für Organisationen kann es sich, im Gegensatz zu solchen für natürliche Personen, um Cloudlösungen oder z. B. eine Erweiterung bestehender Identitätsmanagementsysteme handeln, um die Nutzung durch eine Vielzahl handelnder Personen im Unternehmen zu ermöglichen.

Zur EUDI-Wallet interoperable juristische Personen-Wallet

Das EUDI-Ökosystem ist grundsätzlich offen konzipiert und kann daher auch mit anderen Wallets und Systemen interagieren. Hierunter fallen insbesondere auch bereits etablierte Lösungen für Cloud-Wallets für juristische Personen. Die EUDI-Wallets können hier als Übermittlungswerkzeuge und Authentisierungsmittel genutzt werden, sofern das Cloud-Wallet nicht selbst zum EUDI Wallet zertifiziert wird. Der Vorteil ist die Bewahrung etablierter Geschäftsmodelle bei gleichzeitiger Nutzung bereits vorhandener Infrastruktur. Aufgrund der fehlenden Zertifizierung als EUDI-

Wallet sind jedoch unter Umständen ein niedrigeres Vertrauensniveau und die fehlenden rechtlichen Vorteile gegeben.

Delegation von Rechten

Während die Delegation von Rechten und die Einrichtung von Vertretungsberechtigungen für Personenwallets eher die Ausnahme als die Regel darstellt, ist dies eine der zentralen Funktionen der Organisationswallet. Hierdurch wird es bestimmten Mitgliedern ermöglicht, basierend auf den ihnen zugewiesenen Rechten im Namen der Organisation zu handeln. Administratoren können in einer zentralen Verwaltungsoberfläche Rollen zuweisen und anpassen. So können zum Beispiel signaturberechtigte Mitarbeiterinnen und Mitarbeiter die Befugnis zur Unterzeichnung von Dokumenten oder Verträgen erhalten. Die Delegationsrechte werden als verifizierbare Nachweise ausgestellt, die Informationen zu den Vertretern und ihrem Handlungsspielraum enthalten.

Art der Nachweise

Natürliche Personen-Wallets sind primär auf persönliche Nachweise ausgelegt. Diese beinhalten Dokumente wie Ausweise, Zeugnisse oder gar Merkmale der natürlichen Person wie Gesundheitsdaten, die in der Regel in Interaktionen zwischen Individuen und Dienstleistungsanbietern benötigt werden. Organisationswallets hingegen verwalten geschäftsbezogene Nachweise, die für die rechtliche und operative Funktionsfähigkeit einer Organisation notwendig sind. Dazu zählen neben den persönlichen Nachweisen der Mitarbeiterinnen und Mitarbeiter auch Organisationsnachweise wie Zertifikate, Vollmachten, regulatorische Zulassungen und Informationen zur Einhaltung gesetzlicher Vorgaben sowie die Autorisierung von Maschinen. Diese Nachweise sind entscheidend für den Betrieb und die Compliance-Anforderungen der Organisation, etwa bei der Verwaltung digitaler Produktpässe oder der Abwicklung von Lieferkettenprozessen.

Stellvertreter und Vollmacht

In der modernen Unternehmenswelt spielen Handlungsvollmachten eine zentrale Rolle bei der Optimierung von Geschäftsprozessen und der Beschleunigung von Entscheidungsfindungen. Ein anschauliches Beispiel hierfür ist in der Praxis, einem Einkaufsleiter eine umfassende Handlungsvollmacht für das Unternehmen, in dem er beschäftigt ist, zu erteilen. Diese Vollmacht ermächtigt ihn in seiner Rolle als Einkaufsleiter, selbstständig Bestellungen zu tätigen, Preisverhandlungen zu führen und Lieferverträge abzuschließen.

Die präzise Dokumentation und der Nachweis solcher Bevollmächtigungen sind von entscheidender Bedeutung, um in Geschäftsbeziehungen Rechtssicherheit und Verbindlichkeit zu gewährleisten. Eine Handlungsvollmacht befähigt den Bevollmächtigten, im Namen des Unternehmens Geschäfte abzuwickeln und alltägliche Entscheidungen zu treffen. Um potenzielle Missverständnisse zu vermeiden und Transparenz für Geschäftspartner zu schaffen, ist eine klare Dokumentation dieser

Vollmachten unerlässlich. In bestimmten Fällen, in denen eine rechtliche Verpflichtung besteht, werden die Befugnisse einer Person im Handelsregister verzeichnet.

Das Handelsregister fungiert als Garant für Transparenz und Sicherheit im Geschäftsverkehr. Als öffentlich zugängliches Verzeichnis enthält es alle wesentlichen Informationen über Unternehmen, einschließlich Rechtsform, Firmensitz, Gesellschafter und vertretungsberechtigte Personen. Diese Offenlegung schafft Vertrauen und bildet das Fundament für solide Geschäftsbeziehungen. Der öffentliche Glaube des Handelsregisters verleiht den eingetragenen Daten eine Vermutung der Richtigkeit, was die Rechtssicherheit erhöht. Weiterhin erfüllt das Register eine wichtige Beweis- und Kontrollfunktion, indem es Veränderungen in der Unternehmensstruktur oder -führung dokumentiert. Dies ermöglicht es Unternehmen und ihren Partnern, sich auf die Korrektheit der Informationen zu verlassen und potenzielle rechtliche Konflikte zu vermeiden.

Für bestimmte Berufsgruppen wie Steuerberater und Notare sind spezifische Berufsträgereigenschaften von essenzieller Bedeutung. Diese umfassen typischerweise die volle Handlungsfähigkeit und außerordentliche Vertrauenswürdigkeit. Diese Anforderungen sind unerlässlich, da diese Berufsgruppen als unabhängige Organe der Rechtspflege eine Schlüsselrolle im Rechtssystem und in der Gesellschaft einnehmen. Steuerberater beispielsweise gelten als "unabhängiges Organ der Steuerrechtspflege" und stehen somit auf einer Ebene mit anderen Organen der Rechtspflege, wie Rechtsanwälten.

Diese Berufe erfordern ein Höchstmaß an Verantwortungsbewusstsein, Integrität und fachlicher Expertise, da sie häufig mit sensiblen finanziellen und rechtlichen Angelegenheiten ihrer Mandanten betraut sind. Die strengen Zulassungsvoraussetzungen und Berufsträgereigenschaften dienen dazu, das öffentliche Vertrauen in diese Berufsgruppen zu wahren und sicherzustellen, dass ausschließlich qualifizierte und vertrauenswürdige Personen diese bedeutenden Funktionen ausüben. Diese Berufsgruppen weisen ihre Zugehörigkeit und Mandatsfähigkeit durch offizielle Ausweise der zuständigen Kammern nach. Die Nachweise für Vollmacht & Stellvertretung werden im Gebrauch und Auftrag des Mandats gegenüber Dritten eingesetzt – diese Bezeigung unterliegt einem hohen Vertrauensbedarf. Notwendige Nachweise werden im Bedarfsfall gegenüber berechtigten Dritten vorgezeigt. Berufsträger setzen diese Nachweise im Kontext einer Vollmacht gemeinsam mit den eigenen Personenidentifizierungsdaten (PID) ein und weisen eine Stellvertretung oder Vollmacht nach.

Die Zukunft verspricht eine digitale Revolution im Bereich der privatwirtschaftlichen und gesetzlich vorgeschriebenen Vollmachten sowie Stellvertreterregelungen. Man kann davon ausgehen, dass natürliche und juristische Personen nur noch digital Ihre Identitäten in einem Prozess Ende zu Ende ohne Medienbruch nachweisen. In diesem innovativen Konzept wird die PID zur einzigen offiziellen Identifizierungsmethode für natürliche Personen. Durch die Verknüpfung einer OrgID oder Juristischen Personen-ID (LPID) mit einer PID lässt sich die Zugehörigkeit zu einer juristischen Person nachweisen. In diesem Kontext lassen sich Rollen der Person in einer Organisation abbilden und bei Bedarf gegenüber berechtigten Dritten als Handlungsvollmacht nachweisen.

Dieser Proof of Representation (PoR) oder Proof of Authority (PoA) dient der rechtsverbindlichen Vertretung eines Unternehmens. Eine validierte und autorisierte Person erhält die Befugnis, die Attribute der Organisation an andere Personen oder Dienste weiterzugeben und somit die OrgID/LPID der Person hinzuzufügen (Vererbung).

Dieser zukunftsweisende Ansatz verspricht eine erhebliche Vereinfachung und Sicherung von Vollmachts- und Vertretungsprozessen im digitalen Zeitalter.

Use Cases

Wie verändern OrgIDs das Gesundheitswesen mit Blick auf die TI?

Die Telematikinfrastruktur (abgekürzt: TI) bildet das Branchennetzwerk für das deutsche Gesundheitssystem und vernetzt damit Versicherte, Leistungserbringer (Ärzte, Apotheker, Krankenhäuser, Therapeuten u. a.) sowie gesetzliche und private Kostenträger. Mit der Öffnung der TI 2.0 in Richtung Zero Trust Architektur hat die gematik[1] als regulatorische Aufsichtsbehörde für die TI den ersten Schritt unternommen, das Netzwerk im Internet ohne Konnektoren aber mit den etablierten zertifikatsbasierten Vertrauensankern (z. B. sektorale IDP in der Föderation) agieren zu lassen. Über den European Health Data Space werden neue Anforderungen an die TI im Hinblick auf die Interoperabilität und Datenkommunikation im europäischen Raum zukommen. Dabei werden Organisationsidentitäten heute noch durch Chipkartentechnologie (SMC-B Karte) und TI konforme Konnektoren realisiert. Mit der Zero Trust Architektur in der TI 2.0 ist eine Umstellung auf dezentralen Trust Ankern der jeweiligen Organisation (Arztpraxis, Krankenhaus u. a.) in Kombination mit dort bestehenden Identity- und Access-Management-Lösungen vorgesehen.

Die Nutzung eIDAS 2.0 konformer OrgIDs in der Telematikinfrastruktur öffnet den Weg des deutschen Gesundheitssystems in ein europäisch harmonisiertes digitales Ökosystem. Ein wichtiger Schritt, um das gemeinsam zu erschaffende Vertrauen in OrgIDs durchgängig über alle Domänen und in ganz Europa zu etablieren. Dies würde bedeuten, dass die Telematikinfrastruktur sich schlicht der dezentralen Vertrauensankern der eIDAS 2.0 Regulatorik bedient. Damit wird jede Organisation im deutschen Gesundheitssystem automatisch Teil des europäischen Ökosystems, ohne dass die Anforderungen an Interoperabilität und IT-Sicherheit der TI eingeschränkt werden. Ziel muss es sein, dass eIDAS 2.0 konforme OrgID damit auch in der TI 2.0

[1] https://www.gematik.de/

genutzt werden können. Die Verantwortung für die Registrierung und den Betrieb der OrgID obliegt dann allerdings nicht mehr primär der gematik und den Leistungserbringerorganisationen, sondern der EUDI Wallet Infrastruktur und den dort verankerten Prinzipien der eIDAS 2.0 Verordnung. Organisationen im Gesundheitssystem erhalten damit die Möglichkeit, ihre einmal registrierte Organisation auch außerhalb der TI für die Digitalisierung ihrer Prozesse (z. B. Beauftragung und Zahlungsverkehr mit Dienstleistern) zu nutzen.

B2B und B2C: E-Rechnung, Dokumentenübermittlung

Die Einführung der E-Rechnung in Deutschland ab 2025 stellt Unternehmen und Behörden vor erhebliche Herausforderungen. Der derzeit geplante Ansatz, Rechnungen per E-Mail zu übermitteln und steuerliche Daten separat an Finanzämter zu melden, führt zu einer fragmentierten Struktur, die ineffizient, kostenintensiv und fehleranfällig ist. Besonders für kleine und mittelständische Unternehmen bedeutet dies zusätzliche Belastungen durch komplexe Prozesse, hohe Einführungskosten für Software und Schnittstellen sowie ein erhöhtes Sicherheitsrisiko, da E-Mails anfällig für Phishing und Manipulation sind. Digitale Organisationsidentitäten in Verbindung mit zertifizierten E-Rechnungsplattformen und qualifizierten Vertrauensdiensten gemäß der eIDAS-Verordnung bieten hier eine zukunftsfähige und sichere Lösung, die den Übergang zu einem effizienten, harmonisierten System ermöglicht.

OrgIDs schaffen eine manipulationssichere digitale Identität für Unternehmen, die nicht nur die Rechnungsübermittlung erleichtert, sondern auch die automatische Zuordnung und Validierung von Geschäftsvorgängen ermöglicht. In Kombination mit Vertrauensdiensten, die den sicheren und rechtsverbindlichen Austausch von Dokumenten gewährleisten, entsteht eine geschützte Kommunikationsinfrastruktur. Diese Vertrauensdienste bieten die rechtliche und technische Grundlage, um sensible Daten sicher zu übermitteln und die Integrität der Informationen zu garantieren. Plattformlösungen wie das italienische „Sistema di Interscambio (SdI)“ könnten als Vorbild dienen, um den Prozess in Deutschland zu zentralisieren und zu standardisieren. Solche Plattformen übernehmen die sichere Übertragung der Rechnungen sowie die automatische Weiterleitung steuerlicher Daten, wodurch separate Softwarelösungen und manuelle Prüfungen obsolet werden. Dies reduziert den Aufwand, minimiert Fehler und bietet klare Sicherheitsvorteile gegenüber der E-Mail-basierten Übermittlung.

Die Integration von OrgIDs und qualifizierten Vertrauensdiensten stellt die Einhaltung von Standards gemäß eIDAS sicher, wodurch eine europäische Interoperabilität ermöglicht wird. Dies erleichtert den grenzüberschreitenden Handel und unterstützt den Aufbau eines digitalen Binnenmarkts. Gleichzeitig profitieren Unternehmen durch weniger Administrationsaufwand, niedrigere Kosten und eine verbesserte Compliance und Sicherheit. Behörden gewinnen durch erhöhte Transparenz, effizientere Prozesse und einen besseren Schutz vor Steuerbetrug. Langfristig bieten zertifizierte Plattformen und Vertrauensdienste nicht nur Lösungen für die E-Rechnung, sondern

auch für weitere digitale Dokumenten- und Kommunikationsprozesse, was die Digitalisierung des gesamten Wirtschaftssystems vorantreibt.

Die bestehenden Herausforderungen bleiben jedoch erheblich:

Die fragmentierte Struktur erhöht den Verwaltungsaufwand und verursacht hohe Kosten, insbesondere für KMU. Sicherheitsrisiken durch den E-Mail-basierten Ansatz gefährden die Integrität sensibler Daten, und fehlende europäische Interoperabilität behindert die grenzüberschreitende Zusammenarbeit. Um diese Probleme zu lösen, sind klare regulatorische Rahmenbedingungen, die Förderung qualifizierter Vertrauensdienste sowie die flächendeckende Einführung zentraler Plattformen unerlässlich. Durch den konsequenten Einsatz von OrgIDs und Vertrauensdiensten kann Deutschland nicht nur die Einführung der E-Rechnung erfolgreich gestalten, sondern auch einen wichtigen Beitrag zu einem sicheren, effizienten und digitalen europäischen Binnenmarkt leisten.

Digitaler Produktpass und digitale Lieferkette

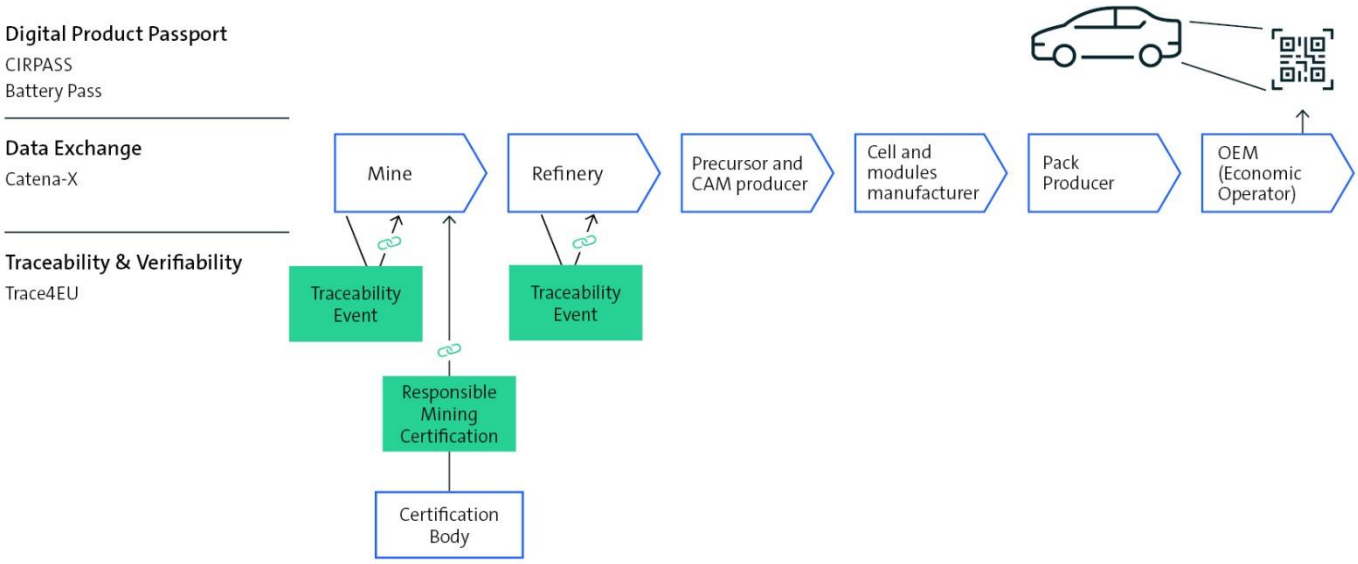
Verschiedene europäische Regulierungen wie z. B. die Batterieverordnung und die so genannte „Ecodesign for Sustainable Products Regulation“ (ESPR) erfordern, dass europäische Unternehmen die Genese ihrer Produkte in einem sog. digitalen Produktpass nachweisen. Hierzu zählt der vollständige Produkt-Lebenszyklus, einschließlich der Produktentwicklung. Ziel ist es, die korrekte Herkunft und Umsetzung europäischer Entwicklungsvorgaben nachzuweisen. Der Produktpass ermöglicht zudem den vereinfachten Nachweis von Sorgfaltspflichten in den Lieferketten, wie dies von nationalen wie europäischen Regulierungen gefordert wird.

Organisationsidentitäten sind der Schlüssel zur vertrauenswürdigen Umsetzung des Produktpasses. Die Unternehmen innerhalb der Lieferkette, in der das Produkt entsteht, werden über ihre OrgID eindeutig identifiziert. Diese ist im Organisationswallet der jeweiligen Organisation abgelegt. Die einzelnen im Entwicklungszyklus entstehenden Teile werden sukzessive je Produktschritt als kleine (qualifizierte) elektronische Attributsbescheinigungen einem Produkt, also einer gesamten Mappe, dem digitalen Produktpass hinzugefügt. Dieser wird im Produktionsprozess bzw. der Lieferkette an die jeweils beteiligten Unternehmen weitergegeben, so dass im Ergebnis der Produktpass entsteht. Der Nachweis der beteiligten Unternehmen ermöglicht die einzelnen Nachweise im Pass.

Eine zusätzliche Verbindung von Produktpass und den einzelnen Nachweisen mit den zugehörigen Prozessschritten in der Lieferkette lässt auch einen einfachen, wie sicheren Nachweis der Lieferkette erzeugen. Organisationsidentitäten ermöglichen so die Automatisierung und digitalen Nachweis industrieller Prozesse.

Der digitale Produktpass und Lieferkettennachweis mit Hilfe von Organisationsidentitäten wird aktuell von der Industrie u. a. in den Projekten Catena X sowie dem europäischen Projekt TRACE4EU pilotiert.

Das nachstehende Bild verdeutlicht den Anwendungsfall:



OrgIDs im Verwaltungskontext

OrgID: C2G

In der Beziehung zwischen Bürgerinnen und Bürgern und öffentlichen Behörden (C2G), bringen OrgIDs viele Vorteile für die beteiligten Parteien. Im ersten Schritt können Bürger durch die eindeutige OrgID einer Behörde sicherstellen, dass sie mit der richtigen Stelle kommunizieren, was Sicherheit und Vertrauen erhöht. Zudem kann sichergestellt werden, dass ausgestellte Dokumente oder Bescheide einer Behörde echt und authentisch sind. Diese Dokumente werden von der Behörde mit Hilfe der OrgID digital signiert, wodurch Bürger diese schnell und rechtssicher erhalten und weiterverwenden können. Der Ursprung der Dokumente ist validierbar. Ein Beispiel für einen vereinfachten und effizienteren Ablauf eines C2G-Prozesses ist die Ummeldung eines Wohnsitzes des Bürgers. Aktuell ist eine Ummeldung nur mit Personalausweis in Präsenz beim Amt möglich und die Meldebestätigung wird dem Bürger schriftlich ausgestellt, die anschließend im Ermessen des Bürgers verwahrt werden muss. Mit der Verwendung einer OrgID kann die Behörde eine Meldebestätigung digital signieren und dem Bürger ausstellen. Dieser kann das Dokument in seiner digitalen Brieftasche, die an ihn gebunden ist, hinterlegen und sicher verwahren. Wenn der Bürger Behörden oder anderen Parteien die ausgestellte Meldebestätigung präsentiert, können diese unabhängig durch die digitale Signatur die Authentizität des Dokuments validieren. Der Bürger hat alle behördlichen Dokumente, die von einer OrgID ausgestellt wurden, an einem sicheren digitalen Ort und muss sich nicht mehr um die physische Verwahrung kümmern.

Ebenso wie papierne Nachweise unterliegen auch (qualifizierte) elektronische Attributsbescheinigungen teilweise jahrzehntelangen Aufbewahrungsfristen. Um diese zu erfüllen, müssen (Q)EAA oder pubEAA durch (qualifizierte)

Bewahrungsdienste (Beweis und Prüfbarkeit) und/oder Archivierungsdienste (Nutzbarkeit & Zuverlässigkeit) sicher aufbewahrt werden.

OrgID: B2G

Im B2G (Business to Government) Bereich spielt die OrgID für beide Parteien eine wichtige Rolle. Sie ermöglicht auf beiden Seiten entsprechend dem Zero Trust Prinzip zweifelsfrei die Identität des Gegenübers festzustellen, was Grundvoraussetzung für einen sicheren, digitalen Datenaustausch ist.

Viele Unternehmen müssen gegenüber Behörden verschiedenen Nachweispflichten nachkommen, um ihren Betrieb aufrechtzuerhalten und gesetzlichen Regelungen nachzukommen. Aktuell werden Dokumente zu Zertifizierungen und Auditierungen häufig auf Papier ausgestellt und unterschrieben. Diese müssen dann bei der jeweiligen Behörde eingereicht und überprüft werden. Die Verwendung von OrgIDs gestaltet den Prozess deutlich einfacherer und sicherer, indem die Dokumente von Auditoren, welche ebenfalls (in Vollmacht) eine OrgID nutzen, als digitale Nachweise ausgestellt und an das auditierte Unternehmen gebunden werden. Die Unternehmen, denen solche Nachweise ausgestellt wurden, können diese anschließend einer Behörde zur Bewertung freigeben. Diese kann unabhängig von Dritten verifizieren, dass der zu erbringende Nachweis von einem akkreditierten Auditor ausgestellt wurde. Um diesen Prozess jedoch zu ermöglichen, benötigt es zusätzliche Register, in denen zugelassene vertrauenswürdige Aussteller von Nachweisen hinterlegt sind. Insgesamt werden solche Prozesse dadurch sicherer, dass die digitalen Signaturen sowie alle anderen Daten wie der Nachweisempfänger fälschungssicher ausgestellt werden.

OrgID: G2G

Bei der innerbehördlichen Kommunikation können standardisierte Organisationsidentitäten ebenfalls verschiedene Vorteile mit sich bringen. Wie bei der Beziehung von Nutzer zu Behörden ermöglicht auch hier eine Organisationsidentität die eindeutige und gegenseitige Identifizierung zweier miteinander datenaustauschender Behörden. Die jeweils von den Behörden ausgestellten Nachweise und Dokumente, können anhand der jeweiligen digitalen Signatur auf schnelle und einfache Weise verifiziert werden. So könnten beispielsweise bei Bauvorhaben das Bauamt und die Denkmalbehörde beim Datenaustausch sich sicher gegenseitig authentifizieren und entsprechende Nachweise austauschen.

Beim gegenseitigen Gewähren von Zugriff auf die Datenbestände der anderen Partei könnten Behörden diese Zugriffsberechtigung durch eindeutige und standardisierte Organisationsidentitäten sicher je Behörde regeln. Damit werden Genehmigungsprozesse für den Datenzugriff einfacher und die Verifizierung von behördlichen Nachweisen kann automatisiert werden. Es entstehen vollautomatisierte Workflows, Bearbeitungszeiten werden dadurch verkürzt und eine deutliche Reduktion in Verwaltungsaufwänden insgesamt ist das Ergebnis. Zugleich wird durch den höheren Grad an Automatisierung die Zahl manueller Fehler verringert. Dies funktioniert auch grenzüberschreitend: So könnte sich z. B. eine EU-Bürgerin beim Umzug in einen anderen EU-Mitgliedsstaat bei der entsprechenden Behörde am Zielort anmelden, während die Abmeldung vollautomatisiert an die Meldebehörde im EU-Staat des ehemaligen Wohnsitzes mitgeteilt wird.

In Deutschland gibt es teilweise technische Lösungen, aber auch Online-Fachverfahren, um Behörden bei der digitalen Kommunikation eindeutig zu authentifizieren und einen sicheren Datenaustausch zu gewährleisten. Durch die „Verordnung des Europäischen Parlaments und des Rates über Maßnahmen für ein hohes Maß an Interoperabilität des öffentlichen Sektors in der Union“ (kurz: Verordnung für ein interoperables Europa) wird auch für grenzüberschreitende Anwendungsfälle auf EU-Ebene eine sichere und interoperable Zusammenarbeit gefordert. Eindeutige, sichere und verifizierbare Organisationsidentitäten sind die Grundlage für solch ein interoperables und digitales Europa. Erst durch die sichere Authentifizierung von Behörden mit Hilfe von Organisationsidentitäten ist eine sichere und vertrauenswürdige behördliche Kommunikation über Ländergrenzen hinweg möglich.

Dafür muss jedoch eine technische Möglichkeit geschaffen werden, entsprechende Behörden im europäischen Raum zu finden und zu identifizieren. In Deutschland haben wir mit dem Diensteverzeichnis der öffentlichen Verwaltung (DVDV) eine Art „Telefonbuch“ für Verwaltungsleistungen im deutschen Behördenkontext. Erst auf Basis von verifizierbaren Organisationsidentitäten kann die behördliche grenzüberschreitende Zusammenarbeit innerhalb der EU ermöglicht werden. Ein Diensteverzeichnis auf europäischer Ebene ist nur durch eine standardisierte, in Europa anerkannte Organisationsidentität (für Behörden und Unternehmen) umsetzbar. Solch ein paneuropäisches Diensteverzeichnis ermöglicht erst das schnelle Auffinden und Authentifizieren der gesuchten Behörden im europäischen Raum, was die Grundvoraussetzung für ein digitales und interoperables Europa ist.

Auch für die Registermodernisierung und für das National-Once-Only-Technical-System (NOOTS) Prinzip spielen Organisationsidentitäten im Verwaltungskontext eine bedeutende Rolle. NOOTS besagt, dass personen- und unternehmensbezogene Daten idealerweise nur einmal erfasst, aber von verschiedenen Behörden (nach Freigabe durch Nutzer / Unternehmen) bei Bedarf von Behörden zugegriffen werden können. Mit Hilfe von Organisationsidentitäten für Behörden und Verwaltungen könnten Nutzer und Unternehmen diesen Zugriff je authentifizierter Behörde individuell freigeben. Behörden können sich mit ihrer Organisationsidentität beim Zugriff eindeutig ausweisen und so den Zugriff (sofern berechtigt) legitimieren.

Know-your-Customer-Prozesse

Die neue EU-Verordnung zur Verhinderung der Nutzung des Finanzsystems für Zwecke der Geldwäsche und der Terrorismusfinanzierung (kurz: EU-AMLR) tritt im Sommer 2027 in Kraft. Zu diesem Zeitpunkt müssen die Verpflichteten – meistens Banken – zusätzliche Daten vom Kunden einholen. Das bedeutet für Banken mit Fokus auf Unternehmenskunden, dass sie erheblich mehr Aufwand in der Datenbeschaffung haben werden. So werden der Legal Entity Identifier, der Gründungsort sowie weitere Informationen zu den wirtschaftlich Berechtigten verlangt.

Hier kann eine europäische OrgID unterstützen. Diese OrgID dient als Identifier für ein Wallet, das alle relevanten KYC-Informationen enthält. Die Befüllung des Wallets erfolgt durch das Unternehmen selbst, wird allerdings unterstützt durch automatisierte Befüllungen aus öffentlichen Registern wie z. B. das Handelsregister. Dass ein Handelsregister allein nicht ausreichend ist, liegt an der umfangreichen Anforderung der EU-AMLR.

Für KYC ist eine Verknüpfung der Unternehmensdaten mit den persönlichen Daten der auftretenden Person und der wirtschaftlichen Eigentümer notwendig. In der Wallet können die Unternehmen und die natürlichen Personen ihre elektronischen Identitäten hinterlegen. Das Unternehmen ist dafür verantwortlich, dass die Daten immer aktuell sind. Die Banken erhalten mit einer Abfrage alle relevanten KYC-Informationen.

Für eine weitere Erleichterung kann eine OrgID bzw. das Wallet sorgen. In der neuen EU-AMLR wurden die Aktualisierungszyklen für die Kunden reduziert – für Kunden mit hohem Risiko auf 1 Jahr (aktuell 2 Jahre) und für Kunden mit normalem Risiko auf 5 Jahre (aktuell 10 Jahre). Durch diese Verkürzung des Aktualisierungszeitraums erhöht sich der Aufwand bei den Banken enorm. Eine europäische OrgID mit den relevanten Informationen und Dokumenten in dem Wallet kann hier Abhilfe schaffen.

Bitkom vertritt mehr als 2.200 Mitgliedsunternehmen aus der digitalen Wirtschaft. Sie generieren in Deutschland gut 200 Milliarden Euro Umsatz mit digitalen Technologien und Lösungen und beschäftigen mehr als 2 Millionen Menschen. 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, kreieren Content, bieten Plattformen an oder sind in anderer Weise Teil der digitalen Wirtschaft. 82 Prozent der im Bitkom engagierten Unternehmen haben ihren Hauptsitz in Deutschland, weitere 8 Prozent kommen aus dem restlichen Europa und 7 Prozent aus den USA. 3 Prozent stammen aus anderen Regionen der Welt. 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 leistungsfähigen und souveränen Digitalstandort zu machen.

Herausgeber
Bitkom e.V.
Albrechtstr. 10 | 10117 Berlin

Ansprechpartner
Clemens Schleupner
T 030 27576-424 | c.schleupner@bitkom.org

Verantwortliches Bitkom-Gremium
Arbeitskreis Digitale Identitäten

Projektleitung
Clemens Schleupner

Titelbild
© jerome – unsplash.com