



## Ausbau und Organisation einer Föderation bestehender und neuer Identity- und Access-Management-Systeme; Rahmenkonzept FIDES: Beschlussfassung

### Das Generalsekretariat berichtet:

- 1 Die EDK hat im Juni 2015 die Fachagentur educa.ch damit beauftragt, ein Konzept für eine Föderation von Identitätsdiensten im Bildungsraum Schweiz zu entwickeln. Der Auftrag stützt sich auf den Punkt 1.6. im Tätigkeitsprogramm 2015–2019 der EDK (Abschnitt «Bildung und ICT»): «Unter Berücksichtigung der Bedürfnisse der Sprachregionen und unter Einbezug der Lehrmittelverlage den Zugang zu Lehrmitteln im Internet ermöglichen, insbesondere durch Ausbau und Organisation einer Föderierung bestehender und neuer Identity- und Access-Management-Systeme».
- 2 Die Fachagentur educa.ch hat das Rahmenkonzept *FIDES. Die Föderation von Identitätsdiensten für den Bildungsraum Schweiz* ausgearbeitet. FIDES soll als Föderation von Identitätsdiensten im Auftrag der Kantone für die Akteure der Primar-, Sek I- und Sek II-Stufen betrieben werden. Ziel ist es, diesen Personen eine einzige digitale Identität für den Zugang zu den von ihnen benötigten Online-Diensten zur Verfügung zu stellen. Die Kantone behalten dabei die Hoheit über die digitalen Identitäten. Das Rahmenkonzept beschreibt die Funktionsweise im Hinblick auf die Steuerungsmöglichkeiten der Kantone und des Bundes, die Dienstleistungen der Föderation und deren Teilnehmenden sowie Szenarien zum Aufbau der Föderation. Das Rahmenkonzept berücksichtigt die unterschiedlichen Konzepte der Kantone in Bezug auf Identity- und Access-Management-Systeme und ermöglicht eine gestaffelte Teilnahme der Kantone an der Föderation.
- 3 Das Rahmenkonzept enthält eine Übersicht zu den Kosten der Föderation, aufgeteilt in Aufbau- und Betrieb. Die Aufwände der Kantone zur Realisierung ihrer Anschlussfähigkeit an die Föderation sind in dieser Aufstellung nicht berücksichtigt. Danach ist vorgesehen, dass sich die Kantone mit Gründung der Föderation an der Finanzierung beteiligen.
- 4 Der Bundesrat hat in seinem Bericht «Herausforderungen der Digitalisierung für Bildung und Forschung in der Schweiz» von Juli 2017 FIDES explizit als Massnahme genannt: „Der Bund unterstützt ein gesamtsystemisch relevantes Projekt der Schaffung einer Föderation von Identitätsdiensten (FIDES), damit die Institutionen der Bildungsstufen (Kindergarten bis Sekundarstufe II) überregional und interinstitutionell auf digitalisierte Medien und Dienste regelkonform zugreifen können («Vertrauensraum»)“. Über den Umfang der Beteiligung des Bundes sind mit dem SBFI Gespräche im Gange.
- 5 Die Erarbeitung des Rahmenkonzepts wurde vom beratenden Ausschuss von Departementssekretären begleitet und in der Folge mehrfach von der Konferenz der Departementssekretäre (KDS) diskutiert. Auch die kantonalen Referenzpersonen wurden zur Stellungnahme eingeladen und in die Überarbeitung einbezogen. Diese Form der Zusammenarbeit mit den Kantonen wird bei den nächsten Schritten fortgesetzt.
- 6 Der Vorstand hat an seiner Sitzung vom 7. September 2017 das Geschäft beraten und den Beschlussentwurf ohne Änderungen zu Händen der Plenarversammlung gutgeheissen. Eine allfällige Beteiligung von Switch soll weiter vertieft werden.

- 7 Die Fachagentur educa.ch soll nun auf der Grundlage des vorliegenden Rahmenkonzepts ein Detailkonzept für den Aufbau der Strukturen einer Föderation FIDES erarbeiten. Das Detailkonzept soll insbesondere folgende Aspekte konkretisieren:
  - Projektorganisation für den Aufbau der Föderation
  - Sicherstellung der ausreichenden Mitwirkung der Dienstleistungsanbieter
  - Rahmenbedingungen, welche die Kantone sicherstellen müssen (z. B. Datenschutz)
  - Beitrittsmodalitäten für Kantone und Dienstleistungsanbieter
  - Die Finanzierung des Aufbaus der Föderation
  - Die Finanzierungsmodalitäten des Betriebs der Föderation
- 8 Das Detailkonzept für den Aufbau sowie die Anträge zur Finanzierung (Budget 2019) soll dem EDK-Vorstand am 25. Januar 2018 vorgelegt werden.
- 9 Der Beschluss über den Aufbau und die Finanzierung obliegt der Plenarversammlung.
- 10 Die Kantone werden eingeladen, parallel zur Erarbeitung des Detailkonzepts, die Meinungsbildung im Hinblick auf einen Beitritt zu FIDES einzuleiten.

**Die Plenarversammlung beschliesst:**

- 1 Das Rahmenkonzept *FIDES. Die Föderation von Identitätsdiensten für den Bildungsraum Schweiz* vom 18. August 2017 wird verabschiedet.
- 2 Die Fachagentur educa.ch wird beauftragt, unter Einbezug des KDS-Ausschusses FIDES und dem Netzwerk der kantonalen Referenzpersonen zu Händen des EDK-Vorstandes vom 25. Januar 2018 ein Detailkonzept gemäss Ziffer 7 der Erwägungen zu erarbeiten.

Zürich, 26. Oktober 2017

**Schweizerische Konferenz der kantonalen Erziehungsdirektoren**

Im Namen der Plenarversammlung:

sig.

Susanne Hardmeier  
Generalsekretärin

Anhang:

- *FIDES. Die Föderation von Identitätsdiensten für den Bildungsraum Schweiz.*  
Rahmenkonzept vom 18. August 2017

Zustellung an:

- Konferenzmitglieder

Publikation auf der Website EDK

232.3-1.8 /ako

# FIDES. Die Föderation von Identitätsdiensten für den Bildungsraum Schweiz

**Rahmenkonzept**  
Version 18.08.2017



## INHALTSVERZEICHNIS

1	Eine Föderation von Identitätsdiensten für den Bildungsraum Schweiz .....	3
1.1	Herausforderungen des digitalen Bildungsraums .....	3
1.2	Die Föderation FIDES als Beitrag zur digitalen Transformation .....	4
1.3	Mögliche Risiken im Zusammenhang mit der Föderation FIDES .....	6
2	Funktionsweise der Föderation FIDES .....	7
2.1	Die Föderation FIDES bildet einen Vertrauensraum .....	7
2.2	Die Föderation FIDES respektiert die Steuerungskompetenz der Kantone.....	7
2.3	Kantone und SP sind Teilnehmende an der Föderation FIDES .....	9
2.4	Dienstleistungen der Föderation FIDES .....	9
2.5	Technische Konzeption der Föderation FIDES .....	10
3	Aufbau der Föderation FIDES .....	11
3.1	Aufbau der Föderation FIDES .....	11
3.2	Verantwortlichkeiten .....	11
3.3	Beitritt und Teilnahme eines Kantons an der Föderation FIDES .....	12
3.4	Kosten der Föderation FIDES .....	15
4	Glossar .....	17
	Anhang I: Zentrale Aspekte der Föderation FIDES .....	18
	Anhang II: Kontext der Föderation FIDES .....	25

# 1 EINE FÖDERATION VON IDENTITÄTSDIENSTEN FÜR DEN BILDUNGSRAUM SCHWEIZ

Eine Föderation von Identitätsdiensten bietet eine Möglichkeit, die wachsenden Herausforderungen, mit denen sich die Kantone durch die Digitalisierung des Bildungsraums konfrontiert sehen, anzugehen und zu lösen. Die Föderation FIDES ermöglicht es, neue und bestehende Identitätsdienste des Bildungsbereichs miteinander zu verbinden. Identitätsdienste ermöglichen es den Endbenutzenden (Lernende, Lehrpersonen und Verwaltungspersonal) sich bei den von ihnen benötigten Online-Diensten zu authentifizieren und darauf zuzugreifen. Insbesondere bietet sie den Bildungsverantwortlichen eine Chance, den digitalen Bildungsraum zu beeinflussen, zu kontrollieren, zu steuern und einen einfachen, gesicherten und steuerbaren Zugang zu Online-Diensten bereitzustellen. Im Folgenden werden allgemeine Herausforderungen des digitalen Bildungsraums beschrieben und Möglichkeiten skizziert, wie die Föderation zur Lösung dieser Herausforderungen beitragen kann.

## 1.1 Herausforderungen des digitalen Bildungsraums

In den letzten Jahren wurden immer mehr Lebensbereiche von den Möglichkeiten der Digitalisierung grundlegend transformiert. Dies gilt auch für den Bildungsraum Schweiz. Nicht nur die Steuerungsmöglichkeiten haben sich im Zuge dieser Entwicklung verändert, die Bildungsverantwortlichen auf kantonaler und Bundesebene sind auch zunehmend gefordert, geeignete Lösungen für verschiedene Herausforderungen anzubieten. Zu diesen Herausforderungen gehören:

- die Kontrolle über die Daten des digitalen Bildungsraums Schweiz
- die Steuerung des digitalen Bildungsraums Schweiz auf kantonaler und nationaler Ebene
- das Schaffen von Vertrauen im digitalen Bildungsraum Schweiz
- die Gewährleistung eines sicheren Zugangs zu Online-Diensten auf allen Ebenen des Bildungssystems
- die Einhaltung der Rechtssicherheit für den digitalen Bildungsraum Schweiz

### 1.1.1 Der digitale Bildungsraum als Datenraum

Der digitale Bildungsraum Schweiz ist ein Datenraum, in dem Personendaten generiert und für den Zugang zu Online-Diensten verwendet werden. In einigen Kantonen bestehen bereits zentrale bzw. zentral koordinierte Lösungen, um die Kontrolle über die Herkunft dieser Daten zu gewährleisten (vgl. Anhang II, *Good Practice zu kantonalen BildungsID-Lösungen*). Die Art und Weise wie Personendaten gestaltet sind und woher sie kommen ist aktuell sehr heterogen. Vielerorts werden sie generiert, ohne dass dabei gemeinsame Standards beachtet werden. Klare Regelungen zum Umgang mit diesen sensiblen Daten fehlen.

Private Unternehmen profitieren heutzutage von der Verarbeitung und Sammlung von Personendaten. Online-Dienste werden zunehmend von privaten Anbietern für den Bildungsbereich lizenzkostenfrei zur Verfügung gestellt (z. B. Google Classroom, Microsoft Classroom etc.). Die Verwendung der bei der Nutzung solcher Produkte generierten Daten und auch deren Speicherort bleiben dabei meist intransparent. Auch verlangen solche Dienste Personendaten zur Identifikation der Endbenutzenden. Das stellt die Schulen vor datenschutzrechtliche Probleme.

### 1.1.2 Ein sicherer Zugang zu Online-Diensten

Neben der Beseitigung datenschutzrechtlicher Probleme gilt es, einen sicheren Zugang zu Online-Diensten für alle Ebenen des Bildungssystems zu schaffen und auf nationaler Ebene einzurichten. Die Sicherheit basiert dabei insbesondere auf der Vertrauensbeziehung zwischen denen, die einen Dienst anbieten, und denen, die einen Dienst nutzen. Eine besondere Herausforderung stellt dabei die Personalisierung der Nutzungsdaten dar. In der Regel gehört es zum Geschäftsmodell von Dienstleistungsanbietern (SP), die Personendaten der Endbenutzenden für eigene Zwecke zu verwenden. Problematisch wird dies, sobald die personalisierten Nutzungsdaten an Dritte weiterverkauft bzw. von Dritten weiterverarbeitet werden, ohne dass die Endbenutzenden davon Kenntnis haben. Endbenutzende müssen überdies eine Vielzahl von Benutzerkonten bzw. Logins verwalten, meist eines

pro genutzten Dienst. Personendaten werden durch die verschiedenen SP jeweils unterschiedlich behandelt, so dass die Endbenutzenden sich mit vielerlei unterschiedlichen Bedingungen konfrontiert sehen. Die Vertrauensbasis zu den einzelnen SP muss jeweils individuell verhandelt werden. Ein sicherer Zugang zu Online-Diensten ist also erst dann möglich, wenn über die Nutzung von Personendaten entschieden werden kann und diese Entscheidung vertraglich festgehalten und durchgesetzt wird.

### 1.1.3 Schaffen von Rechtssicherheit

Da die Vertragsbedingungen grosser internationaler SP häufig einseitig ausgestaltet sind, wird insbesondere für Schulen und auch einzelne Kantone das Einfordern und Durchsetzen elementarer Rechte stark erschwert oder gar verunmöglicht. Um die Rechtssicherheit im digitalen Bildungsraum Schweiz zu gewährleisten und vertragliche Ungleichgewichte zu korrigieren müssen Bedingungen ausgehandelt werden, die mit der Schweizer Rechtspraxis kompatibel sind (z. B. Anwendung von Schweizer Recht, Gerichtsstand in der Schweiz, Einhaltung datenschutzrechtlicher Bestimmungen etc.).

## 1.2 Die Föderation FIDES als Beitrag zur digitalen Transformation

Mit der Föderation FIDES werden die erwähnten Herausforderungen des digitalen Bildungsraums Schweiz auf nationaler Ebene angegangen. Die Föderation gibt den kantonalen Bildungsverantwortlichen Instrumente in die Hand, um die notwendigen Massnahmen umzusetzen und die Zusammenarbeit der Kantone zur strategischen Entwicklung des digitalen Bildungsraums voranzutreiben. Die Föderation trägt daher substantziell zur Konstitution des digitalen Bildungsraums Schweiz bei.

### 1.2.1 Kontrolle über die Personendaten

Im Hinblick auf die Kontrolle des digitalen Bildungsraums Schweiz als Datenraum bietet die Föderation FIDES zwei Vorteile: Erstens werden standardisierte Attribute einer nationalen BildungsID festgelegt (vgl. Anhang I, *Modell nationale BildungsID*). Diese Liste von Attributen soll die Kantone nicht in der Gestaltung ihrer eigenen BildungsID einschränken, sondern ihnen aufzeigen, welche Attribute aus dem Bildungskontext die SP bei einer Anmeldung auf ihre Online-Dienste benötigen. Sind diese standardisierten Attribute Teil jeder kantonalen BildungsID, erleichtert dies sowohl den SP als auch den Kantonen die Anbindung von Diensten an die Föderation. Zweitens wird mit der Verwendung standardisierter Attribute eine kantonale und nationale Vereinheitlichung der BildungsID ermöglicht, womit sich die Kontrolle und der Schutz von Personendaten optimieren lassen. Die Weitergabe von Personendaten wird über die Teilnehmerverträge der Föderation für alle Teilnehmenden geregelt (vgl. Anhang I, *Reglemente und Verträge*). Mittels Teilnehmervertrag kann zudem ein Opt-In-Prinzip bezüglich der Nutzungsdaten verankert werden (vgl. Anhang I, *Grundsätze, Verfahren und Standards der Föderation*). Wie die Verwendung der Nutzungsdaten genau zu regeln ist, steht noch zur Diskussion.

### 1.2.2 Steuerungsmöglichkeiten für die Kantone

Die Geschäftsstelle der Föderation FIDES entscheidet anhand einer Liste von Kriterien (vgl. Anhang I, *Reglemente und Verträge*), die gemeinsam mit den teilnehmenden Kantonen erarbeitet wird, welche SP in die Föderation aufgenommen werden. Die Diskussion über diese Kriterien wird zwischen der Geschäftsstelle der Föderation und den kantonalen Vertretern zunächst in der Aufbau- und später in der Betriebsphase der Föderation geführt. Die Kantone können also sowohl in der Aufbau- als auch in der Betriebsphase über die bestehenden Strukturen auf die Föderation Einfluss nehmen (vgl. [Kapitel 2](#)). Die Föderation soll eine zentrale innerkantonale Koordination des Identitätsmanagements (IdM) fördern (vgl. [Kapitel 3.2](#)), um Qualität und Herkunft der Identitätsdaten sicherzustellen. **Vertrauen und Sicherheit**

Vertrauen innerhalb der Föderation FIDES entsteht mittels gemeinsam vereinbarter Regeln und Prozesse. Darüber hinaus ergibt sich Sicherheit (im Sinne von *safety*) aus der Verwendung gemeinsam festgelegter Technologien (vgl. Anhang I, *Grundsätze, Verfahren und Standards der Föderation*).

Die Föderation implementiert auf nationaler Ebene gemeinsame Kriterien, Standards und Regeln bezüglich des Anmeldeprozesses bei Online-Diensten (vgl. Anhang I, *Grundsätze, Verfahren und Standards der Föderation*). An diese müssen sich sowohl die SP als auch die Identitätsdiensteanbieter (IdP) halten. Damit werden im Rahmen der

Föderation gleiche Voraussetzungen für alle Teilnehmenden geschaffen, was das Vertrauen in den Zugang zu den Diensten der SP stärkt. Jeder SP der zur Teilnahme an der Föderation zugelassen wird, schliesst Verträge mit der Föderation ab und verpflichtet sich so zur Verwendung derselben Technologien und Prozesse, womit ein sicherer Zugang zu Online-Diensten gewährleistet werden kann (vgl. [Kapitel 2.1](#)).

Dank der Verträge zwischen der Föderation FIDES, den SP und den Kantonen gewinnen die Teilnehmenden an Rechtssicherheit. Der Vorteil dabei ist, wie bereits erwähnt, dass die Rahmenbedingungen für alle Teilnehmenden gleichermassen gelten und nicht mehr einzeln zwischen Kantonen/Gemeinden/Schulen und SP ausgehandelt werden müssen. Die vertraglichen Beziehungen zwischen Schulen/Gemeinden/Kantonen und SP zur Nutzung von Online-Diensten werden dadurch aber nicht ersetzt.

#### 1.2.4 Zusammenarbeit

Der gemeinsame Auftritt der Instanzen des Bildungssystems im Rahmen der Föderation FIDES stärkt deren Verhandlungsposition gegenüber den SP. Die gemeinsamen Standards und der Erfahrungsaustausch innerhalb der Föderation unterstützen die Kantone bei der Identitätsverwaltung und der Bereitstellung einer kantonalen Bildung-ID folgendermassen:

- Bereitstellung eines personalisierten, sicheren und kontrollierbaren Zugangs zu Daten und Diensten
- Optimierung des Monitorings dank verbesserter Qualität und Integrität der digitalen Daten
- Qualitätssteigerung der Identitätsdaten durch standardisierte Attribute der Bildung-ID

Die Dienstleistungen der Föderation FIDES schaffen zugleich einen Nutzen für das schweizerische Bildungssystem und den Bildungsraum Schweiz, und zwar:

- Einheitliche Anforderungen an die SP bezüglich Sicherheit und Datenschutz
- Starke Verhandlungsposition gegenüber den SP für vorteilhafte Geschäftsmodelle und Preise
- Unterstützung in strategischen Bereichen, z. B. Erschliessung neuer Leistungen, Beziehungen zwischen Föderationen, technische Weiterentwicklung, Optimierung administrativer und technischer Verfahren, Risikomanagement

Eine Teilnahme an der Föderation FIDES ist auch für die SP vorteilhaft. Die gemeinsamen Standards und der Erfahrungsaustausch werden auch auf ihre Bedürfnisse abgestimmt, und die Reglemente und Verträge der Föderation verleihen auch ihnen Sicherheit und Vertrauen. Für die SP ergibt sich aus den Dienstleistungen der Föderation folgender Nutzen:

- Einfache und effiziente Zugangskontrolle zu ihren Angeboten dank zentraler Infrastruktur, Organisation, Technik und Standards
- Qualität, Sicherheit und Vertrauen dank offiziell geprüften digitalen Identitäten

### 1.3 Mögliche Risiken im Zusammenhang mit der Föderation FIDES

Mit der Föderation FIDES entstehen sowohl direkte, auf die Föderation wirkende, als auch indirekte, mit der Föderation in Zusammenhang stehende Risiken, die von allen Teilnehmenden getragen werden müssen:

- Die von der Föderation geforderte Koordination in Bezug auf kantonale und kommunale IdM kann für einige Kantone mit mehr Aufwand verbunden sein als für andere (vgl. [Kapitel 3.3](#))
- Die Teilnahme der SP setzt deren Bereitschaft voraus, die Rahmenbedingungen der Föderation zu akzeptieren. Einige Bedingungen (Standardisierung, pseudonymisierte Attribute, Weiterverarbeitung der Nutzungsdaten) könnten einen Einfluss auf die Geschäftsmodelle der SP haben, was sie von einer Teilnahme abhalten könnte
- Es müssen ausreichend Kantone an der Föderation teilnehmen, damit diese aufgebaut und nachhaltig betrieben werden kann
- Die Kumulation von Personendaten birgt generell ein gewisses Sicherheitsrisiko, dem angemessen Rechnung getragen werden muss (vgl. Anhang I, *Grundsätze, Verfahren und Standards der Föderation FIDES*)
- Die Betreiber der IdM-Lösungen haften für Integrität, Verfügbarkeit und Gültigkeit der BildungsID. Sie müssen sicherstellen können, dass die BildungsID nicht von Unberechtigten missbraucht werden kann.

## 2 FUNKTIONSWEISE DER FÖDERATION FIDES

Die Föderation FIDES berücksichtigt die Verantwortlichkeiten von Bund und Kantonen und trägt zu einer allseitigen Kooperation im Bildungsraum Schweiz bei. Sie bietet den Mitgliedern des Bildungssystems einen vereinfachten, nutzerfreundlichen und sicheren Zugang zu Online-Diensten.

### 2.1 Die Föderation FIDES bildet einen Vertrauensraum

Wie bereits eingangs erwähnt, bietet die Föderation FIDES ein Rahmenwerk für die Zusammenarbeit zwischen Kantonen und SP. Innerhalb dieses reglementierten Rahmens erhalten die Mitglieder des Bildungssystems Zugang zu Online-Diensten und verpflichten sich zur Einhaltung gleichbleibender Standards hinsichtlich der Verwaltung und Verwendung digitaler Identitäten sowie der Nutzung von Personendaten. So lässt sich der Anspruch nach einer staatlichen Steuerung des digitalen Bildungsraumes, nach einer Einhaltung des Personendatenschutzes sowie nach einer vertragskonformen Nutzung von Online-Diensten umsetzen.

Dabei regelt die Föderation nicht etwa die Verantwortlichkeiten zwischen den Teilnehmenden an der Föderation neu. Vielmehr schafft die Föderation einen Vertrauensraum zwischen den IdP der teilnehmenden Kantone und den an die Föderation angeschlossenen SP. Der Vertrauensraum definiert sich einerseits über die Verbindung der Sicherheitsdomänen aller IdP und SP die an die Föderation angeschlossen sind, in welchen die Verwaltung von Identitäts- und Nutzungsdaten geregelt wird. Andererseits werden mit der Föderation verbindliche und einheitliche Standards und Regeln für den Anmeldeprozess eingeführt.

Im Einzelnen ergeben sich daraus für die verschiedenen Akteure folgende Vorteile:

- Die Kantone definieren, welche Identitätsdaten an den SP übermittelt werden. Darüber hinaus können sie mitbestimmen, wie die Identitäts- und Nutzungsdaten ihrer Endbenutzenden durch die SP bearbeitet werden dürfen
- Endbenutzende können darauf vertrauen, dass ihre Anmeldung bei einem Online-Dienst nach den in der Föderation definierten und akzeptierten Standards und Regeln erfolgt
- Die SP wissen, dass die Endbenutzenden, die sich bei ihrem Online-Dienst anmelden, auch dazu berechtigt sind

### 2.2 Die Föderation FIDES respektiert die Steuerungskompetenz der Kantone

Auftraggeber für die Föderation FIDES sind die Kantone. Sie steuern die Föderation mittels einer Leistungsvereinbarung, in der die Ziele, Leistungen und verfügbaren finanziellen Mittel festgelegt werden (vgl. Anhang I, *Reglemente und Verträge*).

Die Kantone werden vertreten durch das Generalsekretariat der EDK (GS EDK). Wie die Beziehung zwischen Bund und Kantonen im Rahmen der Föderation konkret ausgestaltet und in die Leistungsvereinbarung aufgenommen wird, ist Gegenstand weiterer Abklärungen. Die zweite Vertragspartei ist die Fachagentur educa.ch, die als Auftragnehmerin für den Aufbau und den Betrieb der Geschäftsstelle der Föderation vorgeschlagen wird.

Nachfolgend werden die für die Steuerung der Föderation relevanten Gremien und Strukturen vorgestellt:

#### 2.2.1 Teilnehmerversammlung

Die Organisationsstruktur der Föderation FIDES sieht Mitsprachemöglichkeiten für die Teilnehmenden vor. Dabei wird klar unterschieden zwischen den Instanzen des Bildungssystems, die in den Steuerungsprozess der Föderation sowie in die betrieblichen Prozesse zur Entwicklung und Implementierung organisatorischer und technischer Lösungen einbezogen sind, und den SP, deren Einflussnahme auf den technischen Bereich beschränkt bleibt.

Zu den an der Föderation beteiligten Instanzen des Bildungssystems gehören auf der lokalen Ebene die Schulen mit ihren Lehrpersonen, dem Verwaltungspersonal, den Schülerinnen und Schülern sowie deren gesetzlichen Vertretenden, für die der Zugriff auf Online-Dienste vorgesehen ist. Vertreten werden sie in der Föderation durch die für das kantonale IdM im Bildungsbereich verantwortliche Person. Diese ist darum besorgt, dass für die Mitglieder des Bildungssystems ein sicherer und geschützter Anmeldeprozess bereitgestellt wird, und kennt die entsprechenden Lösungen zur Umsetzung dieses Anspruches auf Schul- bzw. Kantonebene. Im Hinblick auf den Anschluss von Schulen an die Föderation sorgt diese Fachperson für die Interoperabilität zwischen der kantonalen BildungsID und der BildungsID der Föderation. In der Föderation kann sich diese Fachperson mit den übrigen kantonalen Vertretenden vernetzen und sich – gemeinsam mit diesen – mit den SP austauschen. Die Föderation sieht dafür die Teilnehmerversammlung vor.

### 2.2.2 Bestehende Steuerungsstrukturen

Der Entscheid für eine Teilnahme an der Föderation FIDES ist Teil der kantonalen Massnahmen zur digitalen Transformation des kantonalen Schulsystems. Einmal getroffen, wird der Entscheid von der oben erwähnten, für das kantonale IdM zuständigen Fachperson umgesetzt.

Der Entscheid wirft aber auch Fragen nach einer gemeinsamen Strategie der Kantone im Hinblick auf die digitale Transformation des schweizerischen Bildungssystems auf. Diese Diskussionen sind von den Verantwortlichen für die Bildungspolitik zu führen. Sie werden an die Strukturen der EDK übertragen, wo sie von den geeigneten Gremien – zu denken ist an die KDS – als wiederkehrendes Traktandum behandelt werden.

Die Föderation ist jedoch nicht eine allein durch die Kantone, sondern gemeinsam mit dem Bund getragene Massnahme. Sie stützt sich auf das Bildungszusammenarbeitsgesetz<sup>1</sup> und gehört in den Arbeitsbereich des «Koordinationsausschusses Digitalisierung (KoA Digi)<sup>2</sup>». In Bezug auf die Föderation bildet dieser die nationale Ebene ab, auf der Bund und Kantone Steuerungsfragen zur Föderation gemeinsam diskutieren. Dem KoA Digi obliegt es, zuhanden der bildungspolitischen Entscheidungsträger bei Bund (SBFI) und Kantonen (EDK) die Formulierung und Vergabe der Leistungsvereinbarung für die Föderation, die Kontrolle über ihre Umsetzung und die Entscheide über die Weiterentwicklung der Föderation vorzubereiten. Vorgesehen ist, dass der KoA Digi dabei substantiell durch die Geschäftsstelle der Föderation unterstützt wird. Als Ausschuss soll er die Vorschläge der Geschäftsstelle validieren und sie zur Verabschiedung durch die Entscheidungsträger auf Seiten des Bunds und der Kantone aufbereiten.

### 2.2.3 Geschäftsstelle der Föderation FIDES

Die Geschäftsstelle der Föderation FIDES gewährleistet die Steuerungs- und Betriebsprozesse der Föderation. Gemäss Leistungsvereinbarung sorgt sie dafür, dass mit den Dienstleistungen der Föderation die strategischen Ziele umgesetzt werden. In Reglementen und Verträgen legt sie dazu die konkrete Organisation der Föderation fest, definiert Rollen, Funktionen, Rechte und Pflichten aller Teilnehmenden an der Föderation und spezifiziert die technischen Dienstleistungen der Föderation (vgl. Anhang I, *Reglemente und Verträge*).

Die Geschäftsstelle beauftragt und führt den Technischen Dienst der Föderation, der die Infrastruktur bereitstellt und für den technischen Betrieb verantwortlich ist.

<sup>1</sup> Die Bundesversammlung (2016). *Bundesgesetz über die Zusammenarbeit des Bundes mit den Kantonen im Bildungsraum Schweiz vom 30. September 2016*. [www.admin.ch/opc/de/federal-gazette/2016/7677.pdf](http://www.admin.ch/opc/de/federal-gazette/2016/7677.pdf) (07.01.2017)

<sup>2</sup> Schweizerische Eidgenossenschaft, Schweizerische Konferenz der kantonalen Erziehungsdirektoren (2016). *Mandat des Koordinationsausschusses Digitalisierung in der Bildung (KoA Digi)*. [edudoc.ch/record/124949/files/mandat-koa-digi\\_d.pdf](http://edudoc.ch/record/124949/files/mandat-koa-digi_d.pdf) (07.01.2017)

## 2.3 Kantone und SP sind Teilnehmende an der Föderation FIDES

Die Föderation FIDES nimmt einerseits Kantone, andererseits SP als Teilnehmende auf. Sie haben die Aufgabe, den Inhabern einer BildungsID den Zugang zu Online-Diensten zu ermöglichen. Die Föderation unterstützt sie dabei, indem sie die dafür bestehenden rechtlichen, organisatorischen und technischen Anforderungen bündelt und in Verträgen und Reglementen festlegt (vgl. Anhang I, *Reglemente und Verträge*). Diese zu akzeptieren, ist die Voraussetzung für den Beitritt zur Föderation. Sowohl die Kantone als auch die SP haben dies mit der Unterzeichnung eines auf ihre Teilnahme abgestimmten Vertrags zu bestätigen.

### 2.3.1 Kantone

Die Kantone anerkennen im Teilnahmevertrag ihre Verantwortung für die BildungsID, welche die Mitglieder ihrer Schulen verwenden. Die vertragliche Formalisierung stellt Verbindlichkeit her, damit die Kantone beim Anmeldeprozess bei Online-Diensten ihre Rolle wahrnehmen können. Mit der Akzeptanz dieser Verbindlichkeit bürgen sie für die Funktion, inhaltliche Ausgestaltung und Qualität der BildungsID. Dies beinhaltet folgende Punkte:

- dass nur Mitglieder des Bildungssystems über eine BildungsID verfügen, jede BildungsID nur einer einzigen Person zugeordnet ist und die darin enthaltenen Attribute den Anforderungen des gemeinsamen Modells der nationalen BildungsID (vgl. Anhang I, *Modell nationale BildungsID*) entsprechen und aktuell gehalten werden.
- dass die BildungsID im Rahmen eines zweckdienlichen IdM auf kantonaler Ebene verantwortet wird.
- dass eine Anmeldung mit der BildungsID jederzeit möglich ist.
- dass die digitalen Identitäten ausreichend vor unberechtigtem Zugriff geschützt sind.

Im Gegenzug erhalten die Kantone als Teilnehmende der Föderation ein Mitspracherecht bei organisatorischen Prozessen und technischen Standards (siehe oben). Als Teilhaber des Vertrauensraums können sie gemeinsam mit der Geschäftsstelle zuhanden des KoA Digi und der Auftraggeber Vorschläge zur Weiterentwicklung von der Föderation erarbeiten.

### 2.3.2 Dienstleistungsanbieter (Service Provider, SP)

Auch für die SP gelten Teilnahmebedingungen (vgl. [Kapitel 1.2.2](#)). Der Teilnahmevertrag enthält die entsprechenden rechtlichen, organisatorischen und technischen Anforderungen. Die Frage nach den pädagogischen Nutzungsmöglichkeiten wird nicht durch die Föderation beantwortet und ist daher nicht Gegenstand des Teilnahmevertrags.

Sobald SP Teilnehmende der Föderation sind, erhalten sie an der Teilnehmerversammlung ein Mitspracherecht im Hinblick auf die Entwicklung und Implementierung von technischen Lösungen.

## 2.4 Dienstleistungen der Föderation FIDES

Die Föderation FIDES erbringt für ihre Teilnehmenden Dienstleistungen in den Bereichen Organisation und Technik. Beide Bereiche werden durch Informations- und Kommunikationsdienstleistungen unterstützt.

Die organisatorischen Dienstleistungen der Föderation stellen die Zusammenarbeit der Teilnehmenden sicher. Dazu gehören:

- Umsetzung der Strategie der Föderation und Pflege der Reglemente
- Innovation und Weiterentwicklung des digitalen Bildungsraums Schweiz
- Geschäftsführung der Föderation
- Aufnahme neuer Teilnehmender an der Föderation
- Kommunikation und Vernetzung

Die technikbezogenen Dienstleistungen der Föderation betreffen das Anschliessen neuer IdP und Online-Dienste sowie die Sicherstellung des technischen Betriebs. Sie werden vom Technischen Dienst erbracht, der den Teilnehmenden Hilfestellungen bietet und sie bei der Planung und Umsetzung ihrer Vorhaben berät. Zentrales Element für den Support bildet eine FIDES-Website. Auf der Website haben die Teilnehmenden Zugang zu allen die Föderation betreffenden Dokumenten und Reglementen. Hier werden aktuelle Listen der Teilnehmenden und der zu ihnen gehörenden Metadaten publiziert.

## 2.5 Technische Konzeption der Föderation FIDES

Die Föderation FIDES orientiert sich in technischer Hinsicht an der im tertiären Bereich erprobten Lösung von SWITCH. Zur Entwicklung der technischen Architektur, zur Bestimmung der Technologien und bei der Umsetzung können bestehende Standards (eCH-Standards und weitere) sowie Good Practice-Beispiele aus der Schweiz (SWITCH, SuisseID, IDV-Schweiz im Bereich E-Gov) und dem europäischen Ausland (Dänemark, Estland, Niederlande, Schweden) herangezogen werden. (vgl. Anhang II, *Projekte und Good Practice zu Föderationen von Identitätsdiensten auf nationaler Ebene; Good Practice zu Föderationen von Identitätsdiensten im Bildungsbereich europäischer Länder*).

Der Kernprozess der Föderation ist die Authentifizierung der Endbenutzenden mit den persönlichen Anmeldedaten durch einen IdP, um den Zugang zu den Online-Diensten der SP zu ermöglichen. In der Föderation wird die Authentifizierung nicht mehr auf der Seite des SP durchgeführt, sondern vom IdP, der für die Überprüfung der Identität des Endbenutzenden verantwortlich ist. Auf Anfrage des Online-Diensts übermittelt der IdP in einem digitalen *Ausweis* die für die Autorisierung notwendigen Attribute an den SP. Mit diesem *Ausweis* erhält der Online-Dienst zwar die für die Autorisierung notwendigen Attribute übermittelt, nicht aber die volle Identität der Endbenutzenden. Endbenutzende werden gegenüber dem SP also pseudonymisiert, womit sich der Datenschutz optimieren lässt.

Die technische Umsetzung dieses Prozesses verlangt, dass die zu übermittelnden Attribute einer BildungsID standardisiert sind. Auf technischer Ebene werden die Vereinbarungen zwischen IdP und SP durch den zentralen Dienst *Metadaten-Download* ausgetauscht. Die Attribute der BildungsID werden via den Browser der Endbenutzenden an die SP übermittelt (vgl. Anhang I, *Modell nationale BildungsID*).

### 3 AUFBAU DER FÖDERATION FIDES

In diesem Kapitel werden Aspekte des Aufbaus der Föderation FIDES vorgestellt. Zunächst wird der Ablauf des Aufbaus mit einem Szenario beschrieben. Dieses Szenario wurde ausgehend von der Einschätzung der aktuellen Situation als das wahrscheinlichste bewertet. Anschliessend werden die Verantwortlichkeiten der Akteure beschrieben, die bei dem Aufbau der Föderation wahrgenommen werden müssen. Schliesslich werden sowohl die Aufwendungen der Kantone für einen Beitritt zur Föderation, als auch die Kosten der Geschäftsstelle und deren Finanzierung vorgestellt.

#### 3.1 Aufbau der Föderation FIDES

Der hier beschriebene Aufbau der Föderation FIDES setzt einen positiven Beschluss der EDK-Plenarversammlung voraus und geht von den aktuellen konzeptionellen Grundlagen aus. Aufgrund dieser Annahmen sind folgende Schritte durchzuführen:

- Die Kantone beauftragen educa.ch in einer Leistungsvereinbarung mit der Gründung und dem Aufbau der Föderation
- Die Geschäftsstelle der Föderation wird statuiert und entscheidet über die Organisation des technischen Diensts
- Die Geschäftsstelle entwickelt die für die Teilnahme notwendigen Verträge und schliesst Verträge mit den teilnehmenden Kantonen ab
- Teilnehmende Kantone prüfen ihr IdM im Hinblick auf ihre Teilnahme an und passen es, falls nötig, mit Unterstützung der Geschäftsstelle an die Anforderungen der Föderation an
- Die Geschäftsstelle organisiert und etabliert die Kernprozesse der Föderation, beschafft dafür notwendige Software, lässt sie entwickeln oder entwickelt sie selbst
- Um das Zusammenspiel der technischen Systeme zu prüfen, stellt die Geschäftsstelle für die IdP und SP eine Testplattform bereit
- Teilnehmende Kantone erarbeiten mit Unterstützung des technischen Diensts der Föderation die technischen Schnittstellen zur Föderation
- Die Geschäftsstelle verhandelt mit den SP die Aufnahme in die Föderation und erarbeitet bzw. schliesst mit ihnen die notwendigen Verträge ab
- Die SP passen ihre Systeme mit Unterstützung des technischen Diensts an die technischen Standards der Föderation an
- Zusammen mit den teilnehmenden Kantonen und SP nimmt die Geschäftsstelle den Betrieb der Föderation auf

Varianten dieses Aufbauszenarios ergeben sich aus der unterschiedlichen Bereitschaft der Kantone und/oder SP der Föderation beizutreten. Sie wirkt sich besonders stark auf den Personalbedarf der Föderation aus (vgl. Anhang I, *Szenarien für den Aufbau der Föderation FIDES*).

#### 3.2 Verantwortlichkeiten

In diesem Abschnitt werden die während Aufbau und Betrieb der Föderation wahrzunehmenden Verantwortlichkeiten beschrieben und den einzelnen Akteuren zugewiesen.

### 3.2.1 Auftraggebende

- Die EDK fasst eine Leistungsvereinbarung für den Aufbau und Betrieb der Föderation FIDES
- Die Finanzierung der Geschäftsstelle muss mit den Auftraggebenden geklärt werden. Sie müssen sicherstellen, dass die finanziellen Mittel vorhanden sind, um den Aufbau und den Betrieb zu gewährleisten
- Die Auftraggebenden müssen über die in Anhang I, *Szenarien für den Aufbau der Föderation FIDES* beschriebenen Umsetzungsoptionen entscheiden

### 3.2.2 Kantone

- Die Kantone sind verantwortlich für das IdM in ihrem Kanton
- Das IdM innerhalb des Kantons kann sowohl zentral als auch dezentral organisiert sein. Entscheidend ist, dass der Kanton die für den Anschluss seiner kantonalen IdP nötigen Informationen und Kontakte an die Föderation FIDES übermitteln kann. Dabei bleibt es den Kantonen freigestellt, wie sie sich organisieren (mögliche Aufwendungen sind unter [Kapitel 3.3](#) beschrieben)
- Die Kantone klären gemeinsam mit ihren Schulen, welche Online-Dienste benötigt werden, und definieren, welche Online-Dienste in die Föderation aufgenommen werden sollen
- Die Kantone koordinieren die Anpassung der Schnittstellen der IdP in ihrem Kanton an die Schnittstelle der Föderation

### 3.2.3 Geschäftsstelle

- Die Geschäftsstelle ist für den technischen Dienst und die für den Aufbau und späteren Betrieb der Föderation FIDES erforderlichen Prozesse zuständig
- Sie leistet Unterstützung für IdP und SP beim Anschliessen an die Föderation und ist Ansprechpartnerin für die Kantone, wenn es um die weitere Entwicklung der Föderation und Probleme während des Betriebs geht
- Die Geschäftsstelle ist zuständig für die Verträge mit den Kantonen und den SP sowie für allfällige Vertragsverhandlungen im Hinblick auf eine Interföderationsverbindung
- Die Geschäftsstelle koordiniert gemeinsam mit den teilnehmenden Kantonen die Diskussion über die Kriterien zur Aufnahme von SP in die Föderation

## 3.3 Beitritt und Teilnahme eines Kantons an der Föderation FIDES

Das Konzept für die Föderation FIDES sieht grundsätzlich vor, dass die Kantone ihr IdM selber an die Anforderungen der Föderation anpassen und für entsprechende Aufwendungen selber aufkommen. Als erste Übersicht folgt hier eine Darstellung der Schritte, die zu unternehmen sind um der Föderation FIDES beizutreten. Aus ihr lassen sich ebenfalls die zu erwartenden Aufwendungen für den Beitritt und die Teilnahme an der Föderation FIDES ableiten. Der Übersicht wird generisch gehalten, da sich die Verhältnisse von Kanton zu Kanton unterscheiden. Sie wurde in Gesprächen mit fünf kantonalen FIDES-Referenzpersonen validiert, indem die getroffenen Annahmen mit den, in ihrem Kanton laufenden bzw. bereits abgeschlossenen IdM-Projekten verglichen wurden.

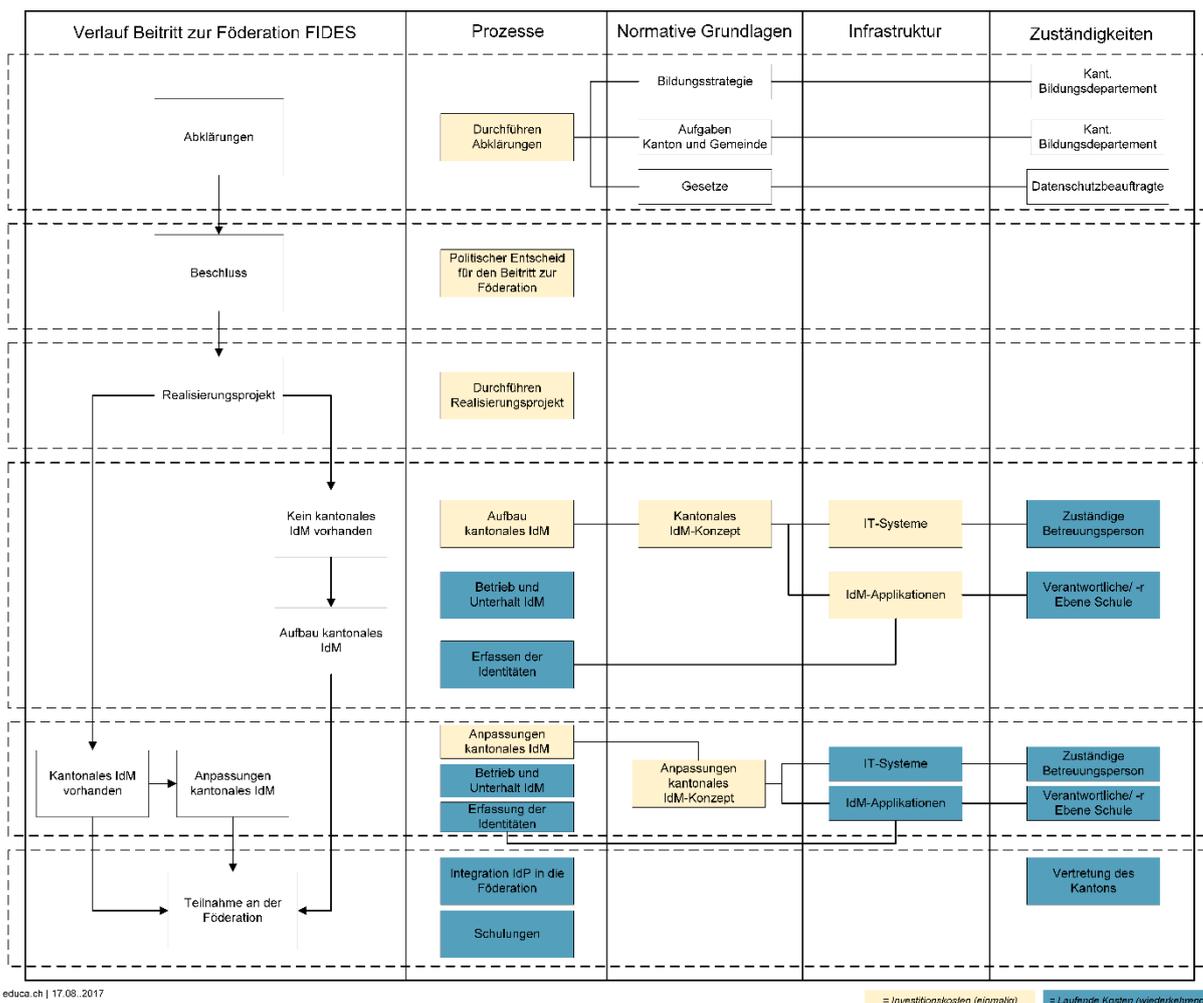


Abbildung 1: Beitritt und Teilnahme eines Kantons an der Föderation FIDES

### 3.3.1 Entscheidungsgrundlagen

Die Grundlage für einen Beitritt zur Föderation FIDES bilden die Ergebnisse der folgenden Abklärungen:

Die Teilnahme an der Föderation FIDES sollte sich auf die kantonale Bildungsstrategie stützen und einen Beitrag leisten zur sicheren und geschützten Nutzung von Online-Diensten im Unterricht, an Schulen und in der Bildungsverwaltung. Dazu müssen gesetzliche Grundlagen ein kantonales IdM erlauben. Zentral für eine Teilnahme an der Föderation FIDES ist, dass die Koordination des IdM in der Hand des Kantons liegt. Eine wichtige Rolle dabei spielt die Aufgabenteilung zwischen Kanton und Gemeinden. In dieser Koordination bzw. der Erarbeitung der konzeptuellen Grundlagen dafür liegt nach Einschätzung der kantonalen Referenzpersonen der grösste Aufwand. Weiter ist zu prüfen, ob im Kanton ein rechtlicher Rahmen über die Verwendung der BildungsID besteht. Dazu ist die bzw. der Datenschutzbeauftragte des Kantons mit einzubeziehen.

Entscheidend für die Eignung eines IdM ist, dass der Kanton die Verantwortung über die bereitgestellten BildungsID übernimmt, die Koordination des IdM in seiner Hand liegt und er in der Lage ist, eine Liste der im IdM eingesetzten Identitätsdienste (IdP) zu erstellen. Ob die IdM-Lösung dann zentral oder dezentral betrieben wird, ist nachrangig. (vgl. Anhang II: 2. Good Practice zu kantonalen BildungsID-Lösungen)

Neben den Abklärungen strategischer und rechtlich-organisatorischer Hinsicht muss der Kanton für sich abwägen, ob die Föderation für ihn einen Nutzen darstellt.

Mögliche Ergebnisse der Abklärungen sind:

- Der Kanton sieht im Beitritt zur Föderation FIDES einen Nutzen und besitzt die zum Beitritt notwendigen Grundlagen bzw. sieht vor, diese zu erarbeiten.
- Der Kanton sieht keinen Nutzen im Beitritt zur Föderation FIDES und/oder hat nicht die Mittel zur Verfügung, die notwendigen Grundlagen bereitzustellen.

### 3.3.2 Beschluss

Der Beschluss über die Teilnahme an der Föderation ist ein politischer Entscheid und wird über die im Kanton bestehenden Strukturen gefasst. Er ist mehrteilig und umfasst folgende Entscheide:

- Grundsätzlicher Entscheid für bzw. gegen eine Teilnahme an der Föderation FIDES,
- Zeitpunkt des Beitritts zur Föderation FIDES,
- Massnahmen des Kantons, die die Teilnahme an der Föderation FIDES ermöglichen und den Beitritt vorbereiten.

### 3.3.3 Realisierungsprojekt

Wenn sich der Kanton für eine Teilnahme an der Föderation FIDES entscheidet, folgt ein auf den Zeitpunkt des Beitritts abgestimmtes Realisierungsprojekt. Der Umfang des Realisierungsprojekts ist vom Ergebnis der Abklärungen abhängig. Kantone mit einem bestehenden IdM werden weniger Aufwand zu gewärtigen haben als Kantone, die noch über kein IdM verfügen. Ist ein kantonales IdM vorhanden und für einen Beitritt zur Föderation FIDES geeignet, sind keine oder nur kleine Anpassungen im Rahmen des Life-Cycle-Managements nötig. Aufwändiger ausfallen wird das Realisierungsprojekt, falls ein kantonales IdM zwar vorhanden ist, aber an die Föderation FIDES angepasst werden muss, oder kein kantonales IdM besteht und aufgebaut werden muss.

#### ▪ **Kantone ohne kantonales koordiniertes IdM**

Bei Kantonen ohne kantonales Identitätsmanagement fallen für den Aufbau des IdM zunächst einmalige Kosten an. Es ist ein kantonales, auf den kantonalen IT-Konzepten basierendes IdM-Konzept zu erstellen. Das Einrichten des IdM bedingt sodann den Betrieb von IT-Systemen, die dessen Infrastruktur bereitstellen, sowie die Implementierung geeigneter IdM-Applikationen. Dabei kann sich der Kanton an den Vorgaben der Föderation FIDES orientieren, um die Kompatibilität seiner Infrastruktur mit der Föderation FIDES zu gewährleisten. Auf der Ebene der Zuständigkeiten werden mit der Einführung des IdM bestehende Aufgabenbereiche von Personen erweitert, um den Betrieb und den Unterhalt der benötigten Infrastruktur zu gewährleisten. Als Zuständige für die Erfassung der Identitäten sind in den meisten Fällen Verantwortliche auf Ebene Schule prädestiniert. Je nach Ausgestaltung des IdM im Kanton kann diese Aufgabe aber auch an andere Personen delegiert werden.

#### ▪ **Kantone mit kantonalem koordiniertem IdM**

Bei Kantonen mit bereits eingerichtetem Identitätsmanagement umfassen die Aufwendungen für ein kantonales IdM die Erfassung von Identitäten, den Betrieb und Unterhalt der nötigen IT-Infrastrukturen. Bereits bestehende Aufwendungen auf der Ebene der Infrastruktur sind die für das IdM in Anspruch genommenen kantonalen IT-Systeme und IdM-Applikationen. Auf der Ebene der Zuständigkeiten bestehen Aufwände hinsichtlich der Betreuung der IT-Systeme und der IdM-Applikationen. Falls die, vor dem Beschluss für die Föderation FIDES getätigten, Abklärungen ergeben haben, dass das bestehende IdM-Konzept angepasst werden muss, entstehen einmalige Kosten auf der Ebene der normativen Grundlagen sowie möglicherweise auch auf der Ebene der Infrastruktur.

### 3.3.4 Beitritt und Teilnahme

Im Hinblick auf die Teilnahme an der Föderation sind die Kantone dafür verantwortlich, die IdP des kantonalen IdM in die Föderation FIDES zu integrieren, was mit sehr unterschiedlichem Aufwand verbunden sein kann. Auf der personellen Ebene bestellen die Kantone die Vertretung für die Teilnehmerversammlung. Im Weiteren sind Aufwendungen für Schulungen des technischen und administrativen Verwaltungspersonal sowie der Schulleitungen, Lehrpersonen und der Schülerinnen und Schüler vorzusehen, da diese mit den Funktionen der Föderation vertraut gemacht werden müssen.

## 3.4 Kosten der Föderation FIDES

Die Kostenfolgen der Föderation FIDES werden im Folgenden Kosten, die für den Aufbau der Föderation anfallen, und Kosten für den Betrieb, die für das Erbringen der Dienstleistungen der Föderation entstehen, unterschieden. Die angeführten Beträge sind Schätzungen, in denen Gehälter auf der Basis der aktuellen «Richtpositionsumschreibung zur Personalverordnung» und Gehaltsklassentabellen des Kantons Bern berechnet wurden. Die Beträge wurden sodann mit den Kosten der, in den Niederlanden bereits bestehenden Föderation von Identitätsdiensten (vgl. Anhang II, *Good Practice zu Föderationen von Identitätsdiensten im Bildungsbereich europäischer Länder*) und denjenigen des technischen Diensts von SWITCHaai (vgl. Anhang II, *Projekte und Good Practice zu Föderationen von Identitätsdiensten auf nationaler Ebene*) verglichen und validiert.

Für die Föderation ist in den Jahren 2018 und 2019 mit Kosten für den Aufbau von total CHF 1'840'000 zu rechnen. Die Betriebskosten belaufen sich im 2019 auf CHF 1'240'000, und ab 2020 sind sodann jährliche Betriebskosten von bis zu CHF 1'680'000 zu erwarten.

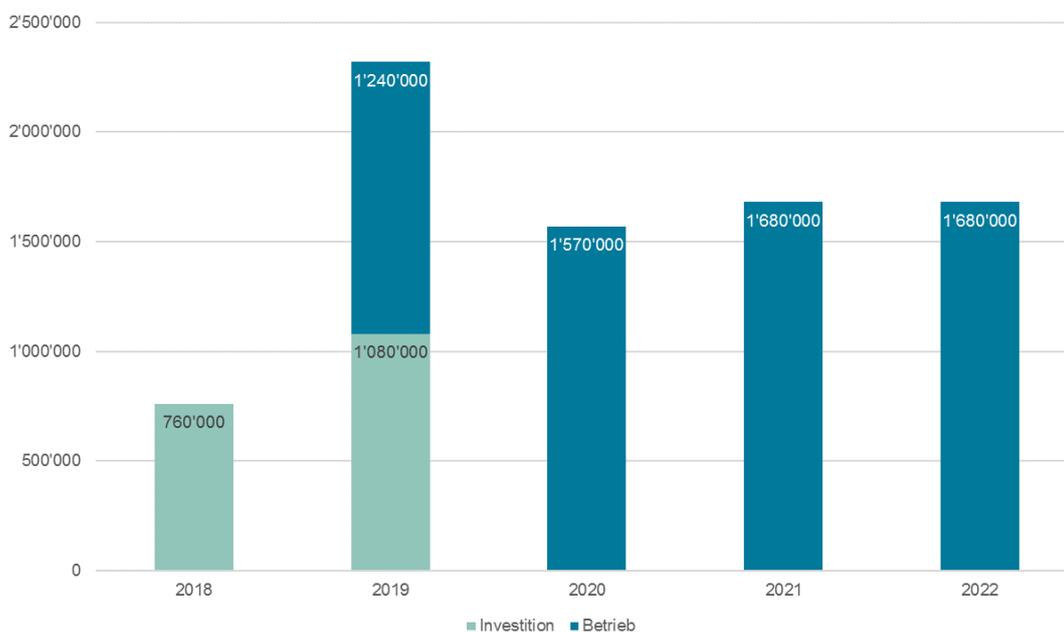


Abbildung 2: Geschätzte Kosten für den Aufbau und den Betrieb der Föderation FIDES

### 3.4.1 Kosten für den Aufbau der Föderation FIDES

Die Kosten für den Aufbau der Föderation FIDES erfassen alle notwendigen Arbeiten, damit sie auf den Jahresbeginn 2019 als Organisation gegründet werden kann. Dafür fallen im 2018 v. a. Vorbereitungsarbeiten an, wozu der Aufbau des Geschäftsstellenmanagements, die Rekrutierung und Anstellung von Personal und das Erstellen der rechtlichen Grundlagen gehören; bereits aufgenommen werden muss ebenfalls die Bekanntmachung der Föderation bei den Anspruchsgruppen, insbesondere im Hinblick auf das Finden von initialen Teilnehmenden. Für das Jahr 2019 ist vorgesehen, die IdP von mindestens zehn teilnehmenden Kantonen und die Online-Dienste von ebenfalls mindestens zehn teilnehmenden SP in die Föderation zu integrieren. Die Marketingmassnahmen zur

Lancierung der Föderation sind daher fortzusetzen. Hinzu kommen die Aufwendungen für den Aufbau der IT-Infrastruktur und die Beratung der initial teilnehmenden Kantone und SP. Es werden technische Grundlagen dokumentiert und den später zu integrierenden IdP und SP zur Verfügung gestellt.

Kosten Aufbau der Föderation FIDES	2018	2019
Aufbau des Geschäftsstellenmanagements (inkl. LV, Steuerung, Governance)	145'000	
Rechtliche Grundlagen (inkl. Verträge, SLA/OLA, Reglement)	290'000	
Rekrutierung und Anstellung (inkl. Personalsuche, Assessment, Arbeitsvertrag)	25'000	
Marketing (inkl. Bekanntmachung, Dokumentation, Website, Veranstaltungen)	220'000	190'000
Aufbau der IT-Infrastruktur (inkl. technische Dienste)		320'000
Beratung initialer Teilnehmer (inkl. Onboarding, Pilots, technische Integration)		460'000
Technische Grundlagen für IdP/SP (inkl. Middleware, Testing, Richtlinien)	80'000	110'000
<b>Gesamtkosten Investition</b>	<b>760'000</b>	<b>1'080'000</b>

### 3.4.2 Betriebskosten

Die Föderation FIDES soll auf den 01.01.2019 gegründet werden, so dass ab diesem Zeitpunkt Betriebskosten anfallen. Im ersten Betriebsjahr belaufen diese sich auf CHF 1'240'000. Sie steigen im 2020 auf CHF 1'570'000 und ab 2021 auf CHF 1'680'000, was auf den fortschreitenden Beitritt weiterer Kantone (inklusive IdP) und SP (inklusive Online-Dienste) zur Föderation zurückzuführen ist. Der Schätzung liegt dabei die Annahme zugrunde, dass im 2020 die Anzahl der neu der Föderation beitretenden SP die Anzahl der neu beitretenden Kantone übersteigt; das Ziel ist, 2021 mindestens 18 Kantone und 150 SP für eine Teilnahme gewonnen und deren IdP respektive Online-Dienste integriert zu haben.

Kosten Betrieb Föderation FIDES	2019	2020	2021	2022
Management (inkl. Leitung, Qualitätssicherung, Prozessmanagement, Risikomanagement, Gremien)	250'000	250'000	250'000	250'000
Verwaltung (inkl. Administration, Kommunikation, Rechnungswesen, Berichterstattung, Personal Management)	200'000	200'000	200'000	200'000
Service Management (inkl. Marketing, Akquisition, Vertragsmanagement, Austritt)	190'000	190'000	190'000	190'000
Supportleistung (inkl. Service Desk, Dokumentation, Schulungen)	130'000	240'000	360'000	360'000
Technische Integration (inkl. IdP, SP, Schnittstellen)		110'000	90'000	90'000
Unterhalt IT-Infrastruktur (inkl. System Administration, Wartung und Betrieb, Lizenzierung)	450'000	450'000	460'000	460'000
Externe Dienstleistungen (z. B. Sicherheit, Recht, Technologie)	20'000	20'000	20'000	20'000
Innovation und Weiterentwicklung		110'000	110'000	110'000
<b>Gesamtkosten Betrieb</b>	<b>1'240'000</b>	<b>1'570'000</b>	<b>1'680'000</b>	<b>1'680'000</b>

## 4 GLOSSAR

Begriff	Begriffsdefinition
Authentifizierung	Vorgang der Prüfung einer behaupteten Identität
Autorisierung	Vorgang des Prüfens der Zugriffsberechtigung einer authentifizierten Entität und der Zugriffserteilung
BildungsID	E-ID, die für den Zugang zu systemrelevanten Online-Diensten im Schweizer Bildungswesen verwendet wird.
BildungsID (kantonale)	Kantonal verantwortete und organisierte BildungsID. Hierbei kann es sich um eine zentrale oder eine – innerhalb eines Kantons – föderierte Lösung handeln. Sie ermöglicht den Zugang zu kantonsweit genutzten Online-Diensten
BildungsID (national föderierbare)	Kantonal verantwortete BildungsID, die dem Modell 'nationale BildungsID' entspricht
BildungsID (nationale)	BildungsID, die dem Modell 'nationale BildungsID' entspricht und von einem Kanton verantwortet wird, der an der Föderation von Identitätsdiensten für den Bildungsraum Schweiz teilnimmt. Sie ermöglicht einen kantonal gesteuerten Zugang zu den Online-Diensten der Föderation
Dienstleistungsanbieter (Service Provider SP)	Organisation, die Online-Dienste betreibt
digitaler Bildungsraum	digitale Ausprägung des Bildungsraums Schweiz
Föderation FIDES	Name der Föderation von Identitätsdiensten für den Bildungsraum Schweiz, früher nur 'Föderation von Identitätsdiensten'
Identifikation	Vorgang, der zum eindeutigen Erkennen einer Entität dient
Identitätsanbieter (Identity Provider IdP)	technische Komponente, die digitale Identitäten verwaltet und herausgibt
Identitätsdaten	Personendaten die in einer E-ID zur Beschreibung einer Person zusammengefasst sind. In manchen Fällen sind auch nur die Angaben für die Anmeldung an einem Computer bzw. digitalen Dienst gemeint.
Identitätsmanagement (Identity Management IdM)	Beschreibt die Verwaltung von Identitäten, das Identitätsmanagement
Nutzungsdaten (personalisierte)	Daten die bei der Nutzung eines Online-Diensts durch Endbenutzende entstehen. Sind sie auf einen Endbenutzer / eine Endbenutzerin rückführbar, sind sie als personalisiert zu verstehen
Online-Dienst	Angebot eines Dienstleistungsanbieters
Personendaten	alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen (DSG, Art. 3)
Pseudonymisierte Attribute	Attribute einer E-ID welche keinen Rückschluss auf einen Endbenutzer/eine Endbenutzerin erlauben
Rechtssicherheit	Der Grundsatz der Rechtssicherheit gewährleistet die Vorhersehbarkeit, die Berechenbarkeit und die Beständigkeit staatlichen Handelns. Es verlangt eine klare, einfache und voraussehbare Regelung rechtlicher Verhältnisse (Schutz vor unklarer oder unvollständiger Gesetzgebung), keine zu häufigen Gesetzesänderungen, eine möglichst konstante Rechtsprechung und ein stabiles funktionierendes Rechtssystem.
Safety	Betriebssicherheit, die durch technische und organisatorische Massnahmen erreicht wird.
Standardisierte Attribute	Attribute einer E-ID für die Aufbau und Bedeutung definiert und vereinbart sind

## **ANHANG I: ZENTRALE ASPEKTE DER FÖDERATION FIDES**

---

1	Modell nationale BildungsID .....	19
1.1	Minimal notwendige Attribute .....	19
1.2	Herkunft der Daten .....	19
1.3	Qualität der Daten .....	19
2	Grundsätze, Verfahren und Standards der Föderation FIDES .....	20
2.1	Grundsätze der Föderation FIDES .....	20
2.2	Verfahren der Föderation FIDES .....	20
2.3	Technologien der Föderation FIDES .....	20
3	Reglemente und Verträge .....	21
3.1	Reglemente der Föderation FIDES .....	21
3.2	Verträge der Föderation FIDES .....	21
4	Szenarien für den Aufbau der Föderation FIDES .....	22
4.1	Voraussetzung für die Aufnahme des Betriebs der Föderation FIDES .....	22
4.2	Szenario A .....	22
4.3	Szenario B .....	23
4.4	Szenario C .....	24
3.6	Bundesamt für Polizei fedpol .....	34

# 1 MODELL NATIONALE BILDUNGSID

Aufbau, Struktur und zulässige Werte der Attribute der nationalen BildungsID werden im «Modell nationale BildungsID» als Standard der Föderation FIDES festgelegt. Das Modell basiert auf den BildungsID der Kantone. Es zielt darauf, deren – im Rahmen des kantonalen Identitätsmanagements (IdM) bestimmten – Attribute und die ihnen zugeordneten Werte interoperabel, das heisst föderationsfähig zu machen. Dabei ist der universale eindeutige Identifikator (UUID, von Universally Unique Identifier) das einzige Attribut, das durch das Modell nationale BildungsID den kantonalen BildungsID hinzugefügt wird. Es wird vom technischen Dienst der Föderation erzeugt und verwaltet.

## 1.1 Minimal notwendige Attribute

- **... zur Übermittlung von Daten vom IdP an den SP**  
Der universal eindeutige Identifikator ist das einzige Attribut, das zur Authentifizierung zwingend übermittelt werden muss. Dieses Attribut erlaubt die Pseudonymisierung der Endbenutzenden und gewährleistet zugleich, dass diese hinreichend identifiziert werden können.
- **... für die Verwaltung der BildungsID innerhalb des IdM**  
Die Endbenutzenden müssen eindeutig mit ihrer BildungsID in Beziehung gesetzt werden können. Hierfür kann der Betreiber des IdM die AHV-Nummer, eine Personalnummer oder eine andere Referenz, die eine rechtlich ausreichende Identifikation der natürlichen Person erlaubt, bestimmen und nutzen. Für die Verwaltung der BildungsID werden von der Föderation FIDES zudem noch der Benutzername und das dazugehörige, individuelle Passwort verlangt.
- **... für die SP**  
Die SP benötigen zur Autorisierung weitere Angaben zu den Endbenutzenden. Wichtige Attribute sind:
  - Rolle (Lehrerin/Lehrer, Schülerin/Schüler etc.)
  - Bildungsinstitution (Name der Schule)
  - Schulstufe/Schuljahr
  - Schulklasse
  - Kanton

Gerne würden SP weitere Attribute von der Föderation anfordern. Hier ist jedoch zu beachten, dass durch die Kombination von einzeln unkritischen Attributen die eineindeutige Identifikation einer Person möglich wird. So ist der Name einer Person noch nicht ausreichend für eine eineindeutige Identifikation. Wird der Name aber mit Geburtsdatum, Geburts- und Wohnort kombiniert – Angaben, die je für sich genommen unkritisch sind –, ist ein grosser Schritt in Richtung eineindeutiger Identifikation gemacht.

## 1.2 Herkunft der Daten

Der universal eindeutige Identifikator muss von einer zentralen Stelle erzeugt, vergeben und verwaltet werden, damit die Übertragbarkeit der BildungsID gewährleistet werden kann. Alle weiteren Attribute und Werte werden von unterschiedlichen Quellen – Bildungsdepartementen, Personalabteilungen, Schulverwaltungen, Schulleitungen etc. – bestimmt und den IdP übermittelt.

## 1.3 Qualität der Daten

Grundsätzlich ist die bestmögliche Qualität der Daten anzustreben. Wegen ihrer dezentralen Herkunft werden diese Daten aber voraussichtlich stark heterogen bereitgestellt, weshalb dieser hohe Qualitätsanspruch nur mit erheblichem Aufwand zu erreichen ist. Der Aufwand zur Qualitätssicherung sollte sich allerdings innerhalb eines tragbaren Rahmens bewegen und ist daher durch Dienstleistungen der Föderation FIDES zu unterstützen. Der angestrebte Standard soll ermöglichen, dass die im normalen Schulbetrieb gepflegte Sorgfalt und Qualität für den Zugang zu Online-Diensten über die Föderation ausreichend sind.

## 2 GRUNDSÄTZE, VERFAHREN UND STANDARDS DER FÖDERATION FIDES

Die Vereinbarung von gemeinsamen Grundsätzen, Verfahren und Standards und deren Einhaltung bilden die Basis für die Umsetzung des Vertrauensraums der Föderation FIDES. Alle involvierten Parteien verpflichten sich vertraglich, sie einzuhalten und in Bezug auf die BildungsID anzuwenden.

Die im Rahmen der E-Government Initiative definierten eCH-Standards dienen als Grundlage bei der Konzeption der Föderation. Insbesondere werden die spezifischen eCH-Standards zu digitalen Identitäten berücksichtigt.

### 2.1 Grundsätze der Föderation FIDES

Die Identifikation der Endbenutzenden wird mit der bestmöglichen Qualität durchgeführt (vgl. Anhang I: *Modell nationale BildungsID*). Dazu sind die Daten der kantonalen BildungsID aktiv und zeitnah auf einem aktuellen Stand zu halten.

Die mit der BildungsID verbundenen persönlichen Daten der Endbenutzenden werden von allen an der Föderation FIDES beteiligten Parteien nach aktuellem Stand der Technik vor unberechtigtem Zugriff und Missbrauch geschützt.

Die durch die Nutzung der Online-Dienste entstehenden Daten werden nicht an Dritte weitergegeben oder für eine kommerzielle Nutzung ausgewertet. SP deklarieren gemäss ihren vertraglichen Pflichten in verständlicher Form, wie Daten, die bei der Nutzung ihrer Online-Dienste generiert werden, weiterverarbeitet und genutzt werden. Auf jeden Fall gilt für die Weiterverwendung von Nutzerdaten das Opt-in-Prinzip, d.h. Endbenutzende müssen vor der Nutzung weiterführender Angebote des SP um ihre explizite Zustimmung gebeten werden.

### 2.2 Verfahren der Föderation FIDES

Verbindliche Prozesse garantieren einen hohen Grad an Verlässlichkeit. Organisationsübergreifende Aktivitäten innerhalb des Kontexts der Föderation FIDES sind dokumentiert und für alle Teilnehmenden transparent.

Alle die Föderation betreffenden Informationen werden allen Teilnehmenden zeitnah zugänglich gemacht.

Organisationsübergreifende Notfallpläne erlauben bei Vorfällen, welche die Sicherheit innerhalb der Föderation gefährden, eine schnelle und zuverlässige Intervention. Verantwortliche und Ansprechpartner sind allen Teilnehmenden bekannt.

Bei der Weiterentwicklung der Föderation werden die Teilnehmenden aktiv und nachvollziehbar mit einbezogen.

### 2.3 Technologien der Föderation FIDES

Die Teilnehmenden an der Föderation FIDES verwenden den OASIS-Standard SAML2 für die sichere Anmeldung von Endbenutzenden sowie für die geschützte Übertragung von Attributen der BildungsID. Dieser Standard wird sowohl von einer grossen Zahl kommerzieller Produkte als auch von Open-Source und freier Software verwendet. Mögliche Weiterentwicklungen sind OpenID Connect oder OAuth2; aktuell sind diese Standards für eine Föderation von Identitätsdiensten aber noch nicht ausreichend stabil spezifiziert.

Die Authentifizierung der technischen Komponenten untereinander verwendet digitale Zertifikate gemäss dem ITU-T Standard X509v3.

Im Weiteren verwendet die Föderation HTTPS für verschlüsselten Informations- und Datenaustausch. Datenübertragungen und Web-Services verwenden REST zur Codierung von Daten.

## 3 REGLEMENTE UND VERTRÄGE

Der Zusammenhalt der Föderation FIDES als Ganzes wird durch Reglemente und Verträge geregelt. Sie werden während der Aufbauphase der Föderation erarbeitet. Die zu diesem Zeitpunkt bereits der Föderation beigetretenen Kantone werden in diese Arbeiten einbezogen.

### 3.1 Reglemente der Föderation FIDES

Die Reglemente der Föderation FIDES sind normative Dokumente, die den reibungslosen Betrieb der Föderation sicherstellen. Sie sind Teil der Verträge, werden von der Geschäftsstelle der Föderation FIDES verantwortet und sind für die Teilnehmenden der Föderation verbindlich.

- **Statuten der Föderation**  
Die Statuten der Föderation beschreiben die Organisationsstruktur und definieren Rollen, Funktionen, Rechte und Pflichten jedes Akteurs der Föderation. Sie regeln unter anderem, wie sich die Geschäftsstelle konstituiert, wie die Teilnehmerversammlung funktioniert und wie diese beiden Gremien zusammenwirken.
- **Service-Reglement und Service-Level-Agreements**  
Im Service-Reglement werden die Angebote der Föderation und deren Dienstleistungen detailliert festgehalten und beschrieben. Verschiedene Service-Level-Agreements (SLA) werden den Vertragspartnern die Dienstleistungen der Föderation zusichern.

### 3.2 Verträge der Föderation FIDES

#### Leistungsvereinbarung

Die Leistungsvereinbarung regelt die Beziehung zwischen den Auftraggebenden und der auftragnehmenden Organisation. Sie beinhaltet den Auftrag für Aufbau und Betrieb der Föderation FIDES auf der Grundlage des Rahmenkonzepts der Föderation. Die Auftragnehmerin bzw. der Auftragnehmer bietet die Föderation als Dienst an und übernimmt die Trägerschaft der Geschäftsstelle. Die Finanzierung wird in der Leistungsvereinbarung geregelt.

#### Dienstleistungsvertrag

Falls der technische Dienst nicht durch dieselbe Organisation wie die Geschäftsstelle betrieben wird, muss ein Leistungsvertrag zwischen der Geschäftsstelle der Föderation und der Organisation, die den technischen Dienst betreibt, unterzeichnet werden.

#### Teilnahmevertrag

Die Teilnahmeverträge regeln die Rechte und Pflichten der Teilnehmenden und werden jeweils zwischen der Geschäftsstelle der Föderation und dem teilnehmenden Kanton (Bildungsdepartement), bzw. zwischen Geschäftsstelle und teilnehmenden SP unterzeichnet. Im Teilnahmevertrag enthalten sind auch die Kriterien für die Aufnahme der SP in die Föderation.

## 4 SZENARIEN FÜR DEN AUFBAU DER FÖDERATION FIDES

Die nachfolgenden Szenarien für den Aufbau der Föderation FIDES beziehen sich auf die Aktivitäten, die zeitlich zwischen dem Entscheid der EDK-Plenarversammlung und der Betriebsaufnahme der Föderation liegen. Alle drei haben zum Ziel, die für die Betriebsaufnahme der Föderation notwendigen Voraussetzungen bereitzustellen. Variablen der Szenarien sind dabei:

- die Anzahl der Teilnehmenden bei Aufnahme des Betriebs
- die zeitliche Verteilung des Beitritts weiterer Teilnehmender während des Betriebs

### 4.1 Voraussetzung für die Aufnahme des Betriebs der Föderation FIDES

Folgende Voraussetzungen für die Aufnahme des Betriebs der Föderation FIDES sind im Rahmen der vorangehenden Aufbauphase zu schaffen bzw. zu klären:

- Entscheid über ausführende Organisationen für Geschäftsstelle und technischen Dienst
- Festlegung der Standards der Föderation bezüglich Technik, Prozessen und Organisation
- Abschluss des Teilnahmevertrags durch eine Mindestzahl von Kantonen
- Abschluss des Teilnahmevertrages durch eine Mindestzahl von SP
- Die teilnehmenden Kantone haben mindestens für einen Teilbereich ihres Schulsystems ein IdM aufgebaut und die Standards der Föderation umgesetzt.
- Die teilnehmenden SP haben die Standards der Föderation umgesetzt.
- Die zentralen organisatorischen und technischen Dienstleistungen der Föderation stehen bereit.

### 4.2 Szenario A

#### Annahme

- Minimale Anzahl Kantone bestätigen Teilnahme
- Keine teilnehmenden SP bekannt

#### Szenario

Die EDK bestimmt die Organisation, mit der sie einen Leistungsauftrag für die Geschäftsstelle der Föderation FIDES vereinbart. Die Geschäftsstelle statuiert sich und entscheidet über die Organisation des technischen Diensts. Die Geschäftsstelle ermittelt die bei Betriebsaufnahme teilnehmenden Kantone. Die Geschäftsstelle entwickelt die für die Teilnahme notwendigen Verträge und schliesst Verträge mit den teilnehmenden Kantonen ab. Die Geschäftsstelle bestimmt mit den teilnehmenden Kantonen, welche SP zur Betriebsaufnahme in der Föderation aufgenommen werden sollen. Die Geschäftsstelle und die teilnehmenden Kantone vereinbaren Kriterien für die Zulassung weiterer SP. Zusammen mit den Kantonen erarbeitet die Geschäftsstelle die Datenschutzerfordernungen an die SP. Teilnehmende Kantone ohne IdM bauen ein IdM mit Unterstützung der Geschäftsstelle auf. Die Geschäftsstelle beschafft die für die zentralen Dienste notwendige Software, bzw. lässt sie entwickeln oder entwickelt sie selbst. Um das Zusammenwirken der technischen Systeme zu prüfen, stellt die Geschäftsstelle den IdP und SP eine Testplattform bereit. Teilnehmende Kantone mit bestehendem IdM realisieren mit Unterstützung des technischen Diensts der Föderation die technischen Schnittstellen zur Föderation. Die Geschäftsstelle verhandelt mit den gewünschten SP die Aufnahme in die Föderation und erarbeitet bzw. schliesst die notwendigen Verträge mit den SP ab. Die Geschäftsstelle definiert zusammen mit den Teilnehmenden das Modell der E-ID, um Aufbau und Inhalt der BildungsID festzulegen. Gemeinsam mit den Teilnehmenden legt die Geschäftsstelle die Prozesse für die organisationsübergreifenden Tätigkeiten fest. Die SP passen, mit Unterstützung des technischen Diensts, ihre Systeme an die technischen Standards der Föderation an. Zusammen mit teilnehmenden Kantonen und den SP nimmt die Geschäftsstelle den Betrieb der Föderation auf (vgl. [Kapitel 3.1](#)).

Vorteile	Nachteile
<ul style="list-style-type: none"> <li>+ Keine Personalspitzen für die Aufnahme von IdP</li> <li>+ Möglichkeit der engen Zusammenarbeit mit Kantonen, wenn die Anzahl der Teilnehmenden am Anfang kleiner ist, und damit bessere Bedürfnisorientierung</li> <li>+ Einbezug der Teilnehmenden ermöglicht einen stabilen und zufriedenstellenden Betrieb</li> </ul>	<ul style="list-style-type: none"> <li>- Hoher Marketingaufwand für die Akquisition von SP</li> <li>- Geringe Anzahl von SP bei Betriebsaufnahme könnte Nutzen schmälern</li> <li>- Umfangreiche Detailarbeiten verzögern die Betriebsaufnahme der Föderation FIDES</li> </ul>

### 4.3 Szenario B

#### Annahme

- Minimale Anzahl Kantone bestätigen Teilnahme
- Kleine Anzahl teilnehmender SP bekannt

#### Szenario

Die EDK vereinbart mit der Geschäftsstelle der Föderation FIDES einen Leistungsauftrag. Die Geschäftsstelle statuiert sich und entscheidet über die Organisation des technischen Diensts. Die Geschäftsstelle entwickelt die für die Teilnahme notwendigen Verträge und schliesst Verträge mit den teilnehmenden Kantonen ab. Teilnehmende Kantone ohne IdM bauen ein IdM mit Unterstützung der Geschäftsstelle auf. Die Geschäftsstelle beschafft die für die zentralen Dienste notwendige Software, bzw. lässt sie entwickeln oder entwickelt sie selbst. Um das Zusammenwirken der technischen Systeme zu prüfen, stellt die Geschäftsstelle den IdP und SP eine Testplattform bereit. Teilnehmende Kantone mit bestehendem IdM realisieren mit Unterstützung des technischen Diensts der Föderation die technischen Schnittstellen zur Föderation. Die Geschäftsstelle verhandelt mit den bekannten SP die Aufnahme in die Föderation und erarbeitet bzw. schliesst die notwendigen Verträge mit den SP ab. Die SP passen, mit Unterstützung des technischen Diensts, ihre Systeme an die technischen Standards der Föderation an. Zusammen mit den teilnehmenden Kantonen und den SP nimmt die Geschäftsstelle den Betrieb der Föderation auf.

Vorteile	Nachteile
<ul style="list-style-type: none"> <li>+ Keine Personalspitzen für die Aufnahme von IdP und SP</li> <li>+ Möglichkeit der engen Zusammenarbeit mit Kantonen, wenn die Anzahl der Teilnehmenden am Anfang kleiner ist, und damit bessere Bedürfnisorientierung</li> </ul>	<ul style="list-style-type: none"> <li>- Geringe Anzahl von SP bei Betriebsaufnahme könnte Nutzen schmälern</li> </ul>

## 4.4 Szenario C

### Annahme

- Alle Kantone bestätigen Teilnahme
- Grosse Zahl teilnehmender SP bekannt

### Szenario

Die EDK schliesst mit der Geschäftsstelle der Föderation FIDES einen Leistungsauftrag ab. Die Geschäftsstelle statuiert sich und entscheidet über die Organisation des technischen Diensts. Die Geschäftsstelle schliesst mit den teilnehmenden Kantonen Verträge ab. Teilnehmende Kantone ohne IdM bauen ein IdM mit Unterstützung der Geschäftsstelle auf. Die Geschäftsstelle beschafft die für die zentralen Dienste notwendige Software, bzw. lässt sie entwickeln oder entwickelt sie selbst. Um das Zusammenwirken der technischen Systeme zu prüfen, stellt die Geschäftsstelle den IdP und SP eine Testplattform bereit. Teilnehmende Kantone mit bestehendem IdM realisieren mit Unterstützung des technischen Diensts der Föderation die technischen Schnittstellen zur Föderation. Die Geschäftsstelle verhandelt mit den bekannten SP die Aufnahme in die Föderation und erarbeitet bzw. schliesst die notwendigen Verträge mit den SP ab. Die SP passen, mit Unterstützung des technischen Diensts, ihre Systeme an die technischen Standards der Föderation an. Zusammen mit den teilnehmenden Kantonen und den SP nimmt die Geschäftsstelle den Betrieb der Föderation auf.

Vorteile	Nachteile
+ Grosses Angebot von Online-Diensten ab Betriebsaufnahme	- Grosser Personalaufwand für die Aufbauphase - Hohe Komplexität bis und bei Betriebsaufnahme

## **ANHANG II: KONTEXT DER FÖDERATION FIDES**

---

1	Ökosystem E-ID in der Bildung.....	26
1.1	Projekt mit Berner Fachhochschule.....	26
1.2	Heterogene Ausgangslage – anhaltende Fragmentierung.....	26
1.3	Herausforderungen, kritische Erfolgsfaktoren .....	26
1.4	Nullszenario .....	27
2	Good Practice zu kantonalen BildungsID-Lösungen.....	28
2.1	Kanton Bern .....	28
2.2	Kanton Basel-Landschaft .....	28
2.3	Kanton Wallis .....	29
2.4	Kanton Neuenburg .....	29
2.5	Kanton Jura.....	30
3	Projekte und Good Practice zu Föderationen von Identitätsdiensten auf nationaler Ebene .....	31
3.1	SWITCHaai .....	31
3.2	SWITCH edu-ID .....	32
3.3	SuisseID.....	33
3.4	Swisscom Mobile ID.....	33
3.5	Identitätsverbund Schweiz (IDV) .....	33
3.6	Bundesamt für Polizei fedpol.....	34
4	Good Practice zu Föderationen von Identitätsdiensten im Bildungsbereich europäischer Länder .....	35
4.1	Dänemark: UNI-Login.....	35
4.2	Estland: HarID.....	35
4.3	Niederlande: Entree Federatie .....	36
4.4	Schweden: Skolfederation.....	36

# 1 ÖKOsystem E-ID IN DER BILDUNG

Das Projekt FIDES situiert sich – mit dem Vorhaben Identitätsdienste für den Bildungsraum Schweiz zu fördern – in einem komplexen Kontext, der sich durch das Zusammenspiel von unterschiedlichen Voraussetzungen, Akteuren, Funktionen und Nutzungen von digitalen Identitäten auszeichnet. Kenntnisse dieses Zusammenspiels sowie der ihm zugrundeliegenden Elemente sind für die konzeptionellen Überlegungen im Projekt FIDES, für die Führung der Anspruchsgruppen sowie für eine erfolgreiche Umsetzung der Förderung zentral.

## 1.1 Projekt mit Berner Fachhochschule

Das Zentrum Digital Society der Berner Fachhochschule (BFH) hat im Auftrag von educa.ch ein Modell des Ökosystem E-ID in der Bildung (ISCED 020-4) entworfen. Ausgangsbasis dafür sind seine Arbeiten für das SECO zu einer nationalen E-ID Schweiz<sup>3</sup>. Das Modell zeigt Zusammenhänge und Abhängigkeiten des Zusammenspiels von IAM-Lösungen im Bildungskontext auf und trägt zu einer einheitlichen Verwendung von Begrifflichkeiten und zur allgemeinen Verständlichkeit der Thematik bei. Mithilfe des Modells (als Diskussionsgrundlage) wurden umfassende Analysen in Form von Interviews und Workshops zum aktuellen Einsatz digitaler Identitäten im Schweizer Bildungswesen durchgeführt und Vorstellungen der einzelnen Akteure zum SOLL-Zustand im Hinblick auf eine Föderationslösung erhoben<sup>4</sup>. Damit wurden Grundlagen erarbeitet, um aus einer übergreifenden Perspektive Massnahmen zu ergreifen, die den Einsatz von E-ID in der Bildung zu nachhaltigem Erfolg führen.

## 1.2 Heterogene Ausgangslage – anhaltende Fragmentierung

Insgesamt zeigt sich bei den im Schweizer Bildungswesen eingesetzten IAM- und E-ID-Lösungen ein sehr heterogenes Bild, das je nach Kanton, Kontext (Schulbetrieb, Verwaltung) und/oder Schulstufe stark variieren kann. Es ist davon auszugehen, dass praktisch alle Schulen bzw. Schulgemeinden sowie kantonalen Bildungsverwaltungen heute eine oder mehrere elektronische Identifikationslösungen einsetzen. Dies primär für Lehrende und Personen aus der Bildungsverwaltung, in zunehmendem Masse aber auch zur Nutzung durch Lernende. Je nachdem welche Akteure und Elemente des Ökosystems bei den einzelnen Lösungen involviert sind (z. B. private Datenquellen vs öffentlich-rechtliche Register), differenzieren diese stark in Bezug auf die Qualität der Identitätsdaten, den Datenschutz sowie die Rechtssicherheit.

## 1.3 Herausforderungen, kritische Erfolgsfaktoren

Das Modell des Ökosystems E-ID in der Bildung macht deutlich, dass für effiziente, sichere und datenschutzkonforme E-ID- und IAM-Lösungen ein geregeltes Zusammenspiel der verschiedenen Akteure (Kantone, IdP, SP) notwendig ist. Dies erfordert eine aktive Kollaboration zwischen den einzelnen Parteien, die je unterschiedliche Bedürfnisse vertreten (je höher der kantonale Steuerungsanspruch, desto kritischer äussern sich beispielsweise die SP). Für den Aufbau und die Organisation einer gesamtschweizerischen Föderation werden vor allem die kantonalen Unterschiede in der Organisation des Bildungswesens (inkl. schulstufenspezifische Differenzen) als deutliche Herausforderung wahrgenommen. Flexibilität und Agilität der Lösung sind hier neben der generell zwingenden Vertrauenswürdigkeit gefragt. Da Mehrwert insbesondere über die Verfügbarkeit und Zugänglichkeit von externen Services und Inhaltsanbietern entsteht, wollen die Kantone eine Garantie, dass die für sie relevanten SP teilnehmen. Umgekehrt entsteht für die SP nur dann ein entscheidender Mehrwert, wenn möglichst alle Kantone partizipieren.

<sup>3</sup> Berner Fachhochschule (Hg.) (2015). *eID-Ökosystem Modell. Projektabschlussbericht*. [https://www.wirtschaft.bfh.ch/uplo-ads/tx\\_frppublikationen/eID-OEkosystem\\_V1\\_2.pdf](https://www.wirtschaft.bfh.ch/uplo-ads/tx_frppublikationen/eID-OEkosystem_V1_2.pdf)

<sup>4</sup> Die Berichte zu den einzelnen Arbeitspaketen des Projektes der Berner Fachhochschule werden ab Frühsommer 2017 auf der Informationsplattform von educa.ch zugänglich sein.

## 1.4 Nullszenario

Ein abschliessendes Nullszenario beleuchtet die Zukunftsperspektive, in der das von den Herausforderungen der Digitalisierung geforderte Bildungssystem ohne Föderationslösung auskommen muss. Das Fazit fällt hier klar aus: Ohne die Etablierung einer schweizweiten Föderation von Identitätsdiensten im Bildungswesen wird die Fragmentierung der E-ID-Landschaft eine effiziente, sichere und datenschutzkonforme Kollaboration zwischen Lehrenden, Lernenden, Schulverwaltung und weiteren Akteuren behindern. Nicht zu überzeugen vermögen auch die Alternativlösungen zur Föderation. So wäre z. B. denkbar, von einer nationalen E-ID-Lösung (vgl. Anhang II, *Projekte und Good Practice zu Föderationen von Identitätsdiensten auf nationaler Ebene*) abgeleitete Identitäten für den Bildungssektor zu kreieren. Da eine solche Lösung jedoch nicht die Eigenschafts- und Funktionsnachweise für das Bildungswesen liefern könnte, bleibt eine schweizweite Föderierung zusätzlicher Attribute weiterhin erforderlich. Eine zusätzliche Herausforderung stellt die Freiwilligkeit des Erwerbs einer solchen E-ID dar, die keinen flächendeckenden Einsatz gewährt.

## 2 GOOD PRACTICE ZU KANTONALEN BILDUNGSID-LÖSUNGEN

Das Projektteam FIDES hat zwischen Februar und März 2017 die Referenzpersonen der Kantone Bern, Basel-Landschaft, Wallis, Neuenburg und Jura getroffen. Ziel dieser Treffen war es, aktuelle Informationen über die kantonalen IdM Lösungen dieser Kantone zu erhalten. Die hier gesammelten Informationen geben jeweils einen Überblick zur kantonalen Situation im Bereich der digitalen Identität, den verwendeten Lösungen sowie der Bereitschaft des Kantons der Föderation FIDES beizutreten.

### 2.1 Kanton Bern

#### 2.1.1 Situation

Es existiert keine gesetzliche Grundlage, die auf kantonomer Ebene ein zentralisiertes IdM für Schulen der obligatorischen und nachobligatorischen Stufen legitimiert. Die meisten, insbesondere die grösseren durch den Kanton getragenen Institutionen der Sekundarstufe II verantworten jeweils ein eigenes IdM.

Das IdM auf der Volksschulstufe liegt in der Verantwortung der Gemeinden, wobei dieses nur teilweise zentralisiert erfolgt und viele Schulen eigene IdP unterhalten. Die IdM-Landschaft auf kommunaler Ebene gestaltet sich sehr heterogen und wenig standardisiert.

#### 2.1.2 Verwendete Lösung

Die Abteilung IT-Services der Erziehungsdirektion des Kantons Bern (ERZ-AZD-AID) bietet unter dem Produkt «EDUBERN» ein Portfolio mit bedarfsorientierten Dienstleistungen und Produkten für Schulen zur freiwilligen, kostenpflichtigen Nutzung an. Das Angebot basiert grösstenteils auf Technologien von Microsoft. Einige Institutionen, darunter vier Gymnasien sowie sechs Berufsfachschulen nutzen unter anderem das Angebot «Cloudomat», welches neben weiteren Diensten auch die Bereitstellung einer kantonalen BildungsID umfasst. Dadurch übt ERZ-AZD-AID im Auftrag dieser Schulen die Rolle eines IdP aus und betreibt das IdM auf der IT-Infrastruktur der ERZ.

Daten zur Erstellung von E-ID für Nutzende der Sekundarstufe II stammen überwiegend aus der Schulverwaltungslösung «Evento». In dieser, durch das Mittelschul- und Berufsbildungsamt (MBA) des Kantons Bern zentral betriebenen Lösung, werden sowohl Datensätze mit Informationen (Attribute) von Schulleitenden und Lehrpersonen (ca. 5'000) als auch von Lernenden (ca. 60'000) verwaltet.

ERZ-AZD-AID positioniert sich als Kompetenz-Center für IT-Services für das kantonale Bildungssystem. In einem Pilot-Projekt werden Dienstleistungen aus dem Portfolio «EDUBERN» auch Schulen der Volksschulstufe angeboten.

#### 2.1.3 Bereitschaft für die Föderation FIDES

Die Grundlagen für einen Beitritt zur Föderation von Identitätsdiensten sind vorhanden. Die realisierten Lösungen auf Sekundarstufe II sind für einen Beitritt geeignet. Eine kantonale Koordination der dezentralen Lösungen ist noch aufzubauen. Das Vorgehen für eine Lösung auf Sekundarstufe I und Volksschule ist zu diskutieren.

### 2.2 Kanton Basel-Landschaft

#### 2.2.1 Situation

Mit dem Abschluss der Einführung der Schuladministrationslösung SAL im August 2016 sind 14 Primarschulen sowie die Sekundarschulen und Gymnasien dem gleichen Informatiksystem angeschlossen. Dass gleich drei Schulstufen auf derselben IT-Lösung basieren und damit für diese Schulen ein zentral bereitgestelltes IdM für Lernende, Lehrpersonen, Schulleitungen, Schulsekretariate und weiteres Schulpersonal eingeführt werden konnte, ist eine Seltenheit auf kantonomer Ebene. Eine Voraussetzung für dessen Betrieb sind gesetzliche Grundlagen, die durch den Landrat verabschiedet wurden. Auch die kantonalen Berufsfachschulen sind – zwar mit einer anderen Administrationslösung – im zentral bereitgestellten IdM erfasst. Kommunal getragene Primarschulen verfügen daneben teilweise auch über ein separates IdM. Und auch die Kantonsbibliothek betreibt ein IdM in eigener Verantwortung.

### 2.2.2 Verwendete Lösung

Die zur Erstellung von E-ID notwendigen Informationen werden meist aus der Schulverwaltungslösung SAL bezogen. Das auf der kantonalen Infrastruktur betriebene Verzeichnis umfasst aktuell ungefähr 17'000 E-ID, rund 4'500 davon identifizieren Nutzende der Sekundarstufe II. Aktuell werden hauptsächlich die beiden Dienste SAL und Microsoft Office 365 Education genutzt. Getestet werden soll ein Zugang zudem auf Dienste wie z.B. n-oo.tv (Film- und Fernsehsendungen), Projekt Neptun (Beschaffung von Hardware) sowie die Verwaltung von Software auf mobilen Geräten. Der Zugang zu digitalen Ressourcen insbesondere der kantonalen Lehrmittelverlage ist ein weiteres zentrales Szenario, das in Zukunft zur Anwendung kommen soll.

### 2.2.3 Bereitschaft für die Föderation FIDES

Mit dem auf drei Schulstufen übergreifenden, zentral verwalteten IdM hat der Kanton Basel-Landschaft eine bemerkenswerte Lösung etabliert. Aus organisatorischer und technischer Sicht sind die Voraussetzungen für einen Beitritt zur Föderation FIDES vorhanden.

## 2.3 Kanton Wallis

### 2.3.1 Situation

Der Kanton Wallis bietet seinen Schuleinrichtungen verschiedene Online-Dienste an (Moodle, educanet<sup>2</sup>, Microsoft Office 365, Multimediaplattform, Verwaltungsprogramm etc.). Diese digitalen Dienste werden vom Kompetenzzentrum ICT-VS beaufsichtigt, das dem Departement für Volkswirtschaft und Bildung (DVB) unterstellt ist. Die kantonalen Schulen (Sekundarstufe II) verfügen über eine zentralisierte Struktur mit einheitlichem Zugriff zu den meisten offerierten Diensten. Für die Schulen der obligatorischen Stufen (Primar, Sekundarstufe I) liegt die Bewirtschaftung der Infrastruktur für die Nutzung von Online-Diensten bei den Gemeinden.

### 2.3.2 Verwendete Lösung

Um den Zugriff zum kantonalen (und interkantonalen) schulischen Informationssystem zu fördern, sieht das ICT-VS eine zentralisierte Lösung für die Identitäts- und Zugriffsverwaltung (IAM) vor. Mittels «einmaliger kantonalen Identifizierung» (Single Sign-on, SSO) soll allen Lehrpersonen, Lernenden sowie zeitweise auch den Eltern der Online-Zugriff auf sämtliche Dienste gewährt werden, zu deren Nutzung sie berechtigt sind.

Die Kreation der E-ID basiert auf zwei verschiedenen kantonalen Referenzdatensätzen (Escada, ISM), in denen alle schulischen Attribute für folgende Stufen enthalten sind: Primar, Sek I und Sek II (allgemein- und berufsbildende Schulen). Letztlich wird auch das Einwohnerregister als Referenzdatensammlung dienen.

Die kantonale IAM-Lösung für den Bildungsbereich («IAM pédagogique») befindet sich aktuell in der Testphase. Erklärtes Ziel des Bildungsdepartementes ist es, den kantonalen Schulen zu Beginn des Schuljahres 2018 ein eigentliches «digitales Arbeitsumfeld» anzubieten.

### 2.3.3 Bereitschaft für die Föderation FIDES

Bei der Konzeption des Walliser IAM-Projekts wurde die Föderation FIDES mitberücksichtigt. Die verwendeten Technologien (insbesondere SAML) sind kompatibel mit der Föderation. Das Modell der E-ID und die verwendeten Standards können sich an jene der Föderation anpassen. Sobald das Bildungsdepartement sein Bildungs-IAM («IAM pédagogique») in Betrieb genommen hat, ist der Kanton Wallis für seinen Beitritt zur Föderation bereit.

## 2.4 Kanton Neuenburg

### 2.4.1 Situation

Ein kantonales IdM-Projekt fusst im Kanton Neuenburg auf verschiedenen vorbestehenden Strukturen, wie z. B. dem 1999 in Betrieb genommenen *Réseau Pédagogique Neuchâtelois (RPN)*, dem die Neuenburger Schulen angehören. Das Netzwerk bildet für sämtliche kantonalen obligatorischen und nachobligatorischen Schulstufen das Fundament im Bereich Telekommunikation. Eine weitere Errungenschaft ist das kantonale Projekt ICT 01-04,

das seit 2001 die schrittweise Informatisierung aller Schulen sowie eine öffentlich-rechtliche Förderung der Nutzung von Medien, Bildern, Informations- und Kommunikationstechnologie (MITIC) an den kantonalen Schulen vorsieht. Die Bemühungen konzentrieren sich auf die technische Infrastruktur, die Schulung der Nutzenden und die Harmonisierung gewisser verwaltungstechnischer Abläufe. Als dritte bereits implementierte Voraussetzung sei das Informatiksystems CLOEE genannt. In diesem werden die Masterdaten der Lernenden sowie der Lehrpersonen des Kantons verwaltet (für die obligatorische und nachobligatorische (Berufs- und Mittelschule) Stufe sowie den Bereich Sonderpädagogik).

#### **2.4.2 Verwendete Lösung**

Mit CLOEE verfügt der Kanton bereits über ein System, das Personendaten zentralisiert verwaltet, und damit über eine RPN-spezifische IdM-Lösung. Die RPN-Logins können beispielsweise bereits für den Zugriff auf die Plattform des *Plan d'études Romand PER* (Lehrplan der französischen Schweiz) verwendet werden.

#### **2.4.3 Bereitschaft für die Föderation FIDES**

Aktuell besteht keinerlei Hindernis in Bezug auf einen Beitritt des Kantons Neuenburg zu einer künftigen Föderation von Identitätsdiensten. Sobald der Entscheid zum Beitritt vom Departement für Bildung und Familie (DEF) gefällt ist, übernimmt das Amt für Schulinformatik und -organisation den Anschluss des kantonalen IdM an die Föderation FIDES, da es für das RPN der obligatorischen Schulstufen zuständig ist. Das kantonale IdM baut auf bestehenden RPN-Strukturen und den in CLOEE gespeicherten Daten auf.

## **2.5 Kanton Jura**

### **2.5.1 Situation**

Im Kanton Jura steht bisher noch keine zentralisierte SSO-Lösung für den Zugriff auf Online-Dienste bereit. Die kantonale Einführung eines zentralisierten IdM wird von einem anonymisierten Export der gemeinsam mit dem Kanton Neuenburg betriebenen Datenbank CLOEE abhängen. Das Projekt muss noch vom Bildungsdepartement bewilligt werden. Bis jetzt schliessen die einzelnen Bildungseinrichtungen mit den Online-Diensteanbietern direkt – und teilweise ohne kantonale Koordination – bilateral Verträge ab.

### **2.5.2 Verwendete Lösung**

Die kantonale Bildungs-ID lässt sich anhand der in CLOEE enthaltenen Daten erstellen. Die Sicherheitsdatenbank CLOEE enthält sämtliche schulbezogenen Daten der Primar- und Sekundarstufen für Lehrpersonen und Lernende (Schülerdatei). Durch den täglichen Export der Datenbank lassen sich Erstellung und Unterhalt der E-ID für den Zugang zu Online-Diensten sicherstellen.

### **2.5.3 Bereitschaft für die Föderation FIDES**

Der Kanton Jura kann der Föderation FIDES erst nach der Genehmigung des kantonalen IdM-Projektes durch die kantonalen Behörden beitreten.

### 3 PROJEKTE UND GOOD PRACTICE ZU FÖDERATIONEN VON IDENTITÄTS-DIENSTEN AUF NATIONALER EBENE

Neben dem Projekt der Föderation FIDES bestehen in der Schweiz noch weitere Beispiele und Initiativen im Bereich IdM. Die konzeptuelle Reflexion zum Projekt FIDES und die Wahl der entsprechenden Technologie basieren und basieren auf diesen Beispielen. Stark beeinflusst wurde das Projekt auch von der bereits für die Tertiärstufe bestehenden Föderation von Identitätsdiensten SWITCHaai. Weitere Anwendungsbeispiele bereits bestehender oder in Entwicklung befindlicher Identitätsdienst-Föderationen oder Single-Sign-on-Dienste wurden eingangs dargestellt. Es ist wichtig, den Entwicklungen anderer Projekte und Initiativen zu folgen, um die Systemkompatibilität und die verwendeten Technologien der Föderation zu gewährleisten. Das soll letztendlich erlauben die Föderation weiterzuentwickeln. Die Systemkompatibilität erlaubt den Zugriff mit externen Zugangsdaten auf die Online-Dienste der Föderation.

#### 3.1 SWITCHaai

##### 3.1.1 Eine Föderation von Identitätsdiensten

Die SWITCHaai ist eine Föderation von Identitätsdiensten für den tertiären Bildungs- und Forschungssektor in der Schweiz und in Liechtenstein. Ursprünglich sollte damit eine Infrastruktur bereitgestellt werden, die einen gegenseitigen Zugriff zu den Webservices der Hochschuleinrichtungen bietet. Inzwischen blickt die Föderation SWITCHaai auf einen zehnjährigen erfolgreichen Betrieb zurück.

##### 3.1.2 Teilnehmende

Teilnehmende der Föderation sind die «Föderationsmitglieder» und die «Föderationspartner». Die Föderationsmitglieder (Home Organizations) gehören der SWITCH-Community als Anbieter digitaler Identitäten (IdP) für ihre Endbenutzenden an. Sie können auch Online-Dienste (SP) anbieten. Die Mitgliedschaft ist den Hochschul- und Forschungseinrichtungen der Schweiz und Liechtensteins vorbehalten.

Die folgenden Organisationen sind SWITCH-Mitglieder: kantonale Universitäten, technische Hochschulen, ETH-Forschungsanstalten, pädagogische Hochschulen, Fachhochschulen sowie das Eidgenössische Hochschulinstitut für Berufsbildung EHB.

Die Föderationspartner bieten mindestens einem Föderationsmitglied einen oder mehrere Online-Dienste (SP wie E-Learningplattform, E-Mail etc.) an (Patenschaftsprinzip). Föderationspartner sind jedoch in der Regel nicht ermächtigt, innerhalb der Föderation eine Identitätsverwaltung (IdP) anzubieten. Als Partner kommen auch Anbieter aus dem Ausland in Frage.

##### 3.1.3 Dienste

Das Basisangebot der Föderation SWITCHaai umfasst die von SWITCH bereitgestellte Authentifizierungs- und Autorisierungsinfrastruktur. Die technische Architektur umfasst ein zentrales Metadatenverzeichnis, in dem die Föderationsmitglieder und -partner beschrieben sind.

Die Hochschulen erfassen und erstellen die E-ID für ihre Studierenden, Lehrpersonen und Angestellten anlässlich ihrer Anmeldung oder Anstellung im Hochschulbereich selber. Mittels SSO-Login erhalten die Endbenutzenden so z. B. Zugriff auf E-Learning-Plattformen oder WLAN mehrerer Hochschulen.

Der Föderation sind über 1'000 Dienste angeschlossen.

##### 3.1.4 Technische Architektur

Die technische Architektur von SWITCHaai verwendet die Open-Source-Technologie Shibboleth zur Verwaltung digitaler Identitäten innerhalb einer Föderation und basiert auf dem Open-Source-Standard SAML (Security Assertion Markup Language).

Die SWITCHHAI-Technologie ist mit jener der Föderation FIDES kompatibel. Diese verwendet die gleichen Technologien und Standards. Die Kompatibilität zwischen der Föderation und SWITCHHAI sowie deren Nachfolger Switche du-ID ist von grosser Bedeutung, denn sie wird den nahtlosen Übergang von der Sekundär- zur Tertiärstufe mit der gleichen BildungsID ermöglichen, d. h. die Endbenutzenden behalten ihre bildungsrelevante E-ID während ihrer gesamten lebenslangen Bildungskarriere.

Die technische Architektur der Föderationen SWITCHHAI und FIDES erlaubt eine interföderative Verbindung mit anderen AAI-Föderationen, beispielsweise über eduGAIN, eine weltumspannende interföderative Vereinigung im Bildungs- und Forschungsbereich.

### 3.1.5 Verwaltung der Föderation

SWITCH ist für die Bereitstellung der zentralen Infrastruktur der Föderation sowie für die Wahrung des Vertrauensraumes zwischen Föderationsmitgliedern und Föderationspartnern zuständig. Letztere unterzeichnen vor dem Beitritt zur Föderation einen Servicevertrag (Service Agreement). Der zwischen SWITCH und den Mitgliedern oder Partnern abgeschlossene Vertrag verpflichtet diese zur Einhaltung gewisser Obliegenheiten und der Datenschutzbestimmungen.

Die Koordination von SWITCHHAI wird von zwei Ausschüssen unterstützt: SWITCH berät sich mit dem *AAI Advisory Committee* und dem *AAI Community Group* über die langfristige Entwicklung und die Optimierung verwaltungstechnischer und technischer Belange. Das *AAI Advisory Committee* setzt sich aus SWITCH sowie Vertretenden der Föderationsmitglieder (IdP) und Vertretenden der verschiedenen Servicegruppen zusammen. Die *AAI Community Group* setzt sich aus den Repräsentanten sämtlicher Organisationen der SWITCH-Community zusammen, die auch Föderationsmitglieder sind.

### 3.1.6 Finanzierung

Die Föderationsmitglieder leisten einen Mitgliederbeitrag an SWITCH für den von SWITCH finanzierten Betrieb der Föderation.

## 3.2 SWITCH edu-ID

### 3.2.1 Eine Föderation von Identitäten

SWITCH edu-ID ist die Nachfolgeorganisation von SWITCHHAI und wird diese in naher Zukunft ablösen. Im Gegensatz zu SWITCHHAI, bei der Identitätsdienste in einer Föderation zusammengefasst sind, soll SWITCH edu-ID eine Föderation digitaler ID mit einem einzigen Identitätsdiensteanbieter (IdP) sein. Die Migration zu SWITCH edu-ID sollte voraussichtlich bis 2020 abgeschlossen sein. Bis dahin sollten alle Organisationen von SWITCHHAI nach SWITCH edu-ID gewechselt haben. Zu diesem Zweck müssen sie ein individuelles Migrationsprojekt erarbeiten und in Kooperation mit SWITCH umsetzen.

Auch in diesem Modell werden die Attribute mit den innerorganisatorischen Rollen wie bei SWITCHHAI von den Hochschulen verwaltet. Neu ist aber bei SWITCH edu-ID, dass die Endbenutzenden ihre ID selber erstellen müssen.

### 3.2.2 Transfer der Endbenutzenden

Der zentralisierte Identitätsanbieter wird den bisherigen SWITCHHAI-Usern und zusätzlich allen an einer Nutzung von SWITCH edu-ID interessierten neuen Endbenutzenden bereitgestellt. Mit der Zeit sollen alle bisherigen SWITCHHAI-User zum Wechsel ins neue IdM-System SWITCH edu-ID aufgefordert werden.

### 3.2.3 Dienste

Bei den Diensten sind keine Änderungen vorgesehen. SWITCH edu-ID ermöglicht jedoch weiterführende Funktionen, von denen auch die Dienste profitieren, was gewisse Anpassungen erfordern wird.

### 3.2.4 Verwaltung der Föderation

Der Wechsel zu SWITCH edu-ID wird direkt innerhalb von SWITCHHAI vollzogen.

### 3.2.5 Finanzierung

Die Finanzierung von SWITCH edu-ID bleibt sich gleich wie bei SWITCHaai.

## 3.3 SuisselD

### 3.3.1 Elektronische Signatur

Die SuisselD ist auf der Grundlage des Bundesgesetzes über die elektronische Signatur ZertES (2003) entstanden, das 2016 revidiert und am 1. Januar 2017 in Kraft getreten ist. Aufgrund des ZertES wurde das Obligationenrecht durch einen neuen Abschnitt ergänzt (Art. 14, Abs. 2bis OR), demzufolge Verträge, für welche die Schriftform vorgesehen ist, nun auch elektronisch abgeschlossen werden können.

Die SuisselD wurde 2010 offiziell vom Bund eingeführt und zur Förderung elektronischer Transaktionen sowie zur allgemeinen Unterstützung der Schweizer Wirtschaft, insbesondere der digitalen Wirtschaft, vom Staatssekretariat für Wirtschaft SECO implementiert. Mit der SuisselD können offizielle Dokumente wie Verträge rechtsgültig elektronisch unterschrieben werden.

Der Dienst wird Anbietern angeboten, die vom Gesetz anerkannt werden:

- QuoVadis Trustlink Schweiz AG
- Die Schweizerische Post/SwissSign AG
- Swisscom (Schweiz) AG
- Bundesamt für Informatik und Telekommunikation BIT

Der Preis für Privatanwender variiert zwischen 147 und 195 Franken für drei Jahre (Die Post; SuisselD Signing Service/QuoVadis). Der Dienst beruht auf einer Authentifizierung mittels USB-Stick oder Chipkarte.

Die SuisselD kann auch für die Nutzung von Online-Diensten eingesetzt werden und könnte somit im Rahmen der Föderation FIDES Verwendung finden.

## 3.4 Swisscom Mobile ID

Mobile ID wird als digitale ID auf der SIM-Karte des mobilen Endgerätes (Smartphone oder andere) gespeichert. Der Dienst wird von Swisscom entwickelt und ist für alle Mobilfunkkunden von Swisscom kostenlos. Mobile ID wird aktuell auch von Sunrise und M-Budget angeboten, demnächst auch von Salt. Mit Mobile ID lässt es sich bei unterstützten Diensten sicher einloggen. Der Dienst ist auch im Ausland verfügbar, sofern SMS-Roaming aktiviert ist. Der Einsatz im Ausland ist ebenfalls kostenlos.

Obwohl Erstellung und Verwendung von Mobile ID kostenlos ist, können manche Anbieter für die Nutzung ihrer Dienste Gebühren erheben. Mobile ID lässt sich auch für das Login bei Online-Diensten verwenden und könnte somit für die Föderation FIDES zur Anwendung kommen.

## 3.5 Identitätsverbund Schweiz (IDV)

### 3.5.1 E-ID und E-Government

Es handelt sich um ein strategisches Gemeinschaftsprojekt von Staatssekretariat für Wirtschaft SECO und E-Government Schweiz. Die Cyber-Administrationsstrategie wird gemeinsam von Bund, Kantonen und Gemeinden getragen, um der Schweizer Bevölkerung einen vollständig elektronischen Zugang zu Verwaltungsdienstleistungen effizient und transparent zu ermöglichen.

Das Projekt «Identitätsverbund Schweiz» soll die erforderlichen Massnahmen und die notwendige Infrastruktur schaffen, damit Schweizerinnen und Schweizer durch den Verbund von Identitätssystemen die verschiedensten Dienste durch den gleichen Authentifizierungsvorgang nutzen können.

Das Projekt sieht für das letzte Quartal 2017 eine Pilotphase vor und sollte im ersten Quartal 2019 finalisiert werden.

### 3.5.2 Dienste

Lokales E-Government, E-Voting, elektronische Steuererklärung sowie die Nutzung weiterer Dienste sind möglich, da die Föderation auf einem erweiterbaren System beruht. Die Föderation FIDES könnte also insgesamt von diesem Projekt profitieren. Die Identitäten der Föderation FIDES könnten die an IDV-Schweiz angeschlossenen Dienste verwenden.

## 3.6 Bundesamt für Polizei fedpol

Der Bundesrat hat das Eidgenössische Justiz- und Polizeidepartement (EJDP) mit der Ausarbeitung eines Konzepts sowie der gesetzlichen Grundlagen für ein künftiges elektronisches Identifizierungsmittel (E-ID) zusammen mit der neuen Identitätskarte beauftragt. Auf dieser Grundlage hat das Bundesamt für Polizei (fedpol) zwischen Mai und Juni 2015 eine informelle Konsultation zum «Konzept für schweizerische staatlich anerkannte E-ID-Systeme» lanciert. Als Folge dieser Konsultation wurde das Konzept revidiert, und es wurde der Weg für die Vorarbeiten zum E-ID-Gesetz geebnet. Am 22. Februar 2017 eröffnete der Bundesrat die Vernehmlassung zu einem Bundesgesetz über anerkannte elektronische Identifizierungseinheiten (E-ID-Gesetz).

### 3.6.1 Das Fedpol-Konzept

Das Fedpol-Konzept «anerkannte elektronische Identifizierungseinheiten (E-ID)» sieht vor, dass der Bund keine eigene E-ID herausgibt, sondern vielmehr geeignete E-ID-Systeme des Marktes staatlich anerkennen und beaufsichtigen kann. Dazu schafft der Bund neu die Anerkennungsstelle für Identitätsdienstleister (AID).

Ausserdem tritt der Bund als vertrauenswürdige Verwaltungsstelle der Identitätsattribute (Attribute Repository) von Inhaberinnen und Inhabern einer staatlich anerkannten E-ID auf, indem er vorhandene Personenidentifizierungsdaten elektronisch übermittelt. Für diese zweite Aufgabe wird die neue Schweizerische Stelle für elektronische Identität (SID) beim Bund geschaffen.

### 3.6.2 Das E-ID-Gesetz

Das Bundesgesetz über anerkannte elektronische Identifizierungseinheiten (E-ID-Gesetz) soll die gesetzlichen Rahmenbedingungen zum anerkannten elektronischen Identifizierungsmittel (E-ID) schaffen und dessen Rechtssicherheit gewährleisten. Es regelt die Voraussetzungen für die anerkannten elektronischen Identifizierungsmittel, die Anerkennung und Beaufsichtigung der Anbieter von Identitätsdiensten (IdP), die Rechte und Pflichten der Inhaberinnen und Inhaber einer E-ID sowie der Anbieter von Online-Diensten (SP). Ausserdem soll das Bundesgesetz einen sicheren elektronischen Geschäftsverkehr fördern und die Standardisierung und Interoperabilität der E-ID sicherstellen.

## 4 GOOD PRACTICE ZU FÖDERATIONEN VON IDENTITÄTSDIENSTEN IM BILDUNGSBEREICH EUROPÄISCHER LÄNDER

In Europa bestehen bereits anderweitig Identitätsdienstföderationen für den Bildungsbereich. Das Projektteam FIDES hat sich bei einigen Ländern nach deren bisherigen Erfahrungen erkundigt und sich mit den Ländervertretern über das Schweizer Konzept einer Föderation von Identitätsdiensten ausgetauscht.

Nachfolgend werden einige dieser Modelle vorgestellt, und es wird erläutert, weshalb sie aus konzeptioneller, organisatorischer, technischer oder betrieblicher Sicht für das Schweizer Projekt interessant sind. Die gesammelten Daten und Erkenntnisse stammen aus einer am 2. Juni 2016 in Partnerschaft mit SwissCore und European Schoolnet in Brüssel durchgeführten Konferenz, an der fünf nationale Identitätsdienstprojekte für den Bildungsbereich vorgestellt wurden. Die fünf vorgestellten Projekte stammen aus Dänemark, Estland, Frankreich, den Niederlanden und der Schweiz. Drei davon werden nachfolgend erörtert.

Ebenfalls vorgestellt wird die Schwedische Föderation «Skolfederation», deren Vertreter zwar an der Konferenz teilgenommen, ihr Modell jedoch nicht präsentiert haben. Das Modell erscheint wegen der Ähnlichkeit mit dem Rahmenkonzept FIDES erwähnenswert.

### 4.1 Dänemark: UNI-Login

Status: aktiv

Das vom dänischen Bildungsdepartement betriebene System UNI-Login ist ein gelungenes Beispiel dafür, wie Lernende Online-Dienste durch ein einmaliges Login (SSO) nutzen können. Der Dienst wurde vor 20 Jahren lanciert und hat sich stetig weiterentwickelt. Heute werden täglich 350'000 Logins zu verschiedensten Diensten wie Online-Ressourcen, Schulintranet, Cloudservices oder WLAN registriert. Eine neue Initiative «User Portal» soll das Modell UNI-Login auf eine für Online-Dienste für den Bildungsbereich standardisierte Zugriffsverwaltung erweitern.

Das Projekt UNI-Login und seine Fortsetzung „User Portal“ ist ein für das Projekt FIDES relevantes Beispiel, denn:

- Es handelt sich um eine Föderation, die mit wenigen IdP und SP gestartet und sukzessive erweitert wurde, im Gegensatz zu einem grossangelegten Start mit zahlreichen Teilnehmenden.
- Die Verbindungsstatistiken zeigen auf, welche Bedeutung der technischen Systemflexibilität zukommt, damit angemessen auf die Entwicklung von Nachfrage und Infrastruktur eingegangen werden kann.

### 4.2 Estland: HarID

Status: Projekt (Testphase)

Die Föderation «HarID» ist ein Estnisches Projekt im Hinblick auf die Bereitstellung einer digitalen Identität für Lehrpersonen und Lernende/Studierende ab 15 Jahren. Der Dienst bietet via SSO-Login Zugriff auf verschiedene Online-Dienste innerhalb einer Estnischen Bildungsinformatik-Cloud (Educloud). Für die Authentifizierung können die Lernenden sowie die Angehörigen des Lehrkörpers ihre nationale Identitätskarte, ihr Handy oder einen anderen anerkannten Identitätsdienst verwenden. Die Estnische Gesellschaft ist im Bereich der Digitalisierung von Verwaltungsdienstleistungen (z. B. E-Government) sehr fortschrittlich. Die Personendaten, auf deren Basis die digitalen Identitäten für Lehrpersonen und Lernende erstellt werden (HarID) sind in bereits bestehenden nationalen Datenbanken gespeichert (Einwohnermelderegister und nationales Bildungsinformationssystem).

Das Projekt HarID ist aus folgenden Gründen interessant:

- Vorbestehende Datenbanken werden für die Erstellung der E-ID verwendet. Der Trend kann bereits bei mehreren kantonalen IdM-Projekten in der Schweiz beobachtet werden.
- Es wird auf der Basis der Föderation von Identitätsdiensten eine Bildungscloud bereitgestellt.

### 4.3 Niederlande: Entree Federatie

Status: aktiv

Die niederländische Föderation von Identitätsdiensten für den Schulbereich «Entree Federatie» wird von «Kennisnet» betrieben, der öffentlich-rechtlichen ICT- und Bildungsorganisation, die vom Ministerium für Bildung, Kultur und Wissenschaften finanziert wird. Im aktuellen Modell «Entree Federatie» können die Bildungsorganisationen ihren Beitritt zur Föderation beantragen und ihren IdP selber wählen. Zur Auswahl stehen vier IdPs, d. h. zwei private und zwei öffentlich-rechtliche. Die Online-Dienstleister unterzeichnen eine Dienstleistungsvereinbarung (Service Level Agreement), um an der Föderation teilnehmen zu können. Die Bildungsorganisationen prüfen, welche Attribute mit den SP ausgetauscht werden. 2017 wird ein neues System in Betrieb genommen, unter welchem die Lernenden ihren IdP selber wählen können. Die Authentifizierung erfolgt über eine anonymisierte Pseudo-ID.

Das Projekt «Entree Federatie» ist aus folgenden Gründen interessant:

- Kooperation zwischen privatem und öffentlichem Sektor bei den Identitätsdienstleistern
- Ein Dashboard für die Schulen für die Feinabstimmung der Attribute, die von den Endbenutzenden mit den Online-Dienstleistern austauscht werden
- Anonymisierung der E-ID via Pseudo-ID; diesen Dienst möchte auch die Föderation FIDES optional anbieten (UUIIDgen)
- Die Verwaltungs- und Entwicklungskosten der niederländischen Föderation bieten sich als Vergleichsrahmen für die Kostenschätzung in der Schweiz an.

### 4.4 Schweden: Skolfederation

Status: aktiv

In Schweden bietet die Föderation «Skolfederation» ein SSO-Login für Lernende und Lehrpersonen im Bildungsbereich an. Die Gemeinden, die mit der Schulorganisation ihrer Bezirke beauftragt sind, sowie die freien Schulen kooperieren mit den Dienstleistern innerhalb der Föderation. Die Dienstleistungsanbieter müssen eine Patenschaft mit einer Gemeinde oder einer freien Schule unterhalten, um in die Föderation aufgenommen zu werden. Die Verwaltung der Föderation wird von der unabhängigen Organisation IIS (Internetföderation Schweden) wahrgenommen.

Das Projekt «Skolfederation» ist aus folgenden Gründen interessant:

- Die Dienstleister müssen eine Patenschaft ausweisen, um der Föderation beitreten zu können.
- Die Verträge, welche die Dienstleister mit den Gemeinden und/oder freien Schulen als Voraussetzung für den Beitritt abschliessen, bilden eine solide Grundlage für die Einrichtung eines Vertrauensraums.