Eine edu-ID für die Wissenschaft in Deutschland
– technisches Konzept –

Jürgen Brauckmann (DFN-CERT), Rainer Fischer (Hochschule Reutlingen), Peter Gietz (DAASI), Gerrit Gragert (Staatsbibliothek zu Berlin), Steffen Hofmann (FU Berlin), David Hübner (DAASI), Heike Kaufmann (DFN-Verein), Winfried Kuiper (Uni Flensburg), Thorsten Michels (TU Kaiserslautern), Bernd Oberknapp (Uni Freiburg), Wolfgang Pempe (DFN-Verein), Ramon Pfeiffer (Uni Tübingen), Frank Schreiterer (Uni Bamberg), Erwin Soldo (DAAD)

Inhalt

1 Einführung und Ziele

Im Kontext von Authentifizierungs- und Autorisierungs-Infrastrukturen (AAI) ist es üblicherweise die jeweilige Heimateinrichtung, die für ihre Angehörigen eine digitale Identität zur Verfügung stellt und diese verwaltet. 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 Mitarbeitendenstatus innerhalb derselben Einrichtung. Eine Unterbrechung oder das Ende eines akademischen Lebenslaufs führt in dieser Hinsicht zu einem völligen Identitätsverlust. Viele der oben erwähnten 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 kommenden Nationalen Forschungsdateninfrastruktur (NFDI) eine wichtige Rolle spielen.

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 zuständigen Stelle abhängig und deren Bereitschaft, die grundsätzliche Attributfreigabe für den betreffenden Dienst zu konfigurieren.

1.1 Aufgabenstellung

Aus der beschriebenen Problemstellung ergibt sich als Ziel die Einführung und Etablierung einer personenbezogenen, institutionsunabhängigen und globalen digitalen Identität für den Bereich Forschung und Bildung, welche eine Person das gesamte wissenschaftliche Leben begleitet und dauerhaft für die Nutzung von Diensten und den Zugriff auf bestimmte Ressourcen eingesetzt werden kann. Vom Beginn des wissenschaftlichen Lebens an (z.B. Studienbeginn) können so Berechtigungen auf Universitätsdienste oder Zugriffsrechte auf Dokumente und Forschungsdaten erteilt werden, die auch bei einem Institutionswechsel bestehen bleiben. Die von einem zukünftigen edu-ID System zu unterstützenden Use-Cases sind ausführlich unter https://doku.tid.dfn.de/de:aai:eduid:usecases beschrieben.

Die sich daraus ergebenden technischen, organisatorischen und juristischen Anforderungen sind unter https://doku.tid.dfn.de/de:aai:eduid:usecases#anforderungen detailliert aufgeführt.

Der Schwerpunkt des edu-ID Konzepts liegt allgemein auf der Authentifizierung und Autorisierung auf Basis von SAML2 im Rahmen der etablierten Föderation DFN-AAI. Eine spätere Ausweitung auf andere Standards, Protokolle und Infrastrukturen ist jedoch vorgesehen und muss insbesondere beim Design von Schnittstellen mit berücksichtigt werden.

1.2 Qualitätsziele

Die wichtigsten Qualitätsziele, die für die jeweiligen Beteiligten an einem edu-ID-System erreicht werden müssen, sind:

1. Heimateinrichtungen
    a. Bestehende Identity-Provider-Systeme (IdP) sollen unverändert weiterbetrieben werden
    b. Keine signifikanten Änderungen an einrichtungsinternen Identity-Management-Systemen (IdM)
    c. Vereinfachung bestehender IdM-relevanter Prozesse insbesondere beim Onboarding
    d. Datenschutzkonformität hinsichtlich DSGVO, Bundes- und Landesdatenschutz
2. Anwender:innen
    a. Höchstmögliches Datenschutzniveau und vollständige Kontrolle über die Übertragung personenbezogener Daten
    b. Eingabe persönlicher Daten (im Idealfall) an nur noch einer Stelle oder Übernahmemöglichkeit der Daten aus vertrauenswürdigen Systemen, z.B. Profile aus Servicekonten der öffentlichen Verwaltung, oder staatliche eID-Token wie der Neue Personalausweis (nPA) oder der elektronische Aufenthaltstitel
    c. Anwender:innen möchten alle persönlichen Daten im edu-ID-System über eine benutzerfreundliche Weboberfläche einsehen und verwalten können
    d. Single Sign-on innerhalb der DFN-AAI ohne Brüche
3. Betreiber des edu-ID-Systems
    a. System ist hochverfügbar
    b. System entspricht hohen Standards von Datenschutz, Daten- und Betriebssicherheit
    c. System interoperiert performant mit Identity- und Service-Providern (SP), d.h. mit maximalen Antwortzeiten < 2 sec

1.3 Stakeholder

Rolle	Erwartungshaltung
Wissenschaftler:innen / inner- + außeruniversitäre Forschung	Unterstützung der gesamten Forschungsarbeit, unterbrechungsfreier Zugriff auf Ressourcen auch beim Wechsel der Heimateinrichtung
Studierende	Vereinfachte Nutzung von Uni-Angeboten auch über Institutionsgrenzen hinweg, unterbrechungsfreier Zugriff auf Ressourcen (insbes. Leistungsnachweise) auch beim Wechsel der Heimateinrichtung

IdP- / IdM-Betreiber:innen	Vereinfachte Erkennung von Doubletten, keinen Mehraufwand für die Heimat-IdMs
Datenschützer:innen	Datenschutzkonformes System
SP-Betreiber:innen	Vereinfachung in der Attributkonfiguration, keinen Mehraufwand bei Einrichtungswechsel der Nutzenden
Fachinformationsdienste (FID)	Single Sign-on-Zugriff auf FID-Ressourcen institutionsunabhängig
NFDI-Konsortien	Einfache Zugriffssteuerung auf geschützte Forschungsdaten, ggf. unabhängig von der aktuellen Heimateinrichtung
Hochschulverwaltung / Campus Management Systeme (CMS)	Vereinfachung von Prozessen aus dem Bereiche Onboarding, Studierendenverwaltung, Personalverwaltung
Föderationsbetreiber (DFN)	Bessere Unterstützung der Bedürfnisse der Zielgruppe(n)
Nationale Bibliotheken	Single Sign-on (SSO) für Nutzer:innen ermöglichen

2 Randbedingungen

Da eine edu-ID perspektivisch auch für Verwaltungsvorgänge wie die Einschreibung an einer Hochschule oder die Anmeldung bei einer öffentlichen Bibliothek genutzt werden können soll, ist das "Gesetz zur Verbesserung des Onlinezugangs zu Verwaltungsleistungen (Onlinezugangsgesetz – OZG[1])" der Rahmen, in dem sich auch ein edu-ID-System in Deutschland bewegen muss.

2.1 Politisch

Eine komplexe Randbedingung stellt das föderale Bildungs- und Wissenschaftssystem in Deutschland dar. Wissenschaft ist in Deutschland Aufgabe der Länder, daher muss das System allen Anforderungen und Ansprüchen aus den einzelnen Bundesländern genügen, um letztendlich erfolgreich zu sein.

Eine entsprechende wissenschaftspolitische Unterstützung auf verschiedenen Ebenen ist daher unabdingbar. Der DFN-Verein ist durch seine Mitglieder und Vernetzung eine entscheidende treibende Kraft. Für die Unterstützung seitens anderer wichtiger Partner in der deutschen

[1] http://www.gesetze-im-internet.de/ozg/

Wissenschaftslandschaft muss jedoch Lobby-Arbeit betrieben werden. Hierzu zählen ZKI, DFG, BMBF oder auch GWK und ggf. KMK.

2.2 Rechtlich

Die rechtlichen Rahmenbedingungen stellen die DSGVO, das Bundesdatenschutzgesetz sowie die Datenschutzgesetze der Länder dar. Ein edu-ID-System muss alle daraus resultierenden Anforderungen erfüllen. Daher muss eine technische Lösung immer auch rechtlich bewertet werden, um dies zu garantieren. Zu klären sind auch sämtliche rechtliche Fragen für den eigentlichen Betrieb des edu-ID-Systems und welche vertraglichen Regelungen zwischen welchen Parteien, die am System und dessen Nutzung beteiligt sind, vereinbart werden müssen, um für alle Seiten Rechtssicherheit herzustellen. Davon sind nicht nur Verträge im engeren Sinn betroffen, sondern auch Nutzungsbedingungen und sonstige Policies. Als Beispiel für solche Policies sei die Festlegung von verbindlichen Vertrauensniveaus für Identitätsdaten, sog. Levels of Assurance (LoA), genannt.

Ein edu-ID-System muss somit verschiedene rechtliche Voraussetzungen erfüllen, um rechtlich sicher und mit einem hohen Vertrauen seitens der Nutzenden betrieben werden zu können. Darunter fällt mindesten ein Grundschutz-Audit für die gesamte Betriebsumgebung. Ebenfalls muss ein juristisches Gutachten zum Datenschutz im Vorfeld den Umgang mit sämtlichen personenbezogenen Daten im System absichern. Im weiteren Verlauf ist auch eine Zertifizierung des Betriebs der edu-ID-Server durch das Bundesverwaltungsamt möglich.

In diesem Zusammenhang wäre eine Einstufung des edu-ID Systems und der darin geführten Identitäten zum Vertrauensniveau ‚substantiell' durch das BSI vorstellbar[2]. Auf diese Weise wären die nicht-technischen Voraussetzungen für eine später mögliche Integration in das digitale Ökosystem der OZG-Servicekonten gegeben.

2.3 Technisch

Das edu-ID-System muss sich in die bestehenden DFN-AAI einfügen, grundsätzlich also die dort verwendeten technischen Standards und Protokolle unterstützen. Es muss so aufgebaut sein, dass der Betrieb eines IdPs in der DFN-AAI unabhängig von zentralen Komponenten des edu-ID-Systems möglich und auch nicht von deren Verfügbarkeit abhängig ist. Dienstanbieter müssen sich jedoch entscheiden, ob und welche Service Provider direkt mit dem edu-ID System verbunden werden. Ein Mischbetrieb ist u.a. aus Gründen der User Experience nicht vorgesehen.

Der Betrieb des edu-ID-Systems muss über die kommenden Jahrzehnte sichergestellt werden.

3 Kontextabgrenzung

Zur inhaltlichen und technischen Abgrenzung gegenüber ähnlichen und zumindest teilweise funktionsäquivalenten Technologien, Projekten und Initiativen sei auf das *Positionspapier der ZKI AG edu-ID zur Verortung des Konzepts einer edu-ID in der aktuellen Landschaft digitaler*

---

[2] Siehe hierzu die BSI-Richtlinie TR-03107-1 „Elektronische Identitäten und Vertrauensdienste im E-Government",
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03107/TR-03107-1.html

Identitäten in Deutschland verwiesen. Dies betrifft u.a. die im Rahmen der OZG-Umsetzung implementierten Technologien und technischen Komponenten, siehe hierzu auch oben unter 2.

3.1 Fachlicher Kontext

Der fachliche Kontext wird im wesentlichen über die in der edu-ID AG Technik anhand von User Journeys erarbeiteten technischen Rahmenbedingungen definiert.

3.1.1 Onboarding, Erfassung von Userdaten über Web Frontend und andere Schnittstellen

- Akzeptieren der Nutzungsbedingungen und Datenschutzhinweise (proprietär, bei Änderungen zu wiederholender Prozess)
- Manuelle Eingabe (Änderung, Löschung)
    - Validierung E-Mail-Adresse und Mobilfunknummer via Challenge-Response (CR) Verfahren
    - (De-)Registrierung eines zweiten Faktors (implementierungsabhängig)
- Übernahme von Daten aus anderen Identitätsquellen
    - Heimateinrichtung (SAML2, über Einrichtungs-IdP)
    - Schulföderation VIDIS (SAML2, über Landes-IdP)
    - staatliche eID (über angebundenen eIDAS-fähigen eID-Server)
    - Servicekonto Bund/Land (SAML2)
    - Domain-/Plattform-spezifische Identifier wie ORCID (OAuth2, ggf. proprietäre Schnittstellen)
- (Verknüpfung der Identitätsdaten mit Angaben zur Verlässlichkeit des jeweiligen Datums, abhängig von Datenquelle, Validierungsverfahren und Alter - erfolgt automatisch im edu-ID-System)

3.1.2 Nutzung von Diensten, Web-SSO

- Zugriff auf einen mit dem edu-ID-System verbundenen Service Provider (SAML2)
- Einrichtungsauswahl am edu-ID Proxy (SP-Komponente, SAML2)
- ggf. Redirect zum ausgewählten Heimat-IdP (SAML2)
- Authentisierung am Heimat-IdP (SAML2)
- Attributfreigabe am edu-ID Proxy (IdP-Komponente, SAML2)
- (Single) Logout (SAML2)

3.1.3 Identity Management

- Prozesse zur Pflege der Identitäten
- Schnittstelle für Servicepersonal (ggf. proprietär, abhängig von der eingesetzten Software)

- Automatisierte Prozesse (siehe technischer Kontext)
- Recovery-Prozesse bei nicht-kommunizierter Änderung der Kontaktdaten (E-Mail-Adresse, Telefonnummer, ...)

3.1.4 Deprovisionierung

- Prozess zum Löschen von Verknüpfungen und davon abhängigen organisationsbezogenen Daten nach mehrmals fehlgeschlagener Verifikation der Verknüpfung
- Anstoßen von Löschen von Accounts nach mehrmals fehlgeschlagener Verifikation der nicht-einrichtungsbezogenen E-Mail-Adresse (langfristige Deprovisionierungsprozesse)
- Löschen durch aktive Benutzerinteraktion („Konto schließen & löschen“)

3.1.5 Incident Management

- Information der betroffenen Systeme bei Missbrauch einer edu-ID
    - Konformität zu Sirtfi (s. Glossar)
- Erstellen einer Benutzungsordnung mit Kriterien zum Ausschluss bei Missbrauch

3.2 Technischer Kontext

In diesem Abschnitt werden die technischen Kanäle zwischen den Komponenten des edu-ID-System sowie deren Schnittstellen zu externen Systemen dokumentiert. Zu den Komponenten siehe auch unter 5. Bausteinsicht.

Identity Management System

- diverse Management-Komponenten
- Verzeichnis (z.B. LDAP)

edu-ID Portal

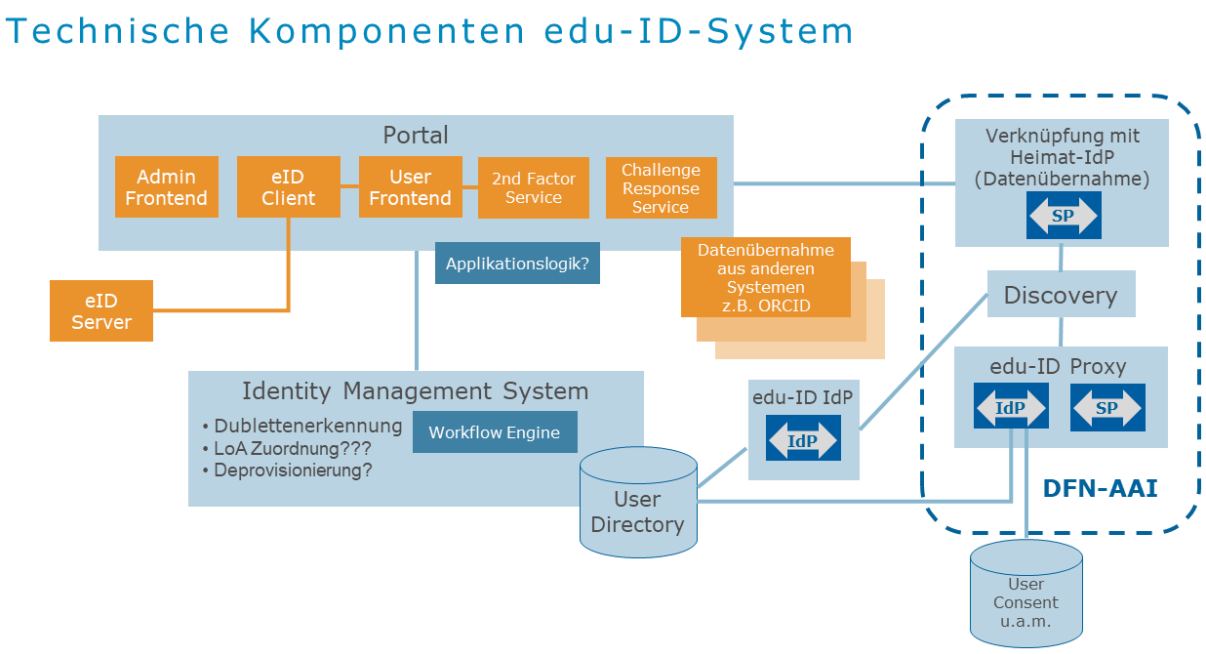
- User Frontend (Self-Service)
- 2nd Factor Service
    - auch als zweiter Faktor für Authentifizierungen an Heimateinrichtungen ohne 2FA nutzbar
- Challenge-Response Service(s)
    - Bsp: Prüfen einer hinterlegten E-Mail-Adresse durch Bestätigung des Empfangs einer verschickten Mail; Bestätigung einer Telefonnummer durch Erhalt einer SMS
- extern: eID-Server (eIDAS)

edu-ID Proxy

- Einrichtungsauswahl / Affiliation Chooser

- Ablauf und Speichern von Entscheidungen siehe unter 6.7.

- IdP-Komponente
- SP-Komponente
- extern: Föderation DFN-AAI
  - Heimat-IdPs (Verbindung zu SP-Kompomente)
  - SPs (Verbindung zu IdP-Komponente)



Das edu-ID-System soll so offen gestaltet werden, dass in späteren Ausbaustufen auf künftige Entwicklungen reagiert werden kann, z.B. in Hinblick auf die Unterstützung des Standards OpenID Connect und weitere Konzepte wie Self-Sovereign Identity (SSI), für die das edu-ID-System als Issuer fungieren könnte.

4 Lösungsstrategie

4.1 Implementierung der Komponenten

Bei der Implementierung des Systems werden offene Standards verwendet. Insbesondere wird zur Kommunikation mit anderen IdPs und SPs SAML2 benutzt. Dazu wird die Shibboleth Software verwendet.

Soweit irgend möglich soll OpenSource-Software verwendet werden.

Alle Komponenten des Systems sind redundant ausgelegt, um Hochverfügbarkeit zu erreichen. Insbesondere ist bei IdM, LDAP und DB darauf zu achten, dass sie in der Lage sind, eine achtstellige Zahl von Benutzern zu verarbeiten.

Die einzelnen Komponenten (IdP/SP, IdM, Benutzer-/Admin-Portal, LDAP, DB) sind voneinander unabhängig und kommunizieren über definierte Schnittstellen bzw. APIs, um ggfs. den Austausch einzelner Komponenten zu ermöglichen.

4.2 Datenstruktur

Zu einem Benutzer werden mehrere Sätze von Attributen gespeichert (vgl. Switch Extended Attribute Model[3]):

- Daten, für deren Quelle der Benutzer selbst verantwortlich ist, ggfs. mit zusätzlicher Verifikation (z.B. durch eIDAS oder OZG-Konto), und weitere Identifier aus Verbindung zu anderen Identitätsdiensten (z.B. ORCID);
- die per pairwise-id verknüpften Identitäten der Heimateinrichtung
- Option für spätere Ausbaustufe: Gruppenmitgliedschaften mit daraus resultierenden Rechten aus anderen Organisationen (als Attribute Query o.ä. zum Authentifizierungszeitpunkt)

Die Attribute werden anhand etablierter Schemata implementiert (z.B. inetOrgPerson, eduPerson, SCHAC, dfnEduPerson). Zu den Attributen werden operationelle Daten wie LoA-, Aktualitäts- und Verlaufsangaben gespeichert.

Die eigentliche edu-ID eines Benutzers muss nicht in einer für Menschen verständlichen Form existieren, sondern kann z.B. als uuid implementiert sein. Von diesem Wert leiten sich dann die Attribute subject-id (samlSubjectID) und pairwise-id (samlPairwiseID) ab, die der edu-ID-Proxy ausliefert. Der Wert der edu-ID selbst kann bei Bedarf als schacPersonalUniqueCode weitergegeben werden. Ein international einheitliches Präfix für den Attributwert soll für diesen Anwendungsfall bei SCHAC normiert werden.

Als Loginname (für den edu-ID-eigenen Login) wird eine der gespeicherten Mailadressen verwendet.

4.3 Umsetzungsphasen

Als erste Use Cases sollen die Verwendung der edu-ID für Nationallizenzen, Staatsbibliotheken, Zugriff auf zentrale Ressourcen und „Homeless Users“ (Use Cases 3.6, 3.7, 3.8 und 3.10 der Liste der Use Cases[4]) implementiert werden.

Die ersten Use Cases sollen in einer Projektphase 1 umgesetzt werden, wobei für Projektphase 1 die folgenden Umsetzungsschritte geplant sind:

1. Proof of Concept bis Ende 2022
2. Pilotphase bis Ende Q2 2023
3. Sukzessive ansteigender Produktivbetrieb

---

[3] https://www.switch.ch/edu-id/docs/services/attributes/extended-model/

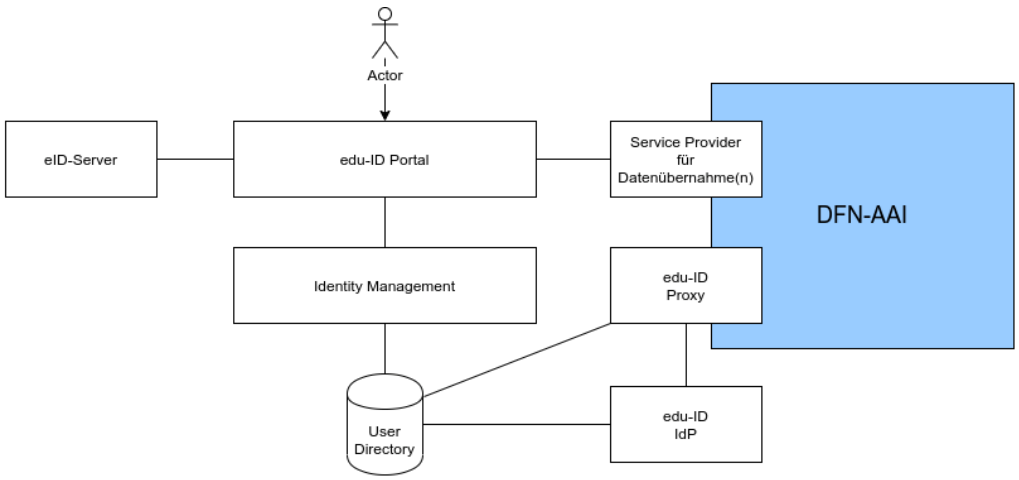
[4] https://doku.tid.dfn.de/de:aai:eduid:usecases

Teil von Projektphase 1 sind auch organisatorische Entscheidungen, beispielsweise für bestimmte Entwicklungsprozesse oder Delegation bestimmter Aufgaben an andere Stakeholder inkl. der Festlegung eines Betriebskonzepts und der Klärung rechtlicher Fragen.

In weiteren Projektphasen sollen dann weitere Use Cases analysiert und umgesetzt werden.

5 Bausteinsicht

5.1 Whitebox Gesamtsystem



5.1.1 Begründung

Es wurde bewusst ein möglichst modularer Ansatz gewählt, der - wo immer möglich - auf offenen Standards und normierten Schnittstellen beruht. Auf diese Weise können einzelne Komponenten weitestgehend unabhängig voneinander implementiert werden. Der Tausch einzelner Komponenten auch im laufenden Betrieb wird auf diese Weise deutlich erleichtert.

5.1.2 Enthaltene Bausteine

Das **edu-ID Portal** bzw. einige der darin zusammengefassten Komponenten interagiert mit folgenden Komponenten:

- eID-Server
- Identity Management System (IdM) mit angeschlossenem oder integriertem User Directory
- einem edu-ID-internen Service (Provider) für Datenübernahmen aus externen Systemen (im Rahmen der edu-ID-Registrierung, sowie zur Datenverifizierung)

Zu Details siehe jeweils unten (Ebene 3).

Der **edu-ID Proxy** bzw. einige der darin zusammengefassten Komponenten interagiert mit folgenden Komponenten:

- edu-ID-IdP: für Nutzende ohne sonstigen Heimat-IdP die einzige Authentifizierungsquelle
- User Directory (liefert edu-ID-interne Attribute sowie Verknüpfungen zu Heimateinrichtungen)

Zu Details siehe jeweils unten (Ebene 3 - Portal und angeschlossene Komponenten).

5.1.3 Wichtige Schnittstellen

5.1.3.1 SAML2

Sämtliche AAI-fähigen Komponenten werden (intern) über SAML2 angesprochen

- Service Provider
- Identity Provider
- Discovery Service

Siehe Ebene 3 - Portal und angeschlossene Komponenten.

Der Einsatz von Shibboleth wird stark empfohlen, auch, aber nicht nur, auf Grund der ubiquitären Verbreitung innerhalb der DFN-AAI.

Offen: Anbindung eID-Server an eID-Client (unkritisch, da vermutlich vom selben Anbieter)

5.1.3.2 LDAP

Das User Directory wird in jeder Richtung über LDAP-Schnittstellen angesprochen. Die Nutzung von OpenLDAP liegt nahe.

5.1.3.3 Anbindung Identity Management System an Portal

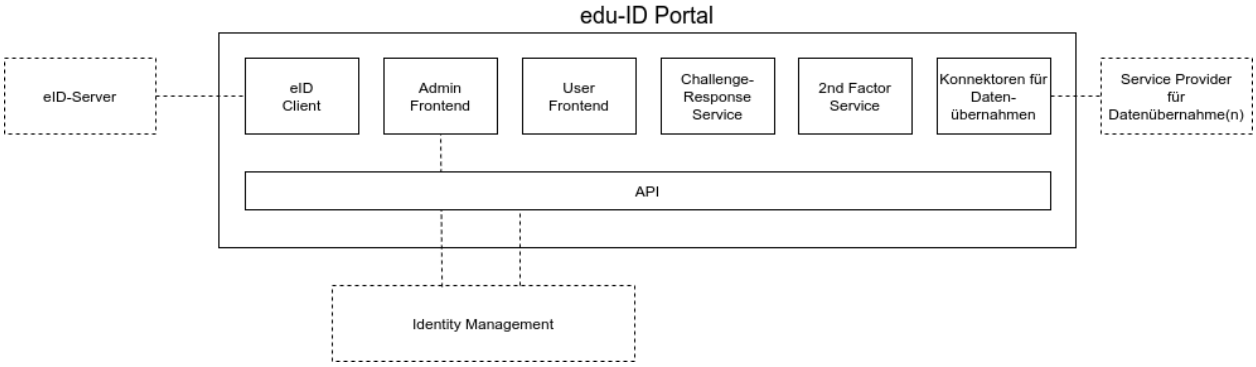
Offen. Produktabhängig.

5.1.3.4 Datenbank

Für die Speicherung von Sessions, User-Consent und Persistent-IDs wird eine relationale Datenbank eingesetzt.

5.2 Ebene 2

5.2.1 edu-ID Portal



Das Portal dient als Integrationsplattform sowohl für Komponenten, die Interaktion mit Nutzer:innen ermöglichen/erfordern, als auch als Schnittstelle zu (externen) Diensten und Komponenten, die von interaktiven Prozessen angesprochen werden. Ermöglicht wird die technische Integration durch eine API-Schicht, die alle Komponenten miteinander verbindet.

Schnittstellen:

Extern:

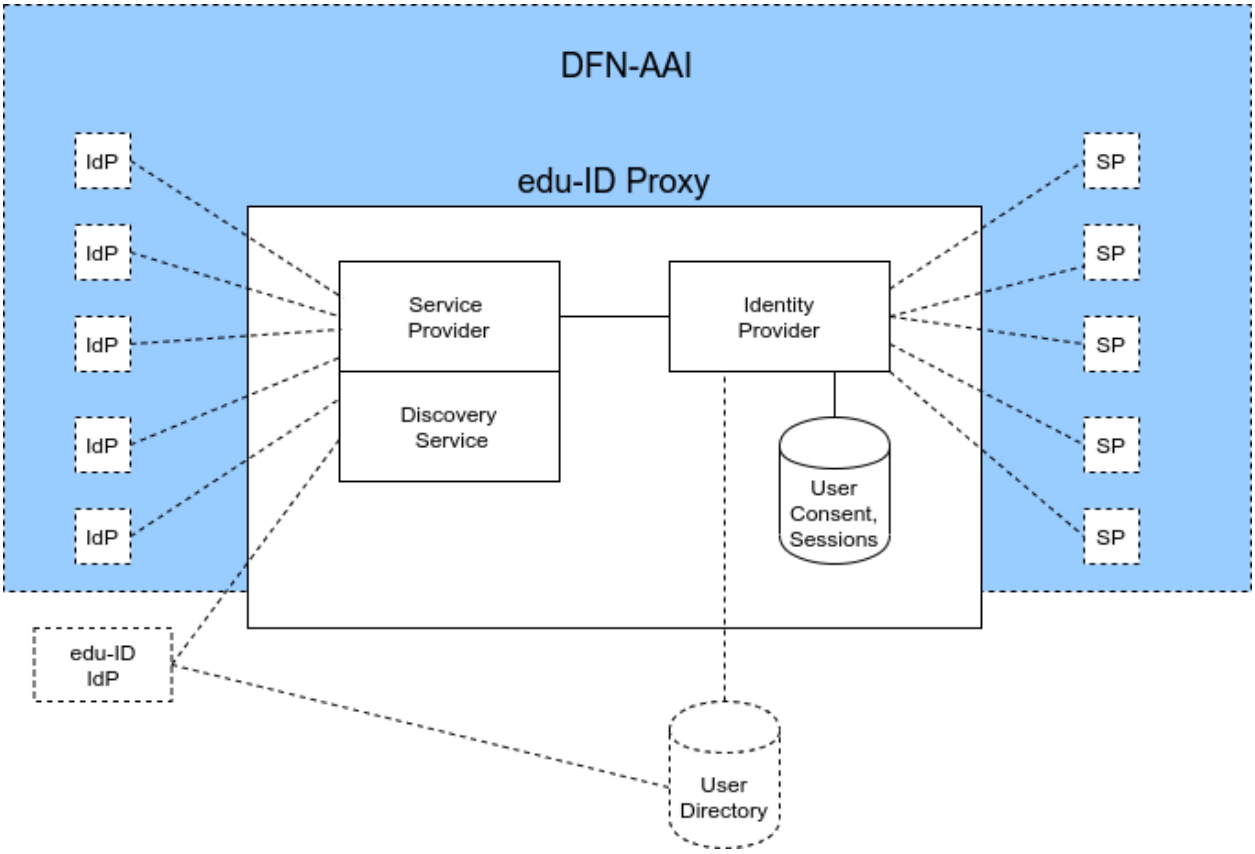
- eID-Server (abhängig von Anbieter)
- Service Provider für Datenübernahmen (SAML)
- Identity Management System (abhängig von Anbieter)

Intern:

- API und/oder Framework, um die einzelnen Komponenten miteinander zu verbinden

Die API bzw. das gewählte Framework muss in der Lage sein, die einzelnen Komponenten des Portals auf eine Weise zu integrieren, die auf Seite der Komponenten nur minimale Anpassungen erfordert und die es ermöglicht, einzelne Komponenten bei Bedarf auszutauschen, ohne dass andere Komponenten deswegen angepasst werden müssen.

5.2.2 edu-ID Proxy



Beim edu-ID-Proxy handelt es sich um einen SP-IdP-Proxy, der gegenüber Service Providern in der Föderation als Identity Provider agiert und gegenüber Identity Providern in der Föderation als Service Provider. In der letztgenannten Funktion delegiert er die Authentifizierung an einen Heimat- oder ggf. den edu-ID-IdP und leitet die vom jeweiligen IdP übertragenen Attribute an den anfragenden SP in der Föderation weiter, sofern der/die Nutzer:in der Übertragung zustimmt.

Schnittstelle(n):

- SAML2, zu einem späteren Zeitpunkt auch OpenID Connect

- Schnittstelle zu relationalen Datenbanken, SQL (Consent, pairwise-id, Session)

5.3 Ebene 3 - Portal und angeschlossene Komponenten

5.3.1 eID-Client

Die eID-Client Anwendung ermittelt die über den neuen Personalausweis, den elektronischen Aufenthaltstitel oder andere eIDAS-konforme IDs verfügbaren Nutzendendaten und kann somit sowohl zum Anlegen eines edu-ID-Accounts als auch zur nachträglichen Verifizierung der entsprechenden Daten genutzt werden. Hierzu muss sie mit einem zertifizierten eID-Server kommunizieren.

Schnittstelle(n)

- Noch offen.

5.3.2 eID-Server

Der eID-Server führt die eigentliche Verifizierung des Ausweis-Tokens durch und überträgt die hinterlegten Nutzendendaten an den Client.

Schnittstelle(n):

- siehe eID-Client

Offene Punkte/Probleme/Risiken

- Kann bei Governikus / D-Trust gemietet werden, es existiert auch eine Variante, für die kein eigenes Berechtigungszertifikat erforderlich ist, vgl. https://www.governikus.de/ausweisident-eid-service
  Andere (Open-Source-) Implementierungen stehen ggf. ebenfalls zur Verfügung (siehe bspw. die entsprechende Liste auf GitHub[5]).

5.3.3 Admin Frontend

Das Admin Frontend ermöglicht es dem hierzu berechtigten Personal, das an das Portal angeschlossene Identity Management System zu bedienen, zunächst bei der Zusammenführung von Dubletten[6]. Zudem erlaubt das Frontend die Verwaltung des 2nd-Factor-Service.

Personen, die End-User-Support leisten, müssen Read-Only-Rollen zugewiesen werden.

Weitere Funktionalitäten werden im Verlauf der Entwicklung des edu-ID-Systems spezifiziert, z.B. Support für IdP- und SP-Betreiber.

Schnittstelle(n)

- definiert durch die o.g. API

---

[5] https://github.com/topics/eid

[6] https://doku.tid.dfn.de/de:aai:eduid:ag4

5.3.4 User Frontend

Das User Frontend erlaubt es Nutzenden, edu-ID-Accounts anzulegen, weitere Daten zu hinterlegen, Daten zu validieren (eID-Client, Challenge-Response), den Account mit anderen Identitäten (sowohl andere [externe] Identifikatoren, als auch andere Zugehörigkeiten zu Heimateinrichtungen) zu verknüpfen, einen zweiten Faktor zu registrieren, gespeicherte Voreinstellungen zurückzusetzen (z.B. den bevorzugt zur Authentisierung verwendeten IdP), sowie den Account zu löschen. Weiterhin sind über das User Frontend Hilfetexte bzw. eine Online-Dokumentation abrufbar. Hierzu gehören auch Kontaktinformationen für Support-Anfragen sowie juristisch vorgeschriebene Informationen wie Impressum und Datenschutzerklärung.

Außerdem müssen vor dem Anlagen eines Accounts sowie bei etwaigen Änderungen die für die Nutzung des edu-ID-Systems geltenden Nutzungsbedingungen akzeptiert werden. Die diesbezüglichen Informationen müssen langfristig und sicher archiviert werden.

Schnittstelle(n)

- definiert durch die o.g. API

5.3.5 Challenge-Response-Service

Der Challenge-Response-Service dient der Validierung von manuell eingegeben E-Mail-Adressen und Mobilfunknummern.

Schnittstelle(n)

- definiert durch die o.g. API

5.3.6 2nd-Factor-Service

Zur Absicherung des edu-ID-Accounts sind die registrierten Personen verpflichtet, einen zweiten Faktor für die Anmeldung am User Frontend sowie am edu-ID-IdP zu hinterlegen. Der 2nd-Factor-Service ermöglicht die Ausstellung und Verwaltung solcher Faktoren (zunächst TOTP, SMS). Siehe auch die Ergebnisse der Arbeitsgruppe Zweiter Faktor[7]. Falls der zweite Faktor von der Heimateinrichtung beigesteuert wird, soll dies für den Login in edu-ID akzeptiert werden (SAML Authentication Context Class Reference, ACR[8]).

Perspektivisch soll der 2nd-Factor-Service auch für den Login in beliebigen SPs verwendet werden können.

Schnittstelle(n)

- definiert durch die o.g. API
- Shibboleth-Plugin für edu-ID-IdP

5.3.7 Konnektoren und Service Provider für Datenübernahmen

Diese Komponenten ermöglichen es den Nutzenden, einen edu-ID Account anhand externer Identitätsquellen anzulegen bzw. diesen mit Daten aus externen Identitätsquellen anzureichern

---

[7] https://doku.tid.dfn.de/de:aai:eduid:ag6

[8] https://docs.oasis-open.org/security/saml/v2.0/saml-authn-context-2.0-os.pdf

oder mit einer externen Identität zu verknüpfen (Account Linking), z.B. ORCID und insbesondere die Heimateinrichtungen. Geplant sind aktuell ein Konnektor für SAML2-fähige Identity Provider sowie eine entsprechende Schnittstelle zum ORCID-System.

Schnittstelle(n)

- zum Portal: definiert durch die o.g. API
- SAML2
- Föderation (DFN-AAI)
- Plattformspezifisch, z.B. OIDC, OAuth2

5.3.8 Identity Management System

Ermöglicht Nutzenden und Admin-Personal die Verwaltung der edu-ID-Accounts bzw. der darüber definierten Identitäten und den damit verbundenen Nutzendendaten. Unterstützung der üblichen IdM-Prozesse sowie die Speicherung von Meta-Informationen wie Art und Zeitstempel der Validierung einzelner Daten. Weitere Anforderungen: Prozess-Engine (z.B. BPMN), Unterstützung beim Identity-Matching.

Schnittstelle(n)

- definiert durch die o.g. API
- SCIM
- LDAP

5.3.9 User Directory / Verzeichnisdienst

Benötigt, sofern nicht im Lieferumfang des Identity Management System enthalten.

Schnittstelle(n)

- LDAP

5.3.10 Schnittstellen: Portal API

Siehe oben zu Ebene 2.

5.4 Ebene 3 - AAI-Proxy und angeschlossene Komponenten

5.4.1 IdP (Proxy-IdP)

IdP-Komponente des Proxy, wird mit Shibboleth-Software umgesetzt. Siehe oben unter Ebene 2.

Schnittstelle(n)

- SAML2
- OIDC (später)
- SQL, DB-Anbindung
- LDAP (Nutzerverzeichnis edu-ID-IdM)

5.4.2 SP

SP-Komponente des Proxy, stellt Verbindung zu IdPs der Heimateinrichtungen her, wird mit Shibboleth-Software umgesetzt. Siehe oben unter Ebene 2.

Schnittstelle(n)

- SAML2
- Föderation (DFN-AAI)

5.4.3 edu-ID-IdP

Separater Identity Provider (Shibboleth), der an das Nutzerverzeichnis des edu-ID-IdM angeschlossen ist. Dient als alleinige Authentifizierungsquelle für Nutzende ohne Einrichtungs-/Heimat-IdP.

Schnittstelle(n)

- SAML2
- SQL, DB-Anbindung
- LDAP (Nutzerverzeichnis edu-ID-IdM)

5.4.4 Discovery

Dient der Auswahl der Authentifizierungsquelle durch den/die jeweilige:n Nutzer:in an der SP-Komponente des Proxy. Der ausgewählte IdP dient in der Regel auch als Attributquelle. Zur Auswahl stehen teilnehmende IdPs aus der DFN-AAI sowie der edu-ID-IdP.

Schnittstelle(n)

- SAML2

Es soll IdP-Hinting (ein SP signalisiert dem edu-ID-Proxy, welche Heimateinrichtung(en) möglich sein sollen) unterstützt werden. Siehe Richtlinie AARC-G049[9].

Es soll eine intelligente Vorauswahl/Speicherung der Auswahl unterstützt werden, die über das edu-ID-Portal verwaltet werden kann.

5.4.5 DB für User Consent, pairwise-ids, Sessions

Relationale Datenbank, die der Ablage der jeweils letzten User Consent Entscheidungen sowie von Session-Informationen dient.

Schnittstelle(n)

- SQL, DB-Anbindung

5.4.6 Auditing-System

Möglicherweise, insbesondere wenn dies durch rechtliche Anforderungen (DSGVO, Sirtfi, KRITIS, etc.) vorausgesetzt wird, soll ein zentrales Auditing-System etabliert werden. Es muss zunächst evaluiert werden, ob diese auch durch ein gesondertes System umgesetzt werden können, z.B. Graylog o.ä. Die Auswertung der Daten erfolgt ausschließlich zur Sicherstellung der Betriebssicherheit (Security Operations) und zur Erfüllung gesetzlicher Anforderungen.

6 Laufzeitsicht

Die folgenden Punkte sollen für den PoC und den Piloten bereitstehen. Weitere Ausbaustufen sind weiter unten im Dokument aufgeführt.

---

[9] https://aarc-community.org/wp-content/uploads/2019/04/AARC-G049-A_specification_for_IdP_hinting-v6.pdf

6.1 Onboarding

Bislang habe ich noch keine edu-ID und möchte mir gerne eine beschaffen. Dazu gehe ich auf das edu-ID-Portal.

6.1.1 Registrierungsprozesse

- Im edu-ID-Portal gibt es einen Button zur Registrierung.
- Auf der Registrierungsseite gibt es eine Auswahlmöglichkeit zwischen Formular, Onboarding per Heimateinrichtung, eID, etc.

6.1.1.1 Per Registrierungsformular

- Auswahl Formular.
- Eingabe aller verpflichtenden und optionalen Attribute aus dem Datenmodell, sowie selbstgewähltes Passwort
- Zustimmung zu den aktuellen Terms of Use (ToU)
- Als primäre E-Mail-Adresse muss eine private Adresse eingegeben werden.
    - Die Validierung (CR) manuell eingegebener E-Mail-Adressen ist verpflichtend, um den Registrierungsprozess endgültig abzuschließen.
- Bei Erfolg wird eine edu-ID und davon abgeleitete subject-Id (samlSubjectID) (Verfahren zur Erzeugung muss noch geklärt werden) erzeugt und die Daten des Accounts mit niedrigem LoA angelegt
- Weiterleiten an das Portal

6.1.1.2 Per Login bei der Heimatreinrichtung

- Discovery-Service mit allen für edu-ID geeigneten IdPs der DFN-AAI
- Auswahl Heimateinrichtung.
- Authentifizierung beim ausgewählten IDP
- Weiterleitung auf Formular wie in 6.1.1.1, nur dass die vom IdP gelieferten Attribute vorausgefüllt und read-only sind
- Eingabe aller übrigen verpflichtenden und optionalen Attribute aus dem Datenmodell, sowie selbstgewähltes Passwort
    - die primäre E-Mail-Adresse muss ebenfalls als private E-Mail-Adresse nachgetragen werden
- Zustimmung zur aktuellen ToU
- Validierung von E-Mail-Adresse verpflichtend um den Registrierungsprozess endgültig abzuschließen
- Bei Erfolg wird eine edu-ID und davon abgeleitete subject-ID (samlSubjectID) (Verfahren zur Erzeugung muss noch geklärt werden) erzeugt und die Daten des Accounts mit niedrigem LoA angelegt

- Weiterleiten an das Portal

6.1.2 Login am Proxy mit einer Heimateinrichtungs-Identität, die nicht im System verknüpft ist

- Zugriff auf einen SP
- Weiterleitung zum edu-ID-Proxy
- Auswahl einer Heimateinrichtung beim Discovery-Service
- Login bei der Heimateinrichtung
- edu-ID-Proxy stellt fest, dass keine edu-ID mit diesem Identifier verknüpft ist
- Auswahlseite:
    a) Neue edu-ID anlegen: Weiter in 6.1.1.2., vierter Punkt
    b) Mit vorhandener edu-ID verknüpfen: Weiter in 6.3.1

6.2 Dublettenerkennung

Nicht Teil des PoC, wird in einer späteren Ausbaustufe behandelt.

6.3 Verknüpfen von weiteren Heimateinrichtungs-Identitäten

6.3.1 Initiiert über Portal

- Login am edu-ID-Portal (unabhängig ob per edu-ID-Portal-Credentials oder per Credentials der Heimateinrichtung [HE])
- Menüpunkt “Verknüpfung mit Heimateinrichtung hinzufügen” (oder “Weitere Identität hinzufügen” oder so...)
- Der SP zur Datenübernahme zeigt Discovery an
- Antwort vom gewählten IdP wird validiert
- Daten gegenüberstellen
- Rückfrage: Willst Du wirklich?
- Eindeutiger Identifier der Heimateinrichtung (HE) schon verknüpft?
    - Ja: Hinweis, dass Link schon mit anderem Account besteht, ggf. Duplikat auflösen
    - Nein: Verknüpfung anlegen

6.3.2 Initiiert über Login

- Start wie in 6.1.2, ansonsten identisch zu 6.3.1

6.4 Validieren des Accounts

6.4.1 über Heimatreinrichtung

- Login am edu-ID-Portal (unabhängig ob per edu-ID-Portal-Credentials oder per HE-Credentials)

- Menüpunkt “Daten validieren über HE”
- Eine der verknüpften HE auswählen (Je ein Button pro HE)
- Dann Attribute Query (AQ) im Hintergrund
- Anzeige der empfangenen Daten
- Entsprechung zu bestehenden Daten vorhanden?
    - JA: Validierung merken, Haken dran
    - NEIN: Anzeige diff. Rückfrage “Daten übernehmen?”
        - JA: Daten übernehmen, Validierungshaken setzen
        - NEIN: Daten nicht übernehmen, Kein Validierungshaken

6.5 Verifizieren der Kontaktinformationen

6.5.1 E-Mail-Adresse

Eine (erste) E-Mail-Adresse wird bei der Registrierung per CR validiert.

Bei Änderung oder dem Hinzufügen einer weiteren E-Mail-Adresse ebenfalls CR, sonst ist die Änderung nicht wirksam.

Es soll die Möglichkeit geben eine der Adressen als primäre E-Mail-Adresse für PW-Reset oder Notifications zu setzen (evt. mit erneutem CR)

6.5.2 Mobilfunknummer

Es können mehrere Mobilfunknummern hinzugefügt werden.

- Eingabe der Nummer
- Token wird verschickt
- Eingabe des Tokens
- Nummer wird hinzugefügt und ist direkt verifiziert

6.6 Self-Service-Funktionen

6.6.1 Verwalten von 2FA-Credentials

Mobilfunknummer

- Nach 6.5.2 sind alle Mobilfunknummern sofort als Zweitfaktoren einsetzbar.

TOTP

- Menüpunkt “Neues TOTP-Gerät koppeln”
- QR-Code generieren und anzeigen
- CR

- TOTP-Gerät ist gekoppelt und aktiv

Entfernen von TOTP-Tokens erlauben, wenn mindestens ein weiteres Token registriert ist. Möglicherweise muss eine Lösung für einen begrenzten Übergangszeitraum gefunden werden.

Szenario: 2FA ist aktiv, Zweitfaktor geht verloren, mit Recovery Code am System anmelden, neuen Zweitfaktor registrieren, CR, alten Zweitfaktor entfernen. Alter Zweitfaktor wiedergefunden, kann neu registriert werden.

6.6.2 Verwalten von Stammdaten

Grundsätzlich sind alle Stammdaten vom Nutzer änderbar. Wenn ein Datum jedoch von dem validierten abweicht, verliert dieses den Validationsstatus (mit entsprechender Warnung)

6.6.3 Verwalten von anderen Identifiern

Analog zu 3. Verknüpfen von weiteren Heimateinrichtungs-Identitäten

6.6.4 Verwalten der Vorauswahl

Für PoC ist nur die Verwaltung der Discovery-Service-Vorauswahl angedacht.

Es muss ermöglicht werden, den/die vom Discovery Service (DS) gesetzten Cookie(s) zu löschen.

6.6.5 Passwortfunktionen

Passwort ändern, wenn eingeloggt

- Altes Passwort und neues Passwort (2x) eingeben
- Per 2FA verifizieren
- Passwort-Policy beachten

Passwort vergessen (Link auf edu-ID-IdP-Loginseite und Portal)

- Eine der hinterlegten, verifizierten E-Mail-Adressen eingeben
- Per 2FA verifizieren (falls vorhanden)
- CR an diese Adresse
- Maske 2x neues PW
- Info an alle hinterlegten E-Mail-Adressen
    - Wenn Du das nicht warst, wende Dich sofort an den Support
- Passwort-Policy beachten

6.6.6 Auskunftsansprüche

Gemäß DSGVO:

- Welche Daten sind über mich gespeichert?

- Auch: Welche externen IDs habe ich verknüpft?
- Exportfunktion CSV oder JSON (Stammdaten und verknüpfte Einrichtungen/IDs)
- Und auch: Welche Daten haben die Heimateinrichtungen über mich gespeichert
  Knopf drücken, AQs werden an die HEs gefeuert, Daten werden tabellarisch aufbereitet angezeigt
    - evtl. Möglichkeit per Formular Anfrage an HE zu senden, dass Daten aktualisiert werden (Kontakt aus Metadaten des DFN evtl. als neue Kontakt-Kategorie)
- Welche Attributfreigaben sind derzeit eingerichtet?
    - basierend auf Informationen aus der Consent-DB des IDP
- Welche Vorauswahlen sind derzeit gesetzt (siehe 6.7)?
    - Discovery (vermutlich erstmal nicht, da wir nur das Löschen des Cookies am DS erlauben)
    - Affiliation (später)
- Terms of Use (ToU)
    - Aktuelle Anzeigen
        - Eigener Menüpunkt „ToU anzeigen“
        - Text der aktuellen ToU anzeigen und Datum der Zustimmung
    - Neuen Zustimmen
        - Asynchrones Vorgehen: Neue ToUs ankündigen (über hinterlegte primäre E-Mail-Adresse)
        - Im Portal: Neuen ToU zustimmen (Anzeigen + Button „Ja, ich will“)
        - Bei der nächsten Anmeldung am Proxy-IdP neue ToU anzeigen und Zustimmung einholen oder „Später“-Button

6.6.7 Löschen

- User kann nach Anmeldung im Portal auf den Button “edu-ID löschen” klicken
- Warnung, was alles passiert
- Rückfragen
- Nochmal volle AuthN: Passwort, 2FA wenn vorhanden
- Logout aus dem System
- “Verbrannte” edu-IDs merken, um Kollisionen zu verhindern

Recovery eines gelöschten edu-ID-Kontos ist nicht möglich. Gelöscht ist gelöscht.

6.6.8 Support

- Kontaktformular

- Evtl. E-Mail-Link, inkl. Systemdaten wie Angabe des Benutzers
- Im Hintergrund Ticketsystem

6.6.9 Recovery

Wenn das erste 2FA-Token registriert wird, werden auch Recovery-Codes erzeugt und einmalig angezeigt.

Es muss eine Möglichkeit geben, neue Recovery-Codes zu generieren und anzuzeigen. Wie oft? RecCodes sollen nicht zur TAN-Liste verkommen.

Beim PW-Reset sind alle hinterlegten E-Mail-Adressen nutzbar.

Recovery eines gelöschten edu-ID-Kontos ist nicht möglich. Gelöscht ist gelöscht.

6.7 Login am Proxy

SP schickt AuthnRequest an edu-ID-Proxy. Diese SPs sollen für dt. IdPs nur am edu-ID-Proxy hängen und nicht parallel auch über die DFN-AAI direkt IdPs anbinden.

6.7.1 Auswahl Heimateinrichtung

Der edu-ID-Proxy kann eine Authentifizierungssession haben, die dann verwendet wird.

Wenn keine Session existiert, muss der Proxy einen IdP zur Authentifizierung bestimmen und hat dafür folgende Möglichkeiten (“Discovery”):

- Der SP kann eine Liste von IdPs mitschicken, die ausschließlich zur Auswahl angeboten werden (IdP-Hinting).
- Bestehendes Ergebnis der Discovery-Vorauswahl (bei einer vorherigen Authentifizierung wurde ein Haken bei “Auswahl merken” gesetzt, diese kann über das Portal zurückgesetzt werden.)
- Anzeige des Discovery-Service mit allen angebundenen IdPs der DFN-AAI, die für edu-ID qualifiziert sind, falls vorhanden mit den zuletzt genutzten IdPs oben.

Bei erfolgreichem Login gegen eine HE soll diese Verknüpfung im edu-ID-System mit dem aktuellen Timestamp markiert werden (“lastUsed”).

6.7.2 Affiliations

Nicht im PoC

6.7.3 User-Consent

Standardverhalten wie bei Shibboleth-IdPs.

6.7.4 Terms of Use (ToU)

Akzeptieren der bei der Registrierung gültigen ToU im Portal, wobei diese dann auch für den edu-ID-Proxy als bereits akzeptiert gespeichert werden sollen.

Wenn neue ToU veröffentlicht werden, soll der Proxy für einen Übergangszeitraum die neuen ToU anzeigen und die Optionen “Jetzt nicht” und “Akzeptieren” anbieten. Nach diesem Zeitraum

wird die Zustimmung verpflichtend, Solange die ToU nach diesem Datum nicht akzeptiert werden, wird der Account solange gesperrt, bis die ToU akzeptiert wurden. Nach Zeitraum X (Vorschlag: 1 Jahr) wird der Account gelöscht.

6.8 Single Logout (SLO)

Nicht im PoC

6.9 Attribute-Queries (AQ)

6.9.1 Delegierte Attribute-Queries (Simples Attribut-Modell)

SP schickt AQ an edu-ID-Proxy (Identifier: Proxy-pairwise-id)

Lookup Proxy-pairwise-id gegen HE-pairwise-id (dies ist die bei der letzten Authentifizierung an diesem SP genutzte HE)

AQ an HE delegieren anhand der HE-pairwise-id

AQ an SP beantworten

Bei erfolgreichem AQ gegen eine HE soll diese Verknüpfung im edu-ID-System mit dem aktuellen Timestamp markiert werden ("lastUsed")

6.9.2 Bei Auswahl einer anderen Affiliation im Affiliation-Chooser als den authentifizierenden IdP

Nicht im PoC

6.9.3 Bei periodischer Prüfung, ob eine Verknüpfung zu einer HE noch existiert (siehe 6.11)

Regelmäßiger Hintergrundprozess, um zu prüfen, ob ein Nutzer bei der / den verknüpften Einrichtung/en noch existiert (z.B. 6 Monate nach letztem last-used am edu-ID-System [EIS]). Eine Abmeldung der:s Nutzer:in an der Heimateinrichtung kann nicht aktiv an das EIS weitergegeben werden. Die HE kann eine Abmeldung an das EIS melden, dort kann die Verknüpfung zur HE aufgehoben werden (nach entsprechender Benachrichtigung an den/die Nutzer:in und einer Wartezeit). Wenn gar keine Verknüpfungen mehr bestehen, kann nach einer weiteren Wartezeit der Löschprozess im EIS angestoßen werden.

6.9.4 Kombinieren von Datensätzen aus verschiedenen (allen verknüpften) HE

Nicht im PoC

6.10 Admin-Funktionen

Grundfunktionen:

- Grundlegende Funktionen eines IAM-Systems insb. Suchen, Sperren und Entsperren über die GUI, so dass dies auch vom 1st-Level-Support übernommen werden kann
- Funktionen im Rahmen des Funktionsumfang des implementierten IdM-Systems

Weitere Anforderungen können im Rahmen des PoC und Pilotbetriebs entstehen.

6.11 Hintergrundprozesse

6.11.1 Regelmäßige Validierung

Ein edu-ID-Account hat einen Wert “lastUsed”. Dieser wird entweder beim Nutzen einer verknüpften HE (AQ oder Authn) aktualisiert, oder wenn die edu-ID mit den lokalen Logindaten verwendet wird.

Wenn “lastUsed” eine bestimmte Grenze (1 Jahr?) überschreitet, wird der Nutzer per E-Mail an die primäre E-Mail aufgefordert, den Account zu bestätigen.

Nach einem weiteren Zeitraum (6 Monate?) werden alle hinterlegten Adressen benachrichtigt.

Bei keiner Reaktion nach weiteren 6 (?) Monaten wird der Account gelöscht.

6.11.2 Periodische Prüfung ob Affiliation noch existiert (AQ)

Analog zu 6.9.3.

6.11.3 Änderungen der ToU an alle Nutzer schicken

Eine Aktualisierung der ToU steht an, in einer Übergangszeit soll eine Zustimmung zu den neuen ToU schon möglich, aber noch nicht verpflichtend sein. Die Info über neue ToU wird über die als primär markierte E-Mail-Adresse verschickt.

6.12 Attributprofile

6.12.1 Heimateinrichtung (HE) an edu-ID-Proxy

Attributname	Verpflichtend	Anmerkungen
pairwise-id	ja	Verknüpfung zu IdP der HE
eduPersonAffiliation	ja	
schacHomeOrganization	ja	
eduPersonAssurance	ja	
mail	ja	
displayName	ja	
eduPersonEntitlement	nein	
schacPersonalUniqueCode	nein	z.B. European Student Identifier (ESI) oder Matrikelnummer

o	nein	

6.12.2 Heimateinrichtung (HE) an Datenübernahme-SP

Attributname	Verpflichtend	Anmerkungen
pairwise-id	ja	Verknüpfung zu IdP der HE
schacHomeOrganization	ja	
eduPersonAssurance	ja	
mail	ja	
sn	ja	
givenName	ja	
displayName	nein	
schacPersonalUniqueCode	nein	z.B. European Student Identifier (ESI) oder Matrikelnummer
schacCountryOfResidence	nein	Zugriff auf Nationallizenzen
schacPlaceofBirth	nein	
schacDateOfBirth	nein	
o	nein	Anzeige der Affiliation im EIS
postalAddress	nein	

6.12.3 edu-ID-Proxy zu SPs in DFN-AAI

Attributname	Verpflichtend	Ursprung des Attributs	Anmerkungen
pairwise-id	ja	EIS	Abgeleitet von edu-ID
subject-id	nein	EIS	Abgeleitet von edu-ID
eduPersonAffiliation	ja	HE	

schacHomeOrganization	ja	HE	
eduPersonAssurance	ja	EIS	
mail	nein	HE/EIS	
displayName	nein	HE/EIS	
eduPersonEntitlement	nein	HE	
schacPersonalUniqueCode	nein	HE (EIS)	z.B. European Student Identifier (ESI) oder Matrikelnummer
o	nein	HE	
schacCountryOfResidence	nein	EIS	Für Zugriff auf Nationallizenzen

Angedacht ist, dass die HEs alle verfügbaren Attribute des (noch zu etablierenden) Kerndatensatzes an den Proxy übermitteln; der Proxy filtert anschließend anhand der Liste der vom SP benötigten Attribute (fest verdrahtet oder per Definition in den Metadaten).

6.13 Levels of Assurance (LoA)

Abhängig von den Diskussionen bzgl. der Attribute.

Vorüberlegungen siehe https://doku.tid.dfn.de/de:aai:eduid:loa

6.14 Weitere Schritte - Ausbaustufen

Siehe hierzu die noch nicht und niedriger priorisierten Aspekte der User Journeys im Anhang (Abschnitt 11).

6.14.1 Dublettenerkennung

Vorschlag; Bei allen Onboarding-Prozessen soll eine Dublettenerkennung basierend auf einem noch zu definierenden Algorithmus stattfinden. Bei Überschreiten einer bestimmten Übereinstimmungsquote mit einem bestehenden Nutzer soll der Nutzer im Registrierungsprozess über eine solche Übereinstimmung informiert und eine E-Mail an die hinterlegte E-Mail-Adresse des gefundenen Accounts geschickt werden

Muss noch besprochen werden

7 Verteilungssicht

Die Details werden im Rahmen des PoC und ggf. Pilotbetriebs von den für den Betrieb zuständigen Organisationen erarbeitet und definiert.

8 Querschnittliche Konzepte

8.1 i18n

Es sind folgende Sprachen vorgesehen:

- Deutsch
- Englisch

8.2 Betriebskonzepte

Werden im Rahmen des PoC und Pilotbetriebs erarbeitet.

8.3 Architektur- und Entwurfsmuster

Werden von den umsetzenden Organisationen festgelegt.

8.4 Barrierefreiheit

Muss bei der Umsetzung eingeplant und bedacht werden.

8.5 User Experience

Während des PoC soll eine dedizierte Arbeitsgruppe (die nicht nur aus Techniker:innen besteht) die Entwicklung der User Experience begleiten. Die UX soll während der Pilotphase dann evaluiert werden. Zusätzlich können auch Hilfetexte und weitere Dokumentationen die UX verbessern.

8.6 Sicherheit

Ein Sicherheitskonzept muss erstellt werden und vom DFN-CERT abgenommen und über geeignete Maßnahmen (z. B. Pentest) überprüft werden.

8.7 Dokumentation

Es muss Support-Material für angeschlossene Systeme erstellt werden.

9 Risiken

9.1 Technische Risiken

- Single Point of Failure: Das edu-ID-System soll zum Login an einer Vielzahl von Diensten verwendet werden. Wenn es ausfällt, sind all diese Dienste nicht benutzbar. Deshalb ist Redundanz der einzelnen Komponenten unbedingt erforderlich (siehe Abschnitte 1.2, 4.1).

- Durch die Verwendung an vielen Diensten und wegen der gespeicherten Daten über eine sehr große Anzahl von Benutzern ist das edu-ID-System ein attraktives Angriffsziel, sowohl zum Ausspähen der Daten als auch für Denial-of-Service-Angriffe. Es müssen deshalb ständig Maßnahmen zum Schutz gemäß dem Stand der Technik vorgenommen werden, z.B. auch ein Überwachung durch das DFN Security Operations Center.

- Mangelnde technische Kompetenzen von Seiten der teilnehmenden Einrichtungen im Bereich föderierter Dienste können dazu führen, dass die edu-ID abgelehnt oder Services schlecht benutzbar werden. Deshalb müssen Schulungen und Workshops für die Dienstbetreiber und die IdM-/IdP-Admins durchgeführt werden.

9.2 Organisatorische Risiken

- Sollte der DFN als Betreiber entfallen oder sich die Verantwortlichkeiten für den Betrieb des edu-ID-Systems ändern, könnte das zum Ausfall des Systems führen. Deshalb wird Wert darauf gelegt, dass die einzelnen Komponenten aus Open-Source-Software bestehen und eine umfassende Dokumentation zum System erstellt wird.

- Zu späte Fertigstellung und dadurch bedingte Parallellösungen mit ähnlichen Problemstellungen können die Akzeptanz der edu-ID senken. Deshalb ist die schnelle Erstellung des Proof-of-Concept auch als politisches Signal an Dienstbetreiber zu verstehen, dass es sich lohnt, auf dieses Konzept zu setzen und die edu-ID zukünftig einzubinden und zu benutzen.
  Um Silobildungen zu vermeiden, soll es aber auch Kooperationen mit ähnlichen, parallel entwickelten Lösungen geben. Das betrifft sowohl ähnliche Konzepte, die bereits in Deutschland im Einsatz sind, als auch edu-ID-Systeme anderer Staaten bzw. NRENs.

- Mangelnde Annahme von Seiten der Nutzer:innen und oder der Dienste:
  Die Chancen für die Annahme der edu-ID stehen gut: In den Beratungen des NFDI-AAI-Kernteams zeichnet sich bereits jetzt ab, dass das edu-ID-System innerhalb der NFDI eine wichtige Rolle spielen wird. Sie soll auch als Basis-ID für BIRD (Bildungsraum Digital) bzw. die Nationale Bildungsplattform genutzt werden.

9.3 Wirtschaftliche Risiken

- Das Betriebsmodell für das edu-ID-System ist zum jetzigen Zeitpunkt noch offen. Sollte die Trägerschaft des DFN-Vereins aus unvorhergesehenen Gründen enden, könnte ein Konsortium der wichtigsten Stakeholder den Betrieb übernehmen.

9.4 Rechtliche Risiken

- Was geschieht mit dem System / der Architektur, wenn sich die rechtlichen Rahmenbedingungen ändern? Aufgrund der modular geplanten Architektur sollten den geänderten Rahmenbedingen entsprechende Änderungen leistbar sein

- Die Verarbeitung von großen Mengen personenbezogener Daten über längere Zeiträume hinweg kann zu datenschutzrechtlichen Problemen führen Deshalb ist eine datenschutzrechtliche Bewertung seitens der zuständigen Behörden für die Pilotphase geplant

10 Glossar

Begriff	Definition
AQ	Attribute Query
CR	Challenge-Response (Verfahren)
EIS	edu-ID-System
HE	Heimateinrichtung
IdM	Identity Management System
IdP	Identity Provider
LoA	Level(s) of Assurance
NeA	Noch ein Akronym
Sirtfi	Security Incident Response Trust Framework for Federated Identity[10]
SP	Service Provider
SweA	Schon wieder ein Akronym
ToU	Terms of Use

11 Anhang

11.1 Übersicht User Journeys und deren Priorisierung

Bezeichnung und Beschreibung	Priorität
1. Onboarding	
a. User registriert sich im edu-ID-Portal	

[10] https://refeds.org/sirtfi

i. per Registrierungsformular	1
ii. per Login bei einer Heimateinrichtung	1
iii. per Login über eID	ohne
b. User loggt sich am edu-ID-Proxy mit einer Heimateinrichtungs-Identität ein, die bisher nicht verknüpft ist (Vorstufe zu 1 a ii.)	1
2. Dublettenerkennung	
a. automatisiert bei Onboarding	
i. Anhand von Fremdschlüssel-Identitäten	1
ii. Anhand von Personendatengleichheit (ggf mit Admin-Bestätigung)	ohne
b. mit Admin-Bestätigung	Ohne
3. Verknüpfen von weiteren Heimateinrichtungs-Identitäten	
a. Initiiert über Portal	1
b. Initiiert über Login (gleicher Einstieg wie 1. b)	1
4. Validieren des Accounts	
a. über Heimateinrichtung (analog zu 3. oder 1 a ii.)	1
b. eID (analog zu 1 a iii.)	ohne
5. Validieren von Kontaktinformationen (Mobilnummer, E-Mail) per Challenge-Response	1
6. Self-Service-Funktionen	
a. Verwalten (Hinzufügen, Entfernen, Bestätigen) von 2FA-Credentials	
i. TOTP	2

ii. SMS	2
b. Verwaltung von edu-ID-Stammdaten	
i. Ändern der Stammdaten	1
ii. führt zu Änderung des Validations-Status	1
c. Verwalten von anderen Identifiern (z.B. ORCID)	
i. Hinzufügen	1
ii. Entfernen	1
d. Verwalten von gemerkten Vorauswahlen (siehe 7.)	
i. Heimateinrichtungen (Discovery) – Authentifizierung	1
ii. Aktive Affiliation (Affiliation-Chooser) - Attributübermittlung Authentifizieren über Heimateinrichtung A und Attribute von Heimateinrichtung B an den Dienst übermitteln. Attr(HE B) werden per AQ geholt	ohne
iii. Zurücksetzen von gesetzten Attributfreigaben	2
e. Passwortfunktionen für edu-ID-IdP-Benutzer (Ändern, Zurücksetzen)	1
f. Auskunftsansprüche DSGVO / Transparenz	
i. Welche Daten sind über mich gespeichert?	
1. Auch: Welche externen IDs habe ich verknüpft?	1
2. Und auch: Welche Daten haben die Heimateinrichtungen über mich gespeichert? Knopf drücken, AQs werden an die HEs gefeuert, Daten werden tabellarisch aufbereitet angezeigt	ohne
a. evtl. Möglichkeit per Formular Anfrage an HE zu senden, dass Daten aktualisiert	ohne

werden (Kontakt aus Metadaten des DFN evtl. als neue Kontakt-Kategorie)	
ii. Welche Attributfreigaben sind derzeit eingerichtet?	2
iii. Welche Vorauswahlen sind derzeit gesetzt (siehe 7 a/b)?	
1. Discovery	1
2. Affiliation	ohne
iv. Terms-of-use	
1. Aktuelle Anzeigen	1
2. Neuen Zustimmen	1
g. edu-ID löschen	1
h. Support	2
i. Recovery-Prozesse (alternative E-Mail-Adressen, Recovery per SMS, Recovery-Tokens für 2FA)	2
7. Login bei SPs über edu-ID-Proxy	
a. Auswahl der Heimateinrichtung beim Login	
i. Auswahl merken	1
ii. IdP-Hinting (schränkt Auswahlmöglichkeiten der/des Nutzenden ein)	ohne
b. Auswahl der Affiliation (welche Attribute von welcher Heimateinrichtung werden übertragen)	
i. Auswahl merken	ohne
ii. Unterstützug der Anforderung von mehreren Affiliations (9 d)	ohne
c. User-Consent	1

d. Terms of Use-Änderungen akzeptieren	1
8. Single Logout	
a. Propagation an weitere SPs, die mit dem edu-ID-IdP benutzt wurden	ohne
b. Propagation an benutzte Heimat-IdPs (und dort ggfs. wiederum weitere SPs)	ohne
9. Attribute-Queries	
a. SP fragt edu-ID-Proxy und dieser delegiert AQ an Heimateinrichtung oder edu-ID-IDP	1
b. Bei Auswahl einer anderen Affiliation im Affiliation-Chooser als den authentifizierenden IDP	ohne
c. Bei periodischer Prüfung, ob eine Verknüpfung zu einer HE noch existiert (siehe 11. b)	2
d. Kombinieren von Datensätzen aus verschiedenen (allen verknüpften) HE	ohne
10. Admin-Funktionen	
a. Manuelles Zusammenlegen von eindeutig geklärten Dubletten-Kandidaten (siehe 2.b)	ohne
b. Allgemeine Administrative Eingriffsmöglichkeiten	
i. Annehmen und Weitergeben an HEs allgemeiner Security-Anfragen (Stichwort Sirtfi)	2
ii. Account(ent)sperrung bei missbräuchlicher Nutzung	2
iii. Löschen alter Zweitfaktoren , Eintragen neuer Zweitfaktoren, ...	2
iv. Admin-Logout im Fall von missbräuchlicher Nutzung	ohne
11. Hintergrundprozesse (automatisiert)	

a. Periodische Prüfung ob ein edu-ID-Nutzer noch existiert (z.B. nach einem Jahr Inaktivität)	
i. Anfrage an eine oder mehrere der hinterlegten Kontaktmöglichkeiten	1
ii. Wenn keine Antwort: Löschprozess einleiten (für eine gewisse Zeit den Account sperren, irgendwann löschen)	1
b. Periodische Prüfung ob Affiliation noch existiert (AQ) (9 c)	2
c. Änderungen der ToU an alle Nutzenden schicken	1