Qualification eIDAS 2017

Dossier Recommande

Section Politiques et pratiques

Politique du service d'envoi Recommandé Electronique ClearBUS

Version	Date	Description	Auteurs	Société
1.0	31/07/2018	Rédaction initiale	Céline Burgod	**ClearBUS**
1.1	05/11/2018	Corrections suite à l'audit	Céline Burgod	**ClearBUS**
1.2	16/11/2018	Corrections mineurs	Céline Burgod	**ClearBUS**

Etat du document	**Classification**
Final	C1
OID du document	
1.3.6.1.4.1.38116.2.1.1.1	
Diffusion	
Document public	

SOMMAIRE

1 INTRODUCTION

1.1 Présentation générale

ClearBUS met en œuvre un Service d'envoi Recommandé Electronique, qui assure une distribution sécurisée et fiable de messages entre parties, en apportant la preuve du processus de distribution pour des besoins de responsabilité juridique. La règlementation en vigueur amène **ClearBUS** à faire qualifier son service de Recommandé Electronique, au sens de l'article 44 du Règlement Européen [eIDAS].

ClearBUS se positionne dans ce contexte en tant que Prestataire de Service d'envoi Recommandé Electronique (ci-après « PSRE »). Le présent document constitue la Politique d'envoi Recommandé Electronique de **ClearBUS** (ci-après « PRE ») présentant ce service.

La présente PRE expose les pratiques que **ClearBUS** applique et s'engage à respecter dans le cadre de la fourniture de son Service d'envoi Recommandé Electronique (ci-après « ClearBUS-SRE »). La PRE identifie également les obligations et exigences portant sur les autres intervenants, et les utilisateurs du service.

Le présent document est complété, dans sa partie mise en œuvre, par une Déclaration des Pratiques d'envoi Recommandé Electronique (ci-après « DPRE »), et des Conditions Générales d'Utilisation du service d'envoi Recommandé Electronique (ci-après « CGURE »).

La présente PRE vise la conformité :

- Au Règlement Européen [eIDAS] N°910/2014 pour le service d'envoi recommandé électronique qualifié ;
- Aux spécifications de l'ETSI [EN_319401] et [TS_102640-3] ;
- Aux exigences prévues par l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) dans les référentiels [PSCO_QUALIF] et [PSCO_ENVOI_RECO].

Le respect de cette politique permet, après un audit de conformité selon les processus établis dans le Règlement Européen [eIDAS], la qualification du Service d'envoi Recommandé Electronique de **ClearBUS** par l'organe de contrôle national, l'ANSSI.

La structure de la présente Politique d'envoi Recommandé Electronique est basée sur les documents issus de la norme ETSI [EN_319401].

1.2 Définitions

Pour les besoins du présent document, les termes et définitions suivants s'appliquent :

Consignation : acte de rendre le contenu d'utilisateur disponible au destinataire, dans les limites du service d'envoi recommandé électronique

Service d'envoi Recommandé Electronique (SRE) : service électronique permettant de transmettre des données entre l'expéditeur et les destinataires par des moyens électroniques et apportant des preuves concernant le traitement des données transmises, y compris la preuve de l'envoi et de la réception des données, et qui protège les données transmises contre le risque de perte, de vol, de dommage ou de toute modification non autorisée

NOTE : Un service d'envoi recommandé électronique est fourni par un PSRE. Les PSRE peuvent coopérer pour transférer les données d'un expéditeur à un destinataire lorsqu'ils sont abonnés à des PSRE différents.

Preuve de Service d'envoi Recommandé Electronique : données générées au sein du service d'envoi recommandé électronique, qui vise à prouver qu'un certain événement s'est produit à un certain moment.

Déclaration de pratiques de Service d'envoi Recommandé Electronique (DPSRE) : déclaration des pratiques employées par un prestataire de services d'envoi recommandé électronique pour fournir ses services.

Prestataire de Services d'envoi Recommandé Electronique (PSRE) : prestataire de services de confiance qui fournit des services d'envoi recommandé électronique.

NOTE : Il s'agit d'un prestataire de services de confiance tel que défini dans le Règlement (UE) n° 910/2014 [i.1].

Agent/application d'utilisateur : système constitué de composants logiciels et/ou matériels par lesquels les expéditeurs et les destinataires participent à l'échange de données avec des prestataires de services d'envoi recommandé électronique.

Service d'envoi Recommandé Electronique qualifié : comme spécifié dans le Règlement (UE) n° 910/2014 [i.1].

Prestataire de Services d'envoi Recommandé Electronique qualifié : prestataire de services de confiance qui fournit des services d'envoi recommandé électronique qualifiés.

Destinataire : personne physique ou morale à laquelle est adressé le contenu d'utilisateur.

Expéditeur : personne physique ou morale qui soumet le contenu d'utilisateur.

Contenu d'utilisateur : données originales produites par l'expéditeur qui doivent être transmises au destinataire.

NOTE : Il s'agit de tout type de documents numériques avec pièces jointes qui composent l'envoi.

Opérateur du Service d'envoi Recommandé Electronique (OSRE) : au sein d'un PSRE, l'Opérateur du Service d'envoi Recommandé Electronique a en charge la mise en œuvre technique du service.

1.3 Abréviations

Pour le présent document, les abréviations suivantes s'appliquent :

AC	Autorité de Certification
AH	Autorité d'Horodatage
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
CGURE Electronique	Conditions Générales d'utilisation du service d'envoi Recommandé
CSPN	Certification de Sécurité de Premier Niveau
DPRE	Déclaration des Pratiques d'envoi Recommandé Electronique

ETSI	*European Telecommunications Standards Institute*
LCR	Liste des Certificats Révoqués
LRE	Lettre Recommandée Electronique
MIE	Moyen d'Identification Electronique
OID	*Object Identifier*
OSRE	Opérateur de Service d'envoi Recommandé Electronique
OTP	*One-time Password*
PC	Politique de Certification
PDF	*Portable Document Format*
PH	Politique d'Horodatage
PKCS	*Public-Key Cryptography Standard*
PRE	Politique d'envoi Recommandé Electronique
PSCE	Prestataire de Services de Certification Electronique
PSCo	Prestataire de Service de Confiance
PSCK	*Portable Symmetric Key Container*
PSHE	Prestataire de Services d'Horodatage Electronique
PSRE	Prestataire de Services d'envoi Recommandé Electronique
RGS	Règlement Général de Sécurité
SRE	Service d'envoi Recommandé Electronique
UTC	*Coordinated Universal Time*

1.4 Identification du document

La présente « Politique d'envoi Recommandé Electronique **ClearBUS** » est identifiée, au sein du référentiel documentaire de l'infrastructure de confiance **ClearBUS**, par un numéro d'identification unique, l'OID : **1.3.6.1.4.1.38116.2.1.1.1.**

D'autres éléments, plus explicites, (nom, numéro de version, date de mise à jour) permettent également de l'identifier.

1.5 Entités intervenant dans le service d'envoi recommandé électronique et obligations

1.5.1 Prestataire de Service d'envoi Recommandé Electronique (PSRE)

Le PSRE est garant de l'application opérationnelle de la Politique d'envoi Recommandé Electronique. **ClearBUS** assure directement ce rôle, et s'organise à partir d'un Comité de Pilotage.

Ce Comité de Pilotage a notamment pour mission de :

- Faire réaliser les analyses de risques sur le périmètre dont il a la charge ;

- Décider de la stratégie de gestion des risques ;
- Valider et suivre les plans d'actions correspondants ;
- Faire réaliser les audits internes sur sa composante, et suivre la mise en place des mesures correctives nécessaires.

ClearBUS assure tout ou partie de ces fonctions directement ou en les sous-traitant. Dans tous les cas, **ClearBUS** en garde la responsabilité.

ClearBUS, en tant que PSRE s'engage à :

- Respecter et se conformer aux exigences et procédures définies dans la présente Politique et dans les Conditions Générales d'Utilisation applicables, même lorsque certaines fonctionnalités sont remplies par des sous-traitants ;
- Surveiller régulièrement le statut des Prestataires de Service de Confiance qualifiés tiers participants à la fourniture de son service à travers la liste de confiance nationale ou européenne ;
- Garantir que la mise en œuvre des exigences exprimées dans le présent document est faite conformément à ce qui est décrit dans sa Déclaration des Pratiques d'envoi Recommandé Electronique ;
- Mettre à disposition de ses clients et utilisateurs l'ensemble des informations nécessaire à la vérification des preuves électronique qu'il aura émises, selon les modalités indiquées dans le présent document ;
- Utiliser des certificats serveur (cachet, SSL) sous sa responsabilité, conformément aux exigences de la Politique de Certification de l'Autorité de Certification (AC) émettrice ;
- Utiliser jetons d'horodatage sous sa responsabilité, conformément aux exigences de la Politique d'Horodatage de l'Autorité d'Horodatage émettrice.

ClearBUS s'appuie sur une organisation interne, nommée Opérateur du Service d'envoi Recommandé (OSRE), pour la mise en œuvre technique du service.

1.5.2 Fournisseur d'identification

ClearBUS assure la fonction qui consiste à vérifier l'identité de ses utilisateurs et la qualité des données fournies avant de procéder à la remise d'un moyen d'identification et/ou d'authentification électronique.

ClearBUS peut s'appuyer sur des fournisseurs d'identification reconnus au niveau national ou européen pour assurer la vérification d'identité de ses utilisateurs. Les services fournis doivent respecter les spécifications de sécurité de niveau « substantiel » ou « élevé » définies dans le règlement d'exécution fixant les spécifications techniques et procédures minimales relatives aux niveaux de garantie des moyens d'identification électronique [RE_2015_1502].

1.5.3 Prestataire de Service de Certification Electronique (PSCE)

CleaBUS installe des certificats cachet serveur pour sceller les preuves électroniques produites au sein du service d'envoi recommandé électronique.

Les certificats cachet serveur sont émis par une Autorité de Certification régie par des règles de certification conformes à la norme ETSI EN 319 411-1, ou par des règles et

pratiques reconnues au niveau national par la règlementation en vigueur (RGS). Cette Autorité de Certification est externe à **ClearBUS**.

L'Autorité de Certification doit :

- Assurer l'émission des certificats cachet serveur dans les conditions décrites dans sa politique de certification ;
- Mettre à destination de ses clients et utilisateurs du service les moyens de vérification des certificats qu'elle aura émis, c'est à dire la chaîne de certification et le statut de révocation des certificats, selon les modalités indiquées dans sa politique de certification ;

1.5.4 Prestataire de Service d'Horodatage Electronique (PSHE)

ClearBUS utilise un horodatage électronique qualifié pour indiquer la date et l'heure d'envoi, de réception et toute modification des données, et pour signer les preuves générées au sein du service d'envoi recommandé électronique

Les jetons d'horodatage sont émis soit par une Autorité d'Horodatage interne à **ClearBUS**, soit par une autorité externe.

Chaque Autorité d'Horodatage est garante des conditions d'émission des jetons, selon sa politique d'horodatage qualifiée selon le Règlement Européen [eIDAS] (cf. section 3.5.2).

L'Autorité d'Horodatage doit :

- Assurer la génération de jetons d'horodatage qualifiés ;
- Mettre à disposition de ses clients et utilisateurs l'ensemble des informations nécessaires à la vérification des jetons d'horodatage qu'elle aura émis, selon les modalités indiquées dans sa politique d'horodatage ;
- Respecter les conditions de disponibilité du service d'horodatage convenues contractuellement.

1.5.5 Utilisateurs

1.5.5.1 Expéditeur

Personne morale ou personne physique ayant besoin d'envoyer et/ou de recevoir des lettres recommandées électroniques (LRE), et qui a accepté les conditions d'utilisation de ce service.

L'Expéditeur est nécessairement un ***Abonné*** (principal ou secondaire) du système **ClearBUS**, auprès duquel il s'est identifié préalablement avec un niveau de garantie « élevé ».

L'Expéditeur s'engage à ne pas envoyer via le service **ClearBUS-SRE** des messages dont le contenu serait contraire à l'ordre public et à la bienséance ou qui porterait atteinte à la moralité d'un tiers. Il s'engage à ne pas envoyer de messages contenant des virus informatiques ou tout autre programme dont la finalité serait d'endommager ou de détruire des appareils informatiques, des systèmes ou des logiciels.

L'Expéditeur doit :

- Utiliser les interfaces fournies par **ClearBUS** pour envoyer et recevoir des recommandés électroniques ;

- Obtenir le consentement du destinataire à recevoir des envois recommandés électroniques, lorsque celui-ci n'est pas un professionnel ;
- Tenir compte des limitations sur l'utilisation du service indiquées dans la présente Politique d'envoi Recommandé Electronique, et dans les Conditions Générales d'Utilisation.

1.5.5.2 Destinataire

Personne physique ou sous-système utilisateur qui utilise le service **ClearBUS-SRE** pour recevoir des recommandés électroniques.

Le ***Destinataire*** peut être ***Inscrit*** ou ***Abonné*** **ClearBUS**, ou bien il est considéré comme un ***Invité*** du système.

Cet utilisateur doit :

- Utiliser les interfaces fournies par **ClearBUS** pour recevoir des recommandés électroniques ;
- Appliquer la Procédures de relève correspondant à son Profil d'Utilisateur ;
- Tenir compte des limitations sur l'utilisation du service indiquées dans la présente Politique d'envoi Recommandé Electronique, et dans les Conditions Générales d'Utilisation ;
- Mettre en œuvre les moyens de conservation du contenu du recommandé électronique qui lui conviennent, après que le système le lui ait délivré.

L'utilisateur assume les limitations connues et documentées du service **ClearBUS-SRE**.

2 GESTION DES RISQUES

2.1 Analyse de risques

Une appréciation des risques est réalisée par **ClearBUS** afin d'identifier, d'analyser et d'évaluer les risques liés au service d'envoi recommandé électronique, en prenant en compte les enjeux techniques et commerciaux. Cette analyse de risque met en exergue, en particulier, les systèmes « critiques » du service.

ClearBUS prend en compte les résultats de l'appréciation des risques pour déterminer les mesures de traitement, de sorte à assurer un niveau de sécurité proportionné au degré de risque.

ClearBUS détermine toutes les exigences de sécurité et procédures opérationnelles nécessaires pour implémenter les mesures de sécurité sélectionnées, comme documenté dans la Politique de Sécurité du Système d'Information et dans la Déclaration des Pratiques d'envoi Recommandé Electronique.

Cette appréciation des risques est revue et révisée régulièrement, a minima tous les deux ans et lors de toute évolution significative d'un système ou d'une composante du service.

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

2.2 Homologation

Le Système d'Information du service doit être homologué préalablement à la fourniture du service. L'appréciation des risques est donc approuvée par la direction de **ClearBUS,** qui accepte ainsi les éventuels risques résiduels identifiés ; cette phase correspond à l'homologation du système d'information du service.

Cette homologation doit être prononcée au moins tous les trois (3) ans.

3 POLITIQUES ET PRATIQUES

3.1 Politique d'envoi Recommandé Electronique

Les caractéristiques principales de cette politique sont les suivantes :

- Utilisation de systèmes et produits fiables, sécurité et fiabilité des processus ;
- Conservation des informations délivrées et reçues dans le cadre de l'envoi d'un recommandé électronique pendant sept (7) ans ;
- Continuité de service suite à l'arrêt d'activité d'envoi recommandé électronique ;
- Identification de l'expéditeur avec un niveau de confiance élevé ;
- Identification du destinataire avant la fourniture des données ;
- Sécurisation de l'envoi et de la réception des données par un cachet électronique qualifié de manière à exclure toute possibilité de modification indétectable des données ;

Pour cette politique, les preuves électroniques liées aux évènements du processus d'acheminement d'un recommandé électronique sont vérifiables pendant au moins un (1) an après leur génération.

La présente politique impose un format de preuve électronique spécifique, décrit au chapitre 5.8.2.1.

3.2 Déclaration des Pratiques d'envoi Recommandé Electronique

ClearBUS a défini un document de Déclaration des Pratiques d'envoi Recommandé Electronique (DPRE) décrivant les mécanismes et les procédures mis en œuvre pour atteindre les objectifs de sécurité de la présente PRE.

La DPRE est une description détaillée des pratiques opérationnelles de **ClearBUS-SRE** mises en œuvre pour fourniture et la gestion de son service.

La DPRE définit comment **ClearBUS-SRE** se conforme aux exigences physiques, environnementales, procédurales, organisationnelles et techniques identifiées dans cette politique d'envoi recommandé électronique.

Ce document interne garantit que **ClearBUS** possède la fiabilité nécessaire pour fournir les Services d'envoi Recommandé Electronique, notamment :

- **ClearBUS** a rédigé une analyse des risques de son service de confiance ;
- **ClearBUS** adresse l'ensemble des exigences décrites dans la présente PRE ;
- La DPH décrit toutes les exigences que doivent respecter les éventuelles tierces parties dans le cadre du Service d'envoi Recommandé Electronique ;
- **ClearBUS** met à disposition des utilisateurs les données nécessaires à la validation des preuves électroniques, soit :
    - Les certificats de signature ;
    - Les CRL de l'AC ;
    - Le certificat de l'AC ;

  - Toutes les versions des Politiques d'envoi Recommandé Electronique avec leur date de validité.
- **ClearBUS** organise un audit interne pour attester que la DPRE est conforme à la PRE ;
- L'audit organisé par **ClearBUS** prend en compte le contrôle des mesures techniques, non techniques et organisationnelles ;
- **ClearBUS** garantit la mise à jour la PRE en cas de changements majeurs des pratiques de son service ;
- **ClearBUS** publiera les nouvelles versions de la PRE sur le site www.clearbus.fr ;
- **ClearBUS** garantit que tout changement majeur dans ses Pratiques d'envoi Recommandé Electronique fera l'objet d'une notification auprès de l'organe de contrôle ayant délivré la qualification eIDAS de son service.

Contrairement à la PRE, la DPRE n'est pas publiée. Les informations publiques de la DPRE sont intégrées aux conditions générales d'utilisation du service d'envoi Recommandé Electronique (cf. section 3.3).

3.3 Conditions Générales d'Utilisation

Compte tenu de la complexité de lecture d'une PRE pour des utilisateurs non-spécialistes du domaine, **ClearBUS-SRE** définit également des conditions générales d'utilisation.

Ces conditions générales d'utilisation ne sont pas destinées à remplacer la Politique d'envoi Recommandé Electronique mais sont destinées à des utilisateurs du service non-techniciens afin qu'ils puissent facilement comprendre l'information essentielle dont ils doivent avoir connaissance.

Les conditions générales d'utilisation peuvent aider à démontrer comment **ClearBUS-SRE** répond aux exigences réglementaires, en particulier celles liées à la protection du consommateur.

Les CGU intègrent à minima les informations suivantes :

- Le cadre d'application des CGURE et le contexte global des engagements de **ClearBUS** via la PRE et la DPRE ;
- La PRE et la DPRE appliquée ;
- Les coordonnées du point de contact de **ClearBUS-SRE** ;
- Les limites sur l'utilisation du service ;
- Les obligations de l'abonné ;
- Les obligations des utilisateurs du service ;
- Les dispositions permettant de valider la chaîne de certificats liée aux preuves électroniques ;
  - La période de temps minimum, hors cas de révocation, durant laquelle les preuves électroniques concernant le traitement des données transmises seront vérifiables ;
- La période de temps durant laquelle les journaux d'évènement sont conservés ;

- Les limites de garantie et limites de responsabilité ;
- Les règles appliquées en matière de protection des informations confidentielles ;
- Les règles appliquées en termes d'assurance ;
- Les lois applicables et les procédures de résolution des litiges ;
- Les niveaux de certifications et les audits obtenus ;
- La description de ce qui est considéré être un envoi recommandé électronique ;
- La durée de disponibilité des données d'un envoi recommandé électronique au destinataire ;

Les CGURE sont accessibles aux abonnés et aux utilisateurs via le site de **ClearBUS** à l'adresse suivante : https://www.clearbus.fr/conditions_generales.

3.4 Politique de Sécurité de l'Information

ClearBUS dispose d'une Politique de Sécurité du Système d'Information (PSSI). Cette PSSI est documentée, implémentée, maintenue, révisée annuellement et approuvée par la Direction.

La PSSI est un document de référence, commun à l'ensemble des services de **ClearBUS**, qui expose les enjeux et la démarche retenue en matière de gestion de la sécurité de l'information. Elle est communiquée à l'ensemble du personnel et des intervenants impactés.

3.5 Documents associés

3.5.1 Produits certifiés

Produit : Librairie ClearBUS Secure version 1.1

Référentiel : Certification de Sécurité de Premier Niveau

Cibles de sécurité : authentification serveur, signature électronique, et protection des données lors de la transmission

Rapport de certification : ANSSI-CSPN-2012/02, disponible à l'adresse suivante https://www.ssi.gouv.fr/administration/certification_cspn/librairie-clearbus-secure-version-1-1

3.5.2 Politique de certification cachet serveur

Politique de certification cachet serveur en vigueur : CERTEUROPE ADVANCED CA V4

OID : 1.2.250.1.105.12.3.1.0

3.5.3 Politique d'Horodatage

3.5.3.1 ClearBUS

Politique d'horodatage en vigueur : Politique d'Horodatage du service ClearBUS

OID : 1.3.6.1.4.1.38116.1.1.1.2

3.5.3.2 Luxtrust

Politique d'horodatage en vigueur : LuxTrust Time Stamping V2 Policy

OID : 1.3.171.1.1.1.10.8

3.5.4 Documents normatifs

3.5.4.1 Règlementation

Renvoi	Document
[CNIL]	Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la Loi n°2018-493 du 20 juin 2018
[eIDAS]	Règlement n°910/2014 du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive n°1999/93/CE Disponible sur http://www.europa.eu
[RE_2015_1502]	Règlement d'exécution (UE) 2015/1502 de la commission du 8 septembre 2015 fixant les spécifications techniques et procédures minimales relatives aux niveaux de garantie des moyens d'identification électronique visés à l'article 8, paragraphe 3, du règlement (UE) no 910/2014 du Parlement européen et du Conseil sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur Disponible sur http://www.europa.eu
[RGPD]	Règlement n°679/2016 du 27 avril 2016 sur la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive n°95/46/CE Disponible sur http://www.europa.eu

3.5.4.2 Documents techniques

Renvoi	Document
[EN_301549]	ETSI EN 301 549 : Accessibility requirements for ICT products and services Disponible sur http://www.etsi.org
[EN_319401]	ETSI EN 319 401 : Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers

	Disponible sur http://www.etsi.org
[GH]	Guide d'hygiène informatique. Disponible sur http://www.ssi.gouv.fr
[ISO_27002]	ISO/IEC 27002:2013 Technologies de l'information -- Techniques de sécurité -- Code de bonne pratique pour le management de la sécurité de l'information
[PSCO_DELIV_CERT]	Services de délivrance de certificats qualifiés de signature électronique, de cachet électronique et d'authentification de site internet - Critères d'évaluation de la conformité au règlement eIDAS, version en vigueur Disponible sur http://www.ssi.gouv.fr
[PSCO_QUALIF]	Services d'envoi recommandé électronique qualifiés - Critères d'évaluation de la conformité au règlement eIDAS, version en vigueur Disponible sur http://www.ssi.gouv.fr
[PSCO_ENVOI_RECO]	Prestataires de services de confiance qualifiés - Critères d'évaluation de la conformité au règlement eIDAS, version en vigueur Disponible sur http://www.ssi.gouv.fr
[TS_102640-3]	ETSI TS 102 640-3 V2.1.2 (2011-09) : Technical Specification Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM); Part 3: Information Security Policy Requirements for REM Management Domains Disponible sur http://www.etsi.org
[TS_119312]	ETSI TS 119 312 : Electronic Signatures and Infrastructures (ESI); Cryptographic suites

3.6 Gestion de la PRE et de la DPRE

3.6.1 Entité gérant la politique et les déclarations de pratiques

ClearBUS dispose d'un Comité responsable de l'élaboration, du suivi, de la modification, et de la validation de la présente PRE, et de la DPRE correspondante.

Ce Comité est composé de membres dirigeants de **ClearBUS** et des experts techniques du service **ClearBUS-SRE** couvrant les compétences de sécurité, réseaux, systèmes nécessaires au service d'envoi recommandé électronique.

Ce Comité approuve la présente Politique d'envoi Recommandé Electronique, et la DPRE correspondante avant la mise en production du service.

3.6.2 Procédure d'approbation de la conformité de la DPRE

L'approbation de la conformité de la DPRE à la Politique d'envoi Recommandé Electronique est prononcée par le Comité **ClearBUS** après un processus de revue de la conformité de la DPRE aux exigences de la PRE.

3.6.3 Point de contact

ClearBUS

75 rue Ampère

38000 Grenoble

FRANCE

Contact email : support@clearbus.fr

3.6.4 Processus de mise à jour

3.6.4.1 Circonstances rendant une mise à jour nécessaire

La mise à jour de la Politique d'envoi Recommandé Electronique est un processus impliquant tous les acteurs et faisant l'objet d'une démarche rigoureuse. Il est enclenché essentiellement pour procéder à des modifications importantes, pour prendre en compte de nouveaux besoins, de nouveaux acteurs, améliorer le cadre juridique ou combler des lacunes.

La Politique d'envoi Recommandé Electronique est réexaminée à minima tous les deux (2) ans.

3.6.4.2 Prise en compte des mises à jour

Toutes les remarques, ou souhaits d'évolution, sur la présente Politique sont à adresser par courriel à l'adresse suivante :

support@clearbus.fr

Ces remarques et souhaits d'évolution sont examinés par le Comité d'Approbation, qui engage si nécessaire le processus de mise à jour de la présente Politique.

3.6.4.3 Information des acteurs

Lorsqu'une mise à jour a été planifiée, les informations relatives à cette évolution sont mises en ligne sur les lieux de publication (cf. 3.7.3).

ClearBUS adresse annuellement à l'ANSSI une synthèse de l'ensemble des modifications apportées à la fourniture de ses services de confiance qualifiés.

Indépendamment de ce mode de communication, les acteurs peuvent à tout moment se renseigner auprès du Comité d'Approbation pour obtenir plus d'informations, en envoyant un courriel à support@clearbus.fr.

La publication d'une nouvelle version de la Politique d'envoi Recommandé Electronique consiste à archiver la version précédente et mettre en ligne dans le répertoire prévu à cet effet, les éléments suivants :

- Document au format PDF ;

- OID du document ;
- Date et heure exacte d'entrée en vigueur.

Le document archivé porte, en filigrane sur ses pages, la mention « Document obsolète ».

3.6.5 Entrée en vigueur de la nouvelle version et période de validité

Lorsqu'une nouvelle version de la Politique d'envoi Recommandé Electronique est mise en ligne, tous les utilisateurs des infrastructures de **ClearBUS-SRE** sont informés de la nature, de la date et de l'heure du changement, par courriel ou via une publication officielle sur le site **ClearBUS** à l'adresse www.clearbus.fr.

La nouvelle version de la Politique d'envoi Recommandé Electronique entre en vigueur après sa mise en ligne et reste valide jusqu'à l'entrée en vigueur d'une nouvelle version.

3.6.6 Cohérence de la documentation

Cette Politique décrit le contexte de production du service d'envoi Recommandé Electronique et, de fait, ne constitue qu'une brique du référentiel documentaire de **ClearBUS-SRE**.

Le Comité **ClearBUS** s'assure de la cohérence de ce référentiel documentaire et de l'adéquation de la présente Politique d'envoi Recommandé Electronique avec les autres documents.

3.7 Responsabilités concernant la mise à disposition des Informations devant être publiées

3.7.1 Entités chargées de la mise à disposition des informations

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

3.7.2 Informations devant être publiées

ClearBUS publie à destination des abonnés et des utilisateurs :

- La présente Politique d'envoi Recommandé Electronique ;
- Les Conditions Générales d'Utilisation liées au service de recommandé électronique ;
- Les certificats serveurs ;
- La Déclaration des Pratiques d'envoi Recommandé Electronique, sur demande auprès de **ClearBUS**.

3.7.3 Publication de la documentation

3.7.3.1 Politique d'envoi Recommandé Electronique

Avant toute publication officielle, la Politique d'envoi Recommandé Electronique est validée par le Comité d'Approbation **ClearBUS**.

La présente PRE est publiée sur l'URL : www.clearbus.fr/Telechargements/PRE_Clearbus_1.3.6.1.4.1.38116.2.1.1.1.pdf

L'ensemble des informations associées, notamment les versions antérieures publiques de ces documents, sont également publiées sur le site interne à la société **ClearBUS**. Les versions antérieures publiques peuvent être fournies sur requête effectuée par courriel à l'adresse suivante : support@clearbus.fr.

3.7.3.2 Déclaration des Pratiques d'envoi Recommandé Electronique

ClearBUS publie, à destination des abonnés de **ClearBUS-SRE**, et sur leur demande effectuée par courriel à l'adresse suivante : support@clearbus.fr, sa DPRE pour rendre possible l'évaluation de la conformité avec sa politique d'envoi recommandé électronique.

Les détails relatifs à ses pratiques ne sont pas rendus publics.

3.7.4 Délais et fréquences de publication

Les informations liées au service sont publiées dès que nécessaire afin que soit assurée à tout moment la cohérence entre les informations délivrées et les engagements, moyens et procédures de **ClearBUS**.

ClearBUS garantit la disponibilité et l'intégrité des informations publiées.

4 IDENTIFICATION ET AUTHENTIFICATION DES UTILISATEURS

4.1 Catégories d'utilisateurs

ClearBUS connait trois catégories d'Utilisateurs, personnes morales ou personnes physiques. Les utilisateurs ***Abonnés***, les utilisateurs destinataires ***Inscrits*** et les utilisateurs occasionnels (dits ***Invités***)

4.1.1 Utilisateurs Inscrits

Les utilisateurs ***Inscrits*** ont fourni des éléments d'identification satisfaisants au moins aux exigences du niveau « substantiel » lors d'une demande d'inscription en ligne sur le Site www.clearbus.fr ou par tout autre moyen mis à leur disposition par la société **ClearBUS**.

Les utilisateurs ***Inscrits*** bénéficient d'une boite aux lettres virtuelle permanente dans le système **ClearBUS.** Leurs droits sont limités à la gestion de leur Espace Utilisateur et à la réception de courriers numériques.

L'utilisation de la fonction de réception de courriers est gratuite.

ClearBUS se réserve le droit de supprimer la boite aux lettres virtuelle d'un utilisateur ***Inscrit*** qui n'aurait pas reçu de courrier d'un tiers pendant une période de douze (12) mois consécutifs.

4.1.2 Utilisateurs Abonnés

Les utilisateurs ***Abonnés*** ont fourni des éléments d'identification satisfaisants aux exigences du niveau « élevé » lors d'une demande d'abonnement en ligne sur le Site www.clearbus.fr ou par tout autre moyen mis à leur disposition par la société **ClearBUS**.

Les utilisateurs ***Abonnés*** bénéficient d'une boite aux lettres virtuelle permanente dans le système **ClearBUS**, leur permettant d'accéder aux fonctions d'envoi et de réception des courriers numériques.

Pour répondre à des besoins professionnels de gestion ou d'organisation, un ***Abonné*** peut vouloir déployer l'usage du service d'envoi recommandé électronique sur d'autres utilisateurs, introduisant une seconde dimension dans les profils :

- **Abonné Principal** : responsable technique et financier des usages ;
- **Abonné Secondaire** : ayant droit de l'Abonné Principal.

4.1.3 Utilisateurs Invités

Les utilisateurs ***Invités*** sont les destinataires d'un courrier numérique confié à **ClearBUS** et qui ne souhaitent pas être inscrits de façon permanente.

Ils s'identifient pour le retrait de chaque courrier et peuvent ainsi accéder à une boite aux lettres temporaire. La boite aux lettres temporaire est supprimée après le retrait du courrier.

4.2 Processus d'identification initiale des utilisateurs

Le processus d'identification initiale de l'utilisateur intervient dans les situations suivantes :

- Demande d'abonnement principal ;
- Demande de rattachement d'un abonné secondaire ;
- Demande d'inscription ;
- Demande de relève d'une LRE en tant qu'utilisateur invité ;

Ce processus vise à valider que les données d'identifications présentées par l'utilisateur dans l'une de ces procédures sont authentiques avec un certain niveau de confiance, et correspondent à un profil utilisateur précédemment déclaré.

Ces procédures sont détaillées section 5.1.

4.3 Vérification initiale de l'identité de l'expéditeur

L'identité de l'utilisateur expéditeur est vérifiée dans les conditions prévues pour le niveau de garantie « élevé », au point 2.1 de l'annexe du règlement [RE_2015_1502] dans les situations suivantes :

- Processus d'abonnement principal (cf. section 5.1.1);
- Processus de rattachement d'un abonné secondaire (cf. section 5.1.2) ;

ClearBUS-SRE garantit l'identification de l'utilisateur avec un degré de confiance « élevé » par l'une des modalités suivantes :

1) Par la présence en personne de la personne physique ou du représentant autorisé de la personne morale ;
2) Au moyen d'un certificat de signature électronique qualifié pour une personne physique ou d'un certificat de cachet électronique qualifié pour une personne morale, délivré conformément au point 1) ci-dessus ou à distance, à l'aide d'un moyen d'identification électronique pour lequel la personne physique ou un représentant autorisé de la personne morale s'est présenté en personne et qui satisfait aux conditions prévues pour les niveaux de garantie « substantiel » ou « élevé », au point 2.1 de l'annexe du règlement [RE_2015_1502].

   Dans ce cadre, **ClearBUS** accepte les certificats qualifiés RGS pour le niveau (**), et les certificats qualifiés ETSI EN 319 411-2.
3) Par « LuxTrust Live Registration Service / Remote Identification », un service d'identification à distance équivalent à la présence en personne de la personne physique ou du représentant autorisé de la personne morale, et conforme à la règlementation [eIDAS] ;
4) Par une procédure de rattachement d'un abonné secondaire ;

Dans tous les cas, les informations relatives à l'identité de l'utilisateur et portées dans le document justificatif d'identité, dans le certificat électronique, ou par le moyen d'identification électronique, doivent correspondre aux informations portées sur les éléments présentés dans le cadre de la vérification d'identité.

4.3.1 Mesures relatives à la vérification de l'identité en face à face

Lors d'un face-à-face, ou en situation équivalente, la personne physique ou le représentant autorisé de la personne morale doit présenter un document officiel d'identité qui sera vérifié par un Agent habilité de **ClearBUS**.

L'information suivant laquelle la validation a été réalisée en face à face, et l'identité de l'Agent **ClearBUS** sont consignées.

4.3.2 Mesures relatives à la vérification de l'identité par le biais d'un certificat

La création de la signature électronique avancée ou du cachet électronique avancé par l'utilisateur est mise en œuvre par le biais de moyens fournis par **ClearBUS**. Ces moyens s'appuient sur la bibliothèque « ClearBUS-Secure version 1.10 » qui a fait l'objet d'une Certification de Sécurité de Premier Niveau (CSPN) auprès de l'ANSSI.

ClearBUS s'assure que le certificat de signature électronique qualifié ou de cachet électronique qualifié utilisé pour la vérification de l'identité a été délivré par une Autorité de Certification qualifiée selon le Règlement Européen [eIDAS].

ClearBUS met en œuvre un processus de validation de la signature ou du cachet, à partir des certificats de la chaine de confiance et des CRL correspondantes.

4.3.3 Mesures relatives au rattachement d'un abonné secondaire

Le contexte de rattachement d'un abonné secondaire correspond à la situation ou un ***Abonné Principal*** prévoit de partager ses droits avec des utilisateurs avec lesquels est établie une relation contractuelle pérenne.

Prenant en compte l'existence d'un lien contractuel probant et durable, existant entre l'***Abonné Principal*** et ***l'Abonné Secondaire***, qui garantit une connaissance détaillée et justifiée de l'identité de ce dernier, la procédure mise en place par **ClearBUS** à l'intention de l'***Abonné Principal*** permet de reconnaître que l'***Abonné Secondaire*** est identifié lui aussi avec un niveau « élevé » (en conformité avec RE 2015/1502).

Pour autant l'identification nécessite que ***l'Abonné Secondaire*** fournisse l'ensemble des données le décrivant à **ClearBUS**, cette condition pouvant être soumise soit à validation par un Agent habilité **ClearBUS**, soit satisfaite par la présentation d'un moyen d'identification de niveau au moins « substantiel », tel que décrit section 4.4.

La responsabilité de ***l'Abonné Principal*** est engagée dans ce processus, notamment sur le plan financier (il paye les courriers émis par ***l'Abonné Secondaire***), et il s'engage à « détacher » ce dernier lorsque les circonstances s'avèrent ; le titulaire de l'abonnement secondaire perd alors son statut ***d'Abonné***.

4.4 Vérification initiale de l'identité du destinataire

L'identité d'un utilisateur destinataire est vérifiée au minimum dans les conditions prévues pour le niveau de garantie « substantiel », au point 2.1 de l'annexe du règlement [RE_2015_1502] dans les situations suivantes :

- Processus d'enregistrement d'un utilisateur ***Inscrit*** (cf. section 5.1.1) ;
- Demande de délivrance d'une LRE à un utilisateur ***Invité*** (cf. section 5.1.2) ;

ClearBUS-SRE garantit l'identification de l'utilisateur avec un degré de confiance au moins « substantiel » par l'une des modalités suivantes :

- Par les moyens référencés en section 4.3 ; ou
- A distance, à l'aide d'un moyen d'identification électronique qui satisfait aux conditions prévues pour les niveaux de garantie « substantiel », au point 2.1 de l'annexe du règlement [RE_2015_1502].

  Dans ce cadre, **ClearBUS** s'appuie sur la plateforme de fédération d'identité « FranceConnect », délivrant ce niveau de garantie ;
- Au moyen d'un certificat de signature électronique qualifié pour une personne physique ou d'un certificat de cachet électronique qualifié pour une personne morale.

  Dans ce cadre, **ClearBUS** accepte les certificats qualifiés RGS pour le niveau (*), et les certificats qualifiés ETSI EN 319 411-1.
- Par une vérification à distance de documents justificatifs d'identité par un Agent habilité **ClearBUS**.

Dans tous les cas, les informations relatives à l'identité de l'utilisateur et portées dans le document justificatif d'identité, ou par le moyen d'identification doivent correspondre aux informations portées sur les éléments présentés dans le cadre de la vérification d'identité.

4.4.1 Mesures relatives à la procédure de vérification à distance par FranceConnect

Le service assuré par « FranceConnect » intègre une authentification de l'utilisateur avec un niveau de confiance paramétré, permettant à l'utilisateur de choisir un fournisseur d'identité agréé à ce niveau.

Le niveau retenu par **ClearBUS** est au minimum « substantiel » ; **ClearBUS** s'assure que ce niveau satisfait aux conditions prévues pour le niveau de garantie « substantiel », au point 2.1 de l'annexe du règlement [RE_2015_1502].

NOTE : Si « FranceConnect » n'est pas en mesure de proposer de fournisseur d'identité de niveau « substantiel », l'utilisateur revient de ce service avec un échec et se trouve renvoyé aux autres moyens disponibles.

4.4.2 Mesures relatives à la vérification de l'identité par le biais d'un certificat

cf. section 4.3.2

4.4.3 Mesures relatives à la procédure de vérification à distance de documents d'identité

Les justificatifs suivants sont acceptés par **ClearBUS** :

- Document officiel d'identité avec photographie (carte nationale d'identité, passeport, titre de séjour ou autre document relatif au séjour) en cours de validité au moment de la vérification ;

- Justificatif portant le numéro de SIREN de l'entité. Pour une entreprise, toute pièce portant le numéro SIREN de l'entreprise ou, à défaut, une autre pièce valide attestant l'identification unique de l'entreprise (extrait KBIS).

ClearBUS permet la transmission de ces justificatifs par téléchargement sur le site du service, à partir d'une session active de l'utilisateur.

L'identité de l'utilisateur est approuvée par un Agent habilité de **ClearBUS** si les pièces justificatives fournies sont valides à la date de réception.

Les justificatifs fournis ne sont pas conservés. Seule l'information suivant laquelle la validation a été réalisée par un Agent habilité de **ClearBUS** est consignée.

4.5 Authentification des utilisateurs

4.5.1 Moyen d'identification électronique ClearBUS

Un utilisateur visant le statut ***Inscrit*** ou ***Abonné*** se voit attribuer par **ClearBUS** un moyen d'identification électronique constitué :

- D'un identifiant unique de boite aux lettres virtuelle (généré par ClearBUS) ;
- D'un mot de passe personnel choisi par l'utilisateur ;

Le MIE **ClearBUS** permet à l'utilisateur d'accéder aux interfaces d'envoi, de réception, et de gestion de compte du service **ClearBUS-SRE**.

Le MIE **ClearBUS** est un premier facteur d'authentification, qui demande à être couplé à un second facteur ou à un moyen additionnel lorsqu'une opération nécessite une authentification forte de l'utilisateur (cf. section 4.5.2).

4.5.2 Authentification forte

Le service d'envoi Recommandé Electronique **ClearBUS** requiert une authentification forte de ses utilisateurs (expéditeur et destinataire) lors de opérations suivantes :

- Envoyer une LRE ;
- Recevoir une LRE ;
- Modifier son Profil Utilisateur.

Les moyens d'identification électronique que les utilisateurs expéditeur et/ou destinataire peuvent utiliser pour s'authentifier et accéder aux opérations précitées sont les suivants :

- Signature ou cachet électronique avancé produit à partir d'un certificat électronique en cours de validité, délivré par un prestataire de services de confiance qualifié (certificat *, ETSI EN 319 411-1, ou supérieur), et soumis à un ensemble de contrôles usuels (reconnaissance de l'AC, validité, non révocation, concordance de l'identité avec les données attendues) ; ou
- Moyen d'identification électronique fourni par la plateforme de fédération d'identité « FranceConnect », et satisfaisant aux exigences des niveaux de garantie « substantiel » ou supérieur ; ou

  REMARQUE : L'identité validée renvoyée par « FranceConnect » est soumise à un ensemble de contrôles dont la concordance de l'identité renvoyée avec l'identité attendue.

- Moyen d'identification électronique **ClearBUS** basé sur un couple identifiant / mot de passe, couplé à un TOTP (RFC 6238) ; ou

  REMARQUE : La mise en œuvre et la transmission de ce facteur d'authentification présume que l'utilisateur a initialisé une application implémentant la RFC 6238 avec une clé secrète générée à la volée lors de son inscription ou de son abonnement (cf. section 5.1.1).

- Moyen d'identification électronique **ClearBUS** basé sur un couple identifiant / mot de passe, couplé à un OTP vocal ;

  REMARQUE : La transmission de ce facteur d'authentification utilise la téléphonie et s'appuie sur le numéro de téléphone renseigné par l'utilisateur dans son Profil Utilisateur ;

- Code à usage unique de type OTP, délivré à des utilisateurs destinataires ***Invité*** dans le cadre de la procédure décrite section 5.1.3 ;

ClearBUS ne traite pas le cycle de vie des certificats électroniques ou des moyens d'identification électronique fournis par exemple par « FranceConnect » ; il est décrit dans la Politique et Déclaration de pratiques du service correspondant.

5 DISPOSITIONS RELATIVES AU SERVICE DE RECOMMANDE ELECTRONIQUE

5.1 Accès au service

5.1.1 Processus d'inscription et d'abonnement

Pour s'inscrire ou s'abonner au service **ClearBUS-SRE**, l'utilisateur doit :

- Créer un compte à partir du Site et remplir le formulaire intitulé « Création du Compte » en renseignant en ligne des champs d'information et d'identification ;
- Choisir un mot de passe d'accès à son Espace Utilisateur ;
  - ⇨ L'utilisateur reçoit un identifiant unique, attestant la création d'une boite aux lettres virtuelle **ClearBUS**.
- Se connecter à son Espace Utilisateur avec son MIE ClearBUS et fournir les justificatifs qui le concerne, et qui sont nécessaires à la validation de son inscription ou de son abonnement (identité, domicile, entreprise, mandat signataire, moyens de paiement) ;
- Valider sa demande en mettant en œuvre un des moyens d'identification initiale du destinataire (au moins de niveau « substantiel ») tels que décrits en section 4.4 dans le cas d'une inscription, ou un des moyens d'identification initiale de l'expéditeur (de niveau « élevé ») tels que décrits en section 4.3 dans le cas d'un abonnement ;

Le traitement de la demande consiste en un contrôle de données à l'identique entre les informations issues du formulaire d'inscription/abonnement et celle confirmées par le moyen mis en œuvre pour cette validation. Le succès de cette phase ouvre ses droits à l'utilisateur, en tant qu'***Inscrit*** *ou* ***Abonné***.

Option complémentaire : l'utilisateur se voit proposer une clé générée conformément à la RFC 6030 (PSKC) à configurer dans son application type « authenticator » (sur mobile ou sur PC) s'il le souhaite et s'il est prêt à faire cette configuration. Cette clé pourra être mise en œuvre conformément à la RFC 6238 pour futurs besoins d'authentification.

5.1.2 Processus de rattachement d'un abonné secondaire

La création d'un abonné secondaire est une initiative de l'***Abonné Principal***, et suit les étapes suivantes :

- Pour l'***Abonné Principal*** :
  - Remplir et valider le formulaire d'enregistrement de l'abonné secondaire, et définir son mot de passe initial (charge à lui de le transmettre à l'abonné secondaire).
  - ⇨ L'***Abonné Secondaire*** obtient un identifiant unique, attestant la création d'une boite aux lettres virtuelle **ClearBUS**.
- Pour l'***Abonné Secondaire*** :

- Se connecter à son Espace Utilisateur et compléter la demande en fournissant les justificatifs qui le concerne, et qui sont nécessaires à la validation de son abonnement (identité, domicile) ;
- Valider sa demande en mettant en œuvre un des moyens d'identification de niveau « substantiel » suivants :
  - Présentation d'un document justificatif d'identité ;
  - Validation en face à face ;
  - Présentation d'un certificat RGS (*) ou ETSI EN 319 411-1 ou supérieur ;
  - Validation d'un certificat qualifié confirmant l'identification du demandeur établi dans un contexte commercial hors LRE ;
  - Validation indirecte par OTP vocal, utilisant un numéro de téléphone fourni par l'***Abonné Principal*** ;

La demande ainsi complétée fait l'objet d'une validation par un Agent habilité **ClearBUS**. Les justificatifs d'identité fournis ne sont pas conservés. Seule l'information suivant laquelle la validation a été réalisée par un Agent habilité de **ClearBUS** est consignée.

La validation par Agent permet l'activation du compte, et ouvre ses droits à l'utilisateur en tant qu'***Abonné Secondaire***.

L'***Abonné Principal*** contrôle l'activation ou la désactivation de ce droit à partir de son Espace Utilisateur ; il est responsable financièrement de l'usage des services que font ses ***Abonnés Secondaires***, et garantit le maintien de la relation contractuelle à travers laquelle il peut les décrire personnellement.

Option complémentaire : l'utilisateur se voit proposer une clé générée conformément à la RFC 6030 (PSKC) à configurer dans son application type « authenticator » (sur mobile ou sur PC) s'il le souhaite et s'il est prêt à faire cette configuration. Cette clé pourra être mise en œuvre conformément à la RFC 6238 pour futurs besoins d'authentification.

5.1.3 Processus de délivrance d'une LRE à un utilisateur Invité

Pour accéder au service de réception d'une LRE, l'utilisateur destinataire ***Invité*** (c'est-à-dire non enregistré dans le Système d'Information **ClearBUS**) doit initier une procédure de délivrance d'une LRE à partir des interfaces WEB **ClearBUS** qui lui auront été communiquées.

Dans une première étape, l'utilisateur complète un formulaire d'identification sur le site de **ClearBUS** dans lequel les informations suivantes doivent être renseignées, et doivent correspondre aux données suivantes :

- Numéro de relève tel qu'indiqué dans les notifications transmises au destinataire ;
- Nom et prénom pour un particulier tels que renseignés par l'expéditeur ; ou
- Raison sociale pour une entreprise telle que renseignée par l'expéditeur ; et
- Adresse postale telle que renseignée par l'expéditeur.

Après validation de ces informations, l'utilisateur utilise l'un des moyens décrit section 4.4 pour s'identifier, et lorsque le moyen le permet, de s'authentifier à un niveau « substantiel » auprès du service **ClearBUS**.

Lorsque le moyen d'identification choisit par l'utilisateur ne permet pas de l'authentifier dynamiquement au niveau « substantiel » (cas par exemple du justificatif d'identité), l'identité du destinataire est validée par un Agent habilité **ClearBUS**. Après validation, un code à usage unique de type OTP est transmis à l'utilisateur destinataire, lui permettant de s'authentifier. Ce code est transmis soit :

- Par appel en synthèse vocale vers le numéro de téléphone fixe ou mobile renseigné par l'expéditeur, et non modifiable par le destinataire ; ou
- Par courrier postal à l'adresse renseignée par l'expéditeur, et non modifiable par le destinataire ;

Une fois authentifié, l'utilisateur se voit présenter l'ensemble des fichiers constitutifs de la LRE.

5.2 Processus de modification de profil utilisateur

Les données du profil d'un utilisateur ***Inscrit*** ou ***Abonné*** constituent des clés de routage (adresse postale), de notification (coordonnées numériques), ou d'authentification. Leur demande de modification doit être authentifiée de manière forte par l'un des moyens décrit section 4.5.2.

5.3 Intégrité et confidentialité du contenu d'utilisateur

Les utilisateurs disposent des fonctionnalités de composition, d'envoi, de réception, et de refus de recommandés électroniques à partir de l'application « CLIC » ou de l'application « WEBCLIC » ou de toute autre application intégrant un connecteur agréé par **ClearBUS** avec le serveur postal numérique de **ClearBUS-SRE**.

Ces interfaces s'appuient sur la bibliothèque « ClearBUS-Secure version 1.10 » ; produit qualifié CSPN par l'ANSSI ; assurant l'intégrité et la confidentialité des données échangées de et vers les services **ClearBUS-SRE**.

Durant le processus d'acheminement d'une lettre recommandée électronique, le contenu utilisateur (c.-à-d. document numérique et pièces-jointes) ne fait l'objet d'aucune modification, et est protégé en intégrité par des jetons d'horodatage qualifiés.

5.4 Processus d'envoi

L'expéditeur est un utilisateur ***Abonné***.

5.4.1 Composition de la LRE

L'expéditeur prépare le message d'origine comprenant un contenu utilisateur composé de tout type de documents numériques avec autant de pièces jointes qu'il le souhaite, et un destinataire décrit avec les informations suivantes :

- Nom et prénom, ou raison social de l'expéditeur ;
- Adresse postale ;
- Moyens de notifications tels que :

- Email ; et/ou
- Numéro de téléphone mobile ; et/ou
- Numéro de téléphone fixe ; et/ou
- Numéro de fax.

NOTE : L'adresse postale ou les numéros de téléphone renseignés par l'expéditeur pourront être mis en œuvre pour la transmission d'un OTP dans le cadre du processus de délivrance de la LRE à utilisateur ***Invité***.

La lettre recommandée électronique peut être postée pour tout destinataire de son choix en France.

5.4.2 Identification et authentification de l'utilisateur

Pour transmettre sa lettre recommandée électronique au service **ClearBUS-SRE,** l'expéditeur doit se connecter aux interfaces **ClearBUS** avec son MIE ClearBUS, et doit s'authentifier de manière forte avec un des moyens décrit en section 4.5.2.

5.4.3 Preuve de dépôt

Après validation de l'identité de l'expéditeur, **ClearBUS-SRE** valide le dépôt.

Cet évènement conduit à la génération d'une preuve électronique de dépôt qui atteste que l'expéditeur, dûment authentifié, a déposé avec succès à l'heure indiquée dans la preuve par un horodatage électronique qualifié, une LRE à **ClearBUS-PSRE** et que **ClearBUS-PSRE** a accepté d'exécuter les tâches demandées pour tenter de la remettre au destinataire prévu.

Un document de preuve reflétant les données de l'envoi et de la preuve électronique de dépôt est automatiquement délivré dans la boite aux lettres virtuelle **ClearBUS** de l'expéditeur (cf. section 5.8.1).

5.5 Processus de réception

Le destinataire est un utilisateur ***Abonné***, ***Inscrit***, ou ***Invité***.

5.5.1 Notification du destinataire

Le service **ClearBUS-SRE** exploite les canaux de communications (c.-à-d. courriel, SMS, FAX, et/ou messagerie vocale) renseignées par l'expéditeur lors du dépôt pour avertir le destinataire de la disponibilité d'une LRE et pour demander au destinataire s'il souhaite l'accepter. Le destinataire n'est pas informé de l'identité de l'expéditeur de la LRE.

Cet évènement conduit à la génération d'un jeton d'horodatage électronique qualifié, qui atteste qu'un processus d'envoi de notifications demandant l'acceptation d'une LRE est déclenché à une heure spécifique indiquée par le jeton lui-même.

Ce jeton n'atteste pas que les notifications ont été reçues par le destinataire. Néanmoins, **ClearBUS-SRE** vérifie la réussite de l'envoi d'au moins une notification. En cas d'échec, l'expéditeur est informé de l'erreur par courriel.

Ce jeton d'horodatage est conservé par **ClearBUS**.

5.5.2 Délai d'acceptation de la LRE

Le délai d'acceptation d'une LRE est de quinze (15) jours à compter du lendemain de l'envoi de la notification.

Si le destinataire ne réagit pas lors du délai d'acceptation, l'accès à la LRE sera supprimé des interfaces du service **ClearBUS-SRE**.

5.5.3 Acceptation ou refus de la LRE

Le destinataire utilise les interfaces **ClearBUS**, ou suit les liens mentionnés dans son message de notification pour accéder aux fonctions d'acceptation ou de refus de la LRE.

5.5.4 Identification et authentification du destinataire

En cas d'acceptation de la LRE et avant la transmission de la LRE, le destinataire doit s'authentifier à partir des interfaces **ClearBUS** avec l'un des moyens décrit en section 4.5.2.

5.5.5 Transmission de la LRE

Après validation de l'identité du destinataire, **ClearBUS-SRE** transmet la LRE au destinataire.

5.5.6 Preuve de réception

L'évènement de transmission de la LRE est suivi par **ClearBUS-SRE**, et conduit à la génération d'une preuve électronique de réception.

La preuve électronique de réception atteste que le contenu utilisateur, à une heure spécifique indiquée par un horodatage électronique qualifié, a été transférée au destinataire – après une identification et une authentification correctes.

Un document de preuve reflétant les données de l'envoi et de la preuve électronique de réception est automatiquement délivré dans la boite aux lettres virtuelle de l'expéditeur (cf. section 5.8.1).

5.5.7 Preuve de refus

L'évènement de refus explicite de réception par le destinataire conduit à la génération d'une preuve électronique de refus.

La preuve électronique de refus atteste que le destinataire, à l'heure indiquée par un horodatage électronique qualifié, a refusé de recevoir un certain contenu utilisateur provenant d'un expéditeur.

Un document de preuve reflétant les données de l'envoi et de la preuve électronique de de refus est automatiquement délivré dans la boite aux lettres virtuelle de l'expéditeur (cf. section 5.8.1).

5.5.8 Preuve de non réclamation

L'évènement de non réclamation de la LRE par le destinataire dans le délai d'acceptation prévu section 5.5.2 conduit à la génération d'une preuve de non distribution au plus tard le lendemain de l'expiration de ce délai.

La preuve électronique de non réclamation atteste que le destinataire n'a pas réagi à la demande d'acceptation ou de refus de recevoir un certain contenu utilisateur provenant d'un expéditeur dans le délai imparti.

Un document de preuve reflétant les données de l'envoi et de la preuve électronique de de non réclamation est automatiquement délivré dans la boite aux lettres virtuelle de l'expéditeur (cf. section 5.8.1).

5.6 Processus de signalement des modifications des données

Sans objet. Le contenu utilisateur d'une LRE n'est pas modifié lors du processus d'acheminement.

5.7 Référence de temps

La date et l'heure des preuves électronique (expédition, réception, sécurisation du contenu utilisateur, etc.) sont indiquées par un horodatage électronique qualifié. Les jetons d'horodatage sont produits avec une exactitude de temps d'une seconde par rapport au temps UTC.

Dans le cadre de la présente politique, cette opération est réalisée par le service d'horodatage qualifié **ClearBUS**, ou par un prestataire de service d'horodatage qualifié tiers.

ClearBUS vérifie systématiquement la validité du jeton d'horodatage qualifié, et régulièrement que les prestataires de services d'horodatage tiers participant ponctuellement aux activités de **ClearBUS-SRE** sont toujours qualifiés.

5.8 Description des preuves

5.8.1 Documents de preuve

Immédiatement après la survenue d'un évènement de dépôt, de réception, de refus ou de non réclamation, un document de preuve reflétant les données de l'envoi et les preuves électroniques scellées de l'évènement est automatiquement délivré dans la boite aux lettres virtuelle de l'expéditeur.

5.8.1.1 Format

Les documents de preuve émis par **ClearBUS** sont au format PDF.

5.8.1.2 Contenu

Tous les documents de preuve comportent les informations suivantes :

- Le nom et le prénom ou la raison sociale de l'expéditeur ;
- Le nom et le prénom ou la raison sociale du destinataire ;
- Le numéro d'identification unique de l'envoi attribué par le service **ClearBUS-SRE** ;
- Le type de preuve, parmi :
    - Dépôt ;

- Réception ;
- Refus ;
- Non réclamation ;

- La date et l'heure du dépôt électronique de l'envoi, indiquées par un horodatage électronique qualifié ;

En plus de ces informations :

- Le document de preuve de réception comporte la date et l'heure de la réception électronique de l'envoi, indiquées par un horodatage électronique qualifié ;
- Le document de preuve de refus comporte la date et l'heure de refus électronique de l'envoi, indiquées par un horodatage électronique qualifié ;

Les dates et heures affichées dans les documents de preuve sont au fuseau CET (UTC+1) en hiver, ou au fuseau CEST (UTC+2) en été.

5.8.1.3 Durée de mise à disposition

Une première instance des documents de preuve de dépôt, de réception, de refus ou de non réclamation est délivrée à l'expéditeur de l'envoi recommandé électronique à partir des interfaces de boites aux lettres virtuelle **ClearBUS**.

Sur demande et pendant sa durée de conservation d'un (1) an, elle peut être remise à disposition de l'expéditeur sur ces mêmes interfaces.

5.8.2 Preuves électroniques

Toutes les preuves électroniques générées lors d'évènements relatifs à l'acheminement d'une LRE sont scellées par un cachet électronique apposé par **ClearBUS-SRE**.

ClearBUS-SRE vérifie systématiquement la validité des cachets électroniques produits sur les points suivants :

- Validité du certificat cachet lors du scellement (non expiré, validité de la chaine de certification) ;
- Intégrité des données scellées ;
- Validité cryptographique du cachet électronique ;

5.8.2.1 Format

Les preuves électroniques sont conservées sous la forme d'un objet de signature au format standard de cryptographie à clé publique (PKCS#7), et comportent :

- Les données scellées ;
- Le cachet électronique (apposé par **ClearBUS-SRE**) ; et
- Les données de vérification du cachet (c.-à-d. l'ensemble de la chaine de certification).

5.8.2.2 Contenu scellé

Les données scellées des preuves électroniques de dépôt, de réception, de refus et de non réclamation sont les suivants :

Type de preuve électronique	Contenu scellé (encodée en base64)
Dépôt	Type de preuve ; Nom, prénom, raison sociale, adresse électronique de l'expéditeur ; Nom, prénom, raison sociale, adresse électronique du destinataire ; Numéro d'identification unique de l'envoi ; Jeton d'horodatage au format PKCS7 correspondant à la date et heure de dépôt ;
Réception	Contenu de la preuve électronique de dépôt ; Jeton d'horodatage au format PKCS7 correspondant à la date et heure de réception ;
Refus	Contenu de la preuve électronique de dépôt ; Jeton d'horodatage au format PKCS7 correspondant à la date et heure de refus ;
Non réclamation	Contenu de la preuve de dépôt ;

5.8.2.3 Algorithmes de signature

Les algorithmes utilisés pour calculer l'empreinte et sceller les données des preuves électroniques sont respectivement SHA-512 et RSA.

5.8.2.4 Mise à disposition

L'expéditeur d'une Lettre Recommandé Electronique et le destinataire (ayant accepté sa réception) peuvent accéder au fichier de preuves sur demande à l'adresse suivante : support@clearbus.fr.

Ce fichier de preuves est composé des preuves électroniques et des jetons d'horodatage produits lors de l'acheminement de la LRE.

Un utilitaire de visualisation, de vérification du fichier de preuves est mis en outre à disposition par **ClearBUS** à l'adresse suivante : https://www.clearbus.fr/Content/Applets/verifieur/verifieur.html. Cet outil permet d'extraire les informations détaillées et de recalculer les différentes signatures électroniques applicables, à des fins probatoires.

5.8.2.5 Durée de mise à disposition

Le fichier de preuves électroniques et de jetons d'horodatage est archivé.

Il est mis à disposition pendant sept (7) an après la date d'envoi de la LRE, y compris en cas d'arrêt d'activité de **ClearBUS-PSRE.**

5.9 Conservation des informations

ClearBUS conserve les données relatives un chaque Recommandé Electronique pendant une durée de sept (7) ans après la date d'envoi et de réception des données toutes les informations pertinentes concernant les données délivrées reçues, notamment afin de pouvoir fournir des preuves en justice.

Les données conservées sont à minima les suivantes :

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

L'ensemble de ces données sont conservées dans le fichier de preuves archivé, et dans les traces applicatives du service **ClearBUS-SRE**.

Les documents de preuve et le contenu utilisateur d'un recommandé électronique sont conservés pendant un (1) an.

6 GESTION ET EXPLOITATION DE CLEARBUS-PSRE

6.1 Organisation interne

6.1.1 Fiabilité de l'organisation

ClearBUS maintient des ressources financières suffisantes et dispose d'une assurance responsabilité appropriée pour couvrir les coûts liés à ses opérations et/ou de ses activités.

ClearBUS dispose des politiques et des procédures pour le règlement des plaintes et des litiges reçus des clients ou d'autres parties prenantes sur la fourniture des services ou toute autre question connexe.

ClearBUS dispose d'un accord documenté et d'une relation contractuelle en place lorsque la fourniture des services implique de la sous-traitance, de l'externalisation ou d'autres arrangements avec de tiers.

6.1.2 Rôles de confiance

Les rôles de confiance sont attribués aux personnes sur lesquelles repose la sécurité du Service d'envoi Recommandé Electronique.

Les rôles de confiance identifiés sont au moins les suivants :

Responsable de sécurité. Le responsable de sécurité est chargé de la mise en œuvre de la politique de sécurité du système d'information. Ce rôle correspond au rôle Security Officer définit dans la norme [EN_319401].

Administrateur fonctionnel. L'administrateur fonctionnel configure et administre les composants du service de recommandé électronique.

Administrateur système. L'administrateur système est en charge de l'installation, de la mise en route, de la configuration, de la restauration et de la maintenance technique des équipements informatiques. Ils assurent l'administration technique des systèmes et des réseaux de la composante, ainsi que leur surveillance (détection d'incident). Ce rôle correspond au System Administrator définit dans la norme [EN_319401].

Opérateur système. L'opérateur système est en charge du suivi et du maintien en conditions opérationnelles du service. Il est habilité à réaliser des sauvegardes. Ce rôle correspond au System Operator définit dans la norme [EN_319401].

Agent ClearBUS. Membre du personnel de **ClearBUS** en charge de la vérification, et de la validation des identités. Il assure les premiers niveaux de support.

Auditeur système. L'auditeur système est en charge de l'analyse récurrente des événements intervenant sur les composantes du service. Il dispose d'un accès aux journaux d'audit et aux archives afin de s'assurer du respect des conditions de sécurité et de la légitimité des opérations réalisées sur le système. Ce rôle correspond au System Auditor définit dans la norme [EN_319401].

Responsable de certificats. Le responsable de certificat est en charge des certificats électronique de service applicatif, et du suivi des AC qui les ont émis.

ClearBUS applique les principes de séparation des rôles et de moindre privilège dans la définition des fonctions des rôles de confiance, et lors de l'affectation des personnels.

Chaque attribution de rôle à un membre du personnel de **ClearBUS** est validée par la Direction et est acceptée formellement. Tant que les contrôles prévus en section cf. section 6.2 ne sont pas achevés, le personnel n'a pas accès aux fonctions de confiance.

6.1.3 Séparation des tâches

ClearBUS met en œuvre une séparation des rôles de confiance de manière à ce que :

- Le responsable de la sécurité n'ait pas de rôle opérationnel directement sur les serveurs du service **ClearBUS-SRE** ;
- L'audit système se fasse par une personne neutre vis-à-vis du service d'envoi recommandé électronique.

6.2 Mesures de sécurité vis-à-vis des ressources humaines

6.2.1 Compétences et qualifications

ClearBUS applique les principes de séparation des rôles et de moindre privilège dans la définition des fonctions et lors de l'affectation des personnels.

Tout intervenant amené à occuper un rôle identifié comme sensible est soumis à une clause de confidentialité, gérée par l'employeur.

Le personnel d'encadrement de **ClearBUS** possède l'expertise appropriée, et est familier des procédures de sécurité.

Toute personne intervenant dans des rôles de confiance est informée de ses responsabilités (fiche de poste) et des procédures liées à la sécurité du système et au contrôle du personnel.

Ces engagements sont réexaminés à intervalles réguliers (au minimum tous les trois ans) et en cas de changements ayant un impact sur les exigences requises, notamment en cas de changement de poste et/ou de projet si nécessaire.

6.2.2 Procédure de vérification des antécédents

Il est demandé aux personnes appelées à occuper un rôle sensible au sein du service d'envoi Recommandé Electronique de fournir une déclaration sur l'honneur attestant pour la personne :

- De ne pas avoir de conflit d'intérêt dans le poste qu'elle occupe ;
- De ne pas avoir commis de délits informatiques.

6.2.3 Exigences en matière de formation initiale

Le personnel est formé aux logiciels, matériels et procédures internes de fonctionnement. Une sensibilisation sur les implications des opérations dont ils ont la responsabilité est également opérée.

Les personnels participant au Service d'envoi Recommandé Electronique ont notamment des connaissances sur les thèmes suivants :

- Technologie et fonctionnement des moyens d'identification électronique et d'authentification des utilisateurs ;
- Technologie et principe de la signature électronique ;
- Connaissance pratique de la conception des documents d'identification et de leurs caractéristiques de sécurité ;
- Connaissance et respect des règles de sécurité pour les personnels techniques.

6.2.4 Exigences et fréquence en matière de formation continue

Chaque évolution dans les systèmes, procédures ou organisations fait l'objet d'information ou de formation aux intervenants dans la mesure où cette évolution impacte le mode de travail de ces intervenants.

Les intervenants sont formés à la gestion des incidents et sont au fait de l'organisation de remontée d'incidents.

6.2.5 Fréquence et séquence de rotation entre différentes attributions

Sans objet.

6.2.6 Sanctions en cas d'actions non autorisées

ClearBUS prévoit la mise en œuvre de sanctions en cas d'actions non autorisées. Le processus de sanctions appliqué est traité par les ressources humaines de **ClearBUS**.

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

Les exigences vis-à-vis des prestataires externes sont contractualisées. Il s'agit essentiellement du personnel réalisant l'hébergement des serveurs de **ClearBUS**.

Les types d'engagement sont des contrats relatifs à la réalisation d'une prestation, des engagements de confidentialité et une charte d'utilisation des moyens informatiques.

6.2.8 Documentation fournie au personnel

Les règles de sécurité sont communiquées au personnel lors de la prise de poste, en fonction du rôle affecté à l'intervenant.

Les personnes appelées à occuper un rôle opérationnel dans le Service d'envoi Recommandé Electronique disposent de la documentation appropriée concernant les procédures opérationnelles et les outils qu'ils mettent en œuvre.

6.3 Gestion des actifs

6.3.1 Dispositions générales

ClearBUS met en œuvre une Politique de Classification de l'Information sur l'ensemble des éléments intervenant dans les activités du service **ClearBUS-SRE**.

Les informations et leurs biens supports sont identifiés, inventoriés et leurs besoins de sécurité définis en disponibilité, intégrité et confidentialité. **ClearBUS** révise l'inventaire

de ses actifs à intervalles réguliers, dans le cadre de l'analyse de risque du service ou si des changements significatifs surviennent.

6.3.2 Conservation des supports

Les supports des biens sont gérés selon des exigences de sécurité en adéquation avec leur sensibilité.

Des contrôles sont mis en œuvre pour protéger les supports contre les dommages, le vol et les accès non autorisés, que ce soit durant leur stockage ou leur éventuel transport.

Des procédures de gestion protègent les supports contre l'obsolescence et la détérioration pendant la période de temps durant laquelle **ClearBUS** s'engage à conserver les informations qu'ils contiennent.

6.3.3 Mise hors service des supports

Les supports recensés comme sensibles en termes de confidentialité font l'objet de mesures de destruction lorsqu'ils parviennent en fin de vie.

6.4 Contrôle d'accès

L'accès aux informations et aux application du système du service **ClearBUS-SRE** est limité aux personnes formellement habilitées, conformément à leur besoin d'en connaître.

Les administrateurs sont munis d'un identifiant personnel permettant de tracer nominativement l'ensemble des accès aux systèmes ; toutes les traces liées à l'administration des systèmes sont conservées conformément aux exigences exposées dans le paragraphe 6.10.1.

En outre, les mesures de sécurité suivantes sont mises en œuvre :

- Configuration des pare feux pour empêcher tous les protocoles et accès non requis pour le fonctionnement du service de confiance.
- Gestion des habilitations en prenant en compte les différents rôles identifiés par la présente politique. Le comité **ClearBUS** en charge du service assure l'attribution, le retrait, et le suivi des habilitations ;
- Gestion des comptes des utilisateurs, notamment la modification et la suppression rapide des droits d'accès ;
- Configuration de contrôles de sécurité informatique fournis par les systèmes du service de confiance pour la séparation des rôles identifiés dans la présente Politique, y compris la séparation des fonctions d'administration de la sécurité et d'exploitation. En particulier, l'utilisation des programmes utilitaires est restreinte et contrôlée ;
- Identification et authentification des utilisateurs avant de pouvoir utiliser des applications critiques liées au service de confiance ;
- Trace de toute action, de sorte à pouvoir être imputable à la personne l'ayant effectuée ;
- Protection des données sensibles contre la divulgation résultant de la réutilisation de ressources par des personnels non autorisés ;

- Protection des données sensibles contre la divulgation résultant de la réutilisation de ressources (par exemple, les fichiers supprimés) par des personnels non autorisés.

6.5 Contrôles cryptographiques

Les modules cryptographiques employés pour les opérations sensibles nécessaires au Service d'envoi Recommandé Electronique qualifié **ClearBUS**, notamment les opérations de création d'horodatages électroniques, respectent les règles spécifiées dans le document [PSCO_QUALIF].

6.6 Sécurité physique et environnementale

6.6.1 Situation géographique et construction des sites

La localisation géographique du site ne nécessite pas de mesures particulières face à des risques de type tremblements de terre, explosion, risque volcanique ou crue.

6.6.2 Accès physique

L'accès physique aux fonctions de **ClearBUS-SRE** (ceci comprend les fonctions de gestion des certificats) est strictement limité aux seules personnes nominativement autorisées, personnel de **ClearBUS** ou personnel identifié du Service d'hébergement.

L'accès physique au système d'envoi recommandé électronique supportant ces fonctions est limité aux seules personnes autorisées par la mise en place d'un périmètre de sécurité physique, permettant la séparation des rôles entre les différents intervenants, et par la mise en place d'un contrôle d'accès électronique par badge ou clé assumé par le Service d'hébergement

La traçabilité des accès est assurée par l'enregistrement des utilisations des badges électroniques de ces intervenants dûment identifiés en application du contrat de service convenu entre **ClearBUS** et son hébergeur.

L'accès physique au système d'envoi recommandé électronique par les personnels **ClearBUS** nécessite une coordination avec les personnels de l'hébergeur, qui permettra cet accès grâce à son propre badge, et tiendra le registre de ces demandes.

En dehors des heures ouvrables, des mesures de détection d'intrusion physique sont mises en œuvre.

6.6.3 Alimentation électrique et climatisation

Les moyens nécessaires au maintien de la disponibilité du système et du service sont pris en compte dans les Conditions du contrat d'hébergement.

6.6.4 Exposition aux dégâts des eaux

Les moyens nécessaires à la protection du matériel sont mis en œuvre contractuellement par l'hébergeur.

6.6.5 Prévention et protection incendie

Les moyens nécessaires au maintien de la disponibilité du système et du service sont pris en compte dans les Conditions du contrat d'hébergement. Son personnel est sensibilisé aux risques incendie, à sa prévention, sa détection et formé à l'utilisation des moyens de lutte.

6.6.6 Sauvegarde hors site

Les fichiers d'audits sont stockés sur les serveurs du service d'envoi recommandé électronique, puis exportés vers un serveur de traces externe à la plateforme de production. Ce serveur de trace est physiquement séparé.

Des sauvegardes hors site de toutes les informations utiles (applications, configurations, bases de données, etc.) sont de plus opérées par l'hébergeur de façon à faire à assurer une reprise du service après incident sur le site d'exploitation la plus rapide possible.

6.7 Sécurité des opérations

6.7.1 Mesures de sécurité liées au développement des systèmes

A l'étape de conception et de spécification de tout nouveau projet de développement, une analyse sur le plan de la sécurité est réalisée et approuvée par le Comité **ClearBUS**.

ClearBUS documente et contrôle les modifications et les mises à niveau, ainsi que la configuration des composantes du service **ClearBUS-SRE**.

En cas de modification majeure impactant la nature du service fourni, l'ANSSI sera notifié du changement mis en œuvre suivant les modalités exigées par l'ANSSI.

En particulier, toute modification impactant la liste de confiance sera notifiée sans délai.

Les solutions **ClearBUS** sont testées en premier lieu au sein d'un environnement de développement, puis de test avant d'être utilisées dans l'environnement de production. Les environnements de production et de développement sont dissociés.

6.7.2 Mesures liées à la gestion de la sécurité

Toute évolution significative d'une composante du service **ClearBUS-SRE** est documentée et signalée au Comité **ClearBUS** pour approbation.

6.7.3 Procédures de fonctionnement et responsabilités

Les opérations de sécurité sur les composantes du Service d'envoi Recommandé Electronique sont réalisées par du personnel de confiance qui est explicitement mis au courant de ses responsabilités.

Les opérations de sécurité incluent notamment :

- Les procédures opérationnelles et les responsabilités ;
- La planification et la qualification des systèmes sécurisés ;
- La veille de sécurité ;
- La protection vis-à-vis du logiciel malveillant ;

- La maintenance ;
- La gestion des sauvegardes ;
- La gestion du réseau ;
- Le contrôle actif des journaux d'audit, l'analyse des événements et les suites à donner ;
- Le traitement et la sécurité des médias ;
- L'échange des données et du logiciel.

6.7.4 Planification de systèmes

Les montées en charge sont contrôlées et des projections de charge dans le futur sont effectuées pour garantir que les puissances de traitement nécessaires, les stockages adéquats et les engagements de services sont disponibles et atteints.

6.8 Mesure de sécurité réseau

ClearBUS protège son réseau et ses systèmes contre les attaques. En particulier :

- Des équipements de filtrage sont positionnés en amont des serveurs du service pour garantir que seuls les flux nécessaires et suffisants sont autorisés à accéder à ces serveurs ;
- Tous les systèmes et équipements d'infrastructure critiques pour le fonctionnement du service sont positionnés dans une zone ou plusieurs zone sécurisées, et leurs configurations sont périodiquement auditées en vue de vérifier leur conformité avec les exigences de la présente politique ;
- Le réseau d'administration des systèmes informatiques est dédié à l'administration de la mise en œuvre de la politique de sécurité, et est séparé du réseau d'exploitation du service de confiance ;
- Les systèmes de production des services de confiance sont séparés des systèmes utilisés pour le développement et les tests ;
- La communication entre les systèmes distincts est établie uniquement par des canaux sécurisés, assurant une authentification de bout en bout et une protection des données transmises contre toute modification ou divulgation ;
- Une analyse de vulnérabilités est régulièrement réalisée sur les adresses IP publiques et privées des services de confiance identifiées par **ClearBUS** ;
- Un test d'intrusion sur les systèmes du service est réalisé au moment de la mise en place et après toute mise à niveau ou modification de l'infrastructure ou des applications que **ClearBUS** évalue comme étant importantes. **ClearBUS** réalise ou fait réaliser ce test par une personne ou une entité possédant les compétences, les outils, l'éthique et l'indépendance nécessaires pour fournir un rapport fiable.

6.9 Gestion des incidents et des vulnérabilités

6.9.1 Procédures de remontée et de traitement des incidents

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

Les incidents sur les systèmes du service de confiance font l'objet de remontées d'alertes vers une équipe en charge de les analyser et de réagir selon des procédures formelles.

Un rapport d'incident et des procédures de réponse aux incidents sont employés d'une telle façon que les dégâts liés aux incidents de sécurité et aux défaillances sont réduits au minimum, notamment :

- Tout dysfonctionnement du Service d'envoi Recommandé Electronique est identifié par l'équipe « Production » de **ClearBUS-SRE**, qui prend les mesures nécessaires à la remise en service de la composante défaillante ;
- En cas de problèmes bloquants, les équipes techniques de **ClearBUS-SRE** sont à même d'analyser l'incident et d'apporter de mesures de contournement ou correctives ;
- Les incidents liés au Service d'envoi Recommandé Electronique sont traités selon la procédure de gestion des incidents en vigueur chez **ClearBUS**.

6.9.2 Rapport d'incident

En cas d'incident majeur de sécurité ou de perte d'intégrité ayant une incidence importante sur le Service d'envoi Recommandé Electronique ou sur les données personnelles qui y sont conservées, **ClearBUS** préviendra directement et sans délai le point de contact de l'ANSSI http://www.ssi.gouv.fr.

Lorsque la violation de la sécurité ou à la perte d'intégrité est susceptible de nuire à une personne physique ou morale à qui le service de confiance a été fourni, **ClearBUS** informera également la personne physique ou morale de la violation de la sécurité ou de la perte d'intégrité sans délai injustifié.

6.9.3 Évaluation des vulnérabilités

Les procédures d'exploitation du Système d'Information du service **ClearBUS-SRE** incluent la veille sécuritaire de ses composants. Ces procédures assurent que les vulnérabilités impactant potentiellement le système sont évaluées et traitées, par le déploiement de correctifs de sécurité ou de mesures d'atténuation, dans des délais cohérents compte tenu de l'impact. La non application d'un correctif de sécurité disponible est motivée et documentée.

Toute vulnérabilité critique ayant un impact potentiel sur le système et qui n'a pas été précédemment adressée est prise en compte dans les plus brefs délai suivant sa découverte.

6.10 Gestion des journaux d'événements

6.10.1 Événements enregistrés

Tous les évènements pertinents intervenant dans la gestion et l'exploitation du Service d'envoi Recommandé Electronique sont enregistrés automatiquement sous forme électronique par les systèmes informatiques depuis leur mise en activité, ou sous forme manuscrite.

ClearBUS met en œuvre une politique d'archivage visant à conserver la traçabilité suffisante en cas d'enquêtes légales, notamment :

- Tous les éléments sauvegardés sont décrits dans une politique d'archivage et de sauvegardes appliquée dans Service d'envoi Recommandé Electronique ;
- Tous les événements d'administration des systèmes informatiques sont tracés et conservés ;
- L'instant précis des événements est tracé. Le temps utilisé pour enregistrer les événements est synchronisé avec une source fiable de temps UTC au moins une fois par jour. En cas de saisie manuelle, l'écriture est faite, sauf exception, le même jour ouvré que l'événement.
- Les événements d'audit sont conservés en sureté de manière à éviter les effacements et la perte de ces données ;
- Les informations nominatives sont conservées et protégées ;
- Tous les événements sont accessibles aux seules personnes autorisées ;
- Tous les événements liés à la gestion du cycle de vie des clés applicatives du service sont tracés (création, renouvellement, destruction, installation) ;
- Tous les événements liés à la gestion du cycle de vie des certificats sont tracés (création, renouvellement, destruction, installation) ;
- Tous les événements liés aux informations délivrés et reçues tout au long du cycle de vie d'un recommandé électronique (cf. section 5.9).

6.10.2 Traitement des journaux d'événements

Les journaux d'évènement du service d'envoi recommandé électronique alimentent en continu le Système de Gestion des Incidents de **ClearBUS**, où ils sont automatiquement analysés de manière à :

- Filtrer les évènements significatifs à vérifier ;
- Détecter des activités anormales du système qui indiquent de potentielles violations de sécurité.

6.10.3 Conservation et archivage des journaux d'événements

Les journaux du service d'envoi recommandé électronique conservés localement sur les systèmes informatiques depuis leur mise en activité.

Ils sont également archivés hors site.

Les journaux d'évènements sont conservés pendant sept (7) ans après leur génération.

6.10.4 Protection des journaux d'événements

ClearBUS assure la disponibilité, la confidentialité, et l'intégrité des journaux d'évènements.

Des mécanismes de contrôle sont mis en œuvre pour que les événements ne puissent pas être facilement supprimés ou détruits pendant la période où ils doivent être conservés.

6.11 Continuité d'activité

ClearBUS a établi et maintient un plan de continuité d'activité afin de réagir à un sinistre majeur.

Ce plan permet à **ClearBUS** de rétablir le fonctionnement du service pour ses clients dans un délai préétabli, après avoir pris les éventuelles mesures de traitement de la menace à l'origine du sinistre.

Des exercices de continuité d'activité sont réalisés à fréquence régulière.

Dans le cas d'un sinistre majeur qui affecte la sécurité du Service de Recommandé Electronique, tel que la perte, la suspicion de compromission, la compromission, le vol de données critiques (clés privées, secrets d'authentification), **ClearBUS** s'engage à :

- Interrompre son service jusqu'à ce que le fonctionnement normal du service puisse être de nouveau garanti ;
- Mettre à disposition des clients et des utilisateurs du service une description du sinistre, et une information appropriée sur les suites à lui donner ;
- Prévenir immédiatement le point de contact précisé sur le site de l'ANSSI http://www.ssi.gouv.fr, du sinistre survenu et de ses conséquences sur le service.

6.12 Fin d'activité

En cas de fin d'activité du Service d'envoi Recommandé Electronique, **ClearBUS** :

- Abrogera l'ensemble des autorisations délivrées à des tiers dans le cadre du service d'envoi recommandé électronique ;
- Transfèrera à un organisme fiable les informations d'audit ;
- Fournira à un organisme fiable les informations nécessaires à la vérification des preuves ;
- Détruira les clés privées applicatives de son service d'envoi recommandé électronique.

Le choix de l'organisme qui récupèrera les données d'audit sera défini dans le cadre du plan de fin d'activité mis en œuvre par **ClearBUS**.

ClearBUS préviendra dès que possible le point de contact précisé sur le site de l'ANSSI http://www.ssi.gouv.fr de la fin d'activité de son service d'envoi recommandé électronique.

ClearBUS prendra les mesures nécessaires pour provisionner financièrement cette fin d'activité.

6.13 Audit et conformité

Les audits et les évaluations concernent, d'une part, ceux réalisés en vue de la délivrance d'une attestation de qualification au sens du règlement [eIDAS] et, d'autre part, ceux que **ClearBUS** doit réaliser, ou faire réaliser, afin de s'assurer que l'ensemble de son infrastructure est bien conforme aux exigences légales et réglementaires et aux engagements affichés dans la PSRE, et dans la DPSRE correspondante.

6.13.1 Fréquences et circonstances des audits et des évaluations

Avant la première mise en service ou suite à toute modification significative du service d'envoi recommandé électronique, **ClearBUS** procèdera à un contrôle de conformité.

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

Ces audits sont réalisés un organisme d'évaluation agréé.

6.13.2 Identités et qualifications des auditeurs

Le contrôleur se doit d'être rigoureux pour s'assurer que les politiques, déclarations et services sont correctement mis en œuvre et détecter les cas de non conformités qui pourraient compromettre la sécurité du service offert.

Le contrôle est assigné par **ClearBUS** à une équipe d'auditeurs interne ou externe compétente en sécurité des systèmes d'information et en particulier dans le domaine d'activité de la composante contrôlée.

6.13.3 Relations entre évaluateurs et entités évaluées

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

6.13.4 Sujets couverts par les évaluations

Les contrôles de conformité portent sur une composante du service ou sur l'ensemble de l'architecture du service.

6.13.5 Actions prises suites aux conclusions des évaluations

À l'issue d'un contrôle de conformité, l'équipe d'audit remet à **ClearBUS** un rapport d'évaluation contenant un avis de présomption de conformité du Service d'envoi Recommandé Electronique.

En cas de manquements ou d'écarts constatés, **ClearBUS** spécifie un plan d'actions et met en œuvre les mesures correctives appropriées.

6.13.6 Communication des résultats

Les résultats de l'audit seront tenus à la disposition du Comité **ClearBUS**, et de l'organisme de qualification en charge de la qualification du service, l'ANSSI.

Suite de la réception du rapport d'évaluation, **ClearBUS** dispose d'un délai de trois jours ouvrables pour le transmettre à l'ANSSI.

7 AUTRES PROBLÉMATIQUES MÉTIERS ET LÉGALES

7.1 Protection des données personnelles

Toute collecte et tout usage de données à caractère personnel par **ClearBUS-PSRE** sont réalisés dans le strict respect de la législation et de la réglementation en vigueur sur le territoire français, notamment par rapport à la Loi Informatique et Libertés [CNIL] et le Règlement Général sur la Protection des Données [RGPD].

Les mesures détaillées prises par **ClearBUS** sont explicitées dans la Documentation RGPD, disponible en ligne sur www.clearbus.fr. Ce document traite en autres les points suivants :

- Politique de protection des données personnelles ;
- Information à caractère personnel ;
- Information à caractère non personnel ;
- Notification et consentement d'utilisation des données personnelles
- Conditions de divulgation d'informations personnelles aux autorités judiciaires ou administratives

7.2 Obligations des utilisateurs

Les utilisateurs (expéditeur et destinataire) sont responsables de l'utilisation qui est faite de leurs moyens d'identification électroniques. Ils doivent :

- Les protéger contre la perte, le vol, ou toute divulgation par des mécanismes de sécurité adaptés ;
- Les révoquer sans délai en cas de compromission réelle ou supposée.

Les MIE **ClearBUS** remis aux utilisateurs sont strictement personnels et ne doivent pas être communiqués ou transmis à des tiers.

Les utilisateurs font notamment leur affaire personnelle de la réparation de tous dommages éventuellement subis par eux-mêmes ou des tiers en cas de mauvaise utilisation ou de compromission des moyens d'identification électroniques leur permettant de s'authentifier auprès du service d'envoi Recommandé Electronique **ClearBUS**.

7.3 Règlement de conflits

Toutes contestations et litiges survenant dans l'interprétation et la mise en œuvre du présent document seront soumis à la juridiction des tribunaux dont ressort le siège social de **ClearBUS**.

7.4 Conformité aux législations et réglementations

Le service d'envoi Recommandé Electronique **ClearBUS** est opéré en France. La présente PRE est soumise au droit français et aux textes législatifs applicables à la présente PRE.

ClearBUS met en œuvre, à chaque fois que cela est possible, des moyens pour faciliter l'accès de ses services aux personnes en situation de handicap.

7.5 Droits sur la propriété intellectuelle et industrielle

Sur le plan de la propriété intellectuelle, les produits mis en œuvre par **ClearBUS** dans le service d'envoi recommandé électronique **ClearBUS-SRE** appartiennent aux éditeurs de ces produits.

Les utilisateurs de ces services ne disposent d'aucun droit de propriété intellectuelle sur ces différents éléments. Toute utilisation ou reproduction, totale ou partielle, de ces éléments et/ou des informations qu'ils contiennent, par quelque procédé que ce soit, est strictement interdite et constitue une contrefaçon sanctionnée par le Code de la propriété intellectuelle, sauf accord préalable et écrit de **ClearBUS**.

7.6 Limitation de responsabilité contractuelle

Les informations relatives à cette rubrique se trouvent dans les CGURE.