PROJEKT
Justitia 4.0

Anhang 8 ISDS-Konzept für die Plattform Justitia.Swiss

Inhaltsverzeichnis

Abbildungen

Tabellen

1 Einleitung

1.1 Präambel

Die vorliegende Version des ISDS-Konzeptes ist ein durch die Gesamtprojektleitung genehmigtes Projektdokument zur Unterstützung der Angebotsphase (AP) für Los 1 (Entwicklung der Plattform «Justitia.Swiss») sowie für Los 2 (Technischer Betrieb der Plattform «Justitia.Swiss»). Die in diesem Dokument geforderten Sicherheitsmassnahmen sind für die Ausschreibung zu berücksichtigen und im Architekturdokument und den Anforderungen aufgenommen.

Das ISDS-Konzept für die Plattform Justitia.Swiss wird im weiteren Projektverlauf an veränderte Rahmenbedingungen und neue Erkenntnisse angepasst werden. Die folgenden bereits absehbaren Ereignisse werden voraussichtlich zu einem Anpassungsbedarf führen:

- Entwicklungspartner und Betriebspartner sind bekannt;
- Der präzise Scope für die Umsetzung des MVP der Plattform ist definiert (insbesondere Kapitel 2.4, 2.5 und 2.6):
  - Die aufgeführten Geschäftsvorfälle stellen keine zu entwickelnden fachlichen Anforderungen dar, sondern dienen der Herleitung relevanter Schutzmassnahmen.
- Das Bundesgesetz über die Plattform für die elektronische Kommunikation in der Justiz (BEKJ) [Ext1]sowie dessen Ausführungsrecht liegen vor;
- Das Ausführungsrecht für das Informationssicherheitsgesetz (ISG) [Ext2] liegt vor;
- Das Ausführungsrecht für das revidierte Datenschutzgesetz (nDSG) [Ext3] liegt vor.

1.2 Ausgangslage

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 sichere zentrale Plattform (Justitia.Swiss) austauschen können.

Das Projekt wird die zentrale Plattform, die in Zukunft die elektronische Akteneinsicht (eAE) und den elektronischen Rechtsverkehr (ERV) in der Schweizer Justiz unterstützen wird, am Markt beschaffen. Das vorliegende ISDS-Konzept ist ein Teil der dafür nötigen Ausschreibungsunterlagen.

1.3 Zielsetzung und Rahmenbedingungen

Bei der Digitalisierung der Schweizer Justiz müssen höchste Anforderungen an die Informationssicherheit und den Datenschutz (ISDS) erfüllt werden. Das vorliegende ISDS-Konzept ist das konstituierende Dokument im Bereich der Informationssicherheit und des Datenschutzes und soll insbesondere die folgenden Fragen beantworten:

- Welches sind die zu berücksichtigenden respektive optionalen rechtlichen Anforderungen?
- Wie gross ist der Schutzbedarf der geplanten Lösung?
- Was sind mögliche Schadenszenarien und was wäre die Tragweite von Schadenereignissen?
- Welche Sicherheitsrisiken sind zu adressieren?
- Welche Sicherheitsmassnahmen (organisatorisch, applikatorisch und technisch) sind zu treffen?
- Welche Restrisiken verbleiben nach Umsetzung dieser Massnahmen?

Die Sicherheitsmassnahmen sollen sicherstellen, dass die Angriffsflächen der technischen Lösung minimiert («*Security by Design*») und die organisatorischen Grundlagen für ein funktionierendes Sicherheitsmanagement geschaffen werden. Dabei müssen sie mit den Vorgaben aus dem zukünftigen Bundesgesetz über die Plattform für die elektronische Kommunikation in der Justiz (BEKJ) und dessen Ausführungsrecht konform sein, soweit dies anhand der heute bekannten Informationen möglich ist.

Das ISDS-Konzept orientiert sich an den per anfangs 2021 aktualisierten Vorgaben von HERMES.

1.4 Umfang (Scope)

Der Scope des vorliegenden ISDS-Konzeptes umfasst die Plattform Justitia.Swiss mit ihren Daten, Benutzergruppen, Systemkomponenten, Schnittstellen und Anwendungsfällen gemäss dem Kapitel 2 «Systembeschreibung und Schutzobjekte». Dies sind insbesondere:

- Alle auf der Plattform verarbeiteten oder über die Plattform transferierten Daten;
- Die operativen Anwendungsfälle (z.B. Eingabe, Zustellung), die administrativen Anwendungsfälle (z.B. Organisationen verwalten, Benutzer verwalten) sowie der Systembetrieb;
- Die Applikation Plattform Justitia.Swiss mit ihren Komponenten und den Schnittstellen zu anderen Applikationen (z.B. elektronische Akte, Identity Provider, Siegel-Service).

1.5 Abgrenzung

Abgegrenzt sind insbesondere:

- Die IT-Systeme von verfahrensleitenden Behörden und von verfahrensbeteiligten Organisationen (inklusive der zukünftigen Justizaktenapplikation JAA);
- Die Endgeräte von teilnehmenden Organisationen und Privatpersonen.

1.6 Governance

Das ISDS-Konzept für die Plattform Justitia.Swiss wird vom CISO als ISDS-Verantwortlichen des Projektes Justitia 4.0 verantwortet und gepflegt.

1.7 Aufbau des Dokuments

- Kapitel 1 ist die vorliegende Einleitung;
- Kapitel 2 «Systembeschreibung und Schutzobjekte» zeigt das Gesamtsystem und beschreibt die Datenbestände, Benutzergruppen, Systemkomponenten, Schnittstellen und Anwendungsfälle;
- Kapitel 3 «Schutzbedarfsanalyse (Schuban)» enthält das Ergebnis der Schutzbedarfsanalyse gemäss HERMES;
- Kapitel 4 «Risikoanalyse» ist das zentrale Kapitel des ISDS-Konzeptes. Es identifiziert die relevanten Sicherheitsrisiken entlang der Schutzobjekte und bewertet diese Risiken in Bezug auf die Auswirkung und die Eintrittswahrscheinlichkeit eines Schadenfalles;
- Kapitel 5 «Sicherheitsmassnahmen» beschreibt die organisatorischen, applikatorischen und technischen Sicherheitsmassnahmen, mit denen die Risiken auf ein tragbares Mass reduziert werden;
- Kapitel 6 «Restrisikobetrachtung» beschreibt und bewertet die Restrisiken, die nach Umsetzung aller Sicherheitsmassnahmen verbleiben.
- Im Anhang A sind wichtige Abkürzungen und Begriffe erläutert.

1.8 Externe Dokumente

[Ref]	Titel	Autor	Version	Datum
[Ext1]	Bundesgesetz über die Plattform für die elektronische Kommunikation in der Justiz (BEKJ)	Bundesversammlung	N/A	N/A
[Ext2]	Informationssicherheitsgesetz (ISG)	Bundesversammlung	N/A	N/A
[Ext3]	Revidiertes Datenschutzgesetz (nDSG)	Bundesversammlung	N/A	N/A
[Ext4]	ZertES	Bundesversammlung	N/A	01.01.2017
[Ext5]	Geschäftsbücherverordnung, GeBüV	Bundesrat	N/A	01.01.2013
[Ext6]	HERMES 2021 Vorlagen für Schutzbedarfsanalyse, ISDS-Konzept und Risikoanalyse	NCSC	4.4	April 2021
[Ext7]	Kriterienkatalog Zustellplattformen	BJ	2.0	16.09.2014
[Ext8]	Qualitätsmodell zur Authentifizierung von Subjekten (eCH-0170)	Verein eCH	2.0	13.09.2017
[Ext9]	Qualitätsmodell der Attributwertbestätigung zur eID (eCH-0171)	Verein eCH	1.0	04.09.2014
[Ext10]	Gestaltungsprinzipien für die Identitäts- und Zugriffsverwaltung (IAM) (eCH-0107)	Verein eCH	3.0	14.01.2019
[Ext11]	Digital Identity Guidelines (NIST SP 800-63-3)	NIST	3.0	Juni 2017
[Ext12]	IKT-Grundschutz in der Bundesverwaltung	NCSC	4.6	April 2021
[Ext13]	Verordnung über den Schutz von Informationen des Bundes (ISchV)	Bundesrat	N/A	01.01.2021

Tabelle 1: Input-Dokumente – Externe Dokumente

1.9 Ansprechpartner und Verantwortlichkeiten

Ansprechpartner und Verantwortlichkeiten gemäss HERMES Vorlage für ISDS-Konzepte ([Ext6]):

Rolle	Organisation
Anwendungsverantwortlicher	Justizkonferenz und KKJPD (paritätisch)
Inhaber der Daten	Bund und Kantone
Systembetreiber (Leistungserbringer)	Öffentlich-rechtliche Körperschaft (örK), in Gründung
Projektleiter Leistungsbezüger	Justizkonferenz und KKJPD (paritätisch)
Projektleiter Leistungserbringer	KKJPD
ISDS-Verantwortlicher des Projekts	KKJPD
Datenschutzverantwortlicher des Projekts	KKJPD

Tabelle 2: Ansprechpartner und Verantwortlichkeiten

2 Systembeschreibung und Schutzobjekte

Die Systembeschreibung basiert auf der Architektur der Plattform Justitia.Swiss (Anhang 7 der Ausschreibung - Architektur Plattform Justitia.Swiss). Bei Anpassungen der Architektur ist das ISDS-Konzept allfällig nachzuführen.

Abbildung 1 zeigt die beteiligten Akteure und Komponenten der Plattform Justitia.Swiss:

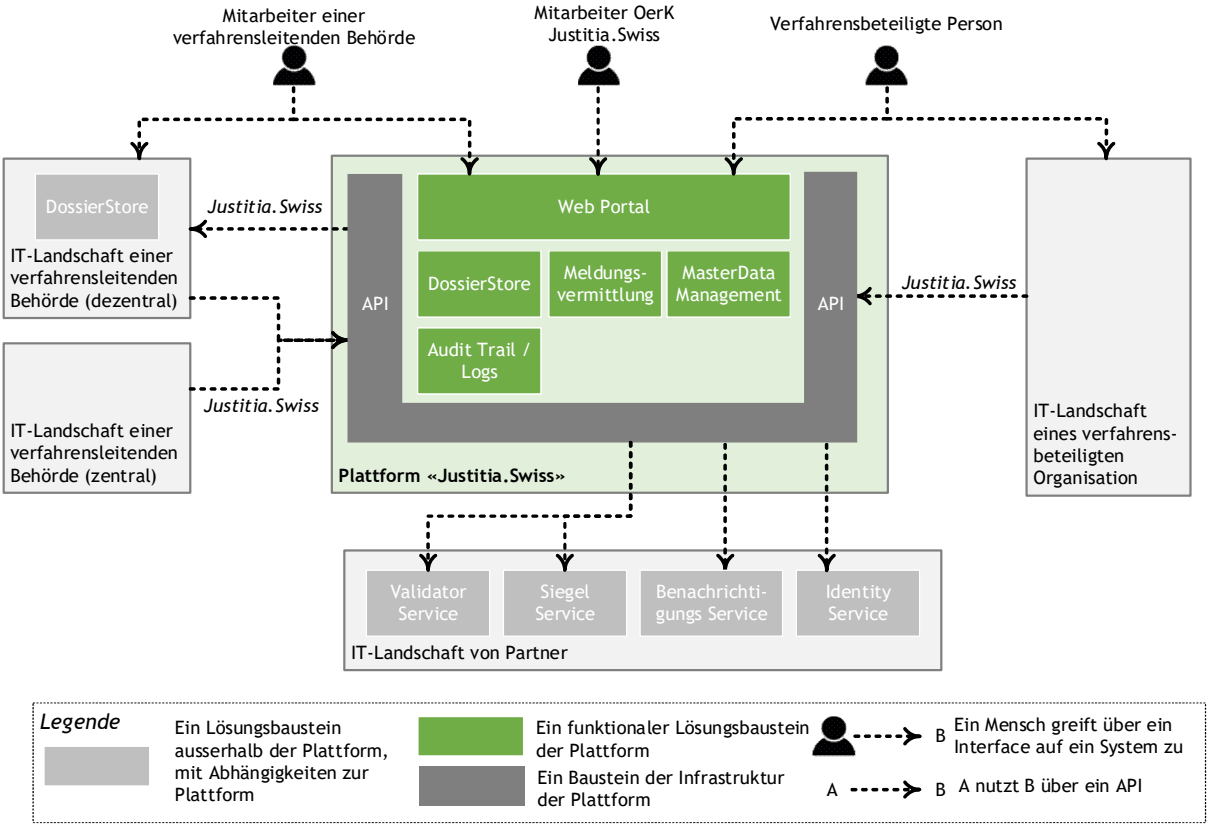

Abbildung 1: Systemübersicht Plattform Justitia.Swiss mit ihren Schnittstellen (Quelle: Anhang 7 der Ausschreibung - Architektur Plattform Justitia.Swiss)

2.1 Systemkomponenten

Die Plattform Justitia.Swiss umfasst die folgenden Komponenten:

- Ein Web-Portal für Mitarbeitende von verfahrensführenden Behörden, verfahrensbeteiligte Personen sowie Mitarbeitende der Betreibergesellschaft (für Administrationsarbeiten). Das Web-Portal hat auch einen Bereich für anonyme Benutzer mit öffentlich zugänglichem Inhalt.
- Eine Komponente DossierStore mit folgenden Funktionen:
  - Speichern und Prüfen der Berechtigungen für den Zugriff auf die einsehbaren elektronischen Aktenstücke (unabhängig davon, ob sie zentral oder dezentral gespeichert sind);
  - Speichern von Kopien der einsehbaren elektronischen Aktenstücke für verfahrensführende Justizbehörden, die dies wünschen;
  - Halten der Behörden und Aktennummern für alle Verfahren der Plattform.
- Die Komponente Meldungsvermittlung vermittelt und verwaltet die ausgetauschten Meldungen des elektronischen Rechtsverkehrs. Die Funktionalität basiert zu grossen Teilen auf einem Postfach je Teilnehmer.
- Die Komponente MasterData Management bietet Verwaltungsservices für die Stammdaten des Adressverzeichnisses.
- Die Komponente Audit Trail / Logs speichert die relevanten Ereignisse und bietet Sichten darauf, sowohl für die Teilnehmer als auch für den Betreiber der Plattform für statistische Auswertungen.

Die Plattform Justitia.Swiss bezieht die folgenden Services von entsprechenden Partnern:

- Der Benachrichtigungsservice versendet Benachrichtigungen, welche Beteiligte über den Status von Meldungen informieren.
- Der Validatorservice validiert die Siegel von Dokumenten.
- Der Siegelservice bringt auf Dokumente ein geregeltes elektronisches Siegel (nach ZertES [Ext4]) an.
- Der Identitätsservice liefert digitale Identitäten zuhanden des Adressverzeichnisses und authentifiziert die Benutzer vor ihrem Zugriff auf die Plattform. Für Mitarbeitende von Behörden kann dieser Identitätsservice von der IT-Landschaft der Behörden zur Verfügung gestellt werden.

Die Plattform Justitia.Swiss kommuniziert mit den IT-Systemen von verfahrensleitenden Justizbehörden, verfahrensbeteiligten Organisationen und Servicepartnern über Application Programming Interfaces (API). Grundsätzlich stehen alle Funktionen des Web-Portals auch über API zur Verfügung.

2.2 Daten

Tabelle 3 identifiziert die für das ISDS-Konzept relevanten Datenbestände mit dem Dateninhaber:

Datenobjekt	**Beschreibung**	**Inhaber**[1]
Eingabe	Dateien, die von einem Verfahrensbeteiligten bei einer Justizbehörde eingereicht werden.	Verfahrensbeteiligter
Zustellung	Eine Liste mit den Abrufadressen von Aktenstücken, die einem Verfahrensbeteiligten zugestellt wird. Die Zustellung berechtigt den Empfänger während ihrer Gültigkeitsdauer dazu, die aufgelisteten Aktenstücke sowie den Aktendeckel der Akte einzusehen.[2]	Verfahrensleitende Justizbehörde
Einsehbares elektronisches Aktenstück	Aktenstücke (inkl. Aktendeckel), die über die Plattform Justitia.Swiss eingesehen werden können. Sie sind in einem DossierStore entweder dezentral bei der verfahrensleitenden Justizbehörde oder zentral auf der Plattform gespeichert.	Verfahrensleitende Justizbehörde
Delegation	Die Weitergabe einer Berechtigung von einem delegierenden Profil an ein anderes Profil. Delegationen werden auf der Plattform verwaltet und können sowohl die Berechtigung zur Einsicht in eine oder mehrere Akten als auch die Berechtigung zur Nutzung von Funktionen und Daten der Plattform betreffen.	Öffentlich-rechtliche Körperschaft (örK)
Quittung	Eingangs- und Abrufquittungen zur Bestätigung der Durchführung eines ERV-Geschäftsvorfalles gemäss den Vorgaben des zukünftigen BEKJ.	Öffentlich-rechtliche Körperschaft (örK)
Adressverzeichnis	Das Verzeichnis aller Organisationen und natürlichen Personen, die über die Plattform Justitia.Swiss am elektronischen Rechtsverkehr (ERV) oder an der elektronischen Akteneinsicht (eAE) teilnehmen.	Öffentlich-rechtliche Körperschaft (örK)

[1] Der Inhaber ist hier die für die Sicherheit verantwortliche Organisation («Schutzobjektverantwortlicher»)

[2] In diesem Dokument bezeichnet 'Zustellung' die Informationen des 'Einsichtsrechts' und der eigentlichen 'Zustellung'.

Audit Trail	Aufzeichnung aller rechtsverbindlichen Ereignisse auf der Plattform Justitia.Swiss. Der Audit Trail erfüllt die Anforderungen, die in der Geschäftsbücherverordnung ([Ext5]) an das Journal zur chronologischen Erfassung aller verbuchten Geschäftsvorfälle gestellt werden.	Öffentlich-rechtliche Körperschaft (örK)
Log	Aufzeichnung aller technischen Vorgänge auf der Plattform Justitia.Swiss, die potentiell sicherheitsrelevant sind.	Öffentlich-rechtliche Körperschaft (örK)
Anschluss-Konfigurationen	Konfigurationsdaten für Umsysteme, die mit der Plattform Justitia.Swiss kommunizieren, wie beispielsweise: • Credentials und Adressen (URL) der über API angeschlossenen IT-Systeme von Justizbehörden und verfahrensbeteiligten Organisationen; • X.509 Zertifikate der akzeptierten Identity Provider; • Technische Anbindungsparameter von Siegel-Service und Mitteilungs-Service; • Kryptographische Schlüssel für die Verschlüsselung gespeicherten Daten des Mandanten (*bring-your-own-key*).	Öffentlich-rechtliche Körperschaft (örK)
Plattform-Konfiguration	Konfigurationsdaten der Plattform Justitia.Swiss, wie beispielsweise: • Der Signierschlüssel für das Plattform-Siegel; • Webserver-Zertifikate der Plattform; • Kryptographische Schlüssel für die Verschlüsselung gespeicherter Daten (*data at rest*).	Öffentlich-rechtliche Körperschaft (örK)

Tabelle 3: Daten im Scope der Plattform Justitia.Swiss

Tabelle 4 identifiziert Datenbestände, die nicht im Scope des ISDS-Konzeptes sind:

Daten	**Beschreibung**	**Inhaber**
Elektronische Akte	Die bei der verfahrensleitenden Justizbehörde geführte elektronische Akte.	Verfahrensleitende Justizbehörde
Kanzleiakte	Elektronische Akte, die von den Verfahrensbeteiligten für eigene Zwecke geführt wird.	Verfahrensbeteiligte (z.B. Anwaltskanzlei)
Login Credentials	Daten für die Authentifizierung von Benutzern (z.B. Passwörter oder kryptographische Schlüssel).	Identity Provider

Tabelle 4: Daten ausserhalb des Scope der Plattform Justitia.Swiss.

2.3 Benutzergruppen

Tabelle 5 identifiziert die für das ISDS-Konzept relevanten Benutzergruppen:

Benutzergruppe	Beschreibung	Beispiele
Justizvertreter	Mitarbeitende einer verfahrensleitenden Justizbehörde (juristisches und nicht juristisches Personal)	Richter, Staatsanwalt, Gerichtsschreiber, Kanzleimitarbeitender
Partei	Kläger und Beklagte in einem Verfahren (Privatpersonen und Mitarbeitende von juristischen Personen)	Zivilkläger, klagender Staatsanwalt, beschuldigte Firma und Person
Parteivertreter	Mitarbeitende einer Anwaltskanzlei (juristisches und nicht juristisches Personal)	Anwalt, Anwaltssekretär
Dritte	Andere Verfahrensbeteiligte, die zur elektronischen Akteneinsicht oder zum elektronischen Rechtsverkehr eingeladen werden.	Gutachter, Grundbuchamt, Strafvollzugsdienst
Justitia.Swiss Administrator	Administratives Personal bei der öffentlich-rechtlichen Körperschaft (örK)	Administrator des Adressverzeichnisses
Plattformbetreiber	Personal bei einem von der der örK mit dem technischen Betrieb der Plattform beauftragten Dienstleister	IT-Admin, Mitarbeitender beim Benutzersupport

Tabelle 5: Benutzergruppen

2.4 Operative Geschäftsvorfälle

Siehe Kapitel Präambel zwecks Einordnung der Geschäftsvorfälle im Ausschreibungsverfahren.

Detailbeschreibungen zu den operativen Geschäftsvorfällen finden sich im Anhang B: Detaillierte operative Geschäftsvorfälle.

SO1 Eingabe

Eine verfahrensbeteiligte Person stellt eine Eingabe einer zuständigen Justizbehörde rechtsgültig elektronisch zur Verfügung.

SO2 Zustellung

Eine Justizbehörde stellt einem Verfahrensbeteiligten ein oder mehrere Aktenstücke rechtsgültig elektronisch zur Verfügung, um einen Schritt im Verfahren oder das Verfahren selber abzuschliessen.

SO3 Akteneinsicht

Eine berechtigte Person nimmt elektronisch Einsicht in ein oder mehrere Aktenstücke.

SO4 Interaktion zwischen Justizbehörden

*Die Plattform Justitia.Swiss unterstützt auch den elektronischen Rechtsverkehr zwischen Justizbehörden. Die Architektur Plattform Justitia.Swiss (*Anhang 7 der Ausschreibung - Architektur Plattform Justitia.Swiss*) beschreibt im Kapitel 5 verschiedene Interaktionsmuster zwischen Behörden.*

SO5 Zentraler DossierStore als Service der Plattform Justitia.Swiss

Verfahrensleitende Justizbehörden, welche die Plattform Justitia.Swiss für die Speicherung der zugestellten und somit einsehbaren Akten im zentralen DossierStore verwenden, liefern bei der Zustellung auch die zuzustellenden Aktenstücke mit.

2.5 Administrative Geschäftsvorfälle

Siehe Kapitel Präambel zwecks Einordnung der Geschäftsvorfälle im Ausschreibungsverfahren.

Detailbeschreibungen zu den administrativen Geschäftsvorfällen finden sich im Anhang C: Detaillierte administrative Geschäftsvorfälle.

Abbildung 2 zeigt die relevanten Informationsobjekte der Plattform Justitia.Swiss (für Details: siehe Anhang 7 der Ausschreibung - Architektur Plattform Justitia.Swiss, Kapitel 4):

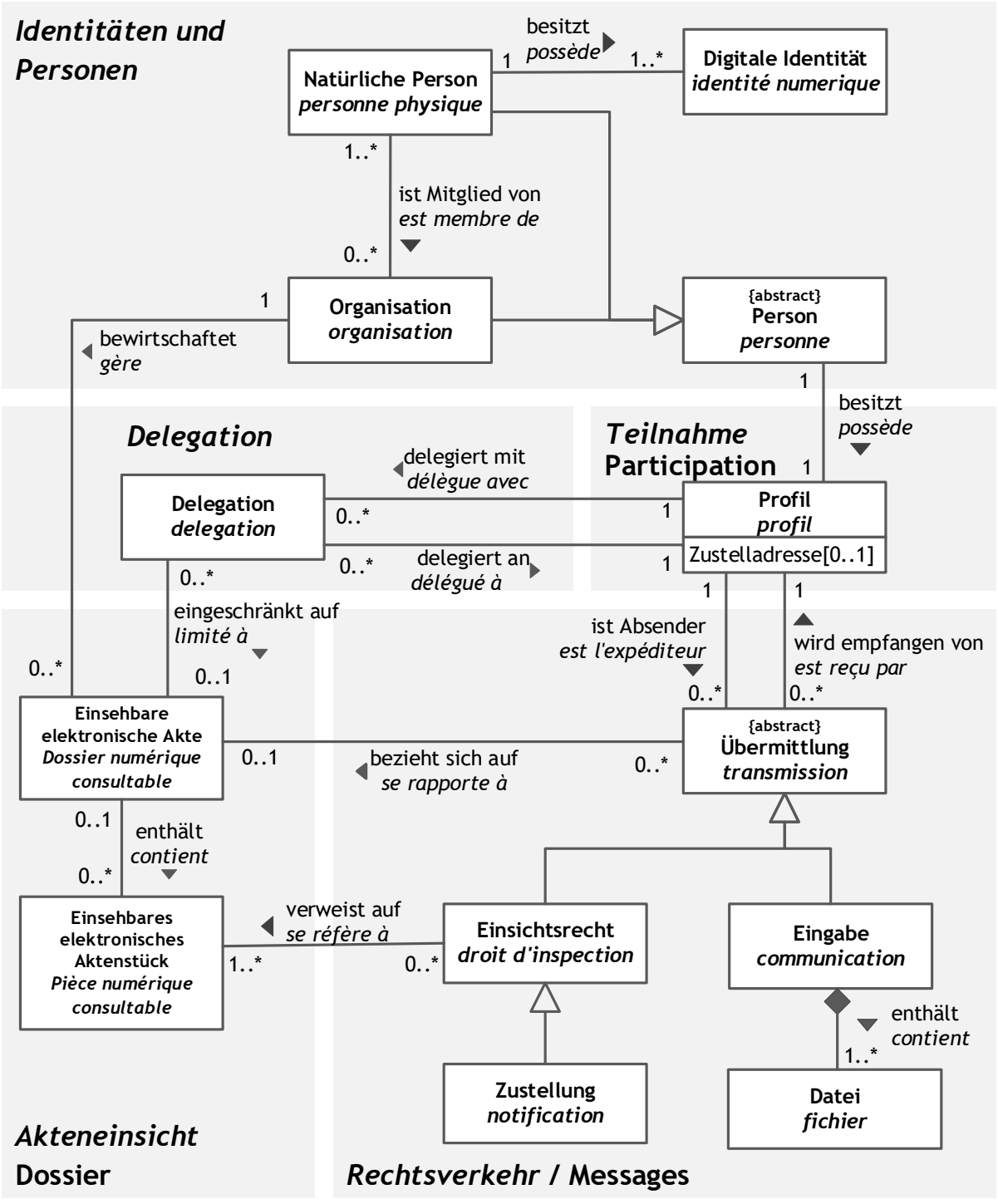

Abbildung 2: Konzeptionelles Informationsmodell (Quelle: Anhang 7 der Ausschreibung - Architektur Plattform Justitia.Swiss)

SO6 Organisationen verwalten

Die öffentlich-rechtliche Körperschaft (örK) verwaltet Organisationen im Adressverzeichnis der Plattform Justitia.Swiss, damit diese am ERV und an der eAE teilnehmen können.

SO7 Benutzer verwalten

Personen, welche die Plattform Justitia.Swiss benutzen wollen, registrieren sich mit einer digitalen Identität eines von der Plattform akzeptierten Identity Providers (IdP) selber im Adressverzeichnis.

SO8 Organisationszugehörigkeiten verwalten

Die Administratoren von Organisationen legen fest, welche natürlichen Personen zur Organisation gehören und welche Funktionen sie für die Organisation wahrnehmen.[3]

SO9 Plattform-Berechtigungen verwalten

Administratoren auf der Plattform Justitia.Swiss legen fest, welche Benutzer welche Funktionalitäten und Daten auf der Plattform Justitia.Swiss nutzen dürfen.

SO10 Delegationen verwalten

Teilnehmer delegieren eine ihrer Berechtigungen an einen anderen Teilnehmer.

[3] Hinweis für die nächste Überarbeitung des ISDS Konzepts. Der Prozess 'Organisation verwalten' muss unterteilt werden. Wir sollten unterscheiden zwischen (1) Organisationen für die die Mitglieder auf der Plattform verwaltet, resp. administriert werden und (2) Organisationen, deren Mitglieder durch einen externen IdP verwaltet werden. Im letzten Fall ist der IdP verantwortlich die korrekten Funktionen der Mitglieder zu liefern. Durch eine entsprechende Aufteilung des Prozesses werden die Risiken vor den Massnahmen reduziert (Security by Design).

2.6 Betriebsprozesse

Siehe Kapitel Präambel zwecks Einordnung der Geschäftsvorfälle im Ausschreibungsverfahren.

Detailbeschreibungen zu den Betriebsprozessen finden sich im Anhand D: Detaillierte Betriebsprozesse.

Abbildung 3 zeigt Operation Modell der Plattform Justitia.Swiss (für Details: siehe Anhang 9 der Ausschreibung - Service- und Betriebskonzept Justitia.Swiss):

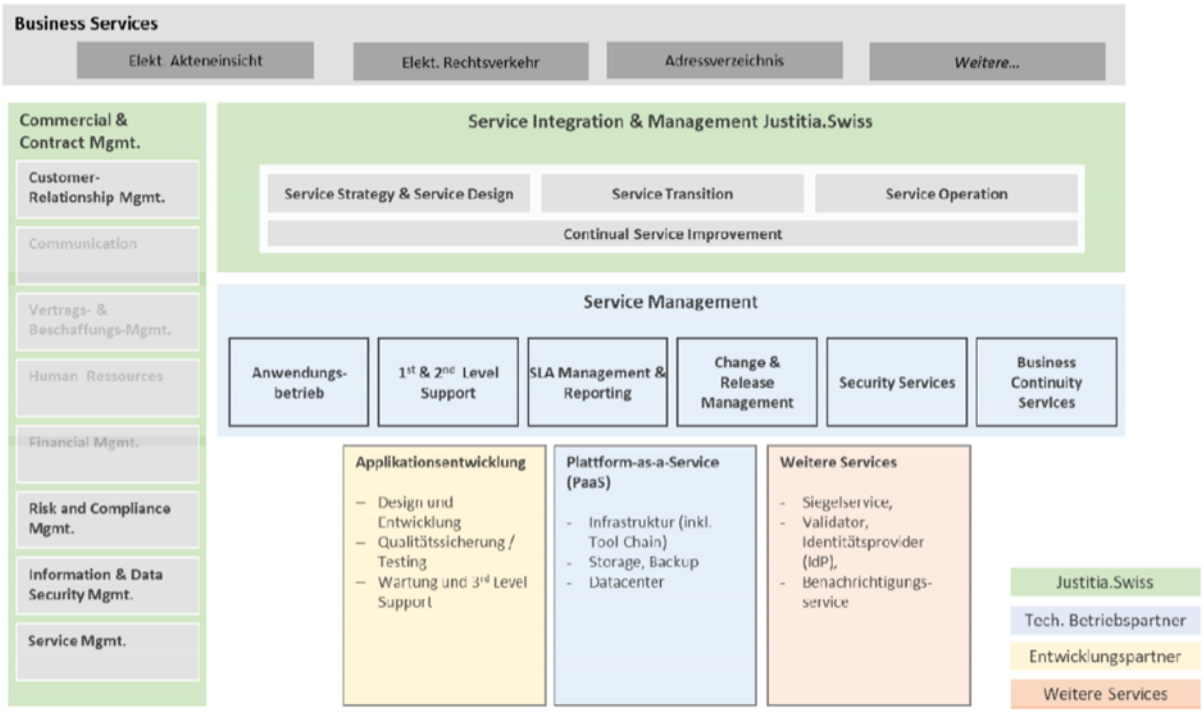

Abbildung 3: Justitia Operation Modell (Quelle: Anhang 9 der Ausschreibung - Service- und Betriebskonzept Justitia.Swiss)

Die Erbringung der Business Services orientiert sich an den ITIL Praktiken und am SIAM (Service Integration & Management) Operating Modell. Dabei bezeichnen die einzelnen Komponenten die Prozessgruppen, die in der jeweiligen Verantwortung von Justitia.Swiss liegen oder durch Partner zu erbringen sind. Justitia.Swiss stellt die nahtlose Integration der Dienstleister sicher mit dem Ziel, durchgängige Dienste zur Bearbeitung der Geschäftsvorgänge zu ermöglichen.

SO11 Service Management

Verschiedene Services im laufenden Betrieb werden durch Mitarbeitende der öffentlich-rechtlichen Körperschaft (örK) erbracht.

SO12 Support der Plattformbenutzer (Service Desk)

Die Verantwortung für das Service Desk liegt beim Plattformbetreiber und wird in enger Zusammenarbeit mit Justitia.Swiss erbracht.

SO13 Betrieb des Security Operations Center (SOC)

Für die Erkennung von und den Umgang mit Sicherheitsvorfällen wird ein Security Operations Center (SOC) etabliert.

SO14 Entwicklung und Weiterentwicklung der Plattform

Die Software der Plattform Justitia.Swiss wird vom Softwarelieferanten entwickelt und weiterentwickelt. Entwicklungswerkzeuge, Server und Programmierumgebungen werden durch den Plattformbetreiber zur Verfügung gestellt.

SO15 Betrieb der Plattform Justitia.Swiss mit ihren Schnittstellen

Der Betrieb der Plattform Justitia.Swiss mit ihren Schnittstellen wird durch den Plattformbetreiber sichergestellt.

3 Schutzbedarfsanalyse (Schuban)

Bei jedem Informatikvorhaben ist vorab eine Schutzbedarfsanalyse durchzuführen. Der Zeitpunkt der Analyse richtet sich nach dem Projektvorgehensmodell HERMES und soll während der Initialisierungsphase erstellt werden. Somit ist gewährleistet, dass die Informatiksicherheit von Anfang an berücksichtigt wird.[4]

Das Resultat der Schutzbedarfsanalyse (siehe Tabelle 7) ist eine Einstufungsbeurteilung des Projektes für die Kriterien Vertraulichkeit, Verfügbarkeit, Integrität und Nachvollziehbarkeit:

Kriterien	Fragen	Antwort	Kommentar, Begründung für alle Zeilen ausfüllen
Vertraulichkeit	**Werden schutzwürdige Daten (nicht DSG / ISchV relevant) bearbeitet?**	Erhöhte Anforderungen an die Schutzwürdigkeit (nicht DSG/ISchV relevant)	Eingaben und einsehbare Aktenstücke beispielsweise aus Verfahren zu Bankengesetzgebung, Steuerrecht oder Patent- und Schutzrechten.
	Welche Art von Personendaten werden bearbeitet (nach Datenschutzgesetz, DSG)?	Personendaten mit sehr hohem Schutzbedarf	Eingaben und einsehbare Aktenstücke aus potentiell allen Straf-, Zivil- und Verwaltungsgerichtsverfahren von Schweizer Justizbehörden. Dazu können auch Personendaten gehören, deren Missbrauch das Leben der betroffenen Person gefährden kann (z.B. Adressen von V-Leuten, von Zeuginnen und Zeugen in bestimmten Strafverfahren oder von Personen, die aufgrund ihrer Gesinnung oder ihrer religiösen oder politischen Zugehörigkeit bedroht sind).
	Sind die Daten / Informationen zu klassifizieren (nach Informationsschutzverordnung ISchV)?	Klassifikation: VERTRAULICH	Straf-, Zivil- und Verwaltungsgerichtsverfahren dürfen geheime Daten nicht über die Plattform "Justitia.Swiss" transferieren. Diese erfordern spezielle Massnahmen (z.B. End-to-end Verschlüsselung oder Kurierdienste).

Tabelle 6: Schuban Einstufung Vertraulichkeit

[4] gem. Unterlage https://www.ncsc.admin.ch/ncsc/de/home/dokumentation/sicherheitsvorgaben-bund/sicherheitsverfahren/beurteilung-schutzbedarf.html, 11.2021

Kriterien	Fragen	Antwort	Kommentar, Begründung für alle Zeilen ausfüllen
Verfügbarkeit	**Max. zulässige Ausfalldauer?**	Ausfalldauer kleiner 1 Tag	Wiederanlaufzeit (RTO) maximal 24 Stunden, Datenverlust (RPO) maximal 15 Minuten. Der elektronische Rechtsverkehr ist insbesondere im Zusammenhang mit Zwangsmassnahmen kritisch, da hier stundengenaue Fristen (auch über Wochenenden und Feiertage) gelten.
	Servicezeiten?	Servicezeiten erhöht	Standard Servicezeit: Montag-Freitag: 7.00 - 18.00 (für alle Arten von Anfragen). Es gilt jedoch eine erweiterte Service zeit von 7:00 bis 24:00 (an alle Tagen der Woche). In der erweiterten Servicezeit werden nur Fehlermeldungen im Zusammenhang mit der Nichtverfügbarkeit oder Erreichbarkeit von Business Services entgegengenommen. Damit können Nutzer nachweisen, dass sie eine fristgerechte Eingabe vornehmen wollten.
	Bedarf nach Katastrophenvorsorge (Business Continuity Management)?	Katastrophenvorsorge notwendig: Ja	Für nicht-aufschiebbare Entscheide (z.B. Superprovisorische Massnahmengesuche) sind bereits heute alternative Kanäle und Prozesse etabliert, deshalb braucht es keine Alternativprozesse für den phyischen Katastrophenfall (z.B. Brand). Es braucht jedoch eine erhöhte Vorsorge gegen logische Fehler (handling Fehler) oder Cyberangriffe.
Integrität	**Muss die Echtheit, Korrektheit und/oder Unversehrtheit der Daten nachgewiesen werden können?**	Spezielle Anforderungen	Zur Sicherstellung der Rechtssicherheit müssen Aktenstücke rechtsverbindlich und nicht abstreitbar sein.
Nachvollziehbarkeit	**Müssen bestimmte Arbeitsvorgänge nachgewiesen werden können?**	Spezielle Anforderungen	Zur Sicherstellung der Rechtssicherheit müssen bestimmte Ereignisse des Rechtsverkehrs (z.B. Eingaben und Zustellungen) rechtsverbindlich und nicht abstreitbar nachgewiesen werden können.

Tabelle 7: Schuban Einstufung Verfügbarkeit, Integrität und Nachvollziehbarkeit

4 Risikoanalyse

4.1 Allgemeine Grundlagen

Dieses Kapitel enthält die allgemeinen HERMES Vorgaben für die Durchführung einer Risikoanalyse im Rahmen des ISDS-Konzeptes; diese sind nicht spezifisch für das Justitia 4.0 Projekt.[5]

4.1.1 Generischer Risikokatalog

Die nachfolgende Tabelle 8 enthält den generischen Katalog der Risiken gemäss HERMES ([Ext6])

Ref	Risiko
GR1	Feuer, Wasser, Naturkatastrophen, Verschmutzung, Staub, Korrosion
GR2	Ausfall oder Störung der Stromversorgung oder von Kommunikationsnetzen
GR3	Ausfall oder Störung von Dienstleistern
GR4	Ausspähen von Informationen, Spionage, Abhören
GR5	Diebstahl oder Verlust von Geräten, Datenträgern oder Dokumenten
GR6	Fehlplanung oder fehlende Anpassung, Ressourcenmangel
GR7	Manipulation von Informationen, Hard- oder Software
GR8	Zerstörung, Ausfall oder Fehlfunktion von Geräten oder Systemen
GR9	Softwareschwachstelle oder -Fehler
GR10	Verstoss gegen Vorschriften oder Regelungen
GR11	Unberechtigte oder fehlerhafte Nutzung oder Administration von Geräten und Systemen, Missbrauch von Berechtigungen
GR12	Personalausfall
GR13	Missbrauch personenbezogener Daten
GR14	Verhinderung von Diensten (Denial of Service), Sabotage
GR15	Unbefugtes Eindringen in Räumlichkeiten
GR16	Datenverlust

Tabelle 8: Generische Risiken gemäss HERMES Vorlage für Risikoanalysen im ISDS-Konzept

[5] gem. Unterlage «P042-Hi02» von https://www.ncsc.admin.ch/ncsc/de/home/dokumentation/sicherheitsvorgaben-bund/sicherheitsverfahren/erhoehter-schutz.html, 11.2021

4.1.2 Risikomatrix

Die nachfolgende Abbildung 4 enthält die Risikomatrix gemäss HERMES ([Ext6]). Die Auswirkungsdimensionen eines Risikos und die Eintrittswahrscheinlichkeit sind in je sechs Stufen von «sehr gering» bis «sehr hoch» bzw. von «sehr unwahrscheinlich» bis «sehr wahrscheinlich» eingeteilt. Die definierten Risken werden in der Entwicklungsphase eingetragen und kontinuierlich nachgeführt.

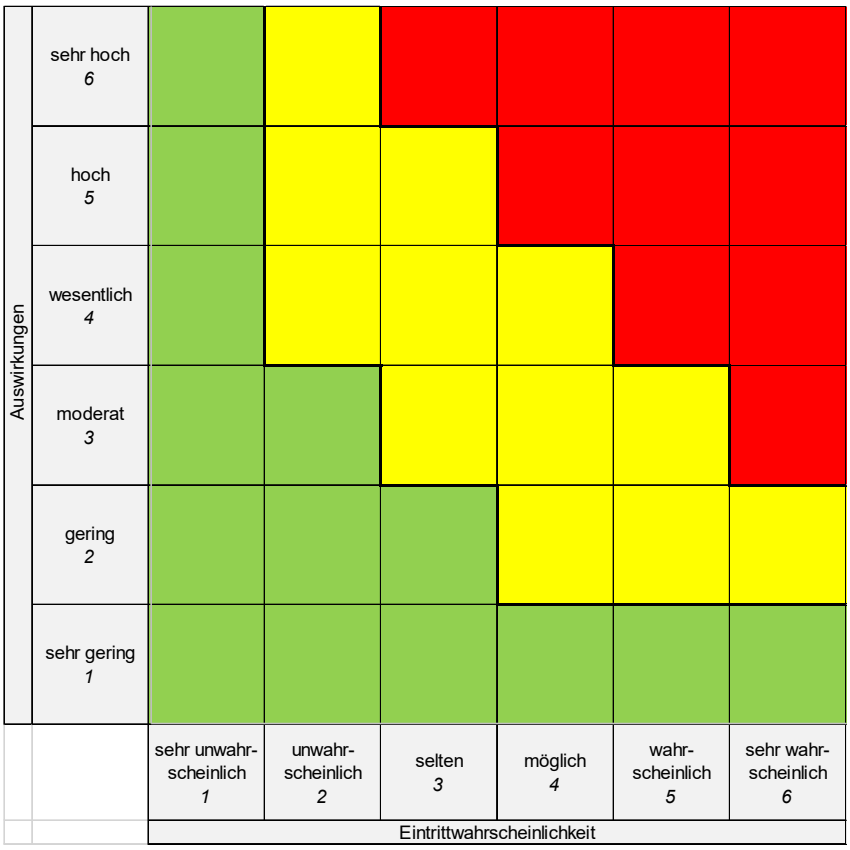

Abbildung 4: Risikomatrix gemäss HERMES Vorlage für Risikoanalysen im ISDS-Konzept

Bedeutung der Farben:

Risiken Farben	
Rot	Grosse Risiken deren Auswirkungen kritisch bis katastrophal sind. Diese Risiken müssen unbedingt reduziert werden.
Gelb	Risiken deren Auswirkungen erheblich sind und deshalb reduziert werden müssen.
Grün	Sind Risiken die entweder inhärent (im Schutzobjekt als solches) sind oder aber vernachlässigt werden können. Sollen mit einfachen Massnahmen minimiert werden können.

4.1.3 Einstufung der Eintrittswahrscheinlichkeit

Eintrittswahrscheinlichkeit					
sehr unwahrscheinlich ***1***	**unwahrscheinlich** ***2***	**selten** ***3***	**möglich** ***4***	**wahrscheinlich** ***5***	**sehr wahrscheinlich** ***6***
über 10 Jahren	alle 5-10 Jahre	alle 3-5 Jahre	alle 2-3 Jahre	alle 1-2 Jahre	Mehrmals pro Jahr

4.1.4 Einstufung der Auswirkungen

	Finanziell	Reputation*	Erbschaftsprozesse*
sehr hoch ***6***	> 10 Mio.	internationale Medienkampagne bis mehrere Jahre; gravierende politische oder wirtschaftliche Konsequenzen; Sanktionen (schwarze Listen, Embargo, …)	Beeinträchtigung von kritischen Geschäftsprozessen in mehreren Bereichen länger als 14 Tage lang; Blockierung Regierungstätigkeit, Staatskrise
hoch ***5***	1-10 Mio. CHF	nationale und internationale Medienkampagne bis zu einem Jahr; politische oder wirtschaftliche Konsequenzen; Handlungsoptionen BR in Frage gestellt	Beeinträchtigung eines kritischen Geschäftsprozesses 7 – 14 Tage lang; negative Auswirkungen auf andere kritische Prozesse; Handlungs-optionen BR eingeschränkt
wesentlich ***4***	500'000-1 Mio. CHF	nationale und teilweise internationale Medienpräsenz bis zu einem Jahr; Glaubwürdigkeit BR in Frage gestellt	Beeinträchtigung eines kritischen Geschäftsprozesses 3 – 7 Tage lang
moderat ***3***	100'000-500'000 CHF	nationale, flächendeckende Medienpräsenz bis zu einem Monat	Beeinträchtigung eines nicht-kritischen Geschäftsprozesses mehr als 3 Tage lang, oder eines kritischen Geschäftsprozesses ½ – 3 Tage lang
gering ***2***	10'000-100'000 CHF	regionale Medienpräsenz bis zu einer Woche	Beeinträchtigung eines nicht-kritischen Geschäftsprozesses 1 – 3 Tage lang, oder eines kritischen Geschäftsprozesses bis ½ Tag lang
sehr gering ***1***	< 10'000 CHF	vereinzelte kritische Reaktionen in lokalen oder regionalen Medien	Beeinträchtigung eines nicht-kritischen Geschäftsprozesses bis zu einem Tag lang

Die Bewertung eines Risikos ist aufgrund des schlimmstmöglichen vorstellbaren Szenarios vorzunehmen («*credible worst case*»). Bereits umgesetzte Massnahmen zur Verminderung eines Risikos werden bei der Bewertung der Auswirkungen berücksichtigt (Nettobewertung).

4.2 Schadenszenarien

In diesem Kapitel sind typische Schadenszenarien beschrieben, die im Zusammenhang mit der Plattform Justitia.Swiss eintreten können und in Bezug auf ihre Auswirkungen (Tragweite, Schadenausmass) bewertet.

4.2.1 Verlust der Vertraulichkeit

Tabelle 9 identifiziert und bewertet Schadenfälle bei einer unberechtigten Einsicht in Aktenstücke einer elektronischen Justizakte oder in andere Datenbestände gemäss Kapitel 2.2.

Für die Bewertung der Auswirkung eines Schadenfalles spielt nicht nur die Art der Daten eine Rolle, sondern auch die Menge der betroffenen Daten und die Art der Kompromittierung.

Ref.	Art der Daten	Umfang der Daten	Auswirkung / Tragweite	Stufe
C1	Aktenstücke oder Eingaben werden unberechtigt eingesehen oder kopiert.	Systematisch und unbemerkt über lange Zeit (Monate)	Viele Verfahren können durch Dritte beobachtet und allenfalls beeinflusst werden. Die gewonnen Informationen können für Erpressung oder andere gezielte Schädigung missbraucht werden.	**5** hoch
C2		Einmalig in grosser Menge (z.B. alle Fälle einer Justizbehörde)	Viele laufende Verfahren werden beeinträchtigt. Die Verletzung des Datenschutzes für zahlreiche Verfahrensbeteiligte gefährdet das Vertrauen in die Schweizer Justiz.	4 wesentlich
C3		Gezielt bezogen auf ausgewählte Personen oder Fälle	Exponierte Personen (z.B. VIP aus Wirtschaft oder Politik) oder Justizbehörden (z.B. Bundesgericht, Bundesstaatsanwaltschaft) können erpresst und massiv im Ruf geschädigt werden.	4 wesentlich
C4		Zufällige einzelne Aktenstücke	Einzelne Verfahrensbeteiligte oder Justizbehörden können in ihrem Ruf geschädigt oder in einem Verfahren benachteiligt werden.	3 moderat
C5	Verfahrensbezogene Randdaten (z.B. Quittungen, Notifikationen, Teilnehmerangaben oder Protokollierungsdaten) werden unberechtigt eingesehen oder kopiert.	Systematisch und unbemerkt über lange Zeit (Monate)	Unberechtigte Kenntnis von Randdaten zu vielen laufenden Verfahren kann deren Beeinflussung ermöglichen.	4 wesentlich
C6		Einmalig in grosser Menge (z.B. alle Zustellungen einer Justizbehörde)	Einzelne Verfahrensbeteiligte oder Justizbehörden können in ihrem Ruf geschädigt oder in einem Verfahren benachteiligt werden.	3 moderat
C7		Gezielt bezogen auf ausgewählte Personen oder Fälle	Einzelne Verfahrensbeteiligte oder Justizbehörden können in ihrem Ruf geschädigt oder in einem Verfahren benachteiligt werden.	3 moderat
C8		Zufällige einzelne Daten	Ein einzelnes Verfahren kann möglicherweise beeinflusst werden.	2 gering

Tabelle 9: Schadenszenarien bei Verlust der Vertraulichkeit

4.2.2 Verlust der Integrität

Tabelle 10 identifiziert und bewertet Schadenfälle bei einer Verletzung der Integrität von Aktenstücken einer elektronischen Justizakte oder von anderen Datenbeständen gemäss Kapitel 2.2.

Für die Bewertung der Auswirkung eines Schadenfalles spielt nicht nur die Art der Daten eine Rolle, sondern auch die Menge der betroffenen Daten und die Art der Kompromittierung.

Ref.	Art der Daten	Umfang der Daten	Auswirkung / Tragweite	Stufe
I1	Aktenstücke oder Eingaben werden manipuliert.	Systematisch und unbemerkt über lange Zeit (Monate)	***Worst Case Szenario*** Verfahren können durch die Manipulation von Aktenstücken gezielt beeinflusst werden, so dass die Integrität der Schweizer Justiz nicht mehr gewährleistet ist.	**6** sehr hoch
I2		Einmalig in grosser Menge (z.B. alle Fälle einer Justizbehörde)	Viele laufende Verfahren werden beeinträchtigt, weil die Aktenstücke neu beschafft und überprüft werden müssen.	4 wesentlich
I3		Gezielt bezogen auf ausgewählte Personen oder Fälle	Wichtige und/oder kritische laufende Verfahren werden beeinträchtigt, weil die Aktenstücke neu beschafft und überprüft werden müssen.	4 wesentlich
I4		Zufällige einzelne Aktenstücke	Einzelne Verfahrensbeteiligte oder Justizbehörden können in einem Verfahren benachteiligt werden.	3 moderat
I5	Verfahrensbezogene Randdaten (z.B. Quittungen, Notifikationen, Teilnehmerangaben oder Protokollierungsdaten) werden manipuliert.	Systematisch und unbemerkt über lange Zeit (Monate)	Verfahren können durch die unbemerkte Manipulation von verfahrensbezogenen Randdaten beeinflusst werden.	4 wesentlich
I6		Einmalig in grosser Menge (z.B. alle Fälle einer Justizbehörde)	Viele laufende Verfahren werden beeinträchtigt, weil die Randdaten neu beschafft und überprüft werden müssen.	3 moderat
I7		Gezielt bezogen auf ausgewählte Personen oder Fälle	Wichtige und/oder kritische laufende Verfahren werden beeinträchtigt, weil die Randdaten neu beschafft und überprüft werden müssen.	3 moderat
I8		Zufällige einzelne Randdaten	Zufällige Fehler werden festgestellt und erfordern einen Bereinigungsaufwand.	1 Sehr gering

Tabelle 10: Schadenszenarien bei Verlust der Integrität

4.2.3 Verlust der Verfügbarkeit

Tabelle 11 identifiziert und bewertet Schadenfälle bei Nichtverfügbarkeit operativer oder administrativer Anwendungsfälle gemäss den Kapiteln 2.4, 2.5 und 2.6:

Ref.	Art des Ausfalls	Umfang des Ausfalls	Dauer des Ausfalls	Auswirkung / Tragweite	Stufe
A1	Die elektronische Kommunikation zwischen Justizbehörden und Verfahrensbeteiligten ist nicht möglich (eAE, ERV).	Viele oder alle Justizbehörden und Verfahrensbeteiligte sind betroffen	Tagelang	Justizverfahren werden schweizweit verzögert, weil auf alternative Kommunikationskanäle (z.B. Fax, Briefpost, Secure E-Mail) zurückgegriffen werden muss.	4 wesentlich
A2			Stundenlang	Laufende Fristen «verlängern» sich auf den Folgetag.	2 gering
A3		Einzelne Justizbehörden oder Verfahrensbeteiligte sind betroffen	Tagelang	Einige Justizverfahren werden verzögert, weil auf alternative Kommunikationskanäle (z.B. Fax, Briefpost, Secure E-Mail) zurückgegriffen werden muss.	3 moderat
A4			Stundenlang	Einige laufende Fristen verlängern sich auf den Folgetag.	1 Sehr gering
A5	Die Verwaltung von Organisationen, Benutzern oder Zugriffsrechten ist nicht möglich.	Viele oder alle Justizbehörden sind betroffen	Tagelang	Administrative Prozesse werden behindert und es sind allenfalls Umgehungslösungen (z.B. Stellvertretung) nötig.	3 moderat
A6			Stundenlang	Die Auswirkung ist vernachlässigbar.	1 Sehr gering
A7		Einzelne Justizbehörden sind betroffen	Tagelang	Administrative Prozesse werden behindert und es sind allenfalls Umgehungslösungen (z.B. Stellvertretung) nötig.	3 moderat
A8			Stundenlang	Die Auswirkung ist vernachlässigbar.	1 Sehr gering

Tabelle 11: Schadenszenarien bei Verlust der Verfügbarkeit

4.2.4 Verlust der Nachvollziehbarkeit

Tabelle 12 identifiziert und bewertet Schadenfälle bei einer Verletzung der Nachvollziehbarkeit von operativen oder administrativen Tätigkeiten oder des Plattformbetriebs.

Ref.	Art der Daten	Anwendungsfall	Auswirkung / Tragweite	Stufe
N1	Operative Anwendungsfälle können nicht nachvollzogen werden.	Eingaben	Verfahrensbeteiligte können abstreiten, eine Eingabe gemacht zu haben und die Verfahrensabwicklung dadurch beeinflussen.	4 wesentlich
N2		Zustellungen	Verfahrensbeteiligte können abstreiten, eine Zustellung erhalten zu haben und die Verfahrensabwicklung dadurch beeinflussen.	4 wesentlich
N3		Elektronische Akteneinsicht	Verfahrensbeteiligte können abstreiten, wichtige Aktenstücke gesehen zu haben und die Verfahrensabwicklung dadurch behindern.	3 moderat
N4	Administrative Anwendungsfälle können nicht nachvollzogen werden.	Verwalten von Organisationen	Es kann nicht nachvollzogen werden, wer eine verfahrensführende Justizbehörde im Adressverzeichnis erfasst, mutiert oder gelöscht hat.	3 moderat
N5		Verwalten von Benutzern	Es kann nicht nachvollzogen werden, wer einen Benutzereintrag im Adressverzeichnis erfasst, mutiert oder gelöscht hat.	3 moderat
N6		Verwalten von Organisations-Zugehörigkeiten	Es kann nicht nachvollzogen werden, wer eine Organisationszugehörigkeit im Adressverzeichnis erfasst, mutiert oder gelöscht hat.	3 moderat
N7		Verwalten von Zugriffsrechten	Es kann nicht nachvollzogen werden, wer ein Zugriffsrecht erfasst, mutiert oder gelöscht hat.	3 moderat
N8	Der Systembetrieb kann nicht nachvollzogen werden.	Betrieb der Plattform Justitia.Swiss	Sicherheitsvorfälle auf der Plattform Justitia.Swiss können weder erkannt noch nachvollzogen werden.	4 wesentlich

Tabelle 12: Schadenszenarien bei Verlust der Nachvollziehbarkeit

4.3 Schwachstellenanalyse

Relevante Risiken entstehen dort, wo eine allgemeine Bedrohung (z.B. Spionage) auf Grund einer Schwachstelle (z.B. mangelhafte Benutzerauthentifizierung) zu einem Schadenszenario (z.B. unbemerkte unberechtigte Einsicht in eine elektronische Akte) führen kann.

Die ***Eintrittswahrscheinlichkeit*** eines Schadenfalles wird durch die Komplexität des Angriffs sowie die Grösse und Motivation des potentiellen Angreifer-Kreises (z.B. anonyme Internetbenutzer, authentifizierte Plattformbenutzer oder Innentäter) bestimmt.

- Der Kreis der anonymen Internetbenutzer;[6]
- Der Kreis der authentifizierten Plattformbenutzer[7];
- Der Kreis der Innentäter[8].

Sie lässt sich nur grob abschätzen anhand von Erfahrungswerten aus anderen Internetanwendungen (Expertenschätzung).

Die ***Auswirkung*** oder Tragweite eines Schadenfalles wird üblicherweise in den Dimensionen «Verlust der Vertraulichkeit», «Verlust der Integrität», «Verlust der Verfügbarkeit» und «Verlust der Nachvollziehbarkeit» bewertet und ergibt sich aus der Art und der Menge der jeweils betroffenen Daten.

- Kapitel 4.2 beschreibt verschiedene Schadenszenarien und bewertet diese in Bezug auf die Auswirkung. Bei der Risikobewertung wird auf diese Schadenszenarien referenziert.

Schwachstellen stehen immer im Zusammenhang mit einem Anwendungsfall bzw. Prozess, weshalb die Schwachstellenanalyse entlang dieser Schutzobjekte erfolgt.

[6] umfasst grundsätzlich die ganze Weltbevölkerung. Dabei geht insbesondere von politisch oder wirtschaftlich motivierten Organisationen eine erhebliche Bedrohung aus, weil solche Organisationen über umfangreiche Angriffsmittel verfügen.

[7] umfasst einerseits etwa 25'000 Personen, die in Justizbehörden und Anwaltskanzleien tätig sind. Zu den authentifizierten Plattformbenutzern zählen aber auch alle natürlichen und juristischen Personen mit einer digitalen Identität, die als Partei oder Dritte an einem Justizverfahren in der Schweiz beteiligt sein können, d.h. ein grosser Teil der Schweizer Bevölkerung. Durch die missbräuchliche Ausnutzung von Sicherheitsschwachstellen, z.B. für die unberechtigte Einsicht in die Aktenstücke von anderen Verfahrensbeteiligten, könnte sich ein Plattformbenutzer einen direkten Nutzen in einem laufenden Verfahren versprechen. Die authentifizierten Benutzer der Plattform Justitia.Swiss dürfen deshalb als potenzieller Angreifer-Kreis nicht vernachlässigt werden.

[8] umfasst einerseits Personen bei der öffentlich-rechtlichen Körperschaft (örK) und bei dem von ihr beauftragten Plattformbetreiber, die unter Umgehung der applikatorischen Zugriffskontrolle auf Funktionalitäten und Daten der Plattform Justitia.Swiss zugreifen können (z.B. Systemadministratoren).

4.3.1 Schwachstellenanalyse für operative Anwendungsfälle

SO1 Eingabe

R1 Eingaben werden nach dem Versand verändert

Dateien, die von einem Verfahrensbeteiligten über die Plattform Justitia.Swiss als Teil einer Eingabe eingereicht wurden, werden nachträglich verändert. Eine solche Manipulation kann an unterschiedlichen Stellen erfolgen:

- Auf der Plattform Justitia.Swiss während der Speicherung im Postfach der adressierten Behörde;
- Auf dem Transportweg, während die Eingabe von der adressierten Behörde abgeholt wird;
- Auf den IT-Systemen der Justizbehörde während der Bearbeitung der Eingabe;
- In der elektronischen Akte der verfahrensleitenden Justizbehörde während der Verfahrensdauer;
- Im DossierStore der verfahrensleitenden Justizbehörde während der Verfahrensdauer;
- Im Archiv der verfahrensleitenden Justizbehörde nach Abschluss des Verfahrens.

Mit einer gezielten derartigen Manipulation kann der Verlauf und/oder das Ergebnis von Justizverfahren beeinflusst werden.

Risikobeurteilung:

Ref.	Generisches Risiko	Szenarien	Auswirkungen	Eintrittsw'keit	Risikostufe
R1	GR7	I1	6 (sehr hoch)	4 (möglich)	**Gross**

Sicherheitsmassnahmen (siehe Kapitel 5):

- MA (1) Elektronisches Plattform-Siegel für alle Eingaben
- MA (2) Möglichkeit zur Eingabe vorgängig digital signierter Dateien

R2 Eingaben werden abgestritten

Ein Verfahrensbeteiligter streitet ab, eine Eingabe über die Plattform Justitia.Swiss eingereicht zu haben, um ein laufendes Verfahren zu sabotieren oder anderweitig zu beeinflussen.

Risikobeurteilung:

Ref.	Generisches Risiko	Szenarien	Auswirkungen	Eintrittsw'keit	Risikostufe
R2	GR10	N1	4 (wesentlich)	4 (möglich)	Mittel

Sicherheitsmassnahmen (siehe Kapitel 5):

- MA (3) Das Plattform-Siegel verlangt eine Willensbekundung des Absenders
- MA (4) Die Plattform zeichnet alle rechtsverbindlichen Ereignisse in einem Audit Trail auf
- MA (5) Die Plattform kann elektronisch gesiegelte Eingangs- und Abrufquittungen erzeugen

R3 Eingaben werden unter einer falschen Identität eingereicht

Ein unbekannter Dritter (ein anonymer Internetbenutzer) reicht eine Eingabe unter der Identität eines im Adressverzeichnis der Plattform Justitia.Swiss registrierten Verfahrensbeteiligten ein, indem er sich unter dessen Identität an der Plattform oder an einer integrierten Kanzleisoftware anmeldet.

Der Verfahrensbeteiligte, unter dessen Identität die Eingabe eingereicht wurde, kann dadurch in einem Justizverfahren wesentlich benachteiligt bzw. geschädigt werden.

Risikobeurteilung:

Ref.	Generisches Risiko	Szenarien	Auswirkungen	Eintrittsw'keit	Risikostufe
0	GR7	I3	4 (wesentlich)	5 (wahrscheinlich)	**Gross**

Sicherheitsmassnahmen (siehe Kapitel 5):

- MA (6) 2-Faktor-Authentifizierung (2FA) aller Benutzer
- MA (7) Anbindung der Identity Provider über sichere Federation Protokolle

R4 Eingaben werden mit einer falschen AkteID eingereicht

Ein Verfahrensbeteiligter gibt beim Einreichen einer Eingabe (manuell oder über API) irrtümlich oder missbräuchlich eine falsche AkteID ein, worauf die eingereichten Dateien in einem falschen Kontext bearbeitet und/oder in der falschen elektronischen Akte abgelegt werden. Dies kann die Führung der betroffenen Verfahren beeinträchtigen.

Risikobeurteilung:

Ref.	Generisches Risiko	Szenarien	Auswirkungen	Eintrittsw'keit	Risikostufe
R4	GR7	I3	4 (wesentlich)	4 (möglich)	Mittel

Sicherheitsmassnahmen (siehe Kapitel 5):

- MA (9) Qualitätssicherung für übermittelte strukturierte Daten
- MA (11) Sichere Postfächer für verfahrensleitende Justizbehörden

R5 Eingaben werden von unberechtigten Dritten eingesehen

Eingaben, die von einem Verfahrensbeteiligten über die Plattform Justitia.Swiss eingereicht wurden, werden von unberechtigten Dritten (anonyme Internetbenutzer, nicht autorisierte Plattformbenutzer oder Innentäter) auf der Plattform Justitia.Swiss oder auf dem Kommunikationsweg zur verfahrensleitenden Justizbehörde eingesehen (das Risiko einer unberechtigten Einsicht auf einem IT-System der verfahrensführenden Justizbehörde ist out-of-Scope für das vorliegende Sicherheitskonzept).

Risikobeurteilung:

Ref.	Generisches Risiko	Szenarien	Auswirkungen	Eintrittsw'keit	Risikostufe
R5	GR4, GR5	C1	5 (hoch)	5 (wahrscheinlich)	**Gross**

Sicherheitsmassnahmen (siehe Kapitel 5):

- MA (10) Sichere persönliche Arbeitsbereiche für Verfahrensbeteiligte
- MA (11) Sichere Postfächer für verfahrensleitende Justizbehörden
- MA (12) Zugriffskontrollsystem für Daten und Funktionen der Plattform Justitia.Swiss
- MA (13) Eingaben und Aktenstücke werden ausserhalb des DossierStore nicht aufbewahrt
- MT (1) Verschlüsselung aller auf der Plattform Justitia.Swiss gespeicherten Daten
- MT (2) Verschlüsselung aller Kommunikationsverbindungen

R6 Eingaben gehen verloren

Eingaben von Verfahrensbeteiligten werden gelöscht, bevor sie in einer elektronischen Akte gespeichert oder anderweitig von der adressierten Justizbehörde verarbeitet wurden.

Risikobeurteilung:

Ref.	Generisches Risiko	Szenarien	Auswirkungen	Eintrittsw'keit	Risikostufe
0	GR5, GR16	A1	4 (wesentlich)	4 (möglich)	Mittel

Sicherheitsmassnahmen (siehe Kapitel 5):

- MA (11) Sichere Postfächer für verfahrensleitende Justizbehörden
- MA (35) QS-System für Transaktionsverarbeitung und Datenbestände

R7 Mit Schadsoftware verseuchte Eingaben schädigen die IT-Systeme anderer Teilnehmer

Im Rahmen einer Eingabe werden Dateien, die mit Schadsoftware (z.B. Ransomware) verseucht sind, zu einer verfahrensleitenden Justizbehörde transferiert. Wenn diese Dateien im weiteren Verfahrensverlauf von der verfahrensleitenden Justizbehörde oder von einem anderen Verfahrensbeteiligten geöffnet werden, kann die Schadsoftware deren IT-Systeme schädigen und/oder sich weiter ausbreiten.

Die Eintrittswahrscheinlichkeit dieses Risikos ist besonders gross, weil jede im Adressverzeichnis registrierte Person beliebige Dateien bei jeder Justizbehörde einreichen kann.

Risikobeurteilung:

Ref.	Generisches Risiko	Szenarien	Auswirkungen	Eintrittsw'keit	Risikostufe
R7	GR7	A4	3 (moderat)	6 (sehr wahrscheinlich)	**Gross**

Sicherheitsmassnahmen (siehe Kapitel 5):

- MO (13) Sicherheitsverantwortung der Verfahrensbeteiligten als Teil der Nutzungsbedingungen
- MT (3) Virenscan auf der Plattform Justitia.Swiss für alle transferierten Dateien
- MT (4) Quarantänebereich für potentiell schädliche Dateien

R8 Eingaben oder Zustellungen können vom Empfänger nicht gelesen werden

Im Rahmen einer Eingabe (oder einer Zustellung, siehe unten) werden Dateien (Binärdateien) übermittelt, die vom Empfänger nicht gelesen werden können. Weil über die Plattform Justitia.Swiss nur Kopien von Aktenstücken verarbeitet werden, resultiert daraus eine vorübergehende Nichtverfügbarkeit der Daten, aber kein dauerhafter Datenverlust.

Risikobeurteilung:

Ref.	Generisches Risiko	Szenarien	Auswirkungen	Eintrittsw'keit	Risikostufe
R8	GR16	A4	1 (sehr gering)	4 (möglich)	Klein

Sicherheitsmassnahmen (siehe Kapitel 5):

- MT (5) Definierter Katalog von gültigen Dateiformaten
- MA (14) Zugestellte Aktenstücke werden online abgeholt

SO2 Zustellung

R9 Aktenstücke werden auf dem Zustellweg manipuliert oder gehen verloren

Zugestellte Aktenstücke einer verfahrensleitenden Justizbehörde werden verändert, während sie über die Plattform Justitia.Swiss zum adressierten Verfahrensbeteiligten transferiert werden.

Mit einer gezielten derartigen Manipulation kann der Verlauf und/oder das Ergebnis eines Justizverfahrens beeinflusst werden.

Risikobeurteilung:

Ref.	Generisches Risiko	Szenarien	Auswirkungen	Eintrittsw'keit	Risikostufe
R9	GR7	I1	6 (sehr hoch)	3 (selten)	**Gross**

Sicherheitsmassnahmen (siehe Kapitel 5):

- MA (5) Die Plattform kann elektronisch gesiegelte Eingangs- und Abrufquittungen erstellen
- MA (10) Sichere persönliche Arbeitsbereiche für Verfahrensbeteiligte
- MA (11) Sichere Postfächer für verfahrensleitende Justizbehörden
- MA (13) Eingaben und Aktenstücke werden ausserhalb des DossierStore nicht aufbewahrt
- MA (14) Zugestellte Aktenstücke werden online abgeholt
- MA (15) Siegel-Validierung bei der elektronischen Akteneinsicht

R10 Der Empfang zugestellter Aktenstücke wird abgestritten

Ein Verfahrensbeteiligter streitet unberechtigterweise ab, zugestellte Aktenstücke erhalten zu haben, um ein laufendes Verfahren zu sabotieren oder anderweitig zu beeinflussen.

Risikobeurteilung:

Ref.	Generisches Risiko	Szenarien	Auswirkungen	Eintrittsw'keit	Risikostufe
R10	GR10	N1	4 (wesentlich)	5 (wahrscheinlich)	**Gross**

Sicherheitsmassnahmen (siehe Kapitel 5):

- MA (14) Zugestellte Aktenstücke werden online abgeholt
- MA (15) Siegel-Validierung bei der elektronischen Akteneinsicht
- MA (4) Die Plattform zeichnet alle rechtsverbindlichen Ereignisse in einem Audit Trail auf
- MA (5) Die Plattform kann elektronisch gesiegelte Eingangs- und Abrufquittungen erzeugen

R11 Die Integrität zugestellter Aktenstücke wird abgestritten

Ein Verfahrensbeteiligter behauptet unberechtigterweise, dass ein zugestelltes Aktenstück manipuliert wurde und beispielsweise nicht mehr identisch mit der ursprünglichen Eingabe ist.

Risikobeurteilung:

Ref.	Generisches Risiko	Szenarien	Auswirkungen	Eintrittsw'keit	Risikostufe
R10	GR10	N1	4 (wesentlich)	4 (möglich)	Mittel

Sicherheitsmassnahmen (siehe Kapitel 5):

- MA (11) Sichere Postfächer für verfahrensleitende Justizbehörden
- MA (15) Siegel-Validierung bei der elektronischen Akteneinsicht

R12 Der Versand einer Zustellung wird abgestritten

Eine verfahrensleitende Justizbehörde streitet unberechtigterweise ab, gewisse Aktenstücke einem Verfahrensbeteiligten zugestellt zu haben und damit diesen Verfahrensbeteiligten zur Einsicht in diese Aktenstücke berechtigt zu haben.

Risikobeurteilung:

Ref.	Generisches Risiko	Szenarien	Auswirkungen	Eintrittsw'keit	Risikostufe
R10	GR10	N1	4 (wesentlich)	4 (möglich)	Mittel

Sicherheitsmassnahmen (siehe Kapitel 5):

- MA (4) Die Plattform zeichnet alle rechtsverbindlichen Ereignisse in einem Audit Trail auf
- MA (5) Die Plattform kann elektronisch gesiegelte Eingangs- und Abrufquittungen erzeugen
- MA (16) Notifikation des Empfängers einer Zustellung

R13 Der Empfänger einer Zustellung wird nicht erreicht

Die Adressaten zugestellter Aktenstücke werden nicht oder zu spät erreicht, beispielsweise auf Grund einer ungeplanten Abwesenheit.

Risikobeurteilung:

Ref.	Generisches Risiko	Szenarien	Auswirkungen	Eintrittsw'keit	Risikostufe
R13	GR12	A3	3 (moderat)	5 (wahrscheinlich)	Mittel

Sicherheitsmassnahmen (siehe Kapitel 5):

- MO (7) Periodische Rezertifizierung aller gültigen Zustellungen
- MO (8) Quartalsweise Rezertifizierung aller gültigen Delegationen
- MA (16) Notifikation des Empfängers einer Zustellung
- MA (17) Berechtigungsrelevante Elemente einer Zustellung werden nie manuell erfasst
- MA (18) Die Berechtigungswirkung einer Zustellung kann geprüft werden
- MA (35) QS-System für Transaktionsverarbeitung und Datenbestände

R14 Eine fehlerhafte Zustellung führt zu unerwünschtem Aktenzugriff

Eine Zustellung enthält auf Grund eines Fehlers bei der Erfassung falsche bzw. unerwünschte Angaben (z.B. eine falsche AkteID, ein falscher Empfänger, eine falsche Gültigkeitsdauer oder falsche Aktenstück-Adressen). Dies führt dazu, dass unerwünschte Berechtigungen zur Akteneinsicht entstehen.

Risikobeurteilung:

Ref.	Generisches Risiko	Szenarien	Auswirkungen	Eintrittsw'keit	Risikostufe
R13	GR12	C3	3 (moderat)	6 (sehr wahrscheinlich)	**Gross**

Sicherheitsmassnahmen (siehe Kapitel 5):

- MA (17) Berechtigungsrelevante Elemente einer Zustellung werden nie manuell erfasst
- MA (18) Die Berechtigungswirkung einer Zustellung kann geprüft werden
- MA (19) Zustellungen können auf der Plattform Justitia.Swiss annulliert werden
- MA (35) QS-System für Transaktionsverarbeitung und Datenbestände
- MO (7) Periodische Rezertifizierung aller gültigen Zustellungen
- MO (8) Quartalsweise Rezertifizierung aller gültigen Delegationen
- MO (12) Sicherheitsverantwortung der Justizbehörden als Bestandteil des Anschlussvertrages

R15 Zustellungen sind nicht mehr aktuell

Eine auf Grund besonderer Umstände (ein Aktenstück muss aus der einsehbaren Akte entfernt werden, auf Grund eines Anwaltswechsels muss ein Zugriffsrecht mit sofortiger Wirkung entzogen werden, …) notwendige Anpassung einer Berechtigung zur Akteneinsicht kann nicht zeitgerecht erfolgen, weil die zu Grunde liegende Zustellung noch gültig ist.

Risikobeurteilung:

Ref.	Generisches Risiko	Szenarien	Auswirkungen	Eintrittsw'keit	Risikostufe
R13	GR12	C3	3 (moderat)	5 (wahrscheinlich)	Mittel

Sicherheitsmassnahmen (siehe Kapitel 5):

- MA (7) Anbindung der Identity Provider über sichere Federation Protokolle
- MA (8) Gegenseitige Authentifizierung der Endpunkte bei allen API-Verbindungen
- MA (19) Zustellungen können auf der Plattform Justitia.Swiss annulliert werden

R16 Es werden gefälschte Zustellungen erfasst

Ein unberechtigter Dritter erfasst, entweder über das Web-Portal oder über das API, auf der Plattform Justitia.Swiss eine gefälschte Zustellung und ermöglicht dadurch einem beliebigen Teilnehmer die Einsicht in eine beliebige Akte.

Risikobeurteilung:

Ref.	Generisches Risiko	Szenarien	Auswirkungen	Eintrittsw'keit	Risikostufe
R13	GR12	C1	5 (hoch)	4 (möglich)	**Gross**

Sicherheitsmassnahmen (siehe Kapitel 5):

- MA (6) 2-Faktor-Authentifizierung (2FA) aller Benutzer
- MA (7) Anbindung der Identity Provider über sichere Federation Protokolle
- MA (8) Gegenseitige Authentifizierung der Endpunkte bei allen API-Verbindungen
- MT (2) Verschlüsselung aller Kommunikationsverbindungen

SO3 Akteneinsicht

R17 Akten werden von unberechtigten Dritten über die Plattform eingesehen

Akten, die von einer verfahrensleitenden Justizbehörde zur Einsicht über die Plattform Justitia.Swiss freigegeben wurden, werden von unberechtigten Dritten (anonyme Internetbenutzer, nicht autorisierte Plattformbenutzer oder Innentäter) über die Plattform Justitia.Swiss bei der verfahrensleitenden Justizbehörde eingesehen (das Risiko einer unberechtigten Einsicht in die heruntergeladenen Aktenstücke auf einem IT-System eines berechtigten Verfahrensbeteiligten ist out-of-Scope des vorliegenden Sicherheitskonzeptes).

Risikobeurteilung:

Ref.	Generisches Risiko	Szenarien	Auswirkungen	Eintrittsw'keit	Risikostufe
R11	GR4, GR5	C1	5 (hoch)	5 (wahrscheinlich)	**Gross**

Sicherheitsmassnahmen (siehe Kapitel 5):

- MA (6) 2-Faktor-Authentifizierung (2FA) aller Benutzer
- MA (7) Anbindung der Identity Provider über sichere Federation Protokolle
- MA (8) Gegenseitige Authentifizierung der Endpunkte bei allen API-Verbindungen
- MT (2) Verschlüsselung aller Kommunikationsverbindungen

R18 Akten werden von unberechtigten Dritten direkt aus einem DossierStore bezogen

Akten, die von einer verfahrensleitenden Justizbehörde zur Einsicht über die Plattform Justitia.Swiss freigegeben wurden, werden von anonymen Internetbenutzern direkt aus einem DossierStore bezogen, indem diese das API des DossierStore aufrufen.

Risikobeurteilung:

Ref.	Generisches Risiko	Szenarien	Auswirkungen	Eintrittsw'keit	Risikostufe
R11	GR4, GR5	C1	5 (hoch)	5 (wahrscheinlich)	**Gross**

Sicherheitsmassnahmen (siehe Kapitel 5):

- MA (8) Gegenseitige Authentifizierung der Endpunkte bei allen API-Verbindungen
- MA (20) Die Berechtigungsprüfung ist Teil der DossierStore-Abfragetransaktion

R19 Akten werden ohne eine vorgängige Zustellung über die Plattform eingesehen

Beim Aufruf eines DossierStore wird eine Aktenstück-Adresse verwendet, ohne dass dem Benutzer vorgängig die Berechtigung für den Zugriff auf das entsprechende Aktenstück erteilt wurde. Dies könnte beispielsweise erreicht werden, indem beim Aufruf des DossierStore-API eine beliebige Aktenstück-Adresse angegeben bzw. in den Request eingefügt wird.

Risikobeurteilung:

Ref.	Generisches Risiko	Szenarien	Auswirkungen	Eintrittsw'keit	Risikostufe
R20	GR7	C3	4 (wesentlich)	3 (selten)	Mittel

Sicherheitsmassnahmen (siehe Kapitel 5):

- MA (20) Die Berechtigungsprüfung ist Teil der DossierStore-Abfragetransaktion

R20 Mit Schadsoftware verseuchte Aktenstücke werden zugestellt

Ein mit Schadsoftware verseuchtes Aktenstück wird von Verfahrensbeteiligten über die Plattform Justitia.Swiss eingesehen und heruntergeladen.

Risikobeurteilung:

Ref.	Generisches Risiko	Szenarien	Auswirkungen	Eintrittsw'keit	Risikostufe
R20	GR7	A4	3 (moderat)	4 (möglich)	Mittel

Sicherheitsmassnahmen (siehe Kapitel 5):

- MA (12) Zugriffskontrollsystem für Daten und Funktionen der Plattform Justitia.Swiss
- MT (3) Virenscan auf der Plattform Justitia.Swiss für alle transferierten Dateien
- MT (4) Quarantänebereich für potentiell schädliche Dateien

R21 Unberechtigte Einsicht in verfahrensbezogene Randdaten

Randdaten zu Verfahren, die auf der Plattform Justitia.Swiss erzeugt und/oder gespeichert werden, werden von unberechtigten Personen eingesehen. Dies schliesst auch authentifizierte Benutzer der Plattform Justitia.Swiss mit ein, wenn sie Zugriff auf Randdaten von Verfahren erhalten, an denen sie nicht beteiligt sind.

Schützenswerte Randdatenbestände zu Verfahren sind insbesondere (nicht abschliessend):

- Das Adressverzeichnis der Plattform Justitia.Swiss;
- Der Audit Trail und die Logs der Plattform Justitia.Swiss;
- Die von der Plattform Justitia.Swiss ausgestellten Eingangs- und Abrufquittungen;
- Die auf der Plattform Justitia.Swiss verwalteten Delegationen und Organisationszugehörigkeiten;
- Die persönlichen Arbeitsbereiche von Verfahrensbeteiligten und Justizbehörden;

- Die Postfächer von verfahrensleitenden Justizbehörden.

Risikobeurteilung:

Ref.	Generisches Risiko	Szenarien	Auswirkungen	Eintrittsw'keit	Risikostufe
R21	GR4, GR13	C1	4 (wesentlich)	4 (möglich)	Mittel

Sicherheitsmassnahmen (siehe Kapitel 5):

- MA (12) Zugriffskontrollsystem für Daten und Funktionen der Plattform Justitia.Swiss
- MA (21) Elektronisches Siegel für alle Aktenstücke im zentralen DossierStore
- MT (1) Verschlüsselung aller auf der Plattform Justitia.Swiss gespeicherten Daten

SO4 Interaktion zwischen Justizbehörden

R22 Für verfahrensbeteiligte Justizbehörden werden Sicherheitsmassnahmen nicht umgesetzt

Bei der Interaktion zwischen Behörden agiert die eine Behörde gegenüber der anderen Behörde in der Rolle eines Verfahrensbeteiligten (sie reicht Eingaben ein, sie empfängt Zustellungen und sie nimmt elektronisch Einsicht in die Akte der verfahrensleitenden Behörde).

Alle unter SO1, SO2 und SO3 identifizierten Sicherheitsrisiken, die sich auf Verfahrensbeteiligte beziehen, gelten gleichermassen auch bei der Interaktion zwischen Behörden. Es besteht das Risiko, dass sich die Vertreter der verfahrensbeteiligten Behörden dieses Rollenwechsels nicht bewusst sind und die für Verfahrensbeteiligte geltenden Sicherheitsmassnahmen nicht konsequent durchgesetzt werden.

Risikobeurteilung:

Ref.	Generisches Risiko	Szenarien	Auswirkungen	Eintrittsw'keit	Risikostufe
R11	GR10	C2, I2	4 (wesentlich)	3 (selten)	Mittel

Sicherheitsmassnahmen (siehe Kapitel 5):

- MO (14) Sicherheitsmassnahmen gelten auch für verfahrensbeteiligte Justizbehörden

SO5 Zentraler DossierStore als Service der Plattform Justitia.Swiss

R23 Aktenstücke im zentralen DossierStore werden verändert

Aktenstücke werden während der Speicherung im zentralen DossierStore verändert.

Jede manuelle Veränderung (z.B. Hinzufügen, Aktualisieren oder Löschen eines Aktenstücks) im zentralen DossierStore führt zu einer Inkonsistenz zwischen der einsehbaren Akte im zentralen DossierStore und der elektronischen Akte bei der verfahrensleitenden Justizbehörde, falls diese nicht synchron und in exakt derselben Weise ebenfalls angepasst wird. Eine solche Inkonsistenz kann die Durchführung von Justizverfahren beeinträchtigen.

Im Falle einer bewussten Manipulation des DossierStore auf der Plattform, beispielsweise durch den gezielten Austausch eines Aktenstücks in der Dokumentenablage, kann der Verlauf und/oder das Ergebnis von Justizverfahren wesentlich beeinflusst werden.

Risikobeurteilung:

Ref.	Generisches Risiko	Szenarien	Auswirkungen	Eintrittsw'keit	Risikostufe
R1	GR7	I1	6 (sehr hoch)	4 (möglich)	**Gross**

Sicherheitsmassnahmen (siehe Kapitel 5):

- MA (21) Elektronisches Siegel für alle Aktenstücke im zentralen DossierStore
- MA (22) Mandantentrennung im zentralen DossierStore
- MA (23) Kein direktes Schreibrecht auf den zentralen DossierStore
- MA (35) QS-System für Transaktionsverarbeitung und Datenbestände
- MT (1) Verschlüsselung aller auf der Plattform Justitia.Swiss gespeicherten Daten

R24 Aktenstücke im zentralen DossierStore werden von unberechtigten Dritten eingesehen

Aktenstücke werden während der Speicherung im zentralen DossierStore von unberechtigten Dritten (anonyme Internetbenutzer, nicht autorisierte Plattformbenutzer oder Innentäter) eingesehen.

Risikobeurteilung:

Ref.	Generisches Risiko	Szenarien	Auswirkungen	Eintrittsw'keit	Risikostufe
R5	GR4, GR5	C1	5 (hoch)	5 (wahrscheinlich)	**Gross**

Sicherheitsmassnahmen (siehe Kapitel 5):

- MA (12) Zugriffskontrollsystem für Daten und Funktionen der Plattform Justitia.Swiss
- MA (22) Mandantentrennung im zentralen DossierStore
- MA (24) Nur Behörden-Administratoren erhalten ein Leserecht für den eigenen DossierStore
- MT (1) Verschlüsselung aller auf der Plattform Justitia.Swiss gespeicherten Daten

R25 Aktenstücke im zentralen DossierStore gehen verloren

Aktenstücke werden aus dem DossierStore gelöscht, obwohl sie noch für die elektronische Akteneinsicht benötigt werden. Da es sich nur um Kopien aus der elektronischen Akte handelt, können die im DossierStore fälschlicherweise gelöschten Aktenstücke durch erneute Zustellung ersetzt werden und die Tragweite eines Schadenfalls ist entsprechend gering.

Risikobeurteilung:

Ref.	Generisches Risiko	Szenarien	Auswirkungen	Eintrittsw'keit	Risikostufe
24	GR16	A2	2 (gering)	3 (selten)	Klein

Sicherheitsmassnahmen (siehe Kapitel 5):

- *Keine nötig*

R26 Aktenstücke im zentralen DossierStore werden nicht nachgeführt

Veränderungen an der elektronischen Akte, die auch elektronisch einsehbare Aktenstücke betreffen, werden im zentralen DossierStore nicht zeitgerecht nachgeführt. Eine solche Inkonsistenz kann die Durchführung von Justizverfahren beeinträchtigen.

Mögliche Beispiele:

- Aktenstücke werden aktualisiert, innerhalb der Akte verschoben oder gelöscht;
- Die Aktenstruktur wird verändert;
- Der Aktendeckel wird mutiert.

Eine solche Inkonsistenz kann der Verlauf und/oder das Ergebnis von Justizverfahren behindern.

Risikobeurteilung:

Ref.	Generisches Risiko	Szenarien	Auswirkungen	Eintrittsw'keit	Risikostufe
R1	GR7	I4	3 (moderat)	4 (möglich)	Mittel

Sicherheitsmassnahmen (siehe Kapitel 5):

- MO (7) Periodische Rezertifizierung aller gültigen Zustellungen
- MO (8) Quartalsweise Rezertifizierung aller gültigen Delegationen
- MO (12) Sicherheitsverantwortung der Justizbehörden als Bestandteil des Anschlussvertrags

R27 Nicht mehr benötigte Aktenstücke im zentralen DossierStore werden nicht gelöscht

Aktenstücke bleiben im DossierStore vorhanden, obwohl keine elektronische Akteneinsicht mehr benötigt wird und bleiben deshalb unnötigerweise dem Risiko einer unberechtigten Einsicht ausgesetzt.

Risikobeurteilung:

Ref.	Generisches Risiko	Szenarien	Auswirkungen	Eintrittsw'keit	Risikostufe
R1	GR7	I4	2 (gering)	6 (sehr wahrscheinlich)	Mittel

Sicherheitsmassnahmen (siehe Kapitel 5):

- MO (6) Periodische Überprüfung des Adressverzeichnis
- MO (7) Periodische Rezertifizierung aller gültigen Zustellungen
- MO (8) Quartalsweise Rezertifizierung aller gültigen Delegationen
- MO (12) Sicherheitsverantwortung der Justizbehörde als Bestandteil des Anschlussvertrages
- MA (28) Definierter Eigentümer für jedes Attribut im Adressverzeichnis
- MA (29) Abgleich mit relevanten Registerdaten, wo sinnvoll
- MA (31) Attribute werden nur angezeigt, wenn ihre Qualität stimmt
- MA (35) QS-System für Transaktionsverarbeitung und Datenbestände

4.3.2 Schwachstellen der administrativen Anwendungsfälle

SO6 Organisationen verwalten

R28 Fehlerhafte Konfiguration von Justizbehörden auf der Plattform Justitia.Swiss

Aktuell sind keine Einschränkungen dafür definiert, welche Benutzer welchen Typ von Organisation eröffnen und/oder administrieren können und es sind keine Verfahren für die Verifizierung der erfassten Organisations-Attribute vorgesehen.

Dies würde bedeuten, dass jede im Adressverzeichnis registrierte natürliche Person eine Justizbehörde (respektive deren Profil) eröffnen und mit beliebige Attributwerten (z.B. ihrer eigenen Zustelladresse und Postadresse) versehen kann und dass keinerlei Gewähr für die Korrektheit dieser Attribute besteht.

Dies eröffnet ein grosses Spektrum von absichtlichem Missbrauch oder unbeabsichtigten Fehlkonfigurationen, wie beispielsweise (Liste ist keinesfalls abschliessend):

- Irgendein Inhaber einer digitalen Identität, der sich vorgängig im Adressverzeichnis registriert hat, eröffnet eine nicht existierende Justizbehörde, deren Name einer real existierenden Justizbehörde zum Verwechseln ähnlich sieht. Dabei trägt er elektronische und postalische Adressen ein, die er unter seiner eigenen Kontrolle hat. Anschliessend verleitet er Anwälte und/oder andere Privatpersonen dazu, bei dieser gefälschten Justizbehörde Eingaben mit vertraulichen Dokumenten einzureichen oder von dieser gefälschten Justizbehörde beliebige fingierte Aktenstücke entgegenzunehmen.
- Eine hierzu nicht berechtigte Person eröffnet im Adressverzeichnis eine tatsächlich existierende Justizbehörde, bevor diese selber ihren Eintrag vornimmt. Diese Person nimmt anschliessend im Namen dieser Justizbehörde am ERV und an der eAE teil, bis der Fehler aufgedeckt wird.
- Ein Administrator einer beliebigen bereits eröffneten Organisation (z.B. einer Anwaltskanzlei, einer Rechtsschutzversicherung oder einer angeklagten Firma) verändert absichtlich oder unabsichtlich das Attribut «Typ der Organisation» auf den Wert «Justizbehörde».
- Ein Administrator einer Justizbehörde verändert absichtlich oder unabsichtlich die Attribute, die Delegationen oder die Organisationszugehörigkeiten «seiner» Justizbehörde und ermöglicht es damit einer beliebigen im Adressverzeichnis registrierten anderen Person im Namen dieser Justizbehörde Eingaben einzusehen oder Aktenstücke zuzustellen.

Alle diese Vorfälle können dazu führen, dass

- Eingaben einem falschen Adressaten zugestellt werden;
- Fingierte Aktenstücke zugestellt werden.

Risikobeurteilung:

Ref.	Generisches Risiko	Szenarien	Auswirkungen	Eintrittsw'keit	Risikostufe
R28	GR7, GR10	C1, I1	5 (hoch)	4 (möglich)	**Gross**

Sicherheitsmassnahmen (siehe Kapitel 5):

- MO (1) Detailkonzepte zur Informationssicherheit (Verwaltung von Organisationen)
- MO (6) Periodische Überprüfung des Adressverzeichnisses
- MO (12) Sicherheitsverantwortung der Justizbehörden als Bestandteil des Anschlussvertrages
- MA (26) Definierte minimale Qualitätsstufe für jedes Attribut im Adressverzeichnis
- MA (27) Mehrstufiges Qualitätsmodell für die Attribute im Adressverzeichnis
- MA (28) Definierter Eigentümer für jedes Attribut im Adressverzeichnis
- MA (29) Abgleich mit relevanten Registerdaten, wo sinnvoll
- MA (30) Option: Initial Load aller Justizbehörden und Anwälte
- MA (31) Attribute werden nur angezeigt, wenn ihre Qualität stimmt

R29 Fehlerhafte Konfiguration von Anwaltskanzleien auf der Plattform Justitia.Swiss

Aktuell sind keine Einschränkungen dafür definiert, welche Benutzer welchen Typ von Organisation eröffnen und/oder administrieren können und es sind keine Verfahren für die Verifizierung der erfassten Organisations-Attribute vorgesehen.

Dies würde bedeuten, dass jede im Adressverzeichnis registrierte natürliche Person eine Organisation vom Typ «Anwalt respektive Anwaltskanzlei» eröffnen und mit beliebige Attributwerten versehen kann und dass keinerlei Gewähr für die Korrektheit dieser Attribute besteht.

Dies eröffnet ein grosses Spektrum von absichtlichem Missbrauch oder unbeabsichtigten Fehlkonfigurationen, wie beispielsweise (Liste ist keinesfalls abschliessend):

- Irgendein Inhaber einer digitalen Identität, der sich vorgängig im Adressverzeichnis registriert hat, eröffnet für sich selber eine nicht existierende Organisation vom Typ «Anwalt», deren Name einer real existierenden Anwaltskanzlei zum Verwechseln ähnlich sieht. Dabei trägt er elektronische und postalische Adressen ein, die er unter seiner eigenen Kontrolle hat.
  - Anschliessend verleitet er Mitarbeitende einer Justizbehörde dazu, beliebige Eingaben dieses falschen Anwalts entgegenzunehmen oder Aktenstücke an diesen falschen Anwalt zuzustellen.
  - Alternativ verleitet sie einen Anwalt oder einen anderen Verfahrensbeteiligten dazu, Akteneinsichtsrechte an den falschen Anwalt zu delegieren oder den falschen Anwalt als zusätzliches Mitglied in die eigene Organisation aufzunehmen.
- Eine hierzu nicht berechtigte Person eröffnet im Adressverzeichnis der Plattform Justitia.Swiss eine tatsächlich existierende Anwaltskanzlei, bevor diese selber ihren Eintrag vornimmt. Diese Person nimmt anschliessend im Namen dieser Anwaltskanzlei am ERV und an der eAE teil, bis der Fehler aufgedeckt wird.
- Ein Administrator einer beliebigen bereits eröffneten Organisation (z.B. einer Justizbehörde, einer Rechtsschutzversicherung oder einer angeklagten Firma) verändert absichtlich oder unabsichtlich das Attribut «Typ der Organisation» auf den Wert «Anwalt respektive Anwaltskanzlei».
- Ein Administrator einer Anwaltskanzlei verändert absichtlich oder unabsichtlich die Attribute, die Delegationen oder die Organisationszugehörigkeiten «seiner» Anwaltskanzlei und ermöglicht es damit einer beliebigen im Adressverzeichnis registrierten anderen Person, im Namen dieser Anwaltskanzlei Eingaben einzureichen oder Aktenstücke einzusehen.
- Ein Administrator einer Anwaltskanzlei trägt absichtlich oder unabsichtlich falsche Attribute ein und behindert damit einen Verfahrensablauf (z.B. falsche Spezialisierung, falsche postalische oder elektronische Adressen, etc.).

Alle diese Vorfälle können dazu führen, dass

- beliebige fingierte Eingaben von den Justizbehörden entgegengenommen werden;
- Aktenstücke an falsche Adressaten zugestellt werden.

Risikobeurteilung:

Ref.	Generisches Risiko	Szenarien	Auswirkungen	Eintrittsw'keit	Risikostufe
R28	GR7, GR10	C1, I1	5 (hoch)	5 (wahrscheinlich)	**Gross**

Sicherheitsmassnahmen (siehe Kapitel 5):

- MO (1) Detailkonzepte zur Informationssicherheit (Verwaltung von Organisationen)
- MO (6) Periodische Überprüfung des Adressverzeichnisses
- MA (26) Definierte minimale Qualitätsstufe für jedes Attribut im Adressverzeichnis
- MA (27) Mehrstufiges Qualitätsmodell für die Attribute im Adressverzeichnis
- MA (28) Definierter Eigentümer für jedes Attribut im Adressverzeichnis
- MA (29) Abgleich mit relevanten Registerdaten, wo sinnvoll
- MA (30) Option: Initial Load aller Justizbehörden und Anwälte
- MA (31) Attribute werden nur angezeigt, wenn ihre Qualität stimmt

SO7 Benutzer verwalten

R30 Registrierung eines Benutzers unter einer falschen Identität

Ein unbekannter Dritter registriert sich unter einer falschen Identität im Adressverzeichnis der Plattform Justitia.Swiss und verwendet sein Profil anschliessend dafür, Eingaben unter falschem Namen einzureichen oder Einsichtsrechte auf zugestellte Aktenstücke zu erschleichen.

Risikobeurteilung:

Ref.	Generisches Risiko	Szenarien	Auswirkungen	Eintrittsw'keit	Risikostufe
R30	GR7	I3	4 (wesentlich)	5 (wahrscheinlich)	**Gross**

Sicherheitsmassnahmen (siehe Kapitel 5):

- MO (1) Detailkonzepte zur Informationssicherheit (Verwaltung von Organisationen)
- MO (6) Periodische Überprüfung des Adressverzeichnisses
- MA (25) Benutzerregistrierung nur über akzeptierte Identity Provider (IdP)
- MA (26) Definierte minimale Qualitätsstufe für jedes Attribut im Adressverzeichnis
- MA (27) Mehrstufiges Qualitätsmodell für die Attribute im Adressverzeichnis
- MA (28) Definierter Eigentümer für jedes Attribut im Adressverzeichnis
- MA (29) Abgleich mit relevanten Registerdaten, wo sinnvoll
- MA (30) Option: Initial Load aller Justizbehörden und Anwälte
- MA (31) Attribute werden nur angezeigt, wenn ihre Qualität stimmt

R31 Fehlerhafte Verwaltung von Benutzerattributen im Adressverzeichnis

Benutzer können sich nur mit einer digitalen Identität eines Identity Providers registrieren, der die von der Plattform Justitia.Swiss geforderten Qualitätsstufe erfüllt (vgl. Massnahme MA (25)). Für die (wenigen) Attribute der zivilen Identität ist somit eine ausreichende Gewähr für ihre Korrektheit gegeben.

Mit Ausnahme der Organisationszugehörigkeit (vgl. SO8) sollen alle Attribute einer natürlichen Person, die nicht von einem Identity Provider bezogen werden, von der natürlichen Person im Sinne einer Selbstdeklaration selber erfasst werden. Der Benutzer kann somit absichtlich oder unabsichtlich beliebige Werte für diese Attribute angeben. Je nachdem, um welche Attribute es sich handelt und von welchen Systemen und zu welchem Zweck diese Attribute verwendet werden, kann dies zu Fehlern oder unberechtigten Datenzugriffen führen.

Hinweis: Bei «normalen» Informationssystemen, die innerhalb einer Organisation betrieben und genutzt werden, stellt sich dieses Problem nicht oder zumindest weniger. Dies liegt daran, dass die Benutzerverzeichnisse solcher Systeme über bereits etablierte organisationsinterne Prozesse der Personalverwaltung administriert werden und einer mehr oder weniger klaren Verantwortlichkeit unterliegen. Dies ist beim Adressverzeichnis der Plattform Justitia.Swiss nicht *per se* gegeben.

Risikobeurteilung:

Ref.	Generisches Risiko	Szenarien	Auswirkungen	Eintrittsw'keit	Risikostufe
R31	GR7, GR10	I3	3 (moderat)	6 (sehr wahrscheinlich)	**Gross**

Sicherheitsmassnahmen (siehe Kapitel 5):

- MO (1) Detailkonzepte zur Informationssicherheit (Verwaltung von Benutzern)
- MO (6) Periodische Überprüfung des Adressverzeichnisses
- MA (26) Definierte minimale Qualitätsstufe für jedes Attribut im Adressverzeichnis
- MA (27) Mehrstufiges Qualitätsmodell für die Attribute im Adressverzeichnis
- MA (28) Definierter Eigentümer für jedes Attribut im Adressverzeichnis
- MA (29) Abgleich mit relevanten Registerdaten, wo sinnvoll
- MA (30) Option: Initial Load aller Justizbehörden und Anwälte

- MA (31) Attribute werden nur angezeigt, wenn ihre Qualität stimmt
- MA (33) Regeln für Organisationszuweisung vorsehen

SO8 Organisationszugehörigkeiten verwalten

R32 Fehlerhafte Erfassung von Organisationszugehörigkeiten

Bei der Erfassung von Organisationszugehörigkeiten sind derzeit keinerlei Einschränkungen oder Plausibilisierungen vorgesehen:

- Eine natürliche Person kann gleichzeitig Mitglied beliebig vieler Organisationen sein;
- Eine natürliche Person kann bei jeder Organisation jede Funktion innehaben;
- Zwischen den elektronischen oder postalischen Adressen der Organisation und ihrer Mitglieder werden keine Übereinstimmungen (z.B. E-Mail-Adresse mit gleicher Domäne) verlangt.

Diese Lösung bietet maximale Flexibilität. Sie eröffnet aber auch viele Möglichkeiten für die missbräuchliche oder irrtümliche Zuweisung einer falschen Organisationszugehörigkeit oder Funktion.

Risikobeurteilung:

Ref.	Generisches Risiko	Szenarien	Auswirkungen	Eintrittsw'keit	Risikostufe
R32	GR10, GR11	C2, I2	4 (wesentlich)	4 (möglich)	Mittel

Sicherheitsmassnahmen (siehe Kapitel 5):

- MO (1) Detailkonzepte zur Informationssicherheit (Verwaltung von Organisationen)
- MO (6) Periodische Überprüfung des Adressverzeichnisses
- MA (33) Regeln für Organisationszuweisung vorsehen

R33 Fehlerhafte Zuweisung von Funktionen mit weitreichenden Berechtigungen

Gewisse Funktionen ermöglichen dem Funktionsinhaber Aktivitäten, die bei einem absichtlichen Missbrauch oder einer Fehlbedienung einen erheblichen Schaden verursachen können. Beispiele solcher Funktionen sind (Auflistung ist nicht abschliessend):

- Ein Benutzer mit der Funktion «Zustellungen aufgeben» kann jedem Teilnehmer volle Einsichtsrechte in alle Akten seiner Organisation erteilen, weil er für die Erfassung der Zustellung alle in der elektronischen Akte gespeicherten Aktenstücke zur Auswahl haben muss;
- Ein Benutzer mit der Funktion «Zustellungen aufgeben» kann, wenn die Justizbehörde den zentralen DossierStore der Plattform nutzt, beliebige Dateien in die einsehbare Akte aufnehmen;
- Der Organisations-Administrator einer Justizbehörde kann einem beliebigen im Adressverzeichnis registrierten Benutzer (und insbesondere auch sich selber) volle Einsichtsrechte in alle Akten seiner Organisation erteilen, indem er ihm die Funktion «Zustellungen aufgeben» zuweist;
- Der Organisations-Administrator einer Anwaltskanzlei benötigt den lesenden Zugriff auf das gesamte Adressverzeichnis, damit er die Organisationszugehörigkeiten verwalten kann;
- Die Funktion «handelnd» ist noch nicht näher definiert. Die Namensgebung impliziert aber, dass der Funktionsinhaber stellvertretend für die Organisation gewisse Handlungen ausführen kann.

Aktuell ist nicht vorgesehen, dass die Zuweisung von Funktionen mit besonders weitreichenden Berechtigungen speziell gehandhabt oder kontrolliert wird.

Risikobeurteilung:

Ref.	Generisches Risiko	Szenarien	Auswirkungen	Eintrittsw'keit	Risikostufe
R32	GR10, GR11	C2, I2	5 (hoch)	3 (selten)	Mittel

Sicherheitsmassnahmen (siehe Kapitel 5):

- MO (1) Detailkonzepte zur Informationssicherheit (Berechtigungskonzept)
- MO (6) Periodische Überprüfung des Adressverzeichnisses

- MO (9) Ein Profil pro Organisationszugehörigkeit

R34 Organisationszugehörigkeiten werden nicht nachgeführt

Organisatorische Veränderungen (z.B. Austritt oder interner Funktionswechsel von Kanzleimitarbeitenden) müssen von den Organisations-Administratoren bei der Verwaltung der Organisationszugehörigkeiten manuell nachgeführt werden, weil die Plattform Justitia.Swiss keinen Abgleich mit externen Systemen (z.B. HR-Systeme von Justizbehörden oder Anwaltskanzleien) vorsieht.

Die Erfahrung aus grösseren Organisationen zeigt, dass Austritte und interne Funktionswechsel in manuell administrierten Benutzerverzeichnissen häufig nur mit Verzögerung oder gar nicht nachgeführt werden. Dies kann dazu führen, dass ein Benutzer, der beispielsweise von einer Justizbehörde zu einer Anwaltskanzlei wechselt, die Berechtigungen seiner alten Anstellung auch im Rahmen der neuen Anstellung für eine gewisse Zeit weiterverwenden kann.

Die Eintrittswahrscheinlichkeit eines Schadenfalles ist in einem solchen Fall besonders gross, weil der Teilnehmer bei einem Wechsel seiner Organisationszugehörigkeit sein Profil auf der Plattform Justitia.Swiss behält (dies als grosser Unterschied zu den organisationsinternen IT-Systemen, bei denen die Benutzerkonten bei einem Austritt des Mitarbeitenden aus der Organisation gesperrt werden).

Risikobeurteilung:

Ref.	Generisches Risiko	Szenarien	Auswirkungen	Eintrittsw'keit	Risikostufe
R32	GR10, GR11	C2, I2	4 (wesentlich)	5 (wahrscheinlich)	**Gross**

Sicherheitsmassnahmen (siehe Kapitel 5):

- MO (5) Periodische Überprüfung des Adressverzeichnisses
- MO (9) Ein Profil pro Organisationszugehörigkeit
- MA (25) Benutzerregistrierung nur über akzeptierte Identity Provider (IdP)

R35 Unerwünschte Rechtekumulation bei «Mehrfachanstellungen»

Ein Teilnehmer, der gleichzeitig Mitglied von mehreren Organisationen ist, verfügt auf der Plattform Justitia.Swiss über die kumulierten Berechtigungen aller seiner Organisationszugehörigkeiten. Dies ist grundsätzlich nicht gewünscht aufgrund der folgenden Risiken:

- Ist ein Anwalt gleichzeitig auch einer Justizbehörde zugeordnet (z.B. als Laienrichter), so verfügt er über Lesezugriff auf das gesamte Adressverzeichnis, auch während er für seine Anwaltskanzlei tätig ist.
- Ist ein Mitarbeiter einer verfahrensleitenden Justizbehörde gleichzeitig als Privatperson Kläger in einem Verfahren, so verfügt er auch als Verfahrensbeteiligter über Lesezugriff auf das gesamte Adressverzeichnis und alle weiteren Berechtigungen seiner Funktion bei der Justizbehörde.
- Arbeitet ein Kanzleimitarbeiter in Teilzeit für mehrere Justizbehörden («Mehrfachanstellung»), so verfügt er während seiner Arbeit bei der einen Justizbehörde auch über alle Berechtigungen, die zu seinen anderen Organisationszugehörigkeiten gehören. Solche «Mehrfachanstellungen» können dazu führen, dass Aktenstücke oder andere schützenswerte Informationen irrtümlich oder missbräuchlich zwischen Justizbehörden ausgetauscht werden.

Risikobeurteilung:

Ref.	Generisches Risiko	Szenarien	Auswirkungen	Eintrittsw'keit	Risikostufe
R32	GR10, GR11	C2, I2	3 (moderat)	4 (möglich)	Mittel

Sicherheitsmassnahmen (siehe Kapitel 5):

- MO (6) Periodische Überprüfung des Adressverzeichnisses
- MO (9) Ein Profil pro Organisationszugehörigkeit
- MA (32) Festlegen der organisationsunabhängigen Grundberechtigungen

SO9 Plattform-Berechtigungen verwalten

R36 Zu weit reichende organisationsunabhängige Grundberechtigungen

Gewisse Berechtigungen auf der Plattform Justitia.Swiss können nicht an eine Organisationszugehörigkeit gebunden sein, weil sie auch für verfahrensbeteiligte Privatpersonen verfügbar sein müssen. Diese organisationsunabhängigen Grundberechtigungen stehen somit jeder natürlichen Person zur Verfügung, die über eine digitale Identität verfügt und sich auf der Plattform Justitia.Swiss registrieren kann, also mindestens der gesamten Schweizer Wohnbevölkerung.

Beispiele für solche organisationsunabhängigen Berechtigungen sind (nicht abschliessend):

- Das Einreichen einer Eingabe;
- Die teilweise Einsicht in das Adressverzeichnis (nur die Einträge der Justizbehörden);
- Das Empfangen einer Zustellung und die elektronische Einsicht in zugestellte Aktenstücke;
- Die Bearbeitung der eigenen Benutzerattribute;
- Das Delegieren der eigenen Berechtigungen an beliebige andere Teilnehmer.

So lange die Liste dieser Grundberechtigungen nicht abschliessend fixiert ist, besteht das Risiko, dass unerwünschte Berechtigungen dabei sind.

Risikobeurteilung:

Ref.	Generisches Risiko	Szenarien	Auswirkungen	Eintrittsw'keit	Risikostufe
R32	GR10, GR11	C2, I2	3 (moderat)	3 (selten)	Mittel

Sicherheitsmassnahmen (siehe Kapitel 5):

- MO (1) Detailkonzepte zur Informationssicherheit (Berechtigungskonzept)
- MA (32) Festlegen der organisationsunabhängigen Grundberechtigungen
- MA (34) Delegationen sind befristet und maximal 12 Monate gültig

SO10 Delegationen verwalten

R37 Delegationen werden nicht nachgeführt

Organisatorische Veränderungen (z.B. Austritt oder interner Funktionswechsel von Kanzleimitarbeitenden) können die Anpassung von Delegationen erforderlich machen.

Die Erfahrung aus grösseren Organisationen zeigt, dass Austritte und interne Funktionswechsel in manuell administrierten Benutzerverzeichnissen häufig nur mit Verzögerung oder gar nicht nachgeführt werden. Dies kann dazu führen, dass ein Benutzer, der beispielsweise von einer Anwaltskanzlei zu einer anderen Anwaltskanzlei wechselt, die Berechtigungen seiner alten Anstellung auch im Rahmen der neuen Anstellung für eine gewisse Zeit weiterverwenden kann.

Risikobeurteilung:

Ref.	Generisches Risiko	Szenarien	Auswirkungen	Eintrittsw'keit	Risikostufe
R32	GR10, GR11	C2, I2	4 (wesentlich)	5 (wahrscheinlich)	**Gross**

Sicherheitsmassnahmen (siehe Kapitel 5):

- MO (7) Periodische Rezertifizierung aller gültigen Zustellungen
- MO (8) Quartalsweise Rezertifizierung aller gültigen Delegationen
- MO (9) Ein Profil pro Organisationszugehörigkeit
- MA (34) Delegationen sind befristet und maximal 12 Monate gültig

R38 Mangelhafte Auskunftsfähigkeit über bestehende Berechtigungen

Die Berechtigungsvergabe auf der Plattform Justitia.Swiss erfolgt auf drei Ebenen:

- Die Berechtigungen zur Einsicht in Akten und Aktenstücke werden durch die Funktion «Zustellungen aufgeben» im Rahmen von Zustellungen erteilt, wobei auch nachträgliche Veränderungen (mindestens die Annullierung von Zustellungen) möglich sind;
- Die Berechtigungen zur Nutzung von Funktionen und Daten der Plattform Justitia.Swiss werden durch die Funktion «Organisations-Administrator» im Rahmen von Organisationsmitgliedschaften mit Funktionszuweisungen erteilt. Ein Teilnehmer kann gleichzeitig Mitglied von mehreren Organisationen sein und bei jeder dieser Organisationen gleichzeitig mehrere Funktionen innehaben;
- Alle diese Berechtigungen können vom berechtigten Teilnehmer nach eigenem Ermessen an beliebige andere Teilnehmer delegiert werden.

Keine Organisation verfügt über alle erforderlichen Daten bzw. Kompetenzen, um die zu einem bestimmten Zeitpunkt für einen bestimmten Teilnehmer gültigen Berechtigungen ausweisen und nachvollziehen zu können.

Risikobeurteilung:

Ref.	Generisches Risiko	Szenarien	Auswirkungen	Eintrittsw'keit	Risikostufe
R32	GR10, GR11	N3, N4	2 (gering)	6 (sehr wahrscheinlich)	Mittel

Sicherheitsmassnahmen (siehe Kapitel 5):

- MO (9) Ein Profil pro Organisationszugehörigkeit

R39 Keine Gesamtverantwortung für die Berechtigungen und Attribute eines Teilnehmers

Die Teilnehmer können zwar mehreren Organisationen als Mitglied zugeordnet sein, sie sind aber keiner einzelnen Organisation zugeordnet bzw. untergeordnet.

Es gibt somit keine Organisation, der die Gesamtverantwortung für die Berechtigungen eines Teilnehmers und die Korrektheit aller seiner Attribute zugewiesen werden kann.

Risikobeurteilung:

Ref.	Generisches Risiko	Szenarien	Auswirkungen	Eintrittsw'keit	Risikostufe
R32	GR10, GR11	N3, N4	2 (gering)	6 (sehr wahrscheinlich)	Mittel

Sicherheitsmassnahmen (siehe Kapitel 5):

- MO (9) Ein Profil pro Organisationszugehörigkeit

4.3.3 Schwachstellen der Betriebsprozesse

SO11 Service Management

R40 Sicherheitsrisiken werden nicht angemessen behandelt

Die Aufbau- und Ablauforganisation der öffentlich-rechtlichen Körperschaft (örK) stellt nicht sicher, dass die von internen und externen Bedrohungen ausgehenden Sicherheitsrisiken angemessen adressiert werden.

Risikobeurteilung:

Ref.	Generisches Risiko	Szenarien	Auswirkungen	Eintrittsw'keit	Risikostufe
R32	GR6	alle	4 (wesentlich)	4 (möglich)	Mittel

Sicherheitsmassnahmen (siehe Kapitel 5):

- MO (2) Nach ISO/IEC 27001 zertifiziertes ISMS der örK
- MA (12) Zugriffskontrollsystem für Daten und Funktionen der Plattform Justitia.Swiss
- MO (18) Pentest (Manual Hacking) aller Benutzerschnittstellen
- MO (19) Vulnerability-Monitoring aller Internet-Zugangspunkte

R41 Mangelhafte Berechtigungsverwaltung für Mitarbeitende der örK

Das administrative Personal der öffentlich-rechtlichen Körperschaft (örK) verfügt auf der Plattform Justitia.Swiss nicht über die Berechtigungen, die es für die Erfüllung ihrer Aufgaben benötigt:

- Fehlende Berechtigungen beeinträchtigen die Aufgabenerfüllung;
- Überflüssige Berechtigungen führen zu unnötigen Risiken für die Datensicherheit.

Risikobeurteilung:

Ref.	Generisches Risiko	Szenarien	Auswirkungen	Eintrittsw'keit	Risikostufe
R32	GR10, GR11	C2, I2	3 (moderat)	4 (möglich)	Mittel

Sicherheitsmassnahmen (siehe Kapitel 5):

- MO (1) Detailkonzepte zur Informationssicherheit (Berechtigungskonzept)
- MO (15) Zuverlässige Anruferidentifikation durch den Service Desk
- MA (12) Zugriffskontrollsystem für Daten und Funktionen der Plattform Justitia.Swiss

SO12 Support der Plattformbenutzer (Service Desk)

R42 Ein Anrufer gibt sich gegenüber dem Service Desk als eine andere Person aus

Einem unbekannten Dritten gelingt es, sich gegenüber dem Service Desk der Plattform Justitia.Swiss (z.B. am Telefon oder via E-Mail) als eine andere Person auszugeben und sich auf diesem Weg den unberechtigten Zugang zu schützenswerten Informationen zu verschaffen.

Weil der Service Desk der Plattform Justitia.Swiss keine Authentifizierungsmittel (Passwörter u.dgl.) zurücksetzen kann (dies ist eine Aufgabe der Identity Provider), ist das Risiko stark begrenzt. Es besteht aber doch eine gewisse Gefahr, dass der Service Desk Auskunft über Informationen gibt, die datenschutzrelevant sind.

Risikobeurteilung:

Ref.	Generisches Risiko	Szenarien	Auswirkungen	Eintrittsw'keit	Risikostufe
R32	GR10, GR11	C2, I2	5 (hoch)	3 (selten)	Mittel

Sicherheitsmassnahmen (siehe Kapitel 5):

- MO (15) Zuverlässige Anruferidentifikation durch den Service Desk

R43 Unberechtigte Dateneinsicht beim Supportzugriff durch den Service Desk

Für die effiziente Unterstützung eines Benutzers ist die Nutzung von Werkzeugen für den Fernzugriff des Service Desk auf das Endgerät des Benutzers (*Remote Assistance*) heute weit verbreitet. Dabei besteht das Risiko, dass Mitarbeitende des Service Desk unberechtigterweise (evtl. sogar unbemerkt) zumindest lesenden Zugriff auf den Bildschirm des Benutzers und die dort dargestellten Daten erhält.

Risikobeurteilung:

Ref.	Generisches Risiko	Szenarien	Auswirkungen	Eintrittsw'keit	Risikostufe
R32	GR10, GR11	C2, I2	5 (hoch)	3 (selten)	Mittel

Sicherheitsmassnahmen (siehe Kapitel 5):

- MT (11) Sichere Remote Support Lösung im Service Desk
- MA (12) Zugriffskontrollsystem für Daten und Funktionen der Plattform Justitia.Swiss
- MA (13) Eingaben und Aktenstücke werden ausserhalb des DossierStore nicht aufbewahrt

R44 Mangelhafte Berechtigungsverwaltung für Mitarbeitende des Service Desk

Das Personal des Service Desk beim Plattformprovider verfügt auf der Plattform Justitia.Swiss nicht über die Berechtigungen, die es für die Erfüllung ihrer Aufgaben benötigt:

- Fehlende Berechtigungen beeinträchtigen die Aufgabenerfüllung;
- Überflüssige Berechtigungen führen zu unnötigen Risiken für die Datensicherheit.

Risikobeurteilung:

Ref.	Generisches Risiko	Szenarien	Auswirkungen	Eintrittsw'keit	Risikostufe
R32	GR10, GR11	C2, I2	5 (hoch)	3 (selten)	Mittel

Sicherheitsmassnahmen (siehe Kapitel 5):

- MO (1) Detailkonzepte zur Informationssicherheit (Berechtigungskonzept)
- MA (12) Zugriffskontrollsystem für Daten und Funktionen der Plattform Justitia.Swiss

SO13 Betrieb des Security Operations Center (SOC)

R45 Datenschutzverletzung beim Betrieb des Security Operations Center

Die Mitarbeitenden des SOC beziehungsweise die vom SOC benötigten Werkzeuge für die laufende Überwachung und Lagebeurteilung benötigen den Zugriff auf das Log und den Audit Trail der Plattform Justitia.Swiss. Es besteht das Risiko einer Datenschutzverletzung, wenn der Zugriff nicht angemessen auf spezifische Daten und Anwendungsfälle beschränkt ist.

Risikobeurteilung:

Ref.	Generisches Risiko	Szenarien	Auswirkungen	Eintrittsw'keit	Risikostufe
R32	GR10, GR11	C2, I2	5 (hoch)	3 (selten)	Mittel

Sicherheitsmassnahmen (siehe Kapitel 5):

- MO (1) Detailkonzepte zur Informationssicherheit (Datenbearbeitungsreglement)
- MO (3) Security Information and Event Management (SIEM)

SO14 Entwicklung und Weiterentwicklung der Plattform

R46 Software mit Sicherheitsschwachstellen

Auf Grund von Sicherheitsschwachstellen in der Software der Plattform Justitia.Swiss werden Funktionen oder Daten der Plattform gegenüber unberechtigten Dritten exponiert.

Risikobeurteilung:

Ref.	Generisches Risiko	Szenarien	Auswirkungen	Eintrittsw'keit	Risikostufe
R48	GR9	C1, I1	6 (sehr hoch)	3 (selten)	**Gross**

Sicherheitsmassnahmen (siehe Kapitel 5):

- MO (16) Secure Software Development
- MO (20) Quelltext-Analyse aller Sicherheitsmodule

R47 Mangelhafte Berechtigungsverwaltung für Mitarbeitende des Softwareentwicklers

Das DevOps-Personal des Softwareentwicklers verfügt auf der Plattform Justitia.Swiss nicht über die Berechtigungen, die es für die Erfüllung ihrer Aufgaben benötigt:

- Fehlende Berechtigungen beeinträchtigen die Aufgabenerfüllung;
- Überflüssige Berechtigungen führen zu unnötigen Risiken für die Datensicherheit.

Risikobeurteilung:

Ref.	Generisches Risiko	Szenarien	Auswirkungen	Eintrittsw'keit	Risikostufe
R32	GR10, GR11	C2, I2	5 (hoch)	3 (selten)	Mittel

Sicherheitsmassnahmen (siehe Kapitel 5):

- MO (1) Detailkonzepte zur Informationssicherheit (Berechtigungskonzept)
- MO (10) Sicherheitsverantwortung des Softwarelieferanten als Vertragsbestandteil
- MA (12) Zugriffskontrollsystem für Daten und Funktionen der Plattform Justitia.Swiss

SO15 Betrieb der Plattform Justitia.Swiss mit ihren Schnittstellen

R48 Erfolgreicher Hackerangriff auf die Plattform Justitia.Swiss

Einem anonym aus dem Internet zugreifenden Hacker gelingt es, z.B. auf Grund eines Softwarefehlers, einer veralteten Softwareversion oder eines Konfigurationsfehlers, sich Zugang auf die Plattform Justitia.Swiss zu verschaffen. In der Folge nutzt er diesen Zugang, um die über die Plattform transferierten Daten einzusehen oder die auf der Plattform gespeicherten Daten zu manipulieren.

Risikobeurteilung:

Ref.	Generisches Risiko	Szenarien	Auswirkungen	Eintrittsw'keit	Risikostufe
R48	GR7, GR9	C1, I1	6 (sehr hoch)	4 (möglich)	**Gross**

Sicherheitsmassnahmen (siehe Kapitel 5):

- MO (3) Security Information and Event Management (SIEM)
- MO (10) Sicherheitsverantwortung des Softwarelieferanten als Vertragsbestandteil
- MO (11) Sicherheitsverantwortung des Softwarelieferanten als Vertragsbestandteil
- MO (18) Pentest (Manual Hacking) aller Benutzerschnittstellen
- MO (19) Vulnerability-Monitoring aller Internet-Zugangspunkte
- MA (6) 2-Faktor-Authentifizierung (2FA) aller Benutzer
- MA (13) Eingaben und Aktenstücke werden ausserhalb des DossierStore nicht aufbewahrt
- MT (6) Web Application Firewall (WAF)
- MT (7) Risikoabhängige Zugriffskontrolle auf der Justitia.Swiss-Plattform
- MT (8) Begrenzte Session-Lebensdauer auf der Justitia.Swiss-Plattform
- MT (9) Physische Separierung (anonymer Bereich sowie nicht-produktiver und produktiver Umgebungen)
- MT (12) Hardware Security Module (HSM) als Schlüsselspeicher auf der Plattform
- MT (13) Zentraler Protokollierungsdienst für technische Logs und den Audit Trail

R49 Missbrauch eines Benutzerzugangs auf die Plattform Justitia.Swiss

Einem angemeldeten Benutzer oder einem API-Client gelingt es, aus dem Applikationskontext auszubrechen und unter Umgehung der Zugriffskontrolle auf die Funktionen und/oder Daten der Plattform Justitia.Swiss zuzugreifen.

Beim Angreifer kann es sich um einen böswilligen Benutzer der Plattform handeln (z.B. eine Privatperson oder einen anderen Verfahrensbeteiligten) oder um einen unbekannten Dritten, der sich die Kontrolle über eine Benutzersession oder das Endgerät eines Benutzers verschafft hat.

Risikobeurteilung:

Ref.	Generisches Risiko	Szenarien	Auswirkungen	Eintrittsw'keit	Risikostufe
R49	GR7, GR9, GR10	C1, I1	6 (sehr hoch)	4 (möglich)	**Gross**

Sicherheitsmassnahmen (siehe Kapitel 5):

- MO (3) Security Information and Event Management (SIEM)
- MO (4) Awareness-Programm für alle Benutzergruppen
- MO (10) Sicherheitsverantwortung des Softwarelieferanten als Vertragsbestandteil
- MO (11) Sicherheitsverantwortung des Plattformbetreibers als Vertragsbestandteil
- MO (13) Sicherheitsverantwortung der Verfahrensbeteiligten als Teil der Nutzungsbedingungen
- MO (17) Auditrecht der öffentlich-rechtlichen Körperschaft beim Plattformbetreiber
- MO (18) Pentest (Manual Hacking) aller Benutzerschnittstellen
- MA (6) 2-Faktor-Authentifizierung (2FA) aller Benutzer

- MA (7) Anbindung der Identity Provider über sichere Federation Protokolle
- MA (8) Gegenseitige Authentifizierung der Endpunkte bei allen API-Verbindungen
- MA (11) Sichere Postfächer für verfahrensleitende Justizbehörden
- MA (12) Zugriffskontrollsystem für Daten und Funktionen der Plattform Justitia.Swiss
- MT (6) Web Application Firewall (WAF) und API-Gateway
- MT (7) Risikoabhängige Zugriffskontrolle auf der Justitia.Swiss-Plattform
- MT (8) Begrenzte Session-Lebensdauer auf der Justitia.Swiss-Plattform
- MT (9) Physische Separierung (anonymer Bereich sowie nicht-produktiver und produktiver Umgebungen)
- MT (13) Zentraler Protokollierungsdienst für technische Logs und den Audit Trail

R50 Missbrauch eines Administrationszugangs auf die Plattform Justitia.Swiss

Ein manueller (Administrationsoberfläche) oder maschineller (Systems Management Werkzeuge) Zugang mit weitgehenden Berechtigungen wird missbraucht, um die über die Plattform transferierten Daten einzusehen oder die auf der Plattform gespeicherten Daten zu manipulieren.

Beim Angreifer kann es sich um einen böswilligen Administrator der Plattform handeln oder um einen unbekannten Dritten, der sich Zugang zur Umgebung des Plattformbetreibers verschafft hat.

Risikobeurteilung:

Ref.	Generisches Risiko	Szenarien	Auswirkungen	Eintrittsw'keit	Risikostufe
R50	GR7, GR10	C1, I1	6 (sehr hoch)	3 (selten)	**Gross**

Sicherheitsmassnahmen (siehe Kapitel 5):

- MO (3) Security Information and Event Management (SIEM)
- MO (11) Sicherheitsverantwortung des Plattformbetreibers als Vertragsbestandteil
- MT (10) Sicherer Administrationszugang beim Plattformbetreiber (PAM)
- MT (12) Hardware Security Module (HSM) als Schlüsselspeicher auf der Plattform
- MT (13) Zentraler Protokollierungsdienst für technische Logs und den Audit Trail

R51 Kompromittierung des Signierschlüssels der Plattform Justitia.Swiss

Der private Schlüssel, mit dem das elektronische Plattform-Siegel für Eingaben erzeugt wird, wird für die Erzeugung von gefälschten Eingaben mit beliebigen Inhalten verwendet.

Dies kann erfolgen, indem der private Schlüssel kopiert und gestohlen wird oder indem die kryptographische Signierfunktion von einer unautorisierten Software aufgerufen wird. In beiden Fällen ist es möglich, eine Attacke unbemerkt durchzuführen.

Risikobeurteilung:

Ref.	Generisches Risiko	Szenarien	Auswirkungen	Eintrittsw'keit	Risikostufe
R51	GR7	I1	6 (sehr hoch)	3 (selten)	**Gross**

Sicherheitsmassnahmen (siehe Kapitel 5):

- MO (11) Sicherheitsverantwortung des Plattformbetreibers als Vertragsbedingung
- MT (12) Hardware Security Module (HSM) als Schlüsselspeicher auf der Plattform

R52 Erfolgreiche Denial of Service (DoS) Attacke auf die Plattform Justitia.Swiss

Die Internetschnittstelle der Justitia.Swiss-Plattform wird von unbekannten Dritten überlastet, so dass der Service gegenüber den berechtigten Benutzern nicht mehr erbracht werden kann.

Risikobeurteilung:

Ref.	Generisches Risiko	Szenarien	Auswirkungen	Eintrittsw'keit	Risikostufe
0	GR14	A2	2 (gering)	5 (wahrscheinlich)	Mittel

Sicherheitsmassnahmen (siehe Kapitel 5):

- MO (3) Security Information and Event Management (SIEM)
- MO (11) Sicherheitsverantwortung des Plattformbetreibers als Vertragsbestandteil
- MT (14) Sichere Konfiguration aller Webserver der Plattform Justitia.Swiss

R53 DNS Spoofing oder Phishing

Mittels DNS-Cache-Poisoning oder Phishing wird der Benutzer auf eine gefälschte Webseite umgeleitet. Der Angreifer hat die volle Kontrolle über diese Seite und kann somit dem Browser des Benutzers beliebige Inhalte liefern. Der Angreifer kann sich in die Kommunikation vom Benutzer zur Webseite einschalten, Inhalte mitlesen und übermittelte Daten manipulieren.

Dies kann insbesondere betreffen:

- Die Verbindung zwischen einem Browser und der Justitia.Swiss-Plattform;
- Die Verbindung zwischen einer integrierten Kanzleisoftware und der Justitia.Swiss-Plattform;
- Die Verbindung zwischen der Justitia.Swiss-Plattform und einem Plattformadapter.

Risikobeurteilung:

Ref.	Generisches Risiko	Szenarien	Auswirkungen	Eintrittsw'keit	Risikostufe
R53	GR7	C2, I2	4 (wesentlich)	3 (selten)	Mittel

Sicherheitsmassnahmen (siehe Kapitel 5):

- MO (3) Security Information and Event Management (SIEM)
- MO (4) Awareness-Programm für alle Benutzergruppen
- MT (14) Sichere Konfiguration aller Webserver der Plattform Justitia.Swiss

R54 Totalverlust der Plattform Justitia.Swiss im Katastrophenfall

Durch den Einfluss höherer Gewalt (z.B. Feuer im Rechenzentrum) oder durch einen gravierenden Fehler seitens des Plattformbetreibers kann die Justitia.Swiss-Plattform nicht mehr genutzt werden.

Risikobeurteilung:

Ref.	Generisches Risiko	Szenarien	Auswirkungen	Eintrittsw'keit	Risikostufe
R54	GR1, GR16	A1	4 (wesentlich)	2 (unwahrscheinlich)	Mittel

Sicherheitsmassnahmen (siehe Kapitel 5):

- MT (15) Ausweichstandort und BCM

4.4 Risikoübersicht vor Massnamen

Die Risikobewertung «vor» Umsetzung der Massnahme kann zum aktuellen Zeitpunkt definiert werden. Die Bewertung «nach» der Umsetzung erfolgt während der Entwicklungsphase. Beide Werte werden kontinuierlich nachgeführt.

ID	Titel	vor	nach
R1	Eingaben werden nach dem Versand verändert	Gross	
R2	Eingaben werden abgestritten	Mittel	
R3	Eingaben werden unter einer falschen Identität eingereicht	Gross	
R4	Eingaben werden mit einer falschen AkteID eingereicht	Mittel	
R5	Eingaben werden von unberechtigten Dritten eingesehen	Gross	
R6	Eingaben gehen verloren	Mittel	
R7	Mit Schadsoftware verseuchte Eingaben schädigen die IT-Systeme anderer Teilnehmer	Gross	
R9	Eingaben oder Zustellungen können vom Empfänger nicht gelesen werden	klein	
R9	Aktenstücke werden auf dem Zustellweg manipuliert oder gehen verloren	Gross	
R10	Der Empfang zugestellter Aktenstücke wird abgestritten	Gross	
R11	Die Integrität zugestellter Aktenstücke wird abgestritten	Mittel	
R12	Der Versand einer Zustellung wird abgestritten	Mittel	
R13	Der Empfänger einer Zustellung wird nicht erreicht	Mittel	
R14	Eine fehlerhafte Zustellung führt zu unerwünschtem Aktenzugriff	Gross	
R15	Zustellungen sind nicht mehr aktuell	Mittel	
R16	Es werden gefälschte Zustellungen erfasst	Gross	
R17	Akten werden von unberechtigten Dritten über die Plattform eingesehen	Gross	
R18	Akten werden von unberechtigten Dritten direkt aus einem DossierStore bezogen	Gross	
R19	Akten werden ohne eine vorgängige Zustellung über die Plattform eingesehen	Mittel	
R20	Mit Schadsoftware verseuchte Aktenstücke werden zugestellt	Mittel	
R21	Unberechtigte Einsicht in verfahrensbezogene Randdaten	Mittel	
R22	Für verfahrensbeteiligte Justizbehörden werden Sicherheitsmassnahmen nicht umgesetzt	Mittel	
R23	Aktenstücke im zentralen DossierStore werden verändert	Gross	
R24	Aktenstücke im zentralen DossierStore werden von unberechtigten Dritten eingesehen	Gross	
R25	Aktenstücke im zentralen DossierStore gehen verloren	klein	
R26	Aktenstücke im zentralen DossierStore werden nicht nachgeführt	Mittel	
R27	Nicht mehr benötigte Aktenstücke im zentralen DossierStore werden nicht gelöscht	Mittel	
R28	Fehlerhafte Konfiguration von Justizbehörden auf der Plattform Justitia.Swiss	Gross	
R29	Fehlerhafte Konfiguration von Anwaltskanzleien auf der Plattform Justitia.Swiss	Gross	
R30	Registrierung eines Benutzers unter einer falschen Identität	Gross	
R31	Fehlerhafte Verwaltung von Benutzerattributen im Adressverzeichnis	Gross	

R32	Fehlerhafte Erfassung von Organisationszugehörigkeiten	Mittel	
R33	Fehlerhafte Zuweisung von Funktionen mit weitreichenden Berechtigungen	Mittel	
R34	Organisationszugehörigkeiten werden nicht nachgeführt	**Gross**	
R35	Unerwünschte Rechtekumulation bei «Mehrfachanstellungen»	Mittel	
R36	Zu weit reichende organisationsunabhängige Grundberechtigungen	Mittel	
R37	Delegationen werden nicht nachgeführt	**Gross**	
R38	Mangelhafte Auskunftsfähigkeit über bestehende Berechtigungen	Mittel	
R39	Keine Gesamtverantwortung für die Berechtigungen und Attribute eines Teilnehmers	Mittel	
R40	Sicherheitsrisiken werden nicht angemessen behandelt	Mittel	
R41	Mangelhafte Berechtigungsverwaltung für Mitarbeitende der örK	Mittel	
R42	Ein Anrufer gibt sich gegenüber dem Service Desk als eine andere Person aus	Mittel	
R43	Unberechtigte Dateneinsicht beim Supportzugriff durch den Service Desk	Mittel	
R44	Mangelhafte Berechtigungsverwaltung für Mitarbeitende des Service Desk	Mittel	
R45	Datenschutzverletzung beim Betrieb des Security Operations Center	Mittel	
R46	Software mit Sicherheitsschwachstellen	**Gross**	
R47	Mangelhafte Berechtigungsverwaltung für Mitarbeitende des Softwareentwicklers	Mittel	
R48	Erfolgreicher Hackerangriff auf die Plattform Justitia.Swiss	**Gross**	
R49	Missbrauch eines Benutzerzugangs auf die Plattform Justitia.Swiss	**Gross**	
R50	Missbrauch eines Administrationszugangs auf die Plattform Justitia.Swiss	**Gross**	
R51	Kompromittierung des Signierschlüssels der Plattform Justitia.Swiss	**Gross**	
R52	Erfolgreiche Denial of Service (DoS) Attacke auf die Plattform Justitia.Swiss	Mittel	
R53	DNS Spoofing oder Phishing	Mittel	
R54	Totalverlust der Plattform Justitia.Swiss im Katastrophenfall	Mittel	

Abbildung 5: Risikoübersicht vor Massnahmen

5 Sicherheitsmassnahmen

5.1 Organisatorische Sicherheitsmassnahmen

MO (1) Detailkonzepte zur Informationssicherheit

Das Projekt erarbeitet für die sicherheitsrelevanten Lösungsbestandteile die nötigen Begleitdokumente zum vorliegenden ISDS-Konzept. Aus aktueller Sicht sind dies:

- Eine Datenschutzfolgeabschätzung gemäss dem revidierten Datenschutzgesetz;
- Ein Datenbearbeitungsreglement für die auf der Plattform Justitia.Swiss bearbeiteten Daten;
- Prozesse für die Verwaltung (Eröffnen, Mutieren, Löschen) von Organisationen;
- Prozesse für die Verwaltung (Eröffnen, Mutieren, Löschen) von Benutzern;
- Ein Berechtigungskonzept für die Plattform Justitia.Swiss (vgl. MA (12));
- Vorgaben für kryptographische Algorithmen und Schlüsselverwaltung (vgl. MT (1), 0);
- Ein Detailkonzept für Siegel-Service und Siegel-Validator (vgl. MA (1), MA (3), MA (15));
- Eine Spezifikation der Anforderungen an die Identity Provider (vgl. MA (6), MA (7), MA (25));
- Ein Detailkonzept für die Implementierung des Audit Trails (vgl. MA (4));
- Ein Konzept für das Security Information and Event Management (SIEM) und den Betrieb eines Security Operations Center (SOC) (vgl. MO (3));
- Sicherheitsanforderungen als Teil der Pflichtenhefte für Softwareentwickler und Plattformbetreiber;
- Sicherheitsvorgaben für den Anschluss der IT-Systeme von verfahrensleitenden Justizbehörden;
- Sicherheitsvorgaben für den Anschluss der IT-Systeme von verfahrensbeteiligten Organisationen;
- Ein BCM-Konzept für die Migration auf einen Ausweichstandort im Katastrophenfall (vgl. MT (15)).

Hinweis zur Umsetzung: Es wird im Projektverlauf entschieden, in welchen Projektphasen diese Dokumente erarbeitet werden.

Reduziert die folgenden Risiken:

- Reduziert alle Risiken

MO (2) Nach ISO/IEC 27001 zertifiziertes ISMS der örK

Die öffentlich-rechtliche Körperschaft (örK) etabliert für die Plattform Justitia.Swiss ein Information Security Management System (ISMS) und lässt dieses nach ISO/IEC 27001 zertifizieren.

Ein ISMS nach ISO/IEC 27001 umfasst unter anderem (Liste nicht abschliessend):

- Stellenbeschrieb und Nominierung des ISDS-Verantwortlichen für die Plattform Justitia.Swiss;
- Ein Security Operations Center (SOC) und ein Emergency Response Team (ERT) (vgl. MO (3);
- Ein vom ISDS-Verantwortlichen aktuell gehaltenes ISDS-Konzept (das vorliegende Dokument);
- Einen vom ISDS-Verantwortlichen geführten Risikokatalog (Risk Register);
- Einen mindestens jährlich aktualisierten Risikobehandlungsplan (Risk Treatment Plan, RTP);
- Einen mindestens jährlich stattfindenden Management Review, bei dem die Leitung der öffentlich-rechtlichen Körperschaft über den Risikokatalog und den Risikobehandlungsplan befindet;
- Eine fachlich unabhängige interne Auditstelle der örK, die den sicheren Betrieb der Plattform Justitia.Swiss sowie die Einhaltung der Sicherheitsvorgaben an Partner (Justizbehörden, Verfahrensbeteiligte) und Lieferanten (Softwareentwickler, Plattformbetreiber) regelmässig überprüft.

Reduziert die folgenden Risiken:

- Reduziert alle Risiken

MO (3) Security Information and Event Management (SIEM)

Die öffentlich-rechtliche Körperschaft (örK) etabliert ein Security Information and Event Management (SIEM), das Anomalien erkennt (auch als *Fraud Detection* bezeichnet) und sicherstellt, dass diese angemessen adressiert werden (technisch und organisatorisch). Das SIEM umfasst neben der Beauftragung eines Security Operations Center (SOC) auch die Etablierung aller Prozesse für die Bearbeitung von Sicherheitsvorfällen durch die entsprechenden Stellen bei der örK, beim Betreiber der Plattform sowie bei den daran angeschlossenen Justizbehörden und verfahrensbeteiligten Organisationen.

Anomalien im System könnten beispielsweise sein:

- Systematische Portscans aus dem Internet;
- Ungewöhnliche (z.B. virenverseuchte) Eingaben (*Fraud Detection*);
- Eine unübliche Häufung von Akteneinsichten, die auf eine automatisierte Attacke hinweist;
- Ungewöhnliche und kritische Mutationen von Benutzer- oder Berechtigungsdaten;

Für die Erkennung von und den Umgang mit Sicherheitsvorfällen wird ein Security Operations Center (SOC) etabliert, das insbesondere sicherstellt:

- Die laufende Überwachung und Lagebeurteilung;
- Die allfällige Sperrung von zugreifenden Systemen (z.B. IP-Adressen);
- Die rechtzeitige Auslösung von Notfallmassnahmen.

Vorerst wird das SOC vom Plattformbetreiber bereitgestellt.

Reduziert die folgenden Risiken:

- R45 Mangelhafte Berechtigungsverwaltung für Mitarbeitende des Service Desk
- R48 Erfolgreicher Hackerangriff auf die Plattform Justitia.Swiss
- R49 Missbrauch eines Benutzerzugangs auf die Plattform Justitia.Swiss
- R50 Missbrauch eines Administrationszugangs auf die Plattform Justitia.Swiss
- R53 Erfolgreiche Denial of Service (DoS) Attacke auf die Plattform Justitia.Swiss

MO (4) Awareness-Programm für alle Benutzergruppen

Alle Benutzer der Plattform Justitia.Swiss werden über die Sicherheitsrisiken informiert und über die Sicherheitsmassnahmen instruiert. Das Awareness-Programm ist an alle Benutzergruppen adressiert:

- Mitarbeitende der öffentlich-rechtlichen Körperschaft (örK);
- Mitarbeitende der angeschlossenen verfahrensleitenden Justizbehörden;
- Mitarbeitende der verfahrensbeteiligten Organisationen (insbesondere Anwaltskanzleien);
- Mitarbeitende des Plattformbetreibers und des Softwareentwicklers;
- Verfahrensbeteiligte Privatpersonen und Dritte;

Reduziert die folgenden Risiken:

- Reduziert alle Risiken

MO (5) Kein Transfer von geheimen Daten über die Plattform Justitia.Swiss

Die verfahrensleitenden Justizbehörden sowie die verfahrensbeteiligten Organisationen und natürlichen Personen verwenden die Plattform Justitia.Swiss nicht für die Zustellung oder die Eingabe von geheimen Daten. Diese Verpflichtung wird in den Anschlussvereinbarungen und Nutzungsbestimmungen entsprechend festgehalten.

Hinweis: Geheime Daten (Klassifizierung gemäss [Ext13] ISchV Art. 5) erfordern spezielle Massnahmen wie end-to-end-Verschlüsselung oder Kurierdienste, die von der Plattform Justitia.Swiss bis auf Weiteres nicht angeboten werden.[9]

Reduziert die folgenden Risiken:

- Reduziert alle Risiken

[9] Siehe Anhang E: Kapitel 2.4.4 aus E29 Varianten Plattform «Justitia.Swiss»

MO (6) Periodische Überprüfung des Adressverzeichnisses

Die Daten im Adressverzeichnis werden periodisch überprüft, damit die definierte minimale Qualitätsstufe pro Attribut gemäss MA (26) eingehalten wird. Elemente dieser Prüfung sind insbesondere:

- Der Organisations-Administrator jeder Organisation (Justizbehörde, Anwaltskanzlei, …) prüft und bestätigt halbjährlich, dass die Attribute der Organisation sowie die Organisationszugehörigkeiten (inkl. Funktionszuweisungen) korrekt und aktuell sind;
- Der Organisations-Administrator jeder Organisation (Justizbehörde, Anwaltskanzlei, …) bestätigt halbjährlich, dass die Attribute der Teilnehmer, die seiner Organisation angehören, korrekt und aktuell sind.
- Für die Prüfung der Zuweisungen von Funktionen mit besonders weitreichenden Berechtigungen (z.B. «Zustellungen aufgeben», «Organisations-Administrator») kann eine kürzere Periode vorgesehen werden;
- Die Bestätigung dafür, dass die Überprüfungen durchgeführt wurde, wird im Audit Trail der Plattform Justitia.Swiss protokolliert.
- Die interne Auditstelle der öffentlich-rechtlichen Körperschaft (örK) überprüft regelmässig, ob diese Vorgaben eingehalten werden.

Die Verpflichtung zur periodischen Überprüfung der eigenen Einträge im Adressverzeichnis wird in den Anschlussvereinbarungen und Nutzungsbestimmungen entsprechend festgehalten.

Reduziert die folgenden Risiken:

- R27 Nicht mehr benötigte Aktenstücke im zentralen DossierStore werden nicht gelöscht
- R28 Fehlerhafte Konfiguration von Justizbehörden auf der Plattform Justitia.Swiss
- R29 Fehlerhafte Konfiguration von Anwaltskanzleien auf der Plattform Justitia.Swiss
- R30 Registrierung eines Benutzers unter einer falschen Identität
- R31 Fehlerhafte Verwaltung von Benutzerattributen im Adressverzeichnis
- R32 Fehlerhafte Erfassung von Organisationszugehörigkeiten
- R33 Fehlerhafte Zuweisung von Funktionen mit weitreichenden Berechtigungen
- R34 Organisationszugehörigkeiten werden nicht nachgeführt
- R35 Unerwünschte Rechtekumulation bei «Mehrfachanstellungen»

MO (7) Periodische Rezertifizierung aller gültigen Zustellungen

Die Plattform Justitia.Swiss verlangt von den verfahrensleitenden Justizbehörden, dass sie mindestens alle drei Monate bestätigen, dass alle aktuell gültigen Zustellungen noch benötigt werden und dass die berechtigungswirksamen Elemente aller aktuell gültigen Zustellungen noch korrekt sind. Namentlich sind dies:

- Der Empfänger der Zustellung;
- Die Gültigkeitsdauer der Zustellung;
- Die Liste der Aktenstück-Adressen, für die eine Akteneinsicht gewährt wird.

Ein spezieller Fokus dieser Rezertifizierung bzw. Qualitätssicherung wird auf Akten und Aktenstücke gelegt, für die mehrere zeitlich überlappende Zustellungen an mehrere Empfänger gültig sind.

Bei verfahrensführenden Justizbehörden, die den zentralen DossierStore nutzen, wird dieser Prozess auch dafür genutzt, nicht mehr benötigte Aktenstücke aus dem DossierStore zu löschen:

- Zu diesem Zweck werden einerseits alle im DossierStore gespeicherten Aktenstücke identifiziert, für die keine gültige Zustellung mehr vorhanden ist, so dass entweder eine Zustellung verlängert oder die Löschung der Aktenstücke ausgelöst werden kann (eine automatische Löschung durch die Plattform findet nicht statt).
- Liegt für eine Akte keine gültige Zustellung mehr vor, dann wird die verfahrensführende Justizbehörde gebeten, diese Akte zu schliessen, worauf alle Aktenstücke aus dem DossierStore gelöscht werden.

Reduziert die folgenden Risiken:

- R13 Der Empfänger einer Zustellung wird nicht erreicht
- R14 Eine fehlerhafte Zustellung führt zu unerwünschtem Aktenzugriff
- R26 Aktenstücke im zentralen DossierStore werden nicht nachgeführt
- R27 Nicht mehr benötigte Aktenstücke im zentralen DossierStore werden nicht gelöscht
- R37 Delegationen werden nicht nachgeführt

MO (8) Quartalsweise Rezertifizierung aller gültigen Delegationen

Die Plattform Justitia.Swiss verlangt von allen Teilnehmern, dass sie mindestens alle drei Monate bestätigen, dass alle aktuell gültigen Delegationen noch benötigt werden.

Wenn sich die Organisationszugehörigkeit eines Profils verändert, dann verlangt die Plattform Justitia.Swiss eine sofortige Rezertifizierung aller Delegationen, bei denen dieses Profil betroffen ist (delegierend oder delegationsempfangend).

Reduziert die folgenden Risiken:

- R13 Der Empfänger einer Zustellung wird nicht erreicht
- R14 Eine fehlerhafte Zustellung führt zu unerwünschtem Aktenzugriff
- R26 Aktenstücke im zentralen DossierStore werden nicht nachgeführt
- R27 Nicht mehr benötigte Aktenstücke im zentralen DossierStore werden nicht gelöscht
- R37 Delegationen werden nicht nachgeführt

MO (9) Ein Profil pro Organisationszugehörigkeit

Ein Profil ist entweder keiner (wenn es eine Privatperson repräsentiert) oder genau einer Organisation (wenn es ein Anstellungsverhältnis repräsentiert) zugeordnet.

Eine natürliche Person, die sowohl als Privatperson (z.B. Kläger, Beklagter) als auch als Repräsentantin einer oder mehrerer Organisationen an ERV und eAE teilnimmt, muss sich entsprechend mehrfach im Adressverzeichnis der Plattform Justitia.Swiss registrieren. Im (eher unwahrscheinlichen) Fall, dass diese natürliche Person denselben Identity Provider und dieselbe Digitale Identität für mehrere Profile verwendet, muss sie bei der Anmeldung an der Plattform Justitia.Swiss das gewünschte Profil auswählen.

Hinweis: Im Falle von Mehrfachanstellungen wird die natürliche Person in vielen Fällen auch pro Anstellung über je eine elektronische Adresse (insb. E-Mail-Adresse) und eine physische Adresse verfügen, was ebenfalls die Verwendung unterschiedlicher Profile nahelegt.

Reduziert die folgenden Risiken:

- R33 Fehlerhafte Zuweisung von Funktionen mit weitreichenden Berechtigungen
- R34 Organisationszugehörigkeiten werden nicht nachgeführt
- R35 Unerwünschte Rechtekumulation bei «Mehrfachanstellungen»
- R37 Delegationen werden nicht nachgeführt
- R38 Mangelhafte Auskunftsfähigkeit über bestehende Berechtigungen
- R39 Keine Gesamtverantwortung für die Berechtigungen und Attribute eines Teilnehmers

MO (10) Sicherheitsverantwortung des Softwarelieferanten als Vertragsbestandteil

Die Aufgaben, Kompetenzen und Verantwortungen (AKV) des Softwarelieferanten in Bezug auf die IT-Sicherheit der Plattform Justitia.Swiss werden vertraglich vereinbart.

Wichtige sicherheitsbezogene Vertragsbestandteile sind insbesondere:

- Die Bereitschaft, den Quellcode durch unabhängige Dritte analysieren zu lassen (vgl. MO (20));
- Die Sicherheit des Softwareentwicklungsprozesses (*Secure Software Development*);
- Die systematische Durchführung manueller Code-Reviews nach definiertem Prozess;
- Die Nutzung von Werkzeugen für die statische und dynamische Code-Analyse (z.B. nach OWASP);
- Der systematische Umgang mit festgestellten Sicherheitsschwachstellen (Patch Management);
- Das Berechtigungskonzept für das Source Code Repository sowie die Build- und Test-Umgebungen;
- Die Sicherheit und Aktualität der eingesetzten Softwarebibliotheken und Entwicklungswerkzeuge;
- Die Sicherheitsausbildung aller an der Softwareentwicklung beteiligten Personen;
- Die Einbindung allfälliger Unterlieferanten in diese Verpflichtungen.

Reduziert die folgenden Risiken:

- R47 Mangelhafte Berechtigungsverwaltung für Mitarbeitende des Softwareentwicklers
- R48 Erfolgreicher Hackerangriff auf die Plattform Justitia.Swiss
- R49 Missbrauch eines Benutzerzugangs auf die Plattform Justitia.Swiss

MO (11) Sicherheitsverantwortung des Plattformbetreibers als Vertragsbestandteil

Die Aufgaben, Kompetenzen und Verantwortungen (AKV) des Plattformbetreibers in Bezug auf die IT-Sicherheit der Plattform Justitia.Swiss werden vertraglich vereinbart.

Wichtige Vertragsbestandteile sind insbesondere:

- Das Vorhandensein eines zertifizierten ISMS nach ISO/IEC 27001 seitens des Plattformbetreibers;
- Die Bereitschaft zur Lieferung der Protokolldaten an ein unabhängiges SOC;
- Das vollumfängliche und ungehinderte Einsichts- und Prüfrecht der örK (vgl. 0);
- Die Sicherheit der Internetanbindung und Kommunikationsverbindungen (inkl. DoS Prävention);
- Die Verfügbarkeit aller für den Plattformbetrieb benötigten Infrastrukturen (Redundanz);
- Die logische und physische Sicherheit aller Plattformkomponenten (Hardening);
- Die Isolation der Justitia.Swiss-Plattform von den Systemen anderer Kunden (Isolation);
- Die Sicherheit der Systems Management Prozesse und der Administrationszugänge (vgl. MT (10));
- Die Sicherheitsausbildung aller am Plattformbetrieb beteiligten Personen;
- Die Durchführung externer Sicherheitsprüfungen (belegt durch entsprechende Testberichte);
- Die Datenspeicherung ausschliesslich in der Schweiz unter Schweizer Rechtshoheit;
- Die Einbindung allfälliger Unterlieferanten in diese Verpflichtungen.

Reduziert die folgenden Risiken:

- R48 Erfolgreicher Hackerangriff auf die Plattform Justitia.Swiss
- R49 Missbrauch eines Benutzerzugangs auf die Plattform Justitia.Swiss
- R50 Missbrauch eines Administrationszugangs auf die Plattform Justitia.Swiss
- R51 Kompromittierung des Signierschlüssels der Plattform Justitia.Swiss
- R52 Erfolgreiche Denial of Service (DoS) Attacke auf die Plattform Justitia.Swiss

MO (12) Sicherheitsverantwortung der Justizbehörden als Bestandteil des Anschlussvertrags

Die Aufgaben, Kompetenzen und Verantwortungen (AKV) der Justizbehörden in Bezug auf die Sicherheit der Plattform Justitia.Swiss und ihrer eigenen an die Plattform angeschlossenen IT-Systeme werden in einem Anschlussvertrag oder einem vergleichbaren Konstrukt verbindlich vereinbart.

Wichtige Bestandteile dieser verpflichtenden Vereinbarung sind insbesondere:

- Die Teilnahme am Information Security Management System (ISMS) der örK (vgl. MO (2));
- Die Teilnahme am Security Information and Event Management (SIEM) der örK (vgl. MO (3));
- Die interne Umsetzung des übergreifenden Awareness-Programms (vgl. MO (4));
- Die Sicherstellung, dass keine geheimen Daten zugestellt werden (vgl. MO (5));
- Die Verantwortung für die eigenen Einträge im Adressverzeichnis (vgl. 0);
- Die periodische Prüfung der eigenen Einträge im Adressverzeichnis (vgl. 0);
- Die quartalsweise Rezertifizierung aller gültigen Zustellungen (MO (7));
- Die zeitgerechte Aktualisierung des eigenen zentralen DossierStore (falls dieser genutzt wird);
- Die Sicherheit des eigenen dezentralen DossierStore (falls ein solcher genutzt wird);
- Die Sicherheit der Mitarbeiter-Endgeräte (insbesondere Arbeitsplatzsysteme);
- Die Einsichts- und Audit-Rechte der öffentlich-rechtlichen Körperschaft (örK);
- Die Nominierung eines technischen Verantwortlichen für den Anschluss an die Plattform.

Reduziert die folgenden Risiken:

- R14 Eine fehlerhafte Zustellung führt zu unerwünschtem Aktenzugriff
- R25 Aktenstücke im zentralen DossierStore gehen verloren
- R26 Aktenstücke im zentralen DossierStore werden nicht nachgeführt
- R27 Nicht mehr benötigte Aktenstücke im zentralen DossierStore werden nicht gelöscht
- R28 Fehlerhafte Konfiguration von Justizbehörden auf der Plattform Justitia.Swiss

MO (13) Sicherheitsverantwortung der Verfahrensbeteiligten als Teil der Nutzungsbedingungen

Die Aufgaben, Kompetenzen und Verantwortungen (AKV) der Verfahrensbeteiligten für die IT-Sicherheit ihrer Systeme werden in den Nutzungsbedingungen für die Justitia.Swiss-Plattform vereinbart.

Wichtige Vertragsbestandteile sind insbesondere:

- Die interne Umsetzung des übergreifenden Awareness-Programms (vgl. MO (4));
- Die Verantwortung für die eigenen Einträge im Adressverzeichnis (vgl. 0);
- Die periodische Prüfung der eigenen Einträge im Adressverzeichnis (vgl. 0);
- Die Sicherheit von Kanzleisoftware, die über ein API mit der Justitia.Swiss-Plattform kommuniziert;
- Die Sicherheit der Mitarbeiter-Endgeräte (insbesondere Arbeitsplatzsysteme);
- Die Einsichts- und Audit-Rechte der öffentlich-rechtlichen Körperschaft (örK);
- Die Nominierung eines technischen Verantwortlichen für den API-Anschluss an die Plattform.

Reduziert die folgenden Risiken:

- R7 Mit Schadsoftware verseuchte Eingaben schädigen die IT-Systeme anderer Teilnehmer
- R49 Missbrauch eines Benutzerzugangs auf die Plattform Justitia.Swiss

MO (14) Sicherheitsmassnahmen gelten auch für verfahrensbeteiligte Justizbehörden

Wenn eine Justizbehörde bei der Interaktion mit einer anderen Justizbehörde die Rolle eines Verfahrensbeteiligten einnimmt (Eingaben einreicht, Zustellungen empfängt und Akten einsieht), dann gelten dieselben Sicherheitsmassnahmen wir bei allen anderen verfahrensbeteiligten Organisationen.

Reduziert die folgenden Risiken:

- R22 Für verfahrensbeteiligte Justizbehörden werden Sicherheitsmassnahmen nicht umgesetzt

MO (15) Zuverlässige Anruferidentifikation durch den Service Desk

Bevor der Service Desk eine Auskunft erteilt oder eine sicherheitsrelevante Aktion ausführt, identifiziert er den Antragsteller zuverlässig auf der Basis von zwei Faktoren. Die hierfür eingesetzten Verfahren sind unterschiedlich je nach Kommunikationskanal.

Für die besonders kritische Anruferidentifikation am Telefon wird heute ergänzend zu den sogenannten Magic Questions (Fragen, deren Antwort nur der legitime Anrufer kennt) zunehmend auch die biometrische Stimmerkennung verwendet. Eine alternative Möglichkeit ist der Rückruf auf die Telefonnummer, die im Adressverzeichnis hinterlegt ist.

Reduziert die folgenden Risiken:

- R41 Mangelhafte Berechtigungsverwaltung für Mitarbeitende der örK
- R42 Ein Anrufer gibt sich gegenüber dem Service Desk als eine andere Person aus

MO (16) Secure Software Development

Der Softwarelieferant wird darauf verpflichtet, einen etablierten Prozess für die Entwicklung sicherer Software auf der Basis eines Security Development Lifecycles (SDL) nachzuweisen. Dieser Prozess soll möglichst viele der folgenden Elemente umfassen:

- Die Dokumentation der Sicherheitsanforderungen an die zu entwickelnde Software zuhanden der Entwickler;
- Die Durchführung einer Bedrohungsanalyse (*Threat Modeling*) nach anerkannten Methoden (z.B. STRIDE);
- Die Dokumentation von Prinzipien und Standards für die sichere Programmierung zuhanden der Entwickler;
- Die systematische Durchführung manueller Code-Reviews (*Peer Reviews*) nach definiertem Prozess (z.B. Fagan Inspektion);
- Die obligatorische Nutzung von mindestens einem Werkzeug, das den Source Code der Software statisch auf Schwachstellen (OWASP Top 10 etc.) analysiert (z.B. Static Application Security Testing SAST);
- Die obligatorische Nutzung von mindestens einem Werkzeug, das die Software zur Laufzeit auf Schwachstellen untersucht (z.B. Dynamic Application Security Testing DAST oder Interactive Application Security Testing IAST);
- Die Abnahmekriterien für Sicherheitstests, beispielsweise als Teil der «Definition of Done»;
- Den systematischen Umgang mit Schwachstellen im Rahmen eines Schwachstellen- und Patch-Managements (Analyse, Behebung, Regression-Testing);
- Die Dokumentation des Berechtigungskonzepts für das Source Code Repository sowie die Build- und Test-Infrastrukturen;
- Die regelmässige Aktualisierung aller eingesetzten Softwarebibliotheken und Entwicklungswerkzeuge;
- Die fortlaufende Integration der Software inklusive automatisierter Tests (CI/CD Pipeline);
- Die Sicherheitsausbildung aller an der Softwareentwicklung beteiligten Personen (Security Awareness Training).

Reduziert die folgenden Risiken:

- R46 Software mit Sicherheitsschwachstellen

MO (17) Auditrecht der öffentlich-rechtlichen Körperschaft beim Plattformbetreiber

Die öffentlich-rechtliche Körperschaft (örK) verlangt vom Plattformbetreiber ein jederzeitiges, vollumfängliches und ungehindertes Einsichts- und Prüfrecht in Bezug auf den Betrieb der Justitia.Swiss-Plattform. Sie verlangt von diesem ausserdem das Einverständnis, dass die Plattform Justitia.Swiss durch von der örK beauftragte Dritte mittels Penetration Tests und Vulnerability Scans auf Sicherheitsschwachstellen überprüft werden kann.

- R49 Missbrauch eines Benutzerzugangs auf die Plattform Justitia.Swiss

MO (18) Pentest (Manual Hacking) aller Benutzerschnittstellen

Alle aus dem Internet nutzbaren Webapplikationen und API der Plattform Justitia.Swiss werden vor der produktiven Einführung jedes neuen Software-Releases durch eine unabhängige und hierauf spezialisierte Firma auf Sicherheitsschwachstellen untersucht. Dieses sogenannte *Manual Hacking* findet in der Integrationstestumgebung statt und es werden hierfür Benutzerkonten und Gerätezertifikate eingerichtet.

Im Scope dieser Prüfung sind insbesondere:

- Die Webapplikationen für Verfahrensbeteiligte (Parteien, Parteivertreter, Dritte);
- Die API für die Anbindung von Kanzleisoftware;
- Die API für die Anbindung von Systemen bei verfahrensleitenden Justizbehörden.

Reduziert die folgenden Risiken:

- R40 Sicherheitsrisiken werden nicht angemessen behandelt
- R48 Erfolgreicher Hackerangriff auf die Plattform Justitia.Swiss
- R49 Missbrauch eines Benutzerzugangs auf die Plattform Justitia.Swiss

MO (19) Vulnerability-Monitoring aller Internet-Zugangspunkte

Alle über das Internet erreichbaren Schnittstellen der produktiven Justitia.Swiss-Plattform werden laufend (mindestens täglich) auf Sicherheitsschwachstellen untersucht. Solche Vulnerability Scans erfordern keinen Benutzerzugang. Sie dürfen den Produktionsbetrieb nicht übermässig beeinträchtigen.

Reduziert die folgenden Risiken:

- R40 Sicherheitsrisiken werden nicht angemessen behandelt
- R48 Erfolgreicher Hackerangriff auf die Plattform Justitia.Swiss

MO (20) Quelltext-Analyse aller Sicherheitsmodule

Die öffentlich-rechtliche Körperschaft (örK) verlangt vom Softwarelieferanten die Bereitschaft, den Quellcode durch unabhängige von der örK beauftragte Dritte analysieren zu lassen.

Die Sicherheitsmodule der Justitia.Swiss-Plattform werden vor der produktiven Einführung jedes in Bezug auf diese Module veränderten neuen Software-Releases durch eine unabhängige und hierauf spezialisierte Firma mit geeigneten Werkzeugen (Analysetools) auf Sicherheitsmängel untersucht.

Im Scope dieser Prüfung sind insbesondere:

- Der Federation Broker (Software zum Anschluss der Identity Provider);
- Der Audit Trail;
- Der Siegel-Service;
- Der Quittungs-Service für die Ausstellung von Eingangs- und Abrufquittungen;
- Das Zugriffskontrollsystem der Plattform Justitia.Swiss.

Reduziert die folgenden Risiken:

- R46 Software mit Sicherheitsschwachstellen

5.2 Applikatorische Sicherheitsmassnahmen

MA (1) Elektronisches Plattform-Siegel für alle Eingaben

Alle Dateien, die ein Verfahrensbeteiligter im Rahmen einer Eingabe über die Plattform Justitia.Swiss einreicht, werden von der Plattform vor der Weiterleitung an die adressierte Justizbehörde mit einem geregelten elektronischen Plattform-Siegel gemäss ZertES ([Ext4]) versehen. Durch die Validierung des Siegels kann anschliessend jederzeit verifiziert werden, dass die gesiegelten Dateien nach der Eingabe nicht mehr verändert wurden.

- Die verfahrensleitenden Justizbehörden sollten das Plattform-Siegel validieren, bevor die Eingabe in eine elektronische Akte aufgenommen («veraktet») wird.
- Die verfahrensleitenden Justizbehörden sollten das Plattform-Siegel zusammen mit der Eingabe in die elektronische Akte aufnehmen, allenfalls zusätzlich zu einem Justizbehörden-Siegel.

Damit das Plattform-Siegel auch nach langer Zeit (insbesondere auch nach Ablauf der Gültigkeit des Siegel-Zertifikats der Plattform) validiert werden kann (sogenannte Long Term Validation, LTV), werden neben dem Siegel und einem Zeitstempel auch das Siegel-Zertifikat der Plattform sowie ein Nachweis für die Gültigkeit des Siegel-Zertifikats zum Zeitpunkt der Siegelung (z.B. eine OCSP Response) zusammen mit der gesiegelten Datei gespeichert.

Reduziert die folgenden Risiken:

- R1 Eingaben werden nach dem Versand verändert

MA (2) Möglichkeit zur Eingabe vorgängig digital signierter Dateien

Verfahrensbeteiligte können im Rahmen einer Eingabe über die Plattform Justitia.Swiss auch Dateien einreichen, die sie bereits selber digital signiert haben. Eine bereits vorhandene digitale Signatur bleibt unverändert erhalten, wenn das Plattform-Siegel angebracht wird.

Reduziert die folgenden Risiken:

- R1 Eingaben werden nach dem Versand verändert

MA (3) Das Plattform-Siegel verlangt eine Willensbekundung des Absenders

Der Benutzer muss die Erzeugung des Siegels im Sinne einer aktiven Willensbekundung explizit auslösen. Die Dateien werden ihm zu diesem Zweck unmittelbar vor oder nach der Siegel-Erzeugung angezeigt, bevor die Eingabe erfolgt (die Implementierung ist im Detail noch festzulegen). Diese manuelle Interaktion über das Web-Portal der Plattform Justitia.Swiss ist auch dann notwendig, wenn die Dateien maschinell über eine integrierte Kanzleiapplikation geliefert wurden, sofern sie nicht bereits vorgängig digital signiert worden sind.

Reduziert die folgenden Risiken:

- R2 Eingaben werden abgestritten

MA (4) Die Plattform zeichnet alle rechtsverbindlichen Ereignisse in einem Audit Trail auf

Die Plattform Justitia.Swiss protokolliert alle rechtsverbindlichen Ereignisse in einem nicht veränderbaren Audit Trail gemäss den Anforderungen, die in der Geschäftsbücherverordnung ([Ext5]) an das Journal zur chronologischen Erfassung aller verbuchten Geschäftsvorfälle gestellt werden.

Ist eine Protokollierung im Audit Trail nicht möglich, so wird der Geschäftsvorfall nicht ausgeführt.

Reduziert die folgenden Risiken:

- R2 Eingaben werden abgestritten
- R10 Der Empfang zugestellter Aktenstücke wird abgestritten
- R12 Der Versand einer Zustellung wird abgestritten

MA (5) Die Plattform kann elektronisch gesiegelte Eingangs- und Abrufquittungen erzeugen

Die Plattform Justitia.Swiss kann für rechtsverbindliche Ereignisse elektronisch gesiegelte Eingangs- und Abrufquittungen gemäss dem Bundesgesetz über die Plattform für die elektronische Kommunikation in der Justiz ([Ext1]) ausstellen und diese den verfahrensleitenden Justizbehörden sowie den Verfahrensbeteiligten zur Verfügung stellen.

Die verfahrensführenden Justizbehörden können die Eingangs- und Abrufquittungen in die elektronische Akte aufnehmen und dort aufbewahren. Die Quittungen gehören zum Verfahren und ihre Aufbewahrungsdauer richtet sich nach der Art des Verfahrens mit den jeweiligen gesetzlichen Vorgaben.

Die Eingangs- und Abrufquittungen enthalten alle Angaben, die für eine spätere Nachvollziehbarkeit der rechtsverbindlichen Ereignisse notwendig sind. Dies sind insbesondere:

- Die Zustelladresse des Absenders der Übermittlung;
- Die Zustelladresse des Empfängers der Übermittlung;
- Identifizierende Meta-Daten der transferierten Dateien (z.B. Filenamen);
- Die kryptographischen Quersummen (Hashwerte) der transferierten Dateien;
- Der Zeitpunkt des Transfers (auf die Minute genau).

Reduziert die folgenden Risiken:

- R2 Eingaben werden abgestritten
- R9 Aktenstücke werden auf dem Zustellweg manipuliert oder gehen verloren
- R10 Der Empfang zugestellter Aktenstücke wird abgestritten
- R12 Der Versand einer Zustellung wird abgestritten

MA (6) 2-Faktor-Authentifizierung (2FA) aller Benutzer

Der Zugriff auf das Web-Portal der Plattform Justitia.Swiss erfordert eine starke Benutzerauthentifizierung mit mindestens zwei Faktoren (2FA).

Die detaillierten Anforderungen in Bezug auf die Vertrauensstufe der Authentifizierung werden in einem Dokument «Detailanforderungen an die akzeptierten Identity Provider» noch spezifiziert (vgl. Sicherheitsmassnahme MO (1)). Grundsätzlich gelten die Kriterien der Vertrauensstufe für Authentifizierung 2 (VSA2) aus dem eCH «Qualitätsmodell zur Authentifizierung von Subjekten» (eCH-170, [Ext8]), die wiederum dem Authentication Assurance Level 2 (AAL2) gemäss den NIST "Digital Identity Guidelines, Band B" (NIST SP 800-63-3B, [Ext11]) entsprechen.

Auch die Nutzung der Plattform Justitia.Swiss über eine integrierte Kanzleisoftware erfordert eine starke Benutzerauthentifizierung mit mindestens zwei Faktoren. In diesem Fall muss die vom Identity Provider authentifizierte Identität des Endbenutzers in einer vom Identity Provider ausgestellten Authentifizierungsbestätigung (auch als *Assertion* oder *Token* bezeichnet) von der Kanzleisoftware an die Plattform Justitia.Swiss weitergereicht werden.

Reduziert die folgenden Risiken:

- R3 Eingaben werden unter einer falschen Identität eingereicht
- R16 Es werden gefälschte Zustellungen erfasst
- R17 Akten werden von unberechtigten Dritten über die Plattform eingesehen
- R48 Erfolgreicher Hackerangriff auf die Plattform Justitia.Swiss
- R49 Missbrauch eines Benutzerzugangs auf die Plattform Justitia.Swiss

MA (7) Anbindung der Identity Provider über sichere Federation Protokolle

Die Plattform Justitia.Swiss delegiert die 2-Faktor-Authentifizierung der Benutzer an vorgelagerte Identity Provider (IdP), welche die verlangte Authentifizierungsstärke garantieren und über ein Federation Protokoll wie OpenID Connect, OAuth 2.0 oder SAML angebunden werden.

Die detaillierten Anforderungen in Bezug auf die Vertrauensstufe der Föderierung werden in einem Dokument «Detailanforderungen an die akzeptierten Identity Provider» noch spezifiziert (vgl. Sicherheitsmassnahme MO (1)). Grundsätzlich gelten die Kriterien der Vertrauensstufe für Föderierung 2

(VSF2) aus dem eCH «Qualitätsmodell zur Authentifizierung von Subjekten» (eCH-170, [Ext8]), die wiederum dem Federation Assurance Level 2 (FAL2) gemäss den NIST "Digital Identity Guidelines, Band C" (NIST SP 800-63-3C, [Ext11]) entsprechen.

Neben den Sicherheitseigenschaften der vom IdP ausgestellten Authentifizierungsbestätigung (z.B. die Art der Übermittlung, die kryptographische Absicherung und Gültigkeitsdauer der Assertion bzw. der Token) wird in der Anforderungsspezifikation auch deren Inhalte (sogenannte *Claims*) festgelegt.

Reduziert die folgenden Risiken:

- R3 Eingaben werden unter einer falschen Identität eingereicht
- R15 Zustellungen sind nicht mehr aktuell
- R16 Es werden gefälschte Zustellungen erfasst
- R17 Akten werden von unberechtigten Dritten über die Plattform eingesehen
- R49 Missbrauch eines Benutzerzugangs auf die Plattform Justitia.Swiss

MA (8) Gegenseitige Authentifizierung der Endpunkte bei allen API-Verbindungen

Bei jedem Aufruf eines API authentifizieren sich die beiden Endpunkte gegenseitig mit einem sicheren kryptographischen Schlüssel oder einem Access Token. Dies betrifft insbesondere die folgenden Kommunikationsverbindungen:

- Ein IT-System einer verfahrensleitenden Justizbehörde sendet eine Zustellung an die Plattform;
- Die Plattform Justitia.Swiss bezieht ein Aktenstück aus einem DossierStore;
- Ein IT-System eines Verfahrensbeteiligten sendet eine Eingabe an die Plattform Justitia.Swiss;
- Ein IT-System eines Verfahrensbeteiligten nimmt Einsicht in ein Aktenstück.

Für die Authentifizierung des Servers wird ein EV-TLS Webserver-Zertifikat eingesetzt. Für die Authentifizierung des Clients wird ein OAuth Access Token oder ein mindestens gleichwertiges Authentifizierungstoken verwendet.

Reduziert die folgenden Risiken:

- R15 Zustellungen sind nicht mehr aktuell
- R16 Es werden gefälschte Zustellungen erfasst
- R17 Akten werden von unberechtigten Dritten über die Plattform eingesehen
- R5 Eingaben werden von unberechtigten Dritten eingesehen
- R49 Missbrauch eines Benutzerzugangs auf die Plattform Justitia.Swiss

MA (9) Qualitätssicherung für übermittelte strukturierte Daten

Die Plattform Justitia.Swiss definiert Mindestvorgaben für die Qualitätssicherung aller strukturierten Daten, die über die Plattform übermittelt werden. Beispiele für solche Mindestvorgaben sind:

- Eine manuelle Erfassung oder Veränderung einer AkteID durch einen Verfahrensbeteiligten ist ausgeschlossen. Wenn sich eine Eingabe auf ein bestehendes Verfahren bezieht, dann wird die AkteID dieses Verfahrens von der Plattform Justitia.Swiss programmgesteuert der Eingabe zugewiesen (dies kann beispielsweise erreicht werden, indem der Verfahrensbeteiligte die Eingabe immer als Replik auf eine vorgängig erhaltene Zustellung einreichen muss);
- Strukturierte Daten zur automatischen Verarbeitung werden nur dann über ein API entgegengenommen, wenn die sendende Organisation und deren Software in Bezug auf die Einhaltung der Mindestvorgaben geprüft wurde.

Reduziert die folgenden Risiken:

- R4 Eingaben werden mit einer falschen AkteID eingereicht

MA (10) Sichere persönliche Arbeitsbereiche für Verfahrensbeteiligte

Das Web-Portal der Plattform Justitia.Swiss bietet den Verfahrensbeteiligten einen sicheren persönlichen Arbeitsbereich an, in dem sie Arbeitsdokumente lokal zwischenspeichern und bearbeiten können. Diese Arbeitsbereiche können insbesondere verwendet werden, um die Dateien für eine Eingabe vorzubereiten oder um Notifikationen über neu zugestellte Aktenstücke zu verwalten.

Die Arbeitsbereiche sind durch das Zugriffskontrollsystem der Plattform Justitia.Swiss geschützt (vgl. MA (12)). Ein Verfahrensbeteiligter kann beliebige andere Benutzer oder Organisationen, die im Adressverzeichnis der Plattform Justitia.Swiss registriert sind, für den Zugriff auf seinen eigenen Arbeitsbereich berechtigen (siehe SO10 Delegationen verwalten).

Reduziert die folgenden Risiken:

- R5 Eingaben werden von unberechtigten Dritten eingesehen
- R9 Aktenstücke werden auf dem Zustellweg manipuliert oder gehen verloren

MA (11) Sichere Postfächer für verfahrensleitende Justizbehörden

Eingereichte Eingaben werden im Postfach der adressierten Justizbehörde gespeichert, bis alle darin enthaltenen Dateien von der Justizbehörde entweder abgeholt oder aus einem anderen Grund gelöscht werden.

Die Postfächer der verfahrensleitenden Justizbehörden sind durch das Zugriffskontrollsystem der Plattform Justitia.Swiss geschützt (vgl. MA (12)). Verfahrensbeteiligte können eventuell ihre eigenen Eingaben einsehen, so lange sie im Postfach der adressierten Justizbehörde gespeichert sind, sie können sie dort aber weder löschen noch verändern. Ansonsten können nur diejenigen Teilnehmer auf das Postfach einer Justizbehörde zugreifen, die dieser Justizbehörde in einer entsprechenden Funktion zugehörig sind (oder an die diese Funktion delegiert worden ist).

Reduziert die folgenden Risiken:

- R4 Eingaben werden mit einer falschen AkteID eingereicht
- R5 Eingaben werden von unberechtigten Dritten eingesehen
- R6 Eingaben gehen verloren
- R9 Aktenstücke werden auf dem Zustellweg manipuliert oder gehen verloren
- R11 Die Integrität zugestellter Aktenstücke wird abgestritten
- R49 Missbrauch eines Benutzerzugangs auf die Plattform Justitia.Swiss

MA (12) Zugriffskontrollsystem für Daten und Funktionen der Plattform Justitia.Swiss

Das Zugriffskontrollsystem der Plattform Justitia.Swiss bestimmt anhand von Plattform-Rollen, welche Benutzer welche Funktionalitäten der Plattform nutzen können und welche auf der Plattform gespeicherten Daten sie einsehen oder bearbeiten können.

Beispiele für Berechtigungen auf der Plattform können sein (nicht abschliessend):

- ERV und eAE Daten auf der Plattform Justitia.Swiss bearbeiten (persönliche Arbeitsbereiche einsehen und bearbeiten, Postfächer einsehen und bearbeiten, Dateien im Quarantänebereich einsehen und exportieren, Zustellungen manuell erfassen oder mutieren, …);
- Geschäftsfunktionen ausüben (Eingaben einreichen, Zustellungen entgegennehmen, …);
- Adressverzeichnis einsehen (Benutzerdaten einsehen, Organisationsdaten einsehen, …);
- Self-Service Funktionen ausüben (eigene Attribute mutieren, Stellvertreter verwalten, …);
- Administrations-Funktionen ausüben (Organisationszugehörigkeiten verwalten, die Berechtigungswirkung einer Zustellung prüfen, …);
- Kontrollfunktionen ausüben (die eigenen Einträge im Audit Trail einsehen, Daten im Adressverzeichnis überprüfen, …);
- Den DossierStore der eigenen Justizbehörde bearbeiten (nur bei der zentralen Datenhaltung).

Das vollständige Inventar aller Plattform-Rollen mit den jeweils enthaltenen Plattform-Berechtigungen wird im Rahmen des Berechtigungskonzeptes für die Plattform Justitia.Swiss erstellt (vgl. MO (1)). Voraussichtlich werden die folgenden Rollen-Typen unterschieden:

- Organisations-bezogene Funktionen gemäss SO8 «Organisationszugehörigkeiten verwalten»;
- Administrative Rollen für Mitarbeitende der örK, des Plattformbetreibers und des Softwareentwicklers (DevOps);
- Basis-Rollen für natürliche Personen ohne Organisationszugehörigkeit.

Reduziert die folgenden Risiken:

- R5 Eingaben werden von unberechtigten Dritten eingesehen
- R20 Mit Schadsoftware verseuchte Aktenstücke werden zugestellt
- R21 Unberechtigte Einsicht in verfahrensbezogene Randdaten
- R24 Aktenstücke im zentralen DossierStore werden von unberechtigten Dritten eingesehen
- R40 Sicherheitsrisiken werden nicht angemessen behandelt
- R41 Mangelhafte Berechtigungsverwaltung für Mitarbeitende der örK
- R43 Unberechtigte Dateneinsicht beim Supportzugriff durch den Service Desk
- R44 Mangelhafte Berechtigungsverwaltung für Mitarbeitende des Service Desk
- R47 Mangelhafte Berechtigungsverwaltung für Mitarbeitende des Softwareentwicklers
- R49 Missbrauch eines Benutzerzugangs auf die Plattform Justitia.Swiss

MA (13) Eingaben und Aktenstücke werden ausserhalb des DossierStore nicht aufbewahrt

Versendete Eingaben und eingesehene Aktenstücke werden in den Arbeitsbereichen der Verfahrensbeteiligten für maximal 90 Tage zwischengespeichert, aber nicht dauerhaft aufbewahrt.

Eingegangene Eingaben werden in den Postfächern der Justizbehörden für maximal 90 Tage zwischengespeichert, aber nicht dauerhaft aufbewahrt.

Reduziert die folgenden Risiken:

- R5 Eingaben werden von unberechtigten Dritten eingesehen
- R9 Aktenstücke werden auf dem Zustellweg manipuliert oder gehen verloren
- R43 Unberechtigte Dateneinsicht beim Supportzugriff durch den Service Desk
- R48 Erfolgreicher Hackerangriff auf die Plattform Justitia.Swiss

MA (14) Zugestellte Aktenstücke werden online abgeholt

Die Zustellung von Aktenstücken im Rahmen des Elektronischen Rechtsverkehrs (ERV) wird technisch als Aufforderung zur gezielten Akteneinsicht implementiert: Klickt der Empfänger auf eine in der Zustellung enthaltene Aktenstück-Adresse, so wird ihm dieses Aktenstück über die Mechanismen der elektronischen Akteneinsicht angezeigt und zum Herunterladen angeboten.

Weil die zugestellten Aktenstücke nicht auf der Plattform Justitia.Swiss zwischengespeichert werden, ist ihre Manipulation während der Zustellung praktisch ausgeschlossen. Auch ein Verlust auf der Plattform Justitia.Swiss ist nicht möglich. Ausserdem kann mit diesem Verfahren auf der Plattform zuverlässig nachvollzogen werden, wer wann eine Zustellung entgegengenommen hat.

Reduziert die folgenden Risiken:

- R8 Eingaben oder Zustellungen können vom Empfänger nicht gelesen werden
- R9 Aktenstücke werden auf dem Zustellweg manipuliert oder gehen verloren
- R10 Der Empfang zugestellter Aktenstücke wird abgestritten

MA (15) Siegel-Validierung bei der elektronischen Akteneinsicht

Bei der elektronischen Akteneinsicht validiert die Plattform Justitia.Swiss das elektronische Siegel aller Aktenstücke und identifiziert die Organisation, die das Siegel angebracht hat.

Die Validierung des Siegels umfasst mindestens die folgenden Prüfungen:

- Entspricht der Hashwert des Aktenstücks dem Hashwert aus dem Siegel?
- Wurde das Siegel von einer Organisation angebracht, die im Adressverzeichnis registriert ist?
- Wurde das Siegel mit einem Schlüssel mit gültigem Zertifikat erzeugt (Prüfung Zertifikatskette)?
- Liegt dem Siegel ein gültiger Zeitstempel bei?
- War das Siegel-Zertifikat bei der Siegel-Erzeugung nicht revoziert (Prüfung OCSP-Response)?

Aktenstücke ohne gültiges Siegel werden entsprechend markiert. Es liegt in der Verantwortung des Empfängers der Zustellung, ob und wie er Aktenstücke ohne gültiges Siegel entgegennimmt und verarbeitet.

Reduziert die folgenden Risiken:

- R9 Aktenstücke werden auf dem Zustellweg manipuliert oder gehen verloren
- R10 Der Empfang zugestellter Aktenstücke wird abgestritten
- R11 Die Integrität zugestellter Aktenstücke wird abgestritten

MA (16) Notifikation des Empfängers einer Zustellung

Die Plattform Justitia.Swiss stellt verschiedene Verfahren dafür bereit, dass der Empfänger einer Zustellung zeitnah über deren Eingang informiert wird:

- Verfahrensbeteiligte können individuell festlegen, über welchen elektronischen Kanal (z.B. E-Mail, SMS) sie über den Eingang einer neuen Zustellung informiert werden wollen;
- Die Plattform Justitia.Swiss informiert neben dem Empfänger der Zustellung auch diejenigen Teilnehmer, für die der Empfänger eine Delegation für die betroffene Akte eingerichtet hat;
- Die Plattform Justitia.Swiss speichert eine Notifikation über den Eingang der Zustellung im persönlichen Arbeitsbereich des Empfängers;
- Verfahrensbeteiligte können andere Teilnehmer für den Zugriff auf ihren eigenen Arbeitsbereich berechtigen und somit eine Stellvertretung sicherstellen.

Reduziert die folgenden Risiken:

- R12 Der Versand einer Zustellung wird abgestritten
- R13 Der Empfänger einer Zustellung wird nicht erreicht

MA (17) Berechtigungsrelevante Elemente einer Zustellung werden nie manuell erfasst

Wenn eine Zustellung über das Web-Portal manuell erfasst wird, dann können der Empfänger und die Aktenstück-Adressen aus einer Auswahlliste selektiert aber nicht manuell als Freitext erfasst werden. Dies reduziert die Wahrscheinlichkeit von fehlerhaften Eingaben deutlich.

Reduziert die folgenden Risiken:

- R13 Der Empfänger einer Zustellung wird nicht erreicht
- R14 Eine fehlerhafte Zustellung führt zu unerwünschtem Aktenzugriff

MA (18) Die Berechtigungswirkung einer Zustellung kann geprüft werden

Das Web-Portal der Plattform Justitia.Swiss bietet den verfahrensleitenden Justizbehörden die Möglichkeit an, die Berechtigungswirkung einer Zustellung vor deren Versand zu prüfen. Bei dieser Prüfung wird einem entsprechend berechtigten Administrator der verfahrensleitenden Justizbehörde aus der Sicht des Empfängers mindestens angezeigt, welche Teile der Akte dem Empfänger mittels dieser Zustellung zur Einsicht bereitgestellt werden.

Reduziert die folgenden Risiken:

- R13 Der Empfänger einer Zustellung wird nicht erreicht
- R14 Eine fehlerhafte Zustellung führt zu unerwünschtem Aktenzugriff

MA (19) Zustellungen können auf der Plattform Justitia.Swiss annulliert werden

Die Plattform Justitia.Swiss ermöglicht es den verfahrensleitenden Justizbehörden, eine aktuell gültige Zustellung zu annullieren und die damit verbundenen Berechtigungen zur Akteneinsicht mit sofortiger Wirkung aufzuheben («Not-Aus»). In diesem Fall muss es möglich sein, einem Anwalt noch 'ein letztes Mal' Zugriff auf ein Aktenstück zu geben, so dass dieser seinen Fall abschliessen kann.

Die Berechtigung, auf der Plattform Justitia.Swiss eine Zustellung zu annullieren, sollte der Funktion «Zustellung aufgeben» zugewiesen werden.

Reduziert die folgenden Risiken:

- R14 Eine fehlerhafte Zustellung führt zu unerwünschtem Aktenzugriff
- R15 Zustellungen sind nicht mehr aktuell

MA (20) Die Berechtigungsprüfung ist Teil der DossierStore-Abfragetransaktion

Die Plattform Justitia.Swiss prüft die Berechtigung des Benutzers zur Einsicht in ein Aktenstück, unmittelbar bevor dieses Aktenstück mittels API-Aufruf aus dem DossierStore bezogen wird. Nach der Berechtigungsprüfung ist keine Veränderung der API Request-Parameter mehr möglich.

Die Berechtigungsprüfung umfasst alle Prüfungen gemäss der Beschreibung von SO3 «Akteneinsicht».

Reduziert die folgenden Risiken:

- R18 Akten werden von unberechtigten Dritten direkt aus einem DossierStore bezogen
- R19 Akten werden ohne eine vorgängige Zustellung über die Plattform eingesehen

MA (21) Elektronisches Siegel für alle Aktenstücke im zentralen DossierStore

Die Plattform Justitia.Swiss stellt sicher, dass alle im zentralen DossierStore gespeicherten Aktenstücke mit einem gültigen geregelten elektronischen Siegel gemäss dem Art. 2 lit. d ZertES versehen sind.

Bei Aktenstücken, die von einer verfahrensleitenden Justizbehörde ohne ein gültiges elektronisches Siegel geliefert werden, bringt die Plattform selber ein Behörden-Siegel für diese Justizbehörde an.

Reduziert die folgenden Risiken:

- R21 Unberechtigte Einsicht in verfahrensbezogene Randdaten
- R23 Aktenstücke im zentralen DossierStore werden verändert

MA (22) Mandantentrennung im zentralen DossierStore

Für jede Justizbehörde, die den zentralen DossierStore als Service nutzen möchte, wird im DossierStore ein eigener Mandant eingerichtet. Die Trennung dieser Mandanten umfasst mindestens:

- Für die Server-Authentifizierung der API-Verbindung für die Zustellung (vgl. MA (8)) wird für jede Justizbehörde ein separates Webserver-Zertifikat verwendet;
- Für die Client-Authentifizierung der API-Verbindung für die Zustellung (vgl. MA (8)) werden die zur Nutzung des API berechtigten Clients separat pro Justizbehörde konfiguriert;
- Bei der Verschlüsselung der gespeicherten Daten (vgl. MT (1)) wird für jede Justizbehörde ein separater Schlüssel verwendet, der von dieser selber verwaltet werden kann (*bring-your-own-key*);
- Für ein allfälliges Behörden-Siegel (vgl. MA (21)) verwendet die Plattform Justitia.Swiss für jede Justizbehörde einen separaten Schlüssel und ein separates Siegel-Zertifikat.

Reduziert die folgenden Risiken:

- R23 Aktenstücke im zentralen DossierStore werden verändert
- R24 Aktenstücke im zentralen DossierStore werden von unberechtigten Dritten eingesehen

MA (23) Kein direktes Schreibrecht auf den zentralen DossierStore

Aktenstücke im zentralen DossierStore können nur über die Mechanismen der Zustellung mutiert werden; eine direkte Bearbeitung des DossierStore über das Web-Portal ist für alle Benutzergruppen (inklusive der Administratoren der Justizbehörden und der Administratoren der Plattform Justitia.Swiss) ausgeschlossen.

Bei verfahrensleitenden Justizbehörden mit einem zentralen DossierStore umfasst die Funktion «Zustellungen aufgeben» auch die Möglichkeit, Dateien in den DossierStore zu importieren. Diese Funktion bzw. Rolle wird ebenso restriktiv zugewiesen wie die Rolle des Organisations-Administrators.

Reduziert die folgenden Risiken:

- R23 Aktenstücke im zentralen DossierStore werden verändert

MA (24) Nur Behörden-Administratoren erhalten ein Leserecht für den eigenen DossierStore

Der lesende Zugriff auf einen DossierStore einer verfahrensleitenden Justizbehörde erfordert die Organisationszugehörigkeit zur jeweiligen Justizbehörde in der Funktion «Zustellungen aufgeben». Alle anderen Teilnehmer können nur über die Mechanismen der elektronischen Akteneinsicht auf einen DossierStore zugreifen.

Reduziert die folgenden Risiken:

- R24 Aktenstücke im zentralen DossierStore werden von unberechtigten Dritten eingesehen

MA (25) Benutzerregistrierung nur über akzeptierte Identity Provider (IdP)

Natürliche Personen können sich im Adressverzeichnis der Plattform Justitia.Swiss nur mit einer digitalen Identität eines Identity Providers (IdP) registrieren, der die von der Plattform Justitia.Swiss geforderten Qualitätskriterien erfüllt.

Die detaillierten Anforderungen in Bezug auf die Vertrauensstufe der Registrierung werden in einem Dokument «Detailanforderungen an die akzeptierten Identity Provider» noch spezifiziert (vgl. Sicherheitsmassnahme MO (1)). Grundsätzlich gelten die Kriterien der Vertrauensstufe für Registrierung 3 (VSR3) aus dem eCH «Qualitätsmodell zur Authentifizierung von Subjekten» (eCH-170 v2) [Ext8]), die wiederum dem Identification Assurance Level 3 (IAL2) gemäss den NIST "Digital Identity Guidelines, Band A" (NIST SP 800-63-3A) [Ext11]) entsprechen.

Der IdP liefert mindestens die Attribute der zivilen Identität (amtlicher Name, Vornamen, Geburtsdatum, Geschlecht, sowie möglicherweise weitere notwendige). Ob bzw. welche zusätzlichen Attribute ein Identity Provider in der geforderten Qualität liefern kann, hängt von dessen Implementierung und

der Vereinbarung zwischen der Plattform Justitia.Swiss und dem Identity Provider ab. Neben den Adressangaben wären insbesondere die Organisationszugehörigkeit und die Funktion innerhalb der Organisation von grossem Interesse.

Reduziert die folgenden Risiken:

- R30 Registrierung eines Benutzers unter einer falschen Identität
- R34 Organisationszugehörigkeiten werden nicht nachgeführt

MA (26) Definierte minimale Qualitätsstufe für jedes Attribut im Adressverzeichnis

Für jedes im Adressverzeichnis der Plattform Justitia.Swiss geführte Attribut von Organisationen und natürlichen Personen wird festgelegt, welche minimale Qualitätsstufe in Bezug auf die initiale Erfassung und die laufende Pflege erforderlich ist.

Die Festlegung dieser Qualitätsstufen kann sich an den folgenden eCH-Standards orientieren:

- Für die Attribute der digitalen Identität: Qualitätsmodell zur Authentifizierung von Subjekten (eCH-170 v2, [Ext8]);
- Für die übrigen Attribute: Qualitätsmodell der Attributwertbestätigung zur eID (eCH-0171, [Ext9]) und Gestaltungsprinzipien für die Identitäts- und Zugriffsverwaltung (IAM) (eCH-0107, [Ext10]).

Reduziert die folgenden Risiken:

- R28 Fehlerhafte Konfiguration von Justizbehörden auf der Plattform Justitia.Swiss
- R29 Fehlerhafte Konfiguration von Anwaltskanzleien auf der Plattform Justitia.Swiss
- R30 Registrierung eines Benutzers unter einer falschen Identität
- R31 Fehlerhafte Verwaltung von Benutzerattributen im Adressverzeichnis

MA (27) Mehrstufiges Qualitätsmodell für die Attribute im Adressverzeichnis

Für eine flexible Handhabung der Attribute im Adressverzeichnis der Plattform Justitia.Swiss sieht dessen Datenmodell zu jedem Attribut das Meta-Attribut «Qualitätsstufe» vor. Dies ermöglicht ein mehrstufiges Qualitätsmodell mit beispielsweise vier Stufen gemäss eCH-0171 ([Ext9]), so dass der Datenbezüger je nach der Qualitätsstufe des bezogenen Attributwerts unterschiedlich mit dem Abfrageergebnis umgehen kann.

Mögliche Qualitätsstufen könnten sein:

- Stufe 0: Selbst-registriert (keine Qualitätskontrolle)
- Stufe 1a: Verifiziert durch die Plattform (z.B. Verifikation der E-Mail-Adresse und/oder der Mobiltelefonnummer, indem ein Einmalpasswort oder eine Validierungs-URL zugestellt und anschliessend überprüft wird, unter Angabe des Zeitpunkts der Verifikation)
- Stufe 1b: Verifiziert durch eine Justizbehörde (z.B. Verifikation des Anwaltsregistereintrages eines Anwalts, unter Angabe des Zeitpunkts der Verifikation)
- Stufe 2: Online mit dem massgeblichen Register abgeglichen

Reduziert die folgenden Risiken:

- R28 Fehlerhafte Konfiguration von Justizbehörden auf der Plattform Justitia.Swiss
- R29 Fehlerhafte Konfiguration von Anwaltskanzleien auf der Plattform Justitia.Swiss
- R30 Registrierung eines Benutzers unter einer falschen Identität
- R31 Fehlerhafte Verwaltung von Benutzerattributen im Adressverzeichnis

MA (28) Definierter Eigentümer für jedes Attribut im Adressverzeichnis

Für jedes im Adressverzeichnis der Plattform Justitia.Swiss bewirtschaftete Attribut von Organisationen und natürlichen Personen wird festgelegt, welche Organisation für die Einhaltung der definierten minimalen Qualitätsstufe verantwortlich ist.

Diese Verantwortung wird im Anschlussvertrag der Justizbehörden (vgl. Massnahme 0 beziehungsweise im Nutzungsvertrag der Verfahrensbeteiligten (vgl. Massnahme MO (13)) vereinbart.

Reduziert die folgenden Risiken:

- R27 Nicht mehr benötigte Aktenstücke im zentralen DossierStore werden nicht gelöscht
- R28 Fehlerhafte Konfiguration von Justizbehörden auf der Plattform Justitia.Swiss
- R29 Fehlerhafte Konfiguration von Anwaltskanzleien auf der Plattform Justitia.Swiss
- R30 Registrierung eines Benutzers unter einer falschen Identität
- R31 Fehlerhafte Verwaltung von Benutzerattributen im Adressverzeichnis

MA (29) Abgleich mit relevanten Registerdaten, wo sinnvoll

Der definierte Eigentümer eines Attributs im Adressverzeichnis entscheidet darüber, mit welchen Registern (z.B. Betriebs- und Unternehmensregister BUR, Handelsregister HR, Adressverzeichnis der Post, Kantonale Anwaltsregister, Register von Anwaltsverbänden, …) die Attributwerte abgeglichen werden und in welcher Form (z.B. manuell oder automatisiert) und Periodizität dieser Abgleich zu erfolgen hat, damit die definierte minimale Qualitätsstufe erreicht wird.

Reduziert die folgenden Risiken:

- R27 Nicht mehr benötigte Aktenstücke im zentralen DossierStore werden nicht gelöscht
- R28 Fehlerhafte Konfiguration von Justizbehörden auf der Plattform Justitia.Swiss
- R29 Fehlerhafte Konfiguration von Anwaltskanzleien auf der Plattform Justitia.Swiss
- R30 Registrierung eines Benutzers unter einer falschen Identität
- R31 Fehlerhafte Verwaltung von Benutzerattributen im Adressverzeichnis

MA (30) Option: Initial Load aller Justizbehörden und Anwälte

Die Gesamtzahl aller Justizbehörden und Anwälte in der Schweiz ist überschaubar. Es wird deshalb geprüft, ob in der Realisierungsphase des Projektes alle Justizbehörden und Anwälte im Adressverzeichnis der Plattform Justitia.Swiss initial erfasst (aber noch nicht aktiviert) werden sollen. Bei einem solchen Initial Load aus einem (oder mehreren) hierfür geeigneten Registern könnte mit vertretbarem Aufwand eine angemessene Qualität der Daten erreicht werden.

Reduziert die folgenden Risiken:

- R28 Fehlerhafte Konfiguration von Justizbehörden auf der Plattform Justitia.Swiss
- R29 Fehlerhafte Konfiguration von Anwaltskanzleien auf der Plattform Justitia.Swiss
- R30 Registrierung eines Benutzers unter einer falschen Identität
- R31 Fehlerhafte Verwaltung von Benutzerattributen im Adressverzeichnis

MA (31) Attribute werden nur angezeigt, wenn ihre Qualität stimmt

Das Adressverzeichnis zeigt nur Daten an, deren Qualität der definierten minimalen Qualitätsstufe entspricht. Selbstdeklarierte Daten, bei denen die minimale Qualitätsstufe eine Verifikation erfordert, werden nur dem Benutzer selber sowie den für die Verifikation verantwortlichen Administratoren angezeigt.

Reduziert die folgenden Risiken:

- R27 Nicht mehr benötigte Aktenstücke im zentralen DossierStore werden nicht gelöscht
- R28 Fehlerhafte Konfiguration von Justizbehörden auf der Plattform Justitia.Swiss
- R29 Fehlerhafte Konfiguration von Anwaltskanzleien auf der Plattform Justitia.Swiss
- R30 Registrierung eines Benutzers unter einer falschen Identität
- R31 Fehlerhafte Verwaltung von Benutzerattributen im Adressverzeichnis

MA (32) Festlegen der organisationsunabhängigen Grundberechtigungen

Im Rahmen des Berechtigungskonzeptes wird definiert, welche Grundberechtigungen allen Teilnehmern unabhängig von einer Organisationsmitgliedschaft zugewiesen werden.

Reduziert die folgenden Risiken:

- R35 Unerwünschte Rechtekumulation bei «Mehrfachanstellungen»
- R36 Zu weit reichende organisationsunabhängige Grundberechtigungen

MA (33) Regeln für Organisationszuweisung vorsehen

Die Plattform Justitia.Swiss sieht die Möglichkeit vor, dass bei der Erfassung einer Organisationszugehörigkeit gewisse konfigurierbare Regeln zur Anwendung kommen. Solche Regeln können beispielsweise sein (nicht abschliessend):

- Es können nur Teilnehmer als Mitglied aufgenommen werden, bei denen die Domain der E-Mail-Adresse mit der Domain der Organisation übereinstimmt;
- Es können nur Teilnehmer als Mitglied aufgenommen werden, deren digitale Identität von einem spezifisch definierten Identity Provider stammt;
- Die Funktion «Administrator» kann nur einem Teilnehmer zugewiesen werden, der die Funktion «Administrator» nicht bereits bei einer anderen Organisation innehat;
- Für Funktionen mit besonders weitreichenden Berechtigungen wird die Organisationszugehörigkeit nicht halbjährlich, sondern quartalsweise überprüft (vgl. 0).

Es ist möglich, für die Zuweisung verschiedener Funktionen verschiedene Regeln anzuwenden.

Reduziert die folgenden Risiken:

- R31 Fehlerhafte Verwaltung von Benutzerattributen im Adressverzeichnis
- R32 Fehlerhafte Erfassung von Organisationszugehörigkeiten

MA (34) Delegationen sind befristet und maximal 12 Monate gültig

Bei der Einrichtung einer Delegation muss eine Gültigkeitsfrist von maximal 12 Monaten angegeben werden. Delegationen können vor dem Ablaufen der Frist erneuert bzw. verlängert werden.

Reduziert die folgenden Risiken:

- R36 Zu weit reichende organisationsunabhängige Grundberechtigungen
- R37 Delegationen werden nicht nachgeführt

MA (35) QS-System für Transaktionsverarbeitung und Datenbestände

Die Plattform Justitia.Swiss implementiert organisatorische und technische Prozesse, mit denen eine ausreichend hohe Qualität der Transaktionsverarbeitung und der Datenhaltung sichergestellt wird. Dieses Qualitätssicherungs-System deckt insbesondere ab:

- Eine automatische Prüfung, dass alle Eingaben und Zustellungen abgeholt oder anderweitig korrekt verarbeitet wurden;
- Eine automatische Prüfung, dass für alle aktuell gültigen Akteneinsichtsrechte eine entsprechende Zustellung und/oder Delegation vorliegt;
- Eine automatische Prüfung, dass für alle aktuell im zentralen DossierStore abgelegten Dateien eine entsprechende Zustellung eingegangen ist;
- Eine automatische Prüfung, dass für alle aktuellen Einträge im Adressverzeichnis ein entsprechender Administrationszugriff im Audit Trail vorhanden ist;
- Eine automatische Prüfung, dass Änderungen / Transaktionen von zulässigen Akteuren durchgeführt werden.

Reduziert die folgenden Risiken:

- R6 Eingaben gehen verloren
- R13 Der Empfänger einer Zustellung wird nicht erreicht
- R14 Eine fehlerhafte Zustellung führt zu unerwünschtem Aktenzugriff
- R23 Aktenstücke im zentralen DossierStore werden verändert
- R27 Nicht mehr benötigte Aktenstücke im zentralen DossierStore werden nicht gelöscht

5.3 Technische Sicherheitsmassnahmen

MT (1) Verschlüsselung aller auf der Plattform Justitia.Swiss gespeicherten Daten

Alle auf der Plattform Justitia.Swiss gespeicherten Daten sind verschlüsselt (Verschlüsselung von *data at rest*). Für die Verschlüsselung wird ein kryptographischer Schlüssel verwendet, der in einer manipulationsgeschützten Hardware (einem Hardware Security Module, HSM) gespeichert ist.[10]

Dies betrifft insbesondere:

- Eingaben im persönlichen Arbeitsbereich des Absenders und im Postfach des Adressaten;
- Zustellungen und alle aus den Zustellungen abgeleiteten Autorisierungsdaten;
- Delegationen;
- Das Adressverzeichnis;
- Der Audit Trail;
- Der DossierStore (bei zentraler Datenhaltung);

Reduziert die folgenden Risiken:

- R5 Eingaben werden von unberechtigten Dritten eingesehen
- R21 Unberechtigte Einsicht in verfahrensbezogene Randdaten
- R23 Aktenstücke im zentralen DossierStore werden verändert
- R24 Aktenstücke im zentralen DossierStore werden von unberechtigten Dritten eingesehen

[10] Siehe Anhang E: Kapitel 2.4.4 aus E29 Varianten Plattform «Justitia.Swiss»

MT (2) Verschlüsselung aller Kommunikationsverbindungen

Alle Kommunikationsverbindungen der Plattform Justitia.Swiss sind verschlüsselt (Verschlüsselung von *data in transit*). Für die Verschlüsselung wird TLS (Transport Layer Security) in der Version 1.2 oder höher oder ein mindestens gleichwertiges Verschlüsselungsprotokoll verwendet.[11]

Dies betrifft insbesondere:

- Die Verbindung zwischen einem Browser und dem Web-Portal der Plattform Justitia.Swiss;
- Die API-Verbindungen zu den IT-Systemen von verfahrensleitenden Justizbehörden;
- Die API-Verbindungen zu den IT-Systemen von Verfahrensbeteiligten;
- Die API-Verbindungen zu den IT-Systemen von Partnern (z.B. Siegel-Service und Identity-Service).

Reduziert die folgenden Risiken:

- R5 Eingaben werden von unberechtigten Dritten eingesehen
- R16 Es werden gefälschte Zustellungen erfasst
- R17 Akten werden von unberechtigten Dritten über die Plattform eingesehen

MT (3) Virenscan auf der Plattform Justitia.Swiss für alle transferierten Dateien

Die Plattform Justitia.Swiss führt für alle transferierten Dateien einen Virenscan durch.

Dies betrifft insbesondere:

- Dateien, die als Eingabe an eine Justizbehörde transferiert werden;
- Dateien, die bei der elektronischen Akteneinsicht aus einem DossierStore bezogen werden.

Reduziert die folgenden Risiken:

- R7 Mit Schadsoftware verseuchte Eingaben schädigen die IT-Systeme anderer Teilnehmer
- R20 Mit Schadsoftware verseuchte Aktenstücke werden zugestellt

MT (4) Quarantänebereich für potentiell schädliche Dateien

Dateien, die potentiell schädlich sind, werden von der Plattform Justitia.Swiss nicht zum adressierten Teilnehmer transferiert, sondern in einem Quarantänebereich abgelegt. Dies betrifft insbesondere:

- Dateien, bei denen die Virenprüfung ein positives Resultat ergeben hat (*Hinweis*: Auch diese Dateien dürfen aus fachlichen Gründen nicht automatisch gelöscht werden);
- Dateien, die nicht auf Viren geprüft werden können (z.B. verschlüsselte Dateien);
- Ausführbare Dateien (z.B. .exe Dateien, Office-Dokumente mit Makros).

Der Absender und der Adressat der Datei werden über die Ablage im Quarantänebereich informiert, so dass sie bei der weiteren Verarbeitung die nötige Sorgfalt anwenden und Massnahmen ergreifen können. Die Plattform Justitia.Swiss verlangt von den Benutzern beim Bezug einer Datei aus dem Quarantänebereich die Bestätigung, dass sie über die Risiken im Umgang mit Schadsoftware informiert sind und die Verantwortung für allfällige Schadenfälle übernehmen. Diese Bestätigung wird im Audit Trail der Plattform Justitia.Swiss protokolliert.

Eingaben können von der Quarantäneregel ausgenommen werden, wenn sie sich auf ein laufendes Verfahren beziehen und von einem Teilnehmer eingereicht werden, der über ein Einsichtsrecht in die Akte zu diesem Verfahren verfügt.

Reduziert die folgenden Risiken:

- R7 Mit Schadsoftware verseuchte Eingaben schädigen die IT-Systeme anderer Teilnehmer
- R20 Mit Schadsoftware verseuchte Aktenstücke werden zugestellt

[11] Siehe Anhang E: Kapitel 2.4.4 aus E29 Varianten Plattform «Justitia.Swiss»

MT (5) Definierter Katalog von gültigen Dateiformaten

Die Plattform Justitia.Swiss definiert einen Katalog von Dateiformaten, die im Rahmen von Eingaben und Zustellungen über die Plattform transferiert werden dürfen. Für Organisationen, deren Software in Bezug auf die Einhaltung von Mindestvorgaben geprüft wurde, kann ein erweiterter Katalog von gültigen Dateiformaten definiert werden.

Reduziert die folgenden Risiken:

- R8 Eingaben oder Zustellungen können vom Empfänger nicht gelesen werden

MT (6) Web Application Firewall (WAF) und API-Gateway

Alle Kommunikationsverbindungen aus dem Internet werden auf einer vorgelagerten Web Application Firewall (WAF) und/oder API-Gateway terminiert und auf schädliche Inhalte kontrolliert.

Die WAF und das API-Gateway stellen insbesondere sicher:

- Dass alle Verbindungen über einen sicher konfigurierten TLS-Endpunkt verschlüsselt sind;
- Dass nur authentifizierte Benutzer eine Verbindung zum Applikationsserver der Justitia.Swiss-Plattform herstellen können (gilt sowohl für Browser-Zugriffe als auch für API-Zugriffe);
- Dass alle transferierten Inhalte (inkl. XML-Dateien) auf schädliche Inhalte geprüft werden.

Reduziert die folgenden Risiken:

- R48 Erfolgreicher Hackerangriff auf die Plattform Justitia.Swiss
- R49 Missbrauch eines Benutzerzugangs auf die Plattform Justitia.Swiss

MT (7) Risikoabhängige Zugriffskontrolle auf der Justitia.Swiss-Plattform

Die Web Application Firewall (WAF) weist jeder Kommunikationsverbindung eine Risikostufe zu. Je nach dem Kontext eines spezifischen Zugriffs (beispielsweise der Zeitpunkt des Zugriffs oder das für den Zugriff verwendete Endgerät) werden gewisse Funktionen nicht erlaubt (z.B. kein Bulk Download von einsehbaren Aktenstücken) oder zusätzliche Sicherheitsmassnahmen aktiviert (z.B. detaillierteres Logging).

Reduziert die folgenden Risiken:

- R48 Erfolgreicher Hackerangriff auf die Plattform Justitia.Swiss
- R49 Missbrauch eines Benutzerzugangs auf die Plattform Justitia.Swiss

MT (8) Begrenzte Session-Lebensdauer auf der Justitia.Swiss-Plattform

Die Web Application Firewall (WAF) bricht die Kommunikationsverbindung mit einem Browser oder einer integrierten Kanzleisoftware nach einer definierbaren Zeit der Inaktivität (*Session timeout*) oder nach maximal 10 Stunden (Maximale session lifetime) ab, so dass sich der Benutzer erneut mit 2 Faktoren beim IdP authentifizieren muss. Ausserdem bietet die Justitia.Swiss-Plattform den Benutzern an, die Session über eine Logout-Funktion aktiv zu beenden.

Reduziert die folgenden Risiken:

- R48 Erfolgreicher Hackerangriff auf die Plattform Justitia.Swiss
- R49 Missbrauch eines Benutzerzugangs auf die Plattform Justitia.Swiss

MT (9) Physische Separierung (anonymer Bereich sowie nicht-produktiver und produktiver Umgebungen)

Auf dem Applikationsserver der Plattform Justitia.Swiss gibt es keinen anonym (d.h. öffentlich) zugänglichen Bereich.

Der Plattformbetreiber bietet zudem eine Option für den Betrieb der Plattform Justitia.Swiss auf einer dedizierten Hardware an, die nicht mit anderen Kunden geteilt wird. Es wird zu einem späteren Zeitpunkt unter Berücksichtigung der Kosten entschieden, ob diese Option wahrgenommen wird.

Die Produktionsumgebung ist von den restlichen (nicht-produktiven) Umgebungen physisch getrennt (minimale geteilte Infrastruktur- und Netzwerkkomponenten).

Reduziert die folgenden Risiken:

- R48 Erfolgreicher Hackerangriff auf die Plattform Justitia.Swiss
- R49 Missbrauch eines Benutzerzugangs auf die Plattform Justitia.Swiss

MT (10) Sicherer Administrationszugang beim Plattformbetreiber (PAM)

Der Plattformbetreiber weist nach, wie er den sicheren Betrieb der Infrastruktur gewährleistet und insbesondere die administrativen Zugänge sichert. Wichtige Sicherheitsmassnahmen sind beispielsweise:

- Die 2-Faktor Authentifizierung aller manuellen Administrationszugriffe;
- Die Überwachung aller manuellen Administrationszugriffe (z.B. Screen Recording);
- Das Verhindern von Datenexporten (Data Leakage Prevention; DLP);
- Die gegenseitige Authentifizierung aller Verbindungen zu Systems Management Tools.

Reduziert die folgenden Risiken:

- R50 Missbrauch eines Administrationszugangs auf die Plattform Justitia.Swiss

MT (11) Sichere Remote Support Lösung im Service Desk

Falls der Service Desk für den Benutzersupport eine Fernzugriffslösung einsetzt, dann weist der Plattformbetreiber deren Sicherheit nach. Wichtige Sicherheitsanforderungen sind beispielsweise:

- Der Benutzer muss den Fernzugriff auf sein Endgerät explizit freischalten;
- Die Session ist verschlüsselt;
- Die Session wird aufgezeichnet.

Reduziert die folgenden Risiken:

- R43 Unberechtigte Dateneinsicht beim Supportzugriff durch den Service Desk

MT (12) Hardware Security Module (HSM) als Schlüsselspeicher auf der Plattform

Die kryptographischen Schlüssel für das Erzeugen von Siegeln und das Entschlüsseln der auf der Plattform Justitia.Swiss gespeicherten Daten (insb. DossierStore) befinden sich in einer sicheren Hardware (*Hardware Security Module*, HSM).

Reduziert die folgenden Risiken:

- R48 Erfolgreicher Hackerangriff auf die Plattform Justitia.Swiss
- R50 Missbrauch eines Administrationszugangs auf die Plattform Justitia.Swiss
- R51 Kompromittierung des Signierschlüssels der Plattform Justitia.Swiss

MT (13) Zentraler Protokollierungsdienst für technische Logs und den Audit Trail

Die Logs aller Infrastrukturkomponenten der Plattform Justitia.Swiss sowie der Audit Trail werden vom Plattformbetreiber in einem zentralen Protokollierungsdienst gesammelt und für die Detektion von Sicherheitsvorfällen genutzt.

Reduziert die folgenden Risiken:

- R48 Erfolgreicher Hackerangriff auf die Plattform Justitia.Swiss
- R49 Missbrauch eines Benutzerzugangs auf die Plattform Justitia.Swiss

- R50 Missbrauch eines Administrationszugangs auf die Plattform Justitia.Swiss

MT (14) Sichere Konfiguration aller Webserver der Plattform Justitia.Swiss

Alle Webserver der Justitia.Swiss-Plattform werden so konfiguriert, dass die Umleitung der Benutzer auf eine gefälschte Website (z.B. technisch durch DNS-Cache-Poisoning oder organisatorisch durch Phishing) möglichst erschwert wird.

Spezifische Massnahmen sind beispielsweise:

- Permanent Redirect;
- HSTS inkl. Pre-Loading;
- DNSSec;
- Nutzung von EV-SSL Webserver-Zertifikaten.

Reduziert die folgenden Risiken:

- R52 Erfolgreiche Denial of Service (DoS) Attacke auf die Plattform Justitia.Swiss
- R53 DNS Spoofing oder Phishing

MT (15) Ausweichstandort und BCM

Der Plattformbetreiber weist den Betrieb eines Managementsystems nach, um die Verfügbarkeit und Disaster-Resilienz der betriebenen Services zu managen. Er ist in der Lage, den Betrieb der Justitia.Swiss-Plattform nach einem physischen oder logischen Schadenereignis an einem Ausweichstandort rasch wieder sicherzustellen. Wesentliche Elemente eines solchen BCM sind:

- Nachweisbare Kenntnisse in Business-Continuity, ein ISO-Zertifikat 22301 ist ein Pluspunkt;
- Disaster Prozesse, um eine Wiederanlaufzeit (RTO) von < 24 Stunden zu gewährleisten;
- Disaster Prozesse, um den maximalen Datenverlust (RPO) auf < 15 Minuten zu beschränken;
- Ein zusätzlicher Datenbackup-Standort;
- Gute Isolation der Ressourcen (Strom, Wasser, Kommunikation, etc.) zwischen den Standorten.

Reduziert die folgenden Risiken:

- R54 Totalverlust der Plattform Justitia.Swiss im Katastrophenfall

5.4 Massnahmenübersicht

ID	Titel	Risiken	Aufwand	Nutzen
Organisatorische Sicherheitsmassnahmen				
MO (1)	Detailkonzepte zur Informationssicherheit	Alle	Mittel	Gross
MO (2)	Nach ISO/IEC 27001 zertifiziertes ISMS	Alle	Gross	Gross
MO (3)	Security Information and Event Management (SIEM)	R45, R48, R49, R50, R52, R53	Gross	Gross
MO (4)	Awareness-Programm für alle Benutzergruppen	Alle	Mittel	Mittel
MO (5)	Kein Transfer von geheimen Daten über die Plattform Justitia.Swiss	Alle	Klein	Gross
MO (6)	Periodische Überprüfung des Adressverzeichnisses	R27, R28, R29, R30, R31, R32, R33, R34, R35	Mittel	Gross
MO (7)	Periodische Rezertifizierung aller gültigen Zustellungen	R13, R14, R26, R27, R37	Mittel	Mittel
MO (8)	Quartalsweise Rezertifizierung aller gültigen Delegationen	R13, R14, R26, R27, R37	Mittel	Mittel
MO (9)	Ein Profil pro Organisationszugehörigkeit	R33, R34, R35, R37, R38, R39	Klein	Gross
MO (10)	Sicherheitsverantwortung des Softwarelieferanten als Vertragsbestandteil	R47, R48, R49	Klein	Mittel
MO (11)	Sicherheitsverantwortung des Plattformbetreibers als Vertragsbestandteil	R48, R49, R50, R51, R52	Klein	Gross
MO (12)	Sicherheitsverantwortung der Justizbehörden als Bestandteil des Anschlussvertrags	R14, R26, R27, R28	Mittel	Gross
MO (13)	Sicherheitsverantwortung der Verfahrensbeteiligten als Teil der Nutzungsbedingungen	R7, R49	Mittel	Gross
MO (14)	Sicherheitsmassnahmen gelten auch für verfahrensbeteiligte Justizbehörden	R22	Klein	Mittel
MO (15)	Zuverlässige Anruferidentifikation durch den Service Desk	R41, R42	Mittel	Klein
MO (16)	Secure Software Development	R46	Klein	Mittel
MO (17)	Auditrecht der öffentlich-rechtlichen Körperschaft beim Plattformbetreiber	R49	Klein	Mittel
MO (18)	Pentest (Manual Hacking) aller Benutzerschnittstellen	R40, R48, R49	Klein	Mittel
MO (19)	Vulnerability-Monitoring aller Internet-Zugangspunkte	R40, R48	Klein	Mittel
MO (20)	Quelltext-Analyse aller Sicherheitsmodule	R46	Klein	Mittel

Tabelle 13: Übersicht organisatorische Sicherheitsmassnahmen

Applikatorische Sicherheitsmassnahmen				
MA (1)	Elektronisches Plattform-Siegel für alle Eingaben	R1	Gross	Gross
MA (2)	Möglichkeit zur Eingabe vorgängig digital signierter Dateien	R1	Klein	Klein
MA (3)	Das Plattform-Siegel verlangt eine Willensbekundung des Absenders	R2	Klein	Mittel
MA (4)	Die Plattform zeichnet alle rechtsverbindlichen Ereignisse in einem Audit Trail auf	R2, R10, R12	Mittel	Gross
0 MA (3)	Die Plattform kann elektronisch gesiegelte Eingangs- und Abrufquittungen erstellen	R2, R9, R10, R12	Gross	Mittel
MA (6)	2-Faktor-Authentifizierung (2FA) aller Benutzer	R3, R16, R17, R48, R49	Gross	Gross
MA (7)	Anbindung der Identity Provider über sichere Federation Protokolle	R3, R15, R16, R17, R49	Klein	Mittel
MA (8)	Gegenseitige Authentifizierung der Endpunkte bei allen API-Verbindungen	R15, R16, R17, R18, R49	Klein	Gross
MA (9)	Qualitätssicherung für übermittelte strukturierte Daten	R4	Klein	Klein
0 MA (10)	Sichere persönliche Arbeitsbereiche für Verfahrensbeteiligte	R5, R9	Mittel	Mittel
MA (11)	Sichere Postfächer für verfahrensleitende Justizbehörden	R4, R5, R6, R9, R11, R49	Mittel	Mittel
MA (12)	Zugriffskontrollsystem für Daten und Funktionen der Plattform Justitia.Swiss	R5, R20, R21, R24, R40, R41, R43, R44, R47, R49	Gross	Gross
MA (13)	Eingaben und Aktenstücke werden ausserhalb des DossierStore nicht aufbewahrt	R5, R9, R43, R48	Klein	Mittel
MA (14)	Zugestellte Aktenstücke werden online abgeholt	R8, R9, R10	Klein	Gross
MA (15)	Siegel-Validierung bei der elektronischen Akteneinsicht	R9, R10, R11	Mittel	Klein
MA (16)	Notifikation des Empfängers einer Zustellung	R12, R13	Klein	Klein
MA (17)	Berechtigungsrelevante Elemente einer Zustellung werden nie manuell erfasst	R13, R14	Klein	Mittel
MA (18)	Die Berechtigungswirkung einer Zustellung kann geprüft werden	R13, R14	Klein	Mittel
MA (19)	Zustellungen können auf der Plattform Justitia.Swiss annulliert werden	R14, R15	Klein	Klein
MA (20)	Die Berechtigungsprüfung ist Teil der DossierStore-Abfragetransaktion	R18, R19	Klein	Mittel
MA (21)	Elektronisches Siegel für alle Aktenstücke im zentralen DossierStore	R21, R23	Mittel	Mittel
MA (22)	Mandantentrennung im zentralen DossierStore	R23, R24	Klein	Mittel
MA (23)	Kein direktes Schreibrecht auf den zentralen DossierStore	R23	Klein	Mittel

MA (24)	Nur Behörden-Administratoren erhalten ein Leserecht für den eigenen DossierStore	R24	Klein	Mittel
MA (25)	Benutzerregistrierung nur über akzeptierte Identity Provider (IdP)	R30, R34	Klein	Gross
MA (26)	Definierte minimale Qualitätsstufe für jedes Attribut im Adressverzeichnis	R28, R29, R30, R31	Gross	Gross
MA (27)	Mehrstufiges Qualitätsmodell für die Attribute im Adressverzeichnis	R28, R29, R30, R31	Mittel	Klein
MA (28)	Definierter Eigentümer für jedes Attribut im Adressverzeichnis	R27, R28, R29, R30, R31	Klein	Mittel
MA (29)	Abgleich mit relevanten Registerdaten, wo sinnvoll	R27, R28, R29, R30, R31	Mittel	Mittel
MA (30)	Option: Initial Load aller Justizbehörden und Anwälte	R28, R29, R30, R31	Klein	Mittel
MA (31)	Attribute werden nur angezeigt, wenn ihre Qualität stimmt	R27, R28, R29, R30, R31	Klein	Gross
MA (32)	Festlegen der organisationsunabhängigen Grundberechtigungen	R35, R36	Klein	Mittel
MA (33)	Regeln für Organisationszuweisung vorsehen	R31, R32	Mittel	Gross
MA (34)	Delegationen sind befristet und maximal 12 Monate gültig	R36, R37	Klein	Mittel
MA (35)	QS-System für Transaktionsverarbeitung und Datenbestände	R6, R13, R14, R23, R27	Gross	Gross

Tabelle 14: Übersicht applikatorische Sicherheitsmassnahmen

ID	Titel	Risiken	Aufwand	Nutzen
Technische Sicherheitsmassnahmen				
MT (1)	Verschlüsselung aller auf der Plattform Justitia.Swiss gespeicherten Daten	R5, R21, R23, R24	Mittel	Gross
0 MT (2)	Verschlüsselung aller Kommunikationsverbindungen	R5, R16, R17	Klein	Gross
MT (3)	Virenscan auf der Plattform Justitia.Swiss für alle transferierten Dateien	R7, R20	Klein	Mittel
MT (4)	Quarantänebereich für potentiell schädliche Dateien	R7, R20	Mittel	Mittel
0 MT (3)	Definierter Katalog von gültigen Dateiformaten	R8	Klein	Klein
MT (6)	Web Application Firewall (WAF) und API Gateway	R48, R49	Mittel	Gross
MT (7)	Risikoabhängige Zugriffskontrolle auf der Justitia.Swiss-Plattform	R48, R49	Mittel	Mittel
MT (8)	Begrenzte Session-Lebensdauer auf der Justitia.Swiss-Plattform	R48, R49	Klein	Mittel
0 MT (9)	Physische Separierung (anonymer Bereich sowie nicht-produktiver und produktiver Umgebungen)	R48, R49	Klein	Gross
MT (10)	Sicherer Administrationszugang beim Plattformbetreiber (PAM)	R50	Klein	Gross
MT (11)	Sichere Remote Support Lösung im Service Desk	R43	Klein	Mittel
MT (12)	Hardware Security Module (HSM) als Schlüsselspeicher auf der Plattform	R48, R50, R51	Mittel	Mittel
MT (13)	Zentraler Protokollierungsdienst für technische Logs und den Audit Trail	R48, R49, R50	Gross	Gross
0 MT (14)	Sichere Konfiguration aller Webserver der Plattform Justitia.Swiss	R52, R53	Klein	Gross
MT (15)	Ausweichstandort und BCM	R54	Gross	Gross

Tabelle 15: Übersicht technische Sicherheitsmassnahmen

6 Restrisikobetrachtung nach Massnahmenumsetzung

Nachfolgend sind, nicht abschliessend, die wichtigsten Restrisiken beschrieben, die nach Umsetzung aller organisatorischen, applikatorischen und technischen Sicherheitsmassnahmen verbleiben und getragen werden müssen.

Abhören aller über die Justitia.Swiss-Plattform transferierten Dateien

- Eingaben und Aktenstücke, die im Rahmen des elektronischen Rechtsverkehrs (ERV) und der elektronischen Akteneinsicht (eAE) über die Plattform Justitia.Swiss transferiert werden, sind während der Übertragung auf der Plattform selber im Klartext vorhanden (keine Ende-zu-Ende Verschlüsselung). Ein Angreifer mit Administrationsrechten auf der Plattform hat somit die Möglichkeit, durch die unbemerkte Installation entsprechender Werkzeuge diese Dateien abzuhören und Kopien davon zu erstellen. Die Risikobeurteilung ist für alle potentiellen Angreifer[12] ähnlich und wird grösstenteils durch die weitgehenden Sicherheitsmassnahmen gegen anonyme Hackerangriffe mitigiert.
- Eine Manipulation der transferierten Daten ist Dank der durchgängigen Verwendung von digitalen Siegeln ausgeschlossen.

Unsichere Endgeräte und Datenablagen der privaten Benutzer

- Die Erfahrung zeigt, dass privat genutzte Endgeräte nur unzureichend gegen Schadsoftware geschützt werden können. Es muss deshalb davon ausgegangen werden, dass unberechtigte Dritte durch die Fernsteuerung von Endgeräten von privaten Parteien in einem Justizverfahren in den Besitz von Aktenstücken gelangen können. Weil solche Angriffe normalerweise ungezielt erfolgen, ist die durchschnittliche Tragweite solcher Attacken allerdings relativ gering.
- Die Endgeräte und Datenablagen von Mitarbeitenden bei Justizbehörden, Anwaltskanzleien und juristischen Personen werden professioneller betrieben und sind insgesamt besser geschützt, wobei allerdings eine sehr grosse Bandbreite anzunehmen ist.

Fehlerhafte Verwaltung von Organisationszugehörigkeiten

- Die Teilnehmer registrieren sich auf der Plattform Justitia.Swiss als natürliche Person und die Organisationszugehörigkeit wird erst anschliessend in einem separaten Prozess festgelegt. Beim Austritt eines Mitarbeiters einer Justizbehörde behält der Mitarbeiter seinen Zugang auf die Plattform Justitia.Swiss mit allen seinen Berechtigungen, bis die Organisationszugehörigkeit gelöscht wird.
- Die Erfahrung zeigt, dass dieser Prozess nicht rasch und zuverlässig funktioniert, wenn er wie aktuell geplant manuell und ohne Integration mit den HR-Systemen (oder einem mit den HR-Systemen der jeweiligen Organisationen verknüpften Identity Provider) umgesetzt wird.

Fehlerhafte Verwaltung von Delegationen

- Die Teilnehmer können ihre eigenen Berechtigungen an andere Teilnehmer delegieren und diese Delegationen bleiben bestehen, wenn der delegierende Teilnehmer oder der delegierte Teilnehmer die Organisationszugehörigkeit wechselt.
- Die Erfahrung mit solchen manuellen Prozessen zeigt, dass die delegierenden Teilnehmer nicht in der Lage sein werden, notwendige Mutationen an den von ihnen eingerichteten Delegationen rechtzeitig und zuverlässig vorzunehmen.

[12] insbesondere anonyme Internetbenutzer; Justitia.Swiss-Plattformbenutzer sowie Innentäter bei der öffentlich-rechtlichen Körperschaft und dem Plattformbetreiber

Anhang A: Fachbegriffe und Abkürzungen

Begriff oder Abkürzung	Bedeutung
EV-TLS Webserver-Zertifikat	Ein Webserver-Zertifikat, bei dem der Inhaber des Zertifikates mit besonderer Sorgfalt verifiziert wurde (EV steht für Extended Validation).
Hardware Security Module (HSM)	Eine sichere Hardware für die Speicherung kryptographischer Schlüssel und die Ausführung kryptographischer Funktionen (insbesondere die Entschlüsselung von Daten und die Erzeugung digitaler Signaturen).
Identity Provider (IdP)	Ein System, das Benutzer identifiziert, registriert und zur Laufzeit authentifiziert. Die Kommunikation zwischen Identity Provider und Service Provider erfolgt über Federation-Protokolle wie ->SAML oder ->OIDC.
ISDS	Informationssicherheit und Datenschutz.
Information Security Management System (ISMS)	Aufbau- und Ablauforganisation für die Etablierung und die kontinuierliche Verbesserung der Informationssicherheit, z.B. nach ISO/IEC 27001.
Mutually Authenticated TLS (MTLS)	Eine TLS-Verbindung, bei der sich nicht nur der Server gegenüber dem Client, sondern auch der Client gegenüber dem Server authentifiziert.
OpenID Connect (OIDC)	Ein Protokoll, über das Benutzerattribute auf sichere Weise von einem ->IdP an einen ->SP übermittelt werden (Alternative zu SAML).
Security Assertion Markup Language (SAML)	Ein Protokoll, über das Benutzerattribute auf sichere Weise von einem ->IdP an einen ->SP übermittelt werden (Alternative zu OIDC).
Service Provider (SP)	Eine Applikation, die den authentifizierten Benutzern Services zur Verfügung stellt, im Falle von Justitia 4.0 insbesondere das Portal Justitia.Swiss.
Security Information and Event Management (SIEM)	Prozesse und Werkzeuge für die Erkennung von Sicherheitsvorfällen und deren angemessene Bearbeitung (technisch und organisatorisch).
Transport Layer Security (TLS)	Verschlüsselung der Kommunikation zwischen einem Client und einem Server (z.B. Browser und Webserver), wobei sich der Server gegenüber dem Client unter Nutzung eines Server-Zertifikats authentifiziert.
Zivile Identität	Attribute einer natürlichen Person gemäss E-ID-Gesetz. Namentlich sind dies die E-ID-Registernummer, der amtliche Name, Vornamen, Geburtsdatum, Geschlecht, Geburtsort und Staatsangehörigkeit.

Anhang B: Detaillierte operative Geschäftsvorfälle

SO1 Eingabe

Eine verfahrensbeteiligte Person stellt eine Eingabe einer zuständigen Justizbehörde rechtsgültig elektronisch zur Verfügung.

Verfahrensbeteiligte können Eingaben über das Web-Portal der Plattform Justitia.Swiss oder über ein mit der Plattform Justitia.Swiss über API integriertes IT-System einreichen. Das Web-Portal der Justitia.Swiss-Plattform stellt den Verfahrensbeteiligten einen Arbeitsbereich für die Vorbereitung der Eingabe (z.B. schrittweises Hinzufügen und/oder Löschen von Beilagen) zur Verfügung. Dateien, die über die Plattform Justitia.Swiss eingereicht werden, werden beim Versand mit dem elektronischen Siegel der Plattform Justitia.Swiss versehen.

Die Plattform Justitia.Swiss notifiziert die adressierte Justizbehörde und speichert die Eingabe als eingehende Meldung in deren Postfach, bis sie entweder von der Justizbehörde abgeholt oder aus einem anderen Grund aus dem Postfach gelöscht wird. Für den Fall, dass sich die Eingabe auf ein laufendes Verfahren bei der adressierten Justizbehörde bezieht, transportiert die Plattform Justitia.Swiss die AkteID der zum Verfahren gehörigen einsehbaren Akte als Teil der Übermittlung vom Absender zum Empfänger.

Die anschliessende Verarbeitung der Eingabe seitens der verfahrensleitenden Justizbehörde (z.B. Validieren des Siegels, Ablegen/Verakten der Eingabe zusammen mit dem Siegel in der Akte, Verarbeiten der Quittungen) ist ausserhalb des Scope der Plattform Justitia.Swiss.

Jede im Adressverzeichnis registrierte Person kann jede angeschlossene Justizbehörde adressieren. Ausserdem sollen keinerlei Einschränkungen in Bezug auf das Format und den Inhalt der beigelegten Dateien gemacht werden. Die adressierte Justizbehörde entscheidet selber, ob bzw. wie sie die in ihrem Postfach gespeicherten Eingaben bearbeitet.

SO2 Zustellung

Eine Justizbehörde stellt einem Verfahrensbeteiligten ein oder mehrere Aktenstücke rechtsgültig elektronisch zur Verfügung, um einen Verfahrensschritt oder das Verfahren abzuschliessen.

Bei der Zustellung werden Aktenstücke (im Unterschied zur Eingabe) nicht mit der Zustellung übermittelt, sondern die Zustellung ist lediglich die Übermittlung der Berechtigung zur Akteneinsicht. Das eigentliche Lesen oder Herunterladen einer Datei entspricht dann einer elektronischen Akteneinsicht.

Verfahrensleitende Justizbehörden können Zustellungen über das Web-Portal der Plattform Justitia.Swiss oder über ein mit der Plattform Justitia.Swiss über API integriertes IT-System versenden. Das Web-Portal der Justitia.Swiss-Plattform stellt den verfahrensleitenden Justizbehörden einen Arbeitsbereich für die Vorbereitung der Zustellung (z.B. schrittweises Hinzufügen und/oder Löschen von Referenzen auf einsehbare Aktenstücke, Festlegen der Empfänger, Setzen einer Frist) zur Verfügung.

Die Plattform Justitia.Swiss speichert die Zustellung und benachrichtigt den Empfänger gemäss seinen Einstellungen im Profil. Der Empfänger kann während der Gültigkeitsdauer der Zustellung auf alle Aktenstücke zugreifen, die in der Zustellung mittels ihrer Aktenstück-Adresse referenziert sind. Eine Zustellung bezieht sich immer auf genau eine Akte, identifiziert mittels ihrer AkteID.

Bei einer Zustellung über die Plattform Justitia.Swiss kann jede verfahrensleitende Justizbehörde jede im Adressverzeichnis registrierte Person adressieren und zur Einsicht in die referenzierten Aktenstücke berechtigen.

SO3 Akteneinsicht

Eine berechtigte Person nimmt elektronisch Einsicht in ein oder mehrere Aktenstücke.

Ein Benutzer der Plattform Justitia.Swiss nimmt Einsicht in ein Aktenstück, indem er über das Web-Portal oder ein API der Plattform Justitia.Swiss die Aktenstück-Adresse aufruft, welche das Aktenstück auf der Plattform Justitia.Swiss eindeutig identifiziert. Die Aktenstück-Adresse ist Teil der Zustellung, die den Empfänger der Zustellung zur Einsicht in dieses Aktenstück berechtigt (siehe SO2).

Die Plattform Justitia.Swiss prüft, ob der Benutzer zur Einsicht in das gewünschte Aktenstück berechtigt ist, indem sie die auf der Plattform verfügbaren Autorisierungsdaten auswertet. Die Einsicht wird gewährt, wenn mindestens eine der folgenden Bedingungen erfüllt ist:

- Der Benutzer ist Inhaber eines Profils, dem eine zum aktuellen Zeitpunkt gültige Zustellung mit der Aktenstück-Adresse des aufgerufenen Aktenstücks zugestellt wurde (siehe SO2);
- Der Benutzer gehört zu einer Organisation, welche ein solches Profil innehat, und hat (von der Organisation) die entsprechenden Rechte zum Lesen der Akten erhalten (siehe SO8);
- Das Recht wurde an den Benutzer delegiert (siehe SO10).

Wenn der Benutzer zur Einsicht in das aufgerufene Aktenstück berechtigt ist, dann bezieht die Plattform Justitia.Swiss das Aktenstück über ein standardisiertes API aus dem DossierStore der verfahrensleitenden Justizbehörde und stellt es dem Benutzer zur Einsicht im Web-Portal, zum manuellen Download über das Web-Portal oder zum Bezug über API zur Verfügung. Ein schreibender Zugriff auf den DossierStore ist über die Akteneinsicht nicht möglich; Aktenstücke können somit auf dem Weg der Akteneinsicht weder gelöscht noch verändert werden.

Berechtigungen zur Einsicht werden ausschliesslich auf einzelne einsehbare elektronische Aktenstücke vergeben, indem eine verfahrensleitende Justizbehörde eine Zustellung an ein Profil übermittelt. Verfügt ein Benutzer über die Berechtigung zur Einsicht in mindestens ein Aktenstück einer Akte, dann ist er auch zur Einsicht in den Aktendeckel und in denjenigen Teil der Aktenverzeichnisstruktur (Rubriken) berechtigt, in den dieses Aktenstück eingeordnet ist.

Bei der Berechtigung zur Einsicht gibt es neben der Ausprägung «darf Inhalt und Meta-Daten lesen» auch die Ausprägung «darf (nur) Meta-Daten lesen». Bei dieser eingeschränkten Ausprägung erhält der Benutzer Einsicht in die identifizierenden (`behördeID`, `akteID`, `aktenstückID`), fachlichen (z.B. fachlicher Typ «Rechtsschrift», fachliche Funktion «Anklage») und technischen (z.B. Media-Typ «application/pdf», Anzahl Seiten `55`) Attribute des Aktenstücks sowie den Aktendeckel und den relevanten Teil der Aktenverzeichnisstruktur, nicht aber in das Aktenstück selber.

Die Berechtigung zur Einsicht in ein Aktenstück erlischt, wenn die entsprechende Akte geschlossen wird oder die Gültigkeit der Zustellung abläuft. Es ist noch nicht spezifiziert, ob und wie und von wem die Gültigkeitsdauer einer Zustellung oder andere Inhalte der Zustellung (z.B. Ausprägung der Berechtigung, Empfänger der Zustellung, Liste der Aktenstück-Adressen) auf der Plattform Justitia.Swiss nachträglich verändert werden können.

Hinweis: Die Implementierung der Akteneinsicht und insbesondere die Berechtigungsprüfung ist unabhängig davon, ob sich der DossierStore mit der einsehbaren elektronischen Akte auf der Plattform Justitia.Swiss (zentrale Datenhaltung) oder in der IT-Landschaft einer verfahrensleitenden Justizbehörde (dezentrale Datenhaltung) befindet; die Berechtigungsprüfung findet in jedem Fall zentral auf der Plattform Justitia.Swiss statt.

SO4 Interaktion zwischen Justizbehörden

Die Plattform Justitia.Swiss unterstützt auch den elektronischen Rechtsverkehr zwischen Justizbehörden. Die Architektur Plattform Justitia.Swiss (Anhang 7 der Ausschreibung - Architektur Plattform Justitia.Swiss) beschreibt im Kapitel 5 verschiedene Interaktionsmuster zwischen Behörden:

- Die Eingabe einer Behörde bei einer anderen verfahrensleitenden Justizbehörde, z.B. die Anklage einer Staatsanwaltschaft beim erstinstanzlichen Gericht;
- Die Weitergabe der Akten einer Behörde an eine andere Behörde, z.B. beim Weiterzug eines Verfahrens oder bei Nichtzuständigkeit;
- Das Akteneinsichtsgesuch in ein laufendes oder abgeschlossenes Verfahren, z.B. für den Beizug einer Verfahrensakte einer anderen Behörde in das eigene Verfahren;
- Die Klagebewilligung, wobei das Aktenstück «Klagebewilligung» zwischen den beteiligten Behörden nicht direkt, sondern über den Kläger oder dessen Vertreter ausgetauscht wird.

Alle Interaktionen zwischen Justizbehörden werden über die operativen Geschäftsvorfälle «Eingabe», «Zustellung» und «Akteneinsicht» abgewickelt, wobei bei jedem Geschäftsvorfall eine der beiden Behörden die Rolle des Verfahrensbeteiligten einnimmt.

SO5 Zentraler DossierStore als Service der Plattform Justitia.Swiss

Verfahrensleitende Justizbehörden, welche die Plattform Justitia.Swiss für die Speicherung der zugestellten und somit einsehbaren Akten im zentralen DossierStore verwenden, liefern bei der Zustellung auch die zuzustellenden Aktenstücke mit.

Die Plattform Justitia.Swiss speichert die von der verfahrensleitenden Justizbehörde gelieferten Aktenstücke im zentralen DossierStore und stellt sie dort zur Einsicht zur Verfügung. Im Laufe eines Verfahrens entsteht im zentralen DossierStore der Plattform Justitia.Swiss ein einsehbarer Auszug aus der elektronischen Akte mit Kopien aller zugestellten Aktenstücke sowie Zusatzinformationen wie dem Aktendeckel und der Aktenstruktur.

Spätestens bei Abschluss eines Verfahrens werden alle Aktenstücke aus dem zentralen DossierStore der Plattform Justitia.Swiss gelöscht.

Anhang C: Detaillierte administrative Geschäftsvorfälle

SO6 Organisationen verwalten

Die öffentlich-rechtliche Körperschaft (örK) verwaltet Organisationen im Adressverzeichnis der Plattform Justitia.Swiss, damit diese am ERV und an der eAE teilnehmen können.

Organisationen sind gemäss dem konzeptionellen Informationsmodell (vgl. Abbildung 2) eine Spezialisierung der Entität «Person». Organisationen verfügen einerseits über ein Profil und damit eine Zustelladresse und können somit als Person am elektronischen Rechtsverkehr (ERV) und an der elektronischen Akteneinsicht (eAE) teilnehmen. Organisationen sind ausserdem Gruppen von natürlichen Personen, die je über ein eigenes Profil sowie eine oder mehrere digitale Identitäten verfügen, mit denen sie sich an der Plattform Justitia.Swiss anmelden können. Organisationen können keine Organisationen enthalten, d.h. die Abbildung von Organisationsstrukturen ist nicht vorgesehen bzw. möglich.

Die folgenden Attribute einer Organisation sind für das Funktionieren der Plattform Justitia.Swiss erforderlich und sollen im Adressverzeichnis der Plattform Justitia.Swiss erfasst werden (die vollständige Liste der Attribute ist noch nicht definiert):

- *Ein eindeutiger Identifikator der Organisation*: Bei Justizbehörden soll dies eine von der örK ausgestellte Behörden-ID sein, deren Struktur und Wertebereich noch zu definieren sind. Bei allen anderen Organisationen ist dies die Unternehmens-Identifikationsnummer (UID) gemäss dem Betriebs- und Unternehmensregister (BUR) des Bundesamtes für Statistik, öffentlich zugänglich über das UID-Register (www.uid.admin.ch).
- *Der Status der Organisationseintrags im Adressverzeichnis*: Der Status kann neben dem Lebenszyklus des Eintrags (z.B. beantragt, aktiv, inaktiv) auch die Qualitätsstufe des Eintrags (z.B. selbstdeklariert, verifiziert, registergeprüft) bezeichnen.
- *Der Typ der Organisation*: Zwei wichtige Typen sind der Typ «Justizbehörde» und der Typ «Anwalt respektive Anwaltskanzlei»; weitere Typen (z.B. Verein, Rechtsschutzversicherung) sind noch nicht definiert, können aber hinzukommen.
- *Das Profil* für die Teilnahme an ERV und eAE umfasst mindestens die Zustelladresse;
- *Elektronische Kommunikationsadressen*: Eine oder mehrere E-Mail-Adressen und eine oder mehrere Telefonnummern, über welche die Plattform Justitia.Swiss mit der Organisation kommunizieren kann;
- *Organisations-Zugehörigkeiten*: Natürliche Personen, die zur Organisation gehören und jeweils eine oder mehrere Funktionen in Bezug auf die Organisation ausüben (vgl. SO8);
- *Organisations-Administrator*: Eine oder mehrere natürliche Personen, welche die Attribute der Organisation, die Organisationszugehörigkeiten (vgl. SO8) sowie die Delegationen (vgl. SO10) für das Profil der Organisation verwalten.

Als spätere Ausbaustufe können im Adressverzeichnis der Plattform Justitia.Swiss auch Organisations-Attribute verwaltet werden, die für das Funktionieren der Plattform nicht notwendig aber aus anderen Gründen nützlich sind. Mögliche Beispiele dafür sind:

- *Postalische Adressen*: Eine oder mehrere Postadressen (z.B. Domiziladresse, Korrespondenzadresse);
- *Spezialisierungen*: Vor allem bei Anwaltskanzleien interessant;
- *Organisationsstrukturen* wie Filialen oder Tochtergesellschaften.

Jede im Adressverzeichnis registrierte natürliche Person kann eine Organisation eröffnen, wobei sie automatisch auch der (erste) Administrator dieser Organisation wird. Es sollen auch administrative Prozesse für die Verwaltung (eröffnen, mutieren und löschen) von Organisationen und Organisations-Attributen möglich sein, diese sind aber noch nicht definiert.

Gemäss Anhang 7 der Ausschreibung - Architektur Plattform Justitia.Swiss sind derzeit kein Abgleich der Organisationsdaten mit einem Register (z.B. UID-Register, kantonale Anwaltsregister) und auch keine anderweitigen Qualitätskontrollen für Organisationsdaten vorgesehen. Dies würde bedeuten,

dass bei der Erfassung einer neuen Organisation beliebige Attributwerte eingegeben werden können und dass keinerlei Gewähr für die Korrektheit dieser Attribute besteht[13].

Es ist noch nicht definiert, ob und welche Typ-spezifischen Organisations-Attribute im Adressverzeichnis der Plattform Justitia.Swiss geführt werden. Für Organisationen vom Typ «Anwalt respektive Anwaltskanzlei» wären für den ERV und die eAE zusätzliche Attribute relevant wie beispielsweise das Anwaltspatent, Angaben zum Status des Anwaltspatents (z.B. suspendiert oder entzogen) oder Spezialisierungen der Kanzlei. Auch für solche Typ-spezifischen Attribute einer Organisation sieht die Plattform Justitia.Swiss aktuell keine Qualitätskontrollen vor, d.h. sie können vom Organisations-Administrator beliebig (auch falsch) erfasst werden.

Es ist derzeit noch keine Einschränkung dafür definiert, welche Benutzer welche Typen von Organisationen eröffnen und/oder administrieren können.

Es ist ebenfalls noch nicht definiert, welche technischen Attribute einer Organisation (z.B. URL und/oder IP-Adressen von API-Clients und API-Servern, Schlüssel oder Zertifikate für die gegenseitige Authentifizierung von API-Verbindungen, Identifikator und Zertifikat des von der Organisation genutzten Identity Providers) für deren Konfiguration auf der Plattform Justitia.Swiss benötigt und wie diese verwaltet werden.

SO7 Benutzer verwalten

Personen, welche die Plattform Justitia.Swiss benutzen wollen, registrieren sich mit einer digitalen Identität eines von der Plattform akzeptierten Identity Providers (IdP) selber im Adressverzeichnis.

Natürliche Personen, die erstmals auf die Plattform Justitia.Swiss zugreifen, registrieren sich selber im Adressverzeichnis. Alle für die initiale Registrierung benötigten Attribute werden aus der *Assertion*[14] des Identity Providers (IdP) übernommen, wobei mindestens die folgenden Attribute benötigt werden:

- Der eindeutige Identifikator des Identity Providers (IdP);
- Der eindeutige Identifikator der natürlichen Person beim Identity Provider (IdP-UID). Dies wäre, bei einer zukünftigen E-ID des Bundes, die E-ID-Kundennummer;
- Die Attribute der zivilen Identität (amtlicher Name, Vornamen, Geburtsdatum, Geschlecht, Geburtsort und Staatsangehörigkeit gemäss einem amtlichem Ausweisdokument).

Ob bzw. welche weiteren Benutzerattribute vom Identity Provider geliefert werden können oder müssen, ist noch nicht definiert. Solche Attribute könnten beispielsweise sein:

- Adressen wie E-Mail-Adresse(n), Postadresse(n), Telefonnummer(n) oder Threema-ID;
- Funktion(en), Organisationszugehörigkeit(en) oder Berechtigungen/Rollen;
- Anwaltszulassung und Zulassungsstatus (nur bei Anwälten relevant);
- Titel, Spezialisierungen, Ausbildungen u.dgl. (vor allem bei Anwälten relevant).

Es ist noch nicht abschliessend festgelegt, welche Attribute von natürlichen Personen im Adressverzeichnis geführt werden. Neben den oben aufgeführten Attributen sind voraussichtlich relevant:

- Das zur natürlichen Person gehörige Profil bzw. dessen Zustelladresse;
- Die Sozialversicherungsnummer (oder AHV-Nummer, AHVN13), sofern erlaubt und vorhanden;

Eine natürliche Person, die über ein aktives Profil auf der Plattform Justitia.Swiss verfügt und sich mit einer digitalen Identität eines von der Plattform akzeptierten Identity Provider anmelden kann, wird im vorliegenden ISDS-Konzept als Benutzer bezeichnet.

Gemäss Anhang 7 der Ausschreibung - Architektur Plattform Justitia.Swiss sollen mit Ausnahme der Organisationszugehörigkeit (vgl. SO8) alle Attribute eines Profils, die nicht von einem Identity Provider bezogen werden, vom Inhaber des Profils im Sinne einer Selbstdeklaration selber erfasst werden. Es

[13] *Hinweis*: Auf elektronischem Weg könnte die Plattform Justitia.Swiss einzig die Korrektheit der elektronischen Kommunikationsadressen verifizieren, indem sie eine einmalige URL oder ein Einmalpasswort an diese Adresse zustellt und der Empfänger den Empfang bestätigt.

[14] Assertion: Eine vom Identity Provider digital signierte Datei mit bestätigten Attributen des Benutzers.

ist aktuell kein Prozess für die Verifikation dieser Attribute vorgesehen, so dass keinerlei Gewähr für ihre Korrektheit besteht[15].

Die administrativen Prozesse für die Verwaltung (eröffnen, mutieren und löschen) von Benutzern und Benutzer-Attributen sind noch nicht definiert.

SO8 Organisationszugehörigkeiten verwalten

Die Administratoren von Organisationen legen fest, welche natürlichen Personen zur Organisation gehören und welche Funktionen sie für die Organisation wahrnehmen.[16]

Die Organisations-Administratoren legen fest, welche natürlichen Personen zur Organisation gehören und welche Funktionen diese Personen für die Organisation wahrnehmen. Falls der Identity Provider eines Benutzers dessen Organisationszugehörigkeit und allenfalls Funktion als Attribut liefert, dann kann diese Information auch automatisch übernommen werden.

Gemäss Anhang 7 der Ausschreibung - Architektur Plattform Justitia.Swiss sind aktuell die folgenden Funktionen[17] vorgesehen:

- Administrator;
- Handelnd;
- Eingaben aufgeben;
- Eingaben empfangen;
- Zustellungen aufgeben;
- Zustellungen (erstmalig) empfangen;
- Akteneinsicht vornehmen.

Ein Administrator kann selber weitere Administratoren einrichten und damit seine eigenen Rechte uneingeschränkt weitergeben (das Recht «Organisations-Administrator» ist transitiv).

Bei der Erfassung von Organisationszugehörigkeiten sind derzeit keinerlei Einschränkungen oder Plausibilisierungen vorgesehen:

- Jede natürliche Person kann gleichzeitig Mitglied beliebig vieler Organisationen sein;
- Jede natürliche Person kann bei jeder Organisation jede Funktion innehaben;
- Zwischen den elektronischen oder postalischen Adressen der Organisation und ihrer Mitglieder werden keine Übereinstimmungen (z.B. E-Mail-Adresse mit gleicher Domäne) verlangt.

Eine natürliche Person mit der Funktion «handelnd» soll die Geschäfte dieser Organisation gemäss Art. 55c ZGB behandeln dürfen, was im Allgemeinen ein Zeichnungsrecht der Organisation, eine Organvertretung oder eine Handlungsbefugnis erfordert. Es ist aber nicht vorgesehen, dass diese Voraussetzungen bei der Vergabe dieser Funktion geprüft werden (z.B. im Handelsregister). Ein Administrator kann somit jede beliebige natürliche Person in der Funktion «handelnd» erfassen, sofern kein anderer Prozess hierfür definiert wird.

---

[15] Hinweis: Auf elektronischem Weg könnte die Plattform Justitia.Swiss einzig die Korrektheit der elektronischen Kommunikationsadressen verifizieren, indem sie eine einmalige URL oder ein Einmalpasswort an diese Adresse zustellt und der Empfänger den Empfang bestätigt.

[16] Hinweis für die nächste Überarbeitung des ISDS Konzepts. Der Prozess 'Organisation verwalten' muss unterteilt werden. Wir sollten unterscheiden zwischen (1) Organisationen für die die Mitglieder auf der Plattform verwaltet, resp. administriert werden und (2) Organisationen, deren Mitglieder durch einen externen IdP verwaltet werden. Im letzten Fall ist der IdP verantwortlich die korrekten Funktionen der Mitglieder zu liefern. Durch eine entsprechende Aufteilung des Prozesses werden die Risiken vor den Massnahmen reduziert (Security by Design).

[17] Für die Ausübung dieser Organisations-bezogenen Funktionen sind spezifische Berechtigungen zur Nutzung von Funktionalitäten und Daten der Plattform Justitia.Swiss erforderlich. Die Gruppierung der Plattform-Berechtigungsobjekte entlang dieser Funktionen wird im Jargon der Informationssicherheit als «Rollenbildung» bezeichnet. Die Zuweisung der Plattform-Berechtigungen mittels der Zuweisung von Organisations-bezogenen Funktionen wird entsprechend als «Rollenbasierte Berechtigungsvergabe» bezeichnet.

SO9 Plattform-Berechtigungen verwalten

Administratoren auf der Plattform Justitia.Swiss legen fest, welche Benutzer welche Funktionalitäten und Daten auf der Plattform Justitia.Swiss nutzen dürfen.

Das Zugriffskontrollsystem der Plattform Justitia.Swiss kontrolliert die Nutzung der einzelnen Funktionalitäten und den Zugriff auf die lokalen Datenbestände der Plattform Justitia.Swiss. Mögliche Beispiele für entsprechende Berechtigungsobjekte sind (Auflistung ist keinesfalls vollständig):

- Das Anbringen des Plattform-Siegels auf eine Eingabe;
- Der lesende und/oder schreibende Zugriff auf den Arbeitsbereich eines Verfahrensbeteiligten;
- Der lesende Zugriff auf das Postfach einer verfahrensleitenden Justizbehörde;
- Das Erfassen, Prüfen und/oder Versenden einer Zustellung;
- Das Annullieren oder Anpassen (z.B. Verlängern) einer bereits versendeten Zustellung;
- Die Einsicht in das Adressverzeichnis oder in Teile davon;
- Die Einsicht in den Audit Trail (eigene Einträge) oder in das Log der Plattform Justitia.Swiss.

Ein vollständiges Inventar aller Berechtigungsobjekte (Funktionalitäten und Datenbestände) der Plattform Justitia.Swiss liegt noch nicht vor und soll im Rahmen des Berechtigungskonzeptes (vgl. MO (1)) erstellt werden.

Die Berechtigungsobjekte der Plattform Justitia.Swiss können nach den unter SO8 beschriebenen «Funktionen der Organisationszugehörigkeit» gruppiert werden. Die Zuweisung der Berechtigungsobjekte erfolgt dann indirekt, indem einem Benutzer eine Funktion in Bezug auf eine (oder mehrere) Organisationen zugewiesen wird. Diese Art der Berechtigungsverwaltung wird im Jargon der Informationssicherheit als Rollenbasierte Berechtigungsverwaltung bezeichnet. Ein vollständiges Inventar aller Rollen mit ihren Berechtigungsobjekten liegt noch nicht vor.

Bei Teilnehmern mit mehreren Rollen bei mehreren Organisationen kumulieren sich alle entsprechenden Berechtigungsobjekte.

Für Benutzer, die zu keiner Organisation gehören (z.B. eine verfahrensbeteiligte Privatperson), muss die Berechtigungszuteilung anders geregelt werden (entweder pauschal abhängig von einem noch zu definierenden Attribut «Benutzertyp» oder durch einen noch zu definierenden Administrator). Solche Regelungen liegen derzeit noch nicht vor.

SO10 Delegationen verwalten

Teilnehmer delegieren eine ihrer Berechtigungen an einen anderen Teilnehmer.

Jede Person (natürliche Person oder Organisation), die auf der Plattform Justitia.Swiss ein Profil mit einer Zustelladresse besitzt, kann eine Berechtigung dieses Profils an ein beliebiges anderes Profil delegieren. Wenn es sich beim delegierenden Teilnehmer um eine Organisation handelt, dann kann jeder Administrator dieser Organisation beliebige Delegationen einrichten.

Die Details der Delegation sind noch nicht festgelegt. Es sollen aber voraussichtlich alle Arten von Berechtigungen delegiert werden können, als da sind:

- Die Delegation von Berechtigungen zur Einsicht in eine oder mehrere Akten, die das delegierende Profil mittels einer Zustellung erhalten hat (vgl. SO2);
- Die Delegation von Berechtigungen zur Nutzung von Funktionalitäten und Daten der Plattform Justitia.Swiss, die dem delegierenden Profil entweder über eine Organisationszugehörigkeit (Rolle) oder direkt zugewiesen worden sind (vgl. SO9).

Anhand D: Detaillierte Betriebsprozesse

SO11 Service Management

Verschiedene Services im laufenden Betrieb werden durch Mitarbeitende der öffentlich-rechtlichen Körperschaft (örK) erbracht.

Es ist noch nicht definiert, welche administrativen Tätigkeiten vom Personal der öffentlich-rechtlichen Körperschaft (örK) auf der Plattform Justitia.Swiss ausgeführt werden und welche Berechtigungen sie hierfür benötigen. Solche Tätigkeiten der örK könnten beispielsweise sein:

- Die Verwaltung von Organisationen im Adressverzeichnis;
- Die Qualitätssicherung von Konfigurationsdaten und/oder Daten im Adressverzeichnis;
- Das Reporting gegenüber angeschlossenen Justizbehörden;
- Das Reporting gegenüber Aufsichtsbehörden und/oder Auditstellen.

SO12 Support der Plattformbenutzer (Service Desk)

Die Verantwortung für das Service Desk liegt beim Plattformbetreiber und wird in enger Zusammenarbeit mit Justitia.Swiss erbracht. Insbesondere umfasst dies die ITIL Praktiken Knowledge Management, Event und Incident Management, Request Fulfillment, Problem Management und Access Management. Weitere Praktiken werden in Zusammenarbeit mit den Partnern bei Bedarf ausgearbeitet.

SO13 Betrieb des Security Operations Center (SOC)

Für die Erkennung von und den Umgang mit Sicherheitsvorfällen wird ein Security Operations Center (SOC) etabliert, das insbesondere sicherstellt:

- Die laufende Überwachung und Lagebeurteilung;
- Die allfällige Sperrung von zugreifenden Systemen (z.B. IP-Adressen);
- Die rechtzeitige Auslösung von Notfallmassnahmen, wenn erforderlich.

Die Mitarbeitenden des SOC beziehungsweise deren Werkzeuge für die laufende Überwachung und Lagebeurteilung benötigen Zugriff auf das Log und den Audit Trail der Plattform Justitia.Swiss.

Vorerst wird das SOC vom Plattformbetreiber bereitgestellt.

SO14 Entwicklung und Weiterentwicklung der Plattform

Die Software der Plattform Justitia.Swiss wird vom Softwarelieferanten entwickelt und weiterentwickelt. Entwicklungswerkzeuge, Server und Programmierumgebungen werden durch den Plattformbetreiber zur Verfügung gestellt, wobei die Anforderungen an die «Toolchain» noch zu spezifizieren sind.

Es ist davon auszugehen, dass der Softwareentwickler Konzepte von DevOps und Agile anwendet: Continuous Integration, Continuous Delivery, Continuous Deployment, Release on Demand. Die Mitarbeitenden des Softwarelieferanten werden somit einen direkten Zugriff auf die produktiven Systeme der Plattform Justitia.Swiss benötigen.

SO15 Betrieb der Plattform Justitia.Swiss mit ihren Schnittstellen

Der Betrieb der Plattform Justitia.Swiss mit ihren Schnittstellen wird durch den Plattformbetreiber sichergestellt. Es ist noch nicht definiert, welche Berechtigungen auf der Plattform Justitia.Swiss das administrative Personal des Plattformbetreibers benötigen wird.

Mögliche solche Berechtigungen könnten sein:

Einsichts- und Schreibrechte auf die Konfigurationsdaten.

Anhang E: Kapitel 2.4.4 aus E29 Varianten Plattform «Justitia.Swiss»

Für Justitia 4.0 ist unbestritten, dass die Kanäle zwischen den teilnehmenden Parteien verschlüsselt sein müssen, dass also die Daten in ‚angemessen geschützten Transportbehältern' über das unsichere Internet gehen müssen. Aufgrund der Komplexität des Schlüsselmanagements und der Nichtvereinbarkeit des strengen end-2-end Begriffs mit den Konzepten der Delegation empfehlen wir, Transportverschlüsselung und Verschlüsselung von gespeicherten Daten(Data at rest) zu verwenden.

Dies bedingt entsprechendes Vertrauen in den Betreiber der Plattform, dass er die Sicherheitsanforderungen umsetzen und regelmässig überprüfen (auditieren) kann, wie das auch im Entwurf des BEK gefordert ist.

Für speziell heikle Fälle könnte in Zukunft eine end-2-end Verschlüsselung wie folgt hinzugefügt werden:

- *Verfahrensleitung und teilnehmende Parteien und Organisationen tauschen ihre Schlüsselpaare aus und definieren einen Prozess zur Erneuerung der Schlüssel, falls ein Teilnehmer einen Diebstahl seines privaten Schlüssels entdeckt oder vermutet. Das Schlüsselmanagement müsste mit dem Teilnehmerverzeichnis der Plattform interagieren, falls Konzepte der Delegation (Stellvertreter) nötig sind.*
- *Anstelle von PDF-Dokumentenfügt die verfahrensführende Organisation für jede berechtigte Partei ein für sie verschlüsseltes Dokument zu den Akten.*
- *Damit wird allerdings die Berechtigungssteuerung stark eingeschränkt, da jeder Empfänger von Aktenstücken nur die explizit für ihn bestimmten Aktenstücke entschlüsseln kann (keine Delegation auf der Plattform möglich).*