POSTMI – DECLARATION RELATIVE A LA POLITIQUE ET AUX PRATIQUES EN MATIERE DE SERVICES

RÉFÉRENCE DU DOCUMENT	PostMi – Déclaration relative à la politique et aux pratiques en matière de service de livraison électronique certifié
OID :	1.3.6.1.4.1.48620.83.1.1.3.2
VERSION	1
DATE	16 10 2025
AUTEUR DU DOCUMENT	Romain Billois
PROPRIÉTAIRE DU DOCUMENT	Laurent Carreda
APPROUVÉ PAR	Franck Dutertre

HISTORIQUE DES RÉVISIONS

VERSION	DATE	AUTEUR DE LA RÉVISION	RÉSUMÉ DES MODIFICATIONS
1.0	16/10/2025	Romain Billois	

APPROBATION

NOM	POSITION	DATE
Laurent Carreda	Administrateur délégué	22/10/2025

	AUTEUR DE LA RÉVISION
Niveau de diffusion	D3 – Diffusion libre (Liste de diffusion libre)
Liste de diffusion	Groupe Be-ys, organismes de contrôle, organismes d'évaluation de la conformité accrédités
Localisation	BeYs Trusted Solutions France

DOCUMENTS DE RÉFÉRENCE

Le présent document « Politique et déclaration de pratiques » fait référence à une liste d'autres documents internes ou externes, tels que des normes, des documents relatifs à la sécurité et à l'architecture fonctionnelle du présent projet.

Nom	Description	Lien
PSI	L'objectif principal de la PSI est de garantir l'application des exigences de sécurité pour maintenir l'état des actifs informationnels, selon les trois principes fondamentaux : Confidentialité, Intégrité et Disponibilité.	Interne
Document d'architecture technique	Document détaillant les choix d'implémentation logicielle et d'architecture réseau, pour répondre aux exigences PSI et normes ETSI.	Interne
Politique de certification OID : 1.3.6.1.4.1.48620.41.1.7.3.2	La politique de certification de BE INVEST International S.A. qui a	http://pki.almerys.com

	délivré le certificat de cachet électronique applicable dans le cadre du service PostMi.	
Politique d'archivage ArchiveMi OID : 1.3.6.1.4.1.62466.82.1.2	La politique d'archivage de la solution ArchiveMi utilisée pour le stockage à long-terme des preuves générées sur une LRE par PostMi.	Document contractuel à signer avec chaque client
Plan de continuité des activités	Document listant l'ensemble de procédures, de processus et de mesures techniques et organisationnelles visant à assurer que le service PostMi puisse continuer à fonctionner (ou reprendre très rapidement) après un incident majeur ou une catastrophe (panne électrique, cyberattaque, sinistre naturel, etc.).	Interne
Plan de cessation d'activité	Document de politique et de procédure qui détaille la marche à suivre si le Prestataire de services be ys Trusted Solutions Luxembourg SA devait arrêter de fournir le service PostMi (de manière volontaire ou forcée).	Interne
Conditions générales d'utilisation (Envoi LRE Qualifiée) OID : 1.3.6.1.4.1.48620.83.2.1.3.2	Document définissant les règles d'utilisation du service PostMi pour les Expéditeurs ayant contracté avec le fournisseur de services be ys Trusted Solutions Luxembourg SA.	https://www.kipmi.com
Conditions générales d'utilisation (Réception LRE Qualifiée) OID : 1.3.6.1.4.1.48620.83.2.4.3.2	Document spécifique aux destinataires du service PostMi. Il établit les règles qui s'appliquent à toute personne physique ou morale	https://www.kipmi.com

	recevant une LRE Qualifiée d'un Expéditeur ayant contracté avec le fournisseur de services be ys Trusted Solutions Luxembourg SA.	

GLOSSAIRE ET TERMINOLOGIE

Type	Entité	Description	Emplacement
	AC	Autorité de certification	
	C2SC	Comité de surveillance des services de confiance	
	CONDITIONS	Conditions générales d'utilisation	
	ANSSI	Agence nationale pour la sécurité des systèmes d'information	
	ILNAS	Institut Luxembourgeois de la Normalisation, de l'Accréditation, de la Sécurité et qualité des produits et services	

	PSC	Prestataire de services de confiance	
	PSCQ	Prestataire de services de confiance qualifié	
	LRE	Lettre recommandée avec accusé de réception	
	SERE-Q	Service d'Envoi Recommandé Électronique Qualifié	
	PSI	Politique de sécurité de l'information	
	UTC	Temps universel coordonné	
	Client	Entité juridique ou personne physique ayant conclu un contrat avec le service PostMi.	
	Expéditeur	Personne identifiée par le service pour déposer une lettre recommandée électronique	

	Prestataire de services	be ys Trusted Solutions Luxembourg SA	
	Destinataire	Personne identifiée par le service pour recevoir une lettre recommandée électronique	
	Parties prenantes	La personne, la machine ou le service impliqué dans le processus de service de confiance	
	Rôle de confiance	Personne de confiance formellement identifiée qui peut participer à l'exécution de contenus et d'actions sensibles du service PostMi	
	Sceau électronique et service	Service qui met en œuvre le sceau électronique pour le compte du service PostMi	
	Service d'horodatage	Service permettant la délivrance de jetons d'horodatage pour attester l'heure précise de la fin d'un événement, à travers les différentes étapes de l'exécution d'un courrier électronique recommandé.	
	Service d'identification vidéo par un tiers	Service permettant d'authentifier la personne identifiée comme expéditeur et la personne identifiée comme destinataire.	
	Utilisateur	Personne utilisant le service PostMi. Elle peut être soit l'expéditeur, soit le destinataire d'une lettre recommandée électronique.	

1. Introduction

1.1. Présentation

PostMi : L'Équivalent Numérique de la Lettre Recommandée

PostMi est un Service d'Envoi Recommandé Électronique Qualifié (SERE-Q). Il constitue une alternative sécurisée et entièrement dématérialisée au courrier recommandé traditionnel. Ce statut lui confère la même valeur juridique et la même force exécutoire que son équivalent papier.

En respectant des normes réglementaires et techniques strictes, PostMi permet aux organisations et aux particuliers de numériser intégralement leurs flux de communication, garantissant ainsi un gain d'efficacité, une sécurité renforcée et une conformité totale aux réglementations européennes et luxembourgeoise.

Cadre Légal et Conformité du Service

PostMi reproduit l'intégralité des fonctionnalités et effets juridiques du courrier recommandé papier. L'envoi est réalisé par voie électronique, accompagné de preuves vérifiables de dépôt et de livraison.

Le service est régi par le même cadre juridique que le recommandé traditionnel, ce qui lui permet de s'y substituer dans divers cas d'usage. PostMi répond spécifiquement aux conditions définies par le Règlement européen eIDAS (UE n° 910/2014) et aux exigences légales du Grand-Duché de Luxembourg.

PostMi est certifié SERE-Q conformément aux dispositions du Règlement eIDAS et satisfait notamment aux exigences définies à l'Article 44 ainsi qu'à la norme associée ETSI EN 319 521.

Engagement du Prestataire et Rôle de la Déclaration des Pratiques

Le service, proposé par le Prestataire, met à disposition une plateforme hautement sécurisée pour l'envoi de documents juridiquement significatifs.

Le service garantit une sécurité de bout en bout pour l'intégralité du processus, incluant :

- L'identification et l'authentification fiables des parties concernées.
- L'horodatage et le processus de scellement des données.

- La traçabilité complète des actions.

La plateforme génère des preuves juridiquement recevables pour chaque étape du cycle de vie d'une lettre recommandée électronique (envoi, rejet, non-réclamation).

La présente Déclaration des Pratiques a pour objet de définir l'engagement pris par BE YS TRUSTED SOLUTION LUXEMBOURG, en tant que Prestataire de Services de Confiance au sens du règlement eIDAS, pour l'envoi de courriers électroniques recommandés. Elle décrit les procédures opérationnelles, de sécurité et juridiques mises en œuvre pour garantir que PostMi répond constamment au niveau de confiance le plus élevé requis pour son statut Qualifié.

1.2. Gestion de la politique PostMi

1.2.1. Identification et date d'entrée en vigueur du document

Ce document est identifié par l'OID suivant : 1.3.6.1.4.1.48620.83.1.1.3.2

Ce document constitue la politique officielle et la déclaration des pratiques du service PostMi, fourni par BE YS TRUSTED SOLUTION LUXEMBOURG. Il décrit les engagements du Prestataire de services, en tant que Prestataire de services de confiance (PSC) au sens du règlement eIDAS, ainsi que les rôles et responsabilités de toutes les organisations externes qui soutiennent la fourniture de PostMi.

Ce document a été rédigé conformément au règlement (UE) 2016/679 (RGPD) ainsi qu'à la législation luxembourgeoise applicable (article 34 de la Loi du 14 août 2000 relative au commerce électronique modifiée par la Loi du 17 juillet 2020). La Politique est publique et peut être modifiée à tout moment par be ys Trusted Solutions Luxembourg SA.

1.2.2. Date d'entrée en vigueur

La politique entre en vigueur après avoir été approuvée par le Comité de surveillance des services de confiance (C2SC) du Prestataire et à la date d'entrée en vigueur fixée par ce comité.

La politique est publiée sur le site web à l'adresse https://www.kipmi.com au moins 72 heures avant sa date d'entrée en vigueur.

Le présent document reste en vigueur jusqu'à la publication d'une nouvelle version.

1.2.3. Gestion de la politique

1.2.3.1. Entité chargée de la gestion de la politique

La gestion de cette politique et des pratiques associées est assurée par les membres du C2SC du fournisseur.

1.2.3.2. Point de contact

Pour toute question concernant la présente politique, veuillez utiliser les coordonnées suivantes :

- Adresse postale : be ys Trusted Solutions Luxembourg SA
  Service PostMi
  17, rue Léon Laval, L-3372 LEUDELANGE - LUXEMBOURG
- E-mail : [support@kipmi.com]

1.2.3.3. Procédure d'approbation de la politique

La politique est examinée et approuvée par le C2SC, après une évaluation approfondie par les membres du comité et les représentants désignés.

Le processus de révision garantit :

- **Conformité :** la conformité de la politique avec les exigences réglementaires et normatives relatives à la fourniture d'un service de courrier électronique recommandé qualifié.
- **Cohérence :** la politique est cohérente avec les autres documents publiés relatifs au service, tels que les conditions générales d'utilisation.
- **Alignement sur les opérations :** les engagements pris dans la politique reflètent les capacités techniques et organisationnelles du Prestataire de services et de ses partenaires.
- **Notification à l'autorité de contrôle :** les modifications importantes apportées au service qualifié sont notifiées à l'autorité de contrôle conformément aux procédures de qualification prescrites.

Les circonstances qui déclenchent la notification à l'autorité de contrôle comprennent, sans s'y limiter :

- Modifications importantes de la manière dont le service est fourni (organisation, processus clés, paramètres techniques)
- Modifications de la déclaration de pratique du service (ce document) ou des conditions générales d'utilisation associées
- Modification des méthodes d'identification et d'authentification des expéditeurs et destinataires
- Modifications des sous-traitants ou des conditions d'hébergement
- Évolutions des horodatages et du modèle de preuve, susceptibles de changer les garanties de preuve fournies
- Modifications des mécanismes cryptographiques et des dépendances qualifiées (ex. service d'horodatage qualifié, certificats utilisés pour protéger l'intégrité des contenus et des preuves)
- Modifications substantielles des politiques de conservation et des journaux/archives du service qui affectent les exigences d'archivage et la disponibilité des preuves
- Intention de suspendre ou de cesser tout ou partie du service qualifié (au minimum 3 mois avant la cessation d'activité)

Le C2SC garantit que les clients du service sont informés suffisamment à l'avance (délai de prévenance d'au moins 1 mois), afin qu'ils aient le temps de prendre connaissance des nouvelles dispositions et de s'y adapter.

1.2.4. Informations publiées

1.2.4.1. Entités responsables de la mise à disposition des informations

Le Prestataire de services veille à ce que toutes les informations pertinentes soient publiées et accessibles aux utilisateurs du service (expéditeurs et destinataires) et aux tiers évaluant la validité des preuves produites sur le site web du Prestataire de services : https://www.kipmi.com

1.2.4.2. Informations à publier

Le Prestataire publie les informations suivantes :

- Le présent document détaillant la politique et les pratiques du service PostMi ;
- Les conditions générales d'utilisation du service ;
- La liste des certificats de sceaux numériques associés au service PostMi ;
- Points de publication des informations relatives aux services des partenaires.

1.2.4.3. Délais et fréquences de publication

Le Prestataire de services garantit la publication en temps opportun des informations relatives au service afin d'assurer la cohérence avec ses engagements opérationnels et ses procédures. Les principales pratiques sont les suivantes :

- **Calendrier :** les mises à jour du service, les nouvelles versions de la politique et autres développements pertinents sont publiés dès que les changements surviennent ou sont approuvés.
- **Communication des changements :** toute nouvelle version de la politique doit être communiquée aux clients avec un préavis suffisant (minimum 1 mois), afin de leur permettre de l'examiner et, si nécessaire, d'accepter à nouveau les conditions mises à jour.
- **Disponibilité continue :** la plateforme de publication est disponible 24 heures sur 24, 7 jours sur 7, garantissant un accès ininterrompu aux dernières informations pour tous les utilisateurs et parties prenantes, avec un engagement de disponibilité de l'hébergeur BeYs Cloud de 99,9 %.

La révision de la politique de sécurité et des pratiques doit être effectuée au moins de façon annuelle.

1.2.4.4. Contrôle de l'accès aux informations publiées

Le Prestataire de services garantit un accès sécurisé et transparent aux informations publiées.

Toutes les informations publiées sont librement accessibles et peuvent être consultées ici : https://www.kipmi.com

- Modifications contrôlées : l'accès au système utilisé pour modifier ou publier des informations est réservé au personnel autorisé. Ces personnes occupent des postes de confiance et utilisent des mécanismes d'authentification forte pour accéder au système.
- Auditabilité : toutes les modifications apportées aux informations publiées sont consignées et vérifiables, ce qui garantit la responsabilité et le respect des normes de sécurité.

1.2.5. Modification du document

1.2.5.1. Procédure de mise à jour

Les modifications proposées à la présente politique sont évaluées afin de vérifier leur conformité avec les exigences réglementaires et normatives applicables. Le C2SC est chargé de valider les modifications apportées à la présente politique. Chaque modification proposée fait l'objet d'une analyse d'impact afin d'évaluer ses effets potentiels sur le service et les utilisateurs. Le C2SC consigne ses décisions dans les procès-verbaux de ses réunions, et les modifications approuvées sont mises en œuvre et communiquées en conséquence.

La date d'entrée en vigueur de la nouvelle version du document est déterminée par le C2SC dans sa décision de validation, en tenant compte de la nature et de la complexité des modifications et, le cas échéant, du temps nécessaire aux parties prenantes du service pour mettre en œuvre les adaptations correspondantes.

1.2.5.2. Circonstances dans lesquelles la politique doit être modifiée

La présente politique peut être modifiée dans les circonstances suivantes, sans que cette liste soit exhaustive :

- Constatations d'audits internes ou externes nécessitant des corrections
- Mises à jour mineures, y compris corrections typographiques ou clarifications supplémentaires
- Améliorations ou extensions du service de courrier électronique recommandé.
- Adoption de nouvelles méthodes d'identification électronique

- Modifications de l'infrastructure technique, y compris les mises à jour des partenaires, des fournisseurs ou du système cryptographique

Pour les modifications importantes, un OID mis à jour est publié et les modifications sont soumises à l'organisme de contrôle et à l'organisme d'évaluation de la conformité pour examen.
Une fois l'évaluation du service validée par le C2SC, la nouvelle politique doit être communiquée aux clients par publication sur le site web, au personnel du Prestataire de services et à toutes les parties prenantes impliquées dans la fourniture du service. Un délai de préavis suffisant est prévu pour leur permettre de prendre connaissance des nouvelles dispositions et d'adapter leurs pratiques si nécessaire.

Le Prestataire de services envoie à l'organisme de contrôle un résumé annuel des modifications apportées au service.

1.2.5.3. Mécanismes et délai d'information sur les modifications

Une fois que le C2SC a validé une modification du service ou de la politique, le processus suivant est suivi afin de garantir une communication transparente et un délai d'adaptation suffisant pour toutes les parties prenantes.

- La politique mise à jour est publiée sur le site web officiel du prestataire de services, garantissant son accessibilité au public au moins 72 heures avant sa date d'entrée en vigueur.
- Des notifications sont envoyées à toutes les parties prenantes concernées, y compris les clients, le personnel du prestataire de services et les tiers concernés, par courrier électronique ou par courrier postal, en fonction de l'importance de la mise à jour.
- Communication avec les parties prenantes : des notifications sont envoyées aux clients et aux prestataires de services tiers, par e-mail ou par un autre moyen, en fonction de l'importance des modifications.

1.2.5.4. Circonstances dans lesquelles l'OID doit être modifié

Toute modification de la présente politique ayant une incidence significative sur le service nécessite une mise à jour de l'OID.

- **Objectif :** permettre une distinction claire entre les différentes versions de la politique et leurs périodes d'application.
- **Transparence :** garantit que les utilisateurs peuvent savoir quelles expéditions sont conformes à quelle version de la politique.

En cas de modification prévue de l'OID de la politique, la politique et son analyse d'impact sont soumises à l'organisme de contrôle et à l'organisme d'évaluation de la conformité pour avis ou commentaires et sont soumises à l'approbation du C2SC.

2. Documents connexes

2.1. Politique en matière d'horodatage

La politique en matière d'horodatage applicable dans le cadre du service PostMi est publiée ici : http://pki.almerys.com

2.2. Politique de certification des cachets électroniques

La politique de certification (OID : 1.3.6.1.4.1.48620.41.1.7.3.2) de l'autorité de certification qui a délivré le certificat de cachet électronique applicable dans le cadre du service PostMi est publiée ici : Politique de certification des cachets http://pki.almerys.com

2.3. Politique d'archivage ArchiveMi

La politique d'archivage (OID : 1.3.6.1.4.1.62466.82.1.2) concerne la politique de la solution d'archivage ArchiveMi utilisée pour le stockage à long-terme des preuves générées tout au long du cycle de vie d'une LRE par PostMi.

ArchiveMi est un service de BE YS TRUSTED SOLUTIONS FRANCE certifié NF461 comme système d'archivage électronique et NFZ42 pour garantir une valeur probante à long terme, empêchant tout accès non autorisé ou perte de données.

2.4. Conditions générales d'utilisation du service PostMi

Les CGU applicables dans le cadre du service sont publiées ici : https://www.kipmi.com

L'accès et l'utilisation du service PostMi sont régis par deux ensembles distincts de CGU, qui sont obligatoirement acceptées par l'utilisateur lors de son inscription et de l'utilisation du service.

Titre du document	**Description du champ d'application**	**OID**	**Date d'entrée en vigueur**
CGU_PostMi - Envoi LRE QUALIFIE - LUX	Définit les droits et obligations de l'utilisateur lors de la création et de l'envoi d'une LRE Qualifiée.	1.3.6.1.4.1.48620.83.2.1.3.2	27/10/2025

CGU_PostMi - Réception LRE QUALIFIE - LUX	Définit les droits et obligations de l'utilisateur lors de la réception, de l'identification et de l'acceptation d'une LRE Qualifiée.	1.3.6.1.4.1.48620.83.2.4.3.2	27/10/2025

2.5. Documents normatifs

Rejet	Document
[EIDAS]	Règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur les services d'identification électronique et de confiance destinés à renforcer les transactions électroniques au sein du marché intérieur https://www.eur-lex.europa.eu
ETSI EN 319 401 V3.1.1 (2024-06)	Signatures électroniques et infrastructures de confiance (ESI) ; Exigences générales en matière de politique pour les prestataires de services de confiance EN 319 401 - V3.1.1 - Signatures électroniques et infrastructures de confiance (ESI) ; Exigences générales pour les prestataires de services de confiance
ETSI EN 319 521 V1.1.1 (2019-02)	Signatures électroniques et infrastructures (ESI) ; Exigences en matière de politique et de sécurité pour les prestataires de services de remise électronique enregistrée EN 319 521 - V1.1.1 - Signatures électroniques et infrastructures (ESI) ; Exigences en matière de politique et de sécurité pour les prestataires de services de remise électronique avec accusé de réception
[HYGIÈNE]	Guide d'hygiène informatique https://cyber.gouv.fr/publications/guide-dhygiene-informatique
[ADMIN_SEC]	Recommandations pour l'administration sécurisée des systèmes d'information

	https://cyber.gouv.fr/publications/recommandations-relatives-ladministration-securisee-des-si
[EBIOS_RM]	EBIOS Risk Manager https://cyber.gouv.fr/la-methode-ebios-risk-manager
[PROCESS_QUALIF_SERVICE]	Processus de qualification des services https://cyber.gouv.fr/procedures-et-formulaires-pour-la-qualification
[RGPD]	https://www.cnil.fr/fr/reglement-europeen-protection-donnees

3. Parties prenantes et obligations

3.1. Prestataire de services

Le Prestataire de services est be ys Trusted Solutions Luxembourg SA.

Le Prestataire est responsable du respect du service avec la législation applicable et la présente politique.

Pour certaines activités, le Prestataire peut faire appel à des tiers. Les relations relatives à ces activités seront régies par des contrats de sous-traitance. Les contrats de sous-traitance définiront les droits et obligations des tiers impliqués dans l'activité liée à la fourniture du service PostMi, et les sous-traitants seront tenus de respecter strictement les procédures, conformément à la présente Politique.

3.2. Expéditeur

Les utilisateurs de PostMi, qu'il s'agisse de personnes physiques ou morales, sont responsables de l'utilisation sécurisée et conforme du service. Ils sont tenus de :

- **Accepter les conditions générales d'utilisation (CGU) :** reconnaître et respecter les conditions publiées régissant le service PostMi.
- **Fournir des informations exactes :** fournir des informations véridiques et à jour lors de l'inscription sur la plateforme.
- **Obtenir le consentement du destinataire :** s'assurer que les destinataires qui ne sont pas des utilisateurs professionnels ont explicitement donné leur consentement à l'utilisation des fonctionnalités du système et conserver une preuve vérifiable de ce consentement.
- **Utiliser des méthodes d'identification approuvées :** utiliser la méthode d'identification électronique prise en charge par le service, processus certifié PVID par l'ANSSI (actuellement assuré par Checkout, anciennement Ubble), pour une utilisation sécurisée du courrier.
- **Garantir la sécurité des certificats (le cas échéant) :** si vous utilisez un certificat électronique qualifié ou tout autre certificat fourni en externe, vous devez en garantir la sécurité, la validité et le renouvellement en temps opportun.
- **Protéger les informations d'authentification :** protégez les informations de connexion et tous les secrets d'authentification associés à votre compte et signalez immédiatement au fournisseur de services toute compromission suspectée ou confirmée.

- **Mettre à jour les modifications d'autorisation :** les personnes morales doivent informer le Prestataire de services de toute modification de l'autorisation des personnes physiques agissant en leur nom.
- **Garantir la sécurité du système :** maintenir une sécurité adéquate sur leurs propres systèmes afin d'empêcher toute intrusion malveillante, telle que des virus, des logiciels malveillants ou des bombes logiques, susceptible de compromettre l'intégrité du service LRE.

3.3. Destinataire

Le destinataire de PostMi, qu'il s'agisse d'une personne physique ou morale, doit :

- **Accepter les conditions générales d'utilisation (CGU)** : accepter et respecter les conditions d'utilisation.
- **Fournir des informations exactes :** soumettre des informations d'inscription exactes et à jour.
- **Utiliser des méthodes d'identification approuvées :** utiliser les méthodes d'identification électronique approuvées, telles que le PVID, pour accéder en toute sécurité au courrier enregistré.
- **Maintenir la sécurité des certificats :** si vous utilisez un certificat externe pour accéder au service, veillez à sa sécurité, à sa validité et à son renouvellement en temps opportun.
- **Protéger les identifiants d'authentification :** protéger les identifiants de connexion et signaler rapidement toute compromission suspectée ou confirmée au Prestataire de services.
- **Mettre à jour les modifications d'autorisation :** les entités juridiques doivent informer le fournisseur de services de toute modification concernant l'autorisation des personnes agissant en leur nom.
- **Acceptez ou refusez le courrier dans les délais spécifiés :** acceptez ou refusez le LRE dans les délais spécifiés par la politique, faute de quoi le courrier pourra être considéré comme non réclamé et rendu indisponible (expiré).
- **Télécharger les données des courriers enregistrés :** récupérer les données associées aux courriers enregistrés acceptés dans les délais spécifiés par le service, avec les documents associés pertinents pour les données des courriers enregistrés.

3.4. Liste des principales parties impliquées dans la fourniture du service

#	Entité juridique	Rôle	Nationalité	Localisation
1	BE INVEST International S.A.	Fournisseur de certificats qualifiés pour les signatures électroniques	Luxembourg	17 rue Léon Laval L-3372 Leudelange, Grand-Duché de Luxembourg
2	BE INVEST International S.A.	Fournisseur d'horodatage qualifié	Luxembourg	17 rue Léon Laval L-3372 Leudelange, Grand-Duché de Luxembourg

4. Identification

4.1. Identification de l'Expéditeur et Destinataire – personne physique

Le Prestataire vérifie l'identité de l'utilisateur – personne physique – par les moyens suivants :

- Vérification d'identité à distance - vérification de l'identité des personnes physiques accessible à l'utilisateur via un service tiers d'identification vidéo certifié PVID par l'ANSSI. Aux fins de la vérification d'identité à distance, l'utilisateur doit présenter une pièce d'identité et se soumettre aux différents tests et actions demandées, notamment pour être sûr qu'il est bien la personne visible sur le document et qu'il est bien une personne vivante.

4.2. Identification de l'Expéditeur et Destinataire – personne morale

Les cas de représentation de personnes morales par le service PostMi sont uniquement les sociétés enregistrées au registre du commerce français ou Luxembourgeois. Les organisations gouvernementales, associations et autres ne sont actuellement pas prise en charge, de même que pour les sociétés en dehors de la France ou du Luxembourg.

Le Prestataire vérifie l'identité de l'utilisateur – personne morale – par les moyens suivants :

- Pour la personne morale représentée par son responsable légal :
  - Un extrait du registre du commerce datant de moins de 3 mois pour la personne morale doit être présenté.
  - Si l'entité morale est dirigée par une autre entité morale, alors on va rechercher la preuve de l'identité de la première personne physique mentionnée sur un des extraits du registre du commerce des entités dirigeante du groupe d'entreprises. (les extraits RCS téléversés doivent dater de moins de 3 mois également).
  - Le Prestataire de services vérifie si la personne physique est mentionnée dans l'extrait du registre du commerce et des sociétés en tant que responsable légale.
  - Vérification d'identité à distance du dirigeant - vérification de l'identité des personnes physiques accessible à l'utilisateur via un service tiers d'identification vidéo certifié PVID par l'ANSSI. Aux fins de la vérification d'identité à distance, l'utilisateur doit présenter une pièce d'identité et se soumettre aux différents tests et actions demandées, notamment pour être sûr qu'il est bien la personne visible sur le document et qu'il est bien une personne vivante.

- Pour la personne physique représentant la personne morale autre que le responsable légal :
  - Un extrait du registre du commerce datant de moins de 3 mois pour la personne morale doit être présenté.
  - Si l'entité morale est dirigée par une autre entité morale, alors on va rechercher la preuve de l'identité de la première personne physique mentionnée sur un des extraits du registre du commerce des entités dirigeante du groupe d'entreprises. (les extraits RCS téléversés doivent dater de moins de 3 mois).
  - Une lettre de procuration du représentant légal mentionnant le délégué doit être fournie, datée et signée (la date ne doit pas être antérieure à 3 mois).
  - La procuration doit être accompagnée d'une copie d'une pièce d'identité en cours de validité (carte nationale d'identité, passeport ou titre de séjour) du représentant légal de l'entité morale.
  - Vérification d'identité à distance - vérification de l'identité des personnes physiques accessible à l'utilisateur via un service tiers d'identification vidéo (PVID) certifié par l'ANSSI. Aux fins de la vérification d'identité à distance, l'utilisateur doit présenter une pièce d'identité et se soumettre aux différents tests et actions demandées, notamment pour être sûr qu'il est bien la personne visible sur le document et qu'il est bien une personne vivante.

4.3. Procédure d'intégration spécifique aux utilisateurs expéditeurs

Les expéditeurs sont systématiquement clients de notre service (la signature d'un contrat est obligatoire avec une personne physique ou morale). Des comptes de services seront fournis aux utilisateurs identifiés.

Le processus d'intégration des utilisateurs expéditeurs (onboarding) est mis en œuvre lors de la signature du contrat avec le fournisseur de service, be ys Trusted Solutions Luxembourg SA. Cette procédure vise à garantir la conformité légale et la sécurité de l'accès aux services.

- **Documentation requise**

  Afin de valider la légitimité de chaque utilisateur à envoyer et/ou recevoir des LRE au nom de l'entreprise concernée, le client s'engage à fournir un dossier complet

pour chaque personne désignée pour représenter l'entreprise. Ce dossier doit inclure tous les documents mentionnés dans la section 4.2.

- **Validation et création de compte**

Une fois que ces documents sont reçus et que les informations ont été vérifiées, notre équipe procède à la création des comptes utilisateurs. Chaque compte est lié de manière sécurisée à l'entité juridique et aux documents d'identification fournis, garantissant la traçabilité de chaque action réalisée sur le service.
Cette approche permet de nous assurer que seuls les utilisateurs autorisés et dûment identifiés peuvent accéder à la plateforme, tout en simplifiant le processus pour le client qui peut ainsi intégrer plusieurs utilisateurs en une seule fois.

Une fois les comptes créés, chacun des utilisateurs est invité à procéder à l'identification PVID directement à partir de la plateforme PostMi. Aux fins de la vérification d'identité à distance, l'utilisateur doit présenter une pièce d'identité et se soumettre aux différents tests et actions demandées, notamment pour être sûr qu'il est bien la personne visible sur le document et qu'il est bien une personne vivante.

L'expéditeur n'est contraint de procéder à son identification PVID qu'à son premier envoi de lettre recommandée qualifiée.

4.4. Procédure d'intégration des utilisateurs destinataires

Il est nécessaire pour le destinataire de procéder à l'identification comme décrite ci-dessus à chaque réception de LRE qualifiée.

Cependant, la plateforme PostMi offre la possibilité au destinataire de créer lui-même son compte à la suite d'une identification réussie pour éviter de devoir repasser par la procédure d'identification à la réception d'une prochaine lettre recommandée qualifiée.

L'identification d'une entité légale est gérée directement par la plateforme dans le cas d'un utilisateur destinataire, ce qui permet lui permet de s'intégrer de manière autonome.

Un destinataire ne peut devenir expéditeur qu'après signature d'un contrat avec notre société, be ys Trusted Solutions Luxembourg SA.

4.5. Rétention des données pour vérification manuelle

Afin de respecter les principes de minimisation des données et du RGPD, la période de rétention des documents utilisés pour les vérifications manuelles est fixée à 60 jours.

Cette rétention maximale de 60 jours concerne uniquement les pièces nécessaires à la validation du mandat, soit la lettre de procuration et la pièce d'identité du représentant légal. Passé ce délai, ces documents sont systématiquement purgés du système.

Le processus de vérification manuelle est géré via NUMENT, une solution développée et exploitée en interne au groupe BE YS.

Les opérations de vérification manuelle sont assurées par les opérateurs de l'entité GRS, située en Roumanie, qui appartient également au groupe BE YS.

4.6. Génération de la preuve d'identification

Après une identification réussie, le système génère une preuve d'identification (contenant l'identifiant de session PVID réalisé sur la plateforme de service PVID (Ubble ou autre), le nom de l'utilisateur, l'identifiant unique de l'utilisateur et le statut résultant du PVID), horodaté et associé à l'utilisateur.

Ce document sera automatiquement joint au dossier de preuve de chaque lettre recommandée qualifiée envoyée ou reçue par cet utilisateur.

4.7. Génération de la preuve de connexion de la personne physique délégataire au représentant légal

- Après une connexion réussie de la personne physique délégataire au représentant légal, le système génère une preuve de confirmation du représentant légal (contenant le statut de la vérification de connexion, le nom du représentant légal, le nom et identifiant unique de la personne physique délégataire qui représente le représentant légal, le nom et le numéro RCS de l'entreprise à laquelle appartient le délégataire, le nom et le numéro RCS de l'entreprise à laquelle appartient le représentant légal ainsi qu'une référence à chacun des documents de preuve de téléversement des extraits RCS utilisés pour établir la connexion, et une référence au document de preuve de la vérification de la prescription avec le document d'identité), horodaté et associé à la personne physique.
- Un document de preuve par téléversement d'extrait RCS (contenant le nom et identifiant unique de l'utilisateur ayant téléversé les documents, le nom de l'extrait RCS téléversé, l'identifiant unique généré du document concerné et son empreinte numérique) est généré, horodaté et associé à la personne physique.

- Un document de preuve attestant la vérification de la prescription avec le document d'identité du représentant légal (contenant le statut de la vérification, le nom et l'identifiant unique de l'utilisateur ayant téléversé les documents, le nom de chacun des documents téléversés (prescription et photos recto-verso de la carte d'identité du représentant légal), l'identifiant unique généré pour chacun des documents concernés et leurs empreintes numériques respectives).
- Ces documents ci-dessus seront automatiquement joint au dossier de preuve de chaque lettre recommandée qualifiée envoyée ou reçue par ce délégataire.

5. Gestion du consentement du destinataire

5.1. Livraison à des destinataires non professionnels

Si l'expéditeur souhaite envoyer une lettre recommandée via le service PostMi à un destinataire **non professionnel**, le service requiert au préalable l'obtention du **consentement explicite du destinataire**, conformément à la législation en vigueur.

Le consentement doit être obtenu pour chaque destinataire distinct. En acceptant le consentement via le courriel de notification reçu, le destinataire confirme implicitement l'adresse électronique qu'il souhaite utiliser pour le service PostMi.

Lors de la demande de consentement, l'identité de l'expéditeur est partagée au destinataire.

Après avoir donné son consentement à un expéditeur, le destinataire autorise la réception d'un nombre illimité de lettres recommandées de cet expéditeur sans devoir renouveler son consentement.

Cependant, le destinataire conserve le droit de révoquer ce consentement à tout moment. Une fois la révocation effectuée, l'expéditeur ne sera plus en mesure de lui adresser de nouvelles lettres recommandées.

Remarque : L'identification du destinataire sera réalisée lors de la réception d'une LRE qualifiée.

5.2. Livraison à des destinataires professionnels

Dans le cadre de l'envoi d'une LRE Qualifiée à un destinataire professionnel, l'Expéditeur est l'unique partie responsable de l'obtention et de la gestion du consentement préalable du destinataire.

L'Expéditeur doit être en mesure de prouver, par tous moyens légaux, l'existence de ce consentement pour l'utilisation de la LRE Qualifié en lieu et place du recommandé traditionnel. Le fournisseur de services PostMi n'assume aucune responsabilité quant à la validité ou à l'existence de ce consentement.

6. Mécanismes d'authentification

Cette section décrit les mécanismes d'authentification appliqués aux expéditeurs et aux destinataires des LRE avec PostMi. L'authentification est précédée d'une vérification d'identité (voir section 4). Toutes les méthodes utilisées garantissent que seules les parties dûment identifiées peuvent accéder au service de livraison électronique qualifié avec accusé de réception (QERDS) et permettent la traçabilité et la non-répudiation des événements de livraison.

L'authentification à deux facteurs (2FA) ne s'applique qu'aux utilisateurs en possession d'un compte PostMi. Si un destinataire n'a pas de compte, il devra s'identifier (voir section 4) à chaque réception d'une lettre recommandée qualifiée. L'expéditeur, en tant que client du service, dispose obligatoirement un compte PostMi pour pouvoir utiliser le service, il est donc tenu de s'authentifier à chaque action sur une lettre recommandée qualifiée et d'effectuer la vérification d'identité à sa première action qualifiée.

L'authentification à deux facteurs (2FA) est conçue pour optimiser l'expérience utilisateur en éliminant le besoin d'une identification PVID à chaque action. Cependant, cette commodité est conditionnée par la création préalable d'un compte PostMi.

6.1. **Authentification de l'expéditeur – Personne physique**

Avant l'envoi d'une lettre PostMi, la personne physique agissant en tant qu'expéditeur doit s'authentifier à l'aide d'**une authentification à deux facteurs (2FA)**.

L'authentification par mot de passe à usage unique (OTP) est prise en charge via des mécanismes standard de mot de passe à usage unique basé sur le temps (TOTP), y compris l'intégration avec des authentificateurs couramment utilisés tels que Google Authenticator, Microsoft Authenticator et FreeOTP.

L'utilisateur a la possibilité de sélectionner son mécanisme d'authentification à deux facteurs (2FA), dont le choix est enregistré dans les préférences de son profil.

Tous les événements d'authentification sont loggés, scellés, horodatés et archivés de manière sécurisée afin de garantir la traçabilité et la non-répudiation. (voir section 9).

6.2. **Authentification de l'expéditeur – Personne morale**

Les entités morales doivent s'authentifier par l'intermédiaire **d'un représentant légal ou d'un délégataire désigné** qui a été identifié et autorisé (voir section 4).

Le représentant légal ou son délégataire s'authentifie via **une authentification à deux facteurs (2FA)** telle que décrite à la section 6.1.

Tous les événements d'authentification sont loggés, scellés, horodatés et archivés de manière sécurisée afin de garantir la traçabilité et la non-répudiation. (voir section 9).

6.3. Authentification du destinataire – Personne physique

Avant la livraison d'une lettre recommandée qualifiée, si elle a créé un compte PostMi, la personne physique agissant en tant que destinataire qui a été identifiée et autorisée (voir section 4) doit s'authentifier via **une authentification à deux facteurs (2FA)** telle que décrite au point 6.1.

Tous les événements d'authentification sont loggés, scellés, horodatés et archivés de manière sécurisée afin de garantir la traçabilité et la non-répudiation. (voir section 9).

6.4. Authentification du destinataire – Personne morale

La livraison d'une LRE à une personne morale est effectuée envers **son représentant légal ou son délégataire** qui a été identifié et autorisé (voir section 4). S'il a créé un compte PostMi, il s'authentifie via **une authentification à deux facteurs (2FA)** telle que décrite au point 6.1.

Tous les événements d'authentification sont loggés, scellés, horodatés et archivés de manière sécurisée afin de garantir la traçabilité et la non-répudiation. (voir section 9).

6.5. Gestion de la session authentifiée et déconnexion automatique

La durée de validité d'un code à usage unique (OTP) est strictement limitée à 15 minutes. Une fois ce délai écoulé, la session d'authentification associée expire immédiatement, sans être déconnecté de PostMi. L'utilisateur est alors contraint de renouveler la procédure d'authentification par OTP afin d'être en mesure de pouvoir exécuter les actions suivantes :

- Envoyer une LRE qualifiée
- Accepter de recevoir une LRE qualifiée
- Refuser de recevoir une LRE qualifiée
- Ouvrir une LRE qualifiée

De plus, toute inactivité de plus de 15 minutes entraîne une déconnexion automatique de l'utilisateur.

6.6. **Preuve d'authentification**

L'identifiant de la session OTP est systématiquement ajouté à toutes les preuves d'action pour les utilisateurs disposant d'un compte.

Pour l'Expéditeur :

- Dans la preuve d'envoi
- Dans la preuve récapitulant les informations de la lettre envoyée

Pour le Destinataire :

- Dans la preuve de réception
- Dans la preuve de refus
- Dans la preuve d'ouverture de la lettre

7. Exigences opérationnelles et processus d'envoi d'une lettre recommandée PostMi

7.1. Présentation du service PostMi

Le service PostMi fournit une plateforme sécurisée et performante pour l'envoi de lettres recommandées électroniques, garantissant la preuve du contenu et de la livraison. Par sa nature numérique, il garantit de manière unique la preuve du contenu envoyé. Contrairement au courrier recommandé traditionnel sur papier, il permet à l'expéditeur et au destinataire d'accéder à tout moment au contenu horodaté et immuable de la lettre. Cette fonctionnalité est particulièrement importante en cas de litige.

7.2. Parcours d'envoi d'une lettre recommandée via les services PostMi

7.2.1. Identification et authentification de l'expéditeur :

- Afin d'accéder aux services PostMi, l'expéditeur doit fournir les informations d'identification et d'authentification requises pour la procédure (voir sections 4 et 6).
- Une fois l'identification et l'authentification réussie, l'expéditeur peut accéder à la fonction « envoyer » de la plateforme PostMi pour les lettres recommandées électroniques.

7.2.2. Obtention du consentement du destinataire (s'il s'agit d'un particulier) (voir section 5) :

- L'expéditeur doit au préalable créer le contact destinataire en y indiquant son adresse électronique.
- La demande de consentement est nécessaire s'il s'agit d'un particulier.
- La demande de consentement se réalise à partir du contact créé dans PostMi.
- Le destinataire est notifié par courriel de la demande de consentement.
- Une fois le consentement donné ou refusé, l'expéditeur et le destinataire reçoivent tous deux une confirmation par courrier électronique.

7.2.3. Contenu de la lettre recommandée PostMi :

- Champ "Objet" (obligatoire) : Définir le titre ou l'objet de la lettre recommandée
- Champ "Destinataire (s)" (obligatoire) : Contact particulier ou professionnel. S'il s'agit d'un particulier, la sélection du contact destinataire n'est possible qu'après son consentement obtenu.
- Prise en charge de plusieurs destinataires :

Pour les envois multiples, le service traite chaque destinataire comme une transaction individuelle. Cela génère une lettre recommandée et un dossier de preuves distincts pour chaque destinataire.

- Message : Message texte optionnel, accompagnant la lettre.
- Piece (s) jointe (s) (obligatoire) : La lettre recommandée doit être attachée en pièce jointe.

7.2.4. Envoi de la lettre :

- Un identifiant unique est attribué par le système à la lettre recommandée électronique.
- Une preuve d'envoi (contenant le nom de l'expéditeur, l'identifiant unique de l'expéditeur, l'objet de la lettre, l'identifiant unique de la lettre, l'identifiant de la session de connexion, l'heure de connexion et l'identifiant de la session OTP utilisée pour l'envoi) est générée par le système dans le dossier de la lettre, et est accessible à tout moment.
- Une preuve de transmission (contenant le nom du destinataire, l'identifiant unique du destinataire, l'objet de la lettre et l'identifiant unique de la lettre) est générée par le système dans le dossier de la lettre, et est accessible à tout moment.
- Un document récapitulant et prouvant les informations de la lettre envoyée (contenant l'objet de la lettre, l'identifiant unique de la lettre, le message de la lettre, le nom de l'expéditeur, l'identifiant unique de l'expéditeur, l'adresse électronique de l'expéditeur, l'identifiant de la session de connexion, l'heure de connexion et l'identifiant de la session OTP utilisée pour l'envoi, le nom du destinataire, l'identifiant unique du destinataire, l'adresse électronique du destinataire, le nom du ou des fichier(s) attaché(s), l'empreinte numérique du ou des fichier(s) attaché(s) et la méthode de hachage) est généré par le système dans le dossier de la lettre, et est accessible à tout moment.

7.2.5. Génération des documents justificatifs (voir section 9) :

- Le système construit un dossier de documents justificatifs pour chacune des étapes de la vie de la lettre (identification PVID expéditeur et destinataire, authentification expéditeur et destinataire inclue dans tous les documents de preuve d'action sur la lettre, preuve de demande de consentement, preuve de consentement donné/refusé/expiré, preuve d'envoi de la lettre, preuve de transmission de la lettre, preuve d'acceptation/refus/non-réclamation de la lettre, preuve d'ouverture de la lettre).
- Chacune des preuves du dossier comporte un horodatage unique et sont enregistrées de manière sécurisée à des fins d'applicabilité juridique.

- Le processus de génération de preuves est explicité en section 9.
- Le dossier de preuves est accessible à tout moment via un lien de téléchargement sécurisé sur la plateforme PostMi. Ce dossier est accessible à l'expéditeur mais aussi au destinataire.

7.2.6. Notification du destinataire et acceptance :

- Le destinataire est informé par courriel qu'une lettre recommandée lui est destiné et en attente d'acceptance.
- L'identité de l'expéditeur et le contenu de la lettre restent confidentiels à ce stade.
- Le destinataire doit s'identifier et s'authentifier comme décrit dans la section 4 et 6.
- Une fois identifié et authentifié, le destinataire peut accepter ou refuser la lettre.
- Le destinataire dispose de 15 jours calendaires (à compter du lendemain de la notification) pour accepter ou refuser la lettre recommandée.

7.2.7. Notifications de rappel envoyés au destinataire :

- Si aucune action n'est entreprise de la part du destinataire, des courriels de rappel sont envoyés à l'adresse électronique du destinataire (aux jours 4, 8 et 12 après réception du courriel initial de notification).
- Une preuve est générée par le système pour chaque rappel envoyé (contenant l'objet de la lettre, l'identifiant unique de la lettre, le nom de l'expéditeur, l'identifiant unique de l'expéditeur, le nom du destinataire et l'identifiant unique du destinataire).

7.2.8. Statuts finaux de la lettre recommandée électronique : Acceptation, refus, non-réclamation :

- **Acceptation :** Si le destinataire accepte explicitement d'ouvrir la lettre recommandée PostMi.
  - La lettre recommandée et son contenu sont remis de manière sécurisée au destinataire après identification et authentification de ce dernier.
  - L'expéditeur est notifié par courriel de l'acceptation de la lettre.
  - Une preuve d'acceptation ou accusé de réception (contenant l'objet de la lettre, l'identifiant unique de la lettre, le statut de la lettre « Accepté », le nom du destinataire et l'identifiant unique du destinataire, l'adresse électronique du destinataire, l'identifiant de la session de connexion, l'heure de connexion et l'identifiant de la session OTP utilisée pour la réception) est générée par le système dans le dossier de la lettre, et est accessible à tout moment.

- Après acceptation, l'identité de l'expéditeur est divulguée au destinataire.

- **Refus :** Si le destinataire refuse explicitement d'ouvrir la lettre recommandée PostMi.
  - La lettre recommandée n'est pas remise au destinataire.
  - L'expéditeur est notifié par courriel du refus de la lettre.
  - Le destinataire reçoit un courriel de confirmation de son refus de recevoir la lettre.
  - Une preuve de refus (contenant l'objet de la lettre, l'identifiant unique de la lettre, le statut de la lettre « Rejeté », le nom du destinataire et l'identifiant unique du destinataire, l'adresse électronique du destinataire, l'identifiant de la session de connexion, l'heure de connexion et l'identifiant de la session OTP utilisée pour le refus) est générée par le système dans le dossier de la lettre, et est accessible à tout moment.
- **Non-réclamation :** la lettre PostMi et son contenu ne sont ni acceptés ni refusés par le destinataire et cela pour plus de 15 jours calendaires (à compter du lendemain de la notification d'envoi).
  - La lettre recommandée est explicitement considérée comme non-réclamée.
  - L'expéditeur et le destinataire sont notifiés par courriel de la non-réclamation de la lettre.
  - Une preuve de non-réclamation (contenant l'objet de la lettre, l'identifiant unique de la lettre, la date et l'heure de l'expiration de la lettre) est générée par le système dans le dossier de la lettre, et est accessible à tout moment.
  - La lettre recommandée et son contenu reste accessible à l'expéditeur.
  - Le destinataire ne peut voir ni consulter les détails de la lettre expirée.

8. Intégrité et sécurité des données

8.1. Transmission sécurisée

Le service PostMi garantit l'intégrité et la sécurité de la transmission contre tout risque de perte, de vol, de détérioration ou de modification non autorisée :

- Toutes les transmissions entre les utilisateurs et le service sont sécurisées afin d'empêcher tout accès non autorisé, perte ou altération.
- Pendant la phase de création de la lettre recommandée, seul l'utilisateur a la possibilité de modifier son contenu (par exemple : corrections, ajout de pièces jointes ou modification des destinataires). L'utilisateur a toujours une vue complète du contenu de la lettre tout au long du processus de création jusqu'à la validation finale.
- Une fois la lettre validée et envoyée, aucune modification du contenu ou des données de la lettre recommandée n'est possible. Le système conserve alors cette version définitive dans le cadre de la preuve enregistrée.
- Un cachet électronique avancé, créé à l'aide d'un certificat qualifié, est apposé sur toutes les preuves générées, garantissant ainsi leur intégrité et leur inviolabilité.

8.2. Politique générale de sécurité de l'information

Le Prestataire de services a mis en place une **politique de sécurité de l'information (PSI)** robuste pour le service qualifié. La PSI définit le cadre organisationnel visant à garantir la sécurité des informations, y compris la gestion des actifs et des infrastructures sensibles.

Les principales caractéristiques de la PSI sont les suivantes :

Documentation et mise en œuvre

- La PSI est documentée de manière exhaustive, mise en œuvre et maintenue en permanence par le Prestataire de services.
- Elle englobe les mesures et procédures de sécurité appliquées à l'infrastructure physique et technique et aux actifs sensibles.

Approbation et communication :

- La PSI et ses mises à jour ultérieures sont officiellement approuvées par l'équipe de direction du Prestataire de services.
- La PSI est communiquée aux personnes suivantes :
  - - aux employés
  - Sous-traitants et prestataires de services
  - Organismes d'évaluation externes

- Responsabilité et surveillance :
  - Le Prestataire de services conserve l'entière responsabilité du respect de la PSI, même lorsque certaines fonctions sont déléguées à des sous-traitants.
- Le Prestataire de services veille à :
  - La mise en œuvre effective des mesures prescrites par la PSI
  - L'inclusion de clauses d'audit dans les contrats conclus avec les prestataires de services tiers afin de contrôler le respect des politiques de sécurité.
- Inventaire des actifs :
  - La PSI tient un inventaire détaillé de tous les actifs du système d'information, qui comprend :
    - L'infrastructure physique
    - Systèmes techniques
    - Les informations sensibles.
  - Cet inventaire est révisé périodiquement et mis à jour à la suite de tout changement important apporté au système.
- Approbation des modifications :
  - Toute modification du service ou du système d'information susceptible d'avoir une incidence sur le niveau de sécurité doit être préalablement approuvée par le C2SC.
- Audits annuels :
  - La configuration du système d'information est auditée au moins une fois par an afin de détecter et de corriger toute modification susceptible de compromettre la conformité aux politiques de sécurité ou d'entraîner des failles de sécurité.

8.3. Certification de sécurité du service

Avant la mise en production du service, le Prestataire de services procède à un processus complet de clarification et d'approbation de la sécurité afin de s'assurer que toutes les mesures de sécurité répondent aux normes requises. Ce processus permet à la direction du Prestataire de services de comprendre pleinement la posture de sécurité du service et de ses systèmes de soutien et d'accepter explicitement tout risque résiduel identifié lors de l'évaluation.

Objectifs du processus de certification de sécurité :

- Sensibilisation aux risques :
  - Veiller à ce que l'équipe de direction soit pleinement informée des risques potentiels associés au service.
  - Fournir une compréhension claire des risques atténués et résiduels.
- Vérification des mesures de sécurité

  - Évaluer l'adéquation et l'efficacité des mesures de sécurité mises en œuvre pour protéger le service et son infrastructure
  - Confirmer la conformité aux normes réglementaires, techniques et opérationnelles applicables en matière de sécurité.
- Conformité aux normes réglementaires :
  - Garantir que le service répond aux exigences de sécurité.
- Acceptation explicite des risques résiduels :
  - Permettre à la direction de reconnaître et d'accepter formellement les risques résiduels qui subsistent après la mise en œuvre de toutes les mesures de sécurité raisonnables.

9. Processus de génération de preuves liés à l'utilisation du service de remise électronique qualifié (QERDS)

Le service de lettre recommandée électronique qualifiée PostMi s'engage à générer des preuves solides et juridiquement recevables pour toutes les étapes critiques du cycle de vie du courrier électronique recommandé. Ces preuves constituent le fondement de la conformité juridique, de la transparence et de la confiance, garantissant que toutes les parties prenantes, y compris les expéditeurs, les destinataires et les parties prenantes, peuvent se fier en toute confiance à l'intégrité et à l'authenticité du service. Les preuves sont conçues conformément aux dernières réglementations et répondent aux normes les plus élevées en matière de sécurité et de responsabilité.

Le Prestataire de services de confiance (PSC) be ys Trusted Solutions Luxembourg SA s'appuie sur le Prestataire de services de confiance qualifié (PSCQ) BE INVEST International S.A. pour l'émission du certificat de sceau qualifié dédié à PostMi et pour l'émission des sceaux avancés.

9.1. Scellement et horodatage des preuves

- Toutes les preuves générées sont scellées à l'aide d'un certificat qualifié et horodatées.
- Le certificat utilisé est qualifié mais la signature, elle, est avancée.
- L'horodatage utilisé est qualifié.
- Le sceau est créé à l'aide d'une clé RSA et respecte un format spécifique, avec un hachage SHA-256.
- Les horodatages sont émis conformément au règlement eIDAS et délivrés par BE INVEST International S.A.,
- Les preuves sont conservées pendant 10 ans sur ArchiveMi à compter de la date de création.

9.2. Sceau électronique et détails cryptographiques

Le service LRE utilise des technologies cryptographiques **avancées** pour garantir l'intégrité, l'authenticité et l'immuabilité des preuves générées.

- Certificat qualifié pour le scellage **avancé** :
  Un cachet électronique avancé est apposé sur toutes les preuves, à l'aide d'un certificat qualifié spécialement délivré au service LRE conformément à sa politique de certification.
- Niveau de cryptage
  Le sceau est créé à l'aide d'une clé privée RSA de 3072 bits, garantissant une sécurité robuste contre tout accès non autorisé ou toute altération.

- Format PDF
  Toutes les preuves sont scellées au format PDF, ce qui garantit la compatibilité avec les normes internationales et permet une validation à long terme du document.
- Détails de l'algorithme :
  Le sceau électronique est signé avec un mécanisme de hachage SHA-256, qui offre une puissance cryptographique et une conformité avec toutes les exigences réglementaires applicables.
- Le Prestataire de services intègre des mécanismes robustes de vérification de chaînes de certificats et de signatures, décrits dans son document d'architecture technique. Cette vérification est effectuée de manière systématique pour s'assurer de l'authenticité et de la validité de tous les éléments cryptographiques appliqués.
- PostMi s'appuie sur un module de signature interne préexistant « ebeesigner », développé au sein du groupe BeYs.
- Ce module de signature électronique est protégé par un Module Matériel de Sécurité (HSM). L'utilisation de cet HSM garantit la sécurité cryptographique des clés et des opérations, et est pleinement conforme aux normes ETSI en vigueur pour les services qualifiés. (voir https://cyber.gouv.fr/sites/default/files/document_type/ANSSI-CC-2025_09fr_0.pdf).

9.3. Horodatage qualifié

Afin de garantir l'intégrité temporelle, le service PostMi intègre des horodatages qualifiés dans toutes les preuves :

- Conformité :

  Les horodatages sont émis par une autorité d'horodatage de confiance (délivrés par BE INVEST International S.A.), conformément aux dernières réglementations.

- Précision :

  Chaque horodatage enregistre le moment exact où un événement se produit, garantissant ainsi un suivi précis et la force exécutoire légale.

9.4. Conservation à long terme des preuves

Le service de lettre recommandée électronique qualifiée PostMi garantit la conservation sécurisée de toutes les preuves générées pendant 10 ans, assurant ainsi leur accessibilité et leur conformité aux exigences réglementaires :

- Stockage sécurisé :

Les preuves sont cryptées et stockées dans des archives inviolables, sur ArchiveMi (service de BE YS TRUSTED SOLUTIONS FRANCE certifié NF461 comme système d'archivage électronique et NFZ42 pour garantir une valeur probante à long terme), empêchant tout accès non autorisé ou perte de données.

- Vérification étendue :
  Le service PostMi garantit la récupération des preuves par l'expéditeur et le destinataire pour une période minimale de 10 ans.

  L'utilisateur peut utiliser des outils mis à disposition par la commission européenne (https://ec.europa.eu/digital-building-blocks/DSS/webapp-demo/validation) pour permettre à tout moment la vérification de l'intégrité et de l'authenticité de ces preuves, assurant ainsi leur valeur légale à long terme, même après l'expiration des certificats de scellement ou d'horodatage d'origine.

  Sur demande de l'utilisateur effectuée via la plateforme de support (support@kipmi.com) et sur présentation de l'injonction judiciaire concernée, le Prestataire de services est en mesure de fournir au demandeur, à tout moment et de manière sécurisée, un dossier de preuves complet stockés sous ArchiveMi associé à l'envoi, pour toute utilisation à des fins juridiques ou contentieuses.

9.5. Vérification des preuves

Le service de lettre recommandée électronique qualifiée PostMi permet aux utilisateurs de vérifier de manière indépendante la validité et l'intégrité des preuves générées.

- Vérification des éléments cryptographiques :

S'assurer de la présence d'un sceau électronique et d'un jeton d'horodatage valides sur la preuve.

- Valider l'intégrité :

  Effectuer la validation cryptographique et d'intégrité du sceau et du jeton d'horodatage à l'aide d'outils de validation reconnus (tels que le DSS Validation Tool de la Commission Européenne).

- Vérifier les certificats :

  Les certificats qualifiés utilisés pour les cachets électroniques et les horodatages qualifiés sont officiellement répertoriés dans le tableau de bord eIDAS de la Commission européenne : https://eidas.ec.europa.eu/efda/trust-services/browse/eidas/tls/tl/LU/tsp/3

L'utilisateur peut donc vérifier l'authenticité et la non-révocation des certificats de PostMi en se référant au tableau de bord eIDAS de la commission européenne.

- Confirmer l'intégrité des données :
  L'utilisateur doit comparer l'empreinte cryptographique (hash) du courrier recommandé (stockée dans la preuve) avec l'empreinte recalculée des données originales. Cette correspondance assure qu'aucune altération du contenu n'a eu lieu depuis l'envoi.
- Validité à long terme :

  Pour les preuves dont les certificats d'origine sont arrivés à expiration, le service PostMi utilise la solution d'archivage certifié ArchiveMi garantissant la continuité de la capacité de vérification de l'intégrité et de l'authenticité de la preuve pendant une durée d'au moins 10 ans.

9.6. Liste des preuves générées

Le service de lettre recommandée électronique qualifiée PostMi garantit que toutes les preuves générées contiennent des métadonnées détaillées afin de garantir leur force exécutoire et leur traçabilité. Les heures indiquées sont exprimées en heure moyenne de Greenwitch (GMT). Les types d'événements liés au processus de livraison pour lesquels le service LRE fournit des preuves sont les suivants :

- **Preuve de demande de consentement**, contenant
  - Le nom de l'expéditeur
  - L'identifiant unique de l'expéditeur
  - L'adresse électronique de l'expéditeur
  - Le nom du destinataire
  - L'identifiant unique du destinataire
  - L'adresse électronique du destinataire
  - Sceau électronique avancé : sceau garantissant l'authenticité
  - Horodatage qualifié : enregistre l'heure exacte de la soumission
- **Preuve de consentement accordé**, contenant
  - Le nom de l'expéditeur
  - L'identifiant unique de l'expéditeur
  - L'adresse électronique de l'expéditeur
  - Le nom du destinataire
  - L'identifiant unique du destinataire
  - L'adresse électronique du destinataire
  - Sceau électronique avancé : sceau garantissant l'authenticité
  - Horodatage qualifié : enregistre l'heure exacte de la soumission

- **Preuve d'identification PVID réussie**, contenant
  - L'identifiant de session PVID réalisé sur la plateforme de service PVID (Ubble ou autre)
  - Le nom de l'utilisateur
  - L'identifiant unique de l'utilisateur
  - Le statut résultant "Réussi" du PVID
  - Sceau électronique avancé : sceau garantissant l'authenticité
  - Horodatage qualifié : enregistre l'heure exacte de la soumission
- **Preuve d'une connexion réussie du représentant légal ou délégataire à l'organisation**, contenant
  - Le statut de la vérification de connexion
  - Le nom du représentant légal
  - L'identifiant unique du représentant légal
  - Le nom et le numéro RCS de l'entreprise à laquelle appartient le représentant légal
  - Le nom de la personne physique délégataire qui représente le représentant légal
  - L'identifiant unique de la personne physique délégataire qui représente le représentant légal
  - Le nom et le numéro RCS de l'entreprise à laquelle appartient le délégataire
  - Une référence au document de preuve de la vérification de la lettre de procuration avec la carte d'identité du représentant légal
  - Le nom du fichier de la lettre de procuration téléversé
  - L'identifiant unique du fichier de la lettre de procuration téléversé
  - L'empreinte numérique du fichier de la lettre de procuration téléversé et la méthode de hachage utilisé
  - Le nom du fichier photo recto de la carte d'identité du représentant légal téléversé
  - L'identifiant unique du fichier photo recto de la carte d'identité du représentant légal téléversé
  - L'empreinte numérique du fichier photo recto de la carte d'identité du représentant légal téléversé et la méthode de hachage utilisé
  - Le nom du fichier photo verso de la carte d'identité du représentant légal téléversé
  - L'identifiant unique du fichier photo verso de la carte d'identité du représentant légal téléversé
  - L'empreinte numérique du fichier photo verso de la carte d'identité du représentant légal téléversé et la méthode de hachage utilisé
  - Une référence à chacun des documents de preuve de téléversement des extraits RCS utilisés pour établir la connexion
  - Le nom de chacun des fichiers d'extrait RCS téléversés
  - L'identifiant unique de chacun des fichiers d'extrait RCS téléversés

- L'empreinte numérique de chacun des fichiers d'extrait RCS téléversés et la méthode de hachage utilisé
- Sceau électronique avancé : sceau garantissant l'authenticité
- Horodatage qualifié : enregistre l'heure exacte de la soumission

- **Preuve de vérification de la lettre de procuration avec la carte d'identité du représentant légal**, contenant
  - Le statut de la vérification
  - L'identifiant du document lui-même, pour permettre sa référence dans la preuve d'une connexion réussie du représentant légal ou délégataire à l'organisation
  - Le nom de l'utilisateur ayant téléversé la lettre de procuration et les photos recto-verso de la carte d'identité du représentant légal
  - L'identifiant unique de l'utilisateur ayant téléversé la lettre de procuration et les photos recto-verso de la carte d'identité du représentant légal
  - Le nom du fichier de la lettre de procuration téléversé
  - L'identifiant unique du fichier de la lettre de procuration téléversé
  - L'empreinte numérique du fichier de la lettre de procuration téléversé et la méthode de hachage utilisé
  - Le nom du fichier photo recto de la carte d'identité du représentant légal téléversé
  - L'identifiant unique du fichier photo recto de la carte d'identité du représentant légal téléversé
  - L'empreinte numérique du fichier photo recto de la carte d'identité du représentant légal téléversé et la méthode de hachage utilisé
  - Le nom du fichier photo verso de la carte d'identité du représentant légal téléversé
  - L'identifiant unique du fichier photo verso de la carte d'identité du représentant légal téléversé
  - L'empreinte numérique du fichier photo verso de la carte d'identité du représentant légal téléversé et la méthode de hachage utilisé
  - Sceau électronique avancé : sceau garantissant l'authenticité
  - Horodatage qualifié : enregistre l'heure exacte de la soumission
- **Preuve pour chaque extrait RCS téléversé**, contenant
  - L'identifiant du document lui-même, pour permettre sa référence dans la preuve d'une connexion réussie du représentant légal ou délégataire à l'organisation
  - Le nom de l'utilisateur ayant téléversé l'extrait RCS
  - L'identifiant unique de l'utilisateur ayant téléversé l'extrait RCS
  - Le nom du fichier de l'extrait RCS téléversé
  - L'identifiant unique du fichier de l'extrait RCS téléversé
  - L'empreinte numérique du fichier de l'extrait RCS téléversé et la méthode de hachage utilisé

- Sceau électronique avancé : sceau garantissant l'authenticité
- Horodatage qualifié : enregistre l'heure exacte de la soumission

- **Preuve d'envoi**, contenant
  - Le nom de l'expéditeur
  - L'identifiant unique de l'expéditeur
  - L'objet de la lettre
  - L'identifiant unique de la lettre
  - L'identifiant de la session de connexion de l'expéditeur
  - L'heure de connexion de l'expéditeur
  - L'identifiant de la session OTP utilisée pour l'envoi
  - Sceau électronique avancé : sceau garantissant l'authenticité
  - Horodatage qualifié : enregistre l'heure exacte de la soumission
- **Preuve de transmission**, contenant
  - Le nom du destinataire
  - L'identifiant unique du destinataire
  - L'objet de la lettre
  - L'identifiant unique de la lettre
  - Sceau électronique avancé : sceau garantissant l'authenticité
  - Horodatage qualifié : enregistre l'heure exacte de la soumission
- **Preuve de réception**, contenant
  - L'objet de la lettre
  - L'identifiant unique de la lettre
  - Le statut de la lettre « Accepté »
  - Le nom du destinataire
  - L'identifiant unique du destinataire
  - L'adresse électronique du destinataire
  - L'identifiant de la session de connexion du destinataire
  - L'heure de connexion du destinataire
  - L'identifiant de la session OTP utilisée pour l'acceptation de la lettre
  - Sceau électronique avancé : sceau garantissant l'authenticité
  - Horodatage qualifié : enregistre l'heure exacte de la réception
- **Preuve de refus**, contenant
  - L'objet de la lettre
  - L'identifiant unique de la lettre
  - Le statut de la lettre « Rejeté »
  - Le nom du destinataire
  - L'identifiant unique du destinataire
  - L'adresse électronique du destinataire

- L'identifiant de la session de connexion du destinataire
- L'heure de connexion du destinataire
- L'identifiant de la session OTP utilisée pour le refus de la lettre
- Sceau électronique avancé : sceau garantissant l'authenticité
- Horodatage qualifié : enregistre l'heure exacte du refus

- **Preuve de non-réclamation**, contenant
  - L'objet de la lettre
  - L'identifiant unique de la lettre
  - La date et l'heure de l'expiration de la lettre
  - Sceau électronique avancé : sceau garantissant l'authenticité
  - Horodatage qualifié : enregistre l'heure exacte du refus
- **Preuve d'ouverture de la lettre**, contenant
  - L'objet de la lettre
  - L'identifiant unique de la lettre
  - Le nom du destinataire
  - L'identifiant unique du destinataire
  - L'adresse électronique du destinataire
  - L'identifiant de la session de connexion du destinataire
  - L'heure de connexion du destinataire
  - L'identifiant de la session OTP utilisée pour l'ouverture de la lettre
  - Sceau électronique avancé : sceau garantissant l'authenticité
  - Horodatage qualifié : enregistre l'heure exacte du refus

10. Désactivation et réactivation du compte utilisateur

10.1. Désactivation d'un compte

La désactivation d'un compte utilisateur est une fonctionnalité permettant d'empêcher un utilisateur de se connecter à la plateforme. Une fois son compte désactivé, l'utilisateur n'est plus en mesure d'envoyer de lettres simples, de lettres recommandées électroniques qualifiées ou d'avis électroniques.

Cependant, il continue de recevoir ces communications via les notifications par courrier électronique. Dans le cas d'une lettre recommandée électronique qualifiée, l'utilisateur désactivé devra obligatoirement passer par un processus d'identification (PVID) à chaque nouvelle réception, car son compte n'est plus considéré comme actif pour ces fonctionnalités.

La désactivation d'un compte entraîne automatiquement le **retrait de tous les consentements** précédemment accordés par l'utilisateur. Les expéditeurs concernés sont informés par notification de ce changement. Si un expéditeur envoie un document à un destinataire dont le compte est désactivé, ce dernier recevra tout de même une notification par courrier électronique, car la réception de ce type de communication ne dépend pas de l'état du compte sur la plateforme.

La désactivation de compte est une fonctionnalité accessible à partir de la page de profil de l'utilisateur.

Si l'utilisateur tente de se reconnecter, un message l'informe que son compte est désactivé et lui propose de le réactiver. Un courriel de confirmation de désactivation est également envoyé à l'utilisateur, incluant un bouton pour la réactivation de son compte.

10.2. Réactivation d'un compte

Un compte désactivé peut être réactivé via trois méthodes distinctes.

Méthode 1 : Depuis la page de connexion

1. L'utilisateur se rend sur la page de connexion et saisit ses identifiants.
2. Un message apparaît au-dessus du formulaire, l'informant que son compte est désactivé et l'invitant à cliquer sur un lien pour le réactiver.
3. Un courriel de confirmation est envoyé.
4. L'utilisateur clique sur le lien de confirmation dans le courriel (valable 15 minutes).

5. Il est redirigé vers une page de succès, confirmant la réactivation.
6. Après un court délai, il est redirigé vers la page d'accueil ou de connexion selon l'état de la session.
7. Un courriel de confirmation est envoyé pour notifier la réactivation.

Méthode 2 : Depuis l'email de désactivation

1. L'utilisateur clique sur le bouton "Activer mon compte" dans le courriel de confirmation de désactivation qu'il a précédemment reçu.
2. Il est redirigé vers la page de connexion, lui demandant de s'authentifier afin de pouvoir réactiver son compte.
3. Un courriel de confirmation est envoyé.
4. L'utilisateur clique sur le lien de confirmation dans le courriel (valable 15 minutes).
5. Il est redirigé vers une page de succès, confirmant la réactivation.
6. Après un court délai, il est redirigé vers la page d'accueil ou de connexion selon l'état de la session.
7. Un courriel de confirmation est envoyé pour notifier la réactivation.

Méthode 3 : A la suite d'une identification PVID réussie

1. A la réception d'une LRE qualifiée, l'utilisateur ayant désactivé son compte est contraint de repasser par le processus d'identification (PVID).
2. Une fois l'identification PVID réussie, l'utilisateur est invité à réactiver son compte ou d'ouvrir la lettre qui lui est adressé.

Conséquences de la réactivation

Une fois le compte réactivé, l'utilisateur peut se connecter. Il devra néanmoins repasser par le processus d'identification (PVID) pour réactiver les fonctionnalités liées aux lettres qualifiées. À noter que les consentements qui ont été révoqués lors de la désactivation ne sont pas automatiquement restaurés et doivent être gérés de nouveau par l'utilisateur.

11. Interopérabilité

Actuellement, le service de lettre recommandée électronique qualifiée PostMi est conçu comme un système autonome, garantissant les plus hauts niveaux de sécurité et de conformité réglementaire.

- **Opérations isolées :**

  En n'intégrant pas d'autres services de livraison recommandée, le service LRE minimise les vulnérabilités potentielles et garantit un contrôle total sur ses processus.

- **Améliorations futures :**

  Des plans d'interopérabilité peuvent être envisagés en fonction des besoins des clients et de l'évolution des exigences réglementaires.

12. Gestion des risques

12.1. Analyse des risques

Avant de lancer un service qualifié, le Prestataire de services a procédé à une évaluation complète des risques afin d'identifier, d'analyser et d'évaluer les risques potentiels, en tenant compte des facteurs techniques, opérationnels et commerciaux. L'analyse des risques met spécifiquement en évidence les systèmes et processus « critiques » du service.

Des mesures de sécurité appropriées sont mises en œuvre sur la base des résultats de cette analyse, afin de garantir que les vulnérabilités identifiées sont correctement atténuées.

Le Prestataire de services documente ces exigences de sécurité et ces procédures opérationnelles dans sa PSI afin de garantir la mise en œuvre efficace des mesures identifiées.

L'analyse des risques est revue et mise à jour chaque année. Elle est également révisée chaque fois que des changements importants surviennent, tels que :

- Modifications du service ayant un impact substantiel sur sa fourniture
- Mises à jour des politiques, des pratiques ou de l'infrastructure technique.
- L'introduction de nouvelles menaces ou vulnérabilités

Les risques résiduels identifiés lors de l'évaluation sont explicitement reconnus et acceptés par le responsable du service LRE. Ces risques acceptés sont ensuite soumis au C2SC et à l'équipe de direction pour approbation finale.

13. Gestion et exploitation

13.1. Organisation interne

13.1.1. Fiabilité

Le Prestataire de services a mis en place une structure organisationnelle solide et fiable afin de garantir la fourniture efficace du service de lettre recommandée électronique qualifiée PostMi. Cette structure définit clairement les rôles et les responsabilités au sein de l'organisation afin de superviser et de gérer les processus liés à la fourniture et à la maintenance du service. Ces processus peuvent être réalisés en interne ou sous-traités à des sous-traitants, et des contrôles appropriés sont en place pour garantir la responsabilité et la qualité.

Les principales mesures comprennent :

- Responsabilités définies
  - Les rôles et responsabilités au sein de l'organisation sont clairement définis afin de garantir le bon fonctionnement et le respect des politiques de service.
  - Les sous-traitants impliqués dans le service sont tenus par des accords contractuels de respecter les mêmes normes élevées de sécurité et de qualité que le Prestataire de services.
- Responsabilité globale :
  - Le Prestataire de services assume la responsabilité globale de veiller à ce que le service soit conforme aux exigences de sécurité et de qualité définies dans la politique.
  - Cela inclut la surveillance des sous-traitants et des partenaires afin de garantir le respect des obligations réglementaires et l'alignement sur les normes internes du Prestataire de services.
- Pratiques non discriminatoires :
  - Le service de lettre recommandée électronique qualifiée PostMi est accessible à toutes les personnes morales et physiques qui satisfont aux exigences de conformité du service. Aucune pratique discriminatoire n'est appliquée.
- Assistance et résolution des litiges :
  - Des procédures complètes d'assistance aux utilisateurs et de résolution des litiges sont mises en œuvre pour traiter toute question soulevée par les utilisateurs ou les parties prenantes.
- Disponibilité des ressources :
  - Le Prestataire de services veille à disposer des ressources matérielles, humaines et financières adéquates pour maintenir le service et respecter toutes les obligations énoncées dans sa politique.

- Des ressources financières sont maintenues pour couvrir toute responsabilité résultant de dommages causés aux utilisateurs en raison de défaillances ou de violations potentielles du service.

13.1.2. Séparation des tâches

Les tâches et les domaines de responsabilité conflictuels sont séparés afin de réduire le risque d'altération, intentionnelle ou non, ou d'utilisation abusive des actifs du service.
Plusieurs rôles peuvent ainsi être attribués à une même personne, dans la mesure où leur combinaison ne compromet pas la sécurité des fonctions mises en œuvre.
Pour les rôles de confiance, les combinaisons suivantes sont interdites :

- Responsable de la sécurité et administrateur ou opérateur système ;
- Auditeur système et tout autre rôle ;
- Administrateur système et opérateur.

13.1.3. Rôle de confiance

Les rôles de confiance, sur lesquels repose principalement la sécurité du système d'information, sont explicitement identifiés :

- **Responsable de la sécurité** : le responsable de la sécurité est chargé de la mise en œuvre de la politique de sécurité du composant. Il gère notamment les contrôles d'accès physique aux équipements des systèmes sensibles.
- **Responsable du cachet** : le cachet utilisé pour sceller les données, même s'il est utilisé par un tiers, reste sous la responsabilité du Prestataire de services. À ce titre, une ou plusieurs personnes sont responsables du cachet vis-à-vis du Prestataire de services, mais également vis-à-vis de l'autorité de certification qui l'a délivré.
- **Responsable de la gestion du service** : Supervise l'ensemble du service LRE Qualifié, assure la conformité à la politique, gère les incidents majeurs et prend les décisions stratégiques pour le bon fonctionnement du service.
- **Administrateur et opérateur système** : personnes responsables du démarrage, de la configuration et de la maintenance technique des équipements informatiques (configuration, sauvegardes, restaurations, etc.). Elles sont chargées de l'administration technique des systèmes et des réseaux du composant, ainsi que de leur surveillance (détection des incidents).
- **Opérateur commercial** : Les opérateurs commerciaux sont les personnes chargées du fonctionnement quotidien du service : assistance à la clientèle, gestion éventuelle des moyens d'authentification, etc.
- **Auditeur système** : L'Auditeur Système contrôle les opérations effectuées dans les systèmes afin de garantir la conformité aux conditions de sécurité et la légitimité des actions menées par les autres acteurs investis d'un rôle de confiance. À cette fin, il

dispose d'un accès aux données et aux archives d'audit du système. Ce rôle est un rôle de contrôle de la sécurité ; l'Auditeur Système n'est pas responsable de la supervision technique des systèmes déployés.

- **Opérateur de contrôle d'identité** : personnes chargées de vérifier l'identité d'un nouvel utilisateur du service. Cette opération de contrôle d'identité est effectuée lors d'un entretien physique en face à face dans les locaux de l'opérateur ;
- **Responsable de la vérification d'identité** : personne chargée de s'assurer que les processus effectivement mis en œuvre pour vérifier l'identité de l'expéditeur et du destinataire sont conformes au processus initial de vérification d'identité spécifié dans la présente politique.
- **Archiviste** : Gère l'archivage sécurisé, l'intégrité et l'accessibilité des LRE Qualifiée conformément aux durées de conservation légales et aux exigences de restitution ou de destruction sécurisée.

L'attribution d'un rôle de confiance est formalisée entre un responsable de la sécurité du service et le personnel qui accepte explicitement ce rôle.

13.2. Gestion des mesures de sécurité des ressources humaines

13.2.1. Compétences et qualifications

Le Prestataire de services veille à ce que son personnel et ses sous-traitants soient mobilisés et compétents pour garantir la sécurité et la fiabilité du service.

Le personnel employé, qu'il soit interne ou sous-traitant, dispose de l'expertise, de l'expérience et des qualifications nécessaires pour exercer ses fonctions. Cela inclut notamment les règles de sécurité relatives aux actifs informatiques sensibles et aux données à caractère personnel. Des sessions de sensibilisation sont organisées régulièrement, au moins une fois par an, sur les nouvelles menaces et les bonnes pratiques en matière de sécurité. Des sanctions disciplinaires appropriées sont prévues pour le personnel qui s'écarte de la politique ou des pratiques du service.

Le personnel d'encadrement dispose de l'expertise et de l'expérience appropriées à leur fonction et connaît les règles de sécurité en vigueur au sein du service.

Les rôles et responsabilités en matière de sécurité sont documentés dans des descriptions de poste accessibles à tout le personnel concerné. Le Prestataire respecte les principes de séparation des rôles et de privilège minimal dans la définition des fonctions et dans leur attribution. L'attribution des rôles tient compte de la sensibilité des responsabilités associées, des compétences et de la probité du personnel. Si nécessaire, la description de poste différencie les responsabilités et les attentes des rôles génériques de beys trusted solutions des spécificités requises par le service qualifié.

Le personnel a pris conscience et comprend les implications des opérations dont il est responsable.

13.2.2. Vérification des antécédents

Le Prestataire met en œuvre tous les moyens légaux à sa disposition pour s'assurer de l'honnêteté du personnel qu'il emploie. En particulier, ce personnel ne doit pas avoir fait l'objet d'une condamnation judiciaire incompatible avec ses responsabilités, ni se trouver dans une situation de conflit d'intérêts susceptible de nuire à l'impartialité des opérations.

13.2.3. Exigences et fréquence de la formation

Le personnel est préalablement formé aux logiciels, au matériel informatique et aux procédures opérationnelles et de sécurité internes qu'il met en œuvre et doit respecter, dans le cadre du service PostMi dans lequel il opère. Le personnel est conscient et comprend les implications des opérations dont il est responsable.

13.2.4. Exigences et fréquence de la formation continue

Le personnel concerné reçoit des informations et une formation adéquate avant toute modification des systèmes, des procédures, de l'organisation, etc., en fonction de la nature de ces évolutions. En outre, la formation continue comprend une formation annuelle sur les nouvelles menaces et les procédures de sécurité appliquées.

13.2.5. Exigences applicables au personnel externe

Le personnel des prestataires de services externes travaillant dans les locaux du Prestataire de services et/ou sur les composantes du service LRE se conforme également aux exigences du présent chapitre. Cela se traduit par des clauses appropriées dans les contrats conclus avec les prestataires de services.

13.2.6. Sanctions en cas d'actions non autorisées

Des sanctions appropriées sont appliquées au personnel qui ne respecte pas les procédures et politiques de sécurité applicables.

13.2.7. Documentation fournie au personnel

Chaque membre du personnel dispose au minimum d'une documentation adéquate sur les procédures opérationnelles et les outils spécifiques qu'il met en œuvre, ainsi que sur les politiques et pratiques générales du composant dans lequel il travaille, plus particulièrement celles de la PSI qui l'affectent.

13.3. Gestion des actifs

13.3.1. Général

Le Prestataire de services assure la protection des actifs (y compris les informations traitées) du service à un niveau approprié.

Un inventaire des actifs est réalisé et tenu à jour dans le cadre de la documentation de l'architecture technique et de l'analyse des risques du service. Les actifs sont gérés conformément à leur classification en termes de sensibilité des informations.

13.3.2. Manipulation des supports

Les supports contenant des informations sensibles sont gérés conformément aux exigences de sécurité adaptées à leur sensibilité.

Des mesures sont mises en œuvre pour prévenir l'obsolescence, l'accès non autorisé, le vol ou l'altération des supports du service. Ces mesures sont efficaces pendant toute la durée de vie prévue des biens. À la fin de leur vie, et selon des procédures conformes au niveau de confidentialité des informations qu'ils contiennent, les supports sont soit détruits, soit réinitialisés en vue d'une réutilisation.

L'équipement HSM est mis en œuvre et exploité par le Prestataire de services conformément aux règles spécifiques qu'il a définies.

13.3.3. Contrôle d'accès

Le Prestataire met en œuvre un contrôle d'accès physique et logique aux systèmes d'information du département.

Des procédures de gestion des autorisations personnelles sont mises en œuvre, en tenant compte des différents rôles identifiés par la présente politique. Ces procédures garantissent que l'octroi et le retrait des autorisations sont effectués en coordination avec la direction des ressources humaines et respectent le principe du moindre privilège.

Tous les utilisateurs doivent être identifiés et authentifiés avant de pouvoir accéder aux systèmes critiques du service. Toute action est tracée de manière à pouvoir être imputée à la personne qui l'a effectuée.

Les autorisations opérationnelles et administratives sont clairement séparées. L'accès aux logiciels d'exploitation (consoles, utilitaires, scripts, etc.) sur les serveurs est restreint et contrôlé.

Les informations sensibles doivent être protégées contre toute divulgation résultant de la réutilisation de ressources (par exemple, fichiers supprimés) par du personnel non autorisé.

13.4. Cryptographie

Le Prestataire garantit la mise en œuvre de mesures de sécurité appropriées pour la gestion des clés et des matériaux cryptographiques tout au long de leur cycle de vie.
Concernant la clé privée LRE-proof :

- La génération et l'utilisation d'une clé privée de scellement sont effectuées dans un module cryptographique sécurisé ;
- Le module cryptographique est placé dans un environnement physique séparé des autres fonctions, dont l'accès est limité à un personnel restreint ayant un rôle de confiance ;
- La clé privée est générée, sauvegardée et restaurée uniquement dans un environnement physiquement sécurisé, par un petit nombre de personnes ayant un rôle de confiance. Au moins deux personnes participent à chacune des opérations. Le nombre de personnes autorisées à effectuer ces opérations est réduit au minimum nécessaire pour garantir le respect des exigences de la présente politique (en particulier la confidentialité et la disponibilité).
- Toute copie de la clé privée doit être conservée dans le même type de module cryptographique ou dans des conditions garantissant au moins un niveau de sécurité équivalent ;
- Le module cryptographique est protégé contre toute altération, tant pendant le transport que pendant le stockage ;
- Le module cryptographique est maintenu en état de fonctionnement et de sécurité, et supervisé afin de garantir son bon fonctionnement ;
- La clé privée du sceau est retirée d'un module cryptographique à la fin de la durée de vie de ce matériel et avant son élimination.

13.4.1. Moyens cryptographiques

Les dispositifs qui mettent en œuvre les clés privées des cachets sont des modules cryptographiques matériels certifiés FIPS 140-2 niveau 3 ou Critères communs EAL4+. La configuration opérationnelle minimale est conforme à la norme FIPS 140-2 niveau 3.

13.4.2. Gestion du cycle de vie

Les clés privées du service PostMi sont générées lors d'une cérémonie de remise des clés en présence de témoins et de détenteurs secrets. Cette cérémonie fait l'objet d'un rapport officiel.

13.4.3. Gestion des secrets

Les données d'activation des certificats de cachet sont sous la responsabilité du Prestataire de services (responsable de cachet) et sont générées et protégées par celui-ci en matière

d'intégrité et de confidentialité. Ce dernier est ensuite chargé d'en garantir la confidentialité, l'intégrité et la disponibilité.

13.4.4. Algorithmes cryptographiques

Les clés utilisées sont de 3072 bits et sont générées selon l'algorithme RSA.

13.5. Sécurité physique et environnementale

13.5.1. Localisation géographique et construction des sites

En fonction de la sensibilité des composants du service de lettre recommandée électronique qualifiée PostMi , les sites sont définis au niveau 1 de la PSI du Prestataire de services : impact vital (majeur pour l'entreprise).
À ce titre, la sécurité du site de construction est conforme aux mesures de sécurité physique de niveau 1 pour la protection périphérique, périmétrique et intérieure, et en particulier aux mesures relatives à :

- Alimentation électrique et climatisation ;
- Vulnérabilité aux dégâts des eaux ;
- Prévention et protection incendie.

Les mesures permettent également de respecter les engagements pris dans la présente politique ou dans les engagements contractuels avec les clients du service PostMi, en termes de disponibilité du service.

13.5.2. Accès physique

Afin d'éviter toute perte, détérioration et compromission des ressources du service de lettre recommandée électronique qualifiée PostMi, l'accès aux locaux est contrôlé conformément au niveau de zonage 1 des locaux : « accès très restreint ».

Pour les fonctions spécifiques au service PostMi ainsi que pour toutes les fonctions identifiées comme critiques dans l'analyse des risques, l'accès est strictement limité aux seules personnes autorisées nommément à pénétrer dans les locaux, et la traçabilité des accès est assurée.

La sécurité est renforcée par la mise en place de moyens physiques et logiques de détection des intrusions. De plus, le contrôle des entrées et des sorties est permanent en dehors des heures de travail (HNO). Chaque entrée et sortie de la zone sécurisée est surveillée de manière indépendante.

Tout personnel non autorisé doit être accompagné d'une personne autorisée. Chaque entrée et sortie est traçable.

Afin de garantir la disponibilité des systèmes, l'accès aux machines est limité aux seules personnes autorisées à effectuer des opérations nécessitant un accès physique aux machines.

Pour ce faire, les composants concernés du service PostMi définissent un périmètre de sécurité physique dans lequel ces machines sont installées. Tout local utilisé conjointement par le composant concerné et un autre composant (appartenant ou non à PostMi) se trouve en dehors de ce périmètre de sécurité. L'ouverture de la porte est contrôlée par un système de contrôle d'accès.

13.5.3. Alimentation électrique et climatisation

Les caractéristiques des équipements d'alimentation électrique et de climatisation permettent de respecter les conditions d'utilisation des équipements du service PostMi telles que définies par leurs fournisseurs.

13.5.4. Vulnérabilité aux dégâts des eaux

Les moyens de protection mis en place par le service PostMi permettent de protéger son infrastructure contre les dégâts des eaux.

13.5.5. Prévention et protection contre les incendies

Le service PostMi met en place des moyens de protection et de lutte contre l'incendie.

13.5.6. Conservation des supports

Les supports (papier, disque dur, disquette, CD, etc.) utilisés au sein du service PostMi sont traités et stockés conformément aux besoins de sécurité des actifs sensibles (en termes de confidentialité, d'intégrité et de disponibilité).

Les supports font notamment l'objet de mesures contre les dommages, le vol, l'accès non autorisé et l'obsolescence. Ces mesures s'appliquent pendant toute la durée de conservation du contenu de ces supports.

13.5.7. Mise hors service des supports

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

Les procédures et moyens de destruction et de réinitialisation sont conformes à la politique de sécurité du prestataire de services.

13.5.8. Sauvegarde hors site

En plus des sauvegardes sur site, les composants du service PostMi mettent en œuvre des sauvegardes hors site de leurs applications et informations. Ces sauvegardes sont organisées de manière à garantir la reprise la plus rapide possible des services en cas d'incident.

Les sauvegardes sont testées régulièrement.

13.6. Mesures de sécurité techniques

13.6.1. Gestion des clés à double estampille

La gestion des clés privées pour le service PostMi est strictement conforme aux exigences spécifiées dans la politique de certification (OID : 1.3.6.1.4.1.48620.41.1.7.3.2). Les clés essentielles pour le cachetage numérique et la garantie de l'authenticité du service sont stockées et gérées de manière sécurisée à l'aide de modules de sécurité matériels cryptographiques (HSM) approuvés par l'industrie.

13.6.2. Gestion du cycle de vie des clés

Le cycle de vie des clés privées, de leur génération à leur destruction, suit un processus rigoureusement contrôlé. Cela inclut des protocoles sécurisés pour la génération, le stockage, l'utilisation, la sauvegarde et la destruction des clés.

13.6.3. Contrôle d'accès aux clés

Seul le personnel occupant des postes de confiance a accès aux clés privées, ce qui empêche tout accès non autorisé.

13.6.4. Mécanisme de double contrôle

Le fournisseur de services utilise des mécanismes de double contrôle, garantissant qu'au moins deux membres du personnel autorisés sont nécessaires pour effectuer toute opération impliquant des clés privées. Cela minimise le risque d'utilisation abusive ou de compromission.

13.6.5. Journaux d'activités liées aux clés

Des journaux détaillés de toutes les activités liées aux clés, y compris leur génération, leur utilisation et leur destruction, sont conservés et révisés périodiquement. Ces journaux sont stockées de manière sécurisée afin de garantir la non-répudiation et la responsabilité.

13.7. Mesures de sécurité pour les systèmes informatiques

Le service PostMi adhère à des objectifs de sécurité rigoureux afin d'assurer la protection, la confidentialité et l'intégrité de ses systèmes informatiques. Les mesures suivantes ont été mises en œuvre :

- Authentification des utilisateurs
  - Des mécanismes d'authentification forte des utilisateurs sont mis en place, notamment l'authentification à deux facteurs (2FA) obligatoire pour tous les utilisateurs.
- Contrôle d'accès

- Les rôles et privilèges des utilisateurs sont définis selon le principe du moindre privilège, garantissant l'accès uniquement aux ressources nécessaires à un rôle spécifique.
- La séparation des rôles est appliquée afin d'éviter les conflits d'intérêts et les actions non autorisées.

- Gestion des sessions :
  - Les sessions des utilisateurs sont surveillées pour détecter toute inactivité et sont automatiquement déconnectées de PostMi après une période de 15 minutes.
  - La durée de validité d'un code à usage unique (OTP) est strictement limitée à 15 minutes.
  - Les journaux d'accès sont régulièrement examinés afin de détecter et de traiter toute anomalie.
- Protection contre les logiciels malveillants
  - Des systèmes anti-malware avancés sont déployés pour détecter et atténuer les menaces, notamment les virus, les ransomwares et les logiciels non autorisés.
  - Toutes les mises à jour logicielles sont soumises à des tests et à une validation rigoureuse avant leur déploiement afin d'éviter l'introduction de vulnérabilités.
- Sécurité
  - Des systèmes de détection d'intrusion (IDS) et de prévention d'intrusion (IPS) surveillent le trafic réseau à la recherche de menaces potentielles.
  - Le chiffrement de bout en bout garantit la confidentialité des données en transit.
- Journaux d'activités
  - Des mécanismes de journalisation complets sont en place pour suivre les actions des utilisateurs, les modifications du système et l'accès aux données.
  - Les journaux sont régulièrement examinés et stockés de manière sécurisée afin de garantir leur intégrité et de faciliter les analyses judiciaires si nécessaire.
- Surveillance du système et alertes
  - Des outils de surveillance continue sont déployés pour détecter en temps réel les accès non autorisés ou les violations des politiques.
  - Des alertes automatisées sont configurées pour informer rapidement le personnel des violations potentielles ou des incidents de sécurité.

13.8. Mesures de sécurité réseau

13.8.1. Segmentation des zones

L'architecture réseau est conçue avec une segmentation robuste afin d'isoler les systèmes critiques et d'améliorer la sécurité et l'évolutivité :

- Segmentation logique et physique :

- Les zones du réseau sont segmentées en fonction de leur sensibilité et de leur fonction, ce qui garantit que les systèmes critiques sont séparés des systèmes non critiques.
- Les environnements de production sont strictement isolés des environnements de test et de développement afin d'éviter toute contamination croisée des données.

- Contrôles d'accès :
  - Les passerelles de sécurité entre les zones sont configurées pour n'autoriser que les protocoles et les communications nécessaires, réduisant ainsi la surface d'attaque.
  - Chaque zone met en œuvre ses propres politiques de sécurité adaptées à son profil de risque spécifique.

13.8.2. Interconnexions

Des interconnexions sécurisées garantissent la protection des transmissions de données :

- Passerelles sécurisées :
  - Les pare-feu et les passerelles entre les réseaux publics et internes sont configurés pour n'autoriser que le trafic essentiel
  - Des protocoles de tunneling sécurisés, tels que TLS et VPN, sont utilisés pour les échanges de données.
- Authentification et intégrité des données :
  - Toutes les données échangées entre les composants du service PostMi sont authentifiées et cryptées afin de garantir leur confidentialité et leur intégrité.

13.8.3. Connexions

L'accès aux zones sécurisées du réseau est réservé au personnel de confiance disposant d'autorisations explicites.

Les réseaux administratifs sont séparés des réseaux opérationnels, garantissant ainsi un environnement dédié et sécurisé pour les opérations sensibles.

Les systèmes sont régulièrement audités afin d'identifier et de supprimer les comptes, applications et services inutilisés, minimisant ainsi les vulnérabilités potentielles.

13.8.4. Disponibilité

Afin d'assurer la continuité du service, les mesures de redondance suivantes sont en place :

- Systèmes à haute disponibilité avec un engagement de disponibilité cloud de 99,99 %.

- Des systèmes redondants et des mécanismes de basculement garantissent un service ininterrompu, même en cas de panne matérielle ou de maintenance.
- Des tests de résistance et des simulations sont régulièrement effectués pour vérifier l'efficacité des mesures de redondance.

- Protocoles de sauvegarde
  - Les sauvegardes des données sont effectuées quotidiennement et stockées en toute sécurité dans des emplacements géographiquement distincts.
  - Les procédures de récupération sont testées régulièrement afin de garantir une restauration rapide en cas de perte de données.

13.9. Gestion des incidents et des vulnérabilités

13.9.1. Surveillance et détection des incidents

Les activités du système sont surveillées en permanence afin de détecter les vulnérabilités ou les violations potentielles :

- Surveillance en temps réel
  - Des outils et des processus dédiés surveillent les performances du système, les modèles d'accès et le trafic réseau.
  - Les menaces potentielles, telles que les accès non autorisés ou les activités inhabituelles, sont immédiatement signalées et transmises aux services compétents.
- Alertes d'incident :
  - Des systèmes automatisés génèrent des alertes en cas d'événements de sécurité critiques, garantissant ainsi des temps de réponse rapides.
  - Les alertes sont classées en fonction de leur gravité afin de hiérarchiser le traitement des incidents.

13.9.2. Gestion et signalement des incidents

Les procédures de gestion des incidents sont conçues pour minimiser l'impact des failles de sécurité :

- Équipes d'intervention
  - Du personnel de confiance est affecté à l'enquête et à la résolution rapide des incidents
  - Une analyse des causes profondes est effectuée afin d'identifier et de corriger les vulnérabilités sous-jacentes.
- Obligations de signalement
  - Toutes les violations de sécurité ou les problèmes d'intégrité des données sont signalés à l'autorité de certification dans les 24 heures suivant leur détection.

- Les personnes ou organisations concernées sont informées sans délai, conformément à la réglementation.

13.9.3. Gestion des vulnérabilités

Le service de lettre recommandée électronique qualifiée PostMi met en œuvre des mesures proactives pour identifier et corriger les vulnérabilités :

- Analyse des journaux d'événements
  - Les journaux de tous les composants sont analysés afin de détecter les schémas indiquant une activité malveillante.
  - Des outils automatisés rationalisent l'identification des menaces potentielles et informent le personnel des résultats critiques.
- Amélioration continue
  - Les enseignements tirés des incidents sont utilisés pour renforcer les mesures de sécurité et mettre à jour les procédures.
  - Des évaluations régulières des vulnérabilités garantissent la résilience du service face aux menaces émergentes.
- Assurance de la conformité :
  - Le fournisseur de services suit un processus structuré pour documenter et vérifier la conformité aux protocoles de sécurité, minimisant ainsi les risques liés aux audits ou aux contrôles réglementaires.

13.10. Gestion des preuves

13.10.1. Événements enregistrés

Le service de lettre recommandée électronique qualifiée PostMi assure une gestion robuste des preuves en enregistrant systématiquement les événements clés liés à la sécurité du système, les transactions de courrier enregistré, les processus cryptographiques, les autorisations et les changements de politique. Les preuves enregistrées garantissent la conformité, la responsabilité et l'auditabilité.

13.10.2. Catégories d'événements enregistrés

13.10.2.1. Événements au niveau du système :

- Démarrage et arrêt des systèmes informatiques et des applications
- Gestion des comptes utilisateurs (création, modification, suppression, gestion des droits d'accès)
- Authentification des utilisateurs et connexions/déconnexions à toutes les composantes du LRE
- Opérations de maintenance du système, y compris les mises à jour logicielles et les correctifs de sécurité

13.10.2.2. Événements liés au service de messagerie enregistré :

- Enregistrement et validation de l'identité des expéditeurs et des destinataires, y compris la méthode d'identification électronique utilisée et les résultats de l'authentification
- Événements du cycle de vie du courrier recommandé (soumission, acceptation, refus, non-réclamation) avec empreintes cryptographiques des données
- Événements liés au cycle de vie des clés cryptographiques et des certificats, tels que la génération (cérémonies de remise des clés), la sauvegarde, la récupération, le renouvellement, la révocation et la destruction
- Génération de preuves qualifiées, y compris les horodatages, les documents scellés et les certificats de validation
- Publication et mise à jour des documents relatifs à la politique et aux conditions d'utilisation du service
- Demandes et approbations/rejets de révocations de méthodes d'authentification

13.10.2.3. Preuves juridiques générées par le service :

- Identité de l'expéditeur et identité du destinataire pour chaque courrier électronique recommandé
- Référence unique identifiée pour chaque courrier électronique recommandé
- Empreintes cryptographiques des documents joints et des métadonnées
- Données garantissant la sécurité des transmissions, y compris les cachets électroniques qualifiés et les horodatages
- Génération des preuves produites par le service

13.10.2.4. Événements liés à la sécurité (enregistrés manuellement ou automatiquement)

- Journaux d'accès physique (enregistrements des entrées et sorties des zones restreintes)
- Changements de rôle du personnel affectant les privilèges d'accès
- Destruction et mise hors service des supports de stockage contenant des données confidentielles (par exemple, clés cryptographiques, informations d'authentification des utilisateurs)

13.10.3. Fréquence de traitement des journaux d'événements

Tous les journaux d'événements sont stockés de manière centralisée dans une base de données sécurisée et sont :

- Analysés manuellement 2 à 3 fois par semaine à des fins de surveillance de la sécurité
- Analysés en continu par des systèmes automatisés de détection des anomalies afin d'identifier en temps réel tout comportement suspect ou toute violation de la sécurité.

Si une anomalie est détectée, des alertes automatiques sont envoyées au personnel de sécurité, garantissant une réponse rapide. Le Prestataire de services s'engage à mettre les enregistrements extraits à disposition à des fins légales ou de conformité dans un délai défini dans les conditions générales.

13.10.4. Période de conservation des journaux d'événements

- Les journaux d'événements actifs sont stockés sur site pendant au moins un mois à des fins de surveillance opérationnelle.
- Les preuves juridiques sont archivées et conservées en toute sécurité pendant 10 ans, conformément aux cadres juridiques et réglementaires (7 ans requis).
- Les autres journaux d'évènements (techniques généraux) sont eux archivés et conservés pendant 2 ans (recommandé de 6 à 12 mois).
- En cas d'interruption du service, toutes les preuves obtenues sont conservées en toute sécurité afin de respecter les obligations légales et d'assurer la continuité du service.

13.10.5. Protection des journaux d'événements

Afin de préserver la confidentialité, la disponibilité et l'intégrité des journaux d'événements, PostMi met en œuvre les mesures de sécurité suivantes :

- Protection de l'intégrité des données
  - Les preuves juridiques sont cryptées et scellées afin d'empêcher toute altération.
  - Les autres journaux d'évènements (techniques généraux) sont cryptés.
  - Des contrôles d'intégrité périodiques sont effectués pour détecter toute modification non autorisée.
- Contrôles d'accès
  - Seul le personnel occupant des postes de confiance a accès aux journaux d'événements.
  - Des mécanismes d'authentification forte, notamment l'authentification multifactorielle (MFA), sont mis en œuvre.
- Synchronisation de l'heure :
  - Tous les événements sont horodatés à l'aide de l'heure système alignée sur UTC.
  - Les horloges système sont synchronisées quotidiennement afin de garantir un suivi précis des événements.
- Stockage inviolable :
  - Les journaux sont cryptés et stockés de manière redondante dans des emplacements sécurisés.
  - Des journaux d'activités sont conservées pour suivre toute tentative d'accès ou de modification.

13.11. Archivage des données

13.11.1. Types de données à archiver

Le service de lettre recommandée électronique qualifiée PostMi met en œuvre l'archivage à long terme des données afin de garantir la durabilité, la conformité et la force exécutoire. Les catégories de données suivantes sont concernées :

13.11.1.1. Documentation relative aux services et au système :

- Versions des logiciels exécutables et fichiers de configuration du système
- Documentation publique, y compris les politiques, les conditions générales et les déclarations de conformité réglementaire.
- Documentation interne régissant les politiques opérationnelles et de sécurité
- Accords contractuels avec des partenaires externes, y compris les prestataires de services de confiance.

13.11.1.2. Courrier recommandé et enregistrements cryptographiques

- Journaux des événements de service, détaillant tous les événements majeurs liés à la sécurité et aux transactions.
- Preuves de dépôt et accusés de réception pour les courriers électroniques recommandés.
- Certificats cryptographiques, enregistrements horodatés et journaux des opérations relatives au cycle de vie des clés (émission, révocation, expiration)

13.11.2. Mesures de stockage et de protection des archives :

- Stockage crypté : toutes les données archivées sont cryptées à l'aide d'algorithmes conformes aux normes de l'industrie afin de garantir leur confidentialité
- Sauvegardes redondantes : les données sont stockées dans plusieurs emplacements géographiquement séparés afin d'éviter toute perte
- Restrictions d'accès : seul le personnel autorisé a accès aux enregistrements archivés
- Mécanismes inviolables : des méthodes de vérification de l'intégrité, telles que le scellage numérique, garantissent l'authenticité des données

Le service PostMi garantit que toutes les données archivées sont conservées en toute sécurité pendant une période minimale de 10 ans, conformément aux exigences réglementaires et à la politique d'archivage (OID : 1.3.6.1.4.1.62466.82.1.2).

14. Gestion de la continuité des activités

Le Prestataire de services a élaboré, documenté, mis en œuvre et maintient actuellement des plans de contrôle, des procédures et des mécanismes visant à garantir le niveau nécessaire de continuité des activités et de sécurité des informations en cas d'événements indésirables.

Un plan de continuité des activités détaillé est en place, qui prévoit la redondance des systèmes critiques. Les sauvegardes sont stockées de manière sécurisée dans des emplacements géographiquement dispersés, conformément aux normes, directives et réglementations applicables en matière de sécurité de l'information.

Le Prestataire de services procède à des examens réguliers de ses mesures de continuité de la sécurité de l'information afin d'évaluer leur efficacité et leur efficience face à d'éventuelles perturbations. L'entreprise veille à ce que les informations et les logiciels essentiels soient régulièrement sauvegardés et puissent être restaurés en cas de sinistre ou de perte de données.

Les processus de reprise sont testés et mis à jour périodiquement afin de garantir leur conformité avec les objectifs définis dans le plan de continuité des activités.

La base de données critique du fournisseur, nécessaire à la restauration des opérations de PostMi à la suite d'un incident ou d'une catastrophe, est conservée en toute sécurité dans des emplacements fiables. Le Prestataire de services est tenu d'informer rapidement les expéditeurs, les destinataires et les tiers concernés de tout incident susceptible d'avoir une incidence sur la prestation des services.

15. Cessation d'activité

Le fournisseur a mis en place un plan de cessation d'activité pour le service PostMi, exploité par BE INVEST International S.A. au Luxembourg et be ys Trusted Solutions Luxembourg SA au Luxembourg, conformément aux exigences des politiques en matière de livraison électronique et du règlement eIDAS.

Objectifs

- Garantir la continuité de la valeur probante des preuves générées par le service, même en cas de cessation ou de transfert du service.
- Se conformer aux normes ETSI, ainsi qu'aux exigences de l'ILNAS (Luxembourg) et de l'ANSSI (France).

Scénarios de fin de vie du service

Transfert à une autre filiale du groupe BeYs

- Maintenir la qualification eIDAS dans le territoire concerné.
- Notification préalable des organismes de contrôle (ILNAS/ANSSI) et des utilisateurs (au moins un mois à l'avance).
- Transfert des archives, des preuves, des responsabilités contractuelles et techniques à la filiale.
- Mise à jour de la politique du service et audit éventuel.
- Révocation des certificats de sceau et destruction des secrets non transférés.

Transfert à un tiers qualifié

- Sélection d'un prestataire déjà qualifié eIDAS via la liste de confiance.
- Notification aux autorités de contrôle et aux utilisateurs (avec un préavis d'au moins un mois).
- Transfert des archives et des preuves au nouveau fournisseur (sans transfert du certificat de sceau).
- Négociation des modalités techniques, organisationnelles et financières.
- Révocation des certificats de sceau et destruction des secrets non transférés.

Interruption définitive du service

- Décision prise après examen des possibilités de transfert.
- Notification aux autorités de contrôle et aux utilisateurs (avec un préavis d'au moins un mois).
- Arrêt progressif du service (plus aucun envoi, accès continu aux messages existants).
- Archivage des preuves juridiques pendant une période de 10 ans et des journaux d'évènements techniques généraux pendant une période de 2 ans, soit en interne, soit auprès d'un archiviste tiers.
- Révocation des certificats de sceau, destruction des secrets et résiliation des contrats liés au service.

Obligations de publication

- Maintien de la publication de la politique du service, des conditions d'utilisation et des certificats de sceau électronique.
- Fourniture des documents nécessaires aux anciens utilisateurs pour la vérification des preuves.

Pour plus de détails, veuillez-vous référer au document original « Plan de cessation d'activité » de BeYs.

16. Audit et conformité

16.1. Fréquence et calendrier des audits et des évaluations

Afin de maintenir la conformité avec les exigences eIDAS, le service PostMi est soumis à des audits de sécurité et de conformité systématiques. Ces audits permettent d'évaluer et de renforcer l'efficacité des contrôles de sécurité, l'intégrité du service et le respect des politiques de certification.

Le processus d'audit est structuré comme suit :

- Audits de conformité réguliers :
  - Réalisés au moins deux fois par an par le C2SC (Comité de pilotage sur la cybersécurité et la conformité)
- Audits déclenchés :
  - Lancés chaque fois qu'une modification importante est apportée à un composant du système PostMi (par exemple, modifications de l'infrastructure, correctifs de sécurité, mises à jour des politiques)
- Audits de certification et de qualification :
  - Requis pour les autorisations réglementaires
- Tests de pénétration et audits de sécurité :
  - Réalisés chaque année et après toute mise à jour majeure du système
- Audits post-incident :
  - Réalisés après une faille de sécurité, une panne du système ou une perturbation opérationnelle majeure afin d'évaluer l'impact de l'incident et de remédier aux vulnérabilités.

16.2. Identité et qualifications des auditeurs, relation entre les auditeurs et les entités évaluées

Le C2SC nomme des auditeurs de sécurité certifiés, internes ou externes, possédant une expertise en matière de services de confiance, de sécurité cryptographique et de conformité réglementaire. Les auditeurs sélectionnés :

- Doivent être indépendants des équipes opérationnelles du service PostMi
- Doivent posséder des connaissances approfondies en matière de sécurité de l'information et des cadres réglementaires applicables.
- Doivent être dûment autorisés à effectuer des évaluations de sécurité, des vérifications de conformité et des évaluations des risques
- Peuvent provenir d'un cabinet d'audit externe spécialisé dans les services de confiance qualifiés.
- Ne doivent avoir aucun conflit d'intérêts avec l'entité évaluée.

Pour la certification eIDAS, les auditeurs doivent être des organismes d'évaluation de la conformité (OEC) reconnus et accrédités.

17. Stratégie de maintien et de renouvellement de la certification

Afin de conserver les certifications requises, le service PostMi suit une stratégie de renouvellement structurée :

- Audits internes annuels : contrôles de conformité réguliers avant les audits externes prévus
- Préparation aux audits : amélioration continue de la sécurité, mise à jour de la documentation et perfectionnement des processus
- Engagement des parties prenantes : collaboration étroite avec les organismes de certification, les équipes juridiques et les consultants en sécurité
- Hiérarchisation des risques : prise en compte des nouvelles menaces de sécurité, des changements réglementaires et de l'évolution des normes du secteur

En maintenant des cycles d'audit stricts, des améliorations proactives en matière de sécurité et une transparence réglementaire, PostMi garantit la conformité continue des certifications et la fiabilité dans le domaine du courrier électronique recommandé.

18. Autres questions commerciales et juridiques

18.1. Tarifs

Les conditions financières régissant le service PostMi sont clairement définies dans le contrat conclu entre le Prestataire de services et ses clients. Ces contrats précisent au moins les éléments suivants :

- Conditions de facturation :
  - Le modèle tarifaire du service PostMi, y compris les différents frais
  - Tous les coûts supplémentaires éventuels (par exemple, frais de stockage des preuves archivées, fonctionnalités de sécurité avancées, rapports de conformité)
- Responsabilités :
  - Obligations du Prestataire de services et du client en matière de conformité, de sécurité et d'utilisation du service.
- Responsabilités financières :
  - Limitations de responsabilité en cas d'interruption du service, d'incidents de sécurité ou de cas de force majeure

Toutes les conditions financières sont juridiquement contraignantes et consignées dans le contrat afin de garantir la transparence et l'applicabilité.

18.2. Responsabilité financière

Le Prestataire de services a conclu un contrat d'assurance avec un organisme d'assurance reconnu qui lui permet de couvrir les risques liés au service PostMi. Ce contrat couvre également les processus de transfert ou de cessation des activités.

18.3. Couverture et garantie pour les entités utilisatrices

- La couverture financière du Prestataire et de ses filiales garantit le respect de tous les engagements contractuels liés à la conservation des preuves, à la disponibilité du service et à la conformité réglementaire.
- En cas de transfert ou de cessation du service, des réserves financières suffisantes sont allouées pour garantir que toutes les données des clients, les enregistrements de preuves et les preuves juridiques restent accessibles et vérifiables pendant la période contractuellement requise.

18.4. Portée des informations confidentielles

Le service PostMi met en œuvre des politiques strictes de classification et de contrôle d'accès afin de protéger les informations commerciales sensibles. Les informations confidentielles sont classées conformément à la PSI (Politique de sécurité de l'information).

Mesures de protection de la confidentialité :

- Restrictions d'accès : Seul le personnel autorisé disposant d'une habilitation de sécurité spécifique peut accéder aux données confidentielles.
- Normes de cryptage : toutes les données stockées et transmises sont protégées à l'aide du cryptage AES-256 et des normes TLS
- Mesures d'intégrité des données : la signature cryptographique garantit que les journaux, les enregistrements et les données de transaction restent inaltérés
- Surveillance de la sécurité : un système de détection d'intrusion (IDS) continu et une analyse automatisée des menaces empêchent tout accès non autorisé aux informations classifiées.

En appliquant des mesures strictes de protection de la confidentialité des données, le service PostMi est conforme au RGPD et aux dernières normes garantissant le respect des réglementations de sécurité essentielles à l'activité.