PROJEKT Justitia 4.0

Justitia 4.0

Für eine sichere digitale Justiz – damit der Weg zum Recht nicht mehr über Papierberge führt

IT-Anforderungen: Was müssen Justizbehörden bezüglich Informationssicherheit und IT-Architektur beachten?

Franz Achermann, Jérôme Barraud

01.12.2023

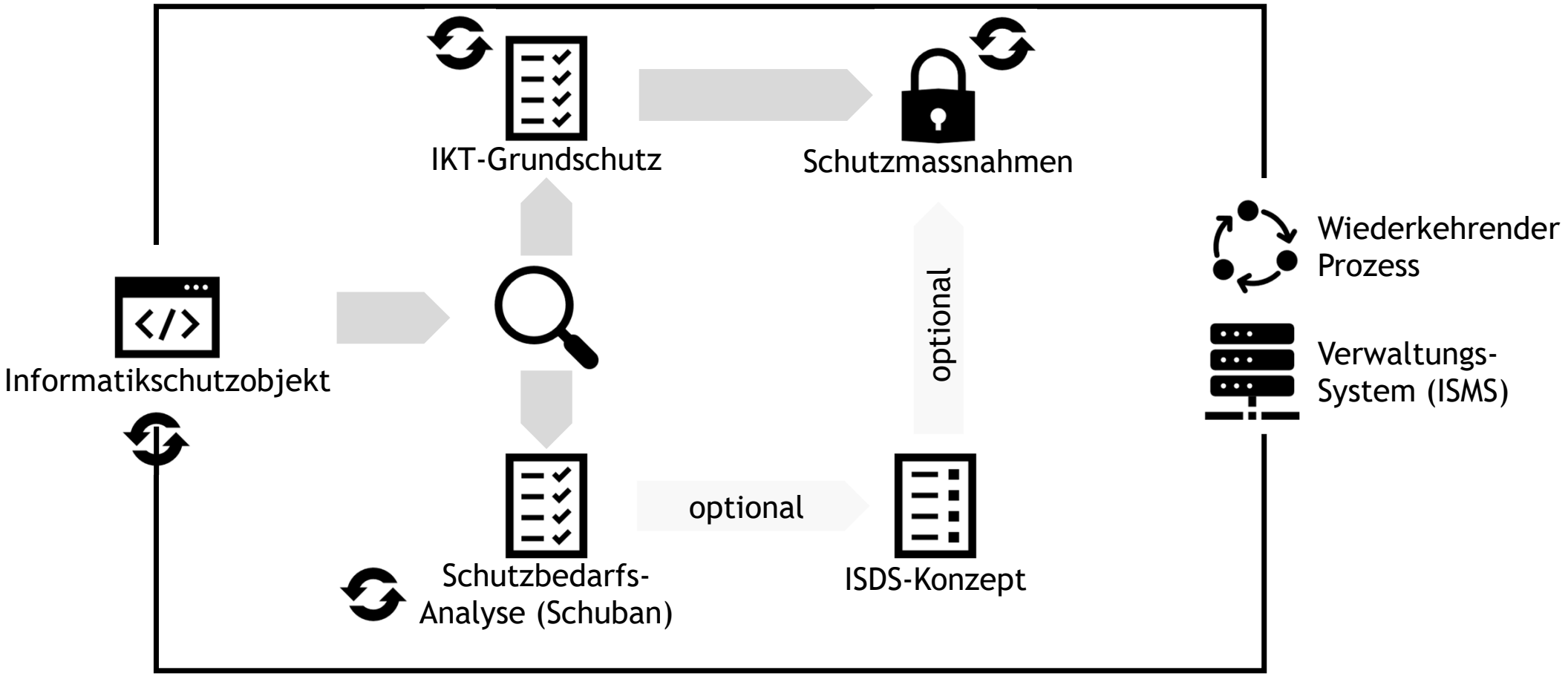
Ziele: Was wollen wir heute in 45 Minuten erreichen

- Informationssicherheit
  - Schutzmassnahmen: Vorgehensweise
  - Generische Risiken
  - Eigenleistungen

- IT-Architektur
  - Wie passen die Systeme JAA und Plattform in ihre IT-Landschaft
  - Integrationsoptionen
  - Migrationsstrategien

Informationssicherheit > Schutzmassnahmen > Vorgehensweise 1/2

- Folgende Vorgehensweise ist anwendbar für alle Informatikschutzobjekte:



Informationssicherheit > Schutzmassnahmen > Vorgehensweise 2/2

- Vorgehensweise für eine Justiz-Fachanwendung bei einer Justizbehörde:

 Informatikschutzobjekt	z.B. Fachapplikation
 IKT-Grundschutz	64 Kontrollen zum ausfüllen (organisatorisch & technisch)
 Schuban	9 Kontrollen zum Eruieren des Schutzbedarfes
 Risikoanalyse	Identifizieren und Bewerten von Risiken vor und nach Einführung von Schutzmassnahmen
 ISDS-Konzept	Bei erhöhtem Schutz: Angabe von Schutzmassnahmen und verbleibenden Risiken (*residual risk*)
 Schutzmassnahmen	Definieren und Umsetzen von Schutzmassnahmen
 Verwaltung	(Kantonales) ISMS-System (bsp. «GRC Toolbox»)

Informationssicherheit > Generische Risiken

- Eine Risikoanalyse ist spezifisch für jedes Informatikschutzobjekt zu erstellen. Das NCSC / HERMES gibt im Dokument P042-Hi02 einige generische Risiken an:

R1	Verletzung der **Integrität** z.B. durch Manipulation oder Fehler im System
R2	Verletzung der **Vertraulichkeit** z.B. durch Schwachstellen im System, […]
R3	Verletzung der **Verfügbarkeit** z.B. durch Ausfall der Systeme, […] oder Ransomware
R4	Verletzung der **Nachvollziehbarkeit** z.B. durch Fälschung oder Verlust der Protokolle
R5	Unrechtmässige Beschaffung und Bearbeitung von **Personendaten**
R6	Verwendung von **Personendaten** zu nicht vorgesehenen Zwecken
R7	Bearbeitung von **inkorrekten Daten**
R8	Unbefugter Zugriff auf **Personendaten**
R9	Übermässig lange Aufbewahrung von **Personendaten**
R10	Verweigerung der **Rechte** der betroffenen Personen

Informationssicherheit > Eigenleistungen 1/2

Identitäten

- Verfahrensleitung: Mitarbeitende von Behörden
  - Anbindung des Mitarbeiters-IAM (z.B. Active Directory) via OIDC oder SAML
  - Alternativen
    - Verwendung des EJPD-SSO Portals (Smartcard)
    - AGOV (Lösung im Aufbau durch Digitale Verwaltung Schweiz)
- Verfahrensbeteiligte: Anwaltschaft und Private
  - Anbindung über SwissID oder TrustID

Administration der Berechtigungen

- Jetzt: Administration der Mitarbeiter über Web-Oberfläche durch einen Administrator
- Später: Synchronisation der Rollen / Organsiationszugehörigkeiten mit Identity & Access Management (IAM) Lösungen

Informationssicherheit > Eigenleistungen 2/2

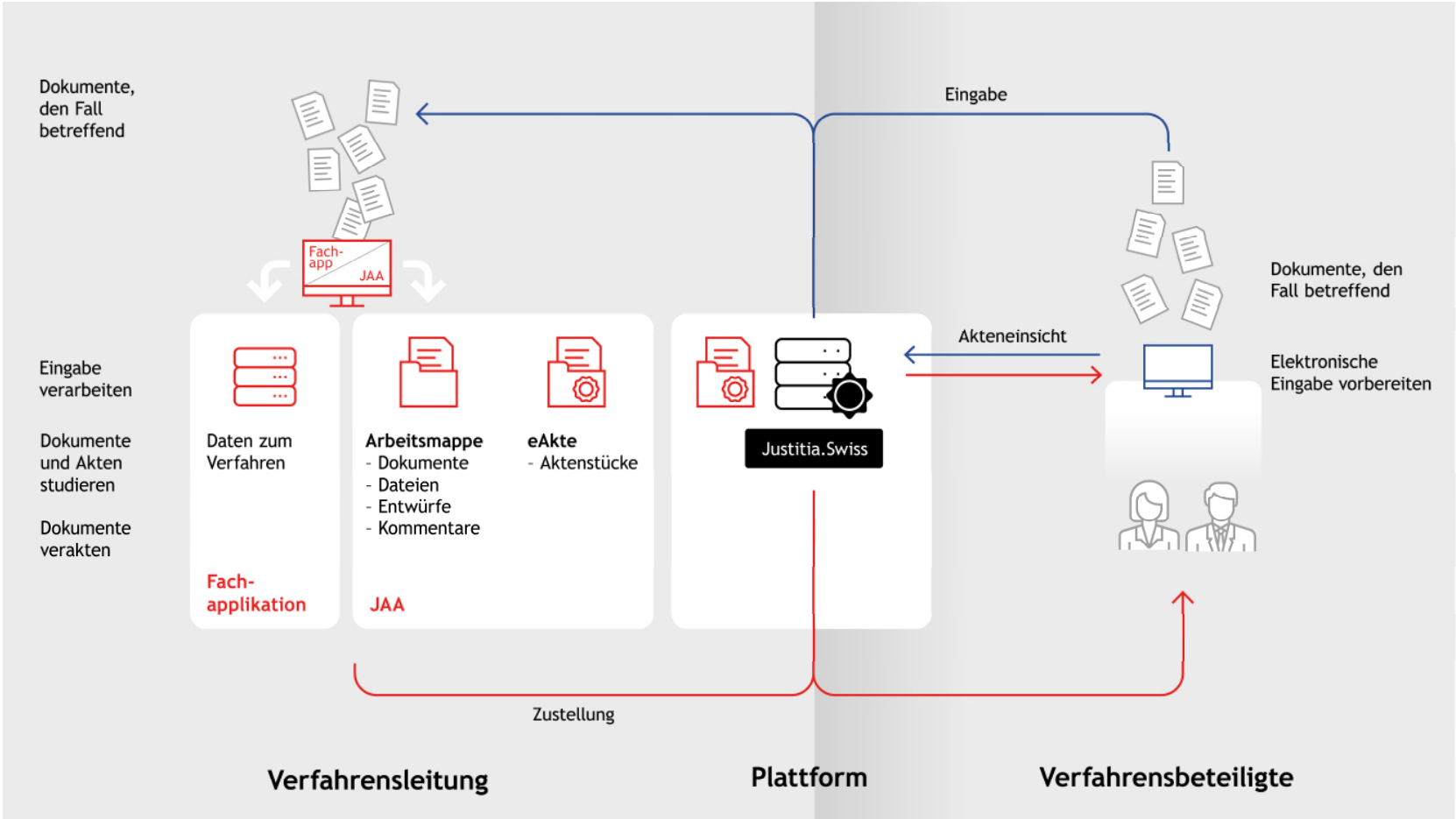
Signaturdienstleistungen

- Pilot VeÜ-ZSSV:
  - Dokumente müssen durch den Sender qualifiziert elektronisch signiert werden
  - Der jeweilige Empfänger validiert die Signaturen

- Betrieb BEKJ:
  - Plattform siegelt die Sendung bei einer Eingabe, Justizbehörde sendet gesiegelte Dokumente
  - Die Plattform prüft, ob ein Behördensiegel vorhanden ist.

→ Per Inkrafttreten BEKJ müssen die Justizbehörden auf ihren Dokumenten ein Behördensiegel anbringen können.

Die Fachapplikation, die JAA und die Plattform sind die Basis für die Digitalisierung



Die Plattform kann flexibel integriert werden

Integrationsoption	1	2	3
Techn. Anbindung	Via Web	Via API	Hybrid (z.B. Aktenhochladen via API, Zustellung manuell)
Identitäten Mitarbeiter	Eigenes IAM	IAM des Bundes (ISC-EJPD)	
Datenhaltung	Zentrale Datenhaltung per MVP	Dezentrale Daten (später)	
Welche Geschäftsfälle	Alles	Einzelne Geschäftsfälle schrittweise…	Strukturierte Daten
Welche Behörden	Bestimmt die Anzahl Behörden-profile		
Zeitpunkt der Implementierung	Pilotierung nach VeÜ-ZSSV	Erst mit BEKJ	
Plattform	Via Justitia.Swiss	Eigene Plattform	

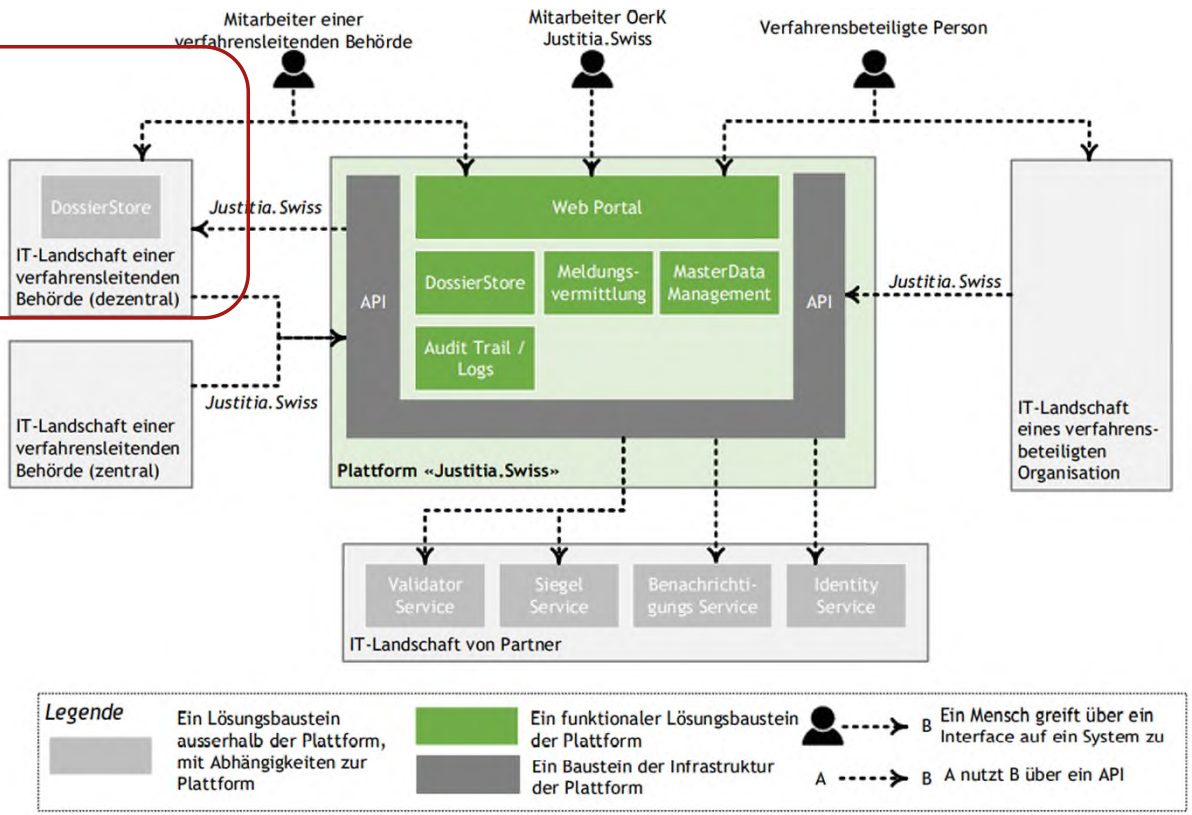
Web oder API

- **Web Anbindung**
  - Benötigt keine IT Anpassung
  - Dateien (Aktenstücke) via Drag & Drop
  - Keine Metadaten für Dateien, also Darstellung der Akte als Liste von Dateien
  - Zustelladressen der Empfänger werden via Copy & Paste übertragen
- **API Anbindung**
  - Benötigt kompatibles System (angepasste der Fachapplikation resp. JAA)
  - Erlaubt automatisierte Verarbeitung

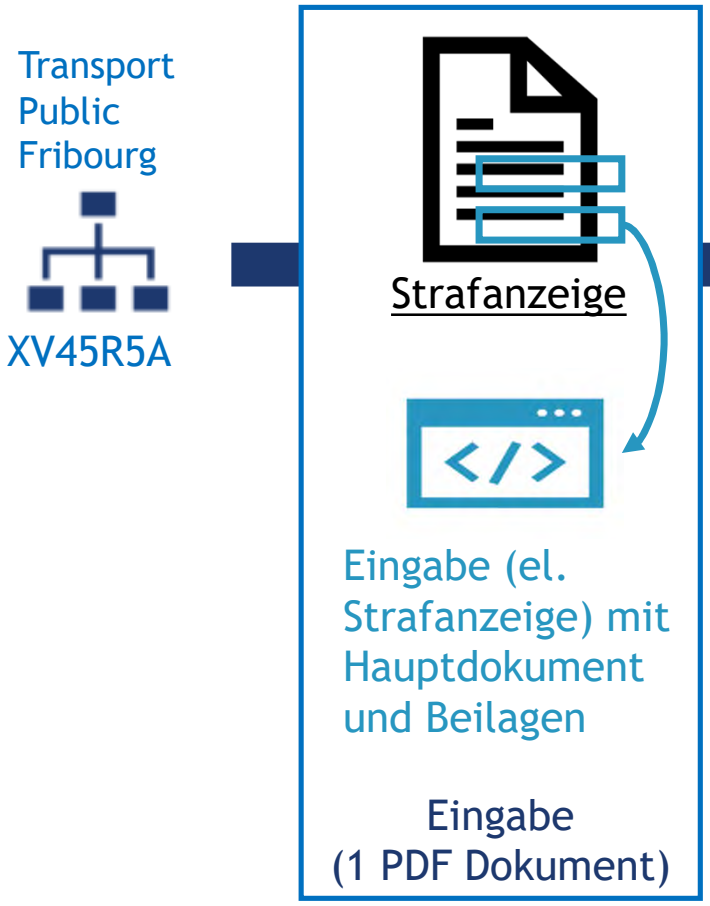
Datenhaltung

- Vorgesehen für Ausbau:
  Aktenstücke verbleiben dezentral
  (z.b. für FMÜ Überwachungen).

- Realisiert: Aktenstücke zentral
  vorhalten



Geschäftsfälle mit strukturierten Daten: Der Sicap Pilot in Fribourg



- Heute: Übermittlung einer Strafanzeige (enthält ein Dokument und Beilagen, z.B. Foto von Ausweis). Muss beim Empfänger erneut erfasst werden.
- Mit Justitia.Swiss kann diese Eingabe elektronisch übermittelt werden: Eingabe vom Profil der TPF zum Profil der Justizbehörde FRSTA
- Mit Sicap kann die Eingabe automatisiert weiterverarbeitet werden:
  - Die Eingabe enthält strukturierte Daten der Strafanzeige.
  - Die Struktur wird nicht von der Plattform geprüft. Die Plattform macht keine Bearbeitung der übermittelten Daten.
  - Projekt Sicap: Definiert die benötigen Datenfelder für die eStrafanzeigen (eCH-0051 überarbeitet)
  - Projekt Plattform: Definiert einen MessageTyp für genau diesen Geschäftsfall (damit Empfänger weiss wie verarbeiten)
- Ausblick: Weitere Geschäftsfälle, Umgang mit legacy Formaten, Versionen und Formatkonversion.

Unterschiede der drei Pilotphasen

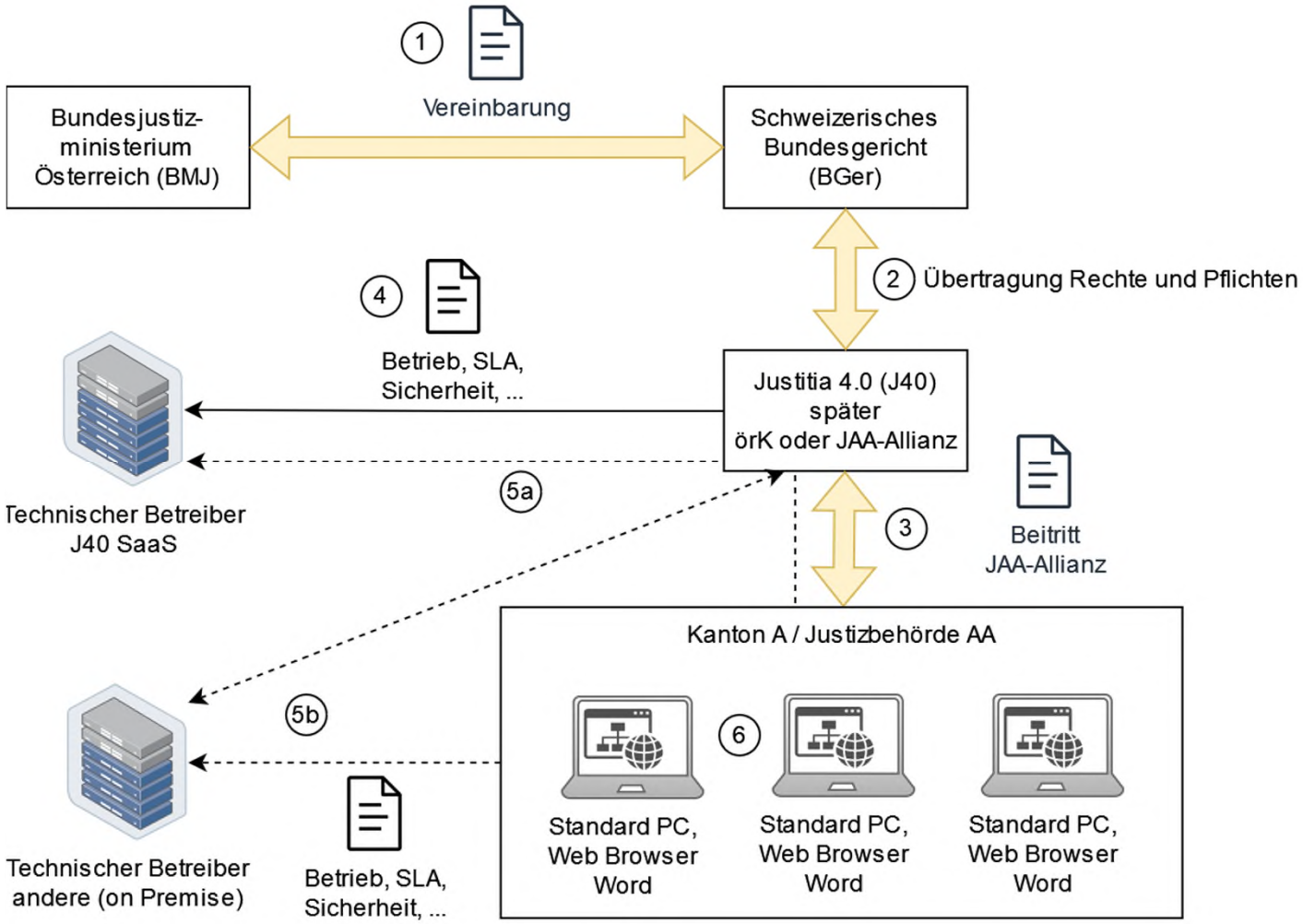
Pilot MVP unter VeÜ-ZSSV	Pilot Weiterentwicklung unter VeÜ-ZSSV	Pilot unter BEKJ
Dokumente müssen qualifiziert elektronisch signiert werden	Dokumente müssen qualifiziert elektronisch signiert werden	Plattform siegelt die Sendung bei einer Eingabe, Justizbehörde sendet gesiegelte Dokumente
StPO & ZPO	StPO & ZPO	Alle Verfahrenstypen
Bewilligung einzeln pro Kanton für Pilotbetrieb	Bewilligung einzeln pro Kanton für Pilotbetrieb	Genehmigung der Plattform
Keine Grundlage für Bundesbehörden	Keine Grundlage für Bundesbehörden	Inklusive Bundesbehörden
Massgebende Akten auf Papier	Massgebende Akten auf Papier	Massgebende Akten können digital sein
Primär Weblösung	API-Lösung	API-Lösung

Die JAA: Der Weg zur sicheren digitalisierung der Jusitzakte

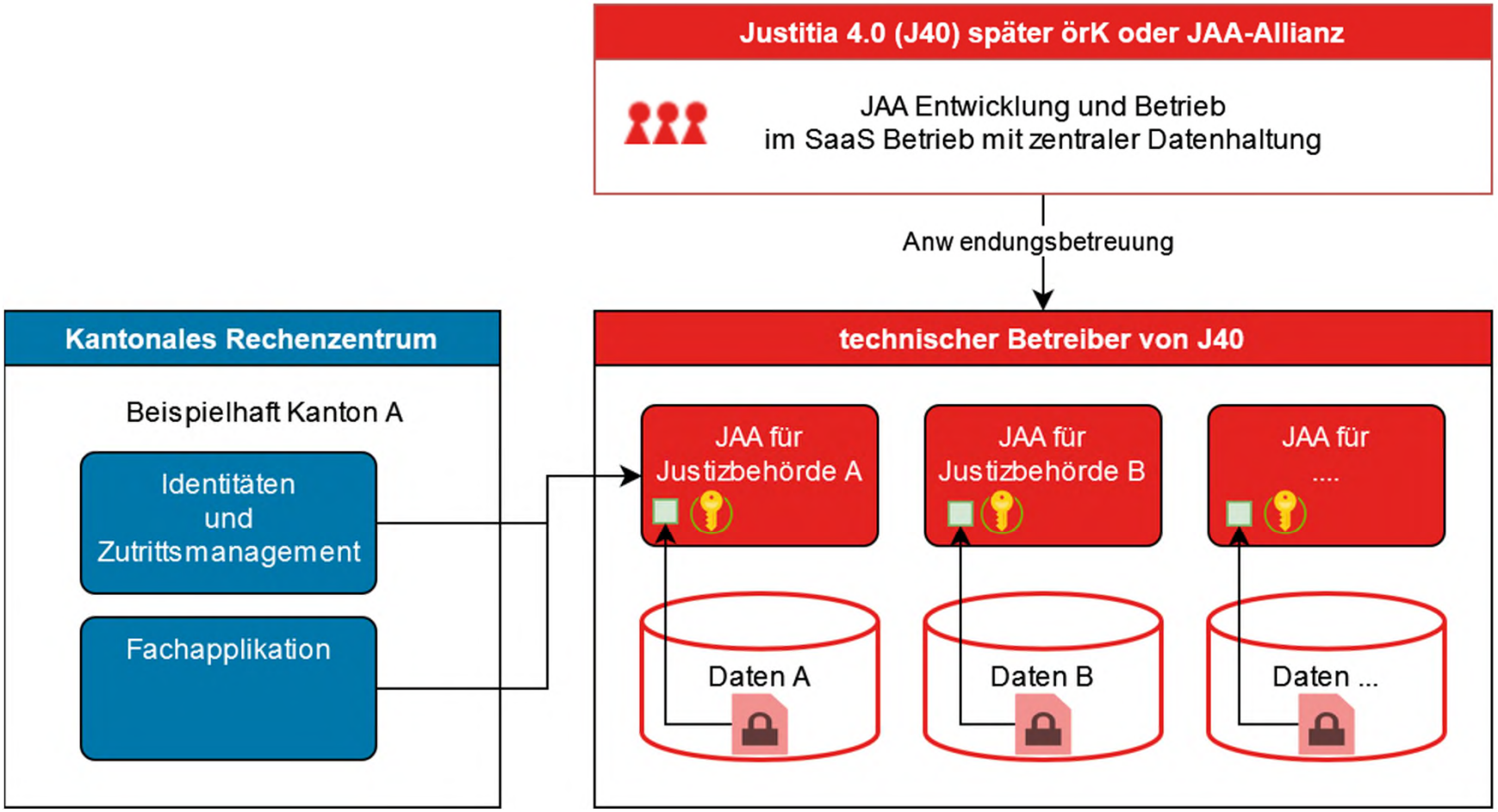
	Option 1	2	3
Betriebsvarianten	As a Service von J40	As a Service eines Partners	On Premise
Anbindung Scanning			
Arbeitsplätze			
Verhandlungssäle			
Roadmap IT-Projekte	Plattform dann Fachapplikation dann JAA	Plattform dann JAA und Fachapplikation	Alles zusammen

Justitia 4.0 stellt sicher:
- Zusammenspiel JAA mit der Plattform
- Die Fachapplikationshersteller kennen die Integration mit JAA und der Plattform

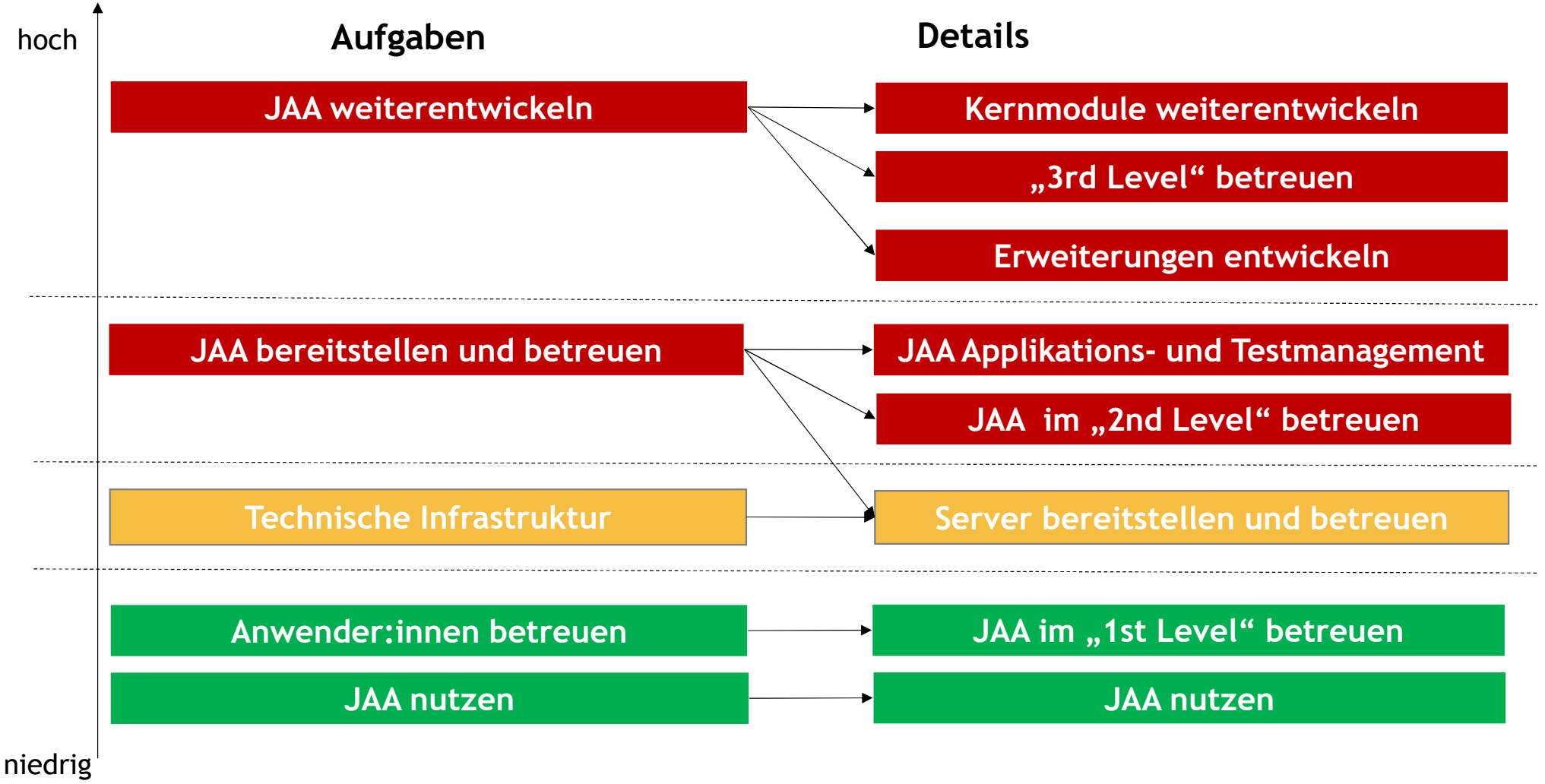
Was bietet Justitia 4.0 den Kantonen an



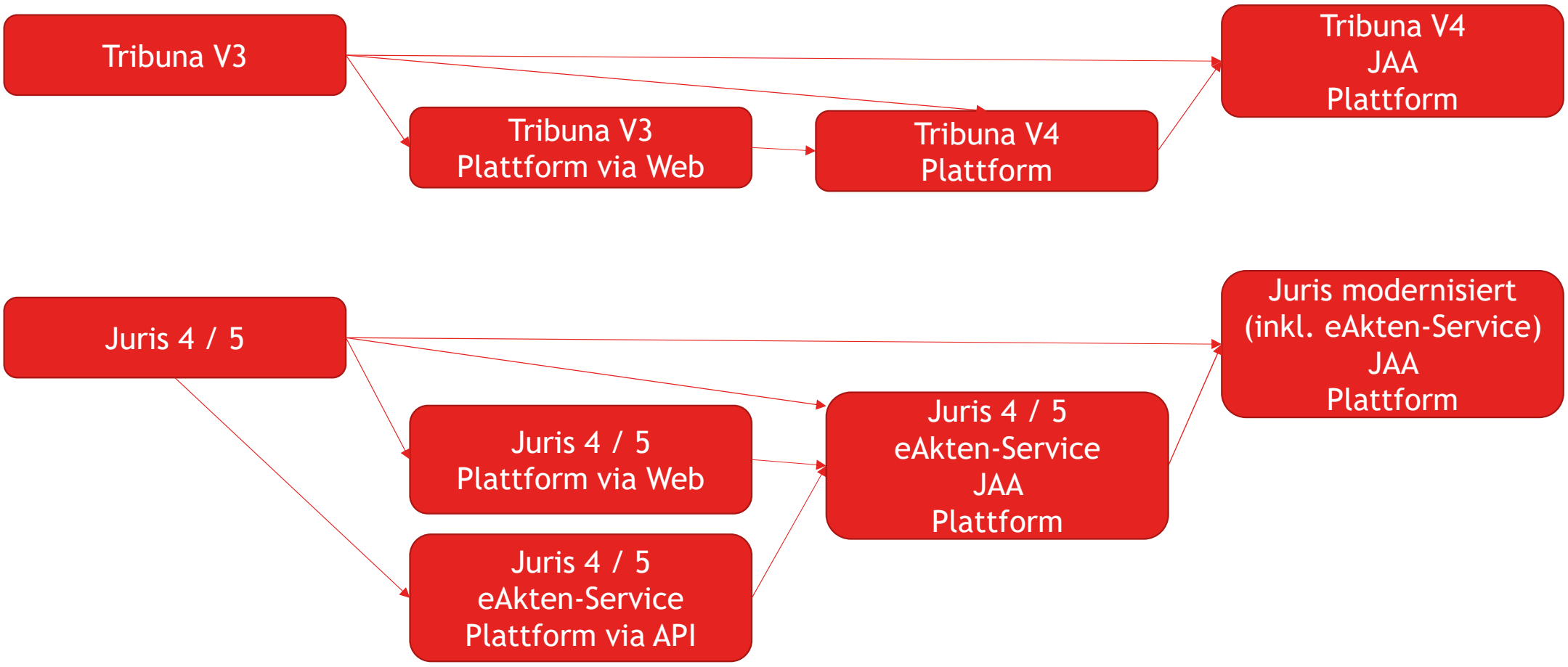
Sicheren und effizienter technischen Betrieb durch Justitia 4.0



Betriebsszenario: Erforderliches JAA-Wissen zur Aufgabenerfüllung



In welcher Reihenfolge können wir vorgehen



Vielen Dank für ihre aktive Mithilfe !