moysies & partners
fine consulting

Der Schlüssel zur digitalen Verwaltung

Konten für Bürger:innen und Unternehmen

Liebe Leser:innen,

kennen Sie das? Am frühen Morgen im Minutentakt den Webbrowser aktualisieren, in der Hoffnung, dass sich doch noch ein freier Termin im Online-Kalender des Bürgeramts auftut, sodass man endlich den abgelaufenen Personalausweis verlängern lassen kann? In manchen Städten Deutschlands muss man hierfür auf ungefähr so viel Glück hoffen wie sonst nur bei der Chance, einen Sechser im Lotto zu landen.

Doch warum müssen wir heute überhaupt noch Termine bei Behörden wahrnehmen? Könnten die meisten Verwaltungsdienstleistungen nicht online angeboten werden? In Zeiten von Homeschooling und Videokonferenzen fühlt sich dieser Schritt längst überfällig an. Denn die neuen Bedingungen erfordern auch auf Seiten der Verwaltung mehr Flexibilität. Die beste Nachricht vorweg: Die Zeichen für mehr Digitalisierung stehen außerordentlich gut! Allen voran durch das Onlinezugangsgesetz (OZG) wurden die gesetzlichen Weichen für den Zugang zu elektronischen Verwaltungsdienstleistungen bereits gestellt. Bürger:innen und Unternehmen sollen dabei auf einfache Weise Zugang zur digitalen Verwaltung mithilfe von Nutzerkonten auf Landes- und Bundesebene sowie des ELSTER-Unternehmenskontos erhalten. Ein einziger digitaler Account also für sämtliche Verwaltungsangebote von Bund, Ländern und Kommunen. So lassen sich künftig unnötige bürokratische Hürden abbauen, Behördengänge reduzieren und die Verwaltung entlasten sowie vereinfachen.

Als **moysies & partners** begleiten wir seit Jahren zahlreiche öffentliche Verwaltungen bei der Umsetzung ihrer Digitalisierungsprojekte. Dabei spielen Vorhaben im Kontext der Kontenlösungen[1] eine zentrale Rolle – ein Gebiet, auf dem sich zuletzt viel Neues ereignet hat. Wir freuen uns deshalb, diesen Fortschritt in unserem Kompendium zu präsentieren und damit aktiv den Diskurs zwischen Stakeholdern sowie Interessierten zu fördern. Das Thema der Kontenlösungen begeistert uns! Nicht nur, weil es trotz seines Nischendaseins uns alle betrifft – ob als Bürger:in oder Unternehmer:in –, sondern auch, weil ihm eine wichtige Schlüsselfunktion in der Digitalisierung unserer Verwaltung zukommt.

Gegenwärtige Diskussionen im Hinblick auf die Bereitstellung und Ausgestaltung der Nutzerkonten von Bund und Ländern zeigen die dynamische Entwicklung dieses Themenfeldes. Wir sind uns sicher: Die Spannung wird dabei so schnell nicht verloren gehen. In diesem Sinne wünschen wir Ihnen beim Lesen des Kompendiums viel Vergnügen und vor allem viele neue Erkenntnisse und frische Anregungen!

Frederike Knuth, Friederike Martin, Maj-Britt Rosier, Sarah Naumann

[1] Die Bezeichnung „Kontenlösungen“ wurde als Überbegriff für die Nutzerkonten und das ELSTER-Unternehmenskonto gewählt.

INHALT

4 **Appetizer**

5 **Abkürzungsverzeichnis**

8-10 **Was bedeutet eigentlich … ?**
Eine Übersicht der wichtigsten Begrifflichkeiten

11-15 **Der rechtliche Rahmen der Nutzerkonten**
OZG, DSGVO, eIDAS-Verordnung und Co.: Die Umsetzung der Kontolösungen wird von zahlreichen Gesetzen und Vorgaben beeinflusst.

16-28 **Eine digitale Identität für alles**
Ein technischer Einblick hinter die Kulissen der Interoperabilität von Prof. Dr. Wolfgang Hommel, Dr. Daniela Pöhn und Michael Grabatin

29-33 **Von der Idee bis zur Umsetzung: Der Weg der interoperablen Nutzerkonten in Deutschland**
Ein Interview mit Martin Kirschenbauer

34-35 **Referent:innen**

36-37 **Die Landschaft der Nutzerkonten in Deutschland**
Nutzerkonten: ein Schlüssel zur digitalen Verwaltung. Doch was können sie eigentlich?
Und wie können Bürger:innen sie nutzen?

38-39 **Think FINK!**
Zugang zu Online-Verwaltungsleistungen in allen Bundesländern – mit nur einem einzigen Nutzerkonto. Wie das möglich ist? Mit Interoperabilität! Ein Text von Dominik Hiemer

40-55 **Das ELSTER-Unternehmenskonto als große Chance**
Wie das einheitliche ELSTER-Unternehmens-konto den Behördenkontakt vereinfacht? Jens Viere weiß mehr.

56-61 **Die Identitäten der Zukunft**
Der selbstbestimmte Umgang mit digitalen Identitäten. Ein Text von Prof. Dr. Wolfgang Hommel, Dr. Daniela Pöhn und Michael Grabatin

62-71 **What's next? Digitale Identitäten als europäische Aufgabe**
Und was macht eigentlich die EU? Sie TOOP(t)! Prof. Dr. Dr. Robert Krimmer wirft einen Blick auf den europäischen digitalen Binnenmarkt und das Once-Only-Prinzip.

72-75 **Once-Only? Only Open Source!**
Das estnische Erfolgsrezept für die Akzeptanz der digitalen Verwaltung.
Ein Text von Chiara Stuttfeld

Glossar 76-79

Fazit und Danksagung 80

Impressum 81

„Der Kreativität sind bei der Weiterentwicklung des Unternehmenskontos kaum Grenzen gesetzt.“

– Jens Viere, Referent im Bayerischen Staatsministerium für Digitales

„Das Beispiel Estland zeigt: Ein zentrales Nutzerkonto wie im Fall von X-Road wird vor allem dann angenommen, wenn es als Tool für die Bürger:innen zur Wahrnehmung ihrer Informations- und Auskunftsrechte konzipiert ist und nicht als komfortables Datenerhebungsinstrument für die Behörde.“

– Chiara Stuttfeld, Junior Marketing und Vertrieb bei publicplan GmbH

„Wichtig für die Zukunft wird es sein, diesen Onlinezugang des Bürgers zur Verwaltung weiterhin auszubauen und vor allem nutzerfreundlich zu gestalten.“

– Martin Kirschenbauer, stellvertretender Referatsleiter im Referat B3.3 im Bayerischen Staatsministerium für Digitales

„Wir dürfen auf die weiteren Entwicklungen im Bereich des europäischen E-Government sehr gespannt sein und hoffen, dass die technischen Lösungen auch das Interesse und die regelmäßige Nutzung durch die Bürger:innen in Zukunft in den Vordergrund stellen.“

– Prof. Dr. Dr. Robert Krimmer, Professor für e-Governance an der Universität Tartu in Estland

„Die Umsetzung der knapp 600 OZG-Leistungen und Online-Verfahren mit ihrer Anbindung an den Verbund der Nutzerkonten ist noch in Arbeit. Ausschlaggebend für den Erfolg ist dabei aber nicht nur die reine Anzahl online verfügbarer Leistungen, sondern auch deren Nutzung und Akzeptanz.“

– Prof. Dr. Wolfgang Hommel, Professor für IT-Sicherheit von Software und Daten an der Universität der Bundeswehr München (UniBw M), Dr. Daniela Pöhn, wissenschaftliche Mitarbeiterin an der Professur für IT-Sicherheit von Software und Daten an der UniBw M & Michael Grabatin, Promovierender am Forschungsinstitut Cyber-Defence der UniBw M

Abkürzungsverzeichnis

AAI	Authentifizierungs- und Autorisierungsinfrastruktur
ABAC	Attribute-based Access Control
BMI	Bundesministerium des Innern und für Heimat
BRIS	Business Registers Interconnection System
BSI	Bundesamt für Sicherheit in der Informationstechnik
DE4A	Digital Europe for All
DFN	Deutsches Forschungsnetz
DIHK	Deutscher Industrie- und Handelskammertag
DLT	Distributed Ledger Technologie
eIDAS	electronic Identification, Authentication and trust Services
EU	Europäische Union
EUCARIS	European Car and Driving Licence Information System
EWR	Europäischer Wirtschaftsraum
FIM	Föderiertes Identitätsmanagement
FINK	Föderiertes Identitätsmanagement Interoperabler Nutzerkonten in Deutschland
IDP	Identity Provider (beziehungsweise Asserting Party; eigenes oder zusicherndes Servicekonto)
IoT	Internet-of-Things
IT	Informationstechnik
I&AM System	Identity & Access Management System
JSON	JavaScript Object Notation
KIOSK	Kompetenzzentrum Interoperable Servicekonten
LDAP	Lightweight Directory Access Protocol
LoAs	Levels of Assurance (Vertrauensniveaus)
LSP	Large-scale Pilot Projects
UK	Unternehmenskonto
NEZO	Nutzung der ELSTER-Zertifikate im Rahmen des OZG
OAuth	Open Authorization
OZG	Onlinezugangsgesetz
PKI	Public-Key-Infrastruktur
REST-API	Representational State Transfer- Anwendungsprogrammierschnittstelle
SAML	Security Assertion Markup Language
SP	Service Provider
SSI	Self-Sovereign Identity (selbstbestimmte Identitäten)
StMD	Bayerisches Staatsministerium für Digitales
STORK (2.0)	Secure Identity across Borders linked (2.0)
SPOCS	Simple Procedures Online for Cross-border Services
TOOP	The Once-Only Principle Project
TOOPRA	TOOP Reference Architecture
TR	Technische Richtlinie
User-ID	User identifier (Benutzer-Identifikationsnummer)
XML	eXtensible Markup Language

Der beste Weg, um die Komplexität der digitalen Verwaltung aufzubrechen? Die Dinge wirklich durchdringen zu wollen!

WAS BEDEUTET eigentlich...

Konten

Servicekonto?
Das Bundesamt für Sicherheit in der Informationstechnik (BSI) versteht unter dem Begriff der Servicekonten elektronische Komponenten, die einerseits die Identifizierung von Nutzer:innen und anderseits die Verwendung und Verwaltung von Nutzerkonten ermöglichen. Als Identifizierungskomponente stellt das Servicekonto die in einem Nutzerkonto gespeicherten Identitätsdaten der Nutzer:innen einer Onlineleistung zur Verfügung. Die Verwaltungsvereinbarung zwischen Bund und Ländern über die Weiterentwicklung und den Betrieb von FINK verwendet hingegen Servicekonten synonym zum Begriff der Nutzerkonten. Der Verwaltungsvereinbarung folgend nutzen wir in diesem Kompendium ebenfalls ausschließlich den Begriff „Nutzerkonto“.

Nutzerkonto?
Das OZG versteht in Art. 2 Abs. 5 unter Nutzerkonten „eine zentrale Identifizierungs- und Authentifizierungskomponente, die eine staatliche Stelle anderen Behörden zur einmaligen oder dauerhaften Identifizierung und Authentifizierung der Nutzer zu Zwecken der Inanspruchnahme von Verwaltungsleistungen der öffentlichen Verwaltung bereitstellt. Ein Nutzerkonto kann als Bürger- oder Organisationskonto angeboten werden.“ Die Verwaltungsvereinbarung FINK hingegen nutzt den Begriff der Nutzerkonten ausschließlich bei Kontenlösungen für Bürger:innen. Daher wird in diesem Kompendium auf die Begriffsverwendung der Verwaltungsvereinbarung zurückgegriffen. Das Nutzerkonto ermöglicht Bürger:innen einen einheitlichen Zugang zu den digitalen Dienstleistungen der Verwaltung in Bund, Ländern und Kommunen. So können mit einem einmalig eingerichteten Konto künftig alle Verwaltungsleistungen genutzt werden – unabhängig davon, bei welchem Teilnehmer des Portalverbunds das Konto angelegt wurde. Perspektivisch ist es geplant, die Funktionalität der Nutzerkonten zu erhöhen und Postfächer, Rückkanäle, sowie die Interoperabilität aller Konten zu verstärken.

Unternehmenskonto?
Das OZG spricht in Art. 2 Abs. 5 von Organisationskonten, um zu unterstreichen, dass die Nutzung des Kontos nicht explizit für Unternehmen, sondern auch für weitere Organisationen, beispielsweise Vereine oder Behörden, offen ist. Natürliche Personen haben ebenfalls die Möglichkeit, für eine gewerbliche oder berufliche Tätigkeit ein Organisationskonto anzulegen. Die bundeseinheitliche Umsetzung des Organisationskontos findet auf Basis von ELSTER statt. In diesem Kontext hat sich der Begriff des ELSTER-Unternehmenskontos etabliert. Seit dem 1. Juni 2021 dient das bundeseinheitliche Unternehmenskonto auf ELSTER-Basis Unternehmen in ganz Deutschland als zentraler Einstiegspunkt für die Kommunikation mit Behörden. Das ELSTER-Unternehmenskonto ist für juristische Personen, wie Organisationen und Unternehmen, vorgesehen, die sich mit einem einfachen zentralen Zugang authentifizieren und auf digitale Verwaltungsleistungen zugreifen möchten. Hierzu werden ELSTER-Zertifikate als Identifizierungs- und Authentifizierungsmittel genutzt. Trotz der rechtlichen Begriffsbestimmung wird in der öffentlichen Kommunikation häufig weiterhin die Bezeichnung „Unternehmenskonto“ verwendet. Daher wird im Folgenden ausschließlich auf die Formulierung „Unternehmenskonto“ zurückgegriffen.

Identifizierung?
Unter dem Begriff der Identifizierung wird die Erbringung eines Nachweises einer behaupteten Identität verstanden. Eine Person kann sich über die Angaben zum Vor- und Nachnamen, Geburtsort und Geburtstag eindeutig identifizieren.

BMI (o.J.): Nutzerkonten. https://www.onlinezugangsgesetz.de/Webs/OZG/DE/umsetzung/ozg-infrastruktur/nutzerkonten/nutzerkonten.html [03.05.22] | **StMD** (o.J.): Digitales Unternehmenskonto. https://www.stmd.bayern.de/themen/digitale-verwaltung/digitales-unternehmenskonto/ [04.05.22] | **Pohlmann, Norbert** (o.J.): Identifikation und Authentifikation. https://norbert-pohlmann.com/wp-content/uploads/2019/08/Identifikation-und-Authentifikation-Vorlesung-Cyber-Sicherheit-Prof-Norbert-Pohlmann-18_03_20.pdf [04.05.22] | **Lewandowska, Eva** (2018): Identifizieren versus Authentifizieren. https://authada.de/identifizierung-vs-authentifizierung [02.05.22] | **BMI** (2021): Das Nutzerkonto Bund. https://www.cio.bund.de/SharedDocs/Publikationen/DE/Innovative-Vorhaben/das_nutzerkonto_bund_0620.pdf?__blob=publicationFile [03.05.22]

Authentifizierung?
Bei der Authentifizierung hingegen wird der Nachweis erbracht, dass eine Person tatsächlich die behauptete Identität besitzt. Gängige Authentifizierungsverfahren sind unter anderem die Eingabe eines Passworts oder die Authentifizierung mithilfe des eigenen Fingerabdrucks. Die Authentifizierung geht in der Praxis häufig eng mit der Identifizierung einher: Um sich authentifizieren zu können, beispielsweise gegenüber einer online angebotenen Verwaltungsleistung, muss zunächst über einen Benutzernamen die Identifizierung erfolgen. Anschließend erfolgt die Authentifizierung, die belegt, dass eine Person tatsächlich diejenige ist, die sie mittels Benutzernamen vorgibt.

Vertrauensniveaus?
Entsprechend den Vorgaben der europäischen Verordnung über elektronische Identifizierung und Vertrauensdienste (eIDAS-VO) gelten für Nutzerkonten unterschiedliche Vertrauensniveaus. Diese beschreiben den Grad der Vertrauenswürdigkeit eines elektronischen Identifizierungsmittels zur Identitätsfeststellung einer Person. Je höher das Vertrauensniveau, desto höher ist auch der Grad der Vertrauenswürdigkeit bei der Identitätsfeststellung.

Interoperabilität?
Im vorliegenden Kontext bedeutet Interoperabilität die Verknüpfung der Nutzerkonten der Länder und des Nutzerkontos Bund. Das soll Bürger:innen und Organisationen ermöglichen, mit nur einer Kontoanmeldung beim Nutzerkonto eines Landes oder des Bundes alle Onlinedienstleistungen von Bund, Ländern und Kommunen nutzen zu können. Das BSI definiert Interoperabilität konkret als „Fähigkeit, zwischen verschiedenen Funktionseinheiten in einer Weise zu kommunizieren, Programme auszuführen oder Daten zu übertragen, die erfordert, dass der Benutzer wenig oder gar keine Kenntnis von den einzigartigen Eigenschaften dieser Einheiten hat."

Der rechtliche RAHMEN der Nutzerkonten

Auf EU-Ebene

eIDAS-Verordnung
Eine europaweite rechtliche Basis für elektronische Identifizierungsmittel, Vertrauensdienste sowie für elektronische Signaturen, Siegel und Zeitstempel wurde mit der im September 2014 in Kraft getretenen „Verordnung (EU) Nr. 910/2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG" (kurz: eIDAS-Verordnung) geschaffen. Die eIDAS-Verordnung zielt darauf ab, sichere und vertrauensvolle elektronische Transaktionen zwischen Behörden, Bürger:innen und Unternehmen grenzüberschreitend zwischen den EU-Staaten zu ermöglichen. Zur Gewährleistung des effektiven Vollzugs der eIDAS-Verordnung wurde am 29. März 2017 durch die Bundesregierung das Gesetz zur Durchführung der eIDAS-Verordnung der EU (kurz: eIDAS-Durchführungsgesetz) verabschiedet. Die eIDAS-Verordnung stellt die Grundlage für die Festlegung von Vertrauensniveaus der Nutzerkonten dar. Anmeldung und Authentifizierung sollen dabei mit dem Grad an Vertraulichkeit und Sicherheit erfolgen, der durch die ausgewählte Verwaltungsdienstleistung vorgegeben wird. Die interoperablen Nutzerkonten müssen sich im europäischen Rechtsrahmen für die elektronische Identifizierung und Vertrauensdienste bewegen und den eIDAS-Anforderungen entsprechen.

SDG-Verordnung
Mit der „Single Digital Gateway"-Verordnung (EU) 2018/1724 (kurz: SDG-VO) beschlossen das Europäische Parlament und der Rat im Oktober 2018 die Einrichtung eines einheitlichen digitalen Zugangstors zur Verwaltung in der EU. Dafür sollen die verschiedenen Portale, Systeme und Dienste, die in den EU-Mitgliedstaaten existieren, erweitert und miteinander verknüpft werden. Unter anderem sollen so Verwaltungsleistungen über ein einziges europäisches Portal abrufbar sein. Kernanforderungsbereich an das interoperable Nutzerkonto ist hiernach der Zugang zu Online-Verfahren.

StMD, IT-Planungsrat (2021): Verwaltungsvereinbarung über die Weiterentwicklung und den Betrieb von FINK. https://dokumente.landtag.rlp.de/landtag/vorlagen/31-V-18.pdf [05.05.22] | **Klein, Manfred** (2017): Was ist ein Nutzerkonto? https://www.egovernment-computing.de/was-ist-ein-nutzerkonto-a-781394/ [04.05.22]

Once-Only-Principle

Das Once-Only-Principle (OOP) wurde von der EU-Kommission als „Grundsatz der einmaligen Erfassung“ im Rahmen des E-Government-Aktionsplans von 2016 bis 2020 formuliert und in Artikel 14 der SDG-Verordnung (EU) 2018/1724 gesetzlich festgehalten. Die eIDAS-Verordnung dient als Rahmenbedingung für das OOP.

Das Prinzip besagt, dass Bürger:innen und Unternehmen ihre Daten und Dokumente den Behörden und Verwaltungen nur noch einmal mitteilen müssen, sodass deren administrative Belastung erheblich reduziert wird. Unter Einbeziehung von Datenschutzbestimmungen und der expliziten Zustimmung der Nutzer:innen ist es der öffentlichen Verwaltung erlaubt, die Daten wiederzuverwenden und untereinander auszutauschen. Nachweisdokumente werden so schrittweise durch Registerabfragen und zwischenbehördliche Datenaustausche ersetzt. Die Umsetzung des OOP geht einher mit dem geplanten Aufbau des SDG.

Das Prinzip der interoperablen Nutzerkonten entspricht bereits den Grundsätzen des OOP: Auch hier werden bestimmte Informationen bei der Registrierung in einem Nutzerkonto einmalig eingegeben und bei der Anmeldung im Rahmen der Interoperabilität zwischen den Nutzerkonten ausgetauscht.

Auf nationaler Ebene

OZG

Das Onlinezugangsgesetz (OZG) trat im August 2017 in Kraft und verpflichtet Bund und Länder, ihre Verwaltungsleistungen bis Ende 2022 auch elektronisch über Verwaltungsportale anzubieten. Die Verwaltungsportale von Bund und Ländern müssen zu einem Portalverbund verknüpft und Nutzerkonten bereitgestellt werden (vgl. §3 OZG). Für die Umsetzung des Onlinezugangsgesetzes ist die Interoperabilität somit eine zwingende Bedingung. §8 des OZG erlaubt zu diesem Zweck die Speicherung der Identitätsdaten bei Zustimmung durch den/die Bürger:in. Grundlage des OZG ist unter anderem die 2014 in Kraft getretene eIDAS-Verordnung (EU), die verbindliche europaweit geltende Regelungen in den Bereichen „Elektronische Identifizierung“ und „Elektronische Vertrauensdienste“ festlegt. Das OZG wird durch verschiedene Rechtsverordnungen spezifiziert, die Auswirkungen auf die interoperablen Nutzerkonten mit sich bringen können, wie beispielsweise durch das Inkrafttreten der IT-Sicherheitsverordnung Portalverbund Anfang 2022 (ITSiV-PV).

DSGVO & BDSG

Seit Mai 2018 gilt die Datenschutz-Grundverordnung (DSGVO) unmittelbar in allen EU- Mitgliedstaaten/EWR und regelt europaweit einheitlich den Umgang mit personenbezogenen Daten. Das betrifft sowohl die (teilweise) automatisierte Verarbeitung von Daten als auch nichtautomatisierte Datenspeicher. Die rechtliche Grundlage für den Datenschutz in Deutschland wurde 2018 mit dem neuen Bundesdatenschutzgesetz (BDSG) geschaffen. Als Ergänzung und Konkretisierung der DSGVO-Vorgaben werden mit dem BDSG spezifische Vorschriften auf nationaler Ebene formuliert. Dabei ist das BDSG der DSGVO unterstellt und liefert Vorschriften für Anwendungsfälle, welche die DSGVO offenlässt.

Auch interoperable Nutzerkonten müssen die Datenschutzvorschriften einhalten. Innerhalb des Nutzerkontos werden personenbezogene Daten von Büger:innen gespeichert und im Rahmen der Interoperabilität ausgetauscht. Die DSGVO sieht vor, dass diese Daten rechtsgemäß geschützt werden und die Hoheit der Daten bei den Nutzer:innen verbleibt. Gemäß dieser Rechtsgrundlage muss ein Nutzerkonto die technische Voraussetzung haben, die es Nutzer:innen ermöglicht, ihre gespeicherten Daten zu korrigieren oder das Nutzerkonto jederzeit zu löschen. Bevor personenbezogene Daten unter dem Schutz der DSGVO gespeichert werden, müssen bestimmte Vorbereitungsvorgänge eingebaut werden, damit die Nutzer:innen dieser Speicherung zustimmen können. Die Verwendung einer nationalen Kennziffer (wie der Steuer-ID) zu Identifizierungszwecken ist nach Art. 87 DSGVO zulässig, solange Datenschutz besteht.

Glockner, Wolf-D. (o.J.): eIDAS-Durchführungsgesetz in Kraft getreten. https://www.deutsches-ausschreibungsblatt.de/2/standard-titel-1/das-eidas-durchfuehrungsgesetz-ist-in-kraft-getreten/ [25.04.22] | **BMI** (o.J.): Grundsätzliche Anforderungen an die EU-Mitgliedstaaten. https://www.onlinezugangsgesetz.de/Webs/OZG/DE/grundlagen/info-sdg/sdg-anforderungen/sdg-anforderungen-node.html [27.04.22] | **BMI** (o.J.): Prinzip des Servicestandards. https://www.onlinezugangsgesetz.de/Webs/OZG/DE/umsetzung/servicestandard/prinzip-4/prinzip-4-node.html [25.04.22] | **Brüstle, Henning & Ehneß, Susanne** (2018): Die DSGVO und ihre Bedeutung für öffentliche Institutionen. https://www.egovernment-computing.de/die-dsgvo-und-ihre-bedeutung-fuer-oeffentliche-institutionen-a-683645/ [28.04.22] | **BSI** (o.J.): BSI TR-03160 Servicekonten. https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03160/tr03160_node.html;jsessionid=6CA58C704C925667E4DDCF1CE17D1E14.internet472 [27.04.22]

BSI-TR

Die vom Bundesamt für Sicherheit in der Informationstechnik herausgegebenen Technischen Richtlinien (BSI-TR) zielen auf die Verbreitung von angemessenen IT-Sicherheitsstandards ab. Sie ergänzen die technischen Prüfvorschriften des BSI und bieten Methoden und Kriterien für Konformitätsprüfungen. Nach § 8 Abs. 3 OZG hat das BSI den Auftrag, die technischen Anforderungen an die Nutzerkonten und deren Verknüpfung, vor allem Datenschutz und Datensicherheit, in einer Technischen Richtlinie festzulegen. Interoperable Konten müssen in ihrer Rolle als Identity Provider (auch IdP oder zusichernde Parteien genannt) sowie als Service Provider (SP oder vertrauende Parteien genannt) des föderierten Identitätssystems bestimmte Anforderungen der BSI-TR erfüllen.

Bisher galten die Vorschriften des BSI als Richtschnur – seit Anfang 2022 wurde die Berücksichtigung der Anforderungen von vier BSI-TR mit Inkrafttreten der IT-Sicherheitsverordnung Portalverbund (ITSiV-PV) verpflichtend.

BMI (o.J.): Einer für Alle – Einfach erklärt. https://www.onlinezugangsgesetz.de/Webs/OZG/DE/umsetzung/nachnutzung/efa/efa-node.html [28.04.22] | **BMI** (2021): Wegweiser „Einer für Alle/Viele“. https://www.onlinezugangsgesetz.de/SharedDocs/downloads/Webs/OZG/DE/wegweiser-efa.pdf?__blob=publicationFile&v=4 [27.04.22]

Smart-eID-Gesetz

Im September 2021 ist das Gesetz zur Einführung eines elektronischen Identitätsnachweises mit einem mobilen Endgerät (kurz: Smart-eID-Gesetz) in Kraft getreten. Die Smart-eID bietet Bürger:innen die Möglichkeit, ihren Online-Ausweis direkt in ihrem Smartphone zu speichern. Die mobile Smart-eID ist eine Ergänzung zur existierenden eID-Lösung. Nutzer:innen können die Smart-eID kostenlos mit der Ausweis-App 2 unter einmaliger Verwendung der Ausweiskarte selbstständig erstellen. Die Personendaten werden dabei aus der Ausweiskarte abgeleitet und in einem sogenannten Vertrauensanker im Smartphone abgelegt. Das Smart-eID-Gesetz stellt mitunter neue Anforderungen an die Identifizierungs- und Authentifizierungsverfahren der Nutzerkonten.

Verwaltungsverfahrensgesetze

Bund & Länder

Das Verwaltungsverfahrensgesetz (VwVfG) enthält allgemeine Verfahrensgrundsätze für das Handeln für Behörden, die für alle Behörden gelten. Sowohl der Bund als auch die Länder verfügen über eigene Verwaltungsverfahrensgesetze. Um zu vermeiden, dass Bürger:innen und Unternehmen im Kontakt mit verschiedenen Behörden in unterschiedlichen Ländern und auf unterschiedlichen Ebenen voneinander abweichenden und/oder widersprüchlichen Regelungen begegnen, arbeiten Bund und Länder gemeinsam an der Fortentwicklung der Verwaltungsverfahrensgesetze. Änderungen in den Verwaltungsverfahrensgesetzen können neue oder veränderte rechtliche Anforderungen an interoperable Nutzerkonten und weitere Basiskomponenten beinhalten, wie zum Beispiel zur Bekanntgabe eines Verwaltungsakts.

BMI (o.J.): Verwaltungsverfahrensgesetz. https://www.bmi.bund.de/DE/themen/moderne-verwaltung/verwaltungsrecht/verwaltungsverfahrensgesetz/verwaltungsverfahrensgesetz-node.html [26.04.22] | **BMI** (2021): Online-Ausweis kann bald im Smartphone gespeichert werden: Smart-eID-Gesetz am 1. September in Kraft getreten. https://www.bmi.bund.de/SharedDocs/pressemitteilungen/DE/2021/09/smart-eID-gesetz-in-kraft.html [26.04.22]

EfA-Prinzip

Das „Einer für Alle“-Prinzip (EfA) leitet sich aus den Anforderungen des OZG ab und bedeutet, dass ein Land oder eine Allianz aus mehreren Ländern eine Leistung zentral entwickelt und betreibt sowie diese anschließend anderen Ländern und Kommunen zur Verfügung stellt, sodass diese den Dienst mit- beziehungsweise nachnutzen können. Bund und Länder haben in den „Einer für Alle“-Mindestanforderungen festgelegt, welche Kriterien ein Onlinedienst zu erfüllen hat, um im Sinne des EfA-Prinzips tatsächlich nachnutzbar zu sein. Die EfA-Mindestanforderungen besagen, dass interoperable Nutzerkonten an EfA-Leistungen angebunden sein müssen.

Eine digitale Identität für alles

So funktioniert die Technik hinter dem Verbund der Nutzerkonten

von Prof. Dr. Wolfgang Hommel, Dr. Daniela Pöhn und Michael Grabatin

Durch ein einziges persönliches Nutzerkonto werden alle OZG- und Online-Verwaltungsleistungen einfach zugänglich. Aber welche Abläufe stecken eigentlich dahinter? Und wie sieht es in Sachen IT-Sicherheit und Datenschutz aus? Wir werfen einen Blick hinter die Kulissen und zeigen, was hinter digitalen Identitäten und deren Anwendung im Verbund der Nutzerkonten steckt.

Egal, ob es ums Einkaufen im Internet, die Teilnahme an sozialen Netzwerken oder um die Nutzung von Onlinediensten für technische Geräte vom Smart Home bis zum modernen Auto geht: Am Anfang muss man sich zunächst registrieren. Daten wie Name und Anschrift sind einzutragen, die E-Mail-Adresse muss bestätigt werden, und spätestens wenn Geld fließen soll, sind die üblichen Bezahlinformationen anzugeben. Im Laufe der Zeit kommen auf diese Weise Dutzende von Online-Angeboten zusammen, denen man seine Daten völlig unabhängig voneinander anvertrauen muss. Ändert sich irgendwann beispielsweise die eigene Anschrift durch einen Umzug oder die Nummer der Kreditkarte, geht das Spiel von vorne los: Man ist eine Weile damit beschäftigt, um Änderungen überall anzupassen und gegebenenfalls erneute Nachweise für die Korrektheit der angegebenen Daten zu erbringen.

Bei Verwaltungsleistungen bot sich lange Zeit ein vergleichbares Bild. Wer einen neuen Personalausweis beantragen, seinen Führerschein umtauschen, Kindergeld beziehen oder heiraten wollte, musste Formulare ausfüllen. Name, Anschrift, das Übliche inklusive passender Nachweise – Bürokratie mit stereotypisch deutscher Gründlichkeit lässt grüßen. Mit der Umstellung auf digitalisierte Prozesse ergeben sich recht offensichtlich viele Gelegenheiten zur Verbesserung solcher Abläufe, durch die sich aus Nutzer:innenperspektive und auch dienstleisterseitig Vieles vereinfacht.

Was ist eine digitale Identität?

Onlinedienste wie Web-Shops oder Verwaltungsleistungen, die nicht anonym genutzt werden können, müssen zwischen den verschiedenen Nutzer:innen unterscheiden und ihnen Daten sowie Berechtigungen zuordnen können. Die digitale Identität ist damit zunächst nichts anderes als ein Datensatz, der seinem/seiner Nutzer:in, in der Regel einer natürlichen Person, eindeutig zugeordnet werden kann. Somit muss auch jeder einzelne Datensatz im gesamten Datenbestand eindeutig identifiziert werden können – er benötigt also einen Identifikator. An diesen Identifikator werden, außer seiner Eindeutigkeit, keine technischen Anforderungen gestellt. Unter Bezeichnungen wie „Username“, „Login-Name“, „User-ID“ oder „Kennung“ begegnet er uns bei jedem Dienst und Gerät, an dem man sich zur Nutzung anmelden muss. Dabei wird der Identifikator je nach Dienst entweder bei der anfänglichen Registrierung vorgegeben, kann selbst frei gewählt werden, oder die Nutzer:innen geben dafür ihre E-Mail-Adresse – wahlweise Telefonnummer – an, woraus sich implizit ein Kommunikationskanal für den Dienstanbieter ergibt.

Vor der Nutzung des Dienstes ist typischerweise eine als Authentifizierung bezeichnete Anmelde- beziehungsweise Login-Prozedur zu durchlaufen, bei der Nutzer:innen ihren Identifikator angeben und beweisen müssen, dass ihnen die jeweils angegebenen digitalen Identitäten gehören. Am bekanntesten und immer noch am weitesten verbreitet ist dabei eine Authentifizierung durch ein Passwort, also ein für die digitale Identität spezifisches Geheimnis, das nur die Nutzer:innen und der Dienstleister kennen sollen. Etwas allgemeiner können Nutzer:innen auf Basis von Wissen (zum Beispiel der Kenntnis eines Passworts oder einer PIN), Besitz (zum Beispiel einer Smartcard wie dem Personalausweis) oder biometrischen Merkmalen (zum Beispiel per Fingerabdruck oder Gesichtserkennung) authentifiziert werden. Wenn mehrere solcher Merkmale kombiniert überprüft werden, zusätzlich zu einem Passwort also zum Beispiel eine Smartcard eingesetzt wird, spricht man von der Mehrfaktor-Authentifizierung. Der Dienstleister muss folglich die Möglichkeit haben, im Rahmen des Authentifizierungsvorgangs vorgelegte Zugangsdaten (sogenannte Credentials) zu überprüfen und dazu bei sich entsprechende Daten sicher zu speichern.

Neben Identifikator und Credentials können im Datensatz einer digitalen Identität beliebige weitere Datenfelder hinterlegt werden. Sie werden aus der technischen Historie hinaus als Attribute bezeichnet. Dabei kann es sich einerseits um klassische Stammdaten wie Vorname, Familienname und Anschrift handeln – andererseits können für konkrete Dienste notwendige Angaben, beispielsweise eine Kontonummer, hinterlegt werden. Die Auswahl und der Umfang erfasster Attribute sind unter Datenschutzaspekten offensichtlich kritisch zu hinterfragen: Wird für das Erbringen eines Dienstes die Telefonnummer eines/einer Nutzer:in zum Beispiel nicht benötigt, so liegt auch kein Grund vor, diese zu erfassen und zu speichern.

Insgesamt ist eine digitale Identität also ein Datensatz, der aus einem Identifikator, Daten zur Abwicklung der Authentifizierung

Das digitale Versteckspiel wird durch Authentifizierungsverfahren gekonnt erschwert.

und beliebig vielen Attributen besteht. Den Attributen kommt dabei eine Schlüsselrolle zu: Aus ihnen lassen sich bestimmte Berechtigungen im Kontext der Dienstnutzung ableiten. Wendet sich eine bestimmte Verwaltungsleistung beispielsweise gezielt nur an Nutzer:innen, die ihren Hauptwohnsitz in einer bestimmten Stadt oder einem bestimmten Bundesland haben, so sind entsprechend Attribute zu erfassen und im Rahmen der Dienstnutzung zu überprüfen. Dieses Verfahren wird als attributbasierte Zugriffskontrolle („Attribute-based Access Control“), kurz: ABAC, bezeichnet.

Von einzelnen Diensten zu ganzen Organisationen

Die Krux mit herkömmlichen digitalen Identitäten liegt darin, dass sie für jeden Dienst und jedes Gerät unabhängig voneinander benötigt werden: Die digitalen Identitäten für den privaten Windows-PC, das Android-Smartphone, die Online-Shopping-Website und den Online-Zugang zum eigenen Bankkonto haben außer der wiederholten Eintragung der größtenteils gleichen Attribute wie Name und E-Mail-Adresse nicht viel gemeinsam, obwohl sie von ein und derselben Person genutzt werden.

In einer ähnlichen Situation befanden sich die IT-Abteilungen größerer Organisationen schon früher: Neueinstellungen und der Weggang von Mitarbeiter:innen führten dazu, dass für jede Person separate digitale Identitäten, zum Beispiel auf dem E-Mail-Server, der gemeinsamen Dateiablage und der Telefonanlage erstellt, gepflegt und nach dem Ausscheiden auch wieder gelöscht werden mussten. Voneinander abweichende Datenbestände und Einschränkungen, beispielsweise bei heiratsbedingten Namensänderungen, waren an der Tagesordnung.

Die heute übliche, fast schon selbstverständlich anmutende, aber damals technisch hart erkämpfte Lösung besteht darin, einen einzigen organisationsweiten Bestand an digitalen Identitäten aufzubauen, der von allen angeschlossenen

IT-Diensten genutzt werden kann: In sogenannte „Identity & Access Management (I&AM)“-Systeme werden die Benutzer:innenbestände zentral eingepflegt und mit Attributen versehen, die festlegen, welche Personen welche Dienste in welchem Umfang verwenden dürfen. Auf technischer Ebene haben sich dabei sogenannte Verzeichnisdienste („Directory Services“) durchgesetzt, auf die beispielsweise über das standardisierte LDAP-Protokoll („Lightweight Directory Access Protocol“) zugegriffen werden kann. Für die zentralen LDAP-Server eines I&AM-Systems existieren Open-Source- sowie kommerzielle Softwareprodukte, in den Microsoft-Windows-basierten Infrastrukturen vieler Unternehmen und Behörden übernimmt in der Regel das zentrale Microsoft Active Directory diese Rolle. Mit diesem technischen Ansatz kommt man seit einiger Zeit aber auch als Privatperson in Berührung: Wer beispielsweise eine digitale Identität bei einem der Big-Tech-Unternehmen wie Google, Apple oder Microsoft hat, kann damit eine breite Palette verschiedener Dienste desselben Unternehmens nutzen, ohne sich für jeden davon komplett neu registrieren zu müssen.

Von einzelnen Organisationen zu Föderationen

Dennoch bleibt auch eine I&AM-Lösung auf die verschiedenen Dienste einer Organisation beschränkt. Wer eine digitale Identität bei seinem Arbeitgeber hat, kann sich darüber nicht auf der Website seines Sportvereins einloggen. Und wer ein Konto bei Facebook hat, kann damit noch lange nicht bei Amazon einkaufen. Während bei vielen solcher willkürlich gewählten Beispiele durchaus kritisch zu hinterfragen ist, ob man diese Funktionalität wirklich braucht und haben will, haben sich in den vergangenen rund 15 Jahren einige Anwendungsgebiete herauskristallisiert, in denen die organisationsübergreifende Nutzung digitaler Identitäten einen konkreten Mehrwert bringt: Historisch betrachtet können Hochschulen, Forschungseinrichtungen und wissenschaftsnahe Dienstleister als Vorreiter gelten, da sich hier früh die Notwendigkeit ergab, dass zum Beispiel im Rahmen gemeinsamer Forschungsprojekte Mitarbeiter:innen einer Universität auf IT-Dienste und Datenbestände anderer beteiligten Einrichtungen zugreifen können. Insbesondere in größeren Unternehmen liegt ein ähnlicher Bedarf im Rahmen der Zusammenarbeit mit Kooperationspartnern und der eigenen Zuliefererkette vor. Nicht zuletzt ergeben sich im E-Government – in Deutschland im Kontext des Verbunds der Nutzerkonten – viele neue spannende Anwendungsmöglichkeiten.

Die organisationsübergreifende Nutzung digitaler Identitäten wird seit dem Entstehen erster technischer Lösungen meist als föderiertes Identitätsmanagement („Federated Identity Management“, kurz: FIM) bezeichnet. Begrifflich ist unter einer Identitätsföderation ein Zusammenschluss von Organisationen zu verstehen, die auf technischer Ebene untereinander Personen- und Berechtigungsinformationen austauschen können. Zwar ergeben sich konzeptionell gewisse Parallelen, aber FIM als Technologie

Wer ein Konto bei Facebook hat, kann damit noch lange nicht bei Amazon einkaufen.

auf der einen und Föderalismus als politisches Gestaltungsprinzip – unter anderem in Deutschland – auf der anderen Seite existieren naheliegend gänzlich unabhängig voneinander. Die Grundidee hinter einer Identitätsföderation ist, dass alle Nutzer:innen einer Heimateinrichtung, die deren digitale Identitäten verwaltet, zugeordnet werden können. Andere Organisationen, die den Nutzer:innen ihre Dienste anbieten, können der Heimateinrichtung die Authentifizierung der Nutzer:innen überlassen und anschließend die benötigten Attribute abrufen.

Datenflüsse und Vertrauensbeziehungen in Föderationen

Durch den organisationsübergreifenden Datenaustausch werden einige Abläufe unvermeidbar etwas komplizierter. Unverändert bleibt dabei der Ablauf für die Nutzer:innen, die authentifiziert werden können und deren digitale Identität weiterhin durch Attribute beschrieben wird. Die Heimateinrichtung, also diejenige Organisation, die eine digitale Identität verwaltet und bereitstellt, wird meist als Identity Provider, kurz: IDP, bezeichnet. Bei einigen technischen Standards und Produkten wird auch der Begriff „Asserting Party“ (also die zusichernde Partei) verwendet. Im Kontext des Verbunds der Nutzerkonten in Deutschland werden ferner Formulierungen wie „eigenes“ oder „zusicherndes Servicekonto“ verwendet. Anbieter von Diensten werden im Kontext von Föderationen auf Englisch als Service Provider, kurz: SP, bezeichnet, wobei auch hier Synonyme wie „Relying Party“ (also die vertrauende Partei), „fremdes“ oder „vertrauendes Servicekonto“ geläufig sind.

Technische Lösungen für föderiertes Identitätsmanagement haben die grundlegende Aufgabe, den folgenden Ablauf zu unterstützen: Nutzer:innen möchten den Dienst eines Service Providers verwenden.

Es gilt also jede Menge Fragen zu klären, damit eine Föderation überhaupt funktionieren kann.

Der Service Provider schickt die Nutzer:innen zu ihrem Identity Provider, der zunächst eine Authentifizierung durchführt. Nach erfolgreicher Authentifizierung werden die für den Dienst relevanten Attribute an den Service Provider übermittelt, und der Dienst kann so genutzt werden, als ob die Nutzer:innen dort eine eigene lokale digitale Identität hätten.

Die praktische Umsetzung dieses recht einfachen Ablaufs ist jedoch mit zahlreichen Herausforderungen verbunden: Woher weiß der Service Provider, welcher Identity Provider für den/die noch gar nicht authentifizierte:n Benutzer:in zuständig ist? Sind die vom Identity Provider gelieferten Attribute zuverlässig im Sinne einer hohen Datenqualität? Wie ist es datenschutzrechtlich zu bewerten, wenn eine Organisation personenbezogene Daten in Form von Attributen an eine andere Organisation weitergibt?

Zentrale Komponenten einer Föderation

Da eine Identitätsföderation ein Zusammenschluss verschiedener Identity und Service Provider ist, muss festgelegt werden, welche Organisationen als Mitglieder dazu gehören. Der Beitritt zu einer Föderation wird dabei üblicherweise vertraglich geregelt.

Von vielen denkbaren Varianten hat sich dabei ein zentraler, sogenannter Föderationsbetreiber („Federation Operator“) als

Vertragspartner für die einzelnen Identity und Service Provider bewährt. Er verwaltet nicht nur die Verträge, sondern stellt mit den sogenannten Föderationsmetadaten auch ein technisches Dokument (meist im XML- oder JSON-Format) bereit, das die technischen Kommunikationsendpunkte aller beteiligten Identity und Service Provider enthält. Diese Metadaten sind für die technische Umsetzung unerlässlich: Ein Service Provider kann die Nutzer:innen auf dieser Basis auswählen lassen, welcher der in der Föderation bekannten Identity Provider ihre Heimateinrichtung ist, und dieser Identity Provider weiß dann genau, wohin er die Attribute zu übermitteln hat, nachdem er die Authentifizierung im Auftrag des Service Providers durchgeführt hat.Die Föderation muss aber auch viele Eigenschaften der Attribute festlegen: Welche Attribute stehen prinzipiell zur Verfügung, wie werden sie genau bezeichnet und welcher Inhalt steckt in diesen Datenfeldern? Beispielsweise könnte die Anschrift einer Person über ein einziges, frei zu gestaltendes Attribut abgebildet werden, oder es werden – zumindest in Deutschland – separate Attribute für Straße, Hausnummer, Zusätze, Postleitzahl und Ort verwendet. Ohne föderationsweit einheitliche Festlegung könnte der Service Provider nur wenig mit den von verschiedensten Identity Providern übermittelten Attributen anfangen.

Ebenso muss verbindlich spezifiziert werden, welche Datenqualität die von den beteiligten Identity Providern bereitgestellten Attribute erfüllen müssen. Können sich die Nutzer:innen beispielsweise mit beliebigen Angaben selbst registrieren? Oder werden Stammdaten wie Name und Wohnort anhand eines amtlichen Ausweises geprüft?

Soweit sich keine einheitlichen Mindeststandards umsetzen lassen, die für alle Service Provider ausreichend sind, besteht die Möglichkeit, Attribute um sogenannte Levels of Assurance (auch als LoAs oder Vertrauensniveaus bekannt) zu ergänzen, die fein granulierte Rückschlüsse auf die Datenqualität jedes einzelnen Attributs zulassen.

Ohne föderationsweit einheitliche Festlegung könnte der Service Provider nur wenig mit den von verschiedensten Identity Providern übermittelten Attributen anfangen.

Dem Datenschutz bei der Weitergabe von personenbezogenen Daten vom Identity Provider an den Service Provider wird im Allgemeinen, insbesondere wenn keine gesetzliche Grundlage für den Datenaustausch vorliegt, mehrstufig Rechnung getragen: Service Provider verpflichten sich vertraglich zur Einhaltung eines Verhaltenskodex, der regelt, dass nur für die Diensterbringung relevante Attribute angefordert werden. Die Liste entsprechender Attribute wird zum Beispiel in den Metadaten der Föderation hinterlegt vom jeweiligen Identity Provider ausgewertet, sodass er nicht alle Attribute der digitalen Identität, sondern nur diese Teilmenge bereitstellt. Üblich ist dabei, den Nutzer:innen

Max Mustermann oder mächtiger Wolf? Im digitalen Raum lassen sich ohne stimmige Vorgaben viele Identitäten annehmen.

nach erfolgter Authentifizierung eine Liste aller zu übertragenden Attribute anzuzeigen und ihr explizites Einverständnis zur Weitergabe an den Service Provider einzuholen. Dieser Schritt kann in spezielleren Föderationen entfallen, beispielsweise wenn für die angestoßene Datenübermittlung in jedem Fall eine gesetzliche Grundlage oder eine mit dem/der Nutzer:in geschlossene vertragliche Vereinbarung vorliegt.

Föderation FINK für den Verbund der Nutzerkonten

FINK – das föderierte Identitätsmanagement für interoperable Nutzerkonten in Deutschland – setzt als Verbund der Nutzerkonten von Bund und Ländern im Kern eine Identitätsföderation auf Basis des Standards SAML mit Identity und Service Providern um. Die Ausgangsbasis bilden hier jedoch die Nutzerkonten, die ihren Nutzer:innen personenbezogene Dienste zur Verwendung von Online-Verwaltungsleistungen anbieten.

Föderationsmitglieder sind dabei der Bund und die Länder, die ihre eigenen Nutzerkonten im Rahmen von FINK interoperabel anbieten: Das bedeutet, dass jedes beteiligte Nutzerkonto als Identity Provider für die Nutzer:innen im eigenen Bundesland auftritt und somit die Authentifizierung und Bereitstellung von Attributen auch für Dienste, die außerhalb des eigenen Bundeslands erbracht werden, übernimmt. Zugleich kann das Nutzerkonto aber auch als Service Provider auftreten und Nutzer:innen aus den einzelnen Bundesländern über deren Nutzerkonten authentifizieren, damit ein Dienst im eigenen Vollzugsbereich genutzt werden kann. Diese Doppelrolle sowohl als Identity als auch Service Provider wird bei FINK als Dipol bezeichnet.

Die resultierende Dipol-Architektur, also eine Föderation, die aus lauter kombinierten Identity und Service Providern besteht, wirkt auf den ersten Blick zwar komplexer als herkömmliche Föderationen, erleichtert die Anbindung von OZG-Leistungen aber maßgeblich: Jede OZG-Leistung wird – je nachdem, ob die Zuständigkeit für den Vollzug bei Bund, Land oder Kommune liegt – an nur genau ein Nutzerkonto, das des Bundes oder des jeweiligen Landes, angebunden. Sie kann über den Verbund der Nutzerkonten jedoch auch von Nutzer:innen verwendet werden, die über ein anderes Nutzerkonto authentifiziert werden.

Aus Perspektive der Nutzer:innen ergibt sich damit der große Vorteil, dass beispielsweise auch nach einem Umzug in ein anderes Bundesland die dortigen kommunalen beziehungsweise länderspezifischen Online-Verfahren, zu denen unter anderem auch alle OZG-Leistungen gehören, mit einer bereits vorhandenen digitalen Identität genutzt werden können. Für die Anbieter von Online-Verfahren ergibt sich die wesentliche Vereinfachung, dass über die Anbindung an das eigene Nutzerkonto hinaus keine zusätzlichen Maßnahmen erforderlich sind, um die Vorteile der Interoperabilität nutzen zu können: Weder muss auf organisatorischer Ebene der Föderation FINK beigetreten werden, noch muss auf technischer Ebene zwingend SAML zum Einsatz kommen. Sofern zur Anbindung an das Nutzerkonto bereits andere Schnittstellen wie OAuth beziehungsweise OpenID Connect zum Einsatz kommen, können diese beibehalten werden. Durch diese technische Flexibilität werden nicht nur länderspezifische Gestaltungsmöglichkeiten eröffnet, sondern auch bereits getätigte Investitionen in Know-how und IT-Infrastrukturen genutzt.

Digitale Identitäten und Datenflüsse in FINK

Zur Verwendung eines Online-Verfahrens oder einer OZG-Leistung müssen über die rein technische Authentifizierung der Nutzer:innen hinaus typischerweise personenbezogene Daten wie Name und Anschrift vorliegen, die früher von Hand in Formulare einzutragen waren. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) legt deshalb in seiner Technischen Richtlinie TR-03160 im Einklang mit der eIDAS-Verordnung der Europäischen Union zum einen fest, dass Identitätsdaten im Kontext von Servicekonten bestimmte Attribute wie Vorname, Familienname, Geburtsdatum und -ort sowie Anschrift umfassen. Zum anderen werden Vertrauensniveaus festgelegt, die widerspiegeln, mit welcher Zuverlässigkeit die Identitätsdaten überprüft worden sind. So erreichen beispielsweise von den Nutzer:innen lediglich selbst eingegebene Daten zunächst nur das niedrigste Vertrauensniveau. Durch Anklicken eines Bestätigungslinks, der an eine von den Nutzer:innen angegebene E-Mail-Adresse verschickt wird, erreicht diese Adresse das Vertrauensniveau „normal“, im Falle einer De-Mail-Adresse auch „substanziell“. Durch die Übernahme der auf dem Personalausweis gespeicherten Daten mittels Online-Ausweisfunktion wird das Vertrauensniveau „hoch“ erreicht.

Haben die Nutzer:innen das von ihnen gewünschte Online-Verfahren ausgewählt, wird ihnen die Möglichkeit geboten, sich über das Benutzerkonto anzumelden, an das das Online-Verfahren angebunden ist. Dieses wiederum stellt zur Auswahl, sich entweder direkt oder über ein anderes Benutzerkonto in der Föderation anzumelden. In Abbildung 1 ist dargestellt, wie die Benutzerkonten zweier Bundesländer Metadaten austauschen und die Nutzer:innen Online-Verfahren in beiden Bundesländern mit nur einem Benutzerkonto nutzen können. Nach dem Login beim so ausgewählten Identity Provider werden die Attribute zunächst an das ursprüngliche Benutzerkonto und von diesem an das Online-Verfahren übermittelt, wo sie automatisch in entsprechende Formularfelder übernommen werden können. Im Regelfall liegen die Angaben dann bereits mindestens mit dem erforderlichen Vertrauensniveau vor und müssen im Laufe der Erbringung des Online-Verfahrens nicht nochmals separat geprüft werden. Für Nutzer:innen und Dienstleister entfallen damit zusätzliche Schritte zur Überprüfung.

Abbildung 1

Nutzung von Verwaltungsleistungen über föderiertes Identitätsmanagement

IT-Sicherheit und Datenschutz in Föderationen

Jegliche Form eines organisationsübergreifenden Identitätsmanagements ist aufgrund der Nutzung personenbezogener Daten und der möglicherweise missbräuchlichen Verwendung von Diensten und Datenbeständen kritisch bezüglich der IT-Sicherheit und des Datenschutzes zu hinterfragen. Da für die Föderation FINK mit SAML eine standardisierte, praxisbewährte und gut untersuchte Technologie zum Einsatz kommt, stellen im Wesentlichen zentrale Föderationskomponenten wie der Metadatenserver, die Benutzerkonten und die einzelnen Online-Verfahren potenzielle Angriffsziele dar, die – bedingt durch die gewünschte einfache Zugänglichkeit für die Nutzer:innen – über das Internet exponiert sind.

Für die am Betrieb der Föderation beteiligten Dienstleister sind deshalb technische Maßnahmen und organisatorische Prozesse definiert, um die Vertraulichkeit, Integrität und Verfügbarkeit aller verarbeiteten Daten sicherzustellen. Sie orientieren sich am Stand der Technik sowie Erfahrungswerten aus dem Betrieb anderer großer Föderationen. Hierzu gehören beispielsweise Prüfverfahren für die Föderationsmetadaten, die ein Einschleusen oder Manipulieren der Angaben zu Benutzerkonten durch unberechtigte Dritte unterbinden, genauso wie eine Regelung für die Zusammenarbeit zwischen allen relevanten Beteiligten, wenn beispielsweise das Konto eines/einer Nutzer:in oder ein ganzes Benutzerkonto mutmaßlich kompromittiert worden ist. Aufgrund der Gesetze und Verordnungen ist auch die Verarbeitung der personenbezogenen Daten klar geregelt. Als Wermutstropfen für den Datenschutz verbleibt beim Einsatz von Identitätsföderationen, dass der Identity Provider im Rahmen der Authentifizierung und Bereitstellung von Attributen in die Nutzung jedes Dienstes der Föderation einbezogen wird: Bei ihm fallen unvermeidbar Informationen darüber an, welche Nutzer:innen wann welche Dienste in Anspruch genommen haben. Während dies zur Aufklärung eingetretener Sicherheitsvorfälle eine durchaus essenzielle Information ist, droht die Gefahr der Bildung von Nutzungsprofilen. Dieser kann nur durch organisatorische Maßnahmen vorgebeugt werden, also einer Unterbindung der Speicherung und Auswertung solcher im Betrieb anfallenden Daten, die der definierten Zweckbindung widersprechen würde. Die Technische Richtlinie TR-03160 des BSI regelt entsprechend, dass im Verlauf einer Transaktion anfallende Daten maximal sieben Tage lang zum Zweck der Missbrauchserkennung gespeichert werden dürfen.

Ausblick auf Weiterentwicklungen

Die Umsetzung der knapp 600 OZG-Leistungen und Online-Verfahren mit ihrer Anbindung an den Verbund der Nutzerkonten ist noch in Arbeit. Ausschlaggebend für den Erfolg ist dabei aber nicht nur die reine Anzahl online verfügbarer Leistungen, sondern auch deren Nutzung und Akzeptanz. Mit der Föderation FINK wird die technische Infrastruktur geschaffen und betrieben, um deutschlandweit Online-Verwaltungsleistungen mit einer einzigen digitalen Identität zu nutzen.

Mit Blick über diesen Tellerrand können sich zukünftig Anwendungen ergeben, die über die aktuellen Grenzen der Föderation FINK hinausgehen. Einerseits spielt dabei die Interoperabilität auf europäischer Ebene eine, auch politisch, wichtige Rolle, andererseits kann es ebenso außerhalb des Sektors E-Government Online-Dienstleister geben, die von der hohen Datenqualität in FINK profitieren könnten. Dabei könnte komplementär zum Föderationsansatz auch verstärkt „Self-Sovereign Identity Management“ (SSI) zum Einsatz kommen, bei dem die Attribute nicht mehr zentral von einem Identity Provider, sondern in Form sogenannter „Verifiable Credentials“ von den Nutzer:innen selbst, zum Beispiel in einer Wallet-App auf dem Smartphone, gespeichert und dem jeweiligen Online-Dienst vorgelegt werden. Einen Einblick in die Abläufe mit SSI und deren nahtlose Integration in Föderationen gibt der Artikel auf Seite 56 dieses Kompendiums.

Praxisbewährte Föderationen am Beispiel DFN-AAI

Dass größere Föderationen langfristig stabil funktionieren und für alltägliche Abläufe unverzichtbar werden, zeigt ein Blick in die deutsche Wissenschaftswelt: Seit 2007 betreibt das Deutsche Forschungsnetz (DFN), ein Verein mit über 300 institutionellen Mitgliedern aus der deutschen Hochschul- und Forschungslandschaft, mit der Authentifizierungs- und Autorisierungsinfrastruktur (DFN-AAI) eine nationale Identitätsföderation auf Basis des technischen Standards SAML („Security Assertion Markup Language“). Sie verbindet Student:innen und Mitarbeiter:innen von über 300 Identity Providern mit über 600 Service Providern, die beispielsweise die Nutzung von Nationallizenzen für wissenschaftliche Literatur, Rahmenverträgen für den Softwarebezug und den hochschulübergreifenden Zugriff auf eScience- und eLearning-Systeme ermöglichen.

Wie im Hochschulumfeld üblich, kommt für die Umsetzung bei den meisten Teilnehmer:innen Open-Source-Software zum Einsatz, zu einem geringeren Teil auch selbstentwickelte Software. Die Verwendung aus Nutzer:innenperspektive verläuft dabei so einfach wie unspektakulär: Student:innen, die beispielsweise im Rahmen ihrer Immatrikulation an einer Hochschule einen amtlichen Lichtbildausweis vorgelegt haben, und Mitarbeiter:innen, die die üblichen Einstellungsmodalitäten absolviert haben, wird ihre Zugehörigkeit („Affiliation“) zur Hochschule als Attribut zugeordnet,

das fortan als Autorisierungsmerkmal bei vielen Service Providern herangezogen wird. Ein Onlinedienst kann somit sehr einfach sicherstellen, dass der Zugriff auf bestimmte Daten und Angebote den offiziellen Angehörigen bestimmter Hochschulen vorbehalten bleibt, ohne dass er weitere Attribute wie Name oder E-Mail-Adresse kennen muss. Es können also sehr datensparsame und damit datenschutzfreundliche Dienste umgesetzt werden, ohne dass sich Einschränkungen, zum Beispiel bei der Abrechnung für kommerzielle Anbieter kostenpflichtiger Dienste, ergeben.

Inter-Föderationen am Beispiel eduGAIN

Die nationale Identitätsföderation DFN-AAI ist nicht nur ein gutes Beispiel dafür, wie hunderte von Organisationen erfolgreich zusammenarbeiten können, sondern veranschaulicht auch ein bewährtes Vorgehen über Föderationsgrenzen hinaus: Offensichtlich enden wissenschaftliche Zusammenarbeit und studentische Mobilität nicht an den Grenzen Deutschlands oder der DFN-AAI. Wie aber können in der DFN-AAI registrierte Nutzer:innen auch auf Dienste in anderen Ländern zugreifen?

Mit der vom europäischen Forschungsnetzverbund GÉANT betriebenen Inter-Föderation eduGAIN wird seit 2011 eine weltweite Infrastruktur aufgebaut, der sich bereits über 70 nationale Föderationen mit mehr als 3.500 Identity Providern und 4.500 Service Providern angeschlossen haben. Rund 27 Millionen Student:innen und Forscher:innen können so täglich mit einer einzigen digitalen Identität bei ihrer Heimateinrichtung weltweit auf die für ihr Studium und ihre Forschung benötigten Dienste zugreifen.

Technisch funktioniert eine Inter-Föderation wie eduGAIN über das Zusammenführen der Metadaten mehrerer Föderationen: Beispielsweise können an der deutschen DFN-AAI beteiligte Identity und Service Provider per Opt-in-Verfahren zustimmen, dass ihre Einträge in den eduGAIN-Metadatensatz aufgenommen werden. Über in diesem Fall zwischen dem DFN-Verein und GÉANT als Betreiber der Inter-Föderation geschlossene Verträge wird die Einhaltung von Richtlinien geregelt, die beispielsweise Themen wie den Datenschutz und die Zusammenarbeit im Falle des Eintretens eines IT-Sicherheitsvorfalls regeln.

Rund 27 Millionen Student:innen und Forscher:innen können so täglich mit einer einzigen digitalen Identität bei ihrer Heimateinrichtung weltweit auf die für ihr Studium und ihre Forschung benötigten Dienste zugreifen.

Von der Idee bis zur Umsetzung: Der Weg der interoperablen Nutzerkonten in Deutschland

Ein Interview mit Martin Kirschenbauer, Bayerisches Staatsministerium für Digitales

Was war der Startschuss der interoperablen Nutzerkonten?

„Als initialer Ausgangspunkt für die interoperablen Nutzerkonten können die Bemühungen rund um den elektronischen Personalausweis und die DE-Mail in der Projektgruppe eID-Strategie (kurz: PG eID-Strategie) des IT-Planungsrats genannt werden. Die PG eID-Strategie wurde im Herbst 2013 beauftragt, unter anderem diese beiden Vorhaben im Rahmen der Erarbeitung einer Strategie hinsichtlich ihrer Verbreitung voranzubringen. Zu dieser Zeit hatten wir in Bayern bereits die BayernID mit dem Ansatz eines Bürgerkontos in einer ersten Version umgesetzt. Die Kommunikationsstrategie, dem Bürger beziehungsweise der Bürgerin einen Zugang mit Postfach für seine Verwaltungskontakte zur Verfügung zu stellen, haben wir seitens Bayern in der PG eID-Strategie vorgestellt. Vergleichbare Lösungen gab es zu diesem Zeitpunkt in Hamburg mit dem sogenannten Hamburg-Gateway, sowie bei zahlreichen Kommunen in NRW. Die Idee fand in der Bund-Länder-übergreifenden Projektgruppe großen Anklang und wurde in zahlreichen Sitzungen fortan präzisiert. Die Bezeichnung des Ansatzes entwickelte sich ausgehend von den steigenden Anforderungen von Bürgerkonto über Servicekonto, Organisations- und Unternehmens- beziehungsweise Behördenkonto, bis hin zu Nutzerkonto, dem Begriff aus dem Onlinezugangsgesetz, weiter.

Dem Grundgedanken des Art. 30 Grundgesetz folgend, welcher besagt, dass der Vollzug Ländersache ist, wurden 16 Nutzerkonten der Länder abgestimmt. Auf diese Art und Weise war es einfach möglich, Länderregularien oder landeseigene Features an den jeweiligen Länderkonten abzubilden und die Verwaltungsleistungen nach den Gegebenheiten vor Ort anzubinden. Darüber hinaus wurde für die Bundesleistungen ein Bundeskonto vereinbart. Durch den Interoperabilitätsansatz wurde man der unabdingbaren Bundesvorgabe gerecht, dass jeder Bürger nur ein Konto bundesweit besitzen soll. Im Sommer 2015 beschloss der IT-Planungsrat eine flächendeckende Verbreitung von Nutzerkonten für Bürger und Unternehmen.“

Welche zentralen Umsetzungsmaßnahmen wurden ergriffen, um den Beschluss des IT-Planungsrats umzusetzen?

„Vor der flächendeckenden Umsetzung wurden in den Jahren 2016 bis 2018 mehrere Prototypen in Laborbedingungen ohne personenbezogene Daten unter Projektleitung Bayerns entwickelt. Sowohl die technische als auch die fachliche Implementierung der Prototypen haben gezeigt, dass die Interoperabilität von Nutzerkonten durchführbar ist. Mit einem IT-Planungsratsbeschluss vom Herbst 2018 konnte die tatsächliche Umsetzung fortgeführt werden. Zum Aufbau der zentralen Komponenten der Interoperabilität wurde 2019 ein Initialprojekt in Bayern gestartet und mit dem „Kompetenzzentrum Interoperable Servicekonten“ (KIOSK) ein Projektteam bereitgestellt. KIOSK kann als Organisationseinheit verstanden werden, die mit der Entwicklung des ausgehend von der Umsetzung der interoperablen Nutzerkonten hervorgehenden Produkts FINK („Föderiertes Identitätsmanagement Interoperabler Nutzerkonten in Deutschland“) beauftragt wurde. Mit der Pilotierung der interoperablen Nutzerkonten von Bund und Ländern konnte anschließend gegen Ende 2019 begonnen werden. Aktuell befinden wir uns in der Übergangsphase zum regulären Betrieb von FINK als Produkt des IT-Planungsrats ab 2023.“

Wie hat die Zusammenarbeit mit den Ländern zu diesem Zeitpunkt funktioniert?

„Die Bedeutung von Nutzerkonten für Bürgerinnen und Bürger wurde und wird in den Ländern als hoch angesehen. Die Zusammenarbeit wird seit jeher als sehr positiv wahrgenommen. Die erfolgreich durchgeführte Prototypphase in den Jahren 2016 bis 2018 zwischen Hamburg, Nordrhein-Westfalen und Bayern zeigte, dass föderales E-Government auf Basis von interoperablen Nutzerkonten in der Praxis erfolgreich umgesetzt werden kann. Mit der Verabschiedung des OZG im Jahre 2017 wurde für Nutzerkonten eine rechtliche Grundlage geschaffen. Dies wurde von vielen Ländern begrüßt, da einheitliche Regularien bundesweit geschaffen wurden. Darauf aufbauend hat sich Bayern zur Verabschiedung eines bayerischen Digitalgesetzes entschieden, um eigene Schwerpunkte zu setzen und im Kontext der Verwaltungsdigitalisierung noch weiterzugehen. So soll in Bayern E-Government noch stärker vom Bürger aus gedacht werden, um den Mensch beim Verwaltungshandeln in den Mittelpunkt zu stellen.“

Sind neue Akteure durch das OZG dazugekommen und hatten diese Einfluss auf die Umsetzung der interoperablen Nutzerkonten?

„Die Umsetzung der interoperablen Nutzerkonten erfolgt auf technischer Ebene seit der Prototypphase konstant mit den fünf Dienstleistern von Bund und Ländern, die als Nutzerkontenhersteller fungieren. Die Zusammenarbeit ist mittlerweile eingespielt und wird als sehr angenehm empfunden. Auf Fachseite in der Bund-Länder-übergreifenden Zusammenarbeit im IT-Planungsrat hat sich in den letzten Jahren ausgehend von der OZG-Umsetzung sehr viel verändert. Zu Anfang wurden die Maßnahmen zu Nutzerkonten ausschließlich in der PG eID-Strategie besprochen und schlussendlich im IT-Planungsrat beschlossen. Mit einsetzender OZG-Umsetzung ab 2017 sind zahlreiche neue Stakeholder sowie Projekte und Gremien hinzugekommen. Davon ausgehend mussten die Aktivitäten zum Informationsfluss unsererseits in Bayern deutlich erhöht werden, um den Interessen und Belange der neu hinzugekommenen Akteure gerecht zu werden. Darüber hinaus war zu beobachten, dass die Kolleginnen und Kollegen bei Bund und Ländern fortan nicht nur bei der Ertüchtigung der Nutzerkonten, sondern vor allem bei der Umsetzung der Onlinedienste zusätzlich immens gefordert waren. Nichtsdestotrotz konnten die Belange der interoperablen Nutzerkonten einvernehmlich entschieden und umgesetzt werden.“

Wie kam es zu der Entscheidung, ein Unternehmenskonto umzusetzen?

„Mit voranschreitender Arbeit der PG eID-Strategie wurden die Rufe nach einem eigenständigen Konto, das die spezifischen Anforderungen von Unternehmen berücksichtigt, als Teil der E-Government-Umsetzung lauter. Vor allem Wirtschaftsverbände, wie zum Beispiel der DIHK, haben die Interessen von Unternehmen im Hinblick auf ein Unternehmenskonto an das federführende BMI herangetragen. Die größte Herausforderung eines Unternehmenskontos lag in der elektronischen Identität der Unternehmen, die zu diesem Zeitpunkt – im Gegensatz zu Bürgerinnen und Bürgern mit der eID-Funktion des Personalausweises – nicht entwickelt war. Um dieser Anforderung zu begegnen, wurde in einer Machbarkeitsstudie das ELSTER-Konto untersucht. Dies geschah vor dem Hintergrund, dass deutsche Unternehmen durch die Gesetzeslage im steuerlichen Kontext bereits über ein ELSTER-Konto verfügen müssen. Durch die sogenannten ELSTER-Organisationszertifikate konnte eine elektronische Identität für Unternehmen gewährleistet werden. Das anfängliche rechtliche Hindernis, dass ELSTER-Zertifikate nach §139b der Abgabenordnung lediglich für Zwecke der Steuer verwendet werden dürfen, wurde durch eine Änderung der gesetzlichen Vorschriften auf Bundesebene beseitigt. Somit erfüllte das ELSTER-Konto die Anforderungen der PG eID-Strategie sowie der Wirtschaftsverbände und wurde als Unternehmenskonto auf ELSTER-Basis als zentrale Lösung umgesetzt.“

„Eine Herausforderung für diese Aktivitäten ist das näherkommende Fristende der OZG-Umsetzung.“

Wie würden Sie den Status Quo der Umsetzung der interoperablen Nutzerkonten beschreiben?

„Der Aufbau der Identitätsföderation in FINK, mit Hilfe derer sich Bürgerinnen und Bürger mit ihrem Konto länderübergreifend an Onlinediensten identifizieren können, ist mit 13 Länderkonten und dem Nutzerkonto Bund mittlerweile erfolgreich abgeschlossen. Im Laufe des Jahres 2022 erfolgt die Umsetzung der Interoperabilität der Postfächer.

Eine Herausforderung für diese Aktivitäten ist das näherkommende Fristende der OZG-Umsetzung. Somit rückt die digitale Umsetzung zahlreicher Verwaltungsleistungen in den Mittelpunkt der Bemühungen der entsprechenden Akteure – sowohl auf Seiten der Politik als auch auf Seiten der IT-Dienstleister. Hiervon ist die Umsetzung der interoperablen Postfächer betroffen, welche die Anforderungen der OZG-Leistungen an die Kommunikation zwischen Behörden und Nutzern mittels der Postfach-Funktion lösen sollen.

Des Weiteren hat der IT-Planungsrat am 9. März 2022 beschlossen, perspektivisch auf ein zentrales Bürgerpostfach beim Nutzerkonto Bund zu setzen. Dieses kann fortan freiwillig von den Ländern anstelle der eigenen Postfachlösung genutzt werden. Die Interoperabilität zu den vorhandenen Postfächern ist herzustellen."

Welches Fazit ziehen Sie rückblickend, wenn Sie sich die Entwicklung der interoperablen Nutzerkonten von der ersten Idee bis zum heutigen Zeitpunkt anschauen?

„Als generelles Fazit lässt sich festhalten, dass sich der Nutzerkontenansatz in der bundesweiten OZG-Umsetzung etabliert hat. Es ist somit gelungen, den Bürgerinnen und Bürgern einen Onlinezugang zur Verwaltung bereitzustellen, mit dem sie zukünftig Verwaltungskontakte deutschlandweit abwickeln können. Ebenso ist zu beobachten, dass nicht nur die reine eID-Funktion des Personalausweises im Mittelpunkt steht, sondern mittlerweile über weitere Zugangsarten, allen voran Wallets, nachgedacht wird. Man spricht in diesem Zusammenhang des Öfteren im Hinblick auf Nutzerkonten von sogenannten „Identitätsbrokern", die zukünftig die unterschiedlichen Zugänge des Bürgers, zum Beispiel die ELSTER-Zertifikate, verwalten können und sollen. Wichtig für die Zukunft wird sein, diesen Onlinezugang des Bürgers zur Verwaltung weiterhin auszubauen und vor allem nutzerfreundlich zu gestalten. Die Identifikation an einem Onlinedienst darf nicht zur Hürde bei der Nutzung der jeweiligen Leistung werden."

„Wichtig für die Zukunft wird sein, diesen Onlinezugang des Bürgers zur Verwaltung weiterhin auszubauen und vor allem nutzerfreundlich zu gestalten."

Wo sehen Sie die interoperablen Nutzerkonten in fünf Jahren?

„Ob die Interoperabilität der Nutzerkonten ein Schritt auf dem Weg zu einem zentralen Nutzerkonto war, wird sich zeigen. Der Beschluss des IT-Planungsrats, perspektivisch auf ein zentrales Postfach zu setzen, geht in diese Richtung. Viel wird davon abhängen, ob der Bund ein Angebot machen kann, das von den Ländern angenommen wird. Zentrale Lösungen bringen die Herausforderung mit sich, dass sie alle landesspezifischen Anforderungen berücksichtigen müssen. Insgesamt muss also abgewogen werden, was auf politischer Ebene gewollt und auf rechtlicher Ebene möglich ist. Sollte sich keine geeignete zentrale Lösung umsetzen lassen, werden die interoperablen Nutzerkonten sicherlich bestehen bleiben.

Darüber hinaus gibt es neben den OZG-Nutzerkonten aktuell eine Vielzahl von weiteren großen Kontenlösungen wie zum Beispiel das ELSTER-Konto, das Konto der Deutschen Rentenversicherung und das der Bundesagentur für Arbeit. Eine interessante Frage wird sein, ob diese in Zukunft autark weiterbestehen wollen oder ob sich der Wunsch nach mehr Zusammenarbeit einstellt. Im Umfeld der Nutzerkonten ist auch zu beachten, dass Entscheidungen durch zahlreiche Einflüsse von außen, wie zum Beispiel dem weiteren Vorgehen der EU (Stichwort: „eIDAS-Novelle", „EU-Wallet") beziehungsweise notwendigen IT-Sicherheitsvorgaben beeinflusst werden. Ebenso gilt es, die Interessen von Organisationen außerhalb der Verwaltung, wie zum Beispiel Kammern und Verbände, zu berücksichtigen, da diese nachvollziehbarerweise die bestmögliche Lösung für ihre konkreten Bedarfe anstreben.

Völlig losgelöst von den Nutzerkonten stimmt mich aktuell in der OZG-Umsetzung sehr hoffnungsvoll, dass sich ein stärkeres Denken „vom Nutzer her" ausbreitet. Auch ist vielerorts der Wille zu erkennen, Experimente zu wagen. Die hierbei wohltuend unvoreingenommene Herangehensweise wird meines Erachtens zu vielen positiven Ergebnissen führen. Projekte wie beispielsweise die bayerischen Innovationslabore oder die Digitalschmiede Bayern tragen dazu bei, dass sich die Verwaltung öffnet."

Vielen Dank für das Gespräch!

Referent:innen

Prof. Dr. Dr. Robert Krimmer ist Professor für e-Governance an der Universität Tartu in Estland. In seiner Forschung fokussiert er sich auf die digitale Transformation des öffentlichen Sektors. Zwischen 2017 und 2021 leitete er den europäischen Großpiloten TOOP zur Erforschung und Demonstration des länderübergreifenden Einsatzes des Once-Only-Prinzips. 2019 erkor ihn Apolitical.io zu einem der 100 wichtigsten Vordenker im Bereich Digitale Transformation.

Dr. Daniela Pöhn ist wissenschaftliche Mitarbeiterin an der Professur für IT-Sicherheit von Software und Daten an der UniBw M. Ihre Forschung konzentriert sich vor allem auf Identitätsmanagement, insbesondere hinsichtlich Geschäftsprozessen und IT-Sicherheit, was sie in das Forschungsprojekt DISPUT einbringt.

Jens Viere hat nach seinem Studium der Rechtswissenschaften in Freiburg und Paris sein Rechtsreferendariat am OLG Karlsruhe absolviert und mit dem zweiten Staatsexamen im Oktober 2019 abgeschlossen. Seit Mai 2020 ist er als Referent im Bayerischen Staatsministerium für Digitales tätig. Dort ist er als Projektleiter in Co-Federführung mit der Hansestadt Bremen, unter anderem für die Entwicklung und Koordination des bundesweit einheitlichen Unternehmenskontos, zuständig.

Chiara Stuttfeld unterstützt das Marketing-Team bei der publicplan GmbH, wo sie ihre berufliche Laufbahn 2016 als Dualstudentin startete. Sie erstellt Inhalte für die Social-Media-Kanäle und Website der publicplan, mitunter auch für den E-Government-Blog, und gestaltet Marketing-Materialien für interne sowie externe Zwecke.

Prof. Dr. Wolfgang Hommel hat die Professur für IT-Sicherheit von Software und Daten an der Universität der Bundeswehr München (UniBw M) inne und ist Leitender Direktor des Forschungsinstituts Cyber-Defence und Smart Data (FI CODE). Seine Forschungsgruppe befasst sich seit rund 20 Jahren mit Themen rund um das Identity Management und begleitet im Rahmen des vom Bayerischen Staatsministerium für Digitales geförderten Forschungsprojekt DISPUT den Auf- und Ausbau der Föderation FINK wissenschaftlich.

Dominik Hiemer unterstützt das KIOSK-Team bei der Unternehmensberatung H&D, wo seine berufliche Laufbahn Ende 2021 als IT-Projektmanager startete. Dabei unterstützt er in der Koordination und Evaluierung des laufenden IT-Managementprozesses und in der Umsetzung neuer Anforderungen.

Michael Grabatin promoviert seit 2016 am Forschungsinstitut Cyber-Defence der Universität der Bundeswehr München. Er forscht hauptsächlich an Techniken zum Föderierten Identitätsmanagement und unterstützt die Lehre zu sicherer Softwareentwicklung und Sicherheitsmanagement. Er studierte Informatik (B.A. & M.A.) an der Ludwig-Maximilians-Universität München.

Martin Kirschenbauer ist stellvertretender Referatsleiter im Referat B3.3 – Onlinezugangsgesetz, Portalverbund, Identitätsmanagement im Bayerischen Staatsministerium für Digitales. Seit 2013 ist er mit kurzer Unterbrechung ständiger Vertreter Bayerns in der Projektgruppe eID-Strategie des IT-Planungsrats. 2019 wurde er mit der Projektleitung zur Umsetzung der zentralen Komponenten der Interoperabilität der OZG-Nutzerkonten in Bayern beauftragt. Er verantwortet somit den Aufbau des Produkts FINK des IT-Planungsrats in Bayern.

DIE LANDSCHAFT DER NUTZERKONTEN IN DEUTSCHLAND

(Stand: März 2022)

Alle 16 Bundesländer haben beschlossen, ihren Bürger:innen ein Nutzerkonto bereitzustellen. Die Länder haben hierzu unterschiedliche Nutzerkonto-Lösungen verschiedener Anbieter eingesetzt. Neben den Landesnutzerkonten wurde zusätzlich ein Konto auf Bundesebene entwickelt – das Nutzerkonto Bund.

Einer der Grundbausteine eines Nutzerkontos ist das Vertrauensniveau. Je nach Sensibilität einer Verwaltungsleistung verlangt diese eine Identifizierung in Form verschiedener Vertrauensniveaus. Je höher das Vertrauensniveau ist, desto gesicherter sind die Identitätsdaten der Nutzer:innen, welche die Behörde über das Nutzerkonto erhält. Die Nutzerkonten können auf einem oder mehreren Vertrauensniveaus eingerichtet und genutzt werden. Diese reichen von der Registrierung und Anmeldung mit Benutzername und Passwort über die Registrierung mit dem ELSTER-Zertifikat und dem dazugehörigen Passwort (für Organisationen) bis hin zur Registrierung und Anmeldung mit der eID des Personalausweises oder des elektronischen Aufenthaltstitels/Registrierung mit dem eID-Mittel der EU-Mitgliedsstaaten (Europäische eID).

Interoperabilität: Verknüpfung der Nutzerkonten in Deutschland

Von den Nutzerkonten in Deutschland sind 15+1 Nutzerkonten interoperabel. Die Bezeichnung +1 bezieht sich umgangssprachlich auf das Nutzerkonto Bund. Interoperabilität beschreibt die länderübergreifende Nutzung von Nutzerkonten. So kann ein bestehendes Nutzerkonto aus einem Bundesland auch verwendet werden, wenn ein Onlinedienst in einem anderen Bundesland in Anspruch genommen wird. Es ist dann nicht erforderlich, sich nochmals ein weiteres Nutzerkonto in dem Bundesland anzulegen, in dem der Onlinedienst verortet ist.

Die Komponenten der Nutzerkonten in Deutschland

Postfach

Das Postfach dient dem Empfang von elektronischen Nachrichten und insbesondere von Bescheiden. Die nutzende Person wird per E-Mail informiert, dass eine neue Nachricht im Nutzerkonto eingegangen ist. Die darin enthaltenen Informationen können nur mit dem Vertrauensniveau geöffnet und gelesen werden, das für das genutzte Fachverfahren beziehungsweise die Verwaltungsleistung notwendig war. Mit dem IT-Planungsratsbeschluss 2022/04 wurde sich perspektivisch für ein zentrales Postfach für Bürger:innen ausgesprochen. Die Länder können anstelle ihrer Länder-Postfachlösungen das Nutzerkonten-Bund-Postfach als Postfach nutzen. Die Interoperabilität zwischen dem Nutzerkonten-Bund-Postfach und den vorhandenen Postfächern soll weiterhin gewährleistet werden.

Dokumenten-Safe

Im Dokumenten-Safe können Nutzer:innen ihre Dokumente geschützt speichern, um diese bei Online-Verwaltungsleistungen als Nachweise beifügen zu können. So wird eine sichere und zentrale Ablage von häufig verwendeten persönlichen Dokumenten zur Inanspruchnahme von Verwaltungsleistungen ermöglicht. Beispielsweise kann die Geburtsurkunde im Dokumenten-Safe abgelegt werden.

Registrierung Nutzerkonto

Die Registrierung für ein Nutzerkonto wird von dem geforderten Vertrauensniveau des jeweiligen Onlinedienstes bestimmt. Möchten Sie einen Onlinedienst in Anspruch nehmen, der eine niedrige Sicherheitsstufe aufweist, so reicht eine Basisregistrierung aus, um das Nutzerkonto anzulegen. Hierfür müssen Sie zunächst Ihre persönlichen Daten, wie Name, Vorname, Geburtsdatum und Adresse eingeben. Die verpflichtend anzugebenden Daten variieren zwischen den verschiedenen Nutzerkonten. So muss zum Beispiel nicht bei jedem Nutzerkonto das Geburtsdatum für die Registrierung angegeben werden.

Für die abschließende Basisregistrierung müssen Sie noch einen Benutzernamen und ein Passwort vergeben. Ein Großteil der Nutzerkonten fordert für die Registrierung zudem eine Sicherheitsfrage sowie die dazugehörige Antwort als zusätzliches Sicherheitskriterium. Nach der Registrierung können Sie sich mit dem festgelegten Benutzernamen und dem Passwort anmelden, um die entsprechenden Onlinedienste in Anspruch zu nehmen.

Onlinedienste, die eine hohe Sicherheitsstufe aufweisen, erfordern hingegen eine Registrierung auf einem hohen Vertrauensniveau. Für diese Art der Registrierung benötigen Sie ein elektronisches Ausweisdokument – Personalausweis mit der eID, elektronischer Aufenthaltstitel oder eID-Mittel der EU-Mitgliedstaaten (Europäische eID). Für die Anwendung der Funktionen der elektronischen Ausweisdokumente wird ein entsprechendes Kartenlesegerät oder ein Smartphone mit den notwendigen technischen Voraussetzungen benötigt. Die meisten Nutzerkonten bieten Ihnen an, Ihre Daten auch manuell eingeben zu können, wenn die eID-Funktion nicht freigeschaltet sein sollte. Das kann allerdings die Konsequenz nach sich ziehen, dass nicht alle Onlinedienste, die ein hohes Vertrauensniveau im Hinblick auf die Registrierung verlangen, in Anspruch genommen werden können.

Eine ausführliche Anleitung, wie Sie sich im ELSTER-Unternehmenskonto mit einem substanziellen Vertrauensniveau anmelden können, finden Sie im Beitrag von Jens Viere ab Seite 40.

Bund (o.J.): Datenschutzerklärung für das Nutzerkonto Bund. https://id.bund.de/de/eservice/konto/datenschutz [13.05.22] | **IT-Planungsra**t (o.J.): Beschlüsse und Empfehlungen des IT-Planungsrats. https://www.it-planungsrat.de/beschluesse [13.05.22]

Zur Umsetzung der Herstellung der Interoperabilität der Nutzerkonten wurde die Föderation FINK („Föderiertes Identitätsmanagement Interoperabler Nutzerkonten in Deutschland“) gegründet. Bund und Länder können der Föderation FINK beitreten, deren Ziel es ist, dass Bürger:innen mit ihrem jeweiligen Nutzerkonto, das in einem Bundesland beziehungsweise beim Bund angesiedelt ist, Verwaltungsleistungen anderer Verwaltungsportale außerhalb ihres Bundeslandes sicher in Anspruch nehmen können. Eine weitere Registrierung beim Nutzerkonto eines anderen Bundeslandes, zum Beispiel nach einem Umzug, soll damit nicht mehr erforderlich sein.

Der Freistaat Bayern wurde beauftragt, die Interoperabilität federführend umzusetzen. Dafür wurde das Kompetenzzentrum Interoperable Servicekonten („KIOSK“) als Föderationsverwaltung ins Leben gerufen. KIOSK kann als Organisationseinheit verstanden werden, welche die technischen Voraussetzungen und die organisatorischen Rahmenbedingungen der Interoperabilität der Nutzerkonten in Deutschland herstellt. Dazu gehören unter anderem die Wartung und Pflege der Schnittstellen sowie die Definition von Regeln für eine erfolgreiche Umsetzung der Interoperabilität. KIOSK erstellt in diesem Rahmen das Produkt FINK. **Es besteht aus drei Teilprodukten:**

1)

Der Metadatenserver

Über einen zentralen Metadatenserver werden die technischen Informationen und Konfigurationen zwischen den Teilnehmenden der Föderation ausgetauscht. Ein Metadatenserver stellt somit die Daten für die Vertrauensstellung und Kommunikation von Systemen in der Föderation der Interoperablen Nutzerkonten bereit. Die zentrale Metadatendatei enthält dabei eine Zusammenstellung der Metadaten aller Nutzerkonten, die an der Föderation der Interoperablen Servicekonten teilnehmen. Der Metadatenserver dient der sicheren und zuverlässigen Kommunikation zwischen den Nutzerkonten sowie zwischen den teilnehmenden Diensten. Es besteht kein Zugriff auf Daten der Bürger:innen.

2)

Die FINK.Spezifikationen

Die FINK.Spezifikationen ermöglichen die Interoperabilität zwischen den Nutzerkonten und deren Basisdiensten, indem sie die Kommunikationsschnittstellen in der Föderation festlegen. Die Vorgaben für die FINK.Spezifikationen sind die technischen Richtlinien des Bundesamtes für Sicherheit in der Informationstechnik (BSI), sowie Richtlinien, die sich aus dem OZG ergeben. Darüber hinaus werden die Standards eng mit den Teilnehmenden der Föderation FINK abgestimmt. So wird die Anbindung der von den Teilnehmenden eingesetzten Produkte vereinfacht. Mithilfe der Trennung zwischen der Spezifikation der Schnittstellen und der individuellen Implementierung von Diensten durch die Teilnehmenden wird ein hoher Grad an Transparenz und digitaler Souveränität gewährleistet.

3)

Die FINK.Labs

Die FINK.Labs stellen Test- und Integrationsumgebungen mit Testnutzerkonten zur Verfügung. Das ermöglicht es den Teilnehmenden, Zusammenspiel und Wechselwirkung der verschiedenen Komponenten interaktiv zu testen. Somit können Teilnehmende in der FINK.Labs-Umgebung Teststellungen ihrer Nutzerkonten mit Testdaten von erfundenen Personen ohne Bezug zur Realität hinsichtlich der Schnittstellen der Interoperabilität erproben.

Dominik Hiemer

DAS BUNDESWEIT EINHEITLICHE UNTERNEHMENSKONTO ALS GROßE CHANCE

In Zeiten der fortschreitenden Digitalisierung trägt das bundesweit einheitliche Unternehmenskonto maßgeblich dazu beitragen, in der gesamten Bundesrepublik einheitliche Standards für die digitale Verwaltung zu etablieren. Ein Text von Jens Viere.

Schon seit einigen Jahren stellt sich bei Nutzerkonten für Bürger:innen und Unternehmen die Frage, wie eine Identifizierung und Authentifizierung auf unterschiedlichen Vertrauensniveaus gewährleistet werden kann. Während für Bürger:innen der Weg in die Interoperabilität von Landes- und Bundesnutzerkonten führte, bildete sich für wirtschaftlich handelnde Organisationen über das Koordinierungsprojekt „Unternehmenskonto“ im Jahr 2019 der Vorschlag heraus, auf ein einheitliches Identifizierungsmittel für ganz Deutschland zu setzen.

In der Folge wurde das Gesamtprojekt „Einheitliches Unternehmenskonto auf Basis von ELSTER“ mit den Beschlüssen 2019/44 vom 23. Oktober 2019 und 2020/01 vom 14. Februar 2020 des IT-Planungsrats ins Leben gerufen. Bayern und Bremen wurden gemeinsam beauftragt, das bundesweit einheitliche, digitale Unternehmenskonto[1] auf Basis der aus der Steuer bekannten und bewährten ELSTER-Technologie zu entwickeln. Das Unternehmenskonto ermöglicht die sichere Kommunikation zwischen den Unternehmen und Behörden im Rahmen des Portalverbunds auf dem Hin- und Rückkanal (Antragstellung und Bescheidübermittlung). Bayern übernimmt hierbei die Entwicklung und den Ausbau der zentralen Bausteine 1 bis 4, Bremen entwickelt die ergänzenden Bausteine 5 und 6.

Ein Knopf, viele Funktionen: Das bundesweit einheitliche Unternehmenskonto gleicht einer umfangreich ausgestatteten Tastatur.

Nr.	Baustein	Kurzbeschreibung
1	Mein Unternehmenskonto[2]	Web-Anwendung – Einstiegsseite und Dashboard für die Administration des Unternehmenskontos
2	NEZO	Basis-Schnittstelle zur Identifizierung und Authentifizierung mit ELSTER-Zertifikaten, kurz für „Nutzung der ELSTER-Zertifikate im Rahmen des OZG“
3	NEZOP	Erweiterte Schnittstelle für Komfortfunktionalitäten wie Single Sign-On
4	Postfach 2.0	Zertifikatsgebundenes Postfach für die gebündelte Bereitstellung von Mitteilungen und Bescheiden
5	OZG-Plus Postfach	Erweitertes Postfach, das zusätzliche Anforderungen abdeckt (in Entwicklung in Bremen)
6	Autorisierungsmodul	Erweiterte Funktionalitäten zur Steuerung von Berechtigungen (in Entwicklung in Bremen)

Die Bausteine 1, 2 und 4 stehen seit Juni 2021 in einer Basisversion bereit. Sie weden seitdem kontinuierlich weiterentwickelt und im Echtbetrieb gemeinsam mit den Nutzenden optimiert. Damit sind bereits folgende Funktionalitäten verfügbar:

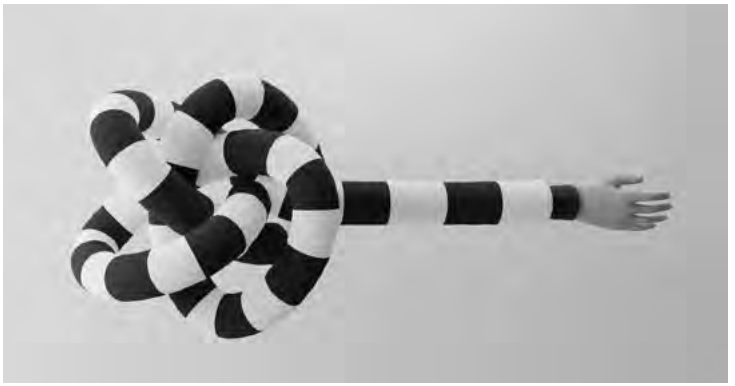
- Eine Web-Anwendung für Unternehmen
- Ein zentraler Identifizierungsdienst sowie der Registrierungsdienst
- Eine Postfachfunktion mit Bekanntgabemöglichkeit, die den gesetzlichen Anforderungen entspricht (§122a AO und §9 OZG)
- Die Infrastruktur für die Anbindung von Kommunen und Fachverfahren/ Verwaltungsleistungen

[1] Das OZG spricht von „Organisationskonto“, um zu unterstreichen, dass die Nutzung des Kontos auch für zum Beispiel Vereine und Behörden offen ist. Wir verwenden im Folgenden den etablierten und bekannten Begriff „Unternehmenskonto“. Letztendlich handelt es sich bei den Begriffen um Synonyme.

[2] Der Baustein „Mein Unternehmenskonto“ wurde im IT-Planungsratsbeschluss vom 14. Februar 2020 noch als „Mein Unternehmensportal“ bezeichnet. Hintergrund ist, dass die ursprüngliche Idee darin bestand, auf dieser Website auch (zumindest steuerliche) Onlinedienste anzubieten und ihr so einen Portalcharakter zu verleihen. Von dieser Idee ist das Projekt in der Entwicklung abgerückt, um die Oberfläche schlank zu halten und möglichst schnell eine erste Basisversion des Unternehmenskontos veröffentlichen zu können.

DAS ZIEL:

Ein Konto für alle unternehmensrelevanten Verfahren



Auch wenn die Ausgangslage noch so komplex ist: Am Ende gibt es immer eine Hand, die den richtigen Weg weist.

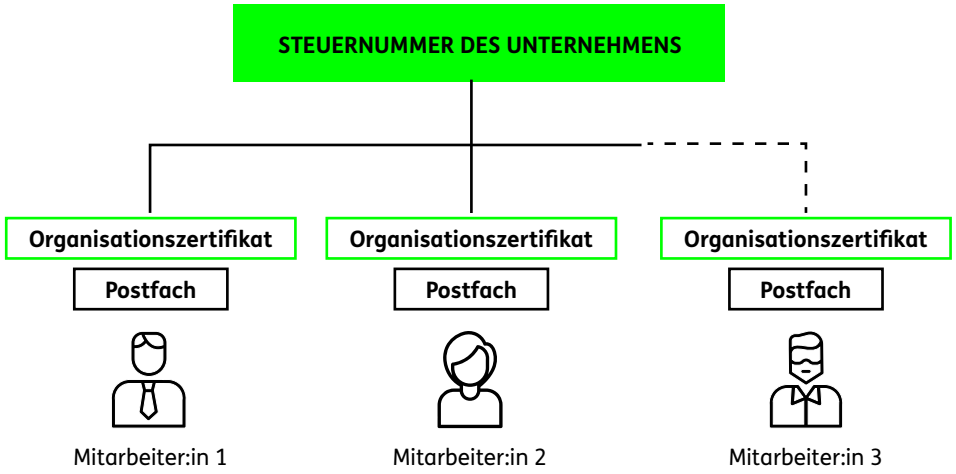
Das einheitliche Unternehmenskonto soll bis 2022 bundesweit als zentraler Einstiegspunkt gelten –egal ob in Flensburg oder Garmisch-Partenkirchen. Deshalb werden sukzessive alle wirtschaftsbezogenen Fachverfahren in Deutschland angebunden. Wichtig ist vor allem, die Authentifizierungskomponente und das Postfach in die Fläche zu bringen. Wirtschaftlich handelnde Organisationen aller Art können sich dann mit Hilfe ihrer ELSTER-Zertifikate bei Onlinediensten anmelden, Anträge authentifiziert ausfüllen, absenden und Bescheide der angebundenen Verwaltungsleistungen über ein Postfach empfangen. Über die Nutzung von ELSTER-Zertifikaten erlangen Organisationen eine hohe Flexibilität und können sich perspektivisch vollständig digital identifizieren. Auf Bundesebene koordiniert die Projektgruppe „Unternehmenskonto“ des IT-Planungsrats den bundesweiten Anschluss aller wirtschaftsbezogenen Verwaltungsleistungen an das zentrale Unternehmenskonto. Insbesondere steht dabei auch die inhaltliche Weiterentwicklung des Unternehmenskontos im Fokus. Für mögliche Erweiterungen des Funktionsumfangs wird derzeit ein Bund-Länder-gesteuertes Anforderungsmanagement entwickelt, um auch hier der Schnelllebigkeit des digitalen Wandels gerecht zu werden.

Weiterführende Informationen finden Sie hier:

- das-unternehmenskonto.de
- Unternehmenskonto-FAQ: service.mein-unternehmensportal.de/faq
- NEZO Organisatorische Vorbedingungen, NEZO Integrationsleitfaden & Postfach 2.0 Integrationsleitfaden (als PDF erhältlich auf Anfrage via info.muk@elster.de)
- Authentifizieren über ELSTER: service.mein-unternehmensportal.de
  Hilfe zu ELSTER-Transfer: elster.de/elsterweb/infoseite/elstertransfer_hilfe

ELSTER-Zertifikate als Grundlage der Unternehmenskonten

Das Unternehmenskonto ist kein einzelnes Konto im klassischen Sinne. In der Praxis interagieren schließlich immer Menschen mit Verwaltungsleistungen – keine Unternehmen als abstrakte Instanzen. Mehrere Mitarbeiter:innen vertreten das Unternehmen in verschiedensten Belangen. Das Unternehmenskonto speist sich deshalb aus einer Vielzahl von ELSTER-Benutzerkonten, die über eine Gemeinsamkeit verbunden sind: die Steuernummer des Unternehmens.
Die entsprechenden ELSTER-Zertifikate dieser Benutzerkonten werden als „Organisationszertifikate“ oder „Mitarbeiterzertifikate“ bezeichnet. Jedem Zertifikat ist ein Postfach zugeordnet, das auch nur über das jeweilige Zertifikat erreichbar ist.



Die Regelung in §87a Abs. 6 Abgabenordnung (AO) ermöglicht die Übermittlung von amtlich vorgeschriebenen Datensätzen mittels ELSTER. Die zur elektronischen Authentifizierung erforderliche Zertifikatsdatei wird im Rahmen der Registrierung kostenlos erstellt. Anhand des zur elektronischen Authentifizierung verwendeten Zertifikats wird der zweifelsfreie Ausweis des Datenübermittlers gegenüber der Verwaltung gewährleistet. Bei der Übermittlung für einen Dritten müssen die Daten dem „Dritten“ (Auftraggeber) in einer für ihn leicht nachprüfbaren Form zur Verfügung gestellt werden.
Die Authentifizierung über ELSTER war nach §87a Abs. 6 AO bislang nur in der Steuer- und Finanzverwaltung möglich. Mit Änderung des Onlinezugangsgesetzes wurde nun der §3 Abs. 2 S. 5 Onlinezugangsgesetz (OZG) eingeführt, der seit dem 1. Januar 2021 wirksam ist. Damit ist es möglich, die entsprechenden sicheren Verfahren auch für Verwaltungsangelegenheiten außerhalb der Steuer einzusetzen. Danach können sich über das Unternehmenskonto Nutzer:innen für die im Portalverbund verfügbaren elektronischen Verwaltungsleistungen von Bund und Ländern einheitlich über ein nach §87a Absatz 6 der Abgabenordnung in der Steuerverwaltung eingesetztes sicheres Verfahren identifizieren und authentisieren. Bei Nutzung der NEZO-Schnittstelle durch das Verwaltungsportal fungiert ELSTER als Nutzerkonto im Sinne des §2 Abs. 5 OZG. Die sogenannten ELSTER-Softwarezertifikate, die sowohl natürlichen Personen als auch Organisationen (zum Beispiel Unternehmen) zur Verfügung stehen, erlauben eine Identifizierung und Authentifizierung anhand der in den Registern des Bundeszentralamtes für Steuern (BZSt) beziehungsweise der Finanzbehörden gespeicherten Daten (§§139b f. AO). Im Übrigen ersetzt ELSTER bei der Antragstellung auch eine möglicherweise notwendige Schriftform, §8 Abs. 6 OZG.

Info

WIE LEGE ICH EIN ELSTER-UNTERNEHMENSKONTO AN?

Die Konto-Registrierung und Beantragung eines Organisationszertifikats

Über einen entsprechenden Button auf der zentralen Webanwendung www.das-unternehmenskonto.de haben Mitarbeiter:innen von Unternehmen und anderen Organisationen die Möglichkeit, ein Benutzerkonto zu erstellen. Der/die Mitarbeiter:in wird in den Registrierungsprozess von ELSTER geleitet, um ein ELSTER-Zertifikat zu beantragen. Die Registrierung erfolgt über die Organisations-Steuernummer eines Unternehmens. Es können beliebig viele Benutzerkonten für ein Unternehmen angelegt werden. Alle Mitarbeiter:innen, die in einem solchen Fall ein Benutzerkonto erstellen, erhalten ein eigenes ELSTER-Zertifikat, das sie zum Handeln im Namen des vertretenen Unternehmens befugt.

Info

Der Sonderfall:

Das persönliche ELSTER-Zertifikat

Im Grundsatz basiert das Unternehmenskonto auf den oben genannten Organisationszertifikaten. In Sonderfällen können aber auch persönliche ELSTER-Zertifikate für die Identifizierung und Authentifizierung genutzt werden. Bei persönlichen ELSTER-Zertifikaten für natürliche Personen liegt die Steuer-Identifikationsnummer zugrunde, die einer natürlichen Person zugeordnet ist. Diese persönlichen Zertifikate werden vor allem im Gründungsprozess relevant, wenn noch keine Gesellschaft oder Organisation besteht, deren Steuernummer Grundlage für die Beantragung eines Organisationszertifikats bilden könnte.

Zertifikate und Berechtigungen

Jede:r Mitarbeiter:in eines Unternehmens, der/die Zugriff auf das Unternehmenskonto haben soll, erhält ein Mitarbeiterzertifikat. Der Aktivierungscode für die Generierung des Zertifikats wird nach der Online-Beantragung durch den/die Mitarbeiter:in per Brief verschickt. Der Brief ist dabei nicht „zu Händen/persönlich“ an den/die Mitarbeiter:in adressiert, sondern wird an die in den Registern der Steuer hinterlegte Adresse des Unternehmens gesendet.

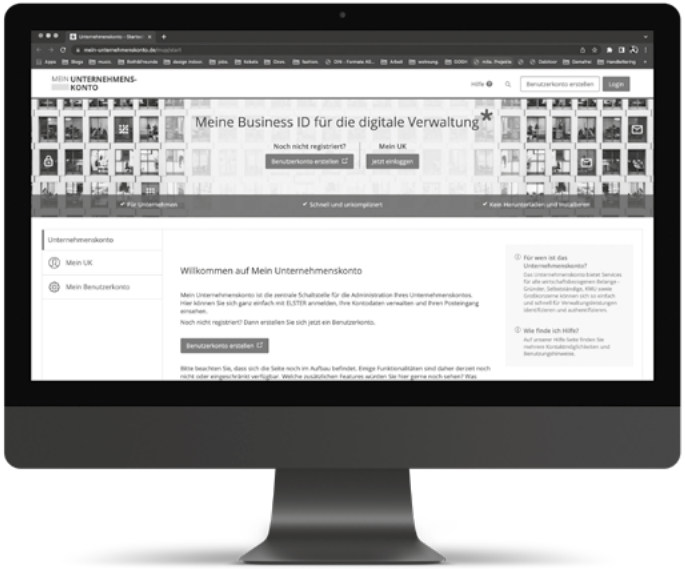
Die Aushändigung des Briefes zur Beantragung des Organisationszertifikats kann daher unternehmensintern kontrolliert werden. Entsprechend der Unternehmenshierarchie können so außerdem bestimmte Berechtigungen vergeben und unterschiedlichen Zertifikatsinhaber:innen ein erlaubter Handlungsumfang vorgegeben werden. Mit der an das jeweilige Zertifikat gekoppelten Account-ID ist eine Zuordnung von Handlungen und Anträgen zu einem/einer Unternehmensmitarbeiter:in möglich. Mit der Weitergabe des Aktivierungscodes an diejenigen Unternehmensmitarbeiter:innen, die ein ELSTER-Zertifikat beantragt haben, erteilt das Unternehmen eine konkludente Innenvollmacht, um digitale Verwaltungsleistungen für das Unternehmen in Anspruch zu nehmen. Eine Begrenzung auf bestimmte Online-Leistungen kann dabei nur im Innenverhältnis vorgenommen werden. Insoweit gilt wie bei Einzelvollmachten in der analogen Welt: Es besteht stets die Gefahr missbräuchlichen Handelns, sofern ein:e Mitarbeiter:in die Grenzen der Innenvollmacht überschreitet oder gar unbefugt an eine Legitimation kommen sollte, die nach außen den Rechtsschein setzt, dass er/sie zu der jeweiligen Handlung auch im Innenverhältnis berechtigt sei. Ein zentrales Tool zur Steuerung dieser Berechtigungen ist in den Bausteinen 1 bis 4 nicht integriert. Die interne Verteilung von Rechten und Rollen wird den Unternehmen selbst überlassen. Sollten Unternehmen ihr Berechtigungsmanagement auslagern wollen, steht ihnen perspektivisch das Autorisierungsmodul (Baustein 6) zur Verfügung.

„MEIN UNTERNEHMENSKONTO“

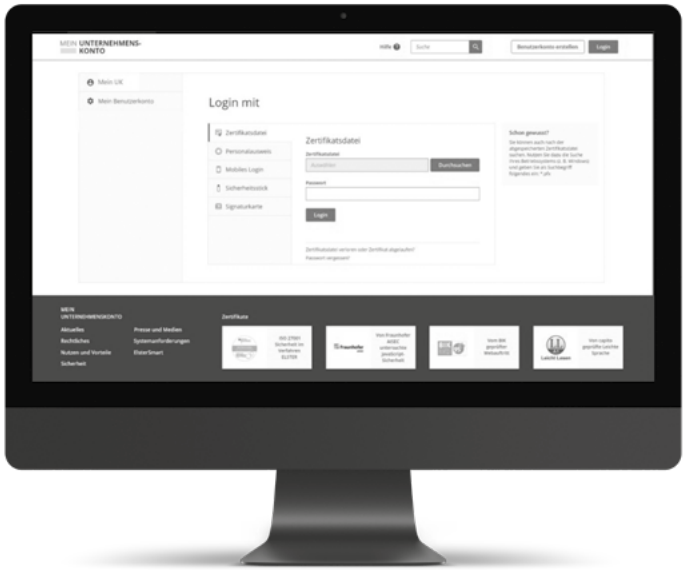
Verfügbare Bausteine (Stand: September 2021)

„Mein Unternehmenskonto“ (Mein UK) dient als Einstiegsseite und Dashboard für alle Unternehmen und Organisationen, wenn es um die Administration des Unternehmenskontos geht. In der Basisversion stehen dort folgende Funktionalitäten zur Verfügung:

- Die Registrierung eines neuen Unternehmenskontos
- Die Verwaltung des Postfachs: Loggt sich der/die Nutzer:in mit dem ELSTER-Zertifikat ein, erhält er/sie Einblick in das unternehmenseigene Postfach. Hier können Bescheide und andere Mitteilungen von Behörden eingesehen werden. Dabei gilt eine 1-zu-1-Beziehung von Zertifikat und Postfach. Nur wer die Berechtigung über ein Zertifikat erhält, kann online Anträge stellen, und nur wer einen Antrag mit einem Zertifikat gestellt hat, kann später die Antwort der Behörde auf diesen Antrag einsehen.
- Die Administration der ELSTER-Zertifikate: Zusätzlich steht dem/der Nutzer:in in der ersten Version von Mein UK der Zugriff auf sein/ihr Benutzerkonto zur Verfügung. Hier können Profilinformationen eingesehen und gegebenenfalls angepasst werden (zum Beispiel Löschung des Zertifikats, Änderung des Passworts, E-Mail-Einstellungen, ...).



Die Startseite von „Mein UK“: www.das-unternehmenskonto.de



Der Login-Bereich mit ELSTER-Zertifikat

NEZO

Die NEZO-Schnittstelle stellt eine der Kernfunktionalitäten des Unternehmenskontos dar. Über eine SAML-Komponente können Verwaltungsportale und Fachverfahren die Identität eines Unternehmens oder einer anderen Organisation einfach und schnell abfragen. So kann das Unternehmenskonto flexibel in unterschiedlichste Portaloberflächen integriert werden. Melden sich Antragssteller:innen zukünftig über ein Verwaltungsportal an, können sie zur Identifizierung und Authentifizierung unter anderem auswählen, das ELSTER-Zertifikat zu nutzen. Sie werden in der Folge auf die ELSTER-Login-Maske im gewohnten ELSTER-Look-And-Feel geleitet, um dort die Anmeldung vorzunehmen. Organisationen werden umfangreich aufgeklärt, können ihre gewohnten ELSTER-Authentifizierungsmittel nutzen und ihre hinterlegten Stammdaten einsehen, bevor diese nach ihrer Bestätigung an die Verwaltungsleistung weitergegeben werden. Durch Anzeige von Logo und Beschreibung der aufrufenden Verwaltungsleistungen wird den Anwender:innen immer der Kontext ihrer Authentifizierung vor Augen geführt und zudem die Möglichkeit gegeben, eine Änderung ihrer jeweiligen Daten zu beantragen. Hierfür wird immer angezeigt, aus welcher Datenquelle (Finanzamt oder Meldebehörde) ihre Daten stammen.
Nach erfolgreicher Anmeldung werden sie auf die Seite des Verwaltungsportals zurückgeführt, und die Antragstellung kann dort fortgeführt werden. Die Unternehmensdaten eingeloggter Nutzer:innen können daraufhin vorausgefüllt, ohne manuelle Eingabe in die Formulare übernommen und auf direktem Weg an die bearbeitende Stelle weitergeleitet werden.
Die NEZO-Schnittstelle wird sukzessive bundesweit in Verwaltungs- und Fachportale eingebunden und ersetzt so bislang bestehende Individuallösungen in den Bundesländern. Grundlage für NEZO ist das seit 2004 kontinuierlich fortentwickelte ELSTER-Identitätsmanagement, das es heute neun Millionen registrierten Bürger:innen sowie rund 1,5 Millionen registrierten Organisationen ermöglicht, über ELSTER mit der Finanzverwaltung zu kommunizieren.

POSTFACH 2.0

Um die vollständige Digitalisierung des Antragsprozesses zu gewährleisten, ist es notwendig, auch den Rückkanal mitzudenken. Das Unternehmenskonto etabliert insoweit ein kontoeigenes Postfach. Die Steuer hat schon heute ein Postfach über ELSTER-Transfer, mit dem seit einigen Jahren digitale Einkommenssteuerbescheide rechtsverbindlich bekannt gegeben werden können. Dieses Postfach soll in einer Version 2.0 nun außerhalb der Steuer genutzt werden. So können Behörden Verwaltungsakte und andere Mitteilungen digital an Organisationen senden und diese über eine Maschine-zu-Maschine-Schnittstelle sogar unmittelbar in den Systemen des Unternehmens eingelesen und verarbeitet werden. Dabei soll ein einheitliches Postfach etabliert werden, das heißt, das Postfach wird nicht in den jeweiligen Landes- oder Kommunalportalen liegen, sondern ausschließlich auf Mein UK erreichbar sein. Steigt das Unternehmen über ein Landesportal in die Verwaltungssuche ein, kann es über einen entsprechenden Reiter zum Postfach des Unternehmenskontos weitergeleitet werden. So können gebündelt an einer Stelle Mitteilungen und Bescheide bereitgestellt werden. Es besteht die Möglichkeit, dem/der Nutzer:in einen Deeplink zum Postfach bereitzustellen. Für den Zugriff ist dann eine Authentifizierung des/der Nutzer:in erforderlich.
Über das ELSTER-Postfach können Verwaltungsakte rechtswirksam nach §9 Abs. 1 OZG bekanntgegeben werden. Die Behörde wird außerdem via ELSTER-Transfer über den erfolgreichen Abruf durch die Organisation benachrichtigt, sodass entsprechende Rechtsbehelfsfristen zu laufen beginnen.

Behördenseitige Anbindung des Unternehmenskontos

Das einheitliche Unternehmenskonto ist modular aufgebaut. Die Bausteine müssen nicht alle gleichzeitig verwendet werden, sondern ermöglichen auch eine sukzessive, schrittweise Anbindung.

Hilfe für NEZO-Partner: das Self-Service Portal

Das Self-Service Portal stellt einen strukturierten Onboarding-Prozess und umfangreiche Informationen für NEZO-Partner bereit. Es zielt darauf ab, die Verbreitung des Unternehmenskontos zu beschleunigen und die Integration für behördliche Betreiber von Verwaltungs- und Fachportalen zu vereinfachen.

Anbindung der NEZO-Schnittstelle

Behördliche Portalbetreiber und Anbieter von Verwaltungsleistungen können mit Hilfe der NEZO-Schnittstelle ihren Zielgruppen den komfortablen und sicheren Login via ELSTER für ihre Webangebote ermöglichen. Die Anbindung der NEZO-Schnittstelle ist die Voraussetzung für alle weiteren Implementierungsschritte.

Je nach Art der Verwaltungsleistungen und des Nutzer:innenkreises sind unterschiedliche Konfigurationen möglich. Sie entscheiden unter anderem, welche Daten die Schnittstelle zurückliefert und welche Zertifikate unterstützt werden.

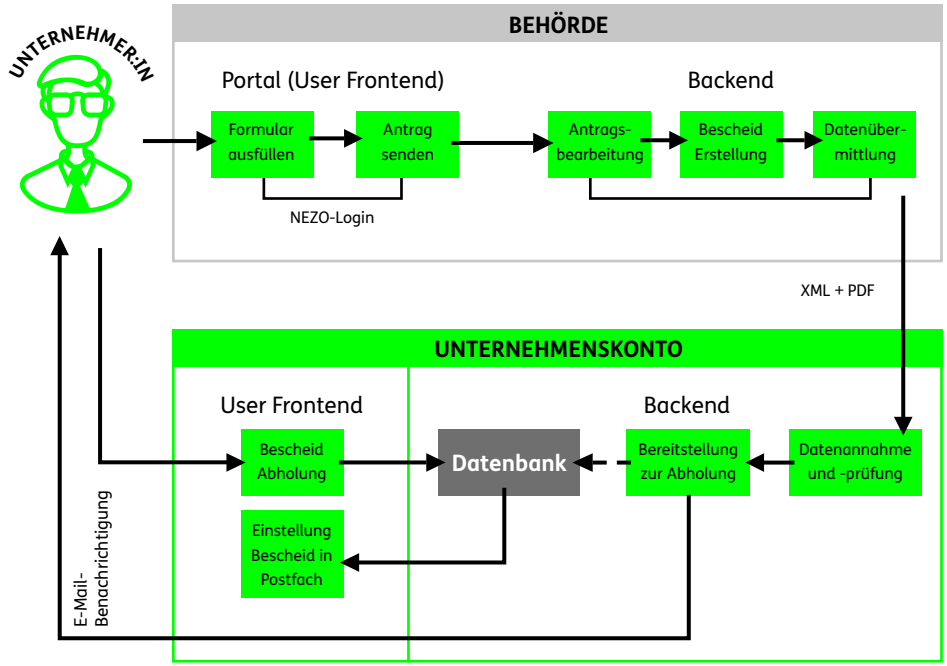
Vorausgefüllte Formulare

Die NEZO-Schnittstelle liefert bei dem Login über ELSTER einen Datenkranz zurück – eine Reihe von Attributen. Einige Attribute sind in jeder NEZO-Konfiguration in dem Datenkranz enthalten. Dazu gehört zum Beispiel eine pseudonymisierte ID (Account-ID), über die das zugehörige Postfach des/der jeweiligen Zertifikatinhaber:in adressierbar ist. Andere Attribute sind bestimmten Konfigurationen vorbehalten.

Wenn die NEZO-Schnittstelle für OZG-Leistungen oder für Leistungen innerhalb der Finanzverwaltung konfiguriert ist, liefert der Datenkranz eine Reihe von Organisations- und Personenattributen zurück, wie Namen und Adressen. Diese geprüften Stammdaten können in Formulare übernommen werden. Das steigert den Komfort für die Nutzer:innen und verschafft bearbeitenden Stellen eine abgesicherte Datenqualität. Die Übernahme der Daten in Formulare ist von der eingesetzten Formularlösung abhängig und muss in der Regel individuell implementiert werden.

Einstellen von Bescheiden und Nachrichten in das Postfach

Behörden können das zentrale Postfach des Unternehmenskontos nutzen, um Unternehmen rechtsverbindliche Bescheide sowie unverbindliche Nachrichten im PDF-Format zukommen zu lassen. Auch hier ist die Voraussetzung eine Anbindung der NEZO-Schnittstelle. Das Postfach kann in allen möglichen NEZO-Konfigurationen genutzt werden. Der Datenkranz liefert immer eine Account-ID zurück, mit der das Postfach eindeutig adressiert werden kann. Die E-Mail-Benachrichtigung zur Abholung von Bescheiden im Postfach des Unternehmenskontos erfolgt über die in ELSTER hinterlegte E-Mail-Adresse. Eine erneute Abfrage der E-Mail-Adresse durch Fachportale ist somit nicht erforderlich.



Auf diese Weise wird ein Bescheid im Postfach des Unternehmenskontos eingestellt.

Für den Versand der Bescheide und Nachrichten kommt das Verfahren „ELSTER-Transfer“ zum Einsatz. Je nach Ausgangssituation können verschiedene Wege für die Übermittlung von Nachrichten genutzt werden. Für Kommunen und Fachbereiche, die noch nicht über digitale Fachverfahren für die Bearbeitung von Anträgen verfügen, steht zum Beispiel eine Client-Anwendung mit grafischer Benutzeroberfläche bereit. Für die Integration in bestehende Fachverfahren bietet ELSTER-Transfer eine REST-API.

Wie viel Hoheit über unsere Daten in unseren Händen liegt, hängt von unterschiedlichsten Faktoren bei der Realisierung von digitalen Dienstleistungen ab.

Info

HINTERGRÜNDE ZUR TECHNISCHEN UMSETZUNG DER NEZO-SCHNITTSTELLE

Für die Realisierung von NEZO wurde das ELSTER-Identitätsmanagementsystem um notwendige Funktionalitäten ergänzt, sodass NEZO innerhalb kürzester Zeit betriebsfähig war und deutlich vor den Meilensteinen des IT-Planungsrats live gehen konnte. Die Funktionen im Überblick:

- Anbindung an die Stammdatensysteme von Bund und Ländern, um aktuelle Identitätsdaten liefern zu können
- Schaffung einer NEZO SAML-Schnittstelle zur Anbindung durch Verwaltungsleistungen
- Aufbau einer komfortablen Benutzeroberfläche für den Authentifizierungs- und Identifizierungsdienst NEZO
- Skalierbare, performante und hochverfügbare Architektur

Bei allen Funktionalitäten wurden die bei ELSTER vorhandenen hohen Ansprüche an Datenschutz und IT-Sicherheit vom Design her berücksichtigt und umgesetzt.

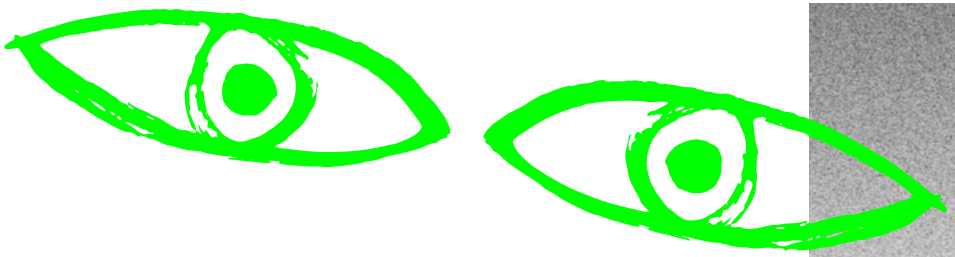
Anbindung von Stammdaten
Für die Lieferung von Identitätsattributen über die NEZO-Schnittstelle wird online auf die jeweiligen Register zugegriffen. Bei persönlichen ELSTER-Zertifikaten ist es die Steuer-Identifikationsnummer-Datenbank, die ihre Daten tagesaktuell aus den Meldebehörden erhält. Für ELSTER-Organisationszertifikate wird direkt auf die Daten der Finanzverwaltung in den jeweiligen Bundesländern zugegriffen, sodass auch hier eine hohe Aktualität der Daten gewährleistet ist. In der Regel hat eine Organisation bereits eine Steuernummer, mit der sie sich bei ELSTER identifizieren und registrieren kann, bevor zum Beispiel Einträge in den Handelsregistern erfolgen. Damit stehen ELSTER-Identitäten den Organisationen schon so frühzeitig zur Verfügung, dass sie ihre ELSTER-Zertifikate über NEZO für andere Verwaltungsleistungen nutzen können.

Standardisierte SAML-Schnittstelle
Die Anbindung von NEZO erfolgt über das durch den IT-Planungsrat vorgegebene SAML-Protokoll. Realisiert wurde NEZO von daher als einfache und standardisierte SAML-Schnittstelle („Security Assertion Markup Language“) nach dem „SAML V2.0 SSO Profile“ und kann durch standardkonforme SAML-Serviceprovider in kürzester Zeit angebunden werden. Durch entsprechende BSI-konform verschlüsselte und signierte Nachrichten wird ein hohes Maß an Authentizität und Vertraulichkeit aller Vorgänge gewährleistet. Je nach zugrundeliegenden Rechtsbereichen der angebundenen Verwaltungsleistungen können an der Schnittstelle auch Identitätsattribute, die über das Onlinezugangsgesetz hinausgehen, transparent für die Anwender:innen geliefert werden.

Skalierbarkeit und Performance
Alle an NEZO beteiligten ELSTER-Komponenten werden durch Loadbalancer angesteuert, sind n-fach vorhanden und auf mehrere Standorte verteilt. Die Zahl der Server kann bei Bedarf jederzeit hochskaliert werden. Dadurch können hohe Verfügbarkeit sowie entsprechende Performance gewährleistet, aber auch die hohen Sicherheitsstandards von ELSTER optimal umgesetzt werden.

Datenschutz
Zur Gewährleistung des Datenschutzes und der Verhinderung einer schleichenden Einführung einer Personenkennziffer, werden die Benutzer- und Organisations-IDs seitens ELSTER individuell pro angebundener Verwaltungsleistung pseudonymisiert. Individuelle Vorgänge auf einzelnen Verwaltungsleistungen können somit nicht anhand übergreifender IDs verfolgt werden. Weitere für die Anwender:innen wichtige Datenschutzfunktionen sind aktuell in Umsetzung.

Ausblick



Mit dem Rollout der Bausteine 1 bis 4 ist das Ende der Fahnenstange selbstverständlich noch nicht erreicht. Neben Identifizierung und Rückkanal kann ein bundesweit einheitliches Unternehmenskonto perspektivisch noch viel mehr bieten. Die bayerischen Bausteine werden zeitnah um weitere Funktionalitäten aus Bremen ergänzt. Mit dem OZG-Plus-Postfach (Baustein 5) wird ein Postfach bereitgestellt, das über den Funktionsumfang des Postfachs 2.0 hinausgeht und insbesondere komplexere Unternehmensstrukturen bedient (zum Beispiel beschränkten Zugriff auf das Postfach, Funktionspostfächer …). Zum einen soll das Autorisierungsmodul Unternehmen und anderen Organisationen ermöglichen, interne Berechtigungsstrukturen zu vergeben, zum anderen sollen hierüber auch Behörden den Zugang zu digitalen Verwaltungsleistungen einzelfallabhängig steuern können.

Der Kreativität sind bei der Weiterentwicklung des Unternehmenskontos kaum Grenzen gesetzt. Als integraler Bestandteil einer bundesweiten Unternehmensplattform kann das Konto eine Vielzahl von Daten aus unterschiedlichsten Registern sammeln und an diverse Stellen weiterverteilen. Als zentrale Datendrehscheibe könnten so Verknüpfungen zur Registermodernisierung, zu EfA-Leistungen und zu XÖV-Standards geschaffen werden. Die weitere Ausgestaltung des Projekts „Bundesweit einheitliches Unternehmenskonto“ bietet insoweit großes Potenzial.

Autor:innen: Prof. Dr. Wolfgang Hommel,
Dr. Daniela Pöhn und Michael Grabatin

DIE IDENTITÄTEN DER ZUKUNFT

Selbstbestimmter Umgang mit digitalen Identitäten

Die rasante Entwicklung von Technologien im Internet und der Digitalisierung wirkt sich auch auf digitale Identitäten aus. Gerade in diesem Bereich wird aber auch deutlich, wie langwierig und schwierig die Einführung neuer Konzepte ist.

Aufgrund der Tragweite für die Sicherheit der Daten digitaler Identitäten und der Systeme, zu denen sie Zugang gewähren, ist es nachvollziehbar, dass die flächendeckende Verbreitung etwas Zeit benötigt. Die aktuelle Diskussion im Bereich Identitätsmanagement dreht sich um die Dezentralisierung von digitalen Identitäten durch sogenannte selbstbestimmte Identitäten („Self-Sovereign Identities“, kurz: SSI). Diese sollen den Nutzer:innen mehr Kontrolle über die Verwendung ihrer Identitätsdaten geben und trotzdem sicher und flexibler einsetzbar sein.

Das Bewusstsein für Datenschutz entwickelt sich stark und sorgt dafür, dass Onlinedienste nicht nur einfach zu benutzen, sondern auch datensparsam sein müssen. Beide Aspekte werden durch das Konzept von selbstbestimmten Identitäten angegangen und verbessert. Es schlägt eine Brücke zur physischen Welt, in der Nachweise über die persönliche Identität beziehungsweise derer Attribute, wie die Zugehörigkeit zu einem Sportverein, dem Alter oder dem Wohnort, durch Ausweise erbracht werden. Je nach Situation kann durch das Vorzeigen eines geeigneten Ausweises so Zugang zum Sportstudio oder Club erlangt oder ein Bankkonto eröffnet werden.

Dabei entscheidet, je nach Situation, jede Person selbst darüber, mit welcher Identität und welchem Ausweis sie ihrem Gegenüber etwas Geeignetes über sich nachweist. Selbstbestimmte digitale Identitäten sollen das gleiche Prinzip online verwirklichen. Sowohl die in der physischen Welt verwendeten als auch die digitalen Ausweise haben dabei unterschiedlich schwer fälschbare Sicherheitsmerkmale. Diese müssen nach einer Risikoabschätzung immer dem geplanten Anwendungszweck angepasst werden.

In der digitalen Welt ist das schwieriger abzuschätzen als bei physischen Ausweisen. Es ist zwar häufig nicht schwer, einen Ausweis für einen Sportverein oder ein Ticket für den öffentlichen Nahverkehr zu fälschen, aber allein die räumliche Begrenzung auf eine bestimmte Sportstätte oder eine Stadt schränkt den potenziellen Missbrauch ein. Weiter ist das Risiko hoch, erwischt und mit den Konsequenzen konfrontiert zu werden. Im digitalen Raum kann

ein:e Angreifer:in vorgeben, an jedem beliebigen Ort zu sein, und sich in vielen Fällen auch vor der Strafverfolgung sicher fühlen.

Bei der Einführung neuer Systeme zum Identitätsmanagement muss daher ein besonderes Augenmerk auf die sichere Umsetzung gelegt werden. Neben der Sicherheit muss auch die Nutzbarkeit jeder Lösung stimmen, um überhaupt angenommen zu werden. Hier gibt es bei den aktuell verwendeten Verfahren zur Verwaltung von digitalen Identitäten eine große Variation in der Art der technischen Umsetzung.

Was macht eine selbstbestimmte digitale Identität besonders?

Bislang liegen die mit einer digitalen Identität verbundenen Daten wie ein Name oder eine E-Mail-Adresse immer bei einem Identitätsprovider. Dort haben die Nutzer:innen sie in der Regel selbst hinterlegt oder der Übertragung von einem anderen Provider zugestimmt. Diese Tatsache wird auch als Identitätssilo bezeichnet, da es einige wenige Orte gibt, an denen alle Daten zu den vorhandenen digitalen Identitäten gespeichert sind. Über das Konzept der Identitätsföderationen können diese Daten zwar zwischen einer größeren definierten Menge an Diensten ausgetauscht und flexibler verwendet werden. Die Daten liegen trotzdem in der Hand eines Identitätsproviders. Gerade aus Sicht des Datenschutzes, der immer darum bemüht sein muss, so wenige Datenspuren in Form von Metainformationen wie möglich zu hinterlassen, ist das zwar eine effiziente, aber mit Risiken verbundene Lösung. Der Identitätsprovider kann jedes Mal, wenn auf diese Daten zugegriffen wird, genau feststellen, mit wem die Daten geteilt werden.

Diese Metainformationen über die Verwendung von digitalen Identitäten sind begehrte Informationen und sicherlich ein Grund dafür, dass große soziale Netzwerke ihren Nutzer:innen die Möglichkeit geben, ihren Account mit anderen Onlinediensten zu verknüpfen. Diese können sich so, im Austausch für die Metainformationen, eine weitere Kombination von Benutzername und Passwort für einen weiteren Dienst sparen. Physische Ausweise hinterlassen keine solche Datenspuren, da nicht jede Verwendung gleich dem/der Aussteller:in des Ausweises meldet, wann, wo und warum der Ausweis vorgezeigt wird.

Selbstbestimmte digitale Identitäten ermöglichen es speziellen Onlinediensten („Issuer“), digitale Ausweise, die üblicherweise als Credentials bezeichnet werden, auszustellen. Die Nutzer:innen können diese, äquivalent zu physischen Geldbörsen, in digitalen Brieftaschen („Wallets“) selbst verwalten. Bei der Verwendung der Ausweise aus der digitalen Brieftasche kann individuell entschieden werden, welcher Teil des digitalen Ausweises dem Gegenüber („Verifier“) gezeigt wird, um Zugang zu einem Onlinedienst zu erhalten. Ein Vorteil dieses Verfahrens ist, dass jede Verwendung von Attributen aus der digitalen Brieftasche Zugriff auf diese und dadurch explizit die Zustimmung der Nutzer:innen erfordert. Das trägt zur Transparenz bei und zeigt auf, welche Dienste es mit der Datensparsamkeit und Minimierung von angeforderten Daten nicht zu genau nehmen. Darüber hinaus sind reale Identitäten auch nicht so binär wie es aktuelle Verfahren darstellen. Eine Person kann in verschiedenen Situationen mit jeweils anderen (Teil-) Identitäten oder Personalitäten auftreten. So unterscheiden sich die relevanten beschreibenden Attribute eines/einer Einzelnen zum Beispiel stark zwischen dem Berufs- und Privatleben. In beiden Fällen kann es auch noch zu weiteren Abstufungen kommen, sodass jede:r eine Vielzahl an unterschiedlichen Kombinationen von Attributen in verschiedenen Situationen nutzt.

Das System der digitalen selbstbestimmten Identitäten erlaubt es jeder Person, eine Menge an Attributen, die sie beschreiben, zu sammeln und je nach Kontext in verschiedensten Kombinationen zu verwenden. Ganz essenziell ist dabei, dass jede:r selbst eine digitale Identität anlegen kann und dafür nicht die Zustimmung eines Dritten benötigt. Daraus ergibt sich auch, dass verschiedene SSI-Systeme miteinander interoperabel gestaltet werden müssen. Ansonsten würden nur neue Identitätssilos geschaffen werden.

Die Entwicklung zu neuen Ansätzen für digitale Identitäten

Im Bereich der digitalen Identitäten gibt es immer neue Entwicklungen und Ideen. Bislang durchgesetzt hat sich davon keine. Für die meisten Onlinedienste ist weiterhin eine Kombination aus Benutzername und Passwort für jede Website nötig. Dass dieser Ansatz besonders anfällig für Angriffe über schwache Passwörter oder Phishing ist, ist allgemein bekannt. Sicherere Alternativen können sich nur schwer durchsetzen. Auch die Verwendung von Mehrfaktorauthentifizierung ist zwar immer häufiger möglich, wird aber wegen der zusätzlichen Abfragen bei der Anmeldung ungern genutzt.

Im Artikel auf Seite 16 wurde beschrieben, wie die Entwicklung von zentralen Identitätssilos hin zu föderierten Identitätssystemen geschafft wurde. Dabei waren Forschung und Wissenschaft Vorreiter in der Erprobung der Systeme und Prozesse, die jetzt auch im E-Government angekommen sind. Viele der dabei gewonnenen Erfahrungen können weiterverwendet werden, um ein dezentrales Identitätssystem aufzubauen.

Bereits bei föderierten Systemen stellen sich Fragen nach einer einheitlichen Reaktion auf Sicherheits- oder Datenschutzvorfälle. Da es hier noch den Föderationsbetreiber als zentrale koordinierende Instanz gibt, kann dieser Vorgaben machen und entsprechende Prozesse moderieren. In einem vollständig dezentralen System wird es schwieriger, über rechtliche Prozesse hinausgehend eine geordnete Moderation zu organisieren.

Ebenfalls müssen Attributsschemata vereinheitlicht werden, damit alle beteiligten Parteien die Attributszusicherungen der anderen verarbeiten und richtig interpretieren können. Und das ist bei Identitätsföderationen eine nicht zu unterschätzende Herausforderung, wodurch der gemeinsame Nenner der von allen unterstützten Attributen nur noch wenige Datenfelder enthält.

Welche Rolle kann dabei die Blockchain-Technologie spielen?

Im Zusammenhang mit selbstbestimmten Identitäten steht meist die Verwendung von Blockchains oder „Distributed Ledger Technologies“ (DLT). Dabei bezeichnen

Letztere eine Obergruppe von Datenstrukturen, zu denen auch Blockchains gehören. Gemein ist allen DLT-Systemen, dass sie ihre Daten über mehrere, voneinander getrennt betriebene Server verteilen. Damit alle immer über den gleichen Datenbestand verfügen, werden Konsensprotokolle verwendet, die dafür sorgen, dass alle Änderungen bei allen Teilnehmer:innen in der gleichen Reihenfolge und nach den gleichen Spielregeln eingefügt werden. So gibt es keine zentrale Instanz, die vorgeben kann, welche Änderungen angenommen werden und welche nicht.

Bei selbstbestimmten Identitäten sorgen DLTs dafür, dass die verschiedenen Teilnehmer:innen mit einer verteilten, aber überall gleichen Datenbasis arbeiten. Diese Datenbasis enthält dabei keine Informationen über persönliche Identitäten, deren Attribute oder Verwendung. Stattdessen dient sie zur sicheren Kommunikation der notwendigen Beschreibungen von Attributen, Schlüsseln und allgemeinen Konfigurationsparametern. Diese Daten sind so für alle Teilnehmer:innen sichtbar und nachvollziehbar festgehalten.

Je nach Ausprägung des Systems werden Blockchains verwendet, deren Unterhalt durch einen sehr aufwändigen Konsensalgorithmus („Proof-of-Work“) sehr energieintensiv sind. Die Alternative dazu sind DLT-Systeme, bei denen der Konsens zwischen den Beteiligten ohne das sogenannte „Mining“ erreicht wird. Diese haben in der Regel neben dem viel geringeren Energieverbrauch auch den Vorteil, dass sie schneller sind, also mehr Transaktionen pro Zeiteinheit verarbeiten können.

Blockchain als Lösung für alles? Ganz so einfach ist das leider nicht.

Im Prinzip kann ein System mit selbstbestimmten Identitäten auch ohne DLTs auskommen. Das Signieren und Überprüfen von digitalen Ausweisen ist auch über eine aus dem Internet von allen mit https ausgestatteten Webseiten bekannte Public-Key-Infrastruktur (PKI) denkbar. Da diese Art der Infrastruktur allerdings strikt hierarchisch und damit abhängig von wenigen Institutionen ist, wird sie häufig als nicht mit dem eigentlichen Ziel von selbstbestimmten Identitäten vereinbar angesehen.

Aktuelle Projekte im In- und Ausland

Der Hype um das Konzept von selbstbestimmten Identitäten sorgt dafür, dass es eine Vielzahl an Projekten gibt, die sich mit dem Thema beschäftigen. In Deutschland ist dabei auf Bundesebene das Bundeskanzleramt mit Projekten wie dem Hotel-Check-in sowie dem digitalen Führerschein oder die Bundesdruckerei mit einem Projekt zum digitalen Personalausweis beschäftigt. Bayern und Nordrhein-Westfalen arbeiten, wie auch andere Länder, an weiteren Projekten zu diesem Thema.

Um all diese Aktivitäten nicht zu stark divergieren zu lassen, sich gegenseitig abzustimmen und zu unterstützen, sind viele der interessierten Organisationen und Unternehmen in Konsortien, wie zum Beispiel IDunion, organisiert. Dort wird über die einzelnen Projekte hinweg daran gearbeitet, Systeme zu bauen, die sicher, kompatibel und leicht nutzbar sind.

Auch außerhalb von Deutschland gibt es viele Projekte zu selbstbestimmten digitalen und mobilen Identitäten. So wird EU-weit in dem Vorschlag der EU-Kommission zur Überarbeitung der eIDAS-Verordnung ganz konkret auch der Einsatz von digitalen Brieftaschen für digitale Identitäten vorgesehen.

Darüber hinaus finden sich auf allen Kontinenten ähnliche Projekte, die entweder in der Erprobung sind, oder sogar produktiv eingesetzt werden.

Ab wann ist diese Technologie einsatzbereit?

Die Chancen und Risiken bei einer neuen Technologie abzuwägen, ist ein Prozess, der viel Sorgfalt und Erfahrung benötigt. Die Vorteile in Bezug auf Datenschutz und Flexibilität herauszustellen, ist dabei das eine – darauf hinzuweisen, dass Selbstbestimmung auch notwendigerweise Selbstverantwortung bedeutet, das andere. Nur weil es einfach ist, einem Onlinedienst seinen digitalen Ausweis mit potenziell hochsensiblen und vertraulichen persönlichen Daten zu zeigen, heißt es nicht, dass das auch eine gute Idee ist. Was in der physischen Welt manchmal bereits schwierig einzuschätzen ist, ist online noch schwieriger. Daher ist es wichtig, dass es verschiedene prototypische Systeme gibt, die darauf hinarbeiten, dass die Technologie erprobt und verbessert wird. Gleichzeitig müssen auch organisatorische und rechtliche Rahmenbedingungen analysiert werden.

Neue Chancen bietet SSI auch im Kontext des Internet-of-Things (IoT). Dort ist mit immer stärker anwachsenden Zahlen von Geräten zu rechnen, die auch jeweils eine digitale Identität haben. Diese Geräteidentität kann zum Beispiel vom Hersteller mit Zusicherungen zu Produkteigenschaften, wie zum Beispiel der Messgenauigkeit, dem Produktionszeitraum und der Echtheit angereichert werden. Auf diese Weise können von den Geräten erfasste Daten automatisch eingeordnet und verarbeitet werden. Die eindeutige Identifizierung jedes einzelnen Geräts ist auch unerlässlich dafür, dass jedes Gerät einen digitalen Zwilling („Digital Twin“) erhält. Diese digitale Repräsentation eines physischen Geräts soll das Management der Geräte vereinfachen.

In einigen Bereichen kann SSI aktuell tatsächlich schon produktiv eingesetzt werden. Für viele Anwendungen ergeben sich noch Probleme mit Details zur Umsetzung, und es gibt weiterhin Bedarf an Untersuchungen und Forschung auf dem Gebiet, um schlussendlich ein wirklich sicheres und funktionierendes neues digitales und selbstbestimmtes Identitätsmanagementsystem zu erhalten.

Digitale Identitäten als europäische Aufgabe

Das Once-Only-Prinzip und der europäische digitale Binnenmarkt

Mit dem Inkrafttreten der eIDAS-Verordnung wurden auf europäischer Ebene auch die digitalen Identitäten neu gedacht und geregelt. Sie zielt auf einheitliche elektronische Identitätsnachweise ab, was als wesentliche Voraussetzung zur Verankerung des Once-Only-Prinzips verstanden werden kann. Als Leiter des europaweiten TOOP-Projekts gibt Prof. Dr. Dr. Robert Krimmer Einblicke in die verschiedenen Initiativen zur Umsetzung des Once-Only-Prinzips auf europäischer Ebene und zeigt auf, dass dabei neben den technischen Aspekten auch die Stärkung des digitalen Mindsets der Bürger:innen unabdingbar ist.

Als Ausgangspunkt für die Schaffung eines europäischen digitalen Binnenmarkts innerhalb der EU können die elektronischen Signaturen und Identitäten, die bereits seit dem Ende der 1990er-Jahre im Fokus der EU stehen, betrachtet werden. Eine erste Regulierung dieser erfolgte mit der Signaturrichtlinie im Jahr 1999. Im Hinblick auf die Transformation des Binnenmarkts hin zu einem digitalen Binnenmarkt erfolgte eine Neuordnung der Bereiche der elektronischen Unterschriften, Siegel und Identitäten im Jahr 2014: Mit Inkrafttreten der Verordnung (EU) Nr. 910/2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG (eIDAS-Verordnung)[1] wurde die digitale Identität auf europäischer Ebene neu geregelt. Schnell zeigte sich jedoch, dass diese Verordnung gewisse Einschränkungen mit sich brachte, hauptsächlich in Bezug auf die grenzüberschreitende Verwendung elektronischer Identitäten und Identifizierungsmittel. Es wurden Probleme für die Bereiche des sogenannten Record-Matching und Identity-Matching erkannt. Unter diesen Begriffen kann im Wesentlichen verstanden werden, dass es bei einer Identifizierung, die über eIDAS notifizierte eIDs erfolgt, zu Schwierigkeiten bei einem Abgleich der Datensätze kommen kann. Das ist insbesondere bei grenzüberschreitenden Services der Fall, wobei die Attribute der natürlichen Person verwendet werden, die vom eIDAS-Mindestdatensatz bereitgestellt werden. Außerdem werden in einigen Fällen zusätzliche, darüber hinausgehende Attribute genutzt, um eine Übereinstimmung der entsprechenden Person zu gewährleisten. Aufgrund eines Mangels an Interoperabilität der verwendeten Anmeldeinformationen, die in den eID-Systemen der einzelnen EU-Mitgliedstaaten definiert sind, kommt es zu Fehlern bei der Überprüfung der Identitäten.

Da die europäische digitale Identität eine der Prioritäten in der digitalen Strategie der Europäischen Kommission darstellt, wurde am 3. Juni 2021 mit dem Vorschlag für die Änderung der eIDAS-Verordnung erstmalig ein Rahmen für eine solche digitale Identität skizziert[2], der das reibungslose Funktionieren des Binnenmarktes gewährleisten und ein angemessenes Sicherheitsniveau für elektronische Identifizierungsmittel und Vertrauensdienste bereitstellen soll.

Der Anwendungsbereich dieser Verordnung konzentriert sich auf die von den EU-Mitgliedstaaten notifizierten elektronischen Identifizierungssysteme, die in der Union niedergelassenen Vertrauensdiensteanbieter und die sogenannten Wallets für digitale europäischen Identitäten. Das Hauptaugenmerkt liegt hierbei auf der Einführung des „European Wallets“. Es handelt sich hierbei um einen Service, der es den Nutzer:innen ermöglicht, ihre Identitätsdaten, Ausweise und andere mit der Person verknüpfte Attribute zu speichern. Diese können die Nutzer:innen online oder offline für Authentifizierungszwecke verwenden und qualifizierte elektronische Signaturen sowie Siegel erzeugen. Es stellt somit ein digitales Äquivalent zur physischen Geldbörse dar, in der wir alle unsere verschiedenen persönlichen Identitäten mit uns tragen – zum Beispiel den Personalausweis, Führerschein, Bankkarten oder die Gesundheitskarte.

Der aktuelle Entwurf der eIDAS-2.0-Verordnung verpflichtet die EU-Mitgliedstaaten, europäische digitale Wallets herauszugeben. Die Unionsbürger:innen profitieren hierbei von der verpflichtenden, kostenlosen Bereitstellung der Wallets und der damit einhergehenden Standardisierung. Die Verwendung der damit verbundenen Protokolle gewährleistet außerdem eine sichere und grenzüberschreitende Kommunikation. Dies soll den EU-Mitgliedstaaten ermöglichen, die auf nationaler Ebene verwendeten internen Authentifizierungsprotokolle frei zu wählen und damit eine Änderung der aktuellen nationalen Infrastruktur überflüssig zu machen. Auch für die Industrie bringt diese Entwicklung die Vorteile mit sich, dass einerseits verlässliche einheitliche Standards zum Einsatz kommen und andererseits die Möglichkeit entsteht, eigene Services auf Basis der bereitgestellten Technologien zu entwickeln und somit eigene Produkte auf den Markt zu bringen.

Die zuvor genannten gesetzlichen Maßnahmen wurden und werden von weiteren Initiativen flankiert. Hierzu gehört insbesondere Verordnung (EU) 2018/1724 über die Einrichtung eines einheitlichen digitalen Zugangstors zu Informationen, Verfahren, Hilfs- und Problemlösungsdiensten und zur Änderung der Verordnung (EU) Nr.

[1] **Verordnung (EU)** Nr. 910/2014 des Europäischen Parlaments und des Rats vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG. https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=celex%3A32014R0910 [06.05.22] |
[2] **Europäische Kommission** (2021): Kommission schlägt vertrauenswürdige und sichere digitale Identität für alle Europäerinnen und Europäer vor. https://ec.europa.eu/commission/presscorner/detail/de/IP_21_2663 [06.05.22]

1024/2012 (SDG-VO)[3]. Das Zugangstor soll einen wesentlichen Beitrag dazu leisten, einen transparenteren Zugang zu Vorschriften und Regelungen für verschiedene Wirtschafts- und Lebensbereiche wie Reisen, Ruhestand, Bildung, Beschäftigung und Gesundheit zu schaffen. Des Weiteren soll durch die konsequente Bereitstellung von Onlinediensten die Interaktionen zwischen Bürger:innen und Unternehmen auf der einen Seite und den zuständigen Behörden auf der anderen Seite vereinfacht werden. Hierfür werden seitens der EU mehrere zentrale Internetportale, zum Beispiel „Your Europe“ und das „European e-Justice Portal“, bereitgestellt.

Für den Betrieb dieser Portale und den damit verbundenen Services liegt ein Schwerpunkt auf einer durchgängigen Umsetzung des Grundsatzes der einmaligen Erfassung, der in Artikel 14 der SDG-VO verankert ist: dem Once-Only-Prinzip (OOP). Dieses Prinzip bietet die Grundlage für eine Steigerung der Nutzer:innenfreundlichkeit und gleichzeitige Möglichkeit zur Datenvermeidung. Damit wird einem steigenden Bedürfnis der Nutzer:innen nach Datenschutz und Kontrolle über die übermittelten Daten Rechnung getragen. Dies wird darüber hinaus dadurch flankiert, dass die SDG-VO mittels eines direkten Verweises herausstreicht, dass die Datenschutzgrundverordnung (DSGVO) in allen Bereichen Anwendung findet.

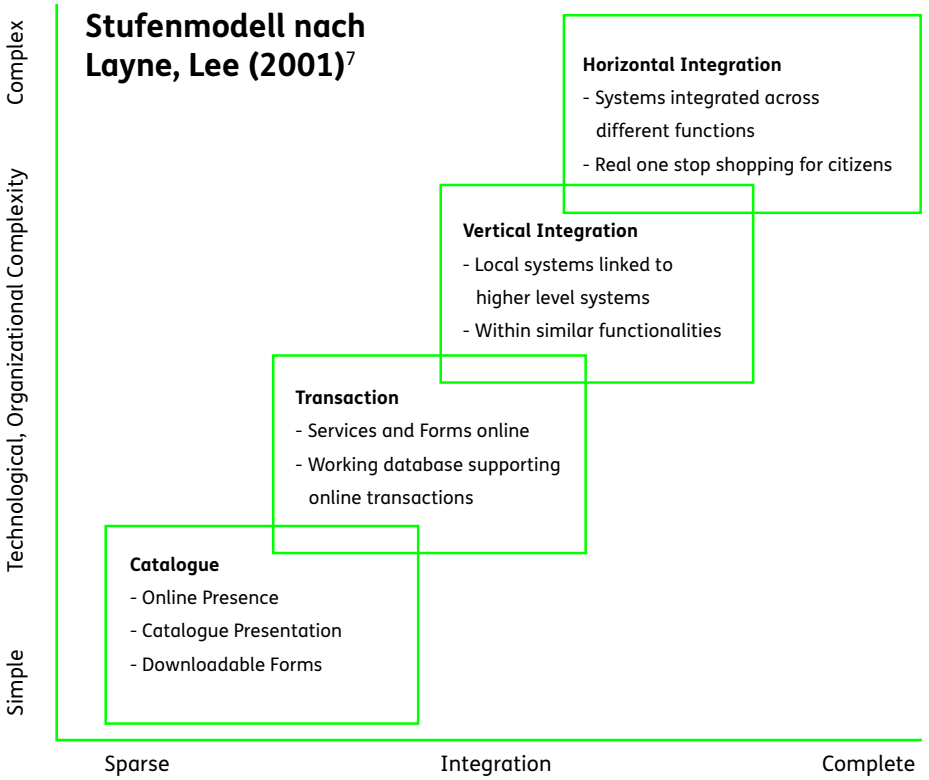
DAS ONCE-ONLY-PRINZIP

Das mit der SDG-VO auf europäischer Ebene rechtlich eingeführte OOP ist ein Konzept aus dem breiteren Kontext des E-Governments, welches darauf abzielt, dass Bürger:innen sowie Unternehmen und andere Organisationen spezifische Informationen nur ein einziges Mal gegenüber einer Behörde zur Verfügung stellen müssen. Das bedeutet, dass eine erneute Übertagung vermieden und stattdessen durch Verweise auf die Originalquellen in Basisregistern oder Nutzerkonten ersetzt werden sollten. Erstmals wurde das OOP als eines der Kernprinzipien im Rahmen der Deklaration von Tallinn des Treffens der IT-Minister während der estnischen Ratspräsidentschaft am 6. Oktober 2017 vorgestellt.[4]

Dieses grenzüberschreitende Übertragen von Informationen erfordert ein gewisses Grundmaß an Vertrauen zwischen den Verwaltungen, das auf dem gemeinsamen rechtlichen Verständnis im Rahmen der SDG-VO fußt. Zusammen mit den organisatorischen und technischen Konzepten des OOP gibt es damit zum ersten Mal in der Geschichte der EU die Möglichkeit eines horizontalen, sektorenübergreifenden Austauschs von digitaler Evidenz zwischen Verwaltungen von EU-Mitgliedstaaten und assoziierten Ländern.

[3] **Verordnung (EU)** 2018/1724 des Europäischen Parlaments und des Rats vom 2. Oktober 2018 über die Einrichtung eines einheitlichen digitalen Zugangstors zu Informationen, Verfahren, Hilfs- und Problemlösungsdiensten und zur Änderung der Verordnung (EU) Nr. 1024/2012. https://eur-lex.europa.eu/legal-content/de/TXT/?uri=CELEX%3A32018R1724 [06.05.W22]

Bisherige Austauschnetzwerke, wie das von EUCARIS[5] oder BRIS[6], stellen eine rein vertikale Vernetzung innerhalb eines Sektors dar, ähnlich wie dies Layne und Lee 2001 in ihrem Stufenmodell für die Entwicklung von nationalem E-Government vorhergesagt haben.



[4] **Europäische Kommission** (2021): Ministerial Declaration on E-Government – the Tallinn Declaration. https://digital-strategy.ec.europa.eu/en/news/ministerial-declaration-egovernment-tallinn-declaration [06.05.22] bzw. **BMI** (o.J.): eIDAS-Verordnung: Tallinn-Erklärung zu E-Government. https://www.bmi.bund.de/Webs/PA/DE/verwaltung/eIDAS-verordnung-der-EU/tallinn-erklaerung-zu-e-government/tallinn-erklaerung-zu-e-government-node.html [06.05.22]

[5] ausgehend vom Prüm Vertrag 2005, **Bundesministerium der Justiz** (o.J.): Vertrag über die über die Vertiefung der grenzüberschreitenden Zusammenarbeit, insbesondere zur Bekämpfung des Terrorismus, der grenzüberschreitenden Kriminalität und der illegalen Migration. https://www.bmj.de/SharedDocs/Downloads/DE/PDF/Themenseiten/Strafrecht/PruemerVertrag.pdf?__blob=publicationFile&v=1 bzw. die Überführung in EU Recht 2008 u.a. hier https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32008D0615 [06.05.22]

[6] **Durchführungsverordnung (EU)** 2015/884 der Kommission vom 8. Juni 2015 zur Festlegung technischer Spezifikationen und Verfahren für das System der Registervernetzung gemäß Richtlinie 2009/101/EG des Europäischen Parlaments und des Rats.https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32015R0884&from=EN [06.05.22]

Die Einführung des OOP sieht die nur einmalige Sammlung und Speicherung von Daten vor, was wiederum sowohl die vertikale als auch horizontale Integration nicht nur innerhalb eines Landes, sondern eben auch länderübergreifend erfordert. Das würde die Vereinfachung von Prozessen durch den automatischen Datenaustausch sowie den Ersatz von redundanter Datensammlung durch Verweise auf die ursprüngliche Quelle ermöglichen[8] und gleichzeitig die Zuverlässigkeit der Daten steigern. Entsprechend der SDG-VO könnte man die Eigenschaften des OOP auch wie folgt erweitern: Nur notwendige Informationen werden erfasst. Daten werden so ausgetauscht, dass sowohl Bürger:innen als auch Unternehmen und andere Organisationen kein zweites Mal danach gefragt werden müssen. Gleichzeitig müssen dabei die erforderlichen Datenschutzmaßnahmen berücksichtigt werden.

NATIONALE UMSETZUNGEN DES OOP

Während die Kodifizierung des OOP erst in den vergangenen Jahren vorgenommen wurde, haben viele EU-Mitgliedstaaten die Nützlichkeit dieses Prinzips bereits erkannt und schon implizit oder teilweise auch explizit mit der Umsetzung begonnen. In vielen Ländern war dies eine Reaktion auf bestehende Insellösungen oder eine geringe Datenqualität aufgrund des fehlenden Abgleichs zwischen den Registern, welcher eine Redundanz der Datensammlung und Duplizierung von Verwaltungsvorgängen zur Folge hatte. Zudem hat die stetig zunehmende Bürokratie auf Seiten der Bürger:innen und Unternehmen verstärkt zu Frustration geführt. Trotz ähnlicher Ursachen haben die EU-Mitgliedstaaten unterschiedliche Ansätze in der Umsetzung des OOP unternommen, was durch einen unterschiedlichen Verwaltungsaufbau oder auch heterogene IT-Systeme bedingt ist. In einer Untersuchung des TOOP-Projekts wurden die rechtlichen Regelungen, die Politik und die technische Umsetzung in EU- und EWR-Mitgliedstaaten zusammengetragen, die nachfolgend vereinfacht zusammengefasst sind[9]. Insbesondere die technischen Lösungsansätze unterscheiden sich zum Teil deutlich. Während die meisten Umsetzungen auf Bussystemen wie der estnischen X-Road beruhen, setzen einige auch auf Aggregationslösungen wie das in Deutschland diskutierte Nutzerkonto.[10]

[7] **Layne, Karen und Lee, Jungwoo** (2001): Developing fully functional E-government: A four stage model. In: Government Information Quarterly, Jg. 18, Nr. 2, S. 122-136

[8] **Krimmer, Robert, Kalvet, Tarmo, Olesk, Maarja und Cepilovs, Aleksandrs** (2017): The Once-Only Principle Project. Position Paper on Definition of OOP and Situation in Europe (updated version). http://dx.doi.org/10.13140/RG.2.2.34198.86089 [06.05.22]

[9] **Mamrot, Szymon und Rzyszczak, Katarzyna** (2021): Implementation of the 'Once-Only'Principle in Europe–National Approach. In: Krimmer, Robert, Prentza, Andriana und Mamrot, Szymon (Hrsg.), The Once-Only Principle. Lecture Notes in Computer Science, vol 12621. Springer, Cham, S. 9-37

[10] **Krimmer, Robert, Fischer, Dirk-Hinnerk und Schmidt, Carsten** (2017): Bürgerkonten und das Projekt „The Once-Only Principle". In: Public Governance, Herbst/Winter (2017), S. 12-15

[11] **Mamrot, Szymon und Rzyszczak, Katarzyna** (2021): Implementation of the 'Once-Only'Principle in Europe–National Approach. In: Krimmer, Robert, Prentza, Andriana und Mamrot, Szymon (Hrsg.), The Once-Only Principle. Lecture Notes in Computer Science, vol 12621. Springer, Cham, S. 9-37

Land	Rechtliche Basis	Politik/Programm	Nationale Infrastruktur
Belgien	x		x
Bulgarien	x	x	x
Dänemark		x	x
Deutschland	x		
Estland	x	x	x
Finnland	x		x
Frankreich	x	x	x
Griechenland			
Irland	x	x	
Island		x	x
Italien	x	x	x
Kroatien	x		x
Lettland		x	x
Liechtenstein			
Litauen	x		x
Luxemburg	x	x	x
Malta		x	
Niederlande	x		x
Norwegen	x	x	x
Österreich	x	x	x
Polen	x	x	
Portugal	x	x	x
Rumänien	x	x	
Schweden		x	x
Slowakei	x	x	x
Slowenien	x	x	x
Spanien	x	x	x
Tschechien	x	x	x
Ungarn		x	x
Zypern			

Übersicht der rechtlichen Regelungen, Politik/Programme und technischen Umsetzungen von OOP in den EU-Mitgliedstaaten[11]

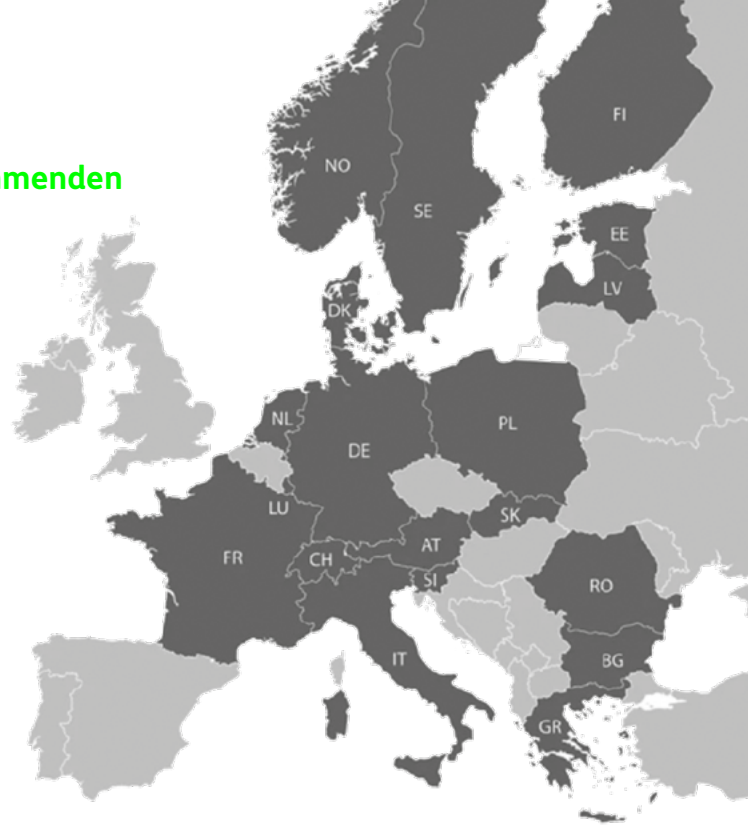
GROßPILOTIERUNGEN UND DAS TOOP-PROJEKT

Im Rahmen eines Austauschs zwischen der Europäischen Kommission und den EU-Mitgliedstaaten Anfang des neuen Jahrtausends ergab sich die Erkenntnis, dass es einer neuen Form der Zusammenarbeit für die Ermöglichung einer (erfolgreichen) Kooperation bei der Integration von Verwaltungsleistungen durch elektronische Hilfsmittel auf europäischer Ebene bedarf.[12] Das Instrument der Großpilotierungen („Large-scale Pilot Projects“, kurz: LSPs) war geboren. Bis 2021 wurden mehrere LSP mit unterschiedlicher Zielrichtung durchgeführt, zum Beispiel:

- beschäftigten sich STORK und STORK 2.0 mit der Entwicklung einer Interoperabilitätsplattform für elektronische Identitäten
- intendierte das SPOCS Projekt die Schaffung einer neuartigen Form des „Point of Single Contacts“
- zielte das epSOS Projekt auf den Bereich Open eHealth ab
- stand im e-CODEX Projekt die grenzüberschreitende e-Justiz Infrastruktur im Fokus
- stärkte das e-SENS Projekt die Entwicklung des Digitalen Binnenmarktes durch Konsolidierung der vorherigen LSP Resultate
- beschäftig(t)en sich das TOOP und das DE4A mit der Erarbeitung der Lösungen für die Umsetzung des einheitlichen Zugangstors (SDG-VO)

Das TOOP-Projekt[13] nimmt dabei als erstes Projekt mit dem Ziel der grenzüberschreitenden horizontalen Integration von verschiedenen Datenquellen eine Vorreiterrolle ein. Es wurde im Januar 2017 im Rahmen des 8. Forschungsrahmenprogramms Horizon 2020 mit dem Ziel der Erforschung, Testung und Umsetzung des OOP für Europa und der Ermöglichung eines grenzüberschreitenden, horizontalen und sektorenübergreifenden Datenaustauschs ins Leben gerufen. Das Hauptziel von TOOP war dabei die Vernetzung der Basisregister in den EU-Mitgliedstaaten. Basisregistern kommt dabei in TOOP eine entscheidende Rolle zu, da diese als maßgebliche Quelle für einen Datentyp in einem Sektor, einer Domäne fungieren, wie zum Beispiel Unternehmensinformationen oder Informationen zum Meldestatus von Bürger:innen. Das bedeutet, dass die in den Basisregistern enthaltenen Informationen immer den Letztstand beinhalten. Am TOOP-Projekt nahmen über 20 Mitgliedstaaten und assoziierte Länder der EU teil.

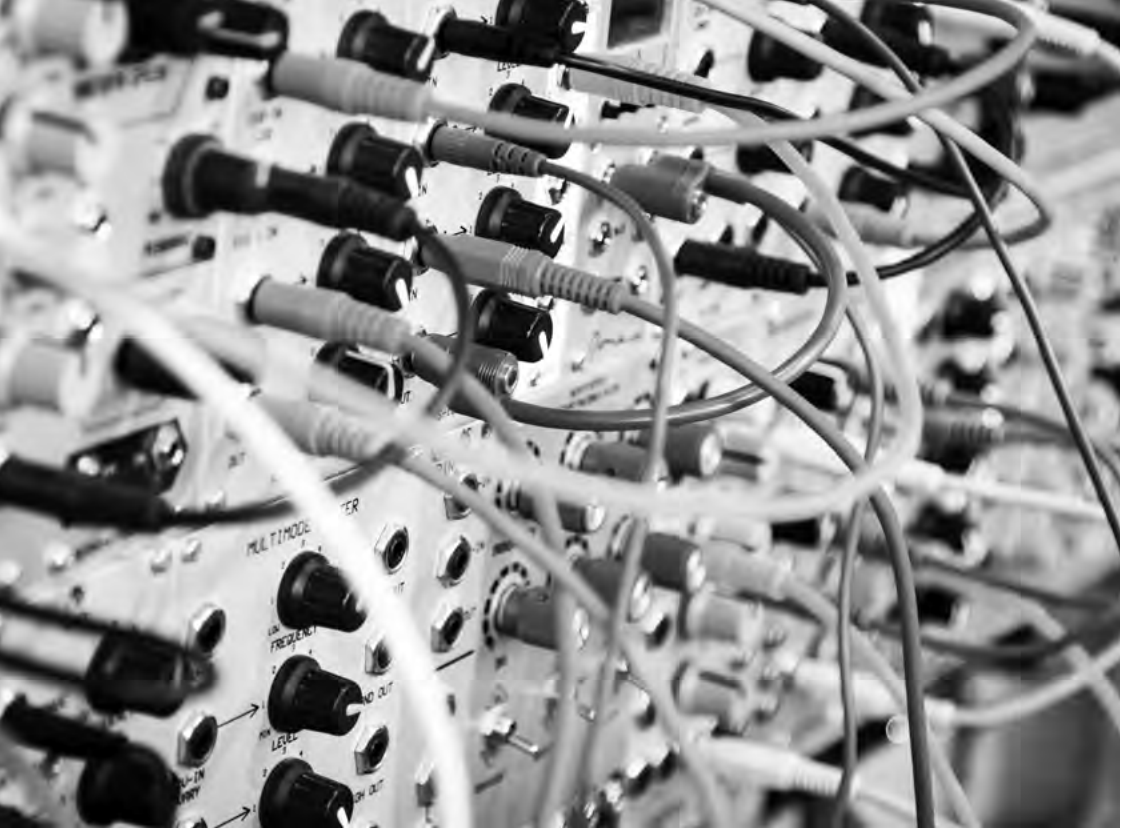
Karte der teilnehmenden Länder in TOOP[14]



Um die Funktionsfähigkeit von OOP zu demonstrieren, hat TOOP Piloten in den folgenden drei Themenfeldern umgesetzt: Unternehmensmobilität, Marine und E-Vergabe. Im Bereich der Unternehmensmobilität ging es um die Nutzung von Unternehmensdaten, beispielsweise für die Beantragung zur Ausstellung eines Zertifikats. Im Marine-Piloten wurde der Austausch von Crew- und Schiffszertifikaten untersucht. Bei dem E-Vergabe-Piloten ging es um die Beschaffung von qualifizierenden Belegen für die angebotslegenden wirtschaftlichen Akteure. Im Rahmen des Projekts wurde eine generische Referenzarchitektur (TOOPRA) entwickelt, die in der Folge auch Teil des Blueprints für das Once-Only-Technical-System im Zusammenhang mit der SDG-VO wurde. Die im Rahmen des EU-Projekts gesammelten Erfahrungen wurden in einem eigenen Buch zu dem Thema zusammengefasst.[15]

[12] **Schmidt, C., & Krimmer, R.** (2022). How to implement the European digital single market: identifying the catalyst for digital transformation. Journal of European Integration, 44(1), 59-80
[13] **Tallinn University Of Technology** (o.J.): providing data once-only.eu. https://toop.eu/ [06.05.22]

[14][15] **Krimmer, Robert, Prentza, Andriana, Mamrot, Szymon und Schmidt, Carsten** (2021): The Once-Only Principle: A Matter of Trust, In: Krimmer, Robert, Prentza, Andriana, Mamrot, Szymon (Hrsg.), The Once-Only Principle. Lecture Notes in Computer Science, vol 12621. Springer, Cham, S. 1-8



DIE ZUKUNFT DES GRENZÜBERSCHREITENDEN DATENAUSTAUSCHS

Das Zusammenwachsen des digitalen EU-Binnenmarkts stellt eine der Kernherausforderungen für die Umsetzung eines EU-weiten E-Government-Ansatzes dar. Im Vergleich zu den zugegebenermaßen unterschiedlich weit vorangeschrittenen, nationalen digitalen Transformationsbestrebungen des öffentlichen Bereichs, steckt die europäische Zusammenarbeit dennoch weiterhin in den Kinderschuhen. Gerade die Tatsache, dass sich die Europäische Union immer noch mit essenziellen Infrastrukturprojekten wie der Schaffung einer Datenaustauschinfrastruktur oder der Identifizierung der Bürger:innen durch europaweit interoperable nationale Identitätskarten beziehungsweise die neuartige EU-ID beschäftigt, zeigt den noch weiten Weg auf, der für die Realisierung eines funktionierenden digitalen Binnenmarkts notwendig ist.

Eine Grundvoraussetzung erscheint dabei die Stärkung der digitalen Bildung und einer daraus resultierenden positiven Einstellung zur Digitalisierung – ja, eines digitalen Mindsets. Dieses würde eine leichtere Überwindung der zuweilen in Deutschland vorherrschenden Datenangst ermöglichen, die oftmals die Diskussionen rund um Digitalisierungsprojekte wie dem Nutzerkonto und anderen Bestrebungen im Bereich des Onlinezugangsgesetzes überlagert.

Zur erfolgreichen Umsetzung benötigt es neben einem digitalen Mindset aber auch Anwendungen, die in den Bürger:innen ein konkretes Interesse wecken, sich mit der Technologie auseinanderzusetzen. Das können keine Infrastrukturprojekte sein, denn deren Vorhandensein stellt nur eine Voraussetzung dar, nicht aber einen Treiber ihrer Nutzung. Vielmehr zeigt sich anhand von positiven Beispielen in Österreich oder Estland, dass etwa Projekte im Bereich der e-Demokratie, wie den Internetwahlen oder dem e-Volksbegehren, Bürger:innen ansprechen. Vielleicht könnte die europäischen Bürger:inneninitiativen („European Citizen Initiative“) eine solche interesseweckende Anwendung darstellen? Möglicherweise liegt aber auch die Antwort in den IT-Lösungen zur Bewältigung der COVID-19-Pandemie, wie dem EU-weit funktionierenden Covid-19-Impfzertifikat. Klar ist aber auch, dass ein gewecktes Interesse allein nicht ausreicht. Vielmehr muss ein solches gewecktes Interesse durch hochfrequentierte und somit regelmäßig nutzbare Anwendungen im privaten Bereich begleitet werden. Ein Beispiel wäre, dass Online-Bankkonten verpflichtend den Einsatz der kommenden EU-ID unterstützen müss(t)en. Es könnte außerdem darüber nachgedacht werden, wie Bürger:innen auch privaten Betreiber:innen einen datenschutzkonformen Zugang zu im Rahmen der SDG-VO austauschbaren Informationen geben können. Das könnte die Nutzungsmöglichkeiten rasant steigern.

Zusätzlich muss diskutiert werden, ob durch den neuen Vorschlag zur EU-ID beziehungsweise zur Erweiterung von eIDAS die elektronischen Brieftaschen (E-Wallets) auch die Funktion eines EU-weit funktionierenden Nutzerkontos übernehmen könnten. Das fordert jedenfalls die bisher geschaffenen Lösungen für den digitalen Binnenmarkt heraus. Die bisher propagierten Ansätze setzen den direkten Austausch der Daten zwischen Verwaltungen voraus. Die E-Wallets und Nutzerkonten bringen hier nun die Bürger:innen ins Spiel, die den Verwaltungen Daten direkt bereitstellen und somit teilweise auch die Funktionsweise von Basisregistern als authoritative Quelle von Informationen infrage stellen.

Wir dürfen auf die weiteren Entwicklungen im Bereich des europäischen E-Government sehr gespannt sein und hoffen, dass die technischen Lösungen auch das Interesse und die regelmäßige Nutzung durch die Bürger:innen in Zukunft in den Vordergrund stellen.

Dank geht an Carsten Schmidt für die unterstützenden Arbeiten an diesem Beitrag!

Once-Only?

Only Open Source!

Die Bereitstellung eines zentralen Nutzerkontos für jede:n Bürger:in bildet einen wichtigen Meilenstein bei der Umsetzung des Once-Only-Prinzips in Deutschland. Doch damit das Angebot besser genutzt wird, muss die öffentliche Hand zeigen, dass sie mit den Daten verantwortungsvoll umgeht. Digitale Souveränität und Open Source werden so zu Garanten für mehr Akzeptanz digitaler Verwaltung.
Ein Text von Chiara Stuttfeld.

Wenn es um Vertrauen geht, lautet ein Lieblingsmotto der Deutschen: Es gibt keine zweite Chance für den ersten Eindruck. Dies gilt umso mehr, wenn das Gegenüber der Staat beziehungsweise die Öffentliche Verwaltung ist. Schließlich helfen alle technischen und regulatorischen Maßnahmen wenig, wenn am Ende Angebote entwickelt werden, denen die Bürger:innen mit einer latenten Grundskepsis begegnen. So passiert es schnell, dass „der Staat", der doch eigentlich wir alle sind, mit einem intransparenten bürokratischen Moloch gleichgesetzt wird, der die Bürger:innen zu Handlungen auffordert, deren Sinn nicht immer gleich verstanden wird. Schlanke und verständliche Informationswege sorgen hier für Abhilfe. Aus diesem Grund wurde im Rahmen des europäischen E-Government-Aktionsplans das Once-Only-Prinzip formuliert: Bürger:innen und Unternehmen sollten bei der Kommunikation mit der Verwaltung ihre Informationen nur noch einmal an zentraler Stelle angeben müssen. Alle relevanten Behörden und Verwaltungsorgane sollten diese Informationen anschließend untereinander teilen können.

Für die Bürger:innen bringt das Once-Only-Prinzip entscheidende Potenziale und Vorteile. Durch die einmalige Übermittlung von Daten wird den Bürger:innen zum einen eine gewisse Last abgenommen. Dank des Datenaustauschs zwischen den Verwaltungen können zudem Bescheide schneller und vor allem auch proaktiv von zuständigen Behörden versendet werden. Ein besonders wichtiger Punkt liegt außerdem in der Erhöhung der Transparenz: Diese liegt dann vor, wenn Bürger:innen ihre Informationen nicht nur zentral abgeben können, sondern auch über ein Nutzerkonto nachvollziehen können, welche Daten von ihnen abgerufen wurden. Auf diese Weise lässt sich die hierzulande (auch historisch begründete) vorherrschende Skepsis vor zu viel Zentralisierung in ein vertrauensvolles Verhältnis auf Augenhöhe drehen.

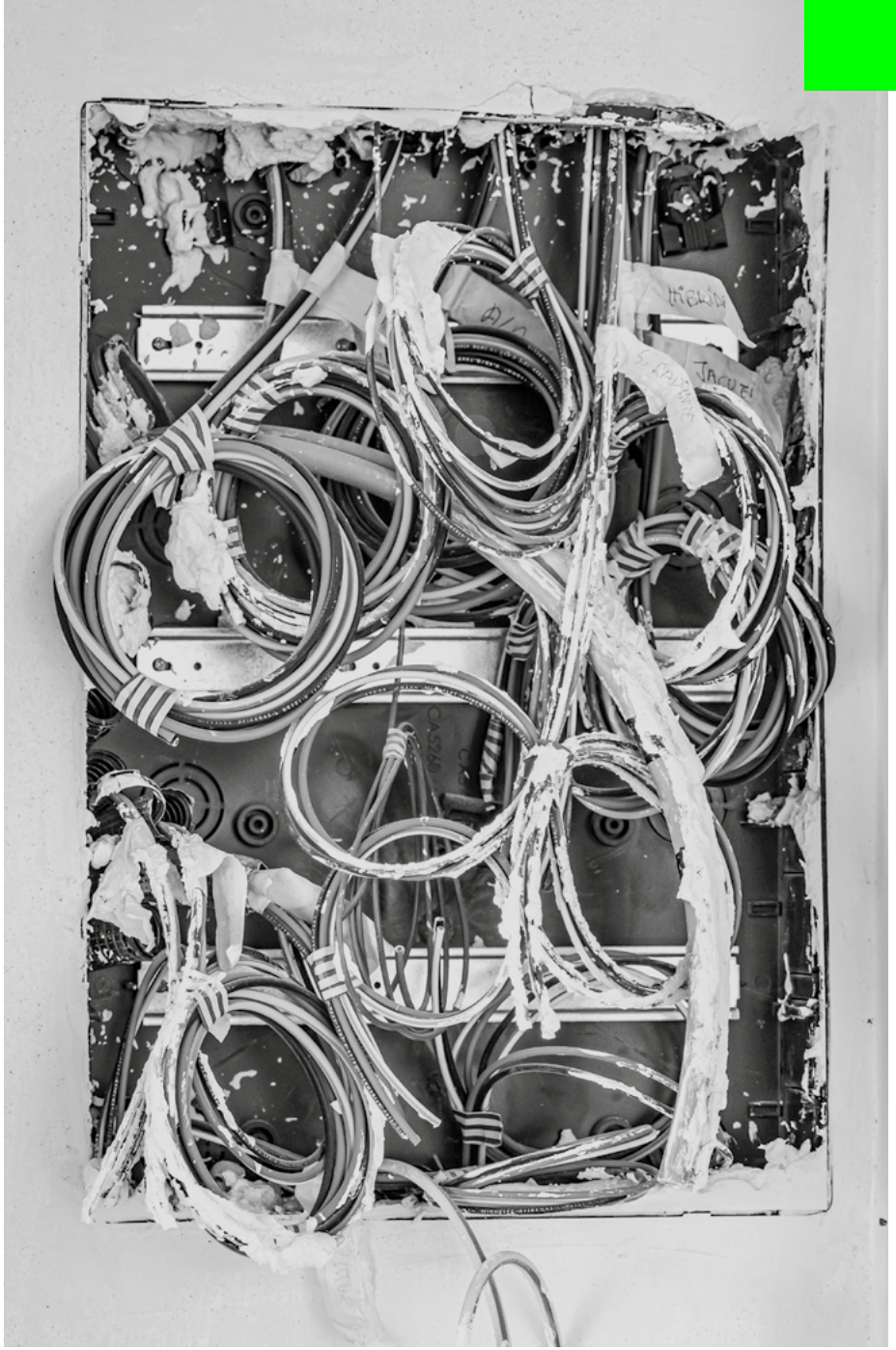
Für die Bürger:innen bringt das Once-Only-Prinzip entscheidende Potenziale und Vorteile.

Von Estland lernen

Wie das konkret aussehen kann, zeigt das europäische Musterland digitalisierter Verwaltung, Estland: Alle Datenbanken der Öffentlichen Verwaltung sind hier über die Software „X-Road" miteinander verbunden. Den Kern von X-Road bilden dabei individuelle Keys. Jeder Behörde, allen Bürger:innen und jedem Unternehmen ist ein digitaler Zwilling mit einer einzigartigen ID zugeordnet. Bei dieser im Grundsatz verteilten Server-Infrastruktur werden die Daten der Bürger:innen an verschiedenen Orten gespeichert und können bei Bedarf sicher geteilt werden. Der estnischen Regierung ist es damit gelungen, die Datensilos einzelner Behörden aufzubrechen. Ein wichtiger Grundsatz des Datenaustauschs liegt jedoch darin, dass Daten nur dann weitergegeben werden, wenn es absolut notwendig ist. Damit wird auch dem Prinzip der Datensparsamkeit Rechnung getragen, das eine zentrale Säule der EU-DSGVO bildet. Wie konkret sich dieses Prinzip auf den Einzelnen auswirkt, zeigt folgendes Beispiel: Wenn ein:e Bürger:in eine Fahrkarte für den Nahverkehr in Tallinn kauft, wird lediglich die Postleitzahl und die Information abgefragt, ob die Person gerade in Tallinn gemeldet ist. Datensätze werden nicht dupliziert und an verschiedenen Orten abgelegt, sondern mithilfe der X-Road ausgetauscht, ohne dass Dritte darauf Zugriff haben. Und dieser Zugriff ist ebenfalls streng geregelt: Beispielsweise können Ärzt:innen in Notfällen auf die digitale Krankenakte ihrer Patient:innen zugreifen. Genauso wichtig wie der praktische Nutzen ist dabei die Auskunftsmöglichkeit über das Nutzerkonto: Die Bürger:innen können selbst jederzeit problemlos einsehen, welche Daten über die X-Road von welcher Stelle – und sogar von welcher Person – abgefragt wurden. In Estland muss sich jede:r Beamt:in persönlich einloggen, bevor er/sie Zugriff auf das System und die Bürgerdaten erhält. Alle Abfragen werden chronologisch in diesem Nutzerkonto gespeichert. Die Bürger:innen sehen jederzeit, welche Behörde wann und zu welchem Zweck Daten abgefragt hat. Diese digital souveräne Infrastruktur wird dabei flankiert von einem juristischen Gerüst, das Datenschutzverstöße empfindlich ahndet und nicht als Kavaliersdelikte abtut. Das zeigt das prominente Beispiel des ehemaligen estnischen Ministerpräsidenten, dessen Krankenakte von mehreren Ärzt:innen unerlaubt eingesehen wurde, nachdem er einen Schlaganfall erlitten hatte. Allen Personen, die den Abruf nicht mit einem fachlichen Argument rechtfertigen konnten, wurde im Nachhinein die Approbation entzogen.

Bürger:innen im Fokus – und nicht die Behörde

Das Beispiel Estland zeigt: Ein zentrales Nutzerkonto wie im Fall von X-Road wird vor allem dann angenommen, wenn es als



Ruhig mal alles offenlegen: Eine Open-Source-Strategie kann das Vertrauen in Lösungen entscheidend steigern.

Tool für die Bürger:innen zur Wahrnehmung ihrer Informations- und Auskunftsrechte konzipiert ist – und nicht als komfortables Datenerhebungsinstrument für die Behörde. Wenn diese Transparenz gewährleistet ist, dann ist die wichtigste Grundvoraussetzung für Once-Only erfüllt. Der weitere Erfolg hängt darüber hinaus vom individuellen Nutzen ab, und hier spielt Open Source eine bedeutende Rolle. X-Road war in Estland nämlich nur erfolgreich, weil die Software komplett Open Source ist – ein Faktor, der von Anfang an in den Anforderungen festgehalten wurde. War der Code anfangs nur auf konkrete Anfrage zu beziehen, wurde er 2016 unter der MIT-Open-Source-Lizenz GitHub veröffentlicht. Die Motivation für den Open-Source-Ansatz lag laut Initiator:innen darin, dass die Bürger:innen der Lösung nur vertrauen würden, wenn auch jede:r den Code überprüfen könne.

Am Ende entscheidet der Nutzwert über die Nutzung

Neben dem Vertrauensaspekt bringt eine Open-Source-Strategie aber noch einen wichtigen Zusatznutzen: die Interoperabilität mit anderen Systemen, womit auch kommerzielle Lösungen eingeschlossen sind. Die X-Road-Infrastruktur konnte durch ihren Open-Source-Aufbau leicht von Banken für die Identifikation von User:innen genutzt werden, die ein Online-Banking-Konto eröffnen wollten. 2002 stiegen die zwei wichtigsten Banken in Estland von Pin-Codes auf die digitale Identifikation um. Durch dieses und andere Angebote stieg der Nutzer:innenanteil bis 2010 auf 40 Prozent aller estnischen Bürger:innen. Heute werden 99 Prozent aller Behördengänge in Estland online erledigt. In puncto Digitalisierung liegen zwischen Estland und Deutschland Welten. Zum Vergleich: Das 2019 in Deutschland veröffentlichte Nutzerkonto Bund verzeichnet derzeit 100.000 registrierte Nutzer:innen. Aktuell ist zwar geplant, weitere Onlinedienste anzubinden und insbesondere das Nutzerkonto einem Relaunch zu unterziehen – doch wenn die Entwicklung hierzulande einen ähnlichen Weg nehmen soll wie beim prominenten baltischen Vorbild, sollten sich unsere Behörden vor allem die Erfolgsfaktoren zu Herzen nehmen. Behördliche Datenerfassung kann nur dezentral, datensparsam und verteilt aufgebaut sein. Bürger:innen müssen in der Behördenkommunikation jederzeit das Gefühl haben, dass sie es sind, die die volle Souveränität über ihre Daten haben. Wer jederzeit einsehen kann, was welche Behörde mit welchen Daten warum anstellt, der versteht am Ende auch die Mechanismen der Öffentlichen Verwaltung und vertraut „seiner“ Behörde, dass sie in seinem Interesse handelt. Open Source spielt bei der Sicherstellung dieser digitalen Souveränität eine Hauptrolle – nicht nur, weil offener Code per se schon vertrauenswürdiger ist, sondern auch, weil er durch seine gemeinfreie Lizenz immer schon „uns allen“ gehört.

Behördliche Datenerfassung kann nur dezentral, datensparsam und verteilt aufgebaut sein.

GLOSSAR

ABAC
Attribute-based Access Control
Eine digitale Identität ist ein Datensatz, der aus einem Identifikator, Daten zur Abwicklung der Authentifizierung und beliebig vielen Attributen besteht. Den Attributen kommt dabei eine Schlüsselrolle zu: Aus ihnen lassen sich bestimmte Berechtigungen im Kontext der Dienstnutzung ableiten.

BRIS
Business Registers
Interconnection System
System zur Verknüpfung von Unternehmensregistern innerhalb der EU und des EWR.

BUSSYSTEM
„Bus“ steht für „Binary Unit System“. Innerhalb eines Netzwerks dient dieses System für die Datenübertragung zwischen den einzelnen Teilnehmer:innen. Die Nachrichten werden dabei über einen gemeinsamen Übertragungsweg versendet, wobei jedoch die einzelnen Datenübertragungen klar voneinander getrennt sind.

DFN
Deutsches Forschungsnetz
Verein mit über 300 institutionellen Mitgliedern aus der deutschen Hochschul- und Forschungslandschaft.

DIPOL-ARCHITEKTUR
Das Nutzerkonto ist sowohl Identity Provider für die Nutzer:innen im eigenen Bundesland als auch Service Provider. Als Service Provider ermöglicht es Bürger:innen aus anderen Bundesländern den Zugang zu bestimmten Diensten. Diese Doppelrolle wird im Kontext von FINK als Dipol bezeichnet.

DLT
Distributed Ledger Technologie
Daten werden über mehrere, voneinander getrennt betriebene Server verteilt. Um Nachverfolgbarkeit zu gewährleisten und um sicherzustellen, dass alle immer über den gleichen Datenbestand verfügen, werden Konsensprotokolle verwendet, die dafür sorgen, dass alle Änderungen bei allen Teilnehmer:innen in der gleichen Reihenfolge und nach den gleichen Spielregeln eingefügt werden.

ESCIENCE- UND ELEARNING-SYSTEME
Systeme für „elektronische“ oder „erweiterte“ (enhanced) Wissenschaft
eScience beschäftigt sich mit der schnellen und gemeinsamen Verarbeitung großer Datenmengen sowie deren Visualisierung. Darüber hinaus fördert eScience kollaborative und disziplinenübergreifende Forschung.
Systeme für „elektronisches“ Lernen
eLearning beschreibt Lernprozesse unter Verwendung moderner Informations- und Kommunikationstechniken (Internet, CD-ROM, Videoseminare, ...).

EUCARIS
European Car and Driving Licence Information System
Europäisches Fahrzeug- und Führerscheininformationssystem, das die zentralen elektronischen Systeme der europäischen Staaten zum gegenseitigen Datenaustauschs miteinander verbindet.

IDENTITÄTSFÖDERATION
Zusammenschluss von Organisationen, die auf technischer Ebene untereinander Personen- und Berechtigungsinformationen austauschen können.

IDENTITÄTSSILO
Bislang liegen die mit einer digitalen Identität verbundenen Daten immer bei einem Identitätsprovider. Dort haben die Nutzer:innen sie in der Regel selbst hinterlegt oder der Übertragung von einem anderen Provider zugestimmt. Diese Tatsache wird auch als Identitätssilo bezeichnet, da es einige wenige Orte gibt, an denen alle Daten zu den vorhandenen digitalen Identitäten gespeichert sind.

IDP
Identity Provider (Asserting Party; eigenes oder zusicherndes Servicekonto)
Die Heimateinrichtung, also diejenige Organisation, die eine digitale Identität verwaltet und bereitstellt, wird meist als IDP bezeichnet.

I&AM SYSTEM
Identity & Access Management System
Es gibt einen einzigen organisationsweiten Bestand an digitalen Identitäten, der von allen angeschlossenen IT-Diensten genutzt werden kann. Benutzer:innenbestände werden zentral eingepflegt und mit Attributen versehen, die festlegen, welche Personen welche Dienste in welchem Umfang verwenden dürfen.

JSON
JavaScript Object Notation
JSON bezeichnet ein standardisiertes Datenformat in Textform. Mittels JSON können Daten in Form eines JavaScript Ojekts dargestellt werden. Es kommt vor allem zum Einsatz, um Daten in Web-Applikationen zu übertragen. Um Daten auf einer Internetseite anzeigen zu können, müssen sie beispielsweise mittels JSON vom Server an den Client übertragen werden.

LDAP
Lightweight Directory Access Protocol
LDAP-Protokoll ermöglicht es, auf die Verzeichnisdienste, die zur technischen Umsetzung von I&AM Systemen benötigt werden, zuzugreifen.

LOAS
Levels of Assurance (Vertrauensniveaus)
Je nachdem, wie groß der Schaden bei Kompromittierung wäre und wie wahrscheinlich eine solche Kompromittierung ist, desto sicherer müssen die Verfahren zum Identitätsnachweis und zur Identitätsprüfung sein.

METAINFORMATIONEN
Metadaten beziehungsweise -informationen sind Informationen zu Daten. Sie beschreiben

andere Daten und erleichtern deren Archivieren und Auffinden.

OPENID CONNECT

OpenID Connect ist eine Authentifizierungsschicht, die es Clients ermöglicht, die Identität eines/einer Anwender:in zu überprüfen.

OPEN-SOURCE-SOFTWARE

Open-Source-Software beschreibt die Entwicklung von Software, die kollaborativ und gemeinschaftlich entwickelt wird. Die Ideen und die Codes teilen die Entwickler:innen mit der Öffentlichkeit. Auf diesem Wege kann jede:r, der/die den Source Code besitzt, mitwirken. Das kann Innovationen fördern.

OPT-IN-VERFAHREN

Opt-in beschreibt ein Marketing-Verfahren, bei dem die Kontakte gefragt werden müssen, ob sie mit Werbung oder Informationen (zum Beispiel Newslettern) bespielt werden dürfen. Möchte ein:e Nutzer:in diese Angebote erhalten, muss er/sie ausdrücklich in einer Anmeldung zustimmen. Somit willigt er/sie auch der Verwendung seiner/ihrer Daten zu.

OZG

Onlinezugangsgesetz

Gesetz zur Verbesserung des Onlinezugangs zu Verwaltungsleistungen.

PKI

Public-Key-Infrastruktur

Eine PKI beschreibt eine organisatorische und technische Infrastruktur, die es ermöglicht, kryptographische Schlüsselpaare (private Schlüssel in Form von PSEs und öffentliche Schlüssel in Form von Zertifikaten) zu verwalten und auszurollen.

PROOF-OF-WORK

Aufwendiger und energieintensiver Konsensalgorithmus der Blockchain-Technologie.

REST-API

Representational State Transfer - Anwendungsprogrammierschnittstelle

APIs beinhalten Regeln, die beschreiben und festlegen, wie Einheiten oder Anwendungen eine Verbindung zueinander herstellen und miteinander kommunizieren können. Somit können Komponenten in Microservices-Architekturen verbunden werden. Die Designvorgabe der REST-Architektur ermöglicht eine Flexibilität für die Entwickler:innen. So sind sie bei der Wahl der Programmiersprache und den Datenformaten weitgehend frei.

SAML-SCHNITTSTELLE

Eine SAML-Schnittstelle beschreibt einen IT-Sicherheitsstandard, der es seinen Anbieter:innen ermöglicht, Autorisierungs- und Authentifizierungsdienste anzubieten.

SP

Service Provider

(Relying Party; fremdes beziehungsweise vertrauendes Servicekonto) Ein Service Provider ist ein Anbieter von unterschiedlichen IT-Infrastrukturleistungen oder IT-Dienstleistungen. Die Kund:innen eines Service Providers können private Personen, Unternehmen oder auch Organisationen sein. Die Kund:innen müssen die Services nicht selbst betreiben, sondern können diese über den Service Provider einkaufen.

SSI

Self-Sovereign Identity

(selbstbestimmte Identitäten)

Das Konzept von SSI schlägt eine Brücke zur physischen Welt, in der Nachweise über die persönliche Identität durch Ausweise erbracht werden. Dabei entscheidet je nach Situation jede Person selbst darüber, mit welcher Identität und welchem Ausweis sie dem Gegenüber etwas über sich geeignet nachweist. Selbstbestimmte digitale Identitäten sollen das gleiche Prinzip online verwirklichen.

(VERIFIABLE) CREDENTIALS

Digitale Nachweise, die von Nutzer:innen selbst, zum Beispiel in einer Wallet-App, auf dem Smartphone gespeichert und dem jeweiligen Onlinedienst vorgelegt werden können.

VERIFIER

Gegenüber, dem der digitale Ausweis vorgelegt werden muss, um Zugang zu einem Onlinedienst zu erhalten.

WALLET

Selbstbestimmte digitale Identitäten ermöglichen es speziellen Onlinediensten, digitale Ausweise auszustellen. Die Nutzer:innen können diese, äquivalent zu physischen Geldbörsen, in digitalen Brieftaschen (Wallets) selbst verwalten.

XML

eXtensible Markup Language

XML ist ein textbasiertes Datenformat (wie JSON).

X-ROAD

Open-Source-Software für einheitlichen und sicheren Datenaustausch zwischen Organisationen.

BSI (o.J.c): Glossar. https://www.bsi.bund.de/DE/Service-Navi/Cyber-Glossar/cyber-glossar_node.html [04.05.22] | **BSI** (2021): Technische Richtlinie TR-03147 Vertrauensniveaubewertung von Verfahren zur Identitätsprüfung natürlicher Personen. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03147/TR03147.pdf?__blob=publicationFicle&v=3&msclkid=a170aa9ac16511ecbc61c2fc47726d7a [04.05.22] | **Datenschutzexperte** (o.J.): Opt-in und Opt-Out. https://www.datenschutzexperte.de/opt-in-und-opt-out/?msclkid=a3259f42c15711eca59246e27a1dcb13 [04.05.22] | **Deutsches Notarinstitut** (o.J.): Registerverknüpfung (BRIS) innerhalb der EU und des EWR. https://www.dnoti.de/informationen/aktuelles/details/registerverknuepfung-bris-innerhalb-der-eu-und-des-ewr/ [06.05.22] | **Fruhlinger, Josh** (2021): Security Assertion Markup Language: Was ist SAML? https://computerwelt.at/knowhow/security-assertion-markup-language-was-ist-saml/?msclkid=7a8e473bc14011ec892a50e58df0e714 [04.05.22] | **IBM** (2021): REST-APIs. https://www.ibm.com/de-de/cloud/learn/rest-apis?msclkid=742d80cfc07b11ec82bad23d29205386 [04.05.22] | **IBM** (o.J.): What is open source software? https://www.ibm.com/topics/open-source#:~:text=%20Some%20of%20the%20most%20popular%20open%20source,a%20free%20software%20license%20that%20allows...%20More%20?msclkid=4a4f03-11c15211ec9b8fafb44932f60f [04.05.22] | **IT-Wissen** (2018): Metadaten. https://www.itwissen.info/Metadaten-metadata.html?msclkid=2fcbe63ec15311ec81f07c8c0ef632cd [04.05.22] | **Kraftfahrtbundesamt** (o.J.): EUCARIS. https://www.kba.de/DE/Themen/ZentraleRegister/EUCARIS/eucaris_node.html [06.05.22] | **MDN Web Docs** (o.J.): Arbeiten mit JSON. https://developer.mozilla.org/de/docs/Learn/JavaScript/Objects/JSON?msclkid=4a18e99ec15b11ec-99b69ab1997582b1 [04.05.22] | **OpenID** (o.J.): What is OpenID Connect? https://openid.net/connect/?msclkid=66b5b69ac14911ec9e7f8c238d2b30ed [04.05.22]

Fazit & Danksagung

moysies & partners bedankt sich sehr herzlich bei allen Referent:innen, die mit ihren Beiträgen im Kompendium spannende Einblicke und wertvolle Impulse rund um den Themenkomplex der Nutzerkontenlösungen gegeben haben. Das Kompendium hat einmal mehr den hohen Stellenwert aufgezeigt, den die Nutzerkonten als Schlüssel zur einfachen und schnellen Nutzung von elektronischen Verwaltungsleistungen auf Ebene des Bundes, der Länder und der Kommunen einnehmen.

Mit Unterstützung der Referent:innen konnte im Rahmen des Kompendiums ein Überblick über den aktuellen Stand der interoperablen Nutzerkonten und des ELSTER-Unternehmenskontos geschaffen, Entwicklungsmöglichkeiten der Kontenlösungen sowie die damit verbundenen Herausforderungen aufgezeigt und Chancen zur Weiterentwicklung der digitalen Identitäten diskutiert werden. Der Blick über den Tellerrand zu Initiativen und Bemühungen auf europäischer Ebene zeigt uns, welche Möglichkeiten intensive und mutige Vorhaben auf diesem Gebiet mit sich bringen können. Es bleibt also spannend, wohin die Reise der Nutzerkonten gehen wird.

Persönlich möchte ich mich noch sehr herzlich bei den Kolleginnen Friederike Martin, Frederike Knuth, Maj-Britt Rosier und Sarah Naumann für die unermüdliche Arbeit und das tolle Engagement bei der Zusammenstellung der Inhalte und der Abstimmung mit den Referent:innen bedanken sowie bei Jördis Hagemeier für die großartige Organisation der Gestaltung und Erstellung dieses Kompendiums.

Christian Mohser
Geschäftsführer, moysies & partners GmbH

Impressum

moysies & partners GmbH
Adolfstraße 15, 65343 Eltville, Deutschland

Kontakt:
M: info@moysies.de
T: +49 6123 20801-00

Rechtsform:
Gesellschaft mit beschränkter Haftung

Vertretungsberechtigte Gesellschafter:
Geschäftsführer: Till Moysies, Nebojsa Djordjevic, Christian Mohser

Register:
Handelsregister: Amtsgericht Wiesbaden
Handelsregisternummer: HRB 33186

UStID-Nr. gem. §27a UStG:
Umsatzsteuer-Identifikationsnummer: DE287527903

Berufshaftpflichtversicherung gem. §2 DL-InfoV:
Markel International Insurance Company Limited,
Niederlassung für Deutschland, Sophienstr. 26, 80333 München
Räumlicher Geltungsbereich: Mitgliedsländer der EU

Inhaltlich verantwortlich i.S.d. §18 Abs. 2 MStV:
Christian Mohser (Geschäftsführer), Anschrift wie oben

Bildnachweise:
Bzgl. der innerhalb dieses Kompendiums verwendeten Bilder wird – sofern nichts anderes angegeben – auf die nachfolgenden urheberrechtlichen Informationen verwiesen:
Unsplash.com: Adrian Swancar, Anh Tuan To, Girl With Red Hat, John Barkiple, Notme, Ralph Ravi Kayden, Simon Lee, Warren Umoh, Gamze Senturk | Die Bilder der Referent:innen wurden von diesen zur Verfügung gestellt.

Design und Umsetzung:
SAO Design

moysies & partners

fine consulting

moysies.de