LEX persona

Cahier des fonctionnalités de la solution Lex Community

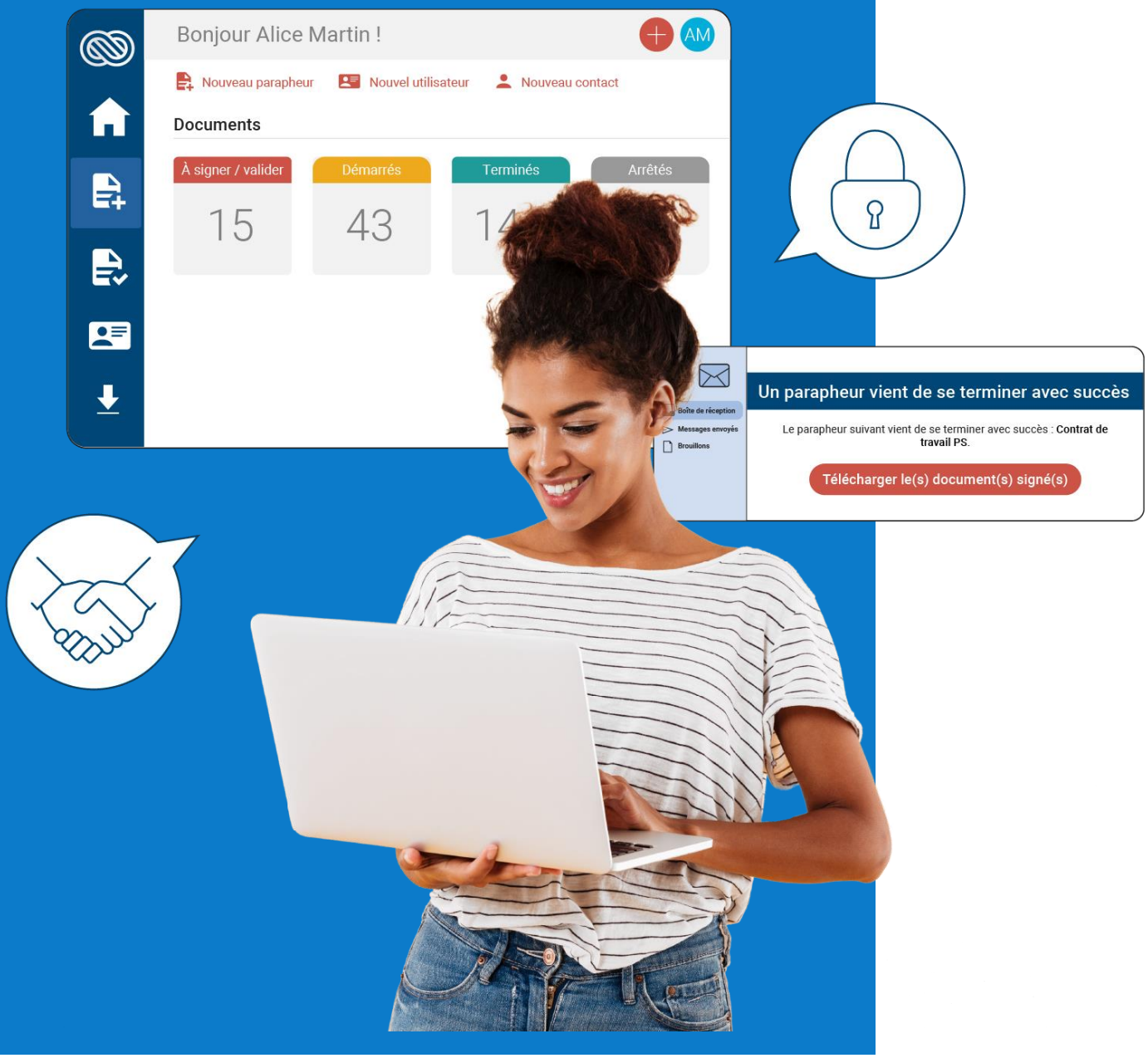


Table des matières

1 – Introduction

Ce document présente l'ensemble des fonctionnalités de la solution de Signature électronique Lex Community.

Lex Community est une plateforme de Signature électronique gratuite développée par la société Lex Persona exposant un Portail de signature en mode Web, qui permet de créer et gérer gratuitement des parapheurs électroniques.

Lex Community permet de faire signer électroniquement gratuitement des documents et de produire des Signatures électroniques simples, avancées et qualifiées au sens du règlement (UE) n° 910/2014 du Parlement européen et du conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance, appelé communément « règlement eIDAS » dans la suite du document.

Lex Community propose à ses utilisateurs de bénéficier des dernières innovations technologiques dans les différents services qui composent le processus de Signature électronique, apportant toutes les garanties de performance et de respect des exigences de sécurité, à toutes les étapes du processus.

Lex Community est à ce jour la seule solution française :

- A délivrer des Certificats de signature "à la volée" pour la Signature électronique avancée sur la base d'une authentification du Signataire par FranceConnect ;
- A délivrer des Certificats de signature "à la volée" pour la Signature électronique qualifiée sur la base d'une authentification du Signataire via L'Identité Numérique La Poste.

2 – Glossaire

Autorité de Certification

Entité légale chargée de la création, la délivrance, la gestion et la révocation de Certificats au titre de sa Politique de Certification.

Bi-clé

Combinaison d'une Clé Privée et d'une Clé Publique utilisée pour effectuer des opérations cryptographiques.

Cachet électronique

Signature électronique consistant pour une personne morale à signer électroniquement un Document à l'aide d'un Certificat et d'une Clé Privée associée lui appartenant.

Certificat

Ensemble d'informations garantissant l'association entre l'identité d'une personne physique ou morale et une Clé Publique, grâce à une Signature électronique de ces données, effectuée à l'aide de la Clé Privée de l'Autorité de Certification qui délivre le Certificat. Un Certificat contient des informations telles que : la Clé Publique et l'identité de son propriétaire, ses usages autorisés, la durée de vie du Certificat, la Signature électronique du Certificat par l'Autorité de Certification et son identité, etc. Le format standard de Certificat est défini dans la recommandation X.509 v3 et dans la RFC 5280.

Certificat de preuve

Rapport détaillé au format PDF listant les principales caractéristiques d'un Parapheur (informations générales, Étapes, Documents, Validateurs, Signataires, etc.), ainsi que les principaux évènements de son cycle de vie (création, validations, signatures, etc.). Le Certificat de Preuve est disponible tout au long du cycle de vie du Parapheur et il est cacheté électroniquement par la plateforme dès que le Parapheur passe en statut « archivé ». Il est alors dans sa version définitive et infalsifiable.

Clé Privée

Clé d'une Bi-clé d'une entité devant être utilisée exclusivement par cette entité.

Clé Publique

Clé d'une Bi-clé d'une entité pouvant être rendue publique.

Contact

Personne physique qui appartient à l'annuaire d'un Utilisateur (ainsi chaque Utilisateur peut disposer de ses propres Contacts).

Destinataire

Contact faisant l'objet d'une demande de Signature électronique.

Dossier de Preuve

Ensemble des éléments collectés par Lex Community pour l'ensemble des Transactions de signature d'un Parapheur constitué des Fichiers de Preuve relatifs à chaque Transaction ainsi que des éléments permettant de vérifier la traçabilité de la Page de Consentement.

Étape

Étape d'un Parapheur exécutée de manière séquentielle permettant la signature d'un ou plusieurs destinataires.

Favoris

Préférences de recherches sauvegardées par un Utilisateur.

Fichier de Preuve

Fichier XML cacheté et horodaté par Lex Persona, intégré dans un Dossier de Preuve, qui rassemble l'ensemble des éléments constitutifs d'une Transaction de signature électronique au sein d'un Parapheur permettant d'assurer la traçabilité et la preuve de la réalisation des signatures effectuées, et qui peut, le cas échéant, être utilisé en justice aux fins de preuve en cas de litige.

FranceConnect

FranceConnect est une solution d'identification créée par l'État français pour faciliter la connexion à différents services en ligne. Dans le cadre du présent document, FranceConnect est utilisé par Lex Community pour identifier le Signataire via le Fournisseur d'Identité qu'il aura choisi parmi ceux que lui aura proposé FranceConnect.

Groupe

Ensemble d'Utilisateurs bénéficiant de droits et d'autorisations définis spécifiquement pour ce Groupe. Chaque Utilisateur appartient à un seul Groupe.

Jeton d'identité

Donnée électronique produite par un Fournisseur d'Identité et attestant de l'identité d'un Signataire.

Lex Community (LC)

Plateforme de Signature électronique gratuite exposant un portail en mode Web.

L'Identité Numérique de la Poste (L'INLP)

Moyen d'identification électronique conforme au niveau substantiel du règlement eIDAS, avec vérification en face à face de l'identité du titulaire.

Page de Consentement

Ensemble d'écrans exposés par Lex Community permettant au Signataire de visualiser et/ou de télécharger les Documents présentés, d'approuver les CGU et d'exprimer explicitement son consentement à signer les documents soumis à la Signature électronique, et d'authentifier le Signataire.

Parapheurs

Circuit composé d'une ou plusieurs étape(s) de Signature(s) électronique(s), par un ou plusieurs destinataire(s) en parallèle, d'un ou plusieurs document(s) à signer, accompagné(s) éventuellement d'une ou plusieurs pièce(s) jointe(s).

Politique de Certification

Ensemble de règles, identifié par un nom (OID), définissant les exigences auxquelles une Autorité de Certification se conforme dans la mise en place et la fourniture de ses prestations et indiquant l'applicabilité d'un Certificat à une communauté particulière et/ou à une classe d'applications avec des exigences de sécurité communes. Une Politique de Certification peut également, si nécessaire, identifier les obligations et les exigences portant sur les autres intervenants, notamment les Signataires.

Portail

Interface Web de Lex Community s'exécutant dans un navigateur Internet pour la gestion des Parapheurs, des Contacts, etc.

Profil de signature

Ensemble de paramètres permettant de configurer la signature qui s'appliquera à un document à signer d'un Parapheur, comme le format de signature (PAdES ou XAdES), la conversion depuis un format Microsoft Office, la visualisation obligatoire du document, etc.

Signataire

Personne physique, rattachée ou non à une entité légale, destinataire d'une étape de Signature électronique.

Signature électronique

Opération désignant la signature d'un document numérique par un Signataire. Une Signature électronique peut être une Signature électronique simple, avancée ou qualifiée au sens du règlement eIDAS.

Transaction

Opérations successives ayant pour finalité la Signature électronique d'un ou plusieurs Document(s) adressé(s) par un Utilisateur à un Signataire.

Utilisateur

Personne physique ayant accès à Lex Community.

3 – Abréviations

AC

Autorité de Certification

AE

Autorité d'Enregistrement

ANSSI

Agence Nationale de la Sécurité des Systèmes d'Information

CAdES

CMS Advanced Electronic Signature

CMS

Cryptographic Message Syntax (format de signature issu du standard PKCS#7)

CRL

Certificate Revocation List (en français : LCR)

CSR

Certificate Signing Request

eIDAS

Electronic Identification and Trust Services

ETSI

European Telecommunications Standards Institute

IGC

Infrastructure de Gestion de Clés (en anglais : PKI)

LCR

Liste de Certificats Révoqués (en anglais : CRL)

OCSP

Online Certificate Status Protocol

OTP

One-Time Password

PAdES

PDF Advanced Electronic Signature

PC

Politique de Certification

PDF

Portable Document Format

PKCS

Public Key Cryptographic Standard

PKI

Public Key Infrastructure (en français : IGC)

QCP

Qualified Certificate Profile

QSCD

Qualified Signature Creation Device

SMS

Short Message Service

XAdES

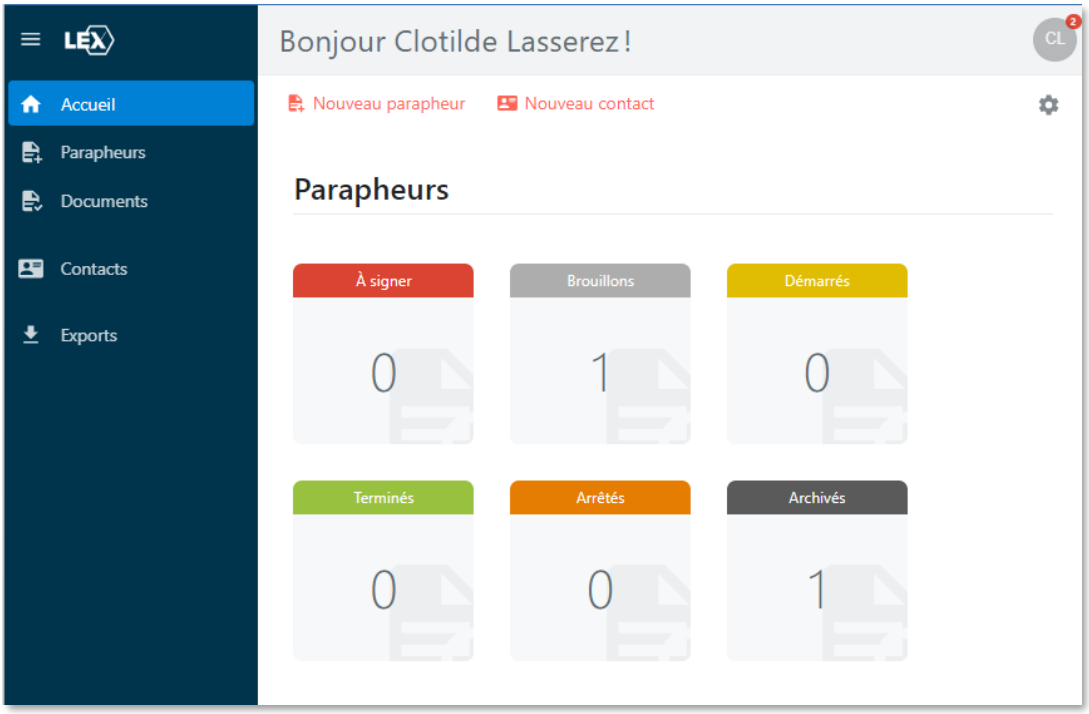
XML Advanced Electronic Signature

XML

Extended Markup Language

4 — Expérience Utilisateur

4.1 — Le tableau de bord



Exemple de tableau de bord d'un Utilisateur

Dès l'ouverture de l'application, l'Utilisateur accède au volet « Accueil » qui se présente sous la forme d'un tableau de bord composé de vignettes personnalisables et de raccourcis.

D'un simple coup d'œil, l'utilisateur visualise immédiatement le nombre de parapheurs selon leur statut. Le tableau de bord de Lex Community aide l'utilisateur à mieux organiser et superviser ses parapheurs.

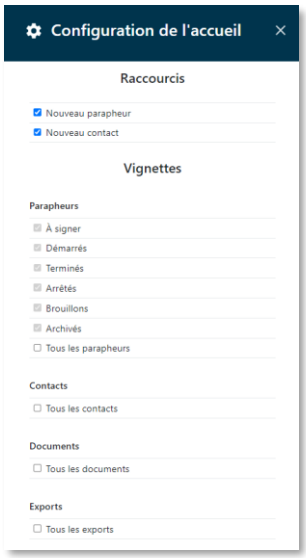
4.1.1 — Les vignettes

Les vignettes sont de type « compteur », c'est-à-dire qu'elles affichent le nombre de résultats selon la requête qu'elles appellent.

A partir d'un bouton de configuration accessible depuis son tableau de bord, l'Utilisateur peut ajouter de nouvelles vignettes :

- Soit en sélectionnant une ou plusieurs vignettes parmi les vignettes mises à sa disposition dans l'outil de configuration ;
- Soit en sélectionnant une vignette créée à partir des préférences de recherche enregistrées par l'Utilisateur, que l'on nomme dans l'application « favoris ».

En effet, dès qu'un nouveau favori est créé par l'Utilisateur, celui-ci peut l'épingler sous forme de vignette sur son tableau de bord.



Page de configuration des raccourcis et des vignettes

Les vignettes standardisées sont les suivantes :
/ À Signer ;
/ Démarrés ;
/ Terminés ;
/ Arrêtés ;
/ Brouillons ;
/ Archivés ;
/ Tous les parapheurs ;
/ Tous les contacts ;
/ Tous les documents ;
/ Tous les exports.

Ces vignettes correspondent pour la plupart aux fonctionnalités de l'application ; ainsi l'Utilisateur y accède facilement.

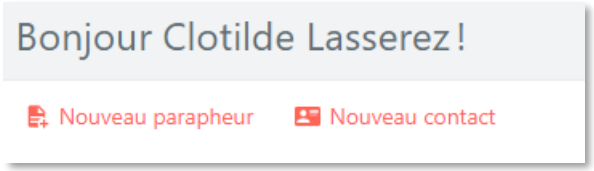
4.1.2 — Les boutons « raccourcis »

Depuis son tableau de bord, l'Utilisateur accède à des boutons d'actions rapide ou raccourcis, lui permettant de créer directement depuis son tableau de bord les items en question.

Ces raccourcis sont configurables par l'Utilisateur.

Pour cela, un bouton de configuration, accessible depuis son tableau de bord, lui permet d'ajouter de nouveaux « raccourcis ».

Les raccourcis disponibles sont les suivants :



/ Nouveau Parapheur ;
/ Nouveau Contact ;

4.2 — Le menu contextuel

On retrouve également à gauche de l'écran, un menu contextuel ; présent sur toutes les pages du Portail, celui-ci permet à l'Utilisateur d'accéder aux différentes fonctionnalités de l'application.

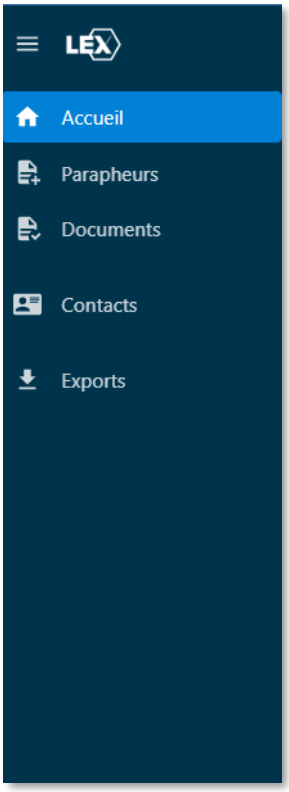
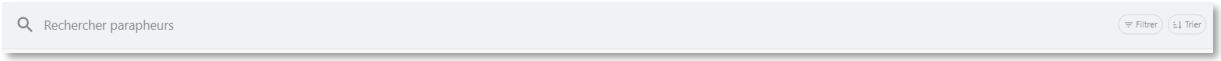


Tableau de bord de l'Utilisateur

4.2.1 — En-tête de recherche

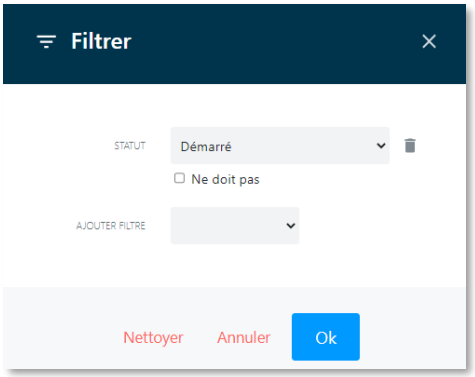
Pour chaque fonctionnalité, un module de recherche par « mot-clé » est disponible.



En-tête de recherche

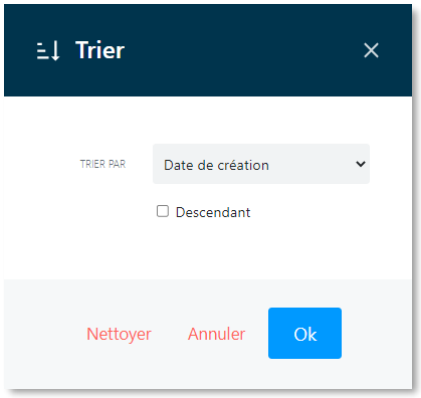
Dans l'objectif d'affiner sa recherche, l'Utilisateur peut utiliser des critères de filtrage : nom, statut, propriétaire, date de création, etc. Chaque champ de métadonnée peut être utilisé comme critère de filtrage.

L'Utilisateur peut ajouter autant de filtres qu'il souhaite :



Exemple de filtre

La liste de résultats peut également être triée. Le tri peut être ascendant ou descendant :



Exemple de tri sur la date de création

Vous pouvez également trier la liste de résultats en cliquant directement sur le nom de la colonne que vous souhaitez trier.

Si vous souhaitez modifier l'ordre de classement (ascendant ou descendant), il vous suffit de cliquer une seconde fois sur la colonne. Une petite flèche symbolise l'ordre du tri.

Un bouton « nettoyer », symbolisé par une petite croix placée à droite de la barre de recherche, permet d'effacer les filtres ou les tris appliqués.

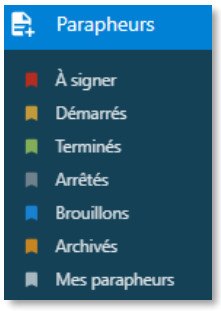
La base de données utilisée est une base Elasticsearch[1], ce qui permet de supporter un très grand nombre de données tout en garantissant des performances optimales en termes d'indexation et de recherche.

4.2.2 — Les favoris

Les préférences de recherche d'un Utilisateur peuvent être enregistrées sous la forme de « favoris ».

Dès qu'un favori est créé, celui-ci sera automatiquement ajouté au niveau du menu contextuel comme sous-volet du volet principal. Cela permet à l'Utilisateur d'accéder facilement aux données enregistrées.

Exemple : je filtre les documents dont je suis le « propriétaire » et je crée le favori « Mes parapheurs ».



Exemple de sous-volet

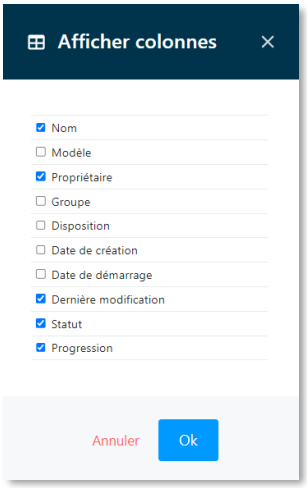
Rappelons également que les « favoris » peuvent être épinglés sur le tableau de bord de l'Utilisateur sous la forme de vignettes.

1 Elasticsearch est une marque de Elasticsearch BV, déposée aux USA et dans d'autres pays. https://www.elastic.co/fr/legal/trademarks

4.2.3 — Paramétrages des colonnes

Pour chaque fonctionnalité, l'Utilisateur peut paramétrer les colonnes qu'il souhaite afficher.

Chaque colonne correspond à une métadonnée. L'Utilisateur peut donc ajouter une colonne correspondant à une métadonnée standard : « nom », « propriétaire », « statut », etc.



Affichage des colonnes

4.3 — Profil Utilisateur

En haut, à droite de l'écran, l'Utilisateur peut accéder à son profil Utilisateur.

A partir de son profil, il accède :

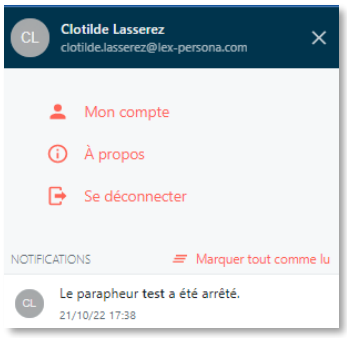
- Aux informations relatives à son compte Utilisateur (Groupe d'Utilisateurs, prénom, nom, courriel, numéro de téléphone mobile, pays, etc.) ;
- Aux notifications qu'il reçoit également par courriel.

L'Utilisateur reçoit une notification en cas de changement de statut d'un Parapheur et lorsqu'un destinataire signe un document.

Lorsqu'une nouvelle notification apparait, le nombre correspondant aux nouvelles notifications s'incrémente.

Nota bene : Un bouton « Marquer tout comme lu » permet d'effacer le nombre de notifications non lues. Les notifications lues restent néanmoins visibles pour l'Utilisateur.

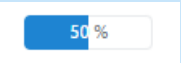
Si l'Utilisateur a le rôle d'administrateur du Tenant, il accède également aux informations du Tenant qu'il administre.



Profil Utilisateur

4.4 — Indicateurs visuels & Boutons d'actions rapide

La solution Lex Community propose des indicateurs visuels et des boutons d'action rapide afin de faciliter la navigation de l'Utilisateur et rendre la solution plus intuitive.

Intitulé	Accessibilité	Bouton
État d'avancement des Parapheurs précisée en pourcentage et matérialisée par une barre d'avancement	Liste des Parapheurs & détail du Parapheur, onglet « Général »	
Statut du Parapheur caractérisé par un code couleur	Liste des Parapheurs & détail du Parapheur, onglet « Général »	
Bouton « œil » pour visualiser les détails d'un item et le modifier si nécessaire	Liste des Parapheurs	
Bouton « Corbeille » pour supprimer un Parapheur	Liste des Parapheurs & détail du Parapheur, onglet « Opérations »	
Bouton « + » pour créer un nouvel item	Tout volet de la solution	
Affichage du nombre de notifications non lues	Profil Utilisateur	

Nota bene : Des boutons « aide » ou « helpers » ponctuent la navigation de l'Utilisateur et l'aident à utiliser la solution de manière autonome et intuitive.

4.5 — Langue de l'interface

La solution est disponible en deux langues : le français et l'anglais.

Le choix de la langue ne se fait pas à partir du profil Utilisateur. En effet, l'application détecte la langue configurée dans le navigateur du Portail Utilisateur ou la Page de Consentement du Signataire.

Ainsi si la langue du navigateur est le français, l'interface de la plateforme sera en français.

La langue de l'Utilisateur est automatiquement enregistrée dans les préférences de l'Utilisateur lorsqu'il se connecte au Portail ou lorsqu'un Signataire accède à la page d'invitation.

4.6 — Mobilité

Lex Community est une solution Full Web compatible avec la plupart des navigateurs : Edge, Firefox, Chrome, Opera et Safari.

Toutes les pages de la solution Lex Community, telles que les pages de consentement sont « Responsive Web Design » et s'adaptent automatiquement à la taille de l'écran du Signataire.

Avec Lex Community la Signature électronique peut s'effectuer depuis tout type de dispositif : PC, Mac, smartphones et tablettes.

5 — Concepts fondamentaux

5.1 — Gestion des contacts

5.1.1 — Qu'est-ce qu'un Contact ?

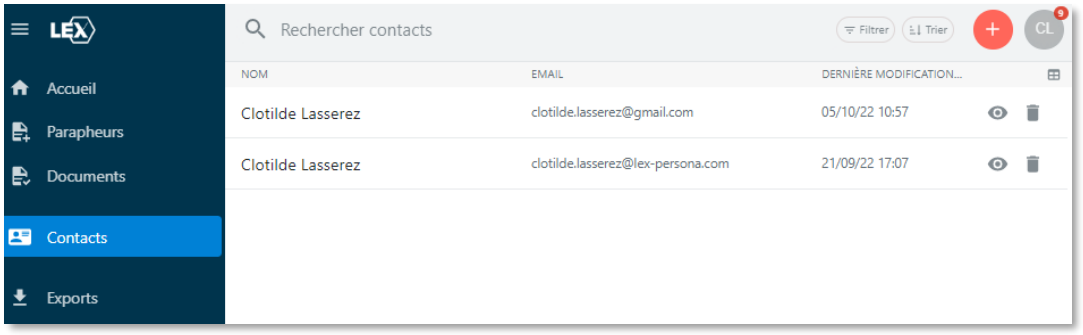
Un Contact est une personne physique qui appartient à l'annuaire privé d'un Utilisateur.

Chaque Utilisateur peut créer les Contacts qu'il souhaite et constituer son annuaire privé.

Chaque Utilisateur dispose de ses propres Contacts et ne peut pas les partager avec d'autres Utilisateurs.

Lors de la création d'un Parapheur, l'Utilisateur peut sélectionner un Contact comme Signataire du Parapheur. L'Utilisateur peut également le créer à la volée

En constituant un annuaire de Contacts, l'Utilisateur n'aura pas à ressaisir les informations d'identité des personnes qu'il fait signer ; celles-ci seront disponibles depuis son annuaire de Contacts.



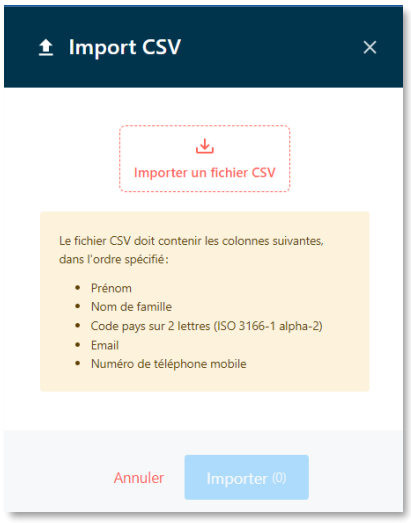
Liste des Contacts

5.1.2 — Import des Contacts

La solution Lex Community permet d'importer vos Contacts grâce à l'import d'un fichier .CSV.

Un bouton en forme de flèche ascendante, en bas de la page, vous permet de réaliser cet import.

Le fichier doit contenir les colonnes spécifiées ci-dessous :

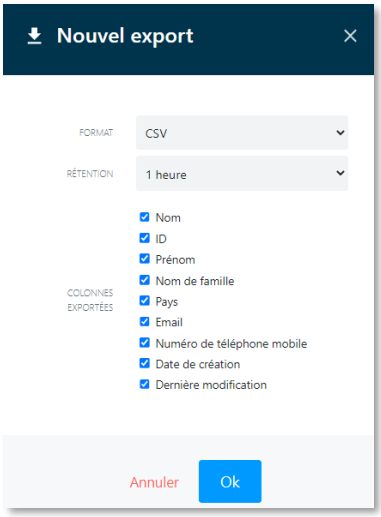


Import des Contacts

5.1.3 — Export des Contacts

La solution Lex Community vous permet également d'exporter vos Contacts sous format JSON ou CSV.

Un bouton en forme de flèche descendante, en bas de la page, vous permet de réaliser cet export.



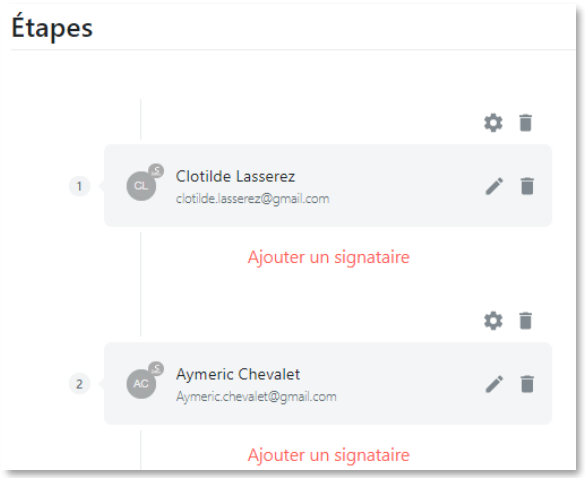
Export des Contacts

Se reporter au chapitre 6.1 « Export des données ».

5.2 — Parapheurs

Dans la solution Lex Community, il est très facile de créer des circuits de Signature(s) électronique(s) appelés Parapheurs. Le terme Parapheur est traduit dans la version anglaise par « Workflow ».

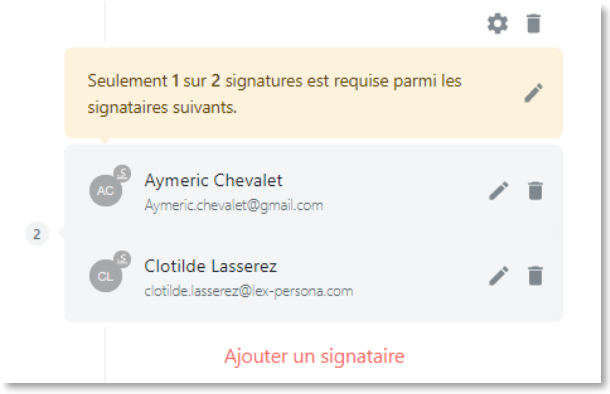
La solution permet d'ajouter des étapes de signature séquentielles.



Exemple de deux étapes séquentielles

Au sein d'une étape, il est possible de faire signer plusieurs destinataires en parallèle. Il est également possible de définir le nombre de Signataires qui doivent signer.

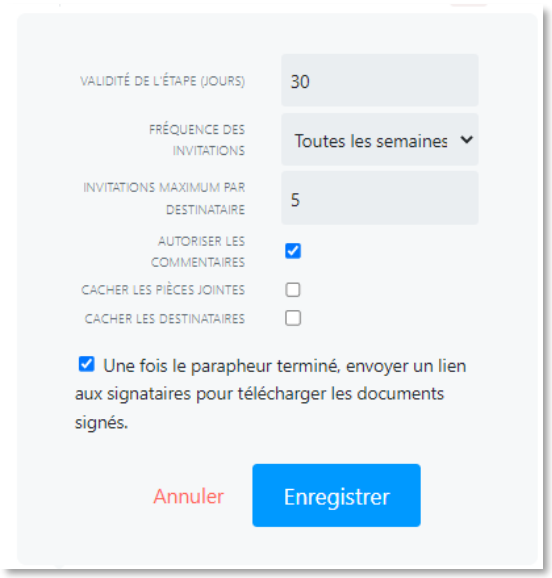
Exemple : sur deux signatures, une seule signature sera requise pour passer à la prochaine étape.



Exemple de deux étapes de signature en parallèle

Chaque étape est caractérisée par :

- La nature de l'étape : signature ;
- La Page de Consentement (qui définit comment la signature doit se dérouler) ;
- Les destinataires : un ou plusieurs Contact(s) (qui définit QUI doit signer) ;
- La durée de validité d'une étape au-delà de laquelle elle expirera : lorsqu'un Utilisateur ajoute une étape de signature, il peut définir la durée de validité de cette étape. Lorsque cette durée est atteinte, alors l'étape de signature devient obsolète ;
- La fréquence d'envoi des invitations : tous les jours, toutes les semaines, toutes les deux semaines, tous les mois ;
- Le nombre de relances maximum ;
- La possibilité d'envoyer un courriel à la fin du circuit contenant un lien de téléchargement des documents signés ;
- La possibilité d'autoriser les commentaires pour les Signataires de l'étape ;
- La possibilité de cacher les pièces jointes aux Signataires de l'étape ;
- La possibilité de cacher les destinataires aux Signataires de l'étape, si la case est cochée, le Signataire ne verra que l'étape qui le concerne et non l'ensemble des étapes qui ont été paramétrées.



Exemple des caractéristiques d'une étape de signature

Lors du paramétrage d'une étape, il est possible de sélectionner pour le destinataire de l'étape la langue préférée parmi la liste proposée : le français ou l'anglais.

Il est possible d'ajouter, de modifier ou de supprimer des étapes d'un Parapheur tant qu'elles ne sont pas terminées.

Nota bene : Lorsqu'un Parapheur est terminé, il est possible d'ajouter des nouvelles étapes et de le relancer.

5.3 — Page de Consentement

Une Page de Consentement est un ensemble de paramètres permettant de configurer le parcours de signature d'un destinataire.

La plateforme Lex Community propose 5 types de parcours correspondant chacun à un niveau de Signature électronique et un mode d'authentification.

Ce concept est essentiel, car c'est ce qui va vous permettre d'adapter la facilité de signer de votre destinataire à l'enjeu juridique et sécuritaire de sa Signature électronique.

Vous trouverez ci-dessous les 5 pages de consentement définies par la plateforme :

- Signature électronique simple avec authentification par courriel : vous déclarez le nom et le prénom du signataire et son adresse courriel. Seule l'adresse est vérifiée par le biais d'un code envoyé par courriel au signataire qui doit le saisir au moment de signer. La signature est saisie graphiquement et fait l'objet Cachet électronique[2] au nom de Lex Persona.
- Signature électronique simple avec authentification SMS : vous déclarez le nom et le prénom du signataire, son adresse courriel et son numéro de mobile. Seul le numéro de mobile est vérifié par le biais d'un code envoyé par SMS au signataire qui doit le saisir au moment de signer. La signature est saisie graphiquement et fait l'objet d'un Cachet électronique au nom de Lex Persona.
- Signature électronique avancée avec authentification SMS : vous déclarez le nom et le prénom du signataire, son adresse courriel et son numéro de mobile, et vous vous engagez

[2] Vous trouverez la définition de « Cachet électronique » dans le Glossaire.

à vérifier sa pièce d'identité. Seul le numéro de mobile est vérifié par le biais d'un code envoyé par SMS au signataire qui doit le saisir au moment de signer. La signature est saisie graphiquement et fait l'objet d'une Signature électronique au nom du signataire.

- Signature électronique avancée avec authentification via FranceConnect : vous déclarez le nom et le prénom du signataire, et son adresse courriel. Le signataire est invité à s'authentifier via FranceConnect au moment de signer, aucune information confidentielle n'est conservée mais les nom et prénom du signataire doivent correspondre très précisément (seuls les nom et premier prénom sont comparés). La signature est saisie graphiquement et fait l'objet d'une Signature électronique au nom du signataire.
- Signature électronique qualifiée avec authentification via L'Identité Numérique La Poste : Vous déclarez le nom et le prénom du signataire, et son adresse courriel. Le signataire est invité à s'authentifier via son application L'Identité Numérique La Poste en indiquant son numéro de téléphone portable au moment de signer, aucune information confidentielle n'est conservée mais les nom et prénom du signataire doivent correspondre très précisément (seuls les nom et premier prénom sont comparés). La signature est saisie graphiquement et fait l'objet d'une Signature électronique au nom du signataire.

5.4 — Profil de signature

Un Profil de signature est un ensemble de paramètres permettant de configurer les signatures qui s'appliqueront aux documents d'un Parapheur.

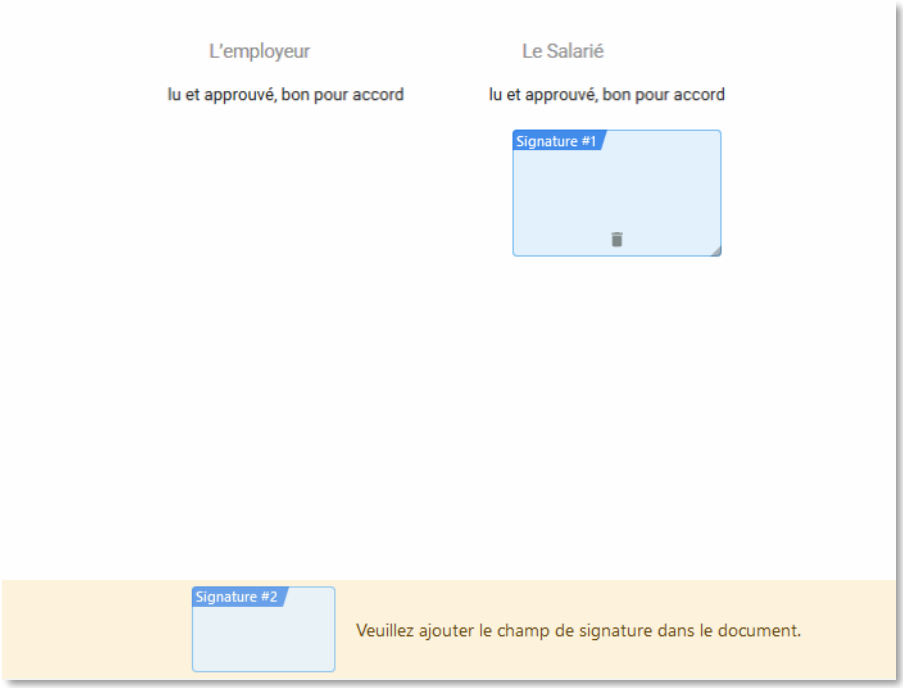
Le Profil de signature utilisé par Lex Community, est défini ainsi :

- Le format de signature : PAdES ;
- La possibilité pour le créateur du parapheur de positionner les champs de signature visible sur les documents PDF ;
- La visualisation obligatoire du document avant signature ;
- Le texte de signature visible qui fait apparaître :
  - Signé électroniquement par [prénom et nom du signataire] ;
  - Le [date au format jour/mois/année] à [heure:minute].

5.4.1 — Positionnement des champs de signature visible

Après avoir téléversé le document à signer, l'Utilisateur doit positionner par glisser/déposer les champs de signature visible dans le document PDF (dans le cas du format PAdES)

Il positionne autant de champs de signature que d'étapes de signature paramétrées.



Positionnement des champs de signature

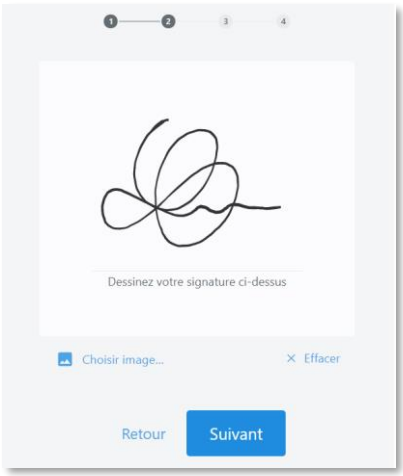
Dans cet exemple, l'Utilisateur doit positionner le deuxième champ de signature.

5.4.2 — Signature visible

Le Signataire, au moment de l'acte de signature d'un document paramétré pour recevoir des signatures visibles, se verra offrir deux possibilités :

- Import d'une image de signature ;
- Dessin de la signature manuscrite sur écran tactile ou à la souris.

Par ailleurs, l'image est enregistrée dans le "local storage" du navigateur Internet du Signataire pour lui permettre de réutiliser cette image pour ses prochaines signatures.



Page de définition de la signature visible

Une griffe de signature apposée sur un document n'a aucune valeur légale, dans la mesure où il s'agit d'une simple image incorporée dans un document. Une griffe de signature intégrée à une signature PAdES d'un document PDF n'a pas non plus de valeur légale en soit, mais elle est protégée dans son intégrité, par la signature électronique à laquelle elle est associée. La

Signature électronique à valeur légale du document est le résultat de plusieurs opérations cryptographiques invisibles pour l'Utilisateur.

Nota bene : Pour garantir une valeur probatoire à la Signature électronique, Lex Community ne propose pas de griffe de signature avec une image sans que celle-ci soit associée à une Signature électronique. Autrement dit, s'il est nécessaire de faire figurer plusieurs signatures visibles sur un document, il est alors nécessaire de prévoir autant de Signatures électroniques.

5.4.3 — Visualisation obligatoire ou non du document

Tant que l'Utilisateur n'a pas parcouru le document, il ne peut pas accéder à la Page de Consentement. Si la visualisation obligatoire du document n'est pas activée, la Page de Consentement s'ouvre directement.

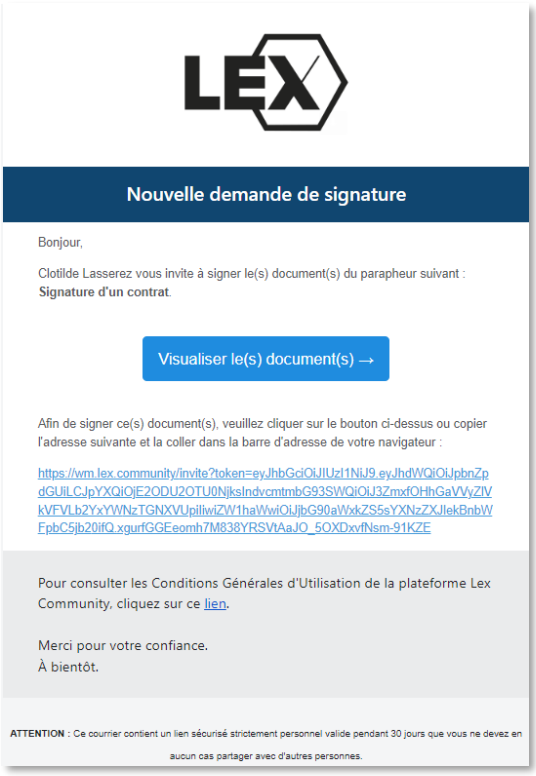
En permettant au Signataire de visualiser les documents à signer, Lex Community respecte le principe du « What You Sign Is What You See ». Attention néanmoins à la présence possible de pièces jointes incorporées à un document PDF qui ne peuvent être affichées dans le visualiseur intégré à la solution.

Les visualisations obligatoires des documents, effectuées par les Signataires, sont tracées dans le Fichier de Preuve de la Transaction.

6 — Personnalisation

6.1 — Invitations

Dans le cas d'une requête de signature transmise par courriel par la plate-forme, le Signataire accède à la page de Signature électronique en cliquant sur le lien fourni, comme présenté dans l'exemple ci-dessous :

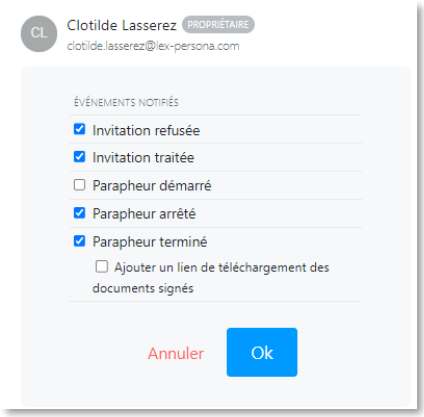


Exemple de notification reçue par courriel – Requête de Signature électronique

6.2 — Notifications par courriel

L'utilisateur peut définir sur quels événements il souhaite être notifié par courriel et au niveau du portail :

- Invitation traitée ;
- Invitation refusée ;
- Changement de statut du Parapheur.

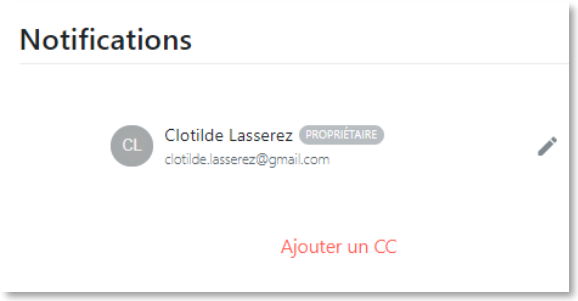


Paramétrage des événements des notifications

6.2.1 — Fonction de partage des Parapheurs

L'Utilisateur peut également ajouter des contacts en « copies carbones » et définir sur quels évènements ils doivent être notifiés.

Cette fonctionnalité permet d'informer, le cas échéant, l'utilisateur et les contacts des actions les plus récentes réalisées au niveau des parapheurs.

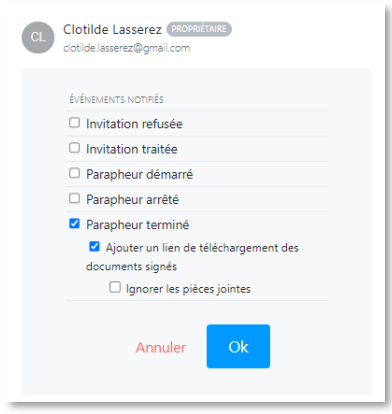


Ajout d'un d'un CC

Lorsqu'un Utilisateur ajoute une « copie carbone », il saisit uniquement l'adresse courriel du destinataire (qui peut être ou ne pas être un Contact préalablement enregistré) ; le destinataire reçoit alors des notifications par courriel.

Nota bene : Lorsqu'un Utilisateur notifie une « copie carbone » d'un Parapheur terminé, il peut également ajouter à cette notification un lien de téléchargement des documents signés.

Une option lui permet d'ignorer les pièces jointes

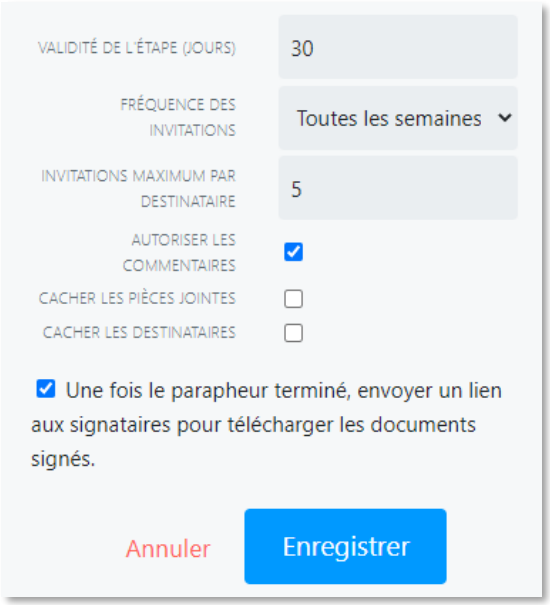


Paramétrage des événements notifiés

6.2.2 — Relances automatiques

La solution permet l'envoi de notifications par courriel pour relancer le Signataire des invitations qu'il doit traiter.

Lors de la création du Parapheur, l'Utilisateur peut définir la fréquence des relances ainsi que le nombre maximum de relances.



Paramétrage des relances des notifications au niveau d'une étape d'un Parapheur

6.3 — Description du Parapheur

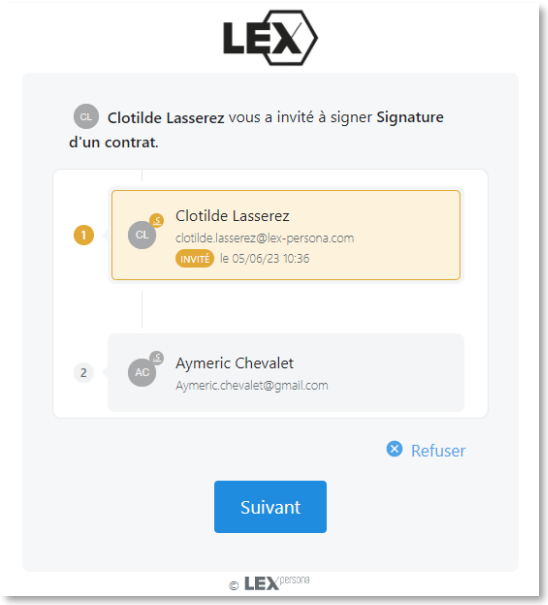
Un Utilisateur peut ajouter un commentaire multilignes pour décrire un Parapheur. Cette description apparait dans la page d'invitation du Parapheur concerné.

7 — Collaboration et automatisation

7.1 — Page de Signature électronique

Lorsqu'un Utilisateur accède à une page de Signature électronique, il peut accéder à l'ensemble des étapes du Parapheur. Il visualise ainsi les étapes qui précèdent et qui vont suivre son étape.

Nota bene : Il est possible pour l'Utilisateur de masquer ces étapes et de ne permettre à l'Utilisateur de visualiser uniquement que l'étape qui le concerne. Ceci se paramètre au niveau de l'étape.



Exemple d'une page d'invitation

L'Utilisateur a la possibilité de refuser une demande de Signature électronique.

Lorsqu'il refuse une demande, il a l'obligation de motiver son refus par un commentaire.

Ce commentaire est visible au niveau des étapes du Parapheur.

Refus de signature

7.2 — Multi-signatures

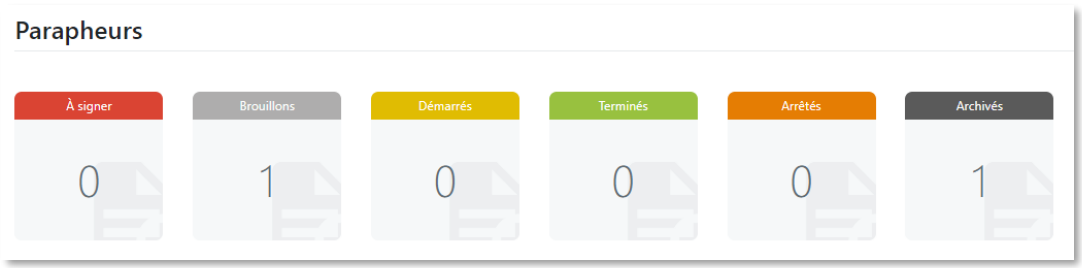
Il n'existe pas de limite sur le nombre de Signataires.

A noter qu'à partir d'une trentaine de Signatures électroniques, des répercussions sur les performances peuvent néanmoins être ressenties.

De plus si vous téléversez un document qui comporte déjà des Signatures électroniques, la solution va conserver ces signatures et les autres signatures s'ajouteront à la suite de ces signatures existantes.

7.3 — Suivi des Parapheurs

À partir du volet « Accueil », l'Utilisateur accède à un tableau de bord à partir duquel il peut visualiser le nombre de Parapheurs selon leur statut ou selon d'autres critères personnalisés.



Affichage des vignettes

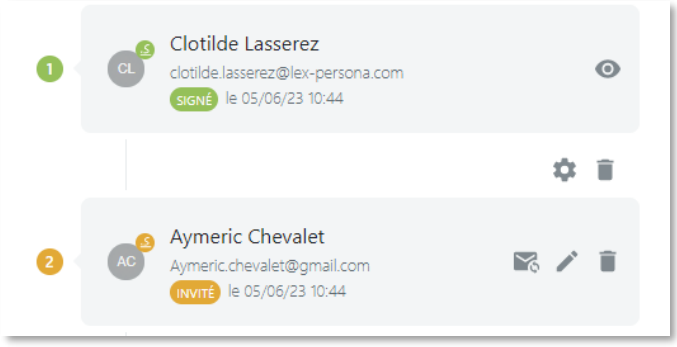
À partir du volet « Parapheurs », l'Utilisateur accède à la liste des Parapheurs et peut accéder d'un simple coup d'œil au statut d'avancement et à la progression du Parapheur.

Le statut d'avancement du Parapheur peut être dans l'un des 3 états suivants :

- Brouillon : le Parapheur est en cours de création ;
- Démarré : le Parapheur a été lancé par l'Utilisateur ;
- Arrêté : soit il a été volontairement arrêté par l'Utilisateur, soit des Signataires ont refusé de signer ;
- Terminé : toutes les étapes du Parapheur se sont terminées avec succès ;
- Archivé : le parapheur a été archivé par l'Utilisateur afin d'interdire toute modification d'un parapheur.

De plus, pour chaque Parapheur, l'Utilisateur peut suivre en temps réel l'état d'avancement des circuits de signature.

Des indicateurs visuels mettent en évidence le statut des étapes : « invité », « signé », etc.



Détail des étapes avec indicateurs visuels

L'Utilisateur peut consulter et modifier les informations relatives à un Parapheur avant de le lancer, pendant et après son exécution.

7.4 — Documents et pièces jointes

Pour téléverser un document, l'Utilisateur peut utiliser la fonction « explorateur de fichiers » ou effectuer un « glisser/déposer ».

Deux encarts sont mis à disposition, l'un pour ajouter les documents à signer, le second pour ajouter les pièces jointes.

Encarts dédiés pour l'ajout des documents et des pièces jointes

Les pièces jointes sont présentées au Signataire en visualisation et en téléchargement mais ne sont pas signées.

Nota bene : en tant que créateur du Parapheur, je peux masquer les pièces jointes aux destinataires d'une étape. Ceci se paramètre au niveau de l'étape.

L'Utilisateur peut également ajouter des dossiers compressés, qui seront décompressés automatiquement par la solution (si la case « Décompresser les zips » est activée).

Une fonction permet également de créer un dossier zippé contenant l'ensemble des documents et des pièces jointes téléversés.

Il est possible d'ajouter ou de supprimer des documents tant que la première Signature électronique n'a pas été réalisée.

À chaque document téléversé dans la solution sont associées des informations qui sont les suivantes :

- Lien vers le Parapheur associé au document ;
- Propriétaire du Parapheur associé au document (information disponible également au niveau du Parapheur) ;
- Groupe du propriétaire du Parapheur associé au document (information disponible également au niveau du Parapheur) ;
- Date de création ;
- Date de dernière modification.

Les documents téléversés sont accessibles depuis la fonctionnalité « Documents » du menu contextuel.

A partir du volet « Documents », l'Utilisateur peut accéder aux informations des documents et les télécharger.

Les documents associés à chaque Parapheur sont également accessibles depuis le menu « Parapheurs ».

7.5 — Conversion des fichiers au format PDF

La solution permet de convertir automatiquement les documents PDF ainsi que les documents MS Office (Word, Excel et Powerpoint) en PDF/A lorsqu'ils sont téléversés dans un Parapheur.

Si le document PDF contient déjà des Signatures électroniques, il n'est pas converti en PDF/A afin que ces Signatures électroniques ne soient pas supprimées.

Le format PDF/A est une version normalisée ISO du format PDF, spécialisée pour l'archivage et la conservation à long terme des documents numériques. Ce format garantit une stabilité sémantique des documents.

7.6 — Opérations liées au Parapheur

Dans le détail du Parapheur, l'Utilisateur accède à différentes opérations.

7.6.1 — Démarrer un Parapheur

Lorsqu'un Parapheur a été paramétré (métadonnées, étapes, documents et notifications), alors l'Utilisateur peut le lancer.

Un Parapheur qui ne contient pas de documents ne pourra pas être démarré. L'opération ne sera pas disponible à l'écran.

Bouton pour démarrer un Parapheur

7.6.2 — Dupliquer un Parapheur

Lorsqu'un Utilisateur crée un Parapheur, il a la possibilité de dupliquer un Parapheur. L'ensemble des informations liées au Parapheur (étapes, notifications, documents) sont alors dupliquées. L'Utilisateur est invité à donner un nouveau nom au Parapheur.

Bouton pour dupliquer un Parapheur

7.6.3 — Supprimer un Parapheur

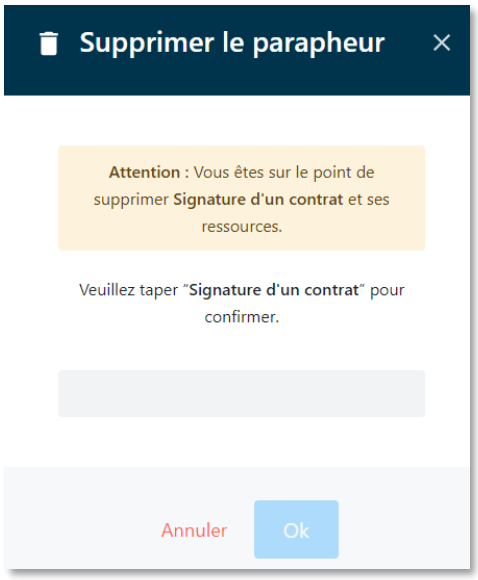
Lorsqu'un Parapheur n'a pas encore été lancé, tout Utilisateur peut supprimer un Parapheur à partir d'un bouton dédié.

Ce bouton est disponible dans la section « Opérations » de chaque Parapheur ».

Bouton pour « supprimer le Parapheur »

Lorsqu'un Utilisateur souhaite supprimer un Parapheur, un message s'affiche, lui demandant de confirmer son souhait de suppression.

L'Utilisateur doit saisir le nom du Parapheur qu'il souhaite supprimer afin de valider l'action de suppression.



Message de confirmation de suppression

7.6.4 — Arrêter le Parapheur

L'utilisateur peut volontairement stopper l'exécution d'un Parapheur. Le statut du Parapheur passe de « démarré » à « arrêté ».

Bouton pour « arrêter le Parapheur »

7.6.1 — Archiver le Parapheur

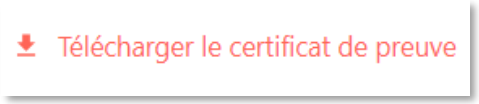
Ce bouton permet à l'utilisateur d'archiver le Parapheur afin de finaliser et interdire toute modification dudit Parapheur. Cette action est irréversible.

Bouton pour « Archiver le parapheur »

7.6.1 — Télécharger le Certificat de Preuve

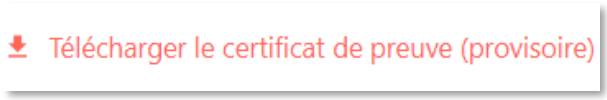
Lorsqu'un Parapheur est terminé, l'utilisateur peut télécharger le Certificat de Preuve associé. Ce fichier au format PDF détaille les principales caractéristiques d'un Parapheur (informations générales, Étapes, Documents, Validateurs, Signataires, etc.), ainsi que les principaux évènements de son cycle de vie (création, validations, signatures, etc.).

Le Certificat de Preuve est disponible tout au long du cycle de vie du Parapheur et il est cacheté électroniquement par la plateforme dès que le Parapheur passe en statut « archivé » (voir également la section ci-dessous « Archivage »).



Bouton pour « Télécharger le Certificat de Preuve »

Tant que le parapheur n'est pas archivé, le Certificat de Preuve est déclaré « provisoire ».



Bouton pour « Télécharger le certificat de preuve (provisoire) »

7.7 — Gestion des absences

Pour répondre à la problématique des absences, la solution permet de :

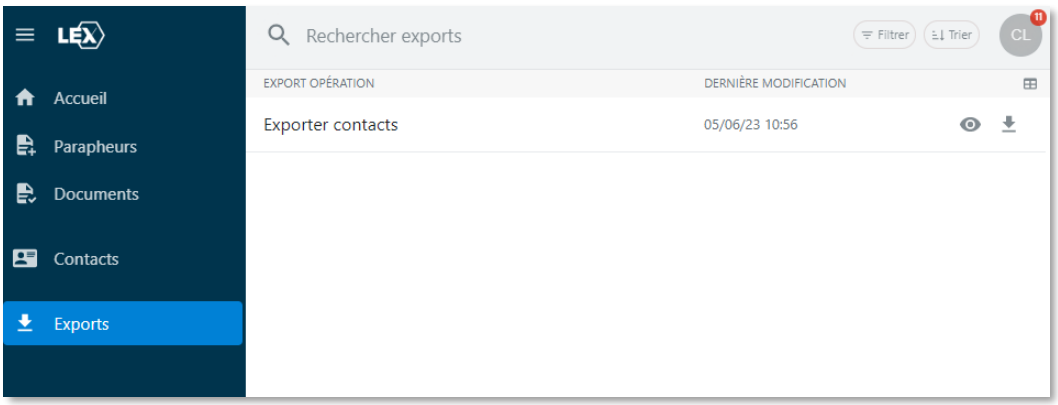
- Modifier à tout moment le circuit d'un Parapheur en cours d'exécution, en remplaçant un Signataire (qui n'a pas encore signé) par un autre Signataire ;
- Paramétrer des étapes dites « suffisantes », en mettant une liste de Signataires potentiels pour une étape et de limiter le nombre de Signatures électroniques attendues pour passer à l'étape suivante et/ou clôturer le Parapheur s'il s'agit de la dernière étape.

7.8 — Exports des données

Chaque volet de la solution propose l'export de ses données.

Pour chaque export il est possible de définir une durée de rétention, pendant cette durée tous les exports effectués sont accessibles dans le menu Exports.

Un export peut être sous format JSON ou CSV.



Liste des exports

7.9 — Fil de discussion & commentaires

Cette fonctionnalité permet à l'Utilisateur ou à un destinataire de Parapheur de créer un fil de discussion à l'attention de l'Utilisateur ou des autres destinataires d'un Parapheur.

Par défaut, un fil de discussion, à l'initiative d'un Utilisateur est public, c'est-à-dire qu'il est visible de l'Utilisateur mais également des destinataires du Parapheur qui visualisent les commentaires au moment de la signature.

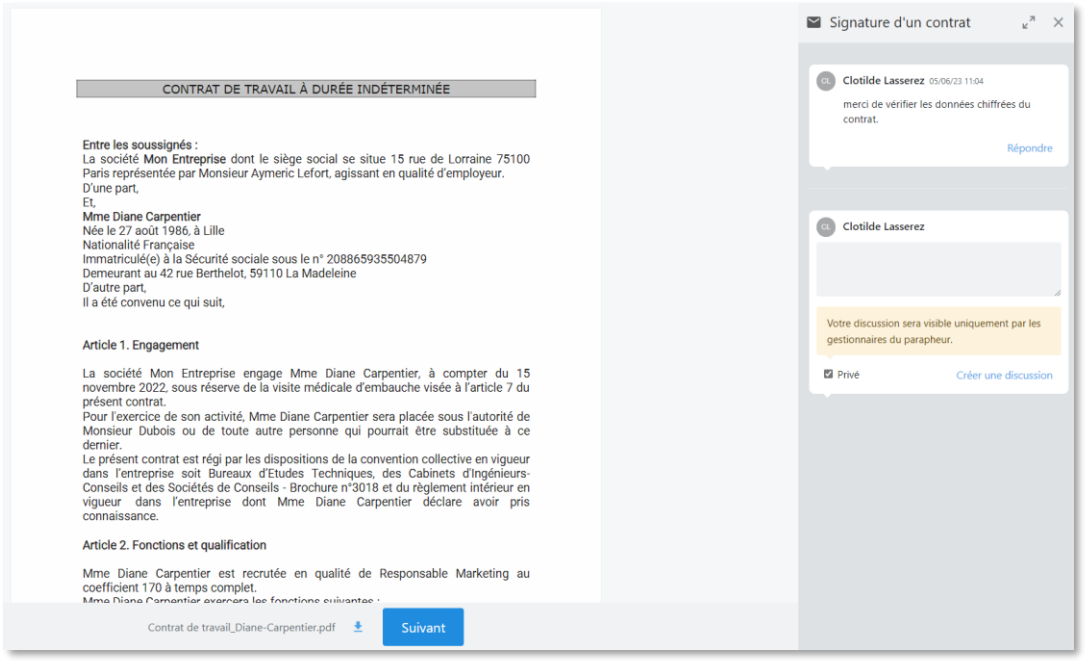
Si ce fil de discussion est rendu privé par l'Utilisateur, il ne sera visible que par l'utilisateur lui-même.

Les destinataires d'un Parapheur peuvent répondre à un fil de discussion existant mais également en créer de nouveaux.

Lorsqu'il est créé par un Signataire, un fil de discussion est privé par défaut, c'est-à-dire qu'il n'est visible que par lui et l'Utilisateur. Lorsqu'il est public, alors tous les destinataires peuvent voir les commentaires.

Par défaut, un fil de discussion créé par un destinataire est privé, de manière à garantir la confidentialité du commentaire.

Le fil de discussion s'affiche dans un volet, à droite de l'interface.



Exemple d'un fil de discussion sur une page d'invitation de signature

Nota bene : Lorsque l'Utilisateur visualise un document, le fil de discussion reste visible à l'écran, afin de permettre à l'Utilisateur de consulter à le fois le contenu des documents et celui des commentaires dans un même écran. Ainsi la prise en compte des commentaires par les Utilisateurs est facilitée, notamment lorsque lesdits commentaires visent une modification du contenu des documents.

8 — Les Signatures électroniques de Lex Community

8.1 — Exposé des principes techniques de la Signature électronique

Avant d'aborder les différents types de Signatures électroniques proposés par Lex Community nous allons tout d'abord rappeler dans cette section quelques principes techniques de base qui sont à l'origine de la conception de la Signature électronique dans les années 90 et qui sont toujours aujourd'hui couramment utilisés dans le contexte des Signatures électroniques de niveaux avancé et qualifié du règlement eIDAS.

Ces principes techniques posent comme prérequis la nécessité pour le Signataire de disposer au préalable d'un Certificat de Signature électronique. Il existe de nombreux types de Certificats destinés à différents usages (serveur Web, code signing, authentification, etc.), mais dans le cas de Lex Community, nous ne nous intéressons qu'aux Certificats de Signature électronique.

Ce Certificat de Signature électronique contient d'une part l'identité du Signataire et d'autre part une Clé Publique, qui est une donnée mathématique aléatoire associée de manière unique au Signataire, et qui est l'équivalent de la griffe de sa signature manuscrite. L'Autorité de Certification, qui délivre le Certificat, garantit l'association entre l'identité du Signataire et la Clé Publique, d'où l'importance du processus de vérification de l'identité du Signataire et de l'unicité de la Clé Publique.

A noter que le Certificat de Signature électronique est signé électroniquement par l'Autorité de Certification qui en garantit ainsi son intégrité et son authenticité.

A la Clé Publique, située dans le Certificat, est mathématiquement liée une Clé Privée, également unique, qui permet de chiffrer l'empreinte du document à signer. C'est le résultat du calcul cryptographique ainsi réalisé qui constitue la Signature électronique du document et qui va ainsi permettre de garantir son intégrité, et, par le biais de la Clé Publique et du Certificat, garantir son lien avec le document auquel elle se rattache. Ainsi, la protection de la Clé Privée est essentielle et son contrôle exclusif par le Signataire qui l'active par un moyen d'authentification au moment de signer est fondamental. La Clé Privée est donc l'équivalent du geste biométrique qui permet d'apposer la griffe de sa signature manuscrite sur un document papier.

Nota bene : on dit couramment que l'on signe un document à l'aide d'un Certificat, mais il s'agit d'un raccourci qui peut prêter à confusion. En effet, on signe un document à l'aide de la Clé Privée associée à la Clé Publique figurant dans le Certificat. Le fait que le Certificat figure dans le document signé dans la majorité des cas, pour faciliter l'identification et la vérification de la Signature électronique en déchiffrant cette dernière à l'aide de la Clé Publique, ajoute à la confusion.

8.2 — Principes juridiques de la signature électronique

Au plan juridique en France, la Signature électronique obéit à 2 règlementations qui parfois s'opposent et parfois se rejoignent :

- Le règlement eIDAS ;
- L'article 1367 du code civil.

8.2.1 — Les Signatures électroniques du règlement eIDAS

Le règlement eIDAS définit 3 niveaux de Signatures électroniques décrits ci-après.

La Signature électronique « simple » (ce terme n'est pas cité dans le règlement mais il est d'usage courant pour désigner la signature électronique de plus bas niveau), définie par l'article 3 (définition n°10) du règlement, est constituée de « données sous forme électronique, qui sont jointes ou associées logiquement à d'autres données sous forme électronique et que le Signataire utilise pour signer ».

La Signature électronique avancée, définie par l'article 26 du règlement, satisfait aux exigences suivantes : « a) être liée au Signataire de manière univoque ; b) permettre d'identifier le Signataire ; c) avoir été créée à l'aide de données de création de Signature électronique que le Signataire peut, avec un niveau de confiance élevé, utiliser sous son contrôle exclusif ; et d) être liée aux données associées à cette signature de telle sorte que toute modification ultérieure des données soit détectable ».

La Signature électronique qualifiée, définie par l'article 3 (définition n°12) du règlement, est « une Signature électronique avancée qui est créée à l'aide d'un dispositif de création de Signature électronique qualifié, et qui repose sur un Certificat qualifié de Signature électronique ». Le Certificat qualifié de Signature électronique, selon l'article 3 (définition n°15) et l'article 28, est défini par « un Certificat de Signature électronique, qui est délivré par un prestataire de services de confiance qualifié et qui satisfait aux exigences fixées à l'annexe I ». Le dispositif de création de Signature électronique qualifié est défini à l'article 29.

A ces 3 niveaux s'ajoute un 4ème niveau défini spécifiquement pour les services publics à l'article 27 qui consiste à effectuer une Signature électronique avancée reposant sur un Certificat qualifié de Signature électronique.

8.2.2 — La Signature électronique du code civil français

La Signature électronique est définie par l'article 1367 du code civil :

- « La signature nécessaire à la perfection d'un acte juridique identifie son auteur. Elle manifeste son consentement aux obligations qui découlent de cet acte. Quand elle est apposée par un officier public, elle confère l'authenticité à l'acte. » ;
- « Lorsqu'elle est électronique, elle consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache. La fiabilité de ce procédé est présumée, jusqu'à preuve contraire, lorsque la signature électronique est créée, l'identité du Signataire assurée et l'intégrité de l'acte garantie, dans des conditions fixées par décret en Conseil d'Etat. ».

Le décret en question est le décret n° 2017-1416 du 28 septembre 2017 relatif à la Signature électronique, qui indique, en citant le règlement eIDAS :

- « La fiabilité d'un procédé de Signature électronique est présumée, jusqu'à preuve du contraire, lorsque ce procédé met en œuvre une Signature électronique qualifiée » ;
- « Est une Signature électronique qualifiée une Signature électronique avancée, conforme à l'article 26 du règlement susvisé et créée à l'aide d'un dispositif de création de Signature électronique qualifié répondant aux exigences de l'article 29 dudit règlement, qui repose sur un Certificat qualifié de Signature électronique répondant aux exigences de l'article 28 de ce règlement ».

8.3 — Eléments de comparaison des cadres juridiques européen et français

Si on fait une analyse comparative des deux cadres juridiques constitués par le règlement européen eIDAS et du code civil français, on peut faire les remarques suivantes :

- La présomption de fiabilité de la Signature électronique selon le code civil français est acquise dès lors qu'il s'agit d'une Signature électronique qualifiée au sens du règlement eIDAS ;
- Les 2 cadres juridiques sont technologiquement neutres, à l'exception de la Signature électronique qualifiée qui est définie de manière précise par des standards techniques de l'ETSI et qui fait référence aux principes techniques de la Signature électronique exposés dans la première partie de ce chapitre ;
- Les niveaux de Signature électronique simple et avancé ne sont pas connus du code civil français ; le niveau avancé est néanmoins identifié dans certaines procédures administratives telle que la règlementation relative aux marchés publics ;
- Le code civil n'est concerné que par les actes juridiques, qui induisent la notion de consentement aux obligations qui découlent de ces actes ; cette notion de consentement ne relève pas du droit européen, c'est pourquoi elle est absente du règlement eIDAS ;
- En revanche, le règlement eIDAS introduit la notion de Cachet électronique, qui permet de garantir l'intégrité et l'authenticité d'un document par une personne morale.

8.4 — Principes généraux des Signatures électroniques de Lex Community

Avant de présenter les différents types de Signatures électroniques proposées par Lex Community, il est nécessaire de rappeler quelques principes de base relatifs à l'utilisation de la Signature électronique dans le contexte d'un Parapheur électronique qui consiste, pour un Utilisateur, à faire signer un ou plusieurs document(s) à un ou plusieurs Signataire(s). On précise qu'il est possible pour un Utilisateur, le cas échéant, d'être un Signataire dudit Parapheur.

Ainsi la solution prévoit de la part de l'Utilisateur une connaissance supposée *a priori* des interlocuteurs qui vont signer le(s) document(s). Autrement dit, l'identification des Signataires est toujours effectuée par l'Utilisateur qui crée (ou modifie) le Parapheur. Cette identification va toujours consister à fournir *a minima* les informations suivantes :

- Le prénom et le nom du Signataire, qui seront utilisés pour composer le Certificat (dans le cas d'une Signature électronique impliquant la génération d'un Certificat à la volée), ou pour caractériser la Signature électronique simple, et dans tous les cas pour la constitution du Fichier de Preuve ;
- L'adresse courriel du Signataire, qui sera utilisée pour envoyer l'invitation à signer au Signataire.

L'Utilisateur peut renseigner d'autres éléments d'identification du Signataire, de manière obligatoire ou facultative :

- Le pays de naissance du Signataire ou le pays de délivrance de son titre d'identité, qui, selon les cas, pourra être utilisé pour composer le Certificat ;
- Le numéro de téléphone du signataire, qui sera utilisée pour envoyer le code OTP SMS au Signataire.

Toutes ces informations sont par conséquent des données qui peuvent être utilisées en tout ou partie par Lex Community, lors du parcours de consentement effectué par le Signataire, afin d'authentifier ce dernier en vue de la génération d'un Certificat et de la réalisation de la Signature électronique des documents à signer.

Ainsi, la section 3.1.1. de la Politique de Certification de l'Autorité de Certification « Sunnystamp Natural Persons CA » décrit la correspondance entre les informations d'identification du Signataire et les informations du Certificat généré consécutivement au processus d'authentification.

A titre de 1er exemple, si le Signataire a été identifié par l'Utilisateur avec « PrénomX NomY » et que le processus d'authentification, qui s'appuie sur FranceConnect, retourne « PrénomZ NomT » (ou toute autre variante différente de l'identification initiale), alors le processus de Signature électronique est obligatoirement interrompu, la cohérence devant être respectée entre les données d'identification et celles résultant du processus d'authentification.

A titre de 2ème exemple, si le Signataire a été identifié par l'Utilisateur avec « PrénomX NomY » et que le processus d'authentification ne s'appuie que sur un OTP envoyé par SMS, alors aucun contrôle n'est effectué par le processus de Signature électronique. Seule une demande de confirmation de l'exactitude des informations relatives à l'identité du Signataire est exigée par ce dernier pour la finalisation du processus de signature des documents.

De manière générale, c'est l'identification effectuée par l'Utilisateur qui fait signer le Signataire qui fait foi pour l'élaboration du Certificat généré à la volée par Lex Community et délivré par l'Autorité de Certification « Sunnystamp Natural Persons CA ».

Il existe une exception à ce principe, qui est détaillée ci-après : dans le cas d'une Signature électronique simple, aucun Certificat n'est généré aux nom et prénom du Signataire ; le document est cependant signé à l'aide d'un Cachet électronique qualifié eIDAS effectué à l'aide d'un Certificat au nom de Lex Persona ; dans le cas d'une signature PAdES, la Signature électronique comporte dans le champ motif les nom et prénom du Signataire tels que fournis par l'Utilisateur, ainsi que l'identifiant de la Transaction, cette dernière information étant particulièrement utile pour constituer et vérifier le Fichier de Preuve ;

Des évolutions logicielles sont prévues permettant de configurer et paramétrer Lex Community de manière à appliquer une « normalisation » des nom et prénom du Signataire au niveau des données d'identification fournies par l'Utilisateur comme des données d'authentification retournées par le Fournisseur d'Identité. Cette normalisation doit permettre d'assouplir les règles de comparaison, en particulier en présence de caractères nationaux tels que les caractères accentués (é, ï, â, ñ, etc.), la présence d'espaces, d'apostrophe, de cédille, de majuscules ou minuscules inappropriées, qui font échouer la Transaction de Signature électronique.

8.5 — Principe de la Signature électronique simple avec Lex Community

Dans le cas d'une Signature électronique de niveau simple, Lex Community propose un dispositif qui va beaucoup plus loin en matière de sécurité et d'authentification que la définition de la Signature électronique au sens du règlement eIDAS :

- A chaque Signature électronique simple correspond un Cachet électronique du document, réalisé à l'aide d'un Certificat au nom de « Lex Persona », en lieu et place d'un Certificat de Signature électronique nominatif pour une Signature électronique avancée ou qualifiée ; ce Cachet électronique a pour principal objectif de sécuriser la Transaction de Signature électronique considérée ;

- La Signature électronique produite, de la forme AdES-LT, est un Cachet électronique qualifié au sens du règlement eIDAS, le Certificat au nom de « Lex Persona » étant un Certificat qualifié eIDAS mis en œuvre sur un HSM qualifié QCP-l-qscd ;
- Lorsqu'il s'agit d'une Signature électronique au format PAdES, l'Utilisateur dispose de la possibilité d'associer à cette Signature électronique une image de la griffe de signature du Signataire, qui peut être saisie par le Signataire sur un écran tactile, ou bien téléversée par le Signataire à partir de son dispositif ;
- Toujours lorsqu'il s'agit d'une Signature électronique au format PAdES, le champ motif de cette Signature électronique comporte les nom et prénom du Signataire, ainsi que l'identifiant de la Transaction de Signature électronique qui figure également dans le Fichier de Preuve associé à la Transaction ;
- La Signature électronique est horodatée par le service d'horodatage de Lex Persona ;
- La Signature électronique peut être conditionnée par un mécanisme d'authentification défini au préalable par l'Utilisateur, tel qu'un OTP envoyé par courriel ou par SMS.

8.6 — Principes de la Signature électronique avancée de Lex Community

Dans le cas d'une Signature électronique de niveau avancé, Lex Community propose une Signature électronique qui respecte en tous points le cahier des charges défini par l'article 26 du règlement eIDAS :

- La Signature électronique avancée respecte les principes techniques décrits dans la 1ère section du présent chapitre, c'est-à-dire qu'elle est réalisée à l'aide d'un Certificat délivré au nom du Signataire par l'AC « Sunnystamp Natural Persons CA » ;
- Le Certificat du Signataire comporte ses nom et prénom ainsi que l'identifiant de la Transaction de Signature électronique qui est également contenu dans le Fichier de Preuve de la Transaction ;
- De manière optionnelle, le Certificat peut également comporter, le cas échéant, le code pays du Signataire ; la Politique de Certification de l'AC « Sunnystamp Natural Persons CA » décrit en détail les gabarits des différents types de Certificats proposés pour la signature avancée ;
- Le Certificat est obligatoirement rattaché à une Transaction de Signature électronique donnée et sa durée de vie est de 1h ;
- La Signature électronique produite est de la forme AdES-LT, ce qui signifie que la Signature électronique n'expire pas au-delà de la date de validité du Certificat du Signataire car les informations de révocation du Certificat et de sa chaine complète de certification sont contenues dans la Signature électronique ;
- Lorsqu'il s'agit d'une Signature électronique au format PAdES, l'Utilisateur dispose de la possibilité d'associer à cette Signature électronique une image de la griffe de signature du Signataire, qui peut être saisie par le Signataire sur un écran tactile, ou bien téléversée par le Signataire à partir de son dispositif ;
- Toujours lorsqu'il s'agit d'une Signature électronique au format PAdES, le champ motif de cette Signature électronique comporte les nom et prénom du Signataire, ainsi que l'identifiant de la Transaction de Signature électronique qui figure également dans le Fichier de Preuve associé à la Transaction ;
- La Signature électronique est horodatée par le service d'horodatage de Lex Persona ;

- La Signature électronique est nécessairement conditionnée par un mécanisme d'authentification du Signataire par l'Utilisateur selon différentes méthodes telles que :
  - Une authentification du Signataire via l'envoi d'un code envoyé par SMS, l'utilisateur s'engage à vérifier l'identité du Signataire à partir de la fourniture d'un titre officiel d'identité : Carte Nationale d'Identité, Passeport ou Titre de séjour ;
  - Une authentification du Signataire sur FranceConnect, via le Fournisseur d'Identité de son choix, au cours du processus de Signature électronique et de manière synchrone, va permettre de récupérer les informations relatives à l'identité de ce dernier : dans ce cas le Certificat, à usage unique et d'une durée de validité d'1 (une) heure, est dénommé « FranceConnect » dans la Politique de Certification ; dans le cas où l'identité fournie par l'Utilisateur diffère de l'identité retournée par FranceConnect, le processus de Signature électronique est interrompu et aucun Certificat n'est généré ; parmi les Fournisseurs d'Identité acceptés par FranceConnect nous pouvons citer impots.gouv.fr ou encore Ameli ; à ce jour FranceConnect compte environ 30 millions d'utilisateurs ; la Signature électronique avancée avec FranceConnect peut être particulièrement pertinente pour des Signataires externes au Client.

8.7 — Principes de la Signature électronique qualifiée de Lex Community

Dans le cas d'une Signature électronique de niveau qualifié, Lex Community propose une Signature électronique qui respecte en tous points le cahier des charges défini par le règlement eIDAS.

Tout d'abord elle respecte toutes les caractéristiques d'une Signature électronique avancée :

- La Signature électronique respecte les principes techniques décrits dans la 1ère section du présent chapitre, c'est-à-dire qu'elle est réalisée à l'aide d'un Certificat délivré au nom du Signataire par l'AC « Sunnystamp Natural Persons CA » ;
- Le Certificat du Signataire comporte ses nom et prénom ainsi que l'identifiant de la Transaction de Signature électronique qui est également contenu dans le Fichier de Preuve de la Transaction ; à la différence d'une Signature électronique avancée, le Certificat doit obligatoirement comporter le code pays de naissance du Signataire qui doit être renseigné par l'Utilisateur ;
- Le Certificat est obligatoirement rattaché à une Transaction de Signature électronique donnée et sa durée de vie est de 1h ;
- La Signature électronique produite est de la forme AdES-LT, ce qui signifie que la Signature électronique n'expire pas au-delà de la date de validité du Certificat du Signataire car les informations de révocation du Certificat et de sa chaine complète de certification sont contenues dans la Signature électronique ;
- Lorsqu'il s'agit d'une Signature électronique au format PAdES, l'Utilisateur dispose de la possibilité d'associer à cette Signature électronique une image de la griffe de signature du Signataire, qui peut être saisie par le Signataire sur un écran tactile, ou bien téléversée par le Signataire à partir de son dispositif ;
- Toujours lorsqu'il s'agit d'une Signature électronique au format PAdES, le champ motif de cette Signature électronique comporte les nom et prénom du Signataire, ainsi que l'identifiant de la Transaction de Signature électronique qui figure également dans le Fichier de Preuve associé à la Transaction ;
- La Signature électronique est horodatée par le service d'horodatage de Lex Persona.

De manière spécifique à une Signature électronique qualifiée, le Certificat est généré « à la volée » conformément à la Politique de Certification de l'AC « Sunnystamp Natural Persons CA » en ce qui concerne un Certificat qualifié eIDAS conforme au standard ETSI EN 319 411-2 au niveau QCP-n-qscd.

Afin de pouvoir garantir la conformité du Certificat au standard indiqué ci-dessus, les dispositions suivantes sont réalisées :

- Initialisation d'une Transaction unique de Signature électronique ;
- Acceptation des CGU indiquant au Signataire qu'un certificat sera généré à ses nom et prénom pour les besoins de la Signature électronique des documents de la Transaction et de la Signature électronique desdites CGU ;
- Authentification du Signataire via un moyen d'identification électronique :
  - Ayant fait l'objet d'une notification par l'un des États membres de l'Union européenne, et
  - Ayant un niveau de garantie substantiel ou élevé, et
  - Pour lesquels il est publié une documentation en langue anglaise ou française permettant d'établir, sans ambiguïté, que la présence de la personne physique ou un représentant autorisé de la personne morale est un prérequis à l'obtention de ce moyen d'identification électronique ;
- Dans le cas où l'identité fournie par le Gestionnaire diffère de l'identité retournée par le moyen d'identification électronique, le processus de Signature électronique est interrompu et aucun Certificat n'est généré ;
- Création d'une Bi-clé sur un HSM qualifié QSCD ;
- Génération d'une CSR et délivrance d'un certificat par l'AC « Sunnystamp Natural Persons CA » aux nom et prénom du Signataire, dénommé « MIE eiDAS » dans la Politique de Certification, valable 1 (une) heure, et utilisable uniquement dans le cadre de la Transaction de signature considérée ;
- Signature électronique des documents de la Transaction de Signature électronique considérée ;
- Signature électronique des CGU ;
- Destruction de la Bi-clé.

Pour la Signature électronique qualifiée, le moyen d'identification électronique utilisé est l'application « L'Identité Numérique La Poste » de Docaposte, entreprise avec laquelle Lex Persona a contractualisé afin de permettre aux Signataires qui disposent d'une telle application la possibilité de réaliser ainsi des Signatures électroniques qualifiées au sens du règlement eIDAS. Aujourd'hui plus de 3 millions de français bénéficient déjà de L'Identité Numérique La Poste. Celle-ci s'obtient gratuitement en ligne ou en bureau de poste en moins de 15 minutes. Il suffit de se présenter avec une pièce d'identité en cours de validité et de son smartphone sur lequel on peut recevoir ses courriels.

D'autres moyens d'identifications électroniques conformes au règlement eIDAS, respectant des caractéristiques en matière de sécurité équivalentes ou supérieures, pourront être fournis ultérieurement.

8.8 — Distinction entre les niveaux de Signatures électroniques

Qu'est-ce qui différencie une Signature électronique de niveau simple et de niveau avancé ? Et qu'ont-elles en commun ?

Tout d'abord les 2 niveaux de Signatures électroniques n'offrent pas le renversement de la charge de la preuve. En effet si le Signataire estime qu'il n'a pas signé votre document, ce sera à vous d'en apporter la preuve. Mais rassurez-vous, grâce à la plateforme Lex Community vous pourrez présenter, en cas de litige, le Fichier de Preuve généré par la plateforme : celui-ci contient toutes les informations collectées lors du processus de Signature électronique, l'identité du Signataire ainsi que la manière dont il s'est authentifié, et permet également de garantir l'intégrité et l'authenticité des documents signés.

Voyons maintenant ce qui les distingue :

- Dans le cas d'une Signature électronique simple, il n'y a pas de vérification de l'identité de la personne, les nom et prénom de la personne sont définis par le Gestionnaire lors de la création de l'Utilisateur ou du Contact qui sera Signataire du ou des documents de la Transaction de Signature électronique ; ces informations ne sont pas vérifiés par un quelconque moyen d'authentification indépendant ; de plus, les documents sont signés à cette occasion par un Certificat numérique délivré au nom de Lex Persona et non au nom du Signataire : il est donc difficile de démontrer de manière absolue le contrôle exclusif, par ledit Signataire, de la clé privée du certificat au nom de Lex Persona.
- La Signature électronique avancée est effectuée à l'aide d'un Certificat à usage unique pour la Transaction de Signature électronique considérée, et délivré au nom du Signataire et généré à la volée par l'Autorité de Certification « Sunnystamp Natural Persons CA », qui impose la vérification de l'identité du Signataire, cette vérification étant effectuée soit à l'initiative et sous le contrôle documenté de l'Utilisateur, soit par le biais d'une authentification du Signataire réalisée par l'intermédiaire d'une connexion à l'un des fournisseurs d'identité associés à FranceConnect.
- La Signature électronique qualifiée est également effectuée à l'aide d'un Certificat à usage unique pour la Transaction de Signature électronique considérée, et délivré au nom du Signataire et généré à la volée par l'Autorité de Certification « Sunnystamp Natural Persons CA », qui impose cette fois une vérification stricte de l'identité du Signataire à l'aide d'un processus d'authentification vis-à-vis d'un moyen d'identification conforme au niveau substantiel ou élevé du règlement eIDAS, et qui de surcroît garantit que ce moyen d'identification a fait l'objet d'un processus de vérification en face à face de l'identité du Signataire.

8.9 — Authentification par OTP SMS ou Courriel

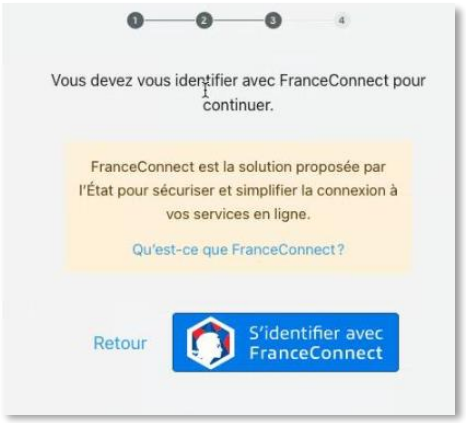
Afin de s'authentifier, le Signataire reçoit un code OTP (One Time Password) à usage unique soit par courriel, soit par SMS.

Page d'authentification par courriel

Les messages reçus par courriel ou par SMS sont personnalisables.

8.10 — Authentification via FranceConnect

Dans le cas où le Signataire est invité à s'authentifier par le service FranceConnect, la page ci-dessous s'affiche :



Page d'authentification avec FranceConnect

Après avoir cliqué sur le bouton « S'identifier avec FranceConnect », le Signataire est redirigé vers la page d'identification « FranceConnect » qui lui propose de choisir le Fournisseur d'Identité de son choix (Ameli, impots.gouv.fr, Identité numérique La Poste, etc.) et de s'authentifier.

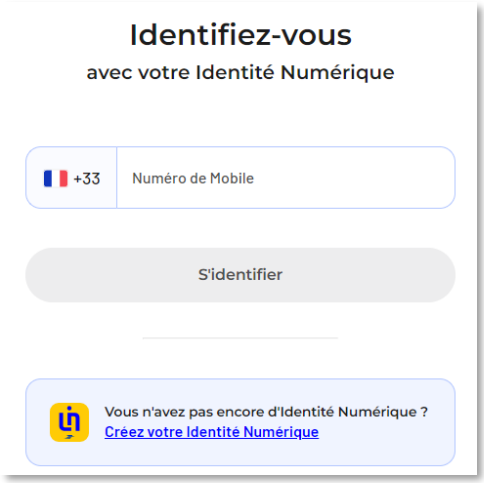
Une fois authentifié sur ce Fournisseur d'Identité, il est redirigé vers « FranceConnect » qui vérifie via la base de l'INSEE que le Signataire existe et qu'il est vivant.

8.11 — Authentification via « l'Identité Numérique La Poste »

Dans le cas où le Signataire est invité à s'authentifier[3] via « L'Identité Numérique La Poste », la page ci-dessous s'affiche :

Page d'authentification via l'INLP

Après avoir cliqué sur le bouton « Utiliser L'Identité Numérique », le Signataire est redirigé vers la page d'identification de « L'Identité Numérique La Poste » qui lui propose en premier lieu de compléter son numéro de téléphone mobile, de manière à débuter l'identification.



Une fois authentifié, il est redirigé vers la plateforme Lex Community.

[3] On rappelle ici que du point de vue de l'action de faire signer un Signataire, l'Utilisateur connait son interlocuteur qu'il a préalablement « identifié » en amont de la transaction de signature et que par conséquent lors de cette étape le Signataire « s'authentifie » afin de prouver qu'il/elle est bien celui/celle qu'elle prétend être.

8.12 — Format de Signature électronique

Lex Community supporte le format de Signature électronique PAdES-B-LT pour les fichiers PDF.

8.13 — Vérification du statut de révocation et du référentiel du Certificat

Lex Community vérifie, avant signature, le statut de révocation et le référentiel du Certificat et inclut dans chaque Signature électronique la preuve de validité du Certificat, récupérée sous la forme d'une réponse OCSP ou, en cas d'absence de répondeur OCSP, sous la forme d'une CRL.

La vérification complète du statut de révocation du Certificat, incluant systématiquement la chaîne de certification de laquelle il dépend, permet de produire des Signature électroniques au format AdES-B-LT.

8.14 — Respect du principe du « What You Sign Is What You See »

Afin de garantir la valeur probatoire des Signature électroniques, y compris pour les documents au format XML, Lex Community respecte le principe du « What You Sign Is What You See » en imposant au Signataire de visualiser l'intégralité des documents à signer. Il est néanmoins possible de rendre facultative cette visualisation.

Les visualisations obligatoires des documents, effectuées par les Signataires, sont tracées dans le Fichier de Preuve de la Transaction.

8.15 — Dossier de preuve

8.15.1 — Constitution du Dossier de Preuve

Le Dossier de Preuve contient l'ensemble des éléments collectés par Lex Community pour l'ensemble des Transactions de Signature électronique électronique d'un Parapheur.

Il est constitué des Fichiers de Preuve relatifs à chaque Transaction ainsi que des éléments permettant de vérifier la traçabilité de la Page de Consentement.

Dès qu'une Transaction de Signature électronique d'un Parapheur se termine avec succès, il est possible de demander la génération du Dossier de Preuve relatif au Parapheur considéré dans son état présent.

8.15.2 — Contenu du Dossier de Preuve

Le Dossier de preuve contient :

- Les Fichiers de Preuve relatif à chaque Transaction de Signature électronique concernant un Signataire donné :
  - Le Fichier de Preuve rassemble l'ensemble des éléments constitutifs d'une Transaction de Signature électronique au sein d'un Parapheur permettant d'assurer la traçabilité et la preuve de la réalisation des Signatures électroniques des documents signés du Parapheur, et qui peut, le cas échéant, être utilisé en justice aux fins de preuve en cas de litige,
  - Chaque Fichier de Preuve est créé au format XML puis cacheté au format XAdES-B-LT par la plateforme Lex Community afin de garantir l'intégrité, l'authenticité et l'antériorité des données qu'il contient par rapport à sa date de création,
  - Un Fichier de Preuve commence toujours par le préfixe « evi » (pour « evidence » en anglais qui signifie « preuve » en français), puis est suivi de l'identifiant (« Client ID ») de la Page de Consentement telle qu'elle est gérée par l'Evidence Manager, puis est suivi d'un identifiant unique du Fichier de Preuve, puis est terminé par l'extension « .xml » ;
- Un sous-dossier nommé « assets » qui contient :
  - Les CGU qui ont été approuvées par les différents Signataires de la Transaction,
  - Le code JavaScript de chaque Page de Consentement,
  - Le code JavaScript de customisation de la Page de Consentement,
  - La feuille de style de la Page de Consentement.

8.15.3 — Contenu du Fichier de Preuve

Le Fichier de Preuve contient les sections suivantes :

- Le nom du Fichier de Preuve ;
- L'identifiant de la Page de Consentement ;
- L'empreinte de hashage de la requête du Workflow Manager contenant les empreintes des documents à signer ainsi que le type de Signature électronique (PAdES, XAdES) ;
- La date et l'heure de création du Fichier de Preuve ;
- La version de l'Evidence Manager ;
- La version du Workflow Manager ;
- L'URL du Workflow Manager qui soumet la Transaction de Signature électronique ;
- L'URL de l'Evidence Manager ;
- L'URL de la page d'invitation à signer le Parapheur ;
- La méthode d'authentification du Signataire et le type de Certificat utilisé ;
- Les informations relatives au Fournisseur d'Identité et à la sécurisation du processus d'authentification, le cas échéant ;
- L'adresse IP publique du Signataire ;
- Le User Agent du Signataire ;
- Les langues autorisées pour la Page de Consentement ;

- Les informations de sécurisation et de vérification des caractéristiques de la Page de Consentement ;
- Les informations relatives à l'acceptation des CGU et à leur Signature électronique ;
- Les informations d'identification et d'authentification du Signataire ;
- Les informations relatives à la demande de Certificat et au Certificat produit ;
- Les informations relatives à la Bi-clé produite puis détruite ;
- Les informations relatives à chaque document signé, avec pour chaque document :
  - Le nom du document,
  - La taille du document avant la réalisation de la Signature électronique,
  - Le hash du document avant la réalisation de la Signature électronique,
  - Le format et les options de la Signature électronique du document,
  - Les données à signer calculées à partir du document (Data To Be Signed),
  - Le résultat du chiffrement du Data To Be Signed (Signature Value),
  - La visualisation obligatoire ou pas du document par le Signataire,
  - La date de la Signature électronique ;
- Les informations relatives à la Signature électronique du Fichier de Preuve et à son horodatage.

En cas de litige, il peut être réconcilié avec les contenus signés présentés par le Signataire afin de vérifier que ce sont bien les contenus qui ont été signés dans le cadre de la Transaction de Signature électronique référencée par le Fichier de Preuve.

Le Fichier de Preuve permet également de reconstituer le parcours déroulé par le Signataire lors du recueil de son consentement et de rejouer l'ensemble des écrans présentés durant la Transaction de Signature électronique.

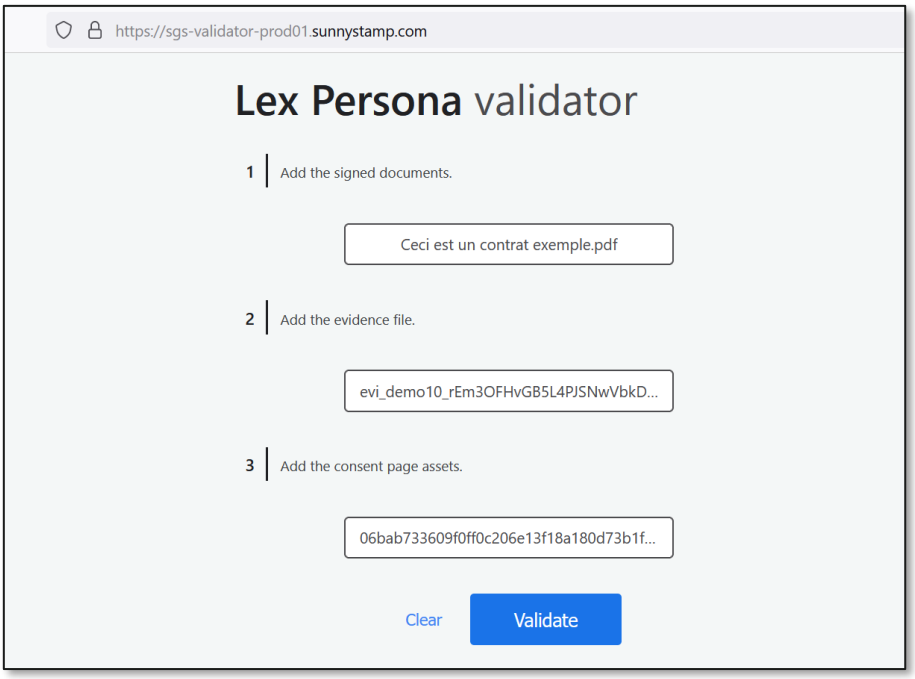
8.15.4 — Vérification d'un Fichier de Preuve

Pour vérifier un Fichier de Preuve, il est nécessaire au préalable d'avoir téléchargé le Dossier de Preuve au format ZIP auquel le Fichier de Preuve est rattaché.

Pour procéder à l'évaluation du Fichier de Preuve, il est nécessaire d'effectuer les étapes suivantes, à partir du Dossier de Preuve correspondant :

- Dézipper le Dossier de Preuve dans un répertoire [dossier_de_preuve] ;
- Repérer le Fichier de Preuve (fichier dont le nom commence par « evi ») concerné ; si besoin ouvrir le Fichier de Preuve et repérer la section signerEmail pour retrouver l'adresse de courriel du Signataire considéré ;
- Ouvrir un navigateur Internet et se rendre sur la page https://sgs-validator-prod01.sunnystamp.com/ ;
- Remplir le formulaire comme suit :
  - Dans le 1er champ il est nécessaire de charger le fichier « soi-disant » signé sur la plateforme que vous aurez préalablement téléchargé depuis le Parapheur considéré,
  - Dans le 2ème champ il est nécessaire de charger le Fichier de Preuve de la Signature électronique considérée (le fichier dont le nom commence par "evi" et relatif au Signataire considéré),

- Dans le 3ème champ il est nécessaire de charger tous les fichiers du répertoire « assets » préalablement enregistré.



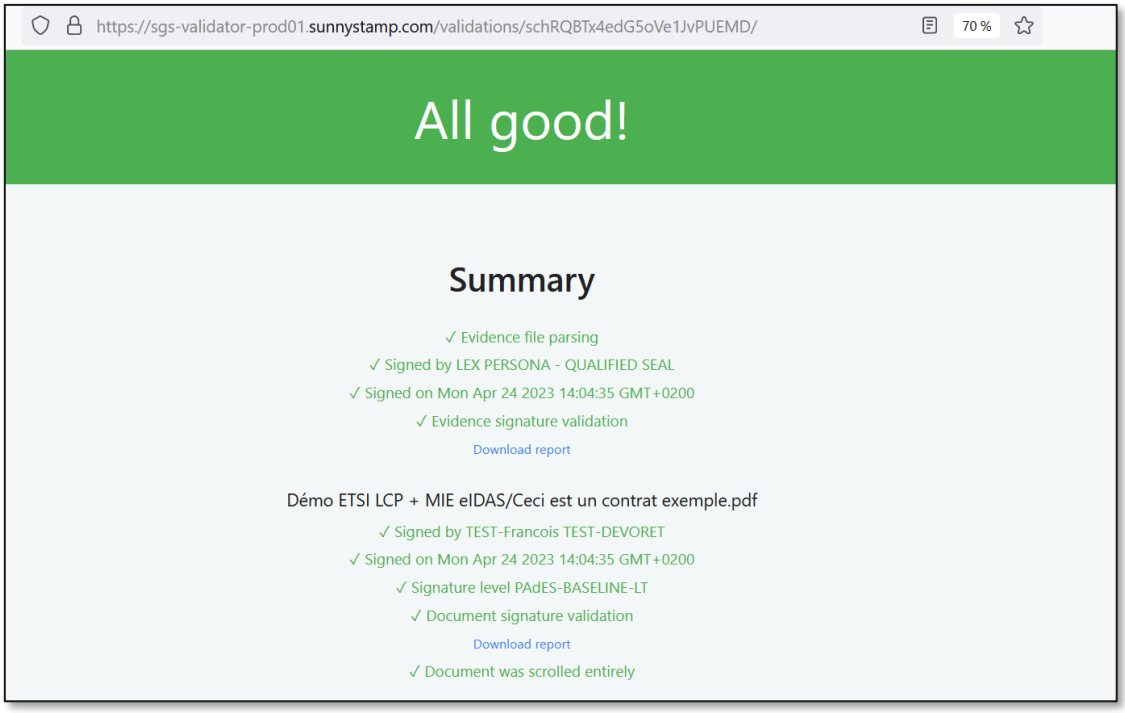
Remplissage du formulaire de validation du Fichier de Preuve

La vérification vérifie alors tout d'abord la cohérence de tous les éléments fournis :

/ L'intégrité des fichiers signés ;

/ La validité de tous les certificats y compris de l'horodatage ;

/ L'intégrité et l'authenticité du fichier de preuve lui-même.

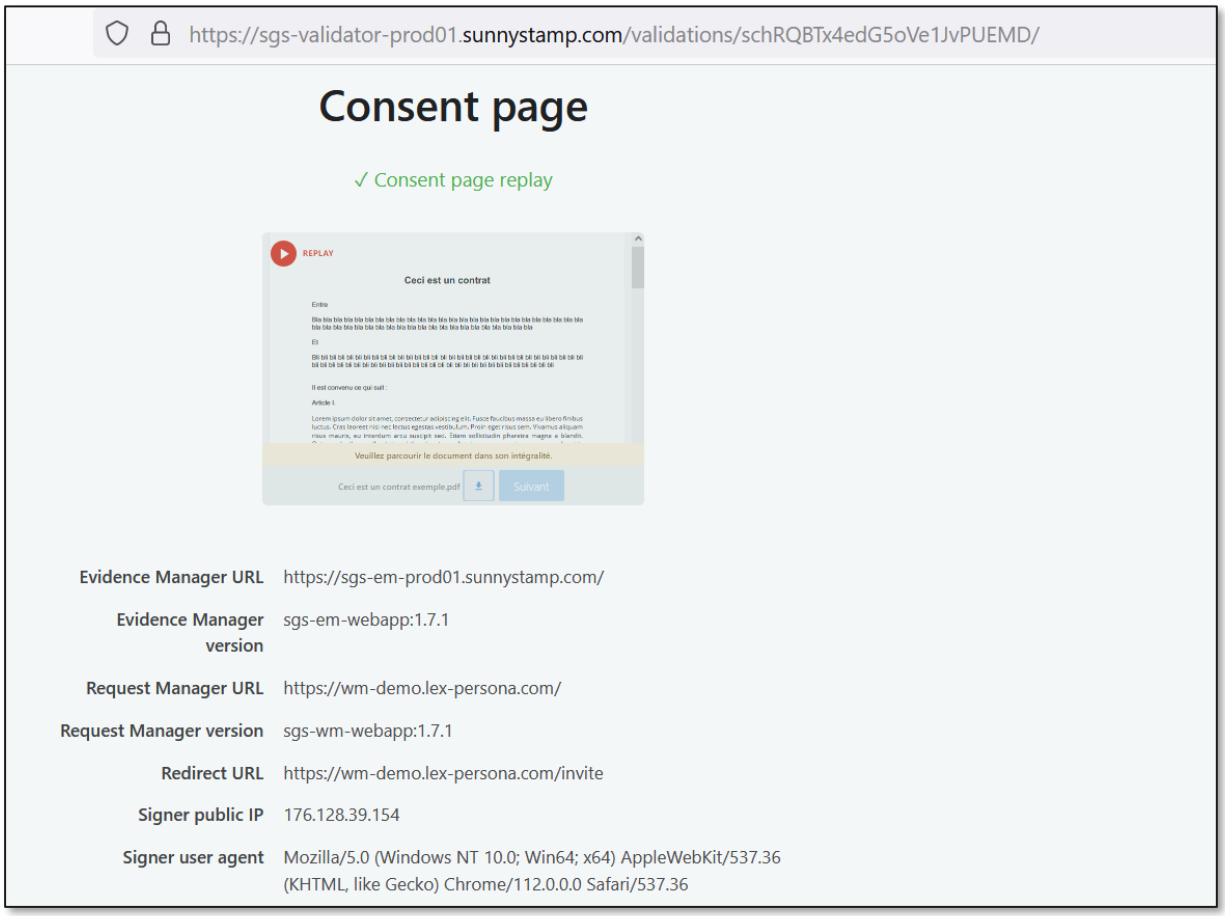


Résumé d'ensemble de la validation du Fichier de Preuve et des documents signés

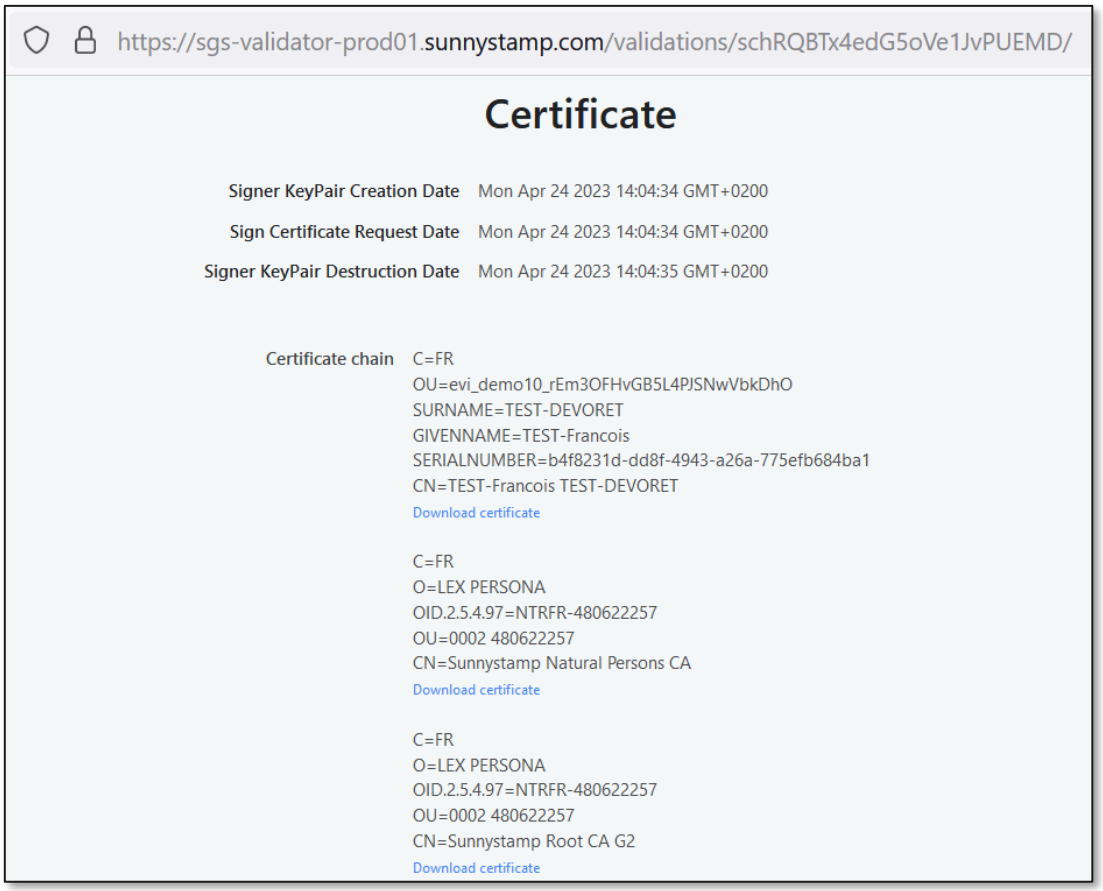
Il est ensuite possible de rejouer les écrans de la transaction ainsi que de consulter les éléments de traçabilité de la transaction :

- Modes d'authentification utilisés ;
- Adresse IP du signataire ;
- Éléments relatifs à l'OTP mail ou SMS ;
- Etc.

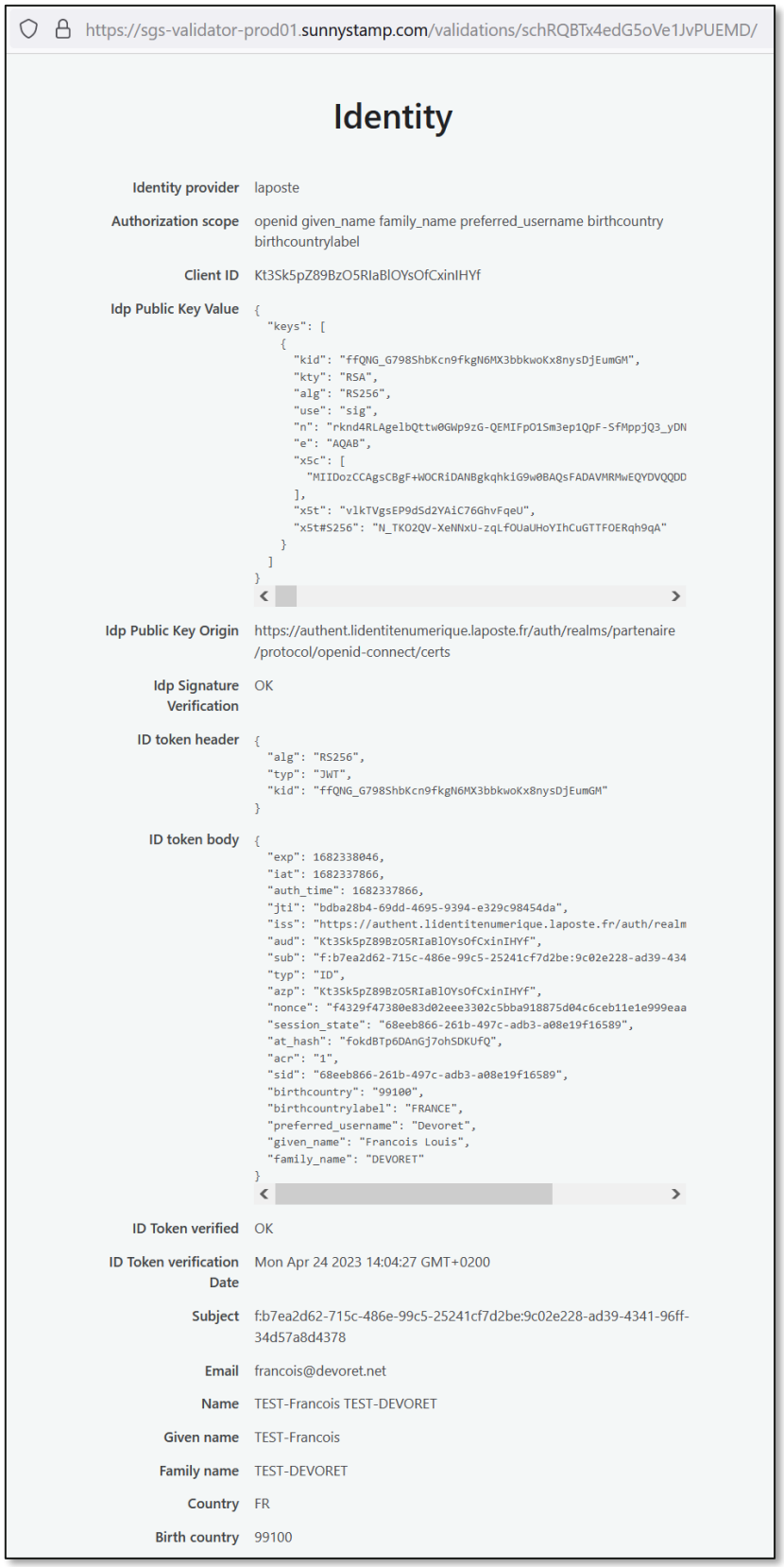
Validation de la Signature électronique des CGU



Validation du rejeu de la Page de Consentement et éléments relatifs au dispositif du Signataire



Validation du Certificat généré à la volée du cycle de vie de la Bi-clé



Validation de l'identité du signataire et du processus d'authentification utilisé

8.16 — Horodatage des Signatures électroniques

Toute Signature électronique réalisée par Lex Community est horodatée par un service d'horodatage RFC3161 opéré par LEX PERSONA afin de garantir l'antériorité de la Signature électronique produite par rapport à la date contenue dans le jeton d'horodatage et de prouver que le Certificat du Signataire n'était pas révoqué au moment de la Signature électronique.

9 — Sécurité & Confidentialité

9.1 — Architecture

Les différents composants sur lesquels repose la solution Lex Community sont présentés dans l'image ci-dessous :

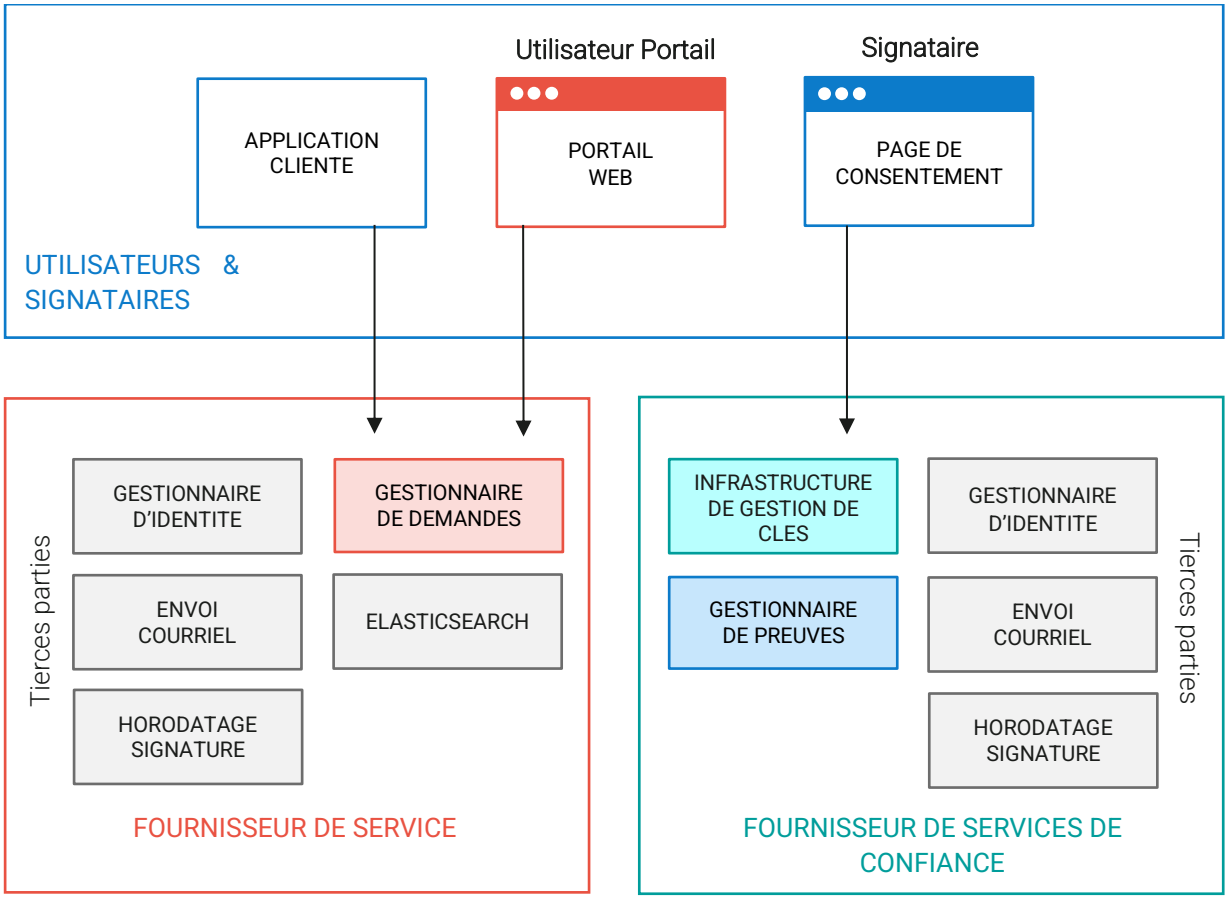


Schéma d'architecture de la solution Lex Community

- Dans la partie « Utilisateurs & Signataires » :
  - Les applications clientes,
  - Le Portail Web s'exécutant dans le navigateur Internet des utilisateurs,
  - La Page de Consentement pour la Signature électronique ;
- Dans la partie « Fournisseur de Services » opérée par Lex Persona ou par le Client (en mode « On Premise ») :
  - Le Gestionnaire de Demandes ou « Workflow Manager », composant central de Lex Community qui expose une API REST et un Portail Web pour gérer les Parapheurs,
  - Le Fournisseur d'Identité utilisé pour identifier et authentifier les Utilisateurs du Portail Web,
  - Le Fournisseur de Messagerie utilisé pour envoyer des notifications par courriel aux Utilisateurs,
  - L'Autorité d'Horodatage pour l'horodatage des Signatures électroniques produites ;

- Dans la partie « Fournisseur de Services de Confiance » opérée par Lex Persona :
  - L'Autorité de Certification qui délivre des Certificats éphémères pour les Signataires,
  - Le Gestionnaire de Preuves ou « Evidence Manager », composant serveur qui collecte les preuves de Signature électronique, gère le protocole de consentement et produit les Fichiers de Preuves,
  - Le Fournisseur d'Identité qui peut être utilisé pour authentifier les Signataires dans la Page de Consentement, avant les Signatures électroniques,
  - Le Fournisseur de Messagerie pour l'envoi des mots de passe à usage unique par courriel aux Signataires avant les Signatures électroniques,
  - Le Fournisseur de SMS qui envoie des mots de passe à usage unique par SMS aux Signataires avant les Signatures électroniques,
  - L'Autorité d'Horodatage qui produit l'horodatage des Fichiers de Preuve.

9.2 — Hébergement et disponibilité

L'infrastructure matérielle et réseau de la plate-forme Lex Community, en mode SaaS, est en capacité d'offrir une haute disponibilité.

Hébergée dans deux datacenters (principal et secours) basés en France, ses caractéristiques sont les suivantes :

- Datacenters situés en France (Production – Tests – PRA & PCA) ;
- Certifiés ISO 27001 ;
- Certifiés HDS (Hébergeur de Données de Santé).

Le Service est accessible 24 heures sur 24 et 7 jours sur 7, sauf en cas de force majeure, en cas de panne, ou d'intervention de maintenance planifiée.

9.3 — Sécurité

L'ensemble des services SaaS et des développements effectués par Lex Persona sont couverts par la certification ISO 27001:2017 et HDS. En plus des audits annuels réalisés pour ces certifications, Lex Persona assure de manière annuelle des tests d'intrusion sur ses services SaaS par des prestataires externes qualifiés.

Critère de sécurité	Valeur
Sécurité physique	- Protection des locaux Lex Persona par badges nominatifs ; - Surveillances des datacenters 24h/24 par vidéo-surveillance et alarmes.
Données	- Ensemble des données hébergées en France ; - Chiffrement de toutes les données (et de leurs sauvegardes) dans la transmission et dans le stockage ;

Critère de sécurité	Valeur
	⁄ Accès aux données en interne réservé aux employés identifiés, contrôlé par accès VPN à plusieurs facteurs ; ⁄ Transmission des données uniquement via le protocole TLS et tests réguliers via les SSL Labs.
Hébergement et réseaux	⁄ Hébergement assuré par 2 datacenters situés en France ; ⁄ Chiffrement HTTPS (TLS) de bout en bout ; ⁄ Authentification des services et applications sur des Reverse Proxy ; ⁄ Cloisonnement des réseaux en fonction des besoins de sécurité ; ⁄ Identification et revue de tous les flux inter-réseaux ; ⁄ Séparation et cloisonnement entre les environnements (production et test).
Plan de reprise	⁄ Nous disposons de procédures de bascules, testées une fois par an ; ⁄ Astreinte 24h/24 et 7j/7.

L'ensemble des actions utilisateurs et administrateurs sont tracées et revues annuellement.

9.4 — Confidentialité des données

Les actions des administrateurs sont journalisées par des « Bastions » d'administration. Ces Bastions assurent une rupture protocolaire et une traçabilité complète. Des alertes sont envoyées lorsque des administrateurs se connectent sur des équipements sensibles ou effectuent certaines commandes sur les serveurs.

Une politique de développement et de maintenance des systèmes d'information est formalisée. Cette politique est maintenue, revue et auditée une fois par an, a minima.

Elle intègre :

⁄ La sécurité de l'environnement de développement ;

⁄ Le respect des bonnes pratiques de sécurité pour chaque langage de programmation utilisé ;

⁄ Le respect des préconisations de l'OWASP, dans le cas d'un développement Web ;

⁄ Les points de contrôle de la sécurité aux différentes étapes clés du projet ;

⁄ La sécurité liée au contrôle des versions.

9.5 — Protection des données

Toute collecte et tout usage de données à caractère personnel par la plateforme Lex Community et l'ensemble de ses composantes sont réalisés dans le strict respect de la législation et de la réglementation en vigueur sur le territoire français, en particulier la loi n° 78-17 du 6 janvier 1978

relative à l'informatique, aux fichiers et aux libertés, modifiée, ainsi que le Règlement général sur la protection des données (dit RGPD) du 27 avril 2016.

Au sens du Règlement européen 2016/679 du 27 avril 2016 sur la protection des données personnelles, Lex Persona, en tant qu'opérateur de la plateforme Lex Community est responsable de traitement.

Les données et fichiers conservés de manière temporaire dans l'environnement Lex Community sont :

- Les données personnelles des signataires, utilisées dans le cadre d'une Signature électronique en mode « distant » pour la génération des Certificats de Signature électronique ;
- Les empreintes des documents signés et cachetés ;
- Tous les éléments de traçabilité relatifs aux Transactions de Signatures électroniques effectuées ; ces éléments sont conservés dans les fichiers de preuve.

Ces données personnelles sont confidentielles et ne seront utilisées que dans la finalité susvisée. Lex Persona s'engage à ne pas divulguer à des tiers non autorisés et non habilités, les données personnelles relatives à chaque utilisateur et à chaque signataire sans l'autorisation préalable des personnes concernées.

Ces données sont conservées sur la plateforme Lex Community pendant une durée qui sera déterminée et pouvant être différenciée par type de donnée. Les données des Utilisateurs et de leurs contacts sont conservées jusqu'à suppression du compte ou pendant une durée maximale définie dans les Conditions Générales d'Utilisation de la plateforme Lex Community après la dernière utilisation du service. Le stockage sécurisé s'effectue sur des serveurs hébergés dans les deux datacenters de Lex Persona.

Lex Persona s'engage, en cas de transfert de données, à présenter les garanties juridiques adéquates décrites dans les articles 45 et suivants du RGPD.

9.6 — Sauvegarde des données

Les sauvegardes sont complètes et effectuées tous les jours. Le contrôle d'intégrité est quotidien et la suppression des données arrivées à la période de rétention est automatique.

Le succès des sauvegardes est contrôlé tous les jours et des tests de restauration sont effectués tous les mois.

Les sauvegardes sont effectuées sur le site principale et sur le site secondaire. Ces sites sont éloignés de plus de cent kilomètres.

9.7 — Stockage chiffré et sécurisé

L'ensemble des serveurs de production utilisés par la plateforme Lex Community sont chiffrés.

L'ensemble des flux sont chiffrés. Seuls les flux explicitement autorisés peuvent aboutir, le reste est bloqué.

Une matrice de redondance des équipements et des personnes est maintenue à jour.

9.8 — Taux de disponibilité

Les taux de disponibilité des services sont calculés automatiquement via une supervision externe qui utilise directement les services de la plateforme Lex Community.

Cette supervision est hébergée dans différentes villes d'Europe afin d'avoir un taux le plus précis possible.

En cas de dysfonctionnement, des alertes sont envoyées directement sur les canaux des services techniques et sur les téléphones de l'équipe d'astreinte.

9.9 — Normes/certifications

La plateforme Lex Community fait l'objet d'audits dans le cadre des différentes certifications maintenues par Lex Persona.

Toutes les certifications, et les normes inhérentes sont basées sur les principes de sécurité et de transparence.

9.9.1 — Certification ISO 27001

Lex Persona est certifiée ISO 27001:2017 depuis le 13 octobre 2017 sur l'ensemble de ses activités sans exclusion d'aucune mesure ou clause citées dans cette norme.

La certification ISO 27001:2017 vise à mettre en place un système de management de la sécurité du système d'information destiné à garantir la sécurité et la disponibilité des services et des prestations fournies auprès de l'ensemble des clients et utilisateurs des produits et services de Lex Persona.

La certification ISO 27001:2017 réalisée par LSTI peut être vérifiée à l'adresse suivante : http://www.lsti-certification.fr/images/20171025.pdf.

9.9.2 — PKI certifiée ETSI EN 319 411-1 LCP

En 2017 également, Lex Persona a fait auditer son Autorité de Certification « Sunnystamp Natural Persons CA » et obtenu la conformité vis-à-vis du standard ETSI EN 319 411-1 LCP.

La certification de la PKI Lex Persona garantit le respect des standards relatifs à la Signature électronique avancée proposée par Lex Persona et sa plateforme de Signature électronique. Elle offre des garanties de sécurité et de disponibilité auprès des utilisateurs.

Nom : Sunnystamp Natural Persons CA
Identifiant de la politique du service : 1.3.6.1.4.1.22542.100.1.1.1.2
Niveau LCP
Statut : valid
Dernière évaluation de conformité : 25/06/2021
Prochaine évaluation de conformité : 24/06/2023

Les exigences de conformité sont décrites dans les documents suivants :

EN 319 411-1 V1.2.2: Signatures électroniques et infrastructures (ESI) - Exigences de politique et de sécurité applicables aux prestataires de service de confiance délivrant des certificats - Partie 1 : Exigences générales

Extraits du certificat de conformité ETSI EN 319 411-1 LCP

Voir également le lien « PDF LIST OF CERTIFIED TSP » sur cette page.

9.9.3 — Horodatage qualifié eIDAS EN 319 421

En juillet 2020, Lex Persona a fait auditer avec succès son service d'horodatage par LSTI en vue d'une qualification eIDAS obtenue au mois de novembre 2020.

Le service d'horodatage qualifié eIDAS proposé par Lex Persona offre des garanties en termes de niveaux de sécurité et de disponibilité.

9.9.4 — Labellisation 2D-Doc / COREF/FNTC

En mars 2018, Lex Persona a obtenu les deux labels FNTC-CEV « mention 2D-Doc », le label pour la génération du code 2D-Doc et celui pour le service de vérification du code 2D-Doc « mention 2D-Doc », en accord avec le référentiel normatif établi par l'ANTS (Agence Nationale des Titres Sécurisés) et mis en place par la FNTC.