



# LRE TRUST



# CGU et Politique de Gestion de LRE Trust

Le site Internet disponible à l'adresse [lre.ma](http://lre.ma) (le « Site ») est la propriété de la société LRE TRUST dont les coordonnées se trouvent à l'Article 1 ci-dessous (« LRE TRUST »).

L'utilisation du Site par les visiteurs non-Membres suppose l'acceptation pleine et entière des dispositions des CGU non-relatives à l'inscription en vigueur au moment de l'accès au Site.

L'utilisation du Site et des Services par les Membres est subordonnée à la validation des conditions générales d'utilisation des Services en vigueur au moment de leur inscription au Site (les « CGU »).

Les CGU sont constitutives d'un contrat entre LRE TRUST et les Membres (individuellement une « Partie », ensemble, les « Parties »), qui s'engagent à les respecter.

LRE TRUST peut proposer des conditions particulières complémentaires pour certains Services, qui devront être dûment validées par les Parties (les « Conditions Particulières »).

## 1. Informations légales

### 1.1. Éditeur du Site

- Raison Sociale : LRE TRUST
- Numéro d'inscription : RC de Rabat sous le n°152 855
- Capital social : 125.000,00 Dhs
- Adresse du siège social : 21C32, Hay Riad, Rabat Maroc
- Email : [contact@lre.ma](mailto:contact@lre.ma)
- Téléphone : 06 61355038

## 2. Définitions

- Loi : Dahir n° 1-20-100 du 16 jourmada I 1442 (31 décembre 2020) portant promulgation de la loi n° 43.20 relative aux services de confiance concernant les transactions électroniques.
- Membre : Tout Utilisateur qui a procédé à la création d'un Compte sur le Site. Chaque Membre peut être une personne physique dans le cadre d'une inscription à titre personnel, ou morale, dans le cadre d'une utilisation pour le compte d'une société. Dans ce dernier cas, l'Utilisateur qui procède à l'inscription pour le compte d'une personne morale garantit qu'il dispose des pouvoirs suffisants pour représenter et engager cette personne morale. Les Membres peuvent utiliser les Services à des fins personnelles (« Membre Consommateur») et/ou aux fins de leurs activités professionnelles (« Membre Professionnel ») □ Utilisateur : Toute personne accédant au Site.
- Services : Ensemble des fonctionnalités utilisables et proposées par LRE TRUST sur le Site et notamment, la transmission, l'acheminement et l'archivage de lettres recommandées électroniques avec accusé de réception dans les conditions visées au Règlement de la loi Marocaine 4320, (« LRE») entre un Membre expéditeur (« l'Expéditeur ») et un Membre ou un non-Membre destinataire (le « Destinataire »). Les LRE peuvent, le cas échéant, contenir (i) un courrier électronique en format texte et/ou (ii) des pièces jointes dans la limite autorisée par les Services en cas d'utilisation du Site pour l'envoi de LRE (la « Plateforme LRE TRUST »). Le cas échéant, la Plateforme LRE TRUST peut être interfacée au sein de la solution d'un partenaire de LRE TRUST (un « Partenaire »).



### 3. Documents contractuels

Les documents contractuels sont constitués par ordre de priorité décroissant :

- Le cas échéant, des Conditions Particulières, de leurs annexes et avenants ;
- Des CGU ;
- D'un ou plusieurs éventuel(s) bon(s) de commande ;

En cas de contradiction ou de difficulté d'interprétation entre documents de même rang, les dispositions contenues dans le document le plus récent prévaudront.

### 4. Inscription et accès au site et services

Les CGU sont réputées conclues entre le Membre et LRE TRUST à compter de l'inscription du Membre et jusqu'à leur résiliation par l'une ou l'autre des Parties dans les conditions visées dans les CGU.

#### 4.1. Condition d'accès au Site et aux Services

L'inscription au Site n'est pas obligatoire. Cependant, l'inscription au Site en tant que Membre entraîne la création d'un compte utilisateur (le « Compte ») qui est nécessaire pour accéder à l'ensemble des Services. Une fois le Compte créé, le Membre peut accéder à l'ensemble des Services sur le Site

#### 4.2. Prérequis techniques

Tout Utilisateur doit disposer d'une installation technique adéquate dont les caractéristiques minimales requises sont les suivantes :

- un terminal fixe ou mobile connecté à Internet, et, pour l'utilisation de la Plateforme LRE TRUST, à même de garantir une utilisation satisfaisante d'un navigateur internet respectueux des standards techniques en vigueur, autorisant l'exécution de modules JavaScript ;
- une adresse de courrier électronique, avec accès permanent aux messages qui y sont adressés.

Les équipements (ordinateur, logiciels, moyens de télécommunications, etc.) permettant l'accès au Site et aux Services demeurent à la charge des Membres, de même que les frais de communications induits par leur utilisation.

#### 4.3. Inscription au Site

La création d'un Compte est gratuite et réservée, pour les personnes physiques, à toute personne âgée d'au minimum 18 ans, et soumise à l'acceptation des CGU du Site. Un seul Compte peut être créé par adresse électronique.

Dans l'hypothèse où le Membre serait mineur, l'autorisation des personnes en charge de l'autorité parentale doit être obtenue préalablement à toute inscription. Le/les titulaire(s) de l'autorité parentale sur le Membre mineur est/sont responsable(s) du respect de l'ensemble des dispositions des CGU par ce dernier.

L'inscription s'effectue par le renseignement d'un formulaire dont les champs obligatoires pour bénéficier des Services sont indiqués par un astérisque.



# LRE TRUST



Le Membre s'engage à ne communiquer que des informations et données personnelles exactes et conformes à la réalité. Il s'engage notamment, à ne pas usurper l'identité d'autrui et à informer LRE TRUST sans délai en cas de modification des informations et données personnelles qu'il a communiquées lors de son inscription et, le cas échéant, à procéder lui-même auxdites modifications au sein de l'espace de gestion du Compte mis à sa disposition sur le Site. Une fois l'inscription réalisée, un courrier de validation sera adressé à l'adresse électronique communiquée par le Membre pour finaliser la création du Compte.

Le Membre donne une autorisation officielle et sans équivoque à LRE Trust, d'envoyer une lettre recommandée électronique en son nom, que le Membre soit une entité physique ou morale.

## 4.4. Identifiant et mot de passe

Le Membre doit, lors de la création de son Compte, choisir un nom d'utilisateur (composé du nom complet ou de la raison sociale de l'Utilisateur) et un mot de passe qui lui sont propres (ensemble, les « Identifiants »). Les Identifiants doivent être suffisamment sécurisés. Les identifiants sont transmis à LRE TRUST de manière chiffrée. Chaque Membre ne peut créer et détenir qu'un seul Compte. Le cas échéant, pour les Membres personnes morales, un Compte principal pourra permettre la gestion de sous-Comptes, sous la responsabilité exclusive du gestionnaire du Compte principal.

Il est de la responsabilité du Membre de conserver ces Identifiants confidentiels. Le Membre est seul responsable de l'utilisation de son Compte et de ses Identifiants. Toute utilisation des Services, connexion ou transmission de données effectuée via son Compte avec ses Identifiants sera présumée avoir été effectuée par ce Membre et sous sa responsabilité exclusive, sauf dénonciation écrite et dûment motivée transmise à LRE TRUST par lettre recommandée avec accusé de réception, le cas échéant électronique, aux adresses de contact figurant à l'Article 1.

LRE TRUST ne saurait être tenu pour responsable de la perte d'un ou plusieurs Identifiants et, à défaut d'opposition préalable et régulièrement notifiée par écrit à LRE TRUST, des conséquences dommageables de l'utilisation de son Compte par une personne non autorisée.

Nonobstant les vérifications d'identité qui s'imposent pour les envois et réception de LRE électronique, LRE TRUST, qui ne possède aucun pouvoir de contrôle quant à la véracité des informations déclaratives transmises par les Membres pour la création de Compte, ne saurait être tenu responsable de fausses déclarations effectuées par les Membres.

En cas d'oubli de son mot de passe, un Membre peut en demander la réinitialisation, dont la procédure lui sera détaillée par courrier électronique adressé à son adresse de contact.

En cas de perte totale de ses Identifiants (oubli du mot de passe et impossibilité d'accéder à son compte de messagerie électronique), le Membre peut adresser une demande de récupération et/ou de réinitialisation de ses Identifiants en se soumettant à la même procédure de vérification d'identité que lorsqu'il s'est inscrit à LRE TRUST à l'adresse [contact@lre.ma](mailto:contact@lre.ma). Cette procédure lui sera facturée 400 Dhs TTC.

## 5. Procédure d'envoi et de réception de LRE

### 5.1. LRE entièrement électronique

Lors de l'envoi d'une LRE au travers de la Plateforme LRE TRUST (le « Dépôt »), LRE TRUST effectue une sauvegarde du contenu de la LRE sur son infrastructure technique, notamment aux fins d'horodatage de l'empreinte de la LRE (« l'Horodatage ») et d'archivage pour le compte de l'Expéditeur et du Destinataire (« l'Archivage »). Le Destinataire est ensuite notifié par LRE TRUST qu'une LRE lui est adressée, sans pour autant avoir connaissance du contenu de la LRE ou de l'identité de l'Expéditeur (la « Première Présentation »). Cette notification prend la forme d'un courrier électronique envoyé à l'adresse électronique du Destinataire, telle qu'indiquée par l'Expéditeur.

Le Destinataire dispose alors d'un délai de 15 (quinze) jours à compter du lendemain de l'envoi par LRE TRUST au Destinataire de la Première Présentation pour :



# LRE TRUST



- accepter et accéder à la LRE (« l'Acceptation»), □
- refuser explicitement la LRE (le « Refus»), ou □
- ignorer la LRE (la « Non Réclamation»).

En cas de Refus ou de Non Réclamation, le Destinataire ne pourra alors plus prendre connaissance du contenu de la LRE et de l'identité de l'Expéditeur et s'expose à toutes les conséquences légales que cela pourrait entraîner pour lui.

En cas de Refus ou de Non Réclamation, LRE TRUST met à la disposition de l'Expéditeur (par courrier électronique et sur son espace sur le Site) une preuve de Non Réclamation ou de Refus, au plus tard le lendemain du délai de 15 (quinze) jours visé au paragraphe précédent. L'Expéditeur est informé que les preuves de Refus ou de Non Réclamation mentionnées au paragraphe précédent produisent les mêmes effets juridiques que ceux attachés à la preuve d'un Refus ou d'une Non Réclamation d'une lettre recommandée.

Chaque « Étape » (Dépôt, Horodatage, Première Présentation, Acceptation, Refus et/ou Non-Réclamation) est consignée et archivée par LRE TRUST, qui en tient l'Expéditeur informé dans les conditions énoncées dans les présentes, conformément au Décret : LRE TRUST notifie l'Expéditeur par courrier électronique envoyé à l'adresse électronique de l'Expéditeur (cf. 4.3).

Le cas échéant, LRE TRUST adressera au Destinataire une ou plusieurs relance(s) de la Première Présentation avant la caractérisation de la Non-Réclamation.

### 5.3. Archivage

L'Archivage est réalisé pour une période de : 10 (dix) ans pour les fichiers de preuve, et de 10 (dix) ans pour les traces à compter du Dépôt de la LRE considérée (la « Durée de Conservation »). À l'issue de la Durée de Conservation, LRE TRUST procédera à la suppression de la LRE considérée et de toute information afférente. Il incombe aux Membres qui le souhaitent de procéder au téléchargement de ces données avant l'expiration de la Durée de Conservation.

Pour chaque LRE, LRE TRUST enregistre et conserve les éléments d'information relatifs à :

1. l'identité de l'expéditeur de la LRE ;
2. une preuve de validation de l'identité de l'Expéditeur ;
3. une référence au document faisant l'objet de la demande de LRE ;
4. les jetons d'horodatage électronique qualifié correspondant à la date et heure d'envoi de la LRE ;
5. l'identité du Destinataire de la LRE ;
6. une preuve de validation de l'identité du Destinataire ;
7. les données relatives à la sécurisation de l'envoi de la LRE (cachets électroniques et empreinte de la LRE).

### 5.3. Réversibilité et portabilité

En tout état de cause, chaque Membre pourra à tout moment pendant la Durée de Conservation accéder et vérifier les éléments de preuve afférents à une LRE tels que décrits à l'Article 18.1 ci-dessous qui les concerne en se rendant sur la page du Site prévue à cet effet.

Ces éléments de preuves sont au format PDF (ISO 32000-1) et sont lisibles par de nombreux logiciels gratuits. Ces preuves recouvrent les informations mentionnées aux points (1), (2), (3), (4) et (5) de l'article 5.3 ci-dessus.

Les éléments de preuves techniques décrits à l'Article 18.2 ci-dessous couvrent les informations mentionnées aux points (2) et (6) de l'article 5.3 ci-dessus et ne sont pas réversibles.



## 6. Obligations de LRE TRUST

LRE TRUST s'engage à ne pas accéder au contenu des LRE échangées au travers des Services, sauf à la demande expresse du Membre concerné ou sur réquisition des autorités. Notamment, LRE TRUST ne saurait vérifier la présence, dans les fichiers joints aux LRE, de virus, vers ou autres programmes malveillants.

LRE TRUST s'engage à mettre en œuvre les moyens techniques appropriés pour répondre aux exigences applicables à la LRE en vertu du Décret, notamment pour assurer la vérification de l'identité de l'Expéditeur, la preuve du dépôt électronique de l'envoi, et garantir l'envoi et la réception des données par le cachet d'un prestataire de services de confiance qualifié. Pour plus d'information, merci de vous référer à la « Politique et Pratiques du Service » disponible sur le Site.

LRE TRUST conserve une preuve de la réception par le Destinataire, ou par son mandataire, des données transmises et du moment de la réception.

LRE TRUST ne modifie pas les informations relatives aux Étapes et s'engage à mettre en œuvre les moyens techniques nécessaires à la conservation de ces informations et à en permettre la restitution, aussi bien en langage clair (affichage des attestations des courriers) que sous forme de données informatiques (restitution des données). À cette fin, les Membres peuvent accéder aux Étapes, et aux éléments de preuve et de vérification des preuves à tout moment pendant la Durée de Conservation.

LRE TRUST met à la disposition des Utilisateurs, via le lien <http://status.lre.ma/>, des informations concernant les éventuels incidents et sur la disponibilité des Services, ainsi que sur les périodes de maintenances planifiées par LRE TRUST sur le Site ou les Services (ensemble, « Évènements »). Les Utilisateurs ont alors la possibilité de définir des alertes en vue d'être informés des Évènements définis par LRE TRUST ou dont LRE TRUST a connaissance (« Alertes »).

LRE TRUST met à la disposition des Utilisateurs un support technique par courrier électronique à l'adresse [contact@lre.ma](mailto:contact@lre.ma), ou par tout autre moyen mis à disposition et renseigné sur la page « Contact » du Site.

Les horaires et jours de disponibilités du support vocal ou par messagerie instantanée sont indiqués sur le Site.

## 7. Obligations des utilisateurs

Les Membres sont informés que le choix du format de la LRE, et notamment entièrement électronique ou en format LRE Hybride, ainsi que la présence ou non d'un accusé de réception, incombe aux Expéditeurs au moment de la procédure d'envoi, sous leur entière responsabilité, notamment au regard du consentement, ou son absence, du Destinataire à recevoir des LRE entièrement électroniques.

En tant qu'Expéditeurs, les Membres garantissent :

□ qu'ils ont, lors du dépôt d'une LRE, transmis à LRE TRUST, conformément au Décret, les informations suivantes :

- (i) leurs nom et prénom s'il s'agit de personnes physiques, leur raison sociale s'il s'agit de personnes morales, ainsi que leur adresse électronique et, le cas échéant, leur adresse postale ;
  - (ii) Les nom et le prénom ou la raison sociale du Destinataire ainsi que son adresse électronique, ou bien son adresse postale en cas de remise de l'envoi recommandé imprimé sur papier ;
- qu'ils ont préalablement obtenu l'accord du Destinataire, lorsque celui-ci est un non professionnel, pour lui adresser une LRE et qu'ils sont en mesure de prouver, par tous moyens, qu'ils ont obtenu le consentement du Destinataire ;

- Le cas échéant, l'Expéditeur peut mandater LRE TRUST pour recueillir ce consentement au travers de l'interface prévue à cet effet, préalablement à l'envoi de la LRE considérée.



# LRE TRUST



- l'identité du Destinataire, la validité de l'adresse électronique de contact à laquelle la LRE sera adressée et la qualité de consommateur ou de professionnel du Destinataire ;
- ne pas porter atteinte à leurs obligations contractuelles ou légales et à ne pas introduire lors de leurs Dépôts tout virus, vers, bombe logique ou tout contenu pouvant être assimilés à du courrier non désiré.

Tout Utilisateur accepte d'accorder aux LRE échangées au travers des Services la même valeur juridique que celle qu'il reconnaît au courrier postal recommandé avec accusé de réception.

L'Utilisateur est seul responsable des conséquences, notamment légales, qui découleraient de ses actions ou de sa négligence dans l'envoi et la réception des LRE.

Il revient à l'Utilisateur, s'il souhaite être informé des Évènements, de souscrire aux Alertes.

Dans le cadre des lettres recommandées électroniques qualifiées, des obligations spécifiques et supplémentaires s'appliquent à l'Utilisateur (voir § 22).

## 8. Conditions financières

Sauf Conditions Particulières, tout envoi de LRE est facturé à l'Expéditeur pour les montants indiqués sur le Site lors de cet envoi et rattaché au sein de la Plateforme LRE TRUST.

La non-remise d'une LRE en raison d'une adresse de Destinataire erronée, de la Non Réclamation du Destinataire ou toute autre raison indépendante de LRE TRUST ne saurait invalider sa facturation par LRE TRUST.

La facturation de l'utilisation des Services s'effectue au début du mois pour toute LRE envoyée durant le mois précédent.

LRE TRUST peut autoriser les Utilisateurs à tester les Services de manière gratuite (les « Services Tests »). Cependant, les LRE envoyées dans le cadre des Services Tests ne peuvent être effectuées qu'aux finalités de test et ne sauraient bénéficier d'aucune garantie, notamment au regard du Décret.

Certaines fonctionnalités des Services ne sont accessibles qu'aux seuls Membres qui ont mis en place un procédé de facturation et/ou de paiement mensuel automatisé ou tout autre procédé valablement accepté par LRE TRUST, notamment lors du dépôt d'une caution auprès de LRE TRUST.

Les paiements s'effectuent en euro et par carte bancaire, virement bancaire et/ou, le cas échéant, prélèvement SEPA, au travers du réseau internet. Les règlements ne sont considérés comme effectifs que lorsque les centres de paiements bancaires concernés auront donné leur accord. En cas de refus desdits centres, les paiements seront automatiquement annulés et le Membre en sera informé sans délai.

Toute facture est établie sur la base des Logs, en dirhams hors taxe applicable au moment de la facturation et est payable dans les 30 (trente) jours suivant sa réception.

Toute somme non réglée à l'échéance rend exigible une indemnité forfaitaire fixée par décret et d'un montant, à la date de mise en ligne des CGU, de quarante euros hors taxes (400 Dhs HT) pour frais de recouvrement, nonobstant les frais de recouvrement réellement exposés par LRE TRUST sur présentation des justificatifs correspondants. En tout état de cause, LRE TRUST se réserve la possibilité de suspendre tout nouvel envoi de LRE à un Utilisateur en manquement des obligations de paiements qui lui incombent.

Aucun remboursement ne saurait être effectué sur les LRE qui ont fait l'objet d'au moins un Dépôt.



## 9. Données personnelles des membres

### 9.1. Généralités

Dans le cadre de l'utilisation des Services par les Membres, LRE TRUST est amené à prendre connaissance et à collecter des données personnelles relatives à ces mêmes Membres (les « Données Personnelles »). La collecte de Données Personnelles intervient lors de l'inscription des Membres aux Services, et lors de toute utilisation des Services par les Membres.

Dans ce cadre, LRE TRUST, tel qu'identifié à l'Article 1 des CGU, doit être considéré comme le responsable de traitement au sens du Règlement marocain et de la loi 4320

Le traitement des données personnelles des Membres par LRE TRUST respecte la réglementation nationale et européenne applicable, et notamment le RGPD.

Néanmoins, dans le cadre des services fournis par LRE TRUST à ses Expéditeurs professionnels, et notamment ses Partenaires, LRE TRUST agit en tant que sous-traitant pour ces mêmes services. Des garanties différentes peuvent le cas échéant s'appliquer aux données à caractère personnelles traitées par ces Expéditeurs. Le cas échéant, LRE TRUST invite les utilisateurs à se rapprocher directement de ces Expéditeurs.

### 9.2. Cookies

LRE TRUST est amené à collecter et à stocker les données d'identification relatives aux Membres afin de leur éviter d'avoir à saisir manuellement leurs Identifiants à chaque connexion, ainsi que les données de navigation des Membres aux fins de fournir et améliorer les Services et à des fins statistiques. Ces informations sont stockées par LRE TRUST notamment au moyen de cookies. Lors de l'utilisation du Site, les cookies suivants peuvent être placés sur le terminal ou autre dispositif de l'Utilisateur :

- **Cookie de navigation** : dès le premier accès, ces cookies permettent au Site de fonctionner correctement et aident l'Utilisateur à visualiser les contenus sur son terminal, en reconnaissant sa langue et le pays depuis lequel il se connecte. Les cookies de navigation sont des cookies techniques, nécessaires au fonctionnement du Site.
- **Cookies analytiques** : Ces cookies sont utilisés afin d'élaborer des analyses statistiques sur les modalités de navigation des Utilisateurs. Les résultats de ces analyses sont traités de manière anonyme et à des fins exclusivement statistiques, uniquement si le fournisseur de services utilise des cookies connexes au navigateur utilisé ou sur d'autres appareils employés pour naviguer sur le Site. Ces données statistiques sont susceptibles d'être partagées avec d'autres Membres.
- **Cookies tiers** : les cookies tiers sont des cookies que les partenaires commerciaux de LRE TRUST placent sur le terminal ou autre dispositif de l'Utilisateur. Les partenaires commerciaux utilisent les cookies tiers à des fins de ciblage, par exemple, pour que les annonces publicitaires qu'ils estiment correspondre le mieux aux intérêts des Utilisateurs soient choisies et transmises à leur terminal ou autre dispositif, sur la base des activités antérieures de ce même terminal ou autre dispositif sur Internet.

La plupart des navigateurs sont configurés pour accepter, contrôler ou éventuellement désactiver les cookies grâce aux paramètres de configuration. En désactivant les cookies de navigation, le bon fonctionnement du Site peut être compromis et/ou les Services proposés peuvent être limités.

Pour la gestion des cookies et des choix de l'Utilisateur, la configuration de chaque navigateur est différente. Elle est décrite dans le menu d'aide du navigateur, qui permettra de savoir de quelle manière modifier la configuration en matière de cookies.

La procédure de gestion des cookies et de préférences en matière de cookies est légèrement différente selon chaque navigateur. L'Utilisateur peut visualiser les étapes de gestion des cookies dans le menu d'aide de son navigateur.

- [pour Internet Explorer™](#)
- [pour Safari™](#)



# LRE TRUST



- [pour Chrome™](#)
- [pour Firefox™](#)
- [pour Opera™](#)

### 9.3. Exploitation des données

Toutes les données relatives à l'utilisation des Services collectées sont exploitées par LRE TRUST et ses prestataires de services situés dans l'Union Européenne dans le but de mettre en œuvre son objet social ainsi que les Services. LRE TRUST pourra notamment effectuer des analyses du volume et des typologies de pièces jointes échangées sur ses services dans un but d'amélioration des Services et de statistiques. L'ensemble des données collectées lors de l'inscription des Membres sur le Site, ou lors de l'utilisation des Services, demeurent la propriété exclusive de LRE TRUST et LRE TRUST s'engage à ne pas transmettre, divulguer, vendre, louer ou commercialiser de quelque façon que ce soit ces données à des tiers autre que ses prestataires de services, sans l'accord des personnes concernées, sauf en cas d'obligation légale, ou d'injonction émanant d'une autorité judiciaire ou administrative.

Les Membres, sous réserve de justifier de leur identité auprès de LRE TRUST, disposent d'un droit d'accès, de rectification et d'opposition ainsi qu'un droit à l'effacement, sur leurs Données Personnelles, dans les conditions du RGPD, en s'adressant à LRE TRUST par courrier ou par courriel aux adresses figurant à l'Article 1.

En cas d'exercice du droit d'opposition par un Membre, LRE TRUST cessera le traitement de ses Données Personnelles, sauf en cas de motif(s) légitime(s) et impérieux pour le traitement, ou pour assurer la constatation, l'exercice ou la défense de ses droits en justice, conformément au RGPD.

Sous réserve de justifier de leur identité auprès de LRE TRUST, les Membres disposent également du droit de récupérer leurs Données Personnelles dans un format structuré, couramment utilisé et lisible par machine, et ont le droit de transmettre ces données à un autre responsable de traitement, au sens du RGPD. Lorsque cela est techniquement possible, les Membres ont le droit de demander à LRE TRUST d'obtenir que les Données Personnelles soient transmises directement à un autre responsable de traitement, au sens du RGPD.

LRE TRUST s'engage, conformément aux dispositions du RGPD, à ne conserver les Données Personnelles collectées que pour une durée strictement nécessaire à la mise en œuvre des Services ainsi que, le cas échéant, pour la durée nécessaire au respect de ses obligations d'archivage légales et réglementaires. Conformément à l'Article 5.3 des CGU, les Données Personnelles seront conservées par LRE TRUST pour une durée de 10 (dix) ans. Les Données Personnelles traitées pour les finalités de gestion de la relation client seront conservées pour une durée de 10 (dix) ans à compter de la fin de la relation commerciale.

LRE TRUST peut envoyer, régulièrement ou ponctuellement, des emails d'information aux Membres, notamment, lors de l'inscription, LRE TRUST proposera de recevoir une newsletter. Le Membre pourra refuser, et, dans l'hypothèse où il accepterait, il pourra à tout moment s'y opposer en cliquant sur le lien hypertexte de désabonnement qui se trouve en bas de chaque courrier électronique ainsi reçu.

En cas de différend entre les Parties concernant le traitement des Données Personnelles du Membre par LRE TRUST dans le cadre du Contrat, le Membre pourra adresser sa réclamation à LRE TRUST en le contactant aux coordonnées figurant à l'Article 1 des CGU. LRE TRUST s'efforcera de trouver une solution satisfaisante pour le Membre, pour assurer le respect de la réglementation applicable et/ou de l'Article 9 des CGU. En l'absence de réponse de LRE TRUST ou si le différent persiste malgré la proposition de LRE TRUST, le Membre a la possibilité d'introduire une réclamation auprès de la Commission Nationale de l'Informatique et des Libertés.

## 10. Propriété intellectuelle

Les Services, le Site et son contenu, comprenant sans limitation tous ses éléments graphiques, visuels, sonores, photographiques et textuels, l'architecture du Site, les bases de données le constituant (les « Contenus LRE TRUST ») sont la propriété exclusive de LRE TRUST ou de leurs titulaires respectifs. Il est interdit de modifier, copier et reproduire tout ou partie des Contenus LRE TRUST sans son autorisation écrite et préalable.



# LRE TRUST



La marque et le logo LRE TRUST, ainsi que les dénominations sociales, et signes distinctifs y afférents sont la propriété exclusive de LRE TRUST. La reproduction ou la représentation de tout ou partie de ces signes est strictement interdite et doit faire l'objet d'une autorisation écrite et préalable de LRE TRUST.

Le non-respect de cet Article 10 est passible de poursuites judiciaires et engage la responsabilité civile et pénale de son auteur.

## 11. Absence de droit de rétractation

Les Membres Consommateurs reconnaissent que les Services sont pleinement exécutés de manière concomitante à l'expédition de la LRE, dont l'exécution immédiate est demandée par l'Expéditeur au moment de l'envoi. En conséquence, le Membre Consommateur renonce expressément à tout droit de rétractation à cet égard.

## 12. Garanties

L'Utilisateur déclare et reconnaît que :

- les transmissions de données sur Internet ne bénéficient pas d'une fiabilité technique absolue, celles-ci circulant sur des réseaux hétérogènes aux caractéristiques et capacités techniques diverses, qui sont parfois saturés à certaines heures de la journée ;
- la fonctionnalité de signature manuscrite virtuelle des accusés de réception n'est fournie qu'à titre indicatif et sous réserve de faisabilité sur le terminal de réception du Destinataire, sans préjudice de la validité et du caractère probant de la procédure électronique d'acheminement de la LRE ; et
- si LRE TRUST prend toutes les mesures possibles pour préserver ses Services de l'intrusion volontaire de virus, LRE TRUST ne saurait contrôler le contenu des LRE et ne saurait donc garantir que ces dernières sont exemptes de tels virus.

## 13. Responsabilité

LRE TRUST s'engage à mettre en œuvre tous les efforts techniques nécessaires aux fins de se conformer aux dispositions réglementaires applicables à la lettre recommandée électronique, et notamment l'Article L. 100 du CPCE, les Articles 43 et 44 du Règlement eIDAS et le Décret d'application de l'art. 93 de la loi n° 2016-1321 du 7 octobre 2016 pour une République numérique.

En particulier, LRE TRUST garantit qu'il bénéficie de la qualification visée dans ces textes. Les Services sont fournis par LRE TRUST conformément à la politique identifiée par l'OID : 1.3.6.1.4.1.50034.1.1.2 disponible sur le Site.

Il appartient à chaque Utilisateur de s'assurer que son utilisation des Services se conforme aux caractéristiques spécifiques de sa situation.

De même, il est de la responsabilité de chaque Utilisateur de s'assurer de l'identité du Destinataire, de la validité de l'adresse électronique du Destinataire, de la capacité du Destinataire à accéder effectivement à la LRE au travers de son infrastructure de courrier électronique, et, le cas échéant, du consentement du Destinataire à recevoir les LRE entièrement électroniques.

LRE TRUST ne saurait voir sa responsabilité engagée du fait de l'indisponibilité de l'infrastructure technique de l'Expéditeur et/ou du Destinataire à l'une quelconque des Étapes et notamment des performances du serveur de messagerie employé par l'Expéditeur et/ou le Destinataire.



# LRE TRUST



Chaque Membre garantit LRE TRUST contre toute condamnation qui pourrait être prononcée à l'encontre de LRE TRUST en raison d'un manquement de la part du Membre à ses obligations au titre des CGU.

LRE TRUST ne pourra voir sa responsabilité engagée que du fait d'une faute de sa part définitivement établie par les juridictions compétentes et passée en force de chose jugée.

LRE TRUST s'efforce d'assurer l'exactitude et la mise à jour des informations diffusées sur le Site et à l'adresse <http://status.lre.ma> / par lui, dont il se réserve le droit de corriger le contenu, à tout moment et sans préavis. LRE TRUST ne peut cependant en garantir l'exactitude, l'exhaustivité, la véracité ou l'absence de modification par un tiers. En outre, LRE TRUST décline toute responsabilité en cas d'erreur ou d'omission quant au contenu des pages du Site ou à l'adresse <http://status.lre.ma> / et à l'utilisation qui pourrait en être faite par les Membres ou des tiers, et des erreurs d'adressage de LRE en raison d'une faute ou d'un manquement du Membre.

LRE TRUST ne saurait être tenu pour responsable de la non-communication des Évènements dès lors que le Membre n'a pas souscrit aux Alertes.

Le Site inclut des liens vers d'autres sites Internet ou d'autres sources externes. Dans la mesure où LRE TRUST ne peut contrôler ces sites et ces sources externes, LRE TRUST ne peut être tenu pour responsable de la mise à disposition de ces sites et sources externes, et ne saurait être tenu pour responsable quant aux contenus, publicités, produits, services ou tout autre matériel disponible sur ou à partir de ces sites ou sources externes. En outre, LRE TRUST ne pourra être tenu pour responsable de tous dommages ou pertes avérés ou allégués consécutifs ou en relation avec l'utilisation des biens ou des services disponibles sur ces sites ou sources externes.

Le Membre est informé qu'LRE TRUST peut être amené à divulguer tout contenu pour se conformer aux lois applicables ou si, de bonne foi, celui-ci estime qu'une telle mesure est nécessaire, notamment dans le cadre d'une procédure judiciaire, par exemple pour faire respecter les CGU, pour répondre à des plaintes et/ou des revendications invoquant la violation des droits de tiers, pour protéger ses droits ou intérêts, ses Membres, ou le public.

Les Services sont fournis en l'état. LRE TRUST ne saurait être tenu pour responsable en cas de détérioration des logiciels du Membre et de tout piratage dont il serait victime du fait de l'utilisation des Services et qui ne serait pas directement imputable à une faute de LRE TRUST.

Des fonctionnalités supplémentaires pour les Services sont susceptibles d'être mise en place par LRE TRUST pour tests avant une intégration définitive dans les Services (les « Fonctionnalités en Version Béta »). Les Fonctionnalités en Version Béta seront clairement indiquées comme telles sur le Site et peuvent présenter des anomalies et ne proposer qu'une version limitée des fonctionnalités du Site. LRE TRUST ne saurait garantir un maintien ou un niveau de service quelconque aux Membres sur les Fonctionnalités en Version Béta.

LRE TRUST n'apporte aucune garantie de validité au regard du cadre réglementaire des LRE sur les envois effectués dans le cadre des Services Gratuits et des Fonctionnalités en Version Béta.

La responsabilité de LRE TRUST ne saurait être engagée dans le cas où l'inexécution de ses obligations serait imputable à un cas de force majeure tel que défini par les juridictions françaises et dans les cas suivants : tout ordre ou décision du gouvernement ou d'une entité administrative, catastrophes naturelles, intempéries, émeutes, grèves, guerres, actes de terrorisme, interruption, suspension, réduction ou perturbations électriques ou autres ou les interruptions de réseaux de communications électroniques.

En tout état de cause, la responsabilité totale de LRE TRUST à l'égard des Membres Professionnels et des Membres personnes morales au titre d'un manquement aux CGU ne saurait excéder les montants effectivement perçus par LRE TRUST au titre des Services rendus à l'Expéditeur au cours des 12 (douze) mois précédent le fait générateur de cette responsabilité de LRE TRUST à l'égard des Membres Professionnels et des Membres personnes morales.



# LRE TRUST



## 14. Disponibilité du site

LRE TRUST s'efforcera dans la mesure du possible d'assurer aux Membres une accessibilité au Site et aux Services à tout moment. Les Membres peuvent suivre en direct la disponibilité du service à l'adresse suivante : <http://status.lre.ma/>

Afin de prévenir tout incident technique, LRE TRUST dispose d'un site de sauvegarde externalisée et a défini un plan d'urgence et de poursuite de l'activité visant à rétablir le service dans un délai maximal de 120 (cent vingt) heures.

L'exploitation du Site et des Services pourra être momentanément interrompue pour toute cause indépendante de la volonté de LRE TRUST, en ce compris en cas de force majeure, de maintenance, de mises à jour ou d'améliorations techniques, ou pour en faire évoluer son contenu et/ou sa présentation.

LRE TRUST n'est pas responsable d'un non-fonctionnement, d'une impossibilité d'accès, ou de mauvaises conditions d'utilisation du Site et/ou des Services, pour quelque cause que ce soit.

LRE TRUST ne saurait être tenu responsable de tout préjudice occasionné par l'indisponibilité du Site et/ou des Services.

## 15. Résiliation

En cas de non-respect d'une des stipulations des CGU, LRE TRUST se réserve le droit, sans préavis et sans aucune indemnisation, et sans préjudice d'autres recours de quelque nature que ce soit, de suspendre la fourniture de tout ou partie des Services, et notamment de suspendre en tout ou partie l'accès au Site, de clôturer le Compte du Membre et de bloquer toute nouvelle demande d'inscription de sa part, et/ou de considérer le présent contrat comme résilié de plein droit, sans préjudice de tous dommages et intérêts auxquels LRE TRUST ou tiers pourraient prétendre.

Cette mesure d'exclusion s'effectue sans préjudice de toutes poursuites, pénales ou civiles, dont le Membre pourrait faire l'objet de la part des autorités publiques, de tiers ou de LRE TRUST pour le cas où le comportement du Membre aurait porté atteinte à ses intérêts.

Tout Membre dispose de la faculté de clôturer son Compte sous réserve d'un préavis de 90 (quatre-vingt-dix) jours adressé à [contact@lre.ma](mailto:contact@lre.ma). La clôture entraîne la suppression du Compte. Le Membre est informé qu'LRE TRUST conservera les données relatives à l'identité du Membre pendant toute la Durée de Conservation.

En cas de manquement par un Utilisateur à l'une de ses obligations au titre des CGU LRE TRUST pourra notifier ledit manquement à l'Utilisateur et mettre ce dernier en demeure de le corriger dans un délai de 8 (huit) jours. A l'expiration de ce délai, ou en cas d'impossibilité de corriger ledit manquement, LRE TRUST pourra de plein droit résilier les CGU sans autre préavis.

LRE TRUST pourra suspendre l'accès à un Compte dès la notification du décès d'un Membre personne physique et/ou de la dissolution d'un Membre personne morale.

LRE TRUST ne sera tenu de permettre l'accès et/ou de transférer le contenu associé à un Compte à un ayantdroit ou à un autre tiers, que sur autorisation de justice ou au vu d'une requête valide du notaire chargé de la succession ou d'un mandataire habilité du ou des héritiers, accompagnée d'un certificat de notoriété.

En cas de résiliation, le montant de la caution qui aurait éventuellement été déposée par le Membre auprès de LRE TRUST, ou tout prépaiement effectué par le Membre, sera restitué, minorée des montants restants alors dus à LRE TRUST.

Il incombe au Membre de procéder à la sauvegarde manuelle de l'ensemble des données lui afférent et disponibles sur la Plateforme LRE TRUST avant la résiliation effective des CGU. La résiliation peut entraîner la suppression ou la suspension de l'accès à toutes les informations associées à ce Compte.



## 16. Modification des CGU

LRE TRUST pourra modifier à tout moment les CGU. Le Membre sera informé de la nature de ces modifications dès leur mise en ligne sur le Site.

Les modifications entreront en vigueur un mois après leur mise en ligne sur le Site. Pour les Membres inscrits postérieurement à la mise en ligne des modifications sur le Site, celles-ci leur seront immédiatement applicables, lors de l'acceptation expresse du Membre au cours du processus de validation de son Compte.

## 17. Dispositions diverses

Si une partie quelconque des CGU devait s'avérer illégale, invalide ou inapplicable pour quelque raison que ce soit, le terme ou les termes en question seraient déclarés inexistantes et les termes restants garderaient toute leur force et leur portée et continueraient à être applicables. Les termes déclarés inexistantes seront remplacés par des termes qui se rapprocheront le plus du contenu de la clause annulée et à l'intention initiale de LRE TRUST.

## 18. Preuve

### 18.1. Preuves relatives aux LRE

Le service de LRE entièrement électronique produit des preuves de Dépôt, d'Acceptation, de Refus et de NonRéclamation qui sont opposables en justice. Leur authenticité est garantie par le jeton d'horodatage qualifié qu'elles contiennent et le cachet électronique avancé d'AR24 et de LRE TRUST qui est apposé dessus. Les preuves de LRE Trust sont mises à disposition de l'utilisateur expéditeur sur le site de LRE TRUST, celles d'AR24 sont sur demande avec un coût de 100 Dhs HT la preuve en adressant une demande sur [contact@lre.ma](mailto:contact@lre.ma).

### 18.2. Traces techniques

Les registres informatisés (les « Logs »), conservés dans les systèmes informatiques de LRE TRUST dans des conditions de sécurité habituellement reconnues comme fiables, sont considérés comme preuves des communications, accords et paiement intervenus entre les Parties, sauf preuve contraire.

La valeur probante de ces Logs ne pourra être remise en cause du simple fait de leur caractère électronique.

## 19. Règlement des différends

### 19.1. Réclamation préalable

En cas de contestation relative à la fourniture des Services par LRE TRUST ou à l'application ou l'interprétation des documents contractuels énumérés à l'Article 3 (un « Différend »), le Membre doit s'adresser en priorité par écrit à LRE TRUST par courrier électronique ou postal aux coordonnées indiquées à l'Article 1, et les Parties s'efforceront d'apporter une solution amiable au Différend.

### 19.2. Demande de médiation

En cas d'échec de la résolution amiable du Différend ou en l'absence de réponse de LRE TRUST dans un délai d'un an à compter de la réception de la réclamation par LRE TRUST, le Membre peut soumettre le Différend à la médiation conformément au règlement de médiation du CMAP auquel les parties déclarent adhérer.

Pour présenter sa demande de médiation, le Membre dispose d'un formulaire de réclamation accessible sur le site du médiateur.

Les Parties restent libres d'accepter ou de refuser la solution proposée par le médiateur.



## 20. Jurisdiction compétente et loi applicable

Les CGU sont soumises au droit marocain.

Tout litige résultant des CGU qui n'a pas été résolu en application de l'Article 19 des CGU sera soumis à l'appréciation des tribunaux compétents, et exclusivement du ressort du Tribunal de Commerce du ressort du siège social de LRE TRUST pour les Membres Professionnels.

## 21. Entrée en vigueur

Sans préjudice des dispositions de l'Article 16 des CGU pour les Membres existants, les CGU entrent en vigueur à compter de 30 jours après leur publication.

## 22. Conditions spécifiques aux lettres recommandées qualifiées

### 22.1. Politique de confiance

Le service de recommandé électronique qualifié est opéré conformément à la politique de confiance identifiée par l'OID suivant : 1.3.6.1.4.1.50034.1.1.2. Cette politique, ainsi que ses éventuelles versions précédentes, est disponible sur le Site.

Le service de recommandé électronique qualifié du partenaire AR24 est qualifié au sens de l'article 44 du *Règlement européen n ° 910/2014 du 23 juillet 2014* ; à ce titre, il est référencé dans la liste de confiance française (<https://www.ssi.gouv.fr/uploads/2016/07/tl-fr.xml>) et peut y être retrouvé grâce à l'OID ci-dessus.

### 22.2. Format des preuves

Les preuves produites par le service de recommandé électronique qualifié sont identifiables par la mention de l'OID ci-dessus et le logo européen<sup>[1]</sup> identifiant les services de confiance qualifiés :

### 22.3. Point de contact

Le point de contact du service de recommandé électronique qualifié est le même que celui du service non qualifié (§1.1).

### 22.4. Obligations relatives aux MIE

En cas de remise d'un moyen d'identification électronique (MIE) à un Destinataire ou un Expéditeur, celui-ci doit :

- Protéger celui-ci de toute perte ou divulgation
- Révoquer sans délai le MIE en cas de perte, vol, compromission ou de suspicion de compromission des moyens fournis

Les MIE sont strictement personnels et ne doivent pas être communiqués ou transmis à des tiers. L'utilisateur est responsable de l'utilisation qui est faite du MIE qui lui a été remis.



**LRE TRUST**



## 22.5. Signalement des modifications

Le service de recommandé électronique qualifié ne procède à aucune modification des données contenues dans les LRE.

# POLITIQUE DE GESTION

## LRE TRUST - SOUSCRIPTION DIGITALE

### Préambule

Le présent document constitue la Politique de Gestion de l'offre de Souscription Digitale LRE TRUST de LRE TRUST. Son objectif est de décrire les règles applicables à la dématérialisation et la signature électronique des documents, la génération et à la conservation des dossiers de preuve relatives aux transactions dématérialisées. Elle a vocation à prouver l'existence et l'intégrité de la signature de documents électroniques.

LRE Trust propose en mode « SaaS » (Software As A Service), via sa plateforme LRE TRUST , un service de signature électronique avec gestion de preuve associée qui a pour objet : - La signature électronique,

- L'horodatage,



# LRE TRUST



- L'archivage,
- La création d'un fichier de preuve ....

A cet égard, le service LRE TRUST permet aux clients de LRE TRUST et aux utilisateurs de signer électroniquement des documents et de les conserver, en leur conférant la même valeur légale qu'un écrit sur support papier, en conformité avec la réglementation applicable.

Il est précisé que LRE TRUST n'intervient pas sur le contenu des données, leur format et/ou sur le choix du type de document sous forme électronique signé entre le client et les utilisateurs. Pour cela, le client s'engage à faire l'étude juridique de validité de la dématérialisation de ses processus, et à respecter dans ce cadre notamment, le droit de la consommation et les droits de rétractation liés à son activité.

*Le présent document est une œuvre protégée par les dispositions du Code de la Propriété Intellectuelle ainsi que par toutes les conventions internationales applicables. Ce document est la propriété exclusive de LRE TRUST. Toute reproduction intégrale ou partielle, toute utilisation par des tiers, ou toute communication à des tiers, sans accord préalable écrit de LRE TRUST est illicite.*

## Sommaire

### 1. Cadre juridique

#### La loi 4320

Depuis la loi 4320 portant aux technologies de l'information et relative à la signature électronique l'écrit sous forme électronique est intégré dans le dispositif probatoire et notamment dans le système légal de la preuve.

**Identifier** quelqu'un consiste à établir l'identité de la personne, c'est-à-dire son caractère permanent et fondamental. Plusieurs méthodes d'identification (login/mot de passe, biométrie, OTP, certificat électronique, etc.) prises séparément ou cumulativement permettent d'attribuer un écrit à une personne. Toutefois, l'apposition de sa signature sur l'écrit reste la méthode privilégiée. Ainsi, l'alinéa 1er de l'article 1367 alinéas 1 du Loi 4320 dispose : « **La signature nécessaire à la perfection de l'acte juridique identifie celui qui l'appose. Elle manifeste le consentement des parties aux obligations qui découlent de cet acte. (...)** ». Ces fonctions d'identification et de manifestation du consentement concernent toutes les signatures, qu'elles soient électroniques ou manuscrites. Par ailleurs, l'article 1367 alinéa 2 du loi 4320 , dispose que la signature électronique est « *un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache* »

Conformément à l'article 1366 du Loi 4320 , l'écrit doit être « établi et conservé dans des conditions de nature à en garantir l'**intégrité** ». Ainsi, l'intégrité de l'écrit sous forme électronique doit être garantie de son établissement jusqu'au terme du délai de conservation et ce, afin qu'il soit recevable en tant que preuve au même titre que l'écrit sur support papier. L'écrit archivé ne doit avoir subi aucune altération ni modification qui n'ait été détectable et détectée.

#### Le règlement eIDAS

Après la directive 1999/93/CE sur la signature électronique, aux effets limités et divers selon les Etats membres, l'Union européenne a adopté, le 23 juillet 2014, un **Règlement sur l'identification et les services de confiance (eIDAS)**. Ce texte établit un socle commun par les interactions électroniques sécurisées entre les citoyens, les entreprises et les autorités publiques.



Ce texte est directement applicable dans tous les Etats membres pour la majorité de ses dispositions depuis le 1er juillet 2016. Il a pour principal objectif de renforcer la confiance et la sécurité juridique des transactions électroniques au sein du marché intérieur. Le règlement instaure un cadre européen en matière d'identification électronique et de services de confiance, afin de faciliter l'émergence du marché unique numérique. Il couvre notamment le sujet de la signature électronique, et abroge la directive 1999/93/CE.

Le règlement eIDAS s'applique à l'identification électronique, aux services de confiance et aux documents électroniques, élargissant ainsi le champ d'application de la directive 1999/93/CE sur la signature électronique. En effet, le règlement est essentiellement consacré à l'identification électronique et aux services de confiance. Il traite également, dans une moindre mesure, des documents électroniques en leur accordant un effet juridique.

Le règlement eIDAS a pour objectif d'instaurer un cadre juridique pour l'utilisation des services de confiance. Il prévoit des exigences pour les services de confiance relatifs à la signature électronique, au cachet électronique, à l'horodatage électronique, à l'envoi de recommandé électronique et à l'authentification des sites internet.

Le règlement établit également **une distinction entre les services de confiance non qualifiés et les services de confiance non qualifiés**. Les services de confiance non qualifiés satisfont à des exigences particulières et peuvent bénéficier d'effets juridiques spécifiques. Les services de confiance non qualifiés ne peuvent être assurés que par des prestataires de services de confiance non qualifiés. **Services de confiance non qualifiés versus non qualifiés**

Nous pouvons tout d'abord noter que les prestataires de services de confiance ayant opté et obtenu le statut « qualifié » doivent se soumettre aux exigences du Règlement pour les services qualifiés ainsi que l'accord de l'organe de contrôle. Pour cela, le prestataire devra avoir été évalué par un organisme accrédité et qualifié par l'organe de contrôle. Néanmoins, rien n'empêcherait le même prestataire de fournir des services non qualifiés et qui ne seraient alors pas assujettis à l'ensemble des exigences du Règlement. En effet, le considérant, le n°35 du règlement stipule que *« Tous les prestataires de services de confiance devraient être soumis aux exigences du présent règlement, notamment en matière de sécurité et de responsabilité, pour assurer une diligence appropriée, la transparence et la responsabilité quant à leurs activités et à leurs services. Toutefois, eu égard au type de services fournis par les prestataires de services de confiance, il y a lieu de faire une distinction, au niveau de ces exigences, entre, d'une part, les prestataires de services de confiance non qualifiés et, d'autre part, les prestataires de services de confiance non qualifiés »*.

Si un prestataire décide de fournir un ou plusieurs services de confiance, il a l'obligation de se conformer aux conditions du Règlement, particulièrement s'il s'agit de services qualifiés. Par ailleurs, un utilisateur de ces services doit pouvoir bénéficier des effets juridiques reconnus par le Règlement à chacun des services de confiance non qualifiés ou non, et les juridictions nationales sont tenues de reconnaître ces effets juridiques.

Le choix entre qualifié et non qualifié dépendra de la stratégie juridique et de la politique de gestion de risque de l'utilisateur.

- Soit on peut se satisfaire d'un niveau de sécurité et de fiabilité faible et/ou pour des opérations juridiques pour lesquelles le risque de contestation est faible et acceptable. Dans ce cas, il pourra se contenter d'un service non qualifié.
- Soit l'utilisateur est dans un domaine où un niveau de sécurité élevé est requis tant les risques d'attaques ou de fraudes sont importants et/ou on ne peut se permettre de prendre le risque d'une contestation. Dans ce cas, il faut recourir à un service de confiance qualifié.

En synthèse, l'utilisation d'un service « qualifié » permet à l'utilisateur de bénéficier de tous les éléments de preuve pour faire valoir le niveau de la signature électronique du fait de la qualité de « qualifiée » de son opérateur de service. En cas d'utilisation d'un service « non qualifié » l'utilisateur devra s'assurer qu'il bénéficie bien de l'ensemble des éléments de preuves nécessaires pour se défendre le cas échéant.

Le choix peut également se faire au vu des effets juridiques qui y sont liés et à la prévisibilité juridique qui en découle. En effet, les services de confiance non qualifiés bénéficient d'une clause de présomption, dispensant ainsi son utilisateur de la charge de la preuve en cas de contestation. La présomption de fiabilité porte sur le respect des exigences au Règlement. En tout état de cause, un opérateur qualifié, via son statut, est présumé capable de fournir tous les éléments de preuves donnant la valeur juridique de la signature électronique qu'il a produite.



A l'inverse, les services de confiance non qualifiés bénéficient simplement de la clause de non-discrimination qui consiste à considérer que l'effet juridique et la recevabilité du service de confiance non qualifié comme preuve en justice ne peuvent être refusés au seul motif que ce service se présente sous une forme électronique ou qu'il ne satisfait pas aux exigences du même service de confiance qualifié. En cas de contestation, il appartient aux parties d'apporter la preuve et ainsi de tenter de convaincre le juge que les garanties normalement attendues de ces services sont présentes.

Les services de confiance non qualifiés sont donc soumis à des exigences plus strictes ce qui justifie les effets juridiques privilégiés. Parmi les exigences, on retrouve la procédure d'autorisation préalable qui doit être soumise à un organe de contrôle national. Cet organe a pour obligation de vérifier que le prestataire de service de confiance respecte les exigences du Règlement. Le prestataire est donc inscrit sur une « liste de confiance » (article 22 du Règlement). Chaque Etat doit désigner un organe de contrôle qui est responsable d'établir, de tenir à jour et de publier cette liste.

Le règlement fait une distinction entre les exigences applicables à l'ensemble des prestataires de services de confiance (qualifiés ou non) et celles uniquement applicables aux prestataires de services de confiance non qualifiés.

Les exigences applicables à l'ensemble des prestataires se traduisent par une obligation générale de sécurité et par une obligation de notification en cas d'atteinte à la sécurité (article 19 du Règlement).

L'article 24 quant à lui prévoit les exigences applicables uniquement aux prestataires de services de confiance non qualifiés :

*« 1. Lorsqu'un prestataire de services de confiance qualifié délivre un certificat qualifié pour un service de confiance, il vérifie, par des moyens appropriés et conformément au droit national, l'identité et, le cas échéant, tous les attributs spécifiques de la personne physique ou morale à laquelle il délivre le certificat qualifié.*

*Les informations visées au premier alinéa sont vérifiées par le prestataire de services de confiance qualifié directement ou en ayant recours à un tiers conformément au droit national:*

- a) par la présence en personne de la personne physique ou du représentant autorisé de la personne morale; ou*
- b) à distance, à l'aide de moyens d'identification électronique pour lesquels, avant la délivrance du certificat qualifié, la personne physique ou un représentant autorisé de la personne morale s'est présenté en personne et qui satisfont aux exigences énoncées à l'article 8 en ce qui concerne les niveaux de garantie substantiel et élevé; ou*
- c) au moyen d'un certificat de signature électronique qualifié ou d'un cachet électronique qualifié délivré conformément au point a) ou b); ou*
- d) à l'aide d'autres méthodes d'identification reconnues au niveau national qui fournissent une garantie équivalente en termes de fiabilité à la présence en personne. La garantie équivalente est confirmée par un organisme d'évaluation de la conformité.*

*2. Un prestataire de services de confiance qualifié qui fournit des services de confiance non qualifiés:*

- a) informe l'organe de contrôle de toute modification dans la fourniture de ses services de confiance non qualifiés et de son intention éventuelle de cesser ces activités;*
- b) emploie du personnel et, le cas échéant, des sous-traitants qui possèdent l'expertise, la fiabilité, l'expérience et les qualifications nécessaires, qui ont reçu une formation appropriée en ce qui concerne les règles en matière de sécurité et de protection des données à caractère personnel et appliquent des procédures administratives et de gestion correspondant à des normes européennes ou internationales;*
- c) en ce qui concerne le risque de responsabilité pour dommages conformément à l'article 13, maintien des ressources financières suffisantes et/ou contracte une assurance responsabilité appropriée, conformément au droit national;*
- d) avant d'établir une relation contractuelle, informe, de manière claire et exhaustive, toute personne désireuse d'utiliser un service de confiance qualifié des conditions précises relatives à l'utilisation de ce service, y compris toute limite quant à son utilisation;*



- e) *utilise des systèmes et des produits fiables qui sont protégés contre les modifications et assure la sécurité technique et la fiabilité des processus qu'ils prennent en charge;*
- f) *utilise des systèmes fiables pour stocker les données qui lui sont fournies, sous une forme vérifiable de manière que :*
  - i) *les données ne soient publiquement disponibles pour des traitements qu'après avoir obtenu le consentement de la personne concernée par ces données;*
  - ii) *seules des personnes autorisées puissent introduire des données et modifier les données conservées;*
  - iii) *l'authenticité des données puisse être vérifiée;*
- g) *prend des mesures appropriées contre la falsification et le vol de données;*
- h) *enregistre et maintient accessibles pour une durée appropriée, y compris après que les activités du prestataire de services de confiance qualifié ont cessé, toutes les informations pertinentes concernant les données délivrées et reçues par le prestataire de services de confiance qualifié, aux fins notamment de pouvoir fournir des preuves en justice et aux fins d'assurer la continuité du service. Ces enregistrements peuvent être effectués par voie électronique;*
- i) *a un plan actualisé d'arrêt d'activité afin d'assurer la continuité du service conformément aux dispositions vérifiées par l'organe de contrôle au titre de l'article 17, paragraphe 4, point i;*
- j) *assure le traitement licite de données à caractère personnel conformément à la directive 95/46/CE;*
- k) *au cas où le prestataire de services de confiance qualifié délivre des certificats qualifiés, il établit et tient à jour une base de données relative aux certificats.*

3. *Lorsqu'un prestataire de services de confiance qualifié qui délivre des certificats qualifiés décide de révoquer un certificat, il enregistre cette révocation dans sa base de données relative aux certificats et publie le statut de révocation du certificat en temps utile, et en tout état de cause dans les vingt-quatre heures suivant la réception de la demande. Cette révocation devient effective immédiatement dès sa publication.*

4. *En ce qui concerne le paragraphe 3, les prestataires de services de confiance non qualifiés qui délivrent des certificats qualifiés fournissent à toute partie utilisatrice des informations sur la validité ou le statut de révocation des certificats qualifiés qu'ils ont délivrés. Ces informations sont disponibles, au moins par certificat, à tout moment et au-delà de la période de validité du certificat, sous une forme automatisée qui est fiable, gratuite et efficace.*

5. *La Commission peut, au moyen d'actes d'exécution, déterminer les numéros de référence des normes applicables aux systèmes et produits fiables, qui satisfont aux exigences du paragraphe 2, points e et f, du présent article. Les systèmes et les produits fiables sont présumés satisfaire aux exigences fixées au présent article lorsqu'ils respectent ces normes. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 48, paragraphe 2 ».*

## **Les services de confiance en particulier**

Aux termes du Règlement, font partie des services de confiance :

- La signature électronique,
- Le cachet électronique,
- L'horodatage,
- Les envois recommandés
- L'authentification de site web.

### La signature électronique :

La section 4 du chapitre 3 du règlement relative à la signature électronique reprend en grande partie les dispositions de la directive 199/93/CE.

Le règlement prévoit 3 niveaux de sécurité de la signature électronique que nous allons reprendre dans le tableau ci-dessous :



Signature électronique	Cadre juridique	Caractéristiques	Recevabilité
<b>Simple</b>	<ul style="list-style-type: none"><li>- Article <b>1367</b> du loi 4320 .</li><li>- Article <b>3.10</b> du règlement 910/2014</li></ul>	<ul style="list-style-type: none"><li>- Identification fiable de l'auteur (déclarative ou vérifiée).</li><li>- Manifestation du consentement (le consentement ne doit pas être vicié : Double clic, OTP SMS...).</li><li>- Intégrité du document (scellement ou cachet électronique).</li><li>- Lien entre le procédé et l'acte auquel il s'attache.</li></ul>	<ul style="list-style-type: none"><li>- Article <b>25</b> du règlement 910/2014 : =&gt; l'utilisateur doit prouver la fiabilité, la signature simple ne bénéficie pas de la présomption de fiabilité.</li></ul>

\* Le moyen doit être validé dans le cadre d'une analyse de risque qui aboutit au résultat du respect de l'exigence liée au contrôle exclusif. A date, ce postulat reste vrai tant que l'autorité française - ANSSI (autorité nationale en matière de sécurité et de défense des systèmes d'information) ne gère pas les services non qualifiés et que les standards techniques applicables à la signature centralisée ne sont pas imposés.

### L'horodatage :

Le règlement définit l'horodatage comme « des données sous forme électronique qui associent d'autres données sous forme électronique à un instant particulier et établissent la preuve que ces dernières données existaient à cet instant» (article 3.33) ».

	Critères	Reconnaissance juridique
<b>Horodatage électronique</b>	Des données sous forme électronique qui associent d'autres données sous forme électronique à un instant particulier et établissent la preuve que ces dernières données existaient à cet instant.	Clause de non-discrimination

### Les recommandés électroniques :

D'après le règlement, un service d'envoi recommandé électronique est « un service qui permet de transmettre des données entre des tiers par voie électronique, qui fournit des preuves concernant le traitement des données transmises, y compris la preuve de leur envoi et de leur réception, et qui protège les données transmises contre les risques de perte, de vol, d'altération ou de toute modification non autorisée. »

	Critères	Reconnaissance juridique
<b>Envoi recommandé électronique</b>	<ul style="list-style-type: none"><li>- Transmet des données entre des tiers par voie électronique,</li><li>- fournit des preuves concernant le traitement des données transmises, y compris la preuve de leur envoi et de leur réception,</li><li>- protège les données transmises contre les risques de perte, de vol, d'altération ou de toute modification non autorisée.</li></ul>	Clause de non-discrimination

## La signature électronique et le code de procédure civile

### Présomption de fiabilité



L'article 1367 alinéa 2 instaure une présomption de fiabilité: « *La fiabilité de ce procédé est présumée, jusqu'à preuve contraire, lorsque la signature électronique est créée, l'identité du signataire assurée et l'intégrité de l'acte garantie, dans des conditions fixées par décret en Conseil d'Etat.* »

Selon l'article 288-1 du code de procédure civile : « *lorsque la signature électronique bénéficie d'une présomption de fiabilité, il appartient au juge de dire si les éléments dont il dispose justifient le renversement de cette présomption* ».

## Vérification de l'acte litigieux

Pour procéder à la vérification de l'acte litigieux, le juge peut se fonder sur les articles 287 à 293 du code de procédure civile. Il a ainsi la faculté de recourir à toutes mesures d'instruction, telle la production de titre ou de fichier de preuve électronique, la comparution personnelle des parties, l'audition de témoins ou le recours à un technicien.

Tout procédé d'identification garantissant le lien entre la signature et le document est susceptible d'être reconnu fiable à condition que la preuve de la fiabilité du procédé soit rapportée.

## **2. Les différentes politiques**

La constitution de la preuve s'appuie sur plusieurs services de confiance. Ces services peuvent être opérés par différents acteurs. Par conséquent, la présente PGP doit être adossée aux politiques suivantes :

**Politique d'Archivage** : ensemble de règles établissant les devoirs et responsabilités du P.S.A et de tous les intervenants dans l'ensemble du cycle de vie des données archivées chez le P.S.A. Elle est sous la responsabilité du P.S.A et doit être auditable.

**Politique de Certification** : ensemble de règles établissant les devoirs et responsabilités de l'A.C et de tous les intervenants dans l'ensemble du cycle de vie d'un Certificat. Elle est sous la responsabilité de l'A.C et doit être auditable.

**Politique d'Horodatage** : ensemble de règles établissant les devoirs et responsabilités de l'A.H. et de tous les intervenants dans l'ensemble du cycle de vie d'un Jeton d'horodatage. Elle est sous la responsabilité de l'A.H. et doit être auditable.

**Politique de Gestion de Preuve (P.G.P)** : ensemble de règles établissant les devoirs et responsabilités de tous les intervenants dans l'ensemble du cycle de vie de la Preuve. Elle est sous la responsabilité de LRE TRUST et doit être auditable.

Protocole Client : document définissant les processus et modalités de mise en œuvre des types de signatures en mode projet.



**LRE TRUST**



### **3. Identification de la présente politique de gestion de preuve**

La présente PGP est identifiée par l'OID 1.2.250.1.229.1.1.1.1.2.

Dans l'hypothèse de modifications ultérieures sur ce document, le numéro d'OID sera modifié.



**LRE TRUST**



#### **4. Objet et champ d'application de la présente politique**

Dans un souci de pérennité de la valeur probante d'un écrit numérique, il peut être utile de conserver l'écrit, la signature électronique et les éléments qui sont associés (certificat, liste de certificats révoqués, jeton d'horodatage, OTP...) destinés à pouvoir vérifier la signature dans le temps.

La gestion de la preuve telle qu'envisagée par LRE TRUST, décrite dans la présente Politique, permet d'assurer la conservation de la valeur juridique initiale de l'écrit numérique pendant toute sa durée de vie, de son établissement jusqu'au terme du délai de conservation.

Le champ d'application de la présente Politique s'étend a priori à l'ensemble des actes établis par voie électronique (documents, actes, données, processus), fournis par LRE TRUST, lorsque les textes le permettent, qu'il s'agisse de documents relevant du droit privé comme du droit public, mais aussi aux faits juridiques (date d'un acte, données de connexion, traçabilité...).

La présente Politique s'adresse à tous les acteurs intervenants dans le cycle de la gestion de la preuve.



## 5. Les entités impliquées

**Autorité de Certification (A.C.) :** entité ayant en charge l'application d'au moins une politique de certification et est identifiée comme telle, en tant qu'émetteur dans les Certificats émis au titre de cette Politique de certification. L'AC a en charge la fourniture des prestations de gestion des certificats tout au long de leur cycle de vie (génération, diffusion...) et s'appuie sur l'IGC. Dans le cadre de cette politique, l'A.C. est la société CERTINOMIS, filiale de la société LRE TRUST.

**Autorité d'enregistrement (A.E.) :** entité dont le rôle est d'identifier les demandeurs ou les porteurs de certificats. Elle s'assure de l'authenticité de l'identité de ces derniers et vérifie que les obligations attachées à l'utilisation d'un certificat sont remplies, tout en étant conforme à la politique de certification.

**Autorité d'Enregistrement Déléguée (A.E.D.) :** entité à qui l'A.E délègue ses missions pour l'identification et l'enregistrement des personnes physiques ou morales.

Elle procède à l'identification du porteur ou de son mandataire de certification, vérifie sa pièce d'identité, inscrit sur la photocopie de cette dernière « certifié conforme à l'original » et la signe.

**Autorité d'Horodatage (A.H.) :** autorité responsable de l'émission et de la gestion de Jetons d'horodatage.

**Client :** toute personne physique ou morale et tout service ou organisme public ou privé requérant les services du P.S.G.P et ayant conclu, directement ou par le biais du réseau commercial, une relation contractuelle avec lui.

**Contractant :** personne physique identifiée dans le Certificat et qui est le détenteur de la clé privée correspondant à la clé publique qui est dans ce Certificat. Le contractant représente également l'une des parties intervenant dans la transaction gérée par LRE TRUST .

**Distributeur :** toute personne physique ou morale et tout service ou organisme public ou privé en relation contractuelle avec le Client pour proposer les Offres du Client et pour les distribuer aux Contractants.

Fournisseur : notion fonctionnelle utilisée par la solution LRE Trust pour définir le client.

**Manipulateur :** personne physique, employée par un Distributeur, utilisant le système « LRE TRUST ».

**Prestataire de Services d'Archivage (P.S.A) :** personne morale en charge de recevoir, de conserver, de restituer, en d'autres termes d'assurer la gestion des éléments de preuves dans le temps pour le compte du Client. Il est en relation contractuelle avec le Client. (Remarque : est souvent appelé Tiers Archiveur).

**Prestataire de Services de Certification Electronique (P.S.C.E) :** toute personne qui délivre des certificats électroniques ou fournit d'autres services en matière de signature électronique.

**Prestataire de Services de Gestion de Preuve (P.S.G.P) :** entité en charge d'assurer la gestion de la preuve d'une Transaction au moment de sa signature. Les éléments suivants sont alors vérifiés :

- l'origine des Données et l'identité du Client/du Contractant ;
- la signature électronique des parties à une Transaction (intégrité des données et validité du Certificat à la date de réception de la Transaction) ;
- un Jeton d'horodatage indiquant la date à laquelle les données ont été signées ; ■ ou d'autres éléments qui seront déterminés dans le Protocole Client.

**Prestataire de Services d'Horodatage Electronique (P.S.H.E) :** toute personne en charge de la production et de la délivrance de contremarques de temps.

**Signataires :** ensemble des Contractants et Clients parties à une Transaction.

## 6. Définitions



**LRE TRUST**



Dans le cadre de la présente P.G.P, sont définis comme suit :

**Attestation de preuve** : correspond au fichier de preuve signé électroniquement par LRE TRUST .

**Bi-clé** : couple clé publique, clé privée (utilisées dans des algorithmes de cryptographie dits à clé publique ou asymétriques).

**Contrat** : convention par laquelle une ou plusieurs personnes s'obligent envers une ou plusieurs autres, à donner, à faire ou à ne pas faire quelque chose. Dans le cadre de LRE TRUST , il s'agit d'un acte signé électroniquement par le Client et le (ou les) Contractant(s).

**Certificat** : fichier électronique attestant qu'une bi-clé appartient au Contractant ou à l'élément matériel ou logiciel identifié, directement ou indirectement (pseudonyme), dans le Certificat. Il est délivré par une A.C. En signant le Certificat, l'A.C valide l'identité de la personne physique ou morale ou l'élément matériel ou logiciel et la bi-clé. Le Certificat est valide pendant une durée donnée, précisée dans un de ses champs (certificats transactionnels).

Remarque : Par abus de langage et au moment de sa délivrance, le certificat comprend également la clé privée.

**Dossier de preuve** : ensemble de fichiers contenant les éléments suivants :

- Fichier de preuve ;
- Contrat ;
- Pièces justificatives liées au contrat (si applicable).

**Fichier de preuve** : fichier contenant l'ensemble des éléments techniques destinés à apporter la preuve d'une action effectuée dans le cadre d'une transaction et en particulier la vérification des signatures. Un tel fichier contient les éléments suivants :

- Transaction signée au format XAdES ;
- Éléments permettant l'identification des Contractants ;
- Éléments identifiant le Client ;
- Éléments décrivant la transaction ;
- Vérifications des signatures ;
- Le cas échéant, d'autres informations en fonction du Protocole Client retenu.

Remarque : par abus de langage le terme fichier de preuve correspond en fait au fichier des éléments techniques de preuve.

**Infrastructure de Gestion des Clés (IGC)** : ensemble des composantes, fonctions et procédures dédiées à la gestion des clés cryptographiques et de leurs Certificats utilisés par des services de confiance. Une IGC peut être composée d'une AC, d'un OC, d'une AE centralisée ou locale, de mandataires de certification, d'un TA, etc.

**Intégrité** : il s'agit ici de l'intégrité au sens du contenu informationnel des documents traités qui correspond en fait à la garantie de non altération desdits documents.

**Jeton d'Horodatage** : élément de données résultant de l'association de données à une date et une heure obtenues à partir d'une source de temps réputée fiable, le tout étant signé.

**Offre** : offre définie par le Client, décrite par un nom, un label et un code. Le détail de l'offre est précisé dans le Protocole Client.

**Protocole Client** : document contenant les règles spécifiques d'identification, de consentement et/ou d'archivage propre à un Client dans le cadre de la mise en œuvre du processus de dématérialisation de signature.



**LRE TRUST**



**Référence contrat** : fichier informatique contenant les éléments permettant de faire le lien entre les éléments de preuve conservés et le contrat d'origine.

**Scellement** : procédé permettant de s'assurer que le Contrat a bien été scellé afin d'en garantir l'intégrité. Ce scellement permet également d'apposer la marque de LRE TRUST dans le document en tant que tiers de confiance ayant veillé au bon déroulement de l'ensemble de la transaction.



## 7. Gestion du Cycle de vie de la transaction et de la preuve

### 1- Demande et collecte des données d'identification du Contractant pour enregistrement.

Le Client a en charge de collecter – directement ou par le biais d'un réseau de Distributeurs – les données permettant d'identifier les Contractants ainsi que les pièces justificatives. Les différentes modalités de collecte sont précisées dans le Protocole Client. Le P.S.G.P. recommande que la procédure d'enregistrement ne soit ouverte qu'aux Contractants connus du Client ou bien que la procédure de vérification d'identité soit particulièrement détaillée pour les prospects dans le cadre de leur Protocole.

### 2- Etablissement du projet de Transaction

Le Distributeur doit établir le projet de Transaction sous format électronique. Il est entendu que des champs de formulaire peuvent être intégrés dans le projet de Transaction pour être enrichis pendant le traitement de la Transaction et dans tous les cas avant la signature de la Transaction.

### 3- Transmission du projet de Transaction au service de gestion de preuve

Le Distributeur doit transmettre au service du P.S.G.P le projet de Transaction au format électronique. Le service de gestion de preuve vérifie l'intégrité du projet de Transaction reçu du Distributeur. Dans le cas où les contrôles opérés par le P.S.G.P sont valides, les paragraphes suivants de la présente Politique trouveront à s'appliquer. En cas d'échec, le P.S.G.P transmettra au Distributeur un message d'erreur en réponse à sa demande de Transaction. Le Distributeur pourra alors après vérification effectuer à nouveau la procédure prévue aux § 4.1 et suivants de la présente Politique.

### 4- Emission du ou des Certificats du ou des contractants et du Certificat du client (optionnel)

#### **Certificat client**

Le Certificat du client est émis selon les modalités figurant dans la Politique de Certification dont il est issu (cf. Protocole).

#### **Certificat du ou des contractants**

Les modalités d'émission des Certificats des contractants figurent dans la Politique de Certification précisée dans le Protocole client selon le type de signature utilisée.

### 5- Signature de la Transaction par le 0 à n contractants

Le Contractant signe pour son compte avec le moyen de Signature requis, la Transaction. La signature est horodatée par l'AH. Le P.S.G.P. vérifie alors la validité du certificat à la date de signature figurant sur le Jeton délivré par l'AH. L'utilisation d'un certificat invalide ou révoqué génère une erreur. Les modalités de Signature et de Protocole de consentement dépendent du Protocole.

### 6- Signature de la Transaction par 0 à n clients

Le P.S.G.P signe pour le compte du client le projet de Transaction afin de le rendre définitif. La signature est horodatée par l'AH. Le P.S.G.P. vérifie :

- la validité du certificat client à la date de signature figurant sur le Jeton délivré par l'AH ;
- la non-révocation de ce certificat. Les listes de révocation des certificats sont récupérées toutes les heures. Un certificat détecté comme révoqué ne peut plus être utilisé.

L'utilisation d'un certificat invalide ou révoqué génère une erreur.



**LRE TRUST**



## 7- Scellement LRE TRUST

Après signature par le Client, le P.S.G.P propose d'effectuer un Scellement de la Transaction attestant du bon déroulement du processus de signature. Le Scellement est horodaté par l'AH. Le P.S.G.P vérifie la validité du certificat de scellement à la date de signature figurant sur le Jeton délivré par l'AH. Si le certificat de scellement est invalide ou révoqué, une erreur est générée.

C'est une option proposée par le P.S.G.P

## 8- Etablissement d'une attestation de preuve

A la suite des opérations de signature et après archivage sécurisé des éléments de la Transaction, le P.S.G.P. établit une attestation de preuve rassemblant les éléments d'information et de vérification.

Cette attestation de preuve est signée, la signature horodatée. L'attestation de preuve est archivée.

La signature de l'attestation de preuve est conforme aux formats de signature du règlement eIDAS :

- XAdES Baseline Profile ETSI TS 103171 v.2.1.1 et/ou
- PAdES Baseline Profile ETSI TS 103172 v.2.2.2

## 9- Transmission de la Transaction/de la Preuve

Un exemplaire de l'attestation de preuve est transmis au Contractant, au Client ainsi qu'aux autres parties utilisatrices de manière sécurisée.

## 10- Acceptation implicite de l'attestation de preuve

Le Contractant accepte implicitement l'Attestation de preuve sauf notification contraire de sa part.

## 11- Versement, conservation et restitution de l'attestation de Preuve

Les conditions entourant l'archivage sécurisé et la restitution des attestations de Preuve pour un Client et les Contractants peuvent être détaillées dans le Protocole Client. Le P.S.G.P s'engage à gérer et à restituer les preuves d'archivage transmises par le P.S.A en lien avec les attestations de Preuve correspondantes.

Le P.S.G.P met à disposition une interface permettant de rechercher les attestations de Preuve en fonction de mots clés, de les récupérer, voire de commander une attestation de Preuve d'une taille supérieure à une limite fixée. Les attestations de Preuve émises par le P.S.G.P sont conservées pendant la durée prévue dans le Protocole Client.

Seront conservées pendant la durée prévue dans le Protocole Client les renseignements liés à la gestion du cycle de vie des attestations de Preuve, en particulier tous les renseignements liés à l'enregistrement, ainsi que les configurations et applications ayant servi à cette gestion. De plus, les informations conservées et sauvegardées par le P.S.G.P peuvent être assujetties aux lois et règlements en vigueur et applicables à l'archivage et la conservation. Le Client doit assurer ou faire assurer l'archivage sécurisé des données ayant concouru à l'établissement de la Transaction.

## 12- Procédure d'intervention du P.S.G.P

Dans le cas où le Client aurait besoin des services du P.S.G.P. suite à la remise en cause de la valeur juridique de la Transaction qu'il a archivée, une procédure d'intervention du P.S.G.P. est mise en place. Le Client fait état d'une demande motivée d'intervention du P.S.G.P. Les motifs peuvent notamment être liés à un litige à naître ou devant les Tribunaux. Il doit par exemple être exposé que la valeur juridique de l'attestation de Preuve est remise en cause par la partie adverse lors d'une expertise judiciaire.



## 13- Journalisation d'événements

### Types d'événements enregistrés

Les événements à enregistrer sont toutes les opérations de pilotage de l'activité de gestion de preuve permettant de suivre l'efficacité et la traçabilité du service rendu au Client. Il s'agira notamment :

- des opérations liées à la gestion du service effectuée par le responsable de sécurité ou le gestionnaire du service,
- des opérations correspondant au service de gestion de preuve, - des opérations effectuées par les utilisateurs du système.

### Fréquence des traitements des journaux d'événements

Le processus de journalisation :

- est effectué en tâche de fond,
- permet un enregistrement immédiat des opérations effectuées. Le processus de journalisation des événements est accompagné d'une chronologie fournie par un service de chronologie interne.

### Durée de conservation des journaux d'événements

Les journaux d'événements sont conservés sur le site pour une période correspondant à celle des attestations de Preuves, tel que prévu au §4.11, dans la mesure où ils en constituent un élément de preuve complémentaire.

### Protection d'un journal d'événements

L'écriture dans les journaux d'événements est conditionnée par des contrôles de droits d'accès. Les journaux d'événements sont protégés en intégrité et le système de chronologie des événements est à la fois sûr et non modifiable.

### Copies de sauvegarde des journaux d'événements

Le journal d'événement est archivé au format XML signé et horodaté quotidiennement.

### Système de collecte des journaux d'événements

Le système de collecte des journaux d'événements interne du P.S.G.P. se déclenche au démarrage du système informatique et reste actif jusqu'à son extinction. Tout contournement du processus de journalisation doit être détectable. Enfin, en cas de saisie manuelle, l'écriture se fait dans le même jour ouvré que l'événement.

### Imputabilité

L'imputabilité d'une action revient à la personne, l'organisme ou le système l'ayant exécuté. L'identifiant de l'exécutant figure dans l'un des champs du journal d'événements. **Analyse des vulnérabilités**

Pour chaque tentative de violation de l'intégrité du système de gestion du P.S.G.P., celui-ci se réserve le droit d'engager des poursuites.

L'analyse des vulnérabilités porte sur :

- le contrôle des journaux d'événements pour identifier des anomalies liées à des tentatives en échec,
- la garantie par l'opérateur de service de la revue de ses journaux d'événement par son personnel à une fréquence hebdomadaire, l'existence d'un processus d'analyse pour tous les éléments de sécurité qui sont remontés en échec,
- la documentation des mesures à prendre à la suite de cette analyse.

### Changement de clé du service de gestion de preuve

Le service de gestion de preuve possède une bi-clé de signature unique avec laquelle sont effectuées les opérations de signature des attestations de Preuve. En cas de compromission effective ou suspectée, la clé privée cesse d'être utilisée et le certificat de la clé publique est révoqué. En cas d'évolution non prévue de l'état de l'art en cryptographie, les certificats du service peuvent être révoqués.



**LRE TRUST**



### **Fin de vie des services du P.S.G.P**

En cas d'interruption de ses activités, le P.S.G.P. s'engage à :

- aviser immédiatement ses Clients et prendre des dispositions pour que les informations détenues par le P.S.G.P. continuent à être archivées et accessibles dans les mêmes conditions,
- convenir d'accords particuliers assurant un bon niveau d'assurance si les opérations du P.S.G.P. sont transférées à un autre opérateur.



## 8. Obligations et responsabilités dans le cycle de gestion de preuve

### 8.1. Obligations

#### 1- Obligations du PSGP

Le P.S.G.P. est responsable vis-à-vis de ses Clients des opérations relatives à la gestion de la preuve réalisées par l'une quelconque des composantes du P.S.G.P. Il garantit le contenu du Fichier de preuve ainsi que son intégrité.

Le P.S.G.P. veille à ce que l'ensemble des prestataires intervenant dans la gestion de preuve se conforme à toutes les modalités pertinentes de la présente Politique. Le P.S.G.P. et son responsable doivent se conformer aux exigences de la présente Politique. Le P.S.G.P. et son personnel doivent respecter les droits des Clients eu égard aux lois et règlements en vigueur.

Le P.S.G.P. doit documenter les relations contractuelles, les versions des contrats avec les Clients ainsi que les conditions d'utilisation du service ainsi que la convention de service, applicables aux Contractants. Le P.S.G.P. avertit ses Clients qu'il ne pourra effectuer les vérifications nécessaires qu'à la condition que les listes de certificats révoqués des A.C. dont les Clients ont besoin, soient accessibles au P.S.G.P. A défaut, le P.S.G.P. serait dans l'impossibilité de réaliser le fichier de preuve dans sa globalité.

Les membres du personnel du P.S.G.P, et les exploitants mandatés, à qui sont assignés des rôles relatifs à la gestion de la preuve (responsable du P.S.G.P, responsable de la sécurité du P.S.G.P...) doivent être personnellement responsables de leurs actes. L'expression « personnellement responsable » signifie que l'on puisse rapporter la preuve qu'une personne a bel et bien fait telle action. Le P.S.G.P doit mettre en œuvre des matériels informatiques selon les procédures adaptées telles que détaillées dans les déclarations des pratiques de gestion de la preuve et leur mise en œuvre opérationnelle.

Le P.S.G.P doit être auditable et être en mesure de répondre aux contrôles techniques et audits de qualité des procédures qui pourraient lui être demandées dans le cadre des obligations légales et de ses engagements. Le P.S.G.P doit utiliser des ressources cryptographiques d'un niveau de sécurité suffisant pour le service de gestion de preuve, contrôler les accès physiques et les limiter strictement et exclusivement aux personnes dûment autorisées.

Le P.S.G.P doit mettre à jour et préserver l'intégrité des listes et documents qu'il publie. Le P.S.G.P doit assurer le contrôle de conformité de ses propres pratiques.

#### Obligations relatives à la gestion de la preuve

Le P.S.G.P doit émettre et gérer les dossiers de preuve pendant la durée prévue dans le Protocole Client.

A ce titre, il doit :

- vérifier la validité du moyen d'identification du Contractant qui a fait la demande ;
- traiter les demandes après identification du Contractant ;
- vérifier la Signature électronique, à savoir effectuer les contrôles auprès de l'A.C. pour déterminer la validité de cette Signature en particulier grâce au Certificat joint à la Transaction envoyée par le Contractant ;
- effectuer la génération des dossiers de preuve qu'il aurait traités favorablement ;
- assurer la mise à disposition des Contrats du Client et du fichier de Preuves au Contractant ;
- archiver le fichier de Preuves pour le compte du Client. Le P.S.G.P a la responsabilité de mettre en œuvre le système qui permet d'assurer la gestion du cycle de vie des dossiers de Preuve selon les demandes du Contractant. Le P.S.G.P s'engage à respecter ses engagements de service formulés dans la Convention de Services avec le Client, en particulier en matière de disponibilité.

#### Obligations en cas de contestation des dossiers de Preuve

Le P.S.G.P s'engage à mettre à disposition des Contractants les dossiers de Preuve en cas de contentieux entre le Client et le Contractant.



1- Obligations relatives à l'AH L'A.H. prend en charge l'ensemble du processus d'horodatage, et donc de la validité des Jetons d'horodatage qu'elle émet. La garantie apportée par l'A.H. vient de la qualité de la technologie mise en œuvre, mais aussi du cadre réglementaire et contractuel qu'elle s'engage à respecter.

L'A.H. doit veiller à ce que les composantes de l'Infrastructure de Gestion des Clés (IGC) qui agissent en son nom se conforment à toutes les modalités pertinentes de la P.H.

L'A.H. est responsable de l'émission des Jetons d'horodatage qui seront utilisés par le P.S.G.P. au moment de la constitution de la Preuve.

L'A.H. assure directement ou indirectement les prestations techniques, en particulier cryptographiques, nécessaires au processus d'émission des Jetons d'horodatage. L'A.H. est en charge du bon fonctionnement et de la sécurité des moyens informatiques et techniques relatifs aux processus d'élaboration des Jetons d'horodatage compris dans la P.H.

L'A.H. est en charge du bon respect des procédures et des dispositifs nécessaires pour garantir un niveau de fiabilité satisfaisant.

## 2- Exigences relatives à l'A.C pour les Certificats Client et les Certificats des Contractants

L'A.C doit veiller à ce que les composantes de l'IGC qui agissent en son nom se conforment à toutes les modalités pertinentes de sa P.C.

L'A.C doit garantir le lien qui existe entre une bi-clé et le Client ainsi que celui qui existe entre une bi-clé et le Contractant. L'A.C a la responsabilité de mettre en œuvre le système qui permet de générer les Certificats et d'assurer la gestion de leur cycle de vie, incluant la génération des listes de certificats révoqués. L'A.C doit ainsi valider la génération des Certificats, transmettre les informations concernant la révocation des certificats. A ce titre, elle doit tenir, mettre à jour et publier une liste de certificats révoqués à destination de tiers, notamment le P.S.G.P dans les plus brefs délais à compter de la révocation du Certificat. L'A.C peut être interne ou externalisée.

## 3- Exigences relatives au P.S.A

Le P.S.A. prend en charge l'ensemble du processus d'archivage des Dossiers de Preuves.

La garantie apportée par le P.S.A. vient de la qualité de la technologie mise en œuvre, mais aussi du cadre réglementaire et contractuel qu'il s'engage à respecter.

Le P.S.A. est responsable de l'archivage et de la restitution des dossiers de preuves sur demande du Client, charge pour ce dernier de restituer les dossiers de Preuves aux Contractants.

Le P.S.A. assure directement ou indirectement les prestations techniques, en particulier cryptographiques, nécessaires à la gestion et à la restitution des dossiers de Preuve. Le P.S.A. est en charge du bon fonctionnement et de la sécurité des moyens informatiques et techniques relatifs au processus de gestion et de restitution des dossiers de Preuve. Le P.S.A. est en charge du bon respect des procédures et des dispositifs nécessaires pour garantir un niveau de fiabilité satisfaisant.

## 4- Obligations du Client

Le client est la personne morale qui s'est engagée contractuellement avec le P.S.G.P. pour bénéficier des services de gestion de preuve décrits dans la présente Politique.

Le client doit vérifier que les coordonnées qu'il a communiquées au P.S.G.P. sont valides et doit porter à la connaissance du P.S.G.P. toute modification qui leur serait apportée. Le client dispose de la faculté de confier la relation commerciale et les prestations relatives à l'enregistrement des Contractants à un réseau de Distributeurs. Ces Distributeurs devront notamment s'assurer de conserver les données permettant d'identifier les Contractants ainsi que les documents contractuels qu'ils pourraient avoir fait signer aux Contractants. Les Distributeurs pourront eux-mêmes s'appuyer sur des Manipulateurs en charge de la saisie des données pertinentes.



## 5- Obligations des Contractants

Le Contractant est la personne ayant accepté expressément les Conditions d'utilisation du service de gestion de preuve du P.S.G.P. dont il bénéficie par l'intermédiaire du Client. Le Contractant doit tenir secret les moyens d'identification mis à sa disposition par le Client pour l'utilisation du service.

Le Client doit vérifier que les coordonnées qu'il a communiquées à l'A.C pour le compte du Contractant sont valides et il doit porter à la connaissance de l'A.C. toute modification qui leur serait apportée.

## **8.2. Responsabilité des acteurs en matière de gestion de la preuve**

### 1- Responsabilité du P.S.G.P

Les contours, limitations et exonérations de responsabilité du P.S.G.P figurent dans les documents contractuels du P.S.G.P (contrat avec le client, conditions d'utilisation, convention de service).

### 2- Responsabilité de l'AH

L'A.H. est tenue responsable des conséquences dommageables dans le cadre :

- des préjudices subis par le Client et/ou par le Contractant et résultant de dysfonctionnement du matériel utilisé par l'A.H. ;
- de la précision et de l'intégrité des Jetons qu'elle délivre ;
- de la fourniture de Jetons d'horodatage basés sur une heure fiable ;
- de s'assurer que tous les aspects des services, exploitation et infrastructures liés aux Jetons d'horodatage sont réalisés selon les exigences, objectifs et garanties de cette politique.

3-Responsabilité des A.C Les A.C. sont tenues responsables du respect de leur P.C. quant à leur mise en œuvre. En cas de défaillance de l'une ou plusieurs des A.C. ayant un impact sur le service de gestion de preuve du P.S.G.P. la responsabilité du P.S.G.P. ne pourra être recherchée.

### 4-Responsabilité du Client

Les contours, limitations et exonérations de responsabilité du Client figurent dans les documents contractuels du P.S.G.P (contrat avec le client, Conditions d'utilisation, Convention de service), ce dernier ayant en charge d'effectuer la répartition des responsabilités vis-à-vis des Distributeurs et des Manipulateurs dans le cadre des prestations d'enregistrement. Seul le Client est responsable des agissements des Distributeurs et des Manipulateurs vis-à-vis du P.S.G.P.

## **9. Confidentialité des données à caractère personnel**

La loi n°78-17 du 6 janvier 1978, relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel s'applique à tous les documents détenus par le P.S.G.P (site de la CNIL <http://www.cnil.fr>).

En vertu de la loi, les Clients et les Contractants disposent d'un droit d'accès, de rectification et d'opposition aux traitements de données qui les concernent. Le P.S.G.P. doit respecter rigoureusement toutes les prescriptions légales et réglementaires applicables et indiquer sur son site WEB, les modalités concrètes d'exercice des droits.

La P.G.P. doit être interprétée de manière à respecter les principes fondamentaux en matière de protection des données à caractère personnel consacrés dans la loi, les directives européennes et toute autre convention internationale entrée en vigueur. Toutes les données collectées et détenues par le P.S.G.P. sur une personne physique (par exemple : procédure d'enregistrement, autres événements consignés, correspondances échangées



**LRE TRUST**



entre le Client et le P.S.G.P., etc.) sont considérées comme confidentielles et ne doivent pas être divulguées sans avoir obtenu le consentement préalable du Client.

Les entités impliquées dans le processus de gestion de preuve font leur affaire du respect des dispositions de la loi Informatique, fichiers et libertés et fourniront à première demande au P.S.G.P. leurs déclarations ou demandes d'autorisations auprès de la CNIL.

En outre, elles s'engagent à déclarer le P.S.G.P. comme tiers autorisé au sens de la CNIL. 3.4 Secret des correspondances et interceptions. Le secret des correspondances émises par voie des communications électroniques est garanti par la loi française. En cas d'atteinte, toute violation est punie par l'article 226-15 du code pénal pour celles commises par une personne et par l'article 432-9 du code pénal pour celles commises par une personne dépositaire de l'autorité publique.

D'une façon générale, aucun salarié du P.S.G.P. et aucun collaborateur ou sous-traitant, dans le cadre de leur participation à l'activité de gestion de preuve, n'a le droit d'intercepter, d'ouvrir, de détourner, de divulguer, de rechercher ou d'utiliser les documents soumis au P.S.G.P., sauf dans les cas prévus dans la présente politique, ou dans le cadre du régime des interceptions ordonnées par l'autorité judiciaire ou des interceptions de sécurité en vertu de la loi n°91-646 du 10 juillet 1991.

## **10. Droits relatifs à la propriété intellectuelle**

Tous les droits de propriété intellectuelle détenus par le P.S.G.P. sur l'offre LRE TRUST sont protégés par la loi, règlements et autres conventions internationales applicables.

Ils sont susceptibles d'entraîner la responsabilité civile et pénale en cas de leur non-respect. Par exemple, conformément au droit applicable les bases de données réalisées par le P.S.G.P. sont protégées.

La contrefaçon de marques de fabrique, de commerce et de services, dessins et modèles, signes distinctif, droits d'auteur (par exemple : logiciels, pages web, bases de données, textes originaux...) est sanctionnée par les articles L. 716-1 et suivants du Code de la propriété intellectuelle.

Dispositions pénales : en vertu des articles 323-1 à 323-7 du Code pénal, applicables lorsqu'une infraction est commise sur le territoire français, les atteintes et les tentatives d'atteintes aux systèmes de traitement automatisé de données sont sanctionnées, notamment l'accès et le maintien frauduleux, les modifications, les altérations et le piratage de données, etc. Les peines encourues varient de 2 à 5 ans d'emprisonnement et d'une amende allant de 30.000 à 375.000 euros pour les personnes morales.



## 11. Mesures de sécurité, des procédures et du personnel

Le service de gestion de preuve doit respecter l'ensemble des mesures de sécurités telles que décrites dans la PGSSI du P.S.G.P.

En particulier :

- Le service de gestion de preuve doit être offert avec une garantie de continuité de service et la mise en œuvre de moyens de sécurité, de procédures et du personnel adaptés.
- Les contrôles d'accès doivent permettre une parfaite identification des personnes quant aux actions qu'elles réalisent en fonction de leur habilitation. Les moyens mis en œuvre afin de respecter les objectifs de sécurité sont détaillés en grande partie dans la D.P.G.P qui sera disponible sur demande motivée du Client.

Le P.S.G.P s'est engagé dans une démarche SMSI avec alignement sur la norme ISO27001:2013. A ce titre, la gestion de la sécurité est incluse dans le cœur du système de management mis en place.

### 1- Gestion des Risques de Sécurité

*Démarche et méthodologie d'appréciation des risques :*

Le processus d'appréciation des risques de sécurité de l'information formalise la démarche standard appliquée pour la prestation projet, la méthodologie est basée sur la norme ISO 27005.

La documentation de l'analyse des risques incorpore l'ensemble des risques du périmètre :

- Les risques transverses à toutes les prestations hébergées par le P.S.G.P

Risques liés à la sécurité des Datacenter, aux processus d'exploitation, etc.

- Les risques spécifiques aux SI du projet/de la prestation

Les risques résiduels importants identifiés dans les résultats de l'analyse de risques sont présentés au DP qui doit décider formellement de la suite à donner : acceptation ou refus (dans le cas d'un refus, soit les sources de risques sont supprimées, soit les mesures de réduction sont revues).

Tout risque résiduel important accepté par le P.S.G.P pourra être porté à la connaissance du client.

La révision et la présentation de l'analyse sont effectuées au moins une fois par an, ou en cas de changement important sur un SI de la prestation, sur une exigence réglementaire et/ou contractuelle.

### 2- Risques liés aux exceptions de sécurité

Tout besoin justifié de dérogation à une ou plusieurs règles ou exigences de sécurité, doit faire l'objet d'une demande d'exception dûment documentée à l'aide du formulaire spécifique.

Chaque demande d'exception de sécurité SI est documentée pour que toutes les parties prenantes au projet puissent signaler tout ce qui sort du cadre fonctionnel et technique défini dans le contexte du projet et pouvant affecter de quelque manière que ce soit la sécurité de la prestation, le Client ou le P.S.G.P.

Le CSSI, doit intégrer dans l'appréciation des risques sécurité de la prestation les risques résiduels identifiés dans chaque demande d'exception / dérogation.

### 3- Politique de la sécurité de l'information

#### a. Politique de Sécurité

Le document Politique Générale de Sécurité des SI (PGSSI) décrit les principes généraux de la politique de sécurité des systèmes d'information du P.S.G.P.



La sécurité des systèmes d'information (SSI) participe activement au projet d'entreprise caractérisé dans la politique managériale énoncée par la Direction Générale et une feuille de route SSI annuelle.

La PGSSI a pour objectif de préciser les enjeux de la SSI, définir les principes et les règles de mise en œuvre au sein des entités métier et support, clarifier les responsabilités et organiser la gouvernance de la sécurité des systèmes d'information en tenant compte des évolutions structurelles du P.S.G.P.

Elle est élaborée en cohérence avec le document de gouvernance de la SSI.

Tous les principes et règles sont précisés dans une hiérarchie de documents (notamment les Politiques Générales de Sécurité – PGS) dont la PGSSI constitue le document fondateur.

## b. Organisation de la Sécurité de l'information

### *I. Fonctions et responsabilités liées à la SSI*

L'organisation du P.S.G.P est définie dans des organigrammes tenus à jour, validés par la Direction Générale.

Les différents responsable sécurité ainsi que l'équipe de sécurité opérationnelle sont rattachés au RSSI, et celui-ci reporte au Directeur des Systèmes d'Information.

Une chaîne fonctionnelle de sécurité de l'information est mise en place, elle est composée d'un ensemble de correspondants sécurité des SI (CSSI) nommés dans chaque entité opérationnelle (Business Unit) et hiérarchiquement rattaché à un Responsable de l'entité.

Plusieurs instances de pilotage de la SSI sont mises en place. L'organisation mise en œuvre pour gérer la sécurité des SI (responsabilités, comitologie, etc.) est détaillée dans le document de gouvernance de la SSI validé par la Direction Générale.

*II. Séparation des tâches* L'organisation de la SSI repose sur le principe de la séparation des pouvoirs. Les fonctions de décision et de contrôle permanent sont placées sous la responsabilité du RSSI du P.S.G.P et des équipes SSI et se distinguent des fonctions de mise en application (équipes métier et support).

### *III. Relations avec les autorités*

Le P.S.G.P entretient des relations dans le cadre de ses obligations légales et réglementaires avec la CNIL (données personnelles) et l'ASIP Santé (hébergement de données de santé à caractère personnel).

Le P.S.G.P tient à jour une liste de contacts afin de pouvoir faire appel à la force publique et à l'office central de lutte contre la criminalité liée aux technologies de l'information et de la communication. Les relations avec les différentes autorités sont gérées en coordination avec la Direction Juridique du P.S.G.P.

### *IV. Politique en matière d'appareils mobiles*

La Politique Générale de Sécurité « Equipements de travail » décrit les règles appliquées pour sécuriser les équipements mobiles.

## c. Sécurité des ressources humaines I.

### *Sélection des candidats*

Les modalités d'embauche sont formalisées par le service RH du P.S.G.P, au travers de processus et procédures documentées. Ces modalités prennent en compte les exigences de sécurité, en fonction des exigences métier des critères de vérification d'informations concernant les candidats, dans le respect des lois et de la réglementation (notamment la confirmation de l'identité du candidat, de ses formations et de son parcours professionnel).

Les modalités d'embauche du P.S.G.P incluent systématiquement la fourniture de l'extrait n°3 du casier judiciaire, dans le respect des textes en vigueur.



## *II. Termes et conditions d'embauche*

Une charte de bonnes pratiques est transmise à chaque acteur du P.S.G.P à son arrivée, et son contenu est rappelé lors des campagnes d'information ou de sensibilisation régulières.

Le contenu de la charte reprend les principes et règles que doit suivre tout acteur du P.S.G.P en conformité avec la Politique Générale de Sécurité des SI (PGSSI) et les Politiques Générales de Sécurité (PGS).

## *III. Responsabilités de la direction*

Le respect des Politiques Générales de Sécurité (PGS) par les salariés du P.S.G.P et ses contractants est assuré par la mise à disposition d'une charte de bonnes pratiques de sécurité de l'information.

Les responsables hiérarchiques et les chefs de projet ont la mission de rappeler les règles et bonnes pratiques aux personnes sous leur responsabilité.

## *IV. Sensibilisation, apprentissage et formation à la sécurité de l'information*

Des séances de sensibilisation sont réalisées sur les risques, sur la réglementation applicable et le corpus de Politiques Générales de Sécurité (PGS).

Un plan annuel de formation et de sensibilisation à la sécurité de l'information est tenu à jour pour tenir compte de l'évolution des besoins de compétence du personnel.

Ce plan comprend des sessions adaptées et organisées régulièrement (ex: formation OWASP pour les développeurs, administration systèmes/réseaux pour les exploitants, réglementation sur les données de santé dont les procédures opérationnelles du Médecin Hébergeur, etc.).

Le suivi des actions de sensibilisation et de formation est documenté (tableau de bord, feuilles d'émargement).

Les acteurs du P.S.G.P sont sensibilisés et formés aux règles et comportements à respecter en termes de sécurité de l'information. Des informations leur sont fournies dans les chartes et les livrets d'accueil.

Les administrateurs et exploitants techniques et fonctionnels sont formés à l'administration des plateformes à leur charge.

## *V. Processus disciplinaire*

Le règlement intérieur du P.S.G.P qualifie le manquement aux règles de sécurité, la protection du secret, les devoirs de l'utilisateur sur ses droits d'accès logiques et l'usage des logiciels au sein de la société.

Toute violation du règlement, des chartes ou des PGS peut entraîner des mesures disciplinaires, qui peuvent aller de l'avertissement verbal (avec ou sans enregistrement dans le fichier du personnel) jusqu'au licenciement. C'est la gravité de l'incident qui déterminera la sévérité des mesures prises.

Les responsabilités relatives aux modifications et fins des contrats de travail sont encadrées par le service RH du P.S.G.P selon les dispositions du contrat d'embauche, de la convention collective et du règlement intérieur.

### *d. Cryptographie*

#### *1. Politique d'utilisation des mesures cryptographiques*

Une politique générale de sécurité sur l'usage des moyens cryptographiques est formalisée et tient compte des recommandations en matière de cryptographie émises par l'ANSSI (Agence Nationale de Sécurité des SI)

La documentation technique de la prestation (spécifications, dossier d'architecture, dossier d'exploitation et procédures de l'équipe de sécurité opérationnelle) formalisent les mécanismes logiciels et l'architecture faisant appel à des mesures cryptographiques, dont les spécificités retenues et les processus organisationnels de gestion de ces mesures.



## II. Gestion des clés

Les règles générales de gestion des types de clés de chiffrement et de leurs cycles de vie sont définies dans la politique générale de sécurité et dans le cas de spécificités retenues pour le projet, elles sont documentées dans les spécifications et le dossier d'architecture de la prestation.

### e. Sécurité physique et environnementale I.

#### *Périmètre de sécurité physique*

Un découpage de chaque site du P.S.G.P en zones physiques de sécurité a été effectué. Des règles fixent les conditions d'accès à ces différentes zones.

Chaque zone sur les sites possède un ensemble cohérent de système de lutte contre l'intrusion physique en rapport avec le niveau d'exigence de sécurité.

Les bâtiments sont entretenus par des sociétés extérieures spécialisées dans leur domaine. Des contrats de maintenance garantissent la bonne réalisation des travaux dont la mise aux normes des tableaux électriques, des ascenseurs, des détecteurs incendie, l'entretien des chauffages, de la climatisation, du toit.

Sur les Datacenter, du personnel qualifié est présent sur site 24h/24 et 7J/7, et en HO et HNO, du personnel de surveillance est présent et dispose de toutes les consignes nécessaires pour lancer les actions en cas d'incident.

Une convention de service, définissant les responsabilités mutuelles en matière de sécurité, est établie entre les tiers qui gèrent en partie ces Datacenter et le P.S.G.P.

## II. Contrôles d'accès physique

L'accès physique aux sites et locaux est maîtrisé et fait l'objet de mesures de sécurité adaptées, notamment :

- Les accès à toutes les zones sont sous contrôle. La délivrance des moyens d'accès physique respecte une procédure formelle permettant de s'assurer de l'identité de la personne, s'appuyant sur le processus d'arrivée et de départ d'une personne.
- Toute autre personne, titulaire ou non d'un moyen d'accès, doit se soumettre aux formalités de contrôle en vigueur sur le site.
- Tous les visiteurs externes doivent se présenter à l'accueil. L'attribution d'un badge d'accès temporaire est soumise à la présentation d'une pièce d'identité. Ce badge leur permet de circuler sur le site (à l'exception des locaux sensibles) sous le contrôle de leur hôte.
- L'accès aux zones de traitement informatique (dont celles situées en Datacenter) est limité à un nombre restreint de personnes dont le besoin est justifié par leur travail.
- Le personnel autre que celui explicitement autorisé et habilité, mais néanmoins appelé à intervenir dans les zones de traitement informatique, intervient obligatoirement sous surveillance permanente.

### III. Sécurisation des bureaux, des salles et des équipements

De nombreuses formations comme l'habilitation électrique, la formation de secouristes ou bien la formation de sécurité incendie garantissent des équipes opérationnelles en cas de besoin.

Les administrateurs techniques et fonctionnels LRE TRUST sont situés dans des locaux protégés par les mesures de contrôle d'accès en vigueur.

Le personnel chargé du développement est localisé dans des bâtiments appartenant à LRE TRUST et protégés par les mesures de contrôle d'accès en vigueur sur le site.

## IV. Protection contre les menaces extérieures et environnementales

Un dispositif de vidéosurveillance et une alarme permet de détecter une intrusion ou une tentative d'intrusion. Une procédure décrit les alertes et les escalades possibles (utilisation du processus Business Continuity - BC ; Rouge ou Noir).



**LRE TRUST**



Une société de gardiennage est en liaison permanente avec ce système et intervient sur le site en cas de besoin.

En ce qui concerne les événements climatiques, les bâtiments sont entretenus par des sociétés extérieures spécialisées dans leur domaine. Des contrats de maintenance garantissent la bonne réalisation des travaux. Une équipe interne a une habilitation électrique (valable trois ans) pour les petits travaux.

Un dispositif complet d'alarme incendie est en place avec des extincteurs, des plans d'évacuation, des personnes sont membre de l'équipe sécurité incendie (formation annuelle) et des exercices incendie effectués tous les semestres.

#### *V. Travail dans les zones sécurisées*

Les principales zones sécurisées sont celles hébergeant les données de la prestation. Ces zones dédiées à LRE TRUST sont localisées dans les Datacenter. Les accès et le travail dans ces zones est documenté et géré via des procédures formalisées.

Les zones qui hébergent les différents personnels de LRE TRUST sont localisées sur des sites de LRE TRUST. Les accès et le travail dans ces zones sont documentés et gérés via des procédures formalisées.

Les responsables de ces sites sont responsables de tenir cette documentation à jour.

#### *VI. Zones de livraison et de chargement*

Les zones spécifiques de livraison et de chargement des Datacenter sont contrôlées et isolées des salles de traitements informatiques. Il n'y a pas de zone d'accès public.



## 12. Administration de la PGP

### 12.1. Évolution de la P.G.P

En tant que document de référence du service de gestion de preuve, la P.G.P est tenue à jour aussi bien vis-à-vis des évolutions internes qu'externes au service de gestion de preuve. Les principes mis en œuvre au sein du service de gestion de preuve sont ainsi en permanence conformes à ceux présentés dans la P.G.P. En cas d'écart constaté, soit la mise en œuvre des principes est corrigée pour être conforme à la P.G.P, soit la P.G.P est corrigée pour être conforme aux principes effectivement mis en œuvre.

L'évolution de la P.G.P est placée sous la responsabilité du P.S.G.P au travers d'un Comité de Suivi.

#### **Comité de Suivi, composition et fréquence de réunion** Ce

Comité est constitué :

- du service informatique,
- du service des risques, -
- du service juridique.

Il se réunit au moins une fois par an.

#### **Procédures de suivi des modifications à appliquer en cas d'évolution**

Les demandes de modification intervenant autour de la P.G.P. peuvent être de natures différentes :

- Modification des objectifs de sécurité de LRE TRUST, évolution de sa structure, de son organisation ou de ses activités,
- Changement de la législation et/ou de la réglementation, nouvelles normes,
- Evolution des menaces et des enjeux liés au système d'information,
- Adaptation ou évolution du périmètre fonctionnel, technologique ou organisationnel,
- Correction suite à une non-conformité...

#### **Procédures en cas de veille réglementaire et juridique**

La veille réglementaire vise à contrôler la prise en compte des impacts des évolutions législatives et réglementaires en matière de gestion de preuve sur le système d'information du P.S.G.P.

LRE TRUST assure cette veille de façon globale. Néanmoins chaque service de LRE TRUST conserve son expertise au travers de son métier et s'engage à avertir l'Autorité de Gestion de Preuve (ci-après dénommée l'A.G.P) de toute modification en la matière.

L'A.G.P. assurera la mise en œuvre des modifications induites sur le système d'information suite à la réunion du Comité de suivi tel que défini précédemment.

#### **Procédure en cas d'évolution fonctionnelle / technique / technologique**

Les demandes d'évolutions fonctionnelles sont envoyées à l'A.G.P. par les usagers ou toute autre entité ou partie du service de gestion de preuve.

Toute demande est transmise au Comité de Suivi afin d'analyser de la nécessité d'actualiser la Politique e gestion de preuve.

Le Comité identifie si la demande présente un intérêt et décide du lancement de l'instruction de la demande ou de son rejet.



## 12.2. Procédures de modifications

### **Délais de préavis**

- Le responsable du P.S.G.P doit donner un préavis de quatre-vingt-dix (90) jours aux A.C., à l'A.H., aux P.S.A. en relations contractuelles avec le P.S.G.P. et de trente (30) jours aux Clients et Contractants avant de procéder à tout changement de la présente politique qui, selon l'évaluation du responsable de la politique, ont un impact majeur sur eux.
- Le responsable du P.S.G.P. doit donner un préavis de trente (30) jours aux A.C., à l'A.H., aux P.S.A. en relations contractuelles avec le P.S.G.P., et de (15) jours aux Clients et aux Contractants avant de procéder à tout changement de la présente politique qui, selon l'évaluation du responsable de la politique, ont un impact mineur sur eux.
- Le responsable du P.S.G.P. peut modifier la présente politique sans préavis aux Clients et aux Contractants lorsque, selon l'évaluation du responsable de la politique, ces modifications n'ont aucun impact sur eux.

**Forme de diffusion des avis** Dans les cas nécessitant un préavis, le responsable du P.S.G.P. doit aviser les A.C., l'A.H., les P.S.A. en relations avec le P.S.G.P., les Clients, des modifications apportées à la politique, en diffusant les changements sur le site web du P.S.G.P. et par message électronique. Lorsque l'avis est à destination des A.C., de l'A.H et des P.S.A. en relations contractuelles avec le P.S.G.P., le préavis est expressément communiqué.

Lorsque l'avis est à destination des Clients, le préavis est communiqué par message électronique si les changements ont un impact majeur, et diffusé sur le site web du P.S.G.P. dans tous les autres cas.

### **Période de commentaires**

Les personnes désirant se prononcer sur les modifications doivent faire parvenir leurs commentaires au responsable de la politique dans des délais inférieurs à la moitié des délais de préavis fixés au §0

**Traitement des commentaires** Aucune exigence particulière.

### **Modifications nécessitant l'adoption d'une nouvelle politique**

Si un changement de politique a, selon l'évaluation du Responsable de la politique, un impact majeur sur un nombre important de Clients, le Responsable de la politique peut, à sa discrétion, instituer une nouvelle politique avec un nouvel identificateur d'objet (OID).

## 12.3. Procédure de diffusion et de publication de la P.G.P. et autres documents

### **Diffusion de la P.G.P.**

La P.G.P. est diffusée à l'ensemble des parties concernées par le service de gestion de preuve afin de permettre à chaque partie de prendre connaissance des principes que le P.S.G.P. s'engage à respecter dans le cadre de la délivrance du service.

### **Informations publiées**

La P.G.P. et les Conditions d'utilisation du service de gestion de preuve, sont disponibles sur le site Internet du P.S.G.P. à l'adresse suivante : <http://www.lre.ma/cgupg>. Elles peuvent également être communiquées dans le cadre d'une négociation commerciale.

### ***Fréquence de diffusion***

La publication de la P.G.P. sera effectuée après chaque modification.

### ***Contrôle de l'accès***

La P.G.P. ne sera accessible, pour création ou modification, qu'au seul personnel autorisé du P.S.G.P, et ce à travers des contrôles d'accès appropriés.

Le service de publication des informations est responsable des conditions de mises en œuvre des mesures de sécurité aux fins de contrôler l'accès aux informations publiées.

## **12.4. Contrôle de l'application de la P.G.P.**

Le P.S.G.P. met en œuvre des procédures et moyens de contrôle interne de l'application et du respect, par les différentes entités intervenant dans le service de gestion de preuve, des principes définis dans la P.G.P. et déclinés dans la D.P.G.P.

## **12.5. Contrôle de conformité des pratiques du P.S.G.P.**

Un contrôle de conformité permet de déterminer si le comportement réel du P.S.G.P. satisfait aux exigences de la présente Politique.

Cette vérification comprend :

- l'examen de la validité du processus de vérification que le P.S.G.P. a mis en place pour valider la qualité de ses services ;
- une comparaison entre les pratiques du P.S.G.P. décrites dans ses procédures et la conformité à ces procédures.

Ce contrôle de conformité est fait sur demande de l'autorité judiciaire ou sur demande du P.S.G.P. elle-même, selon les conditions précisées dans ses procédures.