BildungsID Kanton Bern

Studienschlussbericht

Jérôme Brugger, Jan Frecè
Version 1.2 vom 13.3.2019

Berner Fachhochschule
Wirtschaft
E-Government-Institut

Inhaltsverzeichnis

Zusammenfassung

Die wachsende Nutzung von digitalen Werkzeugen und Inhalten in der Schule stellt alle Beteiligten vor die Herausforderung, eine geordnete, sichere und benutzerfreundliche Verwendung dieser Instrumente in Zukunft sicherzustellen. Zentraler Baustein einer digitalen Schulinfrastruktur ist eine elektronische Bildungsidentität (B-ID) für Lernende und Lehrende. Die B-ID hat zwei Funktionen: Erstens stellt die B-ID einen eindeutigen Identifikator dar, der über die Bildungslaufbahn oder Berufslaufbahn als Lehrperson bestehen bleibt. Mit diesem Identifikator können weitere Daten verknüpft werden. Zweitens soll mit der B-ID ein Zugangsschlüssel (z.B. Benutzername und Passwort) verbunden werden, der einer Person erlaubt, sich an unterschiedlichen Applikationen des Kantons und von Dritten mit demselben Zugangsschlüssel anzumelden.

Im Hinblick auf eine mögliche Umsetzung haben die in Workshops erhobenen Anforderungen mit Vertreterinnen und Vertretern des Amts für Kindergarten, Volksschulen und Beratung (AKVB) und des Mittelschul- und Berufsbildungsamtes (MBA) gezeigt, dass der einfache Zugriff auf Inhalte und Applikation in beiden Schulstufen das zentrale Bedürfnis ist. Weiter ist auch die Weitergabe von Identitätsdaten zwischen Schulen bei Schulwechseln eine Verwendung mit grossem Nutzenpotential. Weitere Akteure (Erziehungsberechtigte, Ausbildungsverantwortliche, …) können ebenfalls den Bedarf nach Zugriff auf einzelne Inhalte haben, die Integration der weiteren Personenkreise soll aber zu einem späteren Zeitpunkt auf der Basis von anderen Identitäten (z.B. dem BE-Login des Kantons) erfolgen können.

Die vorgeschlagene dezentrale Lösungsvariante für den Kanton Bern beinhaltet drei zentrale Elemente, die neu geschaffen werden müssen:

- Eine BildungsID als Identifikator, die an jede Schülerin, jeden Schüler und jede Lehrperson vergeben wird und bestehen bleibt
- Ein Register der BildungsIDs, das selbst nur die Nummer und den Verweis auf die datenführende Schule beinhaltet und so die Entstehung von doppelten Einträgen verhindert.
- Eine Vermittlungsinstanz (Hub oder Broker genannt), die die Identitätsanfragen zwischen den Lösungsanbietern und den datenführenden Schulen vermittelt und die von der Erziehungsdirektion verwaltet wird

Zusätzlich dazu müssen alle Schulen dabei begleitet werden, die Identitätsdaten ihrer Schülerinnen und Schüler sowie der Lehrpersonen so aufzubereiten, dass daraus Identitätsinformationen und Attribute (Rolle, Zugehörigkeit zu einer Klasse) elektronisch bestätigt werden können. Während die Mittel- und Berufsschulen über eine weitgehend homogene Infrastruktur des Kantons verfügen, in der alle Personendaten elektronisch geführt werden und für eine B-ID genutzt werden könnte, ist die Infrastruktur in den Volksschulen sehr heterogen. Schulen, die heute die Verwaltung der Schülerdaten mittels Excel oder Filemaker bewerkstelligen, können diese Daten nur sehr schwer automatisiert beziehen oder bestätigen. Eine Schulverwaltungslösung mit Möglichkeiten zum automatisierten Datenaustausch sind Voraussetzung für eine dezentrale Umsetzung der BildungsID.

Der Bericht empfiehlt, die skizzierte Lösung so bald als möglich in einem begrenzten Umfang zu pilotieren, um die Funktionsweise den verschiedenen Akteuren demonstrieren zu können und Detailfragen in der praktischen Anwendung zu klären. Dazu können teilweise bestehende Infrastrukturen genutzt werden.
Weiter empfiehlt der Bericht, die gesetzlichen und organisatorischen Voraussetzungen zu prüfen, um insbesondere die Volksschulen durch den Kanton so zu begleiten, dass ihre Infrastruktur die Voraussetzungen für die Nutzung der BildungsID genügend sind.
Zuletzt empfiehlt der Bericht, die auf nationaler Ebene im Projekt FIDES unter der Federführung von educa.ch laufenden Aufbauarbeiten für eine nationale Föderation von Bildungsidentitäten kritisch-konstruktiv zu begleiten und die Lösung frühzeitig auch im Kanton Bern zu pilotieren.

1 Ausgangslage und Projekteziele

Im Bildungswesen stellt sich im Zuge der Digitalisierung die Frage, welche grundlegenden Instrumente und Infrastrukturen in Zukunft benötigt werden, um Lehren und Lernen auf allen Schulstufen zukunftsgerichtet zu gestalten. Welche dieser Dienste und Infrastrukturen müssen - aus unterschiedlichen Gründen - zentral bereitgestellt werden? Können die bestehenden Angebote des Marktes genutzt werden oder muss der Kanton oder andere staatliche Stellen Angebote entwickeln oder Anforderungen definieren? In diesem Bericht werden diese Fragen für die elektronische Bildungsidentität (B-ID) diskutiert, die als eine Infrastrukturkomponente für digitales Lernen und Lehren gesehen wird.
Der Fokus liegt dabei auf dem Kanton Bern. Berücksichtigt werden in den Überlegungen die Ausgangslage und Bedürfnisse der Volksschule (AKVB) und der Mittel- und Berufsschulen (MBA).
Die Ziele des Projektes waren:

- Stakeholder und Anforderungen an die Lösung sind übersichtlich dokumentiert, Schwerpunkt liegt bei der Nutzung durch Dritte.
- Die Ausganglage und Zielperspektive für eine BildungsID sind dokumentiert. Die Dokumentation umfasst eine grobe grafische Darstellung der Systemarchitektur und dazugehörige Erläuterungen.
- Auf der Basis der Lösungskonzepte des Kantons Bern soll das Zusammenspiel mit den Arbeiten von educa.ch im Projekt FIDES besser gesteuert werden können. Darüber hinaus soll der Nutzen einer BildungsID auch unabhängig von FIDES geprüft werden.
- Die Analysen können als Grundlage für Entscheidungen zum weiteren Vorgehen genutzt werden.

2 Vorgehen

Die oben beschriebenen Ziele wurden im Rahmen des Projektes in vier Arbeitspaketen abgearbeitet.
In einem ersten Schritt wurden auf der Basis des bestehenden eID-Ökosystem-Modells[1] Anwendungsfälle und Stakeholder für die beiden Stufen und Ämter, AKVB und MBA, ermittelt und die wichtigsten Use Cases in Bezug auf Häufigkeit und Wirkung zusammengestellt.
Im zweiten Arbeitspaket wurden die bestehenden Infrastrukturen betrachtet und eine mögliche grobe Architektur für die Bereitstellung einer BildungsID vorgeschlagen.
Im dritten Arbeitspaket wurden Überlegungen zur Ausgabe, Nutzung und Revokation von Bildungsidentitäten angestellt. Dabei wurden mögliche Anforderungen an die Qualität von Identitäten betrachtet.
Im vierten Arbeitspaket werden die Möglichkeiten der Nutzung von BildungsIDs durch Dritte evaluiert, indem Stakeholdersichten auf die Lösung erhoben wurden.

3 Grundsätze einer BildungsID

Für die Projektarbeit wurde eine Arbeitsdefinition einer BildungsID angenommen. Diese geht davon aus, dass eine BildungsID zwei zentrale Aspekte und Funktionalitäten beinhaltet:

- Eine BildungsID ist ein eindeutiger Identifikator in Form einer Nummer, die für die gesamte Bildungslaufbahn der Lernenden (mit Durchlässigkeit hin zur Tertiärstufe) oder durch die gesamte Berufslaufbahn als Lehrperson in den Schulen des Kantons Bern mit einer Person verbunden ist. Mit dieser Nummer können weitere Daten verknüpft werden.
- Mit dieser BildungsID verbunden ist ein Zugangsschlüssel (z.B. in Form eines Benutzernamens und Passworts), das der Person erlaubt, gegenüber unterschiedlichen Diensten ihre Identität zu bestätigen und damit Zugriff zu unterschiedlichen Diensten im Bildungssektor zu erhalten. Je nach Ausgestaltung ist denkbar, dass der Schlüssel von der jeweiligen Bildungsinstitution verwaltet wird und damit bei einem Wechsel der Schule auch ändern kann.

[1] Vgl. Projektberichte der BFH auf https://www.educa.ch/de/dossiers/eid/modell-oekosystem

Mit der BildungsID werden die technischen, organisatorischen und rechtlichen Voraussetzungen geschaffen, damit die Identitätsbestätigung und die Bestätigung von einzelnen Attributen in einer sicheren und vom User kontrollierten Art und Weise von weiteren Diensten und Institutionen genutzt werden können.

4 Stakeholder und Use Cases für eine BildungsID

4.1 Volksschule

Die Ausgangslage in den Volksschulen wurde an einem halbtägigen Workshop mit vier Vertreten der Volksschule Mitte September 2018 erhoben. Dazu wurde das eID-Ökosystem-Modell der Berner Fachhochschule verwendet. Dieses erlaubt, die Diskussion auf der Basis einer generischen Liste von Nutzenden und Anwendungsfällen zu führen und daraus die spezifischen Anforderungen für den Kanton Bern zusammenzutragen. Die wichtigsten Aussagen aus dem Workshop werden in den weiteren Unterkapiteln zusammengefasst.

4.1.1 Nutzende

Wichtigste Nutzende sind die *Lehrenden und Lernenden*. Sie benötigen die BildungsID für die Aktivitäten in ihrem Schulalltag. Weiter sind die *Erziehungsberichtigten* eine weitere mögliche Gruppe von Nutzenden, die für den Zugang zu Daten und für den Informationsaustausch berücksichtigt werden müssen. Eine Ausgabe und die Verwaltung von BildungsIDs für Erziehungsberechtigte erscheint in einer ersten Beurteilung als zu grossen Aufwand für Schulen. Eine Nutzung des BE-Login soll für diese Gruppe geprüft werden.
Wichtige Nutzende sind weiter die *10-12 Schulverlage und Anbieter von digitalem Content,* auf die im Rahmen des Unterrichts zugegriffen werden muss. Teilweise bestehen die digitalen Angebote schon, es kann davon ausgegangen werden, dass die Zahl und Bedeutung weiter wachsen werden.

4.1.2 Anwendungsfälle

Wichtigster Anwendungsfall ist der Zugang von Lernenden und Lehrenden mit einer BildungsID zu einzelnen Lehrmitteln, die aktuell oder in Zukunft online angeboten werden. Damit wird sichergestellt, dass digitale Lernangebote effizient genutzt werden können. In diesem Anwendungsfalls authentisiert sich ein Schüler mit seiner BildungsID an einer Verlagsplattform.
Der Zugang zur lokalen Infrastruktur (Computer, WLAN) könnte ggf. als zusätzliche und optionale Nutzungsmöglichkeit angeboten werden. Die Voraussetzungen in den Volksschulen sind in Bezug auf die vorhandene Infrastruktur und auf den Professionalisierungsgrad des Betriebs und des Managements der IT-Infrastruktur sehr unterschiedlich.

Zweiter Anwendungsfall ist die Verwendung der BildungsID für den Zugang durch Lehrpersonen zu kantonalen Applikationen (Beurteilung 21, Pensenbuchhaltung), die von der ERZ betrieben werden. Dabei stellt sich die Frage, ob der Zugang mit der BildungsID oder mit dem BE-Login für diese Applikationen zweckmässiger ist.

Dritter Anwendungsfall ist die Nutzung der BildungsID für die Zusammenarbeit von mehreren Lehrpersonen auf einer vom Kanton angebotenen und/oder betriebenen Kollaborationsplattform, die heute noch nicht existiert.

Vierter Anwendungsfall ist die Nutzung der BildungsID für die Anmeldung und für den Zugang zu Weiterbildungskursen und Inhalten der Pädagogischen Hochschule Bern und ggf. weitere Hochschulen. Dazu wäre eine Durchgängigkeit der BildungsID zur ID, die im tertiären Bildungsbereich genutzt wird, erwünscht.

Ein fünfter Anwendungsfall betrifft die Nutzung einer BildungsID als Identifikator bei der Übermittlung von Daten zwischen Schulen bei Umzug oder Schulwechsel oder die Übermittlung von Daten von den Schulen an die ERZ. Für diese Nutzung ist die Rolle der einzelnen prozessbeteiligten Akteure noch nicht klar, sodass der Anwendungsfall noch nicht weiter präzisiert werden kann.

4.1.3 Weitere Anforderungen

Darüber hinaus wurde im Workshop ein grosser Verbesserungsbedarf beim Abgleich bzw. bei der Übermittlung von Daten zwischen der Einwohnerkontrolle der Gemeinde und der Schule geäussert. Dieser Aspekt wird aber aufgrund der thematischen Erweiterung in den Projektüberlegungen nur am Rand behandelt. In der Folge dieser Diskussion wurde aber deutlich, dass zu prüfen ist, auf welcher Datenbasis die BildungsID generiert wird. Aus Überlegungen zur Aktualität und Praktikabilität erschient die Generierung aus Daten der Schule besser zu realisieren, damit würden aber schulpflichtige Kinder, die in privaten Bildungseinrichtungen oder zu Hause unterrichtet werden, keine BildungsID erhalten.

4.2 Mittelschulen und Berufsbildung

Die Ausgangslage in den Berufs- und Mittelschulen wurde an einem halbtägigen Workshop mit einer Vertreterin und drei Vertretern der Schulstufe Mitte September 2018 erhoben. Auch in diesem Workshop wurde mit dem E-ID-Ökosystem-Modell gearbeitet. Die wichtigsten Aussagen aus dem Workshop werden in den weiteren Unterkapiteln zusammengefasst.

4.2.1 Nutzende

Die BildungsID wird in erster Linie durch die *Lernenden und Lehrenden* im Schulbetrieb für den Zugang zu unterschiedlichen Diensten und Inhalten benötigt. Für die organisatorische Abwicklung wird die BildungsID schon vor dem Beginn der Ausbildung an den Berufs- und Mittelschulen benötigt und muss über die Ausbildungsdauer Bestand haben. Damit stellt sich die Frage nach den Schnittstellen und der Übergabe der Daten von und zu vor- und nachgelagerten Bildungsinstitutionen im konkreten Anwendungsfall.
Weiter wird eine BildungsID von den *Mitarbeitenden der Schuladministration* benötigt, um auf die unterschiedlichen Applikationen in der Schule und beim MBA zugreifen zu können. Zugriff auf Noten und Stundenpläne könnte auch für die *Erziehungsberechtigten* von Bedeutung sein.
Ein weiterer Aspekt, der insbesondere für die Berufsschulen zentral ist, ist die Zusammenarbeit und der Austausch mit den *Lehrbetrieben und den Ausbildnern*. Möglichkeiten des elektronischen Austauschs und des gemeinsamen Zugriffs wären hier ebenfalls gegeben. Dabei müssen die bestehenden Branchenlösungen für Lernen und Kollaboration berücksichtigt werden.
Wichtiger Nutzer sind weiter die *Anbieter von digitalen Inhalten*, auf die im Rahmen des Unterrichtes zugegriffen werden muss. Dies können neben Verlagen und Anbietern von Software auch Berufsverbände sein.

4.2.2 Anwendungsfälle

Wichtigster Anwendungsfall aus der Sicht der Akteure im Berufs- und Mittelschulbereich ist die Authentifizierung von Lernenden und Lehrenden gegenüber den verschiedenen Plattformen und Portalen, die im Unterricht verwendet werden. Der Zugang zur lokalen Infrastruktur ist in den Schulen bereits abgedeckt.

Dieser generische Anwendungsfall kann für die unterschiedlichen Angebote noch weiter spezifiziert werden. Dazu gehören:

- Standard-Software von Microsoft (in der Cloud)
- in den grafischen Berufen Produkte von Adobe (in der Cloud)
- Plattformen wie Swiss Learning Hub, Schooltas, SwissDoc (SDBB) und NanooTV
- Bestehende und zukünftige Angebote von Schulverlagen

In der Berufsbildung ist zudem eine Vielzahl von branchenspezifischer Spezialsoftware im Einsatz, weiter verlangen auch gewisse Maschinen und Geräte eine Authentifikation bei der Benutzung. Zugriff auf Berufsbildungsplattformen der Berufsorganisationen wäre weiter notwendig, um alle Anwendungen abzudecken. Grundlage für eine grosse Verbreitung wäre, dass der Implementationsaufwand für die Anbieter technisch und organisatorisch sehr gering ist.

Zweiter Anwendungsfall ist der Zugriff auf Evento für die Erfassung von Noten, Absenzen und weiterer administrativer Arbeiten. Weitere administrativen Arbeiten erfordern Zugriff auf Untis. Auf beide

Systeme ist auch ein Zugriff für Lernende, Ausbildner und für Erziehungsberechtigte für die Einsicht in die eigenen Daten, bzw. eines Lernenden denkbar.

Dritter Anwendungsfall ist der Zugriff von Lehrpersonen auf Kollaborations- und Datenaustauschplattformen (Moodle, Ilias, weitere, noch nicht existierende Lösungen) zu berücksichtigen.

Vierter Anwendungsfall ist die Übernahmen von Daten der Lernenden von vorgelagerten Bildungsinstitutionen. Die Rollen in diesem Anwendungsfall müssen noch weiter präzisiert werden

4.2.3 Weitere Anforderungen
In der Diskussion der Anwendungsfälle wurden weitere allgemeine Anforderungen an die Lösung formuliert:

- Die Anwendung bisheriger Accounts soll nicht verdrängt werden.
- Es sollen keine zusätzlichen Benutzernamen und Passwörter für den Nutzer entstehen.
- Die ID soll keine Rückschlüsse auf den/die Benutzer/in erlauben.
- Eine Verknüpfung mit folgenden Single Sign On-Accounts ist gewünscht:
    - MS Office 365 ID
    - Google ID
    - Adobe ID
- Attribute der BildungsID sollen in Vertraulichkeitsstufen eingeteilt werden.
    - Attribute ohne Vertraulichkeitsstufe können ohne zusätzliche Freigabe an Trusted Partys (d.h. Parteien, welche die BildungsID zur Authentifikation akzeptieren) weitergegeben werden.
    - Attribute mit Vertraulichkeitsstufe benötigen zur Weitergabe eine stufenabhängige Freigabe.
    - Freigaben können sich auf eine Person, aber auch auf eine Rolle beziehen.
- Nutzung der Identitätsdaten durch unbeteiligte Dritte (z.B. zur statistischen Auswertung) darf nur in anonymisierter Form erfolgen (keine Pseudonymisierung!)
- Die Anonymisierung der Identitätsdaten erfolgt zentral durch Fachpersonal nach neuster Erkenntnis der Datenwissenschaft.

4.3 Zwischenfazit: Anwendungsfälle und Anforderungen an eine BildungsID

Trotz der unterschiedlichen Ausgangslage in den beiden untersuchten Stufen wurde versucht, eine gemeinsame Basis von Anforderungen zu identifizieren.

Wichtigster Anwendungsfall ist aus der Perspektive der beiden Schulstufen der Zugang zu digitalen Lerninhalten und Anwendungen. Dieses Bedürfnis besteht übereinstimmend für alle Anwenderinnen und Anwender in der Schule. Während für die Volksschule eine Aufzählung der wichtigsten Anbieter von Lerninhalten überschaubar ist, wächst diese Zahl insbesondere mit der Diversität der berufsspezifischen Inhalte und Software in der Berufsbildung erheblich.
Aus der Perspektive der Schulen erhält die Lösung dann einen besonderen Nutzen, wenn die BildungsID zum wichtigsten, wenn nicht gar einzigen, Zugangsschlüssel für den Unterricht wird. Dazu gehört auch der Zugang zur lokalen Infrastruktur. Auf den ersten Blick besteht in beiden Schulstufen keine Notwendigkeit, den Zugang auf eine BildungsID abzustützen. In den Mittel- und Berufsschulen ist der Zugang bereits abgedeckt, in der Volksschule ist der Zugang sehr unterschiedlich, in vielen Schulen wird bis zur vierten Klasse mit Klassenlogins für den Zugang zu lokalen Geräten gearbeitet. Trotz dieser Ausgangslage ist zu prüfen, ob nicht auch der lokale Zugang, optional und freiwillig, über eine BildungsID organisiert bzw. mit der BildungsID verknüpft werden kann, damit alle Zugänge für den Benutzer mit demselben Login funktionieren.

Der Zugriff von Lehrpersonen auf spezifische Applikationen der ERZ ist für beide Schulstufen ein Thema, allerdings sind unterschiedliche Applikationen in Verwendung. In beiden Fällen ist die Verwendung der BildungsID gegenüber der Verwendung eines BE-Logins abzuwägen.

Als weiterer Anwendungsfall mit einer eigenen Kategorie von Nutzenden kommt hier der Zugang der Erziehungsberechtigten hinzu, der aus der Überlegung zur Zuständigkeit und Handhabbarkeit vorzugsweise über das BE-Login organisiert werden sollte.

Das Bedürfnis nach Kollaborationsumgebungen für die Verwendung zwischen Lehrpersonen scheint in beiden Schulstufen gegeben, aber mit den aktuellen Lösungen noch nicht genügend unterstützt. Der Zugang zu einer Kollaborationsumgebung für Lehrpersonen sollte über die BildungsID organisiert werden.

Die durchgängige Benutzbarkeit der BildungsID und die Weitergabe von Daten im Falle von Schulwechseln (infolge Umzugs oder Curriculum) sind weitere, grundlegende Anforderungen an eine BildungsID. Diese Anforderungen werden in einem ersten Schritt in dieser generischen Form aufgenommen, eine weitere Klärung der Beteiligten und der Rollen soll zu einem späteren Zeitpunkt erfolgen.

Zuletzt wurden auch die Anforderungen an den Schutz der persönlichen Daten betont. Dieser Anforderung muss dadurch nachgekommen werden, dass die Umsetzung in den einzelnen Anwendungsfällen, insbesondere die Weitergabe von Informationen an Dritte, die Nutzung von Informationen für Auswertungen sowie die Datenweitergabe zwischen Bildungsinstitutionen detailliert unter diesem Gesichtspunkt betrachtet werden muss. Die Frage der Identifikation und der Nutzung der Daten müssen getrennt betrachtet werden.

5 Bestehende Systeme und Schnittstellen

In diesem Kapitel wird die Frage diskutiert, in welcher Art und Weise die bestehenden Systeme und Infrastrukturen Personendaten enthalten und nutzen. Auf dieser Basis kann geprüft werden, wie die bestehenden Infrastrukturen für den Betrieb der BildungsID genutzt werden können. Damit soll auch erreicht werden, dass nur dringend notwendige neue Elemente aufgebaut werden.

5.1 Volksschule

Die Heterogenität der bestehenden Systeme in den Volksschulen ist nicht systematisch erfasst. Anhaltspunkte für die weiteren Aussagen ist das Erfahrungswissen des Projektteams bei der ERZ und die Resultate einer Umfrage von educa.ch zur Nutzung und Verwaltung von Personendaten im Rahmen des Projektes FIDES.
Die Volksschulen verwalten ihre Daten in den meisten Fällen mit einer Schulverwaltungslösung, die auf dem Markt erhältlich sind. Es sind drei Anbieter, die die grösste Verbreitung im Markt haben. Gemäss der Umfrage (vgl. Abbildung 1) von educa.ch (mit einer Rücklaufquote von 35%) sind im deutschsprachigen Kantonsteil iCampus, LehrerOffice (mit je fast 40 Nennungen) und Scolaris (mit knapp 30 Nennungen) die am häufigsten benutzten Programme zur Erfassung von Personendaten in den Schulen. Excel und Filemaker werden von je rund 25 Schulen genutzt, eine Handvoll Schulen nutzen Access. Im französischsprachigen Kantonsteil sind BD GAF, EP Géstion (beide auf der Basis von Access) und Scolaris die in 16 Fällen verwendeten Lösungen, zusätzlich zu den Standard-Tools, die bei 9 antwortenden Schulen eingesetzt werden. Bei der Umfrage waren auch Mehrfachnennungen zugelassen, sodass sich in einigen Fällen die Instrumente ergänzen.

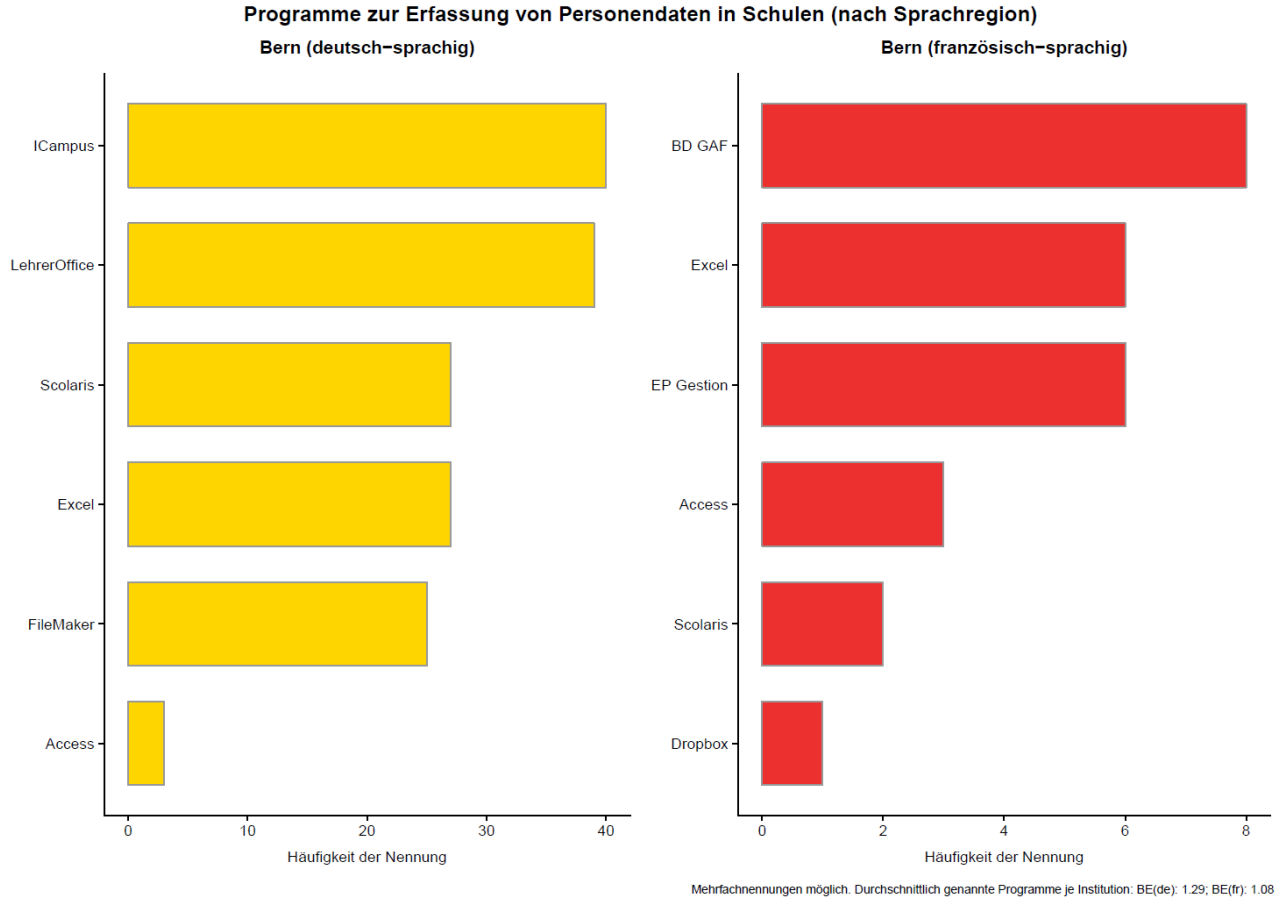

Abbildung 1 - Verwendete Schulverwaltungsprogramme Kt. Bern (Quelle: educa.ch (2018): Digitale Identitäten im Bildungsraum Schweiz. Eine Standortbestimmung.)

Die Personendaten in diesen Lösungen werden aus Angaben der Gemeinden alimentiert und von der Schulleitung oder Schuladministration gepflegt. Die Datensätze enthalten gemäss Umfrageergebnissen Name, Vorname, Adresse und in sehr vielen Fällen auch die AHVN13. Es gibt aber keine Anforderungen an einen minimalen Datensatz noch eine standardisierte Form. Offen ist beispielsweise, ob der gesamte offizielle Vor- und Nachname geführt, oder ein Feld mit Rufnamen hinzugefügt wird.
Für die Verwendung in den Diensten von eduBern werden die Daten im csv-Format aus den Schulverwaltungslösungen exportiert. Das Verfahren ist aufwändig und fehleranfällig aufgrund der kleinen Unterschiede zwischen den Formatierungen der unterschiedlichen Anbieter und des unterschiedlich gehandhabten Exports.
Die ERZ verfügt weiter zur Organisation des Lastenausgleichs und für statistische Zwecke über eine Datensammlung mit allen Schülerinnen und Schülern im Kanton Bern. Diese Daten sind von hoher Qualität, da sie von der Schule und von den Finanzverwaltern der Gemeinde überprüft werden. Jedoch bildet diese Zusammenstellung immer nur die Situation für ein definiertes Stichdatum ab und wird nur einmal jährlich aktualisiert.
Ein automatisierter Datenaustausch zwischen Schulen im Zuge von Schulwechseln existiert aktuell nicht.

5.2 MBA

Im Vergleich zu den Volksschulen sind die Mittel- und Berufsschulen in ihrer Infrastruktur zentraler und homogener organisiert. Das zentrale Instrument zur Erfassung von Lernenden und Lehrenden ist Evento. Im Grossteil der MBA-Schulorganisationen ist Evento ein de facto Standard und damit in den allermeisten Fällen der Master-Datensatz eines jeden Lernenden und Lehrenden dieser Schulstufe. Jede Schule hat einen eigenen Mandanten auf dem System, die Daten der einzelnen Schulen sind also getrennt. Obwohl der Einsatz eines alternativen Schulsystems eine Sondergenehmigung benötigt, gibt

es doch einige Schulen (z.B. Privatschulen und überkantonale Schulen wie die Hotelfachschule Thun), die ein von Evento abweichendes Schulsystem einsetzen. Es kann folglich nicht davon ausgegangen werden, dass die zentrale Evento-Instanz in näherer Zukunft für alle MBA-Schulen zum Datenspeicher ihrer Wahl wird. Dies nicht zuletzt deswegen, weil im Evento zwar Personen- und Adressdaten erfasst werden, allerdings sehr spezifisch auf die Bedürfnisse der Lehrausbildung ausgerichtet. Es wurde daher in der Praxis mehrfach festgestellt, dass Evento in der jetzigen Form nur sehr bedingt für Volksschulen nutzbar ist.
Datenübergaben von einer Schulorganisation an die nächste sind derzeit nicht möglich und werden durch manuelle Prozesse durchgeführt. Eine Datenübernahme findet also nicht statt, falls Lernende beispielsweise das Gymnasium abbrechen und anschliessend eine Lehre beginnen. In diesem Fall kommt es zu einer Neuerfassung der persönlichen Daten.
Die in den Schulorganisationen gespeicherten Daten beruhen meist auf Selbstdeklarationen der Lernenden oder der Erziehungsberechtigten. Eine Identitätsprüfung findet bei Schuleintritt in der Regel nicht statt.
Für den Austausch von Daten mit Umsystemen ist das Datenaustauschformat csv weit verbreitet. Es soll aber mittelfristig durch den Einsatz von Webservices ersetzt werden. Das System weist aber derzeit keine strukturierten Schnittstellen auf, sondern beruht auf situativen Einzellösungen.
Rollen-Profile und die damit verbundenen Zugriffsrechte sind stark schulspezifisch geprägt und variieren entsprechend stark. Derzeit sind pro Schule 1-2 Superuser für die Vergabe der Zugriffsrechte und die Datenqualität zuständig, allerdings gibt es keine Vorgaben betreffend Qualität oder Validierungsprozessen.
Obwohl eine dezentrale Pflege der Profile aus diesem Grund auch zukünftig sinnvoll erscheint, ist eine Angleichung kongruenter oder ähnlicher Rollenprofile anzustreben. Damit kann zum einen die Interoperabilität der verschiedenen Schulorganisationen gestärkt werden, zum anderen können Organisationsdaten besser abgeglichen werden. So könnte die Qualität der vorliegenden Daten oder zumindest das Bewusstsein für die Qualität gesteigert werden.
Aus der Sicht des MBA sollen auch künftig Empfehlungen und Abschlüsse via BildungsID einsehbar sein, die Speicherung und Bestätigung dieser Attribute erfolgt immer noch bei den vergebenden Schulorganisationen. Diese Schulorganisationen bleiben auch nach Abgang der Lernenden für die sichere Aufbewahrung und verzugsfreie Bestätigung von Attributen zuständig, was die Wichtigkeit von Datenschutz, Datenintegrität und Datenqualität unterstreicht.

6 Zielarchitektur

In diesem Kapitel werden mögliche Zielarchitekturen skizziert. Als Grundlage für die Überlegungen zu möglichen Architekturen dient die systematische Aufzählung von drei Hauptanforderungen, die aus den Workshops und der Erhebung der bestehenden Systeme abgeleitet wurden:

1. Die Identitätsdaten der Schülerinnen und Schüler sowie Lehrpersonen und Angestellten der Schuladministration können gegenüber kantonalen Applikationen und Applikationen von Dritten bestätigt werden.
    a. Die zu bestätigenden Attribute müssen definiert und standardisiert werden.
    b. Die Schulen müssen in der Lage sein, die Attribute in der der geforderten Form bestätigen zu können, also als Identitätsprovider im Sinne des eCH-Standards 107 agieren zu können.
    c. Um die Verwendung über die gesamte Bildungslaufbahn und eine minimale und kontrollierte Weitergabe von Attributen zu ermöglichen, muss eine BildungsID als Identifikator geschaffen werden, die über die gesamte Bildungslaufbahn verwendet werden kann.
2. Standardisierte Daten werden auf elektronischem Wege zwischen den Akteuren ausgetauscht, um damit den Übertritt zwischen Schulen administrativ zu vereinfachen.
    a. Die Weitergabe von Daten benötigt einen Prozess zur Datenfreigabe durch die Erziehungsberechtigten. Diese kann auf Papier oder elektronisch, z.B. auf Basis des BE-Logins erfolgen.
    b. Alle Daten, die weitergegeben werden sollen, müssen in einem standardisierten Format sein.

3. Um längerfristig die Daten nur an einem Ort zu führen und Doubletten der BildungsID auszuschliessen, wird ein Register der BildungsIDs und der dazugehörigen datenführenden Institution angelegt.

Zur Erreichung des ersten Ziels sind im Grundsatz zwei Modelle – ein zentrales und dezentrales- denkbar. In der konkreten Ausgestaltung sind als weitere Modelle als Varianten des dezentralen Modells denkbar. Alle Umsetzungsvarianten haben Vor- und Nachteile, die basierend auf den Anforderungen aus den Anwendungsfällen und auf den Voraussetzungen im Kanton und den einzelnen Schulgemeinden betrachtet werden müssen. Die vorgeschlagenen Variantenkommen den unterschiedlichen Anforderungen unter der Nutzung von vorhandenen Elementen am nächsten.

6.1 Die zentrale BildungsID

Um dem heterogenen Umfeld gerecht zu werden und einen standardisierten, allen zugänglichen Informationsraum zu schaffen, sieht diese Herangehensweise die von einer kantonalen Stelle geführten BildungsID als Masterversion für alle beteiligten Institutionen vor. Dieser zentralisierte Ansatz zieht folgende Konsequenzen nach sich:

1. Sämtliche Änderungen an der BildungsID müssen von allen Beteiligten ausschliesslich an dieser zentralen Masterversion vollzogen werden und Daten müssen ebenfalls von allen Beteiligten immer nur aus dieser Quelle angezogen werden. Lokal gespeicherte und damit potentiell veraltete Daten werden somit nicht mehr geführt.

2. Alternativ dazu könnte eine Synchronisationslösung dienen, welche den lokalen Datenbestand einer Schule mit dem zentralen Datenbestand der BildungsID abgleicht. Das Auflösen von Konflikten zwischen einzelnen Versionen muss aber gelöst werden.

3. Um Daten aus den Attributen der BildungsID zur weiteren Verarbeitung in die lokalen Schulsysteme übernehmen zu können, müssten alle bestehenden Schulsysteme dieselben Schnittstellen bzw. Standards unterstützen. Dies ist derzeit nicht flächendeckend gegeben.

4. Datenkonflikte gehören der Vergangenheit an, da die Daten der kantonalen BildungsID von allen Beteiligten als Referenzinformation angesehen werden. Trotzdem sind Fehler aufgrund von nicht vorgesehenen Rückgriffen auf lokale Daten oder Synchronisationskonflikte in der Praxis nicht vollständig zu vermeiden.

5. Die BildungsID kann für Authentifikationsvorgänge und zur Bestätigung sämtlicher bildungsbezogener Attribute genutzt werden.

6. Der Kanton baut und unterhält eine grosse Datensammlung, in der alle Schülerinnen und Schüler sowie Lehrpersonen verzeichnet sind.

6.2 Die dezentrale BildungsID

Ähnlich dem Zugang, wie er im Hochschulbereich mit SwitchAAI gewählt wurde, sieht diese Variante nicht vor, dass die BildungsID bei Logins verwendet wird. Sie dient vielmehr dazu, lokale Schulidentitäten über die lokale Institution hinaus benutzbar zu machen, da die verschiedenen Identitätsräume mit der BildungsID über einen gemeinsamen Bezugspunkt verfügen. Dieser Ansatz einer Föderation hat folgende Konsequenzen:

1. Um die Vorteile der BildungsID nutzen zu können, muss jede beteiligte Organisation über lokale Identitäten verfügen und in der Lage sein, Attribute zu speichern und anderen auf Anfrage zur Verfügung zu stellen bzw. deren Richtigkeit zu bestätigen.

2. Die BildungsID speichert selbst keine Identitätsattribute, sondern dient lediglich als verbindendes Attribut lokaler Schulidentitäten. Dies hat zur Folge, dass einer BildungsID nicht

zu entnehmen ist, welche Schulidentitäten damit in Verbindung stehen.

3. Sämtliche bildungsbezogenen Attribute (abgeschlossene Ausbildungen, Noten, Klassenzugehörigkeit, usw.) werden von den jeweiligen Schulen auf den lokalen Schulidentitäten vergeben und verwaltet. Diese lokale Schulorganisation bleibt auch zukünftig für die Sicherung und Zurverfügungstellung dieser Attribute verantwortlich, solange dies als notwendig definiert wird. Sollen Attribute auch ausserhalb einer Schulorganisation benutzt werden können, muss deren Benennung und Beschreibung vereinheitlicht werden, um so anderen Schulorganisationen deren richtige Interpretation zu ermöglichen.

4. Da die BildungsID über keine eigenen datenführenden Attribute verfügt, kann sie bei Informationssuchen nur als zentraler Ausgangspunkt dienen. Um Informationen über ein Curriculum eines Lernenden oder Lehrenden zu erhalten, muss eine entsprechende Anfrage unter Angabe der BildungsID und eventueller Berechtigungsnachweise an sämtliche beteiligten Schulorganisationen verschickt werden. Erst durch das Zusammensetzen der einzelnen Antworten entsteht eine Gesamtübersicht über die mit dieser BildungsID in Zusammengang stehenden Geschehnisse. Da jede lokale Schulorganisation über die Freigabe von Daten entscheidet, können die diesbezüglichen Hürden je nach Attribut der BildungsID variieren.

5. Das einzige im BildungsID-Register geführte Attribut ist die aktuelle datenführende Organisation. Dieses Attribut zeigt an, welche der angeschlossenen Schulorganisationen momentan dafür verantwortlich ist, nicht-bildungsbezogene Attribute aktuell zu halten. Während bildungsbezogene Attribute von mehreren Schulorganisationen bearbeitet werden können, ohne dass die Gefahr konfligierender Zugriffe bestünde, sehen sich nicht-bildungsbezogene Attribute (wie Adresse, Telefonnummer, Erziehungsberechtigte usw.) potentiell parallel stattfindenden Schreibzugriffen ausgesetzt. Daher werden nicht-bildungsbezogene Attribute ebenfalls lokal geführt. Sollte es beim Zusammenzug dieser Informationen zu widersprüchlichen Informationen aus verschiedenen Quellen kommen, sind die Angaben der datenführenden Organisation als ausschlaggebend anzusehen. Im Normalfall handelt es sich dabei um die Schulorganisation, die derzeit den Grossteil der Aus- oder Weiterbildungsleistung erbringt. Bei einem Schulwechsel muss diese Organisation entsprechend im Attribut der BildungsID angepasst werden.

6. Ein Login mit einer expliziten BildungsID ist nicht möglich. Vielmehr kann je Benutzerin und jeder Benutzer sich mit jeder Identität der angeschlossenen Organisationen einloggen, da jedes angeschlossene System (Relying Party) in der Lage ist, die Login-Anfrage an den für die jeweilige Identität zuständigen IDP weiterzuleiten. Die Rückmeldung des IDPs deckt drei Thematiken ab: 1) Bestätigung der erfolgreichen Authentifikation, 2) die authentifizierte BildungsID und 3) zu der ID zugehörige Attribute, falls nachgefragt und berechtigt. Damit wird die Anforderung nicht erfüllt, dass eine Username-Passwort-Kombination über die gesamte Schullaufbahn als BildungsID genutzt werden kann, auch wenn die Lösung eine BildungsID beinhaltet, welche Lernende und Lehrende über ihre gesamte schulische Laufbahn hinweg begleitet.

6.3 Variante 1: Dezentrale BildungsID mit Infrastrukturkomponenten für Schulen

Diese Umsetzungsvariante basiert auf der dezentralen Umsetzung der BildungsID, berücksichtigt aber die Tatsache, dass nicht alle beteiligten Schulorganisationen bereits über geeignete, lokale Identitäten verfügen. So sieht diese Umsetzungsvariante zwei unterschiedliche Möglichkeiten der Teilnahme vor.

- Verfügt eine Schulorganisation über das notwendige Know-How sowie die entsprechenden Prozesse und Infrastruktur, kann sie direkt mit den lokal verwalteten Identitäten an der BildungsID-Föderation teilnehmen. Sie verwaltet sämtliche lokalen Attribute weiterhin selbst, muss die lokalen Identitäten lediglich mit dem Attribut der BildungsID ausstatten.

- Verfügt eine Schulorganisation nicht über die notwendigen Voraussetzungen eine lokale Verwaltung von Schulidentitäten zu leisten, kann dieser Dienst zentral vom Kanton bezogen

werden und beinhaltet das Erstellen und Verwalten von Schulidentitäten inkl. der dazugehörigen Attribute und bietet eine offene Authentifikationsdienstleistung an, so dass die hinterlegten Identitäten auch für Logins oder Attributbestätigungen zur Anwendung kommen können. Die Organisationsform für die Bereitstellung ist weiter zu diskutieren, der Kanton könnte für passende Infrastrukturelemente auch einen Rahmenvertrag mit Anbietern aushandeln und damit die Implementierung in den Gemeinden fördern. Die Verantwortung für die Pflege der Identitäten bleibt aber bei der Schule.

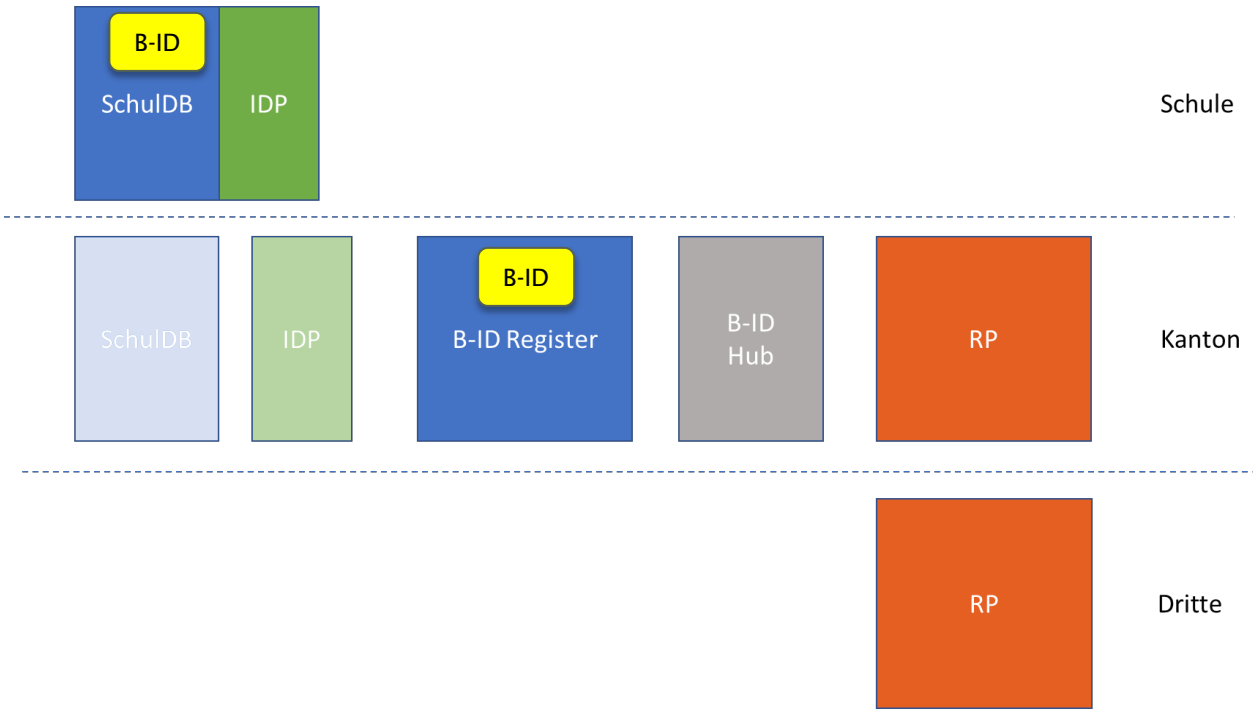

Abbildung 2 - Infrastrukturelemente einer dezentralen BildungsID

Die Abbildung 2 zeigt die Elemente der Infrastruktur für eine BildungsID. Zu den einzelnen Elementen wurden folgende Überlegungen angestellt:
Auf der Ebene jeder Schule besteht, so die Annahme, eine Datenbank (*SchulDB*) mit den relevanten Identitätsdaten der Lernenden und Lehrenden. Diese liegt in unterschiedlicher Form und in unterschiedlichen Instrumenten vor. In dieser Datenbank wird eine Erweiterung um einen Identifikator in Form der BildungsID realisiert.
Die Schulen benötigen als zweites Element die technische Infrastruktur, um auf standardisierte Anfragen im gesamten System, Identitäten zu authentifizieren und/oder deren Attribute zu bestätigen. Dieses Element wird in der Terminologie des gültigen eCH-Standards als Identitätsprovider (*IDP*) bezeichnet.
Im Sinne der beschriebenen dezentralen Varianten stehen diese beiden Komponenten, die SchulDB und der IDP auch auf der Ebene des Kantons zur Verfügung, um Schulen ans System anzuschliessen, die keine genügende IT-Maturität für den Betrieb des IDPs haben.

Auf der Ebene des Kantons sind zwei weitere Infrastruktur-Elemente vorgesehen, die für den Betrieb unerlässlich sind: Erstens wird ein zentrales Register (*B-ID Register*) der bereits ausgestellten BildungsIDs mit der dazugehörenden datenführenden Organisation, wo die Daten aktuell geführt werden. Zweitens wird ein *B-ID Hub* benötigt, der Anfragen der Applikationen an die datenführenden Schulen vermittelt und als Resultat dieser Anfragen, die BildungsID und definierte weitere Attribute an die Applikationen vermittelt. Der B-ID Hub vermittelt die Identitätsinformationen zwischen den unterschiedlichen Relying Parties und den unterschiedlichen IDPs. Mit dem Hub erhalten die RP eine einheitliche Schnittstelle, die in technischer und insbesondere in organisatorischer Hinsicht den Zugang zu den Identitätsbestätigungen regelt und die RPs von sensitiven Informationen wie Benutzername und Passwort isoliert. Diese werden direkt an den Identity Hub (B-ID Hub) getunnelt, der wiederum den für die ID zuständigen IDP kontaktiert. Als Bestätigung der Identität erhalten die

RPs die bestätigte BildungsID vom Identity Hub. Je nach Definition und Bedarf der RPs könnten auch weitere Attribute wie Schule, Klasse, und Rolle (SuS oder Lehrperson) übermittelt werden. Damit stellt der Identity Hub die Pseudonymisierung der einzelnen Benutzerinnen und Benutzer gegenüber Applikation von Dritten sicher. Als weiterer Aspekt kann geprüft werden, ob der Identity Hub auch eine Weiterleitungsfunktion für Nachrichten anbieten kann. Damit ist gemeint, dass analog der Weitergabe von bestätigten Identitätsdaten in Form der BildungsID auch Mitteilungen in Form von E-Mails von den Applikationen an die Mailadresse der Benutzer weiteregeleitet werden kann, ohne die Identität und die Adresse selbst sichtbar zu machen.

Die Applikationen, entsprechend den Use Cases kantonale Angebote oder Angebote von Dritten, werden gemäss der Terminologie von eCH170[2] als *«Relying Parties» (RP)* bezeichnet. Damit kommt zum Ausdruck, dass die Applikationen sich auf bestätigte Attribute verlassen, um Zugriff auf ihren Inhalt zu gewähren. Der Relying Party wird mit zusätzlichen Attributen ermöglicht, die Ansicht gemäss den Attributen zu gestalten, also z.B. eine Ansicht für Lehrpersonen anzuzeigen.

6.4 Variante 2: Dezentrale BildungsID mit der Trennung von Identität und Attributen

Ebenfalls auf einer dezentralen Architektur basierend sieht diese Variante vor, die Funktionen Identity-Provider und Attribute Provider aufzutrennen und eine digitale Identität zu nutzen, die schon besteht. Damit werden die Schulorganisationen von der Aufgabe der Authentifizierung entlastet und sind nur für die korrekte Zuordnung von Attributen zuständig.

In solch einem Setup besteht ein zentraler Identity Provider (oder derer mehrere, falls der Bedarf besteht), der sämtliche Anfragen von Relying Parties entgegennimmt und für alle angeschlossenen Schulorganisationen bearbeitet. Dazu provisionieren die Schulorganisationen den Identity Provider regelmässig mit aktuellen Berechtigungsnachweisen sämtlicher Benutzer.
Nach einer erfolgreichen Authentifizierung durch den Identity Provider erfolgt die Attributzuweisung. Diese kann entweder durch eine durch die jeweilige Schulorganisation betriebene Lösung oder aber über eine zentral zur Verfügung gestellte Plattform erfolgen, auf der Schulorganisationen die Attribute ihrer Accounts administrieren können. Es ist naheliegend, dass eine solche Plattform offene Schnittstellen für Schulverwaltungslösungen anbietet, so dass ein automatisierter Abgleich der Daten erfolgen kann.
Organisationen wie beispielsweise der Kanton Bern mit BE-Login oder Switch, aber auch kommerzielle Anbieter von Cloud-IDP-Lösungen wie Bedag oder Abraxas wären für den IDP-Betrieb geeignet, da das technische Know-how bereits vorhanden ist und in absehbarer Zukunft auch auf hohem Niveau weitergeführt wird. Sollte die Lösung in anderen Kantonen Nachahmer finden, wäre das Synergiepotenzial insofern hoch, da ein gemeinsamer Identity Provider genutzt werden könnte, so dass sich die Schulorganisationen nicht auf technische Fragen sondern auf administrative Aufgaben konzentrieren können.
Dieser Lösungsansatz entlastet die Schulorganisationen von der eher technischen Seite der sicheren Authentifikation, während sie die volle Kontrolle über die Administration der Attribute behalten. Sie bedingt allerdings, dass die Bildungs-ID diejenige Identität ist, welche die relevanten und aktuellen Attribute trägt, d.h. die Bildungs-ID wird zum Hauptwerkzeug der Lernenden und Lehrenden, welches sie durch ihre gesamte Karriere begleitet. Ist eine Person in mehreren Schulorganisationen aktiv, so kann jede dieser Schulen unabhängig voneinander entsprechende Attribute für die selbe Bildungs-ID vergeben, ohne einander in die Quere zu kommen.

6.5 Zwischenfazit

Die in diesem Kapitel detailliert vorgestellten Lösungsansätze, die zentrale Umsetzung und die beiden auf einer dezentralen Realisierung basierenden Varianten weisen in folgenden Aspekten Unterschiede aus:

1. Werden Identitäten und Attribute zentral oder dezentral verwaltet?
2. Wer übernimmt die Funktion des Identity Providers?

[2] eCH Standard Qualitätsmodell zur Authentifizierung von Subjekten https://www.ech.ch/standards/39522

3. Wer übernimmt die Funktion des Attribute Providers?
4. Wird die BildungsID als datenführende oder als verbindende Identität geführt?

Tabelle 1 - Übersicht der Lösungsvarianten

	Zentrale BildungsID	Variante 1	Variante 2
1 Verwaltung der Identitäten und Attribute	Sämtliche Angaben zu Identitäten und Attributen sind in einer kantonalen Datenbank erfasst	Sämtliche Angaben zu Identitäten und Attributen sind dezentral in den jeweiligen Schulen erfasst	Sämtliche Angaben zu Identitäten und Attributen sind dezentral in den jeweiligen Schulen erfasst. Die Identitätsinformationen werden in regelmässigen Abständen an den zentralen IDP übermittelt.
2 Funktion des IDP	Die zentrale Verwaltungsstelle übernimmt die Rolle des Identity Providers bzw. stellt einem externen Identity Provider alle benötigten Identitäts- und Attributsinformationen.	Jede Schule stellt entweder selbst IDP-Funktionalitäten zur Verfügung oder schliesst sich einer kantonalen Lösung an, welche diese Funktionalitäten als Dienstleistung für Schulorganisationen erbringen kann.	IDP-Funktionalitäten werden zentral durch eine oder wenige Stellen angeboten. Die dafür benötigten Berechtigungsnachweise werden von den angeschlossenen Schulorganisationen regelmässig hochgeladen und somit auf den neusten Stand gebracht.
3 Funktion des AP	Sämtliche Attribute sämtlicher Identitäten werden zentral verwaltet. Diese zentrale Stelle übernimmt ebenfalls die Rolle den Attribute Providers.	Jede Schule stellt entweder selbst Attribute-Provider-Funktionalitäten in Kombination mit dem IDP zur Verfügung oder schliesst sich einer kantonalen Lösung an, welche diese Funktionalitäten als Dienstleistung für Schulorganisationen erbringen kann.	Jede Schule stellt entweder selbst Attribute-Provider-Funktionalitäten zur Verfügung oder schliesst sich einer kantonalen Lösung an, welche diese Funktionalitäten als Dienstleistung für Schulorganisationen erbringen kann.
4 Funktion der BildungsID	Die BildungsID übernimmt datenführende Funktion, da andere Identitäten, zu denen verbunden werden könnte, nicht vorgesehen sind.	Die BildungsID übernimmt primär eine verbindende Funktion, da sie als Bindeglied zwischen allen organisationalen Identitäten dient. Ausser der derzeit datenführenden Institution verfügt die Bildungs-ID über keine weiteren Attribute.	Die BildungsID übernimmt primär eine verbindende Funktion, da sie als Bindeglied zwischen allen organisationalen Identitäten dient. Ausser der derzeit datenführenden Institution verfügt die Bildungs-ID über keine weiteren Attribute.

7 Prozesse

Mögliche Prozesse für die Ausgabe, die Nutzung und die Revokation einer BildungsID wurden auf der Basis der Zielarchitektur definiert. Anhand dieser angenommenen Ausprägung können weitere, zu klärende Fragen aufgeworfen werden. Mit der Pilotierung können diese Konzepte weiter verfeinert werden.

7.1 Anforderungen an den IDP

Generische Anforderungen an den Identitätsprovider werden im eCH-Standard 107[3] definiert. Gemäss diesen Anforderungen gilt für den IDP:

- Ermöglicht die Registrierung von Subjekten
- Stellt Funktionen zur Ausgabe, Pflege und Verwaltung von eIdentities bereit
- Stellt die physische Identifizierung des Subjekts anhand definierter Regeln abhängig von der angestrebten Qualität sicher
- Kennt andere eIdentity Services und ermöglicht die Pflege der linkedID zu anderen Identities des Subjekts[4]
- Stellt in geeigneter Weise die Qualität und Aktualität der eIdentity sicher
- Begrenzt die Lebensdauer von eIdentities und unterstützt die Subjekte in der Erneuerung ihrer eIdentities
- Kann eIdentities widerrufen
- Gewährt vertrauenswürdigen Credential und Attribute Services elektronischen Zugang zu den eIdentities
- Gewährt vertrauenswürdigen Authentication Services elektronischen Zugang zu den eIdentities

7.2 Registrierung

Die Schaffung einer BildungsID als Identifikator geschieht mit der Erfassung einer neuen Person durch eine Schule. Dabei wird bei der Erfassung einer neuen Person nach einer Abfrage am B-ID Register eine neue BildungsID zugewiesen und registriert, oder falls bereits eine BildungsID für die Person erstellt wurde, bei der als datenführenden Institution einen Austausch von bestehenden Daten angefragt. Einmal geschaffen bleibt die BildungsID bestehen.
Die BildungsID wird auf der Grundlage der AHV13 geschaffen, anderenfalls (z.B. im Falle von Sans-Papiers) wird eine entsprechende 13-stellige Laufnummer generiert (z.B. SP00000000001). Beide 13-stelligen Nummern werden einer Hashoperation (einer der aktuellen NIST-Standards sei empfohlen, zurzeit beispielsweise SHA256 oder SHA512). So ist sichergestellt, dass von der BildungsID nicht auf die Identität der damit in Verbindung stehenden Person geschlossen werden kann. Je nach Bedarf kann die ID auf eine Maximallänge begrenzt werden, wobei die Einzigartigkeit der ID beachtet werden muss. Eine Kürzung auf 16 Stellen würde beispielweise bedeuten, dass die AHV-Nummer 756.652.357.204.0 die BildungsID 5DD176DF1800334B@bid.be.ch ergibt. Alternativ dazu könnte ein zufällig generierter String als BildungsID dienen. Dieser müsste allerdings in einem Register (z.B. der Zentralen Ausgleichsstelle ZAS) als sektoren-spezifische Identität neben der AHVN13 hinterlegt werden, so dass die Verbindung administrativ nachvollziehbar bleibt und gleichzeitig keine logische Verbindung zwischen den beiden Identitäten besteht.

Die Daten der Person werden von der Schule erfasst oder im besten Falle automatisiert aus den Einwohnerregistern bezogen. In diesem Falle ist die Möglichkeit eines manuellen Hinzufügens einer Person notwendig, um auch nicht registrierte Schülerinnen und Schüler mit einer ID auszustatten.

Mit der Registrierung und der Schaffung der BildungsID ist die Frage der Qualität verbunden. Wichtiger Anhaltspunkt zur Bestimmung der Qualität von elektronischen Identitäten ist der Standard

[3] eCH Standard Gestaltungsprinzipien für die Identitäts- und Zugriffsverwaltung (IAM) https://www.ech.ch/standards/38631

[4] Die BildungsID stellt im Sinne des Standards die linkedID dar

eCH170. Es werden darin unterschiedliche Vertrauensstufen definiert, die von den Vertrauensstufen in den Teilmodellen der Registrierung, der Authentifizierung, der Föderierung und der Steuerung abhängig sind. Alle vier Aspekte der digitalen Identität ergeben in der Kombination die erreichte Vertrauensstufe. In allen Teilaspekten sind die heutigen Prozesse und die erforderliche Vertrauensstufe zu betrachten. Um einen Vertrauensraum zu schaffen, müssen Mindestanforderungen definiert werden, die alle Schulen erfüllen müssen.
Der Standard sieht für höhere Qualitätsstufen vor, dass im Registrierungsprozess die Identität der Person überprüft werden muss. Diese Praxis ist in der Schule nicht umsetzbar, sodass über den Bezug von Daten aus Registern die Aktualität und Fehlerfreiheit der Daten garantiert werden muss.

7.3 Nutzung

Die Nutzung der BildungsID für die Authentifikation an einer Applikation würde folgende Schritte beinhalten:
Nach dem Aufrufen der Applikation und Wahl des Logins mit der BildungsID wird die Benutzerin auf eine vom B-ID Hub betriebene Webseite resp. ein Fenster weitergeleitet, in dem sie den Usernamen und das Passwort eingibt, das sie von ihrer Institution erhalten hat und die mit der BildungsID verknüpft sind. Die Anfrage wird vom B-ID-Hub an den entsprechenden IDP weitergeleitet. Nach der korrekten Authentifikation werden die bestätigte Identität und angeforderte Attribute über den B-ID Hub an die Applikation weitergeleitet. Der B-ID Hub prüft dabei, ob die Applikation berechtigt ist, die Identitätsinformationen und die angeforderten Attribute zu erhalten und ob die Applikation auch diejenige ist, die sie vorgibt zu sein.
Aus der Sicht der Applikation kann aufgrund der bestätigten Identität und der Attribute der Zugriff auf die Inhalte gewährt werden. Möglich wird damit auch, die Lizenzverwaltung auf der Basis von Attributen umzusetzen.
Denkbar dabei auch – z.B. für Lehrpersonen, die an unterschiedlichen Schulen tätig sind - die Option eines ID-Wechsels, d.h. nach erfolgreicher Authentifizierung kann zu jeder anderen Identität gewechselt werden, die auf dieselbe BildungsID gemappt ist. Da die hinter der Identität stehende Person bereits authentifiziert wurde, ist eine erneute Abfrage von Berechtigungsnachweisen überflüssig.

7.4 Revokation

Die BildungsID als Identifikator kann nicht revoziert werden. Revoziert werden die mit diesem Identifikator verbundenen elektronischen Identitäten der Institution, die sie ausgegeben hat. Damit muss der jeweilige IDP in der Lage sein, Identitäten zu revozieren.

8 Zusammenspiel mit dem Projekt FIDES

Im Austausch mit educa.ch wurden Mitte Dezember 2018 die geplanten Schnittstellen zwischen der entworfenen BildungsID-Infrastruktur im Kanton Bern und der nationalen Infrastruktur diskutiert, die educa.ch im Auftrag der Schweizerischen Konferenz der kantonalen Erziehungsdirektoren (EDK) realisiert. Im Gespräch konnte die grundlegende Kompatibilität der Überlegungen auf kantonaler und nationaler Ebene bestätigt werden. Zu diesem Zeitpunkt war von Seiten des FIDES-Projektes noch nicht vollständig geklärt, welche in diesem Bericht vorgeschlagenen Infrastrukturkomponenten auf nationaler Ebene zur Verfügung gestellt werden und welche Elemente von den Kantonen realisiert werden müssen. Damit war die Systemgrenze (vgl. Abbildung 3) zwischen FIDES und der kantonalen Infrastruktur unklar.
In einem weiteren Gespräch mit educa.ch im Januar 2019 konkretisierte educa.ch diese Frage: Im Projekt FIDES wird erstens die Funktionalität des B-ID-Hubs realisiert, mit dem der Kernauftrag des Projektes erfüllt wird: die Föderation von unterschiedlichen Identitäten. Zweitens wird FIDES auch einen Identifikator und damit die Funktionalität eines B-ID-Register zur Verfügung stellen. Damit werden die wichtigsten Komponenten von FIDES realisiert (rechte Darstellung in Abbildung 3).

Ausgeschlossen ist hingegen, dass im Projekt FIDES ein IDP realisiert wird, der von allen Schulen genutzt werden kann. Ein verbindliches schriftliches Konzept zu dieser Ausgestaltung liegt noch nicht vor.

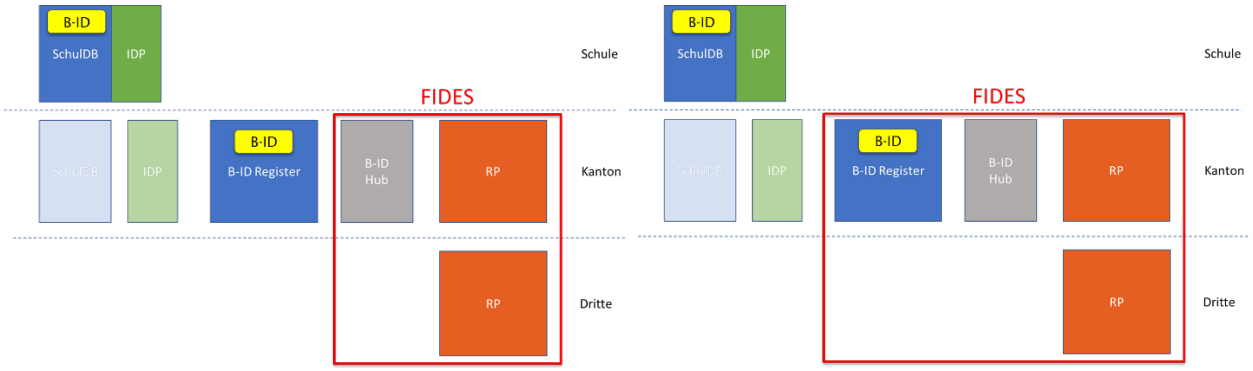

Abbildung 3 - Mögliche Systemgrenzen von FIDES

Es kann also vorläufig davon ausgegangen werden, dass eine Pilotierung im Kanton Bern mit den technischen Infrastrukturen aus dem Projekt FIDES durchgeführt werden kann.
Unabhängig von der Pilotierung mit den FIDES-Komponenten muss der Kanton Bern die Generierung von nutzbaren Identitäten aus den Schulverwaltungs-Systemen realisieren. Zu prüfen ist dabei, ob für diese Entwicklung eine Zusammenarbeit mit weiteren Kantonen realisiert werden kann.

9 Rückmeldungen der Stakeholder

In neun Gesprächen mit Vertreterinnen und Vertretern unterschiedlicher Stakeholdergruppen wurden, angepasst auf das Vorwissen der Akteure, der Kontext und die Ausganglage des Projektes geschildert, die Grundzüge der Lösungskonzeption vorgestellt und in halbstrukturierter Form sechs Fragen gestellt.

- Grundsätzliche Unterstützung für eine BildungsID
- Vor- und Nachteile des Lösungskonzeptes aus der Sicht der Stakeholder
- Spezifische Anforderungen an die Lösung aus der Sicht der Stakeholder
- Kritische Faktoren bei der Umsetzung
- Möglicher Beitrag der Stakeholder zum Gelingen der Lösung
- Weitere Bemerkungen zur BildungsID

Diese Stakeholderinterviews dienten neben der Erhebung von Positionen und der Gewichtung von Anforderungen auch der frühzeitigen Präsentation der Idee.
Die Gespräche von 45-60 min. werden in der Folge summarisch wiedergegeben.

9.1 Lehrpersonen

Die Sicht der Lehrpersonen wurde in zwei Gesprächen mit Vertreterinnen und Vertretern des VPOD Bern (Béatrice Stucki) und Bildung Bern (Christian Robert, Franziska Schwab und Stefan Wittwer) erhoben.

Die Vertreterin des VPOD führt aus, dass aus der Perspektive des Lehrpersonals eine BildungsID begrüsst wird, wenn sie in erster Linie der Vereinfachung und der administrativen Entlastung der Lehrpersonen dient. Die Einfachheit und die hohe Anwenderfreundlichkeit der Lösung sind dabei zentral. Spezifisch zu beachten ist dies auch für Lehrpersonen, die an mehreren Schulen tätig sind. Der Systemaufbau muss so gestaltet sein, dass die «gläserne Lehrperson» verhindert wird und eine detaillierte Nachvollziehbarkeit der Tätigkeiten der Lehrperson nicht möglich ist. Zu diesem Aspekt ist insbesondere auch eine klare Position der ERZ wichtig, dass der Zugang zu den Arbeitsinstrumenten und nicht deren Verwendung im Zentrum des Interesses sei. Der Zugang darf nicht als Kontrollinstrument missbraucht werden.

Im weiteren Kontext der Digitalisierung ist auch eine weiterhin zu gewährleistende Balance zwischen physischen/haptischen Lernformen und digitalen Instrumenten wichtig. Weiterhin müssen die Lehrpersonen mit entsprechender Infrastruktur befähigt werden, die Instrumente auch nutzen zu können. Bei der Umsetzung der BildungsID muss verhindert werden, dass die Platzierung von Produkten von Anbietern zur Regel wird und damit keine Ungleichheit zwischen grösseren, städtischen Schulen und ländlichen Schulen oder zwischen Kindern bildungsnaher und bildungsferner Eltern/Erziehungsberechtigten entsteht.
Ein weiterer zu diskutierender Aspekt aus der Sicht der Lehrpersonen ist die Definition und Umsetzung von Prozessen zum Sperren und ggf. Entzug der BildungsID. Eine einheitliche Lösung, die auch interkantonal einsetzbar ist, wäre wünschenswert. Zuletzt sind bei der Umsetzung auch die Aspekte der Barrierefreiheit zu beachten, damit der Beruf als Lehrperson auch Menschen mit Beeinträchtigung offensteht.

Die Vertreterin und die Vertreter von Bildung Bern sehen aufgrund der Alltagserfahrungen von Lehrpersonen die Idee eines einfachen und vielseitig einsetzbaren Identifikationsmittels sehr positiv. Die zentralen Anforderungen liegen aus ihrer Sicht in der Einfachheit und hohen Anwenderfreundlichkeit aber gleichzeitig auch in der hohen Sicherheit der Lösung und einer umfassenden Kontrolle darüber, wer welche Daten erhalten kann.
Ein Abgleich mit Einwohnerregistern wird als problematisch angesehen, da die Schule in der Lage sein muss, ohne Probleme auch Kinder ohne Aufenthaltstitel zu integrieren und mit einer BildungsID auszustatten. Im Kontext der BildungsID muss auch der Frage der Chancengleichheit Beachtung geschenkt werden: Es ist darauf zu achten, dass die Ausstellung und Benutzung für Schülerinnen und Schüler in der Schule erfolgt.
Christian Robert sieht die Beständigkeit der BildungsID für Lernende als Problem. Er plädiert dafür, diese am Ende der obligatorischen Schulzeit zu löschen und eine neue Identität für (Weiter-)Bildung im Erwachsenenalter zu haben.
Wichtig ist aus Perspektive der Lehrerinnen und Lehrer und insbesondere der Verantwortlichen für Medien und Informatik an den Schulen, dass mit der BildungsID eine erhebliche Vereinfachung der Lizenzierung digitaler Instrumente erreicht werden kann.
Eine weitere, zentrale Anforderung ist ein umfassender Support und eine gute Unterstützung der Lehrpersonen, sodass das eine BildungsID nicht zu einem zusätzlichen Aufwand und Störfaktor im Unterricht wird.
Weiter wird herausgestrichen, dass eine gute Kommunikation im Hinblick auf die Schaffung von Vertrauen in die Lösung erfolgen muss. Die Pilotierung der Lösung und lange Übergangsfristen helfen weiter, die Akzeptanz für dieses Instrument bei den Lehrpersonen zu stärken.

9.2 Schulleitung

Die Perspektive der Schulleitungen wurde mit Andreas Hachen, Co-Präsident des Schulleiterverbandes VSLBE diskutiert. Im Gespräch floss auch die spezifische Situation der Schule untere Emme ein, in der er Schulleiter ist.
Der Umgang mit Daten, Logins und Lizenzen bringt für die Schulen einen grossen Aufwand mit sich, nicht nur technisch, sondern auch in der Weiterbildung der Lehrpersonen. Insbesondere die aktuelle Situation mit der Verwaltung gerätebasierter Lizenzen ist sehr aufwändig. In der Schule untere Emme, als Beispiel eines relativ grossen Schulverbandes, bestehen sowohl pädagogische wie auch technische Richtlinien zum Umgang mit digitalen Instrumenten. Die Schulverwaltungslösung erlaubt einen wöchentlichen Abgleich mit den Daten der Einwohnerkontrolle. Die Schule löscht Daten über Schülerinnen und Schüler, die nicht zwingend archiviert werden müssen, nach deren Austritt, um nicht mehr den Schutz dieser Daten gewährleisten zu müssen.
Aus der Perspektive des Schulleiterverbandes sieht Andreas Hachen im Vorhaben generell eine Unterstützung, weil es den Aufwand und das Risiko für Schulen minimieren würde. Er sieht eine Dynamik bei den Schulen hin zu Schulverwaltungslösungen, sodass Schulen mit einer angemessenen Frist eine Umstellung auf eine Schulverwaltungslösung vornehmen könnten. Weiter soll mit einem passenden Rahmen auch das Vertrauen in das System gestärkt werden. Dieses soll vor allem durch das Engagement der ERZ für die Lösung gestärkt werden. Die Kontrolle der ERZ über die Zulassung der Dienste zum System ist aus der Sicht der Schulleiter nicht problematisch.

In der Kommunikation sieht er die Notwendigkeit, der Wahrnehmung, dass die Systeme immer teurer werden, auch den Nutzen und die generelle Frage der «digital fitness» der Schulen in den Vordergrund zu stellen. Unterstützung für das Vorhaben kann Andreas Hachen über Information an die Verbandsmitglieder leisten, es sind rund die Hälfte der Schulleitenden im Verband vertreten. Darüber hinaus sind auch Pilotanwendungen im Schulverband untere Emme denkbar.

9.3 Gemeindeverband

Die Sicht der Gemeinden wurde in einem Gespräch mit Daniel Arn, Geschäftsführer des Verbandes der Bernischen Gemeinden, erhoben.
Das Bedürfnis nach einer BildungsID ist für den Gemeindeverband unbestritten und wichtig, eine aktive Rolle des Kantons gegenüber den Anbietern wird begrüsst, um so auch die Marktmacht nutzen zu können. Aus der Perspektive des Beschaffungsrechts wären dazu Anpassungen der gesetzlichen Grundlagen notwendig, sodass der Kanton anstelle der Gemeinden beschaffen könnte. Eine konsistente Lösung ist aus Sicht des Gemeindeverbandes zu begrüssen, auch wenn ein Paradigmenwechsel Zeit braucht.
Aus der Sicht der Gemeinden ist die Standardisierung der Lösungen auf der Basis einer guten Evaluation zu begrüssen, damit wird viel Aufwand für die Schulen gespart. Ziel muss sein, Handlungsempfehlungen und gute Lösungen für die Gemeinden bereitstellen zu können. Rahmenverträge funktionieren dazu nur beschränkt.
Arn regt weiter an, dass die Lösung nicht an den spezifischen Bedürfnissen von Kleinstgemeinden auszurichten, sondern die mittleren Gemeinden als Orientierungspunkt für die Umsetzung zu sehen. Zentraler Erfolgsfaktor aus der Sicht des Gemeindeverbandes ist der Stakeholderdialog, der fortgesetzt werden muss. Neben den bereits angefragten Interviewpartnern könnte auch das Gespräch mit dem Verband der Schulbehörden im Kanton Bern gesucht werden.

9.4 Anbieter von Schulverwaltungslösungen

Zur Perspektive der Hersteller von Schulverwaltungslösungen gab Tino Gruse Auskunft, Mitglied der Geschäftsleitung von Roth Soft AG.
Aus seiner Sicht besteht eine grundsätzliche Unterstützung des Anliegens, hinzu kommt auch eine mögliche Rolle als Relying Party, da sich die Lehrpersonen auf Lehreroffice einloggen müssen. Im Hinblick auf den Austausch und die Nutzung von Daten erläutert Tino Gruse, dass ein Datenaustauschformat (xml) in Zusammenarbeit mit anderen Anbietern erarbeitet und implementiert wurde. Dieses erlaubt Datenimport bzw. Datenabgleich mit Scolaris, iCampus und weiteren Anwendung. LehrerOffice ist aber eher Instrument für die Lehrer, Daten kommen in den meisten Fällen von einer Schulverwaltungslösung, als Stand-alone ist LehrerOffice nur für kleine Schulen sinnvoll.
Sein Hauptanliegen im Hinblick auf eine BildungsID ist die Implementierung einer Schnittstelle für alle Kantone (in ihrem Fall nur D-CH-Kantone), Sonderlösungen für jeden Kanton machen die Umsetzung zu teuer. Aus seiner Sicht besteht im Markt ein grosses Bedürfnis nach einer Verbindung mit dem Microsoft-Login. Eine Verbindung der Bildungs-ID mit den Angeboten von Microsoft ist deshalb unbedingt anzustreben.

In einem weiteren Gespräch mit einem Hersteller von Schulverwaltungslösungen gab Thomas Oberle, Leiter Scolaris EDU bei PMI.AG, Auskunft.
Die BildungsID ist für Scolaris von grossem Interesse, insbesondere auch die Ergebnisse aus dem Projekt FIDES. Bereits heute sind Identifikationsprozesse mit der Lösung machbar, offen ist aber immer wieder die Frage, wie die Beteiligten (Schüler, Lehrpersonen, Schulverwaltung, Eltern, etc.) mit einer elektronischen ID eingebunden werden können. Deshalb verfolgt der Hersteller unter anderem die Entwicklung der SwissID. PMI.AG ist bereits jetzt in der Lage, als Identitätsprovider zu wirken oder mit Scolaris Connect die Daten aus der Schulverwaltung Scolaris mit einem Active Directory oder einem Azure Active Directory abzugleichen. Weiter bestehen viele Standard-Schnittstellen mit den Systemen der Einwohnerkontrollen, basierend auf dem Datenstandard eCH-0020. Bestehend ist auch das Angebot, die Schulverwaltungslösung Scolaris «as a service» zu nutzen, was kleineren und dezentral organisierten Schulen entgegenkommt.

Zentrale Anforderung aus Sicht von Scolaris ist eine allgemeine Lösung, die breit genutzt werden kann. Das heisst, dass der technische Standard die Anbindung an unterschiedliche Anbieter erlaubt. Die Kompatibilität mit nationalen Lösungen wie FIDES oder Swiss EDU-ID sind zentral, auch um Handhabbarkeit über Kantonsgrenzen hinaus gewährleisten zu können.
Aus den bisherigen Erfahrungen als Anbieter ist die Implementierung verschiedener Rollen für eine Identität (z.B. bei Pensen in unterschiedlichen Schulen) eine Anforderung, die berücksichtigt werden muss. Für eine Pilotierung verweist Thomas Oberle darauf, dass unterschiedliche Schulen im Kanton Bern bereits die Steuerung der Identitätsverwaltung in Office 365 über die Schulverwaltungslösung implementiert haben.

9.5 Lehrmittelverlage

Für den Lehrmittelverlag Plus gab der Verlagsleiter Bernhard Kobel Auskunft.
Von Seiten des Schulverlages besteht ein grosses Interesse an einer BildungsID, denn die einfache Identifikation ist geschäftskritisch für die Verlage. Ohne einfachen Zugang und einfache Lizenzverwaltung wird die Legitimation für das Geschäftsmodell der Verlage wegbrechen.
Das aktuelle Lizenzmodell und die Lizenzverwaltung generieren viel Aufwand, eine einfachere Lösung ist in Arbeit, das Abstützen der Lösung auf Attribute einer BildungsID würde eine weitere Vereinfachung bedeuten. Kobel sieht den aktuellen Lehrmittelmarkt mit unterschiedlichen Anbietern als Garant für Vielfalt und Qualität.
Nicht zuletzt ist auch die Verwaltung der Schülerdaten mit Aufwand und Risiko verbunden, ohne dass der Verlag ein Interesse an der genauen Identität der Benutzerin/des Benutzers hat. Die Umsetzung einer BildungsID und damit als mögliche Entwicklung einhergehend, eine vermehrte Lizenzierung auf der Ebene der Schulen, würde Lehrmittelentscheidungen auf der Ebene der Schule fördern, was eine grosse Vereinfachung und mehr Möglichkeiten der Zusammenarbeit zwischen Lehrpersonen schaffen würde. Eine weitere Entwicklung hin zu kantonalen Entscheidungen zu Lehrmitteln und der entsprechenden Lizenzierung auf Ebene des Kantons, wäre ebenfalls denkbar. Bereits heute existieren die Gremien und die Prozesse zur Zulassung von Lehrmitteln auf kantonaler Ebene. In der vielschichtigen Diskussion um die BildungsID steht die administrative Vereinfachung im Umgang mit Lizenzen für Schulen, Lehrpersonen und Verlagen im Zentrum. Als Risiko sieht Kobel die Umsetzung von Spezialfällen wie Lehrpersonen, die an zwei Schulen tätig sind. Diese können die Komplexität der BildungsID und damit den zentralen Aspekt der Anwenderfreundlichkeit beeinträchtigen.
Zentrale Anforderung aus der Sicht eines Verlages ist eine nationale Lösung, denn die Implementation kantonaler Lösungen schafft zu grossen Aufwand. Kobel wünscht sich zudem eine Lösung, die mit einer möglichst kleinen kantonalen Intervention auskommt, um das Risiko der Komplexität und der hohen Kosten zu minimieren.

Mit Manuel Schär, Verlagsleiter des hep-Verlages, konnte die Sicht auf die Lösung mit Schwerpunkt auf Sek II diskutiert werden.
Zu Beginn erläutert der Verlagsleiter die Ausrichtung des Verlages mit Schwerpunkt in den Berufs- und Berufsmaturitätsschulen sowie Gymnasien. Einzelne Titel werden auch in der Volksschule eingesetzt. Eine Möglichkeit für den einfachen Zugang zu den Angeboten, ein «single-sign-on» für unterschiedliche Lernangebote ist ein Bedürfnis, das von den Schulen geäussert wird, wobei auch teilweise die Meinung vertreten wird, dass sowieso zahlreiche Logins im Einsatz sind und eine Vereinheitlichung bei den Lehrmitteln nicht so sehr ins Gewicht fällt. Trotz dieser Einzelmeinungen besteht von Seiten des Verlages ein grosses Interesse an einer BildungsID.
Manuel Schär wies darauf hin, dass für den Erfolg der Lösung auch die unterschiedlichen Geschäftsmodelle der Verlage berücksichtigt werden müssen. Für seinen Verlag mit Kunden in der Sek II-Stufe werden Lehrbücher und digitale Angebote von den Lernenden selbst gekauft, allenfalls auch von den Lehrbetrieben oder den Eltern. Damit müssen für diese Anwendungsfälle auch eine Vertragsbeziehung und ein Zahlungsprozess vom Verlag zu den Lernenden funktionieren.
Für die Frage der Datennutzung und das Konzept der Datensparsamkeit hat Schär zwei Sichten: Einerseits kann die Pseudonymisierung den Verlag entlasten, andererseits besteht ein Interesse an weiteren demografischen Daten der Nutzenden, um die Verwendung der digitalen Angebote zu erfassen und für die Weiterentwicklung der Lösungen zu nutzen. Eine Verwendung dieser Daten zu Werbezwecken schliesst Schär aktuell aus.

Um einen verhältnismässigen Implementierungsaufwand sicherzustellen, ist eine nationale Lösung anzustreben. Manuel Schär merkt weiter an, dass eine Ablösung ihrer eigenen Identitätsverwaltung nicht denkbar sei, denn ihre digitalen Inhalte werden auch in vielen unterschiedlichen Kurs- und Weiterbildungsformaten genutzt, ausserhalb der grossen Bildungsinstitutionen.

9.6 Datenschutz-Aufsichtsstelle

Der Aspekt des Datenschutzes wurde mit Urs Wegmüller, wissenschaftlicher Mitarbeiter bei der Datenschutz-Aufsichtsstelle des Kantons besprochen.
Aus der Sicht von Urs Wegmüller sind einige Design-Entscheidungen zentral: Eine Umsetzung, die zentral die Logik der Erfassung bestimmt und auch Support für die erfassenden Stellen bietet. Die Etablierung einer Vertrauensbeziehung zu den RPs muss über eine Vertragsbeziehung geregelt werden. Eine besondere Herausforderung aus der Sicht des Datenschutzes entsteht mit der Generierung von Inhalten, die die Leistung der Schülerinnen und Schüler reflektieren. Diese Inhalte werden als besonders schützenswerte Personendaten angesehen und damit muss ein Informations- und Datensicherheits-Konzept der Applikationsanbieter vorliegen. Weiter wäre es angebracht, dass diese Daten durch einen zweiten Authentifikationsfaktor zu schützen. Eine vertiefte Prüfung muss auf der Basis genauerer Spezifikationen erfolgen.

10 Fazit und Empfehlungen

Der Tenor der Gespräche mit den Stakeholdern und die in den Workshops geäusserten Bedürfnisse zeigen, dass der Handlungsbedarf von allen Seiten deutlich gesehen wird. Insbesondere die Wünsche nach einer Vereinfachung des Zugangs zu digitalen Angeboten und der Verwaltung von Lizenzen für digitale Angebote werden hervorgestrichen.
In dieser Situation ist baldige und konsequente Umsetzung des Vorhabens angezeigt, auch wenn von Seiten der Schulen und der Lehrpersonen der Wunsch nach längeren Übergangsfristen geäussert wird. Mit einer BildungsID als Identifikations- und Authentifizierungsmittel wird die Grundlage für eine Vielzahl digitaler Prozesse geschaffen. In Kombination mit einer komplexen Struktur von Beteiligten und Schnittstellen im Bildungswesen besteht das Risiko, dass sehr viele Anforderungen an die BildungsID gestellt werden. Die Workshops mit Vertreterinnen und Vertretern des AKVB und des MBA zeigen die klare Priorisierung der Nutzung einer BildungsID durch Lehrpersonen, Schulverwaltung und Lernende, um sich an Applikationen des Kantons und Applikationen von Dritten zu authentisieren. Dieser Fokus soll für die weitere Arbeit beibehalten werden.

Eine zentrale Herausforderung, die für die Umsetzung einer Lösung angegangen werden muss, ist eine Steigerung der Maturität der Instrumente, die zur Verwaltung der Identitätsdaten in den Schulen eingesetzt werden. Definierte Schnittstellen zwischen den Systemen der Einwohnerkontrolle, der Schulverwaltung und von Identitätsdiensten müssen vorhanden sein, um eine BildungsID automatisiert zur Verfügung zu stellen. Die Datenverwaltung mit Office-Tools und Datenbanken bietet dazu keine genügende Grundlage. Um diese Umstellungen erfolgreich zu bewältigen und die erforderliche Maturität zu erreichen, bedürfen die Schulgemeinden, die aktuell Office-Tools für die Schulverwaltung nutzen, der inhaltlichen und organisatorischen Unterstützung durch den Kanton.

Eine wichtige Anforderung, die von verschiedener Seite gegenüber dem Vorhaben geäussert wird, ist der konsequente Schutz persönlicher Daten. Insbesondere die Auswertung von Nutzungsverhalten oder der Leistung von Lehrpersonen soll nicht möglich sein. Die vorgeschlagene Lösungsarchitektur mit einem Hub erlaubt es, sowohl vertragliche Auflagen als auch das Prinzip der Datensparsamkeit zu implementieren. Damit werden Grundlagen geschaffen, um den Erhalt und die Nutzung von Daten zentral zu steuern und verbindliche, durchsetzbare Regeln zu definieren. Dies stellt eine erhebliche Verbesserung gegenüber der heutigen Situation dar, in der trotz Empfehlungen keine einheitliche und kontrollierbare Praxis besteht. Die Verwendung von Daten auf einer Lernplattform erlaubt aber keine vollständige Anonymisierung, so muss beispielsweise die Zuordnung zu einer Klasse erfolgen können, die Rückschlüsse auf die Person vereinfachen.
Die Bereitstellung einer Identität und die Frage des Umgangs mit den Daten sind zu trennen. Die vorgeschlagene Lösung erlaubt die Definition und Umsetzung von Regeln. In diesen Regeln kann die

Auswertung von Daten zu Nutzungsgewohnheiten und deren Weitergabe eingeschränkt oder verboten werden. Diese Auswertungen durch Anonymisierung zu verhindern, ist mit Blick auf die für eine funktionierende Lernumgebung erforderlichen Informationen nicht möglich.

Neben der inhaltlichen Aufbereitung der Anforderungen und der Zielarchitektur konnten im Hinblick auf die Umsetzung unterschiedliche Stakeholder in die Überlegungen einbezogen werden:
Erstens konnte eine Klärung der konkreten Ausgangslage erreicht werden, um die Sicht des Kantons Bern noch besser in die Arbeiten von FIDES einbringen zu können. Die Gespräche mit educa.ch im Projektverlauf haben zu einer Klärung des Umfangs von FIDES beigetragen. Die Äusserungen der Softwareanbieter und der Schulverlage zeigen klar, dass eine nationale Lösung gefunden werden muss, damit der Aufwand für die Implementierung nicht multipliziert wird. Die Akzeptanz für kantonale Lösungen ist demnach bei dieser Akteursgruppe limitiert. Die vorgeschlagene Infrastruktur passt mit dem Projekt FIDES insofern zusammen, als dass das Element des B-ID Hubs für eine nationale Verwendung vom Projekt FIDES entwickelt wird. Weiter kann vorläufig davon ausgegangen werden, dass auch das Element des Identifikators und des dazugehörigen Registers von FIDES zur Verfügung gestellt wird. Einen IDP wird das Projekt hingegen nicht zur Verfügung stellen. Für eine Pilotierung im ersten Halbjahr 2019 stehen die Elemente von FIDES zur Verfügung. Einzelne Pilotschulen mit einer Schulverwaltungslösung, die die Generierung einer B-ID erlauben, können einbezogen werden.

Eine Pilotierung der BildungsID im Kanton Bern kann in einem ersten Schritt mit einigen Elementen von FIDES erfolgen und so die Prozesse der Ausgabe, der Nutzung und der Revokation getestet werden. Alternative Pilotierungsvarianten wurden ebenfalls geprüft und könnten bei Bedarf als Alternative zur Pilotierung im Rahmen von FIDES vertieft werden. Als Pilotszenario ist eine Konstellation von zwei Schulen und zwei Applikationen angestrebt. Für eine Pilotierung mit Test-Identitäten können Schulen eingebunden werden, die bereits in der Lage sind, funktionsfähige Identitäten zu generieren. Dazu gehören Mittel- und Berufsschulen, die aus Evento Identitäten bilden können und Volksschulen, die eine Schulverwaltungslösung benutzen. So ist beispielsweise in Scolaris die Bildung elektronischer Identitäten möglich. Auf der anderen Seite haben Schulverlage ebenfalls Interesse an der Pilotierung angemeldet.
Für einen Pilotversuch ohne FIDES-Infrastruktur könnte das BildungsID-Register eine von Hand geführte Liste sein und muss noch nicht als automatisierte Komponente zur Verfügung stehen. Der Hub könnte – basierend auf den geschilderten Varianten – für einen Piloten entweder als eigenständige Komponente betrieben werden oder aber es wird eine Identität benutzt, die die Hub-Funktionalität bereits mitbringt. Im ersten Fall kann dazu eine Verwendung des IDV Schweiz in Betracht gezogen werden, während für den zweiten Fall eine Nutzung der Swiss EDU-ID von Switch zu prüfen wäre.

Zusammenfassend empfehlen die Autoren der Studie weitere Aktivitäten in drei Richtungen:

1. Eine Pilotierung der BildungsID im Kanton Bern ist so bald wie möglich zu realisieren. Ziel muss es sein, mit zwei Schulen und zwei Applikationen erste Erfahrungen zu sammeln. Dazu kann entweder die Infrastruktur mit einem IDP und einem von FIDES betriebenen Identitäts-Hub genutzt oder, falls die Pilotierung nicht zu Stande kommt, mit existierenden Infrastrukturen operiert werden. Dazu bietet sich auf den ersten Blick die Nutzung der Swiss edu-ID von Switch an in Kombination mit Schulen, die mit Scolaris oder Evento verwaltet werden.

2. Für eine kantonale BildungsID müssen insbesondere diejenigen Schulen eine Weiterentwicklung ihrer IT-Infrastruktur anstreben, die heute die Schulverwaltung mit gängigen Office-Produkten bewältigen. Für eine Schaffung einer digitalen Identität ist die Nutzung einer Schulverwaltungslösung notwendig, welche die Daten in einem passenden Format automatisiert für die Ausgabe digitaler Identitäten zu Verfügung stellen kann. Dieser Entwicklungsschritt ist für jegliche Art der Bereitstellung digitaler Identitäten Voraussetzung, damit ein zuverlässiger, automatisierter Abgleich durchgeführt werden kann. Um diesen Schritt umzusetzen, empfehlen die Autoren in einem ersten Schritt Anforderungen zu definieren, welche Daten exportiert werden können müssen und in welchem Format diese

Daten übertragen werden können müssen. Auf der Basis dieser Anforderungen sind insbesondere die organisatorischen und rechtlichen Fragen zu klären, die es der ERZ ermöglichen, die Gemeinden in der Modernisierung ihrer Infrastruktur zu unterstützten. In den Gesprächen und Workshops wurden die Möglichkeiten von Rahmenverträgen oder auch des Leistungseinkaufs durch den Kanton für die Gemeinden erwähnt, alle Varianten sowie ihre Machbarkeit und Konsequenzen sind zu prüfen.

3. Insbesondere die Anbieter von Schulverwaltungslösungen und die Verlage machen deutlich, dass sie nicht eine spezifische Berner Lösung implementieren wollen und können. Auch von Seiten der Lehrpersonen besteht der Wunsch, dass eine BildungsID auch über die Kantongrenzen hinaus funktionieren soll. Um dieses Ziel zu erreichen, müssen die Chancen des Projektes FIDES genutzt werden und die Arbeiten kritisch-konstruktiv begleitet werden. Auf diesem Weg kann eine nationale Lösung geschaffen werden.

11 Abbildungsverzeichnis

12 Tabellenverzeichnis

13 Literaturverzeichnis

Brugger, J., Buchser, N., Selzam Th.: Ökosystem eID in der Bildung, https://www.educa.ch/sites/default/files/uploads/2017/10/oekosystem_e-id.pdf (Abgerufen am 28.1.2019)

eCH: eCH-0107 Gestaltungsprinzipien für die Identitätsund Zugriffsverwaltung (IAM), http://www.ech.ch/dokument/167ccf46-b902-4b58-88f2-eed05ed58c05 (Abgerufen am 28.1.2019)

eCH: eCH-0170 Qualitätsmodell zur Authentifizierung von Subjekt, http://www.ech.ch/dokument/e0bf1a15-42e6-48f5-9bf3-28b293d5a52f (Abgerufen am 28.1.2019)

14 Versionskontrolle

Version	Datum	Beschreibung	Autor
0.1	19.09.2018	Dokument erstellt	Jérôme Brugger
0.2	11.10.2018	Dokument ergänzt	Jan Frecè, Jérôme Brugger
0.3	15.10.2018	Dokument bearbeitet / ergänzt	Jan Frecè, Jérôme Brugger
0.4	19.10.2018	Dokument ergänzt	Jan Frecè
0.5	13.12.2018	Resultate Interviews ergänzt	Jérôme Brugger
1.0	20.12.2018	Dokument fertiggestellt	Jan Frecè, Jérôme Brugger
1.1	28.1.2019	Rückmeldungen eingearbeitet	Jérôme Brugger
1.2	13.3.2019	Präzisierung einer Formulierung in Kap. 9.2	Jérôme Brugger