EDK | CDIP | CDPE | CDEP |
Schweizerische Konferenz der kantonalen Erziehungsdirektoren
Conférence suisse des directeurs cantonaux de l'instruction publique
Conferenza svizzera dei direttori cantonali della pubblica educazione
Conferenza svizra dals directurs chantunals da l'educaziun publica

Beschluss Plenarversammlung
27. Juni 2019

Föderation von Identitätsdiensten im Bildungswesen: Beschlussfassung

Das Generalsekretariat berichtet:

1 Am 22. März 2018 hat die Plenarversammlung beschlossen, dass mit einer Föderation von Identity- und Access-Management-Systemen ein einziger Zugang zu Online-Diensten für Schülerinnen und Schüler, Lernende, Lehrpersonen und Verwaltungspersonal der Bildungsinstitutionen zur Verfügung gestellt werden soll. Die Föderation soll zudem ermöglichen, Online-Dienste auch privater Anbieter koordiniert zu beschaffen und zu nutzen, beispielsweise über die Aushandlung von Rahmenvereinbarungen.

2 Die Projektleitung für den Aufbau der Föderation wurde der Fachagentur educa.ch übertragen. Diese hat die notwendigen Grundlagen für die Föderation entwickelt und anhand von Pilotprojekten mit Dienstleistungsanbietern und Pilotkantonen die Anwendungsfälle und -szenarien getestet. Die Pilote zeigen, dass die Bereitschaft der Anbieter digitaler Dienste und der Lehrmittelverlage, jetzt der Föderation beizutreten, hoch ist. Im Zusammenhang mit den bereits durchgeführten und noch laufenden Pilotprojekten richten Anbieter zur Zeit ihre Geschäftsprozesse auf die Föderation aus.

3 Es wurden laufend Kommunikationsmaterialien zur Föderation und den verschiedenen Nutzungsfällen entwickelt und über fides.educa.ch zugänglich gemacht.

4 Die Projektleitung legt nun den Bericht «Grundlage für die Einführung der Föderation der Identitätsdienste im Bildungsraum Schweiz» mit diversen Beilagen vor, der die wesentlichen Elemente der Föderation beschreibt und in Bezug setzt zur Ausgangslage in den Kantonen.

4a Die Föderation ist auf ihre Grundfunktion, den datenschutzkonformen Zugang zu digitalen Diensten für Schülerinnen und Schüler, Lernende und Lehrpersonen (der Primarstufe, Sekundarstufe I, Sekundarstufe II, beruflichen Grundbildung) ausgelegt. Sie föderiert die bestehenden und noch aufzubauenden Identitätsdienste.

4b Verwendet wird ein personenbezogener, über den gesamten Bildungsweg (inkl. Tertiärbereich) eindeutiger Identifikator. Die gegenseitige Durchlässigkeit der Föderation mit dem Tertiärbereich (Switch-Dienste) ist gewährleistet. Sollte sich künftig eine nationale, bereichsübergreifende nationale Identitätslösung etablieren, kann die Föderation in diese überführt werden.

4c Die aktuelle Situation in Bezug auf digitale Identitäten in den Kantonen wurde im Bericht *Landschaft der digitalen Identitäten im Bildungsraum Schweiz* vom 15. März 2019 dargelegt. Die Informationen daraus dienten als Grundlage für die weiteren Arbeitsschritte.

4d Die Aspekte des Datenschutzes wurden unter Einbezug der Konferenz der schweizerischen Datenschutzbeauftragten (privatim) geklärt und im Bericht Datenschutz-Folgeabschätzung vom 5. April 2019 beschrieben. Mit Bezug auf die Architektur wird das Konzept «privacy by design» verfolgt.

5 Die jährlichen Kosten für den Betrieb der zentralen Infrastruktur der Föderation werden auf Basis der geklärten Gesamtarchitektur auf CHF 1'840'000 veranschlagt. Der in Budget und Finanzplan der EDK

eingestellte Beitrag von CHF 987'000 p.a. beruht auf der Kostenschätzung von 2017 und muss um CHF 200'000 auf jährlich CHF 1'187'000 erhöht werden.

6 Die vorliegenden Grundlagen erlauben es den Kantonen, die für den Beitritt zur Föderation notwendigen rechtlichen und organisatorischen Voraussetzungen zu prüfen und ihre Beitrittsbereitschaft zu klären. Das Vorgehen für den Beitritt liegt in Form von Prozessdefinitionen vor, die Projektleitung unterstützt die Kantone bei der weiteren Klärung. Angestrebt wird eine schweizweit flächendeckende Nutzungsmöglichkeit durch die Bildungsteilnehmer binnen dreier Jahre.

7 Für die Föderation wird ein externes Finanzcontrolling vorgesehen.

8 Die operativen Aufgaben der Föderation werden einer Geschäftsstelle übertragen, die von der Fachagentur educa.ch geführt wird. Der technische Betrieb wird mittels Ausschreibung vergeben.

9 Der definitive Beschluss für die Einführung und den Betrieb der Föderation soll der Plenarversammlung für ihre Sitzung vom 24./25. Oktober 2019 vorgelegt werden. Die Inbetriebnahme kann so per 1. Januar 2020 erfolgen, mit Schulbeginn 2020/21 kann damit aus ersten Kantonen flächendeckend via Föderation auf Dienste zugegriffen werden können.

Die Plenarversammlung beschliesst:

1 Der Bericht «Grundlage für die Einführung der Föderation der Identitätsdienste im Bildungsraum Schweiz» wird zur Kenntnis genommen.

2 Die Steuergruppe wird beauftragt, der Plenarversammlung für ihre Sitzung vom 24./25. Oktober 2019 die definitiven Entscheidgrundlagen für Einführung und Betrieb der Föderation vorzulegen.

3 Die Mitglieder der EDK werden eingeladen, bis zu diesem Datum ihre Beitrittsbereitschaft zu klären.

Bern, 27. Juni 2019

Schweizerische Konferenz der kantonalen Erziehungsdirektoren
Im Namen der Plenarversammlung:

sig.

Susanne Hardmeier
Generalsekretärin

Anhang:
- Bericht «Grundlage für die Einführung der Föderation der Identitätsdienste im Bildungsraum Schweiz» vom 29. Mai 2019

Zustellung an:
- Mitglieder der EDK
- Steuergruppe Aufbau FIDES
- Staatssekretariat für Forschung, Bildung und Innovation (SBFI)

Dieser Beschluss wird auf der Website der EDK publiziert.

232.3-1.21 ako

FIDES
FÖDERATION DER IDENTITÄTSDIENSTE
FÉDÉRATION DES SERVICES D'IDENTITÉS

Grundlage für die Einführung der Föderation der Identitätsdienste im Bildungsraum Schweiz

Dossier z. H. der EDK-Plenarversammlung

29.05.2019

educa.ch

INHALTSVERZEICHNIS

MANAGEMENT SUMMARY

Die zentralen **Grundlagen** liegen vor. Sie weisen Bedarf und Machbarkeit einer Föderation der digitalen Identitätsdienste als Herzstück der Digitalisierung im Bildungsraum Schweiz aus. Die Architektur, Geschäftsprozesse und Organe sind dokumentiert. Als Basis dienen Abklärungen mit einer überwiegenden Mehrheit der Kantone und mit einer repräsentativen Auswahl von Lehrmittelverlagen und Online-Diensten. Vertreterinnen und Vertreter aller Anspruchsgruppen äussern sich klar für eine zeitnahe Umsetzung der Föderation.

Die **Standortbestimmung** (educa.ch 2019b) macht drei Modelle für Generierung und Verwaltung digitaler Bildungsidentitäten sichtbar. Innerhalb dieser Modelle bestehen zum Teil erhebliche Unterschiede von einem Kanton zum andern. Dieser Bericht dient zusammen mit der Datenschutzfolgenabschätzung als Referenzquellen für die technische und rechtliche Implementierung der Föderation.

In der **Kostenschätzung** werden die zentralen EDK-Leistungen und die individuellen Kantonskosten auseinandergehalten. Die zwei Ebenen unterscheiden sich in ihrer Verbindlichkeit:

- Verlässliche Angaben sind für die technische Installation und den Betrieb der Föderation möglich. Diese Kosten werden durch die EDK nach dem etablierten Verteilschlüssel getragen.
- Sehr unterschiedlich sind die Bereitstellungs- und Beitrittsaufwendungen für die einzelnen Kantone. Diese Kosten stehen in direktem Zusammenhang mit dem individuellen Vorgehen pro Kanton (vgl. Kapitel 5). Sie werden individuell im Verlauf des bevorstehenden Klärungsprozesses mit jedem Kanton erarbeitet.

Das **Beitrittsverfahren** für Identitätsanbieter (IdP) ist dokumentiert (vgl. educa.ch 2019a). Es strebt auf der technischen Ebene minimale Umstellungen der bestehenden Identitätsdienste an. Das Pendant für die Dienstleistungsanbieter (SP) erfolgt auf der gleichen Basis nach dem Entscheid der Plenarversammlung im Juni 2019. Die Architektur und Prozesse sind bewusst so gestaltet, dass jeder Kanton frei über die Granularität seiner Mitwirkung entscheiden kann. Im Vordergrund stehen zwei Hauptszenarien:

- Zentral: Der Kanton bindet alle Bildungsinstitutionen in die Föderation ein. Dabei unterscheidet er allenfalls Volksschule und Sekundarstufe II (inkl. Berufsbildung).
- Individuell: Der Kanton überlässt es den einzelnen Bildungsinstitutionen bzw. Schulgemeinden, der Föderation beizutreten. Eine spätere Bündelung der Föderationsmitgliedschaft auf Kantonsebene ist jederzeit möglich.

Der Beitritt zur Föderation durch einzelne Identitätsdienste ist an keine organisatorischen Vorbedingungen wie z. B. die Zentralisierung innerhalb des Kantons gebunden. Wichtig ist bloss, dass der einzelne Kanton das bevorzugte Vorgehen vor dem Start des Beitrittsverfahrens klärt.

Die **Organisationsstruktur** der Föderation besteht aus einer Steuergruppe, einer Geschäftsstelle und einem Technischen Betrieb. Die Trennung dieser drei Ebenen bietet Gewähr für kohärente Governance unter der Verantwortung der EDK. Die Geschäftsstelle wird für die operative Steuerung zwischen den Interessen der Bildung sowie den Markt- und Technologieentwicklungen verantwortlich sein. Nach Einschätzung des GS EDK ist die Fachagentur educa.ch dafür prädestiniert. Der technische Betrieb gilt als kritische Infrastruktur. Er wird zeitlich befristet ausgeschrieben und in einem selektiven Verfahren durch die Plenarversammlung der EDK vergeben.

Die Föderation ist auf die **Besonderheiten der obligatorischen Schule und der Sekundarstufe II (inkl. Berufsbildung)** ausgerichtet. Die Durchlässigkeit mit dem Tertiärbereich (SWITCH) ist gewährleistet (Cross Federation). Die Architektur basiert auf sektorenspezifischem ID-Management und hält somit den Weg für ein mögliches Szenario mit einer späteren «nationalen Lösung» bewusst offen.

Nach dem Beschluss durch die Plenarversammlung am 27. Juni 2019 kann die Geschäftsstelle ihre Arbeit am 1. Januar 2020 aufnehmen. Für den technischen Betriebsstart im Frühling 2020 kommen vorab die Pilotpartner (Pilotkantone und -dienstleister) infrage. Die Voraussetzungen für einen flächendeckenden Betrieb werden bis Schulbeginn 2020/21 erfüllt sein.

1 Funktionen, Anforderungen und Möglichkeiten der Föderation

Die Föderation föderiert die digitalen Identitätsdienste der obligatorischen Schule und der Sekundarstufe II (inkl. Berufsbildung) im Bildungsraum Schweiz. Die Identitätsdienste der Kantone, Gemeinden und Schulen bilden den Kern der Föderation. Zentrale Partner sind die Dienstleistungsanbieter von Online-Diensten im Bildungsbereich.

Durch die Föderierung der Identitätsdienste schaffen die Kantone ein Instrument, das ihnen die Hoheit über Zuweisung und Nutzung der digitalen Identitäten samt ihren Attributen im Bildungsraum Schweiz langfristig gewährleistet. So entsteht im dynamischen Technologie- und Marktumfeld ein verlässlicher Vertrauensraum mit vereinbarten Regeln und Rechtssicherheit.

1.1 Funktionen der Föderation

Die Föderation richtet einen datenschutzkonformen Zugang zu digitalen Diensten im Bildungsraum Schweiz für Schülerinnen und Schüler, Lehrpersonen und Verwaltungspersonal ein.

Sie stellt keine eigenen digitalen Identitäten bereit, sondern föderiert die bestehenden und noch aufzubauenden Identitätsdienste der Kantone, Gemeinden und Schulen.

Ein personenbezogener Identifikator ermöglicht die eindeutige Identifikation für jeden Endbenutzenden über den gesamten Bildungsweg.

1.2 Technik, Sicherheit und Datenschutz

Die technische Architektur der Föderation ist ausgearbeitet und geklärt. Sie basiert auf dem offenen Standardprotokoll SAML 2.0 (vgl. Föderationsarchitektur; educa.ch 2019a). Die technische Architektur ist eine sicherheitsrelevante Infrastruktur. Details dazu werden auf Anfrage bei educa.ch zugänglich gemacht.

Der Datenschutz ist über die Datenschutz-Folgenabschätzung (educa.ch 2019c) in Zusammenarbeit mit privatim geklärt. Die Risiken der Föderation wurden erkannt und sind mit Massnahmen unterlegt. Die Datenschutz-Folgenabschätzung wird von den kantonalen Datenschutzbeauftragten validiert.

1.3 Möglichkeiten durch die Föderation

Mit der Föderation der bestehenden und noch aufzubauenden Identitätsdienste eröffnen sich den Kantonen in Zukunft weitere Möglichkeiten, den digitalen Bildungsraum Schweiz auf gesamtschweizerischer Ebene aktiv zu gestalten und ihre hoheitliche Aufgabe besser wahrnehmen zu können.

Der Übergang in die Tertiärstufe wird mittels einer geplanten «Cross Federation» mit der bereits bestehenden Föderation von SWITCH gewährleistet.

Eine allfällige bereichsübergreifende nationale Identitätslösung wird von der Föderation antizipiert. Die geplante technische Umsetzung der Föderation erlaubt eine Überführung in eine derartige Identitätslösung.

2 Erkenntnisse aus der Standortbestimmung

Das Projektteam FIDES hat im Rahmen des Aufbauprojekts von Februar bis Dezember 2018 die Identitätsanbieter der Kantone besucht, um den Stand der Dinge bezüglich der Verwaltung von Identitäten festzuhalten. Die Ergebnisse wurden im Bericht «Landschaft der digitalen Identitäten im Bildungsraum Schweiz» (educa.ch 2019b) festgehalten.

2.1 Drei technische Modelle

Drei generische Modelle der technischen Infrastruktur der Identitätsdienste konnten im Bildungsraum Schweiz identifiziert werden:

- M1: Der Kanton stellt digitale Identitäten bereit und verwaltet die Attribute in einer zentralen Schulverwaltungslösung (vgl. educa.ch 2019b, S. 10).
- M2: Der Kanton stellt zentrale Schulverwaltungslösungen bereit. Die Schule generiert und verwaltet auf der Basis der zentralen Schulverwaltungslösung digitale Identitäten (vgl. educa.ch 2019b, S. 11).
- M3: Schulen haben ein eigenes Identitätsmanagement inklusive Schulverwaltungslösung und verwalten diese selbstständig (vgl. educa.ch 2019b, S. 12).

Der Zugang zu Cloud-Diensten (wie beispielsweise Microsoft O365) wird über diese bestehenden Modelle gewährleistet (vgl. educa.ch 2019b: S. 13).

2.2 Organisatorische Vielfalt

Die in der Standortbestimmung beschriebenen Modelle der technischen Infrastruktur der Identitätsdienste beinhalten zwar auch organisatorische Komponenten. Letztendlich sind die in den einzelnen Kantonen vorhandenen Organisationsformen vielfältiger Natur. Die Modelle geben aber nicht vor, wie die Organisation der Identitätsdienste zu gestalten ist. Beispielsweise kann der Identitätsdienst einer grossen Gemeinde im Sinne von Modell 1 aufgebaut sein. Die Modelle enthalten in Bezug auf den Beitritt zur Föderation unterschiedliche Kostentreiber (vgl. Kapitel 4.2).

Einige Kantone haben ihre Identitätsdienste bzw. ihren Identitätsdienst zentral organisiert und decken damit alle Schulstufen ab. In anderen Kantonen wird ein zentraler Identitätsdienst nur auf einzelnen Schulstufen zur Verfügung gestellt (häufig auf Sekundarstufe II (inkl. Berufsbildung)) und die Gemeinden sind frei in der Organisation ihrer Identitätsdienste. Es existieren auch Kantone, die keinen zentralen Identitätsdienst für den Bildungsbereich anbieten. In allen beschriebenen Fällen können auf der Ebene der Schulgemeinden und der einzelnen Schulen einzelne Identitätsdienste im Einsatz stehen.

2.3 Spezifische Situation in den Kantonen

Im Folgenden wird für jeden Kanton aufgelistet, welche der drei unter Kapitel 2.1 aufgeführten technischen Modelle auf ihn zutreffen. Es kann sein, dass pro Kanton und Schulstufe mehrere dieser Modelle gleichzeitig aufzufinden sind. Aufgrund der generischen Natur der Modelle müssen Abstriche bezüglich der exakten Zuteilung auf die effektive Situation im Kanton gemacht werden (vgl. Kapitel 2.2). Wenn in einem Kanton mehrere Modelle identifiziert wurden, bedeutet das, dass auf der angegebenen Schulstufe ein Identitätsmanagement in vergleichbarer Art und Weise existiert bzw. in einer Mischform vorkommt.

Kanton	Primarschule	Sek I	Sek II
ZH	in Abklärung	M1	
BE	M1, M3		M1, M2
LU	M2, M3		M1
UR	in Abklärung		
SZ	in Abklärung		
OW	in Abklärung		
NW	M2, M3	in Abklärung	M2, M3
GL	M3		M3
ZG	M2	in Abklärung	M1, M2
FR	M1		
SO	in Abklärung	in Abklärung	M2
BS	M1		
BL	M2		
SH	M1		
AR	M1		
AI	M1		
SG	M2, M3		M1, M2
GR	M3	in Abklärung	M3
AG	in Abklärung		
TG	M1, M2, M3		M2
TI	M1		
VD	M1, M3		
VS	M1		
NE	M1		M1
GE	M1		
JU	M1		in Abklärung

Der Anschluss an die Föderation ist nicht abhängig von der Art und der Ausprägung des Modells. Existiert ein Identitätsdienst im Bildungsraum des Kantons (wenn auch «nur» auf der Ebene der Gemeinden oder der Schulen), ist ein Anschluss des Identitätsdienstes an die Föderation möglich.

3 Anwendungsfälle und Ergebnisse aus den Pilotprojekten

3.1 Anwendungsfälle

Die Beispielschule «Fliedermatte» auf der Website fides.educa.ch macht den konkreten Nutzen einer Föderation im Schulalltag sichtbar. Handlungsort ist eine mittelgrosse Stadt im Schweizer Mittelland. Für jede Rolle von der Schülerin bis zum kantonalen Bildungsdirektor wurden Personas definiert. Die beschriebenen Anwendungsfälle basieren auf realen Situationen. Sie wurden gemeinsam mit Personen aus der Bildungspraxis erarbeitet und redigiert. Die Fotos aus dem Schulalltag stammen aus einer siebten Klasse. Auch das seit Dezember 2018 monatlich erscheinende Projektbulletin und Beiträge in Fachpublikationen dienten zur Vermittlung des konkreten Föderationsnutzens. Vier Anliegen bilden die Substanz der beschriebenen Anwendungsfälle:

3.1.1 Mobilität zwischen Stufen, Bildungsinstitutionen und Kantonen

Jede und jeder einzelne Lernenden durchläuft von der Grundstufe bis zum Abschluss der beruflichen Grundbildung oder einer Mittelschule zahlreiche Bildungsinstitutionen. Jeder Wechsel ist für die Verantwortlichen, aber auch für die Lernenden selber, mit administrativem Aufwand verbunden. Ein wesentlicher Aufwandtreiber ist die digitale Identität. Sie muss bei jedem Klassen- bzw. Schulwechsel übertragen und mit den relevanten Diensten verbunden werden. Dieser Aufwand variiert je nach Modell, das der einzelne Kanton auf den Stufen der Volksschule und der Sekundarstufe II (inkl. Berufsbildung) betreibt (vgl. Kapitel 2.1).

Unabhängig vom Modell eröffnet die Föderation Möglichkeiten, diesen repetitiven Aufwand für Schulleitungen, Lehrpersonen, Lernende und nicht zuletzt das Administrationspersonal bei den kommunalen und kantonalen Verzeichnisdiensten zu mindern. Daraus resultiert eine Vereinfachung der Mobilität. Die fällt primär innerhalb des Kantons ins Gewicht, ist aber gleichzeitig eine substanzielle Erleichterung beim Wechsel von Lernenden, Lehrpersonen und PH-Studierenden über Kantons- und Sprachgrenzen hinweg.

3.1.2 Durchlässigkeit mit SWITCH für Aus- und Weiterbildung von Lehrpersonen

Eine spezifische Form der Mobilität betrifft die Aus- und Weiterbildung von Lehrpersonen. Innerhalb der Föderation können PH-Studierende ihre von SWITCH ausgestellte digitale Identität auch im Rahmen der Praktika verwenden. Umgekehrt erhalten praktizierende Lehrpersonen mit der von ihrer Schule, Gemeinde oder dem Kanton ausgestellte digitale Identität im Rahmen von Weiterbildungen oder für die Mitarbeit in PH-Gremien Zugang zu PH-Ressourcen.

3.1.3 Single Sign-On (SSO) für Dienste mit gleichem Identitätsanbieter

Ein zentraler Nutzen für alle Beteiligten ist das vereinfachte Login-Verfahren zu Diensten, die über den gleichen Identitätsanbieter erschlossen sind. Konkret: Eine Schülerin oder eine Lehrperson hat mit ihrer föderierten Identität vereinfachten Zugriff auf alle Dienste, mit denen die Schule über eine gültige Nutzungsvereinbarung verfügt. Damit ermöglicht die Föderation den Dienstleistungs- und den Identitätsanbietern, für definierte Nutzungsszenarien SSO-Verfahren anzubieten.

3.1.4 Anonymisierung zur Datenminimierung

Im Markt der Lern- und Lehrmedien ist die digitale Transformation weit fortgeschritten. Neue Produktionen enthalten praktisch immer digitale Komponenten, die häufig den geschützten Zugriff mit einer qualifizierten Identität erfordern. Das stellt die Dienstanbieter vor ein Dilemma: Sie müssen Gewähr haben, dass nur tatsächlich berechtigte Personen auf die einzelnen Dienste zugreifen, wollen bzw. dürfen aber aufgrund der Datenschutzbestimmungen keine persönlichen Daten der mehrheitlich minderjährigen Nutzerinnen und Nutzer erhalten. Die anonymisierte Vermittlung von Identitäten und Attributen durch die Föderation löst dieses Dilemma. Die Dienstleistungsanbieter erhalten statt *Nutzer-* verlässliche *Nutzungsdaten*. Der Grundsatz der Datenminimierung ist damit erfüllt.

3.2 Technische Pilotprojekte

Mit einer Reihe von Kantonen und Dienstleistungsanbietern aus den Märkten der Lehrmittel und der Schulverwaltungssysteme wurden Pilotprojekte durchgeführt. Diese dienten den beteiligten Partnern und der Projektleitung dazu, in der institutionellen, organisatorischen und technologischen Vielfalt die gemeinsamen Nenner für eine gesamtschweizerische und zukunftsfähige Föderation zu erkennen. Die folgende Tabelle zeigt einen Überblick der Pilotprojekte, mit denen bereits detaillierte Anwendungsfälle für die spätere Integration von Identitäts- und Online-Diensten geprüft werden konnten.

Pilotpartner	Gegenstand der Tests	Ergebnis
Klett & Balmer AG Kanton Basel Stadt	Validierung der Grundprinzipien der Identifizierung, Authentifizierung und Autorisierung der Föderation	Der Lösungsansatz konnte positiv bestätigt werden.
PMI AG Kanton Appenzell Ausserrhoden	Vereinfachung der Integration von Identitätsbereitstellungssystemen, um die Benutzerverwaltung zu rationalisieren.	Die Kernelemente der Anwendungsfällen konnten identifiziert werden.
Microsoft Schweiz AG	Zugang zu Online-Diensten (z. B. O365) mit Unterstützung der Föderation über die bestehende Identitätsmanagement-Struktur im Bildungsbereich	Die konzeptionellen Grundlagen konnten festgelegt werden. Darauf basiert die weitere Integrationsplanung.
nanoo.tv Kanton Luzern	Untersuchung der Nutzungsmessung zur Schaffung von Kostentransparenz	Eine erste Bewertung des Konzepts und seiner Machbarkeit konnte erreicht werden.
Mindsteps (UZH/IBE) Kanton Basel-Landschaft	Validierung der Grundprinzipien der Identifizierung, Authentifizierung und Autorisierung der Föderation	Ein erster Workshop zur Identifizierung konkreter Anwendungsfälle ist geplant.
plandetudes.ch (CIIP)	Validierung der Grundprinzipien der Identifizierung, Authentifizierung und Autorisierung der Föderation im Falle mehrerer Kantone, die denselben Dienst verwenden.	Gemeinsames Verständnis zur Integration der Dienste, inkl. Schnittstelle zu SWITCH
Lehrmittelverlag Zürich	Technische Überprüfung Erarbeitung und Validierung zweier Use-Cases	Der Lösungsansatz ist in Abklärung Vertiefungsworkshops sind im Gange.
Schulverlag Plus	Validierung der Grundprinzipien der Identifizierung, Authentifizierung und Autorisierung der Föderation	Die Workshops werden nach Abschluss des Attribute-Datenmodells weitergeführt.

3.3 Usability Tests

Bei aller politischen, organisatorischen und technischen Sorgfalt muss sich die Föderation letztlich bei den Nutzerinnen und Nutzern bewähren. Je schlüssiger und flinker die Lösung auf Lernende und Lehrpersonen aller Stufen wirkt, desto eher wird sich die Föderation als selbstverständlicher Teil des Bildungssystems etablieren. Logik und Ergonomie der Nutzungsoberfläche wurden in Schulklassen aller Stufen in zwei Sprachregionen getestet.

Datum	Schule	Stufe
25.02.2019	Schule Untere Emme	Primar, Sek I
26.02.2019	Schule Aarwangen	Primar, Sek I
20.03.2019	Gymnasium Burgdorf	Sek II
27.03.2019	Techn. Berufsschule Bern	Sek II
01.04.2019	Schule Lutry	Primar

In einer eigens entwickelten Testumgebung mit zwei fiktiven Lehrmittelverlagen mussten die Schülerinnen und Schüler sich über die Föderation nacheinander bei verschiedenen Diensten einloggen.

Die Beobachtungen durch das Entwicklungsteam und die schriftlichen Rückmeldungen der Probanden ergaben zwei Schlüsselerkenntnisse. Sie dienen als Basis für die Umsetzung im Betrieb:

- Die geplante Benutzerführung durch die drei Phasen *Identifizierung, Authentifizierung* und *Autorisierung* wurde positiv bewertet.
- Auf den Login-Seiten der über die Föderation zugänglichen Online-Dienste, muss eine eindeutige, klar erkennbare *Schaltfläche* platziert werden.

4 KOSTEN FÜR DIE KANTONE

4.1 Kosten für den Betrieb der Föderation

Die unten aufgeführten Kosten decken den Grundbetrieb der Föderation ab. Sie wurden auf der Basis der Geschäftsarchitektur der Föderation – insbesondere der Prozesslandschaft – und des Organisationsmodells ermittelt (Prozesskostenrechnungsmodell). Die Hauptkostentreiber sind Investitionskosten (vor allem Software und andere immaterielle Vermögenswerte), Personalkosten (ca. 5 VZÄ) und Betriebsausgaben (wie beispielsweise die Nutzung der Infrastruktur).

Die Kosten für den technischen Betrieb der Föderation leiten sich von Erfahrungswerten aus vergleichbaren Identitätsmanagementlösungen in der Schweiz ab.

Es bestehen Restunsicherheiten bezüglich der Verhandlungen der Betriebskosten des technischen Betriebs. Zudem können in Zukunft entstehende Anforderungen an die Föderation zusätzliche Kosten verursachen.

Bezeichnung	**Kosten pro Jahr** (CHF, ohne MWST)
Governance & Steuerung	115'000
Ausrichtung, Planung & Organisation	293'000
Akquisition & Weiterentwicklung	780'000
Service Delivery & Support	652'000
Gesamtkosten	**1'840'000**

Die Finanzierung dieser Kosten unterliegt einem bildungspolitischen Entscheid. Die Konditionen und der Anteil der Beiträge der Dienstleistungsanbieter werden in diesem Rahmen besprochen.

4.2 Kosten für den Beitritt zur Föderation

Neben den oben erwähnten Kosten für den Aufbau und den Betrieb der Föderation von Identitätsdiensten, die von allen Kantonen gemeinsam getragen werden, entstehen für jeden Kanton individuelle Beitrittskosten. Diese sind von den organisatorischen und technischen Rahmenbindungen innerhalb des Kantons abhängig und müssen individuell evaluiert werden (vgl. educa.ch 2019a).

Aus Sicht der Föderation verringern sich die organisatorischen Aufwände, wenn weniger Identitätsdienste pro Kanton anzubinden sind.

5 Beitrittsverfahren der Kantone und Bereitschaft der Dienstleistungsanbieter

5.1 Beitritt von Identitätsanbietern (Kantone, Gemeinden, Schulen)

Beim Beitritt zur Föderation sind auf der Prozessebene die Absichtserklärung des Kantons zur Teilnahme und die technische Integration eines bzw. mehrerer Identitätsdienste zu unterscheiden (vgl. educa.ch 2019a).

Die Föderation ist in der Lage, alle bestehenden Modelle von Identitätsdiensten aufzunehmen.

Dabei spielt es für die Föderation auf der technischen Ebene keine Rolle, ob der Identitätsdienst von einem Kanton, einer Gemeinde oder einer einzelnen Schule verwaltet wird und ob die Identitäten zentral oder dezentral verwaltet werden. Ein zentral auf Kantonsebene verwalteter Identitätsdienst ist keine Grundvoraussetzung für den Beitritt zur Föderation.

Es ist ein bildungspolitischer Entscheid jedes einzelnen Kantons, ob er nur kantonal verwaltete Identitätsdienste der Föderation beitreten lassen will, oder ob er es den Gemeinden und einzelnen Schulen (inkl. Privatschulen) frei überlässt, ihre Identitätsdienste eigenständig anzubinden. Ebenso liegt es in der Entscheidung des Kantons, ob er die bestehenden Identitätsdienste in seinem Bildungsbereich (sowohl diejenigen der Gemeinden als auch der Schulen) in Vorbereitung auf den Beitritt zur Föderation zentral organisieren will oder nicht. Der Beitritt mehrerer Identitätsdienste (bspw. unterschiedlicher Schulstufen) innerhalb eines Kantons kann auch gestaffelt erfolgen.

5.1.1 Prozesse

Zwei detaillierte Prozesse beschreiben den Ablauf des Beitritts und regeln die Integration eines Identitätsdiensts (vgl. Prozesslandschaft). Der Beitrittsprozess schliesst mit der bildungspolitischen Verbindlichkeit des Beitritts ab. Der Integrationsprozess beschreibt die technische und organisatorische Integration eines Identitätsdienstes in die Föderation (vgl. educa.ch 2019a).

5.1.2 Organisatorische Anforderungen

- Die Verantwortlichkeiten bezüglich der Identitätsdienste im Bildungsbereich des Kantons sind geklärt.
- Eine rechtliche Grundlage in Bezug auf die Weitergabe von Attributen an die Föderation liegt vor.
- Ein System zum Erstellen und Verwalten digitaler Identitäten im Bildungsraum ist vorhanden (vgl. educa.ch 2019a).

5.1.3 Technische Anforderungen

- Die technische Architektur der Schnittstelle der Föderation baut auf dem offenen Protokoll SAML 2.0 auf. Um einen Identitätsdienst an die Föderation anschliessen zu können, müssen dem Protokoll entsprechende Schnittstellen und Funktionen bereitgestellt werden (vgl. Föderationsarchitektur; educa.ch 2019a).
- Die für Personendaten zuständigen Stellen gewährleisten die Data Governance (d. h. Datenqualität und Integrität) der Attribute der digitalen Identitäten.
- Jeder Identitätsanbieter muss alle technischen und organisatorischen Massnahmen die zur Sicherheit der Daten beitragen, gewährleisten können.

5.2 Bereitschaft der Dienstleistungsanbieter

Das Interesse der Dienstleistungsanbieter an einer Föderation im Bildungsraum Schweiz ist sehr gross. Das gilt nicht nur für Grossplattformen wie beispielsweise Microsoft, Lehrmittelverlage oder Anbieter von Schulverwaltungslösungen, sondern auch für kleinere Firmen.

Das Projektteam stand während der Aufbauphase mit vielen Dienstleistungsanbietern in regelmässigem Kontakt. Daraus sind gemeinsame Pilotprojekte mit Identitätsanbietern entstanden. Diese hatten zum Ziel, konkrete Anwendungsfälle zu identifizieren und zu testen (vgl. Kapitel 3.2).

Die Bemühungen des Projektteams um die Dienstleistungsanbieter haben zu folgenden Ergebnissen geführt:

- Die Föderation wird als ein essentieller Grundstein für die Digitalisierung der eigenen Geschäftsprozesse gesehen.
- Die Unternehmen ergreifen in der Erwartung der Inbetriebnahme der Föderation bereits technische Massnahmen, um ihre Dienste anzupassen.
- Dienstleistungsanbieter haben bereits begonnen, ihre Geschäftsprozesse im Hinblick auf das zukünftige Potenzial der Föderation (vgl. Kapitel 1.3) zu überprüfen und/oder neu zu konzipieren.
- Erkannte Probleme in Bezug auf Vertrauen und Transparenz, Effektivität, Kosteneffizienz oder Verbesserungen bei der Integration von Dienstleistungsanbietern und Kantonen in die vorgeschlagene Architektur der Föderation werden bereits als gelöst wahrgenommen.

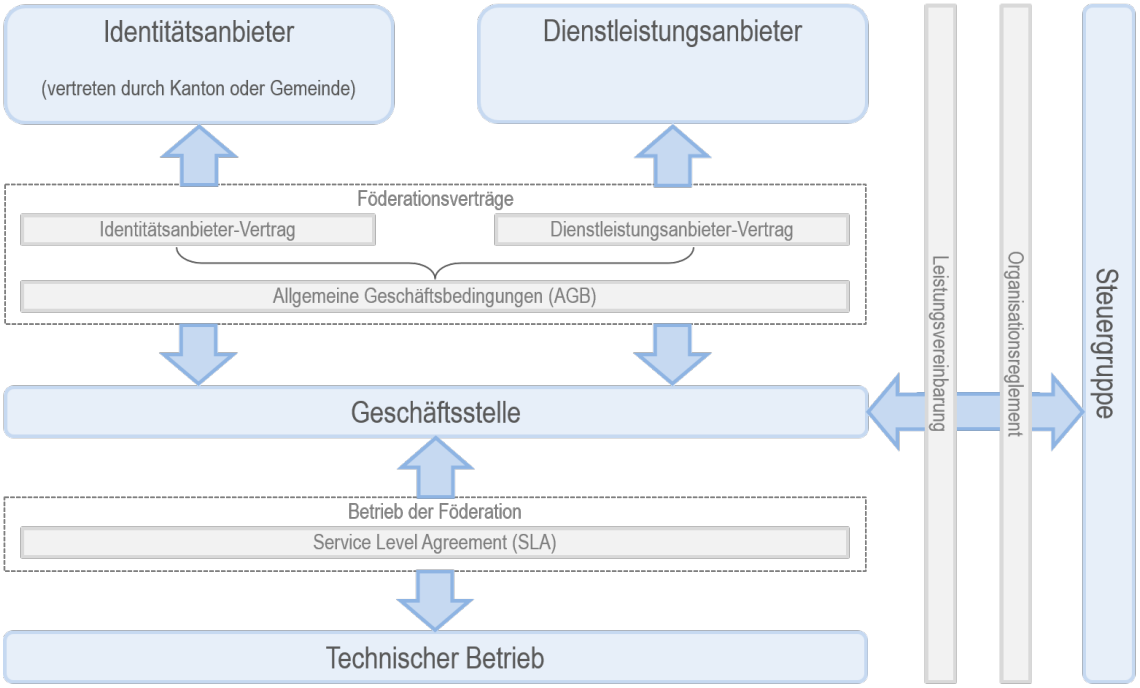
Für den Beitritt und die Integration der Dienstleistungsanbieter sind analog zu den Identitätsanbietern zwei Prozesse definiert (vgl. Prozesslandschaft).

6 Organisation der Föderation

Die Organisation der Föderation ermöglicht eine zeitnahe Entscheidungsfindung auf allen relevanten Ebenen, stellt den Betrieb für alle Teilnehmenden sicher und gestattet ihnen, an der Entwicklung der Föderation teilzunehmen.

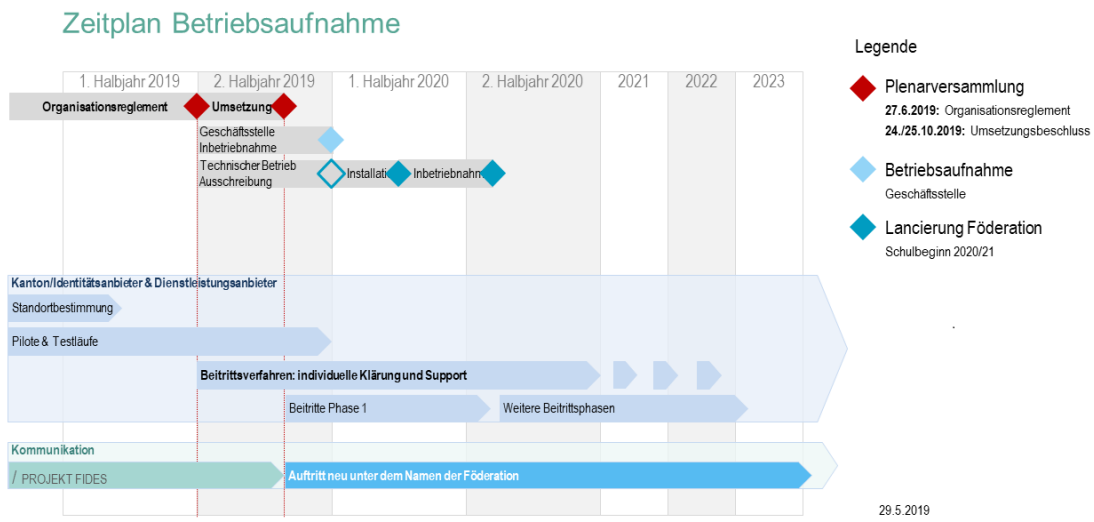
Die Organisation der Föderation berücksichtigt die bestehenden Steuerungsstrukturen des schweizerischen Bildungssystems.

Sie wird auf der Ebene der EDK über ein Organisationsreglement festgelegt und gemäss folgender Struktur abgebildet:



7 Zeitplan der Betriebsaufnahme

Mit dem Organisationsreglement, der Klärung der technischen Rahmenbedingungen und dem Namen der Föderation sind die Grundlagen für den operativen Start der Föderation ab 1.11.2019 gelegt. Die Unterlagen für die Ausschreibung des technischen Betriebs sind ab Juni 2019 zur Publikation bereit (vgl. Ausschreibungsunterlagen). Das erste Halbjahr dient der technischen Inbetriebnahme mit den ersten beitretenden Identitäts- und Dienstleistungsanbietern. Ab Schulbeginn 2020 ist die Föderation für den flächendeckenden Ausbau in allen Landesteilen aufgestellt.



8 Erarbeitete Lieferobjekte

Im Rahmen des Projekts «Aufbau der Föderation von Identitätsdiensten für den Bildungsraum Schweiz» wurden folgende Lieferobjekte bereits fertiggestellt bzw. sind noch in Erarbeitung. Dokumente mit sicherheitsrelevanten Informationen sind auf Anfrage verfügbar:

Lieferobjekt	Beschreibung	Status
educa.ch (2019a): *Föderation der Identitätsdienste im Bildungsraum Schweiz. Beitritt der Identitätsanbieter, 29.05.2019*	Beschreibung des Beitritts der Identitäts- und Dienstleistungsanbieter	Im Anhang
educa.ch (2019b): *Landschaft der digitalen Identitäten im Bildungsraum Schweiz. Grundlageninformationen aus der Standortbestimmung (Due Dilligence), 15. März 2019*	Bericht zur Standortbestimmung der Identitätsdienste in den Kantonen.	Im Anhang
educa.ch (2019c): *Projekt FIDES: Datenschutz-Folgenabschätzung, 05.04.2019*	Analyse der datenschutzrelevanten Risiken und der im Projekt zu treffenden Massnahmen	Im Anhang
Bericht aus den Pilotprojekten	Beschreibung der Ergebnisse der durchgeführten Pilotprojekte	Verfügbar auf Anfrage
Risikomanagementpolitik (inkl. Risikoprofil)	Beschreibung des Umgangs mit Unsicherheiten und Risiken im Betrieb	Verfügbar auf Anfrage
ISMS-Grundlagen	Beschreibung der Sicherheitsmassnahmen im Betrieb die im Rahmen von ISO/IEC 27001 erforderlich sind.	Verfügbar auf Anfrage
Prozesslandschaft	Überblick zu den definierten Prozessen der Föderation	Verfügbar auf Anfrage
Föderationsarchitektur	Detailbeschreibung der technischen Infrastruktur, der Applikationen und Datenbanken der Föderation	Verfügbar auf Anfrage
Ausschreibungsunterlagen	Unterlagen zur Ausschreibung des technischen Betriebs der Föderation	Im Juni 2019 vorliegend