PROJEKT Justitia 4.0

Anhang 7 Architektur Plattform Justitia.Swiss

Inhaltsverzeichnis

1 Einleitung

1.1 Projekt Justitia 4.0

Das Projekt Justitia 4.0 gestaltet die digitale Transformation der Schweizer Justiz in Straf-, Zivil- und Verwaltungsgerichtsverfahren. Bis 2026 sollen alle an einem Justizverfahren beteiligten Parteien auf kantonaler und eidgenössischer Ebene mit den rund 300 Gerichten, den Staatsanwaltschaften und Justizvollzugsbehörden Daten elektronisch über eine hochsichere zentrale Plattform (die Plattform «Justitia.Swiss») austauschen können.

Das Projekt hat im Juli 2021 die WTO-Ausschreibung der Plattform gestartet, mit der in Zukunft die elektronische Akteneinsicht (eAE) und der elektronische Rechtsverkehr (ERV) in der Schweizer Justiz unterstützt werden. Das vorliegende Dokument ist ein Teil der dafür notwendigen Ausschreibungsunterlagen und dient gleichzeitig als Basis für die weitergehende Architekturkonzeption.

1.2 Zweck des Dokuments

Das vorliegende Dokument beschreibt und erklärt potenziellen Anbietern die fachlichen Konzepte der elektronischen Akteneinsicht und des elektronischen Rechtsverkehrs über die Plattform. Es formuliert damit gleichzeitig Anforderungen an den Beschaffungsgegenstand, die potenzielle Anbieter in ihren Angeboten berücksichtigen müssen: Anbieter sollen im Rahmen der Ausschreibung Lösungen anbieten, die mit denen in diesem Dokument beschriebenen fachlichen Konzepten kompatibel sind. Das fachliche Modell (Kapitel 0 bis 5) beinhaltet begrifflich und inhaltlich konsolidierte und konsistente Beschreibungen der Konzepte basierend auf Anforderungen, die in den Fachgruppen im Rahmen von Abklärungen der Bedürfnisse an die Plattform formuliert wurden.

Neben dem fachlichen Modell wird in Kapitel 6 die Systemsicht mit Interfaces und den nötigen Datenhaltungen konkretisiert. Im Kapitel 7 werden die wichtigsten Anforderungen an die technische Architektur beschrieben, welche im späteren Verlauf des Projekts vertieft werden muss.

1.3 Governance dieses Dokuments

Damit dieses Dokument als Referenz für das Projekt und die Weiterentwicklung dienen kann, werden im Verlauf des Projekts weitere Kapitel bei Bedarf ergänzt und präzisiert. Insbesondere werden eine Überarbeitung und Erweiterung dieses Dokuments erfolgen, sobald ein Partner für die Entwicklung definiert ist.

2 Grundlegende Prinzipien

Dieses Kapitel verdichtet die fachlichen Rahmenbedingungen (Abschnitt 2.1), die Anforderungen an Sicherheit und Datenschutz (Abschnitt 2.2), technische Prinzipien (Abschnitt 2.3) und die Anforderungen bezüglich Entwicklung und Betrieb (Abschnitt 2.4). Diese Zusammenstellung dient einer einheitlichen «Unité de doctrine». Die Prinzipien sind nicht eine vollständige Anforderungssammlung, sondern sollen primär die während der Konzeptphase eingeflossenen Grundüberlegungen und Absichten verschriftlichen. Da jede Absicht auch eine Konsequenz hat, ist es wichtig, diese zu diskutieren und in den weiteren Phasen des Projekts zu würdigen und bei Bedarf anzupassen. Damit werden auch Änderungen und Erkenntnisse im Laufe des Projekts transparent dargestellt.

2.1 Fachliche Prinzipien

Die folgenden Prinzipien bestimmen das Verhalten der Plattform bezüglich Stammdaten und erlauben die Einbindung von extern verwalteten digitalen Identitäten und bei Bedarf Organisationen. Details zu diesen Prinzipien finden sich in Kapitel 4.1 über Personen, Kapitel 4.2 über Profile und Kapitel 4.4 über die Delegation.

Prinzip 1 Trennung der Informationen zu realweltlichen Personen und Organisationen von Profilen der Teilnahmen am Rechtsverkehr und der Akteneinsicht
- Natürliche Personen, Gruppen von Personen und juristische Personen existieren ausserhalb der Plattform. - Diese Subjekte sollen jedoch auf der Plattform am elektronischen Rechtsverkehr teilnehmen resp. elektronisch Akten einsehen können. Im Profil kann jeder Teilnehmer seine Einstellungen zum Rechtsverkehr steuern und Tätigkeiten delegieren. - Durch diese Trennung wird die Datenhoheit der entsprechenden Stammdaten geschärft: Die Plattform kontrolliert den Datenlifecycle der Teilnahmen (Stammdaten zu Profilen, Berechtigungen). Die Daten der Personen werden durch diese selber resp. durch deren Identitätsprovider (IDP) verwaltet. - Eine natürliche Person kann mehrere Rollen auf der Plattform einnehmen.

Prinzip 2 Attribute der natürlichen Person werden von externen Identitätsprovidern übernommen
- Die Plattform soll keine eigenen digitalen Identitäten vergeben, sondern die Attribute der Personen von externen Identitätsprovidern übernehmen. - Hat dieselbe natürliche Person (bei verschiedenen Identitätsprovidern) unterschiedliche digitale Identitäten, erlaubt die Plattform ein Duplikat dieser Person zu führen und versucht nicht, dieses aufzulösen. Nutzer der Plattform müssen mit Dubletten umgehen können. - Die Datenqualität der Personenattribute wird vom externen Identitätsprovider gewährleistet.

Aktuell ist keine gesetzliche Grundlage vorhanden, Dubletten aufzulösen. Justizbehörden machen Zustellungen an natürliche Personen nur, wenn diese Personen zuerst ein Profil eröffnet haben und über diese Profile kommunizieren und damit ihre Einwilligung gegeben haben.

Prinzip 3 Organisationen können über Identitätsprovider oder auf der Plattform definiert werden
- Organisationen können durch die Einbindung ihres IDPs an die Plattform angebunden werden. Dadurch können die Organisationen die Zugriffsrechte und Rollen ihrer Mitarbeiter auf das Organisationsprofil durch ihren eigenen IDP steuern. - Zum anderen können Organisationen (als Gruppe von Personen) auf der Plattform definiert werden. In diesem Fall verwaltet die Plattform (in Ausnahme von Prinzip 1) die Beziehungen zwischen Organisation und den einzelnen Mitgliedern.

Folgende Prinzipien fassen die Rolle der Plattform als zentraler Hub der Schweiz für den Rechtsverkehr und die Akteneinsicht zusammen. Details siehe Kapitel 4.4 über den Rechtsverkehr und Kapitel 4.3 über die Akteneinsicht. In Kapitel 5 wird anhand von Mustern illustriert, wie verfahrensleitende Behörden untereinander über die Plattform kommunizieren.

Prinzip 4 Eine einzige[1] schweizerische Plattform für den elektronischen Rechtsverkehr und die elektronische Akteneinsicht
- Die Plattform stellt den Rechtsverkehr als einzige Plattform sicher. Der Nachweis von Eingaben und Zustellungen ist Aufgabe der Plattform. Eingaben gelten mit der Aufgabe als erfolgt, Zustellungen gelten mit dem erstmaligen Abfragen als zugestellt. - Heute bestehende Unterschriftserfordernisse werden durch die Authentifizierung auf der Plattform sowie das automatisierte Anbringen von geregelten elektronischen Siegeln ersetzt.

[1] Prinzip 4 reflektiert die Anforderungen, dass es gemäss BEKJ-VE Art. 4 nur eine Plattform für den Rechtsverkehr und die elektronische Akteneinsicht geben soll. Neueste Diskussionen zeigen, dass vielleicht dieser Artikel aufgeweicht wird und ein Kanton eine eigene Plattform realisieren könnte. Sollte diese Idee sich in der parlamentarischen Diskussion zum BEKJ-Gesetz durchsetzen, müsste die Plattform also interoperabel mit weiteren Plattformen sein. Mit der dezentralen Datenhaltung (Kapitel 6.2) wäre ein Grundstein für eine solche Interoperabilität gelegt.

Obiges Prinzip enthält auch eine implizite Abgrenzung: Die Plattform unterstützt die Akteneinsicht, jedoch nicht (!) das Erstellen oder Bearbeiten von Akten. Die Plattform unterstützt auch keine 'verteilte' Aktenbearbeitung von mehreren Behörden am selben Verfahren.

Prinzip 5 Berechtigung zur Akteneinsicht und Zustellungen werden dezentral vergeben, können delegiert werden und werden zentral geprüft
- Die Justizbehörden sind Eigner der Akten und vergeben (und widerrufen) Berechtigungen zur Einsicht auf Aktenstücke an verfahrensbeteiligte Personen. - Verfahrensbeteiligte können ihre Rechte zur Akteneinsicht an weitere Personen delegieren. - Die Plattform validiert jeden Zugriff auf Aktenstücke.

Prinzip 6 Zustellung wird technisch auf der Akteneinsicht realisiert
- Zustellungen erfolgen auf den bei den Justizbehörden verakteten Dokumenten (Aktenstücke). Diese werden technisch auf der Plattform als einsehbare Kopien zur Einsicht bereitgestellt. Dabei werden die verfahrensbeteiligten Personen zur Einsicht berechtig und über die Zustellung benachrichtigt. - Für die Zustellung werden somit – im Gegensatz zu den Eingaben - keine Dateien übermittelt. - Der erstmalige Zugriff auf eine Zustellung oder das Ende der Abholfrist wird protokolliert.

2.2 Sicherheit und Datenschutz

Die Architektur der Plattform «Justitia.Swiss» trägt mit den nachfolgend aufgeführten Massnahmen zur Erreichung der Schutzziele Vertraulichkeit, Integrität, Verfügbarkeit und Nachvollziehbarkeit bei. Details und Begründungen zu diesen Massnahmen finden sich im Anhang 8 ISDS-Konzept der Plattform Justitia.Swiss. Für eine umfassende Sicherheit müssen diese architektonischen Prinzipien mit organisatorischen und technischen Massnahmen gemäss dem Konzept ergänzt werden.

Prinzip 7 IT-Sicherheitsperimeter
Die Plattform «Justitia.Swiss» schützt ihre angebotenen Services entsprechend dem neusten Stand der Technik. Für Betreiber von Services, welche über APIs an die Plattform angeschlossen werden, werden in Anschlussverträgen oder Nutzungsvereinbarungen Sicherheitsanforderungen bezüglich ihrer Systeme formuliert.

Prinzip 8 Technische Massnahmen zur Sicherstellung der Vertraulichkeit
Die auf der Plattform «Justitia.Swiss» bearbeiteten Daten können nur von hierzu berechtigten Personen eingesehen werden. Dies wird durch die Architektur wie folgt unterstützt: - Alle im Adressverzeichnis geführten natürlichen Personen verfügen über eine digitale Identität mit dem Sicherheitsniveau substanziell oder höher. - Die Nutzung der Plattform «Justitia.Swiss» erfordert eine starke Benutzerauthentifizierung mit dem Sicherheitsniveau substanziell oder höher. - Der Zugriff auf die Aktenstücke wird nur gewährt, wenn ausreichende Zugriffsrechte für den lesenden Benutzer in der Komponente DossierStore hinterlegt wurden. - Aktenstücke sind auf der Plattform «Justitia.Swiss» verschlüsselt gespeichert. - Alle Schnittstellen von und zur Plattform «Justitia.Swiss» sind verschlüsselt.

Prinzip 9 Technische Massnahmen zur Sicherstellung der Integrität
Die auf der Plattform «Justitia.Swiss» bearbeiteten Daten können nicht unbemerkt verändert werden. Dies wird durch die Architektur wie folgt unterstützt:

- Geregelte elektronischen Siegel werden für die Dateien der Eingaben erstellt.
- Alle im DossierStore gespeicherten Aktenstücke sind elektronisch gesiegelt.
- Bei jeder Akteneinsicht wird die Gültigkeit des elektronischen Siegels überprüft.

Prinzip 10	Technische Massnahmen zur Sicherstellung der Verfügbarkeit

Die auf der Plattform «Justitia.Swiss» bearbeiteten Daten sind gegen Verlust geschützt. Dies wird durch die Architektur wie folgt unterstützt:

- Auf der Plattform «Justitia.Swiss» werden nur einsehbare Kopien von Aktenstücken gespeichert, d.h. die rechtsrelevante Akte verbleibt bei der verfahrensleitenden Justizbehörde;
- Die Verfügbarkeiten der Business Services und Datenbestände (z.B. Adressverzeichnis, Audit Trail) der Plattform «Justitia.Swiss» werden durch entsprechende Service Level Agreements (SLA) mit dem Plattformbetreiber sichergestellt.

In Ergänzung zu diesem Prinzip wird die Verfügbarkeit auch durch Prinzip 14 und Prinzip 20 gewährleistet.

Prinzip 11	Technische Massnahmen zur Sicherstellung der Nachvollziehbarkeit

Alle rechtsverbindlichen Ereignisse auf der Plattform «Justitia.Swiss» können nachvollzogen werden. Dies wird durch die Architektur wie folgt unterstützt:

- Alle rechtsverbindlichen Ereignisse werden in einem nicht veränderbaren Audit Trail aufgezeichnet;
- Die Plattform «Justitia.Swiss» kann für rechtsverbindliche Ereignisse eine Quittung ausstellen und diese mit einem geregelten elektronischen Siegel versehen.

Der Audit Trail wird im Abschnitt Quittung und Nachvollziehbarkeit (Abschnitt 6.3 Rechtsverbindliche Ereignisse quittieren) beschrieben.

Prinzip 12	Privacy by Design und by Default

Das Design der Plattform muss sich an den Grundsätzen des Privacy by Design orientieren:

- Proaktiv, nicht reaktiv: Datenschutz-Risiken von Anfang an berücksichtigen.
- Datenschutz als Standardeinstellung: Personenbezogene Daten müssen in allen IT-Systemen geschützt werden. Dies beinhaltet:
    - Der Zweck der benötigten Personendaten soll klar spezifiziert sein
    - Beschränkung des Sammelns von Daten für den Zweck
    - Datenminimierung
    - Verwendung, Aufbewahrung und Offenlegung muss dem Verwendungszweck entsprechen
    - Datenklassifikation ist jederzeit für alle Daten und Objekte definiert
- Für Datenschutz konzipiert: Datenschutzmassnahmen sind keine zusätzlichen Add-Ons, sondern bereits vollständig in die Software integriert
- Volle Funktionalität: Es werden keine Kompromisse im Funktionsumfang gemacht, um Datenschutz und Datensicherheit zu erreichen. Die Interessen und Ziele der Datenerhebung und Sammlung sind formuliert und transparent kommuniziert.
- Durchgängige Sicherheit: Schutz der Daten während ihrer gesamten Lebensdauer sowie vollständige Löschung (inkl. Vernichtung auf dem Backup) oder Unkenntlichmachung auf Wunsch und sofern erlaubt.
- Sichtbarkeit und Transparenz: Die Datenbearbeitung auf der Plattform darf ausschliesslich der Aufgaben der Plattform dienen. Die Überprüfung dieser Forderung wird unter anderem durch öffentliche Transparenz des Designs und des Source Code ermöglicht.
- Die Privatsphäre der Nutzer respektieren: Unterstützen von individuellen Datenschutzinteressen durch starke Datenschutzrichtlinien und -standards und benutzerfreundliche Optionen.

Siehe [PbD] für eine (englische) Erläuterung und Vertiefung dieser Grundsätze. Der Grundsatz für Transparenz des Designs und Codes wird auch für die Sourcing Strategie als Basis genommen.

Eine wichtige Umsetzung dieses Prinzips erfolgt in Daten Lifecycle Prozessen für Benutzer und Profile, sowie durch die Tatsache, dass sämtliche Daten eines Verfahrens auf der Plattform gelöscht werden, wenn das Verfahren beendet ist (Kapitel 6.7). Die Plattform macht explizit keine inhaltlichen Analysen der übermittelten Dokumente, gemäss Leitsatz 6[2].

2.3 Technische Prinzipien

Die technischen Prinzipien stellen sicher, dass die Plattform mit den existierenden föderal geprägten IT-Umgebungen in den Behörden und Kantonen interagieren kann und dass die verwendete Grundarchitektur der Plattform zukunftssicher ist.

Das folgende Prinzip referenziert den strategischen Entscheid, Aktenstücke zur Einsicht sowohl zentral auf der Plattform als auch dezentral – in der IT der Justizbehörden – halten zu können. Für Details siehe Kapitel 6.2 über die Datenhaltung der einsehbaren elektronischen Akte.

Prinzip 13	Zentrale und dezentrale Bereitstellung von einsehbaren Aktenstücken
- Aktenstücke zur Einsicht können zentral auf der Plattform in einem mandantenfähigen DossierStore als Kopien abgelegt werden. - Aktenstücke können auch dezentral in den IT-Systemen der verfahrensleitenden Behörden vorgehalten werden.	

Prinzip 14	Cloud Operating Model
- Die gesamte Plattform Justitia.Swiss wird im Cloud Operating Model entwickelt, d.h. alle Services werden Cloud Native implementiert, integriert und betrieben. - Entkoppelung und Flexibilität: Einzelne Komponenten können voneinander unabhängig entwickelt und in Form von Containern oder Funktionen deployed und betrieben werden (Microservice Architektur-Stil wo möglich und sinnvoll). Technische Abhängigkeiten sind dokumentiert. - Skalierbarkeit und Verfügbarkeit der Plattform und einzelner Komponenten werden dynamisch mittels Cloud Services gewährleistet. - Die Daten müssen einfach von einem Servicebetreiber zu einem anderen Betreiber migriert werden können. Entsprechende Tests und Migrationspfade sind von Anfang an zu berücksichtigen.	

Folgender Grundsatz der Interoperabilität wird bereits im Entwurf des Gesetzes (Art. 18, VE-BEKJ) und in den Leitsätzen 7 und 8 gefordert.

Prinzip 15	Schnittstellen (API) Justitia.Swiss
- Sämtliche Funktionalitäten der Plattform sollen sowohl über ein Web-Interface direkt über Web-Browser für Nutzer verwendbar sein als auch über APIs mit Standard-Web-Protokollen für Maschinen nutzbar sein. - Diese Interfaces sind versioniert und bis zu einem sinnvollen Grad rückwärtskompatibel.	

Hinweis: Die Nutzung über APIs bedingt auch eine Möglichkeit von technischen Benutzern, welche in Kapitel 6.1 erwähnt werden.

Prinzip 16	Mandantenfähigkeit
- Die Software und Datenhaltung soll mandantenfähig konzipiert werden.	

[2] Siehe https://www.justitia40.ch > Dokumente > Leitsätze Plattform

- Dies gilt primär für die Isolation der Daten der einsehbaren Akten, aber auch für APIs und deren Versionen, um das Risiko von Release-Zwängen auf Seiten der Behörden zu minimieren.

Mit dem Entscheid, eine zentrale Plattform für Akteneinsicht und elektronische Kommunikation für die Justiz zu realisieren wird auch die Diskussion um Zentralisierung versus dezentrale Kontrolle und Vertrauen angestossen. Diese Diskussion ist für die Architektur vor allem im Sinne des langfristigen Weiterausbaus interessant:

Prinzip 17	Bewährte Technik für das zentrale IT-System der Plattform

- Die Plattform soll durch den elektronischen Rechtsverkehr und die elektronische Akteneinsicht helfen, die digitale Transformation in der Justiz zu ermöglichen.
- Dazu wird ein vertrauenswürdiges IT-System durch die Justizbehörden aufgebaut und betrieben und dazu werden bewährte Technologien eingesetzt.

Dieses Prinzip soll aufzeigen, dass es einige Aspekte gibt, die man mit neuen Technologien auch anders lösen könnte (early adopter), diese Technologien aber noch nicht so verbreitet sind, dass diese 'out-of-the box' - Komponenten verwendet werden können. Einige Beispiele:

- Die Identitäten der Benutzer werden föderiert mit bewährten Protokollen wie OAuth2.0/OpenIdConnect, anstelle einer komplett dezentralen Lösung durch Self-Sovereign-Identity.
- Die Plattform muss Aktenstücke umschlüsseln, da diese auf dem Transport verschlüsselt sind, und verschlüsselt abgelegt werden, d.h. die Plattform hat prinzipiell Einsicht in die Aktenstücke. Es gäbe neue kryptographische Protokolle (Proxy-Reencryption), mit denen die Plattform die Dokumente umschlüsseln könnte, ohne Einsicht in die Aktenstücke zu bekommen.

2.4 Entwicklung und Betrieb

Prinzip 18	Agile (Weiter-)Entwicklung und Delivery

- Die Plattform soll nach den agilen Grundsätzen realisiert und weiterentwickelt werden.
- Changeability und Nachvollziehbarkeit: Entwicklung, Delivery, Konfiguration und Deployment von Software sowie Infrastruktur Komponenten erfolgen ausschliesslich über CI/CD Pipelines.
- Konfiguration von Infrastruktur- und Softwarekomponenten folgen den Ansätzen von infrastructure-as-code und configuration-as-code.
- Es gibt regelmässige und kurze Release-Zyklen für sämtliche Komponenten der Plattform
- Software Deployments erfolgen automatisierbar aus der Pipeline heraus. Die Services laufen always-on, D.h. die Softwarearchitektur ist so zu gestalten, dass Deployments unterbrechungsfrei stattfinden können.
- Neue Versionen können einfach (und mit weniger oder keiner) manuellen Intervention eingespielt und getestet werden.

Prinzip 19	Deployment Umgebungen

- Neue Versionen können automatisiert (ohne manuelle Intervention) nach erfolgreichem Testing auf unterschiedlichen Deployment-Umgebungen (Test, Preprod, Prod) eingespielt werden. Es gibt immer eine lauffähige, produktive Umgebung.
- Für Hersteller von Kanzleisoftwaren, für IT-Behörden und andere Beteiligte sollen geeignete Testumgebungen bereitgestellt werden.

Die agile Entwicklung basierend auf Cloud bringt auch ein Risiko. Software und Applikationslogik können zwar schnell ausgerollt werden, dies gilt jedoch nicht für Daten. Entsprechend sind im Design Datenkonsistenz und Prüfprozesse zu beachten.

Prinzip 20	Verfügbarkeit und Monitoring

- Von der Testphase bis zur Einführung des Obligatoriums muss die Qualität der Support- und Betriebsprozesse kontinuierlich mit den Nutzern und dem Anspruch wachsen können.
- Alle applikatorischen Service und Infrastrukturkomponenten generieren Logdaten, Metriken und Tracing by Design.
- Alle Service Level Indicators (aus diesen Logdaten, Metriken und Tracing-Informationen) fliessen zusammen und können zentral ausgewertet und korreliert werden.
- Es existiert ein zentrales Monitoring für sämtliche technisch oder fachlich relevanten Events, welches die definierten SLA Werte ausweisen kann und gegebenenfalls alarmieren kann.
- Sicherheitsrelevante Audit-Events sind Teil des Mentorings. Unregelmässigkeiten können überwacht und alarmiert werden.

Siehe Anhang W1 Service Level Agreement für die Anforderungen bezüglich technischer Verfügbarkeit und Servicezeiten.

Prinzip 21	Technologiemanagement

- Die eingesetzten Technologieprodukte müssen punkte Betrieb und kontinuierlicher Weiterentwicklung.
- Alle eingesetzten Technologieprodukte sind im zentralen Monitoring eingebunden
- Regelmässige und automatisierte Patch- und Updatezyklen sind auf sämtlichen Technologiekomponenten und eingesetzten Softwarelibraries etabliert (Vermeidung von Software- und Infrastruktur Erosion).

Prinzip 22	Umgang mit Deployment-Artefakten

- Deployment-Artefakte werden zur Build-Zeit (vor dem Deployment) automatisierten Acceptance und Security Checks unterzogen (bspw. Docker security Scans, Schwachstellen Scans).
- Es ist sichergestellt, dass lediglich geprüfte Artefakte auf der Runtime-Umgebung eingespielt werden können.
- Es ist jederzeit ersichtlich, welche Libraries, Software-Artefakte und Patchlevel von Drittherstellern in welcher Version im Einsatz sind.

Prinzip 23	Testing

- Entlang der Testpyramide existieren für alle Levels (Unit, Component, Integration, API, End-2-End) automatisierte und nachvollziehbare Tests.

2.5 Design Tradeoff

Die erwähnten Prinzipien können nicht alle zu 100% erfüllt werden. Es müssen immer wieder Tradeoff Entscheide gefällt werden. Vergleiche dazu das sog. CAP-Theorem, welches besagt, dass in einem verteilten System nicht gleichzeitig Konsistenz, Verfügbarkeit (Availability) und Partitionstoleranz erreicht werden kann. Wir priorisieren in diesem Sinne:

> Die Integrität von Dokumenten über ihren gesamten Lifecylce ist zentral. Die Unveränderbarkeit der Daten und der Audit Trail über den gesamten Datenlifecycle ist mit höchster Priorität zu behandeln. Dann hat Zugriffsschutz auf die Daten hat Priorität. D.h. Akten dürfen in keinem Fall von nicht autorisierten Personen eingesehen werden können.

3 Business Services der Plattform «Justitia.Swiss»

Dieses Kapitel beschreibt die Business Services der Plattform «Justitia.Swiss».

3.1 Elektronische Akteneinsicht

Elektronische Akteneinsicht (eAE) bedeutet, dass an Verfahren beteiligte und berechtigte Personen oder Organisationen über digitale Kanäle Einblick in elektronisch geführte und einsehbare Akten nehmen. Die berechtigten Akteure können dank der digitalen Akten jederzeit, ortsunabhängig und parallel Akten einsehen.

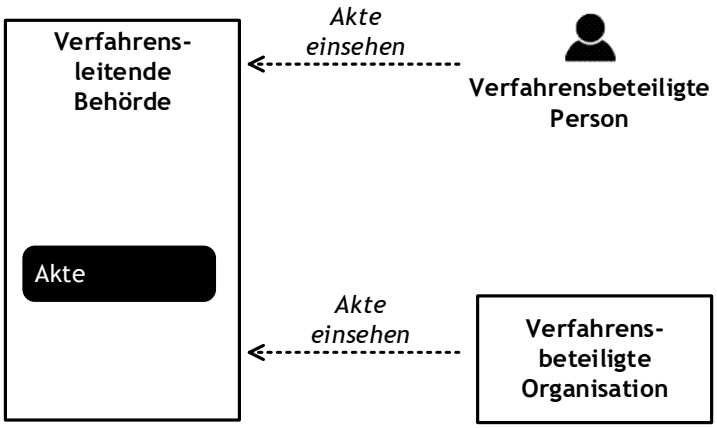


Abbildung 1: Elektronische Akteneinsicht – Beteiligte Akteure

Erläuterungen:

- Eine **verfahrensleitende Behörde** (Justizbehörde, Verwaltungseinheit) leitet das Verfahren. Sie ist die Eignerin der Akte. Sie, beziehungsweise ihre Mitarbeitenden, bewirtschaften die Akte und entscheiden, wer welche Aktenstücke zu welchem Zeitpunkt einsehen darf. Aus Sicht der Plattform verfügt die Behörde über eine IT-Landschaft, um Akten digital zu bewirtschaften, resp. einsehbare Aktenstücke digital zur Verfügung zu stellen.
- Eine **verfahrensbeteiligte Person** ist eine natürliche Person, die berechtigt ist, die Aktenstücke eines Verfahrens einzusehen. Typische Beispiele: Eine prozessfähige Person, die Partei in einem Verfahren ist, oder ihr/e Rechtsvertreter/in. Sie greift über ein Web-Interface auf die Akten zu.
- Eine **verfahrensbeteiligte Organisation** ist eine Organisation, die berechtigt ist, die Aktenstücke einzusehen. Typisches Beispiel: Eine juristische Person in einem Verfahren oder eine Anwaltskanzlei mit mehreren beschäftigten Anwälten/Anwältinnen, die als Rechtsvertreterin an einem Verfahren beteiligt ist und unter Umständen in einer eigenen, spezialisierten IT-Umgebung arbeitet. Zu beachten ist, dass eine verfahrensleitende Behörde auch in der Rolle einer verfahrensbeteiligten Organisation Einsicht in Verfahren anderer Behörden nehmen kann.

3.2 Elektronischer Rechtsverkehr

Im **Elektronischen Rechtsverkehr (ERV)** tauschen verfahrensleitende Behörden und Verfahrensbeteiligte Organisationen oder Personen über digitale Kanäle Meldungen mit elektronischen Dokumenten rechtsgültig, fristwahrend und ausreichend sicher[3] aus.

[3] Siehe Kapitel 6.3 für die Schutzziele der Informationssicherheit für das Verständnis von «sicher».

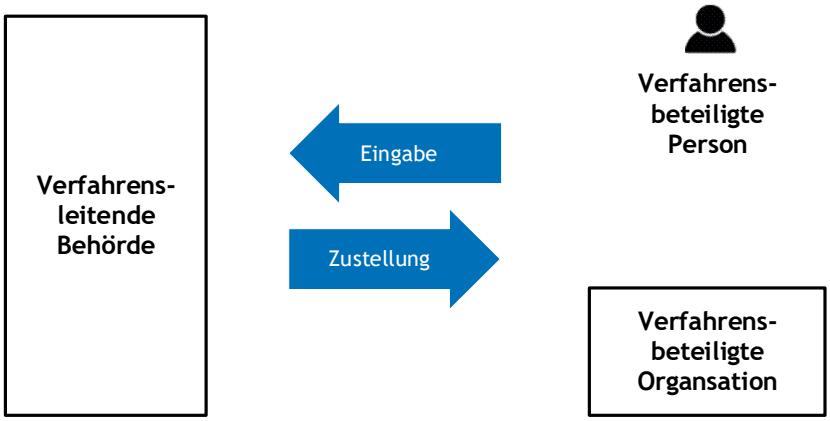


Abbildung 2: Elektronischer Rechtsverkehr – Beteiligte Akteure

Erläuterungen:

- Die **verfahrensleitende Behörde** (Justizbehörde, Verwaltungseinheit) leitet das Verfahren.
- Eine **verfahrensbeteiligte Person** ist eine natürliche Person, die an einem Verfahren beteiligt ist und über ein Web-Interface kommuniziert. Typische Beispiele sind eine Partei, ein/e Rechtsvertreter/in, ein/e Experte/in oder ein/e Dolmetscher/in.
- Eine **verfahrensbeteiligte Organisation** ist eine Organisation, die an einem Verfahren beteiligt ist und unter Umständen über eine eigene IT-Infrastruktur verfügt.
- Mit **Zustellung** bezeichnen wir den elektronischen Versand von Meldungen durch eine verfahrensleitende Behörde an eine verfahrensbeteiligte Person oder Organisation. Oft wird das auch ausgehender Rechtsverkehr genannt. Zustellungen sind meist mit einer rechtswirksamen Frist versehen.

Mit **Eingabe** bezeichnen wir die elektronische, rechtswirksame Übermittlung von Dokumenten durch eine verfahrensbeteiligte Person oder Organisation an eine verfahrensleitende Behörde. Oft wird das auch eingehender Rechtsverkehr genannt.

3.3 Adressverzeichnis

Die Plattform führt ein schweizweites Verzeichnis aller verfahrensleitenden Justizbehörden und am elektronischen Rechtsverkehr, resp. der elektronischen Akteneinsicht teilnehmenden verfahrensbeteiligten Organisationen und Personen. Das Adressverzeichnis erlaubt den Verfahrensbeteiligten, je nach Rolle und Verfahren am Rechtsverkehr teilzunehmen und Akteneinsicht wahrzunehmen.

4 Fachliches Modell der Plattform

Folgendes Modell zeigt die relevanten Informationsobjekte[4] der Plattform. Dieses wird in den folgenden Unterkapiteln vertieft.

[4] Das Dokument verwendet die Notation der Unified Modeling Language (UML). 8.5 enthält dafür eine kurze Zusammenfassung und Einführung.

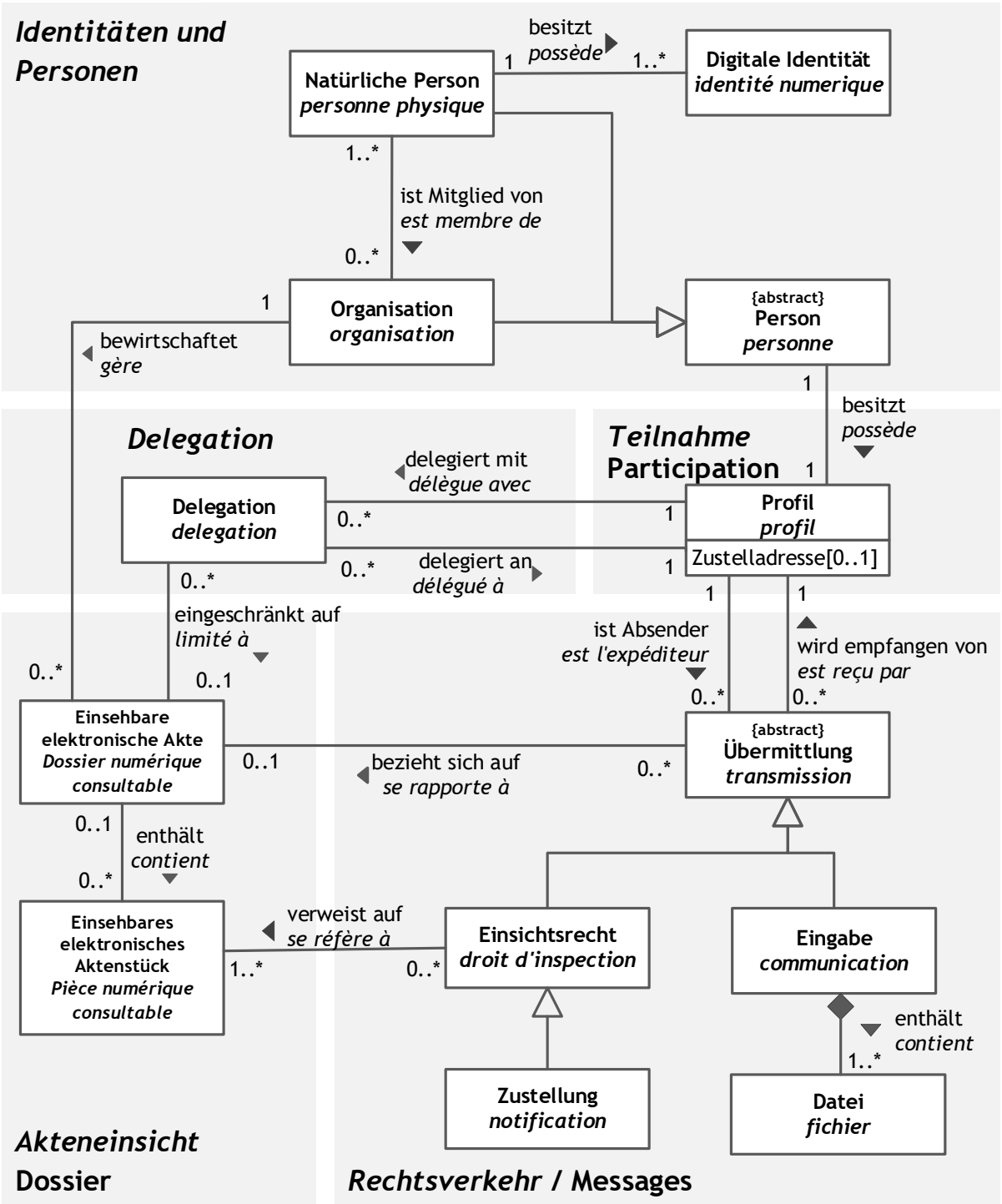


Abbildung 3: Konzeptionelles Informationsmodell

4.1 Identitäten und Personen

Die Plattform «Justitia.Swiss» wird Stammdaten zu den Personen und Organisationen bewirtschaften, die die Plattform für die elektronische Akteneinsicht oder den elektronischen Rechtsverkehr nutzen.

4.1.1 Personen

Die Plattform wird Daten über Personen halten, bewirtschaften und mit dem Umfeld austauschen. Zusammenfassend bezeichnen wir diese Daten als **Personen-Stammdaten** (siehe Abbildung 4).

- Das Konzept und den Begriff der **natürlichen Person** übernehmen wir aus [eCH-0219]: «Eine natürliche Person ist ein Mensch als Rechtssubjekt». Die Plattform unterscheidet zwischen natürlichen Personen als (potentiell) verfahrensbeteiligte Personen in Justizverfahren und Mitarbeitern einer Organisation.

- Wir verwenden das Konzept einer **Organisation,** um eine Gruppe von Personen zu bezeichnen. Diese können sein:

    - Eine verfahrensbeteiligte Organisation, z.B. Anwaltskanzlei, juristische Personen etc. gemäss eCH-0219 (aus [eCH-0219]).

    - Eine verfahrensleitende oder verfahrensbeteiligte Behörde.

Als abstrakten Oberbegriff für eine natürliche Person und Organisation verwenden wir **Person**. In anderen fachlichen Domänen (Finanzwesen, Industrie, etc.) verwendet man dafür oft den Begriff Geschäftspartner oder einfach Partner.

Eine detaillierte Sicht auf Personen und Organisationen und deren Zusammenhänge gibt Abbildung 4. Das UML-Diagramm unterscheidet identifizierende Attribute der verschiedenen Arten von Personen. Der Subtyp 'nat. Person' ist ausschliesslich auf diesem Modell gezeichnet, um Einzelpersonen von Organisationen zu unterscheiden. Wir verzichten auf die umständliche Formulierung von 'natürlichen, verfahrensbeteiligten Personen'. Ebenfalls zeigt und betont das Diagramm, dass Mitarbeiter einer IDP-verwalteten Organisation nur genau einer Organisation (siehe Kapitel 4.1.1.3) zugeordnet sind, über die sie das Login haben.

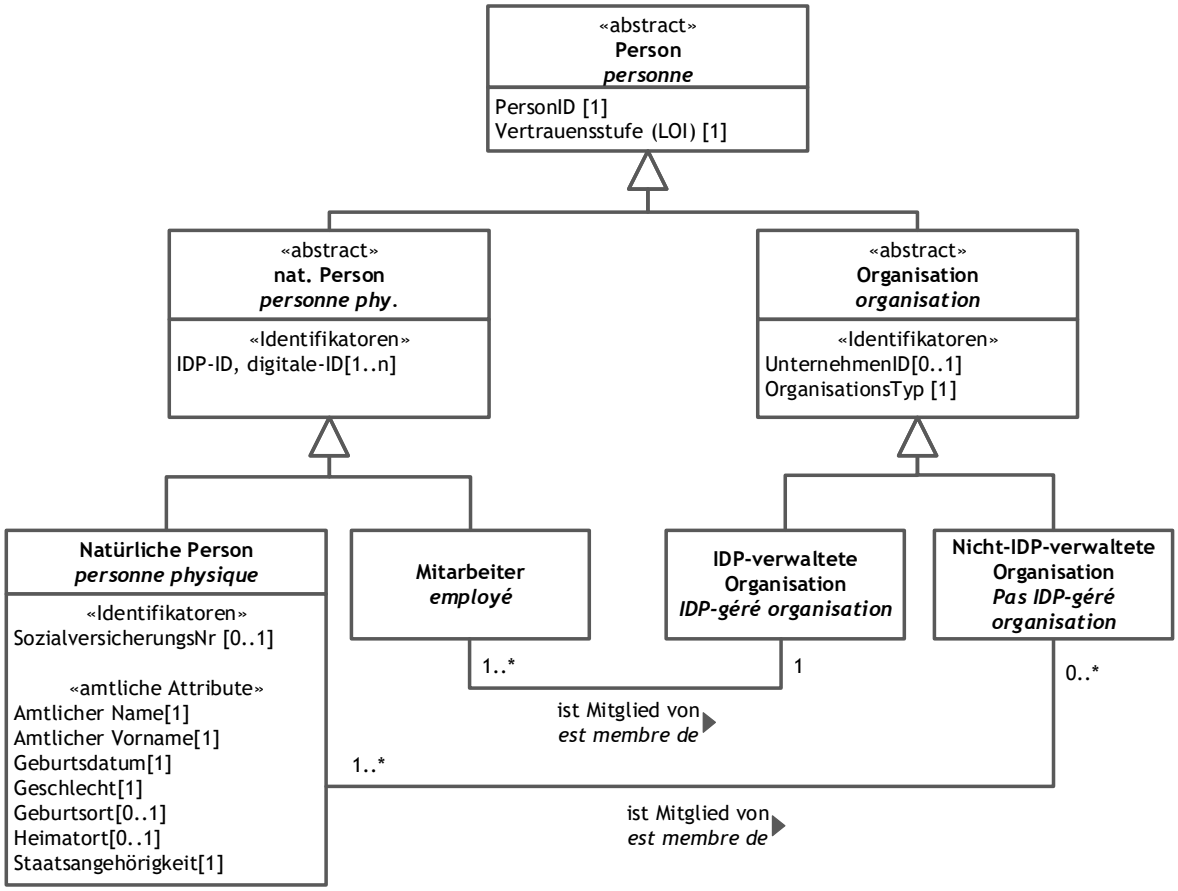


Abbildung 4: Personen und ihre Identifikatoren

Auf abstrakter Ebene nehmen wir an, dass die Plattform für Personen einen eigenen fachlichen Identifikator, die **PersonenID** vergibt und diesen für interne Zwecke nutzt. Da die Plattform jedoch keine Aufgabe in der Verwaltung von Personen hat, soll dieses Attribut nicht über Schnittstellen kommuniziert werden, sondern nur die extern verwalteten Identifikatoren.

Fachlich relevant aus Abbildung 4 sind 3 Arten von Personen, da diese in späteren Prozessen und Regeln anders behandelt werden müssen:

Typ der Person	Beschreibung
Natürliche Person	Natürliche Personen als (potenziell) verfahrensbeteiligte Personen in allen möglichen Rollen (Partei, Beteiligter, Vertreter etc.) Von diesen Personen muss die Plattform die amtlichen Attribute kennen, um sie als handelnde Personen nachweisen zu können.
Mitarbeiter	Personen als Mitarbeiter einer Organisation. Diese Personen handeln immer im Namen der Organisation. Für diese Personen muss die Plattform nur ihre digitale Identität kennen. (gleich wie technischen Schlüssel)
Organisation	Organisationen in verschiedenen Ausprägungen (OrganisationsTyp).

Tabelle 1: Typen von Personen

4.1.1.1 Natürliche Personen

Die **Sozialversicherungsnummer** (oder AHV-Nummer, AHVN13) ist eine eindeutige Personenidentifikationsnummer (für natürlicher Personen) in der Schweiz. Es bleibt bis zur Ausschreibung offen, ob die Sozialversicherungsnummer auf der Plattform bewirtschaftet werden darf. Zurzeit gibt es Argumente dafür und dagegen:

- Es gibt keine gesetzliche Grundlage dafür. Namentlich sieht das AHVG zurzeit nicht explizit vor, dass die AHV-Nummer auf der Plattform «Justitia.Swiss» verwendet werden darf. Gesetzliche Grundlagen gibt es für die Verwendung der Sozialversicherungsnummer in Strafverfahren, nicht aber explizit in Zivil- oder Verwaltungsverfahren. Im Strafprozess wird die AHV-Nummer als Identifikator für Personen verwendet, deshalb muss die Plattform eventuell für Prozesse die AHV-Nummer auch kennen und an berechtigte Akteure weiterleiten.
- Andererseits ist zurzeit das Geschäft «Systematische Verwendung der AHV-Nummer durch Behörden» in der parlamentarischen Beratung. Der Bundesrat schlägt damit vor, dass Behörden in Zukunft die AHV-Nummer systematisch als Personenidentifikator verwenden dürfen.

Anbieter müssen die Sozialversicherungsnummer auf der Plattform für natürliche Personen halten und bewirtschaften können. Sie können aber nicht davon ausgehen, dass für jede auf der Plattform bewirtschaftete natürliche Person eine eindeutige Sozialversicherungsnummer bekannt ist.

Da das ursprünglich vorgesehene E-ID Gesetz im Referendum vom März 2021 abgelehnt wurde, gehen wir davon aus, dass die Plattform verschiedene Identitätsprovider anschliesst und diese jeweils ihre eigenen IDs zur **digitalen Identifikation** der Personen haben (IDP-ID und digitale-ID in Abbildung 4).

Zu jeder natürlichen Person muss die Plattform eine Gruppe von personenidentifizierenden Attributen führen können. Dabei handelt es sich um folgende Attribute, die das E-ID-Gesetz als Teil der Personenidentifizierungsdaten für die Sicherheitsniveaus niedrig und substanziell bezeichnet:

- E-ID-Kundennummer
- amtlicher Name
- Vorname
- Geburtsdatum
- Geschlecht

- Geburtsort oder Heimatort[5]
- Staatsangehörigkeit

Die Wertebereiche dieser Attribute bleiben bis zur Ausschreibung offen.

Personenidentifizierende Attribute für natürliche Personen werden auf der Plattform aus zwei Gründen geführt:

1. damit Personenidentifikationsdaten von einem IDP für eine digitale-ID übernommen werden können, sofern die natürliche Person als Benutzerin der Plattform und Inhaberin der digitalen-ID dem zustimmt.
2. damit Behörden (zum Beispiel ein Gericht) im Adressverzeichnis beispielsweise nach Namen, Vornamen, Geburtsdatum und Geschlecht suchen kann, um zu prüfen, ob eine natürliche Person auf der Plattform bereits über ein Profil mit einer Zustelladresse verfügt.

Die Attribute der natürlichen Personen werden immer vom entsprechenden Identitätsprovider übernommen. Behörden können Profile mit Zustelladresse suchen, die Plattform garantiert jedoch nicht, dass die so gefundenen Profile genau einer realweltlichen Person gehören (Prinzip 2).

4.1.1.2 Organisationen

Die **UnternehmensID** (oder UID) ist ein eindeutiger Identifikator für Organisationen aus dem Betriebs- und Unternehmensregister (BUR). Wenn einer Organisation im BUR eine UnternehmensID zugeordnet ist, dann wird sie auf der Plattform geführt und bewirtschaftet. Die UID wird namentlich auch für Anwälte definiert, welche in kantonalen Anwaltsregistern eingetragen sind und welche auf der Plattform eine Organisation für sich als praktizierende Anwälte eröffnen wollen.

Einzelne Justizbehörden haben (bisher) keine UID. Man beachte jedoch, dass Behörden ihre zur Einsicht gegebenen Aktenstücke mit einem amtlichen Siegel nach ZertES (Art. 2) versehen müssen. Dieses Siegel muss die UID als Identifikator der siegelnden Organisation enthalten.

Anbieter müssen die UnternehmensID einer Organisation auf der Plattform halten und bewirtschaften können. Sie können aber nicht davon ausgehen, dass für jede auf der Plattform bewirtschaftete Organisation eine eindeutige UnternehmensID bekannt ist. Ferner müssen sie keine Mechanismen bereitstellen, um die Stammdaten auf der Plattform mit den Stammdatenbeständen des BUR abzugleichen.

Bis auf weiteres soll ebenfalls kein Anschluss oder Abgleich mit den kantonalen Anwaltsregistern vorgesehen sein.

Organisationen haben einen **OrganisationsTyp**. Abhängig vom Typ sind unterschiedliche Businessregeln möglich. Die wichtigste Unterscheidung erfolgt durch die beiden Typen:

- **Justizbehörde**: die Organisation ist eine verfahrensleitende Justizbehörde und handelt im Namen der Justizbehörde.[6]
  Motivation:
  - Auf der Plattform ist damit aus den Stammdaten klar, welche Profile einer verfahrensleitenden Behörde gehören.
  - Damit kann die Plattform im Adressverzeichnis ausweisen, welche Zustelladressen einer verfahrensleitenden Behörde gehören und damit an welche Zustelladressen im eingehenden ERV Eingaben übermittelt werden können.

[5] Das abgelehnte E-ID-Gesetz sieht tatsächlich Geburtsort vor, nicht Heimatort, wie in der Schweiz traditionell üblich. Wir verlangen, dass für Schweizer Bürger (Staatsangehörigkeit = CH) der Heimatort bekannt ist, für Ausländer der Geburtsort.

[6] Beachte, dass eine solche Organisation auch als Verfahrensbeteiligte am ERV oder eAE teilnehmen kann (siehe Beispiele in Kapitel 5.)

- **Verfahrensbeteiligte Organisation:** Aus Sicht der Plattform sind das Personen, die Eingaben erfassen und Akteneinsicht wahrnehmen, resp. Zustellungen empfangen können. Es wird erwartet, dass hier im Lauf der Zeit eine weitergehende Verfeinerung erfolgen wird. z.B.:
    - Benutzer als Anwälte nutzen die Plattform besonders intensiv. Die Plattform umfasst deshalb Funktionalitäten, die voraussichtlich ausschliesslich Anwälten zur Verfügung stehen werden. Kandidaten dafür sind fortgeschrittene Funktionen bei der elektronischen Akteneinsicht (Vermerke und Tags auf einsehbaren elektronischen Akten anbringen) oder die Möglichkeit, eigene Berechtigungen an andere Benutzer delegieren zu können. Die Plattform muss deshalb in den Stammdaten bewirtschaften, ob es sich bei einer Person um einen Anwalt handelt oder nicht.
    - Weitere Typen für Vereine, Stiftungen, Rechtsschutzversicherung etc.
    - Typen für verfahrensbeteiligte Behörden wie Polizei und andere Verwaltungsbehörden.

  Der Anbieter muss einen flexiblen Mechanismus vorsehen, damit mit vertretbarem Aufwand weitere Typen mit spezifischen Geschäftsregeln definiert werden können. Es ist insbesondere zu beachten, dass weitere Organisationen auch behördlicher Natur sind, wie Polizei oder andere Verwaltungsbehörden.

4.1.1.3 Administrierte und selbst-administrierte Organisationen

Die Plattform unterscheidet zwischen administrierten Organisationen und selbst-administrierten Organisationen, je nach Art des Prozesses zur Eröffnung (und Veränderung) der Organisation.

- Jede natürliche Person kann selbst-administriert eine Organisation auf der Plattform gründen. Ob diese Organisation ein realweltliches Pendant hat (z.B. eine juristische Person) wird durch die Plattform nicht geprüft. Entsprechend kann die Plattform keine Qualitätsgarantie für diese Organisation abgeben. Die Kommunikation mit dieser Organisation erfolgt 'auf eigenes Risiko'.
- Grosse (bekannte) Unternehmen wie Banken, Versicherungen und öffentliche Verkehrsunternehmen können über die Plattform am Rechtsverkehr teilnehmen. Durch den administrierten Prozess für solche Unternehmen garantiert die Körperschaft eine gewisse Qualität der Organisation und gewährleistet insb. den Namen dieser Organisation im Adressverzeichnis.
- Justizbehörden und andere Behörden sind immer administrierte Organisationen, da diese durch 'die Kantone' resp. 'den Bund' auf der Plattform erfasst werden.

4.1.1.4 IDP-verwaltete Organisationen

Für administrierte Organisationen bietet die Plattform die Möglichkeit an, dass ihre Mitarbeiter mit ihrem Mitarbeiterlogin auf der Plattform arbeiten können (Single-Sign-On). Für solche Mitarbeiter braucht die Plattform keine (!) amtlichen Attribute zu kennen. Einzig für die Nachvollziehbarkeit im Fehlerfall wird eine digitale Identität benötigt.

Solche Personen als Mitarbeiter dürfen kein Profil erstellen, mit dem sie am Rechtsverkehr oder der Akteneinsicht teilnehmen. Sie sollen einzig die Funktionen, die sie für ihre Arbeit benötigen, ausführen können (siehe Kapitel 4.1.2.1 über die Beziehungen von Personen zu Organisationen).

4.1.1.5 Anwälte als Organisation – Anwaltspatent

Die Plattform wird natürlichen Personen erlauben, eine Organisation vom Typ Anwalt, resp. Anwaltskanzlei zu bewirtschaften, damit diese Person ihre Kommunikation mit Justizbehörden als professioneller Vertreter wahrnehmen kann.

Die Plattform wird für solche Organisationen Attribute vorsehen, mit denen sie selbstverwaltet festlegen, wie sie auf der Plattform sichtbar sein wollen. Die Einzelheiten (detailliertes Datenmodell für die Attribute) werden erst nach der Ausschreibung festgelegt. Eine Anbindung an Anwaltsregister steht nicht im Fokus. Diese Attribute sollten jedoch (gemäss Prinzip 1) nicht auf der Organisation bewirtschaftet werden, sondern auf dem Profil dieser Organisation.

Ein Anwaltspatent kann aufgrund von Massnahmen aus kantonalen Anwaltsgesetzen oder gemäss Bundesgesetz über die Freizügigkeit der Anwältinnen und Anwälte [BGFA] suspendiert oder entzogen werden. Es gibt aber keine Absicht, auf der Plattform «von Amtes wegen» jederzeit den aktuellen Status eines Anwaltspatents zu bewirtschaften und ausweisen zu können. Attribute über ihren beruflichen Status werden Anwälte ausschliesslich selbstbedient bewirtschaften können. Die Attribute werden nicht «von Amtes wegen» auf der Plattform für Anwälte bewirtschaftet und nachgeführt (weder durch Gerichte noch durch kantonale Justizbehörden noch durch die öffentlich-rechtliche Körperschaft (örK) noch durch Anwaltsverbände).

Folgende Konsequenzen ergeben sich daraus:

- Die Plattform wird nie Attribute über den beruflichen Status von Anwälten auf der Plattform nutzen, um auf dieser Basis Berechtigungen zu erteilen oder zu entziehen.
- Die Plattform wird Informationen über den beruflichen Status eines Anwalts im Adressverzeichnis nur soweit und nur in der Form ausweisen, wie sie Anwälte selbstbedient auf der Plattform erfasst haben.
- Behörden werden sich nicht auf Attribute über den beruflichen Status eines Anwalts in den Personenstammdaten auf der Plattform stützen, wenn sie einem Anwalt Einsicht in eine Akte gewähren oder entziehen, oder wenn sie einen Anwalt als Vertreter in einem Verfahren zulassen oder ausschliessen. Sie werden verlässliche Informationen über den beruflichen Status eines Anwalts aus den gleichen Quellen wie bisher und nicht von der Plattform beziehen.

4.1.1.6 Postalische Adressen

Zu Personen werden auf der Plattform keine postalischen Adressen bewirtschaftet.

- Es sind keine Prozesse vorgesehen, in denen die Plattform mit Personen auf dem Postweg kommuniziert. Die Plattform wird Parteien in einem Verfahren namentlich keine Zustellungen und Einsichten auf dem Postweg zukommen lassen. Die Plattform wird deshalb keine postalischen Adressen für die Zustellung oder Einsichtsrechte bewirtschaften.
- Benutzern wird die Nutzung der Plattform nicht in Rechnung gestellt. Die Plattform wird die zukünftige öffentlich-rechtliche Körperschaft (örK) nicht in Rechnungsprozessen unterstützen. Auf der Plattform sind deshalb keine postalischen Adressen zu bewirtschaften, die als Rechnungsadresse bewirtschaftet werden.
- Für Personen, die als Ansprechpartner von administrierten Organisationen gelten, kann es nötig sein, ihre postalischen Adressen (z.B. für Verträge) zu kennen. Diese Adressen werden höchstwahrscheinlich nicht auf der Plattform bewirtschaftet, sondern in einem administrativen Tool ausserhalb. Details dazu werden im Operating Model erarbeitet.

Auf der Plattform werden jedoch zu Personen Attribute für **elektronische Adressen** bewirtschaftet, siehe z.B. Kapitel 4.2.2 über Benachrichtigung.

4.1.1.7 Rollen von Personen in Verfahren

Personen sind in bestimmten Rollen an Verfahren beteiligt. In einer ersten groben Klassifikation nehmen Personen in einem Verfahren eine verfahrensleitende oder eine verfahrensbeteiligte Rolle ein. Differenziert man weiter, nehmen verfahrensbeteiligte Personen in einem Verfahren die Rollen Partei, Vertreter oder weiterer Beteiligter ein (Abbildung 5).

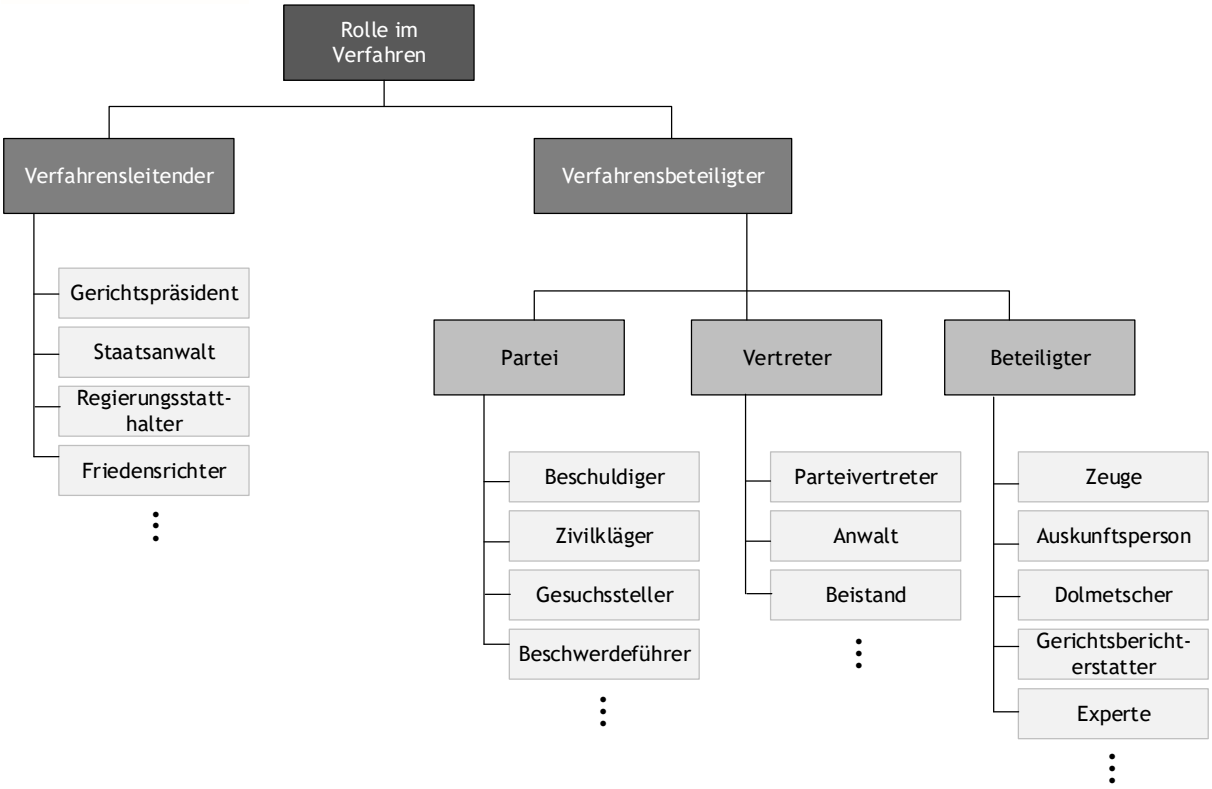


Abbildung 5: Rollen von Personen im Verfahren (Verfahrens-Rollen)

Für verfahrensleitende Behörden (Gerichte, Staatsanwaltschaften, etc.) ist es wichtig zu wissen, welche Personen mit welchen Verfahrens-Rollen an einem Verfahren beteiligt sind. Sie bewirtschaften deshalb in ihren Fachapplikationen die dafür notwendigen Stammdaten. Verfahrensleitende Behörden übertragen zudem Stammdaten zu Personen und ihren Verfahrens-Rollen in den einsehbaren elektronischen Aktendeckeln einer einsehbaren elektronischen Akte (siehe Abschnitt 4.3.1).

Die Plattform selbst bewirtschaftet keine Daten zu Verfahrens-Rollen, sie kennt lediglich die elementare Unterscheidung:

- Organisationen vom Typ 'Justizbehörden' können Eingaben empfangen und Zustellungen vornehmen;
- Alle anderen Organisationen und natürlichen Personen können Eingaben vornehmen und Zustellungen empfangen.

4.1.2 Beziehungen zwischen Personen

In diesem Kapitel wird die Beziehung zwischen Personen beschrieben, welche die Plattform braucht (es gibt nur eine Beziehung mit verschiedenen Ausprägungen) und welche sie nicht braucht.

4.1.2.1 Die Beziehung «ist Mitglied von»

In den Stammdaten der Plattform kann/können jeder Organisation eine oder mehrere natürliche Personen über eine Beziehung «ist Mitglied von» zugeordnet sein. Diese Beziehung selbst drückt das Recht aus, das die natürliche Person in Bezug auf die Organisation hat. Es gibt unterschiedliche Arten von Rechten oder Funktionen, welche die Plattform kennen muss:

Funktion	Berechtigung
Administrator	Darf die Beschreibung der Organisation ändern, neue Personen hinzufügen, Delegationen auf dem Profil errichten (siehe Kapitel 4.4). Eine Organisation braucht immer einen Administrator.

Handelnd	Ist die natürliche Person, welche die Geschäfte der Organisation behandelt (Art. 55c ZGB). Diese Person hat im Allgemeinen Zeichnungsrecht der Organisation, Organvertretung oder eine Handlungsbefugnis. Bei Eingaben prüft die Justizbehörde, ob die formellen Voraussetzungen erfüllt sind. Eine Organisation, welche keine Justizbehörde ist, braucht mindestens eine handelnde Person.[7]
Eingaben aufgeben	Person kann Eingaben über die Plattform erfassen und aufgeben.
Eingaben empfangen	Nur für verfahrensleitende Behörden: Person kann Eingaben empfangen.
Zustellung aufgeben	Nur für verfahrensleitende Behörden: Person kann Zustellungen aufgeben.
Zustellungen (erstmalig) empfangen	Person kann eine Zustellung empfangen und damit u.U. die Frist auslösen.
Akteneinsicht vornehmen	Person kann Aktenstücke (sofern diese zugestellt wurden) einsehen.

Tabelle 2: Funktionen der Mitglieder einer Organisation

Die Relation «ist Mitglied von» wird für IDP-verwaltete Organisationen im IAM-System des IDP verwaltet. Deshalb sind sämtliche Mitarbeiter einer IDP-verwalteten Organisation genau dieser Organisation zugeordnet. Bei einer nicht-IDP-verwalteten Organisation werden jedoch natürliche Personen als Mitglieder der Organisation auf der Plattform verknüpft. Eine natürliche Person kann damit (mit demselben Login) Mitglied von mehreren Organisationen sein.

4.1.2.2 Keine wechselseitigen Beziehungen zwischen natürlichen Personen

In den Stammdaten der Plattform werden keine wechselseitigen Beziehungen zwischen natürlichen Personen bewirtschaftet.

Die Plattform wird die anerkannten Anforderungen erfüllen, dass namentlich Anwälte bestimmte Rechte an andere Benutzer delegieren oder auf der Plattform eine Art Stellvertreter hinterlegen können. Sie wird diese Anforderungen erfüllen können, ohne wechselseitige Beziehungen zwischen natürlichen Personen bewirtschaften zu müssen (siehe Abschnitt 4.5.1).

Für Stammdaten auf der Plattform gilt folgendes:

- Die Plattform bewirtschaftet keine Stammdaten zu disziplinarischen Beziehungen in Anwaltskanzleien («Mitarbeiter A arbeitet für Anwalt B in Kanzlei C»).
- Die Plattform bewirtschaftet keine Stammdaten zu disziplinarischen Beziehungen in Behörden («Mitarbeiter A arbeitet für Staatsanwältin B in Staatsanwaltschaft C»).
- Die Plattform bewirtschaftet keine Stammdaten zu Vertretungs-Beziehungen («Anwalt A ist Rechtsvertreter von Person B», «Natürliche Person ist Elternteil von natürlicher Person B», «Natürliche Person A ist Beistand/Vormund von natürlicher Person B», etc.).

4.1.2.3 Keine hierarchischen Beziehungen zwischen Organisationen

In den Stammdaten der Plattform werden keine hierarchischen Beziehungen zwischen Organisationen abgebildet.

[7] Hinweis: im BEKJ-VE Art. 24 ist der Gruppenadministrator sowohl die juristisch handelnde Person als auch der (technische) Administrator.

Für Stammdaten auf der Plattform gilt Folgendes:

- Die Plattform bewirtschaftet keine Stammdaten zur Aufbauorganisation einer Anwaltskanzlei («Anwaltskanzlei A hat die Bereiche A1 und A2. Der Bereich A2 ist in die Abteilung A21, A22 und A23 unterteilt»). Falls solche Bereiche mit eigenen Zustelladressen definiert werden sollen, wären das 4 «eigenständige» Organisationen: A1, A21, A22 und A23.
- Die Plattform bewirtschaftet keine Stammdaten zur Aufbauorganisation einer Behörde («Das Gericht G besteht aus den Spruchkörpern S1, S2 und S3»).

4.1.3 Digitale Identitäten von natürlichen Personen

Natürliche Personen, die die Plattform nutzen wollen, müssen sich ausreichend vertrauenswürdig identifizieren und authentisieren: Sie müssen über eine **Digitale Identität** verfügen, die von der Plattform akzeptiert wird.

Wir verwenden das Konzept digitale Identität wie in [eCH-0219], schärfen die Definition aber etwas[8]:

> *Eine **digitale Identität** ist die Repräsentation einer natürlichen Person. Eine digitale Identität hat einen Identifikator (eindeutiger Name), meist zusammen mit einer Menge von zusätzlichen Attributen, welche innerhalb eines Namensraumes (und damit einer Domäne) eindeutig einer natürlichen Person zugewiesen werden können. Eine natürliche Person kann mehrere digitale Identitäten haben.*

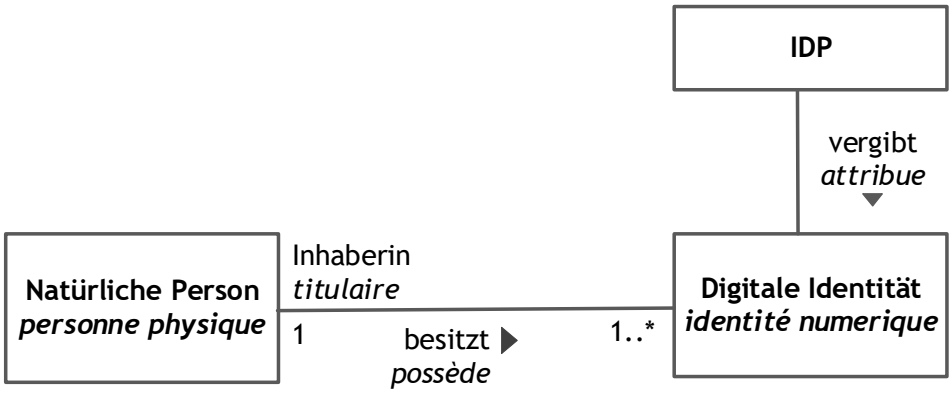


Abbildung 6: Digitale Identität und Identitätsprovider

Eine digitale Identität wird durch die Plattform **akzeptiert**, wenn sich eine natürliche Person als deren Besitzerin mit dieser digitalen Identität bei der Plattform identifizieren und authentisieren kann und die Plattform den entsprechenden Identitäts-Provider akzeptiert. Die Plattform wird strenge Bedingungen an digitale Identitäten stellen, bevor sie diese akzeptiert. Gemäss [VE-BEKJ] muss eine digitale Identität für die Plattform das Sicherheitsniveau substanziell haben. Inhaber einer digitalen Identität, die die Plattform akzeptiert, werden sich mit einem Verfahren der starken Authentisierung gegenüber der Plattform authentisieren müssen. Die organisatorischen Bedingungen müssen noch beschrieben werden.

Heute gibt es bereits zahlreiche konkrete Beispiele für digitale Identitäten, die die Plattform möglicherweise akzeptieren wird:

- Digitale Identitäten, die Kantone ihren Bürgerinnen und Bürgern ausstellen, zum Beispiel das ZUGLOGIN oder die digitale Identität des Kantons Schaffhausen.

[8] Statt Subjekt verwenden wir natürliche Person. Andere Formen von Subjekten (Dinge, Organisationen) sind hier nicht relevant. Zudem verwenden wir durchgehend digitale Identität statt E-Identity. eCH-0219 verwendet die beiden Begriffe synonym.

- Digitale Identitäten, die von IAM-Dienstanbietern als Dienstleistung an natürliche Personen vergeben werden, zum Beispiel die SwissID des IAM-Dienstanbieters Suisse Sign Group AG oder die Mobile-ID der Swisscom AG.

- Digitale Identitäten, die Behörden und Unternehmen ihren Mitarbeitenden als natürliche Person zuteilen, zum Beispiel das «Mitarbeiter-Login» einer Mitarbeiterin oder eines Mitarbeiters des Bundesgerichts.

Bis zur Ausschreibung bleibt offen, welche digitalen Identitäten die Plattform akzeptieren wird. Anbieter können in ihren Angeboten von folgenden Rahmenbedingungen ausgehen:

1. Die Plattform wird selbst keine neue digitale Identität vergeben.

2. Die Plattform wird mindestens eine digitale Identität akzeptieren, die ein externer IAM-Dienstleister vergibt. Die Plattform wird zu diesem Zweck über Protokolle des föderierten IAM mit dem externen IAM-Dienstleister gekoppelt. Um welche digitale Identität es sich konkret handeln wird, bleibt bis zur Ausschreibung offen.

Jede digitale Identität hat einen Identifikator, den wir als **Digitale-Identität-ID** bezeichnen. Format und Wertebereich des Identifikators unterscheidet sich von IAM-Dienstanbieter zu IAM-Dienstanbieter. Der Identifikator wird durch den IAM-Dienstanbieter vergeben.

Falls eine natürliche Person eine akzeptierte digitale Identität **besitzt**, kann die Plattform die natürliche Person mit der digitalen Identität **verknüpfen**. Die Plattform stellt damit eine Verknüpfung zwischen der Personen-ID (dem fachlichen Identifikator der natürlichen Person) und dem Identifikator der digitalen Identität (Digitale-Identität-ID) her.

Eine digitale Identität wird auf der Plattform mit der natürlichen Person verknüpft, wenn sie sich zum ersten Mal erfolgreich (via den IAM-Dienstanbieter, der die digitale Identität ausgibt) bei der Plattform anmeldet. Die digitale Identität gilt dann als verknüpft. Eine natürliche Person, die über mindestens eine verknüpfte digitale Identität verfügt, kann zusätzliche akzeptierte digitale Identitäten verknüpfen. Eine natürliche Person kann die Verknüpfung mit einer digitalen Identität auf der Plattform lösen.

Wenn eine natürliche Person (aus was für einem Grund auch immer) den Identitätsprovider wechselt, muss sie die Möglichkeit haben, die neue digitale Identität mit der alten zu verknüpfen. Die Plattform muss entsprechende Funktionalitäten anbieten, damit Personen dies selbstständig tun können.

Ein **Benutzer** (der Plattform) ist eine natürliche Person oder ein Mitarbeiter, die auf der Plattform mit mindestens einer akzeptierten digitalen Identität verknüpft ist.

4.2 Profile ermöglichen die Teilnahme

Eine Person, die über die Plattform Akteneinsicht wahrnimmt oder am elektronischen Rechtsverkehr teilnimmt, macht dies über **Profile**. Ein Profil ist ein Stammdatenobjekt, das auf der Plattform folgende zentrale Aufgaben wahrnimmt:

1. Das Profil kann die Zustelladresse der besitzenden (natürlichen) Person oder der Organisation tragen. Das Profil repräsentiert in diesem Fall ein Postfach für Übermittlungen.[9]

2. Zur Zustelladresse können optionale Beschreibungen des Inhabers definiert werden, die im Adressverzeichnis dargestellt werden sollen.

[9] Beachte, dass die Zustelladresse optional auf dem konzeptionellen Modell ist. Das bedeutet, dass diese natürliche Person selber nicht als Partei am elektronischen Rechtsverkehr teilnimmt. Ein Beispiel wäre ein Mitarbeiter einer Organisation, der (aus modelltechnischen Gründen als natürliche Person gezeichnet ist), aber eigentlich 'nur' als berechtigte Person innerhalb der Organisation auf dem Profil der Organisation Eingaben und Zustellungen bearbeitet.

3. Das Profil ist der Anknüpfpunkt für Delegationen (siehe Kapitel 4.4).
4. Das Profil steuert das Life-Cycle Management der Stammdaten (siehe Kapitel 6.7.1).
5. Auf dem Profil können die Benachrichtigungspräferenzen definiert werden (siehe Kapitel 4.2.2).
6. Auf dem Profil können persönliche Einstellungen für das Look & Feel der Plattform definiert werden.

Ein **Teilnehmer** ist eine Person (natürliche Person oder Organisation), die auf der Plattform mindestens ein **Profil mit einer Zustelladresse** besitzt.

Hinweis: zurzeit gehen wir davon aus, dass genau ein Profil je Person den Bedürfnissen der Anwender genügt. Wir können jedoch nicht ausschliessen, dass es in Zukunft das Bedürfnis geben wird, für eine Person unterschiedliche Profile mit unterschiedlichen Zustelladressen oder Adresstypen zu verwalten. In der physischen Welt in anderen Domänen haben sich auch unterschiedliche Typen von Postadressen (Korrespondenz- vs. Domiziladresse) etabliert. Entsprechend könnte das Bedürfnis entstehen, unterschiedliche Systeme oder unterschiedliche Typen von Verfahren über unterschiedliche Profile steuern zu wollen. Deshalb ist im Modell das Profil als eigenständiges Objekt mit einer 1-zu-1 Beziehung darstellt, damit das später auch zu 1-zu-n werden könnte. Eine Person ist nicht eine Adresse, sondern hat eine (oder eben mehrere) Adressen.

4.2.1 Zustelladresse

Das [VE-BEKJ] (Art. 17) definiert als Adresse:

> «Die E-Justiz-Plattform enthält ein Verzeichnis mit den Adressen, die für die Kommunikation über die Plattform verwendet werden.»

In den Stammdaten der Plattform ist die Zustelladresse ein Attribut des Profils. Anders gesagt: Das Profil ist der Träger der Zustelladresse. Jedes Profil hat genau eine Zustelladresse und die Zustelladresse ist über alle Profile eindeutig. Sie ist damit ein identifizierendes Attribut des Profils.

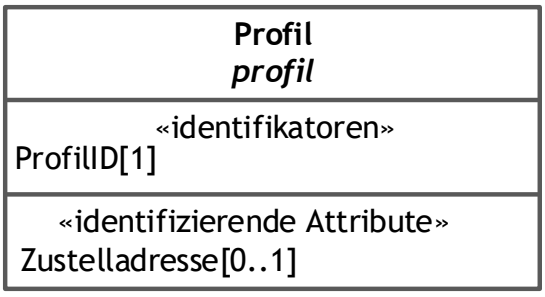


Abbildung 7: Zustelladresse als Attribut des Profils

Format und Wertebereich einer Zustelladresse werden erst nach Abschluss der Ausschreibung festgelegt.

4.2.2 Benachrichtigungs-Adressen

Wenn Teilnehmer im ERV eine Übermittlung erhalten, kann sie die Plattform über traditionelle asynchrone Kommunikationssysteme wie E-Mail oder SMS darüber benachrichtigen. Das ist eine Fähigkeit der Plattform, welche die Teilnehmer auf der Plattform optional nutzen können. Sie können zu diesem Zweck eine oder mehrere **Benachrichtigungs-Adressen** auf ihrem Profil hinterlegen.

Bis zur Ausschreibung bleibt offen, über welche traditionellen asynchronen Kommunikationssysteme die Plattform Benachrichtigungen verschicken wird. Die drei folgenden Kandidaten werden möglicherweise dazugehören. Potenzielle Anbieter müssen damit rechnen, dass sie Benachrichtigungs-Adressen für einen, alle oder weitere verwandte Kanäle in den Stammdaten bewirtschaften müssen:

- E-Mail mit einer E-Mail-Adresse als Benachrichtigungs-Adresse
- SMS mit einer Telefonnummer als Benachrichtigungs-Adresse
- Threema mit einer Threema-ID als Benachrichtigungs-Adresse

Hinweis: Beachte, dass die Benachrichtigung nicht nur ein Attribut des Profils ist, sondern auch dazu die Häufigkeit der Benachrichtigung, Filtermöglichkeiten (z.B. nur 'wichtige' Verfahren) oder ähnliches, eingestellt werden können müssen. Die Details dazu werden während agilen Entwicklungsiterationen definiert.

4.2.3 Sichtbarkeit und Vertrauensstufen des Adressverzeichnisses

Das Adressverzeichnis ist eine Sicht auf die Profile mit ihren Adressen, verknüpft mit den Inhabern, die die Profile besitzen.

Aus Gründen des Persönlichkeitsschutzes muss die Sichtbarkeit und Durchsuchbarkeit des Adressverzeichnisses eingeschränkt sein. Das Gesetz fordert ([VE-BEKJ] Art. 17):

- Mitarbeiter von Justizbehörden haben Zugriff auf alle Einträge des Adressverzeichnisses,
- Alle anderen haben nur Zugriff auf die Profile von Justizbehörden.

Deshalb wird die Plattform keinen allgemeinen Service bieten, mit dem auf eine 'geratene' Zustelladresse die Attribute des Profils angezeigt werden. Für das Verwalten von Delegationen (siehe Kapitel 4.4) müssen jedoch trotzdem Bezeichnungen des Profils sichtbar gemacht werden, damit der delegierte und der delegierende Benutzer wissen, wer 'die andere Seite' ist. Dieser Prozess soll durch ein Einladungsverfahren erfolgen.

Als Mitglied einer Organisation kann dieselbe natürliche Person 'mit unterschiedlichen Hüten' auf unterschiedliche Profile Zugriff haben. Daher sollen Datenfelder vorgesehen werden, mit denen der Inhaber des Profils optional den Zweck des Profils näher bezeichnen kann.

Die sichtbaren Attribute des Adressverzeichnisses stammen aus verschiedenen Quellen:

- Amtliche Attribute der natürlichen Personen als Inhaber
- Selbstdeklarierte Attribute auf einem Profil (z.B. die Bezeichnung oder Spezialisierung der Anwaltskanzlei)
- Bezeichnung von administrierten Organisationen (insbesondere Justizbehörden) mit durch den Betreiber geprüften Attributen

Um Fehler in nachgelagerten Systemen oder manuellen Prozessen, die diese Daten nutzen, zu vermeiden, soll immer die Herkunft und damit die **Vertrauensstufe dieser Attribute** ersichtlich sein (siehe dazu auch die Massnahme «Qualitätsmodell für die Attribute im Adressverzeichnis» im Anhang 8 ISDS Konzept Plattform Justitia.Swiss.

4.2.4 Zusammenfassung der Arten von Profilen

Zur Vereinfachung des Wordings für das Adressverzeichnis verwenden wir folgende Konvention:

Konvention	**steht für**	**Eigenschaften des Profils**
Profil einer Privatperson	Profile, dessen Inhaber eine natürliche Person (4.1.1.1) ist.	- Amtliche Attribute der Identität mit Qualität 'substantiell'. - Kann eine Zustelladresse enthalten, wenn die Person am Rechtsverkehr teilnimmt.
Profil einer Justizbehörde	Profil mit dem Inhaber Organisation vom Typ Justizbehörde (4.1.1.2)	- Mit Justizbehörde kann auch nur eine Abteilung innerhalb einer Justizbehörde gemeint sein. - Qualität der Attribute durch administrativen Prozess gewährleistet.

		- Hat immer ein Zustelladresse. - Profil kann Zustellungen aufgeben und Akteneinsicht geben. - Behörde kann IDP-verwaltet sein. - Dieses Profil ist im Adressverzeichnis für alle Benutzer sichtbar.
Selbst-administriertes Profil	Profil einer selbst-administrierten Organisation (4.1.1.3) vom Typ 'Verfahrensbeteiligte Organisation'	- Attribute selbstdeklariert. - Handelnde Person ist der Inhaber (und jur. Verantwortliche) des Profils. - Kann eine Zustelladresse enthalten.
Profil einer administrierten Organisation	Profil einer administrierten Organisation (4.1.1.3) vom Typ 'Verfahrensbeteiligte Organisation'	- Die Qualität einiger Attribute wird durch den administrativen Prozess sichergestellt. - Kann eine Zustelladresse enthalten. - Organisation kann IDP-verwaltet sein.
Mitarbeiterprofil	Profile eines Mitarbeiters einer IDP-verwalteten Organisation (4.1.1.4)	- Hat keine Zustelladresse. - Enthält persönliche Einstellungen (Präferenzen) des Mitarbeiters. - Zugehörige Organisation ist IDP-verwaltet.

Tabelle 3: Typen von Profilen

4.3 Akteneinsicht

Die Digitalisierung von Justizverfahren oder kurz Verfahren ist die zentrale Motivation des Projektes Justitia 4.0. In der Reichweite des Projekts liegt namentlich die Digitalisierung von drei **Typen von Justizverfahren**: Straf-, Zivil- und Verwaltungsgerichtsverfahren in der Schweizer Justiz.

Ein **Verfahren** ist ein gemäss Verfahrensvorschriften (StPO, andere Bundesgesetze) durchgeführter Prozess der Rechtsfindung.

Die Plattform Justitia.Swiss wird den ERV und die eAE in folgenden Arten von Verfahren unterstützen:

- in Vorverfahren und Untersuchungsverfahren der Staatsanwaltschaften (wie beschrieben in der StPO)
- in Straf-, Zivil-, Verwaltungsgerichtsverfahren (wie beschrieben in der StPO, ZPO, VwVG und den kantonalen Verwaltungsverfahrensgesetzen)
- in Verfahren bei Zwangsmassnahmengerichten (Untersuchungs- und Sicherheitshaft, Zwangsmassnahmen, wie beschrieben in der StPO)
- über alle Instanzen (Beschwerdeverfahren, Berufungsverfahren)

Ein Verfahren wird durch die **verfahrensleitende Behörde** geführt. Um welche Behörde es sich handelt, hängt von verschiedenen Kriterien ab, unter anderem von der Art des Verfahrens, ob es sich noch um ein Verfahren bei einer Staatsanwaltschaft oder bereits um ein Verfahren vor Gericht handelt, von der Instanz (1., 2. oder letzte Instanz) oder von der geographischen Zuständigkeit (Amt/Bezirk, Kanton oder ganze Schweiz).

Eine Akte gehört zu genau einem Verfahren «im engeren Sinne». Erläuterungen dazu:

- Aus Sicht der Anwälte kann man Verfahren «im engeren» und «im weiteren Sinn» unterscheiden. Verfahren «im weiteren Sinn» umfassen alles, was ein Anwalt im Rahmen einer bestimmten Kundenbeziehung als Verfahren führt. Verfahren «im engeren Sinn» umfassen das, was eine Behörde als Verfahren bezeichnet. Konkretes Beispiel: Wenn ein Anwalt zugleich in einer Kundenbeziehung ein Strafverfahren und ein damit verbundenes Verfahren für unentgeltliche

Rechtspflege führt, entspricht das aus der Sicht der Anwälte einem Verfahren «im weiteren Sinn» und aus der Sicht der Behörden zwei Verfahren «im engeren Sinn». Gleiches gilt, wenn ein Verfahren «im weiteren Sinn» an eine höhere Instanz gezogen wird. Die obere Instanz macht ein neues Verfahren «im engen Sinn» auf.

- In der Realität können Verfahren manchmal fachlich eng zusammengehören (sogenannte connex-Verfahren). Verfahren werden in der Realität manchmal in mehrere Verfahren aufgeteilt oder zu einem Verfahren zusammengelegt. Wir gehen davon aus, dass diese Fälle für die Plattform unerheblich sind. Die Behörde, die allenfalls ein Verfahren aufteilt, stellt sicher, dass jedes der neuen Verfahren in genau einer Akte dokumentiert wird und dass soweit nötig, eine bestehende Akte in diese neue Akte aufgeteilt wird. Die Behörde, die allenfalls mehrere Verfahren zusammenführt, stellt sicher, dass das resultierende Verfahren in genau einer Akte dokumentiert wird und dass soweit nötig, die Akten aus den Verfahren in einer neuen Akte zusammengeführt werden.

Um Unklarheiten bezüglich des Scopes eines Verfahrens zu vermeiden, sehen wir davon ab, die Identifikatoren VerfahrensID und AktenID synonym zu verwenden. Die Plattform identifiziert Verfahren ausschliesslich im engen Sinne über die **eindeutige AktenID**[10].

Wie in Abschnitt 4.1.1.7 über Rollen im Verfahren beschrieben, führt und kennt die Plattform die Rollen der beteiligten Personen an einem Verfahren **nicht**. Hingegen muss die Plattform die Akten identifizieren können. Für das Projekt Justitia 4.0 insgesamt sind diese Akten in allen Ausprägungen (Papier- oder elektronische Akten) und über den ganzen Lebenszyklus relevant, vom Zeitpunkt, zu dem die Akte angelegt, über den Zeitraum, während dem sie bewirtschaftet, bis zum Zeitpunkt, an dem sie archiviert oder anderweitig geschlossen wird.

Die verfahrensleitende Behörde dokumentiert das Verfahren in einer Akte. Sie gewährt verfahrensbeteiligten Personen über die Plattform Einsicht in die elektronische Akte.

4.3.1 Einsehbare elektronische Akte

Die Behörde, die das Verfahren führt, bewirtschaftet auch die einsehbare elektronische Akte, indem sie Aktenstücke im elektronischen Rechtsverkehr an verfahrensbeteiligte Personen zustellt. Damit werden Aktenstücke gesiegelt und sind damit unveränderlich und enthalten keine (persönlichen) Kommentare und keine Versionen. Wir sagen, dass in der Zustellung die Aktenstücke zu 'einsehbaren' Aktenstücken werden, da der Empfänger diese über die Akteneinsicht konsultieren kann. Entsprechend können wir von der einsehbaren elektronischen Akte reden, welche die einsehbaren – d.h. mindestens einmal zugestellten – Aktenstücke enthält, sowie die Aktenstruktur und die minimal nötigen Daten des Aktendeckels.

[10] Das ist insofern erwähnenswert, als dass wir von 'verfahrensleitenden Behörden' reden, was aber aus Sicht der Plattform die 'aktenführende Behörde' ist.

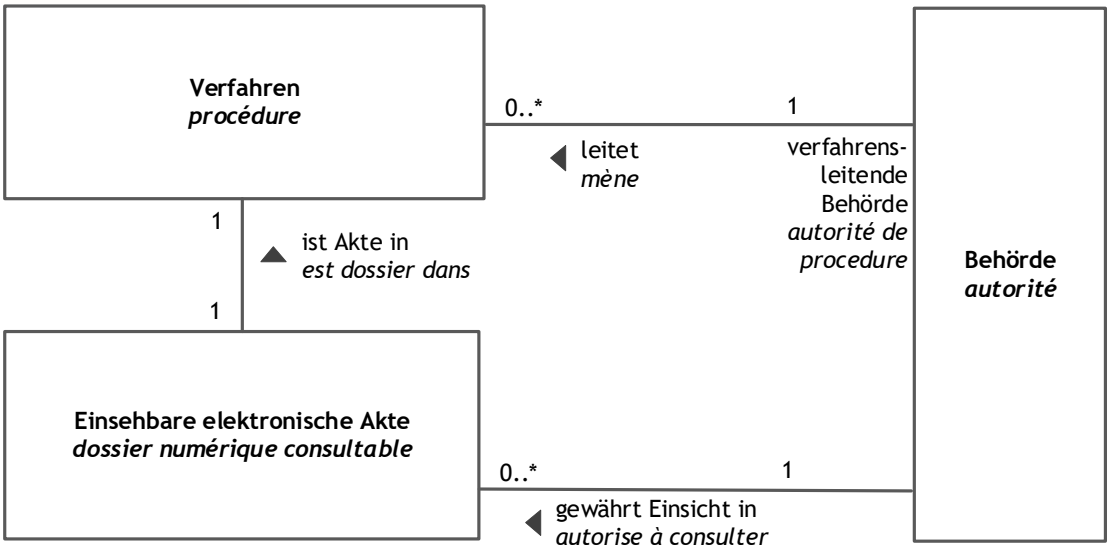


Abbildung 8: Einsehbare elektronische Akte – Bezug zum Verfahren und zur Behörde

Für die Plattform Justitia.Swiss und damit für die geplante Ausschreibung sind Akten nur in der Ausprägung der **einsehbaren elektronischen Akte** relevant.[11]

Eine Akte besteht aus Aktenstücken. Sie hat eine hierarchische Struktur analog zu einem Dateisystem, die Aktenstruktur, die in Rubriken (analog zu Verzeichnissen in einem Dateisystem) gegliedert ist. Jedes Aktenstück ist in genau einer Rubrik eingeordnet. Für eine Akte gibt es einen Aktendeckel sowie einen Datensatz, der die Akte und ihr Umfeld beschreibt. (Abbildung 9)

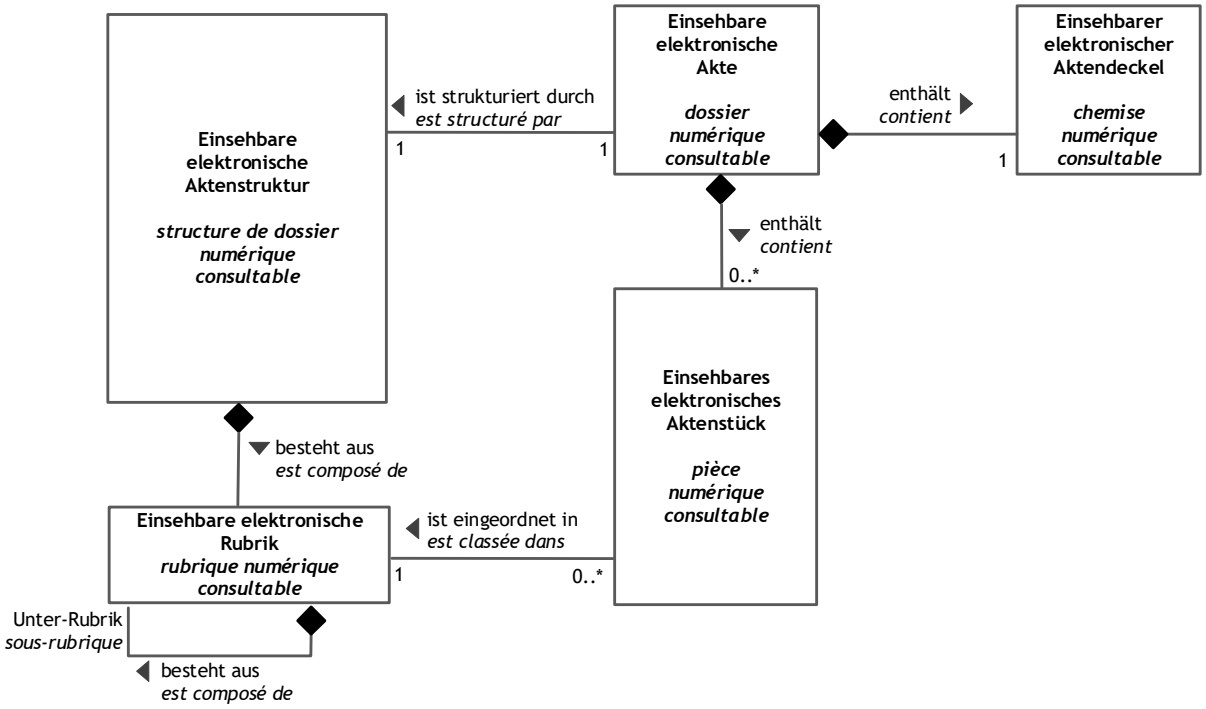


Abbildung 9: Einsehbare elektronische Akte – Konzeptionelles Modell

[11] Um die Konzepte der einsehbaren elektronischen Akte von anderen Modellen der CH-Justiz zu Akten abzugrenzen, verwenden wir im Modell durchgehend das Präfix «elektronisch einsehbar». Um den Text in diesem Abschnitt lesbarer zu machen, verwenden wir jedoch nur die Bezeichnungen ohne Präfix (Akte, Aktenstruktur, Aktenstück, Aktendeckel, Rubrik) – gemeint ist immer die einsehbare elektronische Akte, die einsehbare elektronische Aktenstruktur, etc.

4.3.2 Berechtigungen im Kontext eAE

Für die elektronische Akteneinsicht müssen Berechtigungen zur Einsicht vergeben werden. Eine Berechtigung zur Einsicht ist eine Beziehung zwischen einem Subjekt und einer Ressource, die durch einen Mitarbeiter einer verfahrensleitenden Behörde bewirtschaftet wird.

Elektronisch einsehbare Akten werden letztlich durch Benutzer (das heisst natürliche Personen oder Mitarbeiter) über die Plattform eingesehen, entweder über das Web-Portal oder über ein Justitia-Swiss.API. Die Behörden berechtigen jedoch nicht unmittelbar einen Benutzer zur Einsicht, sondern ein Profil (mit Zustelladresse), dem sie ein Einsichtsrecht gewähren. Ein Benutzer kann gewährtes Recht zur Einsicht auf diese Arten wahrnehmen:

1. Er ist Inhaber eines Profils einer natürlichen Person
2. Er gehört zu einer Organisation, welche dieses Profil innehat und hat (von der Organisation) die entsprechenden Rechte zum Lesen der Akten (siehe Abschnitt 4.1.2.1 über die Funktionen der Mitglieder einer Organisation)
3. Das Recht wurde ihm delegiert (siehe Abschnitt 4.4)

Berechtigungen zur Einsicht werden ausschliesslich auf einzelnen einsehbaren elektronischen Aktenstücken vergeben und geprüft. Dementsprechend werden keine vererbbaren Berechtigungen unterstützt:

- auf einsehbaren elektronischen Rubriken,
- auf ganzen einsehbaren elektronischen Akten oder
- auf einsehbaren elektronischen Aktendeckel.

Für einsehbare elektronische Rubriken, Akten und Aktendeckel gelten Sichtbarkeitsregeln basierend auf den 'elementaren' Berechtigungen auf die Aktenstücke.

Die Berechtigung zur Einsicht ist in drei Stufen gemäss der folgenden Tabelle gegliedert.

	Konsequenzen		
	Kann einsehbares elektronisches Aktenstück **im einsehbaren elektronischen Aktenverzeichnis** sehen?	Kann **Meta-Daten** des einsehbaren elektronischen Aktenstücks einsehen?	Kann **Inhalt** des einsehbaren elektronischen Aktenstücks einsehen?
Ausprägung			
keine Einsicht (Default)	nein	nein	nein
darf Meta-Daten lesen	ja	ja	nein
darf Inhalt lesen	ja	ja	ja

Tabelle 4: Berechtigungen zur Einsicht – Abstufungen

Ein Profil darf eine einsehbare elektronische Rubrik in einem Aktenverzeichnis sehen, wenn folgende Bedingung erfüllt ist:

Es gibt mindestens ein einsehbares elektronisches Aktenstück,

- welches in der Rubrik oder einer ihrer Unter-Rubriken eingeordnet ist
- und für das das Profil mindestens auf der Stufe «darf Meta-Daten lesen» zur Einsicht berechtigt ist.

Ein Profil darf den einsehbaren elektronischen Aktendeckel sehen, wenn folgende Bedingung erfüllt ist:

> Es gibt in der Akte mindestens ein einsehbares elektronisches Aktenstück, für das das Profil mindestens auf der Stufe «darf Meta-Daten lesen» zur Einsicht berechtigt ist.

4.3.3 Daten des Einsichtsrechts

Die Akte besteht aus Aktenstücken. Ein Aktenstück hat einen Inhalt und wird durch Metadaten-Attribute beschrieben. Die verfahrensleitende Justizbehörde vergibt das Einsichtsrecht (über ihr Profil) an das berechtige Subjekt, welches für die Plattform als Profil repräsentiert wird.

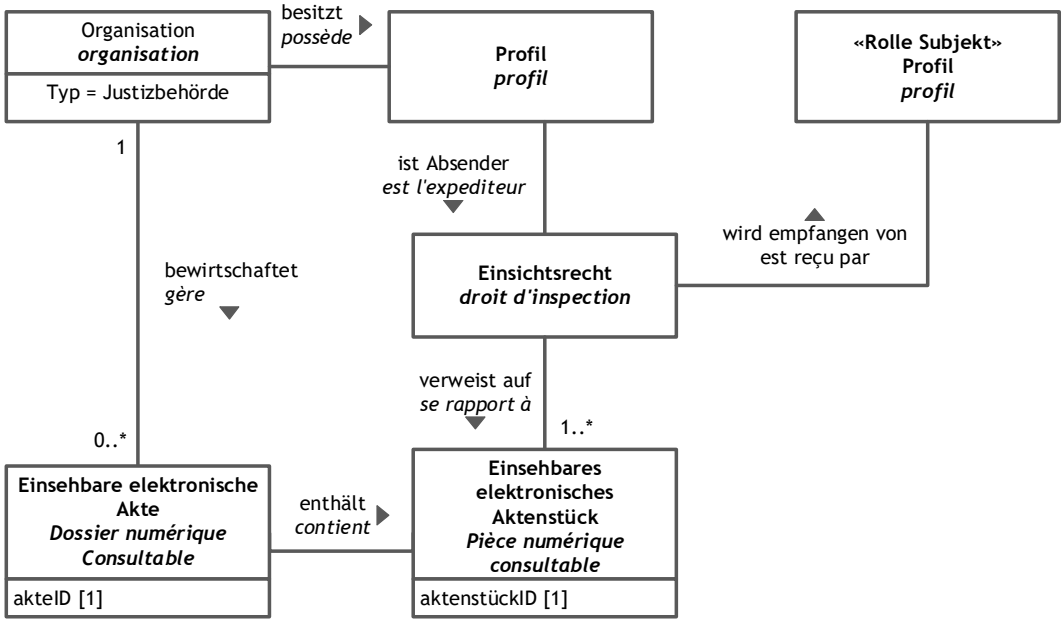


Abbildung 10: Einsichtsrecht auf Aktenstücken

- AktenstückID – ein innerhalb einer Akte eindeutiger Identifikator für ein Aktenstück[12]. Einzelheiten zum Format und zum Wertebereich werden erst nach der Ausschreibung festgelegt.
- Kombination AktenID, AktenstückID– lokal eindeutig innerhalb einer Justizbehörde

Möglicherweise wird jedem Aktenstück eine global eindeutige ID (eine GUID) zugeordnet: die `AktenstückUUID`. Einzelheiten dazu werden erst nach der Ausschreibung festgelegt.

Einige Kantone (z.B. der Kanton Genf) haben ein System für die Bearbeitung sämtlicher Verfahren seiner Behörden. Damit sind deren AktenID nicht nur innerhalb der Behörde, sondern in einem weiteren Scope eindeutig. Die Plattform darf sich jedoch nicht darauf verlassen.

Der Inhalt eines Aktenstücks ist eine Folge von *octets* (oder Bytes), kurz: ein *octet stream*. Er hat einen bestimmten Typ, den Media-Typ. Als Wertebereich werden die standardisierten *media types* der *Internet Assigend Numbers Authority* (IANA) verwendet, zum Beispiel

- `application/pdf` – ein PDF als Aktenstück
- `image/jpeg` – ein Bild in JPEG-Format als Aktenstück

Der Inhalt eines Aktenstücks ist unveränderlich. Er kann über die Plattform nur eingesehen und nicht bearbeitet werden.

[12] Im Modell Ehrenreich als Aktenstück-Kennzahl bezeichnet.

Neben dem Media-Typ verwendet die Plattform noch eine erweiterbare **Kategorie der Dateitypen**. Diese Kategorien werden aus folgenden Gründen vorgesehen:

- Die Kategorie bestimmt (beim Empfänger) ein anderes Routing. Beispielsweise sollen bestimmte strukturierte Dateien (vom text/xml) mit einem definierten Schema (z.B. eCH-0051) automatisiert verarbeitet werden. Über diese Kategorie kann die Art der Benachrichtigung gesteuert werden.
- Einige Medientypen sind zu grob-granular und müssen für unseren Kontext verfeinert werden. Beispielsweise sollen gesiegelte oder archivierbare PDF/A Dokumente anders behandelt werden.

Wir unterscheiden fachliche und technische Attribute (Metadaten) eines Aktenstücks:

- Fachliche Attribute beschreiben fachliche Eigenschaften des Aktenstücks. Typische Beispiele sind
  - Fachlicher Typ (Rechtsschrift, Beweismittel, etc.)
  - Fachliche Funktion im Verfahren (Anzeige, Anklage, Urteil, etc.)
  - Datum Veraktung
  - etc.

  Die Einzelheiten zu den fachlichen Attributen (Name, Bedeutung, Wertebereich, Optional/Zwingend etc.) werden erst nach der Ausschreibung festgelegt.

- **Technische Attribute**

  Technische Attribute beschreiben technische Eigenschaften des Aktenstücks. Typische Beispiele sind

  - Media-Typ und Kategorie
  - Grösse
  - Anzahl Seiten
  - etc.

  Die Einzelheiten zu den technischen Attributen (Name, Bedeutung, Wertebereich, optional/zwingend) werden erst nach der Ausschreibung festgelegt.

Verfahrensleitende Behörden stellen einsehbare elektronische Akten in einem DossierStore für die Einsicht bereit. Die Plattform wird über ein standardisiertes API auf einsehbare elektronische Akten im DossierStore zugreifen und damit den Benutzern der Plattform Einsicht in die Akten ermöglichen.

4.3.4 Einsehbares elektronisches Aktenverzeichnis

Eine Akte hat eine hierarchische Struktur, das Aktenverzeichnis. Benutzer können über die Plattform nicht nur Aktenstücke, sondern auch diese Struktur, das **Aktenverzeichnis**, einsehen.

Einzelheiten dazu, wie das Aktenverzeichnis Benutzern auf dem Portal dargestellt wird (UI-Design) und wie die Benutzer im Aktenverzeichnis navigieren können (Öffnen/Schliessen von Rubriken, suchen in Rubriken, etc.) werden erst nach der Ausschreibung festgelegt.

Für die Aktenstruktur werden auf der Plattform Sichtbarkeitsregeln für die Einsicht gelten. Ein Benutzer sieht auf dem Portal nur Rubriken im Aktenverzeichnis, für die er berechtigt ist. Das konzeptionelle Modell für die Sichtbarkeitsregeln ist später (Abschnitt 4.3.2) beschrieben.

Die Plattform wird das Aktenverzeichnis einer Akte über das Dossier-API aus einem DossierStore lesen können. Einzelheiten zu diesem API, namentlich zum Format und zum Schema eines Aktenverzeichnisses, das ein DossierStore an die Plattform übermittelt, werden erst nach der Ausschreibung festgelegt.

4.3.5 Einsehbarer elektronischer Aktendeckel

Eine Akte wird in einem bestimmten Kontext bereitgestellt. Sie wird durch eine Behörde in einem Verfahren bewirtschaftet, an dem Personen mit unterschiedlichen Rollen beteiligt sind Für jede Akte existiert mit dem **Aktendeckel** ein Datensatz mit Attributen über den Kontext, in dem die Akte bereitgestellt wird. Der Datensatz umfasst

- Attribute, die die Akte selbst beschreiben (Bezeichnung, AkteID, etc.)
- Attribute über das Verfahren, das in der Akte dokumentiert ist (Bezeichnung, VerfahrensID, etc.)
- Attribute über die Behörde, die die Akte bewirtschaftet und das Verfahren führt (Bezeichnung, BehördenID, etc.)
- Attribute über verfahrensbeteiligte Personen (Stammdaten zu natürlichen Personen und Organisationen und ihren Rollen im Verfahren)

Bestimmte Attribute des Aktendeckels werden aus den Systemen der Justizbehörden auf die Plattform repliziert, um verfahrensbeteiligten Personen den Kontext der Akte zu geben (Abbildung 11):

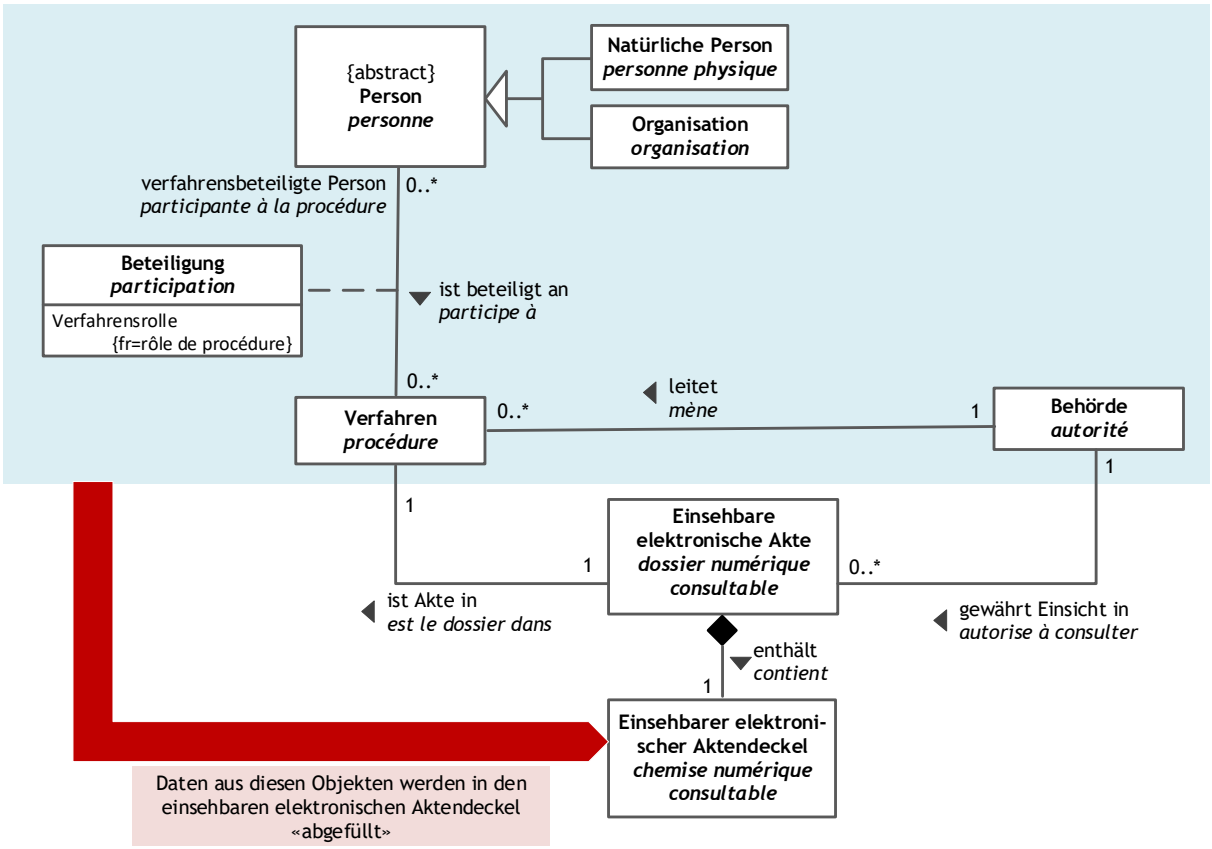


Abbildung 11: Einsehbarer elektronischer Aktendeckel – Beschreibung des Kontexts einer Akte

Der Aktendeckel ist ein strukturierter Datensatz, kein Dokument (keine PDF-Datei).

- Format – ein zeitgemässes, in der Praxis bewährtes Format wie XML, JSON oder YAML. Das Format wird im Projekt Justitia 4.0 definiert und muss durch die Behörden, die Akten zur Einsicht bereitstellen, eingehalten werden. Einzelheiten werden erst nach der Ausschreibung festgelegt.
- Struktur – gemäss einem spezifizierten, standardisierten Schema. Das Schema wird im Projekt Justitia 4.0 definiert, anschliessend durch die örK festgelegt und muss durch die Behörden, die

Akten zur Einsicht bereitstellen, eingehalten werden. Einzelheiten werden erst nach der Ausschreibung festgelegt.

Der Aktendeckel bleibt im Gegensatz zu Aktenstücken **editierbar**. Wenn sich der Kontext einer Akte ändert (andere verfahrensbeteiligte Personen, Status des Verfahrens, etc.) muss der Aktendeckel angepasst werden. Das Projekt Justitia 4.0 wird Vorgaben an die Aktualisierung des Aktendeckels formulieren. Behörden, die über die Plattform Akten zur Einsicht anbieten, werden diese Vorgaben einhalten. Einzelheiten dazu werden erst nach der Ausschreibung festgelegt.

Folgende Abbildung illustriert an einem Beispiel die Replikation der Daten eines Verfahrens (hier Trader: Verfahren) auf den einsehbaren elektronischen Aktendeckel.

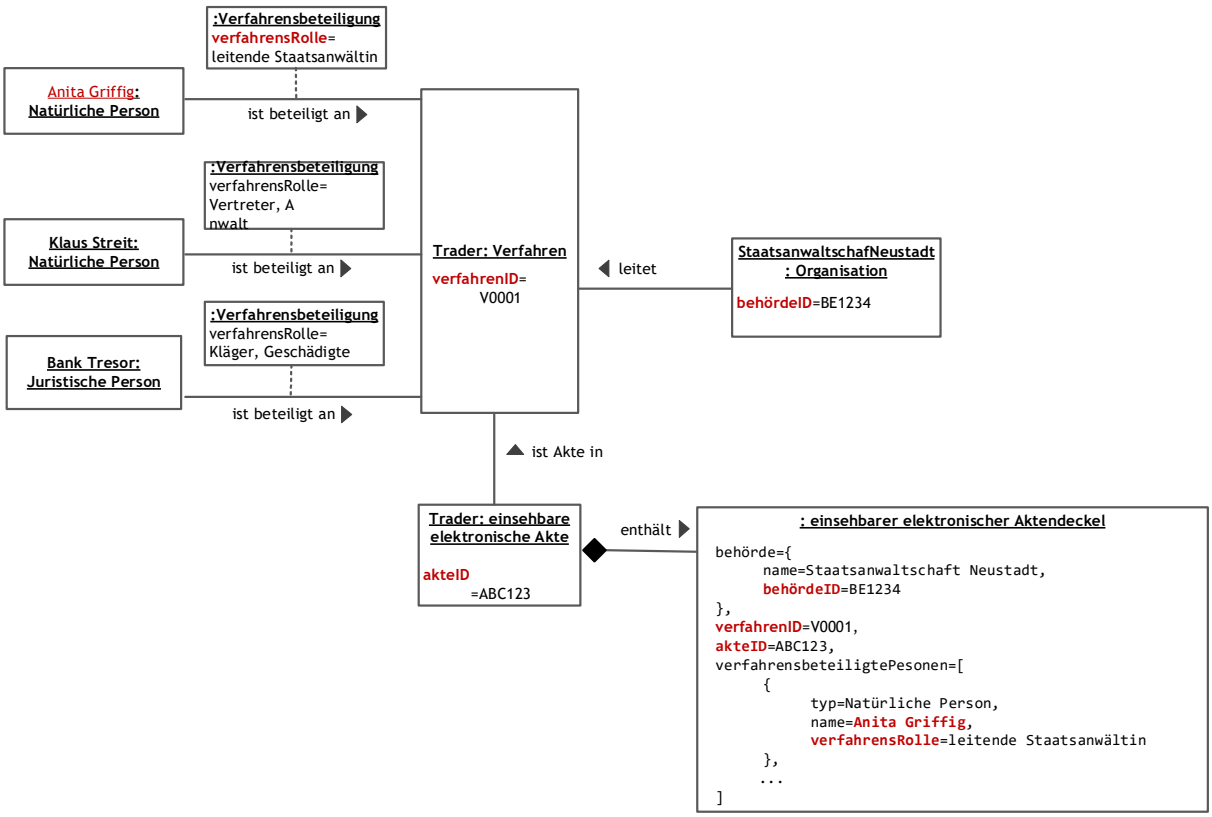


Abbildung 12: Einsehbarer elektronischer Aktendeckel – Beispiel

4.3.6 Akteneinsicht entziehen

Das Recht zur Akteneinsicht erlischt, wenn (1) die Akten geschlossen werden, oder (2), wenn die Gültigkeit der Berechtigung abläuft. Der erste Fall tritt ein, wenn die verfahrensleitende Behörde das Verfahren schliesst und damit der Plattform mitteilt, dass die Zustellungen und damit Akteneinsichten für dieses Verfahren nicht mehr gültig sind.

Für den zweiten Fall ist auf dem Einsichtsrecht ein Gültigkeitsbereich zu führen (siehe Abschnitt 4.4.2 über die Zustellung).

Es kann auch Fälle geben, in denen eine Akteneinsicht (welche ursprünglich) bis zum Ende des Verfahrens gegeben wurde, entzogen werden muss. Dies kann auf einem menschlichen Fehler beruhen, oder durch einen Anwaltswechsel bedingt sein.

Für diesen Fall muss es möglich sein, einem Anwalt noch ‘ein letztes Mal’ Zugriff auf das Aktenstück zu geben, so dass dieser seinen Fall abschliessen kann. Details dazu werden erst im Design und der Benutzerführung entworfen.

4.4 Rechtsverkehr

Im Rahmen des elektronischen Rechtsverkehrs (ERV) tauschen verfahrensleitende Justizbehörden und Parteien **Übermittlungen**[13] aus. Die beiden Grundtransaktionen sind die Eingabe und die Zustellung.

- Eine Übermittlung im eingehenden ERV (von Parteien an verfahrensleitende Justizbehörden) bezeichnet man als **Eingabe**.
- Eine Übermittlung im ausgehenden ERV (von einer verfahrensleitenden Justizbehörde an eine Partei) wird als **Zustellung** bezeichnet. Bei einer Zustellung kann die verfahrensleitende Justizbehörde eine Frist setzen.

Übermittlungen können auf einer konzeptionellen und/oder einer physischen Ebene beschrieben und modelliert werden:

- Auf der **konzeptionellen Ebene** wird modelliert, welche Arten von Meldungen vorkommen und aus welchen fachlichen Teilen sie bestehen.
- Auf der **physischen Ebene** wird beschrieben und modelliert, in welchem Format, in welcher Struktur, in welchen Arten von «Container» (zum Beispiel eine ZIP-Datei) Meldungen digital über Netzwerke transportiert oder auf der Plattform gehalten werden.

Das vorliegende Dokument ist auf die konzeptionelle Ebene beschränkt. Die physische Ebene bleibt bis zur Ausschreibung offen. Anbieter werden möglicherweise auf der physischen Ebene Lösungen basierend auf eCH-Standards (zum Beispiel [eCH-0039] oder [eCH-0058]) oder basierend auf Internet-Standards rund um E-Mail ([RFC2045] und Verwandte) vorschlagen. Die Einzelheiten werden erst nach der Ausschreibung zusammen mit dem Anbieter festgelegt.

4.4.1 Eingabe

Eine Eingabe ist eine elektronische und rechtsgültige Übermittlung von Rechtsschriften (Dokumente und weitere Dateien) durch eine verfahrensbeteiligte Person/Organisation an eine verfahrensleitende Behörde. Das grobe Interaktionsmuster der Eingabe ist in Abbildung 13 dargestellt.

[13] In sprachlicher Anlehnung an BEKJ-VE Art. 21 reden wir von Übermittlung anstelle der gebräuchlicheren Meldung.

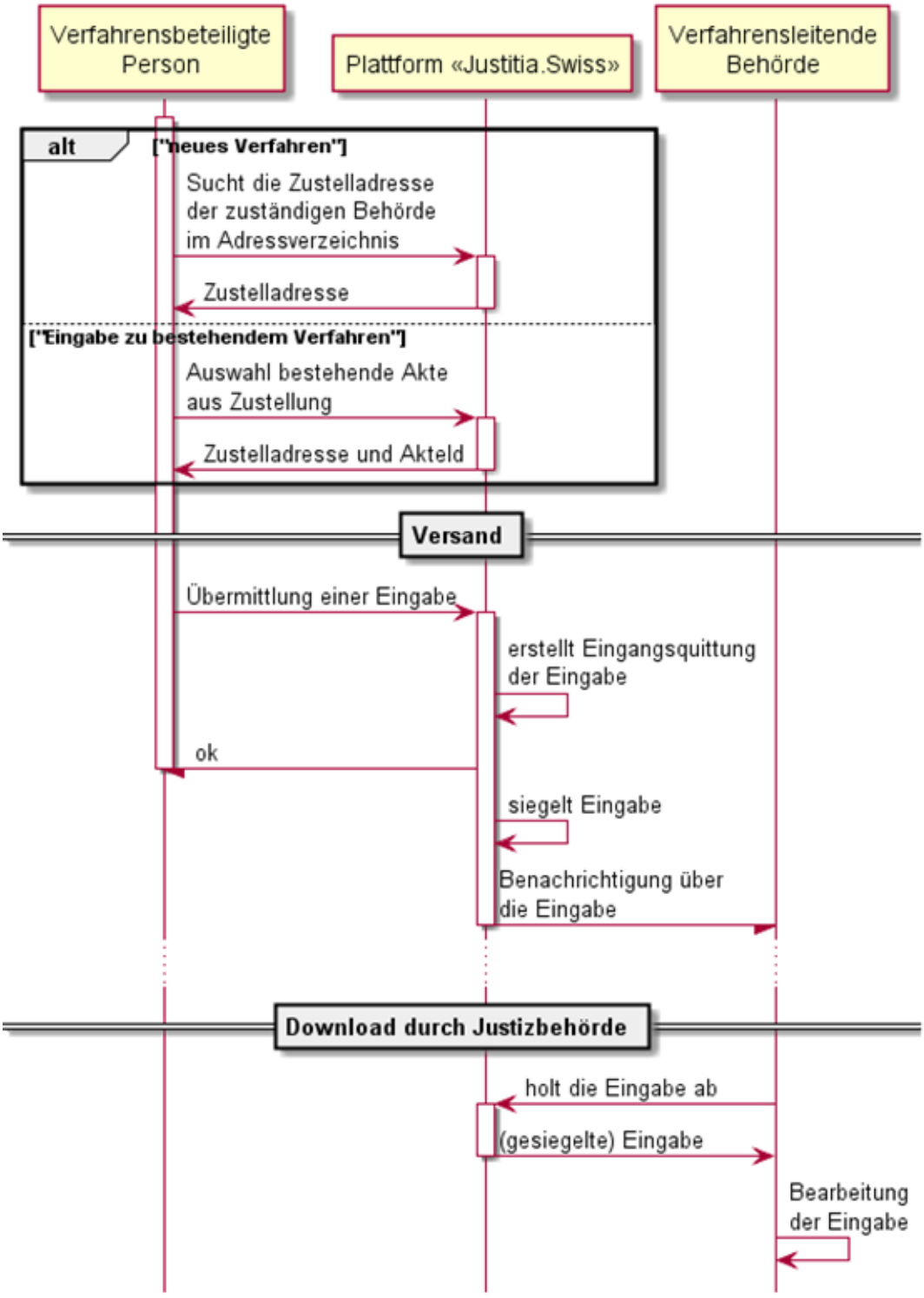


Abbildung 13: Grundtransaktion im eingehenden ERV – die Eingabe

Erläuterung:

- Eine verfahrensbeteiligte Person sucht (im öffentlichen Adressverzeichnis) die gewünschte Justizbehörde als Empfänger oder macht eine Eingabe basierend auf einer bestehenden Akteneinsicht, resp. aufgrund einer Zustellung.
- Sie übermittelt an die gefundene Zustelladresse rechtsverbindlich eine Eingabe.
- Die Plattform erstellt die Eingangsquittung.

- Die Plattform siegelt die Dokumente der Eingaben und legt diese im Postfach der empfangenden Behörde (als eingehende Meldung) ab.
- Die Plattform benachrichtigt die verfahrensleitende Behörde gemäss ihren Präferenzen im Profil über den Eingang der Eingaben. Ob die Eingaben basierend auf der Benachrichtigung der Plattform (Trigger) oder in regelmässigen Abständen (Pull-Verfahren) erfolgt, wird zu einem späteren Zeitpunkt definiert werden.
- Die Behörde bearbeitet die Eingabe mit ihren Mitarbeitenden in ihren Prozessen und unterstützt durch ihre IT-Landschaft. Die Plattform ist daran nicht beteiligt.

Der Lebenszyklus einer Eingabe ist anhand Abbildung 14 dargestellt. Beachte, dass die Eingabe über das Web-Portal das schrittweise Hinzufügen (und wieder Löschen) von Beilagen unterstützt. Im Sequenzdiagramm ist dieses Mutieren nicht dargestellt. Wurde eine Eingabe jedoch einmal versandt, kann sie weder durch den Sender noch durch den Empfänger mutiert werden.

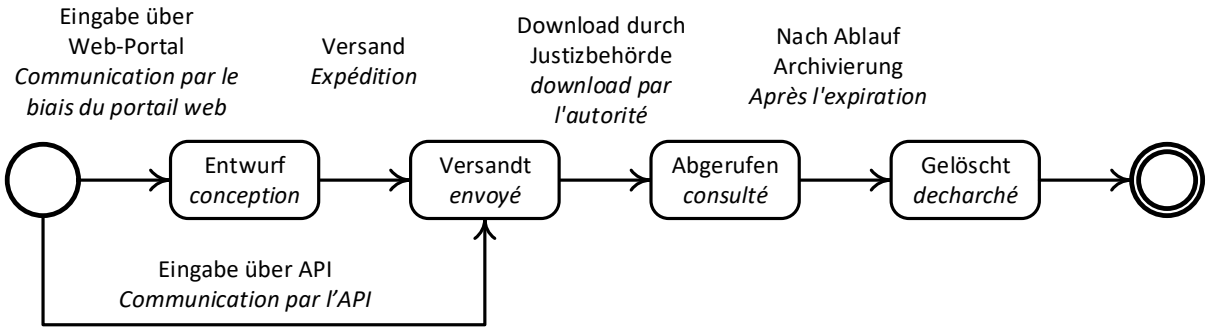


Abbildung 14: Zustandsdiagramm Eingabe

Vor dem Versenden werden diverse Prüfungen auf den übermittelten Dateien gemacht und diese mit Metadaten angereichert. Dabei spielen auch der Medientyp und die Kategorie (siehe auch Kapitel 4.3.3) eine Rolle. Sinn und Zweck dieser Validierungen können sein:

- Dateien werden auf Viren o.ä. geprüft und in einen Quarantänebereich verschoben.
- Verbesserung der Usability durch Hinweis auf PDF Versionen, bereits signierte PDF Dateien o.ä.

Mit dem Versenden erstellt die Plattform eine Eingangsquittung (sofern vom Sender gewünscht), siegelt die Beilagen und benachrichtigt den Empfänger.

Im Zustand 'Abgerufen' wurde die Eingabe vom Empfänger (der verfahrensleitenden Behörde) heruntergeladen.

Nach Ablauf einer definierbaren Zeitspanne (ca. 30 Tagen) wird die Eingabe auf der Plattform definitiv gelöscht.

Die Informationsobjekte einer Eingabe sind in Abbildung 15 visualisiert.

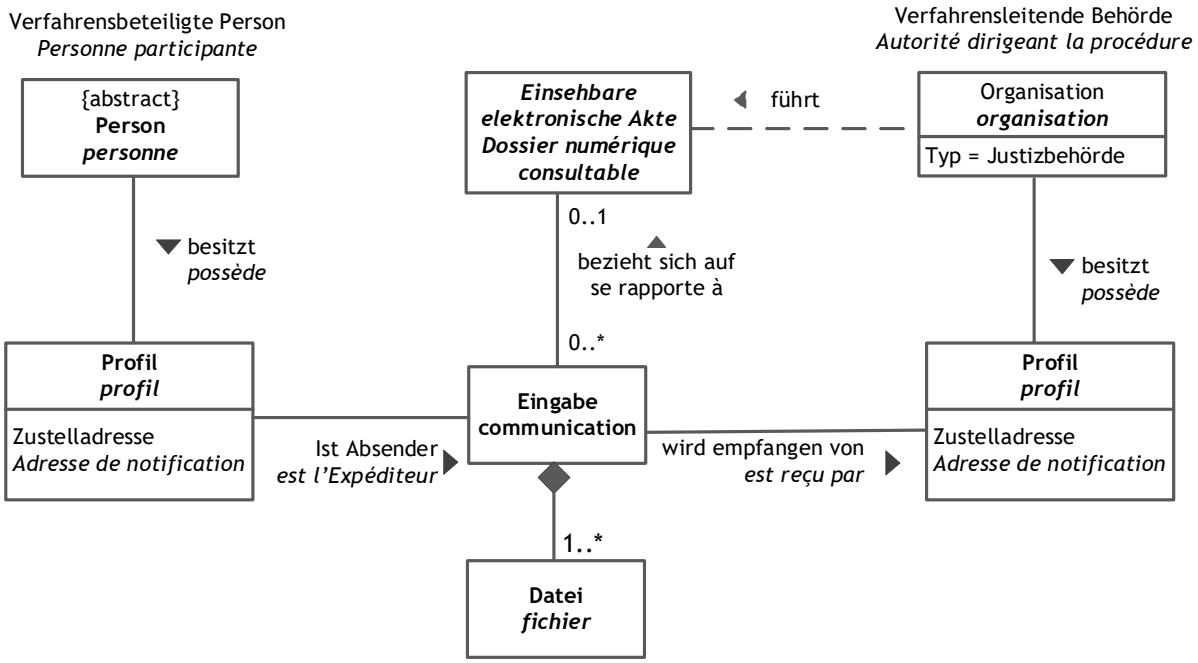


Abbildung 15: Informationsobjekte einer Eingabe

Eine verfahrensbeteiligte Person macht eine Eingabe an eine verfahrensleitende Behörde. Diese Eingabe kann sich auf ein laufendes Verfahren dieser Behörde beziehen. Die Plattform prüft dies aber nicht, sondern transportiert einfach die akteId[14] der einsehbaren Akte als Teil der Übermittlung vom Absender zum Empfänger.

Die Eingabe besteht aus verschiedenen Dateien in diversen Formaten als Attachments, welche vom Absender übermittelt werden. Während dem Versand der Eingabe wird die Plattform weitere Dateien logisch mit dieser Eingabe verknüpfen:

- Falls ein Attachment (z.B. eine Access Datenbank) gesiegelt werden muss, wird die Plattform einen Hashwert als 'Siegel' als zusätzliche Datei hinzufügen. Mit diesem Hashwert kann später die Integrität des Dokuments nachgewiesen werden.
- Falls die Plattform Quittungen erstellt, werden auch diese mit der Eingabe verknüpft und können daraus erneut empfangen werden.[15]

Die Metadaten der Dateien der Eingabe entsprechen den Metadaten der einsehbaren Aktenstücke (siehe Abschnitt 4.3.3). Informationsattribute der Eingabe, wie Dringlichkeit werden im Design festgelegt.

4.4.2 Zustellung

In einer Zustellung übermittelt die Justizbehörde elektronisch und rechtsgültig einem Verfahrensbeteiligten ein oder mehrere Aktenstücke. Aktenstücke werden jedoch nicht (im Unterschied zur Eingabe) mit der Zustellung übermittelt, sondern die Zustellung basiert auf dem Einsichtsrecht. Gegenüber der reinen Akteneinsicht enthält die Zustellung Funktionalitäten für Quittungen und Fristen. Das eigentliche Lesen oder Herunterladen eines Dokuments entspricht der Wahrnehmung des Einsichtsrechts.

---

[14] Siehe Kapitel 4.3 über die Verwendung der akteId als Identifikator des Verfahrens im engen Sinn.

[15] Vgl. BEKJ-VE Art. 21 Ziffer 8 wird verlangt, dass Quittungen sowohl vom Absender als auch vom Empfänger heruntergeladen werden können. In diesem Sinn fügt die Plattform der Meldung eine Quittung hinzu. Heute erstellt beispielsweise die Kanzlei des Bundesgerichts bei Eingaben selber eine Eingabequittung mit Zustellzeitpunkt und einer Auflistung der eingegebenen Dokumente und veraktet diese Quittung. Neu könnte das BGer diese Quittung als Teil der Eingabe 'herunterladen'.

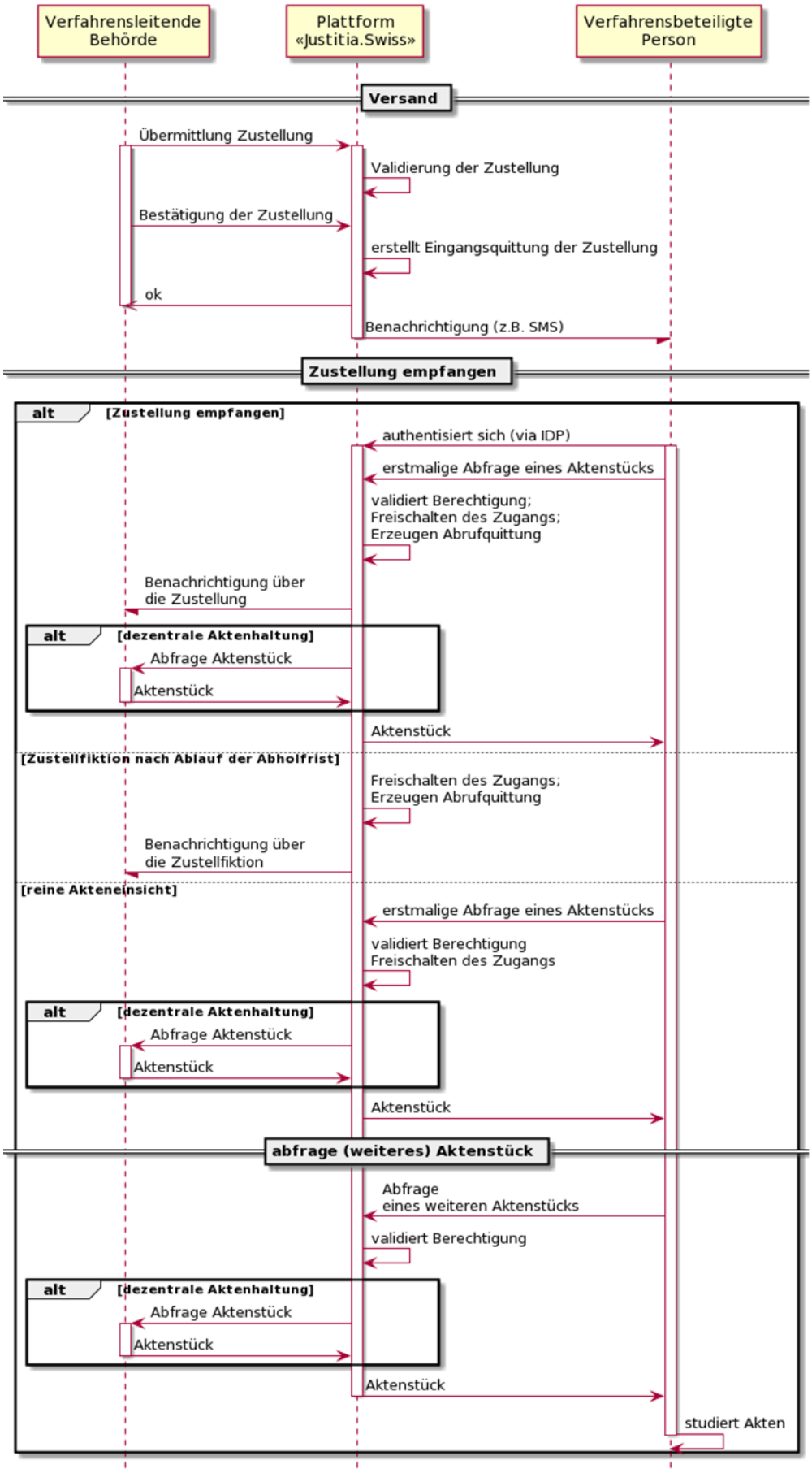


Abbildung 16: Grundtransaktion im ausgehenden ERV – die Zustellung

In Abbildung 16 manifestiert sich der Unterschied einzig im Schritt 'Zustellung empfangen': Dieser Schritt ist eigentlich nur für Zustellungen relevant, da die sendende Justizbehörde über die erfolgreiche Zustellung (nach erstmaligem Lesen, resp. nach 7 Tagen) benachrichtigt wird. Wir verwenden dies jedoch auch für reine Akteneinsichten, damit das Ereignis des erstmaligen Lesens für den Empfänger prägnant im Audit Trail (Kapitel 6.3 über Quittungen) sichtbar ist.

Erläuterung:

- Die verfahrensleitende Behörde **versendet** eine Zustellung. In der Validierung der Zustellung zeigt die Plattform der Behörde, welche Profile (und damit welche Empfänger) damit Einsicht in welche Aktenstücke erhalten. Mit der formellen Bestätigung wird die Zustellung ausgelöst.
- Die Plattform benachrichtigt den Empfänger (gemäss seinen Einstellungen im Profil)
- und erstellt (falls nötig) eine Eingangsquittung. Mit dieser Quittung kann die Behörde nachweisen, dass sie bestimmte Dokumente zugestellt hat.
- Zum **Empfangen der Zustellung, resp. dem Einsichtsrecht** gibt es 3 Varianten:

  1) Die Zustellung wird 'aktiviert', wenn die verfahrensbeteiligte Person ein Aktenstück daraus öffnet oder herunterlädt.

     - Die Plattform erstellt eine Abrufquittung, mit der der Beginn der Frist festgelegt ist
     - Und holt das entsprechende Aktenstück (entweder vom zentralen Aktenspeicher oder dezentral aus der IT der verfahrensleitenden Behörde – siehe Kapitel 6.2).

  2) Falls die beteiligte Person die Zustellung nicht innerhalb der Abholfrist abholt, resp. öffnet, gilt nach einer definierten Anzahl Tage (normalerweise 7 Tage plus kantonale Feiertage) die Zustellfiktion. Das heisst, die Zustellung gilt als erfolgt.

     - Die verfahrensleitende Behörde wird über das Nichtabrufen der Zustellung benachrichtigt.
     - Die Plattform erstellt eine entsprechende Quittung, mit der der Beginn der Frist festgelegt ist.

  3) Falls es sich um die reine Übermittlung des Einsichtsrechts handelt, wird die zustellende Behörde entsprechend auch keine Abrufquittung erhalten.

     - Beim erstmaligen Anfordern eines Aktenstücks wird lediglich für den Verfahrensbeteiligten der Zeitpunkt auditiert und die Zustellung aktiviert. Damit kann der Verfahrensbeteiligte nachvollziehen, wann er die Zustellung zur Kenntnis das erste Mal gelesen hat und er seine Frist für eine mögliche Replik wahrnehmen muss.

- Bei **erneuter Abfrage** des gleichen Aktenstücks oder anderer Aktenstücke dieser Zustellung wird keine weitere Abrufquittung erzeugt. Es erfolgt lediglich der Zugriff (wieder zentral oder dezentral) auf das Aktenstück.

Der Lebenszyklus einer Zustellung ist in Abbildung 17 dargestellt. Erfassungen über das Web-Portal erfordern einen Entwurfsmodus, so dass der Mitarbeiter der verfahrensleitenden Behörde die Zustellung der Aktenstücke prüfen kann. Bei einer Zustellung über das API ist dieser Zustand nicht nötig.

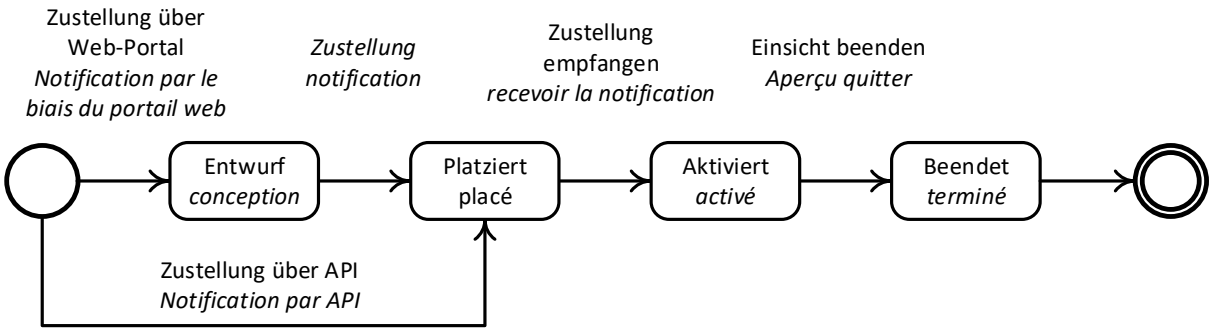


Abbildung 17: Zustandsdiagramm Zustellung

Während der Zustellung erstellt die Plattform eine Eingangsquittung und benachrichtigt den Empfänger über die Zustellung.

Im Schritt 'Zustellung empfangen' öffnet der Empfänger das erste Mal die Zustellung oder er lässt die Abholfrist verstreichen. Jetzt wird die Abrufquittung erstellt, damit die verfahrensleitende Behörde den Start der Frist festhalten kann. Im Zustand «Aktiviert» können die berechtigten Aktenstücke eingesehen werden. Mit der Zustellung teilt die verfahrensleitende Behörde mit, ob eine Frist gesetzt werden soll oder nicht. Eine Zustellung ohne Frist überspringt den Schritt 'Zustellung empfangen', d.h. die Zustellung ist gleich nach Versand aktiviert.[16]

Die Akteneinsicht wird beendet, wenn das Verfahren abgeschlossen ist, wenn die Gültigkeit der Einsicht erlischt oder wenn durch einen Aufruf der verfahrensleitenden Behörde die Einsicht entzogen wird.

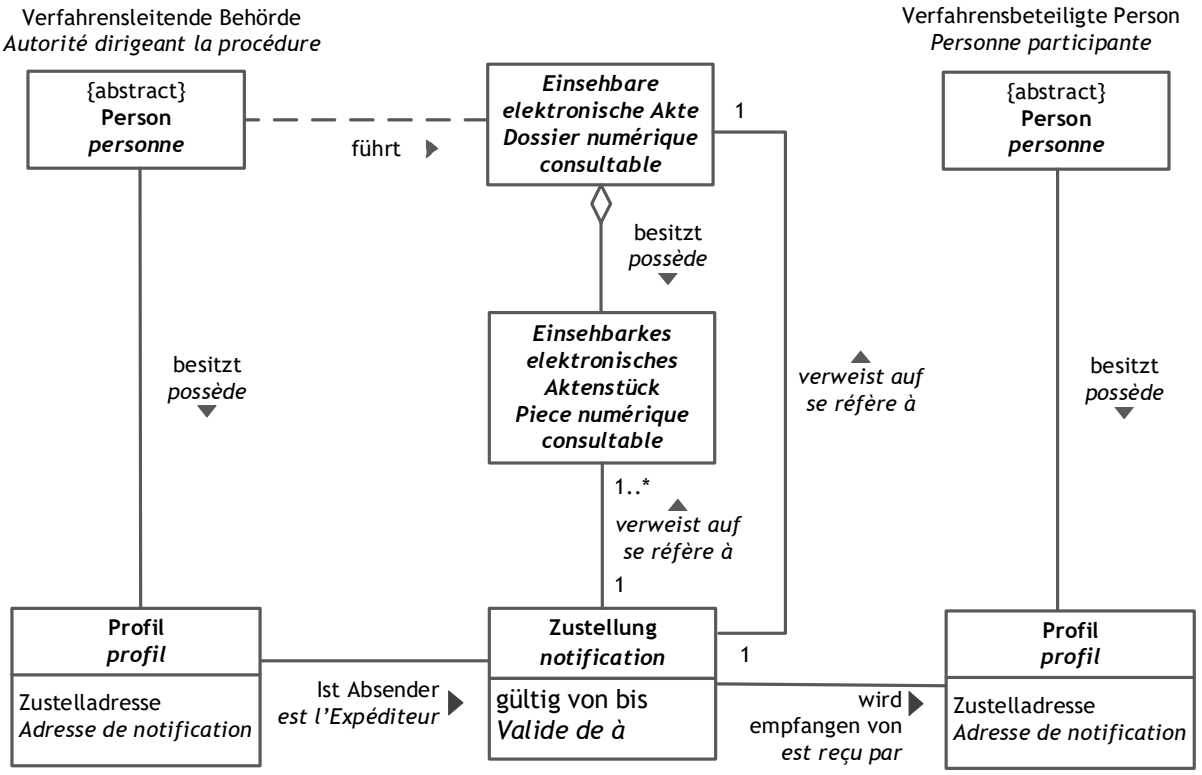


Abbildung 18: Informationselemente einer Zustellung

[16] Das heisst, es können auch Personen das Aktenstück lesen, welche **kein** Recht zum erstmaligen Öffnen der Zustellung haben. Dies ist jedoch unkritisch, da ja die Zustellung ohne Frist (und damit ohne Rechtsverbindlichkeit) erfolgt.

In Abbildung 18 sind die Informationselemente einer Zustellung visualisiert. Die verfahrensleitende Behörde macht eine Zustellung an die verfahrensbeteiligte Person. Die Zustellung enthält aber – im Gegensatz zu der Eingabe – keine Attachments der aufgebenden Behörde. Die zu übermittelnden Dokumente werden als Referenzen auf einsehbare elektronische Aktenstücke mitgegeben (siehe 6.5 über Berechtigungen und Aktenstückadressen). Hingegen können– diesmal analog zur Eingabe – die nötigen Quittungen als Attachment zur Zustellung verstanden werden. Da die Quittungen jedoch im strengen Sinn keine eigenständigen Informationsobjekte, sondern lediglich zeitbezogene Sichten auf den Zustand der Zustellung sind, haben wir sie weggelassen.

4.4.3 Zustellung ohne ein Verfahren zu eröffnen

Eine Zustellung erfolgt normalerweise aus einem Verfahren, welches in einer Akte dokumentiert wird. Damit enthält die Zustellung (genauer das Einsichtsrecht) auch die akteId für die Darstellung der Aktenhierarchie oder um auf die Zustellung mit einer Eingabe zu diesem Verfahren zu reagieren.

In Ausnahmefällen verzichten jedoch die Justizbehörden auf das Eröffnen eines Verfahrens und antworten dem Absender direkt. Beim Bundesgericht hat sich dazu der Begriff «Bürgerbrief» etabliert. Erfolgt diese Kommunikation über die Plattform, verwenden wir dazu auch die Mechanismen der Zustellung, jedoch ohne zugehörige akteId. Entsprechend können solche Dokumente durch den Empfänger nicht als Teil einer Akte eingesehen werden, und die 'Akteneinsicht' kann nicht delegiert werden.

4.5 Delegation

Das Gesetz (VE-BEKJ, Art. 24) fordert in der Gruppenverwaltung die Möglichkeit, Berechtigungen zu Akteneinsicht und zum Rechtsverkehr zu delegieren.

4.5.1 Delegation als Informationsobjekt

Die Plattform unterstützt **Delegation** von Berechtigungen. Unter Delegation verstehen wir, dass ein Benutzer A Berechtigungen, die er wahrnehmen kann, an einen anderen Benutzer B delegieren kann, so dass Benutzer B diese Berechtigungen ebenfalls wahrnehmen kann.

Zwei typische Anwendungsfälle:

a. Ein Benutzer als Anwalt A delegiert an seinen Mitarbeiter M seine Berechtigung zur Einsicht in die Akte A.

b. Ein Benutzer als Anwalt A delegiert an seinen Mitarbeiter M seine Berechtigung zur Einsicht in alle Zustellungen oder Einsichtsrecht aus dem Verfahren V.

Eine Delegation wird auf der Plattform durch einen Benutzer angelegt oder gelöscht. Sie besteht zwischen zwei Profilen – zwischen dem delegierenden und dem delegierten Profil (Abbildung 19). Die Plattform unterstützt verschiedene Ausprägungen von Delegationen, damit Benutzer bestimmte Ausprägungen von Berechtigungen delegieren können. Wir beschreiben die Ausprägungen der Delegationen in den folgenden Abschnitten.

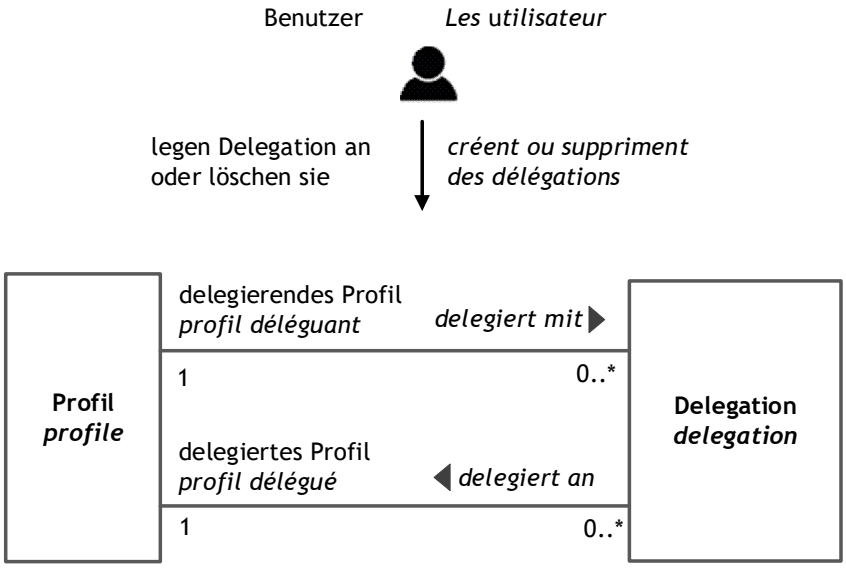


Abbildung 19: Konzept der Delegation

Die Lesbarkeit des Diagramms ist für eine Instanz verbessert:

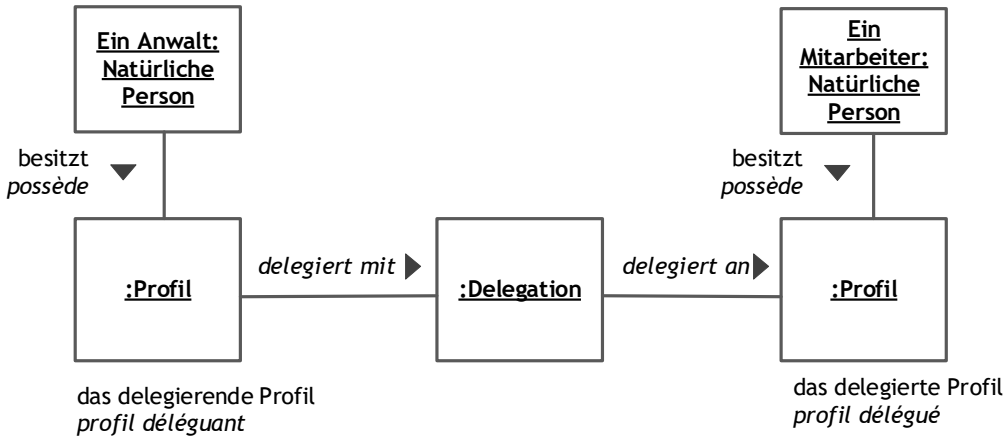


Abbildung 20: Beispiel einer Delegation

Die Delegation kann auch für nur eine Akte (ein Verfahren im engeren Sinn, siehe Kapitel 4.3) erfolgen.

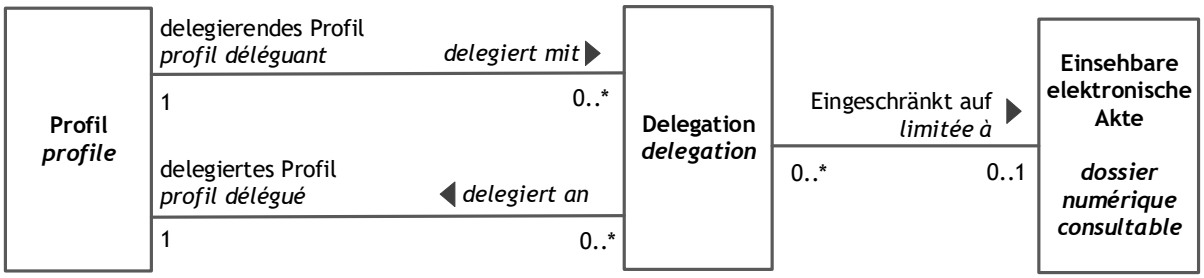


Abbildung 21: Delegation zur Einsicht in eine Akte

Ein konkretes Beispiel ist in Abbildung 22 dargestellt. Eine Behörde hat Sara Dubois zur Einsicht in die Akte A001 berechtigt. Sie delegiert diese Berechtigung an ein Profil von Jean Michel weiter. Jean Michel ist damit im Kontext dieses Profils soweit berechtigt, die Akte A0001 einzusehen, wie Sara Dubois dazu berechtigt ist. Wenn Sara Dubois ein Aktenstück in der Akte einsehen kann, kann auch Jean Michel das Aktenstück einsehen.

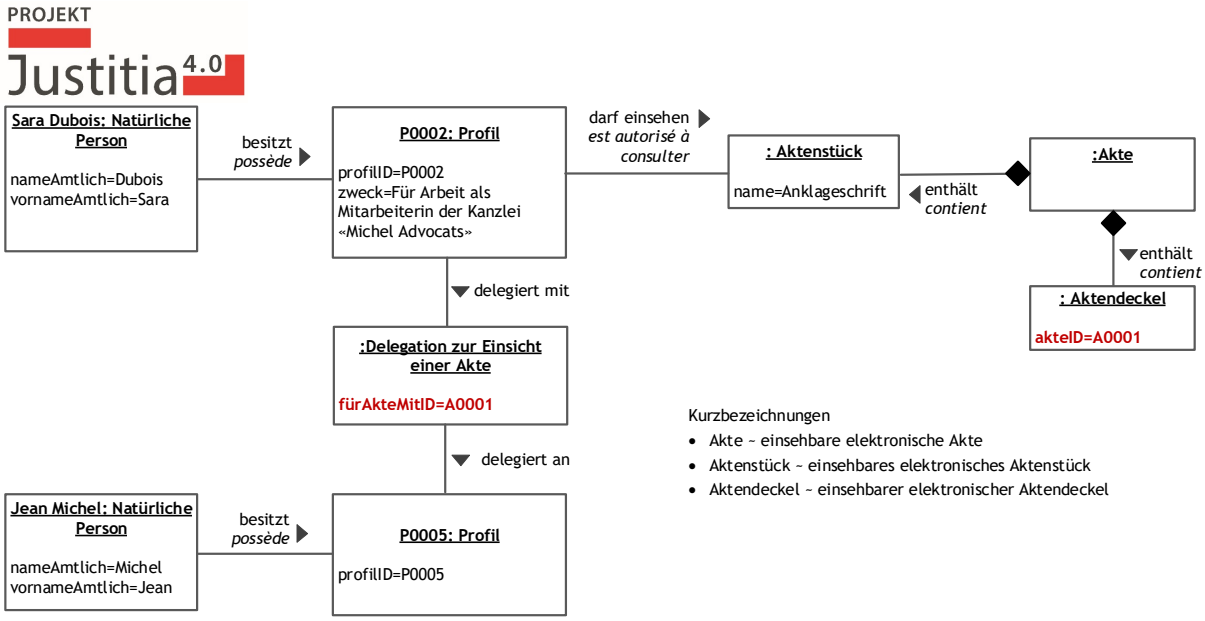


Abbildung 22: Delegation zur Einsicht in eine Akte – Konkretes Beispiel

Beachte, dass die Berechtigung zur Akteneinsicht von der verfahrensleitenden Behörde (mit der Zustellung des Aktenstücks) an Sara Dubois gegeben wurde. Sara Dubois ihrerseits delegiert diese Berechtigung weiter. Entsprechend nimmt Jean Michel Akteneinsicht im Namen von Sara Dubois.

Hinweis: die Relation 'darf einsehen' vom Profil zum Aktenstück basiert auf einer Zustellung (siehe Kapitel 4.4.2).

4.5.2 Arten von Delegation

Folgende Auflistung illustriert die verschiedenen Möglichkeiten der Delegation:

1. Blanko-Eingabe: Möglichkeit einer Eingabe unabhängig vom Verfahren.
2. Spezifische-Eingabe: Möglichkeit einer Eingabe nur im Kontext eines Verfahrens, resp. einer AkteID.
3. Blanko-Zustellung: Möglichkeit eine Zustellung zu empfangen – mit Frist Auslösung.
4. Spezifische-Zustellung: Möglichkeit einer Zustellung zu einem spezifischen Verfahren zu empfangen.
5. Blanko-Einsicht: Möglichkeit Akten einzusehen unabhängig vom Verfahren.
6. Spezifische-Einsicht: Möglichkeit Akten eines Verfahrens einzusehen.
7. Aktenstücke Einsicht: Möglichkeit nur ein spezifisches Aktenstück einzusehen.
8. Kommentare-Einsicht: Möglichkeit Tags und Vermerke zu sehen und oder anzubringen (siehe Kapitel 6.8).
9. Substitution: Möglichkeit, dass das delegierte Profil selbst seine Berechtigungen weiter delegieren kann.

Die genauen Details der Delegation werden erst nach der Ausschreibung in einem iterativen Vorgehen festgelegt. Es gilt hier, den für die Benutzer der Plattform sinnvollen Mittelweg zwischen maximaler Flexibilität und einer einfach, intuitiv und verständlich zu bedienender Plattform zu finden (siehe Leitsatz 1).

5 Interaktionen zwischen Behörden in Justizverfahren

In diesem Kapitel werden die verschiedenen Muster für den Rechtsverkehr zwischen verfahrensleitenden Behörden beschrieben. Durch Interaktionen und wechselseitigen 'Aktenbeizug' entstehen bei verschiedenen Behörden Akten zum selben Sachverhalt. [17]

[17] Siehe auch Kapitel 4.3 bei Akteneinsicht über Verfahren im weiteren und engeren Sinn.

Die Interaktionsmuster sollen aufzeigen, was die Bedeutung von *Akten zwischen den Behörden verschieben* ist und sollen Hinweise über benötigte Metadaten bei Eingaben und Zustellungen sein, damit über die Plattform weitergehende Automatisierung mit verfahrensbeteiligten Behörden möglich wird, ohne das Prinzip 4 zu verletzten, welches lediglich Eingabe, Zustellung und Akteneinsicht fordert, jedoch keine gemeinsame Bearbeitung von über mehrere Behörden 'verteilten' Akten zum selben Verfahren oder Geschäft:

- Bei einer **Eingabe** liefert der eingebende Akteur Dokumente mit. Die zuständige Justizbehörde veraktet die eingegangenen Dokumente.
- Bei einer **Zustellung oder Akteneinsicht**, gibt die einsichtsgebende Behörde der einsichtsnehmende Behörde Akteneinsicht. Die einsichtsnehmende Behörde kopiert dann die benötigten Aktenstücke in ihre eigene Akte.

Damit ist das Lifecycle Management der Aktenstücke und Akten immer klar einer Behörde zugeordnet, und die Datenverantwortung definiert.[18]

5.1 Eingabe einer Behörde bei einer verfahrensleitenden Justizbehörde

In diesem Muster stellt eine Justizbehörde eine Anfrage bei einer anderen Justizbehörde und erwarten eine Antwort in Form eines Entscheides.

Als Anfrage kann man sich z.B. die ein Staatsanwaltschaft vorstellen, welche im Rahmen einer Untersuchung beim Zwangsmassnahmengericht einen Entscheid zur Anordnung einer Untersuchungshaft braucht. Beide beteiligten Behörden, die Staatsanwaltschaft und das ZMG, sind in diesem Fall verfahrensleitende Behörden und dokumentieren ihr Verfahren in ihrer jeweiligen Akte. Dieses Beispiel ist in Abbildung 23 visualisiert.

Ein anderes Beispiel ist die Anklage einer Staatsanwaltschaft beim erstinstanzlichen Gericht. Auch hier stellt die Staatsanwaltschaft eine Anfrage und erwartet einen Entscheid. Beachte, dass in diesen beiden Fällen die Zeitdauer zwischen der Anfrage und der Antwort keine Rolle spielt.

Die Plattform unterstützt die Kommunikation zwischen den beiden Behörden wie folgt:

1. Die anfragende Behörde übermittelt ihre Anfrage als **Eingabe** (siehe Abschnitt 4.4.1) Weil es sich um eine Eingabe handelt, liefert die beantragende Behörde Dokumente als Anhänge der Meldung.

2. Die verfahrensleitende Behörde übermittelt ihre Anordnung oder Entscheid als **Zustellung** (siehe Abschnitt 4.4.2). Weil es sich um eine Zustellung handelt, schickt die verfahrensleitende Behörde nur Referenzen auf Aktenstücke in ihrer Akte zusammen mit der Abholfrist. Die anfragende Behörde konsultiert diese Aktenstücke dann über die Plattform mit Hilfe von elektronischer Akteneinsicht.

[18] Aus Gründen der Usability kann sehr wohl ein Userinterface entworfen werden, in dem man ganze Bereiche einer Akte markieren kann, und diese als Eingabe übermittelt. Dies wurde in der Infra.SB Sandbox so als Feature geschätzt. Im Weiteren ist es technisch möglich, die so kopierten Aktenstücke in einer Dokumentverwaltung trotzdem nur einmal vorzuhalten, aber logisch als Teil von 2 Akten darzustellen.

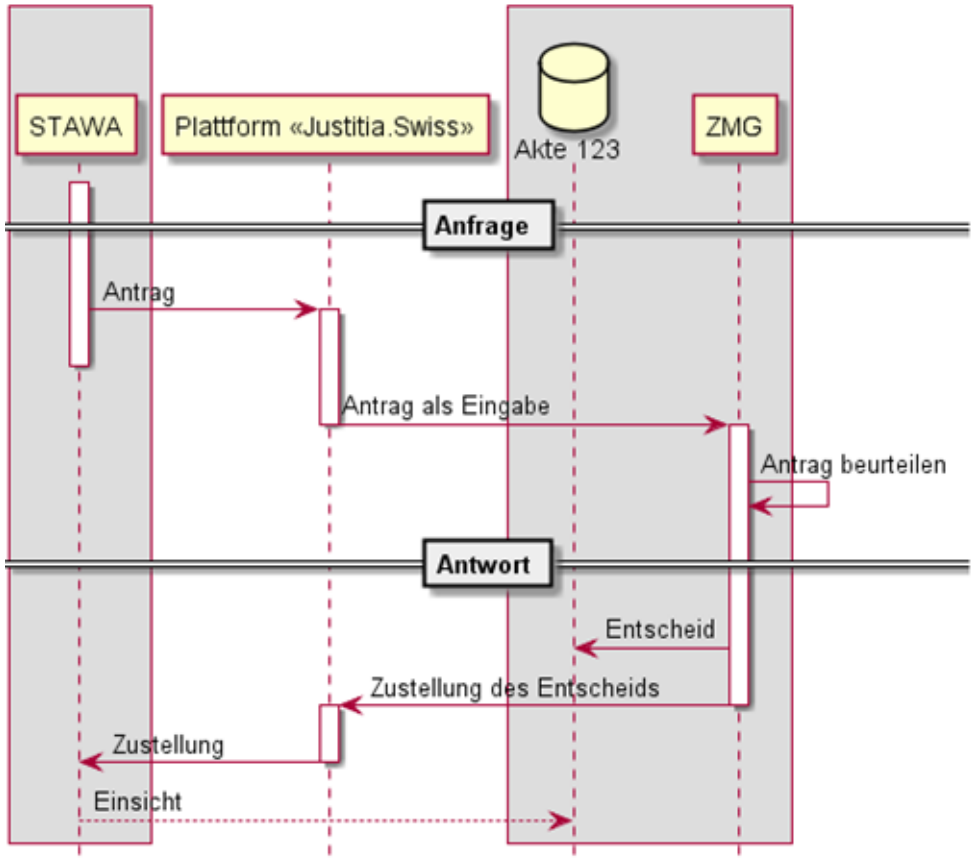


Abbildung 23: Anfrage und Antwort einer Behörde
Beachte, dass – obwohl die anfragende Behörde (also hier die Staatanwaltschaft) auch eine Akte führt – die angefragte Behörde **keine** Akteneinsicht bei der anfragenden Behörde braucht.

In obiger Abbildung wird – wie in allen Abbildungen dieses Kapitels – die Akteneinsicht als Zugriff auf die Akte der verfahrensleitenden Behörde visualisiert. Technische gesehen muss diese jedoch nicht ein Zugriff auf ein IT-System der Behörde realisiert werden. In Abschnitt 6.2 über die Datenhaltung der einsehbaren Akte wird erklärt wie der Zugriff technisch realisiert wird.

5.2 Weitergabe der Akten

Im Weiterzug zieht eine Partei (z.B. Staatsanwaltschaft, Kläger etc.) ein Urteil an die nächste Instanz. Das Verfahren wird weitergezogen. Fachlich übergibt die erste Instanz die Akte (alle Aktenstücke) an die nächste Instanz.

Dasselbe Muster tritt im Fall der Weiterleitung infolge Nichtzuständigkeit einer Behörde auf.

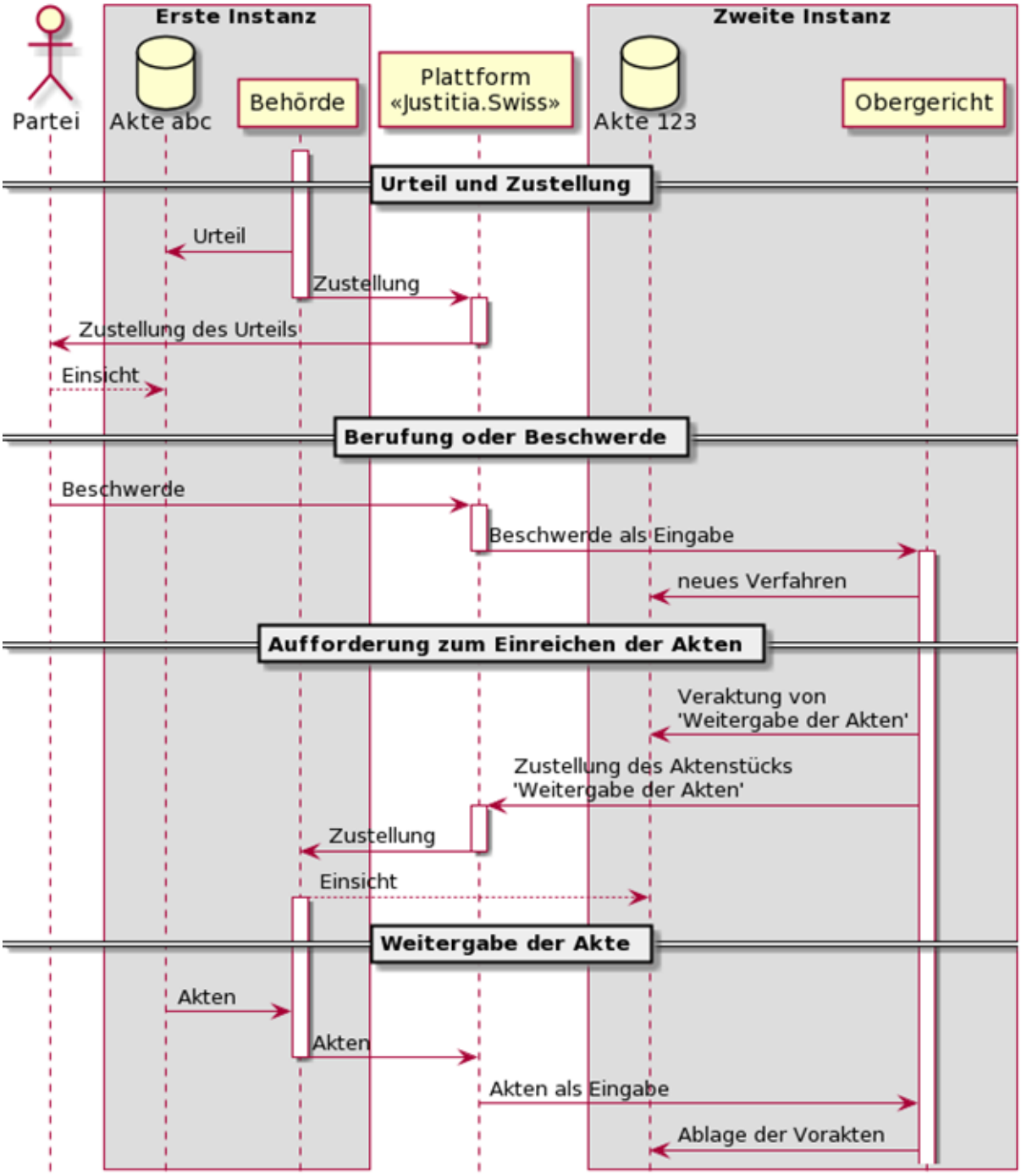


Abbildung 24: Weiterzug

Erläuterung:

1. Die erste Instanz fällt ein Urteil und stellt dieses der Partei (über die Plattform) zu.
2. Partei macht eine Eingabe bei nächster Instanz (z.B. Berufung, Beschwerde) und diese eröffnet ein neues Verfahren.
3. Die Rechtsmittelinstanz fordert die Vorinstanz zum Einreichen der Akten auf (Zustellung).
4. Die Vorinstanz übergibt die Akten als Eingabe an die nächste Instanz.

Hinweis: im letzten Schritt kann auch vorgesehen werden, dass anstelle einer Eingabe mit Dateien, eine Eingabe mit gleichzeitigem Erteilen eines Einsichtsrechts erfolgt.

5.3 Akteneinsichtsgesuch in laufendes oder abgeschlossenes Verfahren

In diesem Szenario möchte eine Behörde Verfahrensakten einer Justizbehörde beiziehen.

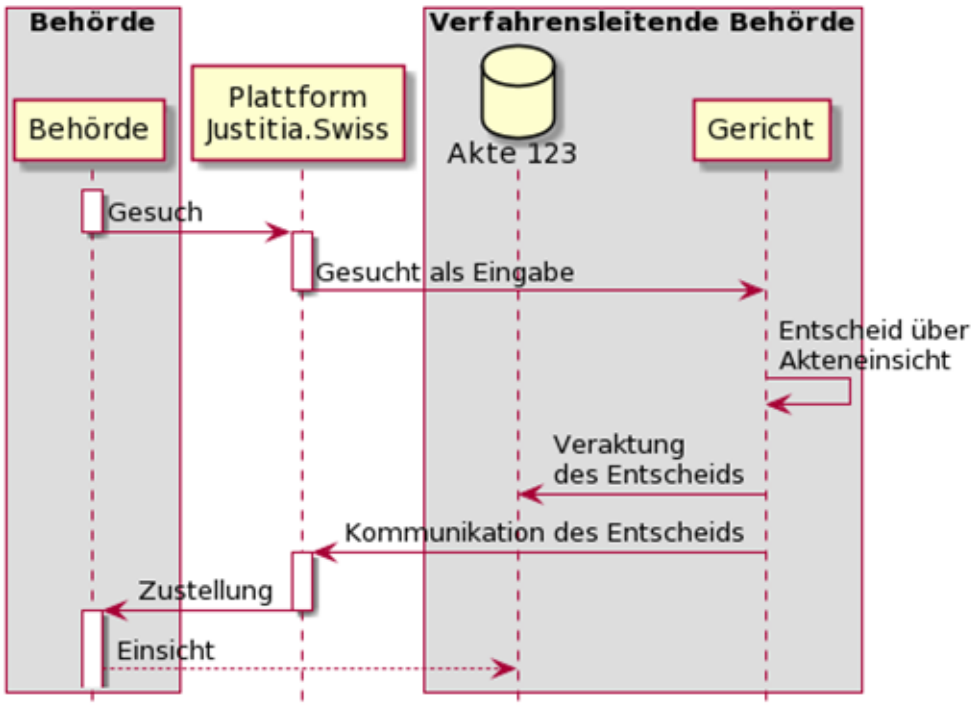


Abbildung 25: Beizug von Akten

Erläuterung:

1. Eine Behörde macht eine Eingabe an die verfahrensleitende Behörde mit Antrag um Akteneinsicht.
2. Diese entscheiden über den Antrag
3. und stellt den Entscheid zu. Im Fall eines ablehnenden Entscheides wird die anfragende Behörde nur Einsicht in ihr Gesuch bekommen und das Aktenstück mit der Ablehnung. Im Fall der gewährten Einsicht werden weitere Aktenstücke zur Einsicht berechtigt.

Hinweis: Man beachte den Unterschied des Gesuchs um Akteneinsicht gegenüber der Zustellung eines 'Weitergabe der Akten' (Abbildung 24) als Zustellung im vorherigen Abschnitt 5.2. Das Gesuch hier ist als Anfrage bei einer Behörde zu verstehen, welches auch abgelehnt werden könnte.

5.4 Klagebewilligung

In diesem Interaktionsmuster stellt die Schlichtungsbehörde ein Dokument (die Klagebewilligung) aus. Ein Kläger oder sein Vertreter kann nur mit diesem Dokument als Teil der Eingabe ein Verfahren bewirken.

Hier interagieren die beiden Behörden nur indirekt miteinander, die Kommunikation erfolgt 'über die Partei' und wird auch von dieser getrieben.

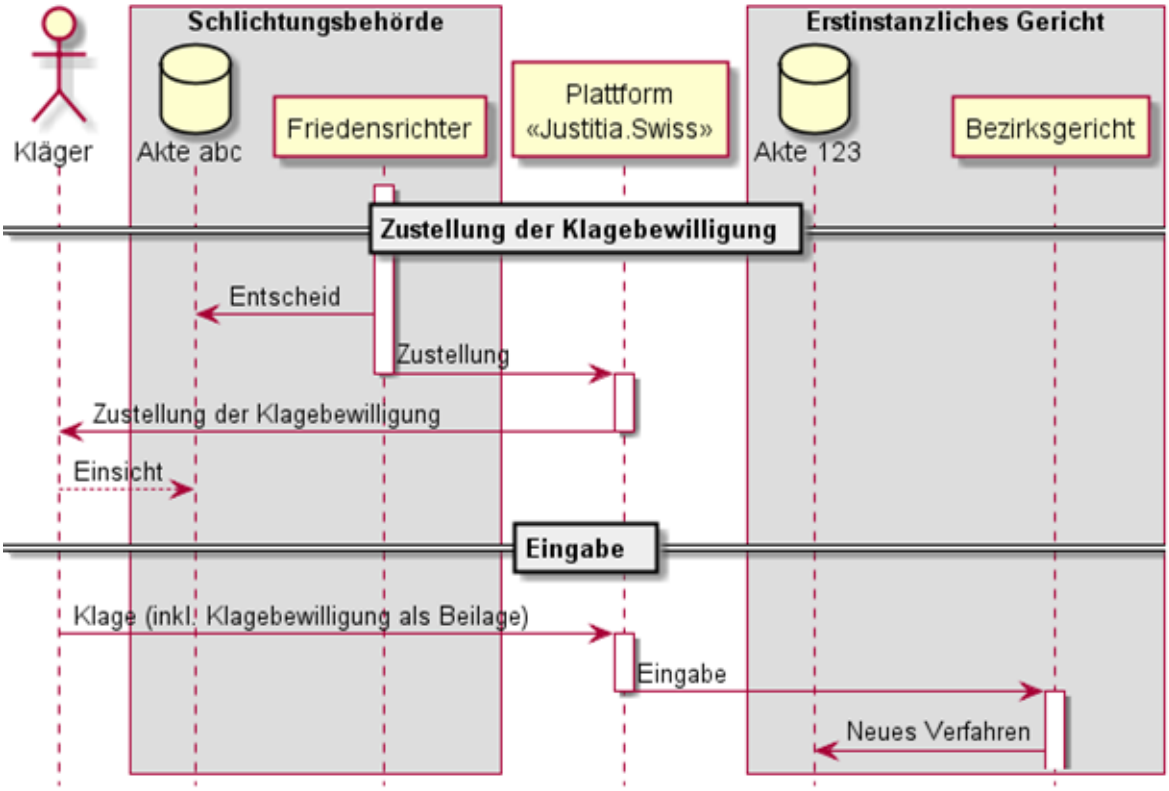


Abbildung 26: Klagebewilligung

Erläuterung:

1. Die Schlichtungsbehörde schliesst Verfahren ab (und macht eine Zustellung an beteiligten Anwalt) mit einer Klagebewilligung. Das wäre ein 'gesiegeltes Dokument durch die Schlichtungsbehörde'.
2. Der Anwalt macht eine Eingabe beim erstinstanzlichen Gericht mit der Beilage 'Klagebewilligung'.
3. Evtl. erfolgt Beizug von Akten durch erstinstanzliches Gericht.

Fazit: Es ist keine Akteneinsicht nötig. Die Beilage bei der Eingabe muss nicht 'gesiegelt' werden, ist schon unterschrieben.

5.5 Verwendung der Metadaten der Eingaben und Zustellung

Teilnehmer (vor allem Behörden) können digital über die Plattform mit Justizbehörden kommunizieren unter Verwendung der Prozesse der Zustellung (resp. Akteneinsicht) und Eingaben. Die Plattform übermittelt nicht nur 'Dokumente' welche von Menschen gelesen und (eventuell intern) weitergeleitet werden, sondern auch strukturierte Daten. Diese strukturierten Daten sollen von entsprechendem System empfangen werden und direkt – eventuell nach einer Prüfung durch einen Menschen - verarbeitet werden.

Die Plattform verwendet dazu die Metadaten der Dateien der Eingabe (Kapitel 4.4.1), resp. der einsehbaren Aktenstücke (Kapitel 4.3.3). Als Beispiel nehmen wir an, dass für die Anfrage bei einer Behörde (Abbildung 23) diese die Personen eines Tatherganges im Format eCH.051 übermittelt. Die Plattform erlaubt und unterstützt dann:

- Die Zuweisung einer Medientyps 'text/xml' für die Datei mit den Personen.
- Die Kategorisierung als 'beteiligte Personen'.

- Einstellungen im Profil der sendenden Person, so dass diese die Kategorie festlegen kann. Eine solche Einststellung darf aus Gründen der Sicherheit nur auf dem administrierten Profil erfolgen. Format der Datei wird durch die Plattform validiert.
- Das empfangende Profil sieht in den Benachrichtigungseinstellungen vor, dass eine Eingabe mit 'beteiligten Personen' an ein spezifisches System geleitet werden muss, damit dieses die entsprechende Eingabe abholen kann. (Im Normalfall nehmen wir an, dass Eingaben in der Kanzlei bearbeitet und manuell verteilt werden).

6 Systemsicht Plattform «Justitia.Swiss»

Die Plattform «Justitia.Swiss» ist **die zentrale Justizplattform** für die elektronische Akteneinsicht und den elektronischen Rechtsverkehr im Justizwesen der Schweiz. Sie wird durch eine öffentlich-rechtliche Körperschaft gebaut und betrieben.

Die Plattform «Justitia.Swiss» hat folgende zentralen Eigenschaften:

- **Sternförmige Integrationstopologie**: Die IT-Landschaften der Justizbehörden und am Verfahren beteiligten Personen oder Organisationen müssen nicht netzförmig (jeder mit jedem) integriert werden. Die Integration erfolgt ausschliesslich über die IT-Landschaft der Plattform «Justitia.Swiss».
- **Single Hop**: Im Gegensatz zum E-Mail-Austausch im Internet soll die Plattform als einzige «Zwischenstation» (im Folgenden als *Hop* bezeichnet) Meldungen resp. Aktenstücke zwischen den Akteuren transportieren. Es ist keine hierarchische- oder Multi-Hop Architektur vorgesehen[19]. Innerhalb der IT einer Justizbehörde oder einer beteiligten Partei können natürlich Meldungen und Aufgaben hierarchisch verteilt werden, dies ist jedoch für die Plattform unerheblich.
- **Arten der Kommunikation**: Im *Scope* ist ausschliesslich eingehender und ausgehender elektronischer Rechtsverkehr zwischen verfahrensleitenden Justizbehörden und verfahrensbeteiligten Personen respektive Organisationen. Allgemeiner Meldungsaustausch (ob rechtsverbindlich oder nicht) zwischen beteiligten Parteien eines Verfahrens ist nicht über die Plattform vorgesehen (z.B. Informationen von Anwalt zu Anwalt).

Die folgende Abbildung zeigt die beteiligten Akteure und Komponenten der Plattform Justitia.Swiss.

[19] In einem Netzwerk mit Paket-Switching ist ein Hop der Trip eines Datenpakets, den es von Zwischenstation zur nächsten benötigt.

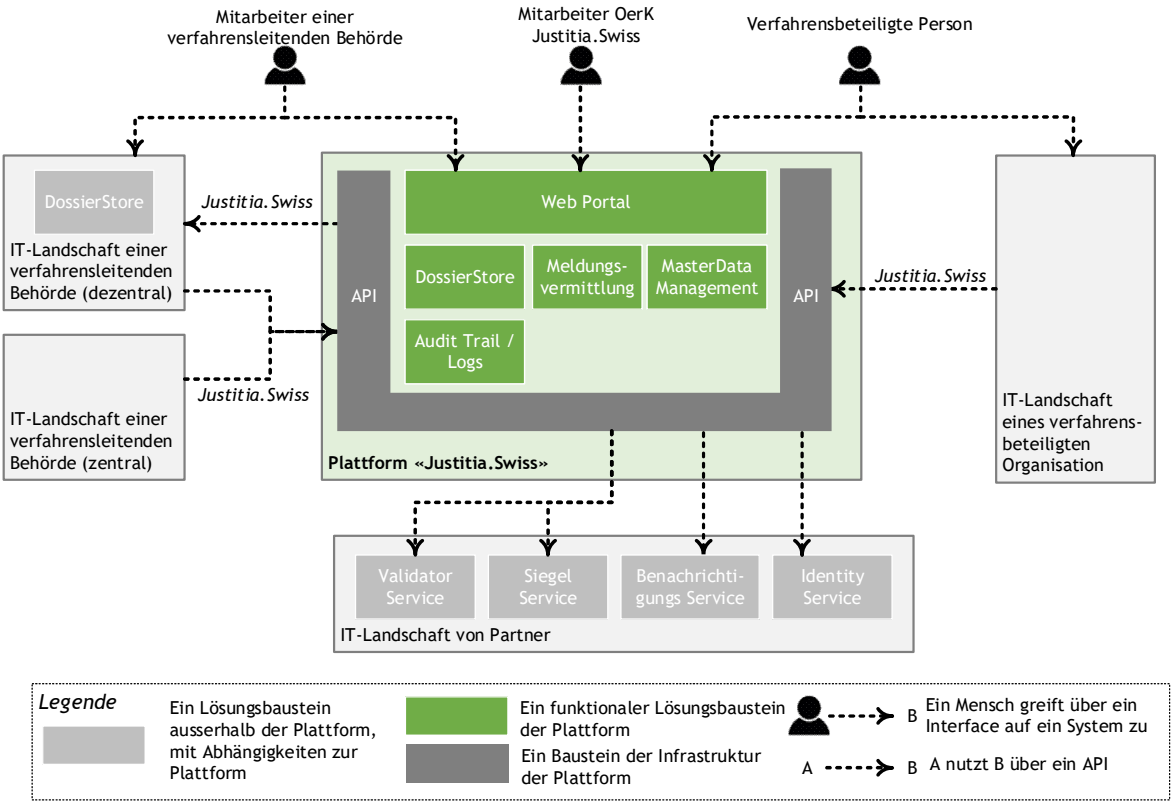


Abbildung 27: Schnittellenübersicht Plattform Justitia.Swiss

Legende:

- Die Plattform bietet ein **Web-Portal** für Mitarbeiter von verfahrensleitenden Behörden, für verfahrensbeteiligte Personen und Mitarbeiter von Verfahrensbeteiligten Organisationen wie auch Mittarbeitern der Betriebsgesellschaft (für Administrationsarbeiten). Das Web-Portal hat ebenfalls einen öffentlichen Bereich für nicht eingeloggte Benutzer mit öffentlich zugänglichem Inhalt (Content Management System).
- Die Komponente **DossierStore** erfüllt 2 Funktionen:
    - Sie speichert die Kopien der einsehbaren elektronischen Akte inkl. Aktendeckel, Aktenstücke und Aktenstruktur für Behörden, die dies wünschen.
    - Sie speichert im Namen der Behörden die Einsichtsrechte für verfahrensbeteiligte Personen und autorisiert die Zugriffe auf diese.
- Die Komponente **Meldungsvermittlung** vermittelt und managet die ausgetauschten Meldungen des elektronischen Rechtsverkehrs. Die Funktionalität basiert zu grossen Teilen auf einem Postfach je Teilnehmer.
- Die Komponente **MasterDataManagement** bietet Verwaltungsservices für die Stammdaten des Adressverzeichnisses.
- Die Komponente **Audit Trail / Logs** speichert revisionssicher die Events der Plattform und bietet Sichten darauf, sowohl für die Teilnehmer als auch für den Betreiber der Plattform für statistische Auswertungen.

Beschreibung von Services welche von Partner bezogen werden:

- Der **Benachrichtigungsservice** versendet Benachrichtigungen, welche Beteiligte über den Status von Meldungen informieren (siehe Kapitel 6.5).
- Der **Siegelservice** bringt auf Dokumente ein geregeltes Siegel an oder erstellt Signaturdateien (siehe Kapitel 6.4).
- Der **Validatorservice** validiert die Siegel von Dokumenten. (siehe Kapitel 6.4).

- Der **Identitätsservice** liefert sichere, digitale Identitäten für die Authentisierung von Nutzern (siehe Kapitel 4.1.3). Es können mehrere Identitätsservices eingebunden werden. Für Mitarbeiter von Behörden kann dieser Identitätsservice von der IT-Landschaft der Behörden zur Verfügung gestellt werden (Kapitel 4.1.1.4).

6.1 API Justitia.Swiss

Folgende API werden durch Justitia.Swiss vorgegeben[20]. Es handelt sich hierbei um einen ersten Überblick, im Design werden diese Schnittstellen entsprechend verfeinert und bei Bedarf angepasst:

Justitia.Swiss.01:	**Adressverzeichnis**
Über dieses API können Berechtigte die Profile mit Zustelladressen durchsuchen, um Empfänger für Übermittlungen zu finden.	
Justitia.Swiss.02:	**Profil**
Über dieses API können natürliche Personen ihr Profil administrieren, Delegationen einrichten, Organisationen (für die sie Administrator sind) verwalten.	
Justitia.Swiss.03:	**Eingabe**
Über dieses API können Verfahrensbeteiligte neue Eingaben erfassen, eine Eingabe zu einem bestehenden Verfahren übermitteln. Verfahrensleitende Justizbehörden können über dieses Interface Eingaben in ihren Postfächern herunterladen.	
Justitia.Swiss.04:	**Zustellung und Einsichtsrechte**
Über dieses API vergeben Justizbehörden Einsichtsrechte auf Aktenstücke und können Zustellungen auslösen. Über dieses Interface werden entsprechend auch Einsichtsrechte zurückgezogen. Hinweis: bei zentraler Datenhaltung verweisen die Einsichtsrechte auf Aktenstücke, welche über das API Justitia.Swiss.06: erstellt wurden.	
Justitia.Swiss.05:	**Aktenstücke**
Dieses Interface wird von Justizbehörden zur Verfügung gestellt, wenn sie Aktenstücke dezentral vorhalten.	
Justitia.Swiss.06:	**Einsehbare eAkte**
Über dieses Interface können Justizbehörden Daten und Dateien der Akten auf die Plattform replizieren. Über dieses Interface wird das Lifecycle Management der Akten (und damit auch der Einsichtsrechte) gesteuert. Bei zentraler Datenhaltung können über diese Interface Aktenstücke hochgeladen werden.	
Justitia.Swiss.07:	**Aktenbrowser**
Über dieses API können Verfahrensbeteiligte Akten, für die sie ein Einsichtsrecht haben, einsehen und herunterladen. Sie können einsehbare Akten auch mit persönlichen Tags und Vermerken versehen.	
Justitia.Swiss.08:	**Audit Trail**
Jeder Berechtige kann seine Historie einsehe, und bei Bedarf aus aufgezeichneten Events, Quittungen erstellen lassen.	
Justitia.Swiss.09:	**Validator**
Über dieses API können sämtliche Personen erhaltene (gesiegelte) Aktenstücke validieren lassen.	
Justitia.Swiss.10:	**Siegel**
Mit diesem API können Justizbehörden Dokumente mit ihrem Siegel versehen.	

[20] Eine konkrete Implementierung dieser API wurde im Rahmen der Infra.SB (Sandbox der Justitia.Swiss Plattform) implementiert. Diese sind unter https://int1.sb.j40.ch/swagger/index.html aufrufbar.

Tabelle 5: Justitia.Swiss APIs

Hinweise:

- Das API Justitia.Swiss.05: Aktenstücke wird (als einziges API) von Justitia.Swiss vorgegeben, muss jedoch durch die teilnehmenden IT-Landschaften implementiert werden, wenn diese dezentrale Datenhaltung (siehe folgendes Kapitel) wünschen.
- Die beiden APIs für Akte administrieren und Akten einsehen werden gegen aussen getrennt, da nur Behörden Akten administrieren können.

Technische Anforderungen an die APIs:

- Offener, moderner Standard (vorzugsweise REST): Damit haben Kantone maximale Freiheit. Es braucht die 3 Arten für Anbindung: Web-interface, Einbau in einer Webseite (Widget) und per Backend API.
- Benutzerkontext wird bei eingehenden Request immer mitgegeben. Requests enthalten Access Token, resp. ID-Tokens für Authentisierung.

Damit eine flexible Einbindung der Funktionalität von Justitia.Swiss in bestehende Systeme oder Abläufe[21] möglich ist:

- Die einfachste Nutzung ist über eine Weiterleitung auf das Web-Interfaces des Service: d.h. die Seitendarstellung erfolgt mittels html Seiten. Daten und Interaktionen erfolgten über Aufruf von dezidierten Services (heute meist über JavaScript, resp. darauf aufbauende Web-Frameworks).
- Bei Bedarf können Teile des Web-Frameworks in eigene Seiten eingebettet werden[22].
- Die APIs können von Maschinen (d.h. nicht aus einem Browserkontext heraus) aufgerufen werden.

Für einen späteren Ausbau muss vorgesehen werden, dass bei Eingaben auch grosse Datenmengen hochgeladen werden können müssen. Die Plattform soll explizit keine Grössenbeschränkungen für zu übermittelnden Daten haben, d.h. grösserer Speicher muss dynamisch alloziert werden können. Entsprechende Protokolle müssen für das parallele Hochladen vorgesehen werden.

Der Aktenbrowser muss flexibel erweiterbar sein, um für spezifische Medientypen Viewer vorzusehen.

Für die Anbindung über APIs müssen im Profil auch API-Keys hinterlegt werden können. Diese Keys werden als Identifikatoren der Maschinen (anlog Personen oder technischen Benutzern), welche eine Funktion bezüglich der Organisation ausführen, verstanden werden. Insbesondere für die ausgehende Kommunikation bei dezentraler Aktenhaltung (siehe Kapitel 6.2) muss die Plattform das Zertifikat und den Zugangspunkt des dezentralen Systems kennen. Ebenfalls kann es möglich sein, dass eingehende Requests von Justizbehörden nur technisch authentifiziert werden.

6.2 Datenhaltung der einsehbaren elektronischen Akte

Verfahrensleitende Behörden bieten verfahrensbeteiligten Personen elektronische Akten über die Plattform zur Einsicht an. Einzelheiten zum Konzept der einsehbaren elektronischen Akte sind Kapitel 4.3 beschrieben.

Technisch kann eine verfahrensleitende Behörde eine einsehbare elektronische Akte auf zwei Arten zugänglich machen:

1) zentral – sie kann die Akte im zentralen DossierStore bereitstellen.

[21] Diese Flexibilität wird unter anderem in Leitsatz 7 der Plattform gefordert, damit Beteiligte an Verfahren in ihrer (bekannten) IT-Infrastruktur arbeiten können.

[22] In der Sandbox wird dieses Integrationsmuster «Widget Integration» genannt.

2) dezentral – sie kann die Akte in der eigenen IT-Landschaft (in einem eigenen DossierStore bereitstellen).

6.2.1 Zentrale Datenhaltung der einsehbaren elektronischen Akte

Die Plattform umfasst einen zentralen DossierStore. Er nimmt folgende Aufgaben wahr:

- Einsehbare elektronische Akten halten und für die Einsicht bereitstellen.
- Die Berechtigungen für die Einsicht halten
- Die Berechtigung zur Einsicht zur Laufzeit prüfen (Autorisierung).

Erhält die Plattform Zustellungen einer Behörde mit zentraler Datenhaltung (Abbildung 28), dann:

- werden die darin enthaltenen Aktenstücke im DossierStore gespeichert und
- die Zustellung wird in der Meldungsvermittlung verarbeitet.

Im Zugriff auf diese Akten, resp. Aktenstücke, prüft die Meldungsvermittlung ob die Zustellung aktiviert ist und der DossierStore prüft in der Funktion 'Autorisierung', ob die lesende Person zur Ansicht des Aktenstücks berechtigt ist.

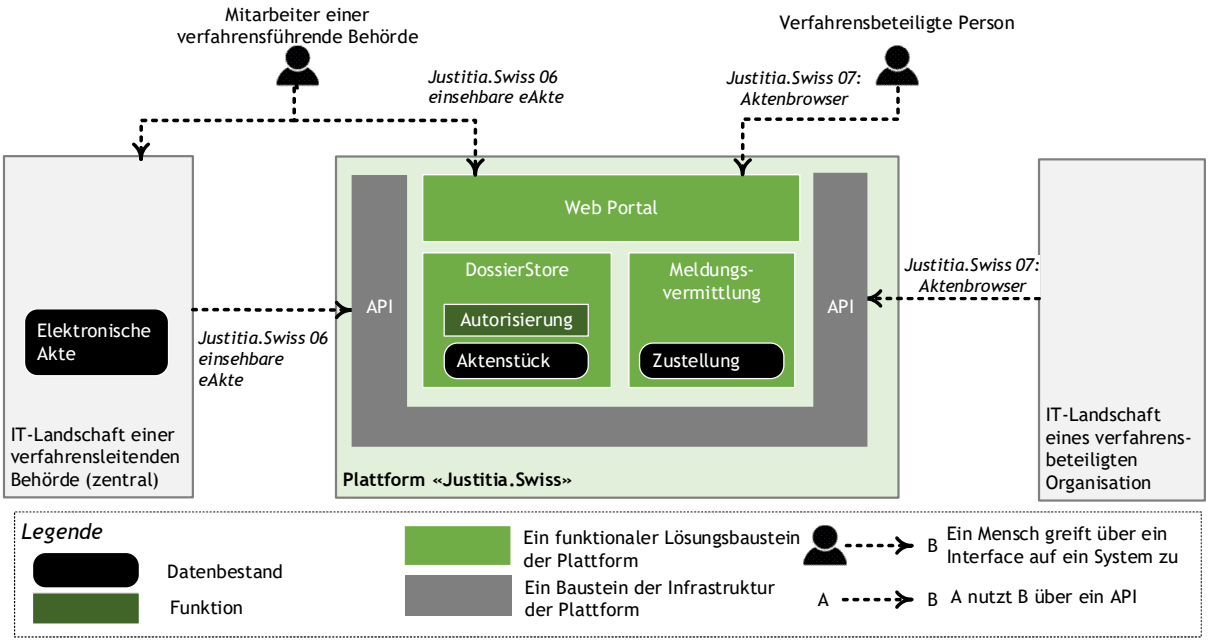


Abbildung 28: Zentrale Datenhaltung der einsehbaren elektronischen Akte

Hinweise:

- Eine Zustellung kann sich auch auf bereits 'hochgeladene' Aktenstücke beziehen. Die Vergabe von eindeutigen Identifikatoren erfolgt (als Teil der Veraktung) durch die Systeme der Justizbehörden.
- Die Funktion 'Autorisierung' muss nicht Teil einer physischen Komponente 'DossierStore' sein. Sie muss auf den Zustand der Zustellung zugreifen können, also die Berechtigungen des Benutzers kennen. Wie dies technisch im Detail umgesetzt ist, soll durch obige Skizze nicht vorweggenommen werden.

6.2.2 Dezentrale Datenhaltung der einsehbaren elektronischen Akte

Eine verfahrensleitende Behörde kann die einsehbaren Aktenstücke in ihrer eigene IT-Landschaft zur Einsicht vorhalten. Wir können sagen, sie führt einen eigene DossierStore (Abbildung 29). Dieser DossierStore ist aber nicht Teil der Plattform. Die Behörden sind frei darin, womit sie einen dezentralen DossierStore realisieren und wie dieser mit der elektronischen Aktenführung gekoppelt ist.

Erhält die Plattform Zustellungen einer Behörde mit dezentraler Datenhaltung, dann:

- Wird die Zustellung in der Meldungsvermittlung verarbeitet.

Im Zugriff auf diese Akten, resp. Aktenstücke, prüft die Meldungsvermittlung ob die Zustellung aktiviert ist und der DossierStore prüft in der Funktion 'Autorisierung', ob die lesende Person zur Ansicht des Aktenstücks berechtigt ist. Falls der lesende Benutzer berechtigt ist, wird das eigentliche Aktenstück vom dezentrale DossierStore über die Schnittstelle Justitia.Swiss.Access gelesen.

Das Projekt Justitia 4.0 wird Vorgaben bezüglich der Schnittstelle Justitia.Swiss.Access formulieren:

- Das Projekt wird die Schnittstelle formal spezifizieren. Ein dezentraler DossierStore wird diese standardisierte Schnittstelle anbieten müssen.
- Das Projekt wird Qualitätsvorgaben erlassen, die ein dezentraler DossierStore erfüllen muss (Vorgaben zu Verfügbarkeit, Durchsatz, Antwortzeiten, Vorgaben zum IT-Grundschutz und weitere)

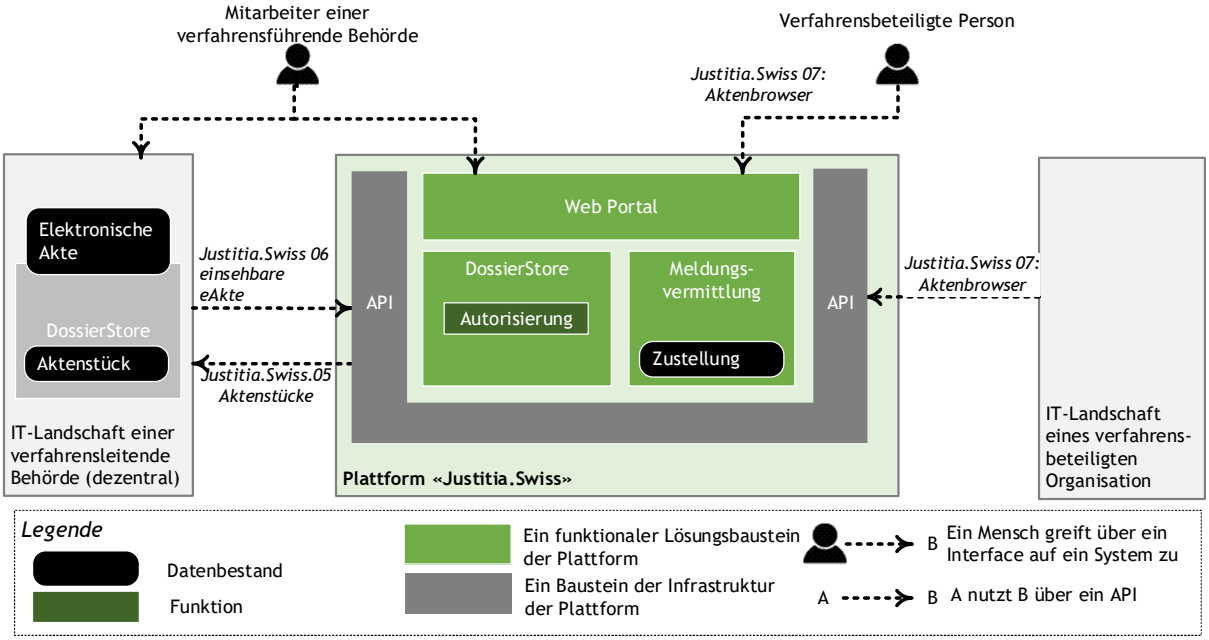


Abbildung 29: Dezentrale Datenhaltung der einsehbaren elektronischen Akte

Hinweise:

- Die Autorisierung wird auf der Plattform gemacht, damit der Status der Zustellung (die Rechtsverbindlichkeit der Zustellung) zentralisiert ist und die Delegationsregeln nicht zu den Justizbehörden repliziert werden sollen.
- Der Zugriff auf den dezentralen Dossierstore erfolgt immer über die Plattform. Dieser ist somit nie direkt von Internet her erreichbar (Security by Design).

6.2.3 Berechtigungen zur Einsicht erteilen und autorisieren

In diesem Kapitel fassen wir nochmals das bereits in Kapitel 4.4.2 über die Zustellung und Kapitel 4.3.6 über Akteneinsicht Gesagte zusammen. Wie wird Akteneinsicht aus Sicht der Justizbehörden verwaltet und geprüft?

- Ein Einsichtsrecht und damit eine Zustellung berechtigt 'ein Profil' für den Zugriff auf Aktenstücke. Beachte, dass diese Berechtigung 3 mögliche Ausprägungen gemäss Kapitel 4.3.2 hat: keine Berechtigung, Metadaten Lesen und Inhalt lesen.

- Einsichtsrechte haben eine Gültigkeitsdauer, welche durch die Behörden vorgegeben wird. Die Plattform bietet das Interface Justitia.Swiss.04: Zustellung und Einsichtsrechte oder die Möglichkeit über das Web um Einsichtsrechte (vorzeitig) zu entziehen, d.h. die Gültigkeit zu mutieren.
- Der Inhaber des Profils kann die Leseberechtigung an andere Profile delegieren (siehe Kapitel 4.5). In diesem Fall muss die Autorisierung diese Delegationskette auflösen. Beachte, dass noch nicht aktivierte Zustellungen je nach Güte der Delegation eventuell nicht gelesen werden dürfen.

6.3 Rechtsverbindliche Ereignisse quittieren

Die Plattform unterstützt verfahrensleitende Behörden und verfahrensbeteiligte Personen im ein- und ausgehenden elektronischen Rechtsverkehr. Der Empfänger und der Absender einer Meldung möchte ausgewählte Ereignisse im ERV rechtsverbindlich und nicht-abstreitbar nachweisen können.

6.3.1 Rechtsverbindliche Ereignisse im ERV

Absender und Empfänger im ERV sind interessiert, dass die Plattform ausgewählte Ereignisse rechtsverbindlich und nicht-abstreitbar festhält.

1. Absender möchten rechtsverbindlich nachweisen, dass sie eine Meldung zu einem bestimmten Zeitpunkt an die Plattform übergeben haben. Daran sind sowohl Behörden im ausgehenden ERV als auch verfahrensbeteiligte Personen im eingehenden ERV interessiert.
2. Absender möchten rechtsverbindlich nachweisen, dass ihre Meldung zu einem bestimmten Zeitpunkt durch den Empfänger eingesehen wurde. Daran ist in erster Linie eine verfahrensleitende Behörde interessiert. Sie möchte rechtsverbindlich nachweisen können, dass eine Zustellung vor einem bestimmten Zeitpunkt geöffnet wurde und dass das in der Zustellung referenzierte elektronische Aktenstück eingesehen wurde.

Das [VE-BEKJ] trägt diesen Bedürfnissen in Artikel 22 Rechnung. Es definiert ausgewählte Ereignisse, die die Plattform rechtsverbindliche und nicht-abstreitbar festhalten soll.

Ereignis	Beschreibung
Eingangsquittung der Zustellung	Eine verfahrensleitende Behörde hat der Plattform erfolgreich ein Einsichtsrecht, resp. Zustellung übergeben.
Eingangsquittung der Eingabe	Eine verfahrensbeteiligte Person hat der Plattform erfolgreich eine Eingabe übergeben.
Abrufquittung	Eine verfahrensbeteiligte Person oder eine andere dafür berechtigte Person greift erstmals erfolgreich auf ein elektronisches Aktenstück zu, das in einer fristbewerten Zustellung referenziert ist.
Zustellfiktion	Die Frist einer fristbewehrten Zustellung läuft ab, ohne dass der Empfänger oder eine andere dazu berechtigte natürliche Person das elektronische Aktenstück eingesehen hat, das in der Zustellung referenziert ist.

Tabelle 6: Rechtsverbindliche Ereignisse im ERV gemäss [VE-BEKJ]

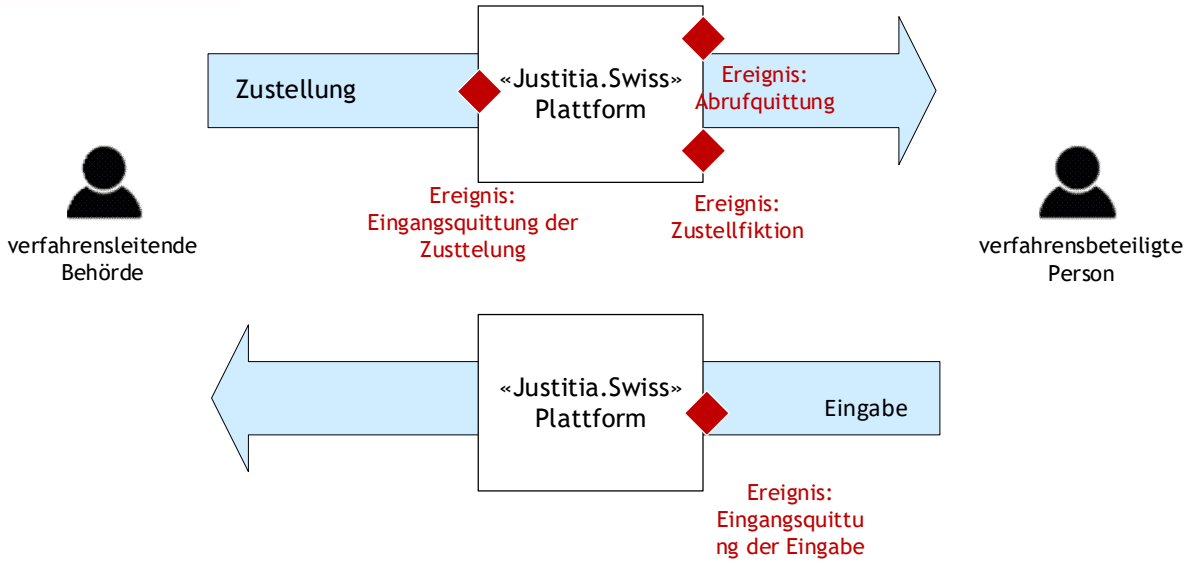


Abbildung 30: Rechtsverbindliche Ereignisse ERV

Die Plattform wird rechtsverbindliche Ereignisse im ein- und ausgehenden ERV erkennen und speziell behandeln müssen. Voraussichtlich wird es sich um die Ereignisse in Tabelle 6 handeln. Die abschliessende Liste der Ereignisse bleibt bis zur Ausschreibung offen.

6.3.2 Rechtsverbindliche Ereignisse nicht-abstreitbar aufzeichnen

Die Plattform wird erkannte rechtsverbindliches Ereignis nicht-veränderbar, authentisch und nicht-abstreitbar aufzeichnen.

Die Plattform wird zu diesem Zweck einen **Audit Trail für rechtsverbindliche Ereignisse** so führen, dass jederzeit aus den geloggten Daten ersichtlich ist, dass:

1. der Audit-Trail-Eintrag für ein rechtsverbindliches Ereignis vertrauenswürdig zu einem bestimmten Zeitpunkt angelegt wurde (qualifizierter Zeitstempel);
2. er zu einem bestimmten Zeitpunkt durch die Plattform (und durch niemand anderen) aufgezeichnet wurden (kryptografisch gesicherte Authentizität);
3. der Audit-Trail-Eintrag für ein Ereignis nicht unbemerkt verändert werden kann (kryptografisch gesicherte Integrität);
4. kein aufgezeichneter Audit-Trail-Eintrag unbemerkt gelöscht werden kann (kryptografisch gesicherte Integrität des ganzen Audit-Trails).

Mit welchen technischen und kryptografischen Ansätzen diese Komponente realisiert werden, bleibt bis zur Ausschreibung offen (Gestaltungsspielraum der Anbieter).

6.3.3 Quittungen für rechtsverbindliche Ereignisse

Damit Empfänger oder Absender im ERV rechtsverbindlich und nicht-abstreitbar nachweisen können, dass ein Ereignis im ERV stattgefunden hat, stellt die Plattform **Quittungen** aus.

Eine **Quittung** ist eine Datei, die ein rechtsverbindliches Ereignis im ERV dokumentiert. Sie hat die folgenden Eigenschaften:

1. Die Nutzdaten in der Datei beschreiben das Ereignis. Sie umfassen zum Beispiel den Zeitpunkt, an dem das Ereignis stattgefunden hat, Daten zum absendenden Profil und/oder zum Absender, Daten zum empfangenden Profil und/oder zum Empfänger, die Meldungs-ID, eine Aktenstück-Adresse etc.

Die Einzelheiten zu den Nutzdaten (welche Datenelemente die Nutzdaten im Details umfassen werden) bleiben bis zur Ausschreibung offen.

2. Die Datei ist mit kryptografischen Mitteln so abgesichert, dass
    - die Quittung nicht unbemerkt abgeändert werden kann (kryptografisch gewährleistete Integrität);
    - jederzeit nachweisbar ist, dass die Datei unter der Kontrolle der Plattform erstellt wurde (kryptografisch gewährleistete Authentizität).

    Als Ansatz der technischen Umsetzung wird die Datei voraussichtlich mit einem qualifizierten elektronischen Siegel der örK elektronisch unterschrieben. Die Einzelheiten der kryptografischen Absicherung bleiben aber bis zur Ausschreibung offen (Gestaltungsspielraum der Anbieter).
3. Das Format und die Struktur der Datei bleibt bis zur Ausschreibung offen (Gestaltungsspielraum der Anbieter). Typischerweise wird es sich um eine PDF/A-Datei handeln, die mit einem qualifizierten elektronischen Siegel versehen wird. Andere Möglichkeiten sind zum heutigen Zeitpunkt aber nicht ausgeschlossen, zum Beispiel eine Quittung als elektronisch unterschriebene XML-Datei gemäss einem standardisierten Schema.

Eine Quittung dokumentiert, dass ein rechtsverbindliches Ereignis zu einem bestimmten Zeitpunkt stattgefunden und dass die Plattform das Ereignis im Audit-Trail aufgezeichnet hat. Eine Quittung ist damit «eine beglaubigte Kopie» für einen Audit-Trail-Eintrag.

Eine entscheidendes Datenelement in einem Audit-Trail-Eintrag und in der Quittung ist der Zeitpunkt, an dem das Ereignis stattgefunden hat. Die Quittung enthält diesen Zeitpunkt in den Nutzdaten. Der Zeitpunkt, an dem eine Quittung ausgestellt wird und der als Zeitstempel im Siegel eingebettet ist, mit der die Integrität und Authentizität der Quittung gewährleistet wird, ist unabhängig vom Zeitpunkt des Ereignisses: Der Zeitstempel im Siegel sagt nichts über den Zeitpunkt des rechtsverbindlichen Ereignisses aus.

6.3.4 Quittungen erstellen

Die Steuerung, ob und wann eine Quittung (als «beglaubigte Kopie» eines Audit-Trails) erstellt wird, kann unterschiedlich designed werden.

- Beim Versenden einer Eingabe, resp. Zustellung gesteuert durch ein Flag ‘ja will eine Quittung für diese Meldung’.
- Durch Stammdaten auf dem zugehörigen Profil: ‘ja ich will immer eine Quittung…’.
- Durch eine Sicht auf die Übermittlung und den expliziten Wunsch: ‘erstelle mir herzu eine Quittung’.

Ob tatsächlich alle drei Optionen oder nur eine Teilmenge davon realisiert werden, bleibt bis zur Ausschreibung offen. Zurzeit sind sich die Justizbehörden gewohnt, immer eine Quittung für Zustellungen und Eingänge zu den Akten zu nehmen. Eventuell wird sich mittelfristig herausstellen, dass diese nicht mehr nötig sein wird, da bei Bedarf auf den Audit Trail zugegriffen werden kann.

6.3.5 Weitere rechtsverbindliche Ereignisse

Aus Sicherheits- und Datenschutzgründen sind weitere Ereignisse in der Plattform aufzuzeichnen, dies betrifft sämtliche Mutationen von Stammdaten (Profile, Verknüpfungen mit digitalen Identitäten, Delegation etc.). Für solche Ereignisse werden keine Quittungen ausgestellt, jedoch muss die Plattform den jeweils berechtigten Personen die Historie der Stammdaten aufzeigen können.

6.4 Siegel und Validierung

Das Gesetz ([VE-BEKJ], Art. 23 – Validator) fordert, dass die Plattform einen Validierungsservice zur Verfügung stellt, mit dem die Signaturen und Zeitstempel der über die Plattform eingesehenen Aktenstücke validiert werden können. Gleiches gilt für von der Plattform ausgestellte Quittungen.

Um Eingaben mit dem Siegel der Körperschaft zu versehen, wird die Plattform eine der bestehenden Signaturservices des BIT oder eines privatrechtlichen Anbieters nutzen. Die Plattform wird Eingaben und Quittungen siegeln. Welcher Anbieter das sein wird, wird im Design entschieden.

Gemäss Grobanforderungen FUN-04-01 soll die Plattform auch die Möglichkeit vorsehen, dass Dokumente von Justizbehörden durch die Plattform im Rahmen einer Zustellung resp. Akteneinsicht gesiegelt werden. Der Vorentwurf des BEKJ enthält jedoch einen Passus (Art 21, Abs 2), dass die Plattform Dokumente von Behörden zurückweisen soll, wenn diese nicht mit einem geregelten Siegel versehen sind. Zum aktuellen Zeitpunkt ist offen, wie der detaillierte Ablauf und die Regeln dazu sinnvoll zu gestalten sind.

Für die Validierung von eingehenden Dokumenten wird die Plattform den Validator-Service des BIT verwenden. Zentral für das Verständnis ist, dass der Validator sogenanntes Behördenzertifikate verwendet soll. Im Behördenzertifikat wird die zertifizierende Organisation im Feld 'OrganisationalUnit' eingetragen. Es soll in der revidierten TAV (TAV – Verordnung des BAKOM über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate) geregelt werden wie die Behördenstellen in den Zertifikaten eingetragen werden [K-GBZ]. Für die Plattform bedeutet das:

- Es sollen keine Spezialregeln auf der Logik der Zertifikate und Siegel implementiert werden. Die Plattform verwendet die Logik, wie sie in den Verordnungen zum ZertES festgelegt sind (SR 943.032 und 943.032.1).

6.5 Benachrichtigungen enthalten Aktenstück-Adressen

Wenn ein Empfänger über die Plattform eine Übermittlung erhält, kann ihn die Plattform über einen anderen (öffentlichen) Kanal (E-Mail, SMS, etc.) benachrichtigen (Siehe Abschnitt 4.2.2). Wie in Kapitel 4.4.1 über die Eingabe angesprochen, wird der Benachrichtigungsmechanismus auch verwendet, damit die Fachapplikation der Justizbehörden Eingaben abholen kann. Damit ist die Fachapplikation der technisch aktive Teil. Benachrichtigungen sind also auch vorgesehen, um technische Trigger direkt an Systeme der IT-Behörden zu senden. (siehe dazu auch Kapitel 5.5 für die Motivation dieses Routings).

Details des Formats und Inhalts der Benachrichtigungen, die Darstellung der Aktenstückadressen als Teil der Benachrichtigung werden im Design geklärt.

Die **Aktenstück-Adresse** erfüllt zwei Aufgaben:

1. Sie enthält genügend Informationen, damit die Plattform weiss, wo sie das elektronische Aktenstück beziehen kann.

2. Sie enthält genügend Informationen, damit die Plattform weiss, welches elektronische Aktenstück gemeint ist, damit also das Aktenstück eindeutig identifiziert ist.

Sie wird so gestaltet werden, dass sie die Aufgaben einer Aktenstück-Adresse erfüllt aber nicht direkt aus dem Browser eines Benutzers zum Aktenstück führt. Eine Aktenstück-Adresse wird also namentlich keine http-URL sein, mit dem direkt auf ein Aktenstück bei einer Behörde zugegriffen werden kann (keine URL à la `https://www.bger.ch/eae/akte-001/aktenstueck002`).

Zur Illustration verwenden wir in diesem Dokument und in den validieren Beispielen eine URL nach dem folgenden Schema:

`https://justitia.swiss/eae/{akteId}/{aktenstückkennzahl}`

also zum Beispiel

`https://justitia.swiss/eae/akte-0001/aktenstück-0002`

In der Realität werden diese Strings aus Gründen des Datensicherheit jedoch in einen unlesbaren Schlüssel gehashed:

`https://justitia.swiss/eae/UXV67ijk32_4`

6.6 Föderiertes Identitätsmanagement

Eine strategische Aussage zur Plattform ist, dass diese keine eigenen (digitalen) Identitäten anbieten will (Prinzip 3). In diesem Abschnitt fassen wir die Konsequenzen daraus und die aktuellen Annahmen für die technische und betriebliche Sicht zusammen. Eine Detaillierung wird im Design erfolgen.

- **IDP für natürliche Personen**: Es sollen mehrere Identitätsprovider angeschlossen werden können. Zurzeit gibt es einige schweizweit operierende Anbieter, die digitale Identitäten ausstellen können. Des Weiteren bieten immer mehr Kantone digitale Dienstleistungen an.
- **IDP für Mitarbeiter**: Organisation können über einen administrativen Prozess ihren IDP einbinden, damit ihre Mitarbeiter über Single-Sign on Zugang auf die Plattform bekommen. (siehe Abschnitt 4.1.1.4). Die Plattform soll flexible Mechanismen vorsehen, damit für solche Mitarbeiter aus der Information die Funktionen (gemäss Tabelle 2 im Abschnitt 4.1.2.1 über Organisationsmitgliedschaft) hergeleitet werden können.
- **IDP für Support Mitarbeiter**: Mitarbeiter des Supports und Service Desks sollen ebenfalls über das Web-Interface auf die Applikation zugreifen, um Supportanfragen zu erledigen. Die Rechte und Organisation der Supportmitarbeiter sollen also entsprechend im IDP hinterlegt werden. Man beachte, dass eine IDP eines Kantons für mehrere Justizbehörden verwendet wird. Entsprechend flexibles Mapping der Funktion und Organisation (beziehungsweise des administrierten Profils) müssen möglich sein.
- Als **technische Protokolle** werden Standardprotokolle wie OpenId Connect oder SAML (namentlich in Bezug auf das ISC-EJPD oder den Kanton VD) vorgesehen.
- Es sind **Prozesse** vorzusehen, damit eine natürliche Person ihren IDP wechseln kann. Dabei ist insbesondere sicherzustellen, dass diese Verknüpfung gemäss Datenschutz sicher erfolgt. Im Weiteren muss geprüft werden, ob die amtlichen Attribute aller IDPs übereinstimmen.

6.7 Daten Lifecycle Management

In diesem Kapitel werden Aspekte des Lifecycle Management von Stammdaten, Bewegungsdaten und Audit Trail Einträgen beschrieben.

6.7.1 Personen, Profile, Delegation

Stammdaten, welche die Plattform bewirtschaftet, sind Personen zugeordnet und müssen (z.B. bei Nichtgebrauch) oder auf Wunsch der Person gelöscht werden können (Prinzip 12). In diesem Abschnitt fassen wir Zusammenhänge und Abhängigkeiten der Stammdaten zusammen, um die Prozesse für die Bewirtschaftung im Design entsprechend vertiefen zu können.

6.7.1.1 Aktive Profile

Das Profil ist der Aufhänger für das Lifecycle Management der Stammdaten und damit der Personendaten. Die Plattform unterscheidet zwischen aktiven und inaktiven Profilen. Ein aktives Profil hat eine validierte Aktivierungsadresse, über welche der Betreiber (oder ein technischer Prozess) den Inhaber oder Administrator des Profils kontaktieren kann. Die Aktivierungsadresse ist eine E-Mail-, SMS- oder ähnliche Adresse. Folgende Ziele werden damit erreicht:

- Beim Eröffnen des Profils wird über diese Adresse das Profil aktiviert. Damit ist sichergestellt, dass die Aktivierungsdresse existiert und 'gültig' ist.
- Hat dieses Profil über einen längeren Zeitraum keine Aktivitäten und keine aktiven Verfahren (keine Berechtigungen zur Akteneinsicht, siehe Kapitel 4.3) kann über diese Adresse geprüft werden, ob das Profile inaktiv ist, resp. gelöscht werden darf.

Folgender Ablauf illustriert das aktivieren eines (neuen) Profils. Konzeptionell legt die Plattform die natürliche Person mit dem erstmaligen Einloggen an und erstellt das Profil. Person und Profil haben im Diagramm Informationsmodell (Abbildung 3) eine eins-zu-eins Beziehung. Um das Profil zu aktivieren, gibt der Benutzer eine Aktivierungsadresse an. Die Plattform sendet ihm dann über diesen (zweiten) Kanal einen 'Aktivierungscode' zum aktivieren des Profils.

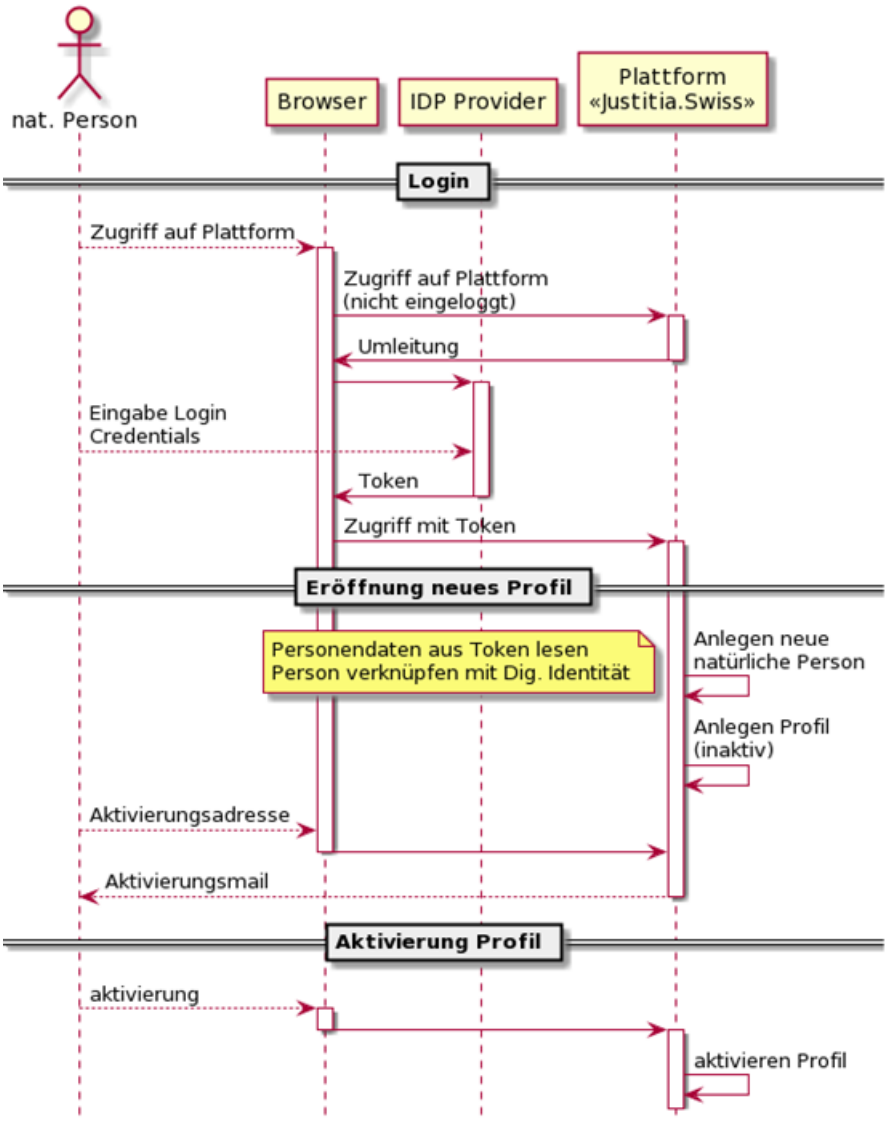


Abbildung 31: Aktivieren eines Profils

Das Profil muss zum Setzen einer Zustelladresse oder um Delegationen empfangen zu können aktiv sein.

6.7.1.2 Dublettenerkennung für natürliche Personen

Über die Aktivierungsadresse realisiert die Plattform eine vereinfachte Dublettenerkennung. Gibt eine natürliche Person eine bereits für ein aktives Profil vergebene Aktivierungsadresse ein, darf die Platt-

form diese Adresse nicht (!) als Aktivierungsadresse verwenden, sondern soll den Benutzer darauf hinweisen, dass diese Aktivierungsadresse bereits in Benutzung ist. Damit soll verhindert werden, dass der 'neue Benutzer' Informationen des bereits bestehenden Profils erraten kann[23].

6.7.1.3 Inaktivierung und Löschung von Profilen

Ein Profil, das keine aktive Akteneinsicht hat, ist potentiell nicht mehr im Gebrauch. Hat auf diesem Profil seit längerer Zeit (ca. 1 Jahr) keine Aktivität mehr stattgefunden, kann diese Profil potentiell gelöscht werden. Es sind Prozesse vorzusehen, um solche Profile zu bestimmen und über die Aktivierungsadressen die entsprechenden Inhaber zu kontaktieren. Bei Bedarf werden die entsprechenden Stammdaten gelöscht.

6.7.1.4 Lifecycle je Art des Profils

Wir orientieren uns anhand der verschiedenen Arten von Profilen (Abschnitt 4.2.4), um die entsprechende LifeCycle Prozesse zu skizzieren:

- **Profil einer Privatperson**: Inaktive Profile werden periodisch gelöscht. Inhaber von potentiell nicht mehr im Gebrauch befindlichen Profilen werden kontaktiert und bei nicht Reagieren gelöscht.
- **Profil einer Justizbehörde**: Eröffnung und Schliessung dieser Profile erfolgt über einen administrativen Prozess.
- **Selbstadministriertes Profil**: Das Lifecycle Management dieses Profils wird nicht über eine eigene Aktivierungsadresse gesteuert, sondern über das Profil des Administrators (welcher selber ein aktives Profil hat). Man beachte, dass die Bewirtschaftung von Mitgliedern von Organisationen mehrere Administratoren zulässt, ebenso auch den Wechsel des Administrators.
  Ist ein selbstadministriertes Profil lange inaktiv und hat keine aktiven Verfahren, werden sämtliche Administratoren (und ev. die Inhaber) kontaktiert, bevor das Profil deaktiviert und gelöscht werden kann.
- **Profil einer administrierten Organisation**: Diese Profile werden – nomen est omen – über einen administrierten Prozess gepflegt und auch gelöscht. Die Plattform muss jedoch Auswertungen vorsehen, damit der Betreiber potentiell inaktive Profile administrierter Organisationen findet.
- **Mitarbeiterprofil**: Für Mitarbeiter von IDP-verwalteten Organisation führt die Plattform nur sehr beschränkt Personendaten, da sie jeweils beim Einloggen vom IPD die Funktion des Mitarbeiters auf dem Profil erhält. Unsere Annahme ist, dass mit IDPs der so verwalteten Organisationen Abgleichprozesse implementiert werden, um inaktive Mitarbeiter zu entfernen, sollten diese auf ihrem Profil eigene Stammdaten bewirtschaftet haben.

6.7.1.5 Einladungsverfahren

Es gibt verschiedene Gründe, warum eine Person eine andere (meist natürliche) Person auf die Plattform einladen will:

- Eine Justizbehörde hat ein Verfahren und möchte einer verfahrensbeteiligten Person etwas zustellen. Diese verfahrensbeteiligte Person hat jedoch noch kein Profil auf der Plattform errichtet, ist aber anderweitig bereit oder sogar genötigt, die Zustellung elektronisch zu empfangen. In diesem Fall eröffnet die anfragende Behörde eine Zustelladresse und lädt die betreffende Person ein, ein Profil zu eröffnen.
- Eine Person möchte eine Delegation errichten oder bei einer nicht IDP-verwalteten Organisation neue Mitglieder hinzufügen. Man beachte, dass aus Datenschutzgründen das Adressverzeichnis nicht öffentlich ist und sich also Personen nicht gegenseitig sehen dürfen.

Die Detaillierung dieses Prozesses erfolgt im Design.

---

[23] Hinweis: damit wird Prinzip 2 nicht aufgehoben. Einer natürlichen Person steht es frei, mehrere E-Mail-Adressen zu bewirtschaften. Jedoch haben keine zwei verschieden natürlichen Personen dieselbe E-Mail-Adresse.

6.7.2 Akten und Übermittlungen

Mit der erstmaligen Zustellung resp. dem Erteilen eines Einsichtsrecht auf einem Aktenstück wird das die AkteId auf der Plattform eröffnet. Ab diesem Zeitpunkt können:

- Verfahrensspezifische Delegation auf diesem Verfahren errichtet werden (siehe Kapitel 4.4).
- Spezifische Eingaben zu diesem Verfahren erfasst werden.

Wenn Verfahren abgeschlossen werden – was im Allgemeinen mit einem rechtskräftigen Urteil erfolgt – muss die Justizbehörde der Plattform dies mitteilen, damit die Plattform entsprechende Delegationen und Sichten für die Verfahrensbeteiligten entfernen kann:

- Verfahrensspezifische Delegationen löschen.
- Übermittlungen (Einsichtsrechte und Zustellungen) zu dieser Akte löschen.
- Dokumente aus dem DossierStore für diese Akte entfernen.

Damit wird sichergestellt, dass keine Akteneinsichten für abgeschlossene Verfahren (im engeren Sinn) mehr auf der Plattform stattfinden können.

Zurzeit ist vorgesehen, das Löschen einer Akte über das Interface Justitia.Swiss.06: der eAkte anzustossen. Es könnte jedoch auch vorgesehen werden, dass in den Metadaten einer Zustellung (Interface Justitia.Swiss.04:) Justiz- und verfahrensspezifische Codes mitgegeben werden, aus welchen die Plattform ableitet, dass mit dieser Zustellung das Verfahren abgeschlossen wird.

Hinweis: Es ist nicht Aufgabe der Plattform, die Daten eines Verfahrens für die Langzeit Archivierung den jeweiligen Staatsarchiven zu übergeben. Diese Aufgabe verbleibt bei den verfahrensleitenden Behörden.[24]

Eingaben werden nach einer definierten Zeit nach Abholung gelöscht (siehe Kapitel 4.4.1).

6.7.3 Audit Trail

Die Daten des Audit Trails 'gehören' der Plattform, enthalten jedoch auch Personendaten der entsprechenden Ereignisse. Auch wenn Stammdaten oder Akten gelöscht werden, werden die entsprechenden Audit Trail Einträge nicht gelöscht.

Ein Löschen der Audit Trail Einträge erfolgt nach einer eigenen Periodizität. Aktuell werden die Empfangsbestätigungen der Gerichtsurkunden (physikalische Welt) von der Post 3 Jahre aufbewahrt. Für die Plattform rechnen wir mit einer ähnlichen Periodizität.

6.8 Sichten auf die Meldungen

Im Gegensatz zum gewohnten E-Mail hat der elektronische Rechtsverkehr für beide Seiten – den Sender und den Empfänger – immer die Sicht auf den aktuellen Zustand der Übermittlung. Während man in einem E-Mail System im 'Ausgang' die versandten Meldungen sieht, sieht man im elektronischen Rechtsverkehr den Zustand der versandten Meldung, also ob der Empfänger die Meldung schon gelesen hat. E-Mail Systeme bieten zwar beispielsweise die Möglichkeit einer 'Lesebestätigung' an, können diese Funktionalität allerding aufgrund der Multi-Hop Architektur des E-Mails nicht garantieren.

In Tabelle 7 ist sichtbar, welche Elemente einer Eingabe in Abhängigkeit des Zustandes über welche Kanäle, resp. APIs sichtbar sind.

Status der Eingabe	**Verfahrensbeteiligte Person (Sender)**	**Verfahrensleitende Behörde (Empfänger)**

[24] Siehe Projektauftrag kurz (Resultat Nr. 012), Kapitel 3.2.1 Grobanforderungen an die eJustizakte / JAA.

	Sicht im Web	Zugang über API	Sicht im Web	Zugang über API
Entwurf	Auf dem Profil berechtigte Benutzer können die Dateien der Eingabe sehen und mutieren.	Nicht sichtbar	Nicht sichtbar	Nicht sichtbar
Versandt **Empfangen**	Aus dem Web und dem API können diese Dokumente heruntergeladen werden (sofern Benutzer auf dem Sender- resp. Empfängerprofil berechtigt ist): - Eingangsquittungen - Originaldokumente - Gesiegelte Dokumente, resp. Hashcodes Die Eingabe kann nicht mehr mutiert werden.			
Gelöscht	Eingabe nicht mehr verfügbar.			

Tabelle 7: Sichtbarkeiten der Eingabe

Auf einem Profil berechtigt ist der Inhaber des Profils, Mitarbeiter der Organisation welcher das Profil gehört oder eine über Delegation ermächtige Person (siehe Kapitel 4.5.2 über die Arten der Delegation).

Man beachte, dass in einem ersten Schritt noch kein API definiert werden soll, welches ein schrittweises Erfassen einer Eingabe (aus einer Anwaltssoftware) unterstützt. Wir nehmen an, dass eine entsprechende Software den Erfassungsschritt selbst vornimmt und das Versenden der Eingabe als einen transaktionalen Schritt realisierst wird.

In Tabelle 8 sind die Sichten auf Zustellungen, resp. Einsichtsrecht je Zustand dargestellt.

Status der Zustellung	Verfahrensleitende Behörde (Sender)		Verfahrensbeteiligte Person (Empfänger)	
	Sicht im Web	**Zugang über API**	**Sicht im Web**	**Zugang über API**
Entwurf	Auf dem Profil berechtigte Benutzer können die Aktenstücke zur Zustellung hochladen und Verfahrensbeteiligte als Empfänger für hochgeladene Aktenstücke berechtigten.	Nicht sichtbar	Nicht sichtbar	Nicht sichtbar
Versandt	Inhalt und Metadaten je zugestelltem Aktenstück ist sichtbar. Die Aufgabequittung kann heruntergeladen werden.		Metadaten je zugestelltem Aktenstück sind sichtbar, sofern der Benutzer auf dem Sender, resp. Empfängerprofil berechtigt ist. Die Aufgabequittung kann heruntergeladen werden	
Aktiviert	Zusätzlich kann die Abrufquittung heruntergeladen werden.		Zusätzlich kann die Abrufquittung heruntergeladen werden. Zusätzlich sind (sofern berechtigt) die Inhalte der referenzierten Aktenstücke einsehbar, resp. können heruntergeladen werden.	
Beendet	Aktenstücke nicht mehr verfügbar.			

Tabelle 8: Sichtbarkeiten der Zustellung, resp. des Einsichtsrechts

Hinweise:

- Man beachte, dass das Erfassen von Zustellungen über das Web-Interface nur bei zentraler Datenhaltung (siehe Kapitel 6.2) sinnvoll ist. Hat eine Behörde dezentrale Aktenhaltung, muss das Erfassen der Zustellung mit der dezentralen Datenhaltung gekoppelt sein und die Übermittlung erfolgt über das API.
- Um entsprechende Sicherheit beim Erfassen zu geben, sollte eine Sicht vorgesehen werden, in der die verfahrensleitenden Behörden je Empfänger (resp. die Verfahrensbeteiligten) sehen kann, welche Aktenstruktur er denn mit Erhalt der Zustellung sehen würde.

6.9 Vermerke und Tags auf dem Web-Portal

Anwälte müssen auf der Plattform Vermerke und Tags auf den Akten und Aktenstücken anbringen können. Gemeint sind *persönliche* Tags und ein *persönlicher* Vermerk, das heisst, Tags und Vermerke, die nur für den Anwalt selbst und delegierbar, aber nicht für andere Benutzer auf der Plattform und nicht für Behörden sichtbar sind.

Im Sinne einer guten User Experience soll diese Möglichkeit auf dem Web-Portal vorgesehen werden. Ob auf die Tags und Vermerke auch über das API zugegriffen werden kann, ist zurzeit offen, da davon

ausgegangen wird, dass ein entsprechendes System auf Seite des professionellen Nutzers mehr Möglichkeiten bietet.

Vermerke und Tags, die Benutzer auf der Plattform auf einsehbaren elektronischen Akten oder Aktenstücken anbringen, bewirtschaftet die Plattform zentral, auch dann, wenn die Akten und Aktenstücke selbst durch eine Behörde dezentral in einem dezentralen DossierStore bewirtschaftet und zur Einsicht angeboten werden.

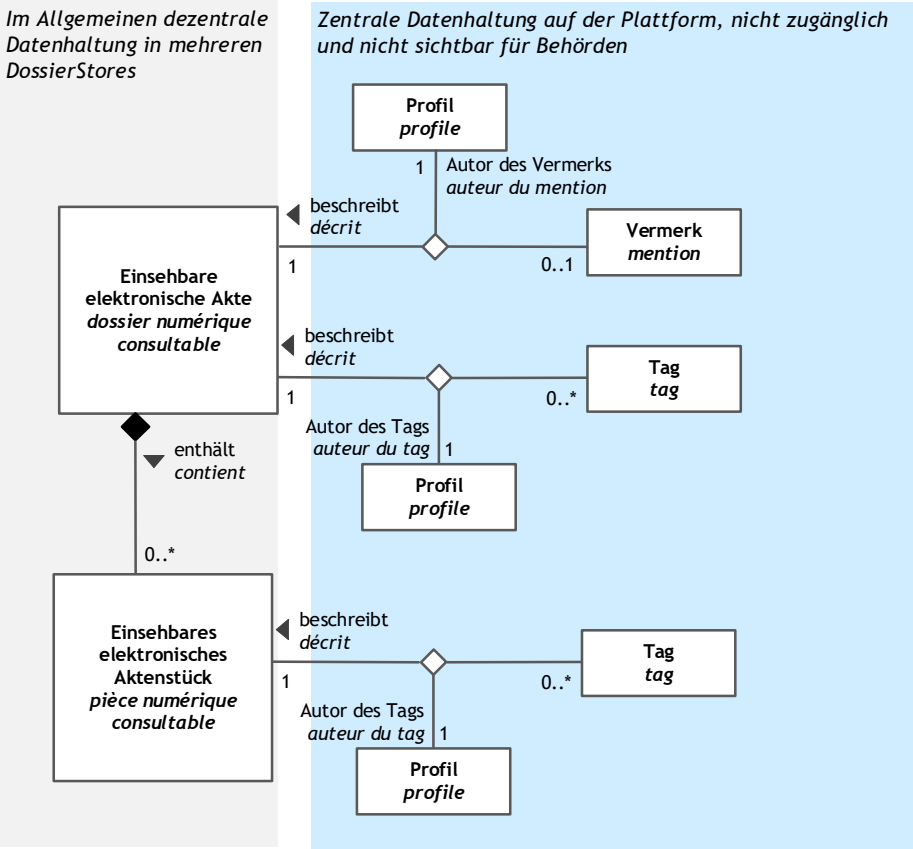


Abbildung 32: Vermerke und Tags – Verteilte Datenhaltung

Mit dem Löschen der Akte (AkteID) werden auch entsprechende Tags und Vermerke entfernt.

Hinweis: Zur Zeit der Ausschreibung ist noch offen, ob solche Tags und Vermerke zur eigentlichen Aufgabe des ERV und eAE gehören. Deshalb werden Tags und Vermerke in der Ausschreibung als Option behandelt.

7 Technische- und Betriebsarchitektur

Dieses Kapitel dient als Startpunkt die Detailierung der technischen Architektur in der Umsetzung. Die Rahmenbedingungen, die Anforderungen wie auch betriebliche und sicherheitsrelevante Aspekte sind darin beschrieben. Während der Umsetzung soll dieses Kapitel initial übernommen werden und fortlaufend dem neusten Stand angepasst werden.

7.1 Cloud Operating Model

Prinzip 14 fordert, dass die Plattform im Cloud Operating Model gemäss dem Prinzip von Cloud Native gebaut wird. D.h. sämtliche Services sind für die Cloud gebaut mit entsprechenden Konzepten und Patterns einer cloud-ready IT-Architektur.

- Applikatorische Komponenten der Plattform werden als Functions oder Container-Images paketiert und auf einer entsprechenden PaaS- oder Container-Runtime Umgebung integriert. Damit kann ein hoher Standardisierungs- und Automatisierungsgrad sowie die Entkoppelung fachlicher Abläufe von benötigten Infrastrukturservices erreicht werden.
- Die Laufzeitumgebung für applikatorische Services ist eine OCI und Docker kompatible und vollständig orchestrierte Container Runtime (PaaS)
- Alle applikatorischen Komponenten werden durchgängig gemäss Cloud Native Prinzipien (u.a. 12-factor-app methodology) gebaut und konfiguriert.
- Zusätzliche Infrastruktur-Services (Datenbanken, Message Queues, Blob-Storage, etc.) werden, wenn möglich, als PaaS Services eingebunden. Aus Gründen von Komplexität, Skalierbarkeit und Kosten ist der Bau von dedizierten IaaS Ressourcen zu vermeiden.
- Softwareentwicklung, Bereitstellung, Testing und Integration erfolgen entlang von CI/CD über entsprechende CI/CD Pipelines (Continuous Integration und Continuous Delivery). Das Deployment erfolgt ebenfalls über die CI/CD Pipeline kann bei Bedarf aber in einem manuellen Schritt erfolgen.
- Konfiguration von Infrastruktur- und Softwarekomponenten folgen den Ansätzen von infrastructure-as-code und configuration-as-code um jederzeit die Nachvollziehbarkeit von Änderungen an der Plattform-Komponenten zu gewährleisten.
- Die Testautomatisierung erfolgt entlang der Testpyramide ("Unit -> Component -> Integration -> API -> E2E"). Bis zur Stufe E2E laufen die Tests automatisiert in der entsprechenden CI/CD Pipeline.
- Das Deyployment von Applikations- und Infrastrukturkomponenten soll unterbrechungsfrei stattfinden. Dazu werden entsprechende always-on Patterns verwendet.
- Die Skalierung sämtlicher Ressourcen erfolgt dynamisch und kann on-demand an ändernde Lastverhältnisse angepasst werden.

Durch die genannten Prinzipien verspricht man sich folgende Vorteile:

- Entkoppelung einzelner Services als separat deploybare und betreibbare Einheiten. Dadurch rasche Entwicklungszyklen sowie einfache Wartung.
- Standardisierung von Deploymenteinheiten. Weniger Fehleranfällig.
- Die Anpassung und Erweiterung durch neue Features werden einfacher und flexibler (agiler) möglich.
- Automatisierungstechniken wie kontinuierliche Integration & Bereitstellung wird möglich.
- Unterstützung von agilen Projekt- und Organisationsmethoden wie DevOps Prinzipien.
- Die unabhängigen Komponenten können für andere Projekte/Services/Features wiederverwendet werden.
- Codes und Applikationen sind zugänglicher für Mitarbeiter, die nicht Teil der Entwickler-Teams sind.
- Einzelne Software-Komponenten lassen sich einfacher testen (automatisiertes Testen).
- Dynamische Skalierung von Ressourcen sowie unterbrechungsfreie Wartungs- und Deployment Prozesse.

7.2 Mandantenfähigkeit

Die Komponenten mit den Kopien der einsehbaren Akten (DossierStore) und den zugehörigen Einsichtsrechten, sowie die Mailboxen der Justizbehörden für das Zwischenspeichern der Eingaben können und sollen mandantenfähig realisiert werden. Die Konfiguration der Schnittstellen zu den Mandanten (Justizbehörden) ermöglicht insbesondere:

- flexible Anpassung an Spezialitäten der einzelnen angeschlossenen Justizbehörden können von anderen Behörden entkoppelt betrachtet und entwickelt werden (spezifischen API Mappings, Konfigurationen, Sicherheitsmerkmale, etc.)
- Zugriff auf Daten für Helpdesk, sowie Logfiles pro Mandanten können unterschiedliche Zugriffsrechte beinhalten.

- die Verschlüsselung der Daten mit mandantenspezifischen Schlüsseln (anstelle eines Masterschlüssel für die Plattform). Im Fall einer Sicherheitskompromittierung der Plattform sind die Bereiche der einzelnen Behörde getrennt.

Folgende Abbildung illustriert das Level der Mandantenfähigkeit: Die Daten der Mandanten (Behörden) können (müssen aber nicht) in eigenen Zonen mit eigener Bewirtschaftung sein. Dies beinhaltet auch eigene kryptographische Schlüssel.

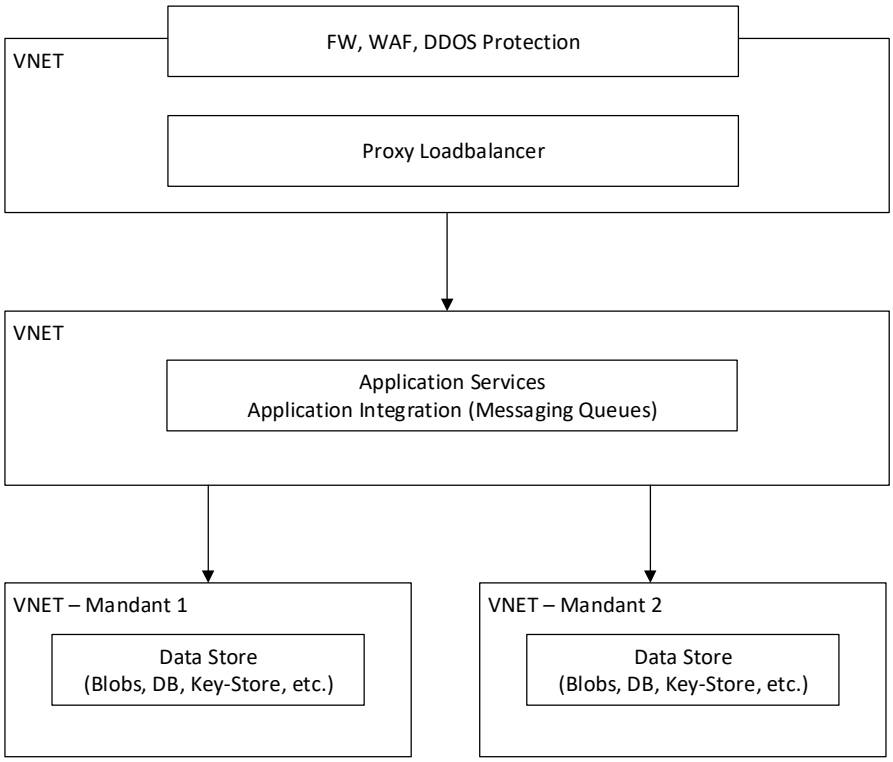


Abbildung 33: Mandantenfähigkeit auf Data Integration Level

7.3 Administrative Prozesse und Benutzer Support

Der fachliche Support durch den Services Desk wie auch 2nd level support haben einen Web-Zugriff auf die Plattform. Aus administrativen Prozessen können so Mutationen von Daten und Konfigurationen vorgenommen werden, die Logs sind über den Web-Zugriff einsehbar, sowie auch das gesamte Monitoring der Services. Diese Zugriffe erfolgen gemäss denselben Zugriffspfaden wie dies auch für die 'regulären' Benutzer gilt. Damit soll insbesondere Folgendes erreicht werden:

- Mitarbeiter der Betriebsgesellschaft und des Service Desks sowie Benutzer haben alle dieselbe Sicht auf die Funktionalität. Es gibt keine Hintertüren mit anderen fachlichen Werkzeugen. Mutation aus administrierten Prozessen und selbstadministrierten Prozessen durchlaufen dieselben Validierungen in der Software.
- Damit ist eine Trennung des fachlichen Supports von den Infrastrukturdienstleitungen des technischen Betreibers gewährleistet.
- Wir gehen davon aus, dass der technische Betreiber ein Service Management Tool bietet, welches die betrieblichen Supportprozesse (Problem- und Incident Management, etc.) abbildet und auswerten lässt. Wir gehen im Weiteren davon aus, dass eine Integration dieses Tools über die technische Architektur und die APIs einfach zu gestalten ist (z.B. Übernahme von Daten aus Profilen für Tickets).

7.4 Serviceverfügbarkeit

Ein Versprechen der elektronischen Akte ist, dass Berechtigte zeit- und ortsunabhängig Zugriff auf die Akten haben. Implizit ist damit eine 7x24 Verfügbarkeit der Plattform angesprochen. Gleichzeitig ist die Fristproblematik für Verfahrensbeteiligte sehr kritisch und hat in der Vergangenheit der Digitalisierung im Rechtsverkehr eher geschadet.

Für die ersten Tests der Plattform ist aber naturgemäss eine dauernde Verfügbarkeit der Plattform nicht wirtschaftlich. Wir gehen momentan von folgenden Annahmen aus:

- Der technische Betrieb kann die Latenz und Servicezeiten der Plattform jederzeit messen und geeignete Massnahmen einleiten, ohne ein vertieftes fachliches Knowhow zu besitzen.
- Sollte ein fachlicher Fehler die Verarbeitung vor 24.00 Uhr behindern (dieser Fall ist für die Anwaltschaft bezüglich Einhaltung von Fristen kritisch), dann muss der technische Betreiber diesen Fakt in erweiterten Servicezeiten nachweisen.
- **Die Verfügbarkeiten und Skalierbarkeit** der Plattform muss einfach anpassbar sein. Das Datenvolumen kann je nach Geschwindigkeit des Digitalisierungsfortschrittes in der Schweiz schneller oder weniger schnell anwachsen. Die Provisionierung von Speicherplatz oder Skalierung in der Rechenleistung soll einfach möglich sein. Die Skalierung von Services bei grösser Last soll durch Instanziierung weiterer Container einfach möglich sein (Skalierbarkeit und Resilienz).

7.5 Sicherheit

Für die konkrete Gestaltung der technischen Architektur sind folgende Annahmen zentral:

- Der technische Betreiber hat ein Security-Operation-Center, welches insbesondere Unregelmässigkeiten im Verhalten (und der Nutzung) der Plattform erkennt. Dieser Aspekt ist heikel, da er sowohl technisches als auch vertieftes fachliches Verständnis voraussetzt. Siehe dazu die Massnahme (3) aus dem ISDS Konzept. Technisch bedeutet dies zum Beispiel, dass Kontextinformationen aus den Web-Sessions mit Daten aus der Plattform verknüpf werden müssen. Zur Illustration: prinzipiell ist ein Zugriff auf ein Aktenstück aus dem Ausland heikel, dies ist aber nicht der Fall, wenn der Verfahrensbeteiligte ein Grenzgänger ist.
- Sicherheitsrelevante Unregelmässigkeiten werden vom technischen Betreiber erkannt und klassifiziert. Je nach Schweregrad der Risikos erfolgt die Bearbeitung und Behandlung dieser Unregelmässigkeiten meist zusammen mit den Betriebsverantwortlichen auf fachlicher Seite im Rahmen von regulären Updates der Plattform oder bei dringenden Problemen durch entsprechende Priorisierung aller Beteiligten.

7.6 Service Transition

Für den Einführung von neuen Features und Patches der Plattform respektive Updates oder Upgrades der unterliegenden Cloud Umgebung gehen wir von folgenden Annahmen aus:

- Minor Releases zeichnen sich dadurch aus, dass sie wenig Regressionsrisiko haben. Sie werden insbesondere auch für das Einspielen von Fehlerkorrekturen eingesetzt und verursachen keinen Serviceunterbruch. Wir rechnen mit täglich bis wöchentlich einzuspielenden Minor Releases.
- Major Releases beinhalten neue Funktionen, die auch nicht rückwärtskompatible Änderungen für Endbenutzer beinhalten oder anspruchsvolle Datenmodelländerungen. Ihnen gehen umfangreiche Tests voraus, sie sind von Releasenotes begleitet. Sie bedingen eine erhöhte Planung.
- Für Tests sind diverse Umgebungen vorzusehen: Testumgebungen mit definierte Referenzdatenset, Testumgebung für IT-Behörden oder Hersteller von Anwaltssoftware für Validierung des ‘nächsten Releases’, Umgebungen für Datenmigrationen, etc.
- Ein etablierter Change- und Release Prozess gibt nachvollziehbar Auskunft über bevorstehende und durchgeführte Änderungen an Infrastruktur und Software Komponenten (inkl. Change-log und Release-Notes).

8 Anhänge

8.1 Gesetzlich geforderte Funktionalitäten

In diesem Anhang werden die im Entwurf der Gesetzlichen Grundlage geforderten Funktionalitäten summarisch aufgelistet:

- Art. 17 – Adressverzeichnis: Siehe den Business Service 3.3 und die fachlichen Konzepte in Kapitel 4.2 über Profile
- Art. 18 – Benutzeroberfläche und Schnittstelle zu Fachapplikationen: Siehe Kapitel 6.1 über die bereitzustellenden APIs und die Einbettung des Web Portals in Abbildung 27.
- Art. 19 – Authentifizierung der Benutzerinnen und Benutzer: Siehe Kapitel 4.1.3 über digitale Identitäten
- Art. 20 – Ausnahmen zur Authentifizierung: Konzept der 'Mitarbeiter' (siehe Kapitel 4.1.1.4) sowie APIs und technische Keys (Kapitel 6.1).
- Art. 21 – Ablauf der Übermittlung: Siehe den Business Services 3.2 und die Beschreibung der Eingabe und der Zustellung im Kapitel 4.4.
- Art. 22 – Zusätzliche Benachrichtigungen: Siehe Kapitel 4.2.2 über Benachrichtigungsadressen und das Auslösen dieser Benachrichtigungen in den Sequenzdiagrammen über die Eingabe (Abbildung 13) und die Zustellung (Abbildung 16).
- Art. 23 – Validator: siehe Kapitel 6.4.
- Art. 24 – Gruppenverwaltung. Für die Gruppenverwaltung gibt es die Profile einer Organisation (Siehe Kapitel 4.1.1.2) und die Verfahrensspezifisch Delegationsmöglichkeiten (Kapitel 4.4).
- Art 25 – Fristen: Die Einhaltung der Fristen kann über die entsprechenden Quittungen (Kapitel 6.3) geprüft werden. Bei Nicht-Verfügbarkeit oder -Erreichbarkeit der Plattform kann ein entsprechender Nachweis erbracht werden.

8.2 Abbildungen und Tabellen

Abbildungen

Tabellen

8.3 Abkürzungen

API	Application Programming Interface
BGEID	Bundesgesetz über elektronische Identifizierungsdienste (E-ID-Gesetz, BGEID)
BGFA	Bundesgesetz über die Freizügigkeit der Anwältinnen und Anwälte (Anwaltsgesetz, BGFA)
BUR	Betriebs- und Unternehmensregister
eEA	elektronische Akteneinsicht
ERV	Elektronischer Rechtsverkehr
HTTP	Hypertext Transfer Protokoll. Wikipedia: http://bit.ly/wikipedia-http
IANA	Internet Assigned Numbers Authority
JWT	JSON Web Token
mTLS	mutual Transport Layer Security
örK	öffentlich-rechtliche Körperschaft
StPo	Strafprozessordnung
TLS	Transport Layer Security. Wikipedia: http://bit.ly/wikipedia-tls
UID	UnternehmenID. Identifikator für Unternehmen aus dem BUR
UML	Unified Modeling Language
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
ZertES	Bundesgesetz über die elektronische Signatur

ZMG	Zwangsmassnahmengericht

8.4 Referenzen

VE-BEKJ	Vernehmlassungsentwurf für das Bundesgesetz über die Plattform für die elektronische Kommunikation in der Justiz (E-Justice-Gesetz, BEKJ). November 2020.
BGFA	Bundesgesetz über die Freizügigkeit der Anwältinnen und Anwälte (Anwaltsgesetz, BGFA). admin.ch
eCH-0011	Steimer, Thomas; Stingeli, Martin (2014): eCH-0011 - Datenstandard Personendaten. Hg. v. Verein eCH. Online verfügbar unter https://bit.ly/3adm589, zuletzt geprüft am 11.08.2020.
eCH-0039	Siegrist, Beat; Wittwer, Daniel (2017): eCH-0039 E-Government-Schnittstelle für Dossiers und Dokumente. Verein eCH. Online verfügbar unter https://bit.ly/33NYr0x, zuletzt geprüft am 11.08.2020.
eCH-0044	Steimer, Thomas; Stingelin, Martin (2014): eCH-0044 - Datenstandard Austausch von Personenidentifikationen. Hg. v. Verein eCH. Online verfügbar unter https://bit.ly/2PIJeWp, zuletzt geprüft am 11.08.2020.
eCH-0058	Steiner, Thomas; Stingelin, Martin (2014): eCH-0058 Schnittstellenstandard Meldungsrahmen. Hg. v. Verein eCH. Online verfügbar unter https://bit.ly/ech-0058, zuletzt geprüft am 14.08.2020.
eCH-0219	eCH-0219. IAM Glossar. Version 1.0. November 2018. https://bit.ly/3hkVjgv
K-GBZ	Konzept geregeltes Behördenzertifikat / Zusammenarbeit mit dem eGov Signaturvalidator. V.1.0 vom 30.12.2019. Kopie im Wiki unter: https://wiki.justitia40.ch/x/eADiAQ
PbD	Ann Cavoukian, Privacy by Design, The 7 Foundational Principles. Verfügbar unter: https://iapp.org/media/pdf/resource_center/pbd_implement_7found_principles.pdf
RFC2045	Freed, N.; Borenstein, N. (1996): Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies. IETF. Online verfügbar unter https://tools.ietf.org/html/rfc2045, zuletzt geprüft am 14.08.2020.
RFC4122	Leach, P.; Mealling, M.; Salz, R. (2005): RFC 4122 - A Universally Unique IDentifier (UUID) URN Namespace. Hg. v. IETF. Online verfügbar unter https://tools.ietf.org/html/rfc4122, zuletzt geprüft am 02.09.2020.

8.5 Unified Modeling Language

Das vorliegende Dokument verwendet die formale Notation der *Universal Modelling Language* (UML)[25], um Konzepte mit ihren wechselseitigen Beziehungen und ihren reichhaltigen Attributen zu beschreiben.

Die UML umfasst eine Notation für **Konzepte** (manchmal auch als **Typen** oder **Klassen** bezeichnet).

[25] Siehe Wikipedia für weiterführende eine Übersicht und weiterführende Informationen (Literatur, etc.): https://de.wikipedia.org/wiki/Unified_Modeling_Language

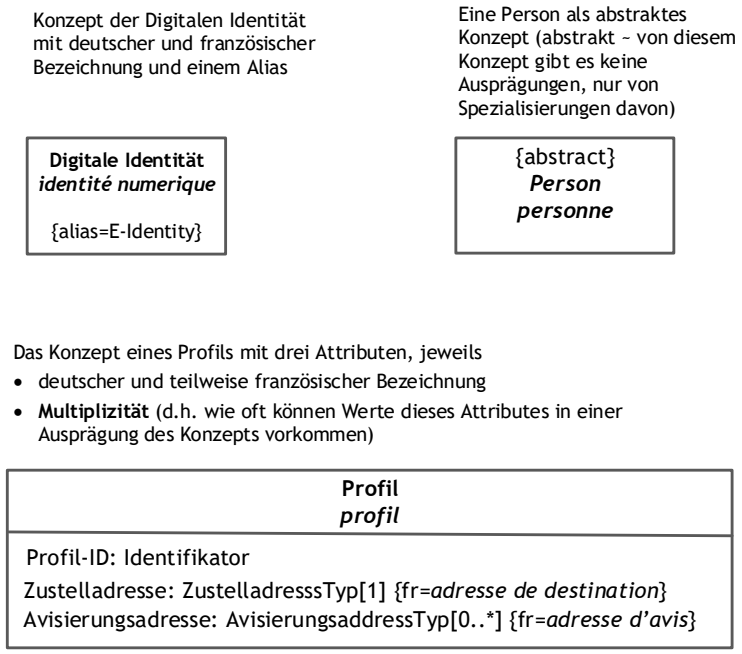


Abbildung 34: Notation – Konzepte

Die Notation kann darstellen, dass ein Konzept K2 eine Spezialisierung des Konzepts K1 ist. Umgangssprachlich kann man diese Beziehung wie folgt lesen: «K2 ist etwas in der Art von K1». Oder im folgenden Beispiel: «Juristische Person ist eine Art Organisation», «Sowohl Organisation als auch natürliche Person sind eine Art Person».

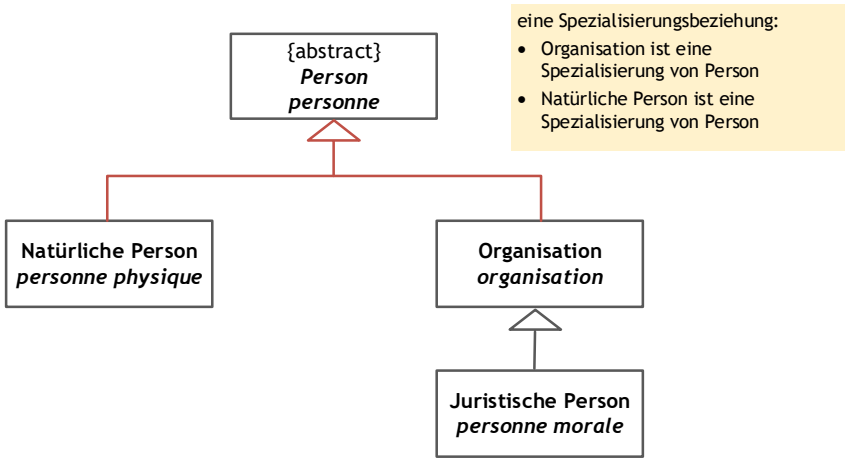


Abbildung 35: Notation – Spezialisierung

Um wechselseitige Beziehungen zwischen Konzepten darzustellen, verwendet die Modellierungssprache **Assoziationen**.

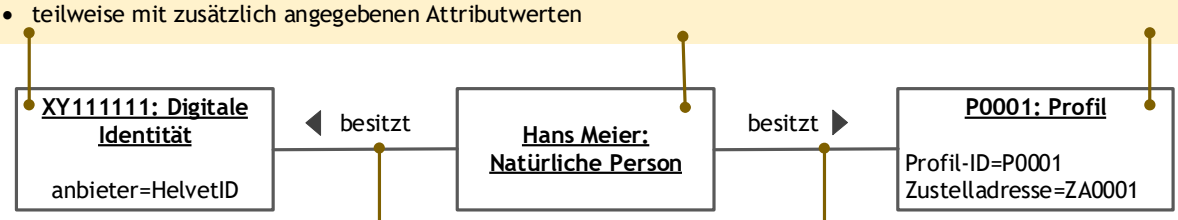
eine Assoziation zwischen zwei Konzepten, mit einem **«Lesehinweis»** und **«Leserichtung»** und zwei **Multiplizitäten**, hier:

- «Eine Natürliche Person ist Mitarbeiter von keiner oder mehrerer Organisation»
- «Keine oder mehrere Personen sind Mitarbeiter einer Organisation»

Abbildung 36: Notation – Assoziationen

Im Dokument werden Ausschnitte des konzeptionellen Modells mit konkreten Beispielen illustriert und validiert. Dafür setzt das Dokument **Objektdiagramme** in der folgenden Form ein:

- drei Objekte, das heisst Instanzen der Konzepte Digitale Identität, Natürliche Person und Profil.
- je mit einer Bezeichnung
- teilweise mit zusätzlich angegebenen Attributwerten



- zwei Links, das heisst Instanzen von Assoziationen

Abbildung 37: Notation – Objektdiagramme

Als Identifikation verwenden wir für Klassen und Objekte die Konvention «Name»ID. Daraus soll jedoch nicht abgeleitet werden, dass diese Identifikatoren so im spezifischen Datenmodell oder den Interfaces vorkommen sollen.