Bundesministerium für Bildung und Forschung

Bundesinstitut für Berufsbildung

VDI|VDE|IT

DIGITALE IDENTITÄTEN UND IDENTITÄTSMANAGEMENT

Technologiehinweise für die INVITE-Projekte

Justus Gutte, Dr. Thomas Hübsch, Dr. Martin Weimer, Dr. Susanne Ritzmann, Elke Vogel-Adham, VDI/VDE Innovation und Technik GmbH (Digitalbegleitung)

Stand April 2022

Digitale Identitäten und das Identitätsmanagement spielen für Weiterbildungspattformen eine wichtige Rolle. Sie sind eine Voraussetzung für „digitale Souveränität“, welche ein wesentlicher Schwerpunkt der deutschen und europäischen Digitalpolitik ist.

Bildungseinrichtungen und -anbieter stehen vor der großen Herausforderung jetzt und in Zukunft Zeugnisse, Abschlüsse, Urkunden und Zertifikate digital vergeben und manipulationssicher verwalten zu können. Selbstsouveräne Identitäten (SSI) der Lernenden könnten dabei ein Weg sein, die Verwaltungsprozesse (der Lernenden und der Bildungseinrichtungen) erheblich zu vereinfachen. Das Überprüfen von Zertifikaten (z. B. der Hochschulzulassung oder bisheriger Qualifikationen) könnte bspw. automatisiert in diverse Verwaltungsprozesse einer Bildungseinrichtung integriert werden. Nutzende wiederum könnten für eine datenschutzfreundliche und selbstbestimmte Verwaltung eigener Nachweise SSI nutzen, um in ihren digitalen Brieftaschen alle relevanten Bildungsfortschritte abzulegen und bedarfsgerecht und selbstbestimmt einzusetzen (z. B. bei Bewerbungen oder aufbauenden Bildungsangeboten).

Weiterhin ermöglicht die Integration von vertrauenswürdigen Single Sign-On-Umsetzungen (SSO) ein sinnvolles Identitätsmanagement, um mit einer Identität mehrere Bildungsangebote wahrnehmen zu können. Es sollte das Ziel sein, Lernende nicht an eine Plattform zu binden, sondern ihnen in einem Bildungs-Ökosystem die Kombination verschiedener Dienstleister und Dienste zu ermöglichen, die ihren derzeitigen Bedürfnissen, die besten Lösungen bieten. Die Konzeption des digitalen Identitätsmanagements sollte trotz aller Vorteile derzeitiger Ansätze anpassungsfähig und ausbaufähig bleiben. Da bspw. SSI bisher im Bildungsbereich wenig verbreitet ist, fehlen derzeit Erkenntnisse und Fallbespiele aus Sicht der verschiedenen beteiligten Akteure. Gleichzeitig erscheint die Einbeziehung der Nutzenden in die Konzeption des Identitätsmanagements auf Plattformen noch unzureichend. Gerade selbstsouveräne Konzepte sollten auch von Nutzenden verstanden werden und gewollt sein, bevor diese in die Anwendung kommen.

Vor diesem Hintergrund sollen die vorliegenden Technologiehinweise dazu dienen, Begriffe und grundlegende Überlegungen zu den Themen digitale und selbstsouveräne Identitäten, Identitätsprüfung, Sicherheitsbedrohungen und Identitäts- und Zugriffsmanagement den Projektmitarbeitenden der geförderten INVITE-Projekte näherzubringen. Eine Einordnung von Begriffen und aktuellen Entwicklungen insbesondere im Bildungsbereich soll so erleichtert werden.

Identitäten

Eine Identität umfasst die Gesamtheit aller Eigenschaften und Attribute einer Person oder einer Sache, die das Bezeichnete als individuelle Instanz von anderen Instanzen unterscheidet. Eine digitale Identität kann hierbei als Sammlung von festgelegten, maschinenlesbaren Identifizierungsmerkmalen für eine Person bzw. ein Objekt angesehen werden. Mit dem Nachweis der eigenen digitalen Identität kann den Nutzenden beispielsweise Zugriff auf Dienste verschiedener Weiterbildungsplattformen ermöglicht werden. Häufig wird erst dadurch eine nachhaltige Interaktion zwischen Nutzendem und (Weiterbildungs-) Plattform möglich. Folgende allgemeine Aspekte betreffen Prozesse rund um Identitäten:

Identifikation

Da eine Identität in ihrer Gesamtheit meist nicht erfasst werden kann, wird eine eindeutige Bezeichnung als Referenz auf die Identität benötigt. In kleinen Gruppen reicht bspw. der Vorname einer Person meist aus. Mit steigender Gruppengröße bzw. Größe der Gesamtheit werden üblicherweise weitere Attribute hinzugezogen, wie zum Beispiel der Vor- und Nachname in Kombination mit dem Geburtstag. In Verwaltungssystemen oder Software-Datenbanken ist die Vergabe einer einzigartigen Kombination aus Zeichen (z. B. Personal- oder Immatrikulationsnummer) weit verbreitet, um eine Referenz auf eine Person herzustellen.

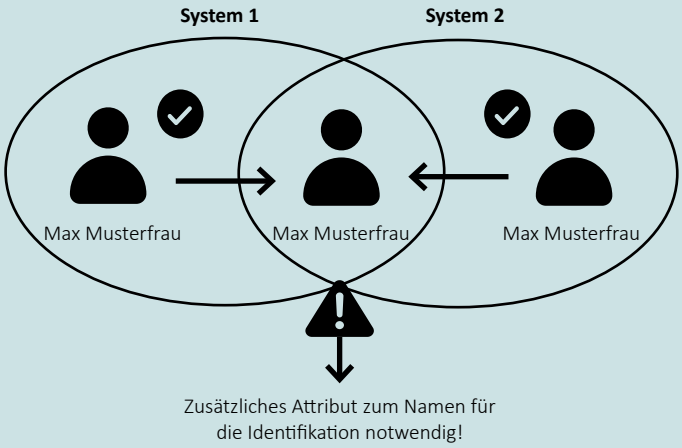

Abbildung 1: Eindeutige Identifikation

Referenz

Das Referenzieren einer Person — das Bestimmen einer Person unter allen Personen — ermöglicht Zuordnungen von Informationen, Zuständen oder Befugnissen dieser Person.

Rollen

Der Zugriff auf Informationen und Dienstleistungen sowie erteilte Befugnisse einer Person sind nicht nur abhängig von der Person, sondern ebenfalls von dem Kontext, in dem die Person agiert. Eine Person kann bspw. in der Rolle einer Projektleitung in einem Projekt und in einem anderen Projekt als mitarbeitend agieren Die Befugnisse sind entsprechend unterschiedlich. Eine Rolle beschreibt demnach einen Teilaspekt der Identität in einem bestimmten Kontext. Im Bildungsumfeld kann natürlich eine Person je nach Kontext Lehrende und gleichzeitig Lernende sein.

Identitätsprüfung

Der Nachweis der eigenen Identität muss üblicherweise erbracht werden, um Zugriff auf bestimmte Informationen (z. B. E-Mails) oder Dienstleistungen (z. B. Banküberweisungen) zu erhalten. Da eine Person über eine Referenz identifiziert wird, ist eine Verifizierung der Referenz auf die jeweilige Person nötig. Bei einem Identitätsdiebstahl wird beispielsweise die Referenz auf eine andere Person umgeleitet und ermöglicht somit Befugnisse, die eigentlich nicht für die umleitende Person bestimmt waren. Dies verdeutlicht die Relevanz der Prüfung von Identitäten und zieht folgende Aspekte nach sich:

Schutzziele

Eine Identitätsprüfung kann mehrere Fragestellungen verfolgen:

- **Existenz:** Es existiert eine natürliche Person, auf die alle angegebenen Attribute zutreffen.
- **Legitimität:** Die angegebenen Attribute gehören zu der sich identifizierenden Person.
- **Eindeutigkeit:** Keine zwei Personen verfügen über identische Attribute.

Prozess einer Prüfung:

Um den Zugang zu den angefragten Informationen oder Dienstleistungen zu erhalten, sollten in der Regel drei Schritte durchgeführt werden: Authentisierung, Authentifizierung und Autorisierung:

Authentisierung

Unter der **Authentisierung** versteht man die Vorlage eines Nachweises der verifiziert, dass die Person ist, wer sie angibt zu sein. In der Regel geschieht dies durch möglichst fälschungssichere Dokumente, wie dem Personalausweis.

Authentifizierung

Während der **Authentifizierung** wird die Authentizität des Nachweises geprüft. Im Falle des Personalausweises kann beispielsweise das Wasserzeichen geprüft werden und das Profilbild mit dem äußerlichen Erscheinungsbild der Inhaberin bzw. des Inhabers abgeglichen werden.

Autorisierung

Bei der **Autorisierung** wird der Inhaberin bzw. dem Inhaber des Identifikationsnachweises Zugriff auf die angefragten Informationen oder Dienstleistungen gewährt oder verweigert.

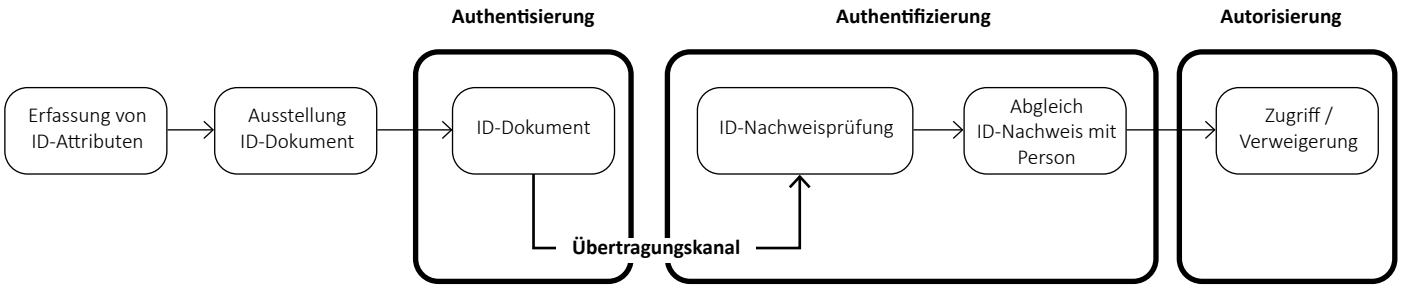

Abbildung 2: Prozess der Identitätsprüfung

Digitales Authentisieren und Authentifizieren

Die weitverbreitetste Art eine Identität im digitalen Raum zu verifizieren ist die Bereitstellung eines Nutzernamens und eines Passwortes. Der Nutzername ist öffentlich zugänglich, auf den andere Nutzer im Netzwerk Bezug nehmen können und somit über die Referenz „Nutzernamen" dieser Person Informationen zukommen lassen können. Das Passwort besteht aus einer Kombination von Zeichen, die nur der jeweiligen Person bekannt ist. Die Eingabe von beiden Bestandteilen ist in diesem Fall die Authentisierung. Die Prüfung durch das jeweilige System, ob die Kombination korrekt ist, beschreibt die Authentifizierung. Die Gewährung des angefragten Zugriffes durch das jeweilige System ist die Autorisierung.

Zwei-Faktor-Authentisierung

Das Verfahren mit Benutzernamen und Passwort ist in der Regel nur so sicher, wie die mögliche Geheimhaltung und die Komplexität des gewählten Passwortes. Sobald eine Person Kenntnis über das Passwort einer anderen Person erlangt, kann sie sich als diese Person ausgeben.
Eine zusätzliche Sicherheitsebene wird über die Zwei bzw. Mehr-Faktor-Authentisierung ermöglicht. Die beiden Faktoren des Identitätsnachweises müssen hierbei aus unterschiedlichen Kategorien stammen. Dabei wird unterteilt in Wissen (z. B. Passwort, PIN), Besitz (z. B. Smartphone, USB-Dongle) oder Biometrie (z. B. Fingerabdruck, Augenscan).

Rollenabhängige Autorisierung

In komplexen Systeme muss gewährleistet werden, dass nicht nur die Identität von Nutzenden verifiziert wird sondern auch die dem jeweiligen Nutzer bzw. der jeweiligen Nutzerin zugeordnete Rolle. Das Identitätsmanagement einer Software muss dementsprechend die Referenz zu einer Identität mit entsprechenden Kontextinformationen anreichern und autorisieren.

Sicherheitsbedrohungen & Vertrauensniveaus

Jeder Prozessschritt einer Identitätsprüfung (siehe Abb. 2) kann kompromittiert werden und unterliegt damit einem ständigen Bedrohungspotenzial. Folgende Aspekte sind in diesem Kontext zu beachten:

Bedrohungspotenzial im Identifikationsprozess

- **Erfassung von ID-Attributen** (Schreibfehler oder Zuordnungsfehler)
- **Ausstellung eines ID-Dokuments** (mangelnde Fälschungssicherheit oder Aktualität der ID-Attribute)
- **Übertragungskanal** (Übertragungsfehler oder Manipulation bei digitalen Kanälen)
- **Prüfung des ID-Nachweises** (Nutzung eines gestohlenen, gefälschten oder abgelaufenen Nachweises)
- **Abgleich des ID-Nachweises mit der natürlichen Person** (Imitation von biometrischen Charakteristika oder fremde Aneignung einer vertraulichen Information wie z. B. das Passwort)
- kompromittierte **Integrität des Prozesses** (unbefugtes Anlegen von Identitäten, Fälschen von Attributen oder mangelhafte Durchführung der Nachweisprüfung)

Klassifizierung von Bedrohungen

Plattform-Betreiber können die Bedrohungen für den Identifikationsprozess anhand folgender Faktoren besser einschätzen: die benötigte Zeit für einen erfolgreichen Angriff, das Expertenwissen über den Identifikationsprozess, das Insiderwissen über die jeweilige Branche, die Zugriffsgelegenheit und die benötigte Ausrüstung für den Angriff. Ein Angriff ist dann erfolgreich, wenn die Identitätsprüfung fälschlicherweise positiv ausfällt. Eine geeignete Maßnahme, um beispielsweise die benötigte Zeit für den Angriff zu maximieren und die Zugriffsgelegenheit zu minimieren ist der Einsatz einer Mehr-Faktor-Authentisierung, bei der ein sich laufend ändernder PIN benötigt wird. Eine ausführliche Liste der möglichen Bedrohungen für Identitäten und Gegenmaßnahmen ist der Technischen Richtlinie TR-03147 (Bundesamt für Sicherheit in der Informationstechnik 2021, S. 8–9) zu entnehmen.

Vertrauens- und Sicherheitsniveaus

Das Vertrauensniveau beschreibt die Wahrscheinlichkeit, mit der eine Identität fälschlicherweise positiv verifiziert wird. Je höher das Vertrauensniveau ist, desto niedriger ist die Wahrscheinlichkeit einer falsch-positiven Verifizierung.
Die Wahl eines Vertrauensniveaus basiert auf der Einschätzung der Schadensauswirkung einer falsch-positiven Verifizierung. Je sensibler der Zugriff auf bestimmte Informationen oder Dienstleistungen ist, desto höher sollte das Vertrauensniveau sein. Folgende Vertrauensniveaus werden in der Praxis verwendet:

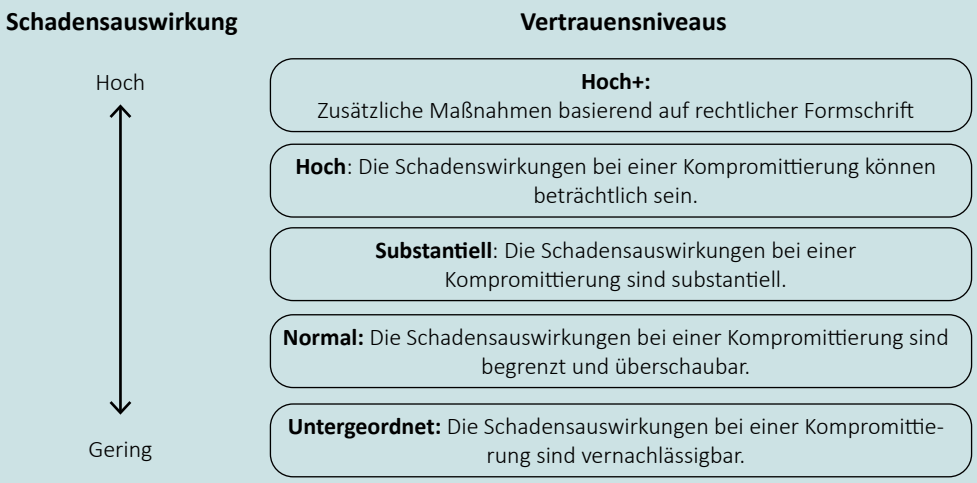

Abbildung 3: Vertrauensniveaus und Schadensauswirkung nach BSI (Technische Richtlinie TR-03107-1, Elektronische Identitäten und Vertrauensdienste im E-Government, 2019)

Beeinflussung des Vertrauensniveaus	Jeder identifizierten Bedrohung kann mit Anforderungen in verschiedenen Sicherheitsstufen begegnet werden. So ist zum Beispiel bei der Wahl des Authentisierungsprozesses die Ein-Faktor-Authentisierung (z. B. PIN) ausreichend für das Vertrauensniveau „Normal“, während die Vertrauensniveaus „Substantiell“ und „Hoch“ eine Zwei-Faktor-Authentisierung erfordern. So unterstützt das Nutzerkonto Bund / Bund ID drei verschiedene Vertrauensniveaus (Bundesministerium des Innern, für Bau und Heimat 2021), welches unterschiedliche OZG-Bildungsleistung ermöglichen soll.

Identitätsmanagement

Das Identitäts- und Zugriffsmanagement umfasst alle Technologien und Prozesse, welche die Verwaltung von Informationen zu digitalen Identitäten sowie die Kontrolle des Zugriffs auf digitale Ressourcen ermöglicht. Das Identitätsmanagement zielt dabei vor allem auf die Verwaltung der identitätsbezogenen Attribute. Das Zugriffsmanagement organsiert die Authentifizierung und die Autorisierung. Folgende Akteure und Konzepte der Umsetzung sind dabei zu beachten:

Identitätsanbieter	Ein Identitätsanbieter (englisch: Identity Provider) ist einen Dienst, welcher eine Person authentifiziert. Dafür werden verschlüsselte Informationen in einer Datenbank gespeichert, die nur der natürlichen Person bekannt oder für diese verfügbar sind (z. B. Passwort oder Fingerabdruck). Bei dem Zugriff auf eine Dienstleistung oder Information wird die Eingabe der Information gefordert und mit der Information in der Datenbank abgeglichen. Ein Identitätsdienst kann lokal verwaltet werden, oder über eine dritte Partei (siehe auch: Single Sign-On) bereitgestellt werden.
Dienstanbieter	Der Dienstanbieter (englisch: Service Provider) stellt eine Dienstleistung bereit, auf die der Nutzer oder die Nutzerin zugreifen möchte und für welche eine Autorisierung erfolgen soll.
Isolierte Identitäten	Das weitverbreitetste Modell eines Identitätsmanagements ist die isolierte Identität. Hierbei verwaltet ein Service Provider die Nutzenden seines Dienstes bzw. der Serviceplattform selbst. Der Service Provider führt ebenfalls die Identitätsprüfung durch. Dadurch entstehen bei den Service Providern „Inseln“ von Identitätsmerkmalen und Nutzende müssen für jeden Service Provider neue Nutzerkonten also Identitäten anlegen, pflegen und schützen.
Föderierte Identitäten	Eine Föderation ermöglicht es, verteilte Ressourcen gemeinsam zu nutzen, indem der Austausch von Identitätsinformationen über Plattform- bzw. Anbietergrenzen hinweg unterstützt wird. Bei föderierten Identitäten haben Nutzende mit einem Anmeldevorgang Zugriff auf mehrere Service Provider. Sie identifiziert sich bei einem Identitätsanbieter ihres Vertrauens und können dann basierend auf dieser Authentifizierung auf Ressourcen unterschiedlicher Service Provider zugreifen. Die digitale Identität wird bei einem zentralen Identity Provider hinterlegt, dem die verschiedenen Service Provider in der Föderation vertrauen. Der Personalausweis mit eID fällt ebenfalls unter die Kategorie der föderierten Identität und wird als staatliche Authentifizierungsmethode angeboten. Eine systemübergreifende Nutzung und zentrale Verwaltung birgt die Gefahr des Kontrollentzugs über die eigene Identität und der Abhängigkeit vom Identity Provider (siehe hierzu auch selbstsouveräne Identität). Eine zentrale Verwaltung von

Identitätsdaten kann grundsätzliche datensparsam und damit datenschutzfreundlich sein, denn die Übertragung von personenbezogenen Daten an die Serviceprovider wird obsolet bzw. nur sehr eingeschränkt nötig. Diese Art der Zentralisierung von Identitätsinformationen bei meist gewinnorientierten Unternehmen führt oft zur Sammlung von persönlichen Nutzungs- und Profildaten, und deren Korrelationen, welche dann potentiell an Dritte zur Profitmaximierung weitergegeben werden könnten. Daher ist die Prüfung bzw. Auswahl des jeweiligen Identity Providers mit großer Sorgfalt und der Abwägung von Schutz- und Komfortinteressen vorzunehmen. Bei föderierten Identitäten müssen die Identitätsdaten der Nutzenden nur an einer Stelle in der Föderation gespeichert und gepflegt werden. Der Föderationsverbund ermöglicht seinen Nutzenden damit ein Single Sign-On.

Single Sign-On (SSO)

Mit einem Single Sign-On (deutsch: Einmalanmeldung) ist die Nutzung mehrerer digitaler Dienste mit nur einem Anmeldevorgang möglich. Es ist ein Authentifizierungsverfahren, welches Nutzenden die Möglichkeit gibt, sich mit einer einzigen ID bei mehreren Diensten gleichzeitig zu autorisieren. Parallel dazu ermöglicht das Single Sign-Off mit einer einzigen Abmeldung den Zugriff auf alle beteiligten Dienste zu beenden. Zu den Vorteilen zählen eine verbesserte Benutzerfreundlichkeit und partiell mehr Sicherheit in Bezug auf Übertragungskanäle, da Passwörter nur einmal übertragen werden. Nutzende werden bestärkt darin, komplexere (starke) Passwörter zu wählen, da sie sich nur noch ein Passwort für den Zugriff auf mehrere Dienste merken müssen.
Nachteilig beim SSO ist der potentiell missbräuchliche Gebrauch der eigenen Anmeldeinformationen durch Dritte, da hiervon dann alle genutzten Dienste betroffen sind. Deshalb sollten beim SSO besonders sichere Authentifizierungsmethoden zum Einsatz kommen. Die Verfügbarkeit ist ebenfalls ein kritischer Faktor, da bei Ausfall bzw. Kompromittierung des Single Sign-On Systems[1] alle unter dem System vereinheitlichten Dienste nicht mehr nutzbar sind.
Folgende Standards und Protokolle zur Identifikation im digitalen Raum sind in der Praxis verbreitet:

SSO-Kommunikationswege

Bei der IdP initiierten Authentifizierung (Abbildung 4, links) authentifiziert sich der Nutzende in Schritt 1 beim Identitätsprovider und kann dann in Schritt 2 auf geschützte Ressourcen beim Service Provider (SP) zugreifen. Bei der SP initiierten Authentifizierung (Abbildung 4, rechts) greift der Nutzende in Schritt 1 auf eine geschützte Ressource zu, wird dann in Schritt 2 zum Identitätsprovider weitergeleitet und kann nach erfolgreicher Authentifizierung in Schritt 3 auf die Ressourcen beim Service Provider zugreifen.

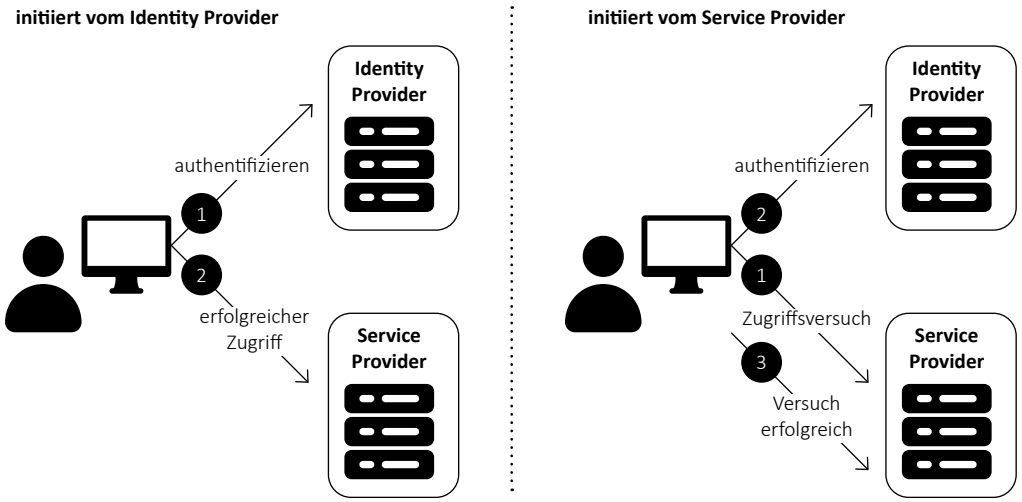

Abbildung 4: Initiierung eines Single Sign-On beim Zugriff auf einen geschützten Dienst, basierend auf OASIS®, 27.

[1] Ein aktuelles Beispiel findet sich unter: tinyurl.com/mr3yt8vw

SAML

Die Security Assertion Markup Language (SAML) ist ein offener Standard (aktuelle Version 2.0, März 2005) zum Austausch von Authentifizierungs- und Autorisierungsdaten zwischen Identitätsanbietern und Dienstanbietern. Der Standard ermöglicht die Integration zwischen Dienstanbietern auf der Ebene des Identitätsmanagements und legt Kommunikationsart und Formate für den Identitätsaustausch fest. Die durch SAML zur Verfügung gestellten Funktionen für den Austausch von Identitätsdaten ermöglichen eine Single Sign-On Authentifizierung. Dabei haben die Nutzenden nach einer einmaligen Authentifizierung ggf. für eine bestimmte Zeit föderationsweit Zugriff auf geschützte Ressourcen wie z. B. verschiedene Webanwendungen. Die mit SAML zwischen Identitätsanbieter und Dienstanbieter ausgetauschten Informationen werden Zusicherungen (englisch: assertions) genannt und machen Aussagen über die erfolgreiche Authentifizierung einer Person, über bestimmte Merkmale einer Person (z. B. jeweilige Rolle) sowie über Autorisierungsentscheidungen.

OAuth2 zur API Integration von Plattformen

Miteinander vernetzte (Weiterbildungs-)Plattformen profitieren von der Integration von Dienstleistungen verschiedener Anbieter. Der Zugriff auf die Funktionalitäten von Drittanbietern erfolgt hierbei oft über Anwendungsprogrammierschnittstellen (API). OAuth2 ist ein Standard und Framework zur Absicherung des Zugriffs auf Funktionalitäten von Drittanbietern über APIs. OAuth2 stellt Anwendungen eine delegierte Autorisierung beim Zugriff auf geschützte Ressourcen innerhalb einer anderen Anwendung zu Verfügung. Durch Verwendung von OAuth2 müssen Anwendungen den Authentisierungsdienst nicht selbst implementieren. Aktualisierungen und Sicherheitsupdates der Authentisierungssoftware werden vom Anbieter des Identitätsmanagements durchgeführt. Nutzende gewähren mit der Nutzung von OAuth2 Drittanwendungen nur Zugriff auf bestimmte Daten (z. B. Kompetenzprofile, Lernpräferenzen oder Bildungszertifikate) ohne die eigenen Anmeldeinformationen preisgeben zu müssen. Diese Berechtigung zum Zugriff durch autorisierte Drittanwendungen kann jederzeit durch die Nutzenden wieder entzogen werden.
Eine Autorisierung mit OAuth2 verläuft in mehreren Schritten. Zuerst wird von der (Dritt-)Anwendung eine Autorisierung von Nutzenden eingeholt. Dazu wird eine Anfrage an den jeweiligen Autorisierungsserver gesendet, dieser holt den betroffenen Nutzenden eine Autorisierungsbestätigung ein (ggf. mit einer Aufforderung zur Eingabe von Anmeldeinformationen) und sendet einen Autorisierungscode, einen Zugriffstoken und eine Ablaufzeit an die (Dritt-)Anwendung zurück. Die Anwendung kann nun innerhalb der eingeräumten Zeitspanne auf die Daten der Nutzenden im vereinbarten Umfang zugreifen.

OpenID Connect

OpenID Connect ist ein weit verbreiteter Standard für den Nachweis der Identität von Nutzenden unter Verwendung eines Autorisierungsservers. Der Standard baut auf OAuth2 auf und fügt diesem eine Authentifizierungsschicht hinzu. Eine Anwendung kann mit OpenID Connect unter Nutzung einfacher JSON basierter Identitätstoken Informationen über authentifizierte Anwenderinnen und Anwender anfordern und erhalten. Das Identitätstoken ist mit einem Personalausweis vergleichbar und digital signiert. Es bestätigt die Identität der Nutzenden, gibt den oder die ausstellende Instanz an und informiert, wann Nutzende authentifiziert wurden. Das Identitätstoken beinhaltet eine Ablaufzeit bzgl. seiner Gültigkeit und kann aus Vertraulichkeitsgründen verschlüsselt werden.

Selbstsouveräne Identität

Der Nachweis der eigenen Identität bei digitalen Diensten ist mit Herausforderungen verbunden, die für physische Identitätsdokumente wie Reisepass, Führerschein oder anderen Ausweisdokumenten nicht existieren. Papiergebundene Dokumente wie z. B. der Personalausweis sind standardisiert, weitgehend fälschungssicher, vor dem Zugriff Dritter geschützt und können ohne Probleme Dritten, die dem Herausgeber der Ausweise vertrauen, zur Anerkennung von Identitätsmerkmalen vorgelegt werden (Strüker 2021). Digitale Identitäten müssen für eine breite Akzeptanz bei Nutzenden diese Merkmale in die digitale Welt transformieren. Selbstsouveräne Identitäten (SSI) spielen hierbei eine zunehmend wichtige aber auch kontroverse Rolle. Sie können eine dezentrale Identitätserzeugung und –verwaltung ermöglichen, die bei sicherer Implementierung (Einsatz sicherer Technologien) den gestiegenen Anforderungen an Interoperabilität, Transparenz und Datenschutz gerecht wird. Für Nutzende, die ihre vielfältigen Identitätsdaten für bspw. E-Mail-Konten, Online-Shops oder Online-Banking vereinheitlichen möchten, ohne dabei auf einen zentralen, womöglich wirtschaftlich eigennützigen Identitätsprovider angewiesen zu sein, können selbstsouveräne Identitäten sinnvoll sein. Souveränität im Umgang mit Daten kann für die Nutzenden dabei natürlich auch partiell umgesetzt werden, beispielsweise mit der souveränen Ablage von Daten in Kombination mit einer föderierten Identität. Durch ein stärkeres Maß an Selbstbestimmung können hier deutliche Vorteile generiert werden.

Definition selbstsouveräne Identität	Eine selbstsouveräne Identität beschreibt im digitalen Kontext die selbstbestimmte Verwaltung aller Attribute einer natürlichen Person durch diese Person. Sie ist selbstsouverän in dem Sinne, dass die Erzeugung und Kontrolle der digitalen Identitäten ohne eine vermittelnde Instanz oder zentrale Partei auskommt. Dieser Ansatz des Identitätsmanagements steht in seiner absoluten Ausprägung im Gegensatz zu der aktuellen Vorgehensweise, in der die Informationen über die eigene Identität von einem externen Identity Provider erhoben, gespeichert und verwaltet werden.
Portabilität & Interoperabilität	Die meisten Software-Angebote sind heutzutage darauf ausgelegt, den Nutzer oder die Nutzerin an die jeweilige Plattform zu binden. Eine Übertragung der Daten zu einem anderen Dienstleister ist nur möglich, wenn die Dienstleister eine entsprechende Export- und Importfunktion bereitstellen. Die Nutzenden sind abhängig von der Kooperationsbereitschaft der Dienstleister. Beispielsweise ist eine einfache Übertragung von Lernprofilen und Zertifikaten von LinkedIn auf ein anderes Lernsystem nur möglich, wenn beide Dienstleister die entsprechende Funktionalität bereitstellen. Die selbstsouveräne Identität kann die Lernprofile und Zertifikate in der eigenen Ablage speichern und diese zu einem anderen Anbieter übertragen. Die Voraussetzung für die Portabilität der Daten ist die anbieterübergreifende Unterstützung des Datenformates.
Akteure	In einem SSI-System sind verschiedene Rollen für die Interaktion zwischen den Beteiligten (Akteure) festgelegt: der Herausgeber, die Inhabenden und die Akzeptanzstelle.
Herausgeber	Der Herausgeber erstellt die Identitätsnachweise für die Inhabenden und bestätigt deren Korrektheit. Dies kann eine Geburtsurkunde, ein Personalausweis oder ein digital verifizierbarer Nachweis sein. Herausgeber können öffentliche Einrichtungen wie z. B. Hochschulen sein, die Attribute des Identitätsinhabenden (z. B. ein Hochschulzeugnis) bestätigen, signieren und dem Inhabenden (englisch: Holdern) zur Verfügung stellen.
Inhabende	Die Inhabenden können Personen oder Organisationen sein, speichern den erhaltenen Nachweis in einem privaten Ablageort und präsentieren ihn der Akzeptanzstelle, um Zugriff auf den bereitgestellten Dienst zu erhalten.

Akzeptanzstelle

Die Akzeptanzstelle stellt einen Dienst bereit, auf den der oder die Inhabende zugreifen möchte. Um den Zugriff zu autorisieren, benötigt die Akzeptanzstelle den Identitätsnachweis des oder der Inhabenden. Die Identitätsprüfung ist nur möglich, wenn die Akzeptanzstelle der Gültigkeit des Identitätsnachweises des Herausgebers vertraut. Dabei ist keine aktive Verbindung zwischen Akzeptanzstelle und Herausgeber notwendig, da durch die kryptographisch gesicherte Signatur überprüft werden kann, ob das präsentierte Zertifikat (verifizierbare Präsentation) echt ist.

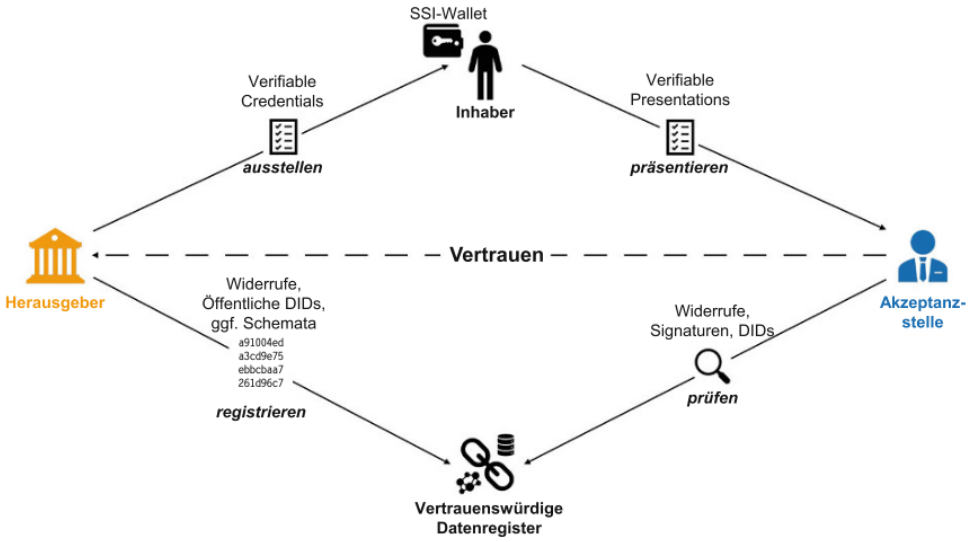

Abbildung 5: SSI-Interaktionsschema, übernommen von (Ehrlich et al. 2021).

Wallet
(deutsch: Brieftasche)

Im Paradigma der selbstsouveränen Identität verfügt jede Nutzerin und jeder Nutzer über eine Ablage/Brieftasche, in der Informationen der jeweiligen Person abgelegt werden. Die Dienstleister können erst nach einer Freigabe der Daten durch Nutzende auf diese zugreifen. Die Ablage kann ebenfalls die Identitätsnachweise der Nutzenden enthalten.

Verifizierbarer Nachweis

Ein verifizierbarer Nachweis (englisch: verifiable credential - VC) ist ein digitales Dokument, das eine oder mehrere Aussagen über ein Subjekt beinhaltet. Jede Aussage kann mit weiteren Metadaten angereichert werden, wie zum Beispiel die Herausgeberin, den Datentyp oder das Erstellungsdatum. Zusätzlich beinhaltet der VC einen Beweis, dass die Aussage korrekt ist und von der Herausgeberin ausgestellt wurde. Die Behauptung wird üblicherweise über ein digitales Signaturverfahren verifiziert.

Verifizierbare Präsentation

Die verifizierbare Präsentation enthält einen oder mehrere VCs, Metadaten und einen Beweis für die Urheberschaft der Daten. Somit können mehrere Nachweise für verschiedene Kontexte zusammengestellt werden. Ebenfalls kann mit der Präsentation nur die zur Authentisierung notwendigen Informationen des Nachweises präsentiert werden.

Zero-Knowledge Proof

Bei einem zero-knowledge proof wird die Korrektheit einer Aussage (z. B. in einem überprüfbaren Zertifikat) bewiesen, ohne den Inhalt der Aussage selbst preiszugeben. Dieses Verfahren wird z. B. beim „Secure Remote Password“-Protokoll angewandt, bei dem die Nutzenden ihr Passwort nicht zu einer Plattform übertragen müssen, um dessen Besitz nachzuweisen. Mit dieser Methode kann die natürliche Person die Hoheit über die eigenen personenbezogenen Aussagen bewahren.

Dezentrale Identifikatoren (DID)	Dezentrale Identifikatoren (englisch: decentralised Identifier) ermöglichen eine Identifikation von digitalen Objekten (wie bspw. Personen, Organisationen, Dingen oder Datenmodellen). Sie wurden als Standard zur Gestaltung von interoperablen SSI-Systemen etabliert. Dadurch können nicht nur Personen und Organisationen, sondern beliebige Informationen referenziert werden. Datenregister sind für das Speichern von DID zuständig.
Datenregister	Das Datenregister ist ein unveränderbarer Speicher, der Informationen über die öffentlichen DIDs und Verifizierungsmechanismen zur Überprüfung der überprüfbaren Zertifikate (VC) enthält. Eine Distributed-Ledger-Technologie (z. B. Blockchain) ist nicht zwingend notwendig, um diesen unveränderbaren Speicher bereitzustellen.

Literaturverzeichnis

Bundesamt für Sicherheit in der Informationstechnik (2021): Technische Richtlinie TR-03147. Vertrauensniveaubewertung von Verfahren zur Identitätsprüfung natürlicher Personen.

Bundesministerium des Innern, für Bau und Heimat (2021): Das Nutzerkonto Bund. Verwaltungen von Bund, Ländern und Kommunen.

Ehrlich, Tobias; Richter, Daniel; Meisel, Michael; Anke, Jürgen (2021): Self-Sovereign Identity als Grundlage für universell einsetzbare digitale Identitäten. In: HMD 58 (2), S. 247–270. DOI: 10.1365/s40702-021-00711-5.

OASIS (2008, 25. März): Security Assertion Markup Language (SAML) V2.0 Technical Overview. Committee Draft 02. Abrufbar unter: http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0-cd-02.pdf

Strüker, J., Urbach, N., Guggenberger, T., Lautenschlager, J., Ruhland, N., Schlatt, V., Sedlmeir, J., Stoetzer, J.-C., Völter, F. (2021): Self-Sovereign Identity – Grundlagen, Anwendungen und Potenziale portabler digitaler Identitäten. Projektgruppe Wirtschaftsinformatik des Fraunhofer-Instituts für Angewandte Informationstechnik FIT, Bayreuth.

Bildnachweis

Wenn nicht anders angegeben, liegen die Bildrechte bei den Autor:innen.