POLITIQUE ET PRATIQUES DU SERVICE « LA LETTRE RECOMMANDEE ELECTRONIQUE » DE LA POSTE
Version 1.1

Table des matières

1 Introduction

1.1 Définitions

- **API :** est un acronyme pour « Applications Programming Interface ». Une API est une interface de programmation qui permet à une application de s'interfacer avec une autre application pour échanger des données. Une API est proposée par le propriétaire du programme à un Editeur qui consomme cette API pour bénéficier des services qu'elle peut rendre.

- **API Lettre recommandée :** L'API Lettre recommandée de La Poste permet à l'application de s'interfacer avec le système d'information de La Poste pour effectuer des commandes de Lettres recommandées en ligne (hybrides) ou de Lettres recommandées électroniques.

- **Client :** la personne morale signataire du Contrat conclu avec La Poste

- **CGU :** Les conditions générales d'utilisation (CGU) sont un document annexé au contrat régissant les conditions et modalités d'utilisation du service recommandé électronique de La Poste.

- **Consommateur de l'API Lettre recommandée :** le Client (direct ou intermédiaire) ayant intégré techniquement l'API Lettre recommandée dans son système d'information.

- **Destinataire :** personne morale ou physique détentrice d'un MIE qui reçoit la Lettre recommandée électronique

- **DSI :** Direction des Systèmes d'information de la Poste

- **Expéditeur :** personne morale qui s'authentifie avec un certificat et qui réalise l'envoi de Lettre recommandée électronique

- **La Poste – BSCC :** Branche Service Courrier Colis du groupe La Poste

- **L'IN :** L'identité numérique La Poste exclusivement pour les particuliers. Elle s'obtient gratuitement sur laposte.fr/lidentitenumerique

- **LRE :** Lettre recommandée électronique

- **MIE :** moyen d'identification électronique

- **OID :** Les OID (pour Object Identifier) sont des identifiants universels, représentés sous la forme d'une suite d'entiers. Ils sont organisés sous forme hiérarchique. L'OID constitue une sorte de matricule pour le service de confiance concerné.

- **Pli :** correspond à une (1) Lettre recommandée électronique

- **Progiciel :** désigne un logiciel applicatif aux multiples fonctions, composé d'un ensemble de programmes paramétrables et destiné à être utilisé par une large clientèle. Le progiciel peut aussi être spécialisé et adresser une corporation de métier comme avocats, notaires, agence immobilière...

- **SRE :** service de recommandé électronique. Le SRE de La Poste se dénomme « LA Lettre recommandée électronique »

- **Service client** : disponible par téléphone au 3634 (0.34€ TTC/min à partir d'un téléphone fixe) pour les professionnels et au 3631 (numéro non surtaxé) pour les particuliers

- **Unité d'affaire Lettre recommandée (UA LR)** : service au sein de la BSCC La Poste en charge des produits de la gamme lettre recommandée.

1.2 Présentation générale

Le groupe La Poste, opérateur historique de la Lettre recommandée et prestataire de Service de confiance qualifié sur l'horodatage électronique, propose un nouveau service de recommandée électronique.

Ce service a pour vocation d'être qualifié au sens de l'article 44 du règlement européen eIDAS, et d'être conforme au Décret no 2018-347 du 9 mai 2018 relatif à la lettre recommandée électronique afin de garantir son équivalence juridique avec l'envoi d'une lettre recommandée papier.

La présente Politique définit les engagements de La Poste dans le cadre de la fourniture de services de lettres recommandées électroniques qualifiées au sens de l'article 44 du règlement européen eIDAS.

1.3 Identification du document

La présente politique est identifiée par l'OID suivant : 1.2.250.1.8.1.1.2.1.1

1.4 Gestion de la politique

1.4.1 Entité gérant la politique

L'entité gérant la présente politique est le comité de pilotage (COPIL) du service LA Lettre recommandée électronique au sein du Groupe La Poste, présidé par le directeur de l'Unité d'Affaire Courrier.

1.4.2 Point de contact

Groupe La Poste Branche Service Colis Courrier (BSCC) 9, rue du Colonel Pierre Avia 75015 Paris lrmarket.ualr@laposte.fr Service client disponible par téléphone : au 3634 (0.34€ TTC/min à partir d'un téléphone fixe) pour les professionnels et au 3631 (numéro non surtaxé) pour les particuliers

1.4.3 Procédure d'approbation de la politique

La politique est approuvée après examen et relecture par membres du COPIL. Cette relecture a pour objectif d'assurer :

- La conformité de la politique avec les exigences réglementaires et normatives portant sur la fourniture d'un service de recommandé électronique qualifié.
- La concordance entre les engagements exprimés dans la politique et les moyens techniques et organisationnels mis en œuvre par La Poste – BSCC et ses partenaires.
- Que toute modification importante dans la fourniture du service de confiance qualifié (y compris celles entrainant des changements dans la liste de confiance) fasse l'objet d'une information de l'ANSSI selon les modalités décrites dans les procédures de qualification.

1.4.4 Amendements à la politique

La Poste – BSCC contrôle que tout projet de modification de sa politique reste conforme aux exigences réglementaires et normatives applicables.

1.4.4.1 Procédures d'amendement

Hormis les corrections induites par les audits ou des corrections mineures (erreurs, oublis, précisions supplémentaires…), les amendements pressentis à la présente politique portent sur :

- L'extension du service de recommandé électronique qualifié à d'autres catégories d'utilisateurs et d'autres modalités d'identification
- L'acceptation ou la mise en œuvre de nouveaux moyens d'identification électronique
- Des changements d'ordre technique et fonctionnel

Avant tout changement effectif du service (passage en production), La Poste – BSCC fait réaliser une analyse d'impact afin de déterminer si les évolutions ont une incidence sur la conformité de l'offre qualifiée, et si celle-ci est majeure (impliquant un changement d'OID). L'analyse d'impact peut, à cette occasion, être soumise à l'ANSSI et à l'organisme de certification pour avis ou commentaire.

Le cas échéant, la politique est mise à jour, approuvée et publiée avant toute mise en œuvre. Les CGU sont amendées concomitamment si besoin.

1.4.4.2 Mécanisme et période d'information sur les amendements

La Poste – BSCC adressera annuellement à l'ANSSI une synthèse de l'ensemble des modifications apportées à la fourniture de ses services de confiance qualifiés.

1.4.4.3 Circonstances selon lesquelles l'OID doit être changé

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

1.5 Documents associés

1.5.1 Politique d'horodatage

La date et l'heure d'envoi, de réception et toute modification des données doivent être indiquées par un horodatage électronique qualifié.

Politique d'horodatage en vigueur : *Politique d'Horodatage électronique de La Poste*, version 6.0a, OID : 1.2.250.1.8.1.1.1.1.6.

1.5.2 Politique de certification du cachet électronique

Politique de certification en vigueur : *Politique de certification Certinomis Prime CA*, OID : 1.2.250.1.86.2.3.3.22.1.

1.5.3 Politique de scellement électronique

Politique de scellement en vigueur : *Politique de Signature électronique de La Poste* en version 3.0 du 13 décembre 2018. OID : 1.2.250.1.8.1.1.3.1.6.1.

1.5.4 Conditions générales d'utilisation

Le Service de Recommandée Electronique (SRE) de La Poste « LA Lettre recommandée électronique » est accessible par le biais d'une API nommée API Lettre recommandée.

Les clients directs peuvent directement intégrer l'API dans leur propre système d'information par le biais d'un développement informatique. L'API peut être aussi intégrée par des Editeurs et être exposés dans des progiciels métiers pour élargir les fonctionnalités de leur progiciel.

Les CGU applicables sont mises à disposition du client lors de la signature du contrat et sont disponibles sur https://www.assistant-courrier.laposte.fr/ (portail entreprise de la BSCC).

1.5.5 Documents normatifs

[ANSSI_LRE]	*Services d'envoi recommandé électronique qualifiés – Critères d'évaluation de la conformité au règlement eIDAS,* Version 1.0 du 3 janvier 2017 https://www.ssi.gouv.fr/uploads/2016/06/eidas_envoi-recommande-electronique-qualifie_v1.0_anssi.PDF
[ANSSI_PSCO]	*Prestataires de services de confiance qualifiés – Critères d'évaluation de la conformité au règlement eIDAS,* Version 1.2 du 5 juillet 2017
[EN_319401]	*ETSI EN 319 401 V2.2.1 (2018-04) Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.*

[GDPR]	*Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016* https://www.cnil.fr/fr/reglement-europeen-protection-donnees
[EIDAS]	*Règlement (UE) N° 910/2014 du Parlement européen et du conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE*
[décretLRE]	*Décret n° 2018-347 du 9 mai 2018 relatif à la lettre recommandée électronique*

1.6 Entités intervenant dans le service de recommandé électronique

1.6.1 Prestataire du service de recommandé électronique (PSRE)

Le prestataire du service de recommandé électronique (PSRE) est La Poste – BSCC.

1.6.2 Opérateur du service de recommandé électronique (OSRE)

L'opérateur du service de recommandé électronique (OSRE) est La Poste – BSCC et fait appel à Docapost.

1.6.3 Prestataire d'horodatage électronique (PSHE)

Le prestataire d'horodatage électronique (PSHE) est La Poste, représentée par la DSI Groupe de La Poste.

1.6.4 Prestataire de cachet électronique

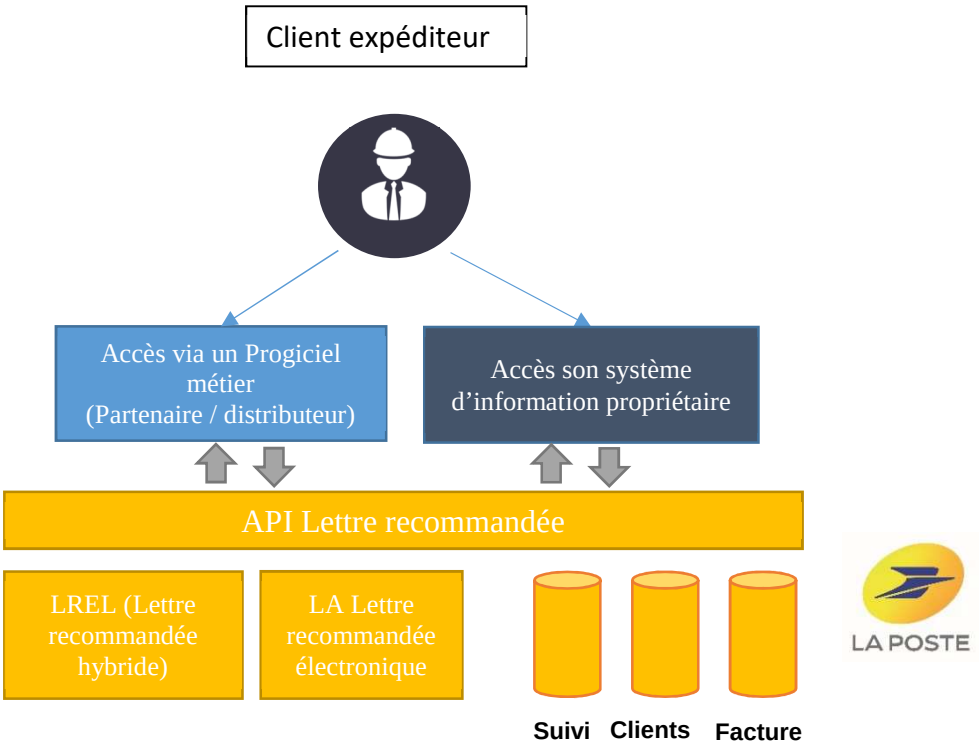
Le cachet électronique utilisé dans le cadre du SRE « LA lettre recommandée électronique » est le Cachet Électronique de La Poste dont le prestataire est La Poste, représentée par la DSI Groupe de La Poste.

1.6.5 Utilisateurs : expéditeurs et destinataires

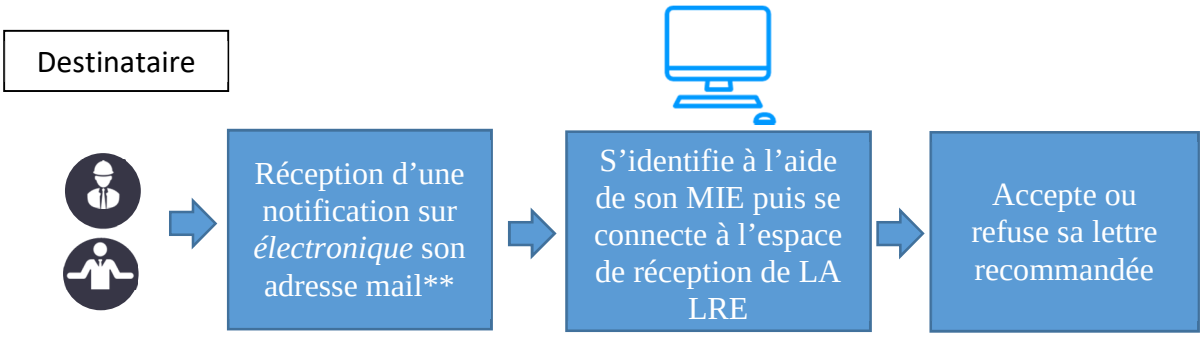
Les utilisateurs du service sont les expéditeurs et destinataires de recommandés électronique.

- Les expéditeurs de recommandé électronique sont uniquement des clients Entreprises (personnes morales) et ont accès au SRE de La Poste soit après avoir directement

intégré l'API Lettre recommandée dans leur propre SI soit par l'intermédiaire d'un logiciel métier qui a au préalable fait l'intégration de l'API Lettre recommandée.



– Les destinataires peuvent être des professionnels ou des particuliers*. Le destinataire est notifié par mail de l'arrivée d'une Lettre recommandée à son attention et réceptionne sa Lettre recommandée via l'IHM de réception.



** Le SRE LA LR électronique sera ouvert aux particuliers détenteurs de certificats ou de l'IN La Poste dès que l'IN sera qualifiée en tant qu'identité numérique substantielle.*

***le destinataire particulier doit au préalable avec consenti à l'envoi numérique de Lettre recommandée conformément au décret LRE (Décret no 2018-347 du 9 mai 2018 relatif à la lettre recommandée électronique)*

- Les moyens d'identification électroniques sont décrits au paragraphe « 3 Identification »

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

2.1 Entités chargées de la mise à disposition des informations

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

Les informations sont publiées à l'adresse suivante : https://www.assistant-courrier.laposte.fr/api-lettre-recommandee

2.2 Informations devant être publiées

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

- Le présent document, décrivant la politique et les pratiques du service de recommandé électronique ;
- Les documents associés mentionnés au 1.5.1, 1.5.2 et 1.5.3, ou, dans le cas où un de ces documents serait maintenu et publié par un tiers, une référence univoque (URL, OID, etc.) à celui-ci et un point de publication ;
- Les conditions générales d'utilisation du service (1.5.4).

2.3 Délais et fréquences de publication

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

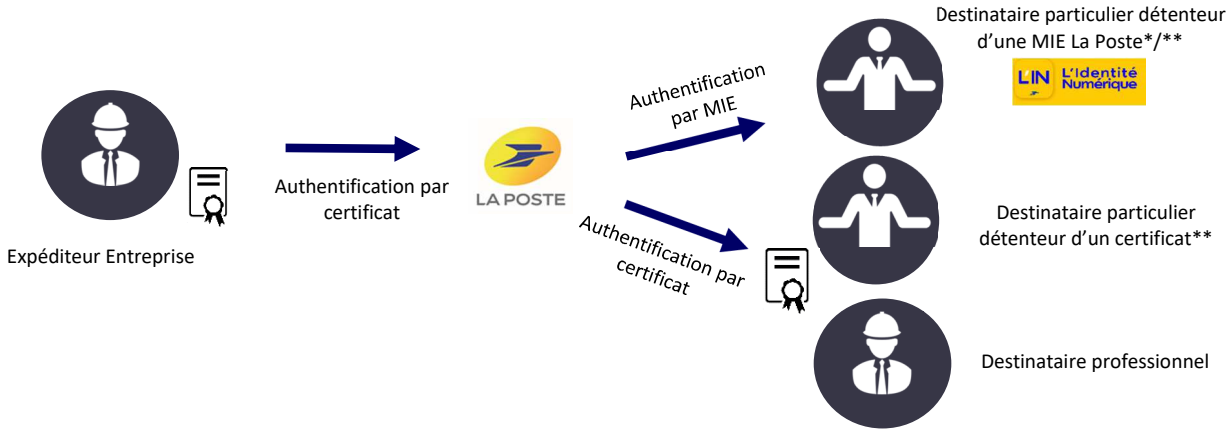
Les systèmes publiant ces informations doivent au moins être disponibles les jours ouvrés.

2.4 Contrôle d'accès aux informations publiées

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

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

3 Identification



**dès la date d'entrée en vigueur de sa qualification en tant qu'identité numérique substantielle*

*** A noter : Le SRE LA LR électronique sera ouvert aux particuliers détenteurs de certificats ou de l'IN La Poste dès que l'IN sera qualifiée en tant qu'identité numérique substantielle.*

3.1 Identification de l'expéditeur

Le service d'envoi recommandé électronique qualifié doit garantir l'identification de l'expéditeur avec un degré de confiance élevé.

- ✓ L'expéditeur (exclusivement une entreprise /personne morale) doit disposer d'un certificat électronique de cachet ou de signature dont le niveau est à minima RGS** ou qualifié eIDAS
- ✓ Parmi ce périmètre éligible, La Poste gère une liste confiance des certificats qui sont utilisables par le service. Cette liste est à disposition des utilisateurs auprès du Service Client et sur Internet sur le site www.assistantcourrier.laposte.fr.
- ✓ La Poste étudiera au cas par cas les demandes de clients disposant d'un certificat éligible mais non répertorié dans la liste de confiance.

3.1.1 Validation initiale de l'identité

L'identité de l'expéditeur est vérifiée en face-à-face dans le cadre de la délivrance de son certificat.

L'expéditeur possède alors un moyen d'authentification forte garantissant son identité avec un degré de confiance élevé.

3.1.2 Informations non vérifiées

La présente politique ne formule pas d'exigence spécifique sur le sujet.

3.1.3 Validation via un moyen d'identification électronique (MIE)

Avant toute opération relative à l'envoi d'un recommandé électronique, l'expéditeur présente son certificat pour s'authentifier. Une fois authentifié, il peut réaliser un ou plusieurs envois dans le cadre d'une même commande. Il doit s'authentifier à chaque nouvelle commande.

3.2 Identification du destinataire

Le service d'envoi recommandé électronique qualifié doit garantir l'identification du destinataire avant la fourniture des données.
Le destinataire doit disposer :

- ✓ Pour une personne morale : d'un certificat électronique d'authentification dont le niveau est à minima RGS** ou qualifié eIDAS
- ✓ Pour un particulier* :
  - o Soit d'un certificat électronique d'authentification dont le niveau est à minima RGS** ou qualifié eIDAS
  - o Soit d'une IN La Poste
- ✓ Parmi le périmètre éligible des certificats, La Poste gère une liste confiance des certificats qui sont utilisables par le service. Cette liste est à disposition des utilisateurs auprès du Service Client et sur Internet : sur www.laposte.fr pour les particuliers et www.assistantcourrier.laposte.fr pour les professionnels.
- ✓ La Poste étudiera au cas par cas les demandes de clients disposant d'un certificat éligible mais non répertorié dans la liste de confiance.

** Le SRE LA LR électronique sera ouvert aux particuliers détenteurs de certificats ou de l'IN La Poste dès que l'IN sera qualifiée en tant qu'identité numérique substantielle.*

3.2.1 Validation initiale de l'identité

Quel que soit le destinataire, qu'il soit un particulier ou un professionnel, la vérification initiale de l'identité du destinataire est réalisée en face-à-face dans le cadre de la délivrance de son certificat ou de son identité numérique d'un niveau substantiel.

Le destinataire possède alors un moyen d'authentification forte garantissant son identité avec un degré de confiance élevé.

Pour le destinataire particulier, il appartient à l'expéditeur de recueillir son consentement à l'envoi numérique.

3.2.2 Informations non vérifiées

La présente politique ne formule pas d'exigence spécifique sur le sujet.

3.2.3 Validation via un moyen d'identification électronique (MIE)

Le destinataire professionnel présente son certificat pour s'authentifier.

Le destinataire particulier s'identifie avec son compte Identité Numérique La Poste*. Il reçoit une notification de l'application L'Identité Numérique sur son smartphone. Il confirme la demande dans l'application et certifie son identité avec son code secret ou TouchID.

Une fois authentifié, le destinataire particulier ou professionnel peut alors accepter ou refuser la ou les Lettres recommandées électroniques reçues.

Le processus d'authentification dépend du MIE utilisé. La Poste contrôle que l'identité présentée est du niveau requis.

**dès la date d'entrée en vigueur de l'IN en tant qu'identité numérique substantielle qualifiée*

4 Exigences opérationnelles

4.1 Processus d'envoi

4.1.1 Processus et responsabilités pour le dépôt d'une LRE

Une LRE ne peut être envoyée que par une personne disposant :

- D'un compte client La Poste et d'un contrat lui permettant d'envoyer des LRE si le consommateur de l'API Lettre recommandée est aussi l'expéditeur ou si le consommateur de l'API Lettre recommandée est distributeur apporteur d'affaire. Le client expéditeur est facturé de ses propres consommations.

  Si l'expéditeur n'est pas le client La Poste (cas où l'expéditeur est client d'un distributeur apporteur d'affaire), l'expéditeur n'a pas besoin d'un compte client La Poste ni d'un contrat.

- D'un MIE reconnu (précisé au paragraphe 3.1)

4.1.2 Traitement du dépôt d'une commande LRE

Une commande de Lettre recommandée électronique correspond à 1 et 1 seul expéditeur professionnel, dont l'identification est issue d'un certificat (cf § 3 Identification) et est caractérisée par 3 informations obligatoires :

- Le SIREN
- La raison sociale
- L'adresse e-mail

Une commande peut comprendre 1 ou plusieurs documents, avec limite de poids maximum de 256Mo par document.

A chaque document est associé 1 ou plusieurs destinataires caractérisés par les informations obligatoires suivantes :

- ✓ Le SIREN (uniquement pour un destinataire professionnel)
- ✓ La raison sociale (pour un destinataire professionnel) ou le nom-/ prénom (pour un destinataire particulier)
- ✓ L'adresse e-mail

Après validation de la commande, les lettres sont prises en charge pour envoi et il n'est alors plus possible de rajouter des documents ou des destinataires. Une commande créée mais non validée dans un délai de 72h est réputée abandonnée ; il n'est alors plus possible de la valider.

Pour l'envoi, chaque couple document (1) / destinataire (1) constitue une (1) Lettre (ou « pli ») qui fait l'objet d'une notification et d'un suivi et d'une facturation distincts.

4.1.3 Exécution des processus d'identification et de validation du dépôt

L'expéditeur doit s'authentifier avec son MIE (3.1.3) avant tout dépôt.

Aucune vérification n'est effectuée sur le contenu du dépôt.

Une fois le dépôt terminé, la commande (soit l'ensemble des documents PDF en pièce jointe) est scellée et horodatée par La Poste. Une commande peut contenir une ou plusieurs LRE.

Lors de la soumission de la commande, La Poste attribue un identifiant de 13 caractères commençant par 5C à chaque Lettre recommandée électronique, afin que l'expéditeur puisse récupérer les éléments de suivi des plis.

4.1.4 Acceptation ou rejet de la commande

La plateforme procède à des vérifications techniques sur le format et la taille de la pièce jointe, l'adresse et le nombre de destinataire,… L'API informe l'expéditeur du succès ou de l'échec de la commande.

4.1.5 Remise de la preuve de dépôt

Une fois l'envoi scellé et horodaté, La Poste met une preuve de dépôt à disposition du consommateur de l'API, et lui restitue à sa demande.

La preuve de dépôt est au format PDF, signé par le Cachet électronique de La Poste. Elle est archivée pendant 7 ans. Elle est consultable pendant 1 an par l'expéditeur.

4.2 Processus de remise

4.2.1 Information du destinataire

Pour les destinataires particuliers ou professionnels, La Poste envoie un mail de notification au destinataire, qui contient un lien cliquable qui permet d'accéder à un espace afin de procéder, une fois identifié, à la réception ou au refus de la ou des Lettres recommandées électroniques.

Si La Poste est notifiée par le serveur du domaine de l'adresse courriel de l'expéditeur d'une impossibilité de délivrer le courrier (utilisateur inexistant, boite pleine, redirection non conforme à la politique de SPF…), le pli est réputé non distribuable à l'adresse indiquée par l'expéditeur ; l'information est mise à disposition du consommateur de l'API.

Le destinataire (professionnel ou particulier) dispose de 15 jours à compter du lendemain du dépôt pour réceptionner la Lettre recommandée électronique.

4.2.2 Exécution des processus d'identification du destinataire

Le destinataire (particulier ou professionnel) qui accède à l'espace d'acceptation ou refus des LRE par clic sur le lien d'accès contenu dans le mail de notification doit s'authentifier avec son MIE (3.2.3) avant toute opération.

La Poste procède alors à la vérification du MIE du destinataire et à l'extraction des informations d'identification du destinataire pour les comparer aux informations d'identification du destinataire fournies par l'expéditeur lors de l'envoi du pli.

4.2.3 Acceptation ou refus de la LRE

Quand le destinataire de la LRE accède à l'espace d'acceptation ou refus, il accède à la liste des lettres en attente pour accepter ou refuser les LRE reçues soit individuellement soit de manière groupée.

4.2.4 Délai d'acceptation de la LRE

Le destinataire dispose de 15 jours (15 périodes de 24 heures) à compter du lendemain du dépôt heure exacte pour réceptionner la LRE. Le délai prendra donc fin à l'heure exacte du dépôt 16 jours après (16 périodes de 24 heures). La notification au destinataire est quasi simultanée au dépôt réalisé par l'expéditeur.

4.2.5 Transmission de la LRE

Le destinataire une fois authentifié accède à l'espace de réception dans lequel il va pouvoir consulter sa ou ses LRE puis se l' (les) envoyer par mail ou la (les) télécharger sur son ordinateur.

4.2.6 Remise de la preuve de réception

Lorsque le destinataire a accepté le pli, La Poste procède à l'horodatage, génère et signe la preuve de réception qui est ensuite mise à disposition du consommateur de l'API, et lui restitue à sa demande.

La preuve est au format PDF, signé par le Cachet électronique de La Poste. Elle est archivée pendant 7 ans. Elle est consultable pendant 1 an par l'expéditeur.

4.2.7 Remise de la preuve de refus

Lorsque le destinataire a refusé le pli, La Poste procède à l'horodatage et génère la preuve de refus de la Lettre qui est ensuite mise à disposition du consommateur de l'API, et lui restitue à sa demande.

La preuve est au format PDF, signé par le Cachet électronique de La Poste. Elle est archivée pendant 7 ans. Elle est consultable pendant 1 an par l'expéditeur avec le contenu de la Lettre.

En refusant la Lettre, le destinataire n'aura pas accès aux données du pli et aux coordonnées de l'expéditeur.

4.2.8 Remise de la preuve de non-réclamation

Après expiration du délai d'acceptation (4.2.4), La Poste procède à l'horodatage et génère une preuve de non réclamation de la LRE qui est ensuite mise à disposition du consommateur de l'API, et lui restitue à sa demande.

La preuve est au format PDF, signé par le Cachet électronique de La Poste. Elle est archivée pendant 7 ans. Elle est consultable pendant 1 an par l'expéditeur avec le contenu de la Lettre.

4.3 Modification des données

Le service ne modifie pas les données et garantit l'intégrité du contenu grâce au scellement de l'envoi par le jeton d'horodatage.

4.4 Description des preuves

4.4.1 Preuve de dépôt

La preuve de dépôt contient :

Donnée	Format	Précisions
Raison sociale de l'expéditeur		Information extraite du certificat

Donnée	Format	Précisions
SIREN de l'expéditeur		Information extraite du certificat
Adresse électronique de l'expéditeur		Information extraite du certificat
Les mentions légales du PSC	RCS + adresse postale du siège + OID	
Nom et prénom ou raison sociale du destinataire		Informations renseignées par l'expéditeur
SIREN du destinataire		Uniquement lorsque le destinataire est un professionnel
Adresse électronique du destinataire		Vérification du format de l'adresse mail
Niveau de garantie		Le niveau de garantie de la LRE est unique et correspond à une indemnisation de 16€ (équivalence avec le niveau R1 de la LR papier)
Numéro d'identification unique de l'envoi		Numéro à 13 caractères commençant par le code alphanumérique 5C
Jeton d'horodatage qualifié	L'heure du jeton d'horodatage est lisible sur la preuve. L'heure affichée est l'heure de Paris.	L'algorithme de l'empreinte est SHA256
Cachet électronique avancé		Le cachet électronique de La Poste signe la preuve pour garantir son authenticité.
Logo EU trust mark		https://ec.europa.eu/digital-single-market/en/eu-trust-mark

4.4.2 Preuve de réception

La preuve de réception contient :

Donnée	Format	Précisions
Les données de la preuve de dépôt	La preuve de réception repend l'ensemble des données de la preuve de dépôt mentionnées dans le tableau 4.4.1	
Identité du récepteur		✓ Pour le destinataire Entreprise ayant accepté le recommandé électronique : raison sociale, SIREN et adresse mail. ✓ Pour le destinataire Particulier ayant accepté le recommandé électronique : nom et prénom et adresse mail.
Jeton d'horodatage qualifié	L'heure du jeton d'horodatage est lisible sur la preuve. L'heure affichée est l'heure de Paris.	L'algorithme de l'empreinte est SHA256

4.4.3 Preuve de refus

La preuve de refus contient :

Donnée	Format	Précisions
Les données de la preuve de dépôt	La preuve de réception repend l'ensemble des données de la preuve de dépôt mentionnées dans le tableau 4.4.1	

Donnée	Format	Précisions
Identité du récepteur		✓ Pour le destinataire Entreprise ayant refusé le recommandé électronique : raison sociale, SIREN et adresse mail. ✓ Pour le destinataire Particulier ayant refusé le recommandé électronique : nom et prénom et adresse mail.
Jeton d'horodatage qualifié	L'heure du jeton d'horodatage est lisible sur la preuve. L'heure affichée est l'heure de Paris.	L'algorithme de l'empreinte est SHA256

4.4.4 Preuve de non-réclamation

La preuve de non-réclamation contient :

Donnée	Format	Précisions
Les données de la preuve de dépôt	La preuve de dépend repend l'ensemble des données de la preuve de dépôt mentionnées dans le tableau 4.4.1	
Date de production de la preuve	Indique lisiblement la date et heure de non-réclamation	
Jeton d'horodatage qualifié	L'heure du jeton d'horodatage est lisible sur la preuve. L'heure affichée est l'heure de Paris.	L'algorithme de l'empreinte est SHA256

4.5 Cycle de vie des MIE

Sans objet, le service ne fournit pas de MIE aux utilisateurs.

5 Gestion des risques

5.1 Analyse de risques

Avant le lancement du service qualifié, La Poste – BSCC effectue une évaluation des risques afin d'identifier, d'analyser et d'évaluer les risques, en tenant compte des aspects techniques et commerciaux. L'analyse de risque identifie, en particulier, les systèmes « critiques » du service.

Les mesures de sécurité seront prises en tenant compte du résultat de cette analyse.

La Poste – BSCC fixe, dans sa PSSI, les exigences de sécurité et les procédures opérationnelles nécessaires pour mettre en œuvre les mesures identifiées.

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

Les risques résiduels identifiés sont acceptés durant le processus d'homologation du service.

5.2 Homologation

Suite à la finalisation de l'analyse de risque, La Poste – BSCC procèdera à l'homologation du service. Cette homologation est réalisée préalablement à la fourniture du service de confiance qualifié puis révisée au moins tous les deux ans.

5.3 PSSI

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

La PSSI et ses différentes versions seront communiquées aux abonnés du service, aux prestataires, aux organismes d'évaluation et à l'ANSSI.

La PSSI est transmise aux employés et aux éventuels sous-traitants.

La Poste – BSCC conserve la responsabilité globale de la conformité avec les procédures prévues dans sa PSSI, même lorsque certaines fonctions sont mises en œuvre par des sous-traitants. En particulier, La Poste – BSCC s'assure de la mise en œuvre effective des mesures prévues dans la PSSI.

La PSSI établit un inventaire des actifs du SI. Cet inventaire est revu régulièrement.

Tout changement susceptible d'avoir un impact sur le niveau de sécurité fourni est approuvé par le comité de pilotage du service.

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

6 Gestion et exploitation du service

6.1 Organisation interne

6.1.1 Fiabilité

L'organisation du service en assure la fiabilité. Les objectifs et mesures pour assurer cette fiabilité sont décrites dans le présent chapitre.

6.1.2 Rôles de confiance

Les rôles de confiance identifiés sont les suivants :

- **Responsable sécurité :** Le responsable de sécurité est chargé de la mise en œuvre de la politique de sécurité de la composante. Il gère notamment les contrôles d'accès physiques aux équipements des systèmes sensibles.
- **Responsable de l'horodatage et du cachet** : l'horodatage utilisé pour sceller et dater l'envoi (1.5.1) même opéré par un tiers, reste sous la responsabilité de La Poste – BSCC. À ce titre, une ou plusieurs personnes sont responsables de l'horodatage vis-à-vis de La Poste – BSCC, mais aussi de l'autorité de certification qui l'a émis. Le cachet utilisé pour signer la preuve (1.5.2) reste sous la responsabilité de La Poste – BSCC.
- **Exploitants (Chefs de Projets d'exploitation informatique) :** Personnes chargées de la mise en route, de la configuration et de la maintenance technique des équipements informatiques (configuration, sauvegardes, restaurations…). Elles assurent l'administration technique des systèmes et des réseaux de chaque composante, ainsi que leur surveillance (détection d'incident).

6.1.3 Séparation des tâches

Plusieurs rôles peuvent être attribués à une même personne, dans la mesure où le cumul ne compromet pas la sécurité des fonctions mises en œuvre.

Typiquement concernant les rôles de confiance, le responsable sécurité ne peut pas être exploitant.

6.2 Ressources humaines

6.2.1 Qualifications, compétences et habilitations requises

La Poste s'assure de la compétence et de l'adéquation des personnels employés.

6.2.2 Procédures de vérification des antécédents

La Poste – BSCC met en œuvre tous les moyens légaux dont elle dispose pour s'assurer de l'honnêteté du personnel qu'elle emploie. Ces personnels ne doivent notamment pas avoir de condamnation de justice en contradiction avec leurs attributions.

À ce titre, La Poste _ BSCC demande la communication d'une copie du bulletin n° 3 du casier judiciaire et peut décider, en cas de refus de communiquer cette copie ou en cas de présence de condamnation de justice incompatible avec les attributions de la personne, de lui retirer ces attributions.

6.2.3 Exigences en matière de formation initiale

Le personnel est préalablement formé aux logiciels, matériels et procédures internes de fonctionnement et de sécurité qu'il met en œuvre et qu'il doit respecter.

Les personnels ont pris connaissance et compris les implications des opérations dont ils ont la responsabilité.

6.2.4 Exigences et fréquence en matière de formation continue

Le personnel concerné reçoit une information et une formation adéquates préalablement à toute évolution dans les systèmes, dans les procédures, dans l'organisation, etc. en fonction de la nature de ces évolutions.

6.2.5 Fréquence et séquence de rotation entre différentes attributions

La présente politique ne formule aucune exigence sur le sujet.

6.2.6 Sanctions en cas d'actions non autorisées

En cas de non-respect des obligations, procédures ou exigences exprimées dans la présente politique ou la PSSI du service (5.3), le personnel s'expose à des sanctions disciplinaires telles que prévu dans le règlement intérieur de la société.

6.2.7 Exigences vis-à-vis du personnel des prestataires externes

Le personnel des prestataires externes intervenant dans les locaux ou sur les composantes du service est soumis aux exigences de la présente section (6.2). Cela apparaît dans des clauses spécifiques dans les contrats avec ces prestataires.

En particulier, la PSSI du service (5.3) est transmise aux prestataires externes.

6.2.8 Documentation fournie au personnel

Chaque personnel dispose au minimum de la documentation adéquate concernant les procédures opérationnelles et les outils spécifiques qu'il met en œuvre ainsi que les politiques et pratiques générales de la composante au sein de laquelle il intervient.

6.3 Gestion des biens

6.3.1 Généralités

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

6.3.2 Supports

Les supports sont gérés en adéquation avec leur classification, telle que déterminée par celle-ci.

6.4 Contrôle d'accès

La Poste – BSCC met en œuvre un contrôle d'accès aux systèmes d'information requis à l'exploitation du service de recommandé électronique.

Des procédures de gestion des habilitations sont mises en œuvre, prenant en compte les différents rôles identifiés par la présente politique (6.1.2). Ces procédures assurent que l'octroi et le retrait des habilitations s'effectuent en accord avec la gestion des ressources humaines.

Tout utilisateur est identifié et authentifié avant de pouvoir accéder aux systèmes critiques du service (cf. 5.1).

Toute action est tracée de sorte à pouvoir être imputable à la personne l'ayant effectuée.

L'accès aux logiciels d'exploitation (console, utilitaires, scripts, etc.) sur les serveurs est restreint et contrôlé.

Les informations sensibles sont protégées contre la divulgation résultant de la réutilisation de ressources (p. ex. fichiers effacés) par des personnels non autorisés.

La PSSI (5.3) décrit en détail les règles de contrôle d'accès applicables au SI du service.

6.5 Cryptographie

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

6.6 Sécurité physique et environnementale

6.6.1 Situation géographique des sites qui hébergent le service

Les conditions d'hébergement des équipements sur lesquelles reposent la sécurité et la continuité du service permettent de respecter les exigences et engagement de la présente politique en matière de disponibilité du service.

6.6.2 Accès physique aux Data Centers (DC)

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

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

6.6.3 Alimentation électrique et climatisation

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

6.6.4 Vulnérabilité aux dégâts des eaux

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

6.6.5 Prévention et protection incendie

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

6.6.6 Conservation des supports

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

Les supports (papier, disque dur, disquette, CD, etc.) correspondant à ces informations sont gérés selon des procédures conformes à ces besoins de sécurité.

6.6.7 Mise hors service des supports

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

6.6.8 Sauvegardes

Les procédures de sauvegarde sont précisées dans le dossier d'exploitation du service.

6.7 Sécurité opérationnelle

6.7.1 Mesures de sécurité des systèmes informatiques

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

6.7.1.1 Exigences de sécurité technique spécifiques aux systèmes informatiques

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

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

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

6.7.1.2 Mesures de sécurité liées au développement des systèmes

L'implémentation du système contribuant au service est documentée et fait l'objet de contrôle de qualité automatisé et régulier. La configuration des composantes du service, ainsi que toute modification et mise à niveau sont documentées et contrôlées.

La Poste – BSCC garantit que les objectifs de sécurité sont définis lors des phases de spécification et de conception.

La Poste – BSCC utilise des systèmes et des produits fiables qui sont protégés contre toute modification.

Conformément au [GDPR], La Poste – BSCC met en œuvre toutes les mesures techniques et organisationnelles nécessaires au respect de la protection des données personnelles, à la fois

dès la conception des produits et des services, en veillant notamment à limiter la quantité de données traitée dès le départ (principe dit de « minimisation »).

6.7.2 Mesures liées à la gestion de la sécurité

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

6.7.3 Évaluation des vulnérabilités

Les procédures d'exploitation du SI incluent la veille sécuritaire de ses composants. Ces procédures assurent que les correctifs de sécurité sont appliqués, au plus tard 2 mois après leur publication. Une campagne de patch management est réalisée tous les mois, elle est obligatoire et les indicateurs sont régulièrement remontés au Directeur des SI de La Poste – BSCC.

Dans le cas de vulnérabilités « critiques » (CVSS≥9), l'analyse d'impact est effectuée dans les 48 heures suivant la publication de la vulnérabilité.

6.7.4 Horodatage / Système de datation

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

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

6.8 Sécurité réseau

Le réseau et ses systèmes sont protégés contre les attaques et respecter les règles du Guide d'hygiène informatique de l'ANSSI (https://www.ssi.gouv.fr/guide/guide-dhygiene-informatique/). En particulier,

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

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

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

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

e) La communication entre des systèmes de confiance distincts n’est établie qu'à travers des canaux sécurisés, logiquement distincts des autres canaux de communication, assurant une authentification de bout en bout, l'intégrité et la confidentialité des données transmises.

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

g) Une analyse de vulnérabilité régulière sur les adresses IP publiques et privées du service, identifiées par TSP, est effectuée par une personne ou une entité ayant les compétences, les outils, le code de déontologie et l'indépendance nécessaires. Cette analyse donne lieu à un rapport.

h) Un test d'intrusion sur les systèmes du service est réalisé lors de la mise en place et après toute évolution de l'infrastructure ou des applications.

6.9 Gestion des incidents et supervision

Les activités du système concernant l'accès aux systèmes informatiques, l'utilisation des systèmes informatiques et les demandes de service sont surveillées (cf. 6.10.2).

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

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

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

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

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

6.10 Gestion des traces

6.10.1 Type d'événements à enregistrer

Concernant les systèmes liés aux fonctions qui sont mises en œuvre dans le cadre du service, chaque entité en opérant une composante journalise au minimum les événements décrits ci-

dessous, sous forme électronique. La journalisation est automatique, dès le démarrage d'un système et sans interruption jusqu'à l'arrêt de ce système.

- Création, modification, suppression de comptes utilisateur (droits d'accès) et des données d'authentification correspondantes (mots de passe, certificats, etc.)
- Démarrage et arrêt des systèmes informatiques et des applications
- Événements liés à la journalisation : démarrage et arrêt de la fonction de journalisation, modification des paramètres de journalisation, actions prises suite à une défaillance de la fonction de journalisation
- Connexion et déconnexion des utilisateurs ayant des rôles de confiance, et les tentatives non réussies correspondantes.

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

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

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

- Réception d'une demande de certificat (initiale et renouvellement)
- Validation ou échec de l'identification de l'expéditeur ou du destinataire
- Événements liés au cycle de vie des clés et des certificats cryptographiques (cachet et horodatage) : génération (cérémonie des clés), sauvegarde et récupération, révocation, renouvellement, destruction, etc.

  Remarque : ces événements peuvent être journalisés par les prestataires ou sous-traitants en charge de la gestion de ces clés et services (horodatage et apposition du cachet).
- Génération des preuves produites par le service (4.4)
- Publication et mise à jour des informations liées au service (politique, conditions générales d'utilisation, etc.) (2.4)

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

- Type de l'événement
- Nom de l'exécutant ou référence du système déclenchant l'événement

- Date et heure de l'événement
- Résultat de l'événement (échec ou réussite).

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

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

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

Les opérations de journalisation sont effectuées au cours du processus.

En cas de saisie manuelle, l'écriture se fait, sauf exception, le même jour ouvré que l'événement. Les événements et données spécifiques à journaliser sont documentés par La Poste – BSCC.

6.10.2 Fréquence de traitement des journaux d'événements

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

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

6.10.3 Période de conservation des journaux d'événements

Les journaux d'événements sont envoyés en asynchrone à intervalle très court de l'ordre de quelques secondes vers l'espace de stockage.

Les journaux d'événements sont conservés dans l'espace de stockage pendant au moins 1 (un) an.

6.11 Archivage des données

6.11.1 Types de données à archiver

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

Les données à conserver sont :

- l'identité de l'expéditeur du recommandé électronique ;
- une preuve de validation de l'identité de l'expéditeur ;

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

6.11.2 Période de conservation des archives

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

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

6.11.3 Protection des archives

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

Pendant tout le temps de leur conservation, les archives :

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

6.11.4 Exigences d'horodatage des données

Voir 6.7.4.

6.11.5 Procédures de récupération et de vérification des archives

Seule La Poste – BSCC a accès aux archives.

6.12 Continuité d'activité

6.12.1 Reprise suite à la compromission

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

Dans le cas d'un incident majeur, tel que la perte, la suspicion de compromission, la compromission, le vol de données critiques (p. ex., clés privées), l'événement déclencheur est la constatation de cet incident au niveau de la composante concernée, qui en informe immédiatement La Poste – BSCC. L'information est transmise au Responsable Sécurité du présent service qui déclare l'incident majeur ou pas. Dans le cas de l'incident majeur le plan de gestion de crise est mis en œuvre (cf document PAGC LRTE). Il est traité sans délais en mobilisant des équipes techniques par l'intermédiaire d'une cellule de crise. Une seconde cellule de crise, managériale celle-ci, est tenue informée de l'évolution de la situation, elle prend toutes les décisions stratégiques et de communication. La Poste – BSCC met

directement dans la boucle de communication l'ANSSI, conformément au § 6.9.1. pour la tenir informée de la création, la gestion et la résolution de cet incident majeur.

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

- En informe tous les utilisateurs et tiers impactés
- le cas échéant, révoque les MIE concernés.

6.12.2 Reprise suite à un sinistre

En cas de sinistre, un processus de gestion de crise (PAGC) est activé.

Le plan de continuité d'activité (PCA) s'appuie sur un hébergement de type Tiers III.

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

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

Ce plan est testé annuellement.

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

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

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

En outre, La Poste – BSCC s'engage à informer tous les clients, les autres entités avec lesquelles il a passé des accords et l'ANSSI, de cette compromission.

6.12.5 Capacités de continuité d'activité suite à un sinistre

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

6.13 Fin d'activité

En cas de cessation des services de recommandé électronique, le PSRE continue à maintenir l'information requise pendant un délai de 7 ans. La procédure de mise à disposition de l'information au-delà de 1 an sera précisée dans la nouvelle version de la politique du service publiée à destination des clients et des utilisateurs en cas de décision de la fin de vie du Service « LA Lettre recommandée électronique »,

En particulier :
Avant de fermer ses services de recommandé électronique, les procédures suivantes sont appliquées :

- ✓ Le PSRE rend disponible aux entités responsables des services demandeurs toute modalité concernant la fin de ses activités (date prévue de fin d'activité, etc.) ;

- ✓ Les autorisations données aux sous-traitants du PSRE intervenant dans le processus d'envois de recommandés électroniques sont révoquées ;

Le PSRE prend les mesures nécessaires afin de :

- ✓ soit continuer à assurer les fonctions de restitutions des preuves des envois antérieurs à l'arrêt du SRE ;
- ✓ soit transférer contractuellement les éléments constitutifs des preuves, le stockage ;

Le PSRE prend les mesures nécessaires afin de continuer à rendre disponible les preuves ;

Le PSRE prend les dispositions financières permettant de couvrir les frais relatifs à ces exigences ;

Les pratiques du PSRE prévoient les mesures à prendre à la fermeture des services. Ces mesures comprennent :

- ✓ La notification des entités affectées ;
- ✓ La transmission des obligations du SRE à d'autres parties.

6.14 Conformité

Les audits et les évaluations concernent, d'une part, ceux réalisés en vue de la délivrance d'une attestation de qualification au sens du règlement eIDAS et, d'autre part, ceux que La Poste – BSCC réalise ou a réalisé afin de s'assurer que l'ensemble de son infrastructure est bien conforme aux engagements affichés dans la présente politique.

6.14.1 Fréquences et circonstances des évaluations

Avant la première mise en service d'une composante ou suite à toute modification significative au sein d'une composante, La Poste – BSCC procèdera à un contrôle de conformité de cette composante.

La fréquence des évaluations au titre du maintien de la qualification est déterminée par les schémas d'évaluation en vigueur.

6.14.2 Identités et qualifications des évaluateurs

Le contrôle d'une composante est assigné par le PSRE à une équipe d'auditeurs compétents en sécurité des systèmes d'information et dans le domaine d'activité de la composante contrôlée.

6.14.3 Relations entre évaluateurs et entités évaluées

L'équipe d'audit n'appartient à l'entité opérant la composante contrôlée, quelle que soit cette composante, et être dûment autorisée à pratiquer les contrôles visés.

6.14.4 Sujets couverts par les évaluations

Les contrôles de conformité portent sur une composante (contrôles ponctuels) ou sur l'ensemble de l'architecture du service (contrôles périodiques) et visent à vérifier le respect des engagements et pratiques définies dans la politique de service et tous les éléments qui en découlent (procédures opérationnelles, ressources mises en œuvre, etc.).

6.14.5 Actions prises suite aux conclusions des évaluations

À l'issue d'un contrôle de conformité, l'équipe d'audit rend au PSRE un avis parmi les suivants :

- ÉCHEC : En cas d'échec, et selon l'importance des non-conformités, l'équipe d'audit émet des recommandations qui peuvent être la cessation (temporaire ou définitive)

d'activité, etc. Le choix de la mesure à appliquer est effectué par le PSRE et doit respecter ses politiques de sécurité internes.

- À CONFIRMER : Le PSRE remet à la composante un avis précisant sous quel délai les non-conformités doivent être levées. Puis, un contrôle de confirmation » permettra de vérifier que tous les points critiques ont bien été résolus.
- RÉUSSITE : Le PSRE confirme à la composante contrôlée la conformité aux exigences de la politique.

6.14.6 Notifications individuelles et communications entre les participants

En cas de changement de toute nature intervenant dans la composition du service, le PSRE aura pour action de :

- au plus tard un mois avant le début de l'opération, faire valider ce changement au travers d'une expertise technique, afin d'évaluer les impacts sur le niveau de qualité et de sécurité des fonctions du service et de ses différentes composantes.
- au plus tard un mois après la fin de l'opération, en informer l'organisme de qualification.

Par ailleurs, les résultats des audits de conformité seront tenus à la disposition de l'organisme de qualification en charge de la qualification du service.

7 Autres problématiques métiers et légales

7.1 Responsabilité financière

7.1.1 Couverture par les assurances

Le Groupe La Poste est titulaire d'un contrat de Responsabilité Civile n° 086892648 (Allianz) garantissant les conséquences pécuniaires de la responsabilité civile pouvant lui incomber en raison des dommages corporels, matériels et immatériels causés aux tiers du fait de ses activités professionnelles.

Montants des garanties :

Responsabilité Civile Exploitation / Professionnelle / Produits: Tous dommages confondus (corporels, matériels, immatériels consécutifs ou non) 5 000 000 € par sinistre et par année d'assurance et pour l'ensemble des garanties

DONT :

- ✓ RC Atteintes à l'environnement soudaines et accidentelles : 5 000 000 € par sinistre et par année d'assurance

dont :

- ✓ Frais d'Urgence : 2 000 000 € par sinistre et par année d'assurance.
- ✓ Pertes Pécuniaires résultant de la Responsabilité Environnementale : 750 000 € par sinistre et par année d'assurance
- ✓ Frais de retrait engagés par l'Assuré : 5 000 000 € par sinistre et par année d'assurance.

- ✓ Virus informatique : 5 000 000 € par sinistre et par année d'assurance
- ✓ Frais de reconstitution des archives et médias confiés : 5 000 000 € par sinistre et par année d'assurance.
- ✓ Défense pénale et Recours : 100 000 € par sinistre

7.1.2 Autres ressources

Sans objet.

7.1.3 Couverture et garantie concernant les entités utilisatrices

Se référer aux sections afférentes aux garanties pécuniaires décrites dans les Conditions Générales d'Utilisation.

7.2 Confidentialité des données professionnelles

7.2.1 Périmètre des informations confidentielles

Les informations considérées comme confidentielles sont au minimum les suivantes :

- Les données d'identité des clients et les pièces associées utilisées pour vérifier leur identité ;
- Les causes de révocations des MIE, sauf accord explicite du porteur ;
- Les secrets cryptographiques utilisés par le service (clés secrètes et privées, mots de passe, OTP et compteurs associés, etc.)

7.2.2 Informations hors du périmètre des informations confidentielles

Pas d'exigence.

7.2.3 Responsabilités en termes de protection des informations confidentielles

La Poste respecte la législation et la réglementation en vigueur sur le territoire français. En particulier, La Poste peut devoir mettre à disposition les données dont il dispose à des tiers dans le cadre de procédures légales. Elle doit également donner l'accès à ces informations à ses clients.

7.3 Protection des données personnelles

7.3.1 Politique de protection des données personnelles

Les données à caractère personnel recueillies font l'objet d'un traitement dont le responsable est La Poste conformément à la réglementation relative à la protection des données à caractère personnel.

Elles sont traitées pour procéder à l'identification de l'expéditeur et du destinataire, la génération des preuves relatives à l'envoi et nécessaires à l'exécution du service recommandé électronique.

Les données d'identification sont collectées auprès de l'expéditeur et des MIE.

Les destinataires de ces données personnelles sont les services concernés de La Poste ainsi que les expéditeurs et les destinataires pour les besoins du service. Les données seront conservées pendant 7 ans, durée nécessaire à l'exécution de la prestation et conformément aux exigences en vigueur.

Conformément à la réglementation en vigueur en matière de protection des données à caractère personnel, la personne concernée bénéficie d'un droit d'accès en écrivant à lrmarket.ualr@laposte.fr en joignant une copie recto d'une pièce d'identité.

La Poste a désigné un délégué à la protection des données, que le participant peut joindre pour toute question en lien avec la gestion de ses données personnelles, ou en cas de difficulté à ce sujet : Madame la Déléguée à la Protection des Données, CP C703, 9 rue du Colonel Pierre Avia 75015 PARIS.

Le participant a également le droit d'introduire une réclamation auprès de la Commission Nationale de l'Informatique et des Libertés (CNIL).

7.3.2 Informations à caractère personnel

Les informations considérées comme personnelles sont au minimum les données d'identité des clients et les pièces associées utilisées pour vérifier leur identité ;

7.3.3 Informations à caractère non personnel

La présente politique ne formule aucune exigence sur ce point.

7.3.4 Responsabilité en termes de protection des données personnelles

Voir 7.3.1.

7.3.5 Notification et consentement d'utilisation des données personnelles

Conformément à la législation et réglementation en vigueur sur le territoire français, les informations personnelles transmises à La Poste par les utilisateurs du service ne doivent ni être divulguées, ni transférées à un tiers, sauf dans les cas suivants : consentement préalable du porteur, décision judiciaire ou autre autorisation légale.

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

Sur ce point, La Poste agit dans le respect de la législation et réglementation en vigueur sur le territoire français.

7.3.7 Autres circonstances de divulgation d'informations personnelles

La présente politique ne formule aucune exigence sur ce point.

7.4 Obligations des utilisateurs

7.4.1 Expéditeurs

Les Expéditeurs garantissent :

– qu'ils ont, lors du dépôt d'une LR électronique, transmis à La Poste, conformément au Décret n° 2018-347 du 9 mai 2018 relatif à la lettre recommandée électronique, 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 prénom ou la raison sociale du Destinataire, ainsi que son adresse électronique ;

(iii) Le niveau de garantie choisi par l'Expéditeur contre les risques de perte ou de vol.

– 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 ;

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

7.4.2 Utilisation des MIE

En cas de remise d'un MIE (4.5) à un Destinataire ou un Expéditeur, celui-ci doit :

- Protéger celui-ci de toute perte ou divulgation

- Révoquer (4.5.3) 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.

7.4.3 Utilisation des LRE

Le SRE produit des preuves de Dépôt, d'Acceptation, de Refus et de Non-Réclamation (4.4) qui sont opposables en justice. Leur authenticité est garantie par le jeton d'horodatage qualifié qu'elles contiennent et le cachet électronique avancé de La Poste qui est apposé dessus.

Toute personne désirant utiliser ces preuves à des fins de justice peut s'assurer de leur recevabilité en vérifiant la validité (technique) des éléments suivants :

– Vérifier la validité du jeton d'horodatage, conformément aux procédures décrites dans la politique correspondante (1.6.1)

– Vérifier la validité du certificat utilisé pour le cachet électronique, conformément aux procédures décrites dans la politique correspondante (1.6.2)

– Vérifier la validité du cachet électronique (en utilisant par exemple un logiciel de lecture des fichiers PDF sachant interpréter les signatures électroniques, p. ex., Acrobat Reader)

7.5 Droits sur la propriété intellectuelle et industrielle

La présente politique ne formule aucune exigence sur ce point.

7.6 Interprétations contractuelles et garanties

La présente politique ne formule aucune exigence sur ce point.

7.7 Durée et fin anticipée de validité de la politique

7.7.1 Durée de validité

La présente politique reste en vigueur au moins un an après la réception, le refus ou la non-réclamation de la dernière lettre recommandée émis au titre de celle-ci.

7.7.2 Fin anticipée de validité

L'adoption d'actes d'exécution ou délégués du règlement eIDAS peut entraîner, en fonction des évolutions apportées, la nécessité pour La Poste de faire évoluer la présente politique (pour la gestion de la politique, voir 1.4, p. 4).

La Poste se réserve aussi le droit d'étendre les moyens d'identification techniques et organisationnels des expéditeurs et destinataires, et le périmètre des populations concernées par la présente politique.

7.7.3 Effets de la fin de validité et clauses restant applicables

Dans tous les cas, La Poste respectera les exigences réglementaires qui lui incombent.

7.8 Conformité aux législations et réglementations

Les pratiques de La Poste sont non-discriminatoires.

La conception et la mise en œuvre des services, logiciels et procédures de La Poste prennent en compte, dans la mesure du possible et dans le respect des exigences liées à l'article 44 du règlement (UE) No 910/2014 du parlement européen et du conseil du 23 juillet 2014 et du décret Décret n° 2018-347 du 9 mai 2018 relatif à la lettre recommandée électronique, l'accessibilité à tous les utilisateurs, « quel que soit leur matériel ou logiciel, leur infrastructure réseau, leur langue maternelle, leur culture, leur localisation géographique, ou leurs aptitudes physiques ou mentales », sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, (https://www.w3.org/Translations/WCAG20-fr/).

7.9 Force majeure

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