

E27 Exigences globales envers la plateforme Justitia.Swiss

Annexe 5 d'appel d'offres plateforme Justitia.Swiss

Table des matières

Introduction	3
FUN-01 Master Data Management	7
FUN-01-01 Gérer le profil	Impératif7
FUN-01-02 Gérer les personnes physiques	Impératif8
FUN-01-03 Gérer soi-même des organisations	Impératif8
FUN-01-04 Administrer les organisations	Impératif8
FUN-01-05 Gérer la délégation spécifique à une procédure	Priorité 18
FUN-01-06 Consulter le registre des adresses	Impératif9
FUN-02 Transmission de messages	9
FUN-02-01 Communication	Impératif9
FUN-02-02 notification	Impératif ... 10
FUN-02-03 Notification avec procédure d'invitation	Priorité 2 ... 10
FUN-02-04 Réponse aux communications sans procédure	Priorité 1 ... 10
FUN-03 Dossier Store - Explorateur de dossiers	11
FUN-03-01 Dupliquer la fourre de dossier	Impératif ... 11
FUN-03-02 Représenter la structure du dossier	Impératif ... 11
FUN-03-03 Autoriser les pièces	Impératif ... 11
FUN-03-04 Révoquer l'autorisation	Impératif ... 12
FUN-03-05 Gestion centralisée des pièces	Impératif ... 12
FUN-03-06 Accéder aux pièces décentralisées	Option 12
FUN-03-07 Types de médias des pièces	Impératif ... 12
FUN-03-08 Annoter et marquer des dossiers	Option 12
FUN-04 Service de cachet électronique.....	13
FUN-04-01 Apposer un cachet électronique pour les autorités judiciaires	Option 13
FUN-04-02 Valider le cachet électronique	Impératif ... 13
FUN-05 Audit Trail.....	13
FUN-05-01 Enregistrer les événements	Impératif ... 13
FUN-05-02 Consulter les événements	Impératif ... 14

FUN-05-03 Générer des quittances	Impératif ... 14
FUN-05-04 Évaluer l'Audit Trail	Impératif ... 14
FUN-06 Portail Internet / API	14
FUN-06-01 Informer le public	Impératif ... 14
FUN-06-02 Garantir un accès sécurisé via API ou portail Internet	Impératif ... 14
FUN-06-03 Fonctionnalité via API	Impératif ... 14
FUN-06-04 Interfaces versionnées	Impératif ... 15
FUN-06-05 Design UX et accessibilité	Impératif ... 15
FUN-07 Sécurité et protection des données	15
FUN-07-01 Mesures organisationnelles	Impératif ... 15
FUN-07-02 Security Information and Event Management (SIEM)	Impératif ... 16
FUN-07-03 Assurer la confidentialité et le contrôle d'accès	Impératif ... 16
FUN-07-04 Assurer la disponibilité des Business Services	Impératif ... 17
FUN-07-05 Matériel dédié pour Justitia.Swiss	Option 17
FUN-08 Opérations	17
FUN-08-01 Service Desk	Impératif ... 17
FUN-08-02 Découplage de l'infrastructure, des données et des applications	Impératif ... 18
FUN-08-03 Gérer le fournisseur d'identité	Impératif ... 18
FUN-08-04 Outil Service Management	Impératif ... 18
FUN-08-05 Environnements de test	Impératif ... 18

Remarques d'ordre rédactionnel

Le présent document contient les exigences générales envers la plateforme Justitia.Swiss en annexe à l'appel d'offres. Pour la phase d'offres, des spécifications techniques (ST) et des critères d'adjudication (CA) sont formulés – et si nécessaires précisés – sur la base de ces exigences globales.

Les exigences globales sont réparties au sens le plus large sur le plan fonctionnel et se situent au niveau 2 avec FUN-xx-yy. Pour une première vue d'ensemble, les concepts techniques, le schéma du système avec les interfaces et l'ébauche de modèle d'exploitation sont présentés en introduction à titre de Big Picture.

Priorités

Les exigences globales ont chacune des priorités différentes. A cet égard, les termes ci-après ont la signification suivante:

- Impératif: l'exigence doit être mise en œuvre pour une exploitation en production.
- Priorité 1: exigence importante à mettre en œuvre en première priorité.
- Priorité 2: exigence moins importante, en deuxième priorité.
- Option: cette exigence est facultative. Selon les besoins, le niveau d'urgence sera ajusté ou l'exigence ne sera pas mise en œuvre.

Pour les options, des offres avec des prix seront remises dans l'appel d'offres afin qu'une décision puisse être prise quant à la réalisation de ces fonctions supplémentaires.

Introduction

Le modèle suivant montre les objets pertinents d'information de la plateforme. En bref:

- Les **personnes** sont des organisations ou des personnes physiques.
- Les personnes physiques sont authentifiées par des **identités** numériques.
- Les personnes sont détentrices de **profils** servant à la communication électronique dans le domaine judiciaire et à la consultation des dossiers.
- Les **transmissions** de la communication électronique dans le domaine judiciaire (CEJ) sont des communications aux autorités judiciaires (transmissions entrantes de la CEJ) ou des notifications des autorités judiciaires (transmissions sortantes de la CEJ).
- Un **dossier électronique consultable** est géré par une autorité judiciaire (profil d'une autorité judiciaire). Il contient des pièces consultables d'un dossier.
- Les notifications sont fondées sur le droit de consultation des pièces de dossiers. Les autorités judiciaires donnent ainsi accès au **dossier d'une procédure**.
- Les autorisations peuvent être **déléguées** (en fonction de la procédure).

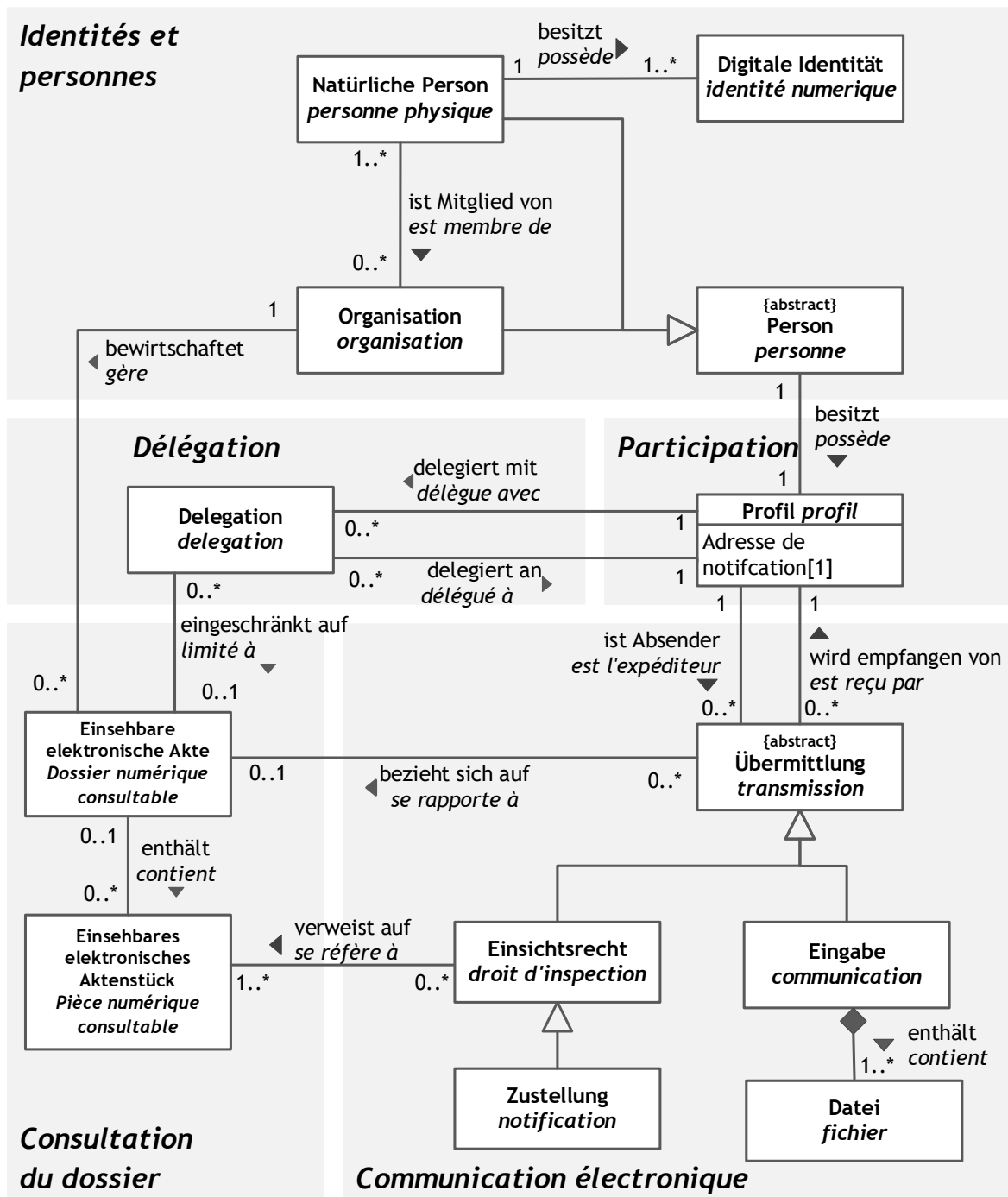


Figure 1: concept de modèle d'information

La figure suivante montre les acteurs impliqués et les composants de la plateforme Justitia.Swiss.

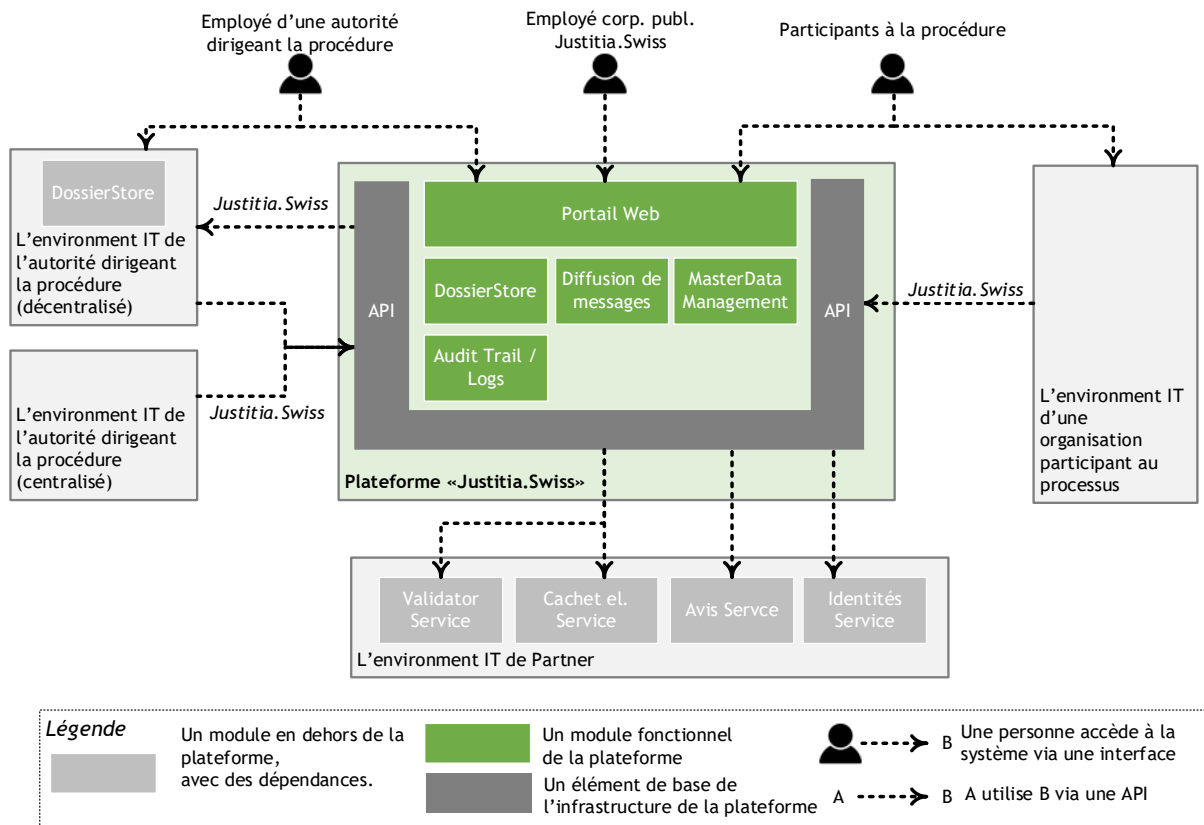


Figure 2: aperçu des interfaces de la plateforme Justitia.Swiss

Description des composants fonctionnels:

- La plateforme propose un **portail Internet** destiné aux collaborateurs (profil de collaborateur) des autorités dirigeant la procédure, aux parties à la procédure et aux collaborateurs de la société d'exploitation (pour les tâches administratives). Le portail Internet comporte également une zone pour les utilisateurs non-connectés avec un contenu accessible publiquement.
- Le composant **DossierStore** remplit 2 fonctions:
 - il stocke les copies des pièces électroniques pouvant être consultées (ainsi que les autorisations correspondantes. La consultation d'une pièce y est autorisée.) pour les autorités qui le souhaitent.
 - Il contient les autorités et les numéros de dossier de toutes les procédures de la plateforme.
- Le composant **transmission des messages** assure la diffusion et gère les transmissions échangées de la communication électronique (CEJ). La fonctionnalité est fondée en large partie sur une boîte aux lettres par participant.
- Le composant **MasterDataManagement** propose des services de gestion des données de base du registre des adresses.
- Le composant **Audit Trail / Logs** enregistre les événements de la plateforme et les préserve de toute modification; il fournit des informations à ce sujet, tant pour les participants que pour l'exploitant de la plateforme à des fins d'évaluation statistique.

Description des services fournis par les partenaires:

- Le **service d'avis** de notification envoie des messages qui informent les participants sur le statut des notifications. Techniquement, il s'agit de courriels et de SMS.
- Le **service de cachet électronique** applique un cachet électronique réglementé (selon SCSE) sur les documents.

- Le **service de validation** valide les cachets électroniques et les signatures des documents.
- Le **service d'identité** fournit des identités numériques sécurisées pour l'authentification des utilisateurs. Pour les collaborateurs des autorités (ou, cas échéant, des entreprises), ce service d'identité peut être fourni par l'environnement informatique de l'organisation.

Les API suivantes sont imposées par Justitia.Swiss. Comme demandé dans FUN-06-03, la fonctionnalité des API est toujours disponible via le portail Internet.

Justitia.Swiss.01:	Registre des adresses
Grâce à cette API, les personnes autorisées peuvent consulter les participants et consulter les attributs administratifs des détenteurs d'adresses de notification.	
Justitia.Swiss.02:	Profil
Grâce à cette API, les personnes physiques peuvent gérer leur profil, attribuer des délégations et gérer des organisations autoadministrées (dont ils sont administrateurs).	
Justitia.Swiss.03:	Communication
Grâce à cette API, les participants à la procédure peuvent regrouper et transmettre des communications. Les directions de procédures peuvent télécharger les communications via cette interface.	
Justitia.Swiss.04:	Notification et droit de consultation
Grâce à cette API, des pièces sont mises à disposition et octroyés des droits de consultation aux participants à la procédure. Cette interface est également utilisée pour révoquer les autorisations. <i>Remarque: dans le cas de la conservation centralisée des données, les notifications ou octrois de droits de consultation se réfèrent aux pièces chargées via l'API Justitia.Swiss.06: .</i>	
Justitia.Swiss.05:	Pièces de dossiers
Cette API est utilisée pour mettre à disposition des pièces de dossiers sous forme décentralisée. L'API est mise en œuvre par les systèmes informatiques des autorités judiciaires et elle est utilisée par la plateforme (explorateur de dossiers).	
Justitia.Swiss.06:	Dossiers électroniques pouvant être consultés
Grâce à cette API, les autorités dirigeant la procédure dupliquent sur la plateforme les données de leurs dossiers pouvant être consultés. Dans le cas d'un stockage centralisé des données, des pièces peuvent être chargées via cette interface.	
Justitia.Swiss.07:	Explorateur de dossiers
Grâce à cette API, les parties à une procédure peuvent recevoir leurs notifications et consulter les dossiers.	
Justitia.Swiss.08:	Audit Trail
Chaque instance autorisée peut consulter son historique et, au besoin, générer des quittances à partir des événements enregistrés.	
Justitia.Swiss.09:	Valideur
Grâce à cette API, toutes les personnes peuvent faire valider les pièces (cachetées) reçues.	
Justitia.Swiss.10:	Cachet électronique
Grâce à cette API, les autorités judiciaires peuvent apposer leur cachet électronique sur les documents.	

Tableau 1: les API de Justitia.Swiss

Pour la fourniture des Business Services, nous suivons les pratiques ITIL et le modèle opérationnel SIAM (Service Integration & Management), présenté à la figure 3. A cet égard, les différents composants désignent les groupes de processus qui sont sous la responsabilité de Justitia.Swiss ou qui doivent être fournis par des partenaires.

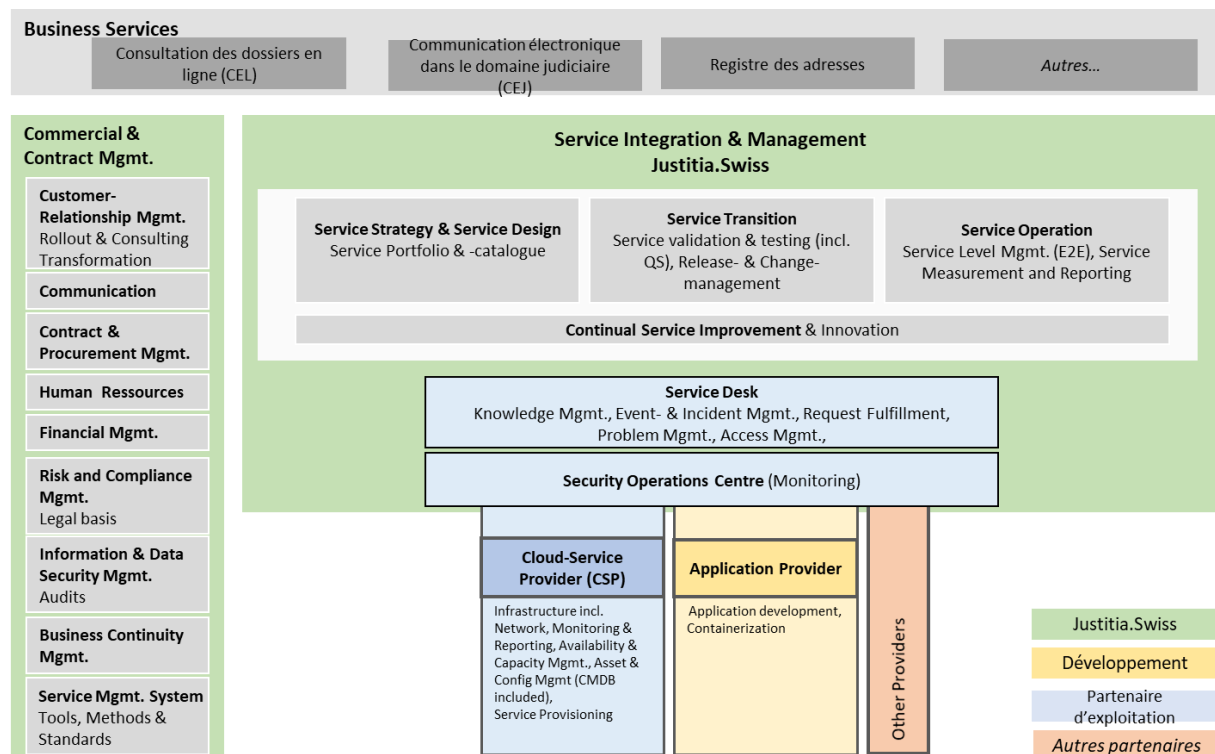


Figure 3: modèle opérationnel de Justitia

FUN-01 Master Data Management

Processus de données de base pour la gestion d'objets d'information pour les personnes, les profils et les délégations.

FUN-01-01 Gérer le profil

Impératif

Le profil est l'objet central de données de base pour utiliser la plateforme. Chaque personne (physique ou organisation) dispose d'un profil. Les caractéristiques suivantes sont enregistrées dans le profil:

- la personne participe à la communication électronique (CEJ) et à la consultation des dossiers en définissant une adresse de notification.
- Une adresse de réception des avis peut être définie. Les paramètres relatifs au type et à la fréquence de avis de notification peuvent être définis.
- D'autres attributs doivent être définis tels qu'une désignation supplémentaire sous laquelle la personne est décrite dans le registre des adresses.

Un participant est une personne (personne physique avec le profil d'une personne physique ou organisation avec un profil autoadministré ou un profil d'une organisation administrée) qui dispose d'une adresse de notification sur la plateforme.

Remarque: la gestion du profil se fait via l'API Justitia.Swiss.02:

FUN-01-02 Gérer les personnes physiques

Impératif

Les attributs des personnes physiques sont repris du fournisseur externe d'identité. Ainsi, la qualité des données des personnes a une qualité définie selon l'art. 19 AP-LPCJ: les attributs administratifs des personnes physiques sont vérifiés par un organisme officiel.

Remarque: cela n'empêche pas les doublons de personnes ayant des rôles différents et provenant de différents fournisseurs d'identité (par ex. un particulier et un employé d'une autorité).

FUN-01-03 Gérer soi-même des organisations

Impératif

Les organisations sont des groupes de personnes physiques conformément à l'art. 24 AP-LPCJ. Une personne physique peut ouvrir et gérer elle-même une organisation. La personne qui ouvre est l'administrateur initial de cette organisation autoadministrée.

Au moyen d'un procédure d'invitation, l'administrateur peut ajouter d'autres personnes comme membres de l'organisation et accorder à ces membres des droits sur l'organisation (et le profil associé).

Remarque: cela permet aux avocats ou autres représentants professionnels d'ouvrir des organisations autoadministrées avec un profil correspondant (d'avocat).

Remarque: la gestion indépendante d'une organisation autoadministrée passe par l'API Justitia.Swiss.02:

FUN-01-04 Administrer les organisations

Impératif

Les autorités judiciaires et les organisations (par ex. des compagnies d'assurance) peuvent également se faire attribuer une organisation sur la plateforme par le biais d'un processus administratif. Les organisations sont des groupes de personnes physiques conformément à l'art. 24 AP-LPCJ. La qualité des profils des organisations administrées a une fiabilité plus élevée qu'une organisation autoadministrée.

Les organisations administrées peuvent associer leur propre service d'identité (=organisations administrées par IDP) pour attribuer de manière dynamique aux utilisateurs des droits sur l'organisation et son profil (par l'utilisateur gérant l'IDP de l'organisation. Elles peuvent intégrer leurs systèmes à la plateforme via l'API et des clés techniques.

Les profils d'organisations autoadministrées peuvent être converties en profils d'organisations administrées.

Remarque: les collaborateurs des autorités judiciaires et organisations peuvent travailler sur la plateforme avec leur accès d'employé.

Remarque: des dispositions appropriées doivent être prises pour la connexion technique, la transmission des clés et le mappage des rôles, voir FUN-08-03.

FUN-01-05 Gérer la délégation spécifique à une procédure

Priorité 1

Le détenteur autorisé d'un profil peut déléguer certaines actions à d'autres personnes. Cette délégation peut être déterminée de manière spécifique pour une procédure au sens strict par autorité.

La création d'une délégation doit garantir le respect de la sphère privée des utilisateurs: il est fait recours à une procédure d'invitation qui n'autorise la visibilité des personnes qu'après accord mutuel.

Remarque: les délégués agissent au nom d'une autre personne.

Remarque: la gestion de la délégation se fait via l'API Justitia.Swiss.02:

FUN-01-06 Consulter le registre des adresses

Impératif

La plateforme tient un registre des adresses qui ont une adresse de notification sur la plateforme. La visibilité du registre des adresses est limitée:

- les collaborateurs des autorités judiciaires (personnes qui ont un profil de collaborateur auprès d'un profil d'une autorités judiciaire) peuvent consulter les attributs définis de tous les profils qui ont une adresse valable de notification.
- Tous les autres utilisateurs de la plateforme peuvent consulter les attributs définis des profils des autorités judiciaires.

Chaque attribut d'utilisateur figurant dans le registre des adresses a un niveau de qualité défini.

Remarque: le registre des adresses peut être consulté via l'API Justitia.Swiss.01: .

FUN-02 Transmission de messages

Les principales opérations de la plateforme pour la communication électronique dans le domaine judiciaire comprennent la transmission des communications des participants aux procédures aux autorités judiciaires et la notification de liens vers des pièces d'un dossier au titre d'une invitation à consulter un dossier.

FUN-02-01 Communication

Impératif

Une communication est constituée d'un ou plusieurs fichiers, et des métadonnées correspondantes qui sont transmis par un participant à la procédure à une autorité judiciaire.

La plateforme autorise un enrichissement souple et extensible de la communication (respectivement des fichiers joints) avec des métadonnées supplémentaires pour une catégorisation. Cet enrichissement peut aussi dépendre du profil de l'expéditeur ou du destinataire.

Les métadonnées sont utilisées à des fins diverses:

- Pour améliorer la sécurité, par ex. en cas de soupçon de virus.
- Permet (au destinataire) le traitement automatique ou le routage de fichiers structurés (par ex. pour la communication entre la police et les autorités).
- Si les documents devant faire l'objet d'une communication proviennent eux-mêmes d'un dossier, les métadonnées contiennent des rubriques et des numéros de dossier afin de pouvoir garantir le référencement ou pour transmettre des renvois (liens) vers des pièces de dossier ou des pièces à conviction mises à disposition.
- Les métadonnées contiennent des clés cryptographiques permettant d'attester l'intégrité des documents.
- Les métadonnées techniques facultatives des documents qui font partie du fichier (par ex. des données exif de photos ou des remarques sur les versions logicielles) sont au besoin affichées à la partie effectuant la communication et peuvent être retirées pour des raisons de protection des données.
- Une communication peut se référer à une procédure en cours d'une autorité via un identifiant de dossier.
- Il est possible de vérifier si le document juridique saisi possède une signature électronique qualifiée valide. Cela peut être nécessaire dans le cadre d'une phase pilote, car l'exigence de signature ne sera pas adaptée avant l'entrée en vigueur de la LPCJ.

Les fichiers sont cachetés par la plateforme avec le cachet électronique de l'entité Justitia.Swiss. Sur demande (argument optionnel de l'appel de service ou dans les paramètres du profil), une quittance, également cachetée, est automatiquement générée lorsque la tâche est terminée.

La communication cachetée est recueillie par les autorités judiciaires à partir de leur boîte aux lettres. Les communications récupérées sont supprimées de la plateforme après un temps déterminé.

Si un avis de notification pour des communications est configuré sur le profil de l'autorité judiciaire (destinataire), cette dernière recevra un message correspondant.

La plateforme offre des possibilités d'extension afin de pouvoir saisir de manière structurée des communications standardisées (par ex. prolongations de délais).

Remarque: les données sont saisies et téléchargées via l'API Justitia.Swiss.03: .

FUN-02-02 notification

Impératif

Une notification est la transmission du droit de consultation d'une ou de plusieurs pièces par l'autorité judiciaire à un participant à la procédure. Il y a plusieurs configurations:

- Une notification avec délai, au cours duquel le destinataire de la notification doit consulter la pièce. La plateforme confirme l'envoi de la notification et la première lecture des pièces ainsi autorisées.
- L'octroi pur et simple du droit de consultation du dossier a lieu sans imposer de délai. La plateforme confirme l'octroi de droit de consultation du dossier.

Sur demande (argument optionnel de l'appel de service ou dans les paramètres du profil), une quittance cachetée est automatiquement générée après la transmission complète et la confirmation des droits de consultation du dossier.

Si un avis de notification est configuré sur le profil de la personne (destinataire), cette dernière recevra un message correspondant.

Remarque: les notifications sont gérées via l'API Justitia.Swiss.04: .

FUN-02-03 Notification avec procédure d'invitation

Priorité 2

Les autorités judiciaires peuvent envoyer une notification à un participant pas encore défini comme tel. Pour ce faire, elles ouvrent un profil temporaire avec une adresse de notification et invitent (par ex. via le canal du courrier) la personne à s'enregistrer sur la plateforme et de s'y connecter avec ce profil.

Remarque: au sein du processus utilisé dans la procédure d'invitation, notamment la gestion du cycle de vie de ce «profil temporaire» en cas d'invitations laissées sans réponse, la possibilité pour un utilisateur de regrouper des invitations parallèles, etc. sera clarifiée au niveau du design.

FUN-02-04 Réponse aux communications sans procédure

Priorité 1

Les autorités peuvent répondre aux communications via la plateforme sans ouvrir de procédure.

Du point de vue des autorités, cette possibilité passe par les mécanismes et interfaces de la notification, ce qui signifie qu'un document est notifié sans identifiant de dossier.

Le destinataire reçoit le droit de consulter un document (la réponse), sans que celui-ci soit intégré à une structure de dossier. Une délégation ou une réplique à une telle réponse n'est pas possible.

La plateforme supprime le document après un temps défini une fois qu'il a été lu par le destinataire.

FUN-03 Dossier Store - Explorateur de dossiers

Le Dossier Store permet à chaque utilisateur autorisé de voir les dossiers des procédures auxquelles il est autorisé à accéder.

FUN-03-01 Dupliquer la fourre de dossier

Impératif

Les procédures sont administrées dans les systèmes informatiques des autorités judiciaires raccordées et l'information minimale d'un dossier pouvant être consulté est dupliquée pour l'affichage des pièces. Cela signifie pour la gestion du cycle de vie des dossiers sur la plateforme:

- lors de la première notification, une identification univoque du dossier est définie
- pendant la durée de la procédure, l'information sur le dossier est mise à jour dans la fourre
- avec la clôture de la procédure, les données sur la plateforme concernant cette procédure sont supprimées, respectivement marquées pour être supprimées. Le moment de la suppression effective est défini dans un règlement de traitement pour chaque objet de données.

Remarque: la quantité exacte de données requises pour chaque dossier sera déterminée dans le cadre du design en tenant compte du principe d'économie des données.

Remarque: le cycle de vie d'un dossier est géré via l'API Justitia.Swiss.06: .

FUN-03-02 Représenter la structure du dossier

Impératif

Avec l'octroi d'un droit d'accès à une pièce, un dossier devient visible pour les participants à la procédure: les utilisateurs ainsi autorisés voient les informations de la fourre du dossier et les pièces auxquelles ils sont autorisés à accéder dans la hiérarchie du dossier.

Une rubrique de la hiérarchie du dossier est visible pour un utilisateur si au moins une pièce de cette rubrique est visible. (En d'autres termes, les rubriques vides ne sont pas visibles).

Les utilisateurs peuvent effectuer des recherches en filtrant tous les dossiers qu'ils peuvent consulter selon divers critères des dossiers (voir les données du dossier selon FUN-03-01) et les métadonnées des pièces.

Remarque: les dossiers sont consultés par le biais de l'API Justitia.Swiss.07: .

FUN-03-03 Autoriser les pièces

Impératif

Le contrôle d'autorisation (Policy Decision Point et Policy Enforcement Point) est assuré sur la plateforme avant chaque accès à une pièce, en particulier:

- l'autorité judiciaire qui dirige la procédure a-t-elle envoyé une notification? (Policy Administration Point)
- La notification est-elle valable (période)?
- La personne qui lit a-t-elle une autorisation sur le profil, pour lequel une notification a été définie, ou le droit de consultation lui a-t-il été délégué?

L'autorisation a 2 configurations possibles:

- seule l'existence est connue, si le participant à la procédure n'est autorisé à lire que les métadonnées. (par ex. existence d'un plan tarifaire de la partie adverse).
- Contenu visible.

Remarque: l'autorisation «seulement sur les métadonnées» est par exemple utile en droit de la concurrence, si une partie doit voir que l'autre partie a remis au tribunal les descriptifs de produits ou des plans tarifaires sans pour autant pouvoir voir le design concret du produit.

FUN-03-04 Révoquer l'autorisation

Impératif

Les notifications ont une durée de validité pendant laquelle un destinataire peut consulter les pièces. La durée de validité peut également être ouverte, c'est-à-dire que la consultation est valable pour une durée illimitée (jusqu'à ce que la procédure soit supprimée).

Dans des cas particuliers, les autorités judiciaires peuvent révoquer prématurément les autorisations octroyées.

Remarque: la révocation d'un droit de consultation se fait via l'API Justitia.Swiss.04:

FUN-03-05 Gestion centralisée des pièces

Impératif

Les pièces peuvent être conservées sur la plateforme. L'accès aux pièces est autorisé via FUN-03-03. Les autorités chargent leurs pièces sur la plateforme via Justitia.Swiss.06: .

Lorsque le dossier est supprimé, toutes les pièces correspondantes sont supprimées.

FUN-03-06 Accéder aux pièces décentralisées

Option

En option, les pièces peuvent être conservées dans des systèmes informatiques sous la responsabilité des autorités judiciaires au lieu d'être centralisées sur la plateforme. A cette fin, les autorités judiciaires mettent en œuvre l'API Justitia.Swiss.05: .

Remarque: même si les pièces sont conservées de manière décentralisée, la plateforme vérifie l'autorisation à chaque consultation de dossier (voir FUN-03-03).

FUN-03-07 Types de médias des pièces

Impératif

La plateforme permet une catégorisation flexible des formats de fichier. Il faut alors prévoir notamment:

- Des fichiers PDF cachetés par les autorités judiciaires.
- Des types de médias (image, son, vidéo) mis à disposition par les autorités judiciaires. Selon le type de média, un module de visualisation correspondant pour ce format est mis à disposition ou un utilisateur peut «seulement» télécharger les fichiers. Des modules de visualisation spéciaux doivent pouvoir être définis pour des formats spécifiques comme des plans ou des scènes en trois dimensions.
- Des formats spéciaux de données ne permettent qu'un cachet électronique sur les propres fichiers (par ex. PKCS#7). Dans ce cas, l'affichage ou le téléchargement du fichier doit être possible avec ou sans cachet.

Il doit être possible d'ajouter d'autres types de médias (image, son, vidéo) si nécessaire. Cela comprend notamment la possibilité de diffuser des vidéos en continu.

Remarque: la catégorisation des pièces est effectuée selon le même principe que celui esquissé pour une communication (FUN-02-01).

FUN-03-08 Annoter et marquer des dossiers

Option

Les participants à la procédure peuvent ajouter sur la plateforme des notes et des étiquettes (tags) aux dossiers et aux pièces qui ne sont visibles que pour eux (ou éventuellement sur délégation).

Lorsque le dossier est supprimé (par les autorités judiciaires), les étiquettes et les notes associées sont également supprimées.

Remarque: le fait d'apposer des notes et étiquettes (tags) sur les dossiers ne doit en aucun cas donner l'impression que les participants à la procédure peuvent modifier des documents sur la plateforme

ou les éditer d'une autre manière. Les notes et étiquettes doivent être davantage comprises au sens de «Important», «Urgent» ou similaire.

Remarque: les étiquettes et les notes sur les dossiers sont attribuées via l'API Justitia.Swiss.07: .

FUN-04 Service de cachet électronique

Grâce au service de cachet électronique, il est possible d'apposer des cachets sur les documents et de valider les documents cachetés.

FUN-04-01 Apposer un cachet électronique pour les autorités judiciaires Option

Lors du chargement de fichiers pour consultation ou notification par les autorités judiciaires, la plateforme vérifie si ces fichiers sont munis d'un cachet électronique des autorités judiciaires. En option, la plateforme peut apposer directement le cachet électronique pour ces autorités judiciaires.

*Remarque: les documents sont cachetés avec l'API **Fehler! Verweisquelle konnte nicht gefunden werden.***

FUN-04-02 Valider le cachet électronique Impératif

La plateforme permet à tous les utilisateurs (pas seulement aux participants enregistrés) de valider le cachet électronique d'un document PDF ou XML mis à leur disposition. Pour cela,

- la validité du cachet électronique de l'autorité est confirmée.

Remarque: pour l'examen à proprement parler, c'est le service de validation de l'OFIT, intégré par le biais de la plateforme, qui est utilisé. Nous considérons que ce module de validation sera à l'avenir étendu pour d'autres types de fichiers (par ex. PKCS#7).

Remarque: les documents sont validés avec l'API Justitia.Swiss.09: .

FUN-05 Audit Trail

L'Audit Trail enregistre les événements (transactions et modifications des données de base) de manière contraignante et incontestable.

FUN-05-01 Enregistrer les événements Impératif

La plateforme enregistre les événements juridiquement contraignants de manière inaltérable, authentique et incontestable. Ces événements sont au moins:

- la conclusion d'une communication
- la transmission d'une notification avec délai
- la première consultation d'une pièce notifiée

D'autres événements pertinents peuvent facilement être configurés, y compris quelles données sont exactement enregistrées dans l'Audit Trail.

Pour les événements de la communication électronique dans le domaine judiciaire, il y a deux personnes intéressées en tant que «propriétaires des données associées»: l'expéditeur et le destinataire de la transmission. En conséquence, deux points de vue différents sur les événements sont proposés. Par exemple, l'autorité judiciaire ne doit pas voir dans les communications la personne connectée, mais la personne agissant sur le profil, et, en cas de délégation, le déléguant voit quelle personne a effectué une action en son nom.

FUN-05-02 Consulter les événements

Impératif

Chaque événement a une personne comme auteur de l'événement. En termes de protection des données, les données relatives à l'événement «appartiennent» à l'auteur, c'est-à-dire que lui seul est autorisé à voir les données et à y donner accès.

Remarque: la vue sur l'Audit Trail est donnée par le biais de Justitia.Swiss.08:

FUN-05-03 Générer des quittances

Impératif

Pour permettre aux destinataires ou aux expéditeurs dans la communication électronique (CEJ) de prouver de manière juridiquement contraignante et incontestable qu'un événement a eu lieu dans la communication électronique (CEJ), la plateforme fournit des quittances sur la base des données des événements.

Les quittances sont sécurisées par des moyens cryptographiques de telle sorte que leur intégrité et leur authenticité puissent être prouvées.

FUN-05-04 Évaluer l'Audit Trail

Impératif

Les données de l'Audit Trail peuvent être analysées (de manière anonyme) par l'entité à des fins statistiques. Cela permet de tirer des enseignements pour l'exploitation et le développement ultérieur de la plateforme.

Remarque: pour des raisons de protection des données, aucune évaluation personnalisée n'est permise ou alors une telle évaluation nécessite l'accord explicite du détenteur des données.

FUN-06 Portail Internet / API

Les utilisateurs de la plateforme peuvent accéder aux fonctionnalités de la plateforme via le portail Internet et l'API.

FUN-06-01 Informer le public

Impératif

La plateforme contient un espace d'information accessible au public et la possibilité de prendre contact. Des textes, images et vidéos multilingues peuvent y être mis à disposition. Il existe une option de prévisualisation des modifications (Content-Management-System).

Le service API Justitia.Swiss.09: de validation des cachets (FUN-04-02) est proposé au public.

L'accès public (non sécurisé) est techniquement et, si raisonnablement possible, physiquement séparé des fonctionnalités sécurisées.

FUN-06-02 Garantir un accès sécurisé via API ou portail Internet

Impératif

L'accès à une fonctionnalité sécurisée survient seulement après authentification par un fournisseur d'identité (IDP) accepté avec un niveau de sécurité substantiel ou supérieur.

Cela concerne toutes les API sauf Justitia.Swiss.09:

FUN-06-03 Fonctionnalité via API

Impératif

La fonctionnalité de la plateforme doit être disponible par le biais de services reposant sur un protocole ouvert.

Le Web Frontend de Justitia.Swiss est fourni par un Single Server Page unique qui accède à l'API.

Remarque: cela signifie que la même fonctionnalité peut être utilisée pour le portail Internet que celle qui est utilisée à partir d'un Backend. Selon FUN-07-03, chaque appel de service est contrôlé.

FUN-06-04 Interfaces versionnées

Impératif

La plateforme offre, dans une mesure raisonnable, des interfaces rétrocompatibles et versionnées.

FUN-06-05 Design UX et accessibilité

Impératif

Le portail doit pouvoir être affiché et lu sur des terminaux différents avec un design adaptatif.

L'interface Internet répond aux exigences en matière d'accessibilité

L'interface Internet est multilingue.

L'interface utilisateur est intuitive.

FUN-07 Sécurité et protection des données

La plateforme contient des données hautement sensibles. Il faut donc accorder une grande importance à l'aspect de la sécurité et de la protection des données. Cela nécessite des mesures organisationnelles, un système de surveillance continue de la sécurité et des mesures techniques pour garantir la confidentialité et la disponibilité. Les exigences de l'application pour garantir l'intégrité des données sont décrites dans le service de cachet électronique et la traçabilité des événements dans l'Audit Trail.

FUN-07-01 Mesures organisationnelles

Impératif

Des concepts détaillés pour les questions relatives à l'information et à la protection des données doivent être élaborés. Cela inclut notamment:

- une analyse d'impact sur la protection des données (exigence de la loi révisée sur la protection des données);
- un règlement de traitement (exigence tirée du modèle HERMES modifié pour les concepts SIPD);
- un concept détaillé pour la gestion des utilisateurs, des groupes et des autorisations;
- un concept détaillé pour la mise en œuvre du service de cachet électronique et du validateur;
- un concept détaillé pour la mise en œuvre d'un Audit Trail et d'un service de journalisation;
- des prescriptions pour des algorithmes cryptographiques, des longueurs de clé et la gestion des clés;
- des prescriptions pour la connexion de fournisseurs d'identité;
- des prescriptions pour la connexion des systèmes des autorités judiciaires et des études d'avocats.

Le partenaire de développement et d'exploitation fournit des contributions essentielles pour ces concepts.

La corporation de droit public (CDP) établit un système de gestion de la sécurité de l'information (ISMS) pour la plateforme «Justitia.Swiss» et le fait certifier selon la norme ISO/IEC 27001.

Mise en place d'un programme de sensibilisation aux mesures de sécurité pour tous les utilisateurs et collaborateurs de la CDP, du partenaire de développement et de l'exploitant.

La CDP a un droit permanent, complet et illimité de consulter et de contrôler l'exploitation de la plateforme «Justitia.Swiss» à tout moment.

La CDP fait appel à des tiers spécialisés et indépendants pour contrôler la sécurité de la plateforme «Justitia.Swiss».

Le partenaire d'exploitation sécurise l'exploitation et en particulier les accès administratifs.

FUN-07-02 Security Information and Event Management (SIEM)

Impératif

La CDP établit un système de gestion de la sécurité des informations et des événements (SIEM) et le fait certifier selon la norme ISO/IEC 27001.

Le SIEM comprend tous les processus et prescriptions nécessaires à la surveillance, l'enregistrement, l'évaluation, la communication et le traitement des incidents de sécurité.

Le SIEM recourt à l'expertise d'un centre d'opérations de sécurité (Security Operations Center, SOC) pour gérer la sécurité d'une organisation et l'améliorer. Les événements qui pourraient représenter un incident de sécurité sont alors classifiés, priorisés et soumis à une analyse des causes. Pour cela, il faut notamment distinguer entre anomalies métier et techniques (par ex. tentative d'accès depuis l'étranger).

Les journaux de tous les composants de l'infrastructure de la plateforme «Justitia.Swiss» ainsi que de l'Audit Trail sont collectés par l'exploitant dans un service central de journalisation et utilisés pour détecter les incidents de sécurité.

Un «Computer Emergency Response Team» (CERT) contribue à résoudre de manière coordonnée les incidents concrets de sécurité informatique.

FUN-07-03 Assurer la confidentialité et le contrôle d'accès

Impératif

Les aspects techniques suivants garantissent l'authenticité des utilisateurs et de leur autorisation:

- La conception des profils et des personnes qui en sont détenteurs garantit que toutes les personnes physiques figurant dans le registre d'adresses disposent d'une identité numérique confirmée avec un niveau de sécurité substantiel ou supérieur. Seuls les utilisateurs disposant d'une autorisation appropriée (membres d'une organisation ou par délégation) peuvent utiliser les fonctions de la plateforme. Voir toutes les exigences globales de FUN-01. L'accès par le biais d'API s'effectuent au besoin par des clés techniques.
- L'utilisation de la plateforme «Justitia.Swiss» nécessite une authentification forte de l'utilisateur avec un niveau de sécurité substantiel ou supérieur. Voir FUN-06-02.
- L'accès aux pièces des dossiers n'est accordé que si des droits de lecture suffisants ont été octroyés par l'autorité judiciaire qui dirige la procédure. Voir FUN-03-03.
- L'application Internet de la plateforme «Justitia.Swiss» offre aux participants à la procédure un espace de travail personnel protégé par un accès où ils peuvent, par exemple, préparer des communications. Voir FUN-02-01.

Mesures techniques:

- Toutes les connexions de communication effectuées via Internet sont cryptées.
- La plateforme «Justitia.Swiss» contrôle tous les fichiers transférés à l'aide d'un antivirus et bloque les fichiers qui ne peuvent pas être contrôlés (par ex. les fichiers cryptés).
- La plateforme «Justitia.Swiss» accepte différents formats de données. Les formats de données acceptés peuvent être étendus de manière flexible et (en particulier pour garantir la sécurité) également restreints.
- Toutes les connexions de communication depuis Internet parviennent à un pare-feu d'application Internet (Web Application Firewall, WAF) en amont et sont vérifiées pour détecter des contenus préjudiciables.

- Il n'y a pas de zone accessible anonymement (c'est-à-dire publiquement) sur le serveur d'application de la plateforme «Justitia.Swiss», voir FUN-06-01.
- « Data at rest », en particulier les fichiers du DossierStore avec les copies des pièces électroniques pouvant être consultées et les fichiers joints aux communications sont cryptées. L'accès aux données à des fins administratives est journalisé.
- Les clés cryptographiques (notamment pour le décryptage des fichiers du DossierStore ou pour la communication cryptée) se trouvent dans un module matériel sécurisé (Hardware Security Module).

FUN-07-04 Assurer la disponibilité des Business Services

Impératif

La disponibilité des Business Services et des données stockées (par ex. le registre des adresses, l'Audit Trail) de la plateforme «Justitia.Swiss» est assurée par des Service Level Agreements (SLA) correspondants avec l'exploitant de la plateforme.

Les Business Services pour la consultation des dossiers et la communication électronique (CEJ) sont disponibles à 99,9%.

Pour garantir que les données soient rapidement à nouveau disponibles, même après une catastrophe, celles-ci sont stockées de manière synchrone dans un centre de données de sauvegarde.

Afin de garantir que des données ne soient en aucun cas perdues, elles sont également sauvegardées séparément (Backup), en plus de la redondance géographique.

FUN-07-05 Matériel dédié pour Justitia.Swiss

Option

Tous les composants logiciels de la zone sécurisée de la plateforme Justitia.Swiss qui ne doivent pas être partagés avec d'autres clients fonctionnent sur du matériel (hardware) dédié.

Remarque: la zone sécurisée de la plateforme Justitia.Swiss comprend tous les composants sur lesquels des pièces de dossiers sont traitées ou enregistrées. Ne font pas partie de la zone sécurisée de la plateforme Justitia.Swiss des sites Internet publics accessibles de manière anonyme ainsi que des infrastructures du prestataire requises pour l'exploitation de la plateforme (par ex. systèmes de pare-feu, Loghost, systèmes de surveillance et similaires).

FUN-08 Opérations

Le partenaire d'exploitation gère un Service Desk pour les utilisateurs en tant que premier interlocuteur pour les demandes et fournit la plateforme technique pour les données, la puissance de calcul et les accès.

FUN-08-01 Service Desk

Impératif

Le Service Desk fait office de point de contact pour tout type d'assistance de la part des utilisateurs. Il assure la surveillance et gère la résolution des incidents et problèmes.

Pour les utilisateurs (notamment les particuliers ou avocats), le Service Desk est le service d'assistance de premier niveau (1st Level Support). Les collaborateurs des autorités ont le plus souvent leur propre organisation de service.

Le Service Desk transmet les problèmes aux unités spécialisées (à savoir l'infrastructure, la sécurité, le développement ou des clarifications métier à la collectivité de droit public).

En cas de problème, un Service Desk peut être contacté par téléphone de 7 heures à minuit.

Remarque: les heures de service en soirée jusqu'à minuit sont destinées en premier lieu aux utilisateurs, qui peuvent ainsi attester simplement l'indisponibilité ou la non-accessibilité de la plateforme afin de justifier une demande de prolongation de délai.

FUN-08-02 Découplage de l'infrastructure, des données et des applications **Impératif**

Le partenaire d'exploitation fournit au partenaire de développement des environnements basés sur des conteneurs selon un modèle Paas (Platform as a service). Il assure l'exploitation continue de l'infrastructure et des applications installées conformément aux exigences du service (SLA).

FUN-08-03 Gérer le fournisseur d'identité **Impératif**

Pour l'intégration de différents fournisseurs d'identité, des données de base ou des options de configuration doivent être fournies. Les processus administratifs correspondants (Onboarding et Offboarding du fournisseur d'identité, mesures de protection des identités gérées par le fournisseur) sont pris en charge.

Si le fournisseur d'identité est l'administrateur d'une organisation (il gère des collaborateurs des autorités), il doit être possible de définir des correspondances (mapping) entre les fonctions et les rôles du fournisseur d'identité et les fonctions de la plateforme.

FUN-08-04 Outil Service Management **Impératif**

Le partenaire d'exploitation fournit son outil Service Management (Service mangement Tool) avec lequel les utilisateurs peuvent saisir de manière indépendante des demandes de service et suivre le traitement de leurs demandes.

L'outil Service Management permet (par exemple pour des tickets) d'accéder aux données correspondantes des personnes de la plateforme.

FUN-08-05 Environnements de test **Impératif**

Il existe des environnements de test dédiés à des essais par les cantons et par les fabricants de logiciels pour avocats.