Ökosystem E-ID in der Bildung

Teilbericht 1: Angepasstes E-ID-Ökosystem Modell für das Bildungswesen Schweiz

Ein Bericht der Berner Fachhochschule
Haute école spécialisée bernoise

Impressum

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

Autoren	Jérôme Brugger (BFH) Thomas Selzam (BFH) Nelly Buchser (educa.ch)
Titelbild	Maksim Kabakou/Shutterstock.com

Juni 2017

Inhaltsverzeichnis Teilbericht 1

1 Ausgangslage und Ziel

In diesem Teilbericht ist das Vorgehen und das Resultat der Anpassungen des Ökosystem-Modells geschildert, das die BFH für den Kontext der nationalen E-ID in der Schweiz entwickelt hat[1]. Ziel dieses Arbeitspaketes war es, dieses Instrument für die Anwendung im Kontext des Bildungswesens nutzbar zu machen. Mit dem angepassten Instrument konnten die weiteren Projektarbeiten auf der Grundlage eines Modells erfolgen, das für die am Akteure des Bildungssystems verständlich und vollständig ist. Die im Modell verwendeten Anwendungsfälle, die Rückmeldungen zum Modell in den Interviews mit Stakeholdern zur *IST-Situation* sowie Überlegungen zum *Nullszenario* werden in den weiteren Teilberichten dargestellt.

2 Vorgehen

Für die Arbeiten wurden in einem ersten Schritt die von educa.ch im Rahmen des Projektes FIDES[2] erarbeiteten Grundlagen ausgeblendet, um eine umfassende Sicht auf das Ökosystem E-ID in der Bildung zu erhalten. Für die Arbeit mit dem Modell wurde der generische Terminus einer BildungsID verwendet. Als Grundlage für die Anpassung des Modells dienten die erarbeiteten Anwendungsfälle, die in einem separaten Bericht dargestellt werden.

2.1 Workshop E-ID-Ökosystem-Modell

Der Workshop zum E-ID-Ökosystem-Modell fand am 26.10.2016 an der BFH statt. Teilgenommen haben Karl Wimmer, Simon Graber, Michael Deichmann, Nelly Buchser und Paul Gerhard von Seiten educa.ch. Thomas Selzam und Jérôme Brugger haben den Workshop moderiert. Die Zielsetzung des Workshops bestand darin, alle am Workshop Beteiligten mit dem Modell vertraut zu machen und Umsetzungsvarianten einer BildungsID in drei Instanziierungen des Modells abzubilden. Im Nachgang zum Workshop wurde zusätzlich eine vereinfachte Instanziierung der Variante 3 erarbeitet, die der Diskussion in den Interviews diente.

Nach Klärung der Fragen zu den Details des E-ID-Ökosystem-Modells wurden folgende kleinere Anpassungen des Modells auf die spezifischen Anforderungen des Bildungssektors vorgenommen:

- BildungsID: Im Zentrum steht nun eine „BildungsID“, nicht wie in der ursprünglichen Version des Modells eine nationale E-ID.
- Staatsverträge: Im Kontext BildungsID haben Staatsverträge ggf. einen Einfluss, allerdings nicht mit Bezug zur entsprechenden EU-Verordnung zu elektronischen Identitäten (eIDAS). Der Verweis auf diese Infrastrukturkomponente wurde entfernt.
- Anwendungsfälle: Die generischen Anwendungsfälle aus dem Modell für eine nationale E-ID wurden durch spezifische Anwendungsfälle im Bildungsbereich ersetzt. educa.ch hat die Grundlagen dazu in einem Workshop erarbeitet. (vgl. Teilbericht 1 Nutzende, Anwendungsfälle und Anwendungsszenarien)
- Als Element der technischen Infrastruktur wurde „Interföderation“ im Sinne einer vorhandenen Schnittstelle zu anderen Föderationen hinzugefügt.

2.2 Das BildungsID-Ökosystem-Modell

Das BildungsID-Ökosystem in einer vereinfachten Darstellung (vgl. Abbildung 1) stellt auf der linken Seite die Nutzenden und die Anwendungsfälle für eine BildungsID dar. Aus diesen Anwendungsfällen ergeben sich einzelne Nutzungen im Sinne von Aktionen, die mithilfe der BildungsID vorgenommen werden.

[1] https://www.wirtschaft.bfh.ch/uploads/tx_frppublikationen/eID-OEkosystem_V1_2.pdf
[2] EDK: Tätigkeitsprogramm 2015–2019, Fortschreibung 2016, S. 8: http://www.edudoc.ch/static/web/edk/tgpro_d.pdf

Auf der rechten Seite des Modells ist die Bereitstellung der BildungsID abgebildet. In der Mitte sind die einzelnen Funktionen einer elektronischen Identität aufgeführt. Darüber stehen die Vertrauensdienste als konzeptioneller Rahmen für den Dienst, unterhalb die technische Infrastruktur, die für die Erbringung notwendig ist. Rahmenbedingungen in organisatorischer und rechtlicher Hinsicht bilden den Rahmen für die Bereitstellung. Um die Nutzung und die Bereitstellung herum ist der politische Rahmen dargestellt, der die Rahmenbedingungen für das gesamte Ökosystem definiert.
Die Leserichtung dieser Darstellung ist von links nach rechts, die Pfeile von rechts nach links stellen die Richtung des Informationsflusses bei der Nutzung dar.

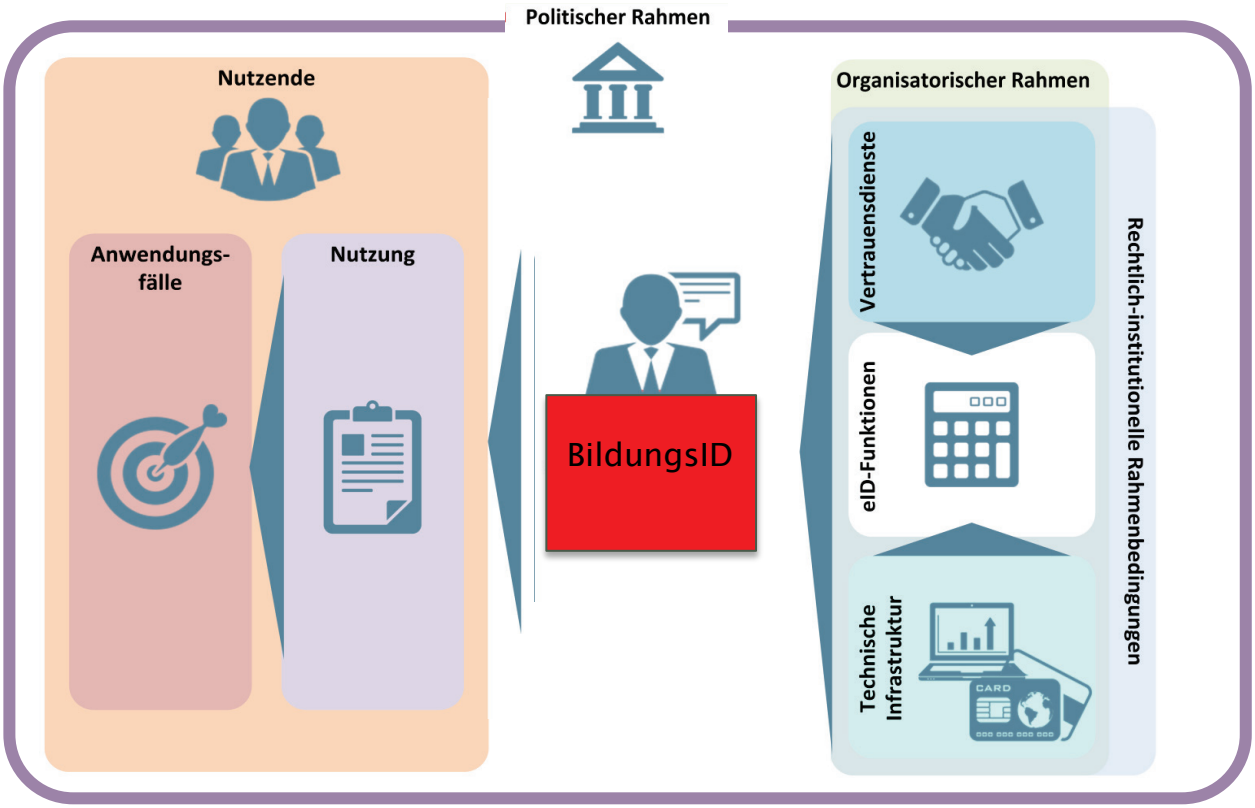

Abbildung 1 – Übersicht BildungsID-Ökosystem-Modell

2.3 Instanziierungen des Ökosystem-Modells E-ID in der Bildung

Auf der Grundlage des angepassten Modells wurden anschliessend drei Instanziierungen erarbeitet. Instanziierungen sind spezifische Zustandsbeschreibungen des Modells in Bezug auf eine mögliche Realisierung eines Systems. Im Workshop wurden in zwei Gruppen eine minimale und maximale Ausprägung einer BildungsID erarbeitet und anschliessend gemeinsam validiert. Nach dem Workshop wurde eine Ausprägung erarbeitet, die dem FIDES-Konzept entspricht.
Der Methodik des Ökosystem-Modells folgend, wurden zunächst die Anwendungsfälle bestimmt, die in der jeweiligen Ausprägung ermöglicht werden sollen. Daraus folgend wurden die notwendigen Elemente der Nutzung definiert. Alle nicht benötigten Elemente werden in der Darstellung durchgestrichen dargestellt. Damit ist sichergestellt, dass die Bereitstellung ausgehend von den Nutzenden und vom zu erreichenden Nutzen konzipiert wird.
In einem zweiten Schritt wurde die Ausprägung der Bereitstellung diskutiert. Ausgehend von den entfallenden Nutzungen wurden nicht benötigte Elemente der Bereitstellung durchgestrichen. Weiter wurde die Frage nach der bereitstellenden Organisation für die einzelnen Elemente im System diskutiert. Es wurde davon ausgegangen, dass Kernelemente hoheitlich sprich von der öffentlichen Hand bereitgestellt werden müssen (gelb eingefärbt). Weitere Elemente können ergänzend und optional durch private Anbieter realisiert werden (in grün dargestellt). Hoheitlicher Betrieb muss nicht zwingend den operativen Betrieb durch den Staat bedeuten. Für die Umsetzung kann eine Firma oder Organisation beauftragt werden, aber Kontrolle und Finanzierung sind Aufgabe des Staates.
Das Zusammenspiel von öffentlicher Hand und privaten Anbietern erfordert, dass erstere sich aktiv darum bemüht und die Verantwortung übernimmt, dass alle gewünschten und notwendigen E-ID-Funktionen im Betrieb zur Verfügung stehen. Dies bedeutet, dass, falls die privaten Akteure für den Betrieb zwingend erforderliche Elemente nicht realisieren, die öffentliche Hand einspringen muss, um den angedachten Funktionsumfangs einer BildungsID sicherzustellen.

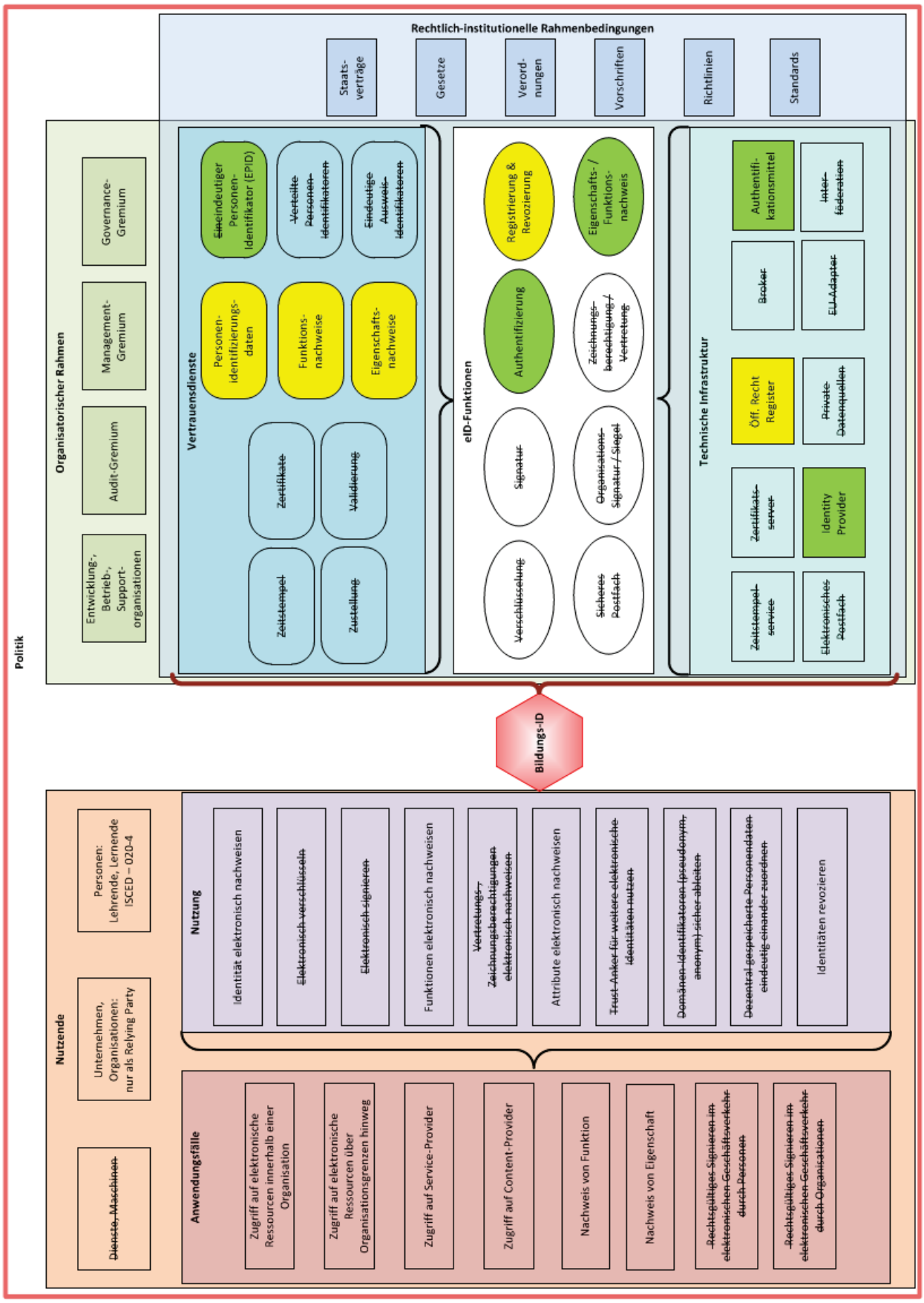

Abbildung 2: BildungsID in minimaler Ausprägung (gelbe Elemente: von der öffentlichen Hand bereitgestellt, grüne Elemente: durch private Anbieter bereitgestellt)

2.3.1 Instanziierung 1: BildungsID in minimaler Ausprägung

Folgende Grundannahmen gelten für die Instanziierung 1:

- Eine BildungsID ist ausschliesslich für Lehrende und Lernende ISCED 020-4 verfügbar.
- Organisationen und Unternehmen treten ausschliesslich im Sinne von Relying Parties als Nutzende auf.
- Ausschliesslich öffentliche Lehranstalten und deren Lehrende und Lernende können die BildungsID benutzen.
- Das eigentliche Authentifikationsmittel der BildungsID ist nicht Hardware gebunden.
- Die Nutzerfreundlichkeit / Usability der BildungsID muss sehr hoch sein.
- Die Integration der BildungsID in Lösungen Dritter muss sehr einfach sein.

Abbildung 2 stellt eine minimale Ausprägung einer BildungsID dar. Diese ist in dem Sinne als minimal zu verstehen, als dass eine derart gestaltete BildungsID die zwangsläufig notwendigen Funktionen umfasst, um gegenüber den gegenwärtigen Lösungen einen zusätzlichen Mehrwert zu liefern.

Diese minimale Ausprägung einer BildungsID bringt deutliche Reduktionen bei den möglichen Nutzungen mit sich. Die BildungsID kann nicht zum elektronischen Signieren eingesetzt werden, ebenso ist die Anwendung von ID-gebundener Verschlüsselung durch die Nutzenden ausgeschlossen. Ausweise von Lernenden (Schülerausweise, Lehrlingsausweise und ähnliche) oder Lehrenden können nicht direkt von der BildungsID abgeleitet werden, die BildungsID liefert keine Funktion eines elektronischen Trust-Ankers. Während personenbezogene Funktionsnachweise (z.B. „Schulleiter“) oder Eigenschaftsnachweise (z.B. „Schüler“) möglich sind, fallen organisationsfokussierte Nutzungen wie das Signieren durch Organisationen, aber auch der Nachweis von Vertretungsberechtigung weg.

Die öffentliche Hand beschränkt sich dabei auf Seite der Bereitstellung auf die Funktionen „Registrierung & Revozierung“, stellt jedoch bei den Vertrauensdiensten die „Personenidentifizierungsdaten“, die „Funktionsnachweise“ der Organisationen sowie „Eigenschaftsnachweise“ bereit. Die Funktionsnachweise werden in „öffentlich-rechtlichen Registern“ geführt, die jedoch nicht im Sinne einer Attribute Authority angesprochen werden können, sondern ihre Daten für einen oder mehrere private „Identity Provider“ verfügbar machen. Es muss daher sichergestellt werden, dass von privaten Anbietern die Funktionen „Authentifizierung“ sowie „Funktions- und Eigenschaftsnachweis“ bereitgestellt werden.

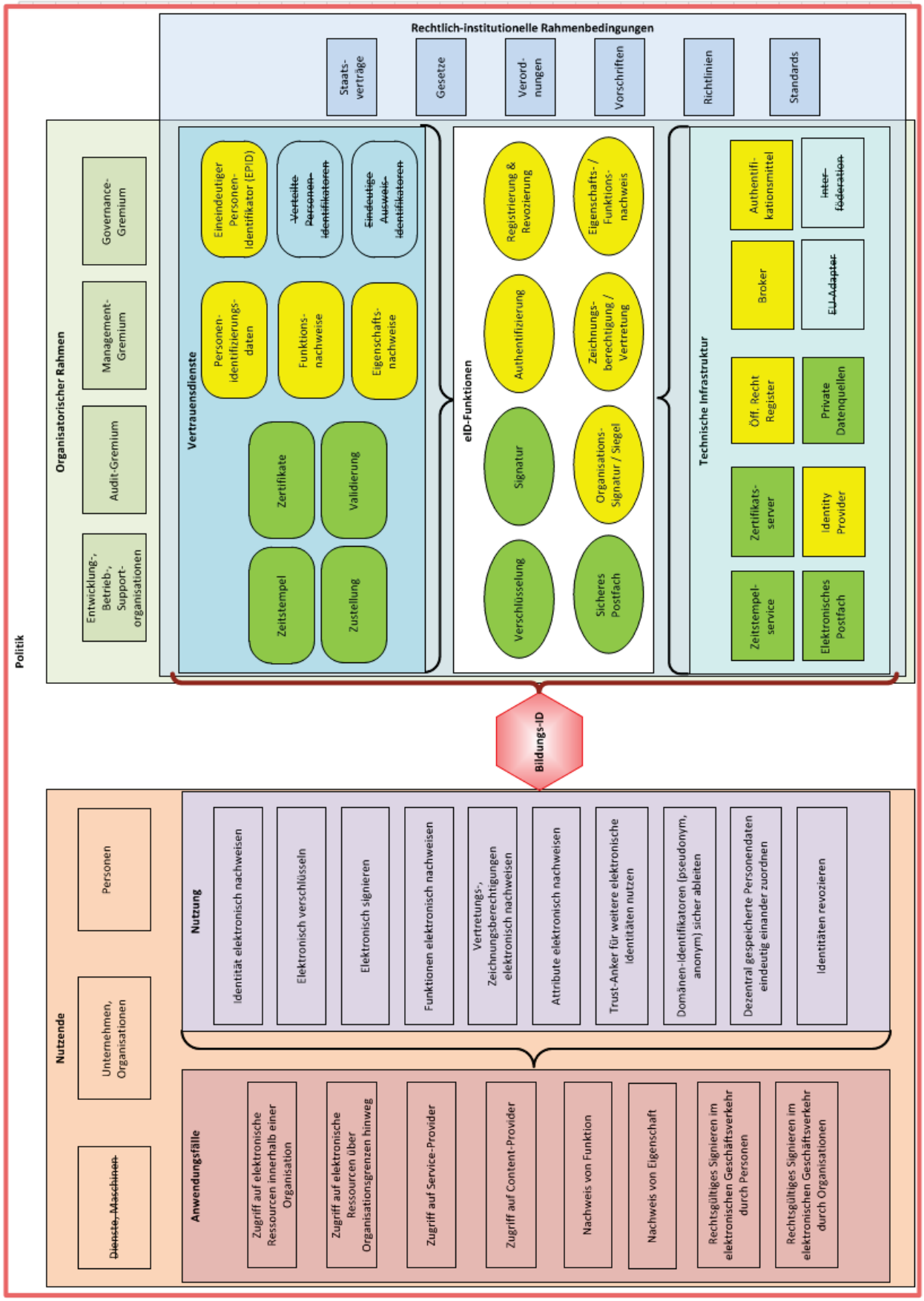

Abbildung 3 – BildungsID in maximaler Ausprägung (gelbe Elemente: von der öffentlichen Hand bereitgestellt, grüne Elemente: durch private Anbieter bereitgestellt)

2.3.2 Instanziierung 2: BildungsID in maximaler Ausprägung

Folgende Grundannahmen gelten für die Instanziierung 2:

- Alle am Bildungswesen beteiligten Personen und Organisationen können eine BildungsID erhalten.
- Alle Anwendungsfälle müssen ermöglicht werden.
- Private Bildungseinrichtungen müssen die BildungsID benutzen können.
- Es wird kein einheitliches Authentifikationsmittel definiert, unterschiedliche Implementierungen in Hard- und Software sind möglich.
- Die BildungsID basierte, elektronische Signatur ist nur für Lehrende, die Bildungsverwaltung und Organisationen relevant. Deshalb wird diese Funktion nicht hoheitlich angeboten, sondern werden private Lösungen nach Bedarf integriert. Es wurde kein Grund gesehen, warum nicht die privat angebotenen Lösungen genutzt werden könnten.

Abbildung 3 stellt eine maximale Ausprägung einer BildungsID dar. Maximal bedeutet in diesem Kontext, dass alle Anwendungsfälle unterstützt und allen am Bildungswesen beteiligten Personengruppen die Nutzung der BildungsID ermöglicht werden müssen. Insbesondere ist die Anwendung der Signatur für Personen und für Organisationen vorgesehen.

Die öffentliche Hand muss in dieser Ausprägung eine umfassende Infrastruktur für die BildungsID anbieten. Dies umfasst ein zentraler IdP für die „Authentifizierung", der für „Registrierung & Revozierung" auf „Personenidentifizierungsdaten" zugreift. Dazu kommen auch Attribute im Sinne von „Funktions- & Eigenschaftsnachweisen" für Lernende, Lehrende und Mitarbeitende der Bildungsadministration. In dieser Ausprägung ist auch die ID gebundene Verschlüsselung vorgesehen.

2.3.3 Instanziierung 3: BildungsID in FIDES-Ausprägung

Folgende Grundannahmen gelten für die Instanziierung 3:

- Die BildungsID ist für Lehrende und Lernende der Stufen ISCED-020-4 erhältlich sowie für Mitarbeitende in den verschiedenen Stufen der Bildungsadministration. Studierende der Pädagogischen Hochschulen müssen im Rahmen von Studiumsaktivitäten in den Schulen ebenfalls eine BildungsID haben.
- Die BildungsID berücksichtigt die Komplexität der Bildungslandschaft in der Schweiz und bildet vielfältige Beteiligungsmöglichkeiten für Kantone ab.
- Angehörige von privaten Bildungsinstitutionen, die als Bildungsstätten für die Volksschule anerkannt sind, müssen ebenfalls die BildungsID erhalten können.
- Organisationen und Unternehmen treten ausschliesslich im Sinne von Relying Parties als Nutzende auf.
- Das eigentliche Authentifikationsmittel der BildungsID ist nicht Hardware gebunden.
- Die Nutzerfreundlichkeit / Usability der BildungsID muss sehr hoch sein.

Abbildung 4 zeigt die Instanziierung des Modells, die dem FIDES-Konzept entspricht. Das Konzept sieht auf der Bereitstellungsseite einen eindeutigen Personenidentifikator (UUID) vor, der den Personen im Bildungswesen zugeordnet wird. Diesem Identifikator werden Personendaten sowie Funktions- und Eigenschaftsnachweise zugeordnet, die aus staatlichen Quellen (mit Ausnahme von Privatschulen) stammen. Die Rolle des IdP kann in unterschiedlicher Ausprägung wahrgenommen werden, durch staatliche Stellen oder durch private im Auftrag und unter Aufsicht durch staatliche Stellen. Identitätszertifikate können dabei optional verwendet werden.
Mit der Funktion der Interföderation kann die Anbindung an weitere Föderationen z.B. von Switch sichergestellt werden, dies aber nicht im Sinne eines Brokers mit Verantwortlichkeit innerhalb des Ökosystems der Bildung.

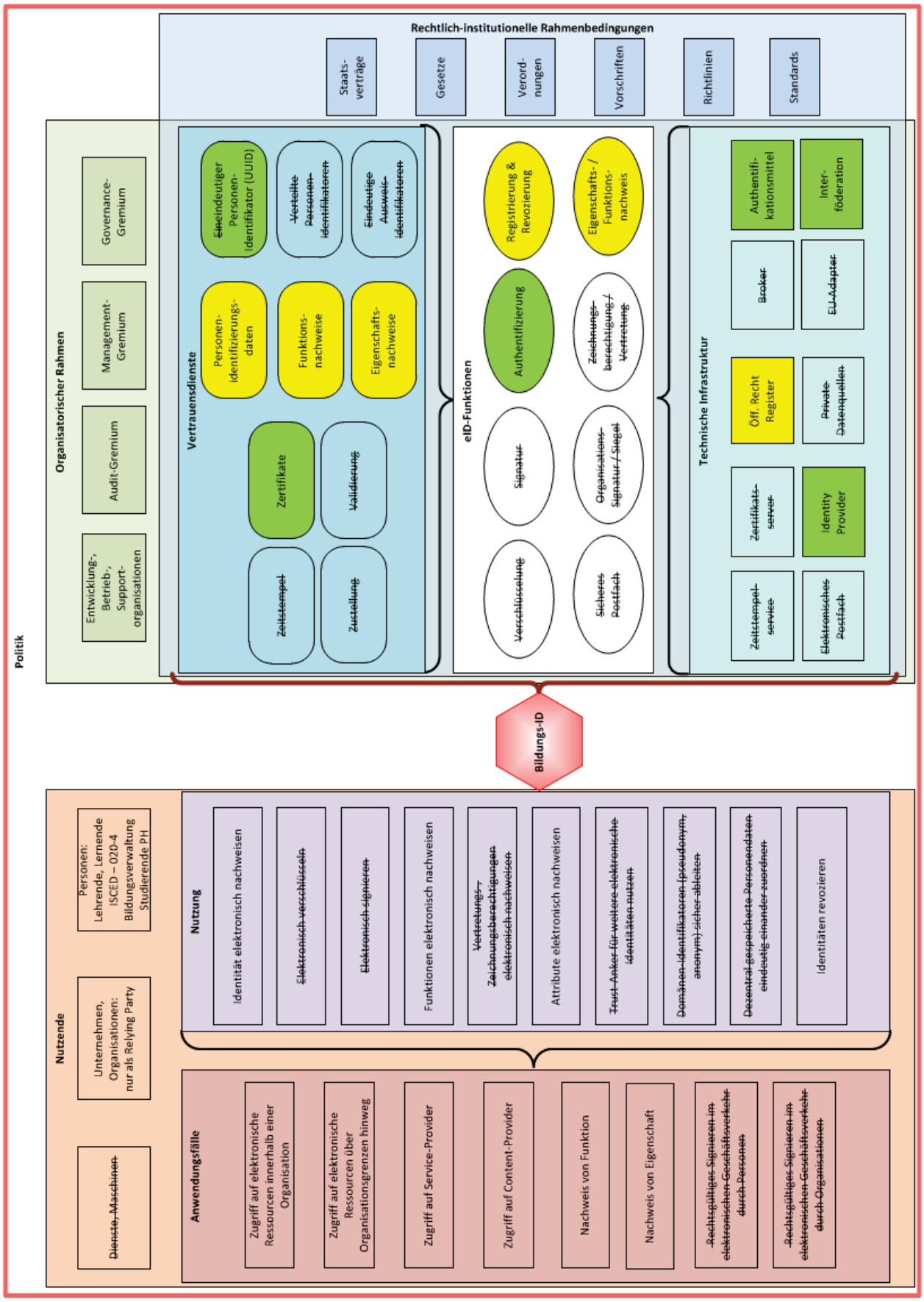

Abbildung 4 – BildungsID in FIDES-Ausprägung (gelbe Elemente: von der öffentlichen Hand bereitgestellt, grüne Elemente: durch private Anbieter bereitgestellt)

3 Fazit

Der Workshop mit dem Projektteam von edcua.ch hat gezeigt, dass nur wenige, kleine Anpassungen notwendig sind, um die für eine nationale E-ID entwickelten Elemente des Ökosystem-Modells im spezifischen Kontext der Bildung verwenden zu können. Das angepasste Modell wurde in den Diskussionen um die Instanziierungen angewendet und dadurch ein erstes Mal validiert.

Das Vorgehen nach der Ökosystem-Modell-Methodik stellt auf der Basis der Anwendungsfälle sicher, dass die Diskussion um technische Elemente und Bereitstellung der Identitätsinfrastruktur von der Nutzung und dem Nutzen der Lösung her beurteilt wird. Die Anwendungsfälle im Modell fassen unterschiedliche Anwendungen auf einer hohen Abstraktionsstufe zusammen. Damit ist eine grundsätzliche Reflektion über die unterschiedlichen Anwendungen möglich. Für die konkrete Ausgestaltung sind die tatsächlichen Anwendungsszenarien, wie sie im Bericht *Nutzende, Anwendungsfälle und Anwendungsszenarien* für drei Fälle ausgearbeitet wurden, wieder hinzuzuziehen.

Die ausgearbeiteten Minimal- und Maximalinstanziierungen zeigen den weiten Handlungsspielraum für die Umsetzung einer BildungsID auf einer konzeptionellen Ebene. Die beiden Extremvarianten weisen auf die folgenden Schlüsselfragen hin:

- Welches ist die Reichweite der Lösung (Beschränkung auf Lernende und Lehrende vs. Integration aller Stakeholder)?
- Wie stark engagiert sich die öffentliche Hand in der Bereitstellung der Infrastruktur (privater oder öffentlicher IdP, der die Registerinformationen aufbereitet)?
- Sind die von einer digitalen Identität abhängigen Funktionen wie Signieren ebenfalls mitzudenken, obwohl sie in erster Linie die Bildungsadministration betreffen?

Die FIDES-Instanziierung als ein von educa.ch favorisierter Soll-Zustand ermöglichte in den Interviews auf der Basis einer konkreten Instanziierung mit den Interviewpartnern zu diskutieren. Auf dieser Basis konnte dann die Verortung der vorhandenen eigenen Infrastruktur im Modell abgefragt und das Zusammenspiel zwischen den lokalen Gegebenheiten und dem gesamten Ökosystem beurteilt werden. Dabei gilt es insbesondere zu beachten, dass die rechtlichen und institutionellen Rahmenbedingungen im Gegensatz zur vereinfachten funktionalen Darstellung im Modell, sehr heterogen sind.