Whitepaper der ZKI AG edu-ID zur Verortung des Konzepts einer edu-ID in der aktuellen Landschaft digitaler Identitäten in Deutschland und Europa

Beitragende

Guido Bacharach (freier Autor), Peter Gietz (DAASI International GmbH), Gerrit Gragert (Staatsbibliothek zu Berlin), Aylin Gündogan (RWTH Aachen), Marcus Hardt (KIT), Thorsten Michels (TU Kaiserslautern), Bernd Oberknapp (Uni Freiburg), Wolfgang Pempe (DFN-Verein), Ramon Pfeiffer (Uni Tübingen), Michel Smidt (FWU), Erwin Soldo (DAAD)

Inhaltsverzeichnis

1. Zielsetzung 1
2. Darstellung des Konzepts einer edu-ID 2
3. Das Umfeld 5
  3.1 Digitale Identitäten in europäischen Inititativen und Projekten 5
    3.1.1 European Student Identifier, ESI (a.k.a. MyAcademicID) 5
    3.1.2 EMREX 6
  3.2 ORCID - Open Researcher and Contributor ID 7
  3.3 AAI-Landesprojekte 8
  3.4 Forschungscommunities und -Infrastrukturen 9
    3.4.1 Beispiel Helmholtz AAI 10
    3.4.2 Beispiel DARIAH AAI 11
  3.5 Online Zugangsgesetz (OZG): Nutzerkonto Bund/Land 12
  3.6 Nationale Bildungsplattform 14
  3.7 Identitäten im schulischen Bereich am Beispiel von VIDIS 15
  3.8 Internationaler Kontext 15
4. Schlussfolgerungen 16

1. Zielsetzung

Ziel dieses Dokuments ist die Einordnung des im nächsten Abschnitt skizzierten edu-ID-Konzepts gegenüber anderen Initiativen, Projekten und den jeweiligen Konzepten digitaler

Identitäten. Hierbei geht es jedoch nicht alleine um die Abgrenzung gegenüber solchen Konzepten, sondern auch um die Identifizierung von Anknüpfungspunkten und möglichen Synergien. Ausgehend von dieser Positionierung werden in einem weiteren Schritt Empfehlungen zu Funktionsumfang, Reichweite und Zielgruppen eines zukünftigen auf dem edu-ID Konzept basierenden Dienstes erarbeitet. Weiterhin werden Überlegungen zum weiteren Vorgehen bei der Entwicklung des Dienstes angestellt.

2. Darstellung des Konzepts einer edu-ID

Im AAI- und Föderationskontext ist es üblicherweise die jeweilige Heimateinrichtung, die für ihre Angehörigen eine digitale Identität zur Verfügung stellt und diese verwaltet. Für gewöhnlich erhält die Person dabei einen Accountnamen und ein dazugehöriges Passwort. Mit diesen Benutzer-Credentials kann sich die Person über einen Login am Authentifizierungsdienst ihrer Heimateinrichtung (Identity-Provider) bei internen und externen Diensten anmelden und – entsprechende Berechtigungen vorausgesetzt – diese auch nutzen. Die hierfür erforderliche Infrastruktur, AAI (= Authentication and Authorization Infrastructure), wird traditionell im Rahmen nationaler Föderationen realisiert und in der Regel von den jeweiligen Forschungsnetzen betrieben. Im Fall der Bundesrepublik Deutschland ist dies der DFN-Verein, der die DFN-AAI[1] betreibt und über die Teilnahme am Interföderations-Dienst eduGAIN[2] auch die föderationsübergreifende Nutzung von AAI-Diensten ermöglicht.

Ändert sich nun im Laufe der akademischen Vita die Affiliation, das heißt die Zugehörigkeit zu einer Einrichtung, wird die bisherige digitale Identität durch eine neue ersetzt. Mit der bisherigen Identität erlöschen somit alle damit verbunden Berechtigungen, Rollen und Verknüpfungen zu anderen Identitäten. In manchen Fällen genügt hierfür bereits der Übergang vom Studierenden- in den Mitarbeitenden-Status innerhalb derselben Einrichtung. Eine Unterbrechung oder das Ende eines akademischen Lebenslaufs führt in dieser Hinsicht zu einem Identitätsverlust. Viele der an eine digitale Identität geknüpften Berechtigungen beziehen sich in aller Regel auf den Zugriff auf hochschul- beziehungsweise einrichtungsinterne Ressourcen und Dienste. Es existieren jedoch Szenarien, in denen ein unterbrechungsfreier Zugriff auf bestimmte Inhalte und Dienste auch nach dem Ausscheiden aus einer bestimmten Einrichtung möglich oder sogar unabhängig von einer bestimmten Affiliation sein sollte. Als Beispiele hierfür seien der langfristige Zugriff auf Leistungsnachweise, Speicherdienste oder Inhalte, die über Nationallizenzen verfügbar sind, genannt. Der unterbrechungsfreie und langfristige Zugriff auf Ressourcen wird auch im Rahmen der Nationalen Forschungsdateninfrastruktur (NFDI) eine wichtige Rolle spielen.

[1] https://doku.tid.dfn.de/de:aai:about
[2] https://edugain.org

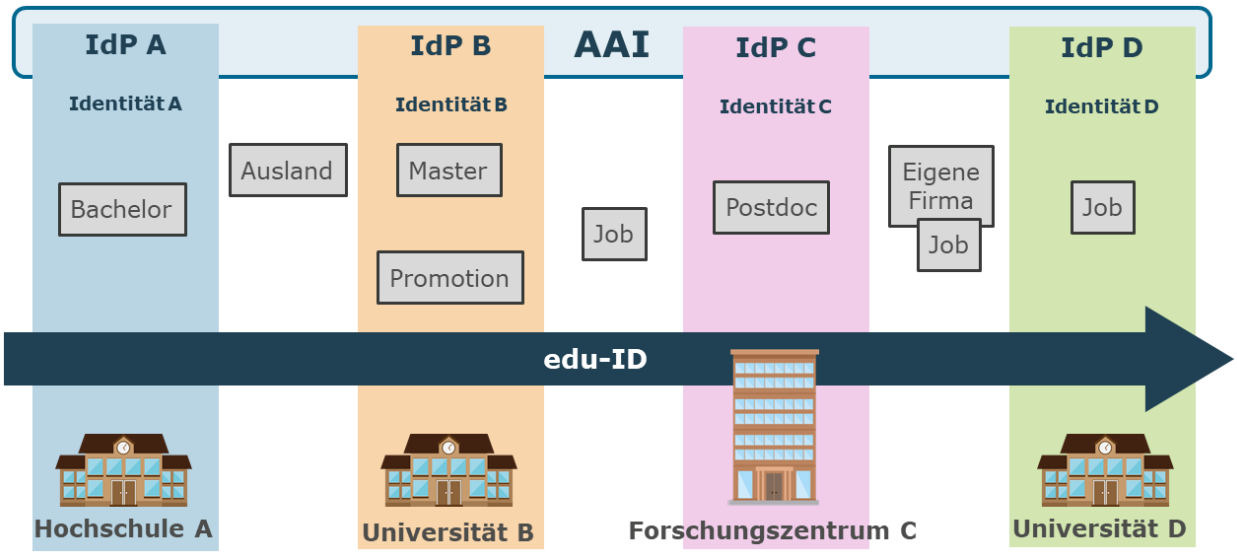

Abb. 1: Die edu-ID als lebensbegleitende digitale Identität

Ein weiterer Punkt, der eine ausschließlich von der Heimateinrichtung verwaltete Identität im AAI-Kontext problematisch macht, ist die Freigabe von Attributen, die zur Nutzung bestimmter Dienste vor allem im Bereich E-Research erforderlich sind. In diesem Modell ist die Nutzerin beziehungsweise der Nutzer von der Attributfreigabe seitens der für den Betrieb des Identity-Providers (IdP) zuständigen Stelle abhängig. Dies führt nicht selten zu kommunikationsbedingten Verzögerungen beim Zugriff auf bestimmte, für die Forschungsarbeit relevante Ressourcen. Im schlimmsten Fall muss die Nutzerin bzw. der Nutzer auf einen Login mit dem privaten Google- oder Facebook-Account ausweichen[3].

Insbesondere um den eben skizzierten Problemen zu begegnen, beschäftigt sich seit März 2019 die ZKI Arbeitsgruppe edu-ID damit, analog zur SWITCH edu-ID ein Konzept für eine nutzerzentrierte, lebenslang gültige digitale Identität für den Bereich der Hochschulen und die öffentlich geförderte und gemeinnützige Forschung in Deutschland zu entwickeln. Hierbei wurde eine Reihe von generischen Nutzungsszenarien identifiziert:

- Unterbrechungsfreie Nutzung von Diensten bzw. Zugriff auf Ressourcen, deren Nutzungsberechtigung nicht an die aktuelle Zugehörigkeit zu einer bestimmten Einrichtung geknüpft ist (Speicherdienste, Nationallizenzen, Leistungsnachweise, …)
- Erleichterung des Managements virtueller Organisationen durch Forschungsprojekte und –Infrastrukturen (User Mobility, Rechte, Rollen, Gruppenmitgliedschaften)
- Community-unabhängige Identifizierung von Nutzenden, die an mehreren ggf. internationalen Community-AAIs teilnehmen, die gemäß der AARC Blueprint Architecture[4] gestaltet sind.
- Identity-Provider für Nutzende ohne Heimat-IdP
- Vereinheitlichung und Vereinfachung der Verfahren bei Onboarding-Prozessen, da eine verlässliche digitale Identität bereits vorhanden ist. Hierzu gehört auch die Dublettenvermeidung, d.h. die Unterstützung beim Aufspüren von mehrfach registrierten Nutzerinnen und Nutzern
- Zusammenführung / Verlinkung verschiedener Identitäten bzw. Accounts und den zugehörigen Nutzendendaten (Attribute)

[3] Zu dieser Problematik siehe DFN-Mitteilungen Nr. 96, S. 13-19.
[4] https://aarc-community.org/architecture/

Hierbei gelten hohe Anforderungen an die Verlässlichkeit und Aktualität der Nutzendendaten sowie die Sicherheit der Anmeldung am edu-ID-System. So ist u.a. vorgesehen, dass das edu-ID-System bei einem Anmeldevorgang die Daten der/des betreffenden Nutzenden in Echtzeit vom Identity-Provider der jeweiligen Heimateinrichtung (sofern vorhanden) abfragt. Der Heimat-IdP ist auch die Stelle, an der der/die Nutzer:in sich authentifiziert. Das edu-ID-System agiert in diesem Kontext als Proxy, d.h. es agiert in der DFN-AAI sowohl als Identity- als auch als Service-Provider. Siehe hierzu das technische Konzept[5] und die nachfolgende Abbildung.

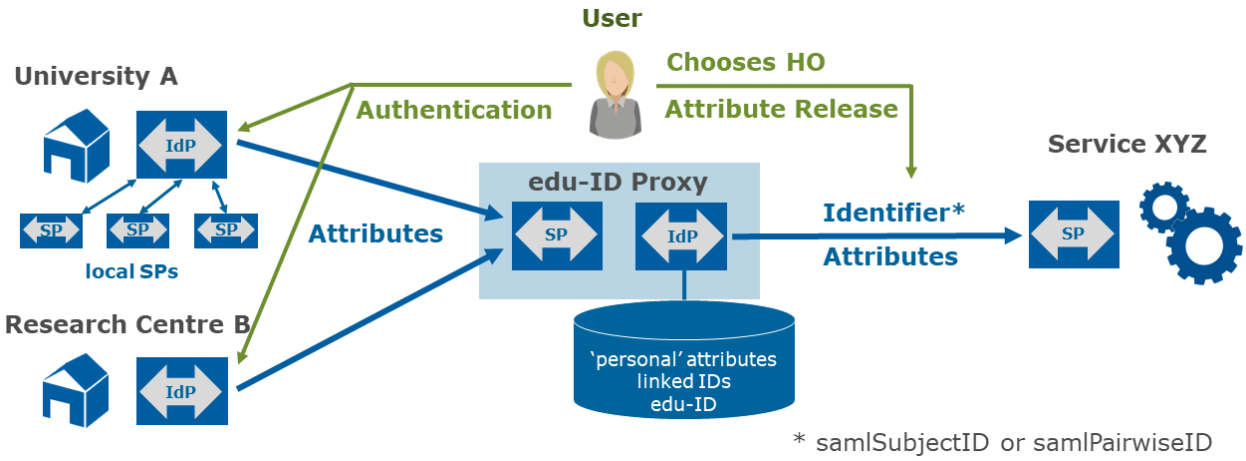

Abb. 2: Das edu-ID-System als Proxy

Das technische Konzept sieht eine nahtlose Integration des edu-ID-Systems in die DFN-AAI vor, an der die überwiegende Mehrzahl der deutschen Hochschulen und Forschungseinrichtungen teilnimmt. Der Schwerpunkt des edu-ID Konzepts liegt zunächst allgemein auf der Authentifizierung und Autorisierung auf Basis von SAML2. Die Unterstützung weiterer Standards, Protokolle und Infrastrukturen ist insbesondere hinsichtlich OpenID Connect geplant. Zudem kann das edu-ID-System zentral für alle angeschlossenen Institutionen zusätzliche Funktionalitäten bereitstellen, zum Beispiel eine 2-Faktor-Authentifizierung.

Perspektivisch soll die edu-ID auch den Übergang zwischen Bildungsinstitutionen und zwischen Bildungssektoren vereinfachen. Eine vollständige Liste der im Rahmen der Konzepterstellung betrachteten Use Cases und der daraus abgeleiteten Anforderungen an eine zukünftige Implementierung findet sich unter https://doku.tid.dfn.de/de:aai:eduid:usecases.

Auf organisatorischer Ebene sind begleitend zur technischen Implementierung neben einem Betriebs- und Supportkonzept auch geeignete Governance-Strukturen zu entwickeln. Diese Aspekte sind aber nicht Gegenstand dieses Papiers.

[5] Technisches Konzept edu-ID https://doi.org/10.5281/zenodo.7418055

3. Das Umfeld

3.1 Digitale Identitäten in europäischen Inititativen und Projekten

3.1.1 European Student Identifier, ESI (a.k.a. MyAcademicID)

Beschreibung

Das Konzept eines European Student Identifiers (ESI) wurde im Rahmen des Projekts MyAcademicID als verbindendes Element für die Nutzung der Komponenten der Erasmus+ Plattform entwickelt. Die Förderung erfolgte durch die Connecting Europe Facility (CEF) der EU. Im Rahmen von CEF wurden digitale Lösungen und Infrastrukturen geschaffen, die als sogenannte „Building Blocks" für einen einheitlichen digitalen Europäischen Binnenmarkt dienen sollen, darunter eID, eArchiving, eSignature und andere mehr. Ein bestimmender Faktor hierbei war die eIDAS-Verordnung[6]. Die Implementierung und der Ausbau der Erasmus+ Plattform erfolgten und erfolgen im Rahmen des ebenfalls von der CEF geförderten Folgeprojekte EDSSI[7] (European Digital Student Service Infrastructure) und EDSSI2. Hiermit wurde eine Onlineplattform für das Studierendenaustauschprogramm Erasmus+ geschaffen, die im Rahmen von EDSSI2 ausgebaut und um weitere Komponenten erweitert wird. Ziel ist es, alle mit dem Austauschprogramm verbundenen Prozesse zu digitalisieren und die Erasmus+ Plattform mit weiteren Komponenten wie der European Student Card Plattform zu einer gemeinsamen Infrastruktur zu verbinden.

Da der Zugang zur Erasmus+ Plattform primär über eduGAIN und somit über SAML-basierten Login am Identity-Provider der jeweiligen Heimateinrichtung erfolgt, wird der ESI als SAML-Attribut übertragen. Hierbei handelt es sich um das Attribut schacPersonalUniqueCode, dessen Wert für den ESI nach folgendem Schema[8] gebildet wird:

`urn:schac:personalUniqueCode:int:esi:<org>:<code>`

Wobei `<org>` die für das Erasmus-Programm zuständige Heimateinrichtung der/des jeweiligen Studierenden und `<code>` für eine relativ zu `<org>` eindeutige Nutzendenkennung der betreffenden Person darstellt. In Deutschland sind dies die jeweilige Hochschule und in aller Regel die Matrikelnummer des/der am Erasmus-Programm teilnehmenden Studierenden.

Bewertung

Im Gegensatz zum edu-ID-Konzept handelt es sich beim ESI um einen lokalen, also plattform-spezifischen Identifier, der im Zweifelsfall nur für die Dauer der Teilnahme am Erasmus-Programm Bestand hat. Der ESI ist insofern weder für die Gesamtheit der Studierenden von Belang noch taugt er als lebensbegleitender Identifier, da die `<code>` Komponenten von der jeweiligen Heimateinrichtung vergeben wird und gepflegt werden muss.

---

[6] https://eur-lex.europa.eu/legal-content/de/TXT/?uri=CELEX:32014R0910

[7] https://edssi.eu

[8] Siehe Dokumentation unter https://wiki.geant.org/display/SM/European+Student+Identifier

Allerdings wäre der ESI ebenso wie ORCID (s.u.) ein Attribut, das im edu-ID-System mit dem jeweiligen Account verknüpft bzw. hinterlegt werden könnte – sofern sich entsprechende Anwendungsfälle ergeben. Denkbar wäre weiterhin, den ESI für Studierende in Deutschland zentral über das edu-ID-System zu vergeben, so dass die `<org>` Komponente durch eine Kennung für das edu-ID-System zu belegen wäre und `<code>` durch einen von der edu-ID abgeleiteten Hashwert. Allerdings ist fraglich, ob dies politisch gewollt und organisatorisch machbar wäre.

3.1.2 EMREX

Beschreibung

EMREX[9] ist eine Lösung für den internationalen Transfer von Studierendendaten in maschinenlesbarer Form. Sie besteht aus zwei Teilen: der technischen Lösung und dem internationalen Netzwerk (EMREX-Nutzergruppe - EUG), das die Aktivitäten ermöglicht und entwickelt. Es entstand als EU-finanziertes Projekt 2015-2017 mit dem Ziel, den Anrechnungsprozess nach einem Studierendenaustausch zu vereinfachen und qualitativ zu verbessern. Das EMREX-Dienstleistungsnetzwerk wurde bereits vor dem erfolgreichen Abschluss des Projekts in Betrieb genommen und ist seitdem in Betrieb. Es ist eines der wenigen EU-Projekte, die sich selbst erhalten und nach dem offiziellen Abschluss des Projekts weiter wachsen können. EMREX ist nicht auf die EU beschränkt, d.h. es kann weltweit genutzt werden. Gegenwärtig ist EMREX in einer Reihe von Ländern in Europa in Betrieb, u.a. in den Niederlanden, Norwegen, Finnland und Polen. Es handelt sich um eine technische Lösung für den sicheren Austausch von Bildungsdaten zwischen Studierenden und Dritten, z. B. Hochschuleinrichtungen oder potenziellen Arbeitgebern. Auf diese Weise kann EMREX die Mobilität von Studierenden erleichtern und den Verwaltungsaufwand für die Einrichtungen beim Austausch von Studierenden verringern. EMREX verwendet eine quelloffene technische Lösung, über die verschiedene Arten von Bildungsdaten übertragen werden können, seien es Leistungsnachweise oder ganze Diplome. Diese Daten werden gemäß des ELMO-Standards in XML strukturiert[10].

Eines der wichtigsten Merkmale von EMREX ist die Qualität und Zuverlässigkeit der Daten. Um dies zu gewährleisten, ist es wichtig, dass die Datenübermittlung auf sichere Weise erfolgt. Zur Sicherung des EMREX-Datentransfers müssen mehrere Schritte beachtet werden:

- Doppelte Anmeldung: Der/die Studierende muss sich sowohl im EMREX-Client (EMC) als auch in der EMREX-Serverfunktionalität (EMREX Contact Point - EMP) mit einem sicheren Login anmelden.
- Digitales Signieren der ELMO-Daten: EMREX wird Signaturen für die ELMO-Daten verwenden, um sicherzustellen, dass der EMP gültig ist. Die öffentlichen Schlüssel werden im Register des Erasmus-Without-Paper (EWP), das gleichzeitig als EMREX-Register verwendet wird, gespeichert.
- Verifizierung der Studierenden: Da sich Studierende auf beiden Seiten des Transfers anmelden müssen, ist eine Überprüfung möglich, ob es sich tatsächlich um dieselbe Person handelt. Dies geschieht anhand des Geschlechts, des Geburtsdatums und des Namens. Da Namen in verschiedenen Ländern unterschiedlich geschrieben werden

[9] Siehe auch https://de.wikipedia.org/wiki/EMREX
[10] https://github.com/emrex-eu/elmo-schemas

können, wird ein Levenshtein-Algorithmus mit Schwellenwert zur Überprüfung des Namens verwendet.
- Darüber hinaus werden die Daten nie von der betreffenden Person "berührt", d. h. die Daten können nicht manipuliert werden.

Bewertung

Seit Ende 2021 ermöglicht die HISinOne Campusmanagement-Software sowohl eine Nutzung von EMREX als EMC wie auch als EMP. D.h. die Nutzung von EMREX wird in Deutschland voraussichtlich stark zunehmen. Allerdings gibt es noch keine bundeseinheitliches Identifizierungs- und Autorisierungsmittel für die oben beschriebene doppelte Anmeldung. Speziell für den EMP wäre eine deutschlandweit einheitliche, bildungsorientierte Lösung empfehlenswert. Eine solche Lösung könnte die edu-ID sein.

3.2 ORCID - Open Researcher and Contributor ID

Beschreibung

ORCID[11] ist der Name einer not-for-profit Organisation, die einen Identifier für wissenschaftlich tätige Personen verwaltet (ORCID iD). Diese ID soll eine Person eindeutig kennzeichnen und so eine exakte Zuordnung zu den von ihr veröffentlichten wissenschaftlichen Artefakten ermöglichen. Hauptsächlich sind dies wissenschaftliche Publikationen, es kann sich aber auch um veröffentlichte Forschungsdatensätze oder anderes handeln, welche im optimalen Fall wiederum mit einer persistenten ID (z.B. einem DOI - Digital Object Identifier) versehen sind. Somit lassen sich nicht nur automatisiert Veröffentlichungsverzeichnisse erstellen, sondern es können auch Netzwerke von Veröffentlichungen und Veröffentlichenden dargestellt werden.

Die Registrierung einer ORCID iD für Personen ist kostenlos. Bei der Registrierung kann ein persönliches Profil erstellt werden mit Angaben zu Anstellungen, Ausbildungen & Abschlüssen, Zugehörigkeit zu anderen Institutionen, persönliche Daten wie Mailadresse, Homepage oder Handles in anderen Netzwerken und natürlich zu getätigten Veröffentlichungen. Abgesehen von der E-Mail-Adresse erfolgt keine Validierung dieser selbst eingetragenen Daten. Aus diesen Informationen wird eine öffentliche Profilseite erzeugt, die alle Daten enthält, die der/die Wissenschaftler:in für die Anzeige freigegeben hat. Diese Seite ist gleichzeitig die Landing-Page der eigenen ORCID iD.

Neben der Registrierung bietet ORCID für Heimateinrichtungen eine RESTful API an, über die mit den Metadaten zu einer ORCID iD gearbeitet werden kann (lesen, neue ORCID iD anlegen, Veröffentlichungen zu einer ORCID iD hinzufügen / löschen). Alternativ können auch CSV-Dateien hochgeladen werden. Diese (kostenpflichtige) Option wird von einigen deutschen Hochschulen genutzt.

Das ORCID-System kann auch über OAuth und OpenID Connect zur Authentifizierung genutzt und so als Anmeldedienst (Identity-Provider) bei anderen Service-Providern eingebunden werden.

[11] Vgl. https://orcid.org/

Bewertung

In der wissenschaftlichen Welt ist ORCID mittlerweile sehr verbreitet und etabliert. Hauptsächlich wird die ORCID iD zur eindeutigen Identifikation von Autorinnen und Autoren verwendet. Eine Vielzahl von Publikationsdiensten und -plattformen speichert die ORCID iD nach Eingabe durch den Autor bzw. die Autorin oder übernimmt dieses Attribut direkt vom jeweiligen Identity-Provider. Die Plattformen nutzen dann die ORCID iD über die ORCID-API, um Publikationslisten für die jeweilige ORCID-Identität zu erstellen. Für andere Personengruppen wie Studierende und Verwaltungspersonal hat ORCID nur eine geringe Relevanz.

In der Funktion als Identity-Provider wird ein einfacher Login mit der eigenen ORCID ermöglicht. Da die Attribute der betreffenden Person abgesehen von der E-Mail-Adresse in diesem Falle aber nicht verifiziert sind, sondern im Zweifelsfall nur vom Nutzer bzw. von der Nutzerin selbst stammen, eignet sich dieser Login nur bedingt zur Zuweisung von anwendungsspezifischen Rechten und befindet sich auf dem gleichen Sicherheitsniveau wie eine Anmeldung via Google oder Facebook. Weiterhin sind keine Aussagen über die Aktualität der über ORCID verfügbaren Nutzendendaten möglich. Allerdings besteht die Möglichkeit, bestimmte Daten seitens der Heimateinrichtung zu verifizieren bzw. via API zu provisionieren, siehe oben. Unabhängig davon liefert ein ORCID-Account keine standardisierten, zur Autorisierung tauglichen Attribute, im Gegensatz zum edu-ID-System, das tagesaktuelle Attribute der jeweiligen Heimateinrichtung transportiert.

Somit bietet die Anmeldung via ORCID nur ansatzweise die Einsatzmöglichkeiten, die ein edu-ID-System mit sich bringt. Durch die weite Verbreitung und intensive Nutzung der ORCID als personenbezogenem Identifikator im wissenschaftlichen Umfeld stellt es für ein edu-ID-System ein wichtiges Feature dar, die ORCID iD als Attribut (eduPersonOrcid[12]) mit einem edu-ID-Account zu verknüpfen und bei Anmeldung via edu-ID direkt an einen Service-Provider übertragen zu können.

3.3 AAI-Landesprojekte

Beschreibung

Bundesweit existieren verschiedene Projekte in einzelnen Ländern, die zum Ziel haben, bestehende Synergieeffekte hinsichtlich Identity & Access Management zu verstärken und neue Synergien zu schaffen. Exemplarisch seien hier bwIDM[13], IDM.nrw[14], RARP[15] und SH-IDM genannt. In diesen Projekten wird insbesondere ein föderiertes Identitätsmanagement mit einer einheitlichen Rechteverwaltung unter Benutzung der DFN-AAI verfolgt, damit Landesdienste an einzelnen Einrichtungen bereitgestellt und von Angehörigen aller teilnehmenden Einrichtungen genutzt werden können. Hierfür muss weder ein eigenes zentrales Identity-Management installiert werden, noch besteht die Notwendigkeit eines eigenen Nutzerkontos für jeden Dienst.

Eine weitere wichtige Motivation für die Etablierung dieser Landesinitiativen ist der föderierte Zugriff auf ressourcenintensive Dienste, zum Beispiel High Performance Computing, sowie auf Dienste mit besonderem Administrationsaufwand, beispielsweise auf die Kursportale der

[12] https://wiki.refeds.org/display/STAN/eduPerson+2021-11#eduPerson202111-eduPersonOrcid
[13] https://bwidm.de
[14] https://idm.dh.nrw
[15] https://rarp.rlp.net

einzelnen Einrichtungen oder auf Mattermost/Gitlab in der Rechenzentrumsallianz Rheinland-Pfalz (RARP). Ferner führen diese Landesinitiativen zu einer insgesamt verstärkten Kooperation und zum Heben von noch unerkannten, aber bestehenden Synergiepotenzialen zwischen den verschiedenen Einrichtungen.

Im Rahmen von bwIDM wurden grundlegende technische Lösungen und Konzepte entwickelt, die von anderen Landesinitiativen übernommen werden konnten. Dazu gehören die Software „RegApp“, ein einheitlicher Satz von Attributen, der von allen IdPs allen angeschlossenen Diensten zur Verfügung gestellt werden kann, sowie ein einheitliches Konzept zur Deprovisionierung ausgeschiedener Nutzerinnen und Nutzer.

Da zum jetzigen Zeitpunkt noch keine einheitliche Lösung für die langfristige Identifizierung von Forschenden existiert, entwickeln einzelne der landesweiten Projekte eigene Verfahren, mit denen die offenbar gewordenen Probleme angegangen werden sollen. Hierfür wird zum Beispiel die ORCID eingesetzt, die aber keinen vollwertigen Ersatz zur edu-ID darstellt, weil das edu-ID-System z.B. einen eigenen IdP zur Verfügung stellt und in der Lage ist, Attribute aus der jeweiligen Heimateinrichtung in Echtzeit abzurufen und an den entsprechenden Dienst weiterzuleiten, siehe hierzu oben 3.2. Grundsätzlich kann gesagt werden, dass abhängig vom Startzeitpunkt der jeweiligen Initiative die Ergebnisse der früher gestarteten von den späteren übernommen werden konnten. Dies zeugt von einem hohen Kooperationsgrad zwischen den Bestrebungen der Länder. Ein Beispiel solcher Kooperationen ist die Allianz zwischen bwIDM und IDM.nrw, im Zuge derer eine gemeinsame Weiterentwicklung der bestehenden bwIDM-Lösungen stattfindet, um die in beiden Ländern unabhängigen Anforderungen zu erfüllen[16], begünstigt durch die inhaltliche und zeitliche Nähe der jeweiligen Projekte.

Bewertung

Das edu-ID-Konzept stellt kein Konkurrenzangebot zu den Landesprojekten dar, sondern ist vielmehr als Hilfsmittel zu sehen, um bestimmte lose Enden dieser Projekte zusammenzufügen. So ist naturgemäß keine bundesweite Eindeutigkeit der landesweit genutzten Identifikatoren gegeben, was bei einer länderübergreifenden Nutzung Probleme in sich birgt. Diese bundesweite Eindeutigkeit kann durch die Verwendung einer edu-ID hergestellt werden.

3.4 Forschungscommunities und -Infrastrukturen

Forschung, insbesondere Drittmittel-geförderte Forschung bedeutet in der überwiegenden Mehrheit der Fälle auch Kooperation über Einrichtungs- und Ländergrenzen hinweg. Forschungsprojekte und -Communities errichten virtuelle Infrastrukturen, an die neben fachspezifische Ressourcen auch generische Dienste wie z.B. HPC-Ressourcen angebunden werden. Aus diesen Rahmenbedingungen hat sich das Konzept einer virtuellen Organisation entwickelt, also einer Organisation, die aus verschiedenen nicht-virtuellen Organisationen besteht und die als Anker für das Rechte- und Rollenmanagement für den Zugriff auf die erwähnten Ressourcen dient.

Als Diskussionsforum und Sprachrohr hinsichtlich AAI-spezifischer Anforderungen von Forschungscommunities dient seit vielen Jahren die Gruppe FIM4R - Federated Identity Management for Research[17]. Im Zuge der Arbeit dieser Gruppe wurden zwei Whitepaper

[16] https://idm.dh.nrw/umsetzungsprojekt/ziel
[17] Vgl. https://fim4r.org

veröffentlicht[18], in denen die Anforderungen der in FIM4R zusammengeschlossenen Communities hinsichtlich föderiertem Identitätsmanagement, Authentifizierung und vor allem Autorisierung formuliert wurden.

Die Aktivitäten von FIM4R waren eine wichtige Motivation für das EU-Projekt AARC - Authentication and Authorization for Research Collaborations[19]. Im Rahmen dieses Projekts wurde in den Jahren 2015 bis 2019 neben zahlreichen technischen Richtlinien und dem sogenannten Policy-Development Kit auch eine Blaupause für Community-AAIs entwickelt, die AARC Blueprint Architecture, kurz BPA[20]. Die AARC Blueprint Architecture hat sich seitdem zum Quasi-Standard für Community-AAIs entwickelt. Als repräsentative Beispiele für die Umsetzung der BPA werden im folgenden die Helmholtz AAI sowie die DARIAH AAI behandelt.

3.4.1 Beispiel Helmholtz AAI

Beschreibung

Die Helmholtz AAI[21] hat das Ziel, einen einheitlichen Zugriff auf IT Dienste innerhalb der Helmholtz Gemeinschaft zu ermöglichen. Dabei sollen Kooperationspartner (Gäste) genauso wie Helmholtz-Mitarbeiter:innen die Identität ihrer jeweiligen Heimateinrichtung verwenden. Die Unterscheidung dient hierbei im wesentlichen der Rechtevergabe.
Um den Kreis an Nutzenden möglichst groß zu gestalten, werden zusätzlich zu Nutzenden aus der DFN-AAI und eduGAIN auch solche aus Social IdPs zugelassen (aktuell ORCID, Google und Github). Die Helmholtz AAI kennzeichnet die Nutzenden über Verlässlichkeitsmerkmale basierend auf dem REFEDS Assurance Framework[22].

Es werden SAML und OpenID Connect (OIDC) Dienste unterstützt.
Aktuell wird an der Integration von Systemen gearbeitet, die standortübergreifend identische Nutzende über den Helmholtz Cloud Agent oder die vertiefte Integration von Unix Diensten (z.B. ssh oder sudo) mit föderierten Identitäten bedienen.
Das Weiterreichen von Deprovisionierungsinformationen ist implementiert und ermöglicht Diensten, die dies unterstützen, eine Benachrichtigung zu erhalten, wenn Nutzende aus einer Gruppe entfernt werden oder ihre Heimateinrichtung verlassen.

Die Architektur der Helmholtz-AAI folgt der AARC Blueprint Architektur[23], dem sogenannten Proxy-Modell. Dabei werden die Attribute über eine Nutzerin / einen Nutzer von der Heimateinrichtung an einen Proxy übermittelt, der dann einen einheitlichen Satz an Attributen (ergänzt um weitere Informationen über die betreffende Person) an die Dienste weiterleitet.

Ein übergeordneter Identifikator, wie z.B. eine edu-ID, wird aktuell am Beispiel von ORCID unterstützt. Diese ID können Nutzer aktuell manuell eintragen. Lösungen, die dies durch

[18] Zuletzt: Federated Identity Management for Research Collaborations v2, June 22, 2018, https://zenodo.org/record/1307551#.YvaCAzXP1hE
[19] https://aarc-community.org/
[20] https://aarc-community.org/architecture/
[21] Helmholtz AAI https://aai.helmholtz.de
[22] REFEDS Assurance Framework (RAF) https://refeds.org/assurance
[23] Authentication and Authorisation for Recearch Communities (AARC) https://aarc-community.org

Automatisierung vereinfachen, nutzerfreundlich und vor allem sicherer gestalten, können integriert werden.

Bewertung

Aufgrund des geplanten Funktionsumfangs des edu-ID-Konzepts kann dieses eine sinnvolle Ergänzung zur Identifizierung der Nutzenden über eine manuell eingetragene ORCID darstellen, da die edu-ID und davon abgeleitete Identifikatoren verlässlich vom System generiert und verwaltet werden. Weiterhin bieten edu-ID-Identitäten ein höheres Maß an Verlässlichkeit als sog. Social IDs, so dass hier ein deutlicher Mehrwert beim Onboarding bestünde. Ein eindeutiger, von der edu-ID abgeleiteter Identifier erleichtert die Deprovisionierungsprozesse.

3.4.2 Beispiel DARIAH AAI

Beschreibung

DARIAH-DE unterstützt die mit digitalen Methoden arbeitenden Nutzenden aus den Geistes- und Kulturwissenschaften in Forschung und Lehre. Dazu wurde u.a. eine digitale Forschungsinfrastruktur aufgebaut, sowie Materialien für Lehre und Weiterbildung im Bereich der Digital Humanities (DH) entwickelt.

Im Rahmen von DARIAH-DE[24] wurde eine zur AARC Blue Print Architecture (BPA) kompatible AAI aufgebaut, die DARIAH-AAI.

Grundsätzlich besteht die DARIAH-AAI aus folgenden Bausteinen[25]:

- Ein Proxy fungiert als SAML IdP für die DARIAH SPs, implementiert selbst einige Workflows (Registrierung, Autorisierung) für diese SPs, und zeigt sich in SAML-basierten Föderationen (eduGAIN) als SP.
- Ein Policy Decision Point (PDP), in dem zentral Zugriffsregeln für Anwendungen verwaltet und entsprechende Access-Tokens erstellt werden können und der gegenwärtig von der DARIAH-DE-Storage-Infrastruktur (DARIAH-DE Repository und DARIAH-DE Publikator), sowie vom Geo-Browser genutzt wird.
- Eine mandantenfähige Benutzerverwaltung, in der jede Virtuelle Organisation Zugriffsrechte auf ihre Dienste vergeben kann, wobei Gruppenmitglieder sowohl Nutzende von Heimat-IdPs als auch DARIAH-Nutzende sein können. Das dazugehörige Self-Service-Interface ermöglicht u.a. das Registrieren von DARIAH-Accounts, sowie die Beantragung von Gruppenmitgliedschaften. Nutzende, die sich in der Föderation (DFN-AAI) nicht über einen Heimat-IdP authentifizieren können, können über den Self-Service einen DARIAH-Account erstellen. Hierbei muss sichergestellt werden, dass es sich bei der betreffenden Person um ein Mitglied einer der für DARIAH-DE relevanten Forschungscommunities handelt. Dies geschieht automatisch, wenn die E-Mail-Adresse der betreffenden Person eine Hochschuladresse ist, bei anderen E-Mail-Adressen geschieht dies über einen manuellen Prozess, in dem diese Person nachweisen muss, dass sie im Bereich Geisteswissenschaften forscht.

[24] Vgl. https://de.dariah.eu/en/web/guest/home

[25] Eine Dokumentation ist unter https://wiki.de.dariah.eu/display/publicde/DARIAH+AAI+Documentation zu finden.

- Ein DARIAH-IdP, der die DARIAH-Accounts in die Föderation (DFN-AAI) einbringt.

Diese AAI wird seit vielen Jahren produktiv betrieben und bietet Zugriff auf zahlreiche Dienste, die mittlerweile von CLARIAH-DE[26], dem Nachfolgeprojekt von DARIAH-DE und CLARIN-D[27] angeboten werden.

Bewertung

Zwar hat sich die DARIAH-AAI bewährt, aber die Verwaltung der DARIAH-Accounts ist relativ arbeitsaufwändig. Ein Account-Linking (sprich, verschiedene Accounts bei Heimat-IdPs verweisen auf eine DARIAH-ID) ist ebenfalls nur über einen aufwändigen manuellen Prozess möglich. Eine domänenübergreifende Nutzendenverwaltung mittels eines im edu-ID-System integrierten IdP könnte langfristig den DARIAH-IdP ersetzen und so dem Projekt Arbeit erleichtern, sowie den Nutzenden einen weiteren Account für Ihre wissenschaftliche Arbeit ersparen. In diesem Rahmen könnte ein edu-ID-System auch die Prüfungsmechanismen für Accounts, die derzeit von der CLARIAH-DE-AAI übernommen werden, erleichtern und ergänzen. Auch im Bereich Account-Linking könnte die CLARIAH-DE-AAI in jedem Fall von einem edu-ID-System profitieren, über das solche Verknüpfungen einfacher und von den Nutzenden gesteuert erstellt werden können. Dies gilt in besonderem Maße für die Verknüpfung von Hochschul-Accounts mit dem jeweiligen edu-ID-Account.

Letztendlich könnte ein edu-ID-System bewirken, dass sich die CLARIAH-DE-AAI auf die Verwaltung der virtuellen Organisationen über Gruppenmitgliedschaften beschränken kann. Der Prozess der Registrierung eines DARIAH-Accounts würde nicht abgeschaltet werden, damit er etwa für DARIAH-Nutzende aus anderen EU-Ländern weiterhin genutzt werden kann.

3.5 Online Zugangsgesetz (OZG): Nutzerkonto Bund/Land

Beschreibung

Das Gesetz zur Verbesserung des Onlinezugangs zu Verwaltungsleistungen (Onlinezugangsgesetz – OZG http://www.gesetze-im-internet.de/ozg/) verpflichtet Bund, Länder und Kommunen, bis Ende 2022 Verwaltungsleistungen über Verwaltungsportale auch digital anzubieten. Zur Identifizierung der Nutzenden dienen Nutzerkonten für Bürgerinnen und Bürger.

> „Einmal registriert, sollen sich Nutzerinnen und Nutzer künftig mit ihrem Nutzerkonto gegenüber allen digitalen Verwaltungsleistungen des Portalverbunds authentisieren können. Registrierung und Anmeldung erfolgen nach den Vorgaben der europäischen Verordnung über elektronische Identifizierung und Vertrauensdienste (eIDAS-VO). Je höher das Sicherheitsniveau einer Verwaltungsleistung, desto höher sind die Anforderungen an die zu verwendenden Identifizierungsmittel. Als Identifizierungsmittel kommen unter anderem die Benutzername-Passwort-Kombination sowie die Online-Ausweisfunktion des Personalausweises, des elektronischen Aufenthaltstitels und der eID-Karte für Unionsbürgerinnen und -bürger in Betracht. [...]

[26] Vgl. https://www.clariah.de/

[27] Vgl. https://de.wikipedia.org/wiki/CLARIN-D

> Durch Speicherung ihrer Identitätsdaten (gemäß § 8 OZG) auf freiwilliger Basis können Nutzerinnen und Nutzer die erneute Dateneingabe vermeiden, indem sie ihre hinterlegten Daten für digitale Verwaltungsleistungen freigeben. Dadurch werden zum Beispiel elektronische Formulare automatisch befüllt."[28]

Die Nutzerkonten sind untereinander interoperabel. Als leitendes Nutzerkonto kristallisiert sich derzeit das vom Bund betriebene „Nutzerkonto Bund"[29] (NKB, auch als bundID bezeichnet) heraus.

Bewertung

Für Identifikation und Autorisierung werden innerhalb des Onlinezugangsgesetzes (OZG)[30] momentan die Nutzerkonten als maßgebend betrachtet. Andere Werkzeuge der Identifikation und Autorisierung sind zwar nicht ausgeschlossen, werden aber höchstens zweitrangig betrachtet. Die Anbindung an ein Nutzerkonto wird als Voraussetzung für die Erfüllung des OZG gesehen. Siehe hierzu OZG § 3, Abs. 2.

Wir können davon ausgehen, dass das Basis- und das niedrige Vertrauensniveau über verschieden autorisierte Nutzer-/Passwort-Identifikationen für die meisten Prozesse im Bildungsbereich nicht von Interesse sind. Interessant werden Identifikationen über das substantielle und über das hohe Vertrauensniveau sein. Dazu gibt es in Deutschland bislang nur zwei Basislösungen:

- Für das substantielle Vertrauensniveau das Elsterzertifikat
- Für das hohe Vertrauensniveau die Online-Ausweisfunktion des deutschen ePA, des elektronischen Aufenthaltstitels sowie der eID-Karte für Unionsbürgerinnen und -Bürger

Beide Identifikationsmittel sind hauptsächlich für erwachsene Bundesbürger gedacht. Identifikationslösungen auch für Minderjährige sind auf diesem Vertrauensniveau bislang noch nicht vorgesehen (speziell für das führende Nutzerkonto Bund ist dieses Thema Gegenstand einer aktuellen Diskussion). Keines dieser Identifikationsmittel transportiert Informationen, die ein dienstseitiges Autorisierungskonzept unterstützen, auch nicht für den Bildungssektor (weder im primären, sekundären noch tertiären Bildungssektor).

Genau hier könnte das edu-ID-System eine Lücke füllen, als ein von den Nutzerkonten akzeptiertes Identifikationsmittel auf mindestens substantiellen und vielleicht auch hohen Vertrauensniveau, das als Basis für Autorisierungskonzepte u.a. im Bildungsbereich dienen kann. Allerdings stellt sich die Frage, ob die Basis-Identität der Nationalen Bildungsplattform für diese Aufgabe nicht besser geeignet ist. Siehe hierzu den nachfolgenden Abschnitt.

Im Augenblick entstehen schon für andere Lösungen (z.B. Keycloak) Arbeitsgruppen innerhalb des NKB-Projekts. Es ist anzuraten, dass die edu-ID-Arbeitsgruppe mit dem NKB-Projekt Kontakt aufnimmt, um zu prüfen, inwieweit eine Zusammenarbeit (z.B. in Form einer selbstständigen NKB-Arbeitsgruppe wie bei Keycloak) möglich wäre.

---

[28] Vgl. https://www.onlinezugangsgesetz.de/Webs/OZG/DE/umsetzung/ozg-infrastruktur/nutzerkonten/nutzerkonten.html; zur eIDAS-VO siehe https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32014R0910

[29] Vgl. https://id.bund.de/de/eservice/konto

[30] https://www.onlinezugangsgesetz.de

In Bezug auf das Nutzerkonto Bund sollte eine Anbindung angestrebt werde, die eine Authentifikation der Nutzenden durch die bereits vorhandenen Mechanismen kostenfrei ermöglicht.

3.6 Nationale Bildungsplattform

Beschreibung

Mit der Nationalen Bildungsplattform (NBP) schafft das Bundesministerium für Bildung und Forschung (BMBF) eine Vernetzungsinfrastruktur für die digitale Bildung[31]. In diese Meta-Plattform sollen existierende digitale Bildungsangebote und sonstige bildungsrelevante Ressourcen und Dienste anhand offener Standards und Schnittstellen integriert und miteinander verknüpft werden. Darüber hinaus soll für die Nutzenden die Möglichkeit einer Ablage für alle Arten digitaler Bildungsnachweise und -Profile geschaffen werden. Die über die NBP verfügbaren Angebote richten sich gleichermaßen an Lernende wie Lehrende.

Das technische Konzept der NBP[32] sieht einen Zugang über Web-basiertes Single Sign-on (SSO) vor, weshalb sowohl eine Integration in die DFN-AAI als auch in die Schulföderation VIDIS (s.u.) angestrebt wird. Weiterhin ist die Anbindung an das Nutzerkonto Bund (s.o.) vorgesehen. Hierbei steht die NBP vor Herausforderungen wie der Notwendigkeit eines dauerhaften und ggf. von der jeweiligen Heimateinrichtung unabhängigen Zugriffs auf bestimmte Ressourcen. Auch wird es Nutzende geben, die keinen Zugriff auf einen Heimat-IdP haben. Daher implementiert die NBP eine eng an das edu-ID-Konzept angelehnte „Basis-Identität“. Diese Basis-Identität dient als Anker für die Verknüpfung der digitalen Identität der/des jeweiligen Nutzenden sowohl mit eigenen digitalen Nachweise und sonstigen Dokumenten sowie mit anderen AAI-Identitäten und der des Nutzerkonto Bund. Ein separater IdP dient als Authentifizierungsquelle für Nutzende ohne Heimat-IdP. Somit bildet die Basis-Identität eine wichtige technische Grundlage für das lebenslange Lernen und die langfristige Nutzung der über die NBP verfügbaren Ressourcen.

Bewertung

Die „Basis-Identität“ der NBP kann als konkrete Implementierung eines edu-ID-Systems betrachtet werden, wenn auch in diesem Kontext lediglich eine Teilmenge der eingangs genannten Use Cases bedient wird und einige im technischen Konzept beschrieben Features fehlen werden. In jedem Fall macht es Sinn, den bereits bestehenden Austausch mit dem BMBF und den Implementierungspartnern der NBP fortzusetzen und zu intensivieren. Da die Proof of Concept Implementierung des edu-ID-Systems annähernd parallel zum Aufbau der NBP erfolgt, können beide Seiten von einem regelmäßigen Austausch profitieren.

[31] https://bildungsraum.de

[32] https://bildungsraum.de/download/attachments/18357001/NBP-Technischer-Rahmen_V21.pdf

3.7 Identitäten im schulischen Bereich am Beispiel von VIDIS

Beschreibung

Das Projekt VIDIS (Vermittlungsdienst für das digitale Identitätsmanagement in Schulen) wurde von den 16 Ländern damit beauftragt, eine föderale Authentifizierungs- und Autorisierungsinfrastruktur (Schul-AAI) für den schulischen Bereich zu entwickeln. Ziel ist die Landes-, Schulträger- und Schulsysteme einheitlich mit digitalen Bildungsangeboten zu verbinden. Neben der technischen Umsetzung eines ID-Proxy ist ein Hauptbestandteil des Projektes die Modellierung eines Rechtsmodells und die damit einhergehende (datenschutz)-rechtliche Absicherung für Nutzende.

Im Vollausbau soll der VIDIS-Dienst für ca. 800.000 Lehrkräfte und 10,9 Millionen Schüler:innen eine föderale Anmeldung ermöglichen. Außerdem versprechen sich die Länder durch eine Vereinheitlichung der Schnittstellen und den einfacheren Zugang Innovationsimpulse für digitale Bildung im System Schule.

Mehr Informationen unter https://www.vidis.schule.

Bewertung

Im Übergang zum Hochschulbereich existieren Use Cases (z.B. der dauerhafte Zugriff auf Leistungs- und sonstige Nachweise), die einen möglichst nahtlosen Übergang von einer Identität aus der Schul-AAI zu einer edu-ID oder der Basis-Identität der NBP, z.B. mittels Account-Linking als hilfreich erscheinen lassen.

3.8 Internationaler Kontext

Beschreibung

Auf internationaler Ebene existieren drei edu-ID-Systeme, die sich bereits im Produktivbetrieb befinden: SWITCH edu-ID[33] (Schweiz), eduID.nl[34] (Niederlande) und eduID.se[35] (Schweden).

Das schwedische edu-ID-System dient primär dazu, Personen, die sich auf einen Studienplatz in Schweden bewerben, mit einer digitalen Identität auszustatten, anhand derer dann Studienplatzbewerbung, Immatrikulation etc. erfolgen. Diese ID ist lebenslang gültig.

Sowohl SWITCH edu-ID als auch eduID.nl befinden sich bereits seit einigen Jahren im Produktivbetrieb und werden laufend um neue Anwendungsfälle erweitert. Im Fall der schweizerischen Lösung ging es zunächst um den Zugriff auf Inhalte, die über Nationallizenzen verfügbar sind, dann kamen Speicher- bzw. Sync & Share Services dazu sowie die zentrale Schweizer Bibliotheksplattform (Swiss Library Service Platform - SLSP)[36]. Damit einher geht der Umbau der Schweizer Föderation SWITCHaai von einer multilateralen, sog. Mesh Federation zu einer Hub-and-Spoke Federation, bei der das edu-ID-System die zentrale Komponente, den sog. Hub bildet.

---

[33] https://www.switch.ch/de/edu-id/
[34] https://eduid.nl
[35] https://eduid.se
[36] https://slsp.ch

Der initiale Use Case des niederländischen edu-ID-Systems ist der lebenslange Zugriff auf Leistungsnachweise, ein weiterer Anwendungsfall ist die Unterstützung der (nationalen) Studierendenmobilität.

Bewertung

Bei SWITCH edu-ID und eduID.nl handelt es sich um zum hier diskutierten edu-ID-System funktionsanaloge Konzepte, deren Reichweite jedoch auf nationale Anwendungsfälle beschränkt ist. Daher ist hier mit hoher Priorität eine Interoperabilität anzustreben. In der Praxis sollte es zukünftig keinen Unterschied machen, ob der Login an einem Dienst, der an ein edu-ID-System angeschlossen ist, über SWITCH edu-ID, eduID.nl oder das hier diskutierte edu-ID-System erfolgt.

4. Schlussfolgerungen

Die oben stehenden Ausführungen haben einen Überblick gegeben, welche Ansätze national und international verfolgt werden, um die reibungsarme Nutzung von elektronischen Diensten und sonstigen Ressourcen durch eine Person zu gewährleisten. Dabei wurde deutlich, dass hinsichtlich deren Anwendbarkeit auf die eingangs genannten Nutzungsszenarien jeweils Einschränkungen unterschiedlicher Art bestehen. Dies betrifft in vielen Fällen auch die Lebensdauer der digitalen Identität. Dieser Umstand kann als hinreichende Motivation gelten, die Entwicklung eines edu-ID-Systems voranzutreiben.

So kann aus den Bewertungen der verschiedenen o.g. Projekten, Systemen und Lösungsansätzen das Thema **Account Linking** als ein zentrales Feature des edu-ID-Systems abgeleitet werden. Dies betrifft in besonderem Maße die Verknüpfung mit der ORCID-Identität, aber auch in anderen Kontexten ergeben sich interessante Anwendungsszenarien hinsichtlich dieser Funktionalität, z.B. in Bezug auf VIDIS oder den European Student Identifier, ESI. Als ein von der deutschen Forschungs- und Bildungs-Community gesteuerter, nicht-kommerzieller Dienst könnte sich das edu-ID-System perspektivisch zu einer Art Switchboard für digitale Identitäten entwickeln. So würde ein Ort für die Domäne Forschung und Bildung entstehen, wo Nutzende Informationen zu ihren Identitäten so zusammenführen bzw. verknüpfen können, dass eine nahtlose und langfristige Nutzung der für sie relevanten Ressourcen ermöglicht wird. Da nicht alle Ressourcen SAML-fähig sind, funktioniert dies nur, wenn weitere Standards wie OpenID Connect unterstützt werden. Die Architektur des edu-ID-Systems muss daher so modular und flexibel sein, dass **Unterstützung für weitere Standards** kurzfristig und mit vertretbarem Aufwand zu implementieren ist.

In diesem Kontext ist auch die angestrebte **Interoperabilität** mit den Lösungen der Niederlande und der Schweiz zu sehen. Die hierfür erforderliche **Kommunikation** und **Abstimmung** muss intensiviert werden. Selbiges gilt für die Zusammenarbeit mit den diversen **Landesprojekten**.

Für den **dauerhaften Zugriff auf Ressourcen** wie Forschungsdaten, Leistungsnachweise und sonstige Daten müssen diese mit einem von der edu-ID abgeleiteten oder einem mit ihr verknüpften langlebigen Identifier verbunden werden. Hierzu bedarf es einer engen Abstimmung mit den zuständigen Stakeholdern, insbesondere den jeweiligen Ressourcen-Anbietern wie den deutschen Hochschulen, der HIS eG, den Forschungscommunities, dem EMREX Exekutivrat und anderen mehr.

Dadurch, dass das edu-ID-System eine **Authentifizierungsquelle**, d.h. einen Identity-Provider für Nutzende ohne Heimat-IdP bereitstellt, entfällt seitens der **Forschungscommunities** (z.B. DARIAH) und anderer Infrastruktur- und Inhaltsanbieter (z.B. Nationallizenzen) die Notwendigkeit, selber einen „IdP of last Resort“ zu betreiben. Dies entbindet diese jedoch nicht von der Notwendigkeit, weiterhin ein Berechtigungsmanagement für den Zugriff auf die bereitgestellten Ressourcen zu betreiben. Für die Umstellung auf neue, über das edu-ID-System provisionierte Identitäten müssen daher gemeinsam entsprechende **Migrationsstrategien** entwickelt, dokumentiert und unterstützt werden.

Was **staatliche Systeme** wie die **bundID** (Nutzerkonto Bund) und die **Basis-Identität** der Nationalen Bildungsplattform angeht, so ist derzeit noch nicht abzusehen, ob und welche Synergien und Kooperationsszenarien sich in Bezug auf das edu-ID-System ergeben werden. Wie oben erwähnt besteht bereits seit einiger Zeit ein Austausch mit der Projektgruppe Nationaler Digitaler Bildungsraum im BMBF und den mit der Implementierung der Nationalen Bildungsplattform betrauten Partnern. Wie sich die beiden Systeme entwickeln und letztendlich zueinander verhalten werden, ist derzeit noch offen.

Die im Abschnitt zum Nutzerkonto Bund (NKB) skizzierte Möglichkeit der Anbindung des edu-ID-Systems an das NKB als Identifikationsmittel mit einem substantiellen bis hohen Vertrauensniveau setzt eine entsprechende Einstufung seitens des BSI voraus. Abgesehen davon, dass die hierfür erforderlichen edu-ID-seitigen Prozesse und Policies mit einigem Aufwand etabliert werden müssten, stellt sich die Frage nach dem tatsächlichen Mehrwert einer solchen Maßnahme für die Zielgruppe des edu-ID-Systems. In die andere Richtung könnte eine Anmeldung mit der bundID am edu-ID-System, verbunden mit einer Übernahme bestimmter Daten, eine entsprechend vertrauenswürdige edu-ID-Identität sicherstellen. Da das edu-ID-System von keiner Stelle der öffentlichen Verwaltung betrieben wird, ist ein solches Szenario derzeit ausgeschlossen. Ob das Nutzerkonto Bund auch als Authentifizierungsquelle für Dienste außerhalb der öffentlichen Verwaltung verfügbar sein wird, ist derzeit nicht abzusehen. In jedem Fall wird es Sinn machen, in dieser Angelegenheit mit der zuständigen Stelle am BMI Kontakt aufzunehmen.

Nachdem das technische Konzept für das edu-ID-System im Juli 2022 fertiggestellt wurde, wird aktuell, d.h. im September 2022, an der Implementierung eines Proof of Concept gearbeitet, der bis Anfang 2023 fertig gestellt sein soll. Hierbei finden die in diesem Whitepaper angestellten Schlussfolgerungen besondere Berücksichtigung. Dies gilt auch für den für 2023 geplanten Pilotbetrieb und die Schaffung der damit verbunden technischen, rechtlichen und organisatorischen Rahmenbedingungen.