# eCH-0224 – Vermittlerbasierte Identity Federation Architekturmodelle

| | |
|---|---|
| **Name** | Vermittlerbasierte Identity Federation Architekturmodelle |
| **eCH-Nummer** | eCH-0224 |
| **Kategorie** | Standard |
| **Reifegrad** | Definiert |
| **Version** | 1.0 |
| **Status** | Genehmigt |
| **Beschluss am** | 2020-06-04 |
| **Ausgabedatum** | 2020-06-05 |
| **Ersetzt Version** | - |
| **Voraussetzungen** | eCH-0107 V3.0, eCH-0170 V2.0, eCH-0219 V1.0 |
| **Beilagen** | - |
| **Sprachen** | Deutsch (Original), Französisch (Übersetzung) |
| **Autoren** | Fachgruppe IAM<br><br>Annett Laube-Rosenpflanzer, BFH TI, annett.laube@bfh.ch<br>Marc Kunz, BFH TI, marc.kunz@bfh.ch<br>Gerhard Hassenstein, BFH TI, gerhard.hassenstein@bfh.ch<br>Bojan Leimer, BFH TI, bojan.leimer@bfh.ch |
| **Herausgeber / Vertrieb** | Verein eCH, Mainaustrasse 30, Postfach, 8034 Zürich<br>T 044 388 74 64, F 044 388 71 80<br>www.ech.ch / info@ech.ch |

## Zusammenfassung

Dieser Standard definiert vermittlerbasierte Architekturmodelle für Identity Federation Systeme im E-Government. Anhand von verschiedenen Anwendungsfällen und den Szenarien G2C, G2G und G2B wird gezeigt, wie die verschiedenen Anforderungen, insbes. zum Schutz der Privatsphäre und Vertraulichkeit, die Auswahl eines Identity Federation Modells beeinflussen. Die möglichen Vermittlermodelle werden detailliert, aber technologieunabhängig beschrieben.

# Inhaltsverzeichnis

**Zusammenfassung** ..... **1**
**Hinweis** ..... **3**
**1 Status** ..... **4**
**2 Einleitung** ..... **4**
**2.1 Ziel des Dokuments** ..... **4**
**2.2 Einordnung** ..... **5**
**2.3 Anwendungsbereich** ..... **5**
**2.4 Zielgruppe** ..... **6**
**2.5 Abgrenzung** ..... **6**
**2.6 Normativer Charakter der Kapitel** ..... **7**
**3 Überblick Identity Federation** ..... **8**
**3.1 Vertrauen** ..... **9**
**3.2 Vertraulichkeit** ..... **10**
**3.3 Session Handling** ..... **11**
3.3.1 Single Sign-on (SSO) ..... 11
3.3.2 Single Logout (SLO) ..... 12
**4 Szenarien im E-Government** ..... **13**
**4.1 Government to Citizen (G2C)** ..... **13**
**4.2 Government to Government (G2G)** ..... **13**
**4.3 Government to Business (G2B)** ..... **14**
**5 Anwendungsfälle** ..... **15**
**5.1 Reine Authentifizierung** ..... **15**
5.1.1 Unabhängige E-Identities ..... 15
5.1.2 Verlinkte E-Identities ..... 15
**5.2 Authentifizierung mit Attributübergabe** ..... **15**
5.2.1 Lebensdauer der Attributwerte ..... 16
5.2.2 Anzahl der Quellen ..... 16
5.2.3 Datenherkunft ..... 16
5.2.4 Qualität der Attribute ..... 16
**5.3 Verwendete technischen Identifikatoren in den Anwendungsfällen** ..... **17**
5.3.1 Verteilter Identifikator (Distributed ID) ..... 17
5.3.2 Relying Party gebundener technischer Identifikator (Persistent ID) ..... 17
5.3.3 Einmaliger zufälliger technischer Identifikator (Transient ID) ..... 17
**6 Anforderungen** ..... **19**
**6.1 Anforderungen an das föderierte IAM-System** ..... **19**
**6.2 Anforderungen des Stakeholders: Leistungsbezüger** ..... **20**
**6.3 Anforderungen des Stakeholders: Leistungserbringer** ..... **22**
**6.4 Anforderungen des Stakeholders: Führung** ..... **24**
**7 Auswahl Identity Federation Modell** ..... **25**
**7.1 Einfluss der Anforderungen** ..... **25**
**7.2 Einfluss der Szenarien** ..... **28**
**7.3 Nicht-vermittlerbasierte Systeme** ..... **28**
**7.4 Vermittler Double Blinding** ..... **29**
**7.5 Vermittler Offene Quellen** ..... **30**

**7.6 Vermittler Vertraulichkeitsschutz ..... 32**
**8 Vermittlermodelle ..... 34**
**8.1 Grundlegende Konzepte zu den Vermittlermodellen ..... 34**
8.1.1 Protokollabschnitte ..... 34
8.1.2 Session Handling ..... 39
8.1.3 Prozesse ..... 39
**8.2 Vermittler Double Blinding ..... 43**
8.2.1 Prozesszuteilung ..... 43
**8.3 Vermittler Offene Quellen ..... 44**
8.3.1 Prozesszuteilung ..... 44
**8.4 Vermittler Vertraulichkeitsschutz ..... 45**
8.4.1 Prozesszuteilung ..... 46
**9 Anwendung eCH-0170 auf vermittlerbasierte Identity Federations ..... 48**
**9.1 Vertrauensstufe der Authentifizierung (VSA) ..... 48**
**9.2 Vertrauensstufe der Registrierung (VSR) ..... 48**
**9.3 Vertrauensstufe der Steuerung (VSS) ..... 48**
**9.4 Vertrauensstufe der Föderierung (VSF) ..... 48**
**10 Haftungsausschluss/Hinweise auf Rechte Dritter ..... 50**
**11 Urheberrechte ..... 50**
**Anhang A – Referenzen & Bibliographie ..... 51**
**Anhang B – Mitarbeit & Überprüfung ..... 52**
**Anhang C – Abkürzungen und Glossar ..... 52**
**Anhang E – Abbildungsverzeichnis ..... 53**
**Anhang F – Tabellenverzeichnis ..... 53**
**Anhang G – Tokenbased Identity Federation Modelle mit Vermittler ..... 54**

# Hinweis

Aus Gründen der besseren Lesbarkeit und Verständlichkeit wird im vorliegenden Dokument bei der Bezeichnung von Personen ausschliesslich die maskuline Form verwendet. Diese Formulierung schliesst Frauen in ihrer jeweiligen Funktion ausdrücklich mit ein.

# 1 Status

***Genehmigt**:* Das Dokument wurde vom Expertenausschuss genehmigt. Es hat für das definierte Einsatzgebiet im festgelegten Gültigkeitsbereich normative Kraft.

# 2 Einleitung

Eine Identity Federation im E-Government ermöglicht es Behörden ihre Leistungen online den Mitarbeitern anderer Behörden und den Bürgern sowie Organisationen und Unternehmen ihres Landes zur Verfügung zu stellen (siehe IAM Glossar [1] 2.62). Die Behörden delegieren dazu die Authentifizierung und die Bestätigung von Attributen an verschiedene IAM-Dienstanbieter. Grundlage der Delegation ist gegenseitiges Vertrauen, das durch rechtliche, organisatorische/architektonische und technischen Vereinbarungen abgestützt wird.

Eine Identity Federaton besteht aus ihren partizipierenden Teilnehmern (Relying Parties und IAM-Dienstanbietern, wie IdP, AP und Vermittler), die eine Gemeinschaft mit einer gemeinsamen IAM-Führung und -Steuerung bilden. Die Relying Parties nutzen die angebotenen IAM-Services der IAM-Dienstanbieter. Zur Laufzeit werden typischerweise die Prozesse “Subjekt authentifizieren”, und “E-Identity anreichern und bestätigen” von den IAM-Dienstanbietern übernommen. Die Autorisierung des Subjektes auf eine Ressource zuzugreifen (Prozess “Zugriff erlauben”) ist alleinige Aufgabe der Relying Parties und kann nicht an IAM-Dienstanbieter delegiert werden.

## 2.1 Ziel des Dokuments

Dieses Dokument konkretisiert die allgemeinen Gestaltungsprinzipien für ein IAM-System (eCH-0107 [2]) und definiert Architekturmodelle für Identity Federations, die die heutigen Anforderungen im E-Government optimal erfüllen.

Dazu werden die betrachteten Szenarien (siehe Kapitel 4) und Anwendungsfälle (siehe Kapitel 5) auf ihre Relevanz hin eingeschränkt, die allgemeinen Anforderungen aus eCH-0107 [2] konkretisiert und mit Anforderungen zum Schutz der Privatsphäre der Subjekte (siehe Kapitel 6) ergänzt.

Die geschärften Anforderungen erlauben es, die Menge der möglichen Identity Federation Modelle auf wenige einzuschränken und genaue Kriterien zur Auswahl zu geben (Kapitel 7). Mit der Wahl von vermittlerbasierten Modellen, können die gestellten Aufgaben am besten erfüllt werden.

Diese Vermittlermodelle werden dann im Folgenden detailliert beschrieben, um den architektonischen und technischen Rahmen für eine mögliche Implementierung zu liefern.

Im letzten Kapitel wird die Anwendung des Qualitätsmodell zur Authentifizierung von Subjekten (eCH-0170 [3]) beschrieben.

## 2.2 Einordnung

Unter dem Standard eCH-0107 [2] positionieren sich Konzepte für föderierte IAM-Lösungen und ergänzende Hilfsmittel. Die Konzepte sind konkrete Beschreibungen, wie ein IAM-Lösungsvorschlag aussieht, und beinhalten Teilkonzepte und Architekturen, die für die Umsetzung berücksichtigt werden müssen. Daneben werden den Konzepten Hilfsmittel zur Seite gestellt, die ergänzende Informationen zur Verfügung stellen und die für mehr als ein Konzept relevant sind. Die dargestellten Qualitäts- und Maturitätsmodelle sind Beispiele für Hilfsmittel und sind nicht abschliessend.

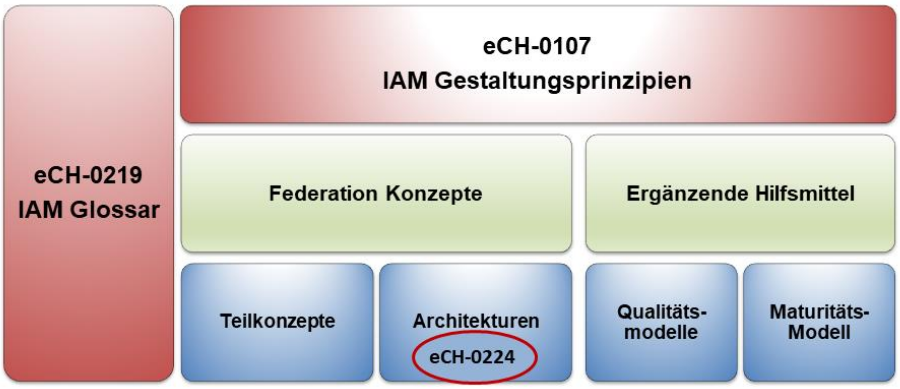


Abbildung 1: Einordnung des eCH-0224 Standards

Der vorliegende Standard eCH-0224 beschreibt Architekturmodelle für vermittlerbasierte *Identity Federation*. Damit wird die im Standard eCH-0168 [4] beschriebene STIAM-Architektur um weitere Architekturen ergänzt und diese zueinander in Beziehung gesetzt.
Zusätzlich wird auf den Standard eCH-0170 [3] verwiesen, der das Qualitätsmodell zur Authentifizierung von Subjekten definiert.
Fachbegriffe zu diesem Standard sind im eCH-0219 [1] erklärt und definiert.

## 2.3 Anwendungsbereich

Das Dokument beschreibt die Anforderungen, die Architektur und Richtlinien zur Implementierung von vermittlerbasierten Identity Federation Systemen im E-Government. Dabei werden hauptsächlich Identity Federation System in organisationsübergreifenden Kontexten adressiert. Die Anwendung derselben innerhalb einer Organisation wird dabei nur empfohlen.

Das Dokument beschreibt Anforderungen, Architekturen und Richtlinien vor allem für neue Systeme, kann aber auch für bestehende IAM-Systeme verwendet werden.

Die Beschreibung in diesem Standard ist technologie-unabhängig und wird in weiterführenden Standards auf konkrete Technologien angewandt.

Der Standard ermöglicht mit Hilfe von verschiedenen Auswahlkriterien die Entscheidung für eines der heute im E-Government einsetzbaren vermittlerbasierten Modelle. Die Richtlinien zur Implementierung dieser Modelle lassen aber auch noch Freiheitsgrade zu, die bei einer Implementierung weiter reduziert werden können.

## 2.4 Zielgruppe

Dieses konzeptionelle Dokument richtet sich hauptsächlich an:

- Geschäftsarchitekten, die Identity Federation Systeme spezifizieren und konzipieren,
- Software-Architekten, die ihre Kunden bei der Konzeption und Realisation eines Identity Federation Systems beraten,
- Datenschutzverantwortliche, die Identity Federation Systeme mit Vertraulichkeit und Schutz der Privatsphäre erweitern wollen,
- IAM-Interessierte mit technischem Hintergrund.

## 2.5 Abgrenzung

Die hier vorgestellten Identity Federation Modelle stützen sich vorrangig auf die Anforderungen des E-Government ab. Sie lassen sich aber auch auf andere Bereiche anwenden.

Für Identity Federation Systeme im E-Government konnten drei Szenarien (siehe Kapitel 4) mit mehreren Anwendungsfällen (siehe Kapitel 5) identifiziert werden. Nur diese Szenarien und Anwendungsfälle werden in diesem Standard betrachtet. So wird z.B. die Vermittlung von Daten, Dokumenten oder elektronischen Signaturen nicht behandelt.

Für Unternehmen (Juristische Personen) handeln natürlichen Personen. Die Prozesse und technischen Implementierung, wie die Rechte an eine natürliche Person übertragen werden, werden in diesem Standard nicht behandelt.

Der Standard beschreibt Identity Federation Modelle, bei denen die Teilnehmer mit Hilfe eines zentralen Vermittlers miteinander kommunizieren. Modelle, bei denen zur Kommunikation mehrere Vermittler oder Identity Federation Systeme miteinander in Verbindung stehen (sog. Interfederation Modelle), werden nicht betrachtet. Ebenso wird eine Integration in internationale Identitäts-Frameworks, wie STORK [5] und eIDAS [6], nicht adressiert.

Die Verwendung von Holder of Key (HoK) wird in diesem Standard kurz erwähnt. Da diese nicht verbreitet ist und Anforderungen, die ein HoK benötigen relativ selten sind, wird auf eine ausführliche Spezifikation verzichtet. Der Standard definiert Verfahren die eine Vertrauensstufe bis VS3 gemäss eCH-0170 [3] (bzw. FAL 2 gemäss NIST 800-63C [7]) unterstützen.

Session Handling wird in diesem Standard nur kurz beschrieben, da die Umsetzung sehr technologieabhängig ist und den Rahmen dieses Standards damit sprengen würde.

In Service-Architekturen (SOA und Microservices) werden mehrere Services miteinander verbunden und die E-Identities der Subjekte müssen weitergegeben (delegiert) werden. Die Delegation von Authentifizierungs- und Attributbestätigungen wird in diesem Standard nicht betrachtet.

**Falls ein IAM-System gemäss BGEID [8] umgesetzt wird, müssen die gesetzlichen Bestimmungen, sowie die dazugehörigen Verordnungen und Ausführungsbestimmungen eingehalten werden, bevor die in den eCH-Standards definierten Richtlinien angewendet werden können. Bei Konflikten hat das BGEID [8] Vorrang.**

## 2.6 Normativer Charakter der Kapitel

Die Kapitel des vorliegenden Standards sind von normativem oder auch deskriptivem Charakter. Folgende Tabelle definiert die Einordnung der Kapitel.

| Kapitel | Beschreibung |
|---|---|
| **2 Einleitung** | **Deskriptiv** |
| **3 Überblick Identity Federation** | **Deskriptiv** |
| **4 Szenarien E-Government** | **Normativ** |
| **5 Anwendungsfälle** | **Normativ** |
| **6 Anforderungen** | **Normativ** |
| **7 Auswahl Identity Federation Modell** | **Normativ** |
| **8 Vermittlermodelle** | **Normativ** |
| **9 Anwendung eCH-0170 auf vermittler-basierte Identity Federations** | **Deskriptiv** |

Anhang A und Anhang C sind ebenfalls normativ. Alle anderen Anhänge dieses Standards sind deskriptiv.

# 3 Überblick Identity Federation

Im Gegensatz zu isolierten IAM-Lösungen, welche voneinander unabhängige Identitäten pflegen, delegiert in einer Identity Federation eine Applikation bestimmte Dienste (z.B. die Identifizierung und Authentisierung eines Subjekts) an dafür spezialisierte Instanzen (Akteuere).
Eine Identity Federation besteht aus ihren partizipierenden Teilnehmern, die eine Gemeinschaft (Meta-Domäne) bilden (siehe Abbildung 4 in eCH-0107 [2]). Diese Gemeinschaft hat eine gemeinsame IAM-Führung und IAM-Steuerung, die sich auf gemeinsame Anforderungen und Richtlinien (IAM-Policy) einigt[1]. Die Tätigkeiten zur Verwaltung der IAM-Policy ist im eCH-0107 [2] beim Prozess „IAM-Policy verwalten“ (Kapitel 6.4.1) ausführlich beschrieben.

Es kann zwischen einer vermittlerbasierten und einer direkten Identity Federation unterschieden werden. Bei einer direkten (oder einfachen) Identity Federation bilden ein Identity Provider (oder eine Menge an ähnlichen IdPs) zusammen mit verschiedenen Applikationsanbietern eine Gemeinschaft, indem sie sich auf gemeinsame Regeln und Anforderungen (Identifikationsvorgaben, Authentifizierungsstufen, zu vermittelnde Attribute, usw.) einigen. Diese Art von Identity Federation bildet eine in sich geschlossene Gemeinschaft. Es bleibt jedem Applikationsanbieter offen in mehreren Gemeinschaften (facebook, Google, twitter, usw.) als Teilnehmer mitzumachen, aber jeder Benutzer hat in jeder Gemeinschaft eine unabhängige Identität. Dies ist eine heute übliche Praxis in sozialen Netzwerken, wie untenstehendes Beispiel zeigt.

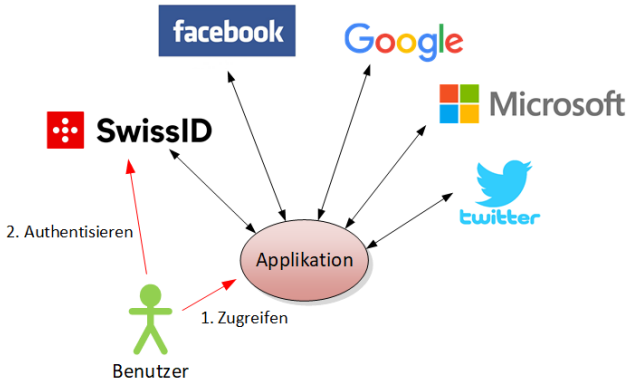


Abbildung 2: Einfache(direkte) Identity Federation

Eine vermittlerbasierte Identity Federation, stellt ihre Dienstleistungen meist mehreren Gemeinschaften zur Verfügung. Basis für die Dienste des Vermittlers ist ein für alle angeschlossenen Gemeinschaften verbindliches Regelwerk, welches auch für den Vermittler gilt. Jede Unter-Gemeinschaft kann spezifischere und strengere Richtlinien verabschieden, diese dürfen aber die allgemeinen Richtlinien aller Gemeinschaften nicht verletzen.
Eine vermittlerbasierte Identity Federation entlastet Applikationen und Identity Provider von bestimmten Aufgaben und Aufwänden und ermöglicht ein einfaches Teilnehmen in einer Gemeinschaft, da Identitätslieferanten und -konsumenten nur mit einem Partner (dem Vermittler) kommunizieren müssen, obwohl sich ein Benutzer bei mehreren IdPs authentisieren kann. Weitere Hinweise zu Vor- und Nachteilen von Identity Federation Systemen können dem Kapitel 7 entnommen werden.

[1] Ein Teilnehmer kann auch in mehreren Unter-Gemeinschaften sein.

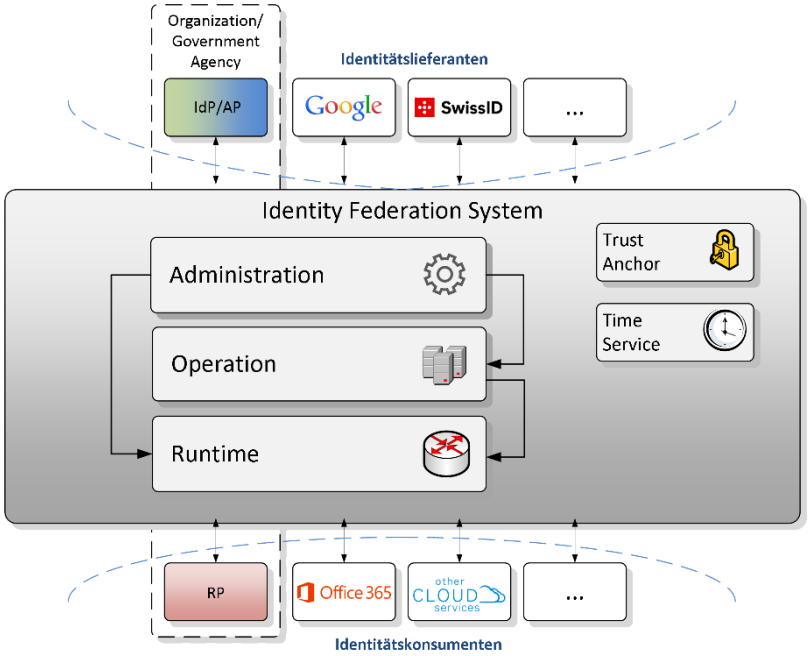


Abbildung 3: Grobstruktur eines vermittlerbasierten Identity Federation Systems

Ein vermittlerbasiertes Identity Federation System stellt alle notwendigen Dienste den Teilnehmern einer Gemeinschaft gemäss ihren Anforderungen und Richtlinien (IAM-Policy) zur Verfügung.

Diese Dienste lassen sich in drei Gruppen einteilen:

- *Administration*: in diese Gruppe gehören alle Prozesse der Definitionszeit und Etablierung (Geschäftsprozesse *IAM definieren* und *IAM führen)* nach eCH-0107 [2],
- *Operation*: die Gruppe umfasst den eigentlichen Betrieb und den Geschäftsprozess *Kernprozesse unterstützen*.
- *Runtime*: hier findet man alle Prozesse der Laufzeit (Geschäftsprozess *Zugriff kontrollieren)*.

Trust Anchor und Time Service werden gemäss eCH-0107 [2] in den Prozessen *IAM-Policy verwalten* bzw. *IAM-Führung führen* festgelegt.

Die Implementierung dieser Dienste beeinflussen den Funktionsumfang des Gesamtsystems.

## 3.1 Vertrauen

Die Grundlage einer Identity Federation ist das gegenseitige Vertrauen in die Partner, dass diese die vereinbarten Richtlinien (IAM-Policy) einhalten (basierend auf Prinzip-8 eCH-0107 [2]). Vertrauen beinhaltet zwei Kategorien: Integrität und Verfügbarkeit.

Die Faktoren von Integrität und Verfügbarkeit sind im Folgenden kurz aufgezählt:

- Integrität
  - **Authentizität**: Herkunft und Unversehrtheit der erhaltenen Authentifizierungs- oder Attributbestätigungen muss nachvollziehbar sein. Das kann z.B. durch Signieren von Bestätigungen erreicht werden (siehe IAM-9 eCH-0107 [2]).

  - **Datenintegrität**: Datenintegrität umfasst die Korrektheit der Daten. Es muss gewährleistet sein, dass die Daten nicht von Unbefugten manipuliert werden können. Dies wird meist durch Signaturen sichergestellt (siehe IAM-9 eCH-0107 [2]).
  - **Nachvollziehbarkeit**: Es muss festgestellt werden können, wer wann bestimmte Daten in welcher Weise verarbeitet hat.

- Verfügbarkeit
  - **Systemverfügbarkeit**: Unter die Systemverfügbarkeit fällt der Grad der Funktionalität der zentralen Komponenten (Vermittler, IdP, AP). Das bedeutet, dass diese Komponenten jederzeit betriebsbereit sein sollten und die Verarbeitung der Daten korrekt abläuft. Dies kann durch die organisatorischen und technischen Massnahmen der IAM-Führung sichergestellt werden. Die Anforderungen an das zu realisierenden IAM-System bestimmt die erwünschte Verfügbarkeit dieser Komponenten.
  - **Zuverlässigkeit**: Die Zuverlässigkeit oder Systemintegrität umfasst die korrekte Funktionsweise der Komponenten. Die IAM-Führung kann durch organisatorische und technische Massnahmen die geforderte Systemintegrität durchsetzen und überwachen.

## 3.2 Vertraulichkeit

In einer Identity Federation im E-Government ist der Schutz der Privatsphäre und der Daten besonders wichtig (siehe auch Anforderungen LB-13, LB-17 und LE-10 eCH-0107 [2]). Es werden Daten verarbeitet, die eine Person identifizieren können (z. B. Name, Vorname, Geburtsdatum). Dieses Dokument geht davon aus, dass bei der Authentifizierung keine besonders schützenswerte Daten (gemäss DSG [9] Art. 3.c) verwendet werden. Falls besonders schützenswerte Daten zum Einsatz kommen, müssen weitere Massnahmen definiert und umgesetzt werden, die in diesem Dokument nicht behandelt werden[2].
Dieser Schutz-Aspekt wird im allg. als **Vertraulichkeit** bezeichnet: Von Vertraulichkeit kann dann gesprochen werden, wenn die Informationen nur für Befugte zugänglich sind. Vertraulichkeit kann durch gesetzliche/organisatorische Massnahmen und/oder technische Massnahmen erreicht werden. Technische Massnahmen haben den Vorteil, dass ein Missbrauch der Daten erschwert wird, für den Fall, dass die gesetzliche/organisatorische Massnahmen nicht wirksam genug sind.

Die Anforderung zur Vertraulichkeit betrifft die Übergabe der Authentifizierungs- und Attributbestätigungen vom Aussteller (IdP, IdP/AP, AP) an den Empfänger (RP). Eine Übergabe von vertraulichen Attributen setzt voraus, dass das Subjekt und die RP mit einer angemessenen Vertrauensstufe authentifiziert wurde.

Im Allgemeinen gilt die Client Plattform als unsicher und es muss sichergestellt werden, dass sie keine Informationen über den Benutzer erhält (wahlweise durch Verschlüsselung oder durch Übermittlung per Back Channel). Siehe auch eCH-0170 [3], Kap. 8.2.3.

Besonders in Architektur-Modellen mit Vermittler muss der Übergabe der Authentifizierungs- und Attributbestätigungen zwischen Aussteller und Empfänger besondere Aufmerksamkeit geschenkt werden, da alle Authentifizierungs- und Attributbestätigungen durch den Vermittler

[2] Ob besonders schützenswerte Daten zum Einsatz kommen, muss im Einzelfall geprüft werden. In Abhängigkeit des Kontexts und Kombinationen der Daten können besondere Schutzmassnahmen erforderlich sein.

hindurchfliessen[3] und dieser die Informationen zur Bildung von Verhaltensmustern verwenden könnte. Authentifizierungsbestätigungen enthalten im Normalfall (eine Ausnahme kann der Identifier sein, wenn dieser nicht zufällig ist und einen Bezug zum Subjekt enthält) keine Personendaten nach DSG [9] Art 3.a und sind daher eher unkritisch. Im Gegensatz dazu enthalten die Attributbestätigungen Angaben zu Personen.

## 3.3 Session Handling

Eine Identity Federation umfasst viele verschiedene Sessions, die zwischen der Client-Plattform und den verschiedenen IAM-Diensten etabliert werden. Diese Sessions gilt es zu unterscheiden:

- Sessions beim IdP bzw. beim Vermittler ermöglichen Single Sign-On (SSO) und reduzieren dadurch die Authentifizierungsvorgänge der Subjekte.
- Sessions beim Discovery-Service können die IdP-Auswahl automatisieren, so dass Subjekte nur beim ersten Mal eine Auswahl treffen müssen.
- Sessions bei der Relying Party ermöglichen ein einmaliges Authentisieren für die verschiedenen (https-)Requests (für die unterschiedlichen Ressourcen) eines User Clients. Diese Sessions können je nach Anwendung sehr unterschiedlich sein.
- Attribute Provider sind im Normalfall ‚stateless' und etablieren keine Sessions.

All diese Sessions bestehen gleichzeitig, aber unabhängig voneinander: D.h., das Ablaufen einer Session bedeutet nicht automatisch das Ablaufen einer anderen. Aber manche Session können miteinander verbunden sein, z.B. über gemeinsame Identifier.

Die Existenz verschiedener z.T. abhängiger Sessions machen SSO, SLO und auch Step-Up-Authentifizierung sehr schwierig, zumal auch die verwendete Technologie einen grossen Einfluss hat. Daher werden in diesem Standard nur kurz die wichtigsten Eigenschaften beschrieben. Die konkrete Umsetzung des Session Handlings ist Bestandteil von weiterführenden, technologiebezogenen eCH-Standards, welche diesen Standard als Basis verwenden.

### 3.3.1 Single Sign-on (SSO)

Nach einer Authentifizierung kann das Subjekt auf die geschützte Ressource zugreifen. Falls das Subjekt innerhalb einer definierten und limitierten Zeitspanne auf eine Ressource von einer anderen Relying Party innerhalb der Gemeinschaft zugreifen möchte, muss sich das Subjekt nicht erneut authentifizieren lassen. Falls Attribute weitergegeben werden, ist jedoch, wenn erforderlich, eine Zustimmung des Subjekts nötig.

Die Relying Party kann allerdings eine Authentifizierung des Subjektes vor dem Zugriff auf ihre Ressourcen erzwingen und so SSO umgehen.

#### 3.3.1.1 Step-Up Authentifizierung

Die Step-Up Authentifizierung ist ein Spezialfall des SSO. Das Subjekt ist bereits authentifiziert, möchte aber nun auf eine Ressource bei derselben oder einer anderen Relying Party

[3] Man spricht in diesem Zusammenhang von einem Vermittler, der «honest but curious» ist. D.h. das Protokoll wird korrekt implementiert (der Vermittler ist ehrlich/honest), aber er könnte die durch ihn hindurchfliessenden Daten anschauen und für seine Zwecke nutzen (er ist neugierig/curious).

zugreifen, die eine höhere Stufe der Authentifizierung verlangt. In diesem Fall sendet die Relying Party einen neuen bzw. erneuten Request und der Benutzer muss sich wie bei der initialen Authentifizierung einen der möglichen IdPs wählen und sich bei diesem authentifizieren. Dies erfordert ein Identity Mapping (siehe Kap. 8.1.3.2) und Identity Linking (siehe Kap. 8.1.3.7). Falls die Step-Up Authentifizierung beim selben IdP gemacht wird, werden diese beiden Funktionalitäten nicht benötigt.

Falls notwendig, müssen die von der neuen Ressource geforderten Attribute in der gewünschten Qualität von einem geeigneten AP geholt werden.

#### 3.3.1.2 Step-Down Authentifizierung

Die Step-Down Authentifizierung, ist wie die Step-Up Authentifizierung, ein Spezialfall des SSO.
Es kommt zu einer Step-Down-Authentifizierung, wenn der Benutzer bei einer RP mit einer hohen Stufe bereits authentifiziert wurde und dann auf eine RP zugreifen möchte, welche eine niedrigere Authentifizierungsqualität fordert und auch nur diese verarbeiten kann. Innerhalb ein und derselben Relying Party, reduziert sich dieser Anwendungsfall auf einen SSO Vorgang, indem automatisch die bereits bestehende höhere Authentifizierung wiederverwendet wird.
Step-Down kann problematisch werden, wenn die bereits bestehende hohe Authentifizierungsqualität zusätzliche Anforderungen an eine RP stellt (z.B. verschlüsselte Attribute), die diese nicht erfüllen kann. Hier muss der Vermittler die entsprechenden Anpassungen vornehmen, um diese technischen Hürden zu nehmen.

Beispiel: Das Subjekt ist bereits mit Vertrauensstufe 3 authentifiziert und möchte sich auf eine Ressource zugreifen, die Vertrauensstufe 1 verlangt. Der Vermittler nimmt die Authentifizierungsbestätigung (mit Vertrauensstufe 3) vom IdP entgegen. Der Vermittler transformiert die Authentifizierungsbestätigung zu einer mit Vertrauensstufe 1 und leitet diese an die RP weiter.

### 3.3.2 Single Logout (SLO)

Single Logout ermöglicht es dem Subjekt sich von allen Sessions innerhalb einer Gemeinschaft (IdP sowie RPs) abzumelden. Dies sollte dem Subjekt so einfach und transparent wie möglich zur Verfügung gestellt werden.

Die beteiligten Akteure (RPs, Vermittler, IdPs) müssen dazu Schnittstellen zur Verfügung stellen, welche das Single Logout unterstützen. Falls der Logout-Prozess bei einer Relying Party nicht funktionieren sollte oder nicht unterstützt wird, muss das Subjekt entsprechend informiert werden.

# 4 Szenarien im E-Government

Ein Identity Federation System im E-Government kann die folgenden Szenarien abdecken:

- Government to Citizen (G2C),
- Government to Government (G2G),
- Government to Business (G2B).

## 4.1 Government to Citizen (G2C)

**Definition**: In einem Government to Citizen (G2C) Szenario nutzen natürliche Personen (Bürger oder Einwohner in der Rolle als Zivilperson, d.h. als nichtbehördlicher Akteur) online die fachlichen Leistungen einer Behörde (RP). Die Behörde delegiert dazu einen Teil der notwendigen IAM-Leistungen an IAM-Dienstanbieter.

Dabei sollen möglichst die E-Identities (und damit IdP/APs) der Einzelperson verwendet werden, die sie bereits besitzen und die den Anforderungen der Behörden genügen. Den Einzelpersonen wäre es daher möglich für Leistungen von Gemeinde-, Kantons- und Bundes-Behörden dieselben E-Identities zu verwenden. Die E-Identities können von behördlicher oder privatwirtschaftlicher Seite verwaltet werden.

Beispiele:

- Eine Einzelperson sollte vom kantonalen IdP/AP authentifiziert werden, der seine Wohnadresse kennt, um auf eine Applikation eines anderen Kantons zugreifen zu können, welche die Wohnadresse verlangt. Die Applikation prüft die erhaltenen Authentifizierungs- und Attributbestätigungen und erteilt anschliessend Zugriff auf ihre Ressourcen.
- Eine Einzelperson verwendet eine E-Identity mit hoher Vertrauensstufe (z. B. SuisseID), um einen Auszug aus dem Betreibungsregister zu bestellen.

## 4.2 Government to Government (G2G)

**Definition**: In einem Government to Government (G2G) Szenario nutzen Mitarbeiter oder Services einer Behörde (Gemeinde, Kanton, Bund) online fachliche Leistungen von anderen und u. U. auch der eigenen Behörde. Die für die fachliche Leistung zuständige Behörde delegiert dazu einen Teil der notwendigen IAM-Leistungen an IAM-Dienstanbieter.

Mitarbeiter und Services handeln dabei im Auftrag der Behörde, was durch bestätigte Attribute nachgewiesen wird. Die bestätigten Attribute können von der RP auch für Zugangs-/Zugriffberechtigungen verwendet werden.

Der Mitarbeiter bzw. der Service wird von einem zuständigen Identity Provider der (Heimat-) Behörde authentifiziert.

Beispiele:

- Ein Mitarbeiter des Kantons Zürich möchte Informationen von einer Bundes-Applikation abfragen. Dazu muss er sich beim kantonalen IdP authentisieren. Die Bundes-Applikation erteilt dem Mitarbeiter Zugriff nach Prüfung der erhaltenen Authentifizierungs- und Attributbestätigungen.
- Der kantonale Steuerservice möchte auf die aktuellen Adressdaten der Gemeinden zugreifen, um die Steuerunterlagen automatisiert zu verschicken.

## 4.3 Government to Business (G2B)

**Definition**: In einem Government to Business Szenario handelt eine natürliche Person für eine nicht handelnde Organisation und nutzt online die fachlichen Leistungen einer Behörde (RP). Die Behörde delegiert die dazu notwendigen IAM-Leistungen an IAM-Dienstanbieter.

Die natürliche Person muss z. B. gemäss eCH-0170 [3] Kapitel 6.2.1 zur Definitionszeit registriert und mit der nicht handelnden Organisation verknüpft werden. Zur Laufzeit kann die RP das entsprechende Enterprise-Attribut abfragen, um die Organisationszugehörigkeit zu bestätigen.

Soweit möglich, sollen bereits vorhandene E-Identities verwendet werden. Die E-Identities können von behördlicher oder privatwirtschaftlicher Seite verwaltet werden.

Beispiele:

- Ein Unternehmer möchte den Handelsregistereintrag seines Unternehmens anpassen. Dazu muss er sich mit einer hohen Vertrauensstufe authentisieren und Attribute liefern können, welche ihn als dazu bevollmächtigten ausweisen.

# 5 Anwendungsfälle

In einer Identity Federation im E-Government sind aus Sicht der RP zwei typische Anwendungsfälle zur Laufzeit zu unterscheiden, die in allen Szenarien aus Kapitel 4 eingesetzt werden können:

- **Reine Authentifizierung**: siehe Kapitel 5.1,
- **Authentifizierung mit Attributübergabe**: siehe Kapitel 5.2.

Die im folgenden definierten Anwendungsfälle sind verschiedene Varianten des Laufzeit Prozesses *E-Identity bestätigen*, der im eCH-0107 [2] spezifiziert ist. Die Unterschiede der Anwendungsfälle betreffen die unterschiedliche Ausprägung des Teilprozesses *E-Identity anreichern*.

## 5.1 Reine Authentifizierung

Beim Anwendungsfall reine Authentifizierung entfällt der Teilprozess E-Identity anreichern ganz. Das Subjekt wird nur von einem IdP authentifiziert. Das Ergebnis der Authentifizierung muss ein technischer Identifikator und die Qualität der Authentifizierung sein. Es wird nur die Authentifizierungsbestätigung übermittelt. Es dürfen keine subjektidentifizierenden Informationen oder Attribute in der Authentifizierungsbestätigung vorhanden sein.

### 5.1.1 Unabhängige E-Identities

Ein Subjekt kann mehreren E-Identities besitzen und kann mit diesen auf eine Ressource zugreifen. Jede E-Identity des Subjekts muss unabhängig von den anderen sein, in dem Sinn, dass eine Ressource nicht feststellen kann, ob zwei unterschiedliche E-Identities demselben Subjekt gehören.

### 5.1.2 Verlinkte E-Identities

Ein Subjekt kann mehrere verbundene E-Identities besitzen. E-Identities sind verbunden, wenn eine Ressource ein Subjekt wiedererkennt, obwohl es bei einem erneuten Zugriff eine andere E-Identity verwendet.

## 5.2 Authentifizierung mit Attributübergabe

Zusätzlich zum Anwendungsfall ‘Reine Authentifizierung’ (siehe Kapitel 5.1), bei der ausschliesslich eine Statusinformation zur erfolgten Authentifizierung und ein technischen Identifikator zurückgegeben werden, werden bei der Authentifizierung mit Attributübergabe zusätzlich eine bestimmte Menge von Attributen abgefragt und geliefert.

Der Prozess ‘E-Identity anreichern’ (eCH-0107 [2] Kapitel 6.1.4) ist demnach Teilprozess des Prozesses Subjekt authentifizieren.

Allenfalls muss das Subjekt die Attribute freigeben (User Consent). Weitere Vorgaben dazu befinden sich im Kapitel 8.1.3.3.

Beispiel G2C:

- Eine RP stösst eine Identitätsvermittlung an, wenn sie einen neuen Benutzer für das Subjekt lokal anlegen will und dessen Attribute füllen will. Die RP delegiert die Authentifizierung des Subjekts an einen IdP/AP.
- Verwendung BE-Login für Steuererklärung oder Antrag auf Stipendien.

Beispiel G2G:
Ein kantonaler Mitarbeiter einer Behörde möchte auf eine RP des Bundes zugreifen. Dazu wird der Mitarbeiter beim IdP des Kantons authentifiziert. Die Attribute 'Kanton' und 'Funktion' werden übermittelt. Der Mitarbeiter muss diese Attribute nicht freigeben, da es sich um Enterprise-Attribute handelt.

Die folgenden Eigenschaften der Attribute haben Einfluss auf die Art und Weise der Attributübergabe und müssen bei der Evaluierung eines IAM-Systems berücksichtigt werden.

**Empfehlung**: Die Eigenschaften bzw. Qualität eines Attributs SOLLTEN in der Attributbestätigung an die RP enthalten sein.

### 5.2.1 Lebensdauer der Attributwerte

Attribute werden bezüglich Lebensdauer grob in zwei Kategorien eingestuft:

- Attribute, bei denen sich die Werte selten ändern (z. B. Name, Vorname, Geburtsdatum).
- Attribute, bei denen die Werte regelmässig geprüft werden müssen (z. B. abgeleitete Attribute wie das Alter des Subjekts, Kantonszugehörigkeit).

### 5.2.2 Anzahl der Quellen

Attribute können von einer oder mehreren Quellen bezogen werden. Falls Attribute von mehreren Quellen übermittelt werden, muss eine Attributaggregation vorhanden sein. Je mehr Quellen involviert sind, desto komplexer wird ein IAM-System.

### 5.2.3 Datenherkunft

Die Verwendung der Attribute auf der RP hat einen Einfluss auf die Anforderungen an die Attributbestätigungen. Wenn z. B. die Attribute für Zugangs- und Zugriffsbestätigungen verwendet werden, kann es wichtig sein die Quelle der Attribute zu kennen.

Beispiele:

- unwichtig: Schuhgrösse
- gefordert: bei Kantonszugehörigkeit

### 5.2.4 Qualität der Attribute

Die Attribute können in unterschiedlichen Qualitäten vorliegen. Wie die Qualität der Attribute bestimmt wird, muss von der IAM-Steuerung der Gemeinschaft festgelegt werden. Die Qualität der Attribute kann von der Qualität der Authentifizierung, Quelle (Datenherkunft) usw. abhängig sein. Die Qualitätsstufe eines Attributs sollte als Teil der Attributbestätigung an die RP übertragen werden.

Beispiele:

- Unbestätigtes Attribut: Titel (bzw. Anrede)

- Bestätigtes Attribut: Wohnadresse (Wohnadresse des Subjekts, die die Post bestätigt)
- Staatlich bestätigtes Attribut: Geburtsdatum

## 5.3 Verwendete technischen Identifikatoren in den Anwendungsfällen

Es können drei unterschiedliche Arten von **technischen Identifikatoren**[4] in einer Authentifizierungsbestätigung verwendet werden. Welcher Identifikator verwendet werden soll, bestimmt sich aus den Anforderungen der Relying Party und den Privatsphärenanforderungen des Subjekts. Unabhängig der drei Arten dieser technischen Identifikatoren sollen damit keine Rückschlüsse auf das Subjekt gezogen werden können. Bei den technischen Identifikatoren sind explizit **nicht** die fachlichen Identifikatoren gemeint (z.B. AHV-Nummer). Diese werden allenfalls als Attribut an die RP übergeben.

**Empfehlung**: Ein technischer Identifikator SOLLTE immer eine zufällige Zeichenfolge sein und SOLLTE KEINE Personendaten gemäss DSG [8] Art 3.a enthalten. Weitere Informationen zu technischen Identifikatoren sind im SAML Core 2.0 [10] im Kapitel 8.3 vorhanden.

### 5.3.1 Verteilter Identifikator (Distributed ID)

Nach der Authentifizierung muss für jede Relying Party und pro Subjekt derselbe Identifikator ausgegeben werden. Somit ist es möglich, ein Subjekt über mehrere Relying Parties wieder zu erkennen.

Wenn dieser Identifikator verwendet wird, ist es für die in der Gemeinschaft beteiligten Relying Parties einfach Verhaltensmustern zu erstellen und Daten der Subjekte zu korrelieren.

**Empfehlung**: Verteilte technische Identifikatoren SOLLTEN NICHT verwendet werden.

### 5.3.2 Relying Party gebundener technischer Identifikator (Persistent ID)

Nach der Authentifizierung muss für jede Relying Party pro Subjekt ein unterschiedlicher, aber immer der gleiche Identifikator ausgegeben werden. Somit ist es für eine Relying Party möglich, ein Subjekt wieder zu erkennen. Da aber eine andere Relying Party einen anderen Identifikator vom selben Subjekt erhält, wird das Korrelieren von Daten erschwert.

**Empfehlung**: Ein RP gebundener technischer Identifikator SOLLTE verwendet werden, wenn die Relying Party die Authentifizierung auslagern möchte, das Subjekt aber dennoch bei jedem erneuten Zugriff wiedererkennen will.

Beispiel G2C: Parkschein-Bestellung in der Gemeinde

### 5.3.3 Einmaliger zufälliger technischer Identifikator (Transient ID)

Pro Authentifizierung des Subjekts muss jeweils ein anderer Identifikator verwendet werden.

[4] In SAML ist der technische Identifikator der Parameter ‘NameID’ In OIDC ist der technische Identifikator der Parameter ‘sub’.

Das Subjekt kann so bei mehrmaligem Zugriff anhand der Authentifizierung von einer RP nicht wiedererkannt werden. Dieser Identifikator ist auch hilfreich, wenn nur anhand der Attribute Zugriff auf eine Ressource gewährt werden soll.

**Empfehlung**: Ein einmaliger zufälliger technischer Identifikator SOLLTE verwendet werden, wenn das Subjekt auch bei mehrmaligem Zugriff nicht wiedererkannt werden darf oder nur anhand der Attribute Zugriff auf eine Ressource gewährt werden soll.

Beispiel G2C:
Online-Beratung zur Suchthilfe (z.B. www.safezone.ch)

Beispiel G2G:
Eine Bundesapplikation ist nur für Kantonsmitarbeiter zugänglich. Dabei ist die Identität des Mitarbeiters nicht relevant.

# 6 Anforderungen

Die Anforderungen an ein föderiertes IAM-System im E-Government sind im eCH-0107 [2] beschrieben. In diesem Kapitel werden diese Anforderungen aufgegriffen und konkretisiert. Es werden nur die relevanten Szenarien im E-Government (G2C, G2B und G2G, siehe Kapitel 4) und die Anwendungsfälle aus Kapitel 5 berücksichtigt. Weiterhin wird ein Schritt in Richtung Implementierung von Identity Federations gemacht und deshalb nur etablierte Technologien und eine möglichst geringe Einstiegshürde für die RPs gefordert.

Die Anforderungen können sich **widersprechen**. Die Einstufung der Anforderungen mit MUSS, SOLL und KANN sind aus Sicht des jeweiligen Stakeholders. In Kapitel 7 und 8 werden die möglichen Umsetzungen beschrieben und wie welche Anforderungen bezüglich Privatsphäre implementiert werden können. Die Anforderungen sind (meist) unabhängig von einem Szenario definiert. Je nach Kontext und abhängig vom Szenario können Anforderungen wegfallen. Die IAM-Steuerung der Gemeinschaft (siehe 224-Führ-1) muss entscheiden, welches Vermittlermodell eingesetzt wird, dass den Anforderungen gerecht wird.

Die neuen bzw. geschärften Anforderungen werden in vier verschiedene Typengruppen eingeteilt:

- B… Business (Geschäftsanforderungen),
- D… Data (Informationen und Daten),
- A… Application (Anwendung),
- T… Technology (Technologie).

Die Begriffe MUSS und DARF NICHT bezeichnen Anforderungen, die einzuhalten sind, um dem Standard zu entsprechen. Ausnahmen müssen durch die IAM-Steuerung der Gemeinschaft entschieden werden (siehe 224-Führ-1).

Die Begriffe SOLLTE und SOLLTE NICHT deuten darauf hin, dass unter mehreren Möglichkeiten eine als besonders geeignet empfohlen wird, ohne andere zu erwähnen oder auszuschließen, oder dass eine bestimmte Vorgehensweise bevorzugt, aber nicht unbedingt erforderlich ist, oder dass (in der negativen Form) eine bestimmte Möglichkeit oder Vorgehensweise abgeraten, aber nicht verboten wird.

Der Begriff KANN bezeichnet eine optionale Möglichkeit.

## 6.1 Anforderungen an das föderierte IAM-System

| Bezeichnung | Typ | Beschreibung | Begründung / Referenz |
|---|---|---|---|
| **224-IAM-1** | B | Es MÜSSEN nur die Szenarien G2C, G2B oder G2G unterstützt werden. Es können gleichzeitig mehrere Szenarien unterstützt werden. | Einschränkung der Szenarien |
| **224-IAM-2** | T | Das föderierte IAM-System MUSS Web-Applikationen, die in Webbrowsern (Chrome, Firefox usw.) ausgeführt werden, und SOLLTE Mobile-Applikationen (App für iOS und Android) unterstützen. | IAM-4 |

| Bezeich-nung | Typ | Beschreibung | Begründung / Referenz |
|---|---|---|---|
| **224-IAM-3** | T | Für die Protokolle des föderierten IAM-Systems MÜSSEN etablierte Technologien[5] verwendet werden. | IAM-4,<br>224-Führ-1<br>224-Führ-2 |
| **224-IAM-4** | A/D | In einem Identity Federation System MUSS ein Qualitätsmodell für die Authentifizierung von allen Beteiligten im IAM-System implementiert und durchgesetzt werden. | IAM-2,<br>224-Führ-3 |
| **224-IAM-4.1** | A/D | Als Qualitätsmodell für die Authentifizierung SOLLTE eCH-0170 [2] verwendet werden. | IAM-2 |
| **224-IAM-5** | A/D | Attribute SOLLTEN nach einem einfachen verständlichen Qualitätsmodell bewertet werden können (Beispiel: nicht bestätigte Attribute; bestätigte Attribute; staatlich bestätigte Attribute). | IAM-2,<br>224-Führ-4 |
| **224-IAM-6** | B/A/T | Die RPs, IdPs und APs MÜSSEN nach definierten Richtlinien integriert werden. | Prinzip-8 |
| **224-IAM-7** | B/A | Es SOLLTE möglich sein, dass mehrere Unter-Gemeinschaften in einem Identity Federation System verwendet werden können, sofern diese zum Gesamtsystem kompatible Anforderungen haben.[6] | IAM-4 |
| **224-IAM-8** | A | Die abgefragte Instanz (Vermittler, IdP, IdP/AP oder AP) MUSS anhand der Authentifizierungs- bzw. Attributanfrage die anfragende Instanz (Vermittler oder RP) eindeutig identifizieren können.[7] | Trust |

Tabelle 1: Anforderungen ans IAM-System

## 6.2 Anforderungen des Stakeholders: Leistungsbezüger

In einem föderierten IAM-System gibt es verschiedene Grundanforderungen, die in der Konzeptionierung der IAM-Architektur berücksichtigt werden müssen.

[5] Heute etablierte Technologien für die Protokolle in einem Identity Federation System sind ausschliesslich SAML und OIDC. Die IAM-Steuerung der Gemeinschaft entscheidet, welche Technologien als etabliert gelten.

[6] Eine Gemeinschaft hat eine gemeinsame IAM-Policy, die in den Unter-Gemeinschaften weiter verschärft, aber nicht gelockert werden kann. Dadurch wird sichergestellt, dass die Anforderungen kompatibel sind und in einem IAM-System implementiert werden können.

[7] Die Identifizierung beinhaltet die Registrierung und Wiedererkennung der anfragenden Instanz (Authentifizierung) gemäss vordefinierten Prozessen und Compliance-Regeln.

Die Privatsphäre muss im Szenario G2C geschützt werden. Ebenso im G2B muss die Privatsphäre berücksichtigt werden, ausser es werden keine personenidentifizierenden Daten ausgetauscht.

Für die Implementierung eines IAM-Systems müssen individuell die Anforderungen an die Privatsphäre abgeklärt werden und entsprechende organisatorische und technische Massnahmen umgesetzt werden, um die Privatsphäre der natürlichen Personen innerhalb des IAM-Systems zu schützen.

Diese Anforderungen können sich widersprechen. In Kapitel 7 und 8 werden die möglichen Umsetzungen beschrieben und wie welche Anforderungen bezügliche Privatsphäre implementiert werden können.

| Bezeichnung | Typ | Beschreibung | Begründung / Referenz |
|---|---|---|---|
| **224-LB-1** | B | Die Privatsphäre der natürlichen Personen MUSS geschützt werden.[8] | LB-2, LB-2.1, LB-13 |
| **224-LB-2** | B | Eine natürliche Person MUSS auf eine E-Ressource zugreifen können, ohne dass Identitätslieferanten des IAM-Systems dies feststellen können.[9] | Nichtverfolgbarkeit (RP) |
| **224-LB-3** | B | Eine natürliche Person MUSS auf eine E-Ressource zugreifen können, ohne dass diese E-Ressource weiss, welche Identitätslieferanten im IAM-System verwendet wurden. [10] | Nichtverfolgbarkeit (IdP), Need-to-Know-Prinzip, Datensparsamkeit |
| **224-LB-4** | B | Einer natürlichen Person MUSS es möglich sein, mehrmals auf E-Ressourcen von mehreren (unabhängigen) RPs zugreifen zu können, ohne dass die unberechtigte RPs oder unberechtigte Dritte diese Ereignisse miteinander verbinden können. | Unverkettbarkeit |
| **224-LB-5** | B | Personenidentifizierende oder sogar sensible[11] Informationen zu einer Person MÜSSEN so geschützt sein, dass nur berechtigte RPs, berechtigte Organe (z.B. interne Aufsicht) und die natürliche Person selbst diese einsehen können. | Vertraulichkeit |

[8] Die verschiedenen Aspekte der Privatsphäre (siehe z.B. eCH-0107 [2] Kap. 9) sollten bei einer konkreten Implementierung mittels Risiko- und Bedrohungsanalyse evaluiert werden.

[9] Es muss sichergestellt werden, dass die Identitätslieferanten nicht erfahren, welche RPs das Subjekt verwendet. Damit wird sichergestellt, dass Identitätslieferanten, die „honest but curious“ sind, keine Verhaltensmuster der Nutzungsgewohnheiten erstellen können.

[10] Es muss sichergestellt werden, dass die RP nicht erfährt, bei welchem IdP sich das Subjekt authentifiziert hat und von welchem AP die Attribute bestätigt wurden. Damit wird sichergestellt, dass die RP keine Informationen erhält, die sie für ihre Funktionserfüllung nicht benötigt.

[11] Je nach Kontext können Rechtezuweisung oder Kombination von bestimmten Attributen sensibel sein.

| Bezeichnung | Typ | Beschreibung | Begründung / Referenz |
|---|---|---|---|
| **224-LB-6** | B | Die Einwilligung der natürlichen Person MUSS erfolgen, bevor Attributbestätigungen mit persönlichen Attributen an eine RP weitergegeben werden. | Einwilligung/Weitergabe,<br>Reg-1 |
| **224-LB-7** | B | Identitätslieferanten, Vermittler und RPs MÜSSEN jederzeit gemäss anwendbaren Datenschutzgesetzen und kantonaler Datenschutzregeln Auskunft geben können. | Auskunftsrecht,<br>Reg-1 |
| **224-LB-8** | B | Es MUSS sichergestellt werden, dass RPs nur Informationen über natürlichen Personen erhalten, für die sie entsprechende Berechtigungen haben. | Abfrageberechtigung |
| **224-LB-9** | B | Die zu einem bestimmten Authentisierungsvorgang vermittelten Informationen und ihre Metadaten MÜSSEN von Identitätslieferanten, Vermittler und RP für einen bestimmten Zeitraum, welcher die IAM-Steuerung (der Gemeinschaft) definiert, vorgelegt werden können. | Nachvollziehbarkeit |
| **224-LB-10** | B | Eine natürliche Person KANN die Löschung seiner Daten bei Identitätslieferanten, Vermittler und RPs beantragen. Die Löschung ist möglich, sobald die Daten für ihre Zweckbestimmung nicht mehr erforderlich sind und der Löschung keine gesetzlichen Aufbewahrungspflichten entgegenstehen. | Recht auf Vergessen,<br>Reg-1 |

Tabelle 2: Anforderungen des Leistungsbezügers

## 6.3 Anforderungen des Stakeholders: Leistungserbringer

| Bezeichnung | Typ | Beschreibung | Begründung / Referenz |
|---|---|---|---|
| **224-LE-1** | B | In G2C: Die Subjekte im IAM-System MÜSSEN natürliche Personen sein.<br>In G2G: Es MÜSSEN natürliche Personen oder Services im Rahmen ihrer Zugehörigkeit zu einer Behörde als Subjekt auftreten. | Einschränkung der Szenarien |

| Bezeich-nung | Typ | Beschreibung | Begründung / Referenz |
|---|---|---|---|
| **224-LE-2** | B/D | Vor allem bei G2G: Die Attributbestätigungen SOLLTEN von vertrauenswürdigen APs kommen.[12] | Einschränkung der Szenarien |
| **224-LE-3** | B | Die Integration an das föderierte IAM-System MUSS für die RP mit einem minimalen Aufwand möglich sein.[13] | Einfachheit für die RP |
| **224-LE-3.1** | B | Die RP SOLLTE nur mit einer Komponente (IdP oder Vermittler) kommunizieren. | |
| **224-LE-3.2** | B | Die RP SOLLTE nur eine Protokollvariante (Version, Flow,…) unterstützen und keine Protokolltransformationen vornehmen müssen. | |
| **224-LE-3.3** | B | Die RP SOLLTE möglichst viele Prozesse (Discovery, User Consent, Identity/Attribut-Mapping & -Transformation,,.. ) delegieren können. | LE-11 |
| **224-LE-3.4** | A | Die Authentifizierungsanfrage und -antwort, sowie Attributanfragen und -bestätigungen MÜSSEN nach einem bestimmten Format definiert sein. Alle Beteiligten können sich darauf verlassen, dass das Format die minimalen Anforderungen erfüllen (z. B. enthält eine Signatur, einen Identifikator, entspricht einem gegebenen Attributschema usw.). | Einfachheit für die RP,<br>IAM-4,<br>224-Führ-5 |
| **244-LE-4** | B/A | Die RP KANN fordern, dass die Auswahl der IdPs eingeschränkt werden kann. | LE-5 |
| **224-LE-5** | B | Eine RP KANN verlangen, dass die Herkunft von Authentifizierungs- und Attributbestätigungen von Subjekten bis zu ihrer Quelle (IdP, IdP/AP oder AP) überprüfbar ist. | Datenherkunft |
| **224-LE-6** | B | Eine RP KANN verlangen, dass die Echtheit und Unversehrtheit der Attributbestätigungen von Subjekten bis zu ihrer Quelle (IdP/AP oder AP) überprüfbar ist. | Datenunversehrtheit, Datenintegrität |

[12] Wenn das Identity Federation System innerhalb einer Organisation verwendet wird, kann diese Anforderung gelockert werden.

[13] Einfache Integration kann z. B. einen Personentag bedeuten. Dabei ist nur das Konfigurieren der Anbindung, und nicht die Umsetzung der Schnittstellen und deren Protokolle gemeint.

| Bezeich-nung | Typ | Beschreibung | Begründung / Referenz |
|---|---|---|---|
| **224-LE-7** | B | Die RP KANN verlangen, dass für ein Subjekt immer derselbe technische Identifikator zurück-gegeben wird, unabhängig vom verwendeten IdP. | Einfachheit für die RP (kein Identity Lin-king/Mapping auf der RP)<br>224-Führ-1 |

Tabelle 3: Anforderungen des Leistungserbringers

## 6.4 Anforderungen des Stakeholders: Führung

| Bezeich-nung | Typ | Beschreibung | Begründung / Referenz |
|---|---|---|---|
| **224-Führ-1** | B | Die IAM-Steuerung (der Gemeinschaft) MUSS entscheiden, welche Anforderungen der ver-schiedenen Stakeholder sinnvollerweise erfüllt werden können und MUSS Widersprüche auf-lösen.[14] | Prinzip-9<br>Führ-5 |
| **224-Führ-2** | B | Die IAM-Steuerung (der Gemeinschaft) KANN Ausnahmen für bestehende (Alt-)Systeme defi-nieren. | Prinzip-9 |
| **224-Führ-3** | B | Die IAM-Steuerung (der Gemeinschaft) MUSS ein Qualitätsmodell für die Authentifizierung de-finieren, das den Anforderungen aller Stakehol-dern gerecht wird. | LE-7,<br>Reg-2 |
| **224-Führ-4** | B | Die IAM-Steuerung (der Gemeinschaft) KANN ein Qualitätsmodell für die Attribute definieren, das den Anforderungen aller Stakeholdern ge-recht wird. | LE-7,<br>Reg-2 |
| **224-Führ-5** | B | Die IAM-Steuerung (der Gemeinschaft) MUSS die Formate der Authentifizierungsanfrage und -antwort, sowie Attributanfragen und -bestäti-gungen definieren, sodass die Anforderungen aller Stakeholdern erfüllt werden. | Prinzip-9,<br>IAM-4,<br>Führ-2 |

Tabelle 4: Anforderungen des Stakeholders: Führung

[14] Die Bewertung der Anforderungen kann nach folgenden Kriterien erfolgen: Wirtschaftlichkeit (Budget, Kosten, Zeitrahmen), Einhaltung der Standards, Benutzerfreundlichkeit, Unterstützung von bestehenden Systemen usw.

# 7 Auswahl Identity Federation Modell

Die sich z.T. widersprechenden Anforderungen aus Kapitel 6, insbesondere zum Schutz der Privatsphäre, haben eine starke Auswirkung auf die Gestaltung des Identity Federation Modells. Daher sind in diesem Kapitel die betroffenen Anforderungen und ihre Auswirkung auf die Modellauswahl beschrieben. Abbildung 4 veranschaulicht graphisch den Auswahlprozess.
Es ist erlaubt, mehrere Vermittlermodelle zu kombinieren. Insbesondere «Vermittler Double Blinding» und «Vermittler Offene Quellen» können gut kombiniert werden. Die Gemeinschaft muss entsprechend den Anforderungen der beteiligten Parteien entscheiden, welche Identity Federation Modelle eingesetzt werden sollen und wie die Parteien eingebunden werden.

## 7.1 Einfluss der Anforderungen

**Anforderung 224-LE-3 (einfache RP-Integration)**

Diese Anforderung kann nur von vermittlerbasierten IAM-Systemen nach dem Hub-'n'-Spoke Modell (siehe eCH-0107 [2] Kap. 4.1) realisiert werden. In diesen vermittlerbasierten Systemen wird die Komplexität zwischen *n* Relying Parties und *m* IdP/APs reduziert und die RP kommuniziert nur noch mit **einer** Komponente, dem zentralen Vermittler. Dieser übernimmt auch zentrale Aufgaben, wie Metadaten-Management, Discovery Service, User Consent Abfrage, etc.

**Richtlinie:** Im E-Government MUSS ein vermittlerbasiertes Identity Federation System eingesetzt werden. Es MUSS eines der Vermittlermodelle («Vermittler Double Blinding», Vermittler Offene Quellen», «Vermittler Vertraulichkeitsschutz») oder eine **Kombination** davon realisiert werden.

**Vertraulichkeitsschutz am Vermittler - Anforderung 224-LB-5**

Der Vertraulichkeitsschutz am Vermittler bedeutet, dass dieser die durch ihn durchfliessenden Authentifizierungs- und Attributbestätigungen vor Missbrauch schützt. Dieser Vertraulichkeitsschutz kann **rechtlich/organisatorisch** oder **technisch** realisiert werden.

**Richtlinie:** Im Fall einer technischen Umsetzung des Vertraulichkeitsschutzes MUSS das Modell «Vermittler Vertraulichkeitsschutz» eingesetzt werden.

In diesem Modell werden die Attributbestätigungen, die ggf. sensible und persönliche Daten enthalten können, nur für den Endempfänger (RP) verschlüsselt dem Vermittler übergeben und können daher von diesem nicht eingesehen werden. Das hat aber Auswirkungen auf andere Anforderungen zum Schutz der Privatsphäre, wie 224-LB-2 (Nichtverfolgbarkeit RP) und 224-LB-3 (Nichtverfolgbarkeit IdP), die dann nur mit zusätzlichen technischen Massnahmen (z.B. anonymisierte Kurzzeit-Zertifikate), die in diesem Standard nicht beschrieben werden, erfüllt werden können.

Im Fall einer rechtlich/organisatorischen Umsetzung müssen andere Kriterien, wie das realisierte Szenario oder die Anforderungen zum Schutz der Privatsphäre des Subjektes zur Auswahl des Identity Federation Modells herangezogen werden.

**Anforderung 224-LB-2 (Nichtverfolgbarkeit RP)**

Diese Anforderung sollte erfüllt werden, wenn der Schutz der Privatsphäre des Subjektes wichtig ist.
Bei Erfüllung der Anforderung wird sichergestellt, dass die Identitätslieferanten nicht feststellen können, welche Ressource (welche RP) das Subjekt verwendet. Die Anforderung wird automatisch erfüllt, wenn der Vertraulichkeitsschutz am Vermittler nicht technisch realisiert wird.

**Richtlinie:** Wenn die Nichtverfolgbarkeit (RP) gefordert ist, MUSS entweder ein «Vermittler Double Blinding» oder ein «Vermittler Offene Quellen» realisiert werden.

**Anforderung 224-LB-3 (Nichtverfolgbarkeit IdP)**

Diese Anforderung sollte erfüllt werden, wenn der Schutz der Privatsphäre des Subjektes wichtig ist. Bei Erfüllung der Anforderung wird sichergestellt, dass die RP nicht feststellen kann, wo sich das Subjekt authentifiziert hat und welche AP die Attribute bestätigt hat. Bei Erfüllung von 224-LB-3 kann 224-LE-5 (Datenherkunft) nicht erfüllt werden.

**Richtlinie:** Wenn die Nichtverfolgbarkeit (IdP) gefordert ist, MUSS ein «Vermittler Double Blinding» realisiert werden.

**Anforderung 224-LE-5 (Datenherkunft)**

Die Anforderung verlangt, dass eine RP die Herkunft von Authentifizierung- und Attributbestätigungen und – je nach Implementierung - die Herkunft der Bestätigungen überprüfen (z. B. durch Prüfen der Signatur des Quellsystems oder anhand eines Attributes) kann. Wird diese Anforderung erfüllt, ist maximal ein einseitiges «Blinding» möglich, da die RP immer die Quellsysteme kennt (224-LB-3 kann nicht erfüllt werden).

**Richtlinie:** Wenn die Datenherkunft gefordert ist, MUSS ein «Vermittler Offene Quellen» realisiert werden.

**Anforderung 224-LE-6 (Datenunversehrtheit)**

Die RP kann die Integrität und Vollständigkeit von Authentifizierung- und Attributbestätigungen ab der Quelle überprüfen (z. B. durch Prüfen einer Signatur des Quellsystems).
Diese Anforderung kann nur erfüllt werden, wenn auch Anforderung 224-LE-5 (Datenherkunft) erfüllt ist. Die Anforderung 224-LB-3 kann nicht erfüllt werden.

**Richtlinie:** Wenn die Datenunversehrtheit gefordert ist, MUSS auch die Anforderung zur Datenherkunft erfüllt werden. Ein «Vermittler Offene Quellen» MUSS realisiert werden.

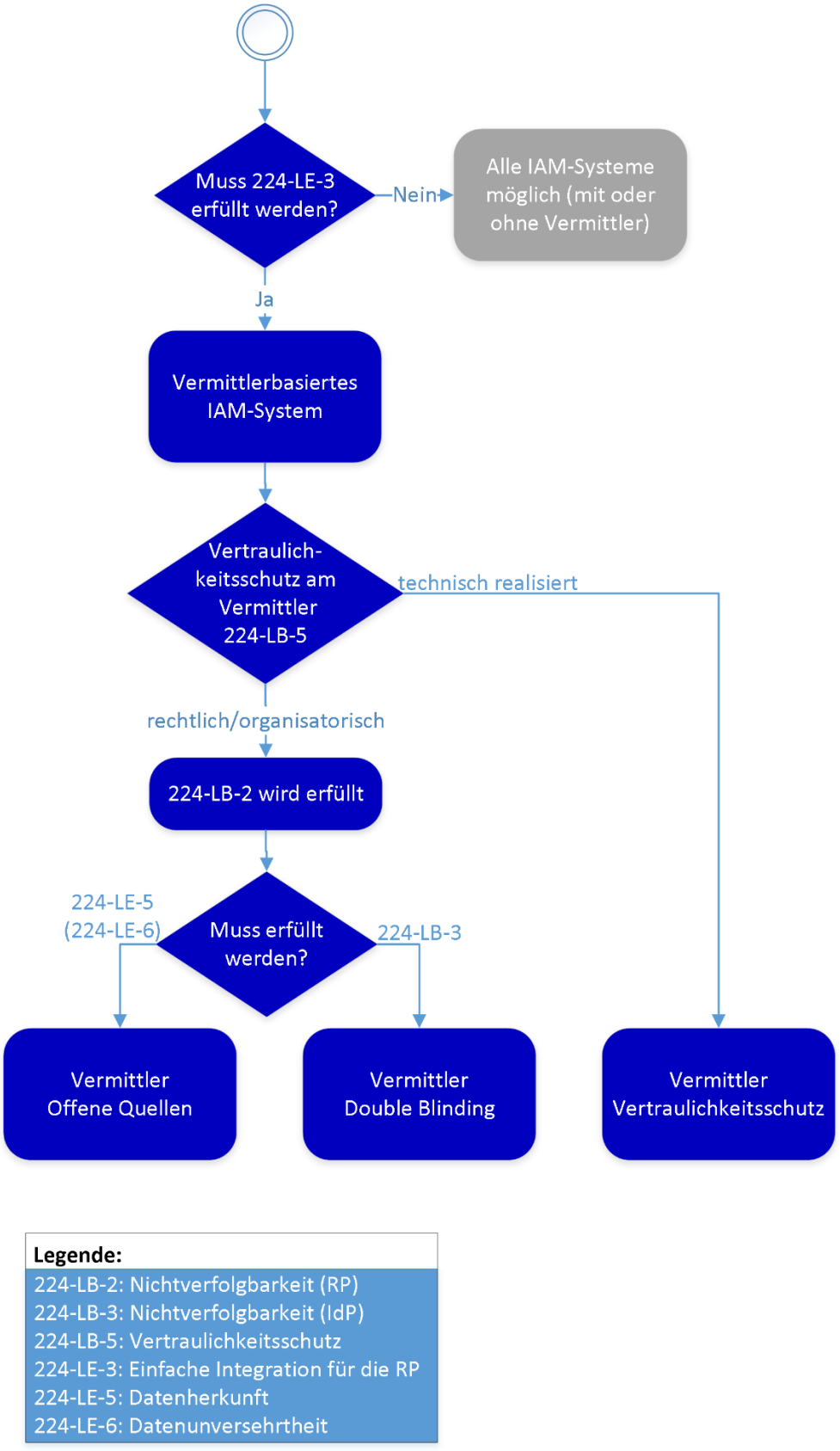


Abbildung 4: Entscheidungsbaum zur Auswahl der Identity Federation Modelle

## 7.2 Einfluss der Szenarien

**G2G Szenario**

In einem G2G Szenario, in dem im Normalfall nur Enterprise-Attribute der Mitarbeiter von Behörden zusammen mit den Authentifizierungsergebnissen bestätigt werden und diese nur für die Zugangs- und Zugriffsentscheidung verwendet werden, ist ein Schutz der Privatsphäre des Subjektes meist weniger relevant. Dafür ist häufig wichtig, die Herkunft der Bestätigungen zu kennen (224-LE-5).

**Empfehlung G2G:** Für ein G2G Szenario SOLLTE ein «Vermittler Offene Quellen» zum Einsatz kommen.

**G2B Szenario**

Im G2B Szenario spielt der Schutz der Privatsphäre eine Rolle, wenn auch nicht ganz so wie im Falle von G2C, da im Normalfall - wie im G2G - nur Enterprise-Attribute für Zugangs- und Zugriffsentscheidung verwendet werden sollten. Persönliche Daten der Personen, die die Organisation vertreten, sollten daher nicht angefordert werden. Die Anforderung 224-LB-5 (Vertraulichkeit) muss daher nicht erfüllt werden. Im Gegensatz zur Anforderung 224-LB-2 (Nichtverfolgbarkeit RP), die erfüllt werden muss, um Missbrauch auszuschliessen.

**Empfehlung G2B:** Für ein G2B Szenario SOLLTE ein «Vermittler Offene Quellen» oder «Vermittler Double Blinding» zum Einsatz kommen, je Realisierungsentscheid von 224-LE-5 (Datenherkunft).

**G2C Szenario**

Die Anforderungen zum Schutz der Privatsphäre 224-LB-2 (Nichtverfolgbarkeit RP) und 224-LB-3 (Nichtverfolgbarkeit IdP), sowie 224-LB-5 (Vertraulichkeit) schliessen sich bei Einhaltung von 224-IAM-3 (etablierte Technologien) aus. Eine Umsetzung all dieser Anforderungen sind nur mit Hilfe «Tokenbasierter Identity Federation Modelle» (Attribute sind im Umfeld des Subjekts hinterlegt - siehe Anhang G) möglich, deren Realisierung beim heutigem Stand der Technik (Q2 2018) sehr aufwändig wäre (widersprüche Prinzip-9 eCH-0107 [2]).

**Richtlinie G2C mit Vertraulichkeit**: Muss in einem G2C Szenario die Anforderung 224-LB-5 (Vertraulichkeit) erfüllt werden, so MUSS ein «Vermittler Vertraulichkeitsschutz» realisiert werden.

**Richtlinie G2C mit Nichtverfolgbarkeit RP**: Muss in einem G2C Szenario die Anforderung 224-LB-2 (Nichtverfolgbarkeit RP) erfüllt werden, so MUSS ein «Vermittler Offene Quellen» oder ein «Vermittler Double Blinding» verwendet, je nach Realisierungsentscheid von 224-LE-5 (Datenherkunft) bzw. und 224-LB-3 (Nichtverfolgbarkeit IdP).

## 7.3 Nicht-vermittlerbasierte Systeme

Eine Identity Federation ohne Vermittler kann unter den folgenden Bedingungen sinnvoll sein:

- Die Identity Federation wird innerhalb einer Organisation eingesetzt. Unter diesen Umständen ist die Nichterfüllung der Anforderungen 224-LB-2 (Nichtverfolgbarkeit

RP) und 224-LB-3 (Nichtverfolgbarkeit IdP) nicht gegeben bzw. wird die Verfolgbarkeit z.T. gefordert. Das schliesst das Szenario G2C aus, da ein Szenario, das den Bürger einschliesst, immer über Organisationsgrenzen hinweg geht.
- Im Normalfall fordert die Erfüllung der Anforderung 224-LE-3 (einfache RP-Integration) den Einsatz eines Vermittlers. Wenn allerdings in der Identity Federation nur ein oder wenige IdPs verwendet werden, kann auf die Vereinfachung mittels Vermittler verzichtet werden.
- Wenn eine Vertrauensstufe 4 nach eCH-0170 gefordert ist, kann der Einsatz eines Vermittlers die Umsetzung der geforderten erhöhten Sicherheit (z.B. Holder-Of-Key-Verfahren) erschweren oder sogar verunmöglichen.

Tabelle 5: Erfüllung der Anforderungen einer nicht-vermittlerbasierten Identity Federation

| Anforderung | Erfüllungsgrad | Bemerkung |
|---|---|---|
| **224-LB-2 (Nichtverfolgbarkeit RP)** | Nicht erfüllt | |
| **224-LB-3 (Nichtverfolgbarkeit IdP)** | Nicht erfüllt | |
| **224-LB-5 (Vertraulichkeitsschutz)** | möglich | |
| **224-LE-3 (einfache RP-Integration)** | Nicht erfüllt | Nur erfüllbar, wenn einer oder wenige IdPs verwendet werden |
| **224-LE-5 (Datenherkunft)** | möglich | |
| **224-LE-6 (Datenunversehrtheit)** | möglich | |

**Richtlinie**: Szenarien, die auf der Erfüllung von Anforderung 224-LB-2 (Nichtverfolgbarkeit RP) oder 224-LB-3 (Nichtverfolgbarkeit) bestehen, SOLLTEN ein Modell ohne Vermittler NICHT verwenden.

## 7.4 Vermittler Double Blinding

Ein «Vermittler Double Blinding» muss die Protokollabschnitte P1 und P2 vollständig voneinander trennen. Protokollabschnitt P1 beschreibt die Kommunikation zwischen RP und Vermittler, P2 die Kommunikation zwischen Vermittler und IdPs, APs sowie IdP/APs.
Alle Beteiligten im IAM System vertrauen dem Vermittler, dass er die durch ihn durchfliessenden Informationen vertraulich behandelt und nicht missbraucht. Dieses Vertrauen wird rechtlich/organisatorisch abgestützt.
Der Vermittler realisiert ein *Double Blinding*, d.h. die RP erhält keinerlei Informationen, aus denen sie darauf schliessen kann, bei welchem IdP das Subjekt authentifiziert wurde und von welchen APs mögliche Attribute stammen. Ausserdem, bekommt auch der IdP bzw. IdP/AP und verwendete APs keine Informationen, auf welche RP das Subjekt zugreifen möchte.

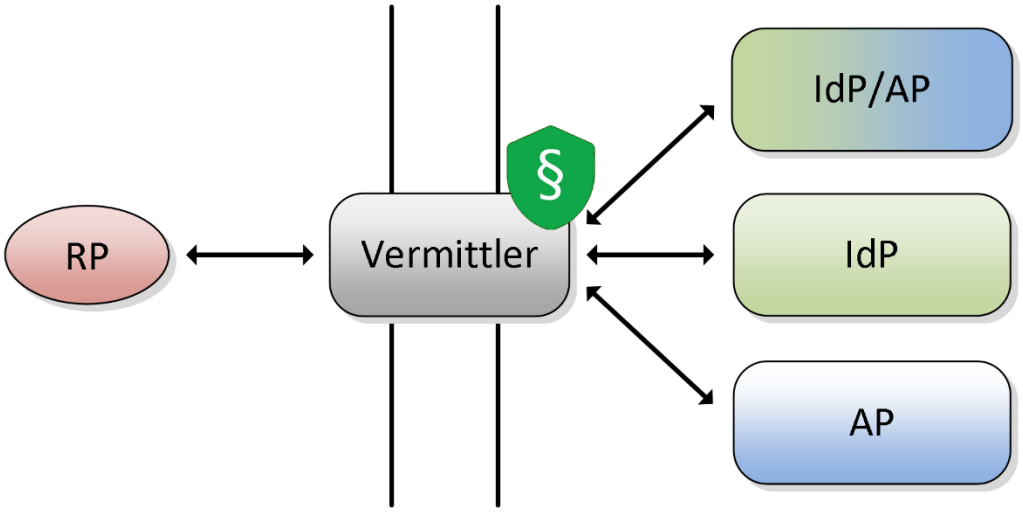


Abbildung 5: Vermittler Double Blinding

In der folgenden Tabelle sind die für eine Entscheidung relevanten Anforderungen sowie deren Erfüllungsgrad aus Kapitel 6 aufgelistet.

Tabelle 6: Erfüllung der Anforderungen des "Vermittlers Double Blinding"

| Anforderung | Erfüllungsgrad | Bemerkung |
|---|---|---|
| **224-LB-2 (Nichtverfolgbarkeit RP)** | erfüllt | |
| **224-LB-3 (Nichtverfolgbarkeit IdP)** | erfüllt | |
| **224-LB-5 (Vertraulichkeitsschutz)** | Nur rechtl./organisatorisch | Vermittler «sieht» Attributbestätigungen |
| **224-LE-3 (einfache RP-Integration)** | erfüllt | |
| **224-LE-5 (Datenherkunft)** | Nicht erfüllt | |
| **224-LE-6 (Datenunversehrtheit)** | Nicht erfüllt | |

Das Modell «Vermittler Double Blinding» kann für alle Szenarien eingesetzt werden.

**Richtlinie**: Szenarien, die auf der Erfüllung von Anforderung 224-LE-5 (Datenherkunft) oder 224-LE-6 (Datenunversehrtheit) bestehen, DÜRFEN das Modell «Vermittler Double Blinding» NICHT verwenden.

Dieses Modell wird auch bei STIAM im Identity Proxying Mode (IP-Mode) verwendet (siehe eCH-0168 [4], Kapitel 3.4.1).

## 7.5 Vermittler Offene Quellen

Ein «Vermittler Offene Quellen» ist von der Funktionsweise ähnlich wie ein «Vermittler Double Blinding» (siehe Kapitel 7.4).
Der Vermittler realisiert nur ein einseitiges «Blinding»:

- IdP bzw. IdP/AP und verwendete APs erhalten wie bisher keine Informationen, auf welche RP das Subjekt zugreifen möchte.

- Der Vermittler übermittelt der RP aber sichtbar die Information darüber bei welchem IdP das Subjekt authentifiziert wurde und von welchen APs die Attribute stammen. Das kann auch nur für den IdP oder ausgewählte APs geschehen.

Bei der Offenlegung von Quellen muss zwischen *Sichtbarkeit* und *Verifizierbarkeit* unterschieden werden.

- **Sichtbarkeit** bedeutet, dass der Vermittler dem RP mitteilt, von wo die ursprüngliche Antwort stammt. Das kann z.B. in Form eines Attributs geschehen.
- **Verifizierbarkeit** bedeutet, dass die RP anhand einer Signatur die Quelle und Unversehrtheit der Attribute überprüfen kann. Dabei werden die ursprünglich signierten Attribute vom Vermittler an die RP weitergeleitet. Dieses Verhalten ist erlaubt, wird aber nicht weiter in diesem Standard behandelt.

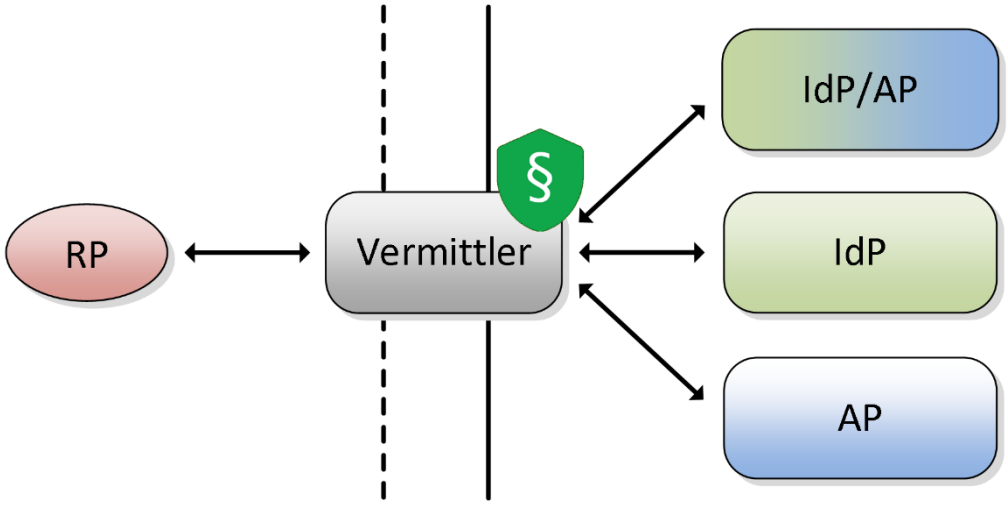


Abbildung 6: Vermittler Offene Quellen

In der folgenden Tabelle sind die für eine Entscheidung relevanten Anforderungen sowie deren Erfüllungsgrad aus Kapitel 6 aufgelistet.

Tabelle 7: Erfüllung der Anforderungen des "Vermittlers Offene Quellen"

| Anforderung | Erfüllungsgrad | Bemerkung |
|---|---|---|
| **224-LB-2 (Nichtverfolgbarkeit RP)** | erfüllt | |
| **224-LB-3 (Nichtverfolgbarkeit IdP)** | Nicht erfüllt | |
| **224-LB-5 (Vertraulichkeitsschutz)** | Nur rechtl./organisatorisch | Vermittler «sieht» Attributbestätigungen |
| **224-LE-3 (einfache RP-Integration)** | erfüllt | |
| **224-LE-5 (Datenherkunft)** | erfüllt | |
| **224-LE-6 (Datenunversehrtheit)** | möglich | Mit Attributbestätigungen, die vom IdP/AP oder AP signiert sind. |

Das Modell «Vermittler Offene Quellen» ist demnach hauptsächlich für G2G Szenarien geeignet. Es kann für G2B und G2C Szenarien verwendet werden, wenn die Erfüllung der Anforderung 224-LB-3 (Schutz der Privatsphäre) nicht gefordert ist.

| **Richtlinie**: Das Modell «Vermittler Offene Quellen» DARF NICHT verwendet werden, wenn die Anforderung 244-LB-3 (Schutz der Privatsphäre) gefordert wird. |
|---|

## 7.6 Vermittler Vertraulichkeitsschutz

Bei einem «Vermittler Vertraulichkeitsschutz» muss die Vertraulichkeit der Attributbestätigungen technisch durch Verschlüsselung realisiert werden. Dadurch ist es dem Vermittler nicht möglich auf die Attributwerte zuzugreifen oder diese zu verändern.
Die Attribute müssen von der Quelle (IdP/AP oder AP) signiert und für die RP verschlüsselt werden. Die RP kann somit nachvollziehen, wer die Attribute ausgestellt hat.
Die technische Realisierung des Vertraulichkeitsschutzes verhindert ein «Blinding» zwischen RP und Attribut Providers (IdP/AP und APs), wie in den anderen beiden Modellen[15].

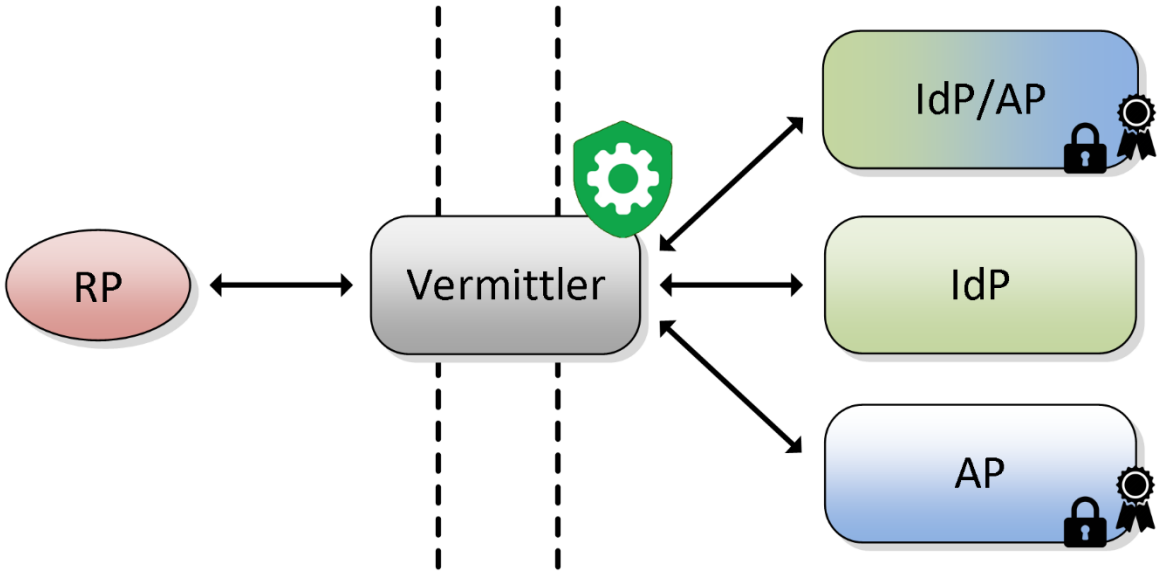


Abbildung 7: Vermittler Vertraulichkeitsschutz

In der folgenden Tabelle sind die für eine Entscheidung relevanten Anforderungen sowie deren Erfüllungsgrad aus Kapitel 6 aufgelistet.

Tabelle 8: Erfüllung der Anforderungen des "Vermittlers Vertraulichkeitsschutz"

| Anforderung | Erfüllungsgrad | Bemerkung |
|---|---|---|
| **224-LB-2 (Nichtverfolgbarkeit RP)** | Nicht erfüllt | |
| **224-LB-3 (Nichtverfolgbarkeit IdP)** | Nicht erfüllt | |
| **224-LB-5 (Vertraulichkeitsschutz)** | Am Vermittler technisch realisiert | |
| **224-LE-3 (einfache RP-Integration)** | z.T. erfüllt | Vertraulichkeitsschutz erhöht den Aufwand für die RP |
| **224-LE-5 (Datenherkunft)** | Erfüllt | |

[15] Ausgenommen es werden anonymisierte Kurzzeitzertifikate zur Verschlüsselung der Daten verwendet. Dieser Ansatz wird in diesem Standard nicht weiterverfolgt.

| | | |
|---|---|---|
| **224-LE-6 (Datenunversehrtheit)** | Erfüllt | |

Das Modell «Vermittler Vertraulichkeitsschutz» ist für G2C Szenarien geeignet, wenn der «Schutz der Privatsphäre» weniger relevant ist. Der Nachteil ist, dass RPs und IdPs dann einfacher Verhaltensmuster der Subjekte erstellen können.

Im G2G Szenarien kann das Modell verwendet werden, wenn die Erfüllung der Anforderung 224-LE-5 (Datenherkunft) und 224-LE-6 (Datenunversehrtheit) gefordert sind. Für G2B ist das Modell eher ungeeignet, da die Anforderung 224-LB-2 nicht erfüllt wird.

**Richtlinie**: Das Modell «Vermittler Vertraulichkeitsschutz» DARF NICHT verwendet werden, wenn die Anforderung 224-LB-2 oder 224-LB-3 gefordert wird.

# 8 Vermittlermodelle

In diesem Kapitel werden die Vermittlermodelle im Detail definiert. Zunächst werden wichtige Konzepte eingeführt und dann die Modelle «Vermittler Double Blinding», «Vermittler offene Quellen», und «Vermittler Vertraulichkeitsschutz» spezifiziert.

## 8.1 Grundlegende Konzepte zu den Vermittlermodellen

In den folgenden Kapiteln werden die grundsätzlichen Konzepte spezifiziert. Einerseits sind die Protokollabschnitte zwischen RP, Vermittler und IdP/AP (AP), sowie die relevanten Prozesse und spezifischen Tätigkeiten erklärt.

### 8.1.1 Protokollabschnitte

Die Kommunikation zwischen den Komponenten wird in zwei verschiedene Protokollabschnitte unterteilt. Wie in der Abbildung 8 beschreibt der Abschnitt P1 die Kommunikation zwischen RP und Vermittler. P2 beschreibt die Kommunikation zwischen Vermittler und IdPs, APs sowie IdP/APs. In P3 läuft die Kommunikation ohne Vermittler, direkt zwischen RP und IdP/AP bzw. AP ab.

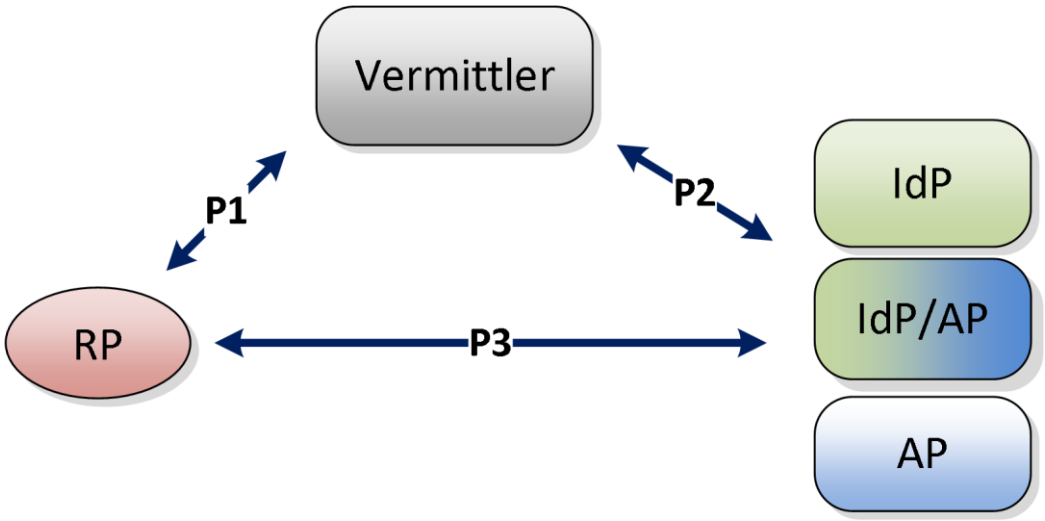


Abbildung 8: Protokollabschnitte

Bei allen Verfahren muss ein Metadaten Management, Trust Management und IdP-Discovery vorhanden sein. Am einfachsten übernimmt das der Vermittler. Die Authentifizierungs- und Attributbestätigungen muss in jedem Fall signiert sein (siehe eCH-0107 [2] Anforderungen IAM-7, IAM-9 und IAM-11). So kann die Authentizität und Integrität der Bestätigungen überprüft werden.

#### 8.1.1.1 Protokollabschnitt zwischen RP und Vermittler (P1)

Für den Protokollabschnitt zwischen RP und Vermittler gibt es zwei Möglichkeiten:

1. Die ganze Kommunikation zwischen der RP und dem Vermittler wird über die Client-Plattform (z. B. Browser) des Subjekts abgehandelt.
2. Nur der Authentifizierung-Prozess wird über die Client-Plattform abgehandelt. Alle folgenden Kommunikationsschritte werden über einen Back-Channel abgehandelt.

Beide Verfahren haben Vor- und Nachteile. Diese werden in den folgenden Kapiteln erläutert. Welches Verfahren eingesetzt wird, muss gemäss Sicherheitsanforderung und Anwendungsgebiet von der Gemeinschaft evaluiert werden.

#### 8.1.1.1.1 Authentifizierungs- und Attributbestätigung über Front-Channel

Bei diesem Verfahren läuft die gesamte Kommunikation über die Client Plattform (z. B. Browser) des Subjekts. Das Subjekt wird über die Client-Plattform authentifiziert. Dabei werden die Authentifizierungs- und eventuellen Attributbestätigungen über die Client-Plattform an die RP übermittelt. Dies ist eine einfache Art, wie ein Subjekt authentifiziert werden kann.

Es müssen einige Sicherheitsaspekte beachtet werden. Da die Kommunikation vollständig über die Client-Plattform läuft, muss evaluiert werden in welchem Umfang die Kommunikation geschützt werden muss. Grundsätzlich kann die Client-Plattform die Kommunikation einsehen und manipulieren.

Als Gegenmassnahme können grundsätzlich zwei Massnahmen getroffen werden. Eine Absicherung auf Transportebene oder auf inhaltlicher Ebene. Nur eine Verschlüsselung der Authentifizierungs- und Attributbestätigung auf inhaltlicher Ebene bietet einen wirksamen Schutz gegen eine neugierige oder kompromittierte Client-Plattform an. Die Verschlüsselung und Authentisierung auf Transportebene (z.B. TLS) bietet nur Schutz auf dem Kommunikationskanal.

Dieses Verfahren ist nicht empfehlenswert, wenn der Vermittler die RP nicht bereits bei der Authentifizierungs- und Attributanfrage eindeutig identifizieren kann, da in diesem Fall der Vermittler nicht überprüfen kann, ob die RP berechtigt ist Authentifizierungs- bzw. Attributbestätigungen anzufordern. In diesem Fall sollte das im Kapitel 8.1.1.1.2 Verfahren verwendet werden.

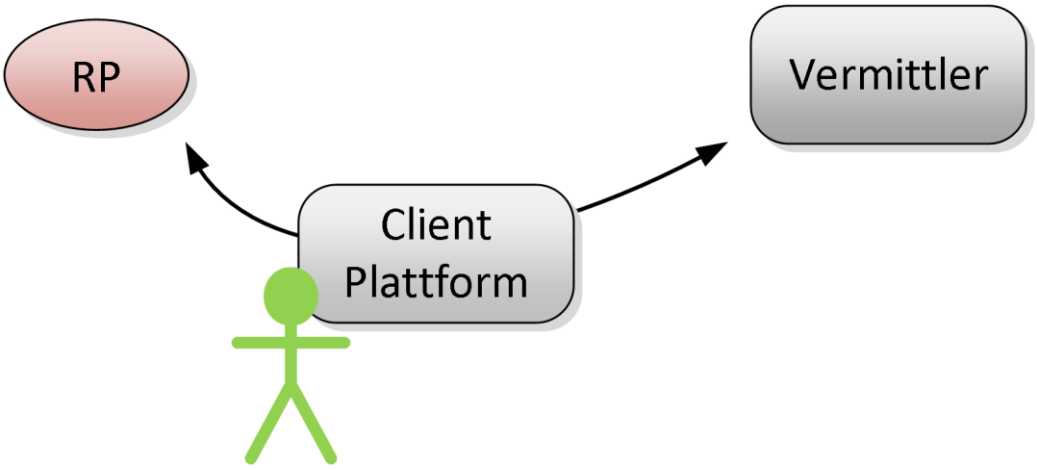


Abbildung 9: Protokollabschnitt P1 – Front-Channel

Nach Erhalt der Authentifizierungs- und Attributbestätigung muss die RP die Signaturen validieren.

#### 8.1.1.1.2 Authentifizierungs- und Attributbestätigung über Back-Channel

Das Subjekt wird mit Hilfe der Client-Plattform (z.B. Browser) authentifiziert. Nach erfolgreicher Authentifizierung wird anstatt einer Authentifizierungs- bzw. Attributbestätigung, eine

Referenz an die RP über die Client-Plattform gesendet. Diese Referenz darf keine Daten beinhalten, die auf die Identität des Subjekts schliessen lassen. Die RP kann nun über einen Back-Channel die Authentifizierungs- bzw. Attributbestätigung beim Vermittler anfordern.

Der Vorteil dieses Verfahrens ist, dass die Client Plattform keine Daten vom Subjekt sieht und somit keine besonderen Massnahmen getroffen werden müssen, um diese zu schützen. Auch kann der Vermittler über diesen sicheren Back-Channel überprüfen, ob die RP berechtigt ist, Authentifizierungs- bzw. Attributbestätigungen anzufordern. Die Back-Channel Kommunikation muss auf der Transport-Ebene geschützt werden (z.B. mittels TLS), da sie direkt zwischen RP und Vermittler abläuft.

Nachteil dieses Verfahrens ist, dass aufgrund einer weiteren Abfrage die RP geringfügig mehr Logik implementieren muss, um die Authentifizierungs- bzw. Attributbestätigungen zu erhalten.

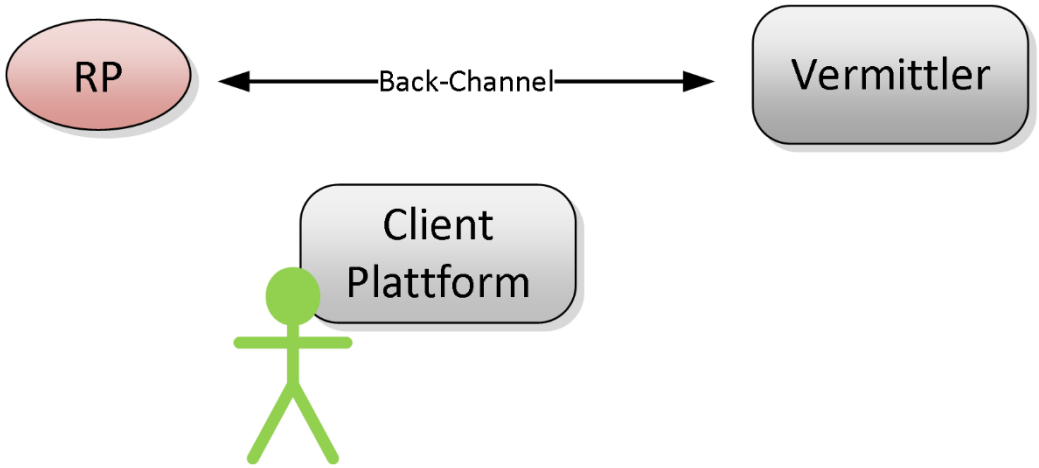


Abbildung 10: Protokollabschnitt P1 - Back-Channel

Nach Erhalt der Authentifizierungs- und Attributbestätigung muss die RP die Signaturen validieren.

#### 8.1.1.2 Protokollabschnitt zwischen Vermittler und IdP, AP und IdP/AP (P2)

In diesem Kapitel wird beschrieben, wie die Kommunikation zwischen Vermittler und den beteiligten IdPs, APs und IdP/APs erfolgt. Es gibt verschiedene Varianten, die je nach Ausgangslage, Sicherheitsanforderungen und Anwendungsgebiet eingesetzt werden.

##### 8.1.1.2.1 Authentifizierung und Attributabfrage von einer Quelle

Bei diesem Verfahren wird das Subjekt authentifiziert und es können Attribute vermittelt werden.

Wie im Protokollabschnitt P1 gibt es auch hier zwei Möglichkeiten Authentifizierungs- und Attributbestätigung weiterzugeben.

Die Authentifizierungs- und Attributbestätigung kann per Front-Channel über die Client Plattform an den Vermittler übermittelt werden (analog zu Kapitel 8.1.1.1.1).

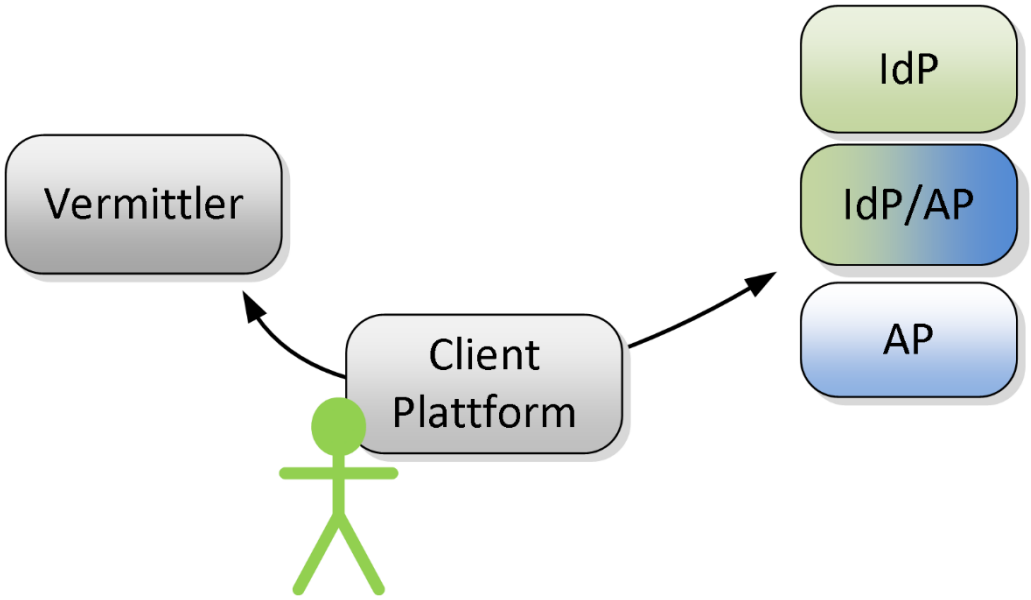


Abbildung 11: Protokollabschnitt P2 - Front- Channel

In der zweiten Möglichkeit kann eine Referenz über die Client Plattform an den Vermittler gesendet werden. Mit Hilfe der Referenz kann der Vermittler die Authentifizierungs- und Attributbestätigung beim IdP abrufen (analog zu Kapitel 8.1.1.1.2).

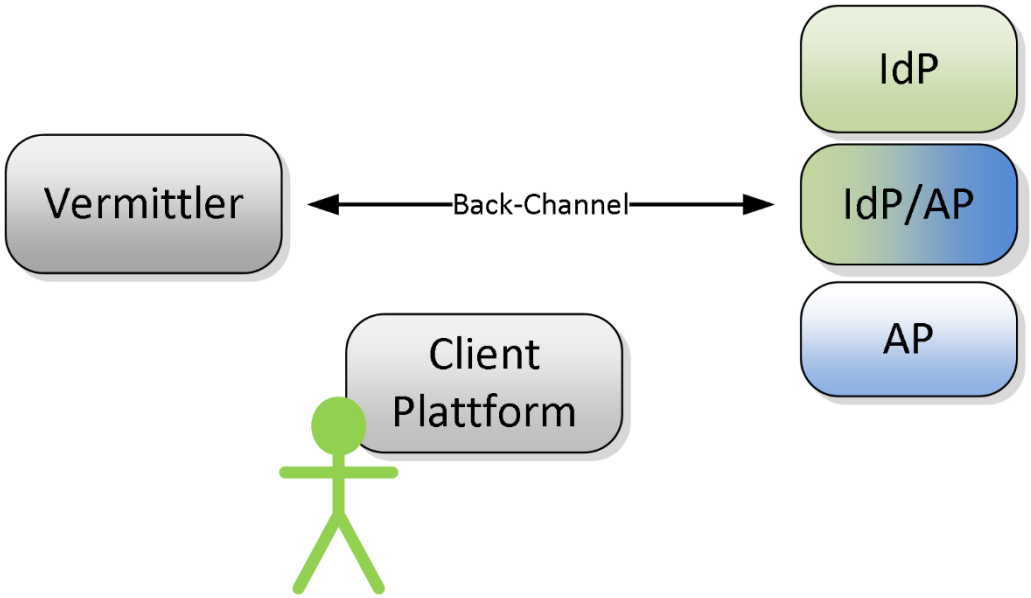


Abbildung 12: Protokollabschnitt P2 - Back-Channel

In beiden Fällen muss der Vermittler die Signaturen der Bestätigungen überprüfen. Eine der beiden möglichen Verfahren muss realisiert werden.

#### 8.1.1.2.2 Abfrage von Attributen aus mehreren Quellen

Bei diesem Verfahren wird das Subjekt authentifiziert und Attribute aus mehreren Quellen werden zusammengetragen und vermittelt. Somit ist eine Aggregation von Attributen nötig. Die dabei verwendeten E-Identities müssen im Vorfeld während der Definitionszeit verknüpft werden.

Es gibt zwei verschiedene Varianten, wie und von wem die Attribute aggregiert werden. Welche Variante verwendet wird, ist abhängig vom verwendeten Vermittlermodell und muss anhand der Ausgangslage, den Sicherheitsanforderungen und dem Anwendungsgebiet entschieden werden.

**Vermittler aggregiert Attribute**

Nach der Authentifizierung (siehe Kapitel 8.1.1.2.1) muss anhand der Metadaten entschieden werden, welche APs abgefragt werden. Der Vermittler sendet eine Attributanfrage an die entsprechenden APs über einen direkten Kanal (Back-Channel).

Die APs muss mit geeigneten Massnahmen die Attributanfragen überprüfen. Nach erfolgreicher Prüfung generieren die APs Attributbestätigungen und senden diese zum Vermittler.

Der Vermittler muss anschliessend die Attributbestätigungen aggregieren.

**Vermittler vermittelt Attributreferenzen**
Diese Variante kommt im Modell «Vermittler Vertraulichkeitsschutz» zum Einsatz.

Nach der Authentifizierung (siehe Kapitel 8.1.1.2.1) muss anhand der Metadaten entschieden werden, welche APs abgefragt werden. Der Vermittler generiert entsprechende Referenzen und muss diese an die RP schickten. Die RP muss anschliessend mit Hilfe der Referenz die AP direkt abfragen (siehe 8.1.1.3).

### 8.1.1.3 Protokollabschnitt zwischen RP und IdP/AP oder AP (P3)

Dieser Protokollabschnitt wird nur verwendet, wenn die RP die Attribute direkt bei der Attributquelle abholt (Vermittler Vertraulichkeitsschutz).

Erhält die RP vom Vermittler eine Referenz (z. B. in Form einer URI und eines Access Token), kann diese über einen Back-Channel Attribute direkt bei einem IdP/AP bzw. einem AP anfordern. Der IdP/AP bzw. AP muss die Echtheit der Referenz überprüfen bevor sie die Attribute an die RP übergibt. Die RP muss beim Erhalt der Attributbestätigung die Signatur validieren.

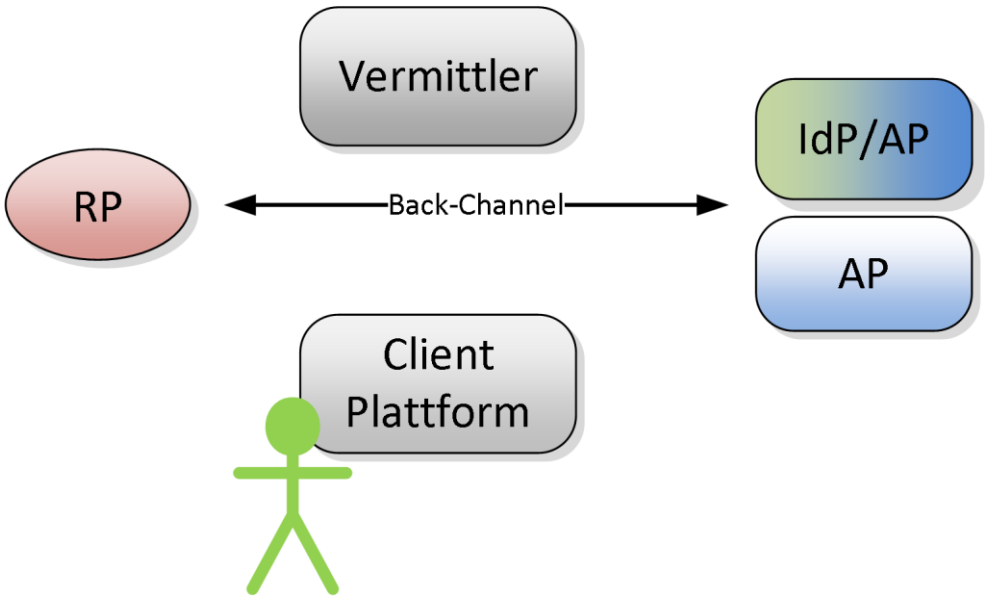


Abbildung 13: Protokollabschnitt P3

### 8.1.2 Session Handling

Je nach Anforderungen und Anwendungsfälle der Identity Federation, kann der Vermittler unterschiedlich implementiert werden:

- **Stateless**: Der Vermittler persistiert grundsätzlich keine Daten zur Laufzeit. Der Vermittler beantwortet Authentifizierungsanfragen mit Authentifizierungsbestätigungen (z. B. in OIDC mit Authentication Code Flow), hält aber keine keine Session bezüglich einer erfolgreichen Authentifizierung. Single Sign-On kann am IdP ermöglicht werden. Single Logout kann nicht realisiert werden. Wenn der Vermittler stateless betrieben wird, können nicht alle Anwendungsfälle abgedeckt werden. Nur die Anwendungsfälle Authentifizierung und Identitätsvermittlung können realisiert werden.
- **Stateful**: Der Vermittler kontrolliert die Sessions. Alle Anwendungsfälle können abgedeckt werden (z.B. können Attribute von mehreren Quellen aggregiert werden). Der Vermittler kann so mehrere Authentifizierungsanfragen unterschiedlichen RPs beantworten, ohne dass sich das Subjekt erneut beim IdP authentifizieren muss. Der User Consent kann zentral beim Vermittler verwaltet werden. Je nach verarbeiteten und gespeicherten Daten, müssen weitere Datenschutzrichtlinien beachtet werden.

### 8.1.3 Prozesse

Die grundlegenden Prozesse eines föderierten IAM sind in den Gestaltungsprinzipien für die Identitäts- und Zugriffsverwaltung (eCH-0107 [2]) bereits ausführlich beschrieben. In den folgenden Abschnitten werden die einzelnen Prozesse eines Identity Federation Systems mit entsprechenden Stellen in eCH-0107 [2] und eCH-0170 [3] referenziert. Wenn notwendig werden die Tätigkeiten der Prozesse konkretisiert oder mit Beispielen ergänzt.

Folgende Prozesse müssen in einer vermittlerbasierten Identity Federation berücksichtigt werden.

Laufzeit:

- E-Identity bestätigen (eCH-0107 Kapitel 6.1.1)
  - Transformation von Authentifizierungsbestätigung
  - Identity Mapping (Identitätszusammenführung)
  - Einholen des User Consent
  - Transformation von Attributbestätigung
  - Attributaggregation
  - Protokoll Transformation
- IdP Discovery (eCH-0107 Kapitel 6.1.2)
- Subjekt authentifizieren (eCH-0107 Kapitel 6.1.3)
- E-Identity anreichern (eCH-0107 Kapitel 6.1.4)
  - Attributbestätigung
- Zugang erlauben (eCH-0107 Kapitel 6.1.5)
- Zugriff erlauben und Attribute offenlegen (eCH-0107 Kapitel 6.1.6)

Definitionszeit:

- E-Identity definieren (eCH-0107 Kapitel 6.2.1)
  - Identity Linking
  - Step-Up Registrierung
- Attribute definieren (eCH-0107 Kapitel 6.2.2)
- Authentifizierungsmittel definieren (eCH-0107 Kapitel 6.2.3)
- Zugangsregeln für E-Ressource definieren (eCH-0107 Kapitel 6.2.5)
- Zugriffsrechte für E-Ressource definieren (eCH-0107 Kapitel 6.2.6)

Etablierung:
- IAM-Führung führen
    - Metadaten Management

Im Folgenden werden die Tätigkeiten bezüglich eines vermittlerbasierten Identity Federation Systems konkretisiert.

#### 8.1.3.1 Transformation von Authentifizierungsbestätigung

Prozess: E-Identity bestätigen

Ein Vermittler muss in Abhängigkeit verschiedener Anforderungen Authentifizierungs- und Attributbestätigung transformieren. Eine Besonderheit ist die Transformation des Identifikators. Ein Vermittler sollte diesen in jedem Anwendungsfall anpassen (siehe Kapitel 5).

#### 8.1.3.2 Identity Mapping (Identitätszusammenführung)

Prozess: E-Identity bestätigen

Eine Applikation, welche mehrere Authentisierungsdienste zulässt (z.B. cloud basierte Lösungen oder Login über soziale Netzwerke), kann ein Identity Linking pflegen (vgl. dazu Kapitel 8.1.3.7).
Sobald ein Vermittler zwischen RP und IdP steht, kann die RP das Identity Mapping in Abhängigkeit des vom Vermittler erhaltenen Identifikators nur noch bedingt selbst ausführen. Die RP sollte das Identity Mapping bei Bedarf an den Vermittler delegieren.

#### 8.1.3.3 Einholen des User Consent

Prozess: E-Identity bestätigen

Generell gibt es zwei verschiedenen Möglichkeiten, den User Consent einzuholen. Eine der Möglichkeiten muss eingesetzt werden:
- **Ohne Attributwerte**: Der User Consent wird vom Vermittler **vor** der Attributabfrage bei den APs eingeholt. Das Subjekt kann so der Attributmenge zustimmen, aber bekommt keine Information über die Attributwerte.
- **Mit Attributwerten**: Der User Consent wird vom Vermittler **nach** der Attributabfrage bei den APs eingeholt. Das Subjekt erhält vollständige Informationen über die Attributwerte.

Grundsätzlich gilt, dass das Subjekt mindestens einmal die Attributmenge für eine Ressource freigibt. Wann welche Attributmenge für welche Ressource vom Subjekt freigegeben wurde, kann gespeichert werden. Somit kann das Subjekt auf eine Ressource zugriefen, ohne erneut das Einverständnis zu geben[16].

Sobald die Ressource eine andere Attributmenge verlangt, muss dem Subjekt die Möglichkeit gegeben werden, erneut das Einverständnis zu geben.

Das Einverständnis kann von mehreren Komponenten beim Subjekt eingeholt werden. Die Gemeinschaft muss entscheiden, welche Komponente den User Consent übernimmt, sowie

[16] Falls es nicht möglich ist das Einverständnis zu speichern, muss das Subjekt bei jeder Anfrage das Einverständnis geben.

die Art und Weise wie der User Consent dem Subjekt präsentiert und in welcher Form das Einverständnis gespeichert wird.

Die Attribute können auch abgefragt werden, wenn das Subjekt nicht (mehr) involviert ist (off-line access). Dazu muss das Einverständnis vom Subjekt eingeholt werden, dass dieser Vorgang erlaubt ist.
Bsp: Bei einem Newsletter-Versand wird die aktuelle E-Mail-Adresse des Subjekts abgefragt, bevor das E-Mail versendet wird.

Bei sogenannten Enterprise-Attributen (siehe IAM Glossar [1]), die implizit vom Subjekt freigegeben wurden (z. B. weil er sonst von Amtes wegen seine Aufgabe nicht wahrnehmen kann), ist keine Zustimmung des Subjekts notwendig.

#### 8.1.3.4 Transformation von Attributbestätigungen

Prozess: E-Identity bestätigen

Der Kontext, in welchem ein Attribut für eine Applikation eine bestimmte Bedeutung hat, muss von der Gemeinschaft vorgegeben werden. Über den Inhalt und die Semantik einer Attributinformation muss eine gewisse Übereinkunft zwischen den Teilnehmern bestehen. Damit Attributinformationen ihre Bedeutung in einem Identity Federation Umfeld nicht verlieren, von einer AP korrekt erstellt und von einer RP korrekt gelesen und interpretiert werden können, gibt es unterschiedliche Ansätze. Wenn eine Transformation von Attributbestätigungen nötig ist, muss mind. ein Ansatz zum Einsatz kommen:

- ***Abgleich über gemeinsames Schema*** (z. B. LDAP Schema). Damit ist keine Transformationslogik notwendig.
- Transformation eines Attributs zwischen Herausgeber und Konsument. Die Gemeinschaft gibt vor in welchem Rahmen eine Transformation erfolgen kann bzw. darf, ohne die Bedeutung eines Attributes zu verändern.
    - ***Transformation des Attributnamens:*** Auf dem Übermittlungsweg muss der Name eines Attributes nach genauen Regeln von einer dafür autorisierten Instanz angepasst werden. (z.B. ‚title' → ‚hasFunction')
    - ***Transformation des Attributwerts***: Auf dem Übermittlungsweg muss der Wert eines Attributes nach genauen Regeln von einer dafür autorisierten Instanz angepasst werden, ohne dabei die Bedeutung zu verändern. (z.B. ein Datumstransfer von '02.14PM' → '14:14' oder eine Aufteilung: ‚Adresse=Bernstrasse 42' → ‚Strasse=Bernstrasse' + ‚Hausnummer=42').

#### 8.1.3.5 Attribut Aggregation

Prozess: E-Identity bestätigen

Mit *Attribut Aggregation* bezeichnet man den Prozess, bei welchem Attribute zu einer bekannten E-Identity aus mehreren Quellen abgefragt und zusammengeführt werden. Dabei spielt es keine Rolle, ob ein AP zugleich auch IdP ist. Dieser Prozess kann zum Einsatz kommen.

#### 8.1.3.6 Protokoll Transformation

Prozess: E-Identity bestätigen
Vermittlerbasierte Identity Federation Systeme trennen die Seite der Informationslieferanten von den -konsumenten. Auf beiden Protokollabschnitten (P1, P2) können dasselbe, wie auch

unterschiedliche Protokolle zur Anwendung kommen (z.B. SAML ↔ SAML oder OIDC ↔ OIDC).
Wenn in einem vermittlerbasierte Identity Federation System unterschiedliche Protokolle auf den Protokollabschnitten (P1, P2) zum Einsatz kommen, muss der Vermittler diese übersetzen bzw. anpassen. Dies ist abhängig von den Eigenschaften und den Fähigkeiten der peripheren Kommunikationspartner.

#### 8.1.3.7 Identity Linking

Prozess: E-Identity definieren

Ein Bestandteil des Prozesses *E-Identity definieren* ist die Verwaltung von verbundenen E-Identities (LinkedID) über das Identity Linking. Dieser Vorgang kann von einem Subjekt selbst oder von einer dazu berechtigten Organisation durchgeführt werden. Beim Verlinken der E-Identities durch das Subjekt muss sichergestellt werden, dass sich das Subjekt so authentisiert, dass die Authentifizierungsstufe der höchsten Qualität der verknüpften E-Identities entspricht.
Das Identity Linking beinhaltet die Aktivierung/Deaktivierung einer Verbindung zwischen zwei bereits bestehenden E-Identities und deren verbundenen Attribute, aber nicht die Erzeugung, den Austausch und die Löschung von Attributen.

Die E-Identities können auf unterschiedliche Arten verlinkt werden. Wenn ein Identity Linking zum Einsatz kommt, muss eine der folgenden Arten verwendet werden:

- Ein gemeinsamer Identifikator (shared identifier).
- Protokoll (Linking Protokoll), um die E-Identities zu verknüpfen. Die Verknüpfung wird typischerweise in einer Linking-Tabelle auf dem Vermittler abgelegt.

#### 8.1.3.8 Step-Up Registrierung

Prozess: E-Identity definieren

Mit der Step-Up Registrierung kann eine E-Identity bezüglich ihrer Qualität aufgewertet werden. Dabei wird der Prozess ‘E-Identity definieren’ neu angestossen und das Subjekt gemäss der gewünschten Vertrauensstufe durch eine RA identifiziert und seine Beweismittel erneut verifiziert. Dazu können weitere Authentifizierungsfaktoren zum Authentifizierungsmittel hinzugefügt werden und/oder weitere Authentifizierungsmittel dem Subjekt ausgestellt werden.
Das Resultat einer Step-Up Registrierung muss folgendes eines der folgenden Resultate sein:

- Die E-Identity erreicht nach der erfolgreichen Registrierung eine höhere Vertrauensstufe.
- Das Subjekt erhält eine weitere E-Identity, die der höheren Vertrauensstufe entspricht.

#### 8.1.3.9 Metadaten Management

Prozess: IAM-Führung führen

Ein Metadaten Management muss von der Führung der Identity Federation übernommen werden. Sie bestimmt, wie die Metadaten im IAM-System aufgebaut sind und über welche Schnittstellen die Metadaten an die Beteiligten vermittelt werden.

Die beteiligten Partner sollten die Möglichkeit haben, über spezifische Schnittstellen Metadaten zu beziehen. Ausserdem sollte die Führung (gemäss den Anforderungen des IAM-Systems) Möglichkeiten anbieten, die Metadaten zu erfassen (z. B. eine RP kann eine E-Ressource erfassen und bestimmen, welche Qualität sie für die Authentifizierung und Attribute verlangt).

## 8.2 Vermittler Double Blinding

Im Fall vom «Vermittler Double Blinding» müssen die Protokollabschnitte vollständig voneinander getrennt werden. Der Vermittler ist der Protokollendpunkt für beide Protokollabschnitte. Die RPs und IdP/APs kennen sich nicht direkt. Dies beinhaltet, dass die Teilnehmer dem Vermittler vollständig vertrauen.

Vorgehen: Die RP möchte das Subjekt mit einer bestimmten Vertrauensstufe authentifizieren lassen und schickt eine entsprechende Anfrage an den Vermittler. Der Vermittler muss die Anfrage überprüfen und zeigt (bei erfolgreicher Überprüfung) dem Subjekt die IdPs an, die die Anforderungen der Anfrage erfüllen. Nachdem das Subjekt einen IdP gewählt hat, muss das Subjekt an den gewählten IdP weitergeleitet werden. Das Subjekt muss vom IdP authentifiziert werden.
Nach der Authentifizierung des Subjekts, muss der Vermittler eine vom IdP signierte Authentifizierungsbestätigung (und allfällige Attributbestätigungen aus derselben oder anderen Quellen) erhalten. Der Vermittler muss die Signatur validieren. Nach erfolgreicher Überprüfung muss der Vermittler die ursprüngliche(n) Signatur(en) entfernen und signiert selbst vor dem Versenden die Authentifizierungsbestätigung (und allenfalls die Attributbestätigung) neu.

Vor dem Signieren können weitere Tätigkeiten vom Vermittler durchgeführt werden:

- Identity Mapping & Transformation von Authentifizierungsbestätigung.
  Um das Korrelieren der E-Identities für die RPs zu erschweren, sollte für jede RP ein einmaliger zufälliger technischer Identifikator oder ein RP gebundener technischer Identifikator verwendet werden (siehe Kapitel 5.3.3 und 5.3.2).
- Attributaggregation & Transformation von Attributbestätigungen
- Protokolltransformation

Die Authentifizierungs- bzw. Attributbestätigung müssen gemäss Kapitel 8.1.1.1 an die RP übermittelt werden.

### 8.2.1 Prozesszuteilung

Beim «Vermittler Double Blinding» können viele Aufgaben vom Vermittler übernommen werden. Dazu gehören das Metadaten Management, Trust Management, Zugang definieren, Discovery, Identitätsdaten Transformation, Attribut Aggregation, Attributtransformation, Protokolltransformation und Zugang erlauben. Sinnvollerweise sollte die Freigabe der Attribute durch das Subjekt (User Consent) auch vom Vermittler übernommen werden. Der User Consent kann alternativ vom IdP und (wenn möglich) vom AP übernommen werden.

Identity Linking und Identity Mapping können vom Vermittler übernommen werden, falls dies notwendig und gefordert ist.

Der Integrationsaufwand für die RP bei dieser Art von Vermittler ist sehr gering, da sie bei der Definitionszeit nur die Zugriffsrechte definieren und bei der Laufzeit anhand der Zugriffsrechte den Zugriff erlauben muss.

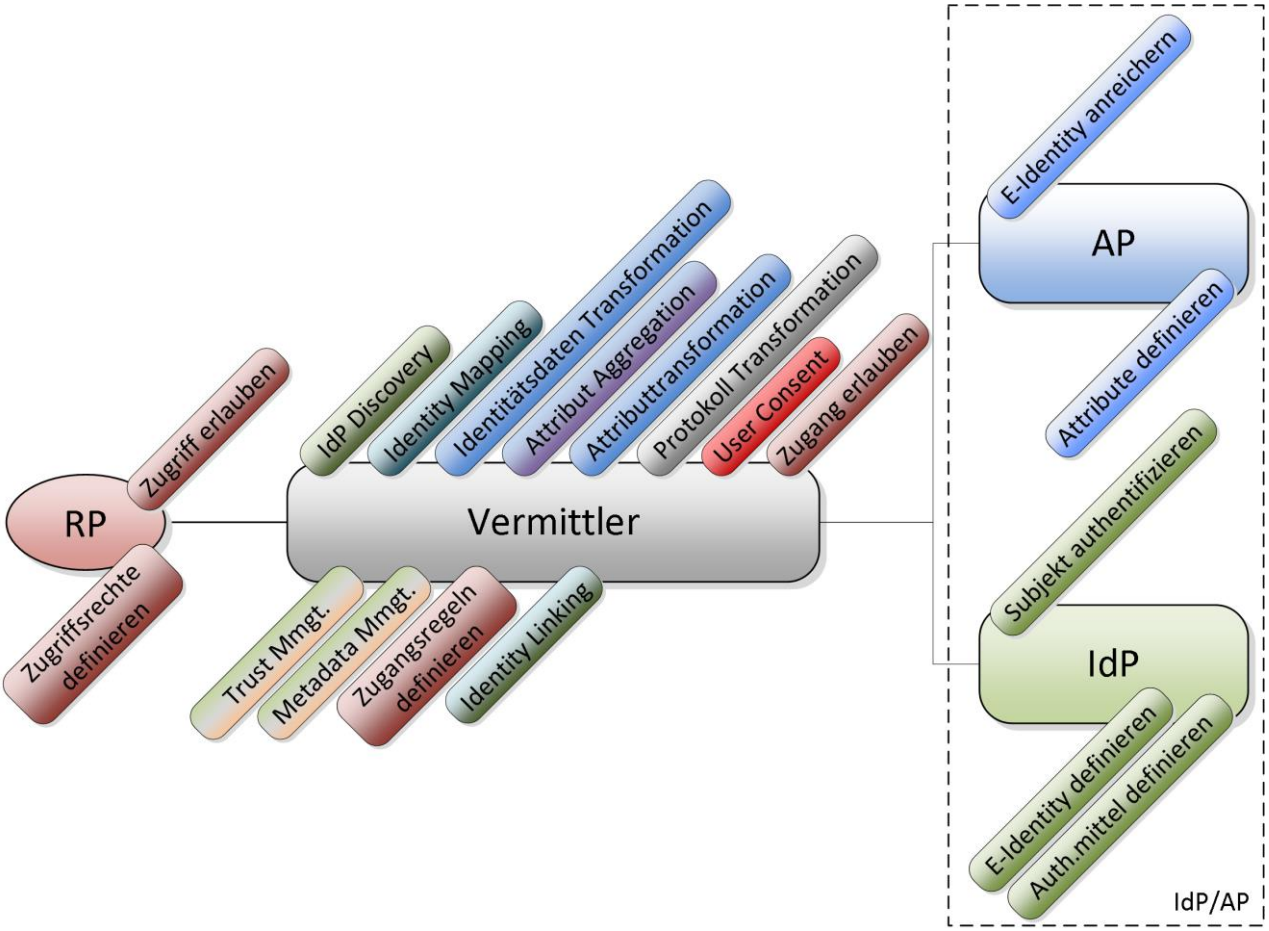


Abbildung 14: Prozess-Zuordnung Vermittler Double Blinding

## 8.3 Vermittler Offene Quellen

Je nach Anforderung ist es gewünscht, dass die RP mehr Informationen über die Authentifizierungs- bzw. Attributbestätigungen erhalten möchte.

Bei diesem Modell müssen die Quellen der Authentifizierung und Attribute für die RP offengelegt werden. Die RP kann nachvollziehen, von welchem IdP das Subjekt authentifiziert wurde und welcher IdP/AP bzw. AP die Quelle der Attribute ist.

Der Ablauf ist ähnlich zur Beschreibung vom Double Blinding gemäss Kapitel 8.2. Zusätzlich muss der Vermittler die Authentifizierungs- und/oder Attributquelle in die Bestätigungen (z.B. als Attribut) im Protokollabschnitt P1 einfügen. Somit kann die RP wahlweise nachvollziehen, von welchem IdP das Subjekt authentifiziert wurde und von welchem AP die Attribute stammen.

Falls die Quellen der Attribute verifizierbar sein sollen, muss der Vermittler die ursprüngliche Attributbestätigung an die RP übermitteln. Die RP kann dann anhand der Signatur die Echtheit und Authentizität der Attributbestätigung verifizieren. Dem Vermittler ist es in diesem Fall nicht möglich die Attribute zu transformieren.

### 8.3.1 Prozesszuteilung

Falls nur die Quellen mit Hilfe von Attributen sichtbar gemacht werden, so entspricht die Prozesszuordnung gemäss Kapitel 8.2.1.

Die Abbildung 15 zeigt die Zuordnung der Prozesse und Tätigkeiten, wenn nur die Attributbestätigung **verifizierbar** sein soll. Im Unterschied zum «Vermittler Double Blinding» hat der Vermittler nicht die Fähigkeit die Attribute zu transformieren und kann allenfalls von der RP übernommen werden.

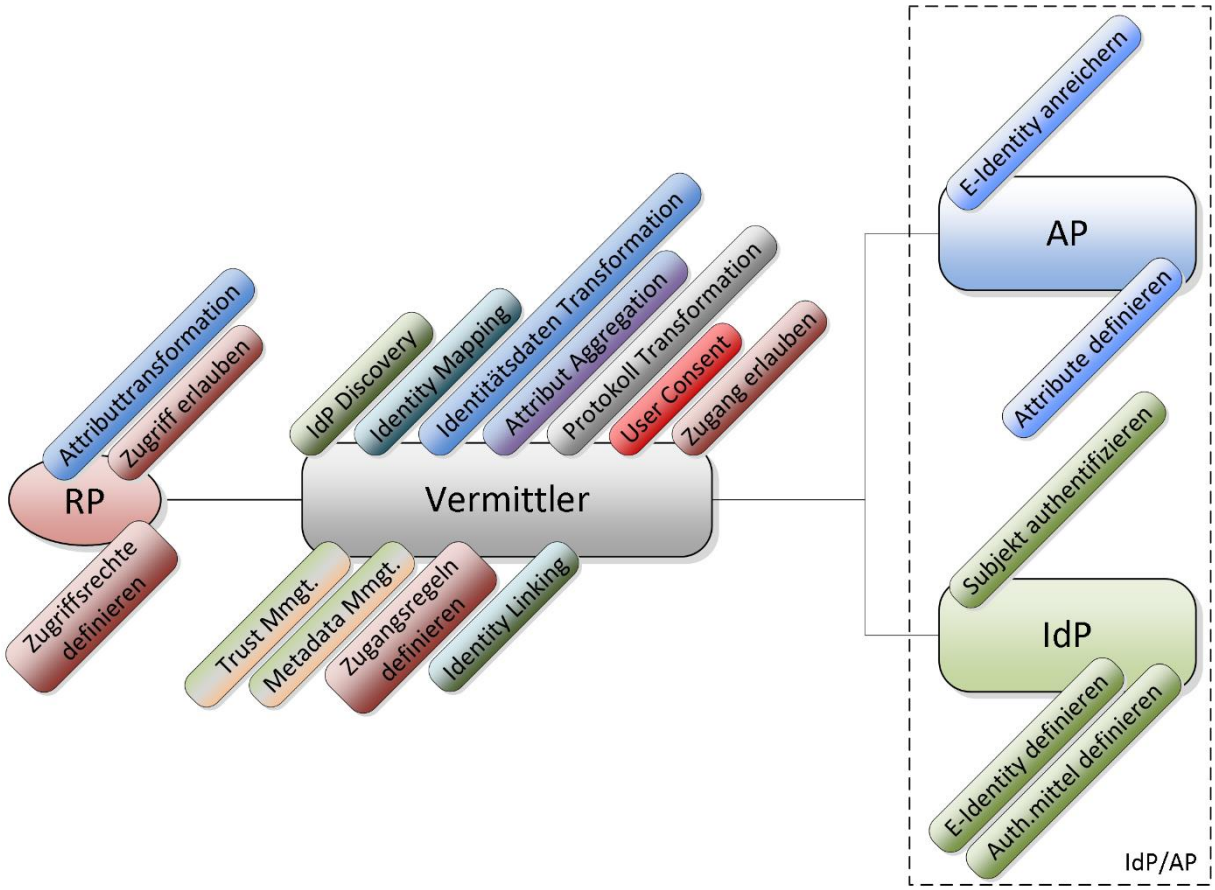


Abbildung 15: Zuordnung Vermittler Offene Quellen

## 8.4 Vermittler Vertraulichkeitsschutz

Beim Vertraulichkeitsschutz geht es darum, dass dem Vermittler bezüglich Einsicht und Transformation von Attributinformationen nicht vertraut wird. Deshalb müssen die Attributbestätigungen vom AP in einer vertraulichen Form für die RP übermittelt werden. Der Vermittler darf nicht in der Lage sein die Attributwerte zu sehen und diese zu transformieren.[17]

Die Übergabe der Authentifizierungsbestätigung ist gleich wie im Modell «Vermittler Offene Quellen».

Dies hat folgende Auswirkungen auf die Teilnehmer bzw. den Prozess:

- Damit die Vertraulichkeit der Attribute gegenüber dem Vermittler bewahrt werden, stehen zwei Möglichkeiten zur Auswahl. Eine Möglichkeit muss eingesetzt werden:
  - Die Attribute werden von der AP für die RP verschlüsselt
  - Die RP erhält vom Vermittler Referenzen, bei der die Attribute direkt abgeholt werden können (über Protokollabschnitt P3).

[17] Falls auch die Authentifizierungsbestätigung für den Vermittler nicht sichtbar sein soll, kann der Vermittler nur die Prozesse IdP Discovery und Verwaltung der Metadaten wahrnehmen, da er selbst die Identität des Subjekts nicht erkennen kann.

- Falls die Attribute verschlüsselt über den Vermittler an die RP übermittelt werden, muss die AP erfahren, für welche RP die Attribute verschlüsselt werden. Dies kann über die Metadaten erfolgen oder während der Laufzeit geschehen.
- Die Einwilligung des Subjekts zur Weitergabe von Attributen (User Consent) muss entweder beim Vermittler oder beim IdP/AP eingeholt werden. Falls der Vermittler dies übernimmt, muss der Vermittler die Einwilligung beim Subjekt einholen, bevor die Attribute beim AP mit Vertraulichkeitsschutz abgefragt werden. Das Subjekt sieht aber nur die Attributnamen, nicht aber die Attributwerte.

Wenn Attribute mit Vertraulichkeitsschutz zwischen AP und RP übermittelt werden, kann grundsätzlich ein Double Blinding nicht mehr aufrechterhalten werden, da der Sender (AP) die Identität des Empfängers (RP) unweigerlich feststellen kann. Um dies weiterhin zu ermöglichen, können z. B. anonymisierte Zertifikate verwendet werden. Somit kann der AP die RP anhand der Informationen im Zertifikat nicht mehr erkennen und das Double Blinding kann damit gewahrt bleiben. Diese und weitere Formen zur Bewahrung des Double Blinding trotz Vertraulichkeitsschutz sind relativ aufwändig in deren Umsetzung (Widerspruch zu Anforderung 224-LE-3) und werden daher in diesem Dokument nicht weiter behandelt.

Beim Vermittler Vertraulichkeitsschutz muss eine einseitige Blindisierung vermieden werden. Entweder es muss offengelegt werden an wen die APs die Daten übertragen und für die RPs von wem die Daten stammen, oder AP und RP haben beide keine Kenntnis vom Datenempfänger bzw. Datenquelle.

In jedem Fall hat der Vermittler keine Möglichkeit die Attribute zu transformieren.

### 8.4.1 Prozesszuteilung

Falls die Attribute verschlüsselt über den Vermittler übermittelt werden, müssen die Prozesse gemäss Abbildung 16 zugeteilt werden.

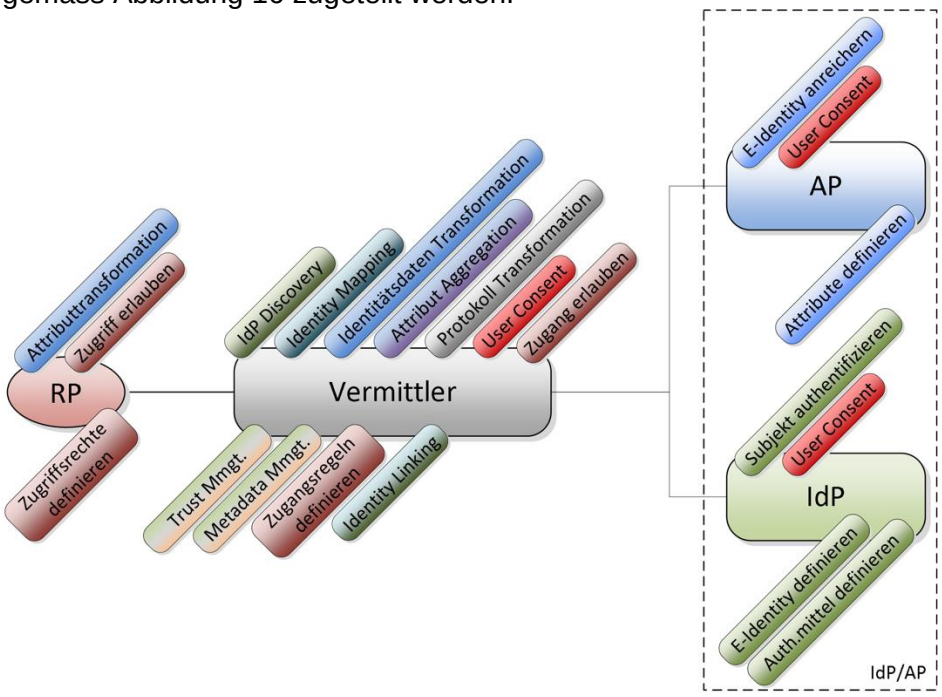


Abbildung 16: Vermittler Vertraulichkeitsschutz (verschlüsselte Attribute)[18]

[18] „User Consent“ muss entweder vom Vermittler oder von IdP und AP durchgeführt werden.

Werden Referenzen an die RP übermittelt, muss die Aggregation der Attribute von der RP übernommen werden (siehe Abbildung 17).

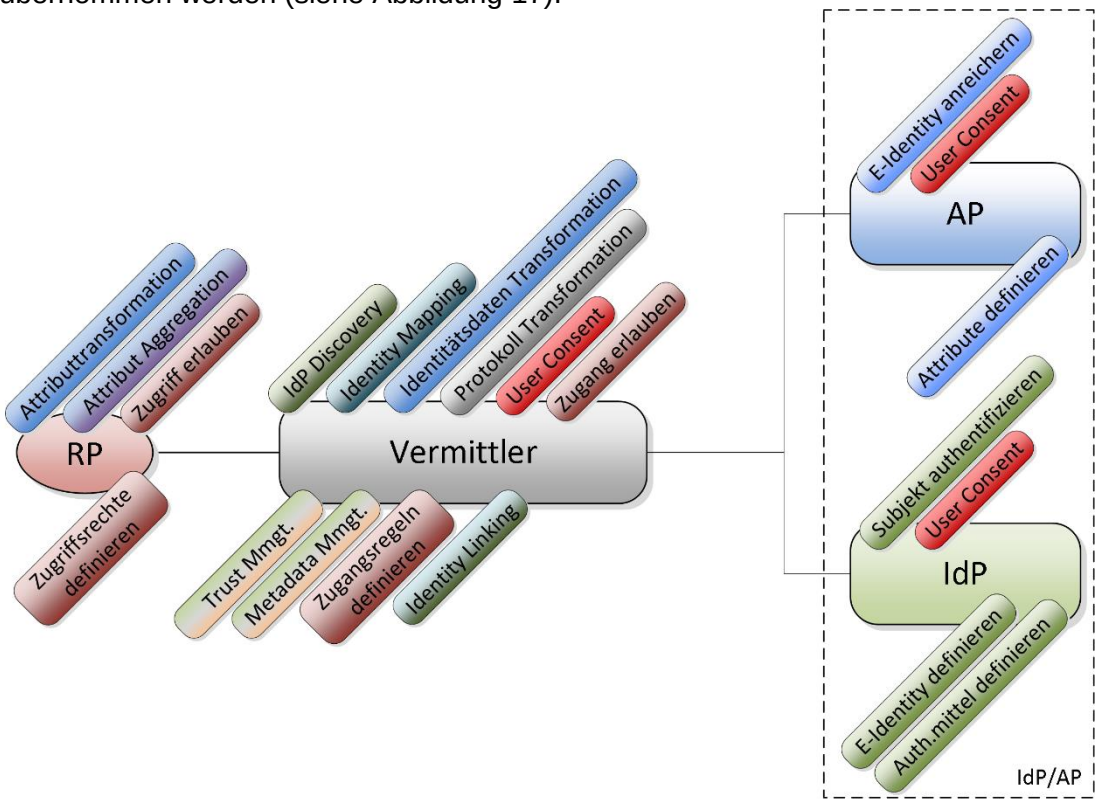


Abbildung 17: Vermittler Vertraulichkeitsschutz (Referenz auf Attribute)[19]

[19] „User Consent“ muss entweder vom Vermittler oder vom IdP bzw. AP durchgeführt werden.

# 9 Anwendung eCH-0170 auf vermittlerbasierte Identity Federations

Der eCH-0170 [3] definiert ein Qualitätsmodell für die Authentifizierung eines Subjektes für einfache IAM-Systeme, bestehend aus IdP und RP (ohne Vermittler). In den folgenden Abschnitten wird für jedes Teilmodell beschrieben, welche Auswirkungen die Einführung eines Vermittlers auf das Qualitätsmodell hat.

## 9.1 Vertrauensstufe der Authentifizierung (VSA)

Auch in einem vermittler-basierten IAM-System, wird ein Subjekt immer von einem IdP authentifiziert. Deshalb müssen bei der Bestimmung der Vertrauensstufe die Kriterien *Authentifizierungsmittel* und *Zertifizierung des Authentifizierungsmittels* auf den verwendeten IdP angewandt werden.

Beim Kriterium *Re-Authentifizierung* muss der Vermittler berücksichtigt werden. Hat der Vermittler die Verantwortung der Benutzer-Sessions, muss er die Re-Authentifizierung einleiten, wenn die Dauer der Authentifizierungs-Session entspr. der Ausprägung überschritten wurde. Der Vermittler muss in diesem Fall eine erneute Authentifizierung entspr. der Ausprägung beim IdP forcieren.

## 9.2 Vertrauensstufe der Registrierung (VSR)

Bei der Bestimmung der Vertrauensstufen der Registrierung wird der verwendete IdP (bzw. die RA des IdPs) untersucht. Der Vermittler hat nur Einfluss auf die Qualität der Registrierung, wenn er ein Identity-Linking ermöglicht.

## 9.3 Vertrauensstufe der Steuerung (VSS)

Bei der Bestimmung der Vertrauensstufe der Steuerung müssen alle involvierten IAM-Dienstanbieter (IdP inkl. RA und Vermittler) berücksichtigt werden. Die IAM-Dienstanbieter müssen jeweils die Kriterien einer Stufe erfüllen, um entsprechend eingestuft zu werden. Das Gesamtergebnis der Vertrauensstufe der Steuerung entspricht der kleinsten Stufe der berücksichtigten Dienstanbieter.

## 9.4 Vertrauensstufe der Föderierung (VSF)

VSF 1 und VSF 2 können in einer Identity Federation mit einem Vermittler ohne weiteres erreicht werden. Es wird davon ausgegangen, dass dem Vermittler bezüglich der Authentifizierung immer vertraut wird. Er ist damit der Protokollendpunkt für die Signatur, sowie für die Verschlüsselung.

Die Authentifizierungsbestätigungen werden immer signiert (Kriterium «Authentizität der Authentifizierungsbestätigung»). Der IdP signiert die Authentifizierungsbestätigung für den Vermittler. Der Vermittler prüft die Signatur und signiert die Authentifizierungsbestätigung erneut für die RP (Die Signatur vom IdP wird nicht weitergegeben). Die RP überprüft anschliessend die Signatur.

Falls die Authentifizierungsbestätigung verschlüsselt wird (Kriterium «Vertraulichkeitsschutz der Authentifizierungsbestätigung»), verschlüsselt der IdP diese für den Vermittler. Der Vermittler entschlüsselt die Authentifizierungsbestätigung und verschlüsselt diese erneut für die RP.

Problematisch ist VSF 3, die eine Implementierung des Holder-of-Key-Prinzips[20] verlangt. Falls VSF 3 erforderlich ist, sollte der Vermittler nur noch IdP-Discovery durchführen. Die RP würde dann die Authentifizierung direkt beim IdP initiieren. Dabei ist zu beachten, dass kein Blinding mehr vorhanden ist. Der IdP kennt die RP und die RP kennt den IdP. Ausserdem muss ein mögliches Identity Linking und Identity Mapping auf der RP erfolgen. Der Vermittler kann die E-Identity nicht transformieren.

[20] . Der Nachweis des Schlüssels (bzw. Geheimnisses) müsste auf beiden Protokollabschnitten (P1 und P2) überprüft werden. Für das Subjekt würde das bedeuten, dass es sich drei Mal authentifizieren müsste. Dies ist vom Benutzererlebnis nicht wünschenswert und sollte vermieden werden.

# 10 Haftungsausschluss/Hinweise auf Rechte Dritter

**eCH**-Standards, welche der Verein **eCH** dem Benutzer zur unentgeltlichen Nutzung zur Verfügung stellen oder welche **eCH** referenzieren, haben nur den Status von Empfehlungen.
Der Verein **eCH** haftet in keinem Fall für Entscheidungen oder Massnahmen, welche der Benutzer auf Grund dieser Dokumente trifft und / oder ergreift. Der Benutzer ist verpflichtet, die Dokumente vor deren Nutzung selbst zu überprüfen und sich gegebenenfalls beraten zu lassen. **eCH**-Standards können und sollen die technische, organisatorische oder juristische Beratung im konkreten Einzelfall nicht ersetzen.
In **eCH**-Standards referenzierte Dokumente, Verfahren, Methoden, Produkte und Standards sind unter Umständen markenrechtlich, urheberrechtlich oder patentrechtlich geschützt. Es liegt in der ausschliesslichen Verantwortlichkeit des Benutzers, sich die allenfalls erforderlichen Rechte bei den jeweils berechtigten Personen und/oder Organisationen zu beschaffen.
Obwohl der Verein **eCH** all seine Sorgfalt darauf verwendet, die **eCH**-Standards sorgfältig auszuarbeiten, kann keine Zusicherung oder Garantie auf Aktualität, Vollständigkeit, Richtigkeit bzw. Fehlerfreiheit der zur Verfügung gestellten Informationen und Dokumente gegeben werden. Der Inhalt von **eCH**-Standards kann jederzeit und ohne Ankündigung geändert werden.
Jede Haftung für Schäden, welche dem Benutzer aus dem Gebrauch der **eCH**-Standards entstehen ist, soweit gesetzlich zulässig, wegbedungen.

# 11 Urheberrechte

Wer **eCH**-Standards erarbeitet, behält das geistige Eigentum an diesen. Allerdings verpflichtet sich der Erarbeitende, sein betreffendes geistiges Eigentum oder seine Rechte an geistigem Eigentum anderer, sofern möglich, den jeweiligen Fachgruppen und dem Verein **eCH** kostenlos zur uneingeschränkten Nutzung und Weiterentwicklung im Rahmen des Vereinszweckes zur Verfügung zu stellen.
Die von den Fachgruppen erarbeiteten Standards können unter Nennung der jeweiligen Urheber von **eCH** unentgeltlich und uneingeschränkt genutzt, weiterverbreitet und weiterentwikkelt werden.
**eCH**-Standards sind vollständig dokumentiert und frei von lizenz- und/oder patentrechtlichen Einschränkungen. Die dazugehörige Dokumentation kann unentgeltlich bezogen werden.
Diese Bestimmungen gelten ausschliesslich für die von **eCH** erarbeiteten Standards, nicht jedoch für Standards oder Produkte Dritter, auf welche in den **eCH**-Standards Bezug genommen wird. Die Standards enthalten die entsprechenden Hinweise auf die Rechte Dritter.

# Anhang A – Referenzen & Bibliographie

[1] A. Laube-Rosenpflanzer, A. Spichiger, M. Kunz, T. Kessler, and A. Müller, “eCH-0219 IAM Glossar,” version 1.0, 2019 [Online]. Available: http://www.ech.ch/dokument/b1a76129-0c3e-4021-a6ff-c3123554fd95

[2] A. Laube-Rosenpflanzer, A. Spichiger, M. Kunz, T. Kessler, T. Gruoner, and M. Heerkens, “eCH-0107 Gestaltungsprinzipien für die Identitäts- und Zugriffsverwaltung (IAM),” version 3.0, 2019 [Online]. Available: https://www.ech.ch/dokument/167ccf46-b902-4b58-88f2-eed05ed58c05

[3] A. Laube-Rosenpflanzer, G. Hassenstein, M. Kunz, T. Gruoner, A. Spichiger, and T. Selzam, “eCH-0170 Qualitätsmodell zur Authentifizierung von Subjekten,” version 2.0, 2017 [Online]. Available: https://www.ech.ch/alfresco/s/ech/download?nodeid=54cce841-215f-4887-9382-25620dcbf9b1

[4] A. Laube-rosenpflanzer, G. Hassenstein, S. Agosti, M. Vinzens, U. Pfenninger, and D. Leiser, “eCH-0168 SuisseTrustIAM technische Architektur und Prozesse,” version 1.0, 2014 [Online]. Available: https://www.ech.ch/alfresco/s/ech/download?nodeid=31499686-813d-4589-b794-11015fbf2059

[5] “Stork 2.0.” [Online]. Available: https://www.eid-stork2.eu/

[6] D. A. S. Europ, I. Parlamentder, R. A. T. D. E. R. Europ, and I. Union, “VERORDNUNG (EU) Nr. 910/2014 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG, (eIDAS),” 2015.

[7] S. K. S. Paul A. Grassi, James L. Fenton, Justin P. Richer, “DRAFT NIST Special Publication 800-63C,” 2017 [Online]. Available: https://pages.nist.gov/800-63-3/sp800-63c.html. [Accessed: 22-Jun-2017]

[8] Eidgenössisches Justiz- und Polizeidepartement EJPD, “E-ID-Gesetz.” [Online]. Available: https://www.bj.admin.ch/bj/de/home/staat/gesetzgebung/e-id.html

[9] Die Bundesversammlung der Schweizerischen Eidgenossenschaft, “DSG: Bundesgesetz über den Datenschutz vom 19. Juni 1992 (Stand am 1. Januar 2014), 235.1,” version 1992, pp. 1–24, 2014 [Online]. Available: https://www.admin.ch/opc/de/classified-compilation/19920153/201401010000/235.1.pdf

[10] S. Cantor, J. Kemp, R. Philpott, and E. Maler, “Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0,” *OASIS Stand.*, 2005 [Online]. Available: https://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf

[11] K. Kane, K. Easterbrook, G. Zaverucha, and C. Paquin, “U-Prove - Microsoft Research.” [Online]. Available: https://research.microsoft.com/en-us/projects/u-prove/

[12] J. Camenisch and M. Dubovitskaya, “IBM Research - Zurich, Identity Mixer.” [Online]. Available: https://www.zurich.ibm.com/identity_mixer/

# Anhang B – Mitarbeit & Überprüfung

| | |
|---|---|
| Gruoner Torsten | ISB |
| Emmenegger Adrian | SwissSign |
| Hangartner Nick | SwissSign |
| Hassenstein Gerhard | ICTM / Berner Fachhochschule |
| Hefti Esther | Staatskanzlei Kanton Zürich |
| Kunz Marc | ICTM / Berner Fachhochschule |
| Laube-Rosenpflanzer Annett | ICTM / Berner Fachhochschule |
| Leimer Bojan | ICTM / Berner Fachhochschule |
| Voge Mario | SwissSign |

# Anhang C – Abkürzungen und Glossar

| | |
|---|---|
| AP | Attribute Provider |
| G2B | Government to Business |
| G2C | Government to Citizen |
| G2G | Government to Government |
| IAM | Identity and Access Management |
| IdP | Identity Provider |
| IdP/AP | Identity Provider/Attribute Provider |
| LDAP | Lightweight Directory Access Protocol |
| OIDC | OpenID Connect |
| RP | Relying Party |
| SAML | Security Assertion Markup Language |
| SLO | Single Logout |
| SOA | Service oriented architecture |
| SSO | Single Sign-On |
| TLS | Transport Layer Security |
| URI | Uniform Resource Indicator |
| VSA | Vertrauensstufe der Authentifizierung |
| VSF | Vertrauensstufe der Föderierung |
| VSR | Vertrauensstufe der Registrierung |
| VSS | Vertrauensstufe der Steuerung |

# Anhang E – Abbildungsverzeichnis

Abbildung 1: Einordnung des eCH-0224 Standards ..... 5
Abbildung 2: Einfache(direkte) Identity Federation ..... 8
Abbildung 3: Grobstruktur eines vermittlerbasierten Identity Federation Systems ..... 9
Abbildung 4: Entscheidungsbaum zur Auswahl der Identity Federation Modelle ..... 27
Abbildung 5: Vermittler Double Blinding ..... 30
Abbildung 6: Vermittler Offene Quellen ..... 31
Abbildung 7: Vermittler Vertraulichkeitsschutz ..... 32
Abbildung 8: Protokollabschnitte ..... 34
Abbildung 9: Protokollabschnitt P1 – Front-Channel ..... 35
Abbildung 10: Protokollabschnitt P1 - Back-Channel ..... 36
Abbildung 11: Protokollabschnitt P2 - Front- Channel ..... 37
Abbildung 12: Protokollabschnitt P2 - Back-Channel ..... 37
Abbildung 13: Protokollabschnitt P3 ..... 38
Abbildung 14: Prozess-Zuordnung Vermittler Double Blinding ..... 44
Abbildung 15: Zuordnung Vermittler Offene Quellen ..... 45
Abbildung 16: Vermittler Vertraulichkeitsschutz (verschlüsselte Attribute) ..... 46
Abbildung 17: Vermittler Vertraulichkeitsschutz (Referenz auf Attribute) ..... 47

# Anhang F – Tabellenverzeichnis

Tabelle 1: Anforderungen ans IAM-System ..... 20
Tabelle 2: Anforderungen des Leistungsbezügers ..... 22
Tabelle 3: Anforderungen des Leistungserbringers ..... 24
Tabelle 4: Anforderungen des Stakeholders: Führung ..... 24
Tabelle 5: Erfüllung der Anforderungen einer nicht-vermittlerbasierten Identity Federation .. 29
Tabelle 6: Erfüllung der Anforderungen des "Vermittlers Double Blinding" ..... 30
Tabelle 7: Erfüllung der Anforderungen des "Vermittlers Offene Quellen" ..... 31
Tabelle 8: Erfüllung der Anforderungen des "Vermittlers Vertraulichkeitsschutz" ..... 32

# Anhang G – Tokenbased Identity Federation Modelle mit Vermittler

Tokenbased Identity Federation Modelle mit Vermittler bieten höchsten Schutz der Privatsphäre eines Subjekts.
Bei klassischen Online-Verfahren (z. B. SAML und OIDC) erfolgt die Identifikations- und Attributvermittlung zeitnah und auf einem softwarebasierten Token. Im Gegensatz dazu verfolgen ‚token-based', oder auch ‚claims-based' bzw. ‚credential-based' genannte Methoden das Prinzip sensible Daten im Umfeld des Subjekts zu hinterlegen bzw. zu speichern. Prominentestes Beispiel dazu ist der *‚neue deutsche Personalausweis' (nPA)*. Die personenidentifizierenden Daten werden von einer autoritativen Quelle ausgegeben und auf der eID-Karte gespeichert. Bei einem Auslesevorgang muss sich der Dienstanbieter (Relying Party) gegenüber der Karte autorisieren. Der Nutzer ist bei einem solchen Auslesevorgang immer integriert, indem er die volle Kontrolle über die von der Karte ausgelesenen Daten hat. Die eID-Karte spielt also die Funktion eines abgesetzten, persönlichen Identity Providers in Form eines Hardwaretokens, welches persistente personenidentifizierende Daten enthält. Microsoft U-Prove [11] und Identity-Mixer (kurz Idemix) von IBM [12] sind zwei weitere Varianten von ‚token-based' Identity Federation Systemen, welche ihren Fokus auf den Schutz der Privatsphäre des Subjekts legen.