



Ökosystem E-ID in der Bildung

Teilbericht 2: Nutzende, Anwendungsfälle und Anwendungsszenarien

Impressum

Projektbericht der Berner Fachhochschule, Zentrum Digital Society www.bfh.ch/digitalsociety,
im Auftrag von educa.ch

Autoren Jérôme Brugger (BFH)
Thomas Selzam (BFH)
Nelly Buchser (educa.ch)

Titelbild Maksim Kabakou/Shutterstock.com

CC BY-NC-ND (creativecommons.org)

Juni 2017

Inhaltsverzeichnis Teilbericht 2

1	Ausgangslage und Ziel	4
2	Vorgehen	4
3	Nutzende	5
4	Anwendungsfälle	5
4.1	Zugriff auf elektronische Ressourcen innerhalb einer Organisation	6
4.2	Zugriff auf elektronische Ressourcen über Organisationsgrenzen hinweg	6
4.3	Zugriff auf Service-Provider	6
4.4	Zugriff auf Content-Provider	7
4.5	Nachweis von Funktion oder Eigenschaft gegenüber Dritten	7
4.6	Rechtsgültiges Signieren im Geschäftsverkehr durch Personen	7
4.7	Rechtsgültiges Signieren im Geschäftsverkehr durch Organisationen	7
5	Clusterung der Anwendungen	8
6	Anwendungsszenarien	10
6.1	Nutzung von Content-Provider-Plattformen	10
6.2	Speicherung und gemeinsame Nutzung von datenschutzrelevanten Daten	11
6.3	Zugriff und Auswertung von Daten aus unterschiedlichen Schulen	12

1 Ausgangslage und Ziel

In diesem Teilbericht werden die bei der weiteren Konzeption und Verwendung des Ökosystem-Modells beigezogenen Anwendungsfälle dargestellt. Sie bilden mit ihrem konkreten Bezug zu aktuellen oder antizipierten Bedürfnissen von Stakeholdern eine zentrale Grundlage für die Projektarbeit. Als Anwendungsfälle werden die kontextspezifischen Kombinationen von Nutzungen einer E-ID bezeichnet. Unterschiedliche Instanziierungen des Modells werden entwickelt, indem die Abdeckung von bestimmten Anwendungsfällen verändert wird. Damit ist die unmittelbare Verbindung zwischen den Nutzenden und dem Nutzen, der aus einer BildungsID entsteht, sichergestellt.

Ziel des Arbeitspaketes war es, eine umfassende Liste von Nutzenden und Anwendungsfällen zu erstellen, die für die Erstellung von Instanziierungen des Modells verwendet werden kann. Über eine Aufzählung der Anwendungsfälle hinaus wurden drei Anwendungen einer BildungsID in spezifischen und ausführlichen Szenarien durchgespielt und dokumentiert. Darin werden die Aktivitäten aller Akteure für das Zustandekommen berücksichtigt. Diese drei Anwendungsszenarien dienen zur konkreten Darstellung der Funktionsweise und des Nutzens einer BildungsID und sollen in erster Linie in der Kommunikation eingesetzt werden. In den Interviews wurden sie auch zur Erläuterung der Funktionsweise des Modells an einem konkreten Beispiel verwendet.

Für die Darstellung im Modell wurden die Anwendungsfälle dann abstrahiert und zusammengefasst, um eine bessere Übersichtlichkeit und Verständlichkeit zu erreichen. In den weiteren Teilberichten sind Rückmeldungen zum Modell und den Anwendungsfällen in den Interviews mit Stakeholdern zur *IST-Situation* sowie Überlegungen zum *Nullszenario* dargestellt.

2 Vorgehen

In einem Workshop mit Mitarbeitenden von educa.ch wurde die Zusammenstellung und Gruppierung der Nutzenden und der Anwendungsfälle einer BildungsID erstellt. Dabei konnte auf bestehende konzeptionelle Überlegungen von educa.ch aufgebaut werden.

Ein Workshop zu den Anwendungen fand am 25.10.2016 nachmittags bei educa.ch statt. Von educa.ch haben Karl Wimmer, Simon Graber, Nelly Buchser und Paul Gerhard teilgenommen; moderiert wurde der Workshop von Thomas Selzam und Jérôme Brugger der BFH.

Ziel des Workshops war das Erstellen einer umfangreichen Liste von aktuellen und potentiellen Anwendungen sowie diese nach Wichtigkeit und Relevanz zu gruppieren. Im Workshop wurden folgende Punkte abgearbeitet:

- Einführung zum Teil Nutzung im E-ID-Ökosystem-Modell
- Identifikation von Nutzenden in Gruppendiskussionen
- Zusammentragen von heute möglichen Anwendungen
- Zusammentragen von denkbaren Anwendungen, für die noch weitere Voraussetzungen geschaffen werden müssen
- Einordnen der Anwendungen in drei Dimensionen (selten bis häufig; einfach bis komplex; kritisch bis unkritisch bezüglich Sicherheitsanforderungen)
- Selektion von drei bis vier komplementären Anwendungen zur Aufbereitung als Anwendungsszenarien

Im Nachgang zum Workshop hat das Projektteam der BFH generische Kategorien von Anwendungsfällen abgeleitet und die drei Anwendungsszenarien entwickelt. Diese wurden anschliessend von educa.ch validiert.

Im Folgenden werden die Ergebnisse des Workshops wiedergegeben, ohne weiter detailliert auf den Prozess der Erarbeitung während des Workshops einzugehen.

3 Nutzende

Alle potentiell an einer BildungsID beteiligten Personen und Organisationen wurden zusammengetragen. Alle werden im Modell als Nutzende bezeichnet. Es kann aber unterschieden werden zwischen Personen, die eine BildungsID besitzen und damit ihre Identität nachweisen können und Organisationen, die Dienste betreiben, für die sie Informationen der BildungsID beziehen (Relying Parties).

Im Verlauf des Workshops wurden folgende Nutzende einer BildungsID identifiziert:

- Lernende der Stufen ISCED 020-4
- Lehrende der Stufen ISCED 020-4
- Erziehungsberechtigte
- Mitarbeitende der Schulleitungen
- Mitarbeitende der Bildungsverwaltungen (auf Ebene Gemeinde, Kanton, Bund sowie interkantonale Organisationen)
- Schule oder Behörde als Organisation

- interne Dienstleister in der Schule (Hauswartinnen und Hauswarte, Mitarbeitende des Sekretariats, ...)
- externe Dienstleister in der Schule (Logopädinnen und Logopäden, ...)
- Lehrmeisterinnen und Lehrmeister
- Mitarbeitende der schulärztlichen Dienste
- Mitarbeitende von schulergänzenden Betreuungsangeboten (Tagesschulen, Mittagstische, ...)
- Schulexterne Betreuende

- Lehrmittelverlage, weitere Content-Provider (kantonale, private)

- Technologieanbieter (Software, Cloud Services, LMS, ...)

- Weiterbildungsanbieter (PH, weitere)

- Hochschulen

- E-ID-Dienstleister der Hochschulen (Switch)

- Berufsverbände mit Aufgaben in der Berufsbildung

- private Bildungsanbieter

- Anbieter von weiteren Angeboten für Lernende im Bereich Kultur, Sport, ...

- Anbieter von Produkten und Dienstleistungen, die Vergünstigungen für Lernende und Lehrende anbieten

4 Anwendungsfälle

In der nachfolgenden Übersicht werden mögliche Anwendungen, in denen Identifikation notwendig ist, aufgelistet und die daraus abstrahierten Anwendungsfälle beschrieben. Diese Anwendungsfälle können, je nach Ausprägung einer BildungsID, über diese abgedeckt werden. Die Aufzählung enthält einerseits heute existierende Anwendungen, auf die mit lokalen Identitäten zugegriffen werden kann, andererseits aber auch Anwendungen, die in Zukunft verwirklicht werden können, nachdem weitere Voraussetzungen organisatorischer, technischer und rechtlicher Art geschaffen wurden. Die Liste zählt viele Anwendungen auf, trifft aber keine Aussagen über die Notwendigkeit, diese Anwendungen in die Konzeption einer BildungsID einzuschliessen.

Die Zuordnung zu sieben abstrakten Anwendungsfällen wurde im Anschluss an den Workshop vom Projektteam der BFH vorgenommen.

Die Aufzählung erhebt weder Anspruch auf Vollständigkeit, noch sind die Anwendungsfälle trennscharf voneinander abgegrenzt. Die Zuordnung von Anwendungen zu den sieben Anwendungsfällen ist nicht exklusiv, je nach Ausprägung des Services verändert sich die Zuordnung. So ändert sich diese beispielsweise, je nachdem ob ein Service intern oder von einem Dritten in der Cloud angeboten wird.

4.1 Zugriff auf elektronische Ressourcen innerhalb einer Organisation

Der Anwendungsfall «Zugriff auf elektronische Ressourcen innerhalb einer Organisation» beschreibt die alltägliche Nutzung von elektronischen (oder weniger häufig auch physischen) Ressourcen, die innerhalb einer Schule¹ zur Verfügung stehen. Nutzende sind hier die Lernenden und Lehrpersonen sowie weitere Dienstleister, die innerhalb der Schule tätig sind. Dieser Anwendungsfall umfasst folgende Anwendungen:

- Zugang zu Computer, E-Mail, Internet etc. (mittels Single Sign On)
- Drucken, Kopieren
- Zugang zu E-Portfolio
- Zugang zu E-Learning-Tool
- Zugang zu Schulverwaltungsprogrammen, das in einer Schule verwendet wird
- Noten eintragen, Zugriff auf Noten und weitere Daten
- Anmeldung für Kurs, Wahlfach, Schulreise etc.
- Buch aus Schulbibliothek ausleihen
- Reservation von Ressourcen (z.B. Raum, Beamer, Laptops etc.)
- Online resp. elektronisch Leistungsüberprüfungen durchführen
- Bezahlen in der Mensa mittels Badge etc.
- Physischer Zugang zum Schulgebäude

4.2 Zugriff auf elektronische Ressourcen über Organisationsgrenzen hinweg

Mit «Zugriff auf elektronische Ressourcen über Organisationsgrenzen hinweg» ist ein Anwendungsfall gemeint, für den Zugriff auf eine Ressource von zwei oder mehreren Organisationen aus ermöglicht werden muss, also beispielsweise der Zugriff einer Schulleiterin und eines Mitarbeiters der kantonalen Bildungsverwaltung auf dieselbe Ressource. In diesen Anwendungsfall müssen mindestens zwei unterschiedliche organisationale Praktiken und ggf. technische Umsetzungen der Benutzerverwaltung berücksichtigt werden. Dieser Anwendungsfall umfasst:

- Zugang zu Schulverwaltungsprogrammen (Zugriff von Schule und Bildungsverwaltung)
- Zugang zu Daten von Lernenden (Zugriff von Schule, Bildungsverwaltung, schulärztlichem Dienst, Lehrmeisterin oder Lehrmeister, schulergänzenden Betreuungsangeboten, o.ä.)
- Zugang und Verwaltung der eigenen Daten (Zugriff durch Lernende oder Erziehungsberechtigte)
- Sichere Kommunikation mit Erziehungsberechtigten, Bestätigung des Erhalts der Nachrichten
- Zugang zu gesichertem E-Maildienst für vertrauliche Kommunikation
- Übermittlung eines Schülerdossiers beim Übertritt in eine andere Schule
- Zugang zu elektronischen Tests und deren Resultate (z.B. ÜGK) durch Lernende, Lehrende, Bildungsverwaltung
- Zugang zu Daten /Erhebungen im Bildungsmonitoring

4.3 Zugriff auf Service-Provider

Der Anwendungsfall «Zugriff auf Service-Provider» beschreibt den Zugriff auf Online-Angebote resp. Cloud-Ressourcen von Dienstleistungsanbietern. Dazu muss die Art und Weise des Zugriffs durch den Service-Provider auf die Identitätsdaten geregelt werden. Der Anwendungsfall umfasst:

¹ «Schule» wird hier zu Bezeichnung einer Organisation verwendet, nicht des Gebäudes.

- Zugriff auf Speicherplatz in der Cloud
- Zugriff auf Kollaborationsplattformen in der Cloud
- Zugriff auf Lernplattformen in der Cloud

4.4 Zugriff auf Content-Provider

Im Anwendungsfall «Zugriff auf Content-Provider» wird der Zugang zu elektronischen Lehrmitteln zusammengefasst. Hier stellt sich die Frage nach der Regelung des Zugriffs auf Identitätsinformationen, insbesondere auf Attribute zu Funktions- oder Eigenschaftsbeschreibungen (Lehrperson an Schule X, Schüler der Klasse 4a, etc.). Für eine einfache Nutzung von elektronischen Lehrmittelplattformen im Unterricht, die eine Auswertung der Resultate durch die Lehrperson vorsieht, muss eine Zuordnung von Lehrenden und Lernenden über Attributsinformationen ermöglicht werden. Damit kann die Zugriffssteuerung entscheidend vereinfacht und automatisiert werden. Dieser Anwendungsfall umfasst:

- Zugriff auf ein elektronisches Buch über Schuldatenbank
- Zugriff auf lizenzierte bzw. kostenpflichtige Angebote von Schulbuchverlagen, inkl. Management von DRM
- Personalisiertes Lernen
- Zugriff auf die Plattform des Plan d'Études Romand

4.5 Nachweis von Funktion oder Eigenschaft gegenüber Dritten

In diesem Anwendungsfall geht es um den Nachweis der Funktion „Lehrperson“ oder der Eigenschaft „Schülerin oder Schüler“, um bei elektronischen Transaktionen von Zugang zu Angeboten oder Spezialkonditionen zu profitieren. Denkbar sind Anwendungen wie:

- Bestellung von vergünstigter Software, Hardware
- Bestellung von ermässigten Abonnements des Öffentlichen Verkehrs
- Anmeldung für vergünstigte Sport- und Kulturangeboten
- Zugriff auf geschützte Ressourcen für Lehrende
- Zugriff auf geschützte Ressourcen für Lernende einer bestimmten Bildungsstufe/ Klasse

4.6 Rechtsgültiges Signieren im Geschäftsverkehr durch Personen

Der Anwendungsfall «Signieren durch Personen» betrifft nicht die primäre Funktion einer BildungsID, die Identifikation, sondern die rechtsgültige Unterschrift basierend auf der Identität einer Person. Die inhaltliche Verbindung von Authentifizierung und Signatur legen nahe, auch diesen Anwendungsfall in die Überlegungen einzubeziehen. Dieser ist auf einen kleinen Teil von Nutzenden im Bereich der Schulleitung und der Schuladministration beschränkt. Mögliche Anwendungen sind:

- Unterschreiben von Verträgen
- Unterschreiben von Verfügungen
- Unterschreiben von Zeugnissen

4.7 Rechtsgültiges Signieren im Geschäftsverkehr durch Organisationen

Als letzter Anwendungsfall wurde das Signieren durch eine Organisation aufgenommen. Damit ist die Signatur von elektronischen Dokumenten im Namen einer Organisation gemeint. Aus der heutigen Sicht wäre damit eine Anwendung realisierbar:

- Ausstellung und der sichere Herkunftsnachweis von elektronischen Zeugnissen

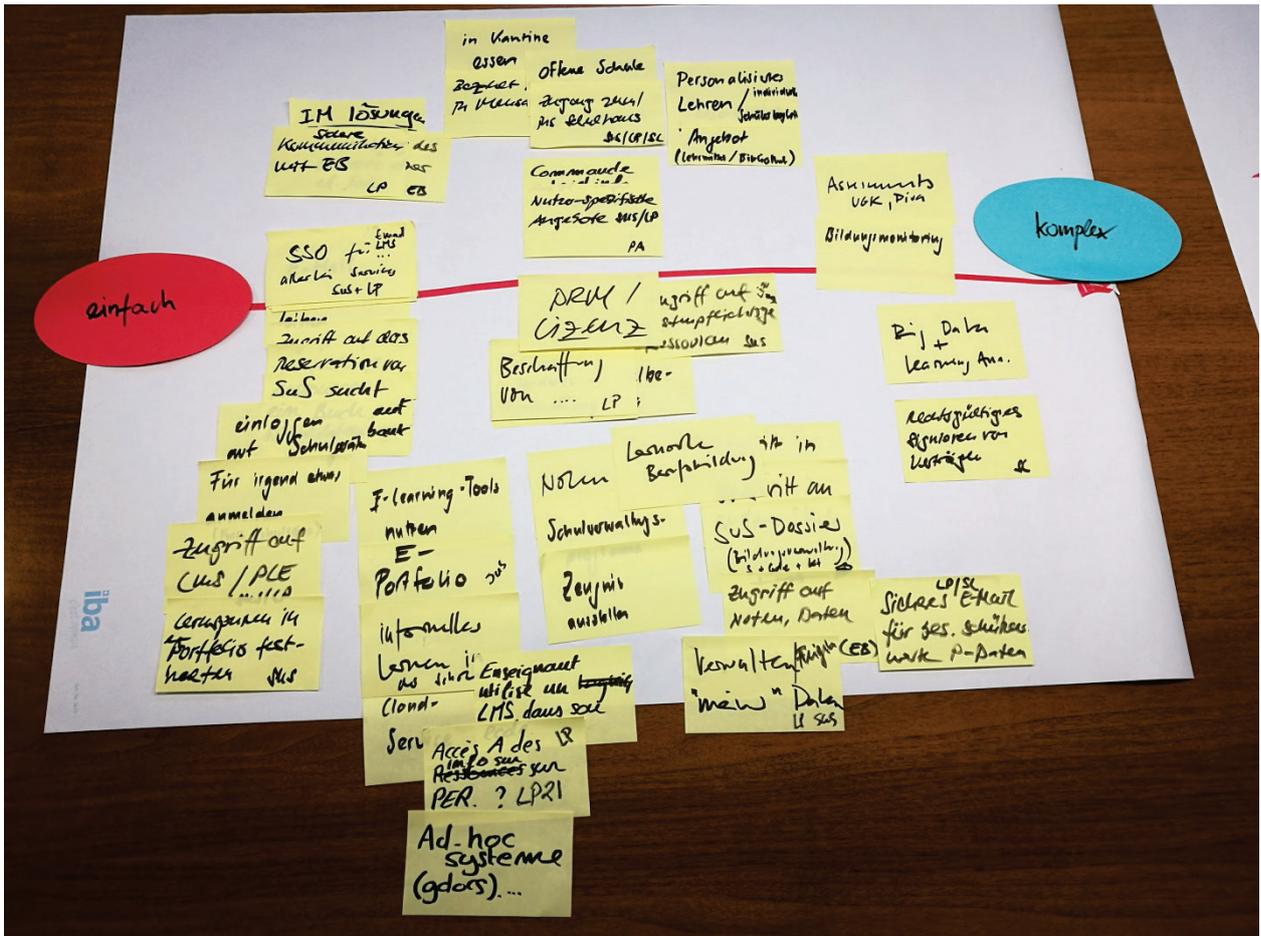


Abbildung 2: Anwendungen nach Komplexität

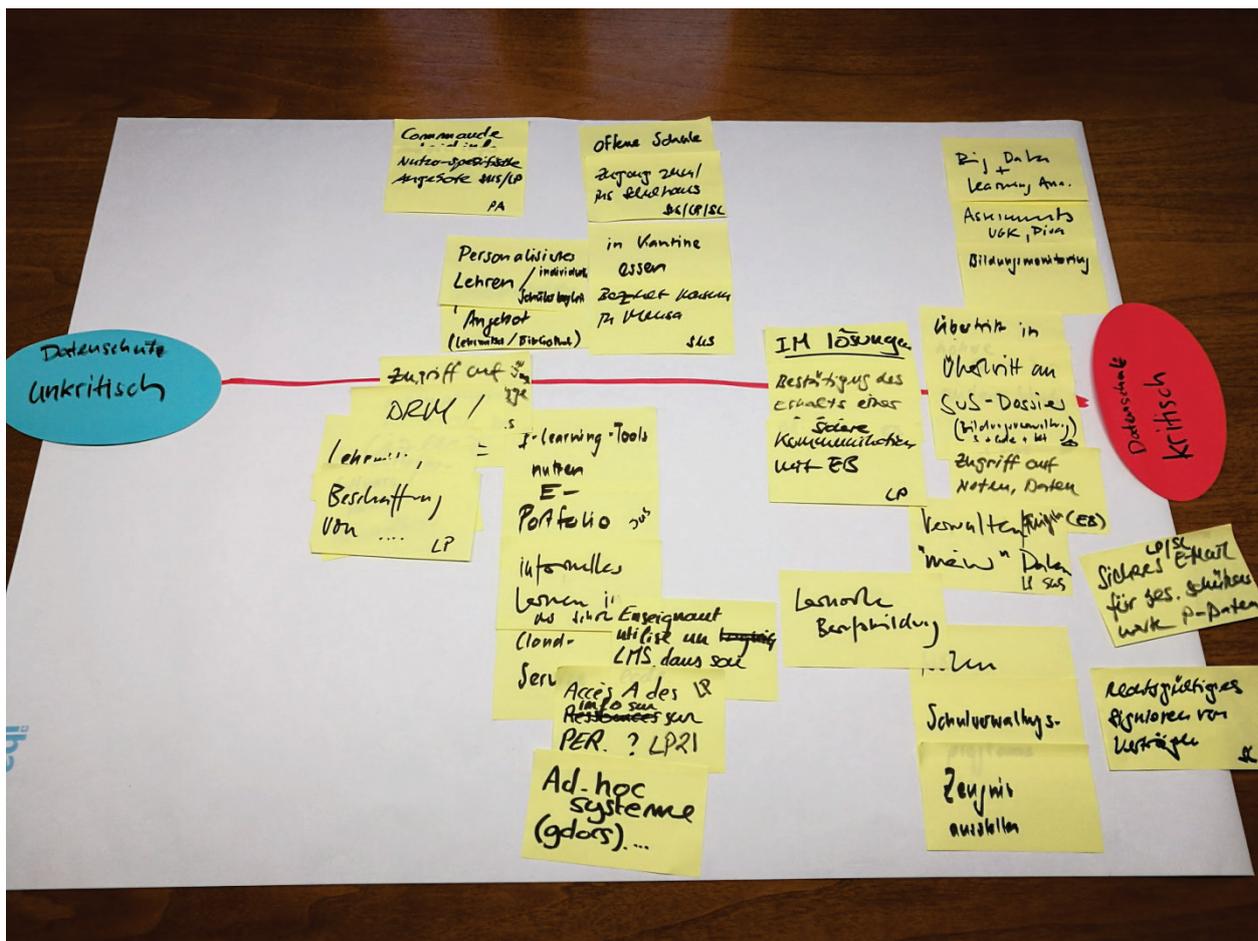


Abbildung 3: Anwendungen nach Anforderungen zum Schutz der Daten

6 Anwendungsszenarien

Aus dem gesamten Spektrum möglicher Anwendungen wurden drei Szenarien erarbeitet, die unterschiedliche Nutzende, Anwendungsfälle und Anforderungen an eine BildungsID berücksichtigen. Diese wurden von educa.ch ausgewählt. Alle beschriebenen Anwendungsszenarien basieren auf realen Aktivitäten im Bildungswesen, die um die hypothetische Verwendung einer BildungsID mit umfassenden Funktionalitäten ergänzt werden. Damit kann beschrieben werden, welchen Mehrwert der Einsatz einer elektronischen BildungsID bieten könnte. Gleichzeitig werden aber auch offene Fragen zu Nutzung und Bereitstellung aufgeworfen.

6.1 Nutzung von Content-Provider-Plattformen

6.1.1 Beschreibung

Frau Humbert-Droz unterrichtet Französisch an einem Gymnasium in der Deutschschweiz. Sie bereitet das nächste Semester vor und schaut sich an einem Abend dazu unterschiedliche Lerninhalte an. Um auf dem Portal zebis.ch und auf weiteren Portalen auf geschützte Inhalte zugreifen zu können und ggf. auch Kommentare zu den einzelnen Angeboten erfassen zu können, meldet Sie sich mit ihrer BildungsID an. Während sie früher unterschiedliche Benutzernamen und Passwörter für die unterschiedlichen Plattformen eingeben musste, kann sie nun die unterschiedlichen Portale mit ihrer BildungsID nutzen. Anschliessend bestellt sie bei einem Lehrmittelverlag den Lehrerkommentar zu einem Lehrmittel. Durch ihre Anmeldung mit der BildungsID ist ihre Funktion als Lehrperson und damit ihre Bezugsberechtigung nachgewiesen und das Buch wird entweder als E-Book zugestellt oder ihr nach Hause an ihre Privatadresse geliefert, während früher Lehrerbücher nur an die Schule geschickt wurden.

Die Plattform des Lehrmittelverlags kann Frau Humbert-Droz als Lehrerin des entsprechenden Gymnasiums erkennen und wird aufgrund des Vertrages mit der Schule die bezogenen Bücher direkt der Schule verrechnen.

Frau Humbert-Droz plant das digitale Lehrmittel im kommenden Semester mit ihren Schülern zu bearbeiten und bringt direkt auf der Plattform – in ihrem persönlichen Bereich – Kommentare und weiterführende Links an. Die Materialien zu einem Kapitel des Lehrbuches will sie mit ihrem Kollegen weiterentwickeln und gibt diese für ihn zum Lesen und Bearbeiten frei. Diese Kommentare und Ergänzungen sind an ihre BildungsID gebunden und können exportiert oder im Falle eines Stellenwechsels an eine andere Schule mitgenommen werden.

6.1.2 Nutzen

Frau Humbert-Droz hat mit der BildungsID einen Vorteil an Nutzbarkeit und Einfachheit für ihren Zugriff auf Materialien. Darüber hinaus stellt die Bestätigung ihrer Zugehörigkeit zu ihrer Schule sicher, dass kostenpflichtige Angebote direkt über die Schule abgerechnet werden. In Online-Ressourcen, die sie gemeinsam mit ihren Schülerinnen und Schülern nutzt, ist ohne manuelle Konfiguration der Zusammenhang zwischen ihr als Lehrerin und den Lernenden durch die Funktions- und Eigenschaftsnachweise der BildungsIDs hinterlegt.

Schule, Schulverbunde oder Kantone können einfacher Gesamtlizenzen für einzelne Angebote verwalten, indem der Zugang für eine gesamte Kategorie von Personen vereinbart werden kann. Zugang zu Ressourcen wird auf der Basis von Funktions- und Eigenschaftsnachweisen organisiert (Attribute Based Access Control). Eine kurzfristig eingestellte Vertretungslehrperson erhält zum Beispiel mit der Zuteilung des Attributes „Lehrperson in der Schule XY“ ohne weiteren Aufwand Zugang zu externen, elektronischen Ressourcen.

Die Plattformbetreiber müssen nicht mehr selbst die Nutzenden mit allen Angaben registrieren und pflegen. Mit der Nutzung der BildungsID können freigegebene Daten (Name, Adresse, Eigenschaft und Zugehörigkeit) föderiert werden. Wechselt Frau Humbert-Droz an eine andere Schule, wird ihre neue Zugehörigkeit auf der Plattform bei der nächsten Anmeldung automatisch übernommen und die Zugangsrechte oder Rechnungsadressen entsprechend der bestehenden Vereinbarungen zwischen ihrer neuen Schule und der Plattformbetreiberin angepasst.

6.2 Speicherung und gemeinsame Nutzung von datenschutzrelevanten Daten

6.2.1 Beschreibung

Herr Matter ist Logopäde und hat nach einer Abklärung einen Bericht zu einem Kindergartenkind verfasst. Er speichert diesen auf einer Datencloud, bei der er sich mit seiner BildungsID authentifiziert hat. Er möchte den Bericht der Lehrperson und den Erziehungsberechtigten zur Besprechung vorlegen. Letztere haben einer elektronischen Zustellung zugestimmt und sind zur elektronischen Bearbeitung der Dokumente in der Lage. Er kann für diese drei Personen Leserechte definieren, die über deren BildungsIDs gesteuert werden. Er macht per Mail die Lehrperson und die Erziehungsberechtigten, ohne Preisgabe von sensiblen Daten, darauf aufmerksam, dass sie den Bericht mithilfe ihrer BildungsID (oder ggf. der BildungsID ihres Kindes) auf der Ablage einsehen können. Bei entsprechend angepassten Prozessen und elektronischen Signaturen kann der Bericht auch unterschrieben und nach vorgesehenen Prozessen digital abgelegt werden.

6.2.2 Nutzen

Für Herrn Matter und die Lehrperson vereinfacht die sicherere elektronische Zustellung von Berichten den Arbeitsalltag. Der Zugang zum Dokument erfolgt dank der Bindung an die BildungsID mit gesicherten Identifikationsmitteln, die im Idealfall eine qualitativ hohe Authentifizierung gewährleisten. Somit können Einsichtnahmen auch überprüfbar aufgezeichnet werden. Damit wird der Datenschutz gestärkt.

Aus einer übergeordneten Perspektive stärkt die Bindung von Zugriffsrechten an die BildungsID den Schutz der persönlichen Daten, indem Zugriff nur mit einer bestätigten Identität möglich wird.

6.3 Zugriff und Auswertung von Daten aus unterschiedlichen Schulen

6.3.1 Beschreibung

Frau Locher ist Mitarbeiterin am Institut für Bildungsevaluation der Universität Zürich. Sie verwaltet für den Bildungsraum Nordwestschweiz den Zugriff auf die Testplattform und wertet die Resultate der Tests aus. Für die Verwaltung des Zugriffs auf den Test können Klassen oder Jahrgänge aufgrund von Merkmalen über die Eigenschaftsnachweise der BildungsID berechtigt werden. Schülerinnen und Schüler melden sich mit ihrer BildungsID auf der Plattform an und absolvieren die jeweiligen Tests. Der Zugriff auf die Testresultate kann dann unter Wahrung des Persönlichkeitsschutzes organisiert werden. Während die Lehrpersonen mittels Funktions- und Eigenschaftsnachweisen ihrer eigenen BildungsID die Resultate ihrer Klassen anschauen können, erhält Frau Locher alle Resultate nur anonymisiert mit einer Identifikationsnummer angezeigt. Da diese Nummer von der BildungsID abgeleitet wird, sind Längsschnittauswertungen möglich, da beim nächsten Testzyklus wieder die gleiche Nummer abgeleitet wird.

6.3.2 Nutzen

Frau Locher kann den Zugang zur Plattform basierend auf Funktions- und Eigenschaftsnachweisen (Lernende / Lehrende, Klasse 4a, Schule XY) verwalten und muss nicht Zugangsinformationen für alle am Test beteiligten Personen einzeln verwalten.

Schülerinnen und Schüler sowie Lehrpersonen können sich mit ihrer BildungsID einloggen und müssen sich keine weiteren Benutzernamen und Passwörter merken. Damit können sie sich auch zu einem späteren Zeitpunkt, z.B. zur Einsicht in die Resultate wieder einloggen, auch über einen langen Zeitraum.

Der Schutz der persönlichen Daten wird gestärkt, indem die Resultate in unterschiedlichen Benutzerkreisen und in unterschiedlichem Grad der Anonymisierung zugänglich gemacht werden können. Gleichzeitig ermöglicht aber die Anonymisierung in Form einer Nummer, die von einer Identität abgeleitet ist, die gleiche Person auch in einem anderen Test zu identifizieren und so Analysen über eine gesamte Bildungslaufbahn vorzunehmen.