Identitätsverbund Schweiz

Situationsbericht z.H. der Kantone und interessierten Behörden

Executive Summary

Mit den Kantonen, für die Kantone
Der Identitätsverbund Schweiz IDV bietet eine technische Lösung, um Login-Prozesse im E-Government und in der elektronischen Zusammenarbeit unter Behörden zu vereinfachen. IDV Schweiz ist ein strategisches Projekt im Schwerpunktplan von E-Government Schweiz, projektverantwortliche Organisation ist das Staatssekretariat für Wirtschaft (SECO).

IDV Schweiz ist eine Zusammenarbeit des Bundes mit den Kantonen. Bei der Entwicklung wurden IT-Experten und -Verantwortliche aus Kantonen und Städten beigezogen. Damit konnte sichergestellt werden, dass der Identitätsverbund die Bedürfnisse der Praxis abdeckt. Das Projekt wurde durch die Schweizerische Informatikkonferenz SIK begleitet, die auch Mitglied im Projektausschuss ist.

Der Identitätsverbund ist ein Cloud-Dienst, der zwei gängige Probleme der öffentlichen Verwaltung im Bereich E-Government löst: a) Vereinfachung des Zugangs zu elektronischen Behördendiensten für Private, b) Vereinfachung bei der elektronischen Zusammenarbeit unter den Behörden.

Synergiepotentiale
IDV Schweiz löst ein Problem, für das in diversen anderen Kontexten Studien und Projekte lanciert wurden. Die Synergiefindung ist darum ein zentrales Anliegen des Projekts. Nebst dem engen Einbezug von Kantonen in das Projekt wurden regelmässige Abstimmungen mit dem Programm IAM Bund vorgenommen. Experten des Informatiksteuerungsorgans des Bundes ISB waren aktiv an der Konzeption von IDV Schweiz beteiligt. Zudem prüfen derzeit diverse kantonale Projekte sowie der Bund den Einsatz des Identitätsverbunds und/oder eine Zusammenarbeit mit IDV Schweiz. Besonders erwähnenswert sind die Projekte FIDES und Justitia 4.0.

Elektronischer Identitätsnachweis E-ID
IDV Schweiz und das Bundesgesetz über elektronische Identifizierungsdienste (E-ID-Gesetz) sind zwei Vorhaben mit unterschiedlichem Fokus. Mit dem E-ID-Gesetz wird der rechtliche Rahmen geschaffen, damit staatlich anerkannte Anbieterinnen (IdP) die Bürger nach den neuen gesetzlichen Vorgaben mit einer E-ID ausstatten können, um Dienste von E-Government und E-Commerce nutzen zu können. Demgegenüber ermöglicht IDV Schweiz eine Nutzung von unterschiedlichen Anmeldeverfahren.

Betriebsorganisation und Kosten
IDV Schweiz ist ein Infrastrukturdienst für die Kantone und andere Akteure, der sicher und ständig verfügbar sein muss. Eine Betriebsorganisation soll bis spätestens 2019 aufgebaut werden. Dazu soll eine Trägerschaft gegründet werden, welche anschliessend der SIK/eOperations den Auftrag zum operativen Betrieb gibt. Die Kosten des Betriebs werden gegenwärtig mit total 2 Mio. CHF jährlich veranschlagt. IDV Schweiz skaliert gut: Ist IDV einmal in Betrieb genommen, so verursacht jeder weitere Nutzerkreis (IDV Domäne) nur noch geringe Zusatzkosten.

Pilotbetrieb
IDV Schweiz ist für den Pilotbetrieb bereit. Ein Start für die Pilotierung wird erfolgen, sobald eine Zusicherung der Kantone und/oder anderer Interessenten vorliegt, dass sie sich in Zukunft finanziell an einer Trägerschaft beteiligen wollen.

Inhalt

Begriffe und Abkürzungen

AA	Attribute Authority
BAG	Bundesamt für Gesundheit
BJ	Bundesamt für Justiz
eCH	Verein eCH
E-Gov	E-Government
E-ID	Strategisches Projekt "Etablierung einer national und international gültigen elektronischen Identität", unter Führung des Bundesamts für Polizei fedpol
FIDES	Rahmenkonzept zur Föderation von Identitätsdiensten für den Bildungsraum Schweiz
G2C	Government-to-Citizen
G2G	Government-to-Government
GUI	Graphical User Interface
HR	Human Resources
IdP	Identity Provider
IDV (Schweiz)	Identitätsverbund Schweiz, Strategisches Projekt unter Führung des SECO
ISB	Informatiksteuerungsorgan des Bundes
Justitia 4.0	Projekt zur Digitalisierung und Transformation der Justiz im Rahmen des HIS-Programms
LoA	Level of Assurance
OIDC	OpenID Connect
PKI	Public Key Infrastructure
PL	Projektleitung
RP	Relying Party
SAML	Security Assertion Markup Language
SECO	Staatssekretariat für Wirtschaft
SIK	Schweizerische Informatikkonferenz
WBF	Eidgenössisches Departement für Wirtschaft, Bildung und Forschung

1 Identitätsverbund Schweiz

1.1 Strategisches Projekt

Das Projekt Identitätsverbund Schweiz (IDV Schweiz) hat zum Ziel, einen Infrastrukturdienst für die Vereinfachung von Anmelde-Prozessen im E-Government aufzubauen.

IDV Schweiz ist ein strategisches Projekt (SP1) im Schwerpunktplan von E-Government Schweiz. Die projektverantwortliche Organisation ist das Staatssekretariat für Wirtschaft (SECO).

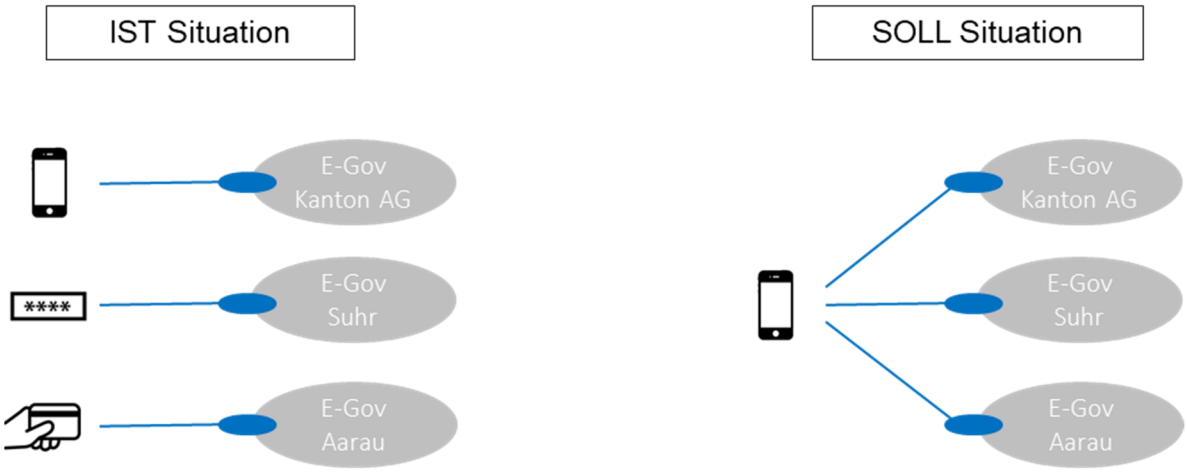
1.2 IDV Schweiz im Überblick

1.2.1 IST und SOLL Situation

Wenn man sich heute bei einem E-Government-Dienst anmeldet, so geschieht dies typischerweise mit einem von der Behörde ausgestellten Zugangsmittel, z.B. Passwort, SMS-TAN usw. (vgl. IST Situation in der Illustration). Die Behörde baut dafür eine Benutzerverwaltung auf, implementiert Prozesse und muss wohl oder übel für Benutzersupport sorgen. Bei höheren Sicherheitsanforderungen ist der Identifikationsprozess des Benutzers für eine Behörde ein Zeit- und Kostenfaktor. Der Benutzer seinerseits muss sich bei jeder Behörde registrieren und das dort benötigte spezifische Zugangsmittel verwalten, d.h. er fügt seiner ohnehin schon überfüllten Sammlung an Konten und Passwörtern weitere hinzu.

Das Problem betrifft nicht nur Private und Unternehmen, sondern auch die Zusammenarbeit unter den Behörden. Noch gibt es keinen Weg, wie sich eine Mitarbeitende mit dem Login, das sie in ihrer Stammbehörde täglich einsetzt, bei einer fremden Behörde, sei es im eigenen Kanton, in einem anderen Kanton oder beim Bund, anmelden könnte. Darum muss eine Behörde, die einer anderen Behörde Zugang zu ihren Diensten gewähren will, die fremden Mitarbeitenden separat identifizieren, ihnen Zugangsmittel aushändigen und ihre Identitäten verwalten. Das ist logistisch und finanziell belastend und stellt nicht zuletzt ein Sicherheitsrisiko dar.

Es wäre für die Behörde weit günstiger, wenn sich der Benutzer mit einem bestehenden Konto, dem die Behörde genügend Vertrauen entgegenbringt, direkt anmelden könnte (vgl. SOLL Situation in der Illustration). Der Benutzer sollte aus einer Liste von bekannten oder häufig verwendeten Anmeldediensten seinen bevorzugten auswählten können.

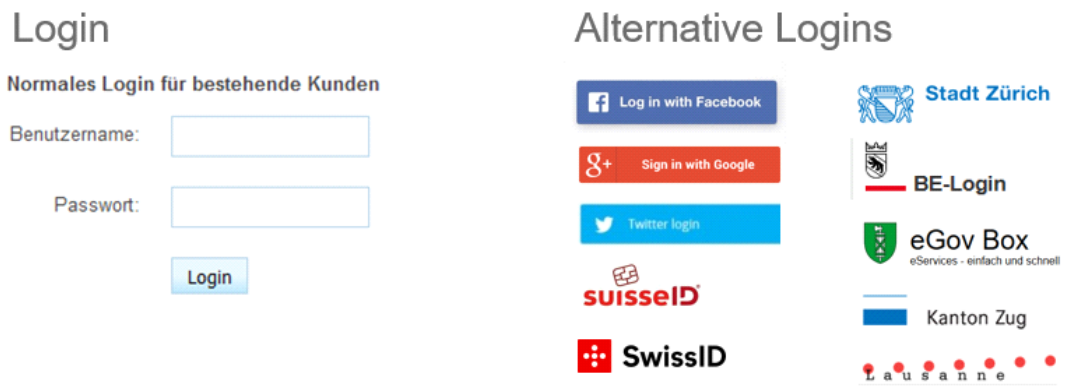


IST: Heute muss der Benutzer für Dienste von unterschiedlichen Behörden unterschiedliche Logins verwenden.
SOLL: Man verwendet überall das gleiche Login.

Die angeführten Behörden in der Illustration sind lediglich Beispiele. Theoretisch kann es jeder andere Kanton, jede andere Gemeinde oder eine Bundesbehörde sein.

1.2.2 Der LOGIN-PLUS Button

Will eine Behörde die Situation für sich und ihre Kunden im Sinne des SOLL-Zustands verbessern, so bleibt ihr heute nur die Option, die häufig und gerne eingesetzten Anmeldedienste von Benutzern für ihr E-Government-Portal zuzulassen. Das könnte dann beispielsweise aussehen wie in der folgenden Illustration.



Beispiel für einen Login-Screen, in dem nebst dem behördeneigenen Login (links) zusätzliche Logins verfügbar sind, die von den Benutzern häufig und gerne verwendet werden (rechts). Die Auswahl ist beispielhaft und kann mehr oder weniger umfassend sein.

Zum normalen Benutzerkonto (links) kommen alternative Anmeldeverfahren hinzu (rechts), die einzeln integriert werden. Eine Ausweitung der Anmeldemöglichkeiten mit diesem Verfahren ist mit hohen Entwicklungs- und Integrationskosten verbunden, die in jedem Portal und für jede Behörde von neuem anfallen. Derartige Konstellationen sind in der Informatik nicht neu. Wo sich Investitionen und Betriebskosten auf mehrere Parteien aufteilen lassen, sind sog. Cloud-Dienste nicht weit. Genau hier liegt der Zweck des Identitätsverbundes IDV: Verschiedene Anmeldeverfahren in einem einfach zu integrierenden Infrastruktur-Dienst zu vereinen, damit Webdienste ihre Anmeldeprozeduren auslagern können.

Anstatt viele Fremd-Logins bei sich einzeln zu integrieren, bietet die Behörde den LOGIN-PLUS Button an. Sie muss dazu nur die Standard-Schnittstelle zum IDV realisieren, und kann umgehend eine breite Palette von Logins anbieten.

IDV Schweiz hat den LOGIN-PLUS Button entwickelt. Dahinter verbirgt sich ein Cloud-Dienst, der eine breite Palette von Anmeldediensten zur Verfügung stellen kann. In obiger Illustration setzt die Behörde den LOGIN-PLUS Button als Alternative zum lokalen Login der Behörde ein. Die Behörde kann ebensogut auf ein eigenes Login verzichten und stattdessen nur den LOGIN-PLUS Button anbieten.

Mit dem LOGIN-PLUS Button gibt die Behörde dem Benutzer die Freiheit, sich mit einem Anmeldeverfahren seiner Wahl einzuloggen,

- das nicht von der Behörde stammt,
- keine zusätzlichen Identifikations- und Registrationsprozesse abverlangt,
- vom Benutzer andernorts schon verwendet wird,
- die Sicherheits- und Qualitätskriterien des E-Government Portals erfüllt.

1.2.3 Die Sicht des Benutzers

Für den Benutzer ist der LOGIN-PLUS Button ein Weg, seinen bevorzugten Anmeldedienst aufzurufen. Der Weg führt über eine Auswahl an bekannten Anmeldediensten, von denen sich der Benutzer einen geeigneten auswählen kann.

IDV Schweiz führt kein Benutzerkonto, d.h. die Benutzer müssen sich nicht mit den Innereien des LOGIN-PLUS Buttons auseinandersetzen. Als Benutzer lässt man sich durch einen Dialog führen und wählt seinen Anmeldedienst aus. In der obigen Illustration beispielsweise werden dem Benutzer mehrere Anmeldeverfahren zur Auswahl gegeben. Der Benutzer kann dafür sorgen, dass sich IDV die Wahl für zukünftige Logins merkt, sodass er bei späteren Anmeldungen nicht mehr gefragt wird.

Nach dem Anklicken des LOGIN-PLUS Buttons erhält der Benutzer eine Auswahl an Logins, mit denen er sich beim Dienst anmelden kann. Der Umfang und die Darstellung der Auswahl sind beispielhaft und dienen nur der Illustration.

1.2.4 Die Sicht der Behörde

Für eine Behörde ist der LOGIN-Button ein Cloud-Dienst, der in die E-Government-Webseite oder ein Portal integriert wird. Die Behörde hat die volle Kontrolle und entscheidet darüber,

- welche Anforderungen ein externer, durch den LOGIN-PLUS Button vermittelter Anmeldedienst erfüllen muss,
- welche externen Anmeldedienste überhaupt akzeptiert würden;
- welche Sicherheitsstufe garantiert sein muss (z.B. 1-Faktor, 2-Faktor usw.),
- ob bei der Anmeldung des Benutzers Personen- oder andere personenbezogene Angaben benötigt werden und falls ja, welche.

IDV zeigt dem Benutzer nur solche Anmeldedienste an, die von der Behörde zugelassen werden und die den sicherheitstechnischen, organisatorischen und anderen Anforderungen der Behörde genügen.

1.2.5 Eignung und Einsatzszenarien

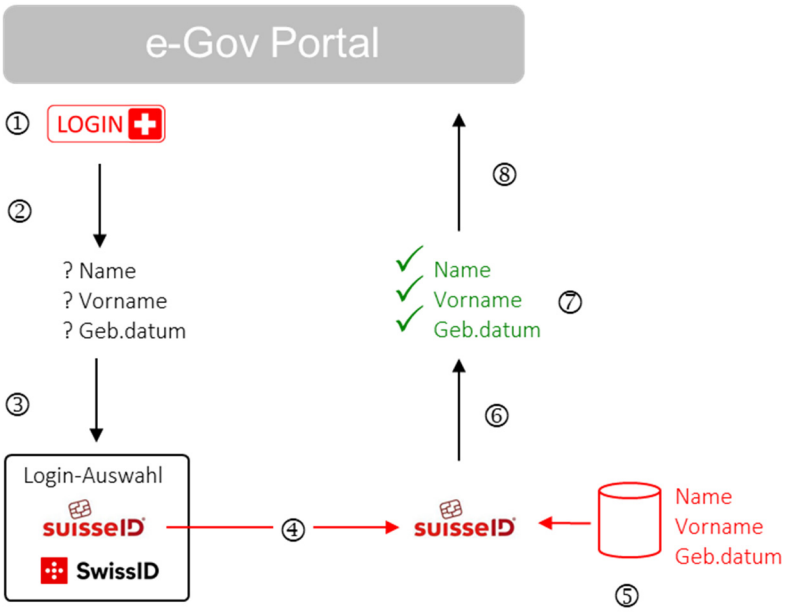
IDV Schweiz ist in enger Zusammenarbeit mit den Kantonen aufgebaut worden. Schon früh haben sich zwei Haupt-Einsatzbereiche mit jeweils unterschiedlichen Anforderungen und Rahmenbedingungen herauskristallisiert.

- Der erste Bereich betrifft die elektronischen Behördendienste für Private (Government-to-Citizen, kurz G2C), wo es darum geht, Privaten die Möglichkeit zu geben, sich mit bestehenden Fremd-Logins wie oben geschildert bei der Behörde anmelden zu können.
- Der zweite Bereich betrifft die elektronische Zusammenarbeit unter den Behörden (Government-to-Government, kurz G2G), damit eine Behörde Mitarbeitenden einer anderen Behörde Zugang zu elektronischen Ressourcen gewähren kann.

Die zwei Einsatzbereiche G2C und G2G müssen teilweise unterschiedliche Anforderungen erfüllen und wurden darum als sog. *IDV-Domänen* umgesetzt. Das bedeutet, dass sie getrennt voneinander verwaltet und betrieben werden können.

Die wichtigsten Einsatzszenarien für den LOGIN-PLUS Button werden im Folgenden kurz erläutert.

Szenario A: Privatperson identifiziert sich bei der Behörde (G2C Domäne)
Das Szenario kann auftreten, wenn die Behörde die Identität einer Person überprüfen muss, z.B. um ein Benutzerkonto mit einem Steuerdossier zu verbinden. Die Behörde benötigt personenbezogene Angaben, beispielsweise Name, Vorname und Geburtsdatum oder andere. Die Angaben dürfen aber nicht reine Behauptungen der Person selbst sein, sondern müssen aus einer vertrauenswürdigen Quelle stammen, z.B. aus einem elektronischen Register. Die Behörde weist den IDV an, der Privatperson nur solche Anmeldedienste zur Auswahl vorzuschlagen, die zur Lieferung der geforderten Personenangaben überhaupt in der Lage wären. Aus Gründen des Datenschutzes muss die Person der Weitergabe ihrer Personendaten ausdrücklich zustimmen.



Der Benutzer klickt auf den LOGIN-PLUS Button im Behördenportal (1). Das Portal fordert vom IDV eine Liste von Personendaten an (2). IDV zeigt dem Benutzer alle Anmeldedienste an, die sich für die Aufgabe eignen, hier SuisseID und SwissID (3). Im Beispiel wählt der Benutzer SuisseID. Nachdem sich der Benutzer mit seiner SuisseID angemeldet hat, werden die Personendaten aus der SuisseID-Datenbank aufbereitet (5) und dem Benutzer zur Kontrolle angezeigt (6). Der Benutzer stimmt der Weiterleitung zu (7). Erst jetzt werden die Daten dem Portal übergeben (8). Der Benutzer ist jetzt angemeldet und das Behördenportal hat die geforderten Angaben.

Das Besondere an diesem Szenario ist die Tatsache, dass potentiell jeder Anmeldedienst, der Personendaten zur Verfügung stellt, den Prozess hätte unterstützen können. Statt mit 2 hätte man auch ein Beispiel mit 20 in Frage kommenden Anmeldediensten machen können. Der Punkt ist, dass die Behörde in jedem Fall nur eine einzige technische Schnittstelle unterhalten muss – jene für den IDV –, um das gewünschte Ergebnis zu erzielen.

Szenario B: Privatperson meldet sich beim Behördenportal an (G2C Domäne)
Dieser Fall tritt auf, wenn die Behörde lediglich sicherstellen muss, dass die Person ein angemeldeter Benutzer ist oder wenn sie ihn als Kunde wiedererkennen will, z.B. um einen Zugriff auf ein persönliches Dossier zu gewähren. Es handelt sich um eine Vereinfachung von Szenario A, weil das Portal keine Personenangaben benötigt, sondern nur die Bestätigung, dass das Login stattgefunden hat.

IDV wird dem Benutzer eine grössere Auswahl von Anmeldediensten anzeigen als im Szenario A, weil diesmal auch Anmeldedienste geeignet sind, die mit dem Login keine Personenangaben mitliefern. Das gesamte Prozedere ist einfacher, u.a. entfällt die Einwilligung zur Weiterleitung von Personendaten, da keine solchen in Spiel sind.

Szenario C: Behördenmitarbeiterin meldet sich bei einer fremden Behörde an (G2G Domäne)
Beispiel: Eine kantonale Angestellte will sich für eine Bundesapplikation einloggen. Der Ablauf ist ähnlich wie in Szenario A, aber mit wesentlichen Unterschieden.

- Es werden Angaben zur Mitarbeiterin benötigt, diesmal nicht Personendaten wie in Szenario A, sondern fachliche Angaben, wie z.B. die Funktion der Mitarbeiterin in der Behörde;
- In einer Behörde gibt es typischerweise einen Anmeldedienst für Mitarbeitende. IDV weiss aus der Verbundkonfiguration, um welchen Anmeldedienst es sich handelt und leitet die Mitarbeiterin ohne weitere Umschweife direkt dorthin weiter;
- Falls die Mitarbeiterin intern bereits (oder noch) angemeldet ist, merkt das der IDV und verlangt keine wiederholte Anmeldung;
- Für die Weiterleitung von Angaben an die Fremdbehörde muss die Mitarbeiterin keine Einwilligung geben. Ein juristisches Gutachten im Auftrag des Projekts besagt sogar, dass es ihr untersagt wäre, die Weiterleitung zu unterbinden.

Nachdem die Mitarbeiterin den LOGIN-PLUS Button betätigt, wird ein Prozess in Gang gebracht, der völlig unbemerkt im Hintergrund abläuft. Ohne weitere Einwirkung der Mitarbeiterin ist sie im nächsten Augenblick bei der Fremdbehörde angemeldet und kann weiterarbeiten. Man kann das mit "Single Sign-On" bezeichnen.

1.3 Unterstützung von gängigen Technologien

Die gängigen Authentisierungstechnologien sind SAML und OpenID Connect (OIDC). Da der IDV technologieneutral konzipiert wurde, sind theoretisch beide Varianten möglich. Aufgrund der Tatsache, dass die am Aufbau beteiligten Kantone vorwiegend SAML-basierte Systeme in Betrieb haben, wurde für den IDV in einem ersten Schritt das SAML-Protokoll umgesetzt.

Es bestehen Konzepte und Pläne, um den IDV auch Kunden anbieten zu können, die OIDC einsetzen. Da heute für OIDC kein einheitlicher Authentisierungsstandard existiert, besteht ein grosses Spektrum an möglichen Umsetzungsvarianten, die aus praktischen Gründen und mit Blick auf die Entwicklungskosten eingeschränkt werden müssen. Konkret würde eine OIDC-Entwicklung vom Anwendungsfall und den beteiligten OIDC-Systemen abhängen. Gemäss einer internen Kostenschätzung wäre eine erste Integration von OIDC im Rahmen eines Proof-of-Concept mit deutlich unter 50 kCHF machbar.

1.4 Bisherige Arbeiten und Projektstand

Die wichtigsten Ergebnisse des Projekts per Ende 2017 sind:

1. *IDV Broker 1.0:* Die Maschinerie hinter dem LOGIN-PLUS Button. Der Vermittlerdienst ("Broker") wurde in enger Abstimmung mit Bund und Kantonen entwickelt. Er implementiert die Anforderungen an ein föderiertes Identitätsmanagement aus Sicht der Behörden. Webdienste (Relying Parties) anerkennen digitale Identitäten aus fremden Anmeldediensten (Identity Provider) und delegieren so die Identifikation und Authentisierung der Benutzer an ein Drittsystem;
2. *Umsetzung des Domänenkonzepts:* Domänen sind eigenständige IDV Broker-Infrastrukturen, die für einen bestimmten Interessentenkreis aufgebaut und konfiguriert werden. Domänen operieren autonom von anderen und haben ihren eigenen IDV Broker. Gewisse Interessentenkreise könnten ohne dieses flexible Instrument gar keinen Identitätsverbund für sich aufbauen, z.B. wenn sie einer besonderen gesetzlichen Bestimmung unterworfen sind, die für andere Kontexte nicht gelten. Domänen definieren ihre eigenen Sicherheitsniveaus und Qualitätsmodelle, legen eigene Bedingungen für die Teilnahme von Anmeldediensten und Webdiensten fest, können eigene Regeln für die Vermittlung von Identitäten anwenden und vieles mehr. Vom Projekt bisher aktiv unterstützt wurden die Domänen **G2C** (Privater Nutzer zu Behörden zwecks E-Government) und **G2G** (Behörden untereinander). IDV Schweiz kann jederzeit um weitere Domänen erweitert werden;
3. *Schnittstellen-Spezifikation Broker 1.0:* Die Kunden-Schnittstelle, mit der sich Anbieter von Identitätsdiensten (Identity Provider) und Webdiensten (Relying Parties) an IDV Schweiz technisch anschliessen;
4. *Integrationsplattform (PROD-INT):* Eine technische Betriebsplattform, welche die Dienste des IDV Brokers 1.0 für pilotwillige Identitätsdienste (Identity Provider) und Webdienste (Relying Parties) anbietet. Die Plattform steht seit Q1/2018 bereit;

5. *Trust Framework:* Die Bildung eines Vertrauensraums ist eine der hauptsächlichen Herausforderungen für den Betrieb eines Verbundes (einer IDV Domäne). In den sog. *Baseline Requirements* werden die Sicherheitsanforderungen definiert und das gegenseitige Vertrauensverhältnis in Form von verbindlichen Regeln beschrieben. Mithilfe von sog. *Practice Statements* demonstriert jeder Verbund-Teilnehmer, mit welchen Massnahmen er die Kriterien aus den Baseline Requirements erfüllt. Baseline Requirements und Practice Statements sind Konzepte, die aus der PKI-Welt entlehnt wurden, um Vertrauen im Identitätsverbund herstellen zu können. Ein derartiges Trust Framework war von den Kantonen als Voraussetzung genannt worden, um Identitäten aus fremden Behörden anzuerkennen.
6. *Trust Modell für G2G:* Zusammen mit Experten von KPMG hat das Projekt die Baseline Requirements für die G2G Domäne definiert, genauer: Eine detaillierte Beschreibung der technischen und organisatorischen Voraussetzungen, die ein IdP erfüllen muss, wenn er Identitäten mit der zweiten Qualitätsstufe (LOA 2) gem. eCH-0170 in der G2G Domäne anbieten will.

1.5 Synergien mit Projekten der öffentlichen Verwaltung

IDV Schweiz steht mit Vertretern aus diversen Projekten und Initiativen in der öffentlichen Verwaltung in Kontakt, sowohl beim Bund als auch bei den Kantonen. Bei den folgenden Projekten ist das Synergiepotential besonders hervorzuheben und es laufend aktuell Kooperationsgespräche.

- **Projekt FIDES der Fachagentur educa.ch**. Das Rahmenkonzept zur Föderation von Identitätsdiensten für den Bildungsraum Schweiz (FIDES) wurde im Oktober 2017 von der EDK-Plenarversammlung verabschiedet. Die Fachagentur educa.ch ist beauftragt, Umsetzungs- und Finanzierungsdetails für den Aufbau und den Betrieb einer solchen Föderation auszuarbeiten. Der Beschluss unter: http://www.educa.ch/de/news/2017-11-15/foederation-fides
- Das **Projekt Justitia 4.0** hat u.a. folgende Vision: Die papierlose eJustizakte wird in allen Verfahrensabschnitten des Zivil,- Straf- und Verwaltungsrechts durch alle Beteiligten verwendet und medienbruchfrei ausgetauscht. Mehr unter: https://www.his-programm.ch
- **Umsetzungsmassnahmen aus dem Programm IAM Bund**. Das ISB prüft den Einsatz von IDV in der nahen Zukunft, um Mitarbeitenden von kantonalen und kommunalen Behörden den Zugang zu Bundesressourcen unter Verwendung ihres angestammten Logins zu ermöglichen.

1.6 Zusammenhang zur staatlich anerkannten E-ID

Unter der Bezeichnung *Etablierung einer national und international gültigen elektronischen Identität* (kurz E-ID) führt das Bundesamt für Polizei fedpol ein strategisches Projekt mit dem Ziel, dass sich Schweizerinnen und Schweizer im Internet mit der gleichen Qualität elektronisch ausweisen können wie sie dies mit dem Pass oder der Identitätskarte in der physischen Welt tun können. Der Bundesrat will klare Regeln für einen digitalen Identitätsnachweis erlassen, der staatlich anerkannt, überprüfbar und eindeutig ist. Am 22. Februar 2017 hat er deshalb die Vernehmlassung zu einem Bundesgesetz über elektronische Identifizierungsdienste (E-ID-Gesetz) eröffnet. Nach Kenntnisnahme der Resultate der Vernehmlassung hat er an seiner Sitzung vom 15. November 2017 das Eidgenössische Justiz- und Polizeidepartement (EJPD) beauftragt, bis im Sommer 2018 einen Gesetzesentwurf auszuarbeiten. Die Vernehmlassung hat gezeigt, dass das E-ID-Gesetz im Grundsatz unbestritten ist.

Das Gesetz soll klare Regeln für einen staatlich anerkannten Identitätsnachweis (E-ID) festlegen. Dieser soll Nutzerinnen und Nutzer in der Schweiz ermöglichen, sich bei bestimmten Angeboten mit voller Kontrolle über die eigenen Daten im Internet zu identifizieren. Dabei geht der Bundesrat von einer Aufgabenteilung zwischen Staat und Markt aus. Konkret sollen geeignete private oder öffentliche Identifizierungsdienstleister von einer Anerkennungsstelle auf Bundesebene eine Zulassung zur Herausgabe von staatlich anerkannten elektronischen Identifizierungsmitteln erlangen können. Mit dem Inkrafttreten des E-ID-Gesetzes ist frühestens 2020 zu rechnen.

E-ID hat damit einen anderen Fokus als IDV Schweiz. Zu den wichtigsten Unterschieden gehört, dass IDV Schweiz keine Identitäten an Personen herausgibt und selber keinen Anmeldedienst betreibt. Personen werden sich bei IDV Schweiz nie identifizieren oder registrieren müssen, das ist die Aufgabe der Anmeldedienste. IDV Schweiz ist vergleichbar mit einem Navigationssystem für Webdienste, mit dem sie ihren Benutzern eine Auswahl von Anmeldediensten präsentieren können (vgl. 1.2 weiter oben).

Staatlich anerkannte E-ID müssen untereinander interoperabel sein. Gemäss dem E-ID-Konzept wird die Interoperabilität auf Protokollebene hergestellt, ohne dass zwingend ein externer Broker beteiligt ist. Zwei durch das EJPD in Auftrag gegebene Studien bei international anerkannten Fachexperten haben ergeben, dass die Interoperabilität mittels Protokollansatz sichergestellt werden kann[1]. IDV Schweiz ist daher nicht Gegenstand des E-ID-Gesetzes.

Was die Vermittlung von E-ID mittels IDV Schweiz betrifft, so werden weitere Abklärungen nötig sein.

1.7 Zusammenhang zur SwissID-Initiative

Der Markt für digitale Identitäten entwickelt sich rasant. Inzwischen sind Identitätssysteme in Arbeit oder aufgebaut, von denen bekannt ist, dass ihre Betreiber diese später als staatlich anerkannte E-ID-Systeme anerkennen lassen möchten. Unter der Bezeichnung SwissID der SwissID-Initiative der SwissSign Group AG soll eine von mehreren Anbietern bereitgestellte, interoperable digitale Identität entstehen. Für die Kunden bedeutet das, dass man seine persönliche SwissID überall dort, wo SwissID akzeptiert wird, für das Login verwenden kann. Die SwissSign AG hat Interesse bekundet, sich zu gegebener Zeit als staatlich anerkannte Anbieterin von E-ID anerkennen zu lassen.

Die thematische Nähe des SwissID-Ecosysems zum Identitätsverbund ist augenfällig, sodass das SECO und SwissSign in der Vergangenheit Möglichkeiten der Zusammenarbeit erörtert haben. In Gesprächen hat sich gezeigt, dass die SwissID u.a. für den privaten Gebrauch bestimmt ist, was auch die E-Government Angebote für Bürger und Einwohner einschliesst. Zu den Erwartungen der SwissID gehört, dass man sich damit als Bürger beim Internetschalter einer Behörde anmelden kann. Um die nötige interne Interoperabilität unter den diversen Anbietern der SwissID zu ermöglichen, soll ein SwissID-Ecoystem inkl. Identitätsvermittler gebaut werden.

Die exakte Abgrenzung zwischen SwissID und IDV Schweiz ist nicht völlig geklärt und vieles ist noch im Fluss. Das SECO und SwissSign AG bleiben deshalb in engem Kontakt und Austausch.

1.8 Potential für Weiterentwicklungen

Die Anforderungen an den IDV Broker 1.0 sind durch die Kantone festgelegt worden. Der heute verfügbare Dienst ist eine erste Umsetzung dieser Vorgaben, ohne sie würde der IDV von den Kantonen nicht akzeptiert. Die Liste der Anforderungen ist lang und musste priorisiert werden, nicht zuletzt, um die Projektrisiken zu minimieren.

Ausgehend vom heute vorliegenden Ergebnisstand (vgl. 1.4) sind weitere Ausbauschritte möglich:

- Unterstützung für LOA 3: Für sehr hohe Sicherheitsanforderungen, wie sie z.B. im Gesundheitswesen gefordert werden, sind entweder End-zu-End-Verschlüsselungen oder Back-Channel Verfahren nötig. Der IDV ist dafür konzipiert, auch diese Anforderungen zu erfüllen, die momentane Implementierung beschränkt sich auf LOA 2, was in etwa dem Sicherheitsniveau einer SuisseID entspricht;
- Authentisierungsprotokolle: Derzeit wird SAML 2.0 unterstützt, was die derzeitige Technologie in behördlichen IAM-Systemen und im Hochschulbereich widerspiegelt (SwitchAAI). Andere Protokolle sind in anderen Kontexten populär. Zu erwähnen ist OpenID Connect (OIDC), das eine weite Verbreitung im Business-to-Business hat und u.a. von der geplanten SwissID verwendet werden soll. Um elektronische Identitäten im OIDC-Kontext vermitteln zu können, müsste der IDV um das entsprechende Protokoll erweitert werden;
- Protokoll-Transformator: Sollte der IDV dereinst mehr als ein Authentisierungsprotokoll unterstützen, würde eine neue Fähigkeit dazukommen, nämlich die Übersetzung von einer Welt in die andere, z.B. von SAML zu OIDC und umgekehrt. Damit könnten OIDC-fähige IdPs auch für RPs geeignet sein, die nur SAML verstehen und umgekehrt;
- Die Grundparameter und Steuerung der Domänen und ihrer teilnehmenden IdPs und RPs erfolgt über Konfigurationsdateien. Heute erfordert jede Anpassung Spezialwissen und einen Systemadministrator. Als Alternative hat das Projekt Konzepte und Pläne für eine Administrations- und Konfigurationsfunktion mit GUI-basierter Verwaltungsoberfläche erarbeitet, mit der die Manager von Domänen, IdPs und RPs ihre Dienste selbständig in den Identitätsverbund integrieren und konfigurieren können.

[1] Interoperable, state-approved Electronic Identities, David Basin and Ralf Sasse, January 26, 2018
Evaluation Report, proof of concept Interoperability E-ID, Jan Camenisch, Maria Dubovitskaya, January 31, 2018.
Beide Studien sind veröffentlicht unter https://www.bj.admin.ch/bj/de/home/staat/gesetzgebung/e-id.html

2 Betriebsorganisation und Trägerschaft

2.1 Organisation während der Projektphase

- SECO: Der Auftraggeber. Hat externe Spezialisten beschafft und mehrheitlich die Kosten für die Entwicklung getragen. Das SECO ist jedoch kein zukünftiger Infrastrukturbetreiber;
- Projektausschuss: Ein Gremium, das den Auftraggeber bei strategischen Entscheiden unterstützt. Die teilnehmenden Organisationen und Personen sind im Anhang A aufgeführt.
- E-Government Schweiz: Überwacht den Fortschritt des Projekts IDV Schweiz in der Eigenschaft als Koordinationsstelle für die Strategischen Projekte des Schwerpunktplans;
- SIK: Hat die Kommunikation zu den Kantonen und Gemeinden gefördert und geholfen, das Projekt besser zu vernetzen. Mit eOperations laufen Gespräche zu Trägerschaft und Betrieb;
- Kantone und Gemeinden: Diese waren eingeladen worden, sich aktiv an der Entwicklung des IDV zu beteiligen. Mit dem *IDV Architecture Board* wurde ein Gremium geschaffen, in dem 15 Interessengruppen, darunter 7 Kantone, in Sitzungen und Workshops aktiv Einfluss auf die Anforderungsanalyse und die Systemarchitektur genommen haben;
- Entwickler, Projektleiter: Durch das SECO beschaffte externe Experten (WTO 2015).

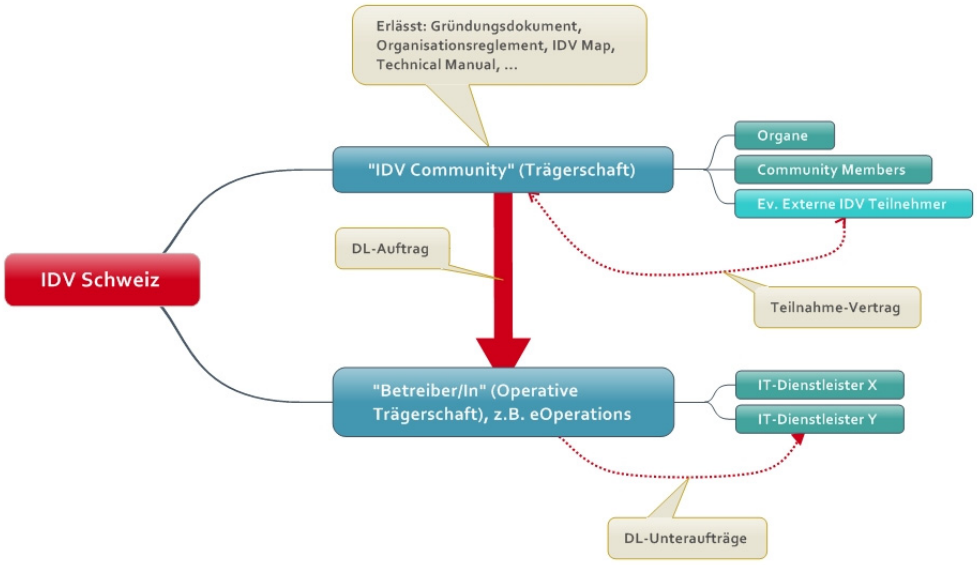
2.2 Organisation nach der Projektphase / Trägerschaft

Die Aufgabe des Projekts IDV besteht darin, einen Identitätsvermittler gemäss den einschlägigen internationalen und nationalen Standards (eCH) zu bauen. Das SECO als Auftraggeberin wird das Ergebnis spätestens zum Zeitpunkt des Projektendes am 31. Dezember 2019 an eine Trägerschaft übergeben müssen. Damit ist eine Organisation gemeint, die den IDV technisch betreibt, ein Service- und Kompetenzzentrum führt und für die Wartung und Weiterentwicklung sorgt. Der Bund signalisierte bisher keine Absichten, den IDV selber zu betreiben.

Das SECO und SIK/eOperations haben gemeinsam den Aufbau einer Trägerschaft durch Kantone, Gemeinden und allenfalls anderen öffentlichen Körperschaften vertieft und dazu eine Vorgehensweise ermittelt. Voraussetzung für die Organisation des Betriebs durch SIK/eOperations Schweiz ist, dass der IDV nachhaltig kostendeckend finanziert werden kann. Wie die Kostenaufteilung sowie ein allfälliger Ausgleich zwischen einer Gruppe von "Pionieren" und später dazu stossenden Behörden aussehen soll, wird bei der Konstituierung der Trägerschaft festzulegen sein.

Wie eine Trägerschaft aufgebaut sein kann, wurde in einer Studie von eJustice.CH untersucht[2]. Laut derselben kommen einfache Rechtsformen für eine Trägerorganisation durchaus in Frage (Verein, Stiftung, einfache Gesellschaft). Eine Variante, die gänzlich ohne "Trägerorganisation" auskommt und allein auf Dienstleistungsverträge mit einer beauftragten Organisation abstützt, wird als besonders vielversprechend dargestellt, sofern eOperations Schweiz gewisse Voraussetzungen erfüllt. Diese Lösung würde es erlauben, auf die Gründung weiterer Organisationen verzichten zu können. Schliesslich stellt die Studie fest, dass sich betreffend gesetzlicher Grundlagen für eine Teilnahme an oder eine Gründung von juristischen Personen durch Gemeinwesen recht grosse Unterschiede zwischen den einzelnen Kantonen, aber auch dem Bund bestehen. Dafür zeigen sich Vorteile für ein pragmatisches Vorgehen ohne "Trägerorganisation", dafür mit Dienstleistungsverträgen.

[2] *Konzept Trägerschaft IDV Schweiz*, Version 0.91 vom 21.12.2017. Die Studie kann per Email beim SECO bezogen werden: markus.pfister@seco.admin.ch



Die Abbildung stammt aus der erwähnten Studie und zeigt die rechtliche Ausgestaltung für IDV Schweiz in der Hauptvariante: Die "Trägerschaft" als gemeinschaftliche Vereinigung (z.B. von Kantonen) beauftragt eine operative Betreiberin, die mit den eigentlichen Leistungserbringern Dienstleistungsverträge unterhält.

Für weitere Details wird auf die Studie von eJustice.CH verwiesen.

2.3 Was IDV Betrieb heisst

IDV Betrieb bedeutet zweierlei:

- Die gesamten IDV Infrastrukturdienste (IDV Broker, Metadata Registry MDR, später evtl. Admin-GUI etc.) werden auf einer produktiven technischen Plattform betrieben, die den Erwartungen und Qualitätsanforderungen der Verbundteilnehmer entspricht. Dafür zuständig ist der sog. technische Betreiber. Eine SLA wird die nötigen Parameter definieren und Bestandteil eines Dienstleistungsvertrags zwischen der Trägerschaft und den Kunden sein;
- Eine Service-Organisation ist Ansprechpartnerin für die verschiedenen Kundengruppen, wie Domänenmanager (Verwalter einer Domäne), RP-Manager, IdP-Manager usw. Die Service-Organisation selbst überwacht die Funktionen des IDV, konfiguriert das System, führt Migrationen durch, prüft ggf. die Einhaltung von Kriterien der IdPs und RPs, betreibt ein Helpdesk, führt Schulungen für Kunden durch etc.

2.4 Langfristige Sicherung des Betriebs

Mit der Entwicklung eines pilotfähigen Identitätsvermittlers (Broker 1.0) sind die technischen Hauptziele des Entwicklungsprojekts IDV erreicht. Nun liegt es an den künftigen Kunden des IDV, diesen als Infrastrukturdienst zu etablieren und den Betrieb langfristig zu sichern.

Heute geht man davon aus, dass in erster Linie die Kantone und Gemeinden als Hauptkunden und -nutzer für den Betrieb der Domänen G2C und G2G aufzukommen haben. Derzeit kann keine abschliessende Aussage über die Rolle des Bundes gemacht werden.

2.5 Übergabe und Migration

Die Übergabe und Migration der IDV Infrastruktur vom Projekt IDV Schweiz an eine Betriebsorganisation beinhaltet die folgenden Aktivitäten:

- Bestimmung eines oder mehrerer Domänen-Manager. Ein Domänen-Manager definiert die Anforderungen an seine IDV-Domäne und die damit verbundenen technischen und organisatorischen Parameter. Darauf aufbauend ergeben sich die weiteren Aufgaben und Schritte;
- Erstellung eines Pflichtenheftes und Beschaffung eines Betreibers für die technischen IDV Infrastrukturdienste, basierend auf den Anforderungen der Domäne(n);
- Aufbau einer Serviceorganisation, die für den reibungslosen organisatorischen Betrieb inkl. Support sowie die Überwachung der IDV Infrastruktur verantwortlich ist. Die Serviceorganisation ist primäre Ansprechpartnerin für den technischen Betreiber und die Domänen-Manager und kann in zentrale Bereiche des IDV Verbundes eingreifen. Ein Geschäftsorganisationskonzept wurde im Rahmen des Projekts IDV Schweiz entwickelt. Darauf aufbauend ist ein Umsetzungsplan zu erstellen, der die bestehenden Organisationsstrukturen und weitere Parameter berücksichtigt. Die Prozesse sind zu dokumentieren und die Organisation ggf. zu zertifizieren. Für bestimmte Tätigkeiten oder Rollen sind Schulungsunterlagen zu erstellen und Schulungen durchzuführen;
- Installation und Inbetriebnahme der IDV Infrastruktur auf die Produktionsumgebung beim technischen Betreiber. Je nach bereits laufenden Pilotanwendungen ist eine Datenmigration mit Tests und Abnahme durchzuführen;
- Falls die unter 1.7 erwähnte Administrations- und Konfigurationsfunktion zum Zeitpunkt der Betriebsaufnahme nicht entwickelt worden ist, muss die Verbundkonfiguration durch einen technischen Experten ausgeführt werden. Das gilt für die allgemeine IDV Infrastruktur wie auch für die Domänen und angeschlossenen Dienste (IdP und RP). Für den Aufbau einer IDV Domäne wäre jeweils ein Domänen-spezifisches Projekt durchzuführen und eine Dienstleistungsvereinbarung mit einem technischen Manager für die IDV Infrastruktur zu erstellen (wahrscheinlich mit dem Ersteller der IDV Infrastruktur).

Die wichtigsten Kostenfaktoren ergeben sich aus den obenstehenden Aufgaben.

Beschreibung	Schätzung
Projektführung für Aufbau, Übergabe und Migration	100 kCHF
Pflichtenheft für den technischen Betrieb basierend auf bestehenden Grundlagen aus dem Projekt IDV Schweiz	50 kCHF
Beschaffung des technischen Betreibers	50 kCHF
Aufbau der Serviceorganisation (Projekt)	100 kCHF
Installation, Migration und Inbetriebnahme IDV	50 kCHF
Unterstützungsleistungen beim Domänen-Aufbau	50 kCHF
Reserve	100 kCHF
Total	**500 kCHF**

Die Schätzung ist sehr rudimentär, da die tatsächlichen Rahmenbedingungen des Aufbaus und der Übergabe derzeit völlig unbekannt sind.

2.6 Betriebskosten

Unabhängig von den Kosten einer Pilotierung (vgl. weiter unten) und denen für die Übergabe und Migration setzen sich die Kosten für den Betrieb der IDV Infrastruktur wie folgt zusammen.

1. *Verwaltungskosten Trägerschaft*. Administration, Marketing, Kommunikation usw.
2. *Serviceorganisation*. Betreuung der IDV Basis-Infrastruktur, Wartung u. Weiterentwicklung, Support, Schulung, Arbeitsgruppen (z.B. Sicherheit, Normen usw.);
3. *Kosten des technischen Betriebs*. Technischer Betrieb und Hosting der IDV Plattformen, insb. für die Kommunikation (PROD-DEMO), das Testing (PROD-TEST), die Integrationsanbindung (PROD-INT) und die eigentliche Produktion (PROD).

Die nachfolgende Zusammenstellung basiert zum einem Grossteil auf einer Studie der FHNW im Rahmen des Geschäftsorganisationskonzepts.

Bereich	Funktion	FTE*	kCHF	Bemerkungen
IDV Management	*Geschäftsführung*	0.8	160	
	M+K	0.5	100	Sales, Presse, Kommunikation, Website
	Rechtliche Unterstützung	0.2	40	Vertragsmanagement, Compliance
	Zentrale Dienste	0.6	120	HR, Sekretariat, Controlling, Finanzen etc.
Business Services	*Domain Account Mgmt*	0.4	80	Domänen Kundenmanagement
	IdP/RP Betreuung	0.6	120	Betreuung und Schulung
Customer Support	*User Support / Helpdesk*	0.5	100	Bearbeitung Kundenprobleme
	Incident Management	0.5	100	Plattform-Probleme, Betriebsstörung
Application Management	*Application Owner IDV*	1	200	Monitoring, Konfiguration, Betrieb sichern
	Product Owner IDV	0.6	120	Anforderungen, Change, Releaseplan, PL
	Security Officer	0.3	60	IT Sicherheit, Governance, Compliance
Platform Operations	*Tech. Betrieb RZ*		500	
	Release / Deployment		50	
Facility Management	*Miete / NK*		50	
Development	*Wartung und Entwicklung***		200	
		TOTAL	**2000**	

* Es wurde eine Vollkostenbetrachtung zugrunde gelegt, die von einem Gesamtaufwand von CHF 200k jährlich pro FTE ausgeht (ungeachtet der Position oder Tätigkeit), inkl. Sozial- und andere Versicherungen sowie Kosten für Arbeitsplatz, Informatik etc.

** vgl. Potential für Weiterentwicklungen weiter oben (Kap. 1.5)

Die geschätzten Gesamtkosten für den Betrieb belaufen sich insgesamt auf rund 2.0 Mio. CHF pro Jahr einschliesslich Wartung und Pflege.

Zu erwähnen ist der Skaleneffekt: Ist der Betrieb einmal initialisiert und aufgenommen worden, so können zusätzliche Nutzerkreise (zusätzliche IDV-Domänen) mit geringen Zusatzkosten aufgebaut werden. Die Schätzungen liegen bei wenigen Zehntausend Franken pro Domäne.

Der Betrag von 2.0 Mio. CHF entspricht einem *jährlichen Kostenanteil von 25 Rappen pro Einwohner/in* (bei rund 8 Mio. Einwohner/innen) über die gesamte Schweiz betrachtet. Diese Art der Kostendarstellung hat sich in diversen Gesprächen mit Interessenvertretern aus Kantonen und Gemeinden als nützlicher Anhaltspunkt erwiesen. Ein künftiges Finanzierungsmodell könnte sich daran orientieren. Anhang B enthält eine entsprechende Modellberechnung als Anhaltspunkt.

Diese Kostenschätzung stellt einen Richtwert dar, der zu überprüfen sein wird.

3 Integrationspilot

3.1 Bedeutung und Signalwirkung

Integrationspilot heisst, dass der IDV Broker 1.0 durch die Entwicklungsfirma (AdNovum) auf der sog. Integrationsplattform PROD-INT professionell betrieben wird, wenn auch mit tieferen SLA-Kriterien als im produktiven Betrieb. Damit können Kantone, Gemeinden und andere sich gemäss der Schnittstellendefinition an den Verbund anschliessen und Identitäten föderieren.

Der Integrationspilot ist mehr als nur ein Testbetrieb, der nach einer gewissen Zeit wieder deaktiviert wird. Im Gegenteil: er nimmt die produktive Einführung des IDV in einer Zeit vorweg, in welcher der definitive technische Betreiber noch bestimmt und die Übergabe der IDV-Infrastruktur (Migration) vollzogen werden muss. Da die projektverantwortliche Organisation SECO die IDV Infrastruktur ab 2020 nicht selber betreiben wird, muss für das SECO zwingend absehbar sein, dass eine Trägerschaft entstehen wird, bevor ein Integrationspilot gestartet werden kann. Für eine Pilotierung unterstützt werden die Domänen G2G und G2C.[3]

Der Pilot hätte eine wichtige Signalwirkung. Kantone und Gemeinden, die noch nicht für den IDV bereit sind, würden Gelegenheit bekommen, sich von der Funktionsweise des IDV zu überzeugen und den Nutzen erlebbar zu machen. Diese Sichtbarkeit wäre ein ideales Werbeinstrument für IDV.

3.2 Organisation

Der Integrationspilot wird durch das Projekt geführt. Die am Pilot beteiligten Parteien sind:

- SECO: Auftraggeber;
- Projektleiter: Betreibt Marketing bei Kantonen, Gemeinden, Anbietern von Behörden-SW usw. Wirbt neue Teilnehmer an, insb. IdP. Führt die Kommunikation innerhalb der Teilnehmer des Integrationspiloten;
- Ersteller: Betreibt Broker 1.0 und die Integrationsplattform PROD-INT zu Bürozeiten. Konfiguriert die Einzelheiten zu jeder Domäne auf Basis von Konfigurationsdateien. Managt alle Domänen des Pilots und ist zuständig für die Registrierung und Integration von IdPs und RPs. Überwacht die korrekte Funktion der IDV Plattform. Nimmt Wartungen am IDV vor. Bietet Unterstützung für Teilnehmer während Bürozeiten;
- Anwendungsverantwortlicher: Führt Befragungen bei den Teilnehmern durch und macht Auswertungen;
- Prozessverantwortlicher: Spezifiziert Rollen und Prozesse innerhalb der Service-Organisation und in der Aussenwirkung zu den Teilnehmern, insb. Domänen-Manager sowie Anbieter von IdPs und RPs. Erstellt ein Organisationshandbuch für die künftige Trägerschaft resp. Service-Organisation sowie ein Prozesshandbuch für den künftigen Betreiber. Für den Pilotbetrieb, der ein Minimalbetrieb ist, könnte die Rolle des Prozessverantwortlichen ggf. ausgelassen werden;
- Kantonale Behörden oder solche von Gemeinden: Primäre Pilotteilnehmer, bieten einen IdP, einen RP oder beides an;
- (optional) Private: Sekundäre Pilotteilnehmer, bieten einen IdP an.

[3] *G2G (Government-to-Government):* Unterstützt die Vernetzung unter den Behörden, indem digitale Identitäten der Mitarbeiter föderiert werden. Mitarbeiter einer Behörde verwenden ihren angestammten IdP (Anmeldedienst), um sich bei angeschlossenen Partnerbehörden für zugriffsgeschützte Dienste anzumelden.
G2C (Government-to-Citizen): Unterstützt die Anmeldefunktion von öffentlichen E-Government-Diensten für Private und Unternehmen. Die Benutzer verwenden einen IdP (Anmeldedienst) ihrer Wahl, um sich einzuloggen.

3.3 Pilotanwendungen (Kandidaten)

Das IDV Architecture Board ist ein Gremium aus Vertretern von kantonalen, städtischen und privaten Organisationen sowie solchen des Bundes. Im Sinne einer stillen Vereinbarung haben die Teilnehmer des Boards im Frühjahr 2016 unverbindlich zugesagt, dereinst eine Pilotanwendung mit dem IDV durchzuführen.

Die im Anhang aufgeführten Use Case Beschreibungen wurden von den bezeichneten Organisationen des Architecture Boards selbst erstellt. Es handelt sich um Anwendungsfälle, die möglicherweise in einem IDV Pilot umgesetzt werden können. Aus heutiger Sicht ist nicht damit zu rechnen, dass die aufgeführten Anwendungsfälle alle pilotmässig umgesetzt werden. Ein Ansturm auf den IDV-Pilotbetrieb, sollte ein solcher aufgenommen werden, ist derzeit nicht zu befürchten. Viel wahrscheinlicher ist, dass sich zu Beginn eher wenige Kantone und Gemeinden zu einer Pilotierung entscheiden und die meisten anderen sich als Beobachter davon überzeugen lassen, dass der IDV in der Tat funktioniert und verfügbar ist. Es ist davon auszugehen, dass sich die meisten Kantone und Gemeinden erst später, im Rahmen des ordentlichen Betriebs, an den IDV anschliessen.

3.4 Kosten für den Integrationspiloten

Durch den Auftraggeber SECO ist sichergestellt, dass unter den bereits genannten Voraussetzungen ein Integrationspilot per 1.1.2019 durchführbar ist. Die Pilotierung kann ohne zusätzliche Entwicklungsarbeiten beginnen, sodass sich die Kosten auf die betrieblichen Aspekte beschränken.

Die Kostenpositionen für den Betrieb eines Integrationspiloten für die Zeit vom 1.1.2019 bis 31.12.2019 sind:

- Administrative Arbeiten, Vorbereitung mit Kunden usw.;
- Betrieb der *Integrationsplattform* PROD-INT, inkl. Überwachung und allfälliges Bug Fixing;
- *Usability Prüfungen* zur Sicherstellung einer benutzergerechten IdP-Auswahl, Attributbestätigung usw.;
- Je nach Anforderung der Pilotteilnehmer: Erarbeitung von Baseline Requirements und Practice Statements, um einen Vertrauensraum für die Domäne zu etablieren (vgl. 1.4);
- Projektleitung zu 60%.

Laut einer ersten Schätzung beläuft sich der Gesamtaufwand für die Integrations-Pilotierung auf rund 520'000 CHF für Betrieb, Support und Projektleitung bei einer Betriebsdauer von 12 Monaten. Nicht einbezogen sind Projekt-, Koordinations- und Integrationskosten, welche bei den Teilnehmern selbst anfallen. Diese sind von jedem Teilnehmer vollständig selbst zu tragen.

Mit diesem Betrag ist ein Minimalbetrieb möglich. Fehlerbehandlung und Support wird nur zu Bürozeiten angeboten. Die Betriebsorganisation besteht aus den Projektteilnehmern (Entwickler, Projektleiter) und der schlussendliche Betreiber wäre voraussichtlich noch nicht bekannt. Die Organisations- und Prozesskonzepte sind nicht implementiert, die Trägerschaft würde diese später umsetzen müssen.

Die folgenden Arbeiten betreffen den Aufbau des operativen Betriebs und sind im Minimalbetrieb nicht enthalten:

- Umsetzung der Einführungsmassnahmen für eine Betriebsorganisation, basierend auf dem Organisations- und Prozesskonzept vom 26.04.2017. Erstellung eines Organisationshandbuchs, Kommunikations- und Schulungsunterlagen;
- Umsetzung der Einführungsmassnahmen für die Betriebsprozesse, basierend auf dem Organisations- und Prozesskonzept vom 26.04.2017. Erstellung eines Prozesshandbuchs;
- Erarbeitung eines Attribut-Kataloges für die Kantone und Gemeinden (G2G Domäne);
- Beschaffung des technischen Betreibers der Produktivplattform;
- Migration vom Pilotsystem auf die Produktivplattform.

4 Voraussetzungen für den Pilotstart

Es wurden folgende Vorgehensweisen geprüft:

- Befristete Pilotierung bis Ende 2019 durchführen und nötigenfalls beenden, wenn bis dahin keine Trägerschaft aufgebaut werden konnte;
- Pilotierung nur auf Basis von eindeutigen Signalen der Bereitschaft seitens der Kantone und Gemeinden, sich an den Kosten zu beteiligen und die Trägerschaft zu etablieren.

Die erste Variante setzt die Pilotteilnehmer einem Risiko aus, da eine Pilotierung meistens nicht nur Testcharakter hat, sondern einem zukünftigen Regelbetrieb vorangeht. Mit dem Start des Integrationspiloten würden die Teilnehmer darum erwarten, dass IDV auch nach der Pilotphase dauerhaft als Infrastrukturdienst zur Verfügung steht.

Daraus ergeben sich aus Sicht des SECO als projektverantwortliche Organisation die nachfolgenden Bedingungen, um einen IDV Integrationspilot zu starten:

- Eine genügend hohe Zahl von Interessenten für den IDV signalisiert die Bereitschaft, sich organisatorisch und finanziell am Aufbau einer Trägerschaft zu beteiligen. Die Trägerschaft soll nach Möglichkeit Anfang 2019 bereitstehen;
- Die Trägerschaft einigt sich auf ein Finanzierungsmodell, das die Kosten für den Aufbau und den operativen Betrieb ab 2019 sicherstellt;
- Eine genügend hohe Zahl von Interessenten für den IDV ist bereit, sich an den Kosten des Integrationspiloten zu beteiligen;
- Mit den Pilotteilnehmern kann eine Vereinbarung abgeschlossen werden, welche die Bedingungen hinsichtlich allfälliger frühzeitiger Beendigung im gegenseitigen Einvernehmen regelt.

5 Planungsvorschlag

Datum	Aktion
April 2018	Erhebung des tatsächlichen Bedarfs für IDV Schweiz in einem Schreiben des SECO und E-Government Schweiz an die Kantone und Gemeinden.
01.07.2018	**Meilenstein SIK:** Gründung eOperations Schweiz (vorbehältlich Beschlüsse der SIK-Gremien).
Q3/2018	Auswertung der Umfrage ist beendet.
Falls Absichtserklärungen in genügender Zahl vorliegen und sowohl Pilot als auch der nachfolgende operative Betrieb finanziell gesichert sind:	
Q3/2018	Ausarbeitung einer Absichtserklärung mit eOperations Schweiz und Projektvereinbarung zur Zusammenarbeit während Pilotphase.
Q4/2018	Eine Trägerschaft hat sich unter Federführung des SECO mit Unterstützung von eOperations und evtl. E-Government Schweiz konstituiert. SECO wird nicht der Trägerschaft angehören.
Q1/2019	Integrationspilot startet.
Q2/2019	Weitere staatliche Akteure sind als Nutzer von IDV akquiriert, definitiver Entscheid zur Aufnahme des Produktivbetriebs liegt vor.
Bei positivem Entscheid für die Aufnahme des Produktivbetriebs:	
Q2/2019	Beschaffung des technischen Betreibers durch eOperations beginnt.
Q4/2019	Beschaffung des technischen Betreibers durch eOperations ist abgeschlossen, Vertrag mit e-Operations liegt vor.
01.12.2019	Übergabe / Migration von PROD-INT auf PROD (produktive Plattform beim technischen Betreiber).
31.12.2019	Projektschluss und Übergabe des IDV an die Trägerschaft.
01.01.2020	Start IDV Produktivbetrieb unter Schirmherrschaft der Trägerschaft.

Anhang A: Personen und Kontakte

Funktion	Organisation	Vertreter
Koordination Umsetzung Schwerpunktplan	Geschäftsstelle E-Government Schweiz	Cédric Roy, Chef de la Direction opérationnelle cedric.roy@isb.admin.ch, +41 58 469 7051
		Marcel Kessler, PL Schwerpunktplan E-Government marcel.kessler@egovernment.ch, +41 58 460 5293
Projekt-verantwortliche Organisation und Auftraggeber	Staatssekretariat für Wirtschaft SECO	Martin Godel, Leiter KMU-Politik martin.godel@seco.admin.ch, +41 58 462 2961
		Markus Pfister, Leiter E-Government für KMU markus.pfister@seco.admin.ch, +41 58 462 3832
Umsetzung eOperations Schweiz	Schweizerische Informatikkonferenz SIK	Urs Jermann, Geschäftsleiter SIK urs.jermann@sik.ch, +41 31 320 00 00
		Daniel Arber, Projektleiter eOperations daniel.arber@sik.ch, +41 79 292 62 23
Ersteller	AdNovum Informatik AG	Marcel Raymann, marcel.raymann@adnovum.ch
Projektleitung	Zweiacker & Partner AG	Marc Zweiacker, marc.zweiacker@zweiacker.com
Projektausschuss	SECO	Martin Godel, martin.godel@seco.admin.ch
	GS WBF	Roger Hertach, roger.hertach@gs-wbf.admin.ch
	ISB	Lars Minth, lars.minth@isb.admin.ch
	BAG	Salomé von Greyerz, salome.vongreyers@bag.admin.ch
	SIK	Urs Jermann, urs.jermann@sik.ch
	Kanton Fribourg	Stéphane Schwab, stephane.schwab@fr.ch
IDV Architecture Board	Kanton GE	Roland Burgniard, roland.burgniard@etat.ge.ch Gianfranco Moi, gianfranco.moi@etat.ge.ch Jean-Marc Mottet, jean-marc.mottet@etat.ge.ch
	Kanton VD	Taymaz Babaki, taymaz.babaki@vd.ch
	Kanton BE, KAIO	Jean-Luc Froideveaux, jean-luc.froidevaux@fin.be.ch Marcus May, Marcus.May@bedag.ch
	Kanton BS	Hansjörg Hänggi, hansjoerg.haenggi@bs.ch
	Kanton AG	Julius Geissbühler, julius.geissbuehler@ag.ch
	Kanton ZH	Leo Stucky, leo.stucky@kitt.zh.ch Lukas Steudler, lukas.steudler@sk.zh.ch
	Kanton ZG, AIO	Rudolf Gisler, rudolf.gisler@zg.ch
	Stadt Zürich, OIZ	Giovanni Groppo, Giovanni.Groppo@zuerich.ch
	Stadt Bern	Roland Brechbühl, Roland.Brechbuehl@BERN.CH
	IG ICT Zürcher Gden	Andrea Mazzocco, andrea.mazzocco@igict.ch
	Polizeitechnik & Informatik	Martin Page, Martin.Page@pti-mail.ch
	EFD, ISB	Marc Heerkens, Marc.Heerkens@isb.admin.ch Torsten Gruoner, Torsten.Gruoner@isb.admin.ch
	HIN (Health Info Net)	Christian Greuter, christian.greuter@hin.ch Aaron Akeret, aaron.akeret@hin.ch
	WBF ISCeco	Christian Ludt, christian.ludt@isceco.admin.ch

Anhang B: Einfaches Preismodell als Anhaltspunkt

Die Projektleitung und das SECO sind in der Vergangenheit häufig angefragt worden, was der Betrieb des IDV die Beteiligten kosten wird. Zum Zeitpunkt dieses Berichts ist nicht geklärt, wie sich eine künftige Trägerschaft zusammensetzen wird. Unter diesen Voraussetzungen ist es praktisch unmöglich, ein Preismodell zu entwickeln, das die zukünftige Konstellation der Kostenträger korrekt abbildet.

Unter der Vermutung, dass die Kantone eine zentrale Rolle bei der Trägerschaft einnehmen werden, wurde ein einfaches Preismodell als Anhaltspunkt ausgearbeitet. Die folgende Tabelle zeigt die Kostenanteile der einzelnen Kantone auf, würden diese den Betrieb allein finanzieren und einen Verteilschlüssel anwenden, der sich an der Bevölkerungsstärke orientiert.

Diese Information ist zur Kostenschätzung gedacht und stellt keinen Versuch dar, die Entscheidung der Kantone bezüglich der Trägerschaft und eines möglichen Verteilschlüssels vorwegzunehmen. Insbesondere ist davon auszugehen, dass nicht alle Kantone von Beginn weg an der Trägerschaft teilnehmen. Dadurch können die effektiven Beiträge von den angegebenen Beiträgen abweichen.

Alternative Modelle, die eine andere Zusammensetzung der Trägerschaft oder einen anderen Verteilschlüssel vorschlagen, sollen damit nicht ausgeschlossen werden.

Kanton	Einwohner	Anteil %	Anteil CHF		Kanton	Einwohner	Anteil %	Anteil CHF
ZH	1'488'000	17.666	353'318		SH	81'000	0.962	19'233
BE	1'026'500	12.187	243'737		AR	55'000	0.653	13'059
LU	403'000	4.785	95'690		AI	16'000	0.190	3'799
UR	36'000	0.427	8'548		SG	502'500	5.966	119'316
SZ	156'000	1.852	37'041		GR	197'500	2.345	46'895
OW	37'500	0.445	8'904		AG	662'000	7.859	157'189
NW	42'500	0.505	10'091		TG	270'000	3.206	64'110
GL	40'000	0.475	9'498		TI	354'500	4.209	84'174
ZG	124'000	1.472	29'443		VD	785'000	9.319	186'394
FR	312'000	3.704	74'083		VS	339'000	4.025	80'494
SO	269'500	3.199	63'991		NE	178'500	2.119	42'384
BS	193'000	2.291	45'827		GE	495'500	5.883	117'654
BL	285'500	3.389	67'791		JU	73'000	0.867	17'333

Die Tabelle wurde unter der Annahme erstellt, dass die jährlichen Betriebskosten sich auf 2 Mio. CHF belaufen. Darin enthalten sind Wartung, Support und eine massvolle Weiterentwicklung des IDV, um mit dem technologischen Wandel schrittzuhalten.

Anhang C: Stimmen zum Identitätsverbund

«Trotz allen anderen Initiativen im Tätigkeitsbereich des Identitätsverbunds, seien es die E-ID des Bundes, private schweizerische Initiativen wie SuisseID oder SwissID oder internationale und kantonale Initiativen, entspricht das Projekt IDV einem Bedürfnis. »

Der Verbund soll nicht nur eine technische Lösung bieten, sondern auch als Enabler fungieren, Vertrauensbereiche und die damit zusammenhängenden Regeln festlegen, damit nicht nur das Identitäts- sondern auch das Zugangsmanagement vereinfacht wird.

Der Kanton Genf verwaltet derzeit die Identitäten für Polizistinnen und Polizisten aus anderen Kantonen, die die Genfer Polizei bei Einsätzen unterstützen. Mit einem Vertrauensbereich «Schweizer Polizei» beispielsweise könnte diese Mehrfachverwaltung vermieden werden und Polizistinnen und Polizisten aus jedem beliebigen Kanton hätten Zugang zu den Informationssystemen der Bundespolizei oder anderer Kantonspolizeien.

Roland Burgniard , Chef de service – Gestion des accès et des identités, République et canton de Genève

Aus dem Französischen übersetzt

« Die IG ICT Zürcher Gemeinden beurteilt das Vorhaben IDV Schweiz als unabdingbare Voraussetzung, um den Durchbruch bei der digitalen Verwaltungsführung auf allen föderalen Ebenen zu ermöglichen. »

Bürgerinnen und Bürger sowie die Verwaltungen warten auf die Erleichterungen, die eine Verwendung von bereits vorhandenen Identitäten für alle Beteiligten bringen werden. Die IG ICT unterstützt das Vorhaben seit Beginn für ihre Mitglieder, die Gemeinden und Städte im Kanton Zürich. Sie wird auch die Umsetzung im Rahmen ihrer Möglichkeiten gerne unterstützen..

Andrea C. Mazzocco, Präsident IG ICT Zürcher Gemeinden

Das Projekt des Identitätsverbunds Schweiz soll allen Verwaltungsmitarbeitenden sowie allen Bürgerinnen und Bürgern ermöglichen, sich mit ihrer elektronischen Identität auf einheitliche und sichere Weise bei allen im IDV-Ökosystem vorhandenen elektronischen Diensten anzumelden. Es hat zwei gewichtige Vorteile:

Erstens können die Nutzerinnen und Nutzer ein einziges Konto verwenden, um auf die Dienstleistungen der verschiedenen Verwaltungen (auf Gemeinde-, Kantons- und Bundesebene) zuzugreifen; so kann beispielsweise ein Nutzer, der in Lausanne im Kanton Waadt wohnt, in Genf arbeitet und ein Ferienhaus im Wallis besitzt, sich über dasselbe Konto mit allen Online-Dienstleistungen der drei Verwaltungen verbinden.

Zweitens muss die Verwaltung für Nutzerinnen und Nutzer, die bereits ein Konto der erforderlichen Vertrauensstufe besitzen, kein Registrierungsverfahren mehr durchführen. Es wird auch nicht mehr nötig sein, viele verschiedene «Peer-to-Peer»-Verbünde mit einer grossen Anzahl an Identitätsausstellern (Verwaltung oder Privatsektor) zu verwalten.

« Eine breite Nutzung des IDV wird zur erfolgreichen Entwicklung und zur Förderung des E-Governments in der Schweiz beitragen... »

Taymaz Babaki, Chef de Programme GDIA, Direction des systèmes d'information (DSI) - Canton de Vaud

Aus dem Französischen übersetzt

« Das Konzept des Identitätsverbundes (IDV) mit einem staatlichen, zentralen Broker passt hervorragend in die heterogene, föderale Landschaft im schweizerischen E-Government. »

Gerade weil die technischen Lösungen einer eID am freien Markt entwickelt und angeboten werden sollen und die Wahrscheinlichkeit gross ist, dass es mehrere solchen Lösungen geben wird, müsste eine zentrale Identitäts-Vermittlerstelle in staatlicher Hand aufgebaut werden. Nur so können Gemeinden, Städte und Kantone davon ausgehen, dass sie dereinst nur an eine Lösung (an den Broker) eine einzige Schnittstelle einführen und betreiben müssen.

Roland Brechbühl, Programmleiter E-Government, Stadtkanzlei Stadt Bern

« IDV, respektive die darin realisierte Brokerlösung, ist unsere Antwort auf die ständig steigende Vielfalt an IDP's auf dem Markt und damit dem Druck diese für den Zugriff auf unsere Dienstleistungen verfügbar zu machen. »

Mit nur einem Interface kann der Aufwand dafür sehr kostengünstig realisiert werden. Bei gleicher oder sogar höherer Sicherheit.

Hansjörg Hänggi, Kanton Basel-Stadt, Fachstelle E-Government

Anhang D: Pilot-Anwendungsfälle (Kandidaten)

Die Liste ist das Ergebnis einer Befragung der am Projekt beteiligten Kantone und Organisationen zu Beginn des Projekts im Jahr 2016 und wurde seither nicht aktualisiert. Die Liste soll dem Leser als Anhaltspunkt dienen, um die Absichten in Sachen Pilotierung verstehen zu können. Es sind Ideen und man darf sie nicht als verbindliche Zusagen missverstehen.

Erläuterungen zur Tabelle:

Wer Ideengeber / Organisation, die den Pilotvorschlag eingebracht hat
Use Case Beschreibung des Pilotvorschlags
Betroffene Die vom Pilot betroffenen Organisationen gem. Ideengeber
Typ Involvierte politische Ebenen
Rolle IdP = Anmeldedienst / RP = Webdienst / AA = Attribute Authority

Nr	Wer	Use Case	Betroffen	Typ	Rolle
1	HIN (Health Info Net)	Asylsuchende werden zuerst in einer Kollektivunterkunft des Bundes und später in Kollektivunterkünften des Kantons untergebracht. Nach Abschluss des Asylverfahrens werden die Personen, die in der Schweiz bleiben dürfen, einer Gemeinde zugewiesen. Die medizinische Versorgung wird auch in diesem Kontext durch Gesundheitsfachpersonen und/oder deren Einrichtungen sichergestellt. Bei den auszutauschenden Daten handelt es sich um sensible Daten, an welchem mehrere IDP (Admin PKI, SuisseID, HIN ID) beteiligt sind. Mit dem IDV-Pilot soll ein PoC für die IDP-übergreifende Authentisierung von Akteuren aus den Bereichen eHealth und eGov umgesetzt werden.	Mitarbeiter Gemeinde Mitarbeiter Kanton (Migrationsamt) Mitarbeiter Bund (Migration) Gesundheitsfachperson	übergreifend Bund Kanton und Gemeinden	IdP, RP
2	HIN	HIN als eID Provider für Gesundheitswesen	Gesundheitsfachpersonen		IdP
3	AG	elektronische Umzugsmeldung Online Meldung durch Einwohnende des Kantons Aargau. Restliche Abwicklung in den bestehenden Systemen durch Angestellte von Gemeinden (Kanton Aargau, evtl. andere Kantone). Kanton Aargau: Rolle Service Provider, Bezug der (nachgewiesenen) Identitäten durch IDV.	Einwohnende der ganzen Schweiz	AG und Gemeinden	RP
4	AG	elektronischer Baugesuchs-Prozess Online-Einreichung des Baugesuchs durch Private, Firmen oder Architektur-Büros. Online-Abwicklung des Verfahrens . Einzelne Schritte werden durch Fachstellen abgewickelt. Kanton Aargau: Rolle Service Provider, Bezug der (nachgewiesenen) Identitäten durch IDV. Nicht benötigt werden Identitäten, die schon vorhanden sind: alle Angestellten des Kantons Aargau sowie einige Angestellte von Gemeinden im Kanton Aargau.	Gesuchs-"Inhaber": Bauherren, Grundstückbesitzer, Architekturbüros. Mögliche Herkunft der Identitäten: schweizweit und weltweit Sachbearbeitende und Fachstellen von Gemeinden und Kanton, sowie Kommissionen von Gemeinden oder Kanton mit Beratungs-, Entscheidungs- oder Einsprache-Befugnis, z.B. Energieberatungsstellen.	AG und Gemeinden	RP
5	AG	MedBBP Medizinischer Berufsausübungs- und Betriebsbewilligungsprozess. Abwicklung der Bewilligungs-Prozesse Online. In einer zweiten Phase Eingabe der Anträge elektronisch durch medizinisches Personal. Kanton Aargau: Rolle Service Provider, Bezug der (nachgewiesenen) Identitäten durch IDV. Nicht benötigt werden Identitäten, die schon vorhanden sind: alle Angestellten des Kantons Aargau.	Elektronische Identitäten von Personen im Medizinalbereich (Register MedReg des Bundes, später evtl. NaReg)	AG intern	RP

Nr	Wer	Use Case	Betroffen	Typ	Rolle
6	AG	Broker erschliesst primär den Onlineschalter. Damit werden Onlineschalter integrierte Services wie z.B Lotteriebewilligung, Lehrstellennachweis, Fischereikarten zugänglich. Benötigte Attribute:Persistent ID, Vorname, Nachname, Email (opt), Geschlecht, Mobile, eCH-0010-mailaddress	Einwohner	AG intern	RP
7	BE	Föderierung Identität BE-Login mit Gemeinden des Kantons. Pilot mit der Stadt Bern.	Bürger/ Unternehmen	BE und Stadt Bern	IdP, RP
8	BE	Upgrade BE-Login auf höheres Authentisierungslevel, z.B. via Bezug von SuisseID Identity-Provider	Bürger/ Unternehmen	BE und Stadt Bern	IdP, RP
9	BS	Anmeldung an Behördenkonto und online Dienstleistungen des Kantons - Zugriff auf persönliche laufende Geschäfte - Abhängig von Authentisierungsstärke (-qualität) - Abwicklung von geschützten Onlinegeschäften	Bürger	Kt. BS	RP
10	GE	A Swiss citizen currently resident in the State of Geneva and formerly resident in the State of Vaud would like to submit a tax return through Geneva's online services internet portal using an ID and related credentials registered in Vaud's on-line services internet portal. (to be validated with the business units at the state of Geneva)	Swiss citizen	GE and VD	IdP, RP
11	GE	A Geneva policeman who has a Geneva ID and related credentials to carry out his daily work would like to use them to connect to applications of the Federal Police through the SSOPortal. (to be validated with the business units at the state of Geneva)	Geneva policemen	GE, Bund	IdP
12	VD	Besoin émit par la FVE : Accéder via leur compte FVE fédéré à l'information relative aux permis de travail (Id, existence, validité, durée,…) des citoyens suisses, des frontaliers, des résidents étrangers et des réfugiés politique se trouvant dans les référentiels de l'ACV, afin de pouvoir contrôler les informations envoyées par l'entrepreneur et de valider les permis de travail transmis. Exemple concret : « Une personne, en charge de l'administration et de la validation des demandes de cartes professionnelles à la FVE, utilise son identité fédérée pour accéder au registre regroupant les permis de travail de l'ACV (à confirmer) afin de comparer celui reçu par une entreprise avec celui contenu dans le registre officiel ».	Fédération Vaudoise des Entrepreneurs (FVE / Projet « Cerbère » (lutte contre le travail au noir)) – Personnel administratif	VD intern	IdP, RP
13	VD	Besoin émit par la FVE : Accéder aux services fournis par l'ACV (cyberadministration et autres) en utilisant leur compte FVE fédéré (compte « Myentrepreneurs ! » SuisseID actuellement déjà géré par SwissSign). L'accès devant être donné sur la base du niveau de trust de l'identité et des attributs renseignés (ABAC – authentification FIS) ainsi que sur le(s) rôle(s) de l'utilisateur définis dans le système IAM de l'ACV (RBAC – autorisation ACV). Exemple concret : « Un entrepreneur utilise son identité fédérée SuisseID pour accéder à ACTIS, l'application de saisie, de traitement, de suivi des demandes de permis de construire afin d'accéder au statut du dossier de construction dont il est le mandataire ».	FVE – Entrepreneurs et tous leurs employés membres de la FVE (citoyens suisses, frontaliers, ressortissants étrangers et réfugiés politique travaillant en Suisse.	VD intern	IdP, RP
14	VD	Besoin de la DFJC : Use cases à définir (réunion avec le DFJC planifié. Use case détaillé sera élaboré suite à cette rencontre). UC haut niveau : - Permettre une fédération des identités délivrées dans le domaine de l'éducation pour accéder aux prestations des cantons et de la Confédération. - Permettre le lien entre le compte délivré dans le cadre de l'éducation (écoles & hautes écoles) et une identité numérique délivrée par les cantons / la Confédération.	Département de la Formation, de la Jeunesse et de la Culture (DFJC)	VD intern	IdP, RP
15	VD	Accéder aux prestations de cyberadministration fournies par l'ACV en utilisant leur nouveau compte fédéré. Permettre à une personne qui a créé un compte dans un canton (Vaud) de l'utiliser pour se connecter et accéder aux prestations d'une commune (du même canton ou d'autres	Citoyens / Résidents suisses (particuliers, représentants d'entreprises, de	VD intern, auf alle Ebenen ausbaubar	IdP, RP

Nr	Wer	Use Case	Betroffen	Typ	Rolle
		cantons), d'un autre canton (Genève, Zurich, etc.) ou de la Confédération. Exemple concret : « Un usager en possession d'une identité numérique dans le canton de Vaud a un permis de pêche professionnel l'autorisant à pêcher uniquement sur sol vaudois. Désireux d'aller pêcher (ponctuellement) dans les eaux d'un canton limitrophe sur le lac de Neuchâtel (NE, FR), il aimerait utiliser son compte vaudois pour accéder à la prestation sur Fribourg et demander son permis de pêche (une autorisation de pêche)».	communes ou de partenaires) Frontaliers (travaillant en Suisse) Résidents étrangers ou réfugiés en Suisse		
16	VD	Permettre à un cyber-usager qui a déjà un compte dans un canton, sur la base d'un trust level requis minimum, de propager son compte afin d'en créer un dans un autre canton, sans avoir à suivre à nouveau la procédure de délivrance d'une identité numérique. Exemple concret : « Un usager ayant une identité numérique délivrée par le canton de Vaud souhaite déménager dans un autre canton. Il doit accéder à un certain nombre de prestations offertes par le nouveau canton. Il n'a pas besoin de re-suivre la procédure de délivrance d'une identité numérique dans le nouveau canton si celui qu'il possède dans le canton de Vaud satisfait aux exigences (Trust) du nouveau canton. L'usager peut alors de connecter sur la plate-forme du nouveau canton et créer un compte en utilisant (en propageant) celui qui lui a été délivré par les autorités Vaudoises. Une fois son compte créer dans le nouveau canton, l'usager peut utiliser ce compte afin : - Annoncer son changement d'adresse au service des automobiles et de la navigation de son nouveau canton de domicile (modification des permis de conduire et de circulation/navigation). - Annoncer ses enfants scolarisés au personnel enseignant et aux autorités scolaires de la nouvelle commune (arrivants). - Etc. ».	Résidents cyber-usager	VD und andere Kantone	IdP, RP
17	VD	Use case en cours de définition. Un employé de l'administration cantonale vaudoise se connecte à des applications de la confédération pour ses activités professionnelles en utilisant son ID délivré par le canton de Vaud. Le système de la confédération identifie le compte comme ayant un trust suffisant et ayant comme attribut « employé du canton de Vaud » et lui permet d'accéder aux applications autorisées.	Employé cantonal	VD	IdP
18	ZG	ZUGLOGIN Benutzerkonto	Einwohner	übergreifend	IdP
19	ZH	Die Bürgerinnen und Bürger können mit ihren Konten aus den Gemeindeauftritten (‚Bürgerkonto') die Angebote des Kanton (via Plattform ZHservices) oder weiterer Kantone nutzen (‚G2C').	Bürgerinnen und Bürger	ZH und Gemeinden	IdP, RP
20	ZH	eEinbürgerungen: Der Ablauf nach (neuem) Gesetz und Verordnung wird eGovernment-tauglich in einem Einstieg und Workflow umgesetzt – Die Bürgerinnen und Bürger können mit ihren Konten aus den Gemeindeauftritten (‚Bürgerkonto') das Angebot nutzen, der Workflow , umfasst alle 3 Ebenen (Gemeinde, Kanton, Bund)	Bürgerinnen und Bürger	ZH und Gemeinden	IdP, RP
21	ZH Gemeinden	Die Gemeinden des Kantons Zürich können sich an folgenden Anwendungen/Portalen mit Ihren Gemeinde-Credentials authentifizieren (‚G2G') im Kanton: ARTS, POLIS, MIGEK, GVZ beim Bund: SSO-Portal, INFOSTAR, ZEMIS	Mitarbeitende der Gemeinden des Kt. ZH	übergreifend Gde, ZH, Bund	IdP
22	WBF	Employees of administration departments of cantons and municipalities need to access protected federal IT systems. Employees authenticate through IDPs of their canton or municipality. Ideally, the accessed IT system can derive further access rights from attributes passed on by the IDP. Main goal(s): - ensure that user is still employed at canton / municipality - externalize / delegate user management and authentication of employees of administration departments	Employee of administration of canton or municipality	übergreifend Gde, ZH, Bund	IdP, RP