# Politique et Pratiques
# du service de recommandé électronique

# LETRECO

Version 1.6 du 1er juillet 2022

| Etat du document – Classification | Référence |
|---|---|
| Validé - Public | OID : 1.3.6.1.4.1.51763.1.1.2 |

# Versions

| Version | Date | Description | Auteurs | Société |
|---|---|---|---|---|
| 1.0 | 12/7/2018 | Création du document | G. Loth Demay | Equisign |
| 1.1 | 27/07/2018 | Modifications après audit de qualification | G. Loth Demay | Equisign |
| 1.2 | 08/06/2020 | Ajout de méthodes d'identification et d'authentification<br>Evolution de l'OID, entrée en vigueur planifiée dès la décision de LSTI et de l'ANSSI | G. Loth Demay | Equisign |
| 1.3 | 13/10/2020 | Suppression de toute référence au mode d'identification à distance | G. Loth Demay | Equisign |
| 1.4 | 8/03/2022 | Changement d'adresse postale | G. Loth Demay | Equisign |
| 1.5 | 07/04/2022 | Ajout des services de cachet et d'horodatage de Universign<br>Précision du plan de transfert ou de fin d'activité<br>Maintien de la conformité avec la norme EN 319 401 v2.3.1<br>Entrée en vigueur planifiée dès la décision de LSTI et de l'ANSSI | G. Loth Demay | Equisign |
| 1.6 | 30/05/2022 | Evolution de l'algorithme du calcul d'empreinte des preuves<br>Précisions sur la génération et la vérification des éléments de preuve d'intégrité des courriers<br>Ajout du nom du prestataire d'hébergement et d'infogérance<br>Entrée en vigueur planifiée dès la décision de LSTI et de l'ANSSI | G. Loth Demay | Equisign |

# Table des matières

# 1 Introduction

## 1.1 Présentation générale

Equisign propose à ses clients un service d'envoi recommandé électronique. Ce service permet d'acheminer de manière sécurisée un courrier électronique depuis un expéditeur, client du service, vers un destinataire désigné par l'expéditeur. Le service assure l'authentification des parties et génère des preuves opposables en justice pour toutes les actions associées aux courriers (envoi, réception, refus, non réclamation).

Le présent document constitue la politique d'envoi des recommandés électroniques du service, ainsi que dans le même temps la déclaration des pratiques associées à sa mise en œuvre.

L'objectif de ce document est de définir les engagements pris par Equisign, en tant que fournisseur de services de confiance (Trust Service Providers au sens eIDAS) pour l'envoi des recommandés électroniques et de définir les obligations des autres participants.

Le service d'envoi recommandé électronique mis en œuvre par Equisign est qualifié au sens du règlement européen eIDAS, et plus précisément conformément à son article 44. La présente politique est ainsi conforme aux exigences du règlement européen et à celles de l'organe de contrôle national français.

## 1.2 Identification du document

La présente politique est identifiée par l'OID suivant : 1.3.6.1.4.1.51763.1.1.2

## 1.3 Date d'entrée en vigueur

La présente politique entre en vigueur à la date de qualification par l'ANSSI du service incluant le service d'horodatage de Universign. Elle reste applicable jusqu'à son remplacement par une nouvelle version de la politique.

## 1.4 Gestion de la politique

### 1.4.1 Entité gérant la politique

La politique est gérée par les membres du comité de pilotage du service au sein de Equisign.

### 1.4.2 Point de contact

Le point de contact du comité de pilotage du service est :

| |
|---|
| Equisign |
| Service Letreco |
| Tour Opus 12 |
| 77 Esplanade du Général de Gaulle |
| 92800 Puteaux |

### 1.4.3 Procédure d'approbation de la politique

La politique est approuvée par Equisign après examen et relecture du document par les membres du comité de pilotage, et par les personnes désignées par celui-ci.

Cette relecture a pour objectif d'assurer :

- La conformité de la politique avec les exigences réglementaires et normatives portant sur la fourniture d'un service de recommandé électronique qualifié ;

- La cohérence de la politique avec les autres documents publiés dans le cadre du service, tels par exemple que les conditions générales d'utilisation ;
- La concordance entre les engagements exprimés dans la politique et les moyens techniques et organisationnels mis en œuvre par Equisign et ses partenaires ;
- L'information effective de l'ANSSI pour toute modification importante dans la fourniture du service de confiance qualifié (y compris celles entrainant des changements dans la liste de confiance), selon les modalités décrites dans les procédures de qualification. Cela comprend notamment, sans s'y limiter :
    - les changements induits par une modification de la politique de service ou des conditions générales d'utilisation associées ;
    - les changements de sous-traitants ;
    - les modifications des conditions d'hébergement ;
    - les changements de matériels cryptographiques ;
    - les modifications d'architecture technique ;
    - les changements de procédures d'enregistrement et d'identification ;
    - les changements dans la gouvernance du service.

Le comité de pilotage s'assure que la date d'entrée en vigueur de la nouvelle politique laisse, dans la mesure du possible, un délai suffisant aux clients pour prendre connaissance des nouvelles dispositions et adapter si besoin leurs pratiques. Le comité de pilotage vérifie que le respect des dispositions prévues au chapitre 2 est bien prévu.

### 1.4.4 Amendements à la politique

#### *1.4.4.1 Procédures d'amendement*

Des amendements à la présente politique peuvent être prévus au cours de la durée de vie du service, par exemple pour :

- Des corrections induites par les audits du service ;
- Des corrections mineures (erreurs, oublis, précisions supplémentaires…) ;
- L'extension du service de recommandé électronique qualifié à d'autres catégories d'utilisateurs ;
- L'acceptation ou la mise en œuvre de nouveaux moyens d'identification électronique ;
- Des changements d'ordre technique (mise en œuvre, partenaires, fournisseurs, etc…).

Toute proposition d'évolution du service fait l'objet d'une analyse d'impact afin de déterminer son éventuelle incidence sur :

- La qualité ou la sécurité du service ;
- Les expéditeurs ou destinataires des envois recommandés ;
- La conformité de l'offre qualifiée aux exigences du règlement eIDAS ;
- La nécessité de mise à jour des autres documents publiés ;
- Les pratiques internes de Equisign ou de ses partenaires et fournisseurs.

En cas d'impact majeur, un changement d'OID de politique est prévu, et l'évolution et son analyse d'impact peuvent être soumises à l'ANSSI et à l'organisme de certification pour avis ou commentaire.

L'analyse d'impact est étudiée par le comité de pilotage qui valide ou non le lancement d'une évolution. Le cas échéant, la nouvelle politique sera soumise à l'approbation du comité de pilotage.

#### *1.4.4.2 Mécanisme et période d'information sur les amendements*

Une fois l'évolution du service validée par le comité de pilotage, les amendements à la politique sont communiqués aux clients et à toutes les parties prenantes dans la fourniture du service. Un délai de prévenance suffisant est prévu pour leur permettre de prendre connaissance des nouvelles dispositions et d'adapter si besoin leurs pratiques.

Equisign adresse annuellement à l'ANSSI une synthèse de l'ensemble des modifications apportées à la fourniture de son service d'envoi recommandé qualifié.

#### *1.4.4.3 Circonstances selon lesquelles l'OID doit être changé*

Toute évolution de la présente politique ayant un impact majeur sur le service se traduit par une évolution de l'OID, afin que les utilisateurs puissent clairement distinguer quels envois correspondent à quelles exigences.

## 1.5 Documents associés

### 1.5.1 Politique d'horodatage

La date et l'heure d'envoi et de réception sont indiquées par un horodatage électronique qualifié.

Ce service d'horodatage répond à une politique d'horodatage identifiée dans chaque contremarque de temps par l'OID suivant :

- Horodatage par DocuSign France : 1.3.6.1.4.1.22234.2.6.5.8 ;
- Horodatage par Universign : 1.3.6.1.4.1.15819.5.2.2

L'horloge de ces services d'horodatage est synchronisée avec le temps UTC avec une exactitude déclarée de une seconde.

### 1.5.2 Politique de certification du cachet électronique

Les preuves générées par le service d'envoi recommandé sont scellées par un service de cachet électronique.

Le certificat de cachet est émis selon une politique de certification, identifiée dans le certificat, par l'OID suivant :

- Certificat émis par DocuSign France : 1.3.6.1.4.1.22234.2.9.3.21 ;
- Certificat émis par Universign : 1.3.6.1.4.1.15819.5.1.3.5

### 1.5.3 Politique de création de cachet

Le cachet électronique avancé utilisé pour sécuriser l'envoi et la réception des données est apposé dans des conditions décrites dans un document de politique de création de cachet. Cette politique, propre à Equisign et respectée quel que soit le prestataire de création de cachet, est identifiée par l'OID suivant : 1.3.6.1.4.1.51763.1.2.1

### 1.5.4 Conditions générales d'utilisation

Les clauses principales de ce document sont synthétisées dans les Conditions Générales d'Utilisation (CGU) du service d'horodatage. Les CGU répondent aux imposées pour les services eIDAS et intègrent ainsi les engagements respectifs du fournisseur du service ainsi que les clients et des utilisateurs.

Les CGU peuvent contenir des clauses supplémentaires régissant les relations entre le client et Equisign, et qui ne remettent pas en cause le contenu de cette politique.

### 1.5.5 Documents normatifs

| | |
|---|---|
| [ANSSI_LRE] | *Services d'envoi recommandé électronique qualifiés – Critères d'évaluation de la conformité au règlement eIDAS,* Version 1.0 du 3 janvier 2017<br>https://www.ssi.gouv.fr/uploads/2016/06/eidas_envoi-recommande-electronique-qualifie_v1.0_anssi.pdf |
| [ANSSI_PSCO] | *Prestataires de services de confiance qualifiés – Critères d'évaluation de la conformité au règlement eIDAS,* Version 1.2 du 5 juillet 2017<br>https://www.ssi.gouv.fr/uploads/2017/01/eidas_psc-qualifies_v1.2_anssi.pdf |
| [EN_319401] | *ETSI EN 319 401 V2.3.1 (2021-05) Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.*<br>https://www.etsi.org/deliver/etsi_en/319400_319499/319401/02.03.01_60/en_319401v020301p.pdf |
| [GDPR] | *Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 – Règlement Général de Protection des Données*<br>https://www.cnil.fr/fr/reglement-europeen-protection-donnees |
| [EIDAS] | *Règlement (UE) 2014/910 du Parlement européen et du Conseil du 23 juillet 2014*<br>https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32014R0910 |
| [RE_2015_1502] | *Règlement d'exécution (UE) 2015/1502 de la Commission du 8 septembre 2015 fixant les spécifications techniques et procédures minimales relatives aux niveaux de garantie des moyens d'identification électronique du règlement eIDAS*<br>https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32015R1502 |
| [TRUSTED_LIST] | *Tableau de bord des services de confiance eIDAS – Navigateur des listes de confiance des services qualifiés*<br>https://esignature.ec.europa.eu/efda/tl-browser/#/screen/home |

## 1.6 Présentation du service Letreco

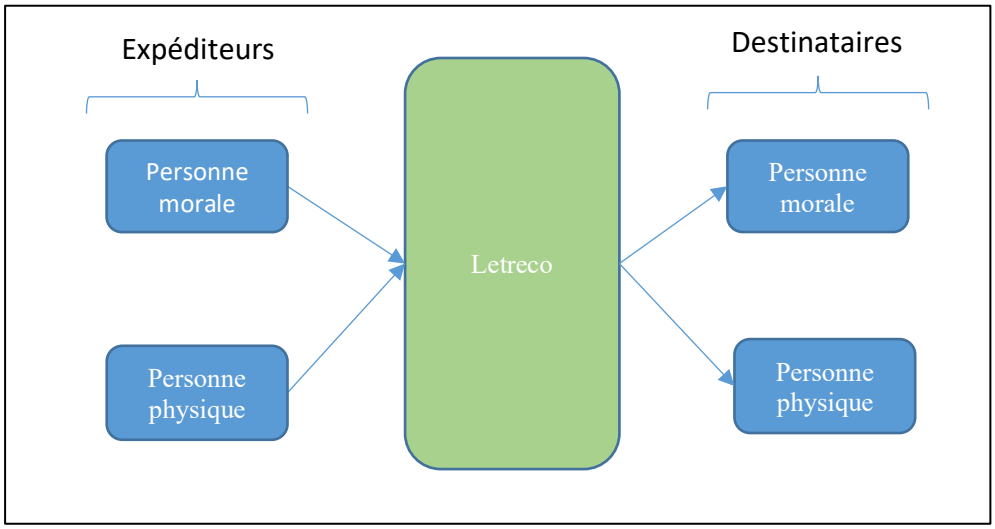
Le service Letreco permet à des personnes morales ou physiques d'envoyer des recommandés électroniques à d'autres personnes morales ou physiques.

L'expéditeur utilise le service via son interface Web ou par des appels WebServices. Il s'authentifie et communique au service les données du courrier à envoyer et son destinataire.

Le service Letreco notifie le destinataire par voir électronique de la réception d'un courrier recommandé électronique, et lui donne un délai de 15 jours pour accepter et télécharger le courrier.

Le destinataire doit s'authentifier pour pouvoir réceptionner les courriers recommandés qui lui sont adressés. Pour une personne morale, le retrait est effectué par un serveur ou une personne physique possédant le pouvoir adéquat.

Le schéma de fonctionnement général est le suivant :




Le service Letreco offre des fonctions :

- D'authentification des expéditeurs et destinataires ;
- De dépôt pour les expéditeurs ;
- De notification des destinataires ;
- D'acceptation, de retrait ou de refus pour les destinataires ;
- De génération de preuve à disposition des expéditeurs ;
- De conservation de preuves légales, horodatées et protégées par un cachet, associées au fonctionnement du service.

## 1.7 Entités intervenant dans le service de recommandé électronique

### 1.7.1 Prestataire du service de recommandé électronique (PSRE)

Le Prestataire du Service de Recommandé Electronique (PSRE) est Equisign.

Le PSRE définit la politique du service et responsable de la conformité de sa mise en œuvre, par ses moyens propres ou par ses partenaires.

### 1.7.2 Opérateur du service de recommandé électronique (OSRE)

L'Opérateur du Service de Recommandé Electronique est Equisign.

L'OSRE est responsable de la mise en œuvre de l'infrastructure du service conformément à la politique du service.

### 1.7.3 Prestataire d'hébergement et d'infogérance

L'opérateur du Service de Recommandé Electronique confie l'hébergement et l'infogérance des infrastructures techniques de production à la société Claranet.

Claranet est un opérateur certifié ISO 27001, dont les activités réalisées dans le cadre du service Letreco sont auditées conformément aux exigences de cette politique.

### 1.7.4 Prestataires d'horodatage, de cachet et de certification

Deux prestataires qualifiés de services de confiance peuvent être indifféremment sollicités par Equisign pour la création d'un cachet électronique sur les preuves et leur horodatage qualifié. Ce sont :

- DocuSign France ;
- Universign.

Ces prestataires sont chacun responsable :

- de la fourniture de jetons d'horodatage conformément à leur politique d'horodatage qualifié (voir au §1.5.1) ;
- de la création de cachets électroniques conformément à la politique de création de cachet et aux exigences techniques et organisationnelles définies par cette politique pour le service (voir au §1.5.3) ;
- de l'émission et de la gestion des certificats de création de cachet électronique selon une politique de certification certifiée ou qualifiée (voir au §1.5.2).

### 1.7.5 Expéditeur

Les expéditeurs sont des personnes morales ou physiques enregistrées sur le service Letreco après avoir signé un contrat en ce sens avec la société Equisign ou l'un de ses distributeurs. Les expéditeurs ont toujours de ce fait accepté les conditions générales du service Letreco de Equisign.

Le service Letreco est accessible à toute personne morale ou physique capable d'accéder au service et de s'authentifier lors de l'envoi (ou du retrait) de recommandés électroniques (selon les modalités définies au §3).

Les expéditeurs sont en charge de recueillir le consentement préalable des destinataires non professionnels à recevoir un courrier recommandé électronique et attestent à Equisign avoir réalisé cette démarche.

Les expéditeurs garantissent l'exactitude des informations qu'ils transmettent au service lors de leur enregistrement ou lors du dépôt d'un courrier, que ce soit leur identité ou celle du destinataire, les adresses électroniques et postales et la qualité de professionnel ou non professionnel du destinataire.

Les expéditeurs s'engagent de plus à respecter leurs obligations contractuelles ou légales imposées par la présente politique ou la législation légale en vigueur (en particulier celle relative à la protection des données personnelles).

Les expéditeurs doivent prendre toutes les mesures appropriées de façon à protéger leurs propres systèmes informatiques des intrusions non autorisées, des actes de destruction ou d'altération, des contaminations éventuelles par des virus, chevaux de Troie ou autre système causant des failles de sécurité sur Internet. Ils veillent à ne pas introduire lors de leurs dépôts

tout virus, vers, bombe logique ou tout contenu pouvant être assimilés à du courrier non désiré.

Les expéditeurs doivent récupérer auprès du service les preuves relatives à leurs envois et les vérifier, et sont responsables de leur conservation pour leur propre compte.

Les expéditeurs doivent protéger leur moyen d'authentification (mots de passe, support de certificat, moyens d'identification électronique, clé TOTP…) contre la perte ou l'utilisation par un tiers. Ils doivent le révoquer sans délai en cas de perte, vol, compromission ou de suspicion de compromission.

### 1.7.6 Destinataire

Les destinataires sont les personnes morales ou physiques auxquelles sont expédiés les courriers recommandés.

Les personnes physiques destinataires doivent accepter ce moyen d'envoi de courrier recommandé préalablement à l'envoi. Cette demande doit être faite par l'expéditeur préalablement à l'envoi.

Les destinataires doivent prendre connaissance et accepter les conditions générales du service Letreco de Equisign avant de pouvoir retirer un courrier.

Les destinataires doivent obtenir un moyen d'authentification satisfaisant aux modalités définies au §3 pour pouvoir retirer les courriers recommandés. Pour ce faire, ils doivent vérifier l'exactitude de l'adresse postale à laquelle ils souhaitent recevoir ce moyen d'identification électronique. En cas d'incomplétude ou d'erreur, ils doivent saisir ou corriger cette adresse, et s'engagent alors à fournir une information exacte.

Les destinataires doivent protéger leur moyen d'authentification (mots de passe, support de certificat, moyens d'identification électronique, clé TOTP…) contre la perte ou l'utilisation par un tiers. Ils doivent le révoquer sans délai en cas de perte, vol, compromission ou de suspicion de compromission. Les destinataires s'engagent à alerter le service clients de Equisign en cas de problème rencontré lors de réception ou de l'utilisation de ce moyen d'authentification.

Les destinataires doivent prendre toutes les mesures appropriées de façon à protéger leurs propres systèmes informatiques des intrusions non autorisées, des actes de destruction ou d'altération, des contaminations éventuelles par des virus, chevaux de Troie ou autre système causant des failles de sécurité sur Internet

Les destinataires doivent protéger la confidentialité des notifications reçues et contenant l'URL unique de retrait de la LRE. Lorsque les destinataires acceptent une LRE, ils doivent la télécharger dans un délai restreint et défini par le service. S'ils constatent une erreur dans le courrier envoyé (mauvaise identité, contenu non conforme, …), ils sont tenus d'en alerter immédiatement l'expéditeur.

### 1.7.7 Utilisateurs et clients

Les utilisateurs du service sont les expéditeurs et les destinataires d'envoi recommandé.

Les utilisateurs doivent respecter les obligations de la présente politique qui leur sont applicables.

Lorsqu'un utilisateur reçoit un moyen d'authentification électronique, il est responsable de l'utilisation qui est faite de ce moyen d'authentification. Il doit :

- Protéger celui-ci de toute perte ou divulgation : Le moyen d'authentification est strictement personnel et ne doit pas être communiqués ou transmis à des tiers ;
- Révoquer sans délai le moyen d'authentification en cas de perte, vol, compromission ou de suspicion de compromission du moyen fourni.

Les utilisateurs doivent télécharger les preuves produites et mises à disposition par le service Letreco, durant leur période de disponibilité. Ces preuves doivent être vérifiées conformément aux recommandations indiquées au §4.4.7.

Les clients sont des entités liées contractuellement à Equisign pour envoyer des recommandés électroniques. Dans la suite du document, un client est donc un expéditeur pouvant éventuellement être aussi un destinataire.

# 2 Responsabilités concernant la mise à disposition des informations devant être publiées

## 2.1 Entités chargées de la mise à disposition des informations

La mise à disposition des informations devant être publiées à destination des utilisateurs du service (expéditeurs et destinataires) et des tiers ayant à déterminer la validité des preuves produites est réalisée par Equisign.

## 2.2 Informations devant être publiées

Equisign s'engage à publier au minimum les informations suivantes à destination des utilisateurs du service et des tiers ayant à déterminer la validité des preuves produites par celui-ci :

- Le présent document, décrivant la politique et les pratiques du service de recommandé électronique ;
- Les documents associés mentionnés aux §1.5.1 , §1.5.2 et §1.5.3, ou, dans le cas où un de ces documents serait maintenu et publié par un tiers, une référence univoque (URL, OID, etc.) à celui-ci et un point de publication ;
- Les conditions générales d'utilisation du service (cf. §1.5.4) ;
- Le certificat de cachet utilisé pour sécuriser l'envoi et la réception de données, et identifiant le service dans la liste de confiance.

Cers informations sont publiées sur le site web suivant : https://www.letreco.fr.

## 2.3 Délais et fréquences de publication

Les informations liées au service (nouvelle version des présentes, etc.) sont publiées dès que nécessaire afin que soit assurée à tout moment la cohérence entre les informations publiées et les engagements, moyens et procédures effectifs de Equisign. En particulier, toute nouvelle version est communiquée aux clients et, le cas échéant, fait l'objet d'un nouvel accord.

Les systèmes publiant ces informations sont disponibles au minimum les jours ouvrés. Il est à noter qu'une perte d'intégrité d'une information mise à disposition (présence de l'information et intégrité de son contenu) est considérée comme une indisponibilité de cette information.

## 2.4 Contrôle d'accès aux informations publiées

L'ensemble des informations publiées est libre d'accès en lecture.

L'accès en modification aux systèmes de publication est strictement limité aux fonctions internes habilitées de Equisign, au moins au travers d'un contrôle d'accès de type mots de passe basé sur une politique de gestion stricte des mots de passe.

# 3 Identification

## 3.1 Identification de l'expéditeur

Le service Letreco qualifié garantit l'identification de l'expéditeur avec un degré de confiance élevé par un certificat d'authentification ou de signature, remis après une validation initiale d'identité, et répondant à un niveau minimal de sécurité, comme exposé ci-dessous.

Les expéditeurs sont :

- Des personnes physiques ou morales ayant ouvert un compte auprès de Equisign et disposant en particulier d'un moyen d'authentification approprié ;
- Des notaires ou des clercs de notaire possédant une clé REAL (voir ci-dessous).

### 3.1.1 Validation initiale de l'identité

La validation initiale de l'identité de l'expéditeur est réalisée :

- par un face à face entre Equisign ou son mandataire et la personne physique ou le représentant autorisé de la personne morale. Cette rencontre se tient par exemple dans la phase d'établissement du contrat d'accès au service Letreco, et permet la remise du secret de génération d'un OTP d'authentification ou l'enregistrement du certificat qui sera utilisé par l'expéditeur pour ses envois ;
- par un face à face entre une Autorité de Certification reconnue par Equisign et la personne physique ou le représentant autorisé de la personne morale. Ce face à face a lieu lors de la demande ou de la remise du certificat de l'expéditeur. Les Autorités de Certification reconnues sont choisies par Equisign parmi celles délivrant les certificats spécifiés au §3.1.2 et dont les pratiques de certification associées ont été auditées par un organisme accrédité selon le référentiel applicable (RGS ou eIDAS) ;
- par un face à face organisé par La Poste, lors de la remise à l'expéditeur d'un moyen d'identification électronique de type OTP par courrier recommandé postal à la personne physique ou au représentant autorisé de la personne morale expéditrice.

Ce face à face permet d'établir le moyen d'authentification électronique qui sera utilisé par l'expéditeur auprès du service Letreco.

La vérification d'identité s'appuie sur des justificatifs fournis par l'expéditeur :

- Pour une personne physique : Pièce d'identité de l'expéditeur (carte nationale d'identité, passeport, titre de séjour) en cours de validité ;
- Pour une personne morale : Copie d'un K-bis de moins de 3 mois, pièce d'identité du responsable légal (carte nationale d'identité, passeport, titre de séjour) en cours de validité ou, si ce responsable légal se fait représenter, copie de la pièce d'identité du responsable légal, mandat et pièce d'identité du représentant autorisé.

### 3.1.2 Validation d'accès au service par un moyen d'identification électronique (MIE)

L'expéditeur s'authentifie auprès du service Letreco par l'un des moyens suivants :

- un certificat d'authentification pour s'authentifier à la connexion au service Letreco ;
- un certificat de signature pour être authentifié avec le dépôt du courrier ;
- un code à usage unique (OTP).

Le certificat d'authentification doit être un certificat SSL client de l'expéditeur. Le service identifie le client par le sujet du certificat communiqué lors de l'enregistrement du client. Le respect des conditions supplémentaires suivantes est imposé :

- Notaires et clercs de notaire : le certificat a été émis selon la Politique de Certification notariale des clés REAL, d'OID REALAUTH : OID 1.2.250.1.78.2.1.3.2.1.1 ou REAL : OID:1.2.250.1.78.1.1.3.1.3.1.1.22 (voir http://www.preuve-electronique).
- Autres personnes physiques ou morales :
    - le certificat a été émis selon une Politique de Certification qualifiée RGS au niveau ** ou *** ; ou
    - le certificat a été émis selon une Politique de Certification certifiée conforme au niveau EVCP ou QCP-w selon le règlement eIDAS.

Le certificat de signature doit être un certificat de signature de la personne physique ou de cachet de la personne morale expéditrice. Le service identifie le client par le sujet du certificat communiqué lors de l'enregistrement du client. Le respect des conditions supplémentaires suivantes est imposé :

- le certificat a été émis selon une Politique de Certification qualifiée RGS au niveau ** ou *** ; ou
- le certificat est un certificat qualifié selon le règlement eIDAS.

Le code à usage unique (OTP) est généré par l'expéditeur à l'aide d'une application installée par celui-ci sur un équipement personnel de type ordinateur, tablette ou mobile. L'expéditeur initialise ce générateur avec un code secret personnel qui lui a été remis lors de la vérification initiale d'identité. Le code à usage unique est un OTP calculé selon le procédé standardisé par la RFC 6238 (HOTP : codes dépendant de l'heure de génération et à validité limitée dans le temps). Le secret de génération des OTP est généré aléatoirement par le service Letreco et remis à l'expéditeur sur papier, en face à face par Equisign ou par courrier recommandé postal.

## 3.2 Identification du destinataire

Le service d'envoi recommandé électronique qualifié garantit l'identification du destinataire avant la fourniture des données.

Les destinataires sont les personnes physiques ou morales désignées par les expéditeurs, et qui n'ont pas obligatoirement déjà ouvert un compte lors de l'envoi du courrier. Pour pouvoir

accepter et télécharger un courrier recommandé, elles devront cependant accepter de se doter d'un moyen d'authentification approprié.

### 3.2.1 Validation initiale de l'identité

La validation initiale de l'identité du destinataire est réalisée :

- par un face à face entre Equisign ou son mandataire et la personne physique ou le représentant autorisé de la personne morale destinataire, lorsque le destinataire est déjà un client du service Letreco ;
- par un face à face entre une Autorité de Certification reconnue par Equisign (idem §3.1.1) et la personne physique ou le représentant autorisé de la personne morale destinataire. Ce face à face a lieu lors de la demande ou de la remise du certificat du destinataire ;
- par un face à face entre un notaire ou un clerc de notaire et la personne physique destinataire ;
- par La Poste, lors de la remise au destinataire d'un moyen d'identification électronique de type Carte à code par courrier recommandé postal à la personne physique ou au représentant autorisé de la personne morale destinataire ;
- à l'aide d'une identité électronique (au sens du règlement [EIDAS]) via le portail FranceConnect+, notifiée par l'un des Etats membres de l'Union européenne, et qui satisfait aux exigences des niveaux de garantie substantiel ou élevé.

Cette validation d'identité constitue le préalable à la délivrance du moyen d'identification qui sera utilisé par le destinataire auprès du service Letreco. En cas d'utilisation d'une identité électronique eIDAS, le destinataire peut aussi accéder directement à l'acceptation et au retrait du courrier.

La vérification d'identité s'appuie sur les mêmes justificatifs que ceux décrits pour l'expéditeur au §3.1.1.

### 3.2.2 Validation via un moyen d'identification électronique (MIE)

Lorsque la vérification initiale d'identité donne lieu à la délivrance d'un moyen d'identification électronique, le destinataire s'authentifie auprès du service Letreco par :

- un certificat d'authentification ; ou
- un code issu d'une carte à codes.

Le certificat d'authentification, remis suite au face à face avec une AC, doit être un certificat SSL client du destinataire. Le service identifie le destinataire :

- pour une personne morale, par le numéro SIREN présent dans le certificat ;
- pour une personne physique, par ses nom et prénom présents dans le certificat, sachant que le cas des homonymes est discriminé par l'accès à l'URL unique communiqué par courriel au destinataire.

Le certificat d'authentification du destinataire doit respecter les mêmes exigences que celles décrites au §3.1.2 pour l'expéditeur.

Une carte à codes consiste en une grille comprenant une série de codes propres à chaque grille. Pour s'authentifier, l'utilisateur doit fournir l'un de ces codes choisi dynamiquement à chaque connexion par le service.

La carte à codes est générée par le service Letreco et remis au destinataire :

- En face à face par Equisign, un notaire ou un clerc de notaire ;
- Par courrier recommandé postal.

# 4 Exigences opérationnelles

## 4.1 Processus d'envoi

### 4.1.1 Processus et responsabilités pour le dépôt d'une LRE

#### *4.1.1.1 Prérequis pour l'expéditeur*

L'expéditeur est un client actif du service Letreco. Il dispose d'un compte client sur le service qui comporte ses informations d'identification, au minimum :

- son nom et son prénom s'il s'agit d'une personne physique ou le représentant autorisé de la personne morale, sa raison sociale s'il s'agit d'une personne morale ;
- son adresse électronique ;
- son adresse postale ;
- la valeur du champ 'sujet' de son certificat d'authentification ou de signature, s'il en possède un.

#### *4.1.1.2 Dépôt*

La connexion et l'authentification de l'expéditeur sur le service sont détaillées au §4.1.2.

L'expéditeur débute le processus de dépôt d'un courrier recommandé, en fournissant :

- le nom et le prénom ou la raison sociale du destinataire ;
- l'adresse électronique du destinataire ;
- optionnellement l'adresse postale du destinataire pour permettre si nécessaire l'envoi d'une carte à codes ;
- le statut professionnel ou non du destinataire (pour un particulier, l'expéditeur a en charge la demande préalable de consentement du destinataire à recevoir un recommandé électronique) ;
- les documents à transmettre sous la forme de documents numériques (les données du courrier).

Le dépôt du courrier recommandé ne sera réalisé que lorsque le service Letreco aura procédé à des vérifications préliminaires et en particulier que le destinataire sera en capacité de s'authentifier pour accepter et télécharger le courrier (voir §4.1.3 et §4.1.4).

Lorsque l'expéditeur est identifié par son certificat de signature, il signe et horodate les documents du courrier à envoyer avec son certificat de signature.

### 4.1.2 Exécution des processus d'identification de l'expéditeur

L'authentification est réalisée conformément au §3.1 :

- soit par l'établissement d'une connexion avec authentification mutuelle sur le service Letreco ;
- soit par la vérification de la signature des documents envoyés, après connexion de l'expéditeur avec son compte sur le service Letreco ;
- soit par un code à usage unique (OTP), après connexion de l'expéditeur avec son compte sur le service Letreco.

Lorsque l'expéditeur utilise un certificat d'authentification ou de signature, il est identifié par la valeur du champ 'sujet' du certificat utilisé. Le service vérifie la validité du certificat en vérifiant ses dates de validité, l'AC émettrice, sa politique de certification, son usage et son statut de révocation.

### 4.1.3 Traitement du dossier de dépôt d'une LRE

Le service effectue les contrôles suivants :

- La présence de toutes les informations non optionnelles citées au §4.1.1.2 ;
- L'absence de virus, cheval de Troie ou autre bombe logique dans les documents constituant les données des courriers (aucun autre contrôle n'est effectué sur le contenu) ;
- La cohérence entre l'expéditeur associé au compte utilisé pour la connexion et le signataire des données pour le cas de l'envoi de documents signés.

### 4.1.4 Acceptation ou rejet du dépôt

Le dépôt est accepté lorsque toutes les vérifications stipulées au §4.1.3 se terminent avec succès.

Sinon, le dépôt est refusé et cet échec est notifié à l'expéditeur. Aucun courrier recommandé électronique n'a été créé dans ce cas, et de ce fait aucune des preuves décrites au §4.3 n'est générée.

### 4.1.5 Obtention du consentement du destinataire non professionnel

L'obtention du consentement du destinataire non professionnel à recevoir un courrier recommandé sous forme électronique est à la charge de l'expéditeur, préalablement au dépôt du courrier. L'expéditeur s'y est engagé avant l'utilisation du service et le service Letreco n'effectue aucun contrôle de cette démarche.

### 4.1.6 Génération et mise à disposition de la preuve de dépôt

Lorsque le dépôt a été accepté, le service génère une preuve de dépôt.

La preuve de dépôt est horodatée par un service d'horodatage qualifié (voir au §1.5.1 et §1.7.3), avec la date et l'heure de la génération de cette preuve. La preuve de dépôt contient l'empreinte des données du courrier et est scellée par un service de cachet avancé (voir au §1.5.3 et §**Erreur ! Source du renvoi introuvable.**). Elle garantit ainsi l'intégrité des données et prouve l'heure de dépôt du courrier recommandé électronique.

La preuve de dépôt est mise à disposition par téléchargement à l'expéditeur. La preuve de dépôt est conservée par Equisign pour une durée de sept ans, et accessible à l'expéditeur pendant un an.

## 4.2 Processus de remise

### 4.2.1 Information du destinataire

Immédiatement après le dépôt, le service Letreco notifie le destinataire par messagerie électronique, à l'adresse indiquée par l'expéditeur, de la réception d'un courrier recommandé, sans en indiquer l'expéditeur.

Ce message de notification contient un lien (URL unique) pour l'acceptation ou le refus du courrier sur le site Web du service.

### 4.2.2 Délai d'acceptation de la LRE

Le délai d'acceptation du courrier est rappelé au destinataire dans le message de notification. Il est de 15 jours à compter du lendemain de l'envoi de la notification de réception.

Au-delà de ces 15 jours, le destinataire ne pourra plus accepter le courrier, qui sera considéré non réclamé (voir §4.2.6).

### 4.2.3 Exécution des processus d'identification du destinataire

L'identification et l'authentification du destinataire s'effectuent conformément au §3.2.

Lorsque le destinataire suit le lien présent dans le message de notification pour l'acceptation ou le refus du courrier, il peut s'authentifier par :

- un certificat d'authentification ; ou
- par un code d'accès (issu d'une carte à codes) à saisir sur une page du service ; ou
- par une identité électronique eIDAS de niveau substantiel ou élevé.

Lorsqu'un certificat d'authentification est utilisé, une connexion avec authentification mutuelle du service et du destinataire est établie. Le service vérifie la validité du certificat en vérifiant ses dates de validité, l'AC émettrice, sa politique de certification, son usage et son statut de révocation.

Lorsqu'une identité électronique eIDAS est utilisée, et une fois l'utilisateur authentifié, le service Letreco vérifie que :

- Les nom et prénom de la personne authentifiée sont strictement identiques à ceux du destinataire désigné par l'expéditeur ;
- L'identité utilisée est de niveau de garantie « substantiel » ou « élevé ».

### 4.2.4 Acceptation ou refus de la LRE

Lorsque le destinataire utilise un lien du message de notification, il sélectionne l'action qu'il veut engager sur le site du service Letreco. L'authentification par code d'accès est demandée uniquement pour l'acceptation du courrier.

L'acceptation ou le refus du courrier est une décision définitive sur laquelle le destinataire ne peut pas revenir, même s'il réutilise les moyens mis à sa disposition. Une preuve d'acceptation, ou de refus le cas échéant, est générée immédiatement après cette décision. Elle est mise à disposition par téléchargement à l'expéditeur. La preuve d'acceptation ou de refus est aussi téléchargeable par le destinataire. La preuve d'acceptation est conservée par Equisign pour une durée de sept ans, et accessible à l'expéditeur pendant un an.

La preuve d'acceptation ou de refus est horodatée par un service d'horodatage qualifié (voir au §1.5.1 et §1.7.3), avec la date et l'heure de la génération de cette preuve. La preuve contient l'identification du destinataire ayant accepté ou refusé le courrier. Elle est scellée par un service de cachet avancé (voir au §1.5.3 et §1.7.4) et prouve l'heure d'acceptation ou de refus du courrier par le destinataire.

#### 4.2.5 Transmission de la LRE

Le téléchargement du courrier recommandé est autorisé au destinataire uniquement lorsque celui-ci a accepté le courrier, et pendant une période de 15 jours à partir du moment de l'acceptation.

La preuve de réception est générée lorsque toutes les données du courrier ont été envoyées au destinataire, i.e. lorsque le téléchargement s'est terminé avec succès. Elle est mise à disposition par téléchargement à l'expéditeur. La preuve de réception est conservée par Equisign pour une durée de sept ans, et accessible à l'expéditeur pendant un an.

La preuve de réception est horodatée par un service d'horodatage qualifié (voir au §1.5.1 et §1.7.3), avec la date et l'heure de la génération de cette preuve. La preuve de réception contient l'identification du destinataire ayant téléchargé le courrier et est scellée par un service de cachet avancé (voir au §1.5.3 et §1.7.4). Elle prouve l'heure de réception du courrier par le destinataire.

#### 4.2.6 Non-réclamation de la LRE

Lorsque le destinataire n'a pas accepté le courrier dans le délai imparti (cf. §4.2.2), le service ne permet plus son acceptation, son refus ou son téléchargement. Une preuve de non réclamation est générée au plus tard le lendemain de l'expiration du délai prévu.

La preuve de non réclamation est horodatée par un service d'horodatage qualifié (voir au §1.5.1 et §1.7.3), avec la date et l'heure de la génération de cette preuve. La preuve de non réclamation est scellée par un service de cachet avancé (voir au §1.5.3 et §1.7.4). Elle prouve l'expiration du délai de réclamation du courrier recommandé électronique.

La preuve de non réclamation est mise à disposition par téléchargement à l'expéditeur. La preuve de non réclamation est conservée par Equisign pour une durée de sept ans, et accessible à l'expéditeur pendant un an.

### 4.3 Modification des données

Le service Letreco n'effectue aucune modification des données de la LRE, que ce soit pour l'envoi ou la remise de celles-ci.

### 4.4 Description des preuves

#### 4.4.1 Format

Le service Letreco génère des preuves sous forme de documents au format PDF.

Ces documents sont scellés par un cachet électronique et horodatés en respectant le standard PAdES Baseline Profile, ETSI TS 103172, v.2.2.2, (niveau T).

#### 4.4.2 Preuve de dépôt

La preuve de dépôt contient les informations suivantes :

| Objet ou entité | Informations indiquées |
|---|---|
| **Tiers d'acheminement** | Raison sociale |

| | |
|---|---|
| | Siège social<br>Adresse de contact |
| **Expéditeur** | Nom et prénom ou raison sociale<br>Adresse de messagerie électronique<br>Adresse postale (optionnel) |
| **Envoi** | Type de service et garanties<br>OID de la politique d'envoi recommandé appliquée<br>Référence unique du courrier<br>Date et heure de dépôt |
| **Données du courrier** | Pour chaque fichier envoyé :<br>• Nom du fichier<br>• Taille en octets<br>• Empreinte calculée en SHA-512 |
| **Destinataire** | Type : Particulier ou Professionnel<br>Nom et prénom<br>Raison sociale et fonction pour un professionnel<br>Adresse de messagerie électronique<br>Adresse postale (optionnel) |

Les données du courrier sont constituées par un ensemble de fichiers transmis par l'envoi recommandé (comme indiqué au §4.1.1.2).

La preuve de dépôt garantit l'intégrité des données du courrier en scellant (par le cachet électronique, puis par l'horodatage électronique), parmi les données de la preuve, la valeur de l'empreinte, calculée avec l'algorithme SHA-512, de chacun des fichiers transmis. Toute modification de l'un de ces fichiers est détectable par comparaison de l'empreinte du fichier considéré par rapport à l'empreinte indiquée dans la preuve. Ceci permet en outre d'identifier nominativement le fichier potentiellement modifié.

### 4.4.3 Preuve d'acceptation

La preuve d'acceptation contient les informations suivantes :

| Objet ou entité | Informations indiquées |
|---|---|
| **Tiers d'acheminement** | Raison sociale<br>Siège social<br>Adresse de contact |
| **Expéditeur** | Nom et prénom ou raison sociale |

| | |
|---|---|
| | Adresse de messagerie électronique<br>Adresse postale (optionnel) |
| **Envoi** | Type de service et garanties<br>OID de la politique d'envoi recommandé appliquée<br>Référence unique du courrier<br>Date et heure de dépôt |
| **Données du courrier** | Pour chaque fichier envoyé :<br>• Nom du fichier<br>• Taille en octets<br>• Empreinte calculée en SHA-512 |
| **Destinataire** | Type : Particulier ou Professionnel<br>Nom et prénom<br>Raison sociale et fonction pour un professionnel<br>Adresse de messagerie électronique<br>Adresse postale (optionnel) |
| **Acceptation** | Date et heure de l'acceptation du courrier |

#### 4.4.4 Preuve de refus

La preuve de refus contient les informations suivantes :

| Objet ou entité | Informations indiquées |
|---|---|
| **Tiers d'acheminement** | Raison sociale<br>Siège social<br>Adresse de contact |
| **Expéditeur** | Nom et prénom ou raison sociale<br>Adresse de messagerie électronique<br>Adresse postale (optionnel) |
| **Envoi** | Type de service et garanties<br>OID de la politique d'envoi recommandé appliquée<br>Référence unique du courrier<br>Date et heure de dépôt |
| **Données du courrier** | Pour chaque fichier envoyé :<br>• Nom du fichier<br>• Taille en octets |

| | |
|---|---|
| | • Empreinte calculée en SHA-512 |
| **Destinataire** | Type : Particulier ou Professionnel<br>Nom et prénom<br>Raison sociale et fonction pour un professionnel<br>Adresse de messagerie électronique<br>Adresse postale (optionnel) |
| **Refus** | Date et heure de refus du courrier |

### 4.4.5 Preuve de réception

La preuve de réception contient les informations suivantes :

| Objet ou entité | Informations indiquées |
|---|---|
| **Tiers d'acheminement** | Raison sociale<br>Siège social<br>Adresse de contact |
| **Expéditeur** | Nom et prénom ou raison sociale<br>Adresse de messagerie électronique<br>Adresse postale (optionnel) |
| **Envoi** | Type de service et garanties<br>OID de la politique d'envoi recommandé appliquée<br>Référence unique du courrier<br>Date et heure de dépôt |
| **Données du courrier** | Pour chaque fichier envoyé :<br>• Nom du fichier<br>• Taille en octets<br>• Empreinte calculée en SHA-512 |
| **Destinataire** | Type : Particulier ou Professionnel<br>Nom et prénom<br>Raison sociale et fonction pour un professionnel<br>Adresse de messagerie électronique<br>Adresse postale (optionnel) |
| **Acceptation** | Date et heure de l'acceptation du courrier |
| **Réception** | Date et heure de fin de transmission des données du courrier |

### 4.4.6 Preuve de non-réclamation

La preuve de non-réclamation contient les informations suivantes :

| Objet ou entité | Informations indiquées |
|---|---|
| **Tiers d'acheminement** | Raison sociale<br>Siège social<br>Adresse de contact |
| **Expéditeur** | Nom et prénom ou raison sociale<br>Adresse de messagerie électronique<br>Adresse postale (optionnel) |
| **Envoi** | Type de service et garanties<br>OID de la politique d'envoi recommandé appliquée<br>Référence unique du courrier<br>Date et heure de dépôt |
| **Données du courrier** | Pour chaque fichier envoyé :<br>• Nom du fichier<br>• Taille en octets<br>• Empreinte calculée en SHA-512 |
| **Destinataire** | Type : Particulier ou Professionnel<br>Nom et prénom<br>Raison sociale et fonction pour un professionnel<br>Adresse de messagerie électronique<br>Adresse postale (optionnel) |
| **Non Réclamation** | Date et heure de génération de la preuve de non réclamation |

### 4.4.7 Vérification des preuves

Les utilisateurs qui téléchargent une preuve doivent en vérifier immédiatement la validité en effectuant les contrôles suivants :

- Contrôle de présence d'un cachet et d'un jeton d'horodatage ;
- Contrôle de l'intégrité du document de preuve par validation cryptographique du cachet et du jeton d'horodatage ;
- Vérification du certificat de cachet utilisé :
    - Le certificat doit être l'un de ceux publiés par Equisign ou dans la liste de confiance eIDAS (cf. [TRUSTED_LIST]) pour identifier le service Letreco qualifié ;

    - Le certificat doit être, au moment de la création du cachet, dans sa période de validité et ni révoqué ni suspendu ;
- Vérification du certificat d'horodatage utilisé :
    - Le certificat doit être l'un de ceux publiés dans la liste de confiance eIDAS (cf. [TRUSTED_LIST]) pour le service d'horodatage identifié par l'OID indiqué au §1.5.1;
    - Le certificat doit être, au moment de l'horodatage, dans sa période de validité et ni révoqué ni suspendu ;
- Contrôle de la politique d'horodatage utilisée : L'OID de la politique d'horodatage indiquée dans le jeton doit correspondre à celui indiqué au §1.5.1 de ce document ;
- Contrôle de l'intégrité des données du courrier pour lequel la preuve est émise, en recalculant l'empreinte (avec l'algorithme spécifié ci-dessus dans le format de la preuve) de chaque fichier constituant le courrier et en la comparant aux empreintes présentes dans la preuve.

## 4.5 Cycle de vie des MIE

### 4.5.1 Cycle de vie des certificats

Le cycle de vie des certificats de signature ou d'authentification que les utilisateurs emploient pour s'authentifier auprès du service Letreco dépend de l'Autorité de Certification émettrice de ces certificats.

Les utilisateurs sont responsables de l'approvisionnement, du renouvellement et de la révocation de ces certificats, conformément à leurs responsabilités en tant que porteurs des certificats.

Les utilisateurs sont tenus d'informer le service Letreco dans les meilleurs délais de la révocation de leur certificat ou d'un changement affectant la reconnaissance du certificat par le service.

### 4.5.2 Cycle de vie des codes d'accès

Lorsqu'un expéditeur ou un destinataire choisit de s'authentifier sur le service par un code OTP ou un code issu de sa carte à code :

- Le secret OTP ou les codes de la carte à code sont générés de façon aléatoire pour lui ;
- Le secret OTP ou la carte à codes sont imprimés sur papier et transmis à l'utilisateur via un courrier recommandé postal ou remis en main propre au moment de la vérification d'identité (cf. §3.1 et §3.2).

L'utilisateur, ou Equisign lorsqu'elle le juge nécessaire, peut demander le renouvellement des codes d'accès. Ce renouvellement s'effectue selon des modalités identiques à la délivrance initiale.

L'utilisateur doit demander, en écrivant par email à l'adresse suivante : support@letreco.fr ou par courrier à l'adresse donnée au §1.4.2, la révocation de ses codes d'accès s'ils ont été

compromis ou sur simple suspicion de compromission. Le service interdit l'usage de ces codes dès la validation de cette révocation, et propose à l'utilisateur le renouvellement de ceux-ci.

Après renouvellement, les codes d'accès de la carte à code ne sont valables que pour les courriers émis après la date de renouvellement de la carte.

#### 4.5.3 Cycle de vie des identités électroniques eIDAS

Le cycle de vie des identités électroniques eIDAS que les utilisateurs emploient pour s'authentifier auprès du service Letreco dépend entièrement du fournisseur de ces identités électroniques.

Les utilisateurs sont responsables de l'approvisionnement, du renouvellement et de la révocation de leur identité électronique, conformément à leurs responsabilités en tant que porteurs de ces moyens d'identification.

Les utilisateurs sont tenus d'informer le service Letreco dans les meilleurs délais de la révocation de leur identité électronique ou d'un changement affectant la reconnaissance de cette identité par le service.

# 5 Gestion des risques

## 5.1 Analyse de risques

Avant l'ouverture du service qualifié, Equisign effectue une évaluation des risques afin d'identifier, d'analyser et d'évaluer les risques, en tenant compte des aspects techniques, juridiques et commerciaux. L'analyse de risques identifie, en particulier, les systèmes « critiques » du service.

Les mesures de sécurité nécessaires sont identifiées en tenant compte du résultat de cette analyse. Equisign fixe, dans sa PSSI, les exigences de sécurité et les procédures opérationnelles de mise en œuvre des mesures identifiées.

L'analyse de risques est examinée, et révisée si besoin, annuellement. Elle est aussi mise à jour à chaque modification ayant un impact important sur le service, notamment en cas de modification des politiques ou pratiques relatives à sa fourniture.

## 5.2 Homologation de sécurité

L'homologation de sécurité, décidée par un responsable de Equisign, atteste aux utilisateurs du service d'envoi de recommandés que les risques qui pèsent sur eux, sur les informations qu'ils manipulent et sur les services rendus, sont connus et maîtrisés par Equisign.

L'homologation de sécurité du service est prononcée après acceptation des risques résiduels identifiés par l'analyse de risques portant sur le système d'information du service. Cette homologation est réalisée préalablement à l'ouverture du service de confiance qualifié puis révisée au moins tous les deux ans.

## 5.3 PSSI

Equisign dispose d'une politique de sécurité du système d'information (PSSI) du service. Cette PSSI est approuvée par la direction de Equisign.

La PSSI, et ses versions successives, est accessible et transmise en premier lieu aux employés. Elle est également communiquée aux clients du service, aux prestataires, aux organismes d'évaluation et à l'ANSSI.

Equisign conserve la responsabilité globale de la conformité avec les procédures prévues dans sa PSSI, même lorsque certaines fonctions sont mises en œuvres par des prestataires. En particulier, Equisign s'assure de la mise en œuvre effective des mesures prévues dans la PSSI.

La PSSI exige la tenue d'un inventaire des actifs du SI. Cet inventaire est revu régulièrement et à chaque évolution de l'infrastructure. Tout changement susceptible d'avoir un impact sur le niveau de sécurité est soumis à l'approbation préalable du comité de pilotage du service.

La configuration du SI est régulièrement auditée afin de détecter tout changement pouvant être à l'origine d'une violation des politiques de sécurité.

# 6 Gestion et exploitation du service d'envoi recommandé électronique

## 6.1 Organisation interne

Equisign dispose des moyens matériels, humains et financiers suffisants pour assurer l'exploitation du service d'envoi recommandé conformément à cette politique.

Une organisation interne au sein de Equisign est en place pour piloter et exécuter les processus définis pour la fourniture et la gestion du service. Les rôles sont définis de manière à séparer les responsabilités et à minimiser le risque d'action, intentionnelle ou non, portant atteinte à la sécurité des biens.

Equisign conserve la responsabilité globale du respect de la conformité de son service à la présente politique, y compris lorsque des prestataires de Equisign prenant part à la fourniture du service. Ceux-ci sont soumis à des obligations contractuelles permettant de garantir le respect des exigences fonctionnelles attendues et le niveau de sécurité global. En particulier, la présente politique et la PSSI leur sont transmises pour application. Equisign respecte les conditions d'emploi des services fournis par ses partenaires , afin de garantir la fiabilité de leurs résultats, par exemple pour ce qui concerne l'usage des services d'horodatage qualifié et de cachet électronique. Les audits réalisés sur le service Letreco couvrent les fonctionnalités fournies par les prestataires et s'assurent du respect des exigences par chacune des parties.

Equisign a souscrit une assurance de responsabilité civile professionnelle, couvrant ce service d'envoi recommandé contre toutes les conséquences pécuniaires de sa responsabilité, résultant de dommages qui pourraient être causés aux utilisateurs.

## 6.2 Ressources humaines

Les personnels de Equisign et de ses prestataires sont les premiers acteurs de la sécurité et de la fiabilité des opérations du service. Equisign s'assure donc du respect des exigences ci-dessous aussi bien en interne que chez ses prestataires.

### 6.2.1 Compétences

Le personnel employé possède l'expertise, l'expérience et les qualifications nécessaires pour accomplir ses fonctions. Le personnel est préalablement formé aux logiciels, matériels et procédures internes de fonctionnement et de sécurité en vigueur. Ceci intègre en particulier les règles de sécurité relatives aux biens sensibles du SI et aux données à caractère personnel. Des sensibilisations régulières sont organisées, au minimum tous les ans, sur les nouvelles menaces et les bonnes pratiques de sécurité.

### 6.2.2 Définition des rôles et responsabilité

Les rôles et responsabilités liés à la sécurité sont documentés dans des descriptions de poste. Equisign respecte les principes de séparation des rôles et de moindre privilège dans la définition des fonctions et lors de leur affection. Les personnels ont pris connaissance et compris les implications des opérations dont ils ont la responsabilité.

Le personnel d'encadrement possède l'expertise appropriée à son rôle et est familier des règles de sécurité en vigueur au sein du service d'envoi recommandé.

Des sanctions disciplinaires appropriées sont prévues pour les personnels dérogeant à la politique ou aux pratiques du service.

### 6.2.3 Définition des rôles de confiance

Les rôles de confiance, sur lesquels repose la sécurité du fonctionnement du service, sont clairement identifiés. Le personnel accédant à un rôle de confiance est nommé par la direction et accepte formellement cette fonction.

Les rôles de confiance définis sont :

- **Responsable du cachet :** Le responsable du certificat de cachet s'assure de l'application des mesures de sécurité relatives à la clé privée et au certificat de cachet avancé de sécurisation des données. Il est responsable du cachet au sein de Equisign, et vis-à-vis de l'autorité de certification qui l'a émis.
- **Responsable sécurité :** Le responsable sécurité est le garant de la mise en œuvre de la politique de sécurité au niveau du service d'envoi recommandé.
- **Administrateur système :** Les administrateurs système sont les personnes chargées de la mise en route, de la configuration et de la maintenance technique des équipements informatiques (configuration, sauvegardes, restaurations…). Elles assurent l'administration technique des systèmes et des réseaux de l'infrastructure du service, ainsi que leur surveillance (supervision, détection d'incident).
- **Opérateur :** Les opérateurs sont les personnes en charge de processus métiers non automatisés du service au sein de Equisign, tels que la gestion des clients et de leurs moyens d'authentification, ou l'authentification en face à face d'utilisateurs. Ils ont accès aux preuves et aux journaux pour le support des utilisateurs.
- **Contrôleur :** Personne autorisée à accéder aux preuves (§4.4), aux journaux et archives du service pour auditer la sécurité du service.

Plusieurs rôles de confiance peuvent être attribués à une même personne, dans la mesure où le cumul ne compromet pas la sécurité des fonctions mises en œuvre. A minima, le cumul des rôles de confiance suivants sont interdits :

- Administrateur système et tout autre rôle ;
- Contrôleur et tout autre rôle.

### 6.2.4 Vérification des antécédents

Equisign met en œuvre tous les moyens légaux dont il dispose pour s'assurer de l'honnêteté du personnel qu'il emploie. Ces personnels ne doivent notamment pas avoir de condamnation de justice en contradiction avec leurs attributions, et être libre de conflit d'intérêt qui pourrait porter préjudice à l'impartialité des opérations.

Ces vérifications sont menées préalablement à l'affectation à un rôle de confiance et revues régulièrement (au minimum tous les 3 ans).

## 6.3 Gestion des biens

### 6.3.1 Généralités

Un inventaire des biens est réalisé et tenu à jour dans le cadre de l'analyse de risques du service (5.1). Les biens sont gérés en adéquation avec leur classification, telle que déterminée par celle-ci.

### 6.3.2 Supports

Les supports des biens sensibles sont gérés selon des exigences de sécurité adaptées à leur sensibilité.

Des mesures sont mises en œuvre afin de prévenir l'obsolescence, l'accès non autorisé, le vol ou l'altération des supports du service. Ces mesures sont effectives pour toute la durée de conservation prévue des biens.

En fin de vie, et selon des procédures en accord avec le niveau de confidentialité des informations qu'ils contiennent, les supports sont soit détruits, soit réinitialisés en vue d'une réutilisation.

## 6.4 Contrôle d'accès

Equisign met en œuvre un contrôle d'accès aux systèmes d'information du service d'envoi recommandé électronique.

Des procédures de gestion des habilitations sont mises en œuvre, prenant en compte les différents rôles identifiés par la présente politique. Ces procédures assurent que l'octroi et le retrait des habilitations s'effectue en accord avec la gestion des ressources humaines.

Tout utilisateur doit être identifié et authentifié avant de pouvoir accéder aux systèmes critiques du service. Les mesures de sécurité du contrôle d'accès garantissent le respect de la séparation des rôles, et en particulier l'accès aux logiciels d'exploitation (console, utilitaires, scripts, etc.) sur les serveurs est strictement contrôlé. Toute action est tracée de sorte à pouvoir être imputable à la personne l'ayant effectuée.

Les informations sensibles sont protégées y compris contre une divulgation accidentelle qui résulterait de la réutilisation de ressources (p. ex. fichiers effacés) par des personnels non autorisés.

La PSSI décrit en détail les règles de contrôle d'accès applicables au SI du service. Le contrôle d'accès au niveau réseau est décrit au §6.8.

## 6.5 Cryptographie

Les fonctions cryptographiques sensibles sont mises en œuvre dans des modules cryptographiques répondant aux exigences du document [ANSSI_PSCO]. Cela concerne au minimum :

- La signature des jetons d'horodatage ;
- La création des cachets de sécurisation des données de l'envoi recommandé.

Les modules cryptographiques, ainsi que les clés et les certificats qui y sont générés et conservés, sont protégés pendant tout leur cycle de vie et chaque étape de celui-ci est tracée.

Equisign effectue une veille de sécurité concernant les moyens et mécanismes cryptographiques employés pour garantir leur maintien à l'état de l'art et le traitement des vulnérabilités qui pourraient survenir.

## 6.6 Sécurité physique et environnementale

### 6.6.1 Situation géographique et construction des sites

Les sites d'implantation des infrastructures du service ne sont pas soumis à des risques environnementaux naturels. Les autres risques naturels et technologiques sont pris en compte et traités.

La construction des sites respecte les règlements et normes en vigueur.

### 6.6.2 Accès physique

Pour les systèmes critiques du service (cf. 5.1), l'accès est strictement limité aux seules personnes nominativement autorisées à pénétrer dans les locaux et la traçabilité des accès est assurée. En dehors des heures ouvrables, la sécurité est renforcée par la mise en œuvre de moyens de détection d'intrusion physique et logique.

Des mesures sont mises en œuvre afin de prévenir la perte ou l'altération des biens nécessaires au bon fonctionnement du service, ou la perte ou le vol d'informations.

### 6.6.3 Alimentation électrique et climatisation

Les caractéristiques des équipements d'alimentation électrique et de climatisation permettent de respecter les exigences et engagement de la présente politique en matière de disponibilité du service.

### 6.6.4 Vulnérabilité aux dégâts des eaux

Les moyens de protection contre les dégâts des eaux permettent de respecter les exigences et engagement de la présente politique en matière de disponibilité du service.

### 6.6.5 Prévention et protection incendie

Les moyens de prévention et de lutte contre les incendies permettent de respecter les exigences et engagement de la présente politique en matière de disponibilité du service.

### 6.6.6 Conservation des supports

Les différentes informations intervenant dans les activités du service sont identifiées, et leurs besoins de sécurité, définis (en confidentialité, intégrité et disponibilité). Equisign maintient un inventaire de ces informations et met en place des mesures pour en éviter la compromission et le vol.

Les supports (papier, disque dur, disquette, CD, etc.) contenant ces informations sont gérés selon des procédures conformes à ces besoins de sécurité. Ces procédures protègent les supports contre l'obsolescence et la détérioration pendant la période de temps durant laquelle Equisign s'engage à conserver les informations qu'ils contiennent.

### 6.6.7 Mise hors service des supports

En fin de vie, les supports sont détruits ou réinitialisés en vue d'une réutilisation, en fonction du niveau de confidentialité des informations qu'ils contiennent.

### 6.6.8 Sauvegardes hors site

Des sauvegardes hors site sont effectuées au moins quotidiennement pour assurer la disponibilité des informations même en cas de sinistre majeur.

## 6.7 Sécurité opérationnelle

### 6.7.1 Mesures de sécurité des systèmes informatiques

Les mesures de sécurité relatives aux systèmes informatiques doivent satisfaire aux objectifs de sécurité qui découlent de l'analyse de risque (5.1).

#### *6.7.1.1 Exigences de sécurité technique spécifiques aux systèmes informatiques*

Les systèmes informatiques doivent permettre de remplir au minimum les objectifs de sécurité suivants :

- identification et authentification forte des utilisateurs pour l'accès au système (authentification à deux facteurs, de nature physique et/ou logique) ;
- gestion des droits des utilisateurs (permettant de mettre en œuvre la politique de contrôle d'accès définie par l'AC, notamment pour implémenter les principes de moindres privilèges, de contrôles multiples et de séparation des rôles) ;
- gestion de sessions d'utilisation (déconnexion après un temps d'inactivité, accès aux fichiers contrôlé par rôle et nom d'utilisateur) ;
- protection contre les virus informatiques et toutes formes de logiciels compromettants ou non- autorisés et mises à jour des logiciels ;
- gestion des comptes des utilisateurs, notamment la modification et la suppression rapide des droits d'accès ;
- protection du réseau contre toute intrusion d'une personne non autorisée ;
- protection du réseau afin d'assurer la confidentialité et l'intégrité des données qui y transitent ;
- fonctions d'audits (non-répudiation et nature des actions effectuées) ;
- éventuellement, gestion des reprises sur erreur.

Les applications utilisant les services des composantes peuvent requérir des besoins de sécurité complémentaires.

#### *6.7.1.2 Niveau de qualification des systèmes informatiques*

Voir 6.5.

#### *6.7.1.3 Mesures de sécurité liées au développement des systèmes*

L'implémentation d'un système contribuant au service doit être documentée et doit respecter, dans la mesure du possible, des normes de modélisation et d'implémentation. La configuration des composantes du service, ainsi que toute modification et mise à niveau, doivent être documentées et contrôlées.

Equisign garantit que les objectifs de sécurité sont définis lors des phases de spécification et de conception.

Equisign utilise des systèmes et des produits fiables qui sont protégés contre toute modification.

Conformément au [GDPR], Equisign met en œuvre toutes les mesures techniques et organisationnelles nécessaires au respect de la protection des données personnelles, à la fois dès la conception des produits et des services, en veillant notamment à limiter la quantité de données traitée dès le départ (principe dit de « minimisation »).

### 6.7.2 Mesures liées à la gestion de la sécurité

Toute évolution significative d'une composante du système doit être signalée à l'entité identifiée en 1.4.1 pour validation. Elle doit être documentée et doit apparaître dans les procédures de fonctionnement interne de la composante concernée et être conforme au schéma de maintenance de l'assurance de conformité, dans le cas de produits évalués.

### 6.7.3 Évaluation des vulnérabilités

Les procédures d'exploitation du SI incluent la veille sécuritaire de ses composants. Ces procédures assurent que les correctifs de sécurité sont appliqués, au plus tard 2 mois après leur publication. Dans tous les cas, une analyse d'impact est réalisée afin de déterminer l'opportunité de les appliquer ; si un correctif n'est pas appliqué, l'analyse en justifie la décision.

Dans le cas de vulnérabilités « critiques » (CVSS≥7), l'analyse d'impact doit être effectuée dans les 48 heures suivant la publication de la vulnérabilité.

### 6.7.4 Horodatage / Système de datation

Plusieurs exigences de la présente politique nécessitent la datation par les différentes composantes des événements liés aux activités du service.

Pour dater ces évènements, les différentes composantes du service recourent à l'utilisation de l'heure système, en assurant une synchronisation quotidienne de celle-ci, au minimum à la minute près, et par rapport à une source fiable de temps UTC.

## 6.8 Sécurité réseau

Le réseau et ses systèmes doivent être protégés contre les attaques. En particulier,

a) Le SI doit être segmenté en réseaux ou zones en fonction de l'analyse des risques, compte tenu de la relation fonctionnelle, logique et physique entre les composants et les services. Les mêmes contrôles de sécurité doivent être appliqués à tous les systèmes partageant la même zone.

b) L'interconnexion vers des réseaux publics doit être protégée par des passerelles de sécurité configurées pour n'accepter que les protocoles nécessaires au fonctionnement de la composante au sein du SI du service. Equisign garantit que les composants du réseau local (routeurs, etc.) sont maintenus dans un environnement physiquement sécurisé et que leurs configurations sont périodiquement auditées en vue de vérifier leur conformité avec les exigences de la présente politique ; des dispositifs de surveillance (avec alarme automatique) de ces configurations doivent être mis en place.

c) Tous les systèmes critiques (cf. 5.1) doivent être isolés dans une ou plusieurs zones sécurisées.

d) L'exploitation des systèmes est réalisée à travers un réseau d'administration dédié et cloisonné. Les systèmes utilisés pour l'administration de la mise en œuvre de la politique de sécurité ne doivent pas être utilisés à d'autres fins. Les systèmes de production du service doivent être séparés des systèmes utilisés pour le développement et les tests.

e) La communication entre des systèmes de confiance distincts ne doit être établie qu'à travers des canaux sécurisés, logiquement distincts des autres canaux de

communication, assurant une authentification de bout en bout, l'intégrité et la confidentialité des données transmises.

f) Si un niveau élevé de disponibilité au service de confiance est nécessaire, la connexion réseau externe doit être redondante pour assurer la disponibilité des services.

g) Une analyse de vulnérabilité régulière sur les adresses IP publiques et privées du service, identifiées par Equisign, doit être effectuée, au minimum une fois par an, par une personne ou une entité ayant les compétences, les outils, la compétence, le code de déontologie et l'indépendance nécessaires. Cette analyse doit donner lieu à un rapport.

h) Un test d'intrusion sur les systèmes du service doit être réalisé, lors de la mise en place et après toute évolution de l'infrastructure ou des applications, et au minimum une fois par an, par une personne ou une entité ayant les compétences, les outils, la compétence, le code de déontologie et l'indépendance nécessaires. Ce test doit donner lieu à un rapport.

## 6.9 Gestion des incidents et supervision

Les activités du système concernant l'accès aux systèmes informatiques, l'utilisation des systèmes informatiques et les demandes de service doivent être surveillées (cf. §6.10).

Equisign doit réagir de manière coordonnée afin de répondre rapidement aux incidents et de limiter l'impact des violations de la sécurité. La responsabilité d'assurer le suivi des alertes sur les événements de sécurité potentiellement critiques et de veiller à ce que les incidents pertinents soient signalés conformément aux procédures doit être attribuée à des personnels de confiance.

Les procédures de déclaration et d'intervention d'incident doivent minimiser les dommages causés par les incidents de sécurité et les dysfonctionnements.

Par ailleurs, Equisign mesure en continu le taux de disponibilité du service et la charge constatée afin de s'assurer de l'adéquation des moyens mis en œuvre vis-à-vis des engagements contractuels avec ses clients et des obligations de cette politique.

### 6.9.1 Procédures de remontée et de traitement des incidents et des compromissions

Equisign notifie à l'ANSSI, dans un délai maximal de 24 heures après en avoir eu connaissance, toute atteinte à la sécurité ou toute perte d'intégrité ayant une incidence importante sur le service de confiance fourni ou sur les données à caractère personnel qui y sont conservées.

Lorsque le manquement à la sécurité ou à la perte d'intégrité est susceptible de nuire à une personne physique ou morale à qui le service de confiance a été fourni, Equisign informe sans délai la personne physique ou morale concernée.

## 6.10 Gestion des traces

### 6.10.1 Type d'événements à enregistrer

Concernant les systèmes liés aux fonctions qui sont mises en œuvre dans le cadre du service, chaque entité en opérant une composante doit au minimum journaliser les événements décrits ci-dessous, sous forme électronique. La journalisation doit être automatique, dès le démarrage d'un système et sans interruption jusqu'à l'arrêt de ce système.

- Création, modification, suppression de comptes utilisateur (droits d'accès) et des données d'authentification correspondantes (mots de passe, certificats, etc.)

- Démarrage et arrêt des systèmes informatiques et des applications
- Événements liés à la journalisation : démarrage et arrêt de la fonction de journalisation, modification des paramètres de journalisation, actions prises suite à une défaillance de la fonction de journalisation
- Connexion et déconnexion des utilisateurs ayant des rôles de confiance, et les tentatives non réussies correspondantes.

D'autres événements doivent aussi être recueillis, par des moyens électroniques ou manuels. Ce sont ceux concernant la sécurité et qui ne sont pas produits automatiquement par les systèmes informatiques, notamment :

- Les accès physiques
- Les actions de maintenance et de changements de la configuration des systèmes
- Les changements apportés au personnel
- Les actions de destruction et de réinitialisation des supports contenant des informations confidentielles (clés, données d'activation, renseignements personnels sur les utilisateurs...).

En plus de ces exigences de journalisation communes à toutes les composantes et toutes les fonctions du service, des événements spécifiques aux différentes fonctions du service doivent également être journalisés, notamment :

- Vérification d'identité d'un utilisateur, comprenant au minimum pour les expéditeurs et destinataires l'identité vérifiée et une référence au moyen d'identification utilisé ;
- Validation ou échec de l'identification de l'expéditeur ou du destinataire
- Événements liés au cycle de vie d'un courrier recommandé : dépôt, acceptation ou refus, téléchargement, non réclamation
- Génération et téléchargement des preuves produites par le service (4.3)
- Événements liés au cycle de vie des clés et des certificats cryptographiques (cachet et horodatage) : génération (cérémonie des clés), sauvegarde et récupération, révocation, renouvellement, destruction, etc.
- Publication et mise à jour des informations liées au service (politique, conditions générales d'utilisation, etc.) (2.4)
- Remise d'un moyen d'authentification (type carte à codes ou secret de génération des OTP) à son porteur (4.5)
- Réception d'une demande de révocation d'un moyen d'authentification (4.5)
- Validation ou rejet d'une demande de révocation d'un moyen d'authentification (4.5)

Chaque enregistrement d'un événement dans un journal doit contenir au minimum les champs suivants :

- Type de l'événement
- Nom de l'exécutant ou référence du système déclenchant l'événement
- Date et heure de l'événement
- Résultat de l'événement (échec ou réussite).

L'imputabilité d'une action revient à la personne, à l'organisme ou au système l'ayant exécutée. Le nom ou l'identifiant de l'exécutant doit figurer explicitement dans l'un des champs du journal d'événements.

De plus, en fonction du type de l'événement, chaque enregistrement devra également contenir les champs suivants :

- Destinataire de l'opération
- Nom du demandeur de l'opération ou référence du système effectuant la demande
- Nom des personnes présentes (s'il s'agit d'une opération nécessitant plusieurs personnes)
- Cause de l'événement
- Toute information caractérisant l'événement

Les opérations de journalisation doivent être effectuées au cours du processus.

En cas de saisie manuelle, l'écriture doit se faire, sauf exception, le même jour ouvré que l'événement. Les événements et données spécifiques à journaliser sont documentés par Equisign.

### 6.10.2 Fréquence de traitement des journaux d'événements

Chaque composante du service doit être en mesure de détecter toute tentative de violation de son intégrité.

Les journaux d'événements doivent être contrôlés régulièrement afin d'identifier des anomalies liées à des tentatives en échec, les anomalies et les falsifications constatées.

Par ailleurs, un rapprochement entre les différents journaux d'événements de fonctions qui interagissent entre elles doit être périodiquement effectué afin de vérifier la concordance entre événements dépendants et contribuer ainsi à révéler toute anomalie.

### 6.10.3 Période de conservation des journaux d'événements

Les journaux d'événements doivent être conservés sur site pendant au moins 1 (un) mois. Ils doivent être archivés le plus rapidement possible et au plus tard 15 (quinze) jours après leur génération.

### 6.10.4 Protection des journaux d'événements

La journalisation doit être conçue et mise en œuvre de façon à limiter les risques de contournement, de modification ou de destruction des journaux d'événements. Des mécanismes de contrôle d'intégrité doivent permettre de détecter toute modification, volontaire ou accidentelle, de ces journaux.

Les journaux d'événements doivent être protégés en disponibilité (contre la perte et la destruction partielle ou totale, volontaire ou non).

Le système de datation des événements doit respecter les exigences du 6.7.4.

La définition de la sensibilité des journaux d'événements dépend de la nature des informations traitées et du métier. Elle peut entraîner un besoin de protection en confidentialité.

### 6.10.5 Procédure de sauvegarde des journaux d'événements

Chaque composante du service doit mettre en place les mesures requises afin d'assurer l'intégrité et la disponibilité de ses journaux.

### 6.10.6 Notification de l'enregistrement d'un événement au responsable de l'événement

Aucune exigence spécifique.

## 6.11 Archivage des données

### 6.11.1 Types de données à archiver

Equisign conserve pendant une durée minimale de 7 (sept) ans après la date d'envoi et de réception des données, toutes les informations pertinentes concernant les données délivrées et reçues, notamment à fin de pouvoir fournir des preuves en justice.

Les données à conserver sont au moins :

- l'identité de l'expéditeur du recommandé électronique ;
- une preuve de validation de l'identité de l'expéditeur ;
- une référence au document faisant l'objet de la demande d'envoi recommandé électronique ;
- les jetons d'horodatage électronique qualifié correspondant à la date et heure d'envoi, d'acceptation et de réception des données le cas échéant ;
- l'identité du destinataire du recommandé électronique ;
- une preuve de validation de l'identité du destinataire (comprenant le cas échéant l'accusé de réception du pli contenant la carte à codes) ;
- les données relatives à la sécurisation de l'envoi (cachets électroniques).

### 6.11.2 Période de conservation des archives

La durée de conservation, les modalités de réversibilité et de portabilité sont précisées dans les conditions générales d'utilisation du service (1.5.4).

Les journaux d'événements sont archivés pendant 7 ans après leur génération.

### 6.11.3 Protection des archives

Les moyens mis en œuvre pour leur archivage offrent le même niveau de sécurité que celui visé lors de leur constitution. En particulier, l'intégrité des enregistrements doit être assurée tout au long de leur cycle de vie.

Pendant tout le temps de leur conservation, les archives doivent :

- être protégées en intégrité ;
- être accessibles aux personnes autorisées ;
- pouvoir être relues et exploitées.

### 6.11.4 Exigences d'horodatage des données

Voir 6.7.4.

### 6.11.5 Procédures de récupération et de vérification des archives

Seul Equisign a accès aux archives.

## 6.12 Continuité d'activité

### 6.12.1 Reprise suite à la compromission et sinistre

Chaque entité opérant une composante du service doit mettre en œuvre des procédures et des moyens de remontée et de traitement des incidents (6.9), notamment au travers de la sensibilisation et de la formation de ses personnels et au travers de l'analyse des différents journaux d'événements (6.10.2).

Dans le cas d'un incident majeur, tel que la perte, la suspicion de compromission, la compromission, le vol de données critiques (p. ex., clés privées), l'événement déclencheur est la constatation de cet incident au niveau de la composante concernée, qui doit en informer immédiatement Equisign. Le cas de l'incident majeur doit être impérativement traité dès

détection et traité dans la plus grande urgence, voire immédiatement, par tout moyen utile et disponible (presse, site Internet, récépissé…). Equisign doit également prévenir directement et sans délai l'ANSSI, conformément au § 6.9.1.

Si l'un des algorithmes, ou des paramètres associés, utilisés par le service ou ses porteurs devient insuffisant pour son utilisation prévue restante, alors Equisign doit :

- informer tous les utilisateurs et tiers impactés
- le cas échéant, révoquer les moyens d'authentification concernés ou bloquer les comptes impactés.

### 6.12.2 Procédures de reprise en cas de corruption des ressources informatiques (matériels, logiciels ou données)

Chaque composante du service doit disposer d'un plan de continuité d'activité permettant de répondre aux exigences de disponibilité des différentes fonctions découlant de la présente politique et des documents associés.

Ce plan est testé annuellement.

### 6.12.3 Procédures de reprise en cas de compromission de la clé privée d'une composante

Le cas de compromission d'une clé d'infrastructure ou de contrôle d'une composante doit être traité dans le plan de continuité de la composante en tant que sinistre.

Dans le cas de compromission de la clé du cachet du service, le certificat correspondant doit être immédiatement révoqué.

En outre, Equisign doit au minimum informer tous les clients, les autres entités avec lesquelles il a passé des accords et l'ANSSI, de cette compromission.

### 6.12.4 Capacités de continuité d'activité suite à un sinistre

Les différentes composantes du service doivent disposer des moyens nécessaires permettant d'assurer la continuité de leurs activités en conformité avec les exigences de la présente politique.

## 6.13 Fin d'activité

Equisign a établi un plan de transfert ou de cessation du service Letreco et provisionné les moyens financiers nécessaires à ces opérations.

### 6.13.1 Transfert d'activité

En cas de transfert d'activité à un tiers, celui-ci se fera avec un préavis d'au minimum un mois. Equisign prévient les clients et utilisateurs du service, les fournisseurs et partenaires (dont Docusign, Universign, FranceConnect) ainsi que l'organisation d'audit de qualification et l'ANSSI.

Le transfert d'activité ne pourra se faire sans interruption de service qu'auprès d'un tiers lui-même déjà qualifié. L'ensemble des archives et des preuves seront transmis au tiers par Equisign, ainsi que les obligations afférentes. Le certificat de cachet ne sera pas transmis au tiers, le nouvel exploitant devant disposer de son propre certificat.

En cas de transfert, la politique du service sera mise à jour et l'OID changé.

Une fois le transfert effectué, Equisign procèdera à la révocation de son certificat de cachet et à la destruction des clés privées et secrets utilisés par son service du recommandé électronique. Equisign met fin à l'ensemble des autorisations données à ses partenaires et fournisseurs pour agir en son nom pour la délivrance du service Letreco.

### 6.13.2 Fin d'activité définitive

En cas de fin d'activité du service, celui-ci se fera avec un préavis d'au minimum un mois. Durant cette période, l'envoi ne sera plus possible, seul le refus ou le retrait d'une LRE le seront.

Equisign prévient les clients et utilisateurs du service, les fournisseurs et partenaires (dont Docusign, Universign, FranceConnect) ainsi que l'organisation d'audit de qualification et l'ANSSI. Equisign s'efforce de trouver pour ses clients des solutions de transfert du service vers des opérateurs qualifiés offrant un service de même nature.

Une fois toutes les preuves relatives aux envois en cours produites (dépôt, réception, refus ou non-réclamation), l'ensemble des preuves seront conservées par Equisign ou déposées chez un tiers archiveur afin de rester disponibles à des fins légales durant la durée prévue au §6.11.2. L'ensemble des obligations d'Equisign concernant ces preuves seront maintenues par Equisign ou transférées à ce tiers archiveur.

Equisign informera ses utilisateurs de l'arrêt d'activité et procèdera à la révocation des moyens d'authentification qu'elle a émis, la révocation de son certificat de cachet et à la destruction des clés privées et secrets utilisés par le service du recommandé électronique. Equisign met fin à l'ensemble des autorisations données à ses partenaires et fournisseurs pour agir en son nom pour la délivrance du service Letreco.

## 6.14 Conformité

Les pratiques de Equisign sont non-discriminatoires.

La conception et la mise en œuvre des services, logiciels et procédures de Equisign prennent en compte, dans la mesure du possible, l'accessibilité à tous les utilisateurs, « quel que soit leur matériel ou logiciel, leur infrastructure réseau, leur langue maternelle, leur culture, leur localisation géographique, ou leurs aptitudes physiques ou mentales » (https://www.w3.org/Translations/WCAG20-fr/).

Equisign garantit la conformité avec les exigences légales et règlementaires. Equisign s'assure du respect du règlement eIDAS et des conditions de qualification en respectant les modalités de qualification exposées par l'ANSSI dans le document [ANSSI_PSCO]. Le respect des exigences légales, et en particulier la protection des données personnelles est présentée au §Autres problématiques métiers et légales.

# 7 Autres problématiques métiers et légales

## 7.1 Responsabilité financière

### 7.1.1 Couverture par les assurances

Equisign atteste avoir souscrit une assurance Responsabilité Civile Professionnelle concernant les prestations décrite dans ce document.

### 7.1.2 Couverture et garantie concernant les entités utilisatrices

La couverture et les garanties concernant les entités utilisatrices sont exposées dans les Conditions Générales d'Utilisation du service pour les expéditeurs et les destinataires du service.

## 7.2 Confidentialité des données professionnelles

### 7.2.1 Périmètre des informations confidentielles

Les informations considérées comme confidentielles sont au minimum les suivantes :

- Les données d'identité des utilisateurs et les justificatifs associés ;
- Les causes de révocations des moyens d'authentification ;
- Les secrets cryptographiques utilisés par le service (clés secrètes et privées, mots de passe, secrets utilisés pour la génération des cartes à codes ou des OTP, etc.).

### 7.2.2 Responsabilités en termes de protection des informations confidentielles

Equisign respecte la législation et la réglementation en vigueur sur le territoire français et est responsable de la protection des informations confidentielles.

Equisign peut cependant devoir mettre à disposition les données dont il dispose à des tiers dans le cadre de procédures légales. Les clients peuvent également accéder à leurs données professionnelles auprès de Equisign.

## 7.3 Protection des données personnelles

### 7.3.1 Politique de protection des données personnelles

Les utilisateurs du service Letreco sont informés que, dans le cadre du service, Equisign est amenée à collecter, héberger, et traiter des données à caractère personnel les concernant, aux seules fins d'assurer l'acheminement du courrier auprès du ou des destinataires.

Equisign s'engage à conserver confidentielles les données personnelles des utilisateurs et à ne pas les divulguer à des tiers, pendant toute la durée de leur conservation. Pour ce faire, Equisign fera ses meilleurs efforts pour :

- Prendre toutes les précautions utiles et mettre en place des contrôles efficaces de protection afin de préserver la sécurité des Données Personnelles, et notamment empêcher qu'elles ne soient déformées, endommagées, ou que des tiers non autorisés y aient accès ;
- Disposer des moyens organisationnels, techniques et financiers permettant de garantir la mise en oeuvre des mesures de confidentialité et de sécurité ;
- Prendre toute mesure de sécurité pour assurer la conservation et l'intégrité des données

### 7.3.2 Informations à caractère personnel

Les informations considérées comme personnelles sont au minimum les suivantes :

- Les données d'identité des utilisateurs et les justificatifs associés ;
- Les courriers électroniques (expéditeurs et destinataires, données du courrier) ;
- Les informations techniques collectées (adresses IP, navigateurs…) lors de la connexion des utilisateurs du service.

### 7.3.3 Responsabilité en termes de protection des données personnelles

Equisign s'engage à respecter la réglementation légale applicable au traitement de données personnelles et notamment le respect du règlement général de protection des données [GDPR]. Equisign agit en qualité de responsable de traitement des données personnelles collectées pour le fonctionnement du service.

#### 7.3.4 Notification et consentement d'utilisation des données personnelles

Les utilisateurs sont information des conditions d'utilisation de leurs données personnelles dans les Conditions Générales d'Utilisation du service, qu'ils doivent lire et accepter avant de bénéficier du service Letreco.

#### 7.3.5 Conditions de divulgation d'informations personnelles aux autorités judiciaires ou administratives

Equisign se conforme strictement aux dispositions légales pour traiter les demandes de divulgation d'informations personnelles aux autorités judiciaires ou administratives.

#### 7.3.6 Autres circonstances de divulgation d'informations personnelles

Equisign n'a pas prévu d'autres circonstances de divulgation d'informations personnelles.

### 7.4 Juridictions compétentes

La présente politique est soumise au droit français.

### 7.5 Dispositions concernant la résolution de conflits

En cas de litige sur l'interprétation ou l'exécution de la présente politique, pour le cas où les parties ne parviendraient pas à trouver un accord amiable dans un délai de 30 jours sauf à ce que ce délai soit reconduit expressément entre les parties, il est attribué compétence expresse et exclusive au tribunal de commerce de Paris, lequel sera la seule juridiction compétente pour connaitre de tout différend, nonobstant pluralité de défendeurs ou appel en garantie, même pour les procédures d'urgence ou les procédures conservatoires par voie de référé ou requête ou les oppositions sur injonction de payer.

### 7.6 Force majeure

Sont considérés comme cas de force majeure tous ceux habituellement retenus par les tribunaux français, notamment le cas d'un événement irrésistible, insurmontable et imprévisible.