Goodflag

Cahier des fonctionnalités de la solution Goodflag Signature

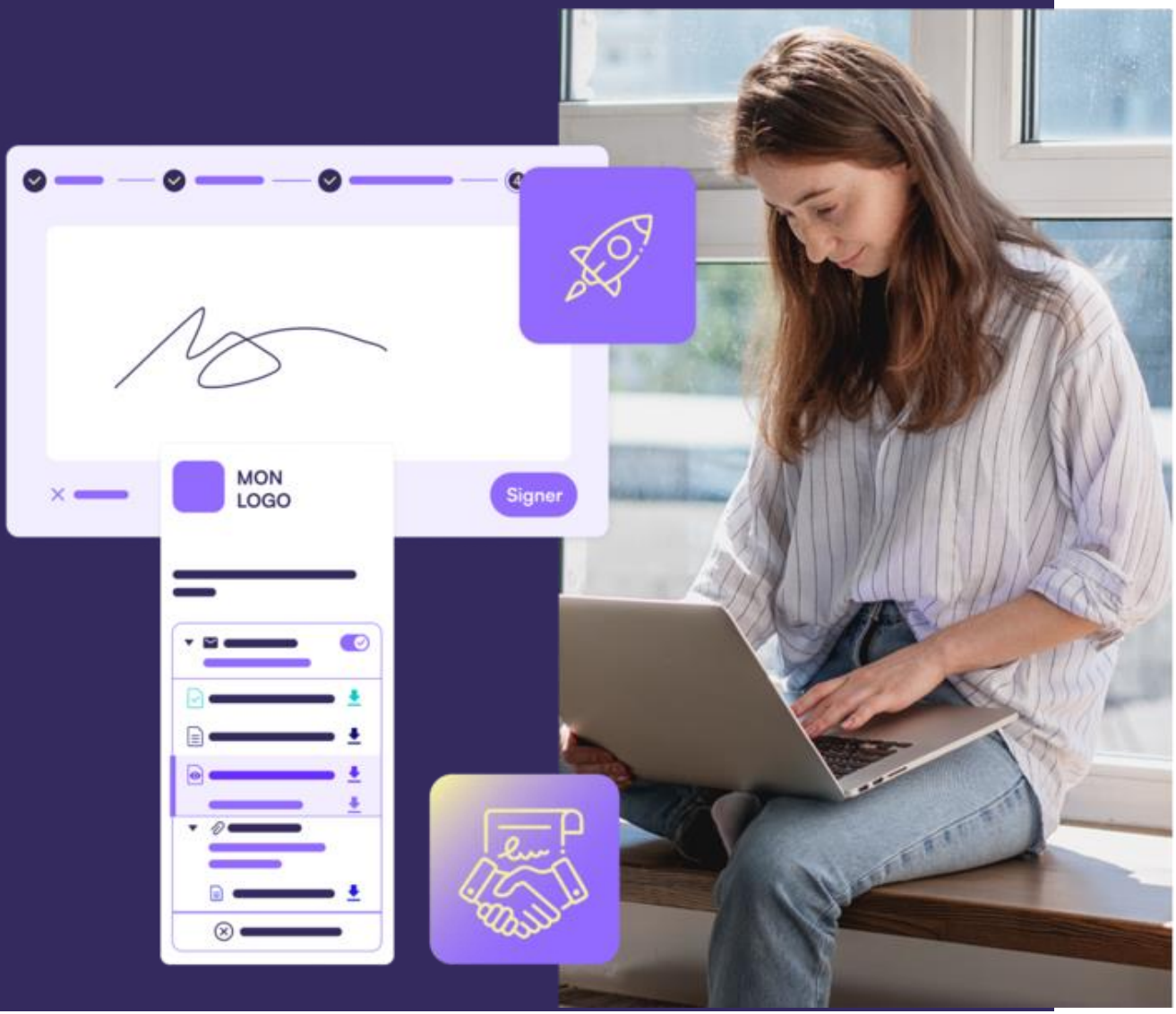


Table des matières

1 – Introduction

Ce document présente l'ensemble des fonctionnalités de la solution de signature électronique Goodflag Signature.

- Goodflag Signature est une application multi-tenant exposant un Portail et une API de signature en mode Web, qui permet de gérer vos Parapheurs électroniques.
- Goodflag Signature permet de faire signer électroniquement 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.
- Goodflag Signature, dont l'architecture originale est brevetée, propose à ses clients 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.
- Goodflag Signature permet de délivrer :

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

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 « clôturé ». 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.

Client

Entité légale qui dispose d'un ou plusieurs Tenant(s) Goodflag Signature utilisé(s) par des Utilisateurs (ou des programmes) pour faire valider et/ou signer des documents respectivement à des Validateurs et/ou Signataires.

Cogestionnaire

Utilisateur habilité à cogérer un Parapheur dès lors qu'il a été nommé comme tel sur un Parapheur et qu'il appartient à un Groupe Utilisateur disposant du rôle de Cogestionnaire.

Contact

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

Destinataire

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

Dossier de Preuve

Ensemble des éléments collectés par Goodflag Signature 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 ou la Validation électronique d'un ou plusieurs destinataires.

Favoris

Préférences de recherches sauvegardées par un Utilisateur.

Fichier de Preuve

Fichier XML cacheté et horodaté par Goodflag, 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.

Fournisseur d'Identité

Entité tierce chargée par Goodflag Signature pour authentifier, le cas échéant, les Signataires. Le Fournisseur d'Identité, après avoir vérifié l'identité de l'Utilisateur, produit un Jeton d'identité attestant de cette identité. Ce Jeton est validé et exploité par Goodflag Signature de sorte que l'AC délivre le Certificat du Signataire sur la base des informations d'identité qu'il contient.

France Identité

Moyen d'identification électronique qualifié au niveau élevé conformément au Règlement eIDAS.

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 Goodflag Signature pour identifier le Signataire via le Fournisseur d'Identité qu'il aura choisi parmi ceux que lui aura proposé FranceConnect. Avec FranceConnect, tous les moyens d'identification proposés sont considérés comme de niveau faible selon le règlement eIDAS.

FranceConnect+

FranceConnect+ est une solution d'identification créée par l'État français pour faciliter la connexion à différents services en ligne nécessitant un moyen d'identification de niveau substantiel ou élevé conformément au règlement eIDAS. Dans le cadre du présent document, FranceConnect+ est utilisé par Goodflag Signature pour identifier le Signataire via le Fournisseur d'Identité qu'il aura choisi parmi ceux que lui aura proposé FranceConnect+ et avec lesquels Goodflag dispose d'un contrat spécifique à FranceConnect+.

Gestionnaire

Utilisateur qui a le droit de créer, modifier et supprimer un Parapheur.

Groupe

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

Jeton d'API

Donnée confidentielle permettant d'appeler les différents endpoints exposés à travers l'API de Goodflag Signature.

Jeton d'identité

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

Goodflag Signature

Plateforme de Signature électronique multi-tenants, chaque Tenant bénéficiant d'un Portail Web et d'une API REST.

L'Identité Numérique de la Poste

Moyen d'identification électronique qualifié au niveau substantiel conformément au Règlement eIDAS.

Organisation

Entité légale à laquelle peut être rattachée un ou plusieurs Utilisateur(s).

Page de Consentement

Ensemble d'écrans exposés par Goodflag Signature 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) ou de Validation(s), par un ou plusieurs destinataire(s) en parallèle, d'un ou plusieurs document(s) à signer ou valider, accompagné(s) éventuellement d'une ou plusieurs pièce(s) jointe(s). Dans le cadre du mode « Signataire unique », les notions de circuit et d'étapes ne sont pas applicables, puisqu'un seul signataire intervient.

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 Goodflag Signature s'exécutant dans un navigateur Internet pour la gestion d'un Tenant, des Parapheurs, des Utilisateurs, etc.

Prestataire de Service de Certification Électronique

Un prestataire de services de certification électronique est une personne physique ou morale qui délivre des certificats électroniques et fournit éventuellement d'autres services en matière de certification électronique.

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.

Tenant

Sous-ensemble de la plateforme Goodflag Signature, dédié à une communauté d'Utilisateurs définie par un client et dont les règles de gestion sont totalement configurables et personnalisables selon les besoins des clients. Chaque client peut personnaliser des espaces indépendants et cloisonnés avec des chartes graphiques différentes. Cela permet à un client de traiter différents cas d'usage de la signature électronique.

Transaction

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

Utilisateur

Personne physique habilitée par le Client à se connecter à Goodflag Signature, qui appartient à un Groupe et a des droits particuliers (Gestionnaire de Parapheurs, Signataire, Validateur, etc.).

Validateur

Personne physique, représentant ou non une personne morale, destinataire d'une étape de Validation électronique d'un Parapheur.

Validation électronique

Opération consistant pour un Validateur à valider électroniquement le(s) Document(s) d'une Transaction, à la suite d'une demande de validation effectuée par l'Utilisateur. L'Utilisateur doit s'assurer, en ce qui concerne l'utilisation de la fonctionnalité de "Demande de validation" (par opposition à une "Demande de signature"), que celle-ci est bien conforme à la définition donnée par le Client en fonction du contexte de la Transaction, et qu'elle est également bien définie par le Client en termes d'exigences vis-à-vis du Validateur.

Webhook

Mécanisme de communication entre applications.

3 – Abréviations

AC

Autorité de Certification

AE

Autorité d'Enregistrement

ANSSI

Agence Nationale de la Sécurité des Systèmes d'Information

API

Application Program Interface

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)

INLP

Identité Numérique La Poste

LCR

Liste de Certificats Révoqués (en anglais : CRL)

MSCAPI

Microsoft Cryptographic API

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)

PSCE

Prestataire de Service de Certification Électronique

QCP

Qualified Certificate Profile

QSCD

Qualified Signature Creation Device

SMS

Short Message Service

XAdES

XML Advanced Electronic Signature

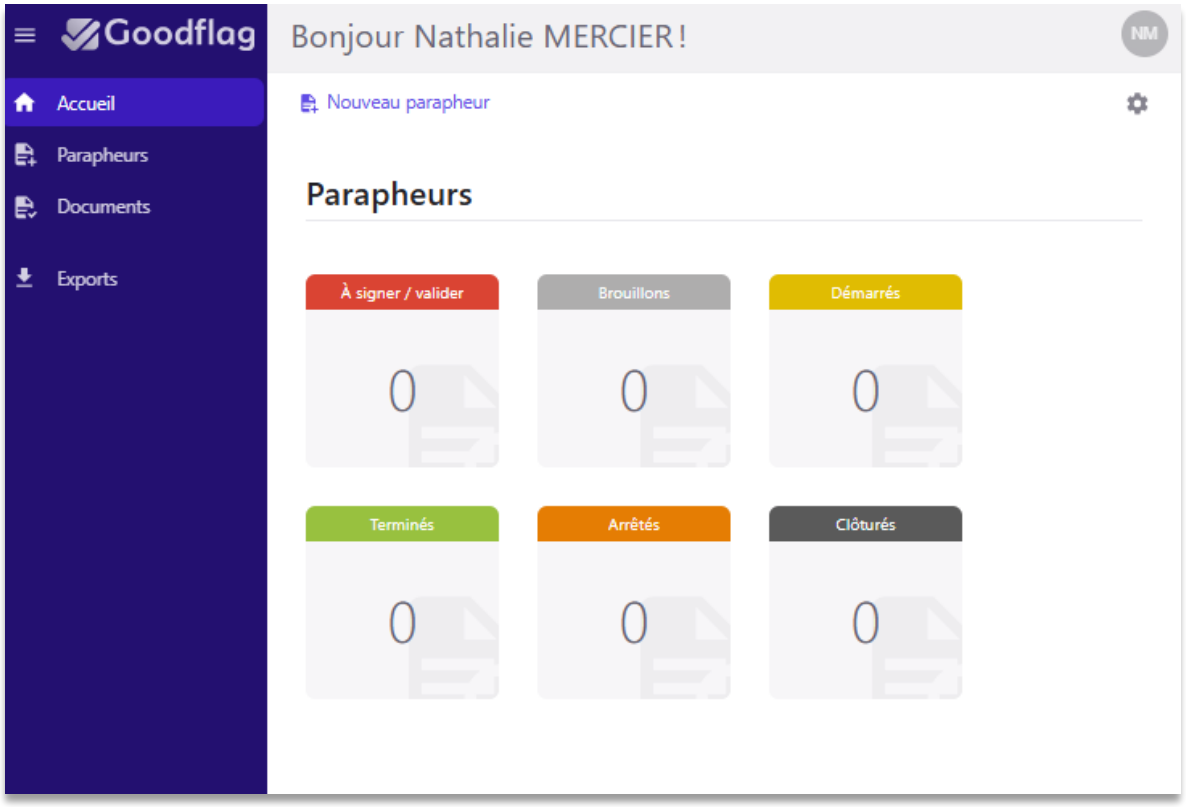
XML

Extended Markup Language

4 — Expérience Utilisateur Portail

4.1 — Le tableau de bord

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



Exemple de tableau de bord d'un Utilisateur

D'un simple coup d'œil, l'Utilisateur visualise immédiatement le nombre d'invitations à valider ou signer, le nombre de Parapheurs selon leur statut. Le tableau de bord de Goodflag Signature aide l'Utilisateur à mieux organiser et superviser ses Parapheurs.

4.1.1 — Suivi des Parapheurs

Grâce aux vignettes épinglées sur le tableau de bord, l'Utilisateur peut visualiser le nombre de Parapheurs selon leur statut ou selon d'autres critères personnalisés.

Affichage des vignettes

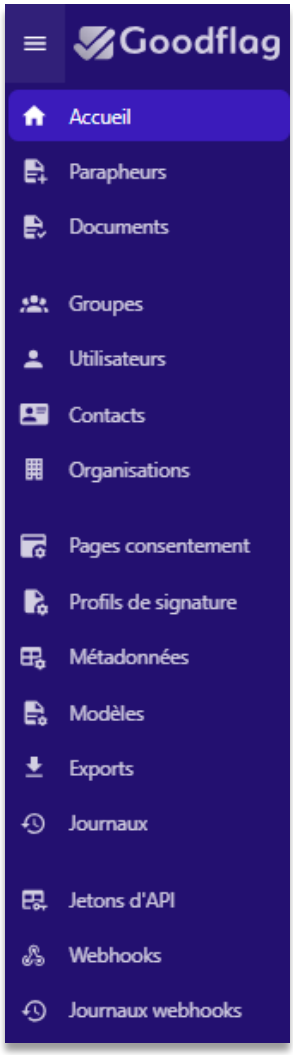
Le statut d'avancement du Parapheur peut être dans l'un des 5 états suivants :

- Brouillon : le Parapheur est en cours de création ;

- Démarré : le Parapheur a été lancé par le Gestionnaire ;
- Arrêté : soit il a été volontairement arrêté par le Gestionnaire, soit des Validateurs ou des Signataires ont refusé de valider ou de signer ;
- Terminé : toutes les étapes du Parapheur se sont terminées avec succès ;
- Clôturé : le parapheur a été clôturé par le Gestionnaire afin d'interdire toute modification d'un parapheur. Un Utilisateur accède aux Parapheurs dont il est propriétaire et ceux dont il est observateur.

4.1.2 — 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, en fonction des droits qui lui sont accordés, aux différentes fonctionnalités de l'application.



Menu contextuel d'un administrateur

4.1.3 — Personnalisation de l'interface

La solution Goodflag Signature est personnalisable selon votre charte graphique.

La solution propose des personnalisations graphiques en termes de couleurs (menu, boutons, lien, en-tête, etc.).

De plus, l'Utilisateur peut configurer son tableau de bord : ajout de nouvelles vignettes ou de raccourcis

L'interface de Goodflag Signature devient votre interface de Parapheur : c'est un véritable portail privé à vos couleurs où la marque Goodflag disparait et n'interfère pas visuellement.

4.1.4 — Les vignettes

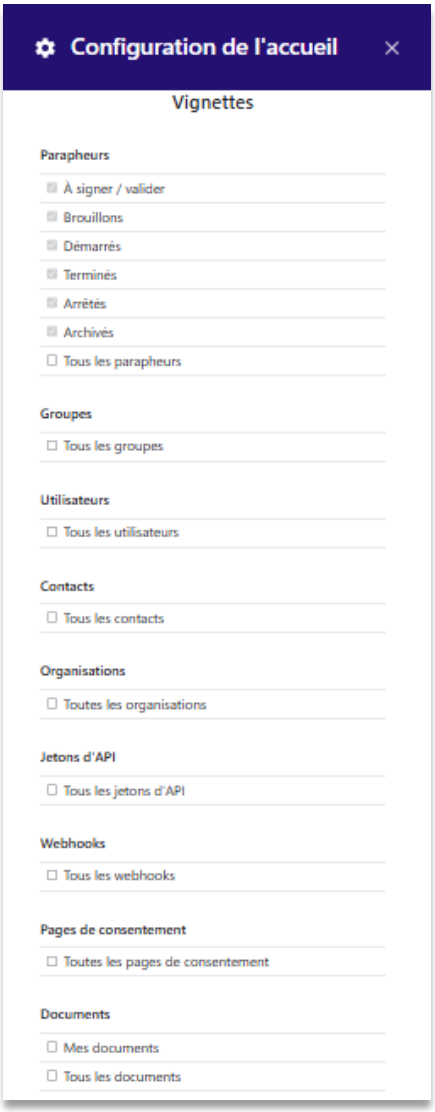
Les vignettes sont de type « compteur », c'est-à-dire qu'elles affichent le nombre de résultats selon la requête qu'elles appellent.

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.

Les vignettes standardisées sont les suivantes :



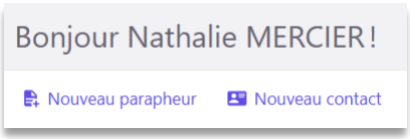
Page de configuration des vignettes

- À Signer / À valider ;
- Brouillons ;
- Démarrés ;
- Terminés ;
- Arrêtés ;
- Clôturés ;
- Tous les groupes ;
- Tous les utilisateurs ;
- Tous les contacts ;
- Toutes les organisations ;
- Tous les jetons d'API ;
- Tous les Webhooks ;
- Toutes les pages de consentement ;
- Tous les documents ;
- Tous les exports ;
- Toutes les dispositions de métadonnées ;
- Tous les journaux ;
- Tous les profils de signature ;
- Tous les modèles ;
- Tous les journaux Webhooks.

Ces vignettes correspondent pour la plupart aux fonctionnalités de l'application ; ainsi l'Utilisateur y accède en fonction des droits qui lui sont accordés.

4.1.5 — 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.



Raccourcis

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 ».

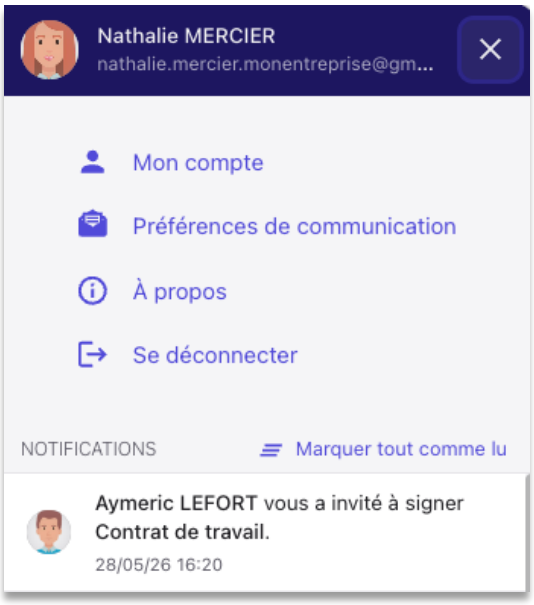
Les raccourcis disponibles sont les suivants :

- Nouveau Parapheur ;
- Nouveau Groupe ;
- Nouvel Utilisateur ;
- Nouveau Contact ;
- Nouvelle Organisation ;
- Nouveau Jeton d'API ;
- Nouveau Webhook.

L'accès à ces raccourcis dépend des droits accordés à l'Utilisateur.

4.2 — Profil Utilisateur

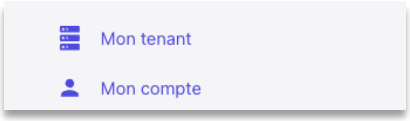
En haut, à droite de l'écran, l'Utilisateur peut accéder à son profil Utilisateur.



Profil Utilisateur

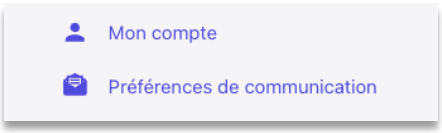
A partir de son profil, il accède à plusieurs sections :

- Mon tenant : si l'Utilisateur a le rôle d'administrateur du Tenant, il accède aux informations du Tenant qu'il administre ;



Profil administrateur

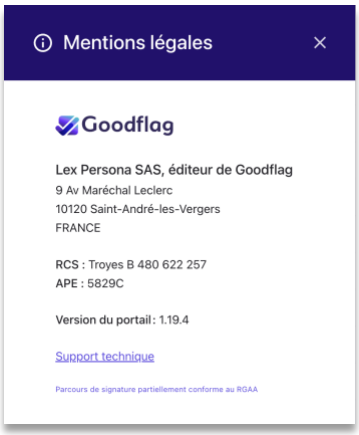
- **Mon compte** : l'Utilisateur accède aux informations relatives à son compte Utilisateur (Groupe d'Utilisateurs, prénom, nom, courriel, numéro de téléphone mobile, pays, etc.) ;
    - S'il le souhaite, l'Utilisateur peut importer une photographie. Par défaut la bulle reprend les initiales du prénom et du nom de l'Utilisateur. À noter que si le Fournisseur d'Identité du Tenant retourne la photographie de l'Utilisateur, cette dernière sera automatiquement importée dans son compte Utilisateur.
- **Préférences de communication** : l'utilisateur choisit s'il souhaite s'abonner à deux listes de diffusion : Nouveautés produit & Actualité Goodflag
    - Les cases sont pré-cochées si l'utilisateur est déjà inscrit aux listes correspondantes.
    - L'utilisateur peut à tout moment modifier ses préférences : s'abonner ou se désabonner d'une ou des deux listes.



Profil utilisateur (SaaS)

Nota bene : Cette section est réservée aux clients SaaS. Pour les clients on premise, les préférences de communication sont recueillies via un formulaire de consentement transmis aux référents lors de l'onboarding.

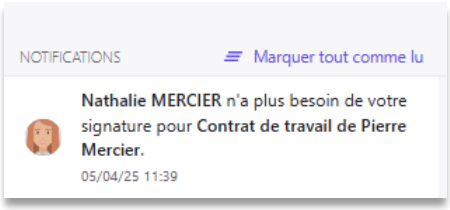
- **A propos** : l'Utilisateur accède aux mentions légales, au numéro de version de la solution, au contact du Support Technique et à la déclaration d'accessibilité RGAA (se reporter au chapitre 4.10)



Section « A propos »

- **Se déconnecter**
- **Aux notifications** qu'il reçoit également par courriel.
    - L'Utilisateur reçoit une notification en cas de changement de statut d'un Parapheur, lorsqu'un destinataire valide ou signe un document ;
    - Lorsqu'une nouvelle notification apparait, le nombre correspondant aux nouvelles notifications s'incrémente ;

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

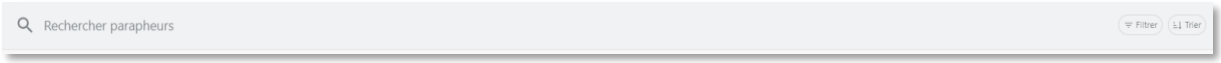


Exemple de notification

4.3 — Outils de recherche

4.3.1 — Recherche par mot-clé

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

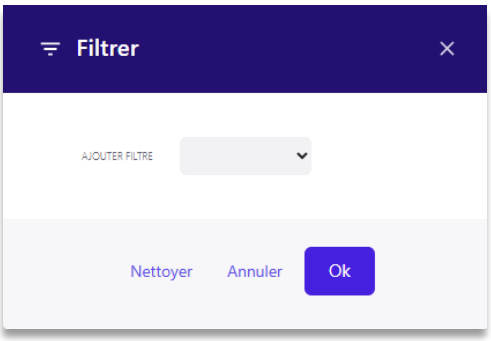


En-tête de recherche

4.3.2 — Filtres & tris

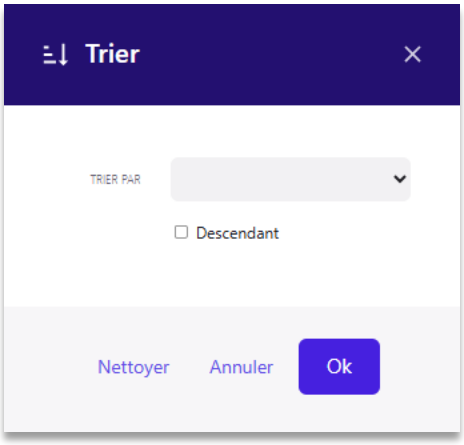
Dans l'objectif d'affiner sa recherche, l'Utilisateur peut utiliser des critères de filtrage : nom, statut, propriétaire, date de création, etc. Chaque champ de métadonnée standard ou personnalisé peut être utilisé comme critère de filtrage.

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



Exemple de filtre

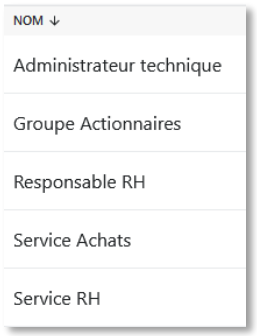
La liste de résultats peut également être triée. Le tri peut être ascendant ou descendant :



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.



Tri ascendant

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.

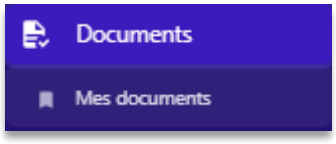
La base de données utilisée est une base Elasticsearch[1], ce qui permet de supporter un très grand nombre de données tout en garantissant des performances optimales en termes d'indexation et de recherche.

4.3.3 — Les favoris de recherche

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 documents ».



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.

Nota bene : L'Utilisateur peut également sélectionner ses favoris dans la page de consolidation des Parapheurs.

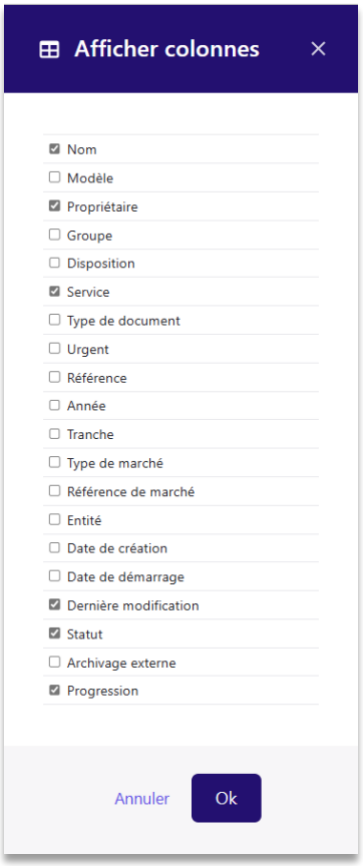
1 Elasticsearch est une marque de Elasticsearch BV, déposée aux USA et dans d'autres pays. https://www.elastic.co/fr/legal/trademarks

4.4 — Affichage des données

4.4.1 — Affichage configurable des données

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 soit à une métadonnée standard (« nom », « propriétaire », « statut », etc.), soit à une métadonnée personnalisée : métadonnée créée pour une disposition de métadonnées.



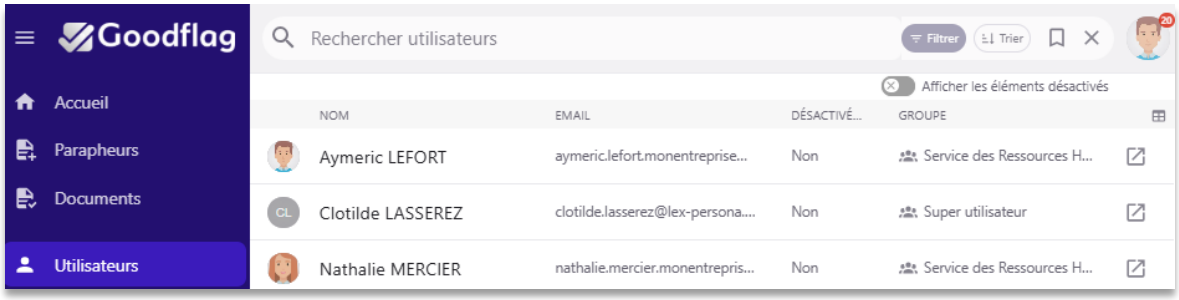
Paramétrage des colonnes

4.4.2 — Affichage des éléments désactivés

La solution permet de désactiver certains items :

- Groupes ;
- Utilisateurs ;
- Pages de consentement ;
- Profils de signature ;
- Métadonnées ;
- Modèles.

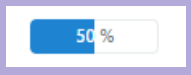
Pour chacun de ces items, un bouton permet d'afficher ou de masquer les éléments désactivés de la liste de résultats.



Bouton « Afficher les éléments désactivés »

4.5 — Indicateurs visuels & Boutons d'actions rapide

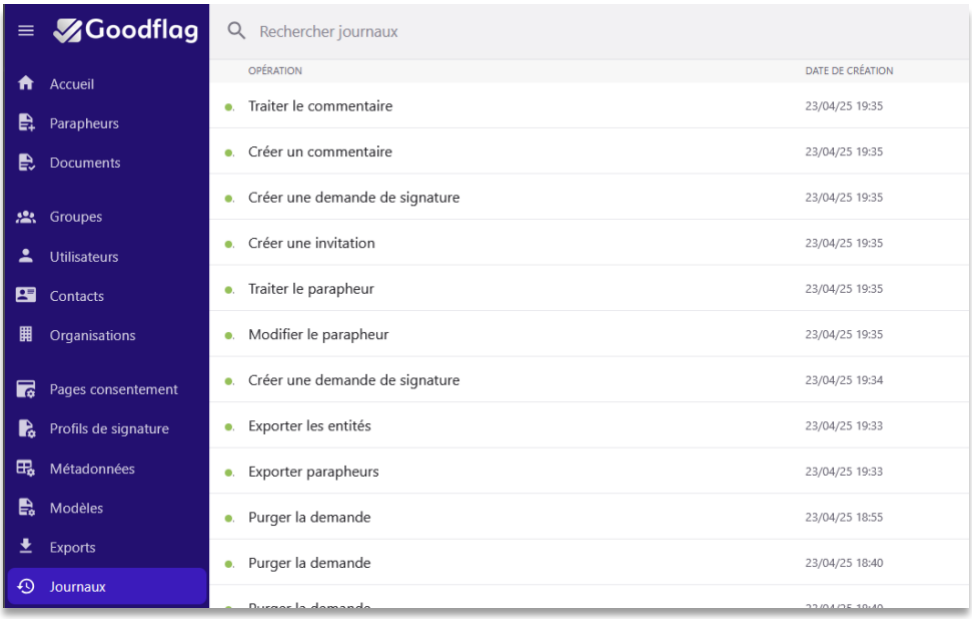
La solution Goodflag Signature propose des indicateurs visuels et des boutons d'action rapide afin de faciliter la navigation de l'Utilisateur et rendre la solution plus intuitive.

Intitulé	Bouton
État d'avancement des Parapheurs précisée en pourcentage et matérialisée par une barre d'avancement	
Statut du Parapheur caractérisé par un code couleur	
Bouton pour visualiser le détail d'un item dans une nouvelle fenêtre	
Bouton pour visualiser le détail d'un item dans la même fenêtre	
Bouton « Valider » pour accéder directement à la page de Validation	
Bouton « Signer » pour accéder directement à la page de Signature électronique	
Bouton « Corbeille » pour supprimer un Parapheur	
Bouton « + » pour créer un nouvel item	
Affichage du nombre de notifications non lues	
Bouton pour « Anonymiser » un 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.

4.6 — Journalisation

Toutes les opérations effectuées dans l'application sont historisées et disponibles au niveau du volet « Journaux ».



Journaux

Les journaux sont uniquement visibles par l''Utilisateur qui dispose du rôle d'administration d'un Tenant.

Les journaux sont conservés 30 jours.

Chaque appel à l'API crée une entrée dans le journal.

Ces journaux ne contiennent ni les Fichiers de Preuve, ni les éléments de traçabilité du cycle de vie des Parapheurs.

4.7 — Exports & imports des données

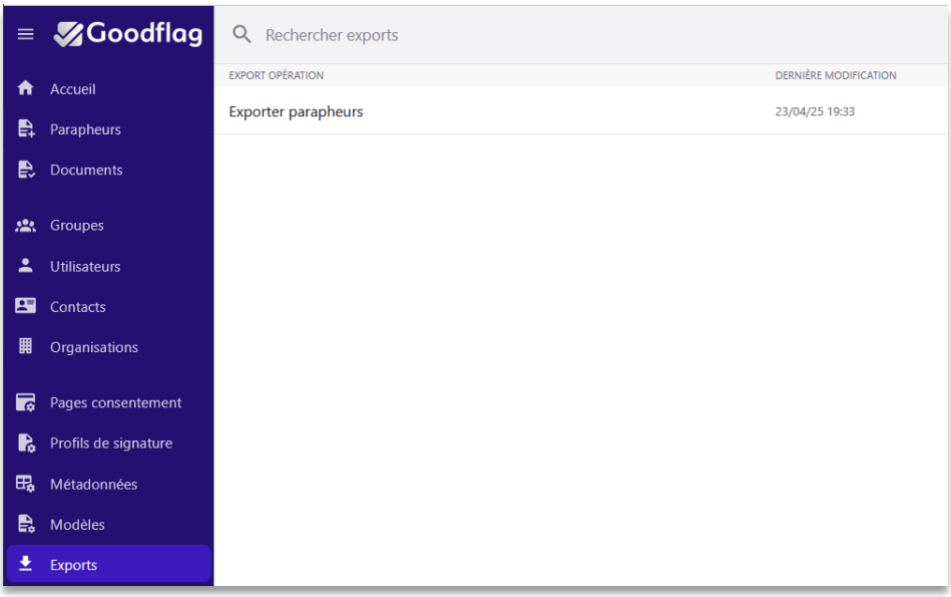
4.7.1 — Exports des données

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.

Pour les exports au format CSV, il est possible de choisir d'inclure ou non les en-têtes de colonnes.



Liste des exports

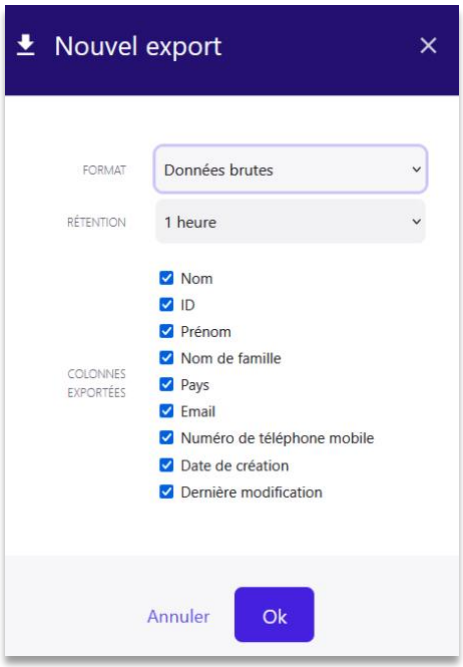
Pour visualiser cet export, il est nécessaire de disposer d'un des deux rôles suivants :

- Le rôle basique de « visualisateur des exports ».
- Le rôle d'« administrateur du tenant » ;

4.8 — Export des utilisateurs et contacts

La solution Goodflag Signature vous permet d'exporter vos Contacts et vos Utilisateurs sous format JSON ou CSV (avec ou sans en-têtes).

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



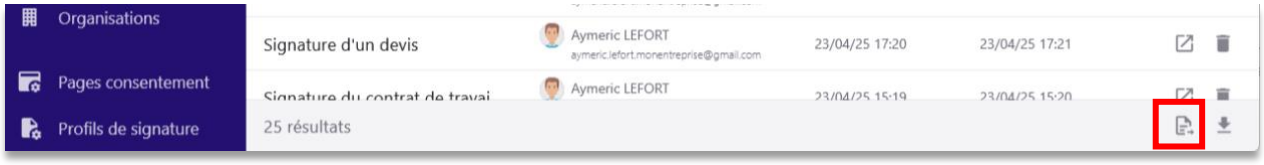
Export des Contacts

4.8.1 — Téléchargement en masse des documents signés

Depuis le volet « Parapheur », une fonctionnalité permet de télécharger en masse les documents signés associés aux parapheurs affichés dans les résultats.

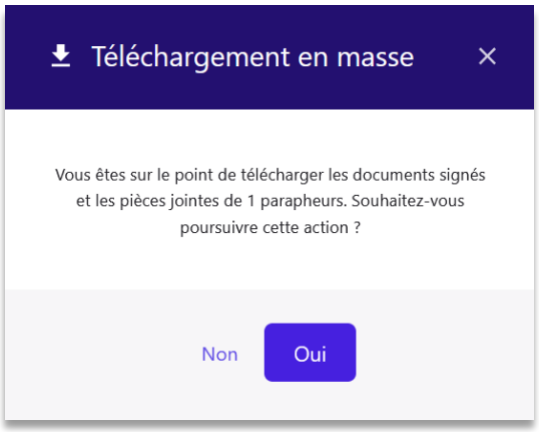
Pour accéder à cette fonctionnalité, l'utilisateur dispose soit du rôle d'« administrateur du tenant », soit du rôle « Exportateur en masse des documents ».

Un bouton dédié déclenche le téléchargement en masse.



Bouton de téléchargement en masse

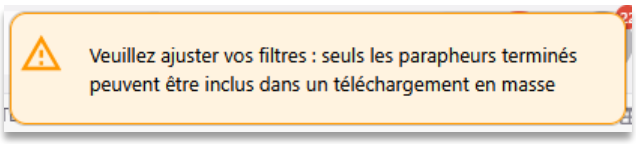
Lors de son activation, un message de confirmation s'affiche pour valider l'opération.



Message de confirmation

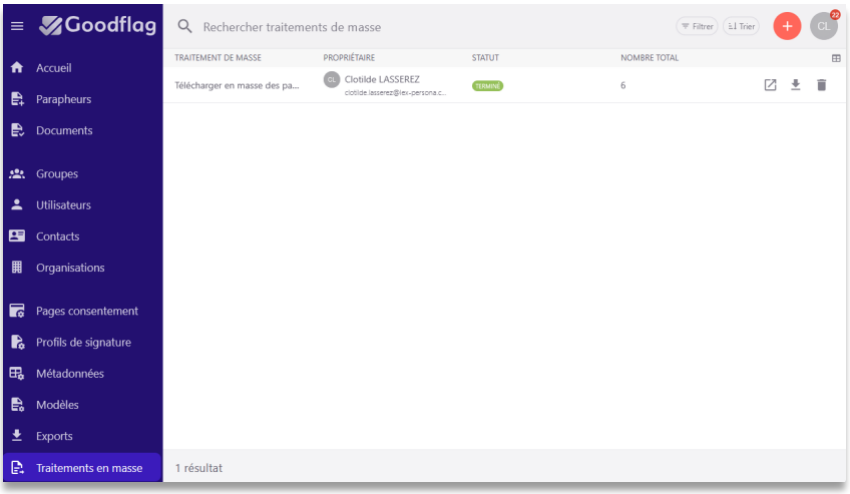
Si la liste de parapheurs est volumineuse, il est conseillé de la filtrer avant de lancer le téléchargement. Il est recommandé de ne pas dépasser 100 parapheurs.

Seuls les parapheurs terminés peuvent faire l'objet d'un téléchargement en masse. Si la sélection contient des parapheurs non terminés, un message d'alerte invite à ajuster les filtres.



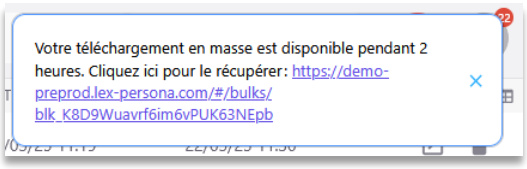
Message d'alerte

Les fichiers générés sont accessibles dans le volet « Traitements en masse », selon la durée de conservation définie lors de l'opération.



Volet « traitements en masse »

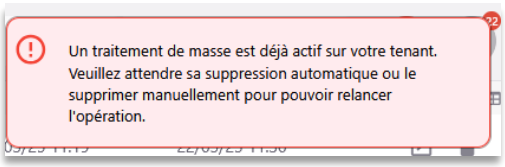
Chaque traitement est valable pendant 2 heures. Passé ce délai, il est purgé, et un nouveau traitement peut alors être initié.



Message informatif

Un seul traitement en masse peut être lancé à la fois par tenant.

Un message d'erreur s'affiche lorsque vous souhaitez générez un deuxième téléchargement en masse.



Message d'erreur

Nous vous recommandons de télécharger le fichier ZIP, puis de supprimer le traitement en masse si vous souhaitez lancer une nouvelle opération.

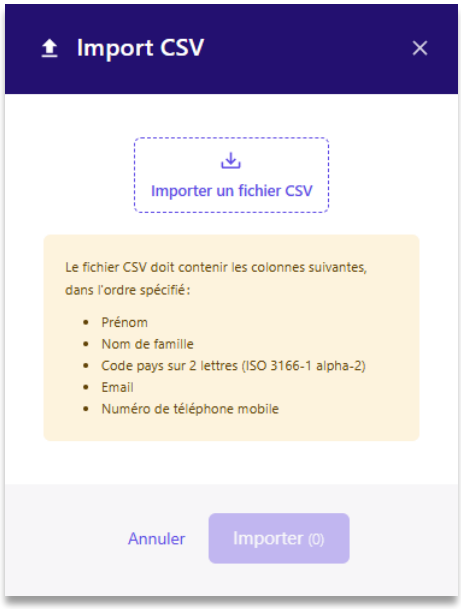
Toutes les opérations de téléchargement en masse sont tracées dans les journaux.

4.8.2 — Imports des utilisateurs & contacts

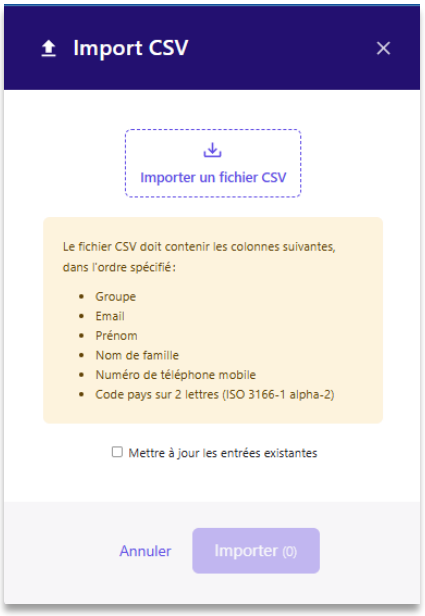
La solution Goodflag Signature permet d'importer vos Contacts et vos Utilisateurs grâce à l'import d'un fichier .CSV.

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



Import des Utilisateurs

Cette fonction vous permet d'importer de nouvelles données ou de mettre à jour les données existantes. Une case à cocher est prévue à cet effet.

4.9 — Langue de l'interface

Le portail est disponible en deux langues : le français et l'anglais.

Le parcours du Signataire est disponible en 3 langues : le français, l'anglais et l'allemand.

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 Validateur ou un Signataire accède à la page d'invitation.

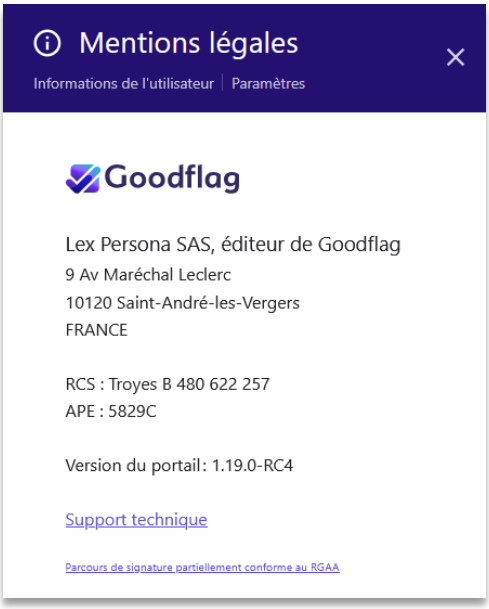
4.10 — Déclaration d'accessibilité RGAA

Pour offrir une expérience plus accessible à l'ensemble de nos utilisateurs, nous mettons désormais à disposition notre déclaration d'accessibilité RGAA (Référentiel Général d'Amélioration de l'Accessibilité).

Le RGAA a pour objectif de garantir que les services numériques restent accessibles au plus grand nombre, notamment aux personnes en situation de handicap.

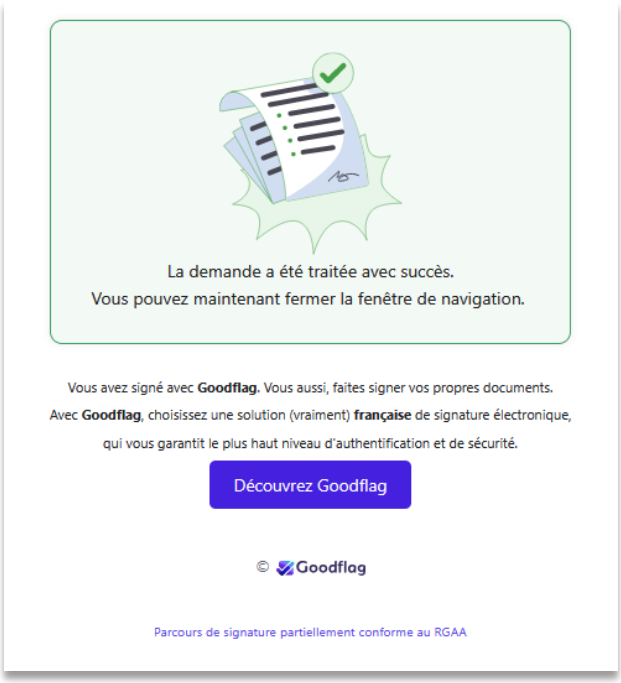
Vous pouvez consulter cette déclaration à tout moment :

- Depuis la section « À propos » du Portail ;



Section « A propos »

/ Depuis les écrans de fin de parcours des demandes traitées, refusées ou expirées.



Ces points d'accès renvoient vers une page web dédiée, conçue pour présenter clairement notre niveau d'accessibilité et nos engagements : Déclaration d'accessibilité

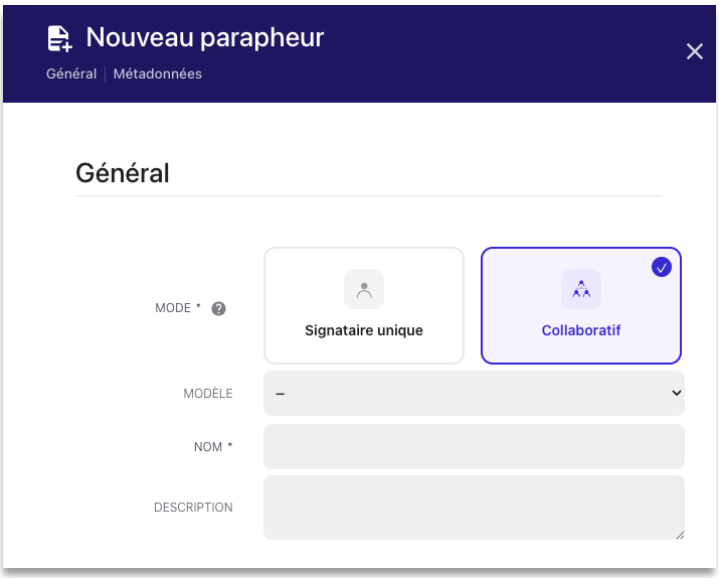
Aujourd'hui, notre parcours de signature est partiellement conforme, et nous poursuivons activement nos efforts pour en améliorer l'accessibilité.

5 — Expérience Créateur d'un parapheur mode collaboratif

5.1 — Sélection du mode de parapheur

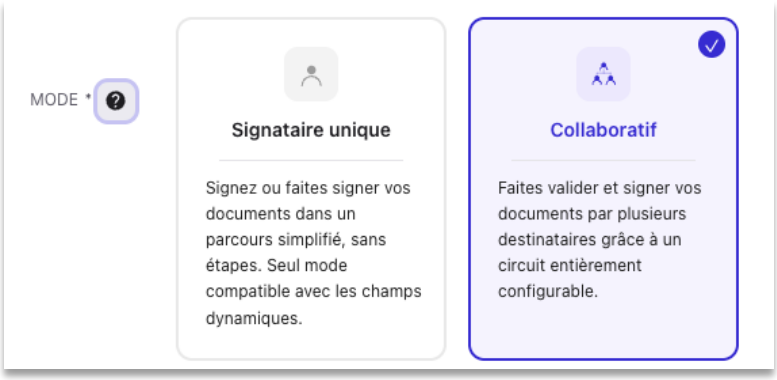
Lors de la création d'un parapheur, l'utilisateur a le choix entre deux modes de parapheur :

- Signataire unique
- Collaboratif



Nota bene : si la sélection du mode n'apparaît pas, le mode Signataire unique a été désactivé au niveau du tenant par votre administrateur. Seul le mode Collaboratif est alors proposé.

Une info-bulle d'aide au choix est accessible en cliquant sur l'icône « point d'interrogation ».



Affichage de l'info-bulle

- Quand choisir le mode Signataire unique

Ce mode est adapté lorsque le parapheur ne comporte qu'un seul signataire ou que vous êtes vous-même le signataire. Il permet en outre le paramétrage des champs dynamiques.

⁄ Quand choisir le mode Collaboratif

Ce mode est adapté lorsque plusieurs destinataires doivent valider et/ou signer le document. Il permet de paramétrer un workflow avec des étapes en série ou des destinataires en parallèle. Selon votre configuration, il offre également la possibilité de créer un parapheur à partir d'un modèle prédéfini ou de l'associer à une disposition de métadonnées.

À noter : les champs dynamiques ne sont pas disponibles dans ce mode.

Un tableau comparatif des deux modes est disponible au chapitre 6.9.

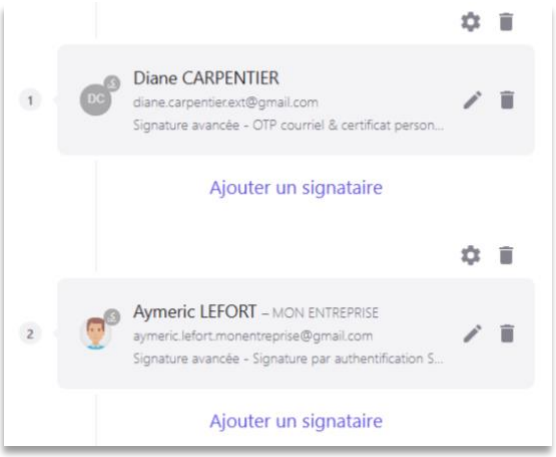
5.2 — Paramétrage des étapes

Dans la solution Goodflag Signature, il est très facile de créer des circuits de Signature(s) électronique(s) et/ou de Validation(s) électronique(s) appelés Parapheurs.

Le terme Parapheur est traduit dans la version anglaise par « Workflow ».

5.2.1 — Étapes séquentielles

La solution permet d'ajouter des étapes de Validation(s) ou de Signature(s) électroniques séquentielles.



Exemple de deux étapes séquentielles

5.2.2 — Destinataires en parallèle

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

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

Exemple de deux étapes de validation en parallèle

Une même étape ne peut pas contenir à la fois des Signataires et des Validateurs (en parallèle). Les étapes doivent être séquentielles.

Nota bene : Il n'existe pas de limite sur le nombre de Signataires. S'il y a beaucoup de Signataires, il est possible de paramétrer une Signature électronique non visible (absence de pavé de signature sur le document). 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.

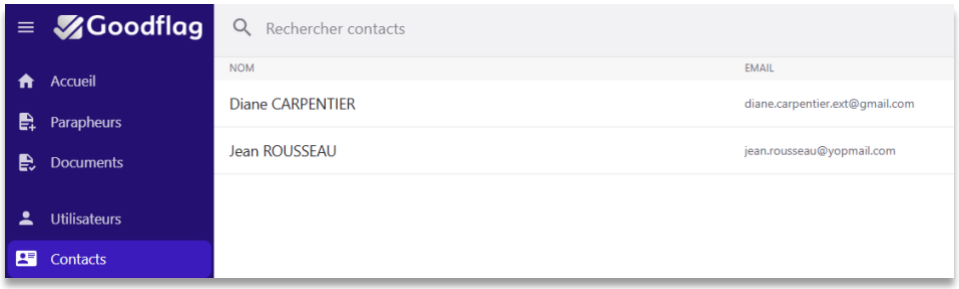
5.2.3 — Destinataires d'une étape

Lors de la création d'un Parapheur, le Gestionnaire d'un Parapheur peut sélectionner soit un Contact, soit un Utilisateur comme Validateur ou Signataire du Parapheur.

L'Utilisateur peut également le créer « à la volée », s'il dispose du droit

Il faut bien différencier la notion d'Utilisateur de celle de Contact :

- Un Utilisateur appartient à un Tenant ; en fonction des rôles et des permissions de son Groupe, il pourra voir et/ou être vu par d'autres Utilisateurs, il pourra administrer la solution, créer des Parapheurs, valider et signer des Parapheurs ;
- Un Contact est une personne physique qui appartient à l'annuaire privé d'un Utilisateur. Un Contact est donc propre à un Utilisateur ; en constituant un annuaire de Contacts, le Gestionnaire d'un Parapheur 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

Chaque Contact est caractérisé par un prénom, un nom, un pays, une adresse courriel.

D'autres champs sont facultatifs comme les champs « numéro de téléphone mobile » et « commentaires ».

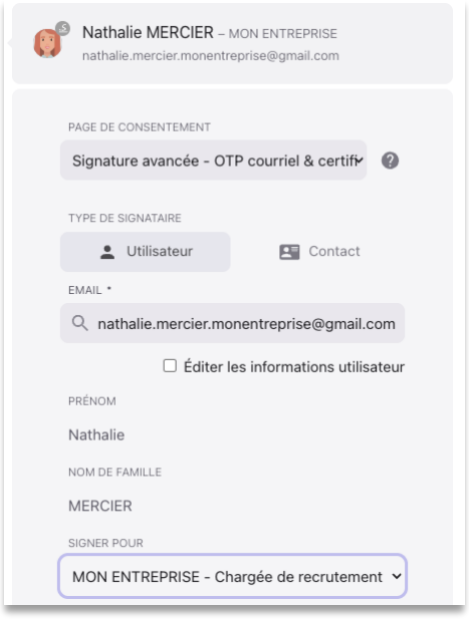
Chaque Utilisateur peut créer les Contacts qu'il souhaite et constituer son annuaire privé.

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

Attention : l'API ne peut accéder aux Contacts d'un Utilisateur qu'en étant connectée en tant que l'Utilisateur lui-même.

5.2.4 — Signature au nom d'une organisation

Lorsqu'un utilisateur est associé à une organisation et/ou une fonction, l'étape peut être configurée pour qu'il signe au nom de cette organisation et/ou de cette fonction.

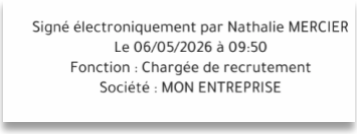


Champ « Signer pour » - Étape

La page de consentement associée à l'étape doit l'autoriser. Dans le détail de la page de consentement, le champ « Autoriser le destinataire à signer pour une organisation » doit être positionné sur Oui.

Champ « Signer pour » - Page de consentement

L'organisation et la fonction peuvent être restituées dans le texte de signature visible apposé sur le document, à condition que le profil de signature le prévoie.



Texte de signature visible

Nota bene : cette fonctionnalité est disponible pour les deux modes de Parapheur.

5.2.5 — Suivi des étapes

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 », « validé », « 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.

5.3 — Pages de Consentement

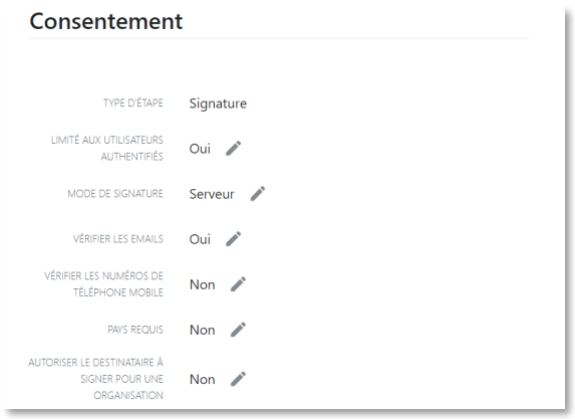
Une Page de Consentement est un ensemble de paramètres permettant de configurer le parcours de Signature ou de Validation électronique d'un destinataire.

La Page de Consentement permet de recueillir le consentement du Validateur ou du Signataire dans le cadre d'un Parapheur déterminé.

Pour chaque Page de Consentement, est défini :

- Le type d'étape : Validation ou Signature électronique ;
- La méthode de Signature électronique : serveur (à distance) ou locale ;
- Les moyens d'authentification requis ;
- La charte graphique (logo de l'organisation et couleur).

Nota bene : L'administrateur peut désactiver une Page de Consentement afin de la rendre inutilisable pour les Utilisateurs. S'il le souhaite, il peut la réactiver ultérieurement.

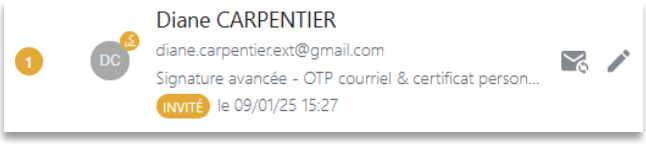


Paramétrage d'une Page de Consentement pour une signature serveur avec OTP courriel

La gestion des pages de consentements s'effectue soit depuis le Portail Web, soit via l'API.

L'administrateur d'un Tenant accède via l'API aux fonctionnalités suivantes : création et modification des pages de consentement, récupération d'une Page de Consentement existante ou de l'ensemble des pages de consentement d'un Tenant.

Nota bene : la page de consentement est affichée au niveau de l'étape.

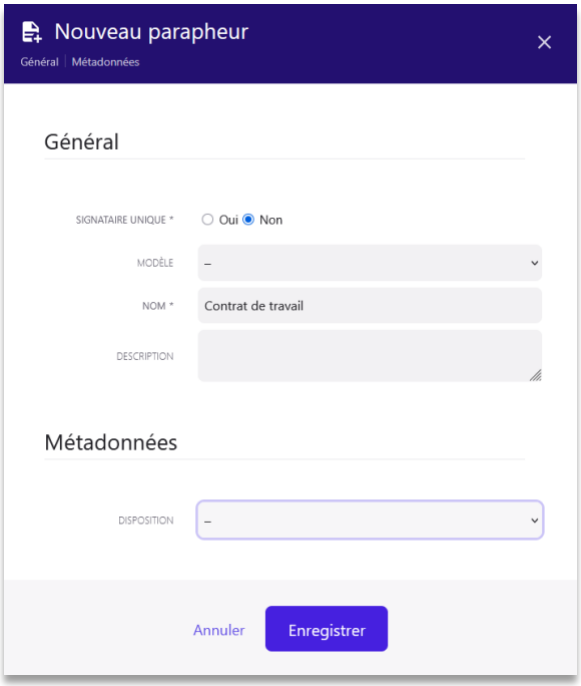


Libellés d'une étape

5.4 — Dispositions de métadonnées

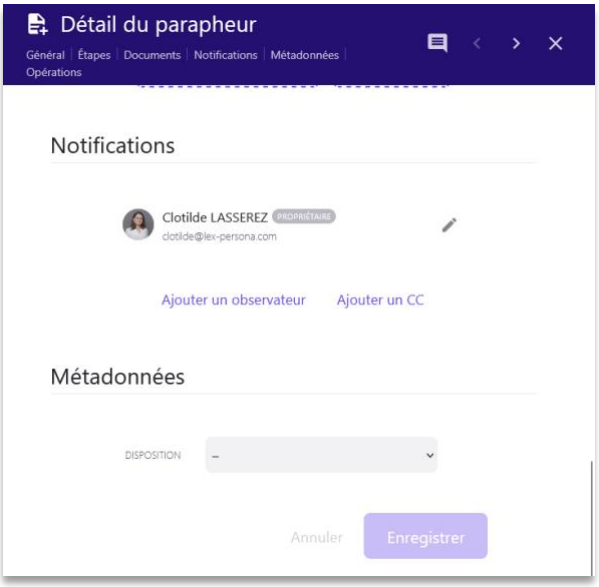
L'utilisateur peut associer une disposition de métadonnées au Parapheur :

- Soit lors de la création du Parapheur ;



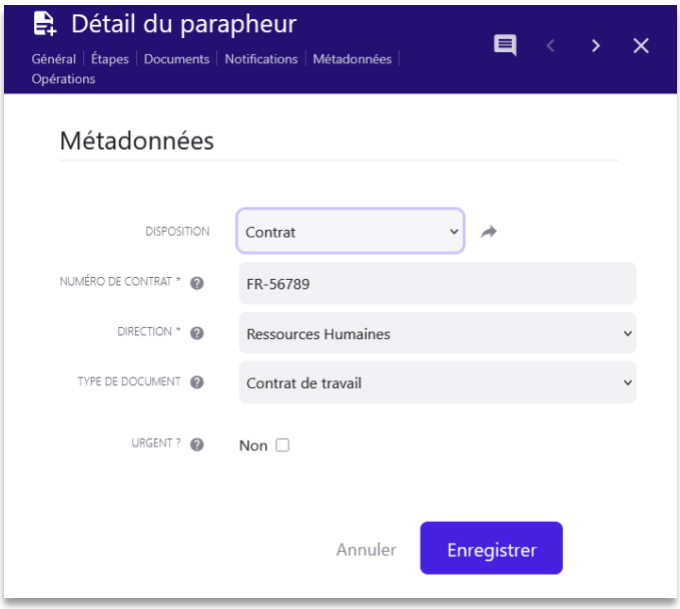
Nouveau parapheur

- Soit depuis le détail du Parapheur, après sa création.



Détail du parapheur : aucune disposition n'a été associée

Lorsque, au moment de la création, une disposition de métadonnées est associée au Parapheur, l'Utilisateur peut soit modifier les champs de cette disposition, soit choisir une autre disposition.



Détail du parapheur : une disposition a été associée

Les dispositions de métadonnées constituent une fonctionnalité importante et différenciante de la solution. Elles sont accessibles depuis le menu contextuel depuis le Portail ou l'API, en fonction des droits accordés à l'Utilisateur.

En ce qui concerne les métadonnées, il y a deux niveaux à distinguer :

- Les métadonnées ;
- Les dispositions de métadonnées.

Les métadonnées permettent l'indexation des Parapheurs et sont utilisées comme filtres de recherche. Elles peuvent également être affichées comme en-tête des colonnes des listes de Parapheurs.

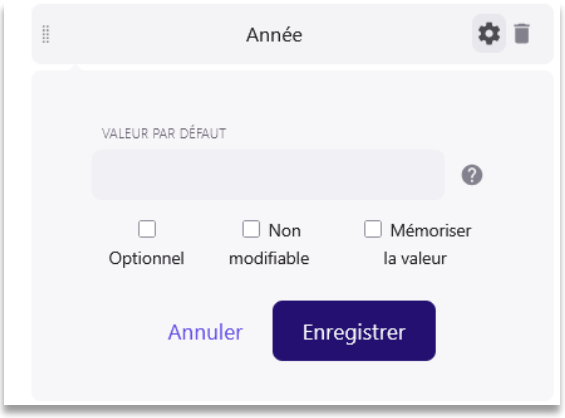
Nota bene : Il est possible de paramétrer jusqu'à 16 métadonnées au sein d'un même Tenant. Ce nombre permet de couvrir la plupart des usages client. A noter que ce nombre maximum peut être augmenté sur demande motivée d'un client.

Une métadonnée peut être de type case à cocher, texte sur une seule ligne, texte multilignes ou liste déroulante et peut également contenir une aide contextuelle qui sera affichée au Gestionnaire lors de l'utilisation de cette métadonnée.

Les dispositions de métadonnées utilisées dans les Parapheurs sont quant à elles un sous-ensemble de métadonnées paramétrées en amont par les administrateurs fonctionnels et complétés par les créateurs lors du paramétrage des Parapheurs.

Pour chaque métadonnée utilisée dans une disposition, il est possible de préciser :

- Sa valeur par défaut ;
- Si elle est obligatoire ou facultative ;
- Si elle est modifiable ;
- Si sa dernière valeur sera conservée en cache dans le navigateur de l'Utilisateur.



Paramétrage d'un champ de métadonnée

La liste des dispositions de métadonnées proposées aux créateurs de Parapheurs dépendra :

/ Soit des droits du Groupe d'Utilisateurs auquel le créateur appartient dans le cas où il n'utiliserait pas de modèle ;

/ Soit du paramétrage du modèle à partir duquel le Parapheur est créé.

En effet, dans le paramétrage d'un Groupe, il est possible de spécifier les dispositions de métadonnées qui pourront être utilisées par les créateurs de Parapheur appartenant à ce Groupe. Néanmoins, si le créateur d'un Parapheur sélectionne un modèle de Parapheur, ce sont les dispositions de métadonnées proposées via le modèle qui prévalent sur celles spécifiées pour le Groupe.

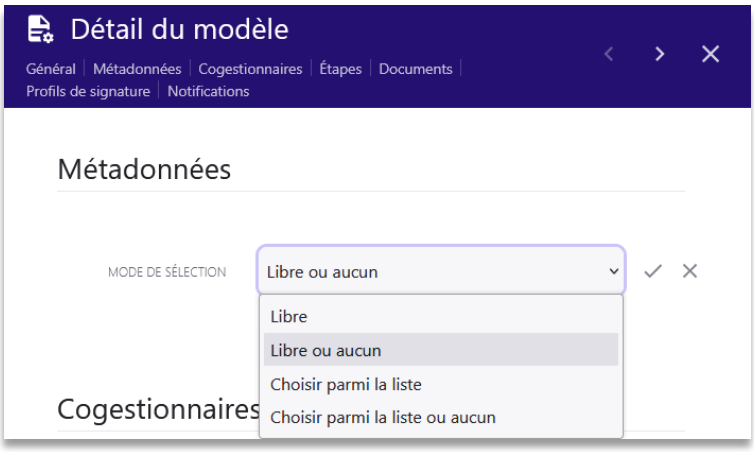
Nota bene : l'utilisation de cette fonctionnalité est optionnelle lors de la création d'un Parapheur.

Lorsque les dispositions de métadonnées sont liées à un modèle de Parapheur, plusieurs paramétrages sont possibles :

/ Soit le créateur du Parapheur choisit librement la disposition de métadonnées qu'il souhaite utiliser ;

/ Soit il la choisit parmi une liste définie ;

/ Soit celle-ci est imposée par le modèle.



Paramétrage des métadonnées au niveau d'un modèle

Les dispositions de métadonnées offrent de nombreux avantages, en effet, elles permettent :

/ D'ajouter des informations spécifiques au Parapheur ;

/ D'organiser les Parapheurs en les regroupant via une métadonnée (exemple : par typologie de documents) ;

/ De faciliter les filtrages et les recherches des Parapheurs ;

/ De faciliter les interfaçages avec les applications métier (GED, SAE, etc.) grâce aux données indexées.

5.5 — Configurations d'une étape

Chaque étape est caractérisée par :

/ La nature de l'étape : Validation ou Signature électronique ;

/ La Page de Consentement (qui définit comment la signature doit se dérouler) ;

/ Le destinataire : soit un Utilisateur du Portail, soit un Contact (qui définit QUI doit valider ou signer) ;

/ La durée de validité d'une étape au-delà de laquelle elle expirera : lorsqu'un Utilisateur ajoute une étape de Validation ou de Signature électronique, il peut définir la durée de validité de cette étape. Lorsque cette durée est atteinte, alors l'étape de Validation ou de Signature électronique devient obsolète ;

/ La fréquence d'envoi des invitations : tous les jours, toutes les semaines, toutes les deux semaines, tous les mois ;

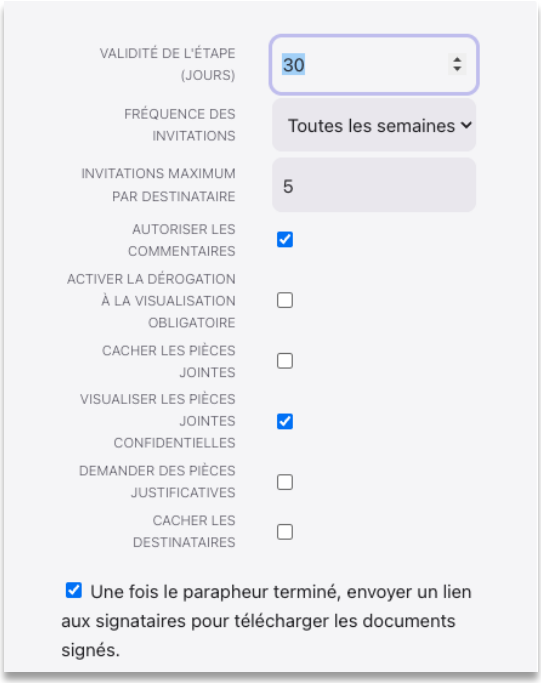
/ Le nombre de relances maximum ;

/ 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 et Validateurs de l'étape ;

/ La possibilité d'activer une dérogation à la visualisation obligatoire (si l'option est activée, les destinataires de l'étape sont dispensés de cette obligation, même lorsque le profil de signature l'impose) ;

- La possibilité de cacher l'ensemble des pièces jointes aux Signataires ou Validateurs de l'étape ;
- La possibilité de définir si les destinataires de l'étape visualiseront ou non les pièces jointes confidentielles ;
- La possibilité de demander au Signataire des pièces justificatives (si la fonctionnalité est activée pour votre espace) ;
- La possibilité d'activer le mode Signature en-face-à-face (si la page de consentement le permet, si l'étape est en série et si le signataire est de type « Contact ») ;
- La possibilité de cacher les destinataires aux Signataires ou Validateurs de l'étape, si la case est cochée, le Signataire ou le Validateur 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 la langue préférée du destinataire de l'étape, en sélectionnant :

- Pour un Utilisateur, soit les préférences Utilisateur, soit une langue parmi la liste proposée : le français ou l'anglais ;
- Pour un Contact la langue préférée parmi cette même liste.

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.

Le paramétrage des Parapheurs s'effectue soit depuis le Portail Web de la solution, soit via l'API. Il existe en effet plusieurs méthodes API pour la gestion des circuits de signature : création d'un nouveau Parapheur, chargement d'un document, ajout d'un commentaire pour un Parapheur, lancement d'un Parapheur, récupération des documents signés et des Fichiers de Preuve d'un Parapheur.

5.6 — Commentaires

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

Il est possible de désactiver cette fonctionnalité dans le paramétrage de l'étape.

Option « Autoriser les commentaires »

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

Par défaut, un fil de discussion, à l'initiative d'un Gestionnaire est public, c'est-à-dire qu'il est visible des autres Gestionnaires mais également des destinataires du Parapheur qui visualisent les commentaires au moment de la Validation ou de la Signature électronique.

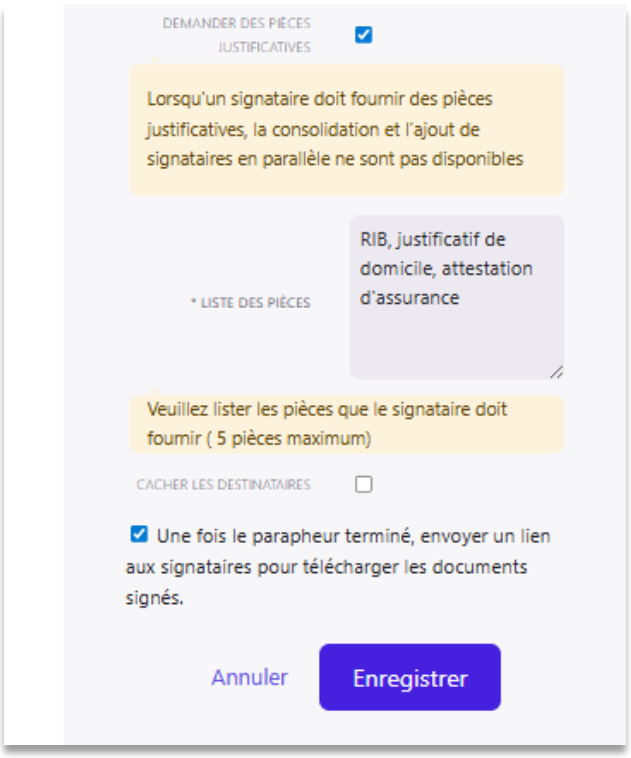
Si ce fil de discussion est rendu confidentiel par le Gestionnaire, il ne sera visible que par lui et les autres Gestionnaires. Une icône permet d'identifier le commentaire confidentiel.

5.7 — Demande de pièces justificatives auprès du Signataire

Le Gestionnaire de Parapheur peut activer, sur une étape de Signature une demande de pièces justificatives.

Cette fonctionnalité n'est pas disponible pour une étape de Validation.

Une fois la fonctionnalité activée, il peut lister les pièces requises, en étant informé que le Signataire ne pourra téléverser que cinq fichiers au maximum.



« Demander des pièces justificatives »

Nota bene : l'ajout de Signataires en parallèle ainsi que la consolidation ne sont pas disponibles lorsqu'une demande de pièces est paramétrée pour l'étape.

Dans le cadre de cette fonctionnalité, nous vous invitons à rédiger une notice d'information à destination de vos Signataires et de l'ajouter dans le détail de votre tenant.

Notre DPO se tient à votre disposition pour vous accompagner : dpo@goodflag.com

Une fois ajoutée, la notice sera accessible aux Signataires depuis la page d'ajout de pièces.

À défaut, nous invitons les Signataires à se rapprocher du Responsable du traitement afin de connaître les modalités de traitement de leurs données lors de l'ajout de pièces.

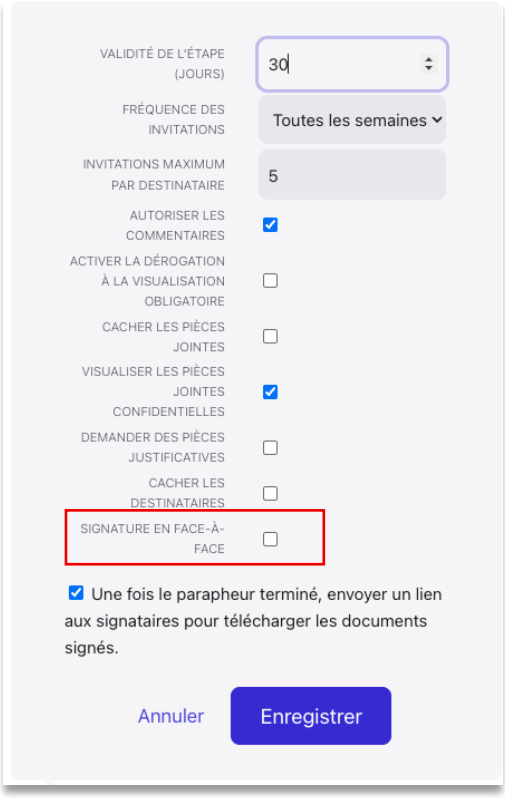
5.8 — Activation du mode Signature en face-à-face

Le créateur d'un Parapheur peut activer le mode face-à-face sur une étape donnée.

Dans ce mode, aucune notification courriel d'invitation à signer n'est envoyée : le signataire signe directement depuis le Portail, sur l'appareil de l'Utilisateur qui anime la session de signature.

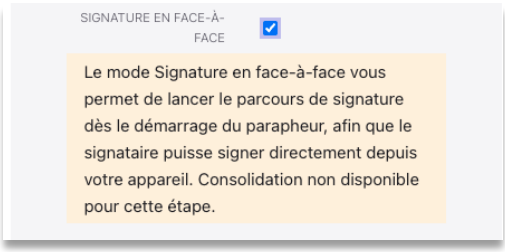
Ce mode est utile typiquement pour une signature en présentiel (rendez-vous client, guichet, etc.).

Le mode face-à-face s'active uniquement sur une étape configurée en série, dont la page de consentement est de type OTP mail ou SMS et le signataire est un contact.



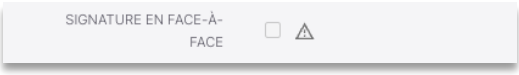
Paramètres de l'étape

Lorsque l'option est activée, une info-bulle précise au gestionnaire le principe du paramètre.



Activation du paramètre

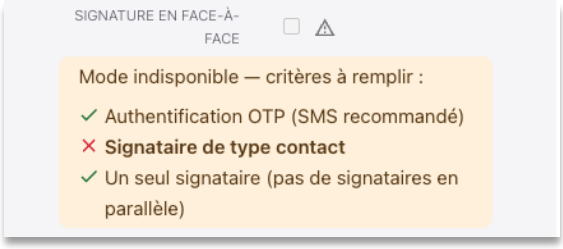
L'option n'est pas activable si l'étape ne remplit pas les critères précédemment cités.



Paramètre désactivé

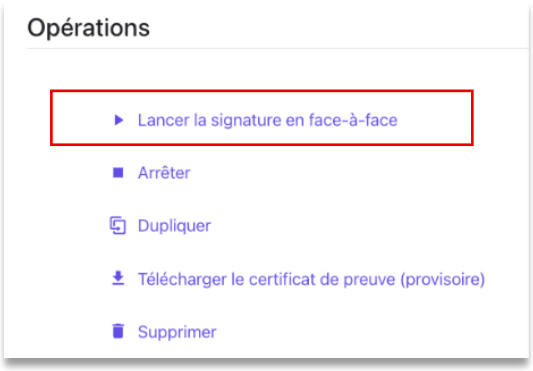
Le Gestionnaire peut cliquer sur l'icône « Triangle » pour afficher le détail des critères satisfaits et non satisfaits.

Un critère rempli est signalé par une coche verte ; un critère non rempli est signalé par une croix rouge et affichée en gras.

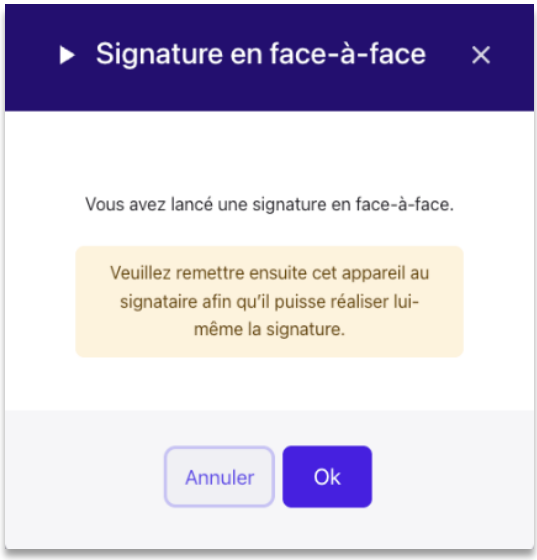


Critères à remplir

Lorsque le créateur ou l'Utilisateur qui anime la session démarre le Parapheur, une nouvelle opération apparaît dans le détail du Parapheur : « Lancer la signature en face-à-face ».



Un écran indique à l'Utilisateur de remettre l'appareil au signataire pour qu'il procède à la signature.



L'expérience du signataire est décrite dans le chapitre 7.5.

Nota bene : cette fonctionnalité n'est actuellement disponible que pour le mode collaboratif.

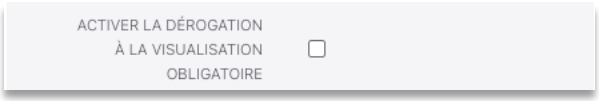
5.9 — Téléversement des documents

L'utilisateur peut ajouter des documents via l'explorateur de fichiers ou par glisser-déposer. Deux encarts distincts sont disponibles : l'un pour les documents à valider et signer, l'autre pour les pièces jointes.

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

Selon le profil de signature configuré, la visualisation des documents peut être obligatoire ou facultative pour le signataire.

Si l'option de dérogation est activée sur une étape, les destinataires concernés sont dispensés de cette obligation, même lorsque le profil de signature l'impose.



Paramètre d'une étape

Le gestionnaire peut ajouter des documents un par un ou en lot. Les archives ZIP sont acceptées et décompressées automatiquement si l'option « Décompresser les zips » est activée. Une fois les documents téléversés, il est possible de générer une archive ZIP regroupant l'ensemble des documents et pièces jointes.

Nota bene : Le nombre de documents par lot n'est pas limité. Néanmoins, le processus de signature est conçu pour fonctionner sur un usage raisonnable de documents et de signataires par parapheur. Tout usage excessif peut amener à une dégradation des temps de réponse.

Chaque document téléversé est associé aux métadonnées suivantes :

- Lien vers le parapheur associé
- Propriétaire du parapheur (accessible aussi depuis le parapheur)
- Groupe du propriétaire (accessible aussi depuis le parapheur)
- Date de création
- Date de dernière modification

Les documents téléversés sont consultables depuis la section Documents du menu contextuel, où l'utilisateur peut accéder à leurs informations et les télécharger. Ils sont également accessibles depuis le menu Parapheurs, au niveau de chaque parapheur.

5.9.1.1. Téléversement des pièces jointes

Les pièces jointes sont présentées au signataire en lecture et en téléchargement, mais ne font pas l'objet d'une signature. Le format accepté (.pdf, .docx, .jpg, etc.) est configurable au niveau du tenant, ce qui permet de maîtriser les formats autorisés.

En tant que créateur du parapheur, il est possible de masquer les pièces jointes aux destinataires d'une étape — ce paramètre se configure au niveau de l'étape concernée.

5.9.2 — Conversion des fichiers au format PDF

5.9.2.1. Conversion des documents PDF

Lors du téléversement d'un document PDF dans un Parapheur, la solution procède automatiquement à sa conversion au format PDF/A.

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

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

5.9.2.2. Conversion des documents Microsoft Office

Une option permet également d'activer la conversion automatique des documents Microsoft Office (Word, Excel et PowerPoint) en PDF/A lors de leur téléversement dans un Parapheur.

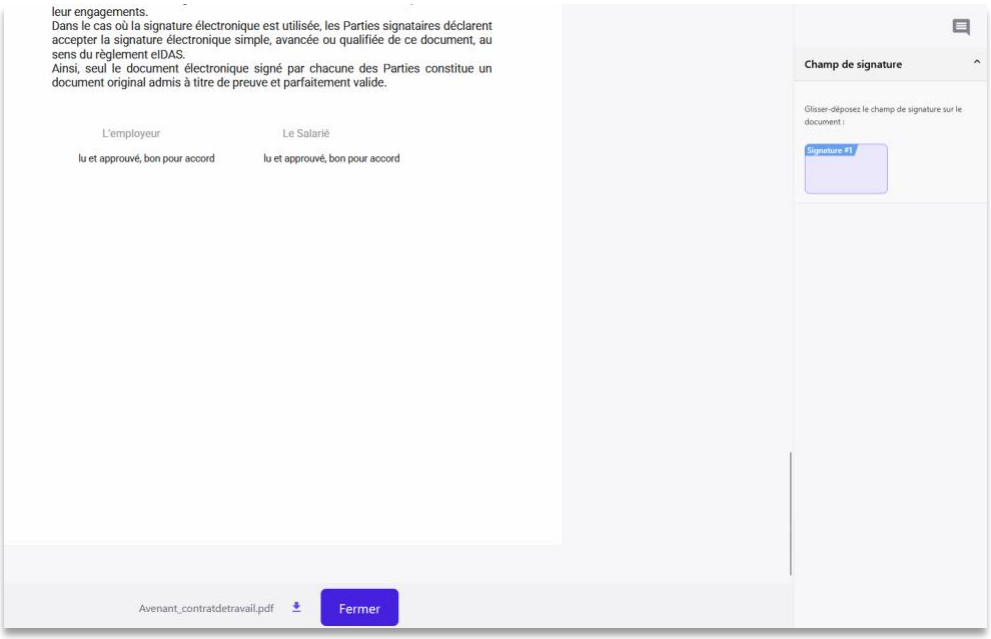
Option de conversion en PDF

La conversion en PDF/A effectuée lors du téléversement peut entraîner de légères variations visuelles par rapport au document initial. Il est donc fortement recommandé de contrôler le fichier généré afin de valider qu'il est conforme à vos attentes.

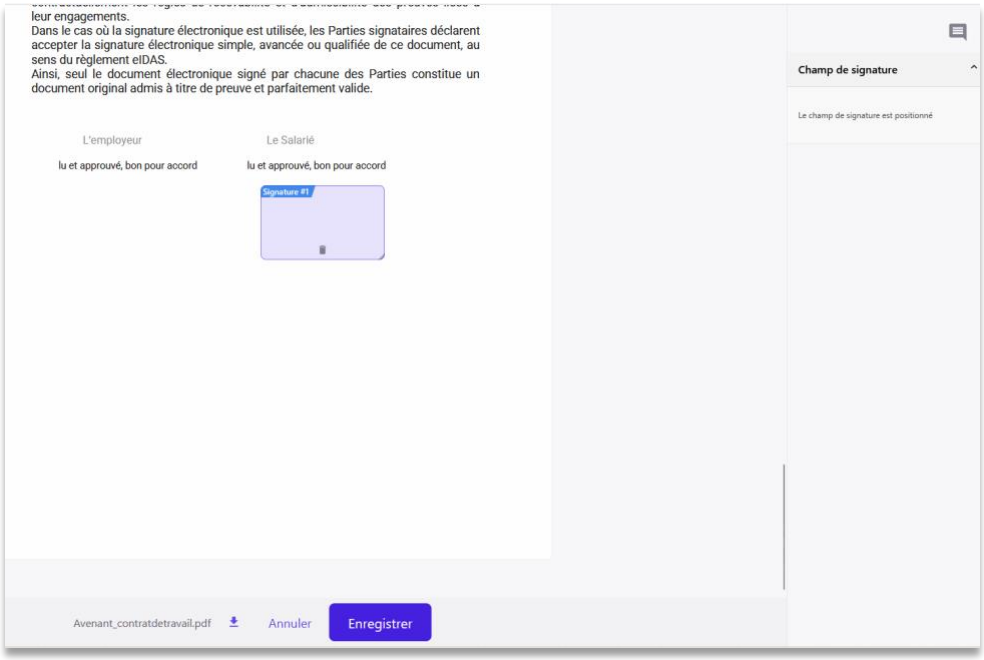
5.9.3 — Positionnement des champs de signature visible

Après avoir téléversé le document à signer, un Gestionnaire 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.



Avant positionnement du champ de signature



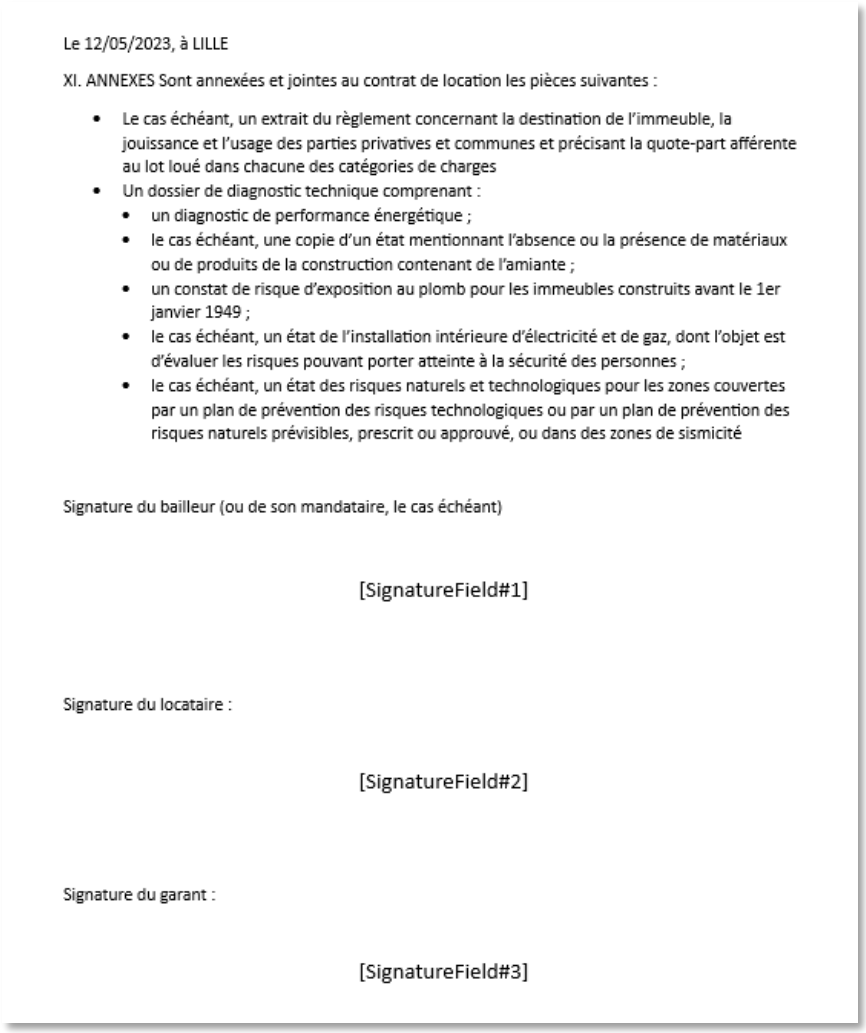
Post positionnement du champ de signature

5.9.4 — Positionnement automatique des champs de signature visible

Un Gestionnaire peut également créer un Parapheur ou un modèle de Parapheur en téléversant un document comportant des jokers de champs de signature.

Cette fonctionnalité ne concerne que les documents PDF signés au format de signature PAdES, issus ou non de documents Microsoft Office (tm).

Un joker de champ de signature est une chaine de caractères de la forme [SignatureField#i], où i est l'index du champ de signature électronique prévu dans le document. Ainsi [SignatureField#3] désigne le champ de la 3ème signature qui sera apposée sur le document. Si jamais le Parapheur ne prévoit que 2 signatures, alors ce 3ème champ de signature ne sera pas utilisé.



Le 12/05/2023, à LILLE

XI. ANNEXES Sont annexées et jointes au contrat de location les pièces suivantes :

- Le cas échéant, un extrait du règlement concernant la destination de l'immeuble, la jouissance et l'usage des parties privatives et communes et précisant la quote-part afférente au lot loué dans chacune des catégories de charges
- Un dossier de diagnostic technique comprenant :
  - un diagnostic de performance énergétique ;
  - le cas échéant, une copie d'un état mentionnant l'absence ou la présence de matériaux ou de produits de la construction contenant de l'amiante ;
  - un constat de risque d'exposition au plomb pour les immeubles construits avant le 1er janvier 1949 ;
  - le cas échéant, un état de l'installation intérieure d'électricité et de gaz, dont l'objet est d'évaluer les risques pouvant porter atteinte à la sécurité des personnes ;
  - le cas échéant, un état des risques naturels et technologiques pour les zones couvertes par un plan de prévention des risques technologiques ou par un plan de prévention des risques naturels prévisibles, prescrit ou approuvé, ou dans des zones de sismicité

Signature du bailleur (ou de son mandataire, le cas échéant)

[SignatureField#1]

Signature du locataire :

[SignatureField#2]

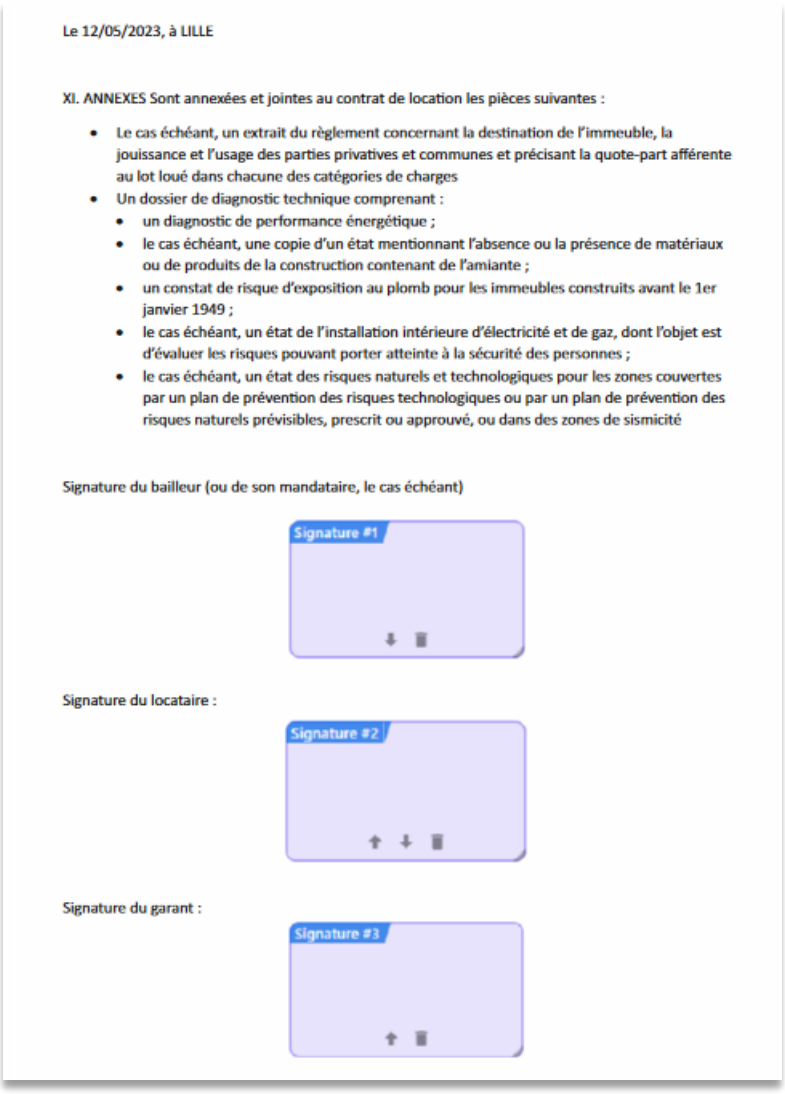
Signature du garant :

[SignatureField#3]

Bail de location avec jokers de signature

Les jokers de champs de signatures peuvent donc être placés dans n'importe quel ordre sur le document. Ainsi le champ de la 2ème signature peut figurer sur la 1ère page du document et le champ de la 1ère signature peut figurer sur la 2ème page du document.

Lorsque le document est téléversé, les jokers de champs de signatures sont automatiquement convertis en champs de signature PAdES dans le document PDF (qu'il soit converti ou non) en respectant l'ordre indiqué.



Champs positionnés automatiquement

Une fois le document téléversé et les jokers de champs de signatures convertis en champs de signature PAdES, le Gestionnaire reste libre de modifier l'emplacement des champs de signatures préalablement positionnés.

Il est également possible pour le Gestionnaire d'ajouter de nouveaux champs de signatures. Dans des documents Microsoft Word (tm), cette fonctionnalité permet de tirer parti des fonctions de publipostage qui peuvent faire varier automatiquement le positionnement des champs de signatures. A noter que le champ de Signature électronique au format PAdES qui se substitue au joker de champ de signature prend une dimension par défaut dont le Gestionnaire doit tenir compte dans la composition des documents à faire signer. Le coin haut et gauche du champ de signature PAdES correspond à la position du premier crochet ("[") du joker de champ de signature.

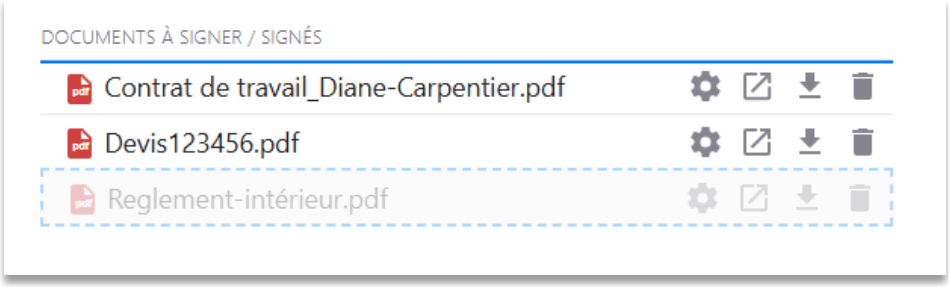
Attention : L'ajout de jokers de signature compromet l'intégrité des signatures ou cachets électroniques déjà présents sur le document.

Cette fonctionnalité va vous permettre de gagner en efficacité dans le paramétrage de vos Parapheurs, d'autant plus si vous l'associez aux modèles de Parapheurs.

5.9.5 — Ordonnancement des documents et des pièces jointes

La solution offre au propriétaire d'un parapheur la possibilité de réordonnancer les documents à signer ainsi que les pièces jointes de manière que les documents puissent être présentés au Signataire dans un ordre défini. Cet ordonnancement se fait par glisser/déposer.

Nota bene : il n'est pas possible de déplacer un document d'un répertoire.



Réordonnancement des documents à signer via glisser/déposer

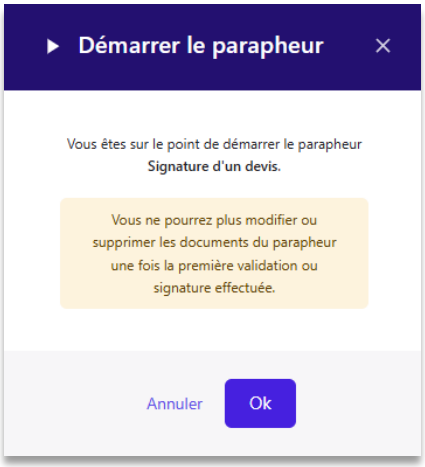
5.9.6 — Modification des documents

Il est possible d'ajouter ou de supprimer des documents :

- Soit tant que la première Validation électronique n'a pas été réalisée,
- Soit tant que la première Signature électronique n'a pas été réalisée.

Cette option se configure au niveau du tenant.

Lorsque l'utilisateur démarre un parapheur, un message lui précise les modalités du verrouillage de document.



Message d'information

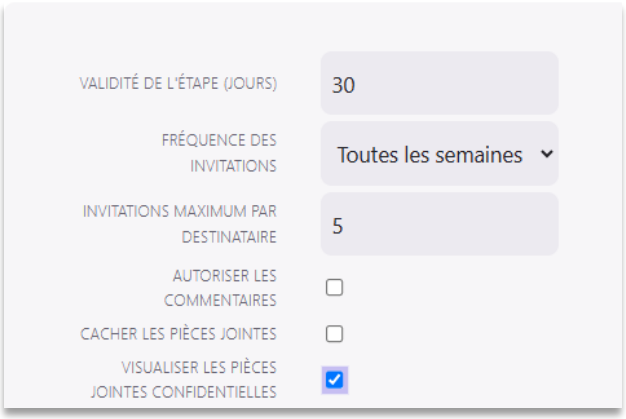
5.9.7 — Gestion de la confidentialité des pièces jointes

Il existe une option au niveau de l'étape qui permet de masquer l'ensemble des pièces jointes au(x) destinataire(s) de l'étape.

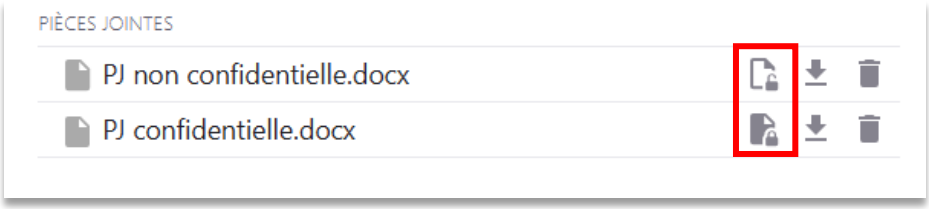
Cette option est libellée « cacher les pièces jointes ».

Option « cacher les pièces jointes » dans le paramétrage d'une étape

Il est également possible de gérer la confidentialité de chaque pièce jointe, afin que le propriétaire d'un parapheur puisse choisir lesquelles seront visibles ou non par les destinataires d'une étape. Pour cela, il peut marquer certaines pièces jointes comme confidentielles, puis décider, pour chaque étape, si les destinataires auront ou non accès à ces pièces jointes confidentielles.



Option « visualiser les pièces jointes confidentielles » dans le paramétrage d'une étape

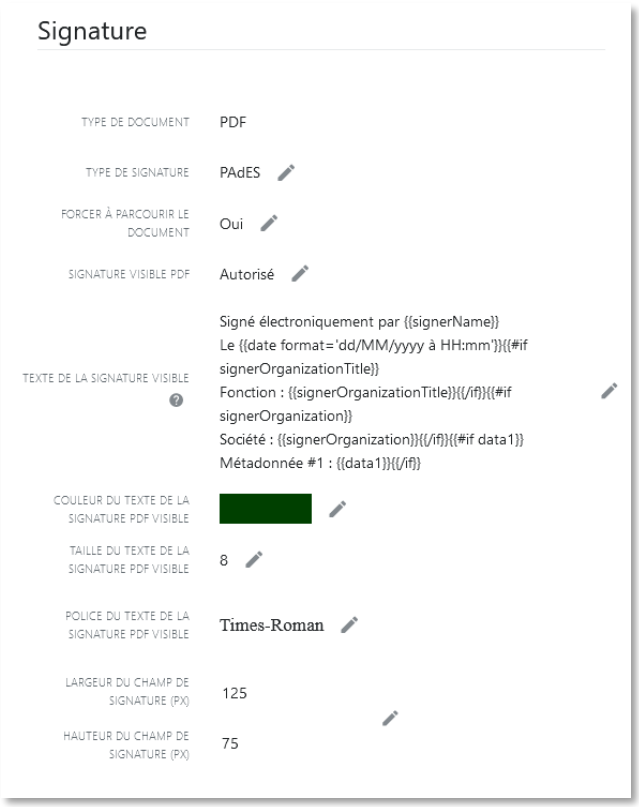


Boutons permettant de préciser la confidentialité de la pièce jointe

5.10 — Profils de signature

La solution permet d'affecter pour chaque document à faire signer un profil de Signature lors de son dépôt.

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



Exemple d'un profil de signature

Pour chaque Profil de signature, est défini :

- Le format de signature électronique : PAdES ou XAdES ;
- La possibilité pour le créateur du Parapheur de positionner les champs de signature visible sur les documents PDF (dans le cas du format PAdES) ;
- La visualisation obligatoire ou non obligatoire du document avant signature électronique ;
- La personnalisation du texte de signature visible ;
- La couleur du texte de signature visible ;
- La police du texte de signature visible ;
- La taille du texte de signature visible ;
- La taille de l'encart de signature ;
- L'ajout d'une image par défaut

Import d'une image signature imposée

Nota bene : L'administrateur peut désactiver un profil de signature afin de le rendre inutilisable pour les Utilisateurs. S'il le souhaite, il peut le réactiver ultérieurement.

Le paramétrage des profils de signature s'effectue soit depuis le Portail Web, soit via l'API. L'administrateur d'un Tenant accède via l'API aux fonctionnalités suivantes : création et modification des profils de signature, récupération d'un profil de signature existant ou de l'ensemble des profils de signature d'un Tenant, export des profils de signature du Tenant.

5.10.1 — Reconnaissance automatique du format des documents

Lorsqu'un document à signer est téléversé dans un Parapheur, le profil par défaut associé à son type de document est automatiquement appliqué. Le créateur du Parapheur peut ensuite, s'il le souhaite, modifier dans le Parapheur, le profil de signature d'un document.

De plus, lorsqu'un Utilisateur téléverse un document PDF, la solution reconnait le format du document et l'ouvre dans le visualiseur intégré de la solution, afin que l'Utilisateur positionne les emplacements de signature. Ceci n'est valable que dans le cadre d'un profil de signature avec signature visible.

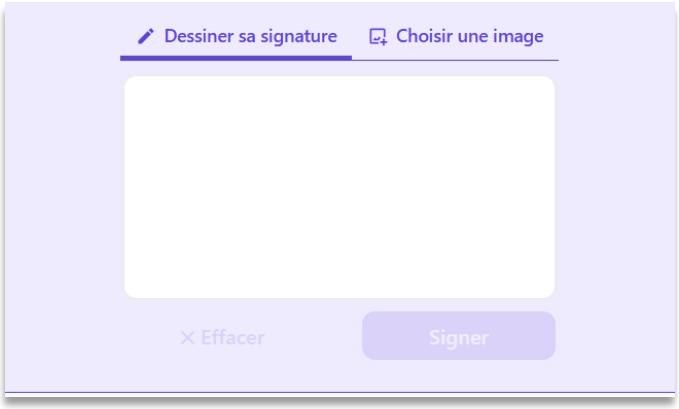
5.10.2 — Signature visible

Lors du paramétrage du profil de signature, l'Utilisateur peut décider, si le format sélectionné est PAdES, de rendre la signature électronique visible ou non visible.

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

- Import d'une image de signature électronique ;
- 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.

La solution permet d'apposer :

- Soit l'image de signature uniquement ;
- Soit le texte uniquement : exemple « Signé par …. le JJ/MM/YYYY HH:MM ». Ce texte est paramétrable et peut inclure également l'organisation, la fonction de l'utilisateur ainsi que des valeurs de métadonnées personnalisées ;

/ Soit l'image de signature et le texte.

Nota bene : Pour garantir une valeur probatoire à la Signature électronique, Goodflag Signature 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 électroniques visibles sur un document, il est alors nécessaire de prévoir autant de Signatures électroniques.

5.10.3 — Visualisation obligatoire ou non du document

Lorsqu'un Utilisateur téléverse un ou plusieurs documents, il doit sélectionner le profil de signature associé. Pour chaque profil de signature, l'Utilisateur peut forcer la visualisation du document ou la rendre facultative. Ainsi, selon le paramétrage souhaité par celui qui fait signer, le Signataire sera amené ou pas à visualiser le ou les documents avant de signer grâce au visualiseur intégré dans la solution.

Tant que l'Utilisateur n'a pas parcouru le document, l'Utilisateur 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, Goodflag Signature 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 contraintes de visualisation sont paramétrables dans les appels à Goodflag Signature par les services appelants.

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

5.10.4 — Identification visuelle du parapheur

Il est possible d'ajouter automatiquement l'identifiant (ID) du parapheur sur les documents à signer.

L'ID est apposé sur les documents dès le premier démarrage du parapheur, à condition que ceux-ci soient associés à un profil de signature ayant la fonctionnalité activée.

Cette fonctionnalité doit également être activée au préalable pour votre tenant.

Une fois la fonctionnalité activée pour votre tenant, elle peut être configurée au niveau de chaque profil de signature.

Dans le détail d'un profil de signature, vous pouvez :

/ Activer l'ajout d'un visuel

/ Choisir son positionnement sur le document :

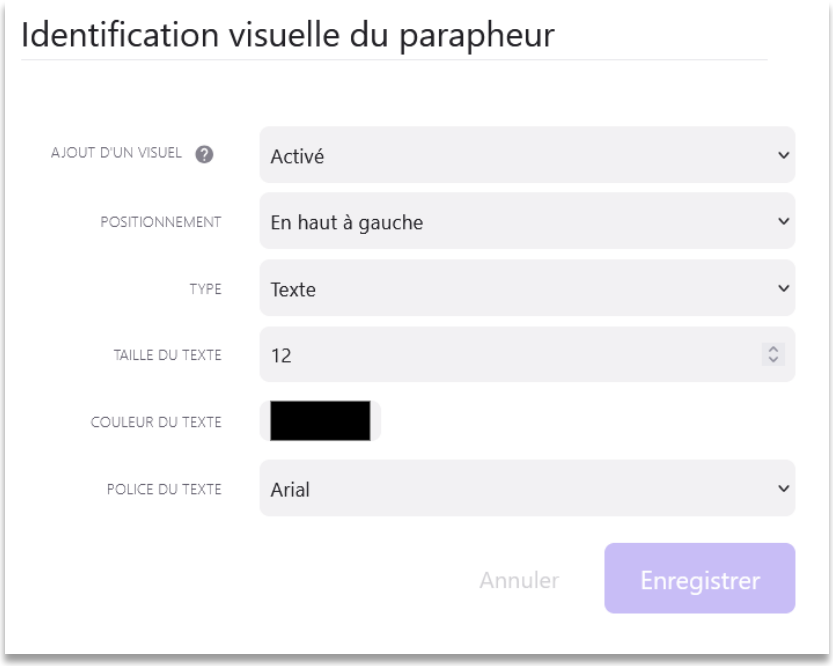
  - En haut à gauche ;
  - En haut à droite ;
  - En bas à gauche ;
  - En bas à droite.

/ Définir le type de visuel (par défaut : texte)

/ Personnaliser le style du texte :

  - Taille ;

- Couleur ;
- Police.



Section « Identification visuelle »

⚠ Attention

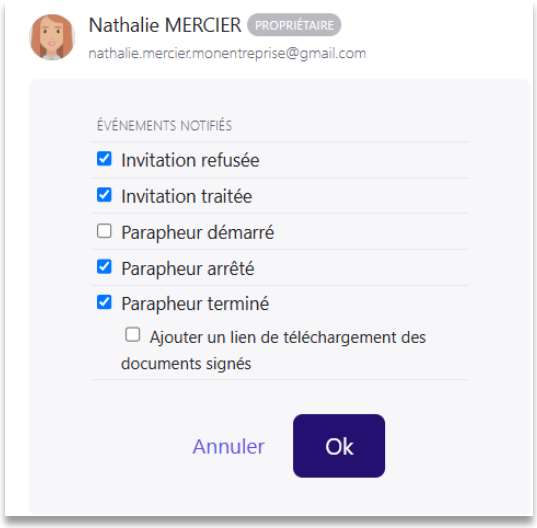
- L'identification visuelle est ajoutée uniquement lors du premier démarrage du parapheur. Tout document ajouté après ce démarrage ne recevra pas d'identification visuelle, même en cas d'arrêt puis de redémarrage du parapheur. Il est précisé dans l'info-bulle que l'ajout de l'identification visuelle se fait au premier démarrage du parapheur.
- Par ailleurs, lors de la duplication d'un parapheur avec ses documents, si ces derniers comportent déjà une identification visuelle, une nouvelle identification sera appliquée au même emplacement, sauf modification de la position du visuel dans le profil de signature associé. En l'absence de modification du profil de signature, cette situation entraînera une superposition des identifications visuelles, rendant l'identification illisible.
- Si l'identification visuelle est appliquée sur un document comportant des signatures existantes, les signatures seront invalidées.

5.11 — Notifications d'un parapheur

5.11.1 — Notifications du propriétaire

En tant que propriétaire d'un Parapheur, je peux définir sur quels événements je souhaite être notifié par courriel et au niveau du Portail :

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

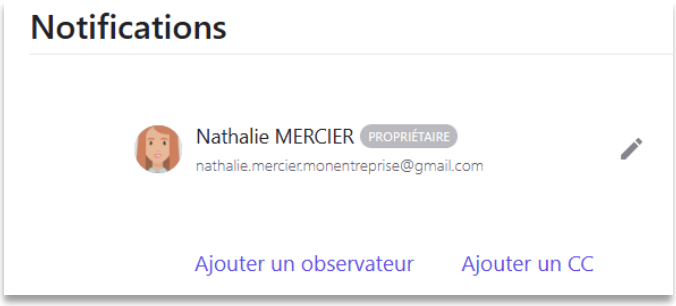


Paramétrage des événements des notifications

5.11.2 — Observateur et copy carbone

Le Gestionnaire peut également ajouter des « observateurs » (Utilisateurs) ou des « copies carbone » (Contacts) et définir sur quels évènements ils doivent être notifiés.

Cette fonctionnalité permet d'informer les Utilisateurs des actions les plus récentes réalisées au niveau des Parapheurs.



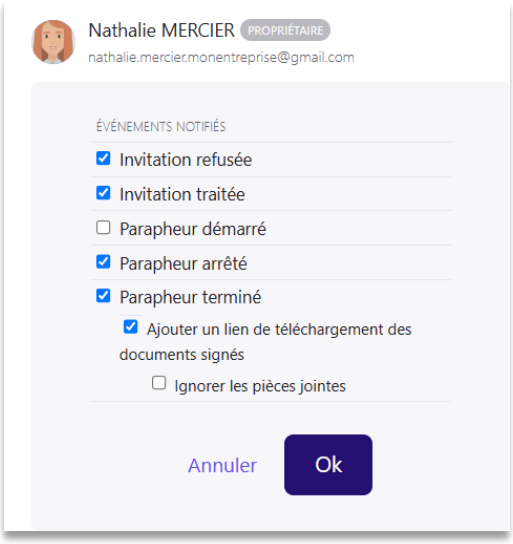
Ajout d'un observateur ou d'un CC

Les observateurs sont des Utilisateurs internes et accèdent au Parapheur pour lequel ils ont été notifiés directement depuis le Portail. Les observateurs ont uniquement des droits de lecture sur le Parapheur.

Lorsqu'un Gestionnaire 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 un observateur ou un cc d'un Parapheur terminé, il peut également ajouter à cette notification un lien de téléchargement des documents signés et des pièces jointes.

Une option lui permet d'ignorer les pièces jointes

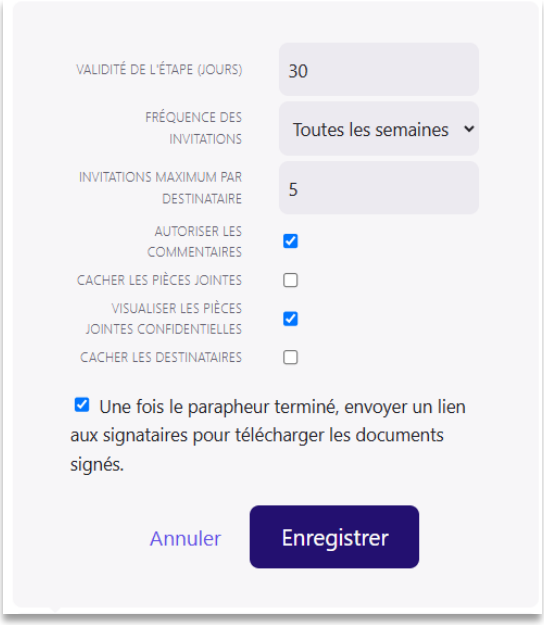


Option « Ignorer les pièces jointes »

5.11.3 — Relances manuelles et automatiques

La solution permet l'envoi de notifications par courriel pour relancer le Validateur ou 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

Il est également possible de relancer manuellement une étape

Relance manuelle

Nota bene : Les invitations groupées n'incluent pas les relances manuelles ou automatiques.

5.12 — Opérations d'un parapheur

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

5.12.1 — Démarrer un Parapheur

Lorsqu'un Parapheur a été paramétré (métadonnées, étapes, documents et notifications), alors le Gestionnaire 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.

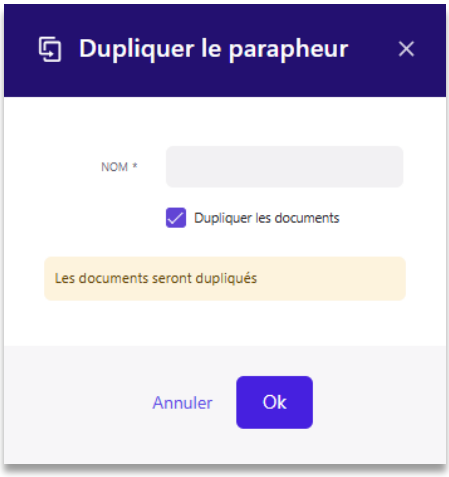
Bouton « Démarrer »

5.12.2 — Dupliquer un Parapheur

Lorsqu'un Gestionnaire crée un Parapheur, il a la possibilité de dupliquer un Parapheur, excepté si son statut est « clôturé ». 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 « Dupliquer »

Lors de la duplication, l'utilisateur a la possibilité de dupliquer le parapheur sans les documents.



Duplication de parapheur

5.12.3 — Supprimer un Parapheur

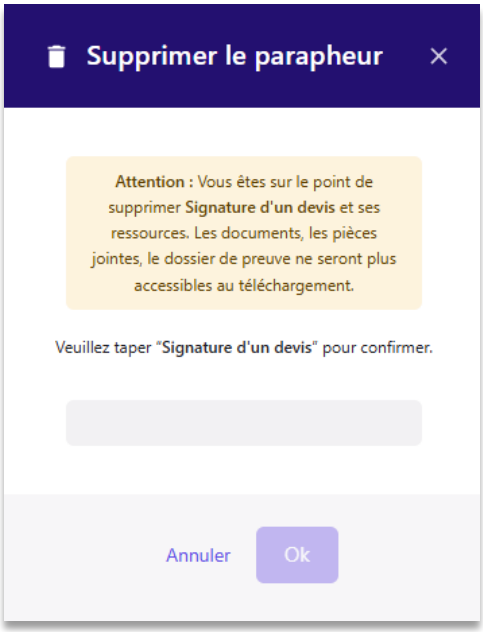
Lorsqu'un Parapheur n'a pas encore été lancé, tout Utilisateur peut supprimer un Parapheur à partir d'un bouton dédié.

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

Bouton « Supprimer »

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

Dès lors qu'un Parapheur est démarré, la fonction de suppression n'est plus disponible, excepté pour les Utilisateurs disposant du rôle d'« effaceur de Parapheurs ».

Principe de fonctionnement :

- Un Utilisateur disposant de ce droit pourra supprimer un Parapheur quel que soit son statut ;
- Un Utilisateur ne disposant pas de ce droit ne pourra pas supprimer les Parapheurs dont les statuts sont : « Démarré », « Arrêté » et « Terminé ».

5.12.4 — Arrêter le Parapheur

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

Bouton pour « Arrêter »

5.12.5 — Valider

Si le Gestionnaire ou l'Utilisateur du Portail fait partie des Validateurs, il accède directement depuis les opérations du Parapheur à un bouton d'action rapide « valider ».

Bouton « Valider »

Ce bouton lui permet d'accéder directement à la page de validation des documents.

Ce bouton est également accessible depuis la liste des Parapheurs.

5.12.6 — Signer

Si le Gestionnaire ou l'Utilisateur du Portail fait partie des Signataires d'une étape en cours, il accède directement depuis les opérations du Parapheur à un bouton d'action rapide « Signer ».

Ce bouton lui permet d'accéder directement à la page de signature des documents.

Ce bouton est également accessible depuis la liste des Parapheurs

Bouton « Signer »

5.12.7 — Clôturer le Parapheur

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

Bouton « Clôturer »

5.12.8 — 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.).

Nota bene : L'identifiant (ID) du parapheur figure sur le certificat de preuve pour permettre le rapprochement avec le parapheur correspondant.

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 « clôturé.

Bouton « Télécharger le Certificat de Preuve »

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

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

Le certificat de preuve est disponible en langues française et anglaise. Le choix de la langue se paramètre au niveau du tenant.

Sélection de la langue du certificat de preuve

5.12.9 — Télécharger le Dossier de Preuve

Lorsqu'un Parapheur est terminé, tout Utilisateur disposant du rôle de « téléchargeur de Dossier de Preuve » peut télécharger le Dossier de Preuve associé.

Vous pouvez accorder ce droit aux Gestionnaires de Parapheurs ou le réserver aux administrateurs fonctionnels.

Bouton pour « Télécharger le Dossier de Preuve »

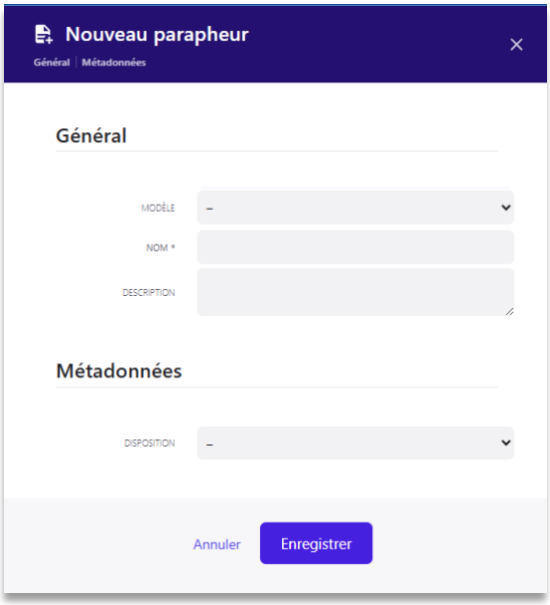
5.12.10 — Télécharger les documents

Lorsqu'un parapheur est clôturé, les documents signés ainsi que les pièces jointes sont disponibles en téléchargement.

Bouton pour « Télécharger les documents »

5.13 — Modèle de parapheur

La solution permet de créer des parapheurs, soit à la volée, soit à partir d'un modèle de parapheur.



Page de création d'un parapheur

La gestion des modèles de Parapheurs constitue une fonctionnalité importante et différenciante de la solution. Elle est accessible depuis le menu contextuel depuis le Portail ou l'API, en fonction des droits accordés à l'Utilisateur.

Un modèle de Parapheur permet de prédéfinir les étapes, les documents et les métadonnées d'un Parapheur et d'indiquer si le créateur d'un Parapheur, à partir de ce modèle, pourra modifier, ou non ces éléments.

Une fois qu'un Parapheur est créé à partir d'un modèle, il devient dépendant de ce modèle. Aucune modification sur un Parapheur qui ne respecte pas son modèle ne pourra être effectuée.

Nota bene : lors de la modification d'un modèle, les Parapheurs liés à ce modèle ne sont pas modifiés, mais leurs modifications par un Gestionnaire devront être conformes aux nouvelles règles du modèle.

Pour créer, modifier ou supprimer un modèle, l'Utilisateur doit appartenir à un Groupe ayant le rôle d'administration des modèles.

Dans un modèle, l'administrateur de modèles peut spécifier un certain nombre de paramètres ou les laisser à la libre création des créateurs de Parapheur, ces paramètres sont les suivants :

- Les dispositions de métadonnées ;
- Les étapes de Validation et de Signature électronique ;
- Les cogestionnaires ;
- Les documents (le nombre maximum de documents et de pièces jointes peut être spécifié) ;
- Les profils de signature ;
- Les notifications (le nombre maximum d'observateurs et de copies carbones peut être spécifié).

Les modèles de Parapheurs remplissent principalement deux objectifs :

Ils facilitent et accélèrent la création des Parapheurs ; en effet cette fonctionnalité permet aux Gestionnaires de ne pas ressaisir les mêmes paramètres à chaque fois ;

Ils permettent aux administrateurs des modèles de laisser le libre choix des paramètres du Parapheur ou au contraire de les figer, ce qui aura l'avantage de produire une cohérence des données.

5.14 — Cogestion des parapheurs

Un cogestionnaire peut cogérer un parapheur dès lors qu'il a été nommé comme tel sur un parapheur et qu'il appartient à un groupe utilisateur disposant du rôle de cogestionnaire.

Grâce à cette fonctionnalité, vous ne sollicitez plus vos administrateurs et n'interrompez plus la gestion de vos parapheurs, en cas d'absence d'un gestionnaire,

Cette fonctionnalité n'est disponible que pour les parapheurs créés à partir d'un modèle.

Il existe 4 modes :

- Aucun ;

Le propriétaire du parapheur ne pourra pas désigner de cogestionnaires

- Choisir parmi la liste ;

Ce mode permet à l'administrateur de modèle de désigner un ou plusieurs cogestionnaires parmi l'ensemble des cogestionnaires autorisés.

L'administrateur peut préciser si la liste qu'il a définie est :

  - Modifiable ou non par le créateur du parapheur,
  - Modifiable ou non par un cogestionnaire.

Nota bene : si l'administrateur décide que la liste n'est pas modifiable par le créateur du parapheur, alors elle ne pourra pas non plus être modifiée par un cogestionnaire

- Libre ;

Ce mode laisse le choix au créateur du Parapheur de désigner au moins un cogestionnaire parmi l'ensemble des cogestionnaires autorisés. L'administrateur peut ajouter des groupes

utilisateurs autorisés, de manière à restreindre la liste des cogestionnaires autorisés. Si l'administrateur d'un modèle ajoute des groupes utilisateur, le créateur du parapheur pourra désigner un cogestionnaire uniquement parmi les groupes qui ont été ajoutés.

Nota bene : si le propriétaire de parapheur ne désigne pas de cogestionnaire, il ne pourra pas démarrer le parapheur.

L'administrateur peut préciser si la section de cogestion est modifiable par un cogestionnaire.

- Libre ou aucun.

Ce mode laisse le choix au créateur du Parapheur de désigner ou ne pas désigner un cogestionnaire parmi l'ensemble des cogestionnaires autorisés. L'administrateur peut ajouter des groupes utilisateurs autorisés, de manière à restreindre la liste des cogestionnaires autorisés. Si l'administrateur d'un modèle ajoute des groupes utilisateur, le créateur du parapheur pourra désigner un cogestionnaire uniquement parmi les groupes qui ont été ajoutés.

Comme pour les modes « Choisir parmi la liste » et « Libre », une option permet d'ouvrir la modification des cogestionnaires aux cogestionnaires eux-mêmes. Par défaut, cette option est désactivée.

Lorsqu'un cogestionnaire est nommé ou supprimé, il reçoit une notification Push sur son tableau de bord, ainsi qu'une notification par courriel.

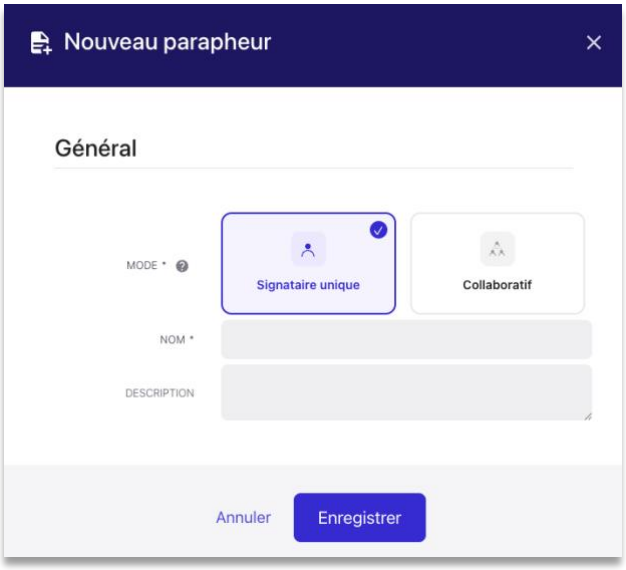
5.15 — Gestion des absences

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/Validateurs potentiels pour une étape et de limiter le nombre de Signatures/Validations électroniques attendues pour passer à l'étape suivante et/ou clôturer le Parapheur s'il s'agit de la dernière étape.

6 — Expérience Créateur d'un Parapheur mode « Signataire unique »

Après avoir sélectionné le mode Signataire unique et nommé votre Parapheur, cliquez sur « Enregistrer ».

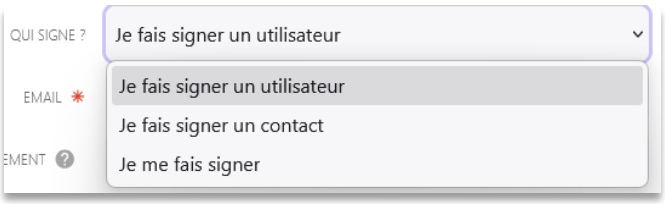


Nota bene : une info-bulle d'aide au choix est accessible en cliquant sur l'icône « point d'interrogation ».

6.1 — Désignation du signataire

En mode « Signataire unique », le signataire peut être :

- Un utilisateur ;
- Un contact ;
- Ou vous-même.

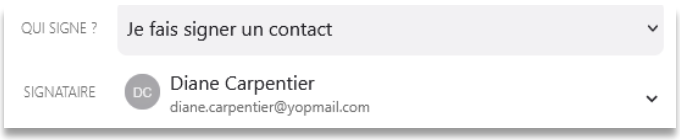


Qui signe ?

Si vous faites signer un utilisateur ou un contact, veuillez saisir l'adresse électronique dans le champ « Email » qui apparait ci-dessous.
Si l'adresse électronique est connue, le champ Email est remplacé par le champ « Signataire »

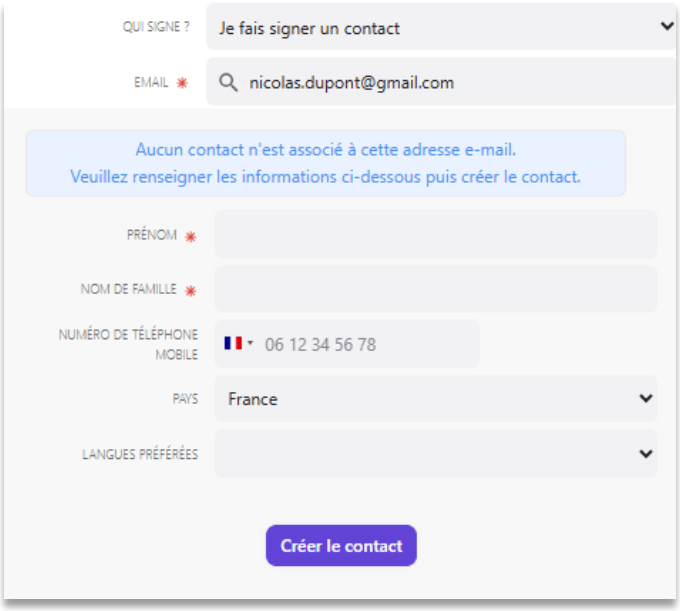
6.1.1 — Faire signer un contact

Vous avez la possibilité soit de créer un contact à la volée, soit de sélectionner un contact déjà enregistré dans votre annuaire.
La création d'un contact à la volée nécessite le rôle de « Créateur de contacts ».



Je fais signer un contact

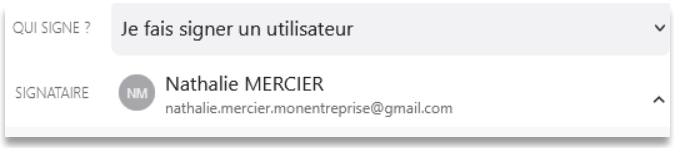
Si le contact n'existe pas, l'utilisateur est invité à renseigner les informations.



Création d'un nouveau contact

6.1.2 — Faire signer un utilisateur

Vous pouvez sélectionner un utilisateur existant ou créer un utilisateur à la volée, à condition de disposer du rôle d' « administrateur des utilisateurs ».



Je fais signer un utilisateur

Comme pour la création d'un contact, si l'adresse de courriel n'est pas connue, l'utilisateur est invité à créer l'utilisateur.

6.1.3 — Se faire signer

Lorsque vous choisissez cette option, il n'est pas nécessaire de saisir vos informations. En effet, elles sont automatiquement enregistrées.

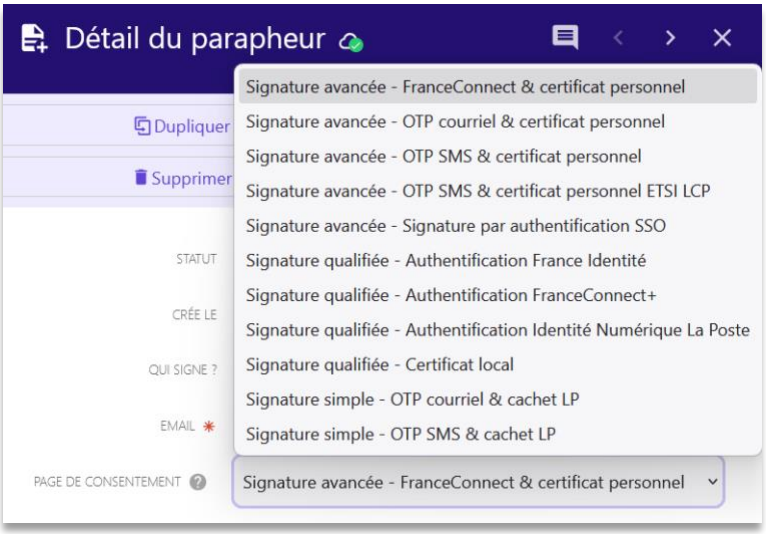
Je me fais signer

6.2 — Sélection de la page de consentement

Comme pour le Parapheur en mode « collaboratif », le gestionnaire doit sélectionner la page de consentement afin de définir :

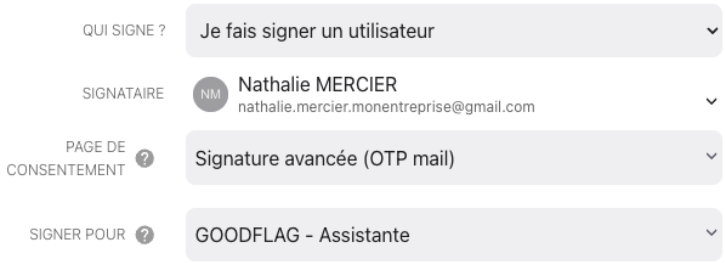
- Le niveau de signature,
- Le mode d'authentification requis pour le signataire.

Pour plus de détails, veuillez-vous reporter au chapitre 5.2. Le fonctionnement est identique, que le parapheur soit configuré en mode « signataire unique » ou « collaboratif ».



Sélection de la page de consentement

Nota bene : si la page de consentement l'autorise et si le signataire (Utilisateur uniquement) est associé à une organisation et/ou une fonction, le champ « Signer pour » est disponible.



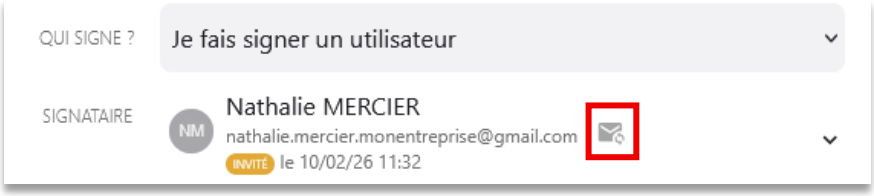
Champ « Signer pour » - Étape

L'organisation et la fonction peuvent être restituées dans le texte de signature visible apposé sur le document, à condition que le profil de signature le prévoie.

Texte de signature visible

6.3 — Relance manuelle

Bien qu'une relance automatique puisse être configurée dans les paramètres du parapheur, le Gestionnaire peut également relancer le Signataire de manière manuelle.

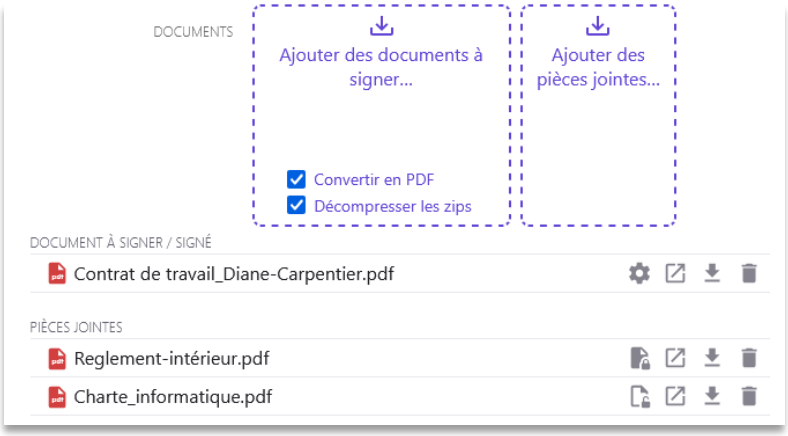


Relance manuelle

6.4 — Téléversement des documents et des pièces jointes

L'utilisateur peut téléverser les documents soit via l'explorateur de fichiers, soit par glisser-déposer.
Deux zones distinctes sont prévues :

- Une pour les documents à valider et signer,
- Une pour les pièces jointes.



Téléversement des documents et pièces jointes

Il est possible de définir la confidentialité de chaque pièce jointe.

Dans l'exemple ci-dessus, « Règlement-intérieur » est une pièce confidentielle tandis que « Charte_informatique » ne l'est pas.

Si l'option "Visualiser les pièces jointes confidentielles" est désactivée dans les paramètres du parapheur, le Signataire ne pourra pas consulter les pièces jointes marquées comme confidentielles par le Gestionnaire.

Une fois les documents téléversés, le gestionnaire peut positionner le champ de signature (si le profil de signature l'autorise) et/ou les champs dynamiques, lorsqu'ils ont été préalablement configurés.

Si le PDF est corrompu, non reconnu, verrouillé ou protégé par un mot de passe, un message d'erreur notifie le gestionnaire et lui indique l'action à mener.

Message d'erreur en cas de PDF protégé par un mot de passe

6.5 — Profil de Signature

Lors du téléversement des documents à signer, un profil de signature est associé à chaque document.

Profil de signature

Pour plus de détails, veuillez-vous reporter au chapitre 5.9.

Le fonctionnement est identique, que le parapheur soit configuré en mode signataire unique ou « collaboratif ».

6.6 — Champs dynamiques

Cette fonctionnalité est proposée en version bêta. Son comportement et ses modalités d'utilisation sont susceptibles d'évoluer dans les prochaines versions.

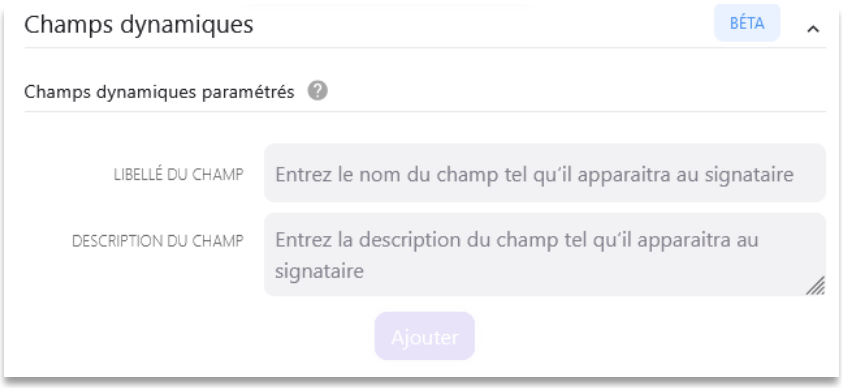
Toutefois, cela ne remet pas en cause la validité de la signature produite dans le cadre du mode « Signataire unique », lorsque des champs dynamiques sont paramétrés.

6.6.1 — Configuration des champs

Le mode « Signataire unique » permet au gestionnaire de configurer des champs dynamiques destinés à être complétés par le signataire.

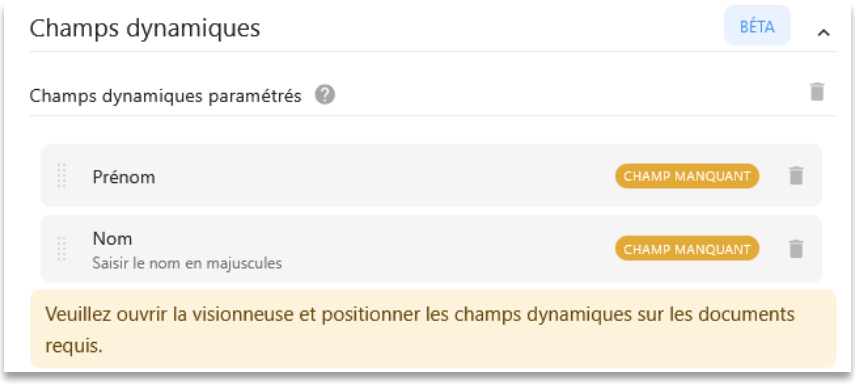
Pour chaque champ créé, le gestionnaire doit renseigner :

- Le libellé du champ ;
- La description (facultative).



Section « Champs dynamiques »

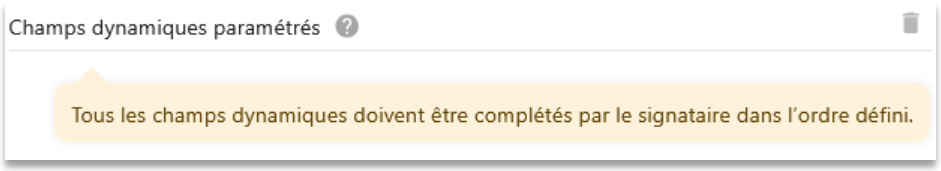
Lors de l'ajout d'un champ, la mention « champ manquant » apparaît pour indiquer qu'il doit être positionné dans un ou plusieurs documents à signer. Un message d'alerte invite également l'utilisateur à ouvrir la visionneuse afin de positionner les champs.



Champs dynamiques à positionner

Ces informations seront affichées au signataire telles qu'elles ont été saisies. De plus, les champs apparaitront dans le formulaire dans l'ordre défini par le gestionnaire.

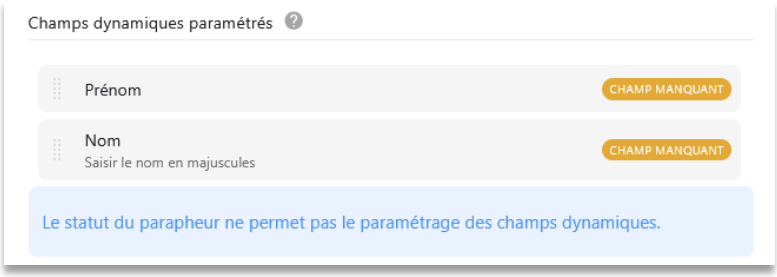
Une info-bulle le précise.



Info-bulle des « Champs dynamiques »

Les champs peuvent être réordonnés par glisser-déposer.

Attention : la configuration des champs dynamiques n'est possible que lorsque le parapheur est au statut « Brouillon » ou « Arrêté ». Dès que le parapheur est démarré, il n'est plus possible de modifier leur paramétrage ou leur positionnement dans le ou les documents à signer.

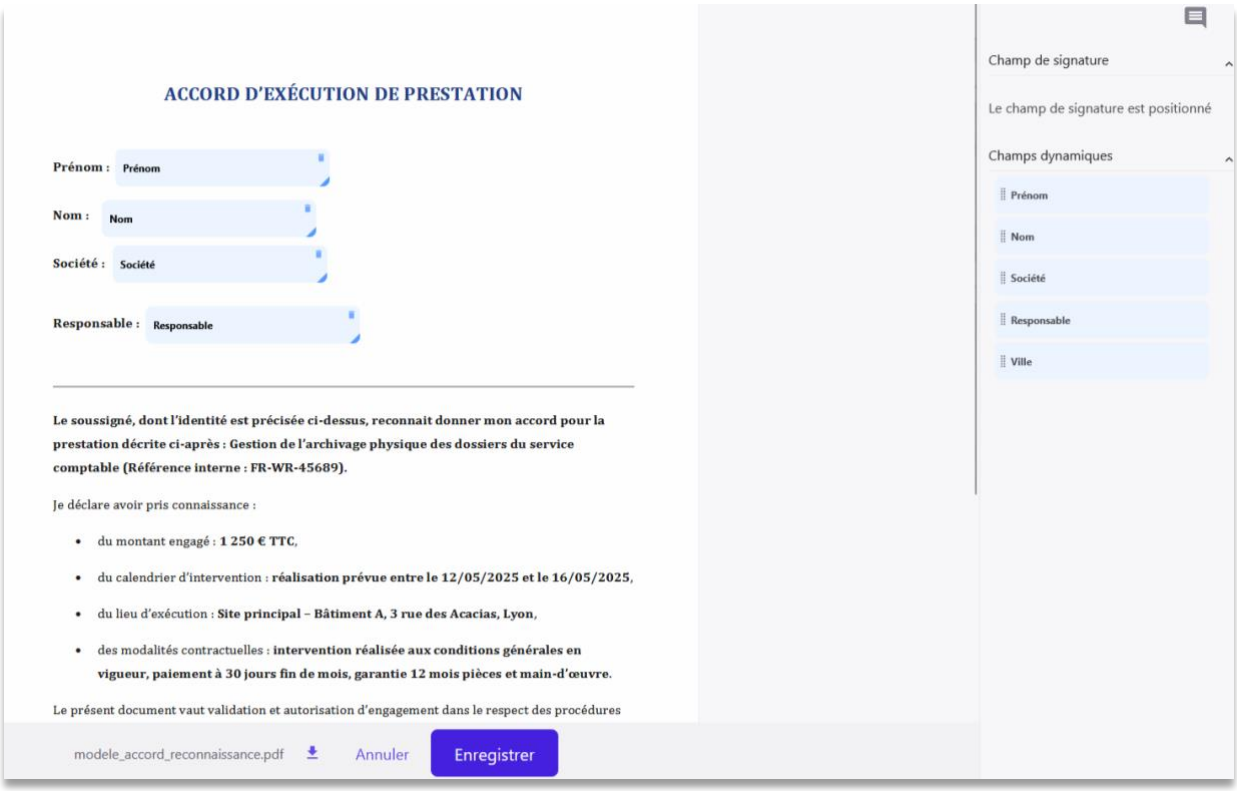


Opération impossible

6.6.2 — Positionnement des champs

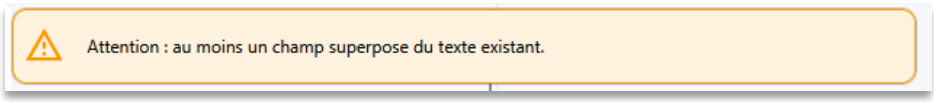
Pour positionner les champs dynamiques, le gestionnaire doit donc ouvrir la visionneuse.

Nota bene : un même champ peut être placé plusieurs fois dans un document : il n'est donc pas nécessaire de le créer plusieurs fois dans le détail du Parapheur.



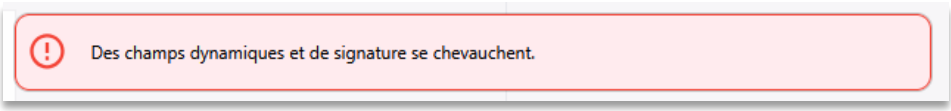
Positionnement des champs

Le gestionnaire doit veiller à ne pas superposer un champ dynamique sur du texte existant du document. Une alerte est affichée au signataire en cas de chevauchement, mais la solution ne bloque pas techniquement cette superposition.



Message d'alerte

En revanche, la superposition de champs de signature et de champs dynamiques bloque l'enregistrement. Un messager d'alerte avertit l'utilisateur.



Message d'erreur

Attention : si le gestionnaire ne positionne pas les champs sur le document, les données saisies dans le formulaire ne pourront pas être injectées dans le document à signer.

6.6.3 — Limitations et recommandations de la fonctionnalité

- Le nombre de champs dynamiques n'est pas limité. Il est toutefois recommandé d'en faire un usage mesuré, ceux-ci devant tous être renseignés par le signataire.
- Les encarts sont redimensionnables en largeur et non en hauteur, ce qui empêche le multilignes.
- La taille de l'encart impose une limite d'affichage. Pour faciliter la lecture, la taille de la police s'adapte automatiquement à la longueur du texte saisi.
  Cependant, si le texte reste trop long malgré cette réduction, une partie de son contenu peut ne plus être visible, tout en étant toujours présente et copiable.

Nous invitons donc les signataires à rester vigilants lors de la saisie. Cette limitation sera améliorée dans une prochaine version.

- Ainsi, lorsque le champ est destiné à contenir un texte long, il est recommandé aux gestionnaires d'étirer la taille de l'encart au maximum, dans la limite de l'espace disponible dans le document, afin d'assurer une meilleure lisibilité du contenu saisi par le Signataire.
- L'utilisation d'un document déjà cosigné n'est pas recommandée : l'ajout de champs dynamiques entraîne l'invalidation des signatures précédemment apposées.
- Ainsi, un document déjà signé et comportant des champs dynamiques peut être cosigné, mais il n'est pas possible d'y ajouter de nouveaux champs dynamiques avant cette cosignature.

6.7 — Paramètres

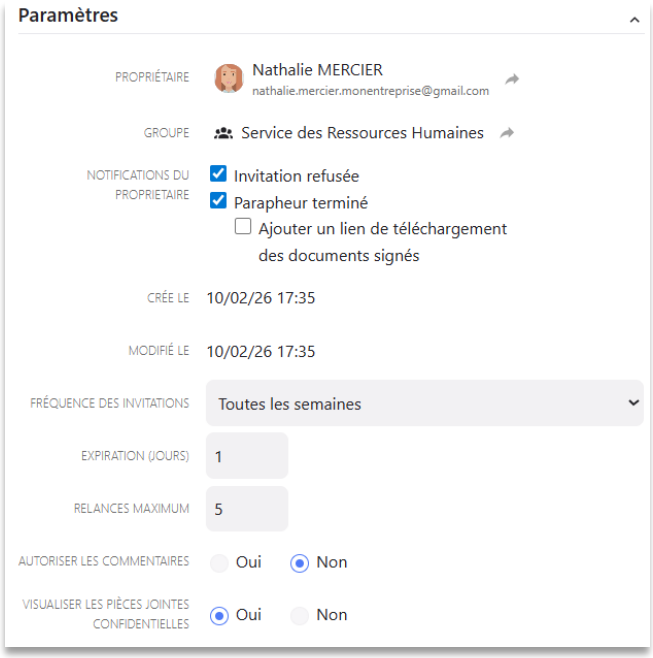
Cette section regroupe des informations renseignées automatiquement :

- Propriétaire
- Groupe
- Notifications du propriétaire :

Le propriétaire d'un parapheur configuré en mode « Signataire unique » peut sélectionner les événements pour lesquels il souhaite recevoir des notifications par courriel et sur le portail :

  - « Invitation refusée » ;
  - « Parapheur terminé », avec les options suivantes :
    - Ajout d'un lien de téléchargement des documents signés ;
    - Exclusion des pièces jointes.

- Créé le
- Modifié le
- Premier démarrage le (non affiché si vide)
- Terminé le (non affiché si vide)
- Arrêté le (non affiché si vide)
- Clôturé le (non affiché si vide)



Section « Paramètres »

Cette section comprend également des paramètres configurables par le propriétaire :

- Fréquence des invitations :
  Le Gestionnaire peut définir la périodicité des relances adressées au Signataire : tous les jours, toutes les semaines, toutes les deux semaines ou tous les mois.
- Expiration (jours) :
  Le Gestionnaire peut définir la durée de validité de l'invitation.
- Relances maximum :
  Le Gestionnaire peut déterminer le nombre maximal de relances envoyées au Signataire.
- Autorisation des commentaires :
  Cette fonctionnalité permet au Gestionnaire ou au Signataire d'ouvrir un fil de discussion à destination du Gestionnaire ou des autres destinataires d'un parapheur. Elle peut être désactivée pour le Signataire.
- Visualisation des pièces jointes confidentielles :
  La confidentialité peut être définie pour chaque pièce jointe. Le propriétaire du parapheur peut ainsi sélectionner celles qui seront visibles par le Signataire. Lorsque l'option est désactivée, les pièces marquées comme confidentielles ne peuvent pas être consultées par celui-ci.

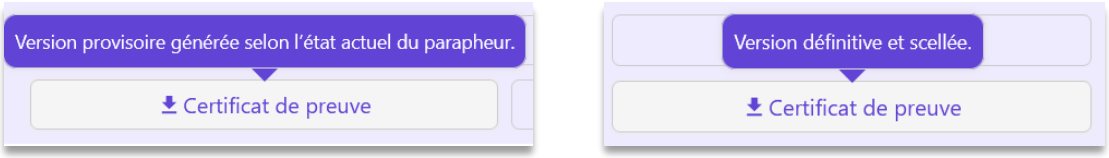
6.8 — Opérations

En mode « Signataire unique », les opérations sont affichées en haut de la page de détail du parapheur.
Ce composant reste fixe afin de garantir un accès permanent aux actions disponibles.

Composant « Opérations »

Les opérations restent communes aux opérations du Parapheur mode « collaboratif » :

Une info-bulle précise la version du certificat de preuve. En effet le certificat de preuve n'est dans sa version définitive, que lorsque le parapheur est clôturé.



Veuillez-vous reporter au chapitre 5.10 pour plus de détails sur celles-ci.

6.9 — Comparatifs des deux modes de Parapheur

	Parapheur Collaboratif	Parapheur Signataire unique
Consolidation	✓	☒
Modèles	✓	☒
Cogestionnaires	✓	☒
Validation	✓	☒
Etapes en série	✓	☒
Destinataires en parallèle	✓	☒
Je fais signer un utilisateur	✓	✓
Je fais signer un contact	✓	✓
Je me fais signer	Via la saisie de l'adresse électronique dans le champ « Contact »	Via la sélection de l'option « Je me fais signer » avec saisie automatique de vos informations
Métadonnées	✓	☒
Commentaires	✓	✓
Pièces jointes confidentielles	✓	✓
Champs dynamiques	☒	✓
Ajout de pièces par le signataire	✓	☒
Notifications propriétaire	✓	✓
Notifications observateurs	✓	☒
Notifications copy carbone	✓	☒
Opérations	Disponible dans le bas du détail du parapheur	Composant fixe en haut
Mode d'enregistrement	Champ par champ	Automatique

7 — Expérience « Validateur » et « Signataire »

Notre parcours de consentement et de signature a été conçu afin d'offrir une expérience optimale à vos Signataires. Veuillez noter que ce parcours est personnalisable (logo et couleurs) via le paramétrage de la page de consentement.

7.1 — Mobilité

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

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

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

7.2 — Invitations reçues par courriel

Dans le cas d'une requête de Signature électronique 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 envoyée par courriel – Requête de signature

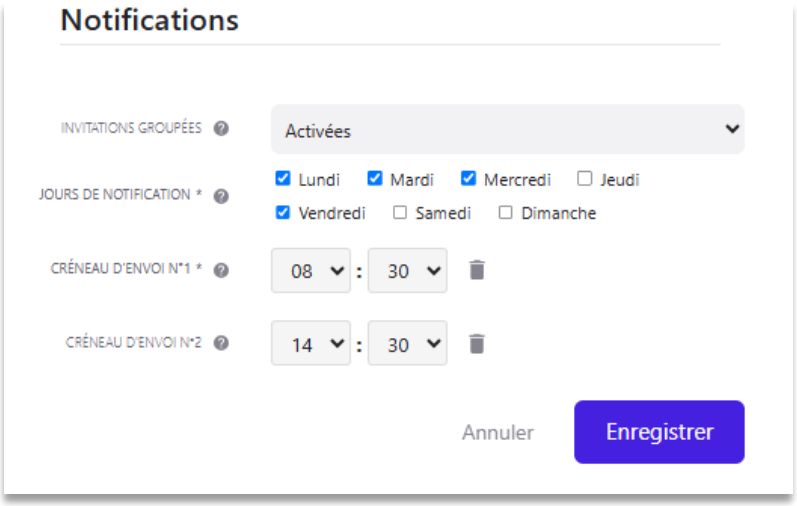
Le contenu des notifications envoyées par courriel peut être personnalisé au niveau des variables suivantes : logo, couleurs ; adresse émettrice, texte et informations sur le Parapheur, lien, etc.

Lorsque le Validateur ou le Signataire clique sur le lien, il accède soit à l'écran de consolidation, soit directement au visualiseur des documents.

7.3 — Invitations groupées

L'administrateur peut activer les invitations groupées et les paramétrer par groupe utilisateur. Les invitations groupées concernent uniquement les nouvelles demandes de validation et de signature.

Lorsqu'elles sont activées, l'administrateur peut définir les jours d'envoi des invitations ainsi que les créneaux d'envoi (1 créneau ou 2 créneaux).

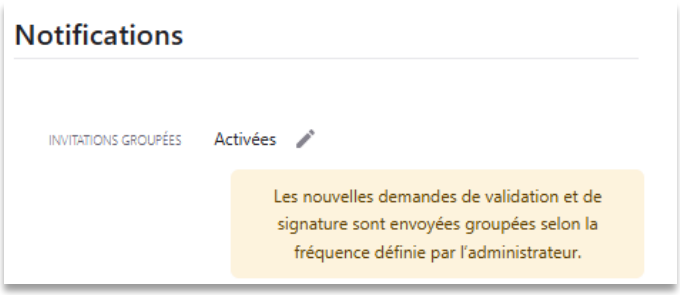


Paramétrage des invitations groupées au niveau du Groupe Utilisateur

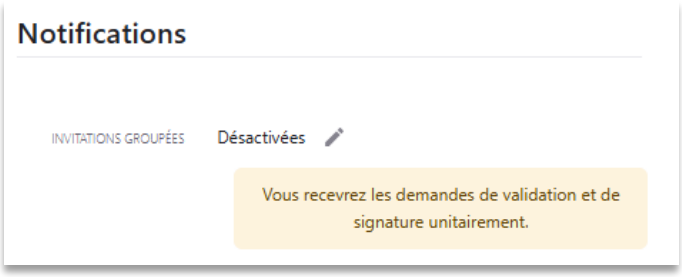
Nota bene : le propriétaire d'un parapheur reste libre d'envoyer immédiatement l'invitation en cliquant sur le bouton « Envoyer l'invitation »

Bouton de relance manuelle

Si les invitations groupées sont activées, l'utilisateur peut s'il le souhaite désactiver les notifications groupées depuis son profil utilisateur.



Invitations groupées activées dans le détail du compte utilisateur



Invitations groupée désactivées dans le détail du compte utilisateur

7.4 — Consolidation

La consolidation n'est pas activée pour le mode « Signataire unique ».

7.4.1 — Page de consolidation

Lorsque la consolidation est activée[2], l'Utilisateur accède à une page de consolidation.

Page de consolidation

Cette page lui permet d'accéder au parapheur ou aux parapheurs consolidés.

Pour chaque Parapheur, l'utilisateur accéder à l'ensemble des étapes du Parapheur. Il visualise ainsi les étapes qui précèdent et qui vont suivre son étape

Il est possible pour le Gestionnaire 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.

Si le Gestionnaire de Parapheur a renseigné le champ « Description » d'un Parapheur, celle-ci apparait dans la page d'invitation du Parapheur concerné.

[2] La consolidation se paramètre à différents niveaux : tenant, modèle de parapheur, parapheur.

7.4.2 — Validation et Signature en masse

La solution propose la Validation ou la Signature électronique en masse via la fonction de consolidation des Parapheurs.

Lorsqu'un Utilisateur a plusieurs Parapheurs en attente de Validation ou de Signature électronique, il peut sélectionner les Parapheurs qu'il souhaite valider ou signer et les valider ou signer dans une seule Transaction de Validation ou de Signature électronique.

Sélection des Parapheurs à signer

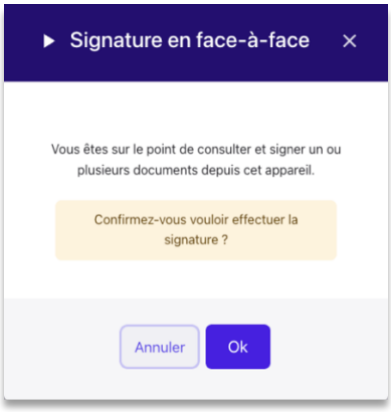
La Signature électronique en masse n'est possible que si les Parapheurs utilisent la même Page de Consentement.

Lorsqu'un Utilisateur valide et/ou signe un Parapheur, l'ensemble des documents (sauf les annexes) sont validés et/ou signés en une seule et même opération.

7.5 — Signature en face-à-face

Le mode Signature en face-à-face n'est pas disponible pour le mode « Signataire unique ».

Si le mode face-à-face est activé pour l'étape, le Signataire ne doit pas se connecter à sa boite mail et cliquer sur le lien, il peut signer directement depuis l'appareil de l'Utilisateur qui anime la session de signature en présentiel



« Écran Signataire »

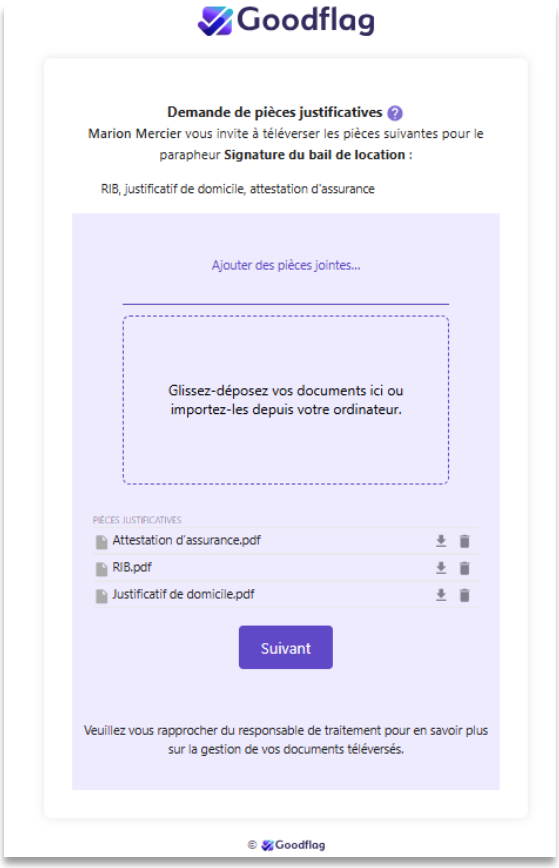
Après avoir cliqué sur « Ok », le signataire est redirigé vers la visionneuse de documents, puis accède au parcours de signature.

7.6 — Ajout de pièces justificatives par le Signataire

L'ajout de pièces justificatives par le Signataire n'est pas disponible pour le mode « Signataire unique ».

Le Gestionnaire de Parapheur peut demander au Signataire de déposer des pièces justificatives avant la Signature des documents.

Cette fonctionnalité n'est pas disponible pour les étapes de validation ni pour celles comportant un ou plusieurs destinataires en parallèle. Lorsqu'elle est activée sur une étape, l'option de consolidation n'est pas proposée.

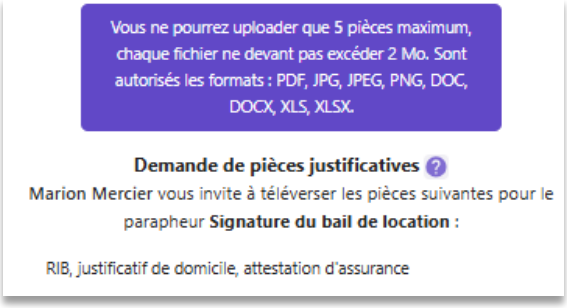


Demande de pièces justificatives

Le Signataire est invité à téléverser 5 documents maximum. La taille de chaque fichier ne doit pas excéder 2 Mo.

Les formats autorisés sont : PDF, JPG, JPEG, PNG, DOC, DOCX, XLS.

Un rappel des règles est fourni au Signataire via l'info-bulle de « Demande des pièces justificatives ».



Info-bulle « Demande de pièces justificatives »

Une fois que le Signataire a ajouté 5 documents, l'encart de téléversement se grise et il n'est plus possible d'ajouter d'autres pièces.

Si le Signataire ne respecte pas ces règles, un message d'erreur s'affiche.

Message d'erreur

Dès que ses pièces sont ajoutées, le Signataire clique sur « Suivant » et accède au visualiseur de documents.

Nota bene : il n'existe pas de dispositif de vérification des pièces.

Le Client peut joindre une notice d'information ; le cas échéant, elle est mise à disposition du Signataire. À défaut de notice, le Signataire est invité à se rapprocher du responsable de traitement, à savoir le Client.

Un signataire, de type contact ou utilisateur, peut supprimer une pièce qu'il vient d'ajouter tant que sa signature n'est pas effective.

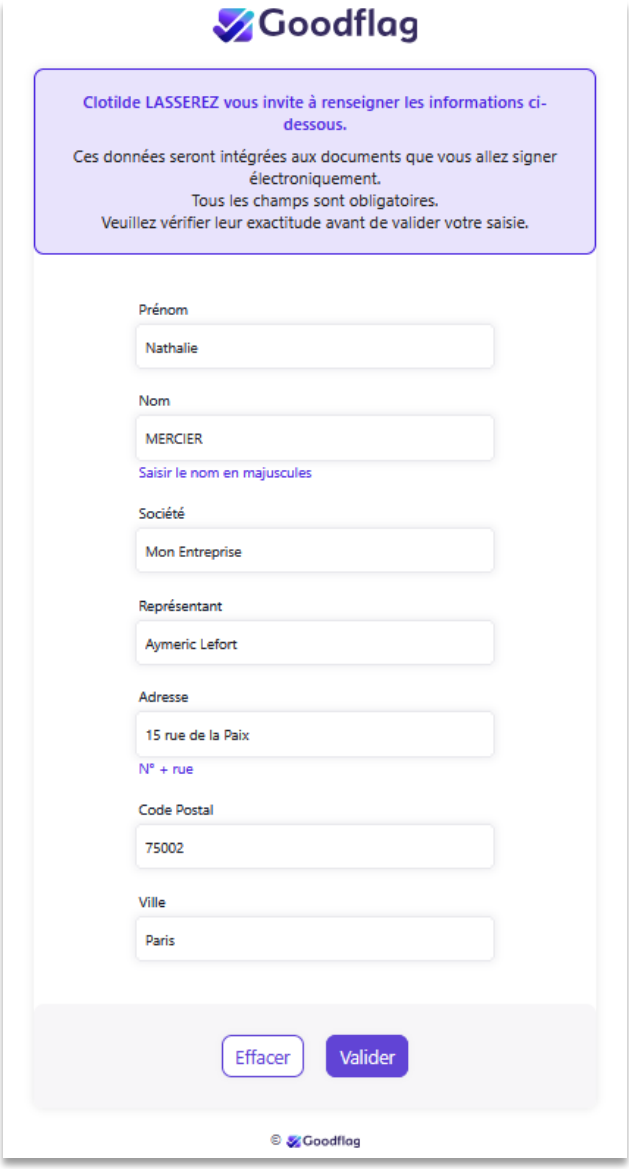
Une fois la signature effective, le Signataire ne peut plus supprimer une pièce directement. Les pièces justificatives sont alors supprimées dans les cas suivants : sur demande du Signataire auprès du gestionnaire (par exemple via le fil de discussion), à l'expiration de l'étape, lors de la suppression de l'étape, ou lorsque le Parapheur passe au statut « Clôturé ».

Les pièces ajoutées par le Signataire demeurent néanmoins tracées dans le détail du certificat de preuve.

7.7 — Saisie des valeurs des champs dynamiques

Cet écran est disponible uniquement dans le cadre du parapheur en mode signataire unique.

Dans ce mode, le gestionnaire peut configurer des champs dynamiques. Ces champs doivent être renseignés par le signataire via un formulaire qui lui est présenté avant l'affichage des documents à signer.



Formulaire de saisie

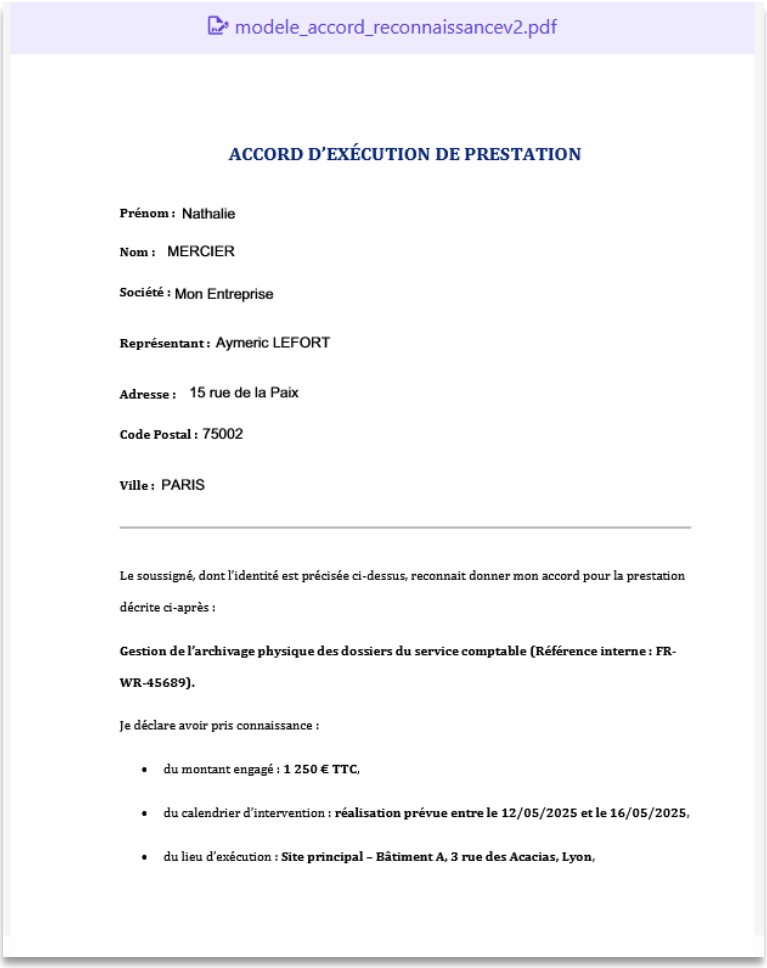
Les informations saisies par le signataire sont ensuite automatiquement intégrées dans le ou les documents à signer.

Les valeurs saisies par le signataire sont enregistrées dans le « session storage » du navigateur et restent conservées jusqu'à la signature effective du document, moment auquel elles sont supprimées.

Attention si l'onglet de navigation est fermé, les données seront également perdues.

Si le signataire accède à la visionneuse puis revient au formulaire, il retrouvera les données qu'il avait précédemment saisies.

En revanche, s'il renseigne un formulaire provenant d'un autre Parapheur avant d'avoir signé le premier document, les données liées à ce second Parapheur se substitueront à celles déjà enregistrées. Les informations du premier formulaire seront alors définitivement perdues.


modele_accord_reconnaissancev2.pdf

ACCORD D'EXÉCUTION DE PRESTATION

Prénom : Nathalie

Nom : MERCIER

Société : Mon Entreprise

Représentant : Aymeric LEFORT

Adresse : 15 rue de la Paix

Code Postal : 75002

Ville : PARIS

Le soussigné, dont l'identité est précisée ci-dessus, reconnait donner mon accord pour la prestation décrite ci-après :

Gestion de l'archivage physique des dossiers du service comptable (Référence interne : FR-WR-45689).

Je déclare avoir pris connaissance :

- du montant engagé : **1 250 € TTC,**
- du calendrier d'intervention : **réalisation prévue entre le 12/05/2025 et le 16/05/2025,**
- du lieu d'exécution : **Site principal – Bâtiment A, 3 rue des Acacias, Lyon,**

Document avec les données injectées

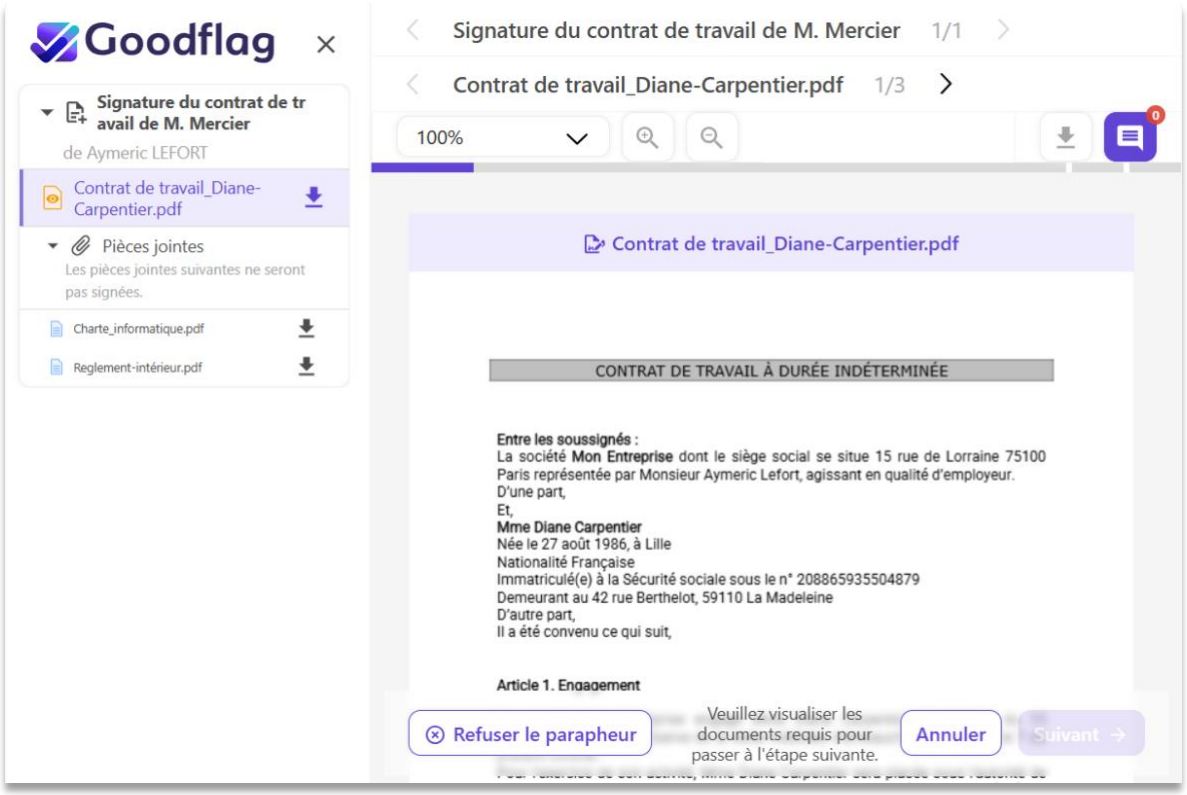
7.8 — Parcours de consentement

7.8.1 — Visualiseur des documents

Le visualiseur des documents intègre :

- Un panneau central qui permet au Validateur ou au Signataire de visualiser le ou les documents à valider ou signer ;
- Un volet à gauche qui présente l'arborescence des documents (pièces à signer et pièces jointes) d'un Parapheur ou de plusieurs Parapheurs en cas de consolidation des Parapheurs ;
- Un volet à droite qui inclut le fil de discussions qui se contextualise en fonction du Parapheur sélectionné.

Nota bene : ces deux volets peuvent être masqués au profit de l'affichage centralisé du document.

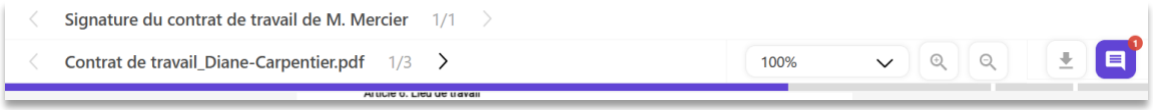


Vue globale de la nouvelle interface

Des outils de zoom et de téléchargement sont disponibles.

Outils de zoom et de téléchargement

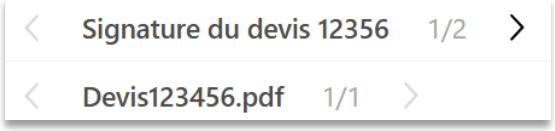
Une barre de chargement informe l'utilisateur de sa progression dans la visualisation ou la lecture du document.



Barre de progression de lecture du document

Plusieurs méthodes de navigation sont proposées :

- les Validateurs ou Signataires peuvent désormais faire défiler verticalement tous les documents du Parapheur et les pièces jointes de manière intuitive depuis cette nouvelle interface ;
- les Validateurs ou Signataires peuvent utiliser l'arborescence des documents pour naviguer entre les documents et les pièces jointes d'un Parapheur et en cas de consolidation entre les documents et les pièces jointes de plusieurs Parapheurs ;
- les Validateurs ou Signataires peuvent utiliser les flèches présentes au niveau des en-têtes afin de naviguer entre les documents d'un Parapheur ou entre les Parapheurs en cas de consolidation des Parapheurs.



En-têtes des Parapheurs et des documents

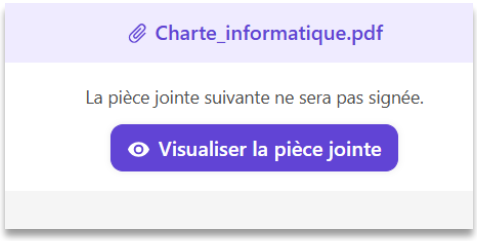
Des icônes distinctes permettent à l'utilisateur de distinguer les documents en visualisation obligatoire des documents en visualisation facultative. Lorsque le document est visualisé, l'icône se modifie.

Document en visualisation obligatoire

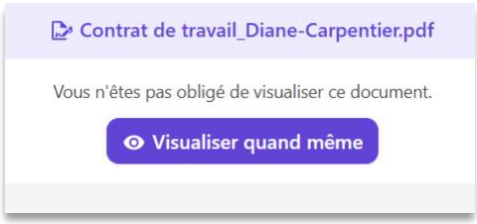
Document en visualisation non obligatoire

Document visualisé

Les pièces jointes ainsi que les documents dont la visualisation est facultative sont clairement identifiés. Un bouton permet à l'utilisateur d'activer la visualisation des documents.



Affichage des pièces jointes



Affichage des documents en visualisation non obligatoire

En cas de consolidation des Parapheurs, l'utilisateur est averti qu'il change de parapheur.

Indicateur de changement de parapheur

7.8.2 — Fil de discussion

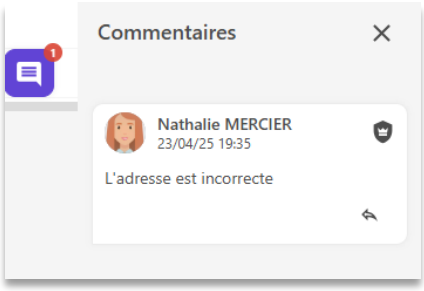
Cette fonctionnalité permet à un destinataire de Parapheur de créer un fil de discussion à l'attention du Gestionnaire ou des autres destinataires d'un Parapheur.

Il est possible pour un Gestionnaire de Parapheur de désactiver cette fonctionnalité dans le paramétrage de l'étape.

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 Validateur ou Signataire, un fil de discussion est privé par défaut, c'est-à-dire qu'il n'est visible que par lui et le Gestionnaire du Parapheur. Lorsqu'il est public, alors tous les destinataires peuvent voir les commentaires.

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



Exemple d'un fil de discussion

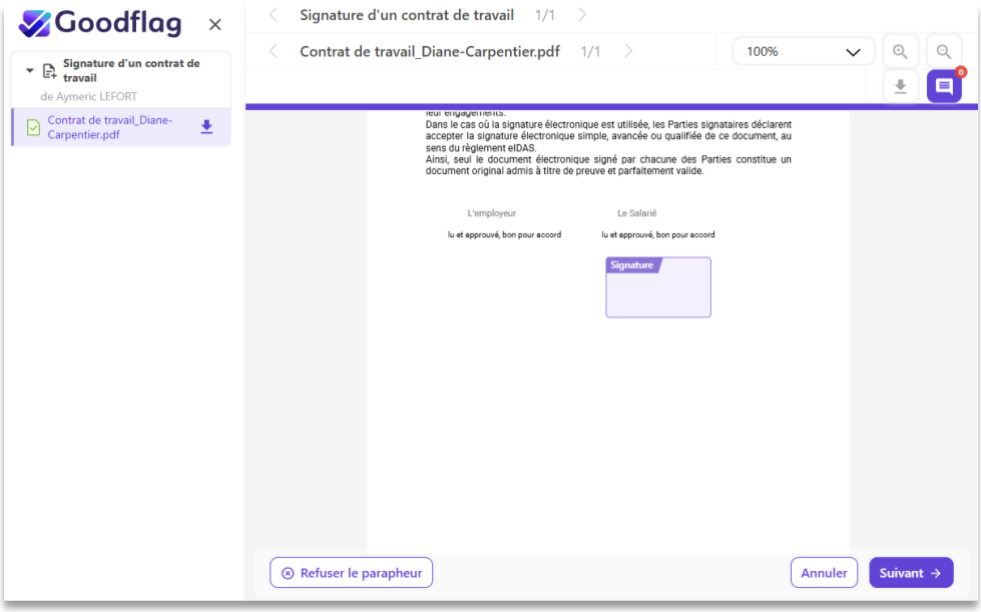
7.8.3 — Refus de Validation ou de Signature électronique

L'Utilisateur a la possibilité de refuser une demande de Validation ou de Signature électronique :

- Soit depuis l'écran de consolidation

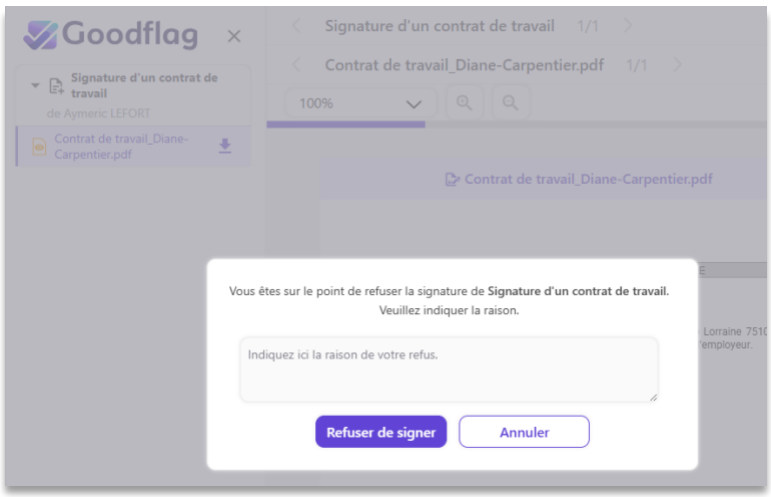
Bouton « Refuser » Ecran de consolidation

- Soit depuis la visionneuse



Bouton « Refuser » depuis la visionneuse

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

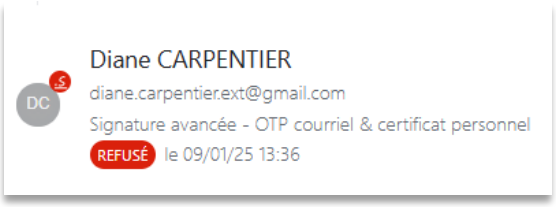


Demande de confirmation de suppression

Lorsqu'il refuse, un nouvel écran s'affiche :

Demande refusée

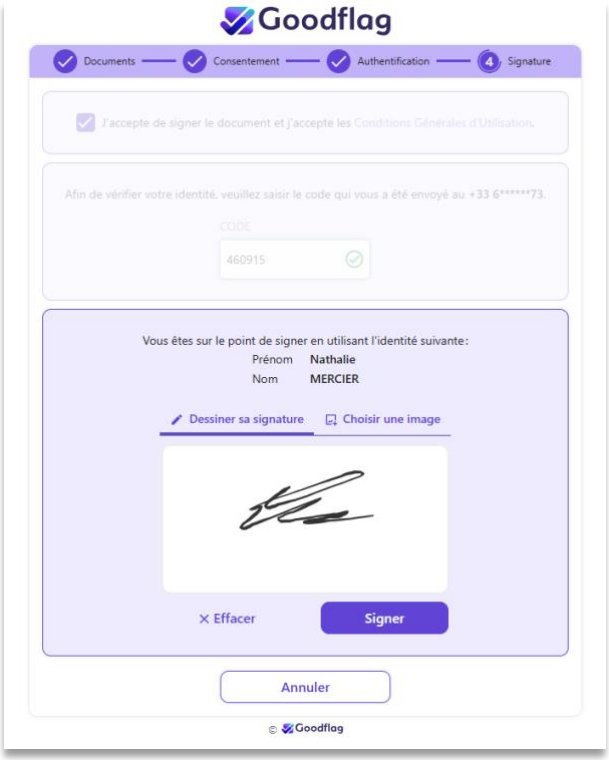
Le commentaire laissé par le Signataire est visible au niveau des étapes du Parapheur.



Exemple de refus de signature

7.8.4 — Écrans d'authentification et de signature

Le parcours de signature se déroule sur un seul écran :



Écran unique

Cet écran regroupe

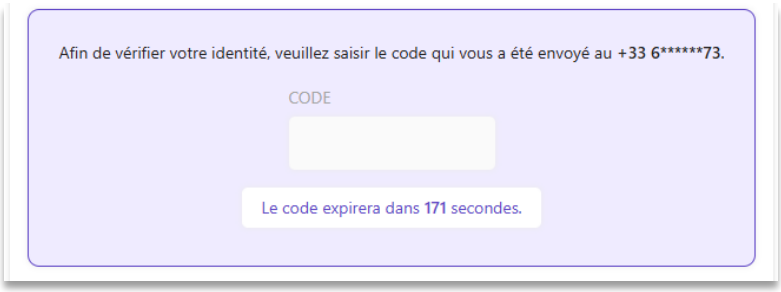
- Le recueil du consentement du Signataire avec l'acceptation des CGU ;

Acceptation des CGU

- L'ajout de la griffe ou de l'image de signature (en cas de signature visible) ;

Dessin de la griffe de signature

- Le procédé d'authentification, avec notamment la validation automatique du code OTP dans le cadre d'une authentification via OTP envoyé par courriel ou sms.

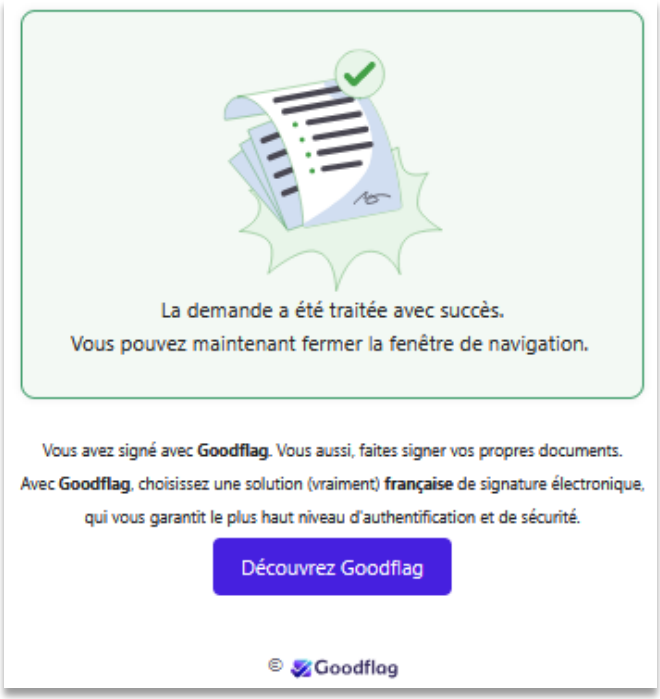


Avant la saisie du code OTP

Validation automatique du code OTP

7.8.5 — Finalisation du parcours

Lorsque la procédure est finalisée, un dernier écran s'affiche :



Demande traitée avec succès

8 — Gestion des droits et des utilisateurs

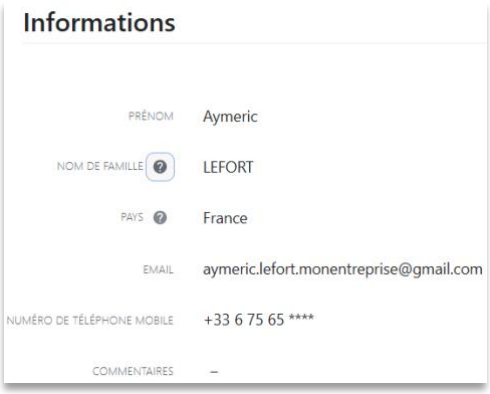
8.1 — Utilisateurs

Dans la solution Goodflag Signature, un Utilisateur est une personne physique qui appartient à un Groupe et a des droits particuliers qui sont définis dans ce Groupe.

Chaque Utilisateur est caractérisé par un prénom, un nom, un Groupe d'Utilisateurs et un identifiant unique.

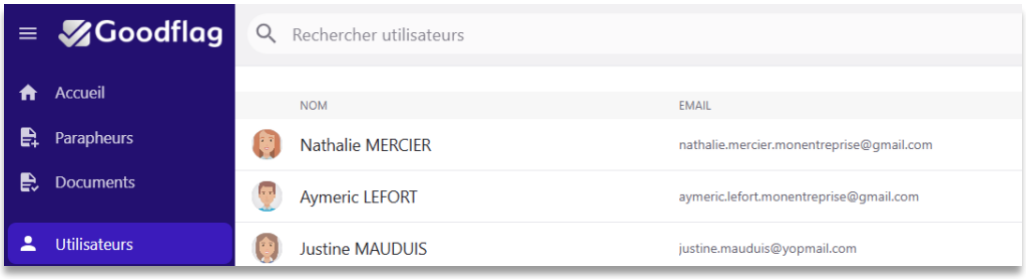
D'autres informations optionnelles sont disponibles : pays, numéro de téléphone, commentaires, etc.

Nota bene : les 4 derniers chiffres du numéro de téléphone mobile des utilisateurs sont masqués pour les utilisateurs ne disposant pas du rôle d'administration des utilisateurs.



Fiche utilisateur

Les utilisateurs peuvent être soit des Utilisateurs du Portail soit des utilisateurs externes. Ces derniers n'accèdent pas au Portail Web de la solution Goodflag Signature.



Liste des Utilisateurs

Cette fonctionnalité est disponible depuis le Portail ou via l'API. Un administrateur des Utilisateurs accède aux mêmes fonctionnalités via l'API : création/modification et suppression d'un Utilisateur, récupération d'un Utilisateur ou de l'ensemble des Utilisateurs, export des Utilisateurs.

Nota bene : La solution permet aux administrateurs disposant du rôle d'administration des Utilisateurs :

- De désactiver un Utilisateur (la réactivation de l'Utilisateur reste cependant possible) ;
- D'anonymiser un Utilisateur : suppression des données liées à l'Utilisateur (nom, prénom, téléphone, adresse courriel, etc.) et désactivation de l'Utilisateur. Les Parapheurs liés à cet Utilisateur ne sont pas supprimés.

Lorsqu'un Utilisateur est « désactivé » ou « anonymisé », il ne peut plus se connecter à la plateforme.

Nota bene : si l'utilisateur dispose du rôle d'« anonymiseur de son compte », il pourra lui-même anonymiser son compte depuis son profil.

8.2 — Organisations

La solution permet de créer des Organisations et d'y rattacher des Utilisateurs.

Une Organisation est une entité légale à laquelle peut être rattachée un Utilisateur.

Lorsque l'Utilisateur est un Signataire, cela permet lors d'une signature serveur, avec un Certificat généré « à la volée » et selon le type de Certificat utilisé, d'indiquer l'Organisation dans le champ « subject » du Certificat.

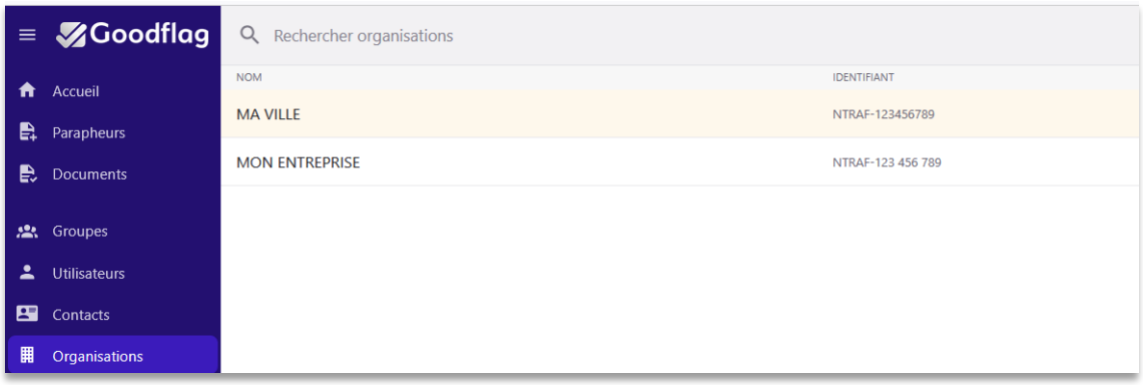
L'Organisation peut également être affichée dans la signature visible d'une signature PAdES.

Un Utilisateur peut être rattaché à plusieurs Organisations. Lorsqu'on fait signer un Utilisateur rattaché à plusieurs Organisations, l'Utilisateur qui fait signer sélectionne l'Organisation de son choix.

Pour chaque Organisation, il est possible de définir des informations telles que le numéro de Siret par exemple.

Cette fonctionnalité est disponible depuis le Portail Web et via l'API.

L'API permet de créer, de modifier et de supprimer une Organisation. Elle permet également de récupérer une Organisation ou l'ensemble des Organisations d'un Tenant.



Liste des Organisations

8.3 — Groupes Utilisateurs

Dans la solution Goodflag Signature, la gestion des droits repose sur les notions de Groupes d'utilisateurs.

Un Groupe d'utilisateurs est un ensemble de droits et d'autorisations s'appliquant aux Utilisateurs appartenant à ce Groupe. **Un Utilisateur appartient à un seul Groupe.**

Les Utilisateurs, disposant du rôle d'administration des Groupes accèdent à la fonctionnalité « Groupes » et visualisent ainsi l'ensemble des Groupes d'Utilisateurs paramétrés par Tenant.

Le tableau ci-dessous illustre les différents rôles pouvant être attribués à un Groupe :

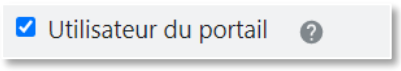
01	Rôles basiques	Utilisateur du Portail Créateur de Parapheur Créateur de Contacts Signataire Validateur Visualisateur des Utilisateurs Visualisateur des Parapheurs Téléchargeur de dossier de Preuve Effaceur de Parapheurs Finaliseur de Parapheurs Cogestionnaire de Parapheurs Anonymiseur de son compte Visualisateur des exports Exportateur en masse des documents
02	Rôles d'administration	Administrateur du Tenant Administrateur des Groupes Administrateur des Utilisateurs Administrateur des pages de consentement Administrateur des Organisations Administrateur des dispositions de métadonnées Administrateur des modèles Administrateur des Parapheurs
03	Rôles de développement	Développeur Lanceur d'invitations

Rôles d'un Groupe

Pour chacun de ses rôles, il est possible de connaitre les privilèges accordés aux Utilisateurs :

Affichage des rôles

Pour attribuer un rôle à un Groupe, il suffit de cocher la case située à gauche du nom de chaque rôle.



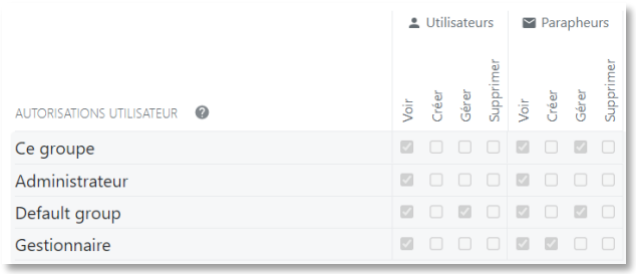
À la notion de rôle, s'ajoute la notion d'autorisation :

Les autorisations d'un Groupe permettent de spécifier si les Utilisateurs de ce Groupe peuvent agir sur les Utilisateurs et les Parapheurs de leur Groupe et/ou d'autres Groupes :

- Exemple 1 :
  - Voir/créer/modifier/supprimer tous les Utilisateurs dans ce Groupe,
  - Voir/créer/modifier/supprimer les Parapheurs dans ce Groupe ,

- Exemple 2 :
  - Voir/créer/modifier/supprimer tous les Utilisateurs dans ce Groupe ainsi que dans les Groupes A et B,
  - Voir/créer/modifier/supprimer les Parapheurs dans ce Groupe ainsi que dans les Groupes A et B.

De la même façon que les rôles, il suffit de côcher les cases des autorisations que vous souhaitez attribuer à ce Groupe comme montré ci-dessous :



Exemple d'autorisations Utilisateur

Dans un même Tenant, il est possible de créer des espaces cloisonnés grâce à la création des Groupes Utilisateur.

Un administrateur des Groupes accéder aux mêmes fonctionnalités via l'API : création d'un nouveau Groupe, récupération d'un Groupe existant ou de l'ensemble des Groupes du Tenant, modification/suppression d'un Groupe.

La solution permet de paramétrer des droits d'accès avec un niveau important de granularité.

9 — Les Signatures électroniques de Goodflag Signature

9.1 — Exposé des principes techniques de la signature électronique

Avant d'aborder les différents types de Signature électronique proposés par Goodflag Signature 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 Goodflag Signature, 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 à l'aide d'un calcul mathématique de chiffrer l'empreinte du document à signer. C'est donc le résultat du calcul mathématique 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 le lien entre l'identité du Signataire et 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 la 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 la signature à l'aide de la Clé Publique, ajoute à la confusion.

9.2 — 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.

9.2.1 — Les Signatures électroniques du règlement eIDAS

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

9.2.2 — 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'État. ».

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 ».

9.3 — Éléments 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.

9.4 — Principes généraux des signatures électroniques de Goodflag Signature

Avant de présenter les différents types de Signatures électroniques proposées par Goodflag Signature, 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 Gestionnaire, à faire signer un ou plusieurs document(s) à un ou plusieurs Signataire(s)[3]. On précise qu'il est possible pour le Gestionnaire du Parapheur, le cas échéant, d'être un Signataire dudit Parapheur.

Ainsi la solution prévoit de la part du Gestionnaire une connaissance supposée *a priori* des interlocuteurs qui vont signer le(s) document(s). Autrement dit, l'identification des Signataires est toujours effectuée par le Gestionnaire qui crée (ou modifie) le Parapheur. Ou bien, de manière alternative mais similaire, par le biais d'une application métier qui s'appuie sur l'API. 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 délivrance d'un Certificat généré « 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.

[3] On omet ici volontairement les notions de Validation électronique, de Validateur et de pièce jointes qui n'entrent pas dans le contexte du propos abordé dans cette section.

Le Gestionnaire peut, selon le paramétrage du tenant et/ou l'application mise en œuvre à l'aide de l'API, renseigner d'autres éléments d'identification du Signataire, de manière obligatoire ou facultative, selon le type de Signature électronique envisagée :

- Le pays de naissance ou le pays de résidence du Signataire, ou encore le pays de délivrance de son titre d'identité, qui, selon les cas, pourra être utilisé pour composer le Certificat ;
- L'Organisation, représentée par son nom et son identifiant (par exemple un numéro de SIREN pour une Organisation française), à laquelle est rattachée le Signataire, et qui pourra, selon les cas, être utilisée pour composer le Certificat d'une personne physique rattachée à une entité légale ;
- La fonction du Signataire (par exemple « Président »), qui pourra, selon les cas être utilisée pour composer le Certificat d'une personne physique rattachée à une Organisation précédemment renseignée.

Toutes ces informations d'identification sont par conséquent des données qui peuvent être utilisées en tout ou partie par Goodflag Signature, lors du parcours de consentement effectué par le Signataire, afin de les comparer avec celles qui peuvent être retournées lors de l'authentification de ce dernier, en vue de la réalisation de la Signature électronique des documents à signer, que celle-ci soit effectuée :

- Soit en local du poste du Signataire à l'aide d'un Certificat au format logiciel respectant le standard PKCS#12 ou sur support cryptographique respectant les standards PKCS#11 ou MSCAPI ;
- Soit sur serveur, à l'aide d'un Certificat généré « à la volée » délivré par l'Autorité de Certification « Sunnystamp Natural Persons CA », dans le cadre d'une Signature électronique avancée ou qualifiée.

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 le Gestionnaire 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 électronique des documents.

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

Il existe deux exceptions à ce principe, qui sont détaillées 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 Certificat de cachet serveur au nom de Goodflag ce qui confère au document un niveau de sécurité très important en garantissant son intégrité et son authenticité ; dans le cas d'une

Signature électronique au format PAdES, la Signature électronique comporte dans le champ motif les nom et prénom du Signataire tels que fournis par le Gestionnaire, ainsi que l'identifiant de la Transaction, cette dernière information étant particulièrement utile pour constituer et vérifier le Fichier de Preuve ;

- Dans le cas d'une Signature électronique effectuée avec un Certificat local propre au Signataire (Certificat logiciel ou sur support cryptographique), deux cas sont envisageables, selon que le Gestionnaire prévoit le contrôle strict du Certificat local propre au Signataire ou non ; dans le cas où un contrôle strict est demandé, Goodflag Signature va contrôler la cohérence des nom et prénom du Signataire fournis par le Gestionnaire et rejeter tout Certificat présenté comportant des informations différentes. Dans le cas où le contrôle strict n'est pas de demandé, alors tout Certificat local peut être utilisé pour signer.

Dans tous les cas de figure, les dispositions suivantes s'appliquent :

- 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 ;
- Lorsqu'il s'agit d'une Signature électronique au format PAdES-LT, 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-LT, le champ motif de cette signature comporte les nom et prénom du Signataire, ainsi que l'identifiant de la Transaction de signature qui figure également dans le Fichier de Preuve associé à la Transaction ;
- La Signature électronique est horodatée par le service d'horodatage de Goodflag.

Des évolutions logicielles sont prévues permettant de configurer et paramétrer Goodflag Signature de manière à appliquer une « normalisation » des nom et prénom du Signataire au niveau des données d'identification fournies par un Gestionnaire 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.

9.5 — Principe de la Signature électronique simple avec Goodflag Signature

Dans le cas d'une Signature électronique de niveau simple, Goodflag Signature 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 « Goodflag – Qualified Seal », 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 qualifié au sens du règlement eIDAS, le Certificat au nom de « Goodflag – Qualified Seal », 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-LT, le Gestionnaire 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-LT, 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 Goodflag ;
- La Signature électronique peut être conditionnée par un mécanisme d'authentification défini au préalable par le Gestionnaire, tel qu'un OTP envoyé par courriel ou par SMS, ou encore une connexion à un SSO.

9.6 — Principes de la Signature électronique avancée de Goodflag Signature

Dans le cas d'une Signature électronique de niveau avancé, Goodflag Signature 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, ainsi que le nom de l'entité légale à laquelle est rattachée le Signataire et la fonction occupée ; 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 ;
- Lorsqu'il s'agit d'une Signature électronique au format PAdES-LT, le Gestionnaire 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-LT, 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 Goodflag ;
- La Signature électronique est nécessairement conditionnée par un mécanisme d'identification du Signataire par le Gestionnaire selon différentes méthodes telles que :
    - La fourniture d'une pièce d'identité par le Signataire, au préalable de la Transaction, que le Gestionnaire utilisera pour identifier le Signataire, suivie lors de la signature d'une authentification également définie au préalable par le Gestionnaire, telle qu'une connexion à un SSO ou un OTP envoyé par courriel ou par SMS : dans ce cas le Certificat, à usage unique et d'une durée de validité d'1 (une) heure, est dénommé « OPEN REG » (pour « open registration » en anglais) dans la Politique de Certification ; aucun contrôle n'est effectué sur l'identité du Signataire, celle-ci repose uniquement sur la vigilance, la rigueur du Gestionnaire ;
    - La fourniture d'une pièce d'identité par le Signataire, téléversée au cours du processus de signature, qui est évaluée de manière synchrone par un service de vérification de pièce d'identité conforme à la norme ETSI EN 319 411-1 LCP, précédée d'une authentification par un OTP envoyé par SMS : dans ce cas le Certificat, à usage unique et d'une durée de validité d'1 (une) heure, est dénommé « ETSI LCP » (car le Certificat est lui-même certifié ETSI EN 319 411-1 LCP) dans la Politique de Certification ; dans le cas où l'identité fournie par le Gestionnaire diffère de l'identité vérifiée, le processus de signature est interrompu et aucun Certificat n'est généré ; à noter que la vérification de la pièce d'identité n'est nécessaire que lors de la première signature du Signataire effectuée de cette manière, car tant que la pièce d'identité est valide, la vérification est considérée viable et le Signataire peut procéder directement à la signature après une authentification de type OTP SMS ;
    - 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 le Gestionnaire 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.

9.7 — Principes de la Signature électronique qualifiée de Goodflag Signature

Pour la Signature électronique qualifiée, Goodflag Signature propose deux modes :

- Un mode « local », dans lequel le Signataire dispose au préalable d'un Certificat qualifié eIDAS reposant sur un dispositif de création de Signature électronique également qualifié (généralement une puce intégrée à une carte à puce ou à un token USB) qui lui ont été remis précédemment par une Autorité de Certification du marché ; cette solution répond de manière directe aux exigences de la Signature électronique qualifiée telle qu'elle est définie par le règlement eIDAS. Sont détaillées les opérations suivantes sont réalisées :

- Initialisation d'une Transaction de Signature électronique sécurisée ;
- Acceptation des CGU relatives à la Transaction de Signature électronique et vérification des documents à signer ;
- Appel par Goodflag Signature du composant local Odisia Desktop qui récupère les empreintes des données à signer et qui les chiffre à l'aide de la Clé Privée du dispositif cryptographique du Signataire en s'appuyant sur les protocoles PKCS#11 ou MSCAPI et la fourniture par le Signataire du code PIN du dispositif cryptographique ;
- Récupération par Goodflag Signature des résultats fournis par Odisia Desktop et création des Signatures électroniques des documents à signer ;
- Les Signatures électroniques sont ensuite horodatées par le service d'horodatage de Goodflag.

/ Un mode « serveur », dans lequel le Signataire ne dispose pas au préalable d'un tel Certificat ; dans ce cas c'est l'Autorité de Certification intégrée à Goodflag Signature, « Sunnystamp Natural Persons CA », qui se charge de délivrer « à la volée », au Signataire, son Certificat ; afin de pouvoir garantir la conformité au standard ETSI EN 319 411-2 au niveau QCP-n-qscd du Certificat, les opérations suivantes sont réalisées :

- Initialisation d'une Transaction de Signature électronique sécurisée ;
- 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 (nom, prénom et pays de naissance) du Signataire 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 ;
- La Signature électronique est horodatée par le service d'horodatage de Goodflag.

Pour la Signature électronique qualifiée en mode « serveur », le moyen d'identification électronique utilisé peut être de différents types :

- L'Identité Numérique La Poste, proposée par la société Docaposte, entreprise avec laquelle Goodflag a contractualisé, afin de permettre aux Signataires qui disposent d'une telle identité numérique, la possibilité de réaliser ainsi des Signatures électroniques qualifiées au sens du règlement eIDAS. Aujourd'hui plusieurs 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.
- France Identité, proposée par France Titres, administration avec laquelle Goodflag a contractualisé, afin de permettre aux Signataires qui disposent d'une telle identité numérique, la possibilité de réaliser ainsi des Signatures électroniques qualifiées au sens du règlement eIDAS. Aujourd'hui plusieurs millions de français bénéficient déjà de France Identité. Celle-ci s'obtient gratuitement en mairie, dès lors que l'on dispose d'une nouvelle carte d'identité (au format carte bancaire) et que l'on a installé l'application France Identité sur son smartphone puis généré le QR code de demande de certification de son identité numérique.

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

A noter que FranceConnect+ ne peut être utilisé aujourd'hui qu'avec France Identité, ceci pour des raisons purement contractuelles.

9.8 — Distinction entre les niveaux de Signature électronique

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 Signature électronique 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 Goodflag Signature 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 Goodflag 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 Goodflag ;
- 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. Celle-ci peut également être certifiée ETSI EN 319 411-1 LCP, sur la base d'une vérification automatisée d'une pièce d'identité et d'une authentification par OTP SMS ;

- La Signature électronique qualifiée « à distance » (à la différence du mode local avec un certificat sur support cryptographique) 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.

9.9 — 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.

9.10 — 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.

Nota bene : notre solution est compatible avec FranceConnect v2 depuis la version 1.17.

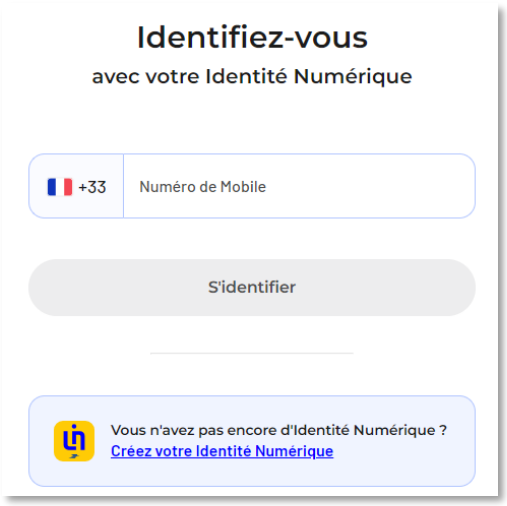
9.11 — Authentification via « l'Identité Numérique La Poste »

Dans le cas où le Signataire est invité à s'authentifier[4] 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.

[4] 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 électronique 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.



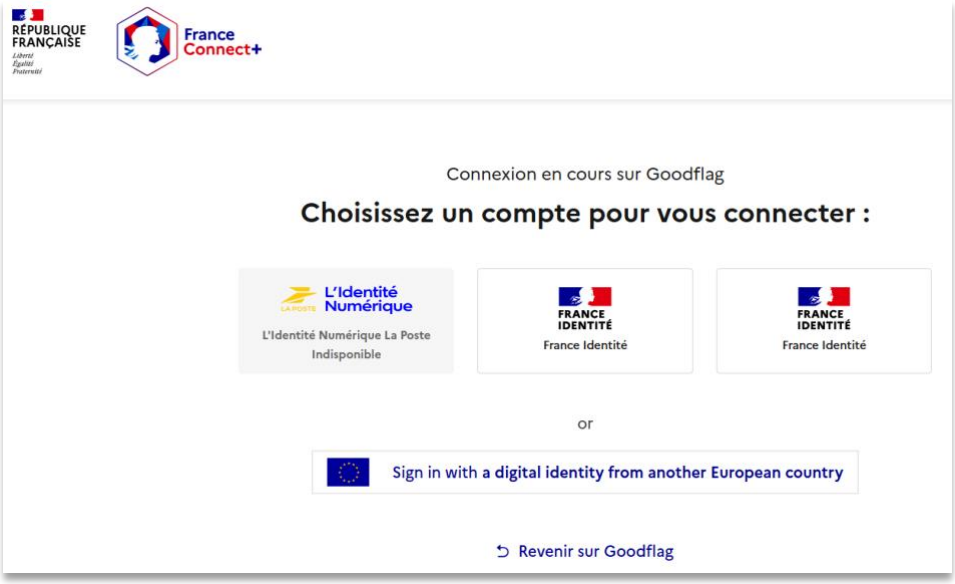
Une fois authentifié, il est redirigé vers la plateforme Goodflag Signature.

9.12 — 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 sélectionner France Identité comme Fournisseur d'Identité.



Page d'identification FranceConnect+

Nota bene : L'Identité Numérique La Poste n'est actuellement pas pris en charge pour l'authentification via FranceConnect+

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

9.13 — Authentification via France Identité

Dans le cas où le Signataire est invité à s'authentifier via France Identité, la page ci-dessous s'affiche :

Page d'authentification avec France Identité

Après avoir cliqué sur le bouton « Se connecter avec France Identité » le Signataire est redirigé vers la page d'identification de France Identité, qui invite le Signataire à scanner le QR code via l'application mobile France Identité.

Page d'identification France Identité

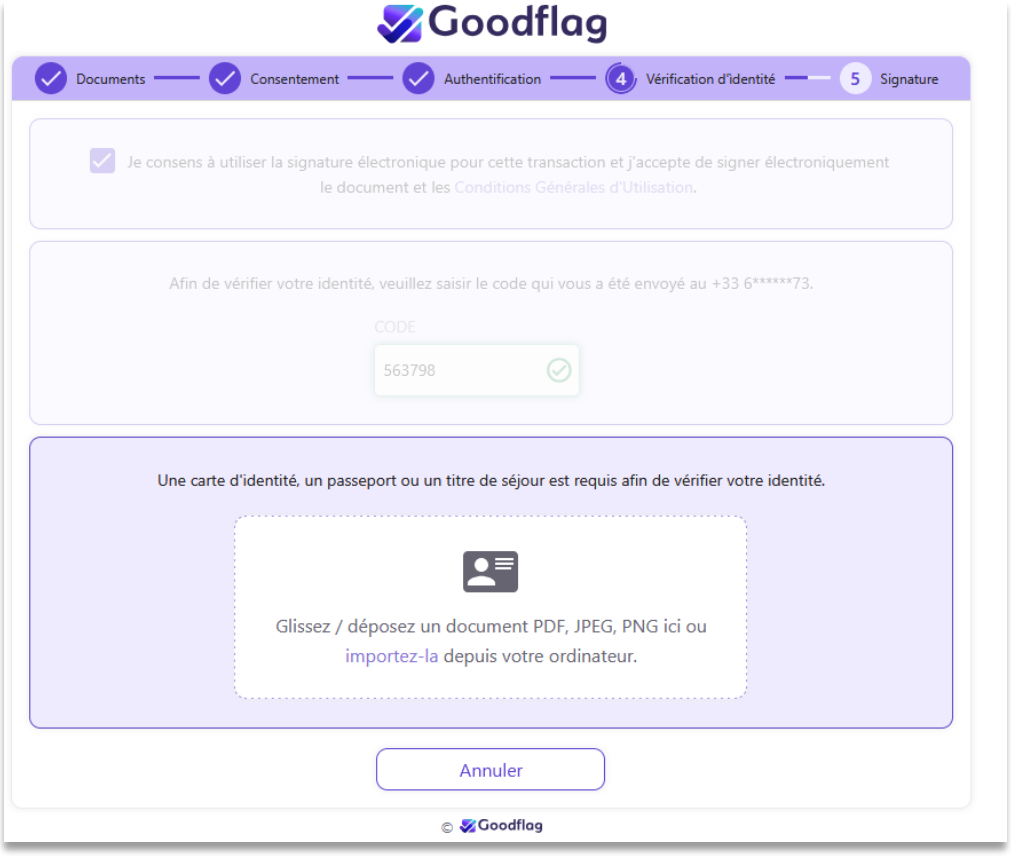
Le Signataire est invité à approuver la demande de connexion et à entrer son code personnel.

Il procède ensuite à la lecture sans contact de sa carte d'identité.

Une fois l'opération validée, il est automatiquement redirigé vers la solution Goodflag Signature.

9.14 — Vérification de la pièce d'identité du Signataire

Si la vérification de la pièce d'identité du Signataire est requise dans le processus, celui-ci téléverse le fichier contenant le scan de sa pièce d'identité en cours de validité.



Page d'authentification avec vérification de la pièce d'identité

9.15 — Signature électronique locale

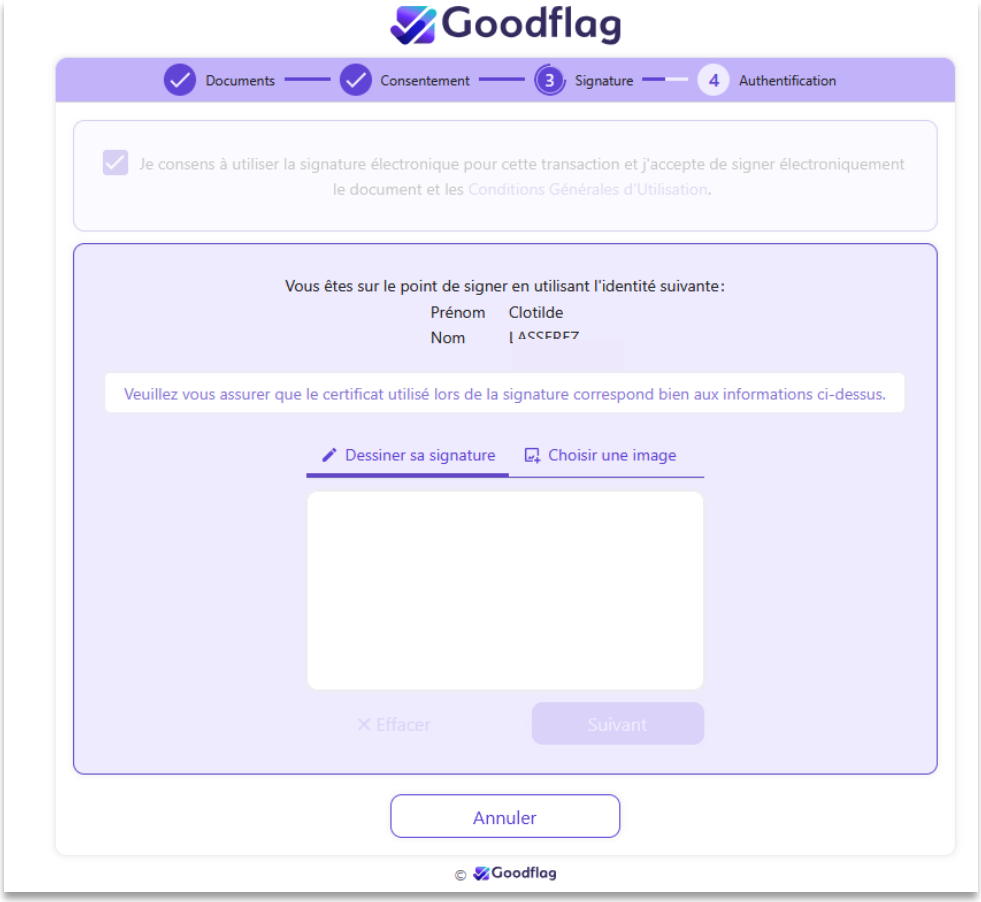
Goodflag Signature prend en charge des Certificats au format logiciel (par exemple les Certificats conformes au niveau RGS*) ou sur support cryptographique de type carte à puce ou clé USB délivrés par des Prestataires de Services de Certification électroniques.

Les protocoles supportés sont PKCS#11 et MSCAPI.

Si le Signataire utilise un Certificat qualifié ETSI EN 319 411-2 QCP-n-qscd, alors la signature produite par Odisia Desktop sera de niveau qualifié au sens du règlement eIDAS.

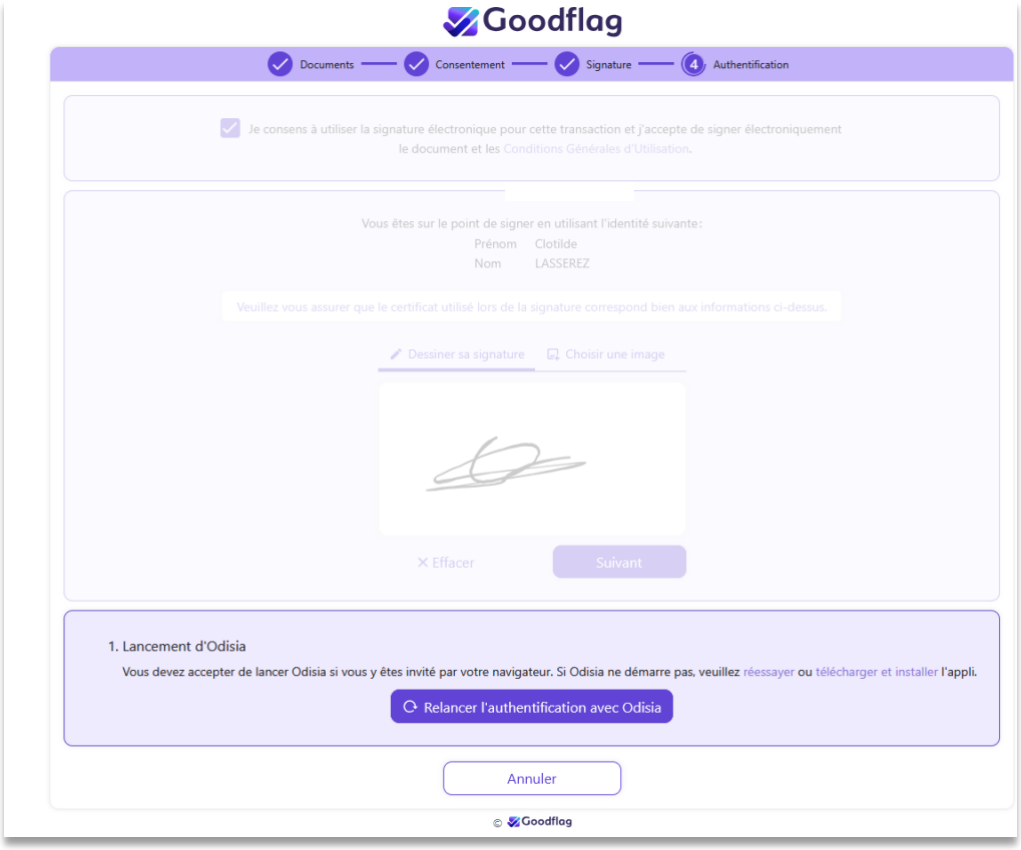
Lorsqu'il s'agit de signer avec un Certificat personnel, sur support cryptographique ou au format logiciel, la page de signature déclenche l'exécution du composant de signature Odisia[5] disponible sur Mac et PC, qui doit être préalablement installé sur le poste de travail du Signataire.

Cette installation peut être déclenchée lors de la première utilisation d'Odisia par le Signataire.



Page d'authentification avec certificat local

[5] Odisia est un composant fourni par Lex Persona. Il s'agit d'une architecture de Signature électronique qui permet de signer en quelques clics tout type de document, que ce soit à l'aide d'un Certificat sur support cryptographique ou logiciel que vous avez en votre possession.



Page de lancement d'Odisia Desktop

Lorsqu'Odisia Desktop se lance, le Signataire est invité à sélectionner le Certificat qu'il souhaite utiliser, parmi les Certificats présents sur son poste. Si un filtrage a été mis en place, par exemple pour imposer la signature de niveau qualifié, Odisia Desktop filtrera pour ne présenter que les Certificats qualifiés disponibles.

Écran de sélection du Certificat sur le poste de travail

Le Signataire saisit le code PIN associé à son Certificat. Les signatures sont créées et l'application Odisia Desktop se ferme automatiquement.

9.16 — Formats de signature

La solution Goodflag Signature produit des Signatures électroniques aux formats PAdES, CAdES et XAdES en fonction des besoins utilisateurs.

Goodflag Signature supporte les formats de signature suivants :

- PAdES-B-LT ou PAdES-B-LTA pour les fichiers PDF ;
- CAdES-B-LT détachée pour tout type de fichier — dans ce cas, le fichier signé résultant est un fichier au format ZIP contenant le fichier d'origine ainsi que le fichier de signature électronique au format binaire nommé signature.p7s. En cas de signatures CAdES détachées multiples, autant de fichiers .p7s sont générés que de signatures apposées sur le document ;
- CAdES-B-LT enveloppante pour tout type de fichier — dans ce cas, le fichier signé résultant est un fichier au format ZIP contenant le fichier d'origine ainsi que le fichier de signature électronique au format binaire nommé signature.p7m, qui encapsule le fichier d'origine. En cas de signatures CAdES enveloppantes multiples, un seul fichier .p7m est généré, contenant l'ensemble des SignerInfos correspondant aux signatures apposées sur le document
- XAdES-B-LT enveloppée pour la signature des fichiers de type PES V2 associés au projet Hélios (bordereaux de dépense, de recette et pièces jointes associées) ;
- XAdES-B-LT détachée avec Manifest, pour tout type de fichier, et en particulier pour la signature des remises règlementaires effectuées auprès de l'ACPR ou d'autres procédures – dans ce cas, le fichier signé résultant est un fichier au format ZIP contenant le fichier d'origine ainsi que le fichier de signature électronique au format XML nommé signature.xml.

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

Goodflag Signature vérifie, avant signature, le statut de révocation et le référentiel du Certificat et inclut dans chaque signature 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.

Goodflag Signature permet également, pour la signature en mode local, le filtrage des Certificats en fonction de critères complexes (OID, Autorités de Certification, usages de la Clé Privée, etc.).

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

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

Afin de garantir la valeur probatoire des Signatures électroniques, y compris pour les documents au format XML, Goodflag Signature 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 contraintes de visualisation sont paramétrables dans les appels à Goodflag Signature par les services appelants.

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

9.19 — Dossier de preuve

9.19.1 — Constitution du Dossier de Preuve

Le Dossier de Preuve contient l'ensemble des éléments collectés par Goodflag Signature pour l'ensemble des Transactions de Signature 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.

9.19.2 — 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 Goodflag Signature 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.

9.19.3 — 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 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 ;
- L'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.

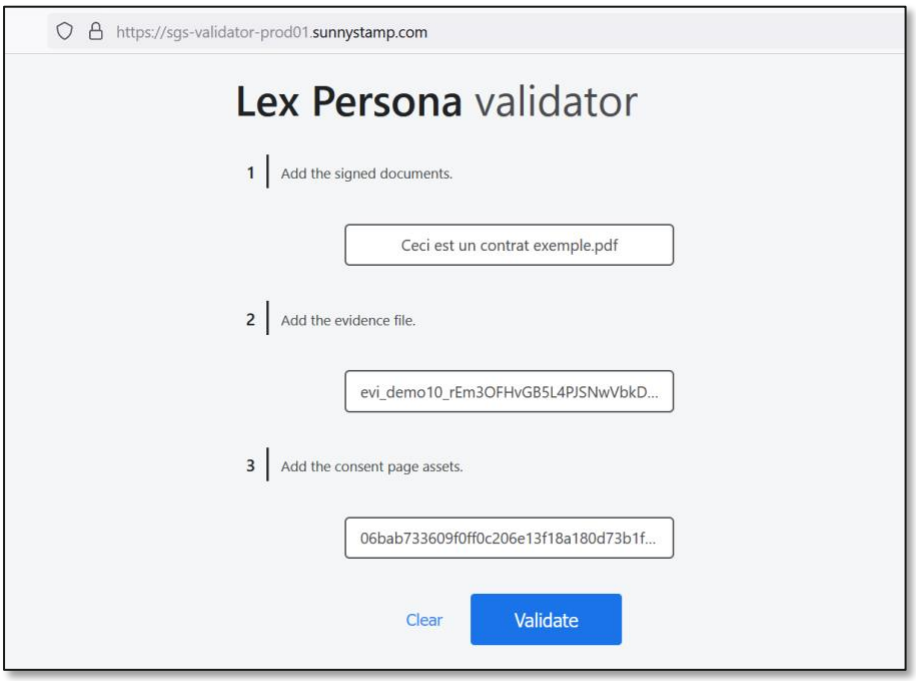
Le Fichier de Preuve permet également de reconstituer le parcours déroulé par le Signataire lors du recueil de son consentement et de rejouer l'ensemble des écrans présentés durant la Transaction de Signature électronique.

9.19.4 — 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 :

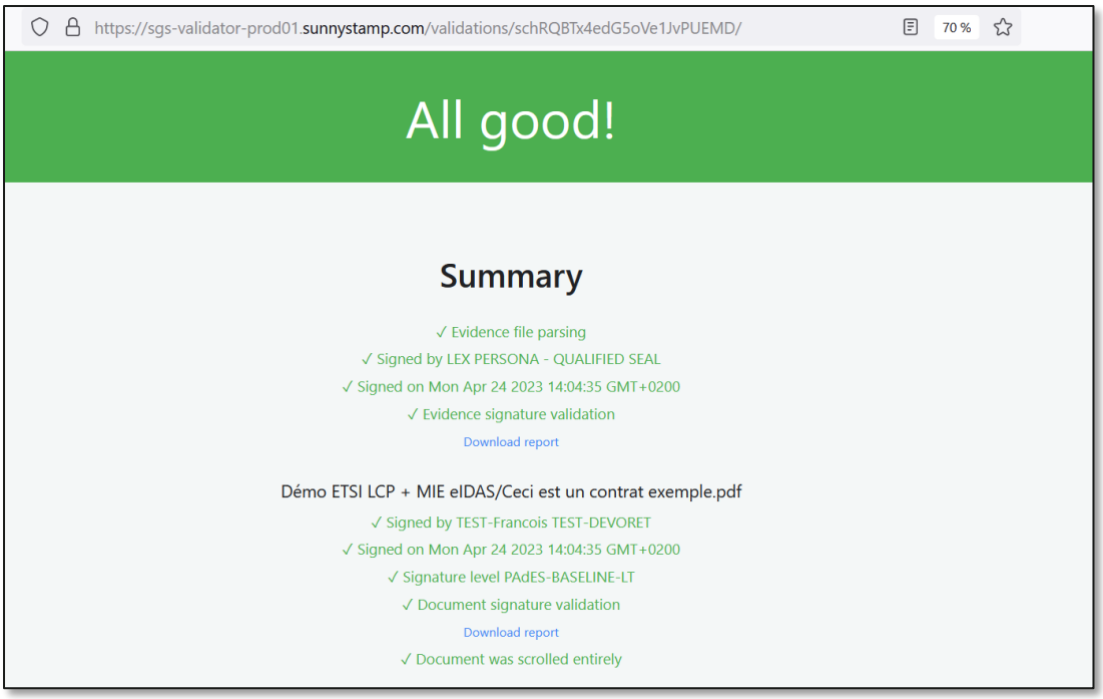
- Dézipper le Dossier de Preuve dans un répertoire [dossier_de_preuve] ;
- Repérer le Fichier de Preuve (fichier dont le nom commence par « evi ») concerné ; si besoin ouvrir le Fichier de Preuve et repérer la section signerEmail pour retrouver l'adresse de courriel du Signataire considéré ;
- Ouvrir un navigateur Internet et se rendre sur la page https://sgs-age-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.

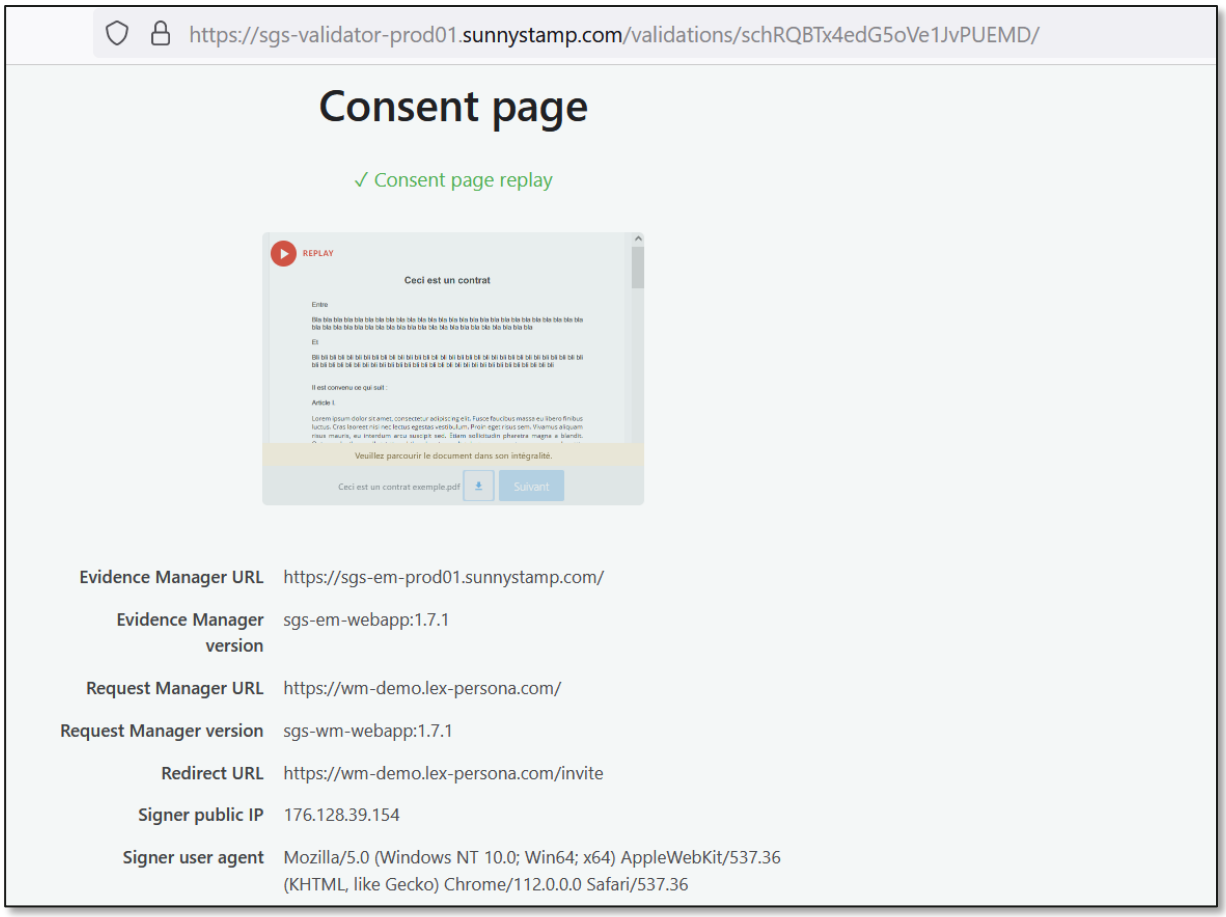


Résumé d'ensemble de la validation du Fichier de Preuve et des documents signés

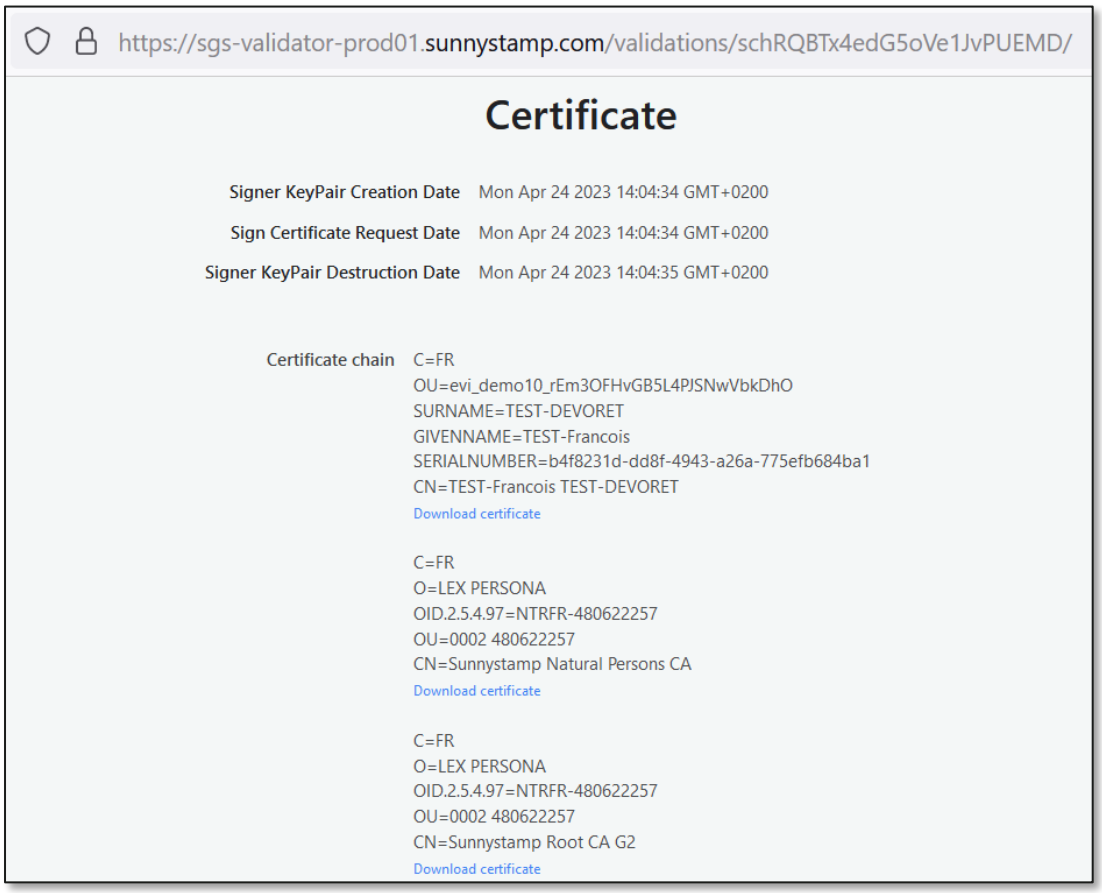
Il est ensuite possible de rejouer les écrans de la transaction ainsi que de consulter les éléments de traçabilité de la transaction :

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

Validation de la signature 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

9.20 — Horodatage des Signatures électronique

Toute Signature électronique réalisée par Goodflag Signature est horodatée par un service d'horodatage RFC3161 opéré par Goodflag afin de garantir l'antériorité de la Signature électronique produite par rapport à la date contenue dans les jetons d'horodatage et de

prouver que le Certificat du Signataire n'était pas révoqué au moment de la Signature électronique.

Les Signatures électroniques peuvent également être horodatées avec le service d'horodatage qualifié eIDAS de Goodflag.

10 — Interopérabilité

10.1 — API REST

Goodflag Signature emploie le protocole HTTPS et fournit une API native de type REST.

Cet API permet de développer des connecteurs avec une application cliente (Portail Web, CRM, ERP, GED, face, coffre-fort numérique) pour générer et suivre automatiquement des Parapheurs et récupérer leurs contenus (documents signés, pièces jointes non signées, métadonnées, Fichiers de Preuve), généralement lorsque leur statut est « terminé », c'est à dire lorsque tous les Validateurs et/ou Signataires ont respectivement validé et/ou signé un Parapheur.

10.1.1 — Prérequis

Pour utiliser l'API REST de Goodflag Signature, il est nécessaire de disposer des éléments suivants :

- Un client REST capable d'envoyer des données au format JSON dans des requêtes HTTPS et traiter les réponses au format JSON ;
- L'URL d'accès à l'API REST ;
- D'une API Key remise par l'équipe Goodflag ou générée depuis le Portail Web de Goodflag Signature par un Utilisateur ayant les droits pour le faire.

10.1.2 — Fonctions

Les principales fonctions de l'API sont listées ci-dessous :

- Création des Tenants ;
- Création des Groupes ;
- Création de comptes Utilisateur et d'Organisations ;
- Création de Parapheurs ;
- Ajout d'étapes à un Parapheur ;
- Téléversement de documents dans un Parapheur ;
- Différents niveaux de personnalisation des notifications ;
- Configuration des Webhooks pour que les applications clientes soient notifiés en temps réel du changement de statut d'un Parapheur afin notamment de récupérer les documents signés et les Fichiers de Preuve une fois qu'un Parapheur est terminé ;
- Téléchargement des documents signés d'un Parapheur ;
- Téléchargement des Dossiers de preuve.

10.1.3 — Approches de surveillance des Parapheurs

L'API REST propose deux approches pour suivre le cycle de vie des Parapheurs :

- Le Polling : L'application métier interroge l'API pour savoir s'il y a des Parapheurs qui sont terminés afin de télécharger les documents signés ;

- Le Webhook : Après chaque changement de statut, suite à une Signature électronique ou à la clôture d'un Parapheur, la plateforme Goodflag Signature permet l'envoi d'une notification HTTP pour informer une application cliente de la possibilité de télécharger les documents signés.

L'application cliente appelle ensuite l'API de téléchargement des documents signés.

À noter qu'en mode non-automatique, Goodflag Signature propose 3 moyens de récupérer des documents signés :

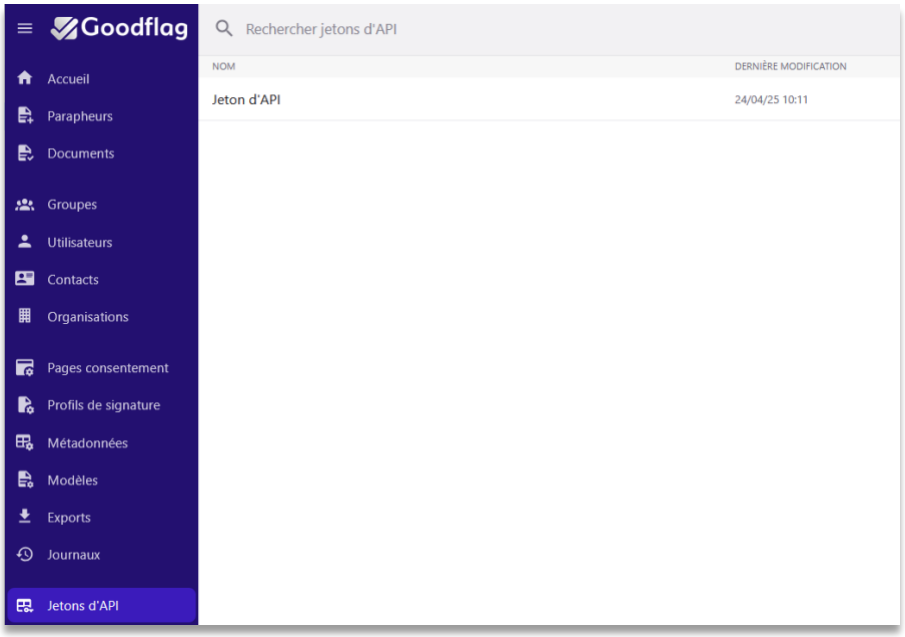
- Au travers du Portail Web, les administrateurs fonctionnels peuvent télécharger à tout moment les fichiers des Parapheurs en cours et terminés, de manière individuelle (fichier par fichier ou en lot dans un ZIP) ainsi que les Dossiers de preuve (Fichiers de Preuve au format XML et les assets de la Page de Consentement). Le Portail Web propose, en plus, une fonction d'export des Parapheurs, des Utilisateurs, des Groupes et des Contacts ;
- Par le Signataire, juste après avoir signé : il est possible de permettre au Signataire d'un Parapheur de télécharger à partir d'un lien de téléchargement le contenu du Parapheur qu'il vient de signer ;
- Réception automatique par courriel : il est possible de paramétrer l'envoi automatique des documents signés, à un destinataire donné (généralement un Signataire externe), en fin de circuit, lorsque tous les Validateurs et/ou Signataires ont validé et/ou signé le Parapheur.

10.2 — Fonctionnalités de l'application liées aux API

10.2.1 — Jetons d'API

Les Utilisateurs disposant du rôle de développeur ont accès depuis la solution au volet « Jetons d'API » qui leur permet de créer des Jetons d'API à destination des applications métier.

Un Jeton d'API permet d'appeler les différents endpoints exposés à travers l'API de Goodflag Signature selon les droits et autorisations qui sont accordés à son propriétaire.



Liste des Jetons d'API

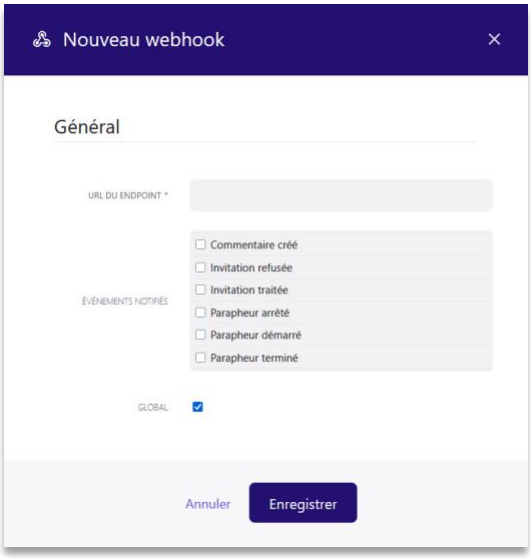
10.2.2 — Webhooks

La solution Goodflag Signature permet également aux Utilisateurs qui disposent du rôle de développeur de créer de nouveaux Webhooks et de consulter les journaux associés à ces Webhooks.

Un Webhook est un mécanisme de communication entre applications qui permet à l'application cliente d'être notifiée en quasi-temps réel par le service lors d'un changement de statut d'une étape et/ou d'un Parapheur.

Il existe deux types de Webhooks :

- Les Webhooks globaux qui peuvent être créés uniquement par des administrateurs du Tenant (et qui notifient des événements concernant tous les Parapheurs du Tenant) ;
- Les Webhooks non-globaux qui peuvent être créés par un développeur (et qui ne notifient que des événements concernant les Parapheurs dont il est propriétaire).



Nouveau Webhook

La création des Webhooks s'effectue depuis le Portail Web de la solution ou via l'API.

La solution permet de paramétrer des en-têtes de webhooks.

10.3 — Interfaçages

10.3.1 — Interfaçages avec les annuaires d'entreprise

La solution Goodflag Signature peut utiliser l'annuaire d'entreprise pour authentifier les utilisateurs. Dans ce cas, elle utilise le protocole OpenID Connect, compatible avec la plupart des Fournisseurs d'Identité du marché.

Les données utilisateurs récupérés de l'annuaire peuvent être utilisées pour la délivrance des Certificats de Signature électronique générés « à la volée », à savoir les nom, prénom et nationalité, ainsi que les moyens d'authentification utilisés pour la Signature électronique, pour des besoins de traçabilité (journaux et Fichiers de Preuve).

10.3.2 — Interfaçage avec la messagerie d'entreprise

Les courriels transmis aux Utilisateurs, Signataires et Validateurs sont transmis par les applications métier du client. Les seuls courriels transmis par la plateforme Goodflag

Signature le sont pour la transmission des codes d'authentification (OTP) dans le cadre de la délivrance des Certificats générés « à la volée ». Ces codes d'authentification sont destinés aux Signataires.

Le Signataire devra, pour la bonne réception des OTP par courriel, configurer son serveur et/ou son application de messagerie pour autoriser les courriels provenant de l'expéditeur des messages.

10.3.3 — Archivage des document signés

Il est possible de stocker vos documents pendant une durée déterminée par votre contrat. Ce stockage sera effectué dans les règles de l'art puisque nous sommes certifiés ISO 27001[6].

La solution Goodflag Signature peut également s'interfacer avec tous les SAE. Il est également possible de récupérer le document signé par API et de le verser dans un coffre-fort électronique.

10.3.3.1. Connecteurs natifs

Goodflag Signature propose deux connecteurs natifs pour archiver automatiquement vos documents signés et dossiers de preuve :

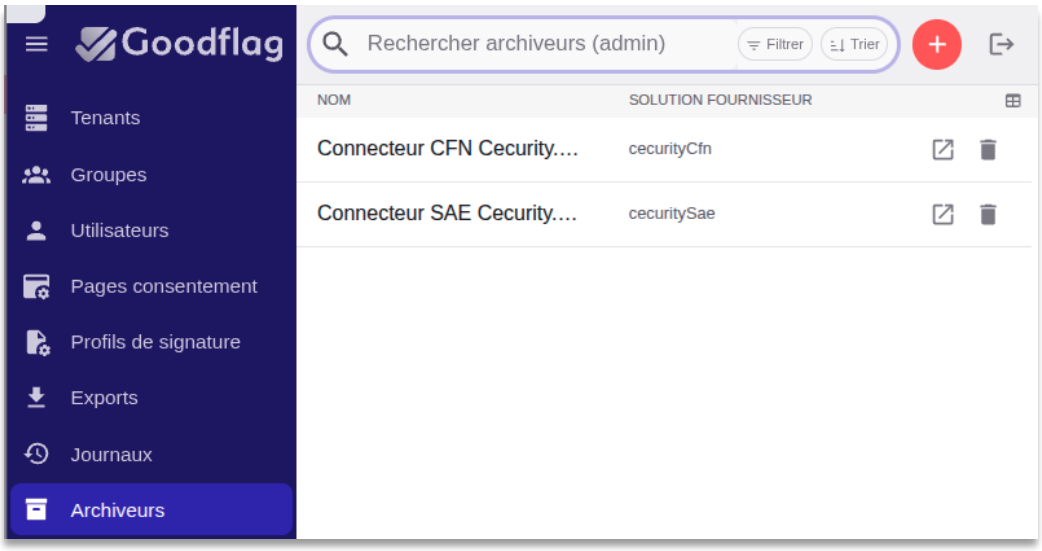
- Service d'Archivage Externe Cecurity.com
- Coffre-fort numérique Cecurity.com

L'archivage se déclenche uniquement sur les parapheurs qui sont clôturés.

Prérequis

Deux conditions doivent être réunies pour activer la fonctionnalité :

- L'archivage externe doit être activé au niveau du serveur (activé par défaut en mode SaaS)
- Une solution d'archivage compatible (Cecurity.com) doit être activée pour votre tenant



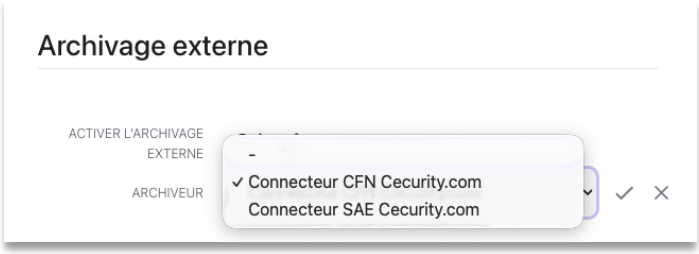
Section « Archiveurs »

[6] https://www.lex-persona.com/certifications/

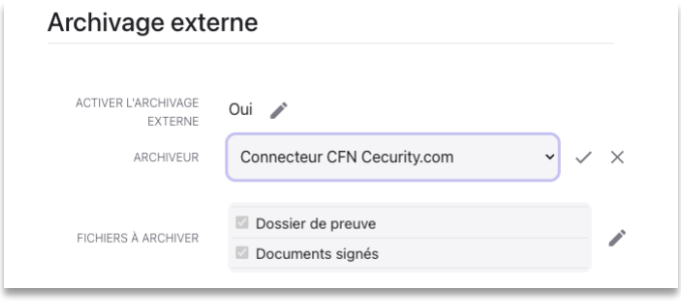
Configuration

Une fois ces prérequis remplis, les paramètres d'archivage externe sont accessibles depuis le détail de votre tenant. Vous y configurez :

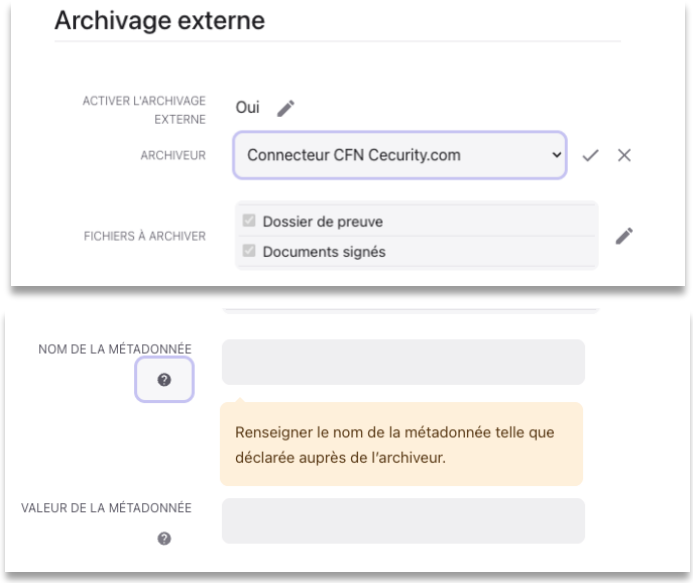
- La solution d'archivage à utiliser ;



- Les types de fichiers à archiver (documents signés, dossiers de preuve) ;



- Les métadonnées transmises à l'archiveur, y compris des métadonnées personnalisées définies selon vos besoins métier.

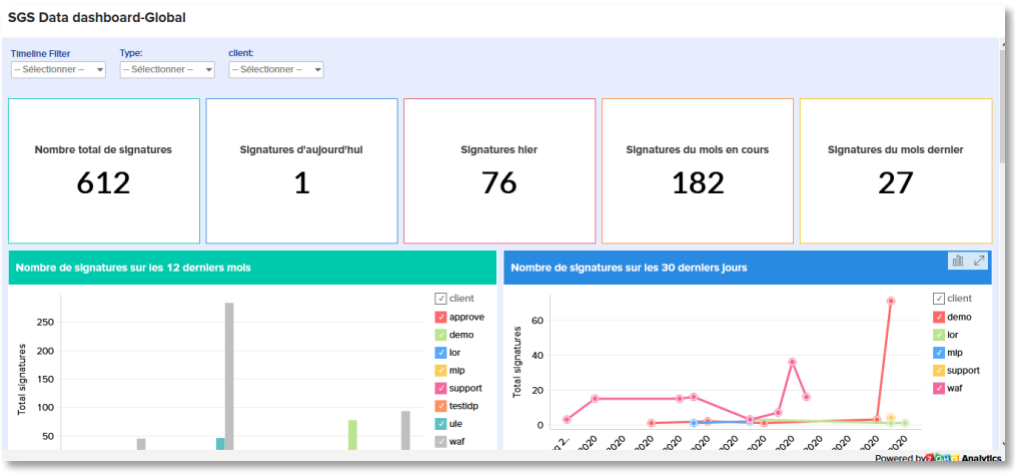


Cette granularité permet de piloter précisément le périmètre archivé et l'indexation des documents côté archiveur.

11 – Indicateurs

Goodflag propose à ses clients un accès à une interface permettant de lister des indicateurs de consommation et performances en temps réel sous forme de graphe circulaire, diagramme en barres, histogramme ou courbe.

Un extrait de Dashboard Goodflag Signature est présenté dans l'image ci-dessous :



Exemple de Dashboard Goodflag Signature

Les indicateurs listés sont les suivants :

- Nombre de Signatures électroniques réalisées :
  - Sur une période,
  - Par format de Signature électronique (PAdES, CAdES ou XAdES),
  - Par mode de Signature électronique (Distant ou Local) ;
- Nombre de Certificats générés :
  - Volume des fichiers signés,
  - Le temps moyen de délivrance d'un Certificat généré « à la volée »,
  - Le temps moyen de signature d'une empreinte de hachage,
  - Le temps moyen de signature d'une Transaction.

Il est possible de :

- Consulter ces statistiques en ligne et/ou à partir de l'application métier ;
- Récupérer l'état des opérations de signature via l'API de la solution ;
- Vérifier la disponibilité de l'application via une URL de « health check » ;
- Consulter les journaux dans les fichiers de log.

12 — Sécurité & Confidentialité

Architecture

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

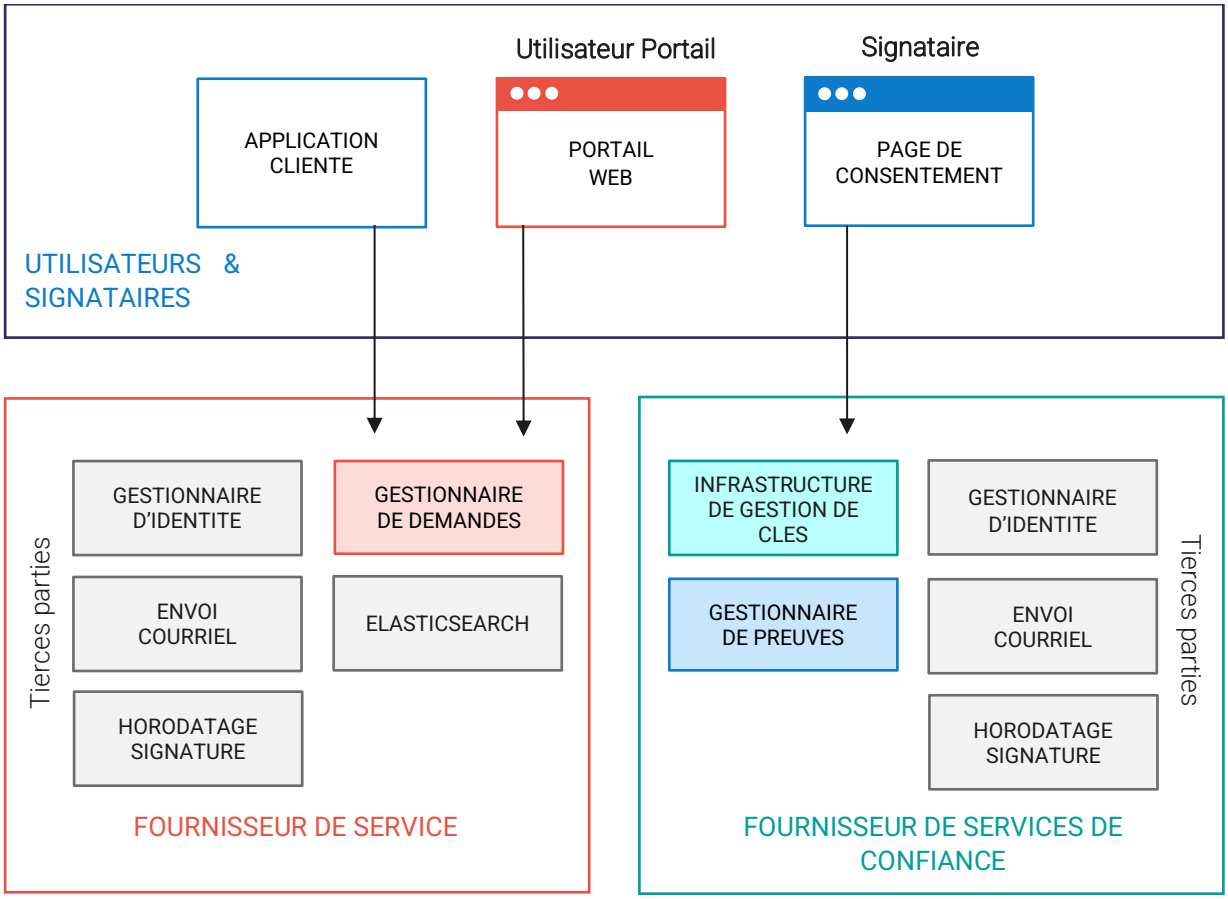


Schéma d'architecture de la solution Goodflag Signature

- 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 Goodflag ou par le Client (en mode « On Premise ») :
  - Le Gestionnaire de Demandes ou « Workflow Manager », composant central de Goodflag Signature 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 Goodflag :
  - 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.

12.1 — Hébergement et disponibilité

L'infrastructure matérielle et réseau de la plate-forme Goodflag Signature, en mode SaaS, a la 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.

12.2 — Sécurité

L'ensemble des services SaaS et des développements effectués par Goodflag sont couverts par la certification ISO 27001:2017 et HDS. En plus des audits annuels réalisés pour ces certifications, Goodflag 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 Goodflag par badges nominatifs ; ∕ Surveillances des datacenters 24h/24 par vidéo-surveillance et alarmes.
Données	∕ Ensemble des données hébergées en France ;

Critère de sécurité	Valeur
	⁄ Chiffrement de toutes les données (et de leurs sauvegardes) dans la transmission et dans le stockage ; ⁄ 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.

12.3 — 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.

12.4 — Protection des données

Toute collecte et tout usage de données à caractère personnel par la plateforme Goodflag Signature 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, Goodflag est sous-traitant du Client qui est responsable de traitement. De ce fait Goodflag, en ce qui concerne les traitements des données personnelles, agit sous son instruction.

L'architecture de la solution Goodflag Signature (brevetée par Goodflag), lorsque le Gestionnaire de Demandes (Workflow Manager) est installé « On Premise » (voir schéma) permet de réaliser des Signatures électroniques et des Cachets sans que les documents ne soient transmis à Goodflag. Seules les empreintes non-signées et signées circulent sur Internet.

Cette disposition spécifique aux logiciels Goodflag garantit tout à la fois la confidentialité des données et, de facto, leur conformité au regard du règlement sur la protection de données personnelles, mais également un meilleur temps de réponse car les empreintes sont plus légères que les documents complets.

Les données et fichiers dupliqués dans l'environnement Goodflag Signature sont :

- Les données personnelles des Signataires, utilisées dans le cadre d'une Signature électronique en mode « serveur » pour la délivrance des Certificats de signature générés « à la volée » ;
- Les empreintes des documents signés et cachetés ;
- Tous les éléments de traçabilité relatifs aux Transactions effectuées ; ces éléments sont conservés dans les Fichiers de Preuve.

Ces données personnelles sont confidentielles et ne seront utilisées que dans la finalité susvisée. Goodflag s'engage à ne pas divulguer à des tiers autres que ses sous-traitants, les données personnelles relatives à chaque Utilisateur sans l'autorisation préalable de la personne concernée.

Ces données sont conservées sur la plateforme Goodflag Signature pendant une durée qui sera déterminée par le client et pouvant être différenciée par type de donnée. Le stockage sécurisé s'effectue sur des serveurs hébergés dans les deux datacenters de Goodflag.

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

Le Prestataire s'engage à restituer ou supprimer les Données à l'expiration du contrat, quelle qu'en soit la cause, et à ne pas en conserver de copie. Une fois les copies détruites, le Prestataire adressera au Client un procès-verbal de destruction.

Le Client reconnaît et accepte que sont soustraites à l'obligation de destruction et de restitution les Données à caractère personnel pour lesquelles le Prestataire a une obligation juridique de conservation.

12.5 — 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.

12.6 — Stockage chiffré et sécurisé

L'ensemble des serveurs de production utilisés par la plateforme Goodflag Signature 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.

12.7 — Taux de disponibilité

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

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.

12.8 — Normes/certifications

La plateforme Goodflag Signature fait l'objet d'audits dans le cadre des différentes certifications maintenues par Goodflag.

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

12.8.1 — Certification ISO 27001

Goodflag est certifiée ISO 27001 depuis le 13 octobre 2017 sur l'ensemble de ses activités (dont Goodflag Community fait partie), sans exclusion d'aucune mesure ou clause citées dans cette norme.

La certification ISO 27001 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 Goodflag.

La certification ISO 27001 (version 2022) réalisée par la société LSTI, organisme de vérification de la conformité agréé par le COFRAC, peut être vérifiée à cette adresse.

12.8.2 — Certificats qualifiés eIDAS de personnes physiques

En 2024, Goodflag a renouvelé la qualification eIDAS de son Autorité de Certification « Sunnystamp Natural Persons CA » pour la délivrance de Certificats qualifiés de personnes physiques basés sur l'authentification du Signataire effectué à l'aide d'un moyen d'identification électronique de niveau substantiel ou élevé notifié à la commission européenne.

La qualification eIDAS de cette Autorité de Certification pour le type de Certificat qualifié référencé ci-dessus selon le standard EN 319 411-2 au niveau QCP-n-qscd permet à la plateforme Goodflag Signature d'effectuer des Signatures électroniques qualifiées eIDAS

12.8.3 — Horodatage qualifié eIDAS

En 2024, Goodflag a renouvelé avec succès la qualification de son service d'horodatage « Lex Persona eIDAS Qualified Timestamp ».

Ce service d'horodatage qualifié eIDAS et conforme au standard EN 319 421 est utilisé par Goodflag Signature pour horodater toutes les Signatures et Cachets électroniques produits par la plateforme.

12.8.4 — Certificats qualifiés eIDAS de personnes morales

En 2024, Goodflag a obtenu la qualification eIDAS de son Autorité de Certification « Sunnystamp Legal Persons CA 1 » pour la délivrance de Certificats qualifiés de personnes morales.

La qualification eIDAS de cette Autorité de Certification pour le type de Certificat qualifié référencé ci-dessus selon le standard EN 319 411-2 au niveau QCP-l-qscd permet à la plateforme Goodflag Signature d'effectuer des Cachets électroniques qualifiés eIDAS, notamment pour la sécurisation des Signatures électroniques de niveau simple ainsi que pour le cachetage des Fichiers de Preuve et des Certificats de Preuve définitifs.

12.8.5 — Hébergement des Données de Santé (HDS)

En 2022, Goodflag a obtenu la certification Hébergement des Données de Santé à caractère personnel (HDS) en tant qu'Hébergeur d'infrastructure physique et Hébergeur infogéreur sur les solutions Goodflag Signature et Sunnyseal.

La certification HDS permet à Goodflag d'assurer la sécurisation des données de santé aux clients qui l'exigent.

L'ensemble de ces qualifications et certifications peuvent être consultés sur cette page https://www.lex-persona.com/certifications/