PROJEKT
Justitia 4.0

Périmètre du pilote de la plateforme Justitia.Swiss

Nom du fichier :	J40_Übersicht_MVP_Plattform
Phase du projet :	Design
Date de création :	23 février 2023
Auteur :	J. Barraud, F. Achermann
Réviseur :	A. Bar, le 14.02.2024

Contenu

1 Introduction

Dans le cadre du projet Justitia 4.0, nous poursuivons l'objectif général de faire progresser la numérisation dans la justice suisse. La motivation principale derrière ce projet est d'affranchir la justice des processus basés sur le papier et d'établir à la place des solutions numériques efficaces.

L'objectif du pilote est de tester l'exploitation en pratique et de manière juridiquement valable de la plateforme « Justitia.Swiss » (ci-après : plateforme) en tant que contribution à la numérisation de la justice.

Les enseignements tirés de l'exploitation pilote sont intégrés dans le développement de la plateforme ainsi que dans la planification du déploiement et de la transition numérique à l'échelle nationale.

Au deuxième trimestre 2024, le *minimal viable product* (MVP) de la plateforme doit être réalisé et exploité dans un mode pilote. Explication :

- logiciel du MVP : ce logiciel a été testé et répond aux exigences formulées à son égard. Le chapitre 2 décrit le fonctionnement du logiciel.
- l'exploitation pilote : le chapitre 3 décrit les disciplines opérationnelles nécessaires à l'exploitation et au développement du MVP.

1.1 Bases légales

Le cadre juridique, qui définit notamment la base de l'exploitation pilote et l'introduction de l'exploitation (pilote), a un impact non négligeable sur l'exploitation pilote.

L'exploitation pilote se déroule dans un premier temps dans le cadre strict de l'article 13a de l'ordonnance du 18 juin 2010 sur la communication électronique dans le cadre de procédures civiles et pénales et de procédures en matière de poursuite pour dettes et de faillite (OCEI-PCPP, RS 210.1) Cela signifie que les dispositions légales contenues dans les lois de procédure, en premier lieu le CPC (RS 272) et le CPP (RS 312), ne sont pas modifiées. En particulier, l'exigence d'une signature électronique qualifiée au lieu d'une signature manuscrite est maintenue. Cette exigence s'applique aussi bien aux communications des parties (par ex. art. 130 al. 2 CPC ou art. 110 al. 2 CPP) qu'aux notifications (par ex. art. 139 CPC ou art. 86 CPP) émanant d'une autorité judiciaire. Ainsi, si l'ordonnance permet l'utilisation de la plateforme en lieu et place des plateformes de messagerie sécurisée actuellement reconnues (PrivaSphere et IncaMail), les exigences formelles liées à ce mode de transmission sont contraignantes pour l'exploitation (pilote) - au moins jusqu'à l'entrée en vigueur de la LPCJ.

En outre, l'Ordonnance exige notamment que le canton dépose formellement une demande auprès du DFJP (art. 13a al. 1 OCEI-PCPP) et que le champ d'application de la plateforme soit clairement défini (art. 13a al. 3 OCEI-PCPP). La documentation technique qui doit être soumise pour approbation sera fournie par le projet.

2 Description du logiciel

Le logiciel ou la plateforme « Justitia.Swiss » permet trois transactions de base : communication, notification et consultation du dossier. Ces transactions se font techniquement par la transmission d'envois composés de documents ou de fichiers individuels. Les fichiers sont chiffrés afin de garantir leur sécurité et les envois sont munis d'un cachet électronique afin de protéger leur intégrité.

Pour chaque transmission d'un envoi, il y a des quittances : la quittance de réception, la quittance de consultation et la quittance de non-consultation. Ces trois quittances servent de preuve juridiquement valable de l'envoi.

2.1 Communications

Une communication se compose de deux sous-processus : La partie émettrice crée la communication (Create Submission) et cette communication est quittancée et traitée par l'autorité judiciaire (Receive Submission) :

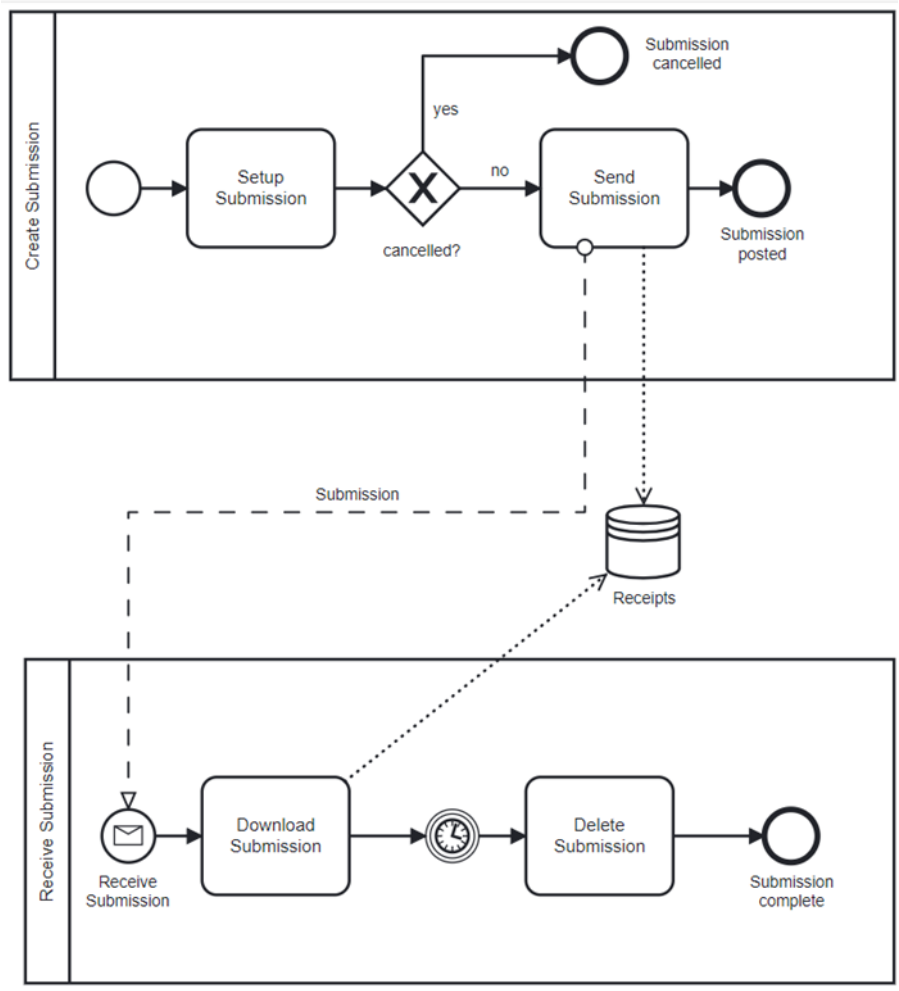


Figure 1 : communication

Créer une communication (« Setup Submission ») **:** par création, on entend le téléchargement de fichiers pour la mise en place d'une communication à l'état de « projet ». Des fichiers ou des documents peuvent être ajoutés ou supprimés à volonté - mais pas modifiés. Une communication en statut « brouillon » peut être supprimée à tout moment.

La **transmission de la communication** au destinataire - l'autorité judiciaire compétente - (« Send Submission ») marque la fin de la communication. A partir de ce moment, la communication ne peut plus être modifiée. La communication est transmise à l'autorité judiciaire et un accusé de réception est établi simultanément.

Recevoir la communication : la consultation de la communication transmise permet à l'autorité judiciaire de télécharger (« Download Submission ») et de traiter les documents introduits. Lors de la première consultation, une quittance de consultation est automatiquement créée.

Au plus tôt nonante jours après la première consultation, la communication et les quittances correspondants sont automatiquement supprimés (« Delete Submission »).

2.2 Notification et consultation du dossier

Le processus suivant illustre l'interaction entre la mise à disposition de dossiers et le transfert de ces dossiers dans le cadre de la notification ou de la consultation du dossier :

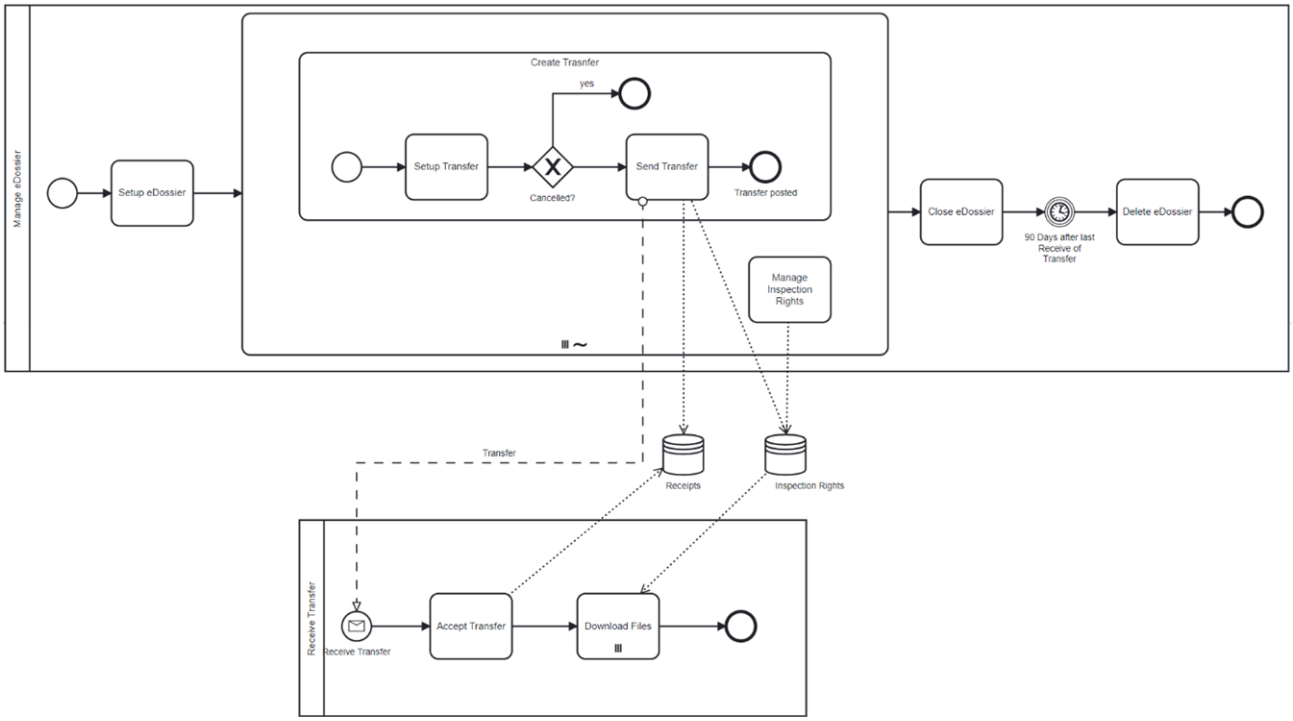


Illustration 2 : Transfert d'un dossier électronique

2.2.1 Gérer un dossier

Avec le processus « Manage eDossier », les autorités judiciaires mettent à disposition, pendant une procédure, une copie consultable du dossier sur la plateforme. Pour ce faire, les principales données de base (numéro de dossier, objet, etc.) sont initialement communiquées (« Setup eDossier »). En cas de modification de ces données, celles-ci peuvent être actualisées ultérieurement.

Pendant les procédures, ces activités peuvent être effectuées plusieurs fois sur la plateforme :

- déclencher le transfert d'un dossier (« Make Transfer ») et
- gérer les droits de consultation (« Manage Inspection Rights »)

A la clôture ou à la suspension de la procédure, les copies consultables des dossiers mises à disposition sur la plateforme sont à nouveau marquées pour suppression (« Close eDossier ») et automatiquement supprimées au plus tard nonante jours après le dernier transfert de dossier (« Delete eDossier »").

2.2.2 Déclencher le transfert du dossier (notification et consultation du dossier)

Pour mettre en place un transfert du dossier, les documents (ou fichiers) relatifs aux procédures peuvent être téléchargés sur la plateforme (« Setup Transfer »). Cela se fait via l'interface web de FileShare ou directement depuis l'environnement informatique existant via l'API.

Le transfert de dossier consiste techniquement à accorder des droits de consultation de documents (ou de fichiers) du dossier au profil d'une personne impliquée dans la procédure. Un transfert peut être utilisé pour la notification ou l'octroi d'une consultation du dossier.

Après vérification du transfert du dossier préparé, celui-ci est transmis (« Send Transfer ») et une quittance de réception est automatiquement établie.

2.2.3 Recevoir un transfert de dossier

Avant que les documents (resp. les fichiers) puissent être lus par le profil destinataire, la réception du transfert de dossier doit être explicitement acceptée (« Accept Transfer »). La quittance de consultation est alors établie et le profil destinataire peut télécharger les documents ou fichiers pour lesquels il a été autorisé (« Download Files »).

Si aucun retrait n'est effectué dans un délai de sept jours, la plateforme génère automatiquement une quittance de non-consultation (fiction de notification).

2.2.4 Gestion des droits de consultation

Les collaboratrices et collaborateurs d'une autorité judiciaire peuvent vérifier à tout moment les droits de consultation accordés sur les pièces du dossier (« Manage Inspection Rights »). Les droits de consultation peuvent être retirés, limités dans le temps (p. ex. pour le changement d'avocat) ou prolongés.

Normalement, la modification des droits de consultation s'accompagne d'une information rapide (p. ex. lettre concernant la prolongation) aux personnes concernées. La plateforme n'indique toutefois pas de procédure à suivre, la transmission de cette information se fait par un transfert de dossier propre.

2.3 Données de base et administration

La plateforme propose différents profils pour différents groupes d'utilisateurs, dont des organisations, des autorités judiciaires et des personnes individuelles. L'authentification des utilisateurs est assurée par des fournisseurs IDP externes (p. ex. TrustID et SwissID), qui contribuent à la sécurité et à la fiabilité de l'accès.

2.3.1 Profil individuel

Un profil individuel permet à une seule personne physique de participer à la communication dans le domaine judiciaire et à l'accès aux dossiers :

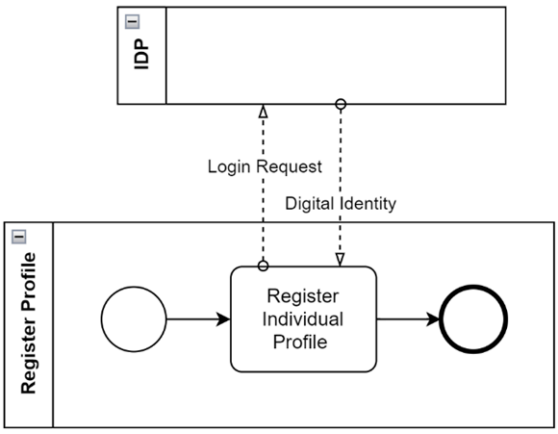


Figure 3 : profil individuel

Avant de pouvoir créer le profil, une identité numérique doit être enregistrée auprès d'un IDP externe intégré.

Enregistrer un profil individuel : un particulier peut saisir un profil à son nom (qui est enregistré auprès du fournisseur IDP externe).

2.3.2 Profil du groupe

Avec un profil de groupe, une personne peut donner accès à son profil à d'autres membres. Les conditions préalables sont les mêmes que pour le profil individuel :

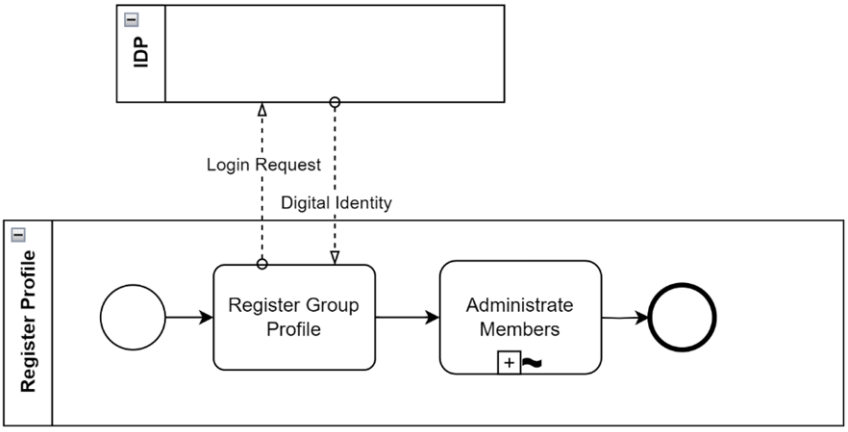


Figure 4 : profil de groupe

Il est possible d'inviter d'autres membres (« Administrer les membres »). Pour ces membres, il est possible de définir s'ils participent uniquement à la communication dans le domaine judiciaire et à la consultation des dossiers, ou s'ils peuvent également gérer eux-mêmes le profil.

2.3.3 Profils pour les autorités judiciaires

Les profils pour les autorités judiciaires sont créés à partir de profils de groupe par une étape administrée :

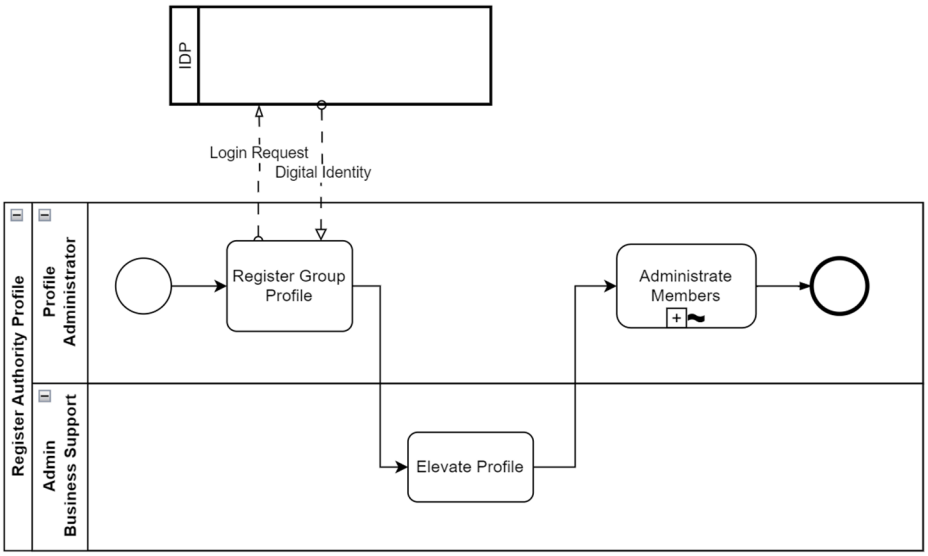


Figure 5 : profil pour les autorités judiciaires

L'enregistrement et la gestion d'un profil administré sont effectués - comme pour le profil de groupe - par l'administrateur du profil.

Dans une étape administrative, le respect des conditions pour la transformation du profil est vérifié et la transformation est effectuée par le support Justitia.Swiss (« Elevate Profile »). Des communications peuvent être envoyées sur le profil d'une autorité judiciaire, l'adresse d'envoi de l'autorité est visible pour tous.

L'administrateur de profil peut donner accès au profil à d'autres collaboratrices et collaborateurs des autorités judiciaires (p. ex. collaborateur ou collaboratrice du greffe).

2.4 Accès web et API

L'accès à la plateforme peut se faire au choix via le portail web ou via une application métier intégrée qui communique directement avec la plateforme via une API résiduelle.

La documentation de l'API résiduelle est mise à disposition par le projet à tous les fabricants de logiciels intéressés. Il existe déjà des premières intégrations de logiciels d'avocats avec la plateforme.

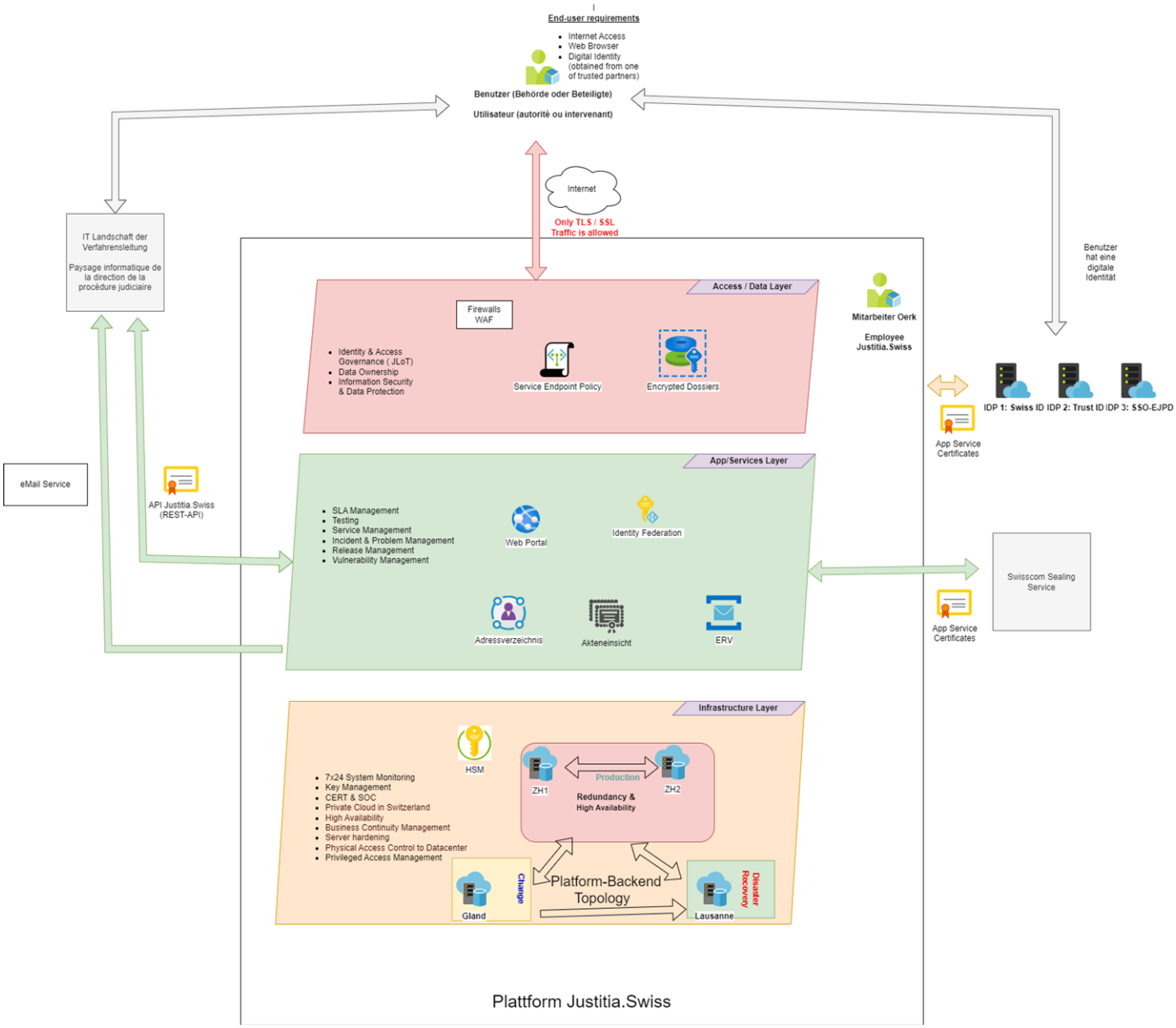
Un aspect important est l'accessibilité de la plateforme « Justitia.Swiss » conformément aux directives WCAG 2.1, afin de garantir une utilisation accessible pour toutes et tous.

2.5 Types de données pris en charge pour le MVP

La plateforme permet de transmettre des fichiers dans les formats les plus courants, les formats primaires sont PDF, images et Office.

La taille maximale d'un fichier est limitée à 100 Mo. Il convient de noter qu'en raison de connexions Internet très lentes, le téléchargement ou le chargement de fichiers très volumineux peut être interrompu.

3 Aperçu de l'architecture



Les transactions de base de la plateorme « Jusitita.Swiss » sont : (1) répertoire d'adresses des personnes impliquées dans la procédure, (2) garantir la consultation des dossiers, et (3) permettre le recours à la communication électronique dans le domaine judiciaire (ERV). Ces services se trouvent au centre, dans la partie verte du graphique.

La couche d'accès et de données au-dessus résume les possibilités d'accès et de frontend des utilisateurs finaux. La couche infrastructure montre la topologie du réseau, avec un cluster de centre de calcul redondant à haute disponibilité (cloud privé), un site de sauvegarde pour assurer la continuité de l'activité, et un centre de calcul pour les travaux de développement et de test.

4 Disciplines d'exploitation pour l'exploitationpilote

L'objectif de l'exploitation pilote est notamment de tester les processus d'exploitation et la sécurité de l'information. Cela concerne les disciplines suivantes :

☐ Couches d'accès et de données :

o dentité et règles d'accès : avec le Justitia-Level of Trust (JLoT), la plateforme garantit que seules des identités numériques de qualité suffisante (p. ex. un deuxième facteur personnel d'authentification lors du login) sont utilisées.

o les exigences du propriétaire des données

o prescriptions relatives à la protection des informations et des données (SIPD)

☐ Couche de service d'application :

o gestion des SLA : mesurer régulièrement la qualité de service obtenue et identifier les domaines dans lesquels la qualité de service doit être améliorée.

o tester les systèmes et les applications pour s'assurer que la plateforme réponde aux exigences et ne contienne pas d'erreurs.

og des services : traiter les demandes de services.

o gestion des incidents et des problèmes : traitement des incidents de service.

o gestion des versions : le processus garantit que les modifications du système et des applications sont mises en production dans le cadre d'un processus ordonné et défini.

o gestion des vulnérabilités : contrôle en permanence les vulnérabilités de sécurité du système.

☐ Couche infrastructure

o surveillance du système 7x24 : contrôle de la sécurité et de la stabilité de la plate-forme. ?

o Key Management : assure la gestion sécurisée des clés cryptographiques.

o SOC & CERT : le Security Operation Center surveille 24 heures sur 24 la sécurité de la plate-forme. L'équipe Computer Emergency Response Team traite les incidents de sécurité.

o cloud privé en Suisse : la plateforme "Justitia.Swiss" fonctionne sur du matériel dédié dans des centres de calcul en Suisse.

o gestion de la continuité des activités : la disponibilité et les performances de la plateforme sont maintenues à un niveau suffisant, même en cas de catastrophe.

o afin de minimiser la surface d'attaque, seuls les composants systèmes nécessaires sont installés et configurés de manière sûre (System Hardening).

o sécurisation physique de l'accès aux centres de calcul.

o gestion contrôlée de l'accès aux systèmes.

5 Effets sur les processus ou les flux de travail existants

La mise en œuvre du logiciel peut entraîner des changements dans les processus de travail et donc nécessiter une formation et l'apprentissage de nouvelles compétences par les personnes concernées. La plateforme numérise les tâches et les étapes de travail et modifie les rôles des collaboratrices et des collaborateurs. Elle peut également modifier la collaboration et la communication. Dans l'ensemble, l'introduction de la plateforme « "Justitia.Swiss » influencera les processus et les méthodes de travail existants des organisations concernées. La démarche choisie par Justitia 4.0 offre aux cantons la possibilité de soumettre leurs processus internes à un examen, de les tester et de les développer.