POLITIQUE ET PRATIQUES DU SERVICE D'ENVOI DE RECOMMANDÉ ÉLECTRONIQUE QUALIFIÉ

OID : 1.3.6.1.4.1.51537.1.1.1.3

Version 3.0

REFERENCE

Type de document :	**Procédure**
Centre(s) :	**Pôle Technologies – service LRE qualifiée**
Référence :	**SMQ-PR-1803**

Niveau de communicabilité : Public

VERSION EN VIGUEUR

N°	Date	Observations	Rédacteur	Vérificateur	Approbateur
3.1	18/11/2022	Version approuvée de la politique suite à décision de renouvellement de la qualification	E. LAVABRE V. PONCE	D. MUNOZ	S. SEILLIER

***Si ce document est à un indice supérieur à ceux précédemment diffusés, il les annule et les remplace.**
Le suivi des versions successives est disponible en annexe.

SOMMAIRE

1. INTRODUCTION 7

1.1. Présentation générale 7

1.2. Identification du document 7

1.3. Date d'entrée en vigueur 7

1.4. Gestion de la politique 8
1.4.1. Entité gérant la politique 8
1.4.2. Point de contact 8
1.4.3. Procédure d'approbation de la politique 8
1.4.4. Amendements à la politique 8
(1) Procédures d'amendement 8
(2) Mécanisme et période d'information sur les amendements 8
(3) Circonstances selon lesquelles l'OID doit être changé 9
1.4.5. Documents associés 9
(1) Politique d'horodatage 9
(2) Politique de certification du cachet électronique 9
(3) Politique de scellement électronique 9
(4) Conditions générales d'utilisation Destinataires 9
(5) Documents normatifs et techniques 9

1.5. Entités intervenant dans le service de recommandé électronique 10
1.5.1. Prestataire du service de recommandé électronique (PSRE) 10
1.5.2. Opérateur du service de recommandé électronique (OSRE) 11
1.5.3. Prestataire d'horodatage électronique (PSHE) 11
1.5.4. Prestataire de cachet électronique (PSCE) 11
1.5.5. Utilisateurs 11
(1) Expéditeur et mandataire 11
(2) Déposant 11
(3) Destinataire 11

2. RESPONSABILITES CONCERNANT LA MISE A DISPOSITION DES INFORMATIONS DEVANT ETRE PUBLIEES 12

2.1. Entités chargées de la mise à disposition des informations 12

2.2. Informations devant être publiées 12

2.3. Délais et fréquences de publication 12

2.4. Contrôle d'accès aux informations publiées 12

3. IDENTIFICATION ET AUTHENTIFICATION DES UTILISATEURS 13

3.1. Identification initiale et authentification de l'expéditeur 13
3.1.1. Vérification de l'identité de l'expéditeur 13
(1) Vérification par certificat RGS a minima ** / qualifie eIDAS 13
(2) Vérification en face à face 13
3.1.2. Vérification de l'identité des déposants de l'expéditeur 14
(1) Vérification initiale de l'identité 14
(2) Moyen d'identification technique 14
3.1.3. Conservation des preuves d'identification 14

3.2. Identification initiale et authentification du destinataire 14
3.2.1. Vérification de l'identité par certificat RGS a minima ** / qualifié eIDAS 15
3.2.2. Vérification de l'identité par l'usage d'une identité électronique figurant sur la liste publiée par la Commission Européenne et notifié par tout Etat Membre 15
3.2.3. Conservation des preuves d'identification 15

3.3. Cycle de vie des Moyens d'Identification Electroniques (MIE) 16
3.3.1. Remise à l'expéditeur 16
3.3.2. Remise au destinataire 16
3.3.3. Validité des MIE 17
3.3.4. Révocation du MIE 17
3.3.5. Origine d'une demande 17
3.3.6. Validation de la demande 17
3.3.7. Traitement d'une demande 17
3.3.8. Délai de traitement d'une demande 17

4. EXIGENCES OPERATIONNELLES 18

4.1. Processus d'envoi 18
4.1.1. Processus et responsabilités pour le dépôt d'une LRE 18
4.1.2. Exécution des processus d'identification et de validation du dépôt 18
4.1.3. Traitement du dépôt d'une LRE 18
4.1.4. Remise de la preuve de dépôt 18

4.2. Processus de remise 18
4.2.1. Information du destinataire 18
4.2.2. Exécution des processus d'identification du destinataire 18
4.2.3. Acceptation ou rejet de la LRE 19
4.2.4. Délai d'acceptation de la LRE 19
4.2.5. Transmission de la LRE 19
4.2.6. Remise de la preuve de réception 19
4.2.7. Remise de la preuve de refus 19
4.2.8. Remise de la preuve de non-réclamation (négligence) 19

4.3. Modification des données 19

4.4. Description des preuves 19
4.4.1. Bordereau de preuve 21
4.4.2. Preuve de dépôt 21
4.4.3. Preuve de réception 22
4.4.4. Preuve de refus 22
4.4.5. Preuve de non-réclamation 23

5. GESTION DES RISQUES 23

5.1. Analyse de risques 23

5.2. Homologation 23

5.3. PSSI 23

6. GESTION ET EXPLOITATION DU PSRE 24

6.1. Organisation interne 24
6.1.1. Fiabilité 24
6.1.2. Rôles de confiance 24
6.1.3. Séparation des tâches 24

6.2. Ressources humaines 25

6.2.1. Qualifications, compétences et habilitations requises 25
6.2.2. Procédures de vérification des antécédents 25
6.2.3. Exigences en matière de formation initiale 25
6.2.4. Exigences et fréquence en matière de formation continue 25
6.2.5. Sanctions en cas d'actions non autorisées 25
6.2.6. Exigences vis-à-vis du personnel des prestataires externes 25
6.2.7. Documentation fournie au personnel 25

6.3. Gestion des biens 26
6.3.1. Généralités 26
6.3.2. Supports 26

6.4. Contrôle d'accès 26

6.5. Cryptographie 26

6.6. Sécurité physique et environnementale 26
6.6.1. Situation géographique et construction des sites 26
6.6.2. Accès physique 26
6.6.3. Alimentation électrique et climatisation 27
6.6.4. Vulnérabilité aux dégâts des eaux 27
6.6.5. Prévention et protection incendie 27
6.6.6. Conservation des supports 27
6.6.7. Mise hors service des supports 27

6.7. Sécurité opérationnelle 27
6.7.1. Mesures de sécurité des systèmes informatiques 27
6.7.2. Exigences de sécurité techniques spécifiques aux systèmes informatiques 27
6.7.3. Niveau de qualification des systèmes informatiques 28
6.7.4. Mesures de sécurité liées au développement des systèmes 28
6.7.5. Mesures liées à la gestion de la sécurité 28
6.7.6. Évaluation des vulnérabilités 28
6.7.7. Horodatage / Système de datation 29

6.8. Sécurité réseau 29

6.9. Gestion des incidents et supervision 30
6.9.1. Procédures de remontée et de traitement des incidents et des compromissions 30

6.10. Gestion des traces 30
6.10.1. Type d'événements à enregistrer 30
6.10.2. Fréquence de traitement des événements enregistrés 31
6.10.3. Conservation des événements enregistrés 31
6.10.4. Protection des événements enregistrés 31
6.10.5. Procédure de sauvegarde des traces 32

6.11. Archivage des données 32
6.11.1. Types de données à archiver 32
6.11.2. Période de conservation des archives 32
6.11.3. Protection des archives 32
6.11.4. Exigences d'horodatage des données 33
6.11.5. Procédures de récupération et de vérification des archives 33

6.12. Continuité d'activité 33
6.12.1. Reprise suite à la compromission et sinistre 33
6.12.2. Procédures de reprise en cas de corruption des ressources informatiques (matériels, logiciels ou données) 33
6.12.3. Procédures de reprise en cas de compromission de la clé privée d'une composante 33
6.12.4. Capacités de continuité d'activité suite à un sinistre 34
6.12.5. Capacités de continuité d'activité suite à risque pandémie 34

6.13. Fin d'activité 34
6.13.1. Transfert d'activité 34
6.13.2. Fin d'activité définitive 34

6.14. Conformité 34
6.14.1. Fréquences et circonstances des évaluations 35
6.14.2. Identités et qualifications des évaluateurs 35
6.14.3. Relations entre évaluateurs et entités évaluées 35
6.14.4. Sujets couverts par les évaluations 35
6.14.5. Actions prises suite aux conclusions des évaluations 35
6.14.6. Notifications individuelles et communications entre les participants 35

7. AUTRES PROBLEMATIQUES METIERS ET LEGALES 36

7.1. Responsabilité financière 36
7.1.1. Couverture par les assurances 36
7.1.2. Couverture et garantie concernant les entités utilisatrices 36

7.2. Confidentialité des données professionnelles 36
7.2.1. Périmètre des informations confidentielles 36
7.2.2. Responsabilités en termes de protection des informations confidentielles 36

7.3. Protection des données personnelles 36
7.3.1. Politique de protection des données personnelles 36
7.3.2. Informations à caractère personnel 37
7.3.3. Responsabilité en termes de protection des données personnelles 37
7.3.4. Notification et consentement d'utilisation des données personnelles 37
7.3.5. Conditions de divulgation de données personnelles aux autorités judiciaires ou administratives 37

7.4. Obligations des utilisateurs 37
7.4.1. Utilisation des MIE (Moyens d'Identification Électroniques) 38
7.4.2. Utilisation des LRE 38

7.5. Droits sur la propriété intellectuelle et industrielle 38

7.6. Durée et fin anticipée de validité de la politique 39
7.6.1. Durée de validité 39
7.6.2. Fin anticipée de validité 39

7.7. Conformité aux législations et réglementations 39

7.8. Force majeure 39

8. ANNEXE 1 : SUIVI DES VERSIONS/REVISIONS SUCCESSIVES 40

1. INTRODUCTION

1.1. Présentation générale

Tessi Documents Services met en œuvre un Service d'Envoi Recommandé Electronique qui assure une distribution sécurisée de lettres recommandées électroniques entre un expéditeur et son destinataire, en apportant la preuve du processus de distribution.
Tessi Documents Services se positionne dans ce contexte en tant que Prestataire de Service d'Envoi Recommandé Electronique (ci-après « PSRE »). Le présent document constitue la Politique et les Pratiques du Service d'Envoi Recommandé Electronique de Tessi Documents Services. Ce document identifie également les obligations et exigences portant sur les autres intervenants du service.

« *La lettre recommandée électronique (LRE) a la même valeur juridique que celle d'une lettre recommandée au format papier, dès lors qu'elle répond à certaines conditions. Une lettre recommandée au format électronique est la version dématérialisée d'un recommandé au format papier. Elle peut être utilisée dans les mêmes situations que celle en version papier. […]*
Pour être juridiquement valable, l'envoi d'une lettre recommandée électronique doit remplir 3 conditions :

- *Le prestataire chargé de l'acheminement se porte responsable de la bonne identité du destinataire et de celle de l'expéditeur*
- *Les dates d'expédition et de réception de la lettre doivent être garanties et vérifiables*
- *Si le destinataire n'est pas un professionnel, son accord préalable est nécessaire (en cas de refus, l'expéditeur doit envoyer le recommandé au format papier)*
- *L'opérateur en charge de l'acheminement délivre à l'expéditeur une preuve du dépôt de sa lettre via un mail. Cette preuve doit être conservée pendant au moins un an.* »

(source https://www.service-public.fr/professionnels-entreprises/vosdroits/F31463)

Le présent document explicite les processus associés à l'envoi de recommandé électronique, en particulier les niveaux de sécurité recherchés (intégrité, authenticité,), de responsabilité, d'identification et la façon dont ils sont assurés (signature électronique, horodatage, traces informatiques notamment).

Pour les besoins du présent document :

- les lettres recommandées électroniques transitant via le Service d'Envoi Recommandé Electronique qualifié de Tessi Documents Services seront dénommées « LRE » ;
- le Service d'Envoi Recommandé Electronique qualifié mis en œuvre par Tessi Documents Services sera dénommé « Service LRE » ;
- Le présent document Politiques et Pratiques du Service d'Envoi Recommandé Electronique se nommera « Politique de Service ».

1.2. Identification du document

La présente politique est identifiée par l'OID suivant : 1.3.6.1.4.1.51537.1.1.1.3 et accessible via l'URL suivante : https://www.mon-recommande-electronique.fr/fr/politique-de-service.

1.3. Date d'entrée en vigueur

La présente politique entre en vigueur le jour de la parution du service et de sa politique dans la Trusted List.

1.4. Gestion de la politique

1.4.1. Entité gérant la politique

Prestataire de Service de Confiance pour la fourniture d'un Service d'Envoi Recommandé Électronique qualifié pour le périmètre décrit dans la présente politique :

TESSI DOCUMENTS SERVICES
SAS au capital de 1.000.000 €
Siège social : 116 rue de Silly – 92100 BOULOGNE-BILLANCOURT
RCS Nanterre : B 326 803 582
N° TVA intra-communautaire : FR 89 326 803 582
Président : TESSI SA (071 501 571 RCS Grenoble), représentée par M. Olivier JOLLAND

1.4.2. Point de contact

Contact : ls.serviceclient@tessi.fr
Téléphone : + 33(0)5 55 77 11 79

1.4.3. Procédure d'approbation de la politique

La politique est approuvée après examen et relecture par les membres du comité de pilotage du service d'envoi recommandé électronique qualifié, ou les personnes désignées par celui-ci. Cette relecture a pour objectif d'assurer :

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

1.4.4. Amendements à la politique

(1) Procédures d'amendement

Tessi Documents Services contrôle que tout projet de modification de sa politique reste conforme aux exigences réglementaires et normatives applicables.
La Politique de service est réexaminée à minima tous les deux (2) ans.

(2) Mécanisme et période d'information sur les amendements

Tessi Documents Services adressera annuellement à l'ANSSI une synthèse de l'ensemble des modifications apportées à la fourniture de ses services de confiance qualifiés.

(3) Circonstances selon lesquelles l'OID doit être changé

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

1.4.5. Documents associés

(1) Politique d'horodatage

La date et l'heure d'envoi, de réception et toute modification des données doivent être indiquées par un horodatage électronique qualifié.
La politique d'horodatage utilisée par le service de LRE de Tessi Documents Services a pour OID : 1.2.250.1.177.2.9.1.

(2) Politique de certification du cachet électronique

L'envoi et la réception de données sont sécurisés par un cachet électronique avancé d'un prestataire de confiance de service qualifié.
La politique de certification du cachet électronique utilisé par le service de LRE de Tessi Documents Services a pour OID : 1.2.250.1.177.2.0.1

(3) Politique de scellement électronique

L'envoi et la réception de données sont sécurisés par une signature électronique avancée.
La politique de scellement électronique utilisé par le service de LRE de Tessi Documents Services a pour OID : 1.2.250.1.177.2.6.4.4.1

(4) Conditions générales d'utilisation Destinataires

Les conditions générales d'utilisation Destinataires de la plateforme LRE de Tessi Documents Services sont référencés « SMQ-PR-1808 – Conditions Générales d'Utilisation » et accessibles sur https://www.mon-recommande-electronique.fr.

(5) Documents normatifs et techniques

[ANSSI_LRE]	Services d'envoi recommandé électronique qualifiés – Critères d'évaluation de la conformité au règlement eIDAS, Version 1.0 du 3 janvier 2017 https://www.ssi.gouv.fr/uploads/2016/06/eidas_envoi-recommande-electronique-qualifie_v1.0_anssi.pdf
[ANSSI_PSCO]	Prestataires de services de confiance qualifiés – Critères d'évaluation de la conformité au règlement eIDAS, Version 1.1 du 3 janvier 2017 https://www.ssi.gouv.fr/uploads/2016/06/eidas_pschttps://www.ssi.gouv.fr/uploads/2016/06/eidas_psc-qualifies_v1.1_anssi.pdfqualifies_v1.1_anssi.pdf

[EN_319401]	ETSI EN 319 401 V2.1.1 (2021-05) Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers http://www.etsi.org/
[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 http://www.etsi.org
[RGS]	Référentiel général de sécurité, Version 2.0 du 13 juin 2014.
[eIDAS]	Règlement Européen [eIDAS] 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 https://eur-lex.europa.eu/legal-content/fr/ALL/?uri=CELEX%3A32014R0910
[GDPR]	*Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016* https://www.cnil.fr/fr/reglement-europeen-protection-donnees
[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
[RGAA|	*Référentiel général d'amélioration de l'accessibilité – RGAA Version 4.1* Afin de faciliter la mise en œuvre de l'accessibilité numérique, la DINUM édite depuis 2009 le référentiel général d'amélioration de l'accessibilité – RGAA, créé pour mettre en œuvre l'article 47 de la loi handicap de 2005 (loi n° 2005-102 du 11 février 2005) et son décret d'application actualisé en 201 (décret n°2019-768 du 24 juillet 2019).

1.5. Entités intervenant dans le service de recommandé électronique

1.5.1. Prestataire du service de recommandé électronique (PSRE)

Le prestataire du service de recommandé électronique qualifié est la société Tessi Documents Services. Tessi Documents Services est le prestataire de services de confiance qui fournit le service qualifié, tel que défini dans le Règlement (UE) n° 910/2014, elle est garante de l'application opérationnelle de la présente Politique de service.

1.5.2. Opérateur du service de recommandé électronique (OSRE)

L'Opérateur du service de recommandé électronique est la société Logidoc Solutions. Logidoc Solutions a la charge de la mise en œuvre technique du service.

1.5.3. Prestataire d'horodatage électronique (PSHE)

La fourniture du service de LRE de Tessi Documents Services s'appuie sur un ou plusieurs prestataires d'horodatage électronique qualifié(s). À la date de rédaction de la présente politique, ce prestataire est la société CERTIGNA. Ce fournisseur est indépendant de Tessi Documents Services.

1.5.4. Prestataire de cachet électronique (PSCE)

Le certificat utilisé par Tessi Documents Services pour apposer ses cachets est fourni par CERTIGNA. Ce fournisseur est indépendant de Tessi Documents Services.

1.5.5. Utilisateurs

Les utilisateurs du service sont les expéditeurs et les destinataires de LRE, ainsi que toute personne ou entité s'appuyant sur les preuves émises par le service.

(1) Expéditeur et mandataire

Les expéditeurs de LRE sont des personnes morales produisant des courriers électroniques destinés à être acheminés par Tessi Documents Services sous le régime de la présente politique de service.
Un expéditeur est représenté par un ou plusieurs mandataires (personnes physiques), dont l'identité et le mandat sont vérifiés en face-à-face.

(2) Déposant

Un déposant est une personne physique ou un service technique d'une personne morale qui dépose des LRE auprès de Tessi Documents Services, habilité par l'expéditeur et ses mandataires pour ce faire.
La présente politique considère deux types de déposants :

- des serveurs informatiques appartenant à l'expéditeur ou à un tiers habilité par l'expéditeur ou ses mandataires ;
- des personnes physiques habilitées agissant pour le compte de l'expéditeur.

et ce si l'expéditeur n'a pas opté pour la signature de chaque LRE par un certificat a minima RGS ** et/ou qualifié eIDAS. Dans ce cas, le déposant est le porteur du certificat.

(3) Destinataire

Les destinataires de LRE sont des personnes morales ou physiques qui utilisent le Service LRE fourni par le PSRE pour recevoir des LRE.

2. RESPONSABILITES CONCERNANT LA MISE A DISPOSITION DES INFORMATIONS DEVANT ETRE PUBLIEES

2.1. Entités chargées de la mise à disposition des informations

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

2.2. Informations devant être publiées

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

- Le présent document, décrivant la politique et les pratiques du service de recommandé électronique qualifié ;
- Les documents associés mentionnés au 1.4.5, ou, dans le cas où un de ces documents serait maintenu et publié par un tiers, une référence univoque (URL, OID, etc.) à celui-ci et un point de publication ;
- Les conditions générales d'utilisation du service (1.4.5).

Lorsqu'une publication d'une nouvelle version de la Politique de service est planifiée, les informations relatives à cette évolution sont mises en ligne sur les lieux de publication à destination des utilisateurs du service LRE. 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.
Le document archivé (ancienne version) portera, en filigrane sur ses pages, la mention « Document obsolète ».

2.3. Délais et fréquences de publication

Les informations liées au service (nouvelle version des présentes, etc.) doivent être publiées dès que nécessaire afin que soit assurée à tout moment la cohérence entre les informations publiées et les engagements, moyens et procédures effectifs de Tessi Documents Services.

Les systèmes publiant ces informations doivent au moins être disponibles les jours ouvrés. Tessi Documents Services garantit la disponibilité et l'intégrité des informations publiées.

2.4. Contrôle d'accès aux informations publiées

L'ensemble des informations publiées est libre d'accès en lecture.
L'accès en modification aux systèmes de publication des autres informations est strictement limité aux fonctions internes habilitées de Tessi Documents Services, au moins au travers d'un contrôle d'accès de type mots de passe basé sur une politique de gestion stricte des mots de passe.

3. IDENTIFICATION ET AUTHENTIFICATION DES UTILISATEURS

3.1. Identification initiale et authentification de l'expéditeur

« *Le service d'envoi recommandé électronique qualifié doit garantir l'identification de l'expéditeur avec un degré de confiance élevé* » [ANSSI_LRE].

3.1.1. Vérification de l'identité de l'expéditeur

Le mode de vérification initiale de l'identité de l'expéditeur dépend du mode d'authentification qui sera utilisé par l'expéditeur par la suite :

- soit l'identité est vérifiée à chaque émission de LRE par la vérification à la volée du certificat RGS ** / qualifié eIDAS (3.1.1.1) de l'expéditeur ;
- soit si l'expéditeur s'authentifie via le certificat SSL de ses serveurs ou par un bi-facteur non rejouable, la vérification initiale de son identité se fera par un face à face (3.1.1.2).

(1) Vérification par certificat RGS a minima ** / qualifie eIDAS

L'expéditeur est identifié à chaque LRE par la vérification des données contenues dans le certificat RGS ** qualifié eIDAS qui est utilisé pour cacheter électroniquement chaque LRE au nom de l'expéditeur. La vérification porte alors sur les éléments suivants :

- Niveau de sécurité du certificat (a minima RGS ** / qualifié eIDAS) par vérification de la liste d'AC autorisées contenant les Autorités de Certification reconnues comme délivrant des certificats RGS ** et/ou *** et/ou qualifié eIDAS;
- Non-révocation du certificat ;
- Période de validité du certificat.

(2) Vérification en face à face

En cas d'authentification de l'expéditeur par usage d'un certificat SSL ou par bi-facteur non-rejouable, l'expéditeur est identifié préalablement à toute utilisation du service lors d'un face à face entre un personnel de Tessi Documents Services (ou d'une entité du groupe Tessi mandaté par elle) et une personne mandatée par l'expéditeur (le mandataire).
Lors de ce face à face, le personnel dûment mandaté et habilité par Tessi Documents Services recueille les éléments suivants :

- Un K-BIS en cours de validité attestant l'identité de la personne morale expéditrice ;
- L'adresse courriel de réception d'envoi recommandé électronique du mandataire (servant d'identifiant sur le site destinataire de la LRE) dans le cas où l'expéditeur est également destinataire du service ;
- Le certificat SSL qui sera utilisé par l'expéditeur pour la transmission des courriers si concerné.

Le personnel de Tessi Documents Services vérifie par ailleurs et atteste de manière contradictoire avoir pris connaissance des éléments suivants :

- Une copie d'une pièce d'identité en cours de validité certifié conforme à l'original du représentant légal de l'expéditeur ;

- Une preuve d'habilitation du mandataire de l'expéditeur (p.ex. délégation signée d'un représentant légal) contenant ses nom et prénom ;
- Une pièce d'identité originale en cours de validité du mandataire.

Il remet enfin à l'expéditeur le code d'enrôlement lié au compte pour l'authentification ultérieure de l'expéditeur dans le cas d'une authentification par bi-facteur non rejouable.
Les copies de pièces d'identité ne sont en aucun cas conservées par le personnel de Tessi Documents Services. Leur vérification est validée par la signature conjointe d'une attestation de remise en main propre précisant que le corpus fourni permet de garantir l'identité de l'Expéditeur.

3.1.2. Vérification de l'identité des déposants de l'expéditeur

(1) Vérification initiale de l'identité

L'identité du (ou des) déposant(s) est établie par le mandataire de l'expéditeur selon un processus propre à l'entité.

(2) Moyen d'identification technique

Si l'expéditeur n'a pas opté pour la vérification d'identité par certificat RGS a minima ** / qualifié eIDAS, Tessi Documents Services authentifie alors le déposant de la façon suivante, selon les cas :

- S'agissant de serveurs transmettant des flux, la communication s'appuie alors sur une authentification par certificat SSL client préalablement déclaré auprès de Tessi Documents Services.
- S'agissant de personnes physiques habilitées agissant pour le compte d'une personne morale venant déposer des courriers à travers une interface Web, celles-ci s'authentifient auprès de Tessi Documents Services en utilisant un couple identifiant/mot de passe et OTP dynamique (authentification bi-facteur non rejouable) défini ultérieurement dans le la présente politique (chapitre 3.3).

3.1.3. Conservation des preuves d'identification

Les preuves relatives à l'identité et à l'identification de l'expéditeur, de ses mandataires et déposants sont rassemblées dans une « enveloppe de preuve » électronique conservée pour a minima sept ans à compter de la réception des données.
L'enveloppe contient :

- L'ensemble des informations vérifiées dans le certificat de niveau suffisant utilisé le cas échéant ;
- L'ensemble des éléments collectés lors de la phase initiale en face à face le cas échéant ;
- Les traces de contrôle de recevabilité ;
- La confirmation ou le rejet de l'identité.

3.2. Identification initiale et authentification du destinataire

« *Le service d'envoi recommandé électronique qualifié doit garantir l'identification du destinataire avant la fourniture des données. […] cette vérification d'identité doit au minimum respecter les exigences du chapitre 2.1 du règlement [RE_2015_1502] pour le niveau substantiel* » [ANSSI_LRE].

La vérification d'identité et l'authentification du destinataire peuvent se faire de 2 manières :

- par l'utilisation d'un certificat électronique de niveau suffisant ;
- par l'utilisation d'une identité électronique figurant sur la liste publiée par la Commission Européenne et notifiée par tout Etat membre (notamment via l'utilisation de FranceConnect) ;
- Si et seulement si le destinataire s'est d'ores et déjà identifié initialement par l'un des deux moyens prévus ci-dessus, par un bi-facteur non-rejouable.

Ainsi, Le mode de vérification initiale de l'identité du destinataire dépend du mode d'authentification qui sera utilisé par le destinataire par la suite :

3.2.1. Vérification de l'identité par certificat RGS a minima ** / qualifié eIDAS

L'identification du destinataire se fait par l'utilisation d'un certificat électronique d'un niveau suffisant et s'opère à chaque réception de lettre recommandée électronique.

Le portail destinataire demande à l'utilisateur de présenter un certificat a minima RGS ** / qualifié eIDAS pour accéder à chaque nouvelle LRE non encore acceptée. Il peut cependant accéder à ses courriers déjà acceptés sans avoir à utiliser son certificat.

Pour récupérer toute nouvelle LRE, l'utilisateur est invité à s'identifier en présentant son certificat. Le portail effectue alors la vérification des points suivants :

- Certificat en cours de validité ;
- Certificat non révoqué ;
- Niveau de sécurité du certificat (RGS** ou *** ou qualifié eIDAS) ;
- Cohérence entre SIREN du certificat et SIREN du destinataire du courrier.

Si tous ces contrôles sont validés, l'utilisateur accède au service complet. Sinon, l'utilisateur obtiendra un message l'informant du point bloquant.

3.2.2. Vérification de l'identité par l'usage d'une identité électronique figurant sur la liste publiée par la Commission Européenne et notifié par tout Etat Membre

L'identification du destinataire se fait par l'utilisation de toute identité électronique de niveau à minima substantiel figurant sur la liste publiée par la Commission Européenne et notifié par tout Etat Membre au moment de l'identification. L'utilisateur, par le l'usage de la plateforme France Connect, peut ainsi faire appel à son identité électronique pour s'identifier et récupérer sa LRE.

NB : FranceConnect + est une plateforme permettant de mettre en relation des fournisseurs d'identité électronique et des fournisseurs de services afin de permettre l'identification des utilisateurs de ces derniers. Chaque fournisseur d'identité électronique est enregistré auprès de FranceConnect + avec l'indication des niveaux de garantie offerts (faible, substantiel, élevé) et chaque fournisseur de service indique le niveau de garantie requis pour l'identification sur ses services en ligne. Le choix du fournisseur d'identité électronique est laissé à chaque utilisateur. Si aucun fournisseur d'identité n'est proposé à l'utilisateur par FranceConnect +, FranceConnect + retourne un échec.

3.2.3. Conservation des preuves d'identification

Les preuves relatives à l'identité et à l'identification du destinataire sont rassemblées dans une « enveloppe de preuve » électronique conservée 7 ans minimum dans un système d'archivage électronique à valeur probatoire.

L'enveloppe contient :

- L'ensemble des informations vérifiées dans le certificat de niveau suffisant utilisé le cas échéant ;
- L'ensemble des éléments collectés lors de la phase initiale en face à face le cas échéant ;
- Le code d'enrôlement pour l'appairage de Tessi Authenticator / grille de codes le cas échéant ;
- Les traces de contrôle de recevabilité ;
- La confirmation ou le rejet de l'identité.

3.3. Cycle de vie des Moyens d'Identification Electroniques (MIE)

Ce chapitre ne traite que des MIE fournis par Tessi Documents Services. Dans le cadre de la présente politique, le MIE est soit une grille de codes, soit une application d'authentification par OTP (Tessi-Authenticator), déployée sur téléphone mobile ou tablette ou PC, venant compléter le mot de passe (statique) des utilisateurs avec un second facteur dynamique non-rejouable.

3.3.1. Remise à l'expéditeur

Lors de la validation initiale de son identité (chapitre 3.1.1 (2)) et si nécessaire, le mandataire de l'expéditeur se voit remettre en main propre un code d'enrôlement à usage unique. Ce code lui permet d'enrôler l'application et de l'associer à son compte sur le portail expéditeur.

Tessi Authenticator est un MIE fourni par Tessi Documents Services qui émet des codes OTP :

- fournis à la volée par l'application ;
- ou bien fournis par l'appel à une grille de codes personnelle fixe dont l'interprétation restitue des codes uniques et aléatoires.

Le code d'enrôlement (qui permet à l'expéditeur d'appairer l'application Tessi Authenticator et le compte utilisateur du Portail Expéditeur) ou la grille de codes liés au compte du déposant permettant l'authentification via bi-facteur non rejouable est remis à l'expéditeur :

- en mains propres ;
- ou par email.

3.3.2. Remise au destinataire

Si et seulement si le destinataire s'est d'ores et déjà identifié par l'un des deux moyens prévus au 3.2.1 et au 3.2.2, le destinataire peut utiliser le moyen d'authentification bi-facteur non-rejouable de Tessi Authenticator associé à son compte pour s'authentifier, accepter, refuser ou consulter des LRE.

Tessi Authenticator est un MIE fourni par Tessi Documents Services qui émet des codes OTP :

- fournis à la volée par l'application ;
- ou bien fournis par l'appel à une grille de codes personnelle fixe dont l'interprétation restitue des codes uniques et aléatoires.

Le code d'enrôlement (qui permet au destinataire d'appairer l'application Tessi Authenticator et le compte utilisateur du Portail Destinataire lors de la première utilisation) ou la grille de codes liés au compte du destinataire permettant l'authentification via bi-facteur non rejouable est remis au destinataire :

- concernant l'appairage de l'application Tessi Authenticator : par un affichage temporaire sur l'espace personnel de l'utilisateur sur le Portail Destinataire lorsque celui-ci est authentifié et clique sur le bouton « changer /renouveler mon MIE » ;
- concernant la grille de codes : par courrier postal à l'adresse du destinataire.

3.3.3. Validité des MIE

L'activation des MIE sujets de ce chapitre ont une durée de validité d'un (1) an. Quinze (15) jours avant la date anniversaire, l'utilisateur est prévenu par mail de la nécessité de renouveler son MIE (c'est-à-dire son enrôlement au MIE choisi). Le process de renouvellement se fait en ligne, depuis l'espace personnel de l'utilisateur, avec une authentification renforcée.

3.3.4. Révocation du MIE

3.3.5. Origine d'une demande

La demande de révocation d'un MIE peut être déposée par le porteur (identifié par le compte associé sur la plateforme expéditeur ou destinataire) de celui-ci, ou par le mandataire dans le cas d'un déposant, ou par le prestataire qualifié Tessi Documents Services dans le cas de fraude avérée ou de non-respect des CGU.
Pour déposer la demande, le porteur se connecte à son compte sur la plateforme (expéditeur ou destinataire).
La demande de révocation est également implicite en cas de refus des CGU préalablement acceptées.

3.3.6. Validation de la demande

Une demande de révocation est validée dès lors que le porteur est authentifié (connecté) si la demande provient du porteur ou du mandataire dans le cas d'un déposant.
La révocation est validée automatiquement dans les autres cas visés ci-dessus.

3.3.7. Traitement d'une demande

La demande est traitée automatiquement par la plateforme.

3.3.8. Délai de traitement d'une demande

La demande est traitée dans les secondes qui suivent sa validation.
En cas de révocation, quelle qu'en soit l'origine, il est de la pleine responsabilité de l'Utilisateur de supprimer l'application Tessi-Authenticator ou son compte lié au service dans l'application Tessi-Authenticator et de détruire sa grille de codes.

4. EXIGENCES OPERATIONNELLES

4.1. Processus d'envoi

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

Les LRE sont transmises par les déposants habilités. Il s'agit, dans tous les cas, de fichiers au format PDF. L'expéditeur est responsable de l'identité (SIREN) et des coordonnées (adresse courriel) du destinataire de la LRE et du recueil du consentement préalable à l'utilisation de la voie électronique pour l'envoi de courriers recommandés des destinataires personnes physiques le cas échéant.

4.1.2. Exécution des processus d'identification et de validation du dépôt

Les déposants sont authentifiés soit sous la forme d'une authentification SSL cliente (flux), préalablement au dépôt des LRE, soit à travers l'utilisation d'un certificat a minima RGS ** / qualifié eIDAS à chaque LRE.

4.1.3. Traitement du dépôt d'une LRE

Dès réception, le fichier PDF reçu (signé le cas échéant par le certificat RGS a minima ** / qualifié eIDAS au nom de l'expéditeur) est scellé avec le cachet électronique du service (1.4.5) et l'heure et la date de dépôt son horodatés (1.4.5) dans le bordereau de preuve (4.4.1).
C'est la date de cet horodatage qui vaut preuve de dépôt de la LRE.

4.1.4. Remise de la preuve de dépôt

Le statut de la LRE est disponible à tout instant dans l'espace personnel de l'expéditeur. Les preuves ne sont mises à disposition de l'expéditeur qu'une fois que le statut final de la LRE concernée est connu (non réclamé, accepté ou refusé).

4.2. Processus de remise

4.2.1. Information du destinataire

Si le destinataire est une personne physique, son consentement à recevoir des LRE a été préalablement recueilli par l'expéditeur ou une personne mandatée par l'expéditeur.
Le destinataire est informé par courriel à l'adresse indiquée par l'expéditeur d'une LRE.
La notification apparaît aussi dans l'espace personnel du destinataire, si celui-ci dispose déjà d'un compte sur le portail destinataire (https://www.mon-recommande-electronique.fr/).

4.2.2. Exécution des processus d'identification du destinataire

Pour toute nouvelle LRE qu'il souhaite accepter ou refuser, le destinataire doit s'identifier et/ou s'authentifier comme indiqué au Chapitre 3 du présent document
Une fois acceptée par le destinataire, la LRE lui est accessible sans suivre le process d'authentification renforcé (pour réceptionner une LRE) de l'article 3.2. La LRE lui est rendue accessible dans son espace personnel du Portail Destinataire, via login/mot de passe.

4.2.3. Acceptation ou rejet de la LRE

L'acceptation et le rejet se font par le biais du portail destinataire.

4.2.4. Délai d'acceptation de la LRE

Le destinataire dispose d'un délai de quinze (15) jours, à compter du lendemain de la première notification, pour accepter ou refuser la LRE. Le destinataire peut également négliger sa LRE, c'est-à-dire ne réaliser aucune action d'acceptation ou de refus dans le délai des quinze 15) jours à compter de la notification.

4.2.5. Transmission de la LRE

Si le destinataire accepte la LRE, le contenu du fichier PDF correspondant lui est présenté. En cas de refus, le destinataire n'aura pas connaissance du contenu de la LRE, ni de l'identité de l'expéditeur.

4.2.6. Remise de la preuve de réception

Suite à l'acceptation d'une LRE par le destinataire, le bordereau de preuve (4.4) est mis à disposition de l'expéditeur et indique le statut final « accepté ».

4.2.7. Remise de la preuve de refus

Suite au refus d'une LRE par le destinataire, le bordereau de preuve (4.4) est mis à disposition de l'expéditeur et indique le statut final « refusé ».

4.2.8. Remise de la preuve de non-réclamation (négligence)

À l'expiration du délai de réclamation, le bordereau de preuve (4.4) est mis à disposition de l'expéditeur et indique le statut final « non-réclamé ».

4.3. Modification des données

Le service de la LRE ne procède à aucune modification des données échangées à l'exception de l'apposition sur chaque courrier du numéro unique d'identification tel que repris dans le bordereau de preuves.

4.4. Description des preuves

Les preuves relatives à une LRE sont rassemblées dans une « enveloppe de preuve » électronique. L'enveloppe contient :

1) Le bordereau de preuve (scellé en fin de processus, voir ci-après)
2) Le fichier PDF signé par le certificat RGS ** /qualifié eIDAS au nom de l'expéditeur le cas échéant, et scellé par le Cachet électronique qualifié du PSRE (contenu de la LRE)
3) Les courriels envoyés au destinataire (EML) :
    a) Notification initiale (avis de mise à disposition)
    b) Expiration du délai de réclamation (délai différent par expéditeur)

4) Les jetons d'horodatage qualifié appliqués sur :
   a) Le fichier PDF scellé (élément 2) ci-dessus)
   b) Le courriel envoyé aux destinataires 3)a) et b)
   c) L'acceptation ou refus d'une LRE,
5) Les traces d'authentification (destinataire),
6) Un fichier XML technique relatif au dépôt par l'émetteur,
7) Les traces de vérification d'identité expéditeur :
   a) Soit le Log du contrôle de niveau de sécurité du certificat,
   b) Soit le code OTP d'enrôlement d'authentification.
8) Les traces de vérification de renforcement d'authentification destinataire :
   a) Soit des certificats RGS ** ou *** qualifiés eIDAS :
      i) Concernant le certificat utilisé :
         (1) Numéro de série,
         (2) Date de validité,
         (3) AC,
         (4) Nom Prénom,
         (5) Entité juridique associée,
         (6) Niveau de sécurité
      ii) Logs :
         (1) Log du contrôle de niveau de sécurité du certificat,
         (2) Log du contrôle du SIREN,
   b) Soit le code OTP d'enrôlement d'authentification et l'identifiant du compte,
   c) Soit le log de réponse du fournisseur d'identité.

4.4.1. Bordereau de preuve

Le bordereau de preuve est un fichier PDF contenant plusieurs sections, structurées comme suit :

B/1	Numéro de LRE	Le bordereau contient un numéro unique permettant d'identifier la LRE.
B/2.1	Chargement : Publié	Contient la trace de réception des données à traiter.
B/2.2	Certifié	Reprend la date de l'horodatage du scellement du contenu de la LRE. Cette section contient l'identité de l'expéditeur telle qu'elle figure dans le certificat RGS ** ou ** qualifié eIDAS utilisé.
B/2.3	Réception et apposition cachet serveur	Réception et apposition cachet Tessi Documents Services.
B/3	Conditions Générales d'Utilisation (CGU)	Un rappel de la trace d'acceptation des CGU par le destinataire.
B/4	Avisé	Preuve de notification au destinataire. Reprend la date de l'horodatage qualifié du courriel de notification. Cette section contient l'identité du destinataire telle qu'indiquée par l'expéditeur.
B/5	Accepté	Section présente si le destinataire a accepté la LRE. Reprend la date de l'horodatage de l'événement.
B/6	Refusé	Section présente si le destinataire a refusé la LRE. Reprend la date de l'horodatage de l'événement.
B/7	Non-réclamé (négligé)	Section présente si le destinataire ne s'est pas manifesté dans les délais. Reprend la date de l'horodatage du courriel d'expiration.

Lorsque le cycle de vie d'une LRE est arrivé à son terme (étape B/5, B/6 ou B/7), le bordereau est scellé électroniquement (1.4.5).
Le bordereau de preuve est mis à disposition de l'expéditeur.

4.4.2. Preuve de dépôt

La preuve de dépôt contient :

Donnée	Précisions
Nom et prénom ou raison sociale de l'expéditeur	Tel que mentionné dans le bordereau de preuve (B/2.2).
Adresse électronique de l'expéditeur	Telle que mentionnée dans le bordereau de preuve (B/2.2).

Adresse postale de l'expéditeur	Cette donnée est optionnelle
Nom et prénom ou raison sociale du destinataire	Tel que mentionné dans le bordereau de preuve (B/4).
Adresse électronique du destinataire	Telle que mentionnée dans le bordereau de preuve (B/4).
Adresse postale du destinataire	Cette donnée est optionnelle
Niveau de garantie	Cette donnée est optionnelle
Numéro d'identification unique de l'envoi	Tel que mentionné dans le bordereau de preuve (B/1).
Date et heure de l'envoi	Telle que mentionnée dans le bordereau de preuve (B/4).
Cachet électronique avancé	Cachet au nom du PSRE apposé sur les données (contenu du pli) pour les protéger contre toute modification

4.4.3. Preuve de réception

La preuve de réception contient :

Donnée	Précisions
Les données de la preuve de dépôt (4.4.1)	Telles qu'apparaissant dans le bordereau de preuve.
Identité du destinataire	Telle que mentionnée dans le bordereau de preuve (B/5).
Référence à l'identification préalable du destinataire	Telle que mentionnée dans le bordereau de preuve (B/5).
Date et heure de réception	Telle que mentionnée dans le bordereau de preuve (B/5).

4.4.4. Preuve de refus

La preuve de refus contient :

Donnée	Précisions
Les données de la preuve de dépôt (4.4.1)	Telles qu'apparaissant dans le bordereau de preuve.
Date et heure de refus	Telle que mentionnée dans le bordereau de preuve (B/6).

4.4.5. Preuve de non-réclamation

La preuve de non-réclamation (négligence) contient :

Donnée	Précisions
Les données de la preuve de dépôt (4.4.1)	Telles qu'apparaissant dans le bordereau de preuve.
Date et heure de non réclamation	Telle que mentionnée dans le bordereau de preuve (B/7).

5. GESTION DES RISQUES

5.1. Analyse de risques

Avant le lancement du service d'envoi recommandé électronique qualifié selon le périmètre décrit à la présente politique, Tessi Documents Services effectue une évaluation des risques afin d'identifier, d'analyser et d'évaluer les risques, en tenant compte des aspects techniques et commerciaux. L'analyse de risque identifie, en particulier, les systèmes « critiques » du service.
Les mesures de sécurité seront prises en tenant compte du résultat de cette analyse.
Tessi Documents Services fixe, dans sa PSSI, les exigences de sécurité et les procédures opérationnelles nécessaires pour mettre en œuvre les mesures identifiées.
L'analyse de risques est examinée et révisée annuellement. Elle est aussi mise à jour à chaque modification ayant un impact important sur le service, notamment en cas de modification des politiques ou pratiques relatives à sa fourniture.
Les risques résiduels identifiés sont acceptés durant le processus d'homologation du service.

5.2. Homologation

Suite à la finalisation de l'analyse de risque, Tessi Documents Services procède à l'homologation de son service LRE. Cette homologation est réalisée préalablement à la fourniture du service de confiance qualifié puis révisée au moins tous les deux ans.

5.3. PSSI

Tessi Documents Services dispose d'une politique de sécurité du système d'information (PSSI) applicable au service LRE. Cette PSSI est approuvée par la direction.
La PSSI et ses différentes versions seront communiquées aux abonnés du service, aux prestataires, aux organismes d'évaluation et à l'ANSSI.
La PSSI est transmise aux employés et aux éventuels sous-traitants.
Tessi Documents Services conserve la responsabilité globale de la conformité avec les procédures prévues dans sa PSSI, même lorsque certaines fonctions sont mises en œuvre par des sous-traitants. En particulier, Tessi Documents Services s'assure de la mise en œuvre effective des mesures prévues dans la PSSI. La PSSI établit un inventaire des actifs du SI. Cet inventaire est revu régulièrement.

Tout changement susceptible d'avoir un impact sur le niveau de sécurité fourni doit être approuvé par le comité de pilotage du service.
La configuration du SI est régulièrement auditée afin de détecter tout changement pouvant être à l'origine d'une violation des politiques de sécurité.

6. GESTION ET EXPLOITATION DU PSRE

6.1. Organisation interne

6.1.1. Fiabilité

Les objectifs et mesures pour assurer la fiabilité du service sont décrites dans le présent chapitre.

6.1.2. Rôles de confiance

Des rôles de confiance sont attribués à des personnes sur lesquelles repose la sécurité du Service d'envoi Recommandé Electronique.

Les rôles de confiance identifiés sont les suivants (liste non-exhaustive) :

- **Responsable opérationnel sécurité SI :** personne chargée de la mise en œuvre de la politique de sécurité sur les composantes du système d'information supportant le service LRE. Elle est en particulier en charge de l'analyse récurrente des événements intervenant sur les composantes du service et dispose d'un accès aux journaux d'audit et aux archives afin de s'assurer que les opérations réalisées sur le système sont légitimes.
- **Technicien d'exploitation :** Personnes chargées de la mise en route, de la configuration et de la maintenance technique des équipements informatiques (configuration, sauvegardes, restaurations…). Elles assurent l'administration technique des systèmes et des réseaux de la composante, ainsi que leur surveillance (détection d'incident).
- **Technicien support informatique :** personnes en charge du fonctionnement quotidien du service (cf. chapitre 4) : support client, gestion éventuelle du MIE, etc.
- **Responsable exploitation Informatique :** Personne autorisée à accéder aux preuves (4.4) et archives du service.
- **Responsable du cachet :** le cachet utilisé pour sceller la LRE, même opéré par le tiers CERTIGNA, reste sous la responsabilité de Tessi Documents Services. À ce titre, une ou plusieurs personnes sont responsables du cachet vis-à-vis de Tessi Documents Services, mais aussi de l'autorité de certification qui l'a émis.

6.1.3. Séparation des tâches

Plusieurs rôles peuvent être attribués à une même personne, dans la mesure où le cumul ne compromet pas la sécurité des fonctions mises en œuvre.
Concernant les rôles de confiance, le cumul suivant est impossible : Responsable opérationnel sécurité SI et tout autre rôle opérationnel.

6.2. Ressources humaines

6.2.1. Qualifications, compétences et habilitations requises

Tessi Documents Services s'assure de la compétence et de l'adéquation des personnels employés.

6.2.2. Procédures de vérification des antécédents

Tessi Documents Services met en œuvre tous les moyens légaux dont il dispose pour s'assurer de l'honnêteté du personnel qu'il emploie. Ces personnels ne doivent notamment pas avoir de condamnation de justice en contradiction avec leurs attributions.
À ce titre, il peut demander la communication d'une copie du bulletin n° 3 du casier judiciaire et peut décider, en cas de refus de communiquer cette copie ou en cas de présence de condamnation de justice incompatible avec les attributions de la personne, de lui retirer ces attributions.
Ces vérifications sont menées préalablement à l'affectation à un rôle de confiance et revues régulièrement (au minimum tous les 3 ans).

6.2.3. Exigences en matière de formation initiale

Le personnel est préalablement formé aux logiciels, matériels et procédures internes de fonctionnement et de sécurité qu'il met en œuvre et qu'il doit respecter.
Les personnels ont pris connaissance et compris les implications des opérations dont ils ont la responsabilité.

6.2.4. Exigences et fréquence en matière de formation continue

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

6.2.5. Sanctions en cas d'actions non autorisées

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

6.2.6. Exigences vis-à-vis du personnel des prestataires externes

Le personnel des prestataires externes intervenant sur les composantes du service est soumis aux exigences de la présente section (6.2). Cela apparaît dans des clauses spécifiques dans les contrats avec ces prestataires.
En particulier, la PSSI du service (5.3) est transmise aux prestataires externes.

6.2.7. Documentation fournie au personnel

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

6.3. Gestion des biens

6.3.1. Généralités

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

6.3.2. Supports

Les supports sont gérés en adéquation avec leur classification.

6.4. Contrôle d'accès

Tessi Documents Services met en œuvre un contrôle d'accès aux systèmes d'information du service de recommandé électronique.
Des procédures de gestion des habilitations sont mises en œuvre, prenant en compte les différents rôles identifiés par la présente politique (6.1.2). Ces procédures assurent que l'octroi et le retrait des habilitations s'effectue en accord avec la gestion des ressources humaines.
Tout utilisateur doit être identifié et authentifier avant de pouvoir accéder aux systèmes critiques du service (5.1).
Toute action doit être tracée de sorte à pouvoir être imputable à la personne l'ayant effectuée.
L'accès aux logiciels d'exploitation (console, utilitaires, scripts, etc.) sur les serveurs est restreint et contrôlé.
Les informations sensibles doivent être protégées contre la divulgation résultant de la réutilisation de ressources (p. ex. fichiers effacés) par des personnels non autorisés.
La PSSI (5.3) décrit en détail les règles de contrôle d'accès applicables au SI du service.
Voir 6.8 pour le contrôle d'accès au niveau réseau.

6.5. Cryptographie

Les modules cryptographiques employés pour les opérations sensibles du Service répondent aux exigences du document [ANSSI_PSCO].

6.6. Sécurité physique et environnementale

6.6.1. Situation géographique et construction des sites

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

6.6.2. Accès physique

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

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

6.6.3. Alimentation électrique et climatisation

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

6.6.4. Vulnérabilité aux dégâts des eaux

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

6.6.5. Prévention et protection incendie

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

6.6.6. Conservation des supports

Les différentes informations intervenant dans les activités du service sont identifiées, et leurs besoins de sécurité, définis (en confidentialité, intégrité et disponibilité). Tessi Documents Services maintient un inventaire de ces informations et met en place des mesures pour en éviter la compromission et le vol.
Les supports (papier, disque dur, disquette, CD, etc.) correspondant à ces informations sont gérés selon des procédures conformes à ces besoins de sécurité.
Des procédures de gestion doivent protéger ces supports contre l'obsolescence et la détérioration pendant la période de temps durant laquelle Tessi Documents Services s'engage à conserver les informations qu'ils contiennent.

6.6.7. Mise hors service des supports

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

6.7. Sécurité opérationnelle

6.7.1. Mesures de sécurité des systèmes informatiques

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

6.7.2. Exigences de sécurité techniques spécifiques aux systèmes informatiques

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

- Identification et authentification forte des utilisateurs pour l'accès au système (authentification à deux facteurs, de nature physique et/ou logique) ;

- Gestion des droits des utilisateurs (permettant de mettre en œuvre la politique de contrôle d'accès, notamment pour implémenter les principes de moindres privilèges, de contrôles multiples et de séparation des rôles) ;
- Gestion de sessions d'utilisation (déconnexion après un temps d'inactivité, accès aux fichiers contrôlé par rôle et nom d'utilisateur) ;
- Protection contre les virus informatiques et toutes formes de logiciels compromettants ou non-autorisés et mises à jour des logiciels ;
- Gestion des comptes des utilisateurs, notamment la modification et la suppression rapide des droits d'accès ;
- Protection du réseau contre toute intrusion d'une personne non autorisée ;
- Protection du réseau afin d'assurer la confidentialité et l'intégrité des données qui y transitent ;
- Fonctions d'audits (non-répudiation et nature des actions effectuées) ;
- Eventuellement, gestion des reprises sur erreur.
- Les applications utilisant les services des composantes peuvent requérir des besoins de sécurité complémentaires.

6.7.3. Niveau de qualification des systèmes informatiques

Voir 6.5.

6.7.4. Mesures de sécurité liées au développement des systèmes

L'implémentation d'un système contribuant au service doit être documentée et doit respecter, dans la mesure du possible, des normes de modélisation et d'implémentation. La configuration des composantes du service, ainsi que toute modification et mise à niveau, doivent être documentées et contrôlées.
Tessi Documents Services garantit que les objectifs de sécurité sont définis lors des phases de spécification et de conception.
Tessi Documents Services utilise des systèmes et des produits fiables qui sont protégés contre toute modification.
Conformément au [GDPR] et dans le respect de la démarche *Privacy by design& by default*, Tessi Documents Services met en œuvre toutes les mesures techniques et organisationnelles nécessaires au respect de la protection des données personnelles, à la fois dès la conception des produits et des services, en veillant notamment à limiter la quantité de données traitée dès le départ (principe dit de « minimisation »).

6.7.5. Mesures liées à la gestion de la sécurité

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

6.7.6. Évaluation des vulnérabilités

Les procédures d'exploitation du SI incluent la veille sécuritaire de ses composants. Ces procédures assurent que les correctifs de sécurité sont appliqués, entre un (1) et six (6) mois après leur publication au plus tard, selon la Politique de Sécurité des Systèmes d'Information de Tessi Documents Services. Dans tous les cas,

une analyse d'impact est réalisée afin de déterminer l'opportunité de les appliquer ; si un correctif n'est pas appliqué, l'analyse en justifie la décision.
Dans le cas de vulnérabilités « critiques » (CVSS=10), l'analyse d'impact doit être effectuée dans les 48 heures suivant la publication de la vulnérabilité.

6.7.7. Horodatage / Système de datation

Plusieurs exigences de la présente politique nécessitent la datation par les différentes composantes des événements liés aux activités du service.
Pour dater ces évènements, les différentes composantes du service recourent à l'utilisation de l'heure système, en assurant une synchronisation quotidienne de celle-ci, au minimum à la minute près, et par rapport à une source fiable de temps UTC.

6.8. Sécurité réseau

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

- Le SI doit être segmenté en réseaux ou zones en fonction de l'analyse des risques, compte tenu de la relation fonctionnelle, logique et physique entre les composants et les services. Les mêmes contrôles de sécurité doivent être appliqués à tous les systèmes partageant la même zone.
- L'interconnexion vers des réseaux publics doit être protégée par des passerelles de sécurité configurées pour n'accepter que les protocoles nécessaires au fonctionnement de la composante au sein du SI du service.
- Tessi Documents Services garantit que les composants du réseau local (routeurs, etc.) sont maintenus dans un environnement physiquement sécurisé et que leurs configurations sont périodiquement auditées en vue de vérifier leur conformité avec les exigences de la présente politique ; des dispositifs de surveillance (avec alarme automatique) de ces configurations doivent être mis en place.
- Tous les systèmes critiques (cf. 5.1) doivent être isolés dans une ou plusieurs zones sécurisées.
- L'exploitation des systèmes est réalisée à travers un réseau d'administration dédié et cloisonné. Les systèmes utilisés pour l'administration de la mise en œuvre de la politique de sécurité ne doivent pas être utilisés à d'autres fins. Les systèmes de production du service doivent être séparés des systèmes utilisés pour le développement et les tests.
- La communication entre des systèmes de confiance distincts ne doit être établie qu'à travers des canaux sécurisés, logiquement distincts des autres canaux de communication, assurant une authentification de bout en bout, l'intégrité et la confidentialité des données transmises.
- Si un niveau élevé de disponibilité au service de confiance est nécessaire, la connexion réseau externe doit être redondante pour assurer la disponibilité des services.
- Une analyse de vulnérabilité régulière sur les adresses IP publiques et privées du service, identifiées par Tessi Documents Services, doit être effectuée par une personne ou une entité ayant les compétences, les outils, la compétence, le code de déontologie et l'indépendance nécessaires. Cette analyse doit donner lieu à un rapport.
- Un test d'intrusion sur les systèmes du service doit être réalisé lors de la mise en place et après toute évolution de l'infrastructure ou des applications.

Tessi Documents Services applique, dans la mesure du possible, l'ensemble des règles du niveau « standard » définies dans le *Guide d'hygiène informatique* publié par l'ANSSI.

6.9. Gestion des incidents et supervision

Les activités du système concernant l'accès aux systèmes informatiques, l'utilisation des systèmes informatiques et les demandes de service doivent être surveillées (cf. 6.10.2).
Tessi Documents Services doit réagir de manière coordonnée afin de répondre rapidement aux incidents et de limiter l'impact des violations de la sécurité. La responsabilité d'assurer le suivi des alertes sur les événements de sécurité potentiellement critiques et de veiller à ce que les incidents pertinents soient signalés conformément aux procédures doit être attribuée à des personnels de confiance.
Les procédures de déclaration et d'intervention d'incident doivent minimiser les dommages causés par les incidents de sécurité et les dysfonctionnements.

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

Tessi Documents Services notifie à l'ANSSI, dans un délai maximal de 24 heures après en avoir eu connaissance, toute atteinte à la sécurité ou toute perte d'intégrité ayant une incidence importante sur le service de confiance fourni ou sur les données à caractère personnel qui y sont conservées.
Lorsque le manquement à la sécurité ou à la perte d'intégrité est susceptible de nuire à une personne physique ou morale à qui le service de confiance a été fourni, Tessi Documents Services informe sans délai la personne physique ou morale concernée.

6.10. Gestion des traces

6.10.1. Type d'événements à enregistrer

Les composantes du système mis en œuvre pour la fourniture du service d'envoi recommandé électronique tracent au minimum les événements décrits ci-dessous sous forme électronique. L'enregistrement des traces est automatique et intervient dès le démarrage d'un système et sans interruption jusqu'à l'arrêt de ce système.

Les événements tracés sont à minimum les suivants :

- Evénements des composantes systèmes supportant le Service LRE et à leur administration (connexion / déconnexion des administrateurs système, des exploitants et des administrateurs fonctionnels, démarrage et arrêt des services système…) ;
- Evénements sur les LRE et sur le fonctionnement du service LRE (événements liés aux informations délivrés et reçues tout au long du cycle de vie d'un recommandé électronique et aux identifications des utilisateurs, archivés par la suite dans les enveloppes de preuve de chaque LRE, voir 4.4) ;
- Evènements applicatifs (Création, modification, suppression de comptes utilisateur, connexion et déconnexion des utilisateurs et les tentatives non réussies correspondantes ainsi que des données d'authentification correspondantes (, certificats, etc.), démarrage et arrêt des applications…)
- Evènements touchants le cycle de vie des clés applicatives du service ou le cycle de vie des certificats (création, génération de clés, installation, import, renouvellement, révocation, sauvegarde, restauration destruction).

  Remarque : ces événements peuvent être tracés par les prestataires ou sous-traitants en charge de la gestion de ces clés et services (horodatage et apposition du cachet) ;

Ces données sont analysées et conservés, notamment pour participer à la continuité de service ou être utilisées comme preuve en cas d'enquêtes légales (pour ceux archivés dans les enveloppes de preuve notamment).

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

- Les accès physiques ;
- Les actions de maintenance et de changements de la configuration des systèmes ;
- Les changements apportés au personnel ;
- Les actions de destruction et de réinitialisation des supports contenant des informations confidentielles (Clés, données d’activation, renseignements personnels sur les utilisateurs...).
- Publication et mise à jour des informations liées au service (politique, conditions générales d'utilisation, etc.) (2.4)

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

- Type de l'événement ;
- Nom ou N° d’identifiant de l’exécutant ou référence du système déclenchant l’événement ;
- Date et heure de l’événement ;
- Résultat de l’événement (échec ou réussite).

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

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

En cas de saisie manuelle, l’écriture doit se faire, sauf exception, le même jour ouvré que l’événement. Les événements et données spécifiques à tracer sont documentés par Tessi Documents Services.

6.10.2. Fréquence de traitement des événements enregistrés

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

Les traces enregistrées sont contrôlées régulièrement afin de vérifier la concordance entre des événements dépendants et contribuer ainsi à révéler toute anomalie et permettre la détection d’éventuelles failles de sécurité.

6.10.3. Conservation des événements enregistrés

Les événements enregistrés sont conservés localement sur chaque composante du système informatique du service LRE entre 1 (un) et 6 (six) mois selon leur type. Les événements des composantes du système informatique du service LRE identifiées comme critiques sont conservés pendant un (1) an minimum.

6.10.4.Protection des événements enregistrés

Tessi Documents Services a mis en œuvre des mesures de façon à limiter les risques de contournement, de modification ou de destruction des événements enregistrés. Les événements sont protégés en confidentialité et en disponibilité (contre la perte et la destruction partielle ou totale, volontaire ou non).

Des mécanismes de contrôle d'intégrité sont mis en place et doivent permettre de détecter toute modification, volontaire ou accidentelle, de ces journaux. Les événements enregistrés sont accessibles aux seules personnes autorisées.
Le système de datation des événements doit respecter les exigences du 6.7.7.

6.10.5.Procédure de sauvegarde des traces

Chaque composante du service a mis en place les mesures nécessaires afin d'assurer l'intégrité et la disponibilité de ses traces d'événements.

6.11. Archivage des données

6.11.1.Types de données à archiver

Tessi Documents Services conserve pendant une durée minimale de 7 (sept) ans après la date d'envoi et de réception des données, toutes les informations pertinentes concernant les données délivrées et reçues, notamment afin de pouvoir fournir des preuves en justice. Les données à conserver sont au moins :

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

6.11.2. Période de conservation des archives

La durée de conservation, les modalités de réversibilité et de portabilité sont précisées dans les conditions générales d'utilisation du service (1.4.5) et au 6.11.1.

6.11.3.Protection des archives

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

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

A cet effet, les données contenues dans les enveloppes de preuves sont archivées à valeur probatoire dans un SAE (service d'archivage électronique) pour garantir leur confidentialité, intégrité, pérennité, authenticité, sécurité et traçabilité.
Lo

6.11.4. Exigences d'horodatage des données

Voir 6.7.7

6.11.5. Procédures de récupération et de vérification des archives

Les archives peuvent être accédées uniquement par le personnel du PSRE (Tessi Documents Services) et/ou par le personnel de son OSRE (Logidoc Solutions) le cas échéant.

6.12. Continuité d'activité

6.12.1.Reprise suite à la compromission et sinistre

Chaque entité opérant une composante du service doit mettre en œuvre des procédures et des moyens de remontée et de traitement des incidents (6.9), notamment au travers de la sensibilisation et de la formation de ses personnels et au travers de l'analyse des différentes traces d'événements (6.10.2).
Dans le cas d'un incident majeur (ou suspicion d'un incident), tel que la perte, la compromission ou le vol de données critiques (p. ex., clés privées), l'incident sera remonté par l'entité opérant la composante du service concernée, qui doit en informer immédiatement Tessi Documents Services. Le cas de l'incident majeur doit être impérativement traité dès détection et traité dans la plus grande urgence, voire immédiatement, par tout moyen utile et disponible (presse, site Internet, récépissé…). Tessi Documents Services doit également prévenir directement et sans délai l'ANSSI, conformément au paragraphe 6.9.1.
Si l'un des algorithmes, ou des paramètres associés, utilisés par le service ou ses porteurs devient insuffisant pour son utilisation prévue restante, alors Tessi Documents Services doit :

- informer tous les utilisateurs et tiers impactés
- le cas échéant, révoquer les MIE concernés.

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

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

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

Le cas de compromission d'une clé d'infrastructure ou de contrôle d'une composante doit être traité dans le plan de continuité de la composante en tant que sinistre.
Dans le cas de compromission de la clé du cachet du service, le certificat correspondant doit être immédiatement révoqué.
En outre, Tessi Documents Services doit au minimum informer tous les clients, les autres entités avec lesquelles il a passé des accords et l'ANSSI, de cette compromission.

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

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

6.12.5.Capacités de continuité d'activité suite à risque pandémie

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

6.13. Fin d'activité

Tessi Documents Services a provisionné les moyens financiers nécessaires au transfert ou à la fin d'activité.

6.13.1.Transfert d'activité

En cas de transfert d'activité à un tiers, celui-ci se fera avec un préavis d'au minimum trois mois.
Le transfert d'activité ne pourra se faire sans interruption de service qu'auprès d'un tiers lui-même déjà qualifié.
L'ensemble des archives et des preuves seront transmis au tiers par Tessi Documents Services, ainsi que les obligations afférentes. Le certificat de cachet ne sera pas transmis au tiers, le nouvel exploitant devant disposer de son propre certificat.
En cas de transfert, la politique du service sera mise à jour et l'OID, changé.
Une fois le transfert effectué, Tessi Documents Services procèdera à la révocation de son certificat de cachet et à la destruction des clés privées et secrets utilisés par son service du recommandé électronique.

6.13.2.Fin d'activité définitive

En cas de fin d'activité du service, celui-ci se fera avec un préavis d'au minimum trois mois. Durant cette période, l'envoi ne sera plus possible, seul le refus ou le retrait d'une LRE le seront.
Une fois toutes les preuves relatives aux envois en cours produites (acceptation, refus ou non-réclamation), l'ensemble des preuves seront déposées par Tessi Documents Services chez un tiers archiveur afin de rester disponibles à des fins de justice durant la durée prévue en 6.11.2. L'ensemble des obligations de Tessi Documents Services seront transférées soit au tiers archiveur, soit à un tiers sous contrat, soit à un prestataire qualifié.
Tessi Documents Services informera ses utilisateurs de l'arrêt d'activité et procèdera à la révocation de son certificat de cachet et à la destruction des clés privées et secrets utilisés par le service du recommandé électronique.

6.14. Conformité

Les audits et les évaluations concernent, d'une part, ceux réalisés en vue de la délivrance d'une attestation de qualification au sens du règlement eIDAS et, d'autre part, ceux que Tessi Documents Services doit réaliser, ou faire réaliser, afin de s'assurer que l'ensemble de son infrastructure est bien conforme aux engagements affichés dans la présente politique.

6.14.1.Fréquences et circonstances des évaluations

Avant la première mise en service d'une composante ou suite à toute modification significative au sein d'une composante, Tessi Documents Services procèdera à un contrôle de conformité de cette composante. La fréquence des évaluations au titre du maintien de la qualification est déterminée par les schémas d'évaluation en vigueur.

6.14.2.Identités et qualifications des évaluateurs

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

6.14.3.Relations entre évaluateurs et entités évaluées

L'équipe d'audit 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.

6.14.4.Sujets couverts par les évaluations

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

6.14.5.Actions prises suite aux conclusions des évaluations

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

- ÉCHEC : En cas d'échec, et selon l'importance des non-conformités, l'équipe d'audit émet des recommandations qui peuvent être la cessation (temporaire ou définitive) d'activité, etc. Le choix de la mesure à appliquer est effectué par le PSRE et doit respecter ses politiques de sécurité internes.
- À CONFIRMER : Le PSRE remet à la composante un avis précisant sous quel délai les non-conformités doivent être levées. Puis, un contrôle de confirmation » permettra de vérifier que tous les points critiques ont bien été résolus.
- RÉUSSITE : Le PSRE confirme à la composante contrôlée la conformité aux exigences de la politique.

6.14.6.Notifications individuelles et communications entre les participants

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

- Au plus tard un mois avant le début de l'opération, faire valider ce changement au travers d'une expertise technique, afin d'évaluer les impacts sur le niveau de qualité et de sécurité des fonctions du service et de ses différentes composantes.
- Au plus tard un mois après la fin de l'opération, en informer l'organisme de qualification.
- Par ailleurs, les résultats des audits de conformité doivent être tenus à la disposition de l'organisme de qualification en charge de la qualification du service.

7. AUTRES PROBLEMATIQUES METIERS ET LEGALES

7.1. Responsabilité financière

7.1.1. Couverture par les assurances

La société mère du groupe Tessi a souscrit pour l'ensemble de ses filiales dont Tessi Documents Services, un contrat d'assurance responsabilité civile adapté aux technologies de l'information.
Tessi Documents Services s'assure que les Entités intervenant dans le service de recommandé électronique (1.5) ont également souscrit à un contrat d'assurance adéquat.

7.1.2. Couverture et garantie concernant les entités utilisatrices

La société mère du Groupe Tessi a notamment souscrit pour elle-même et pour l'ensemble de ses filiales dont Tessi Documents Services, un contrat « responsabilité civile après livraison ».
Tessi Documents Services s'assure que les Entités intervenant dans le service de recommandé électronique (1.5) ont également souscrit à un contrat d'assurance adéquat.

7.2. Confidentialité des données professionnelles

7.2.1. Périmètre des informations confidentielles

Les informations considérées comme confidentielles sont au minimum les suivantes :

- Les données d'identité des clients et/ou les données contenues dans les certificats RGS ou SSL associés et utilisées pour vérifier leur identité ;
- Les secrets cryptographiques utilisés par le service (clés secrètes et privées, mots de passe, etc.).

7.2.2. Responsabilités en termes de protection des informations confidentielles

Tessi Documents Services respecte la législation et la réglementation en vigueur sur le territoire français. En particulier, Tessi Documents Services peut devoir mettre à disposition les données dont il dispose à des tiers (organismes de contrôle public) dans le cadre de procédures légales et doit également donner l'accès à ces informations à ses clients.

7.3. Protection des données personnelles

7.3.1. Politique de protection des données personnelles

Toute collecte et tout usage de données à caractère personnel par Tessi Documents Services et l'ensemble de ses composantes sont réalisés dans le strict respect de la législation et de la réglementation en vigueur sur le territoire français, en particulier, la loi Informatique et Libertés et le Règlement Général sur la Protection des Données (RGPD).

Les politiques détaillées de protection et d'utilisation des données personnelles des utilisateurs du service sont rendues disponibles sur les portails expéditeurs et destinataires dédiés.

Toute demande complémentaire d'information ou bien toute demande d'exercice d'un droit (selon la base légale du traitement , l'utilisateur, bénéficie d'un droit d'accès, d'opposition, de rectification, de suppression et de portabilité de ses Données Personnelles ou, le cas échéant, de retrait de son consentement à tout moment, ainsi que d'un droit à la limitation) doit être envoyée à l'attention du Data Protection Officer de Tessi Documents Services sur : DPO TESSI : 45, rue Saint Jean de Dieu, 69007 Lyon.

7.3.2. Informations à caractère personnel

Les informations considérées comme personnelles sont au minimum les suivantes :

- Les données relatives à l'identification, dont notamment les données d'état civil (nom, prénom(s), date de naissance), les coordonnées postales et électroniques des Utilisateurs ;
- Les adresses IP, *hostname* et les *UserAgents* des navigateurs utilisés par les utilisateurs pour accéder au service.

7.3.3. Responsabilité en termes de protection des données personnelles

Voir 7.3.1.

7.3.4. Notification et consentement d'utilisation des données personnelles

Les données personnelles transmises à Tessi Documents Services par les utilisateurs du service ne doivent ni être divulguées, ni transférées à un tiers, sauf dans les cas suivants : consentement préalable du porteur, décision judiciaire ou autre autorisation légale.

7.3.5. Conditions de divulgation de données personnelles aux autorités judiciaires ou administratives

Tessi Documents Services agit dans le respect de la législation et réglementation en vigueur sur le territoire français.

7.4. Obligations des utilisateurs

Les utilisateurs sont des personnes physiques agissant au nom et pour le compte des expéditeurs et destinataires de LRE.
Les expéditeurs garantissent ne pas porter atteinte à leurs obligations contractuelles ou légales et à ne pas introduire dans leur LRE tout virus, vers, bombe logique ou tout contenu pouvant être assimilés à du courrier non désiré.
Le destinataire déclare être le destinataire désigné dans l'avis de mise à disposition qui lui est notifié, et reconnaît que toute usurpation d'identité est un délit passible de sanctions pénales.
L'utilisateur s'engage à fournir des données exactes quant à son identité, celle de son mandant éventuel, et l'adresse courriel servant à la réception notifications et s'engage à mettre ces données à jour régulièrement et directement auprès de Tessi Documents Services, si celles-ci ont changé, ou ont atteint leur fin de validité.
L'utilisateur s'engage à prendre toute mesure utile pour assurer la parfaite confidentialité et le secret de ses données d'identification, ainsi que le contrôle sur son téléphone et l'adresse courriel servant à la réception notifications qu'il a déclaré sur la plate-forme.

L'utilisateur s'engage à informer immédiatement Tessi Documents Services de toute utilisation non autorisée de son compte sur la plateforme et, plus généralement, de toute atteinte à la sécurité dont il aurait eu connaissance.
À défaut, toute utilisation de la plate-forme effectuée avec ses identifiants de connexion sera présumée avoir été effectuée par l'utilisateur concerné, sous sa seule responsabilité.

7.4.1. Utilisation des MIE (Moyens d'Identification Électroniques)

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

- protéger leur MIE de toute perte ou divulgation par des mécanismes adaptés ;
- révoquer sans délai leur MIE en cas de perte, vol, compromission ou de suspicion de compromission des moyens fournis.

Les MIE sont strictement personnels et ne doivent pas être communiqués ou transmis à des tiers.

7.4.2. Utilisation des LRE

Le service de LRE produit des preuves de Dépôt, d'Acceptation, de Refus et de Non-Réclamation (4.4) qui sont opposables en justice. Leur authenticité est garantie par le jeton d'horodatage qualifié associé et le scellement de l'enveloppe de preuve.
Toute personne désirant utiliser ces preuves à des fins de justice peut s'assurer de leur recevabilité en vérifiant la validité (technique) des éléments suivants :

- Vérifier la validité du jeton d'horodatage, conformément aux procédures décrites dans la politique correspondante (1.4.5)
- Vérifier la validité du certificat utilisé pour le cachet électronique, conformément aux procédures décrites dans la politique correspondante (1.4.5)
- Vérifier la validité du cachet électronique (en utilisant par exemple un logiciel de lecture des fichiers PDF sachant interpréter les signatures électroniques, p. ex., A*crobat Reader*)

.

7.5. Droits sur la propriété intellectuelle et industrielle

Tessi Documents Services (PSRE) et Logidoc Solutions (OSRE) détiennent et conservent tous les droits de propriété intellectuelle relatifs à la Solution d'Envoi Recommandé Electronique qualifié selon le périmètre décrit dans la présente politique, à la Plateforme et aux services associés, tant dans leur structure, leur graphisme que dans leur contenu, en dehors du contenu des LRE et/ou CSE.

L'ensemble des données, textes, informations, images, photographies ou tout autre contenu diffusé sur le site Internet, la Solution et la Plateforme fait l'objet d'une protection au titre du droit de la propriété intellectuelle.

Par conséquent, sauf autorisation écrite et préalable de Tessi Documents Services, l'Utilisateur ne peut utiliser ces éléments qu'à des fins exclusivement privées, et toute reproduction, représentation, utilisation ou adaptation, sous quelque forme que ce soit, de tout ou partie des éléments du site Internet, de la Solution et/ou de la Plateforme, quel que soit le procédé ou le support, sans l'accord écrit et préalable de Tessi Documents Service et de Logidoc Solutions est constitutive d'un acte de contrefaçon sanctionné par le Code de la Propriété Intellectuelle et passible de sanctions civiles et pénales.

Toutes marques, logos et autre signe distinctif apparaissant sur le site Internet de Tessi Documents Services, la Solution et/ou et la Plateforme sont la propriété exclusive de Tessi Documents Services et Logidoc

Solutions. Par conséquent, toute reproduction et/ou représentation, et tout usage de ces signes distinctifs sont prohibés sauf autorisation écrite et préalable de Tessi Documents Services et Logidoc Solutions.

7.6. Durée et fin anticipée de validité de la politique

7.6.1. Durée de validité

La présente politique reste en vigueur au moins un an après la réception, le refus ou la non-réclamation du dernier courrier recommandé émis au titre de celle-ci.

7.6.2. Fin anticipée de validité

L'adoption d'actes d'exécution ou délégués du règlement eIDAS peut entraîner, en fonction des évolutions apportées, la nécessité pour Tessi Documents Services de faire évoluer la présente politique.

7.7. Conformité aux législations et réglementations

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 Tessi Documents Services. La loi applicable est la loi française.

Les pratiques de Tessi Documents Services sont non-discriminatoires.

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

7.8. Force majeure

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

8. ANNEXE 1 : SUIVI DES VERSIONS/REVISIONS SUCCESSIVES

ETAT DES VERSIONS ET REVISIONS SUCCESSIVES

N°	DATE	OBSERVATIONS	Rédacteur	Vérificateur	Approbateur
1.0	03/01/2019	Version Initiale OID : 1.3.6.1.4.1.51537.1.1.1.1	R.LAMY	D.MUNOZ V. PONCE	T. CAYE
1.1	23/01/2020	Complément pour traiter les personnes physiques disposant d'un certificat	R. LAMY	V. PONCE	T. CAYE
2.0	01/07/2020	Version mise à jour pour nouveaux schémas d'identification. Suppression de l'utilisation de certificat pour personnes physiques.	R. LAMY	V. PONCE	S. SEILLIER
3.0	06/07/2022	Refonte des informations en vue du renouvellement de qualification du service Changement de versionning OID MAJ charte graphique	E. LAVABRE V. PONCE	D. MUNOZ	S. SEILLIER