PARAGON

# Politique et pratiques du service de lettre recommandée électronique qualifié

## e-velop

OID : 1.3.6.1.4.1.52671.1.1.1.4

Réf : PO-PE-SSI-EVELOP Date : 26/05/2025

Publique

# Gestion des versions du documents

| Version | Date de version | Objet de la modification | Rédacteur | Approbateur |
|---|---|---|---|---|
| 1.0 | 01/06/2019 | Version initiale | MAJOREL | |
| 1.1 | nov-20 | Mise à jour de la procédure d'enrôlement des destinataires | MAJOREL | |
| 1.2 | mai-21 | Relecture, changements mineurs | MAJOREL | |
| 1.2.1 | juin-21 | Changements mineurs | MAJOREL | |
| 1.2.2 | juin-23 | Relecture et changements mineurs | MAJOREL | |
| 1.3 | septembre 2023 | Relecture, mise à jour de la procédure d'enrôlement des utilisateurs selon le type de certificat utilisé | MAJOREL | |
| 2.0 | Mai 2025 | Reprise des services par Paragon | PARAGON | *KLEIBER D. CISO & DPO* |

# Sommaire

# I. Introduction

## 1. Présentation générale

Le présent document décrit la politique du service de lettre recommandée électronique (LRE) qualifié e-velop proposé par DOCUMENT CHANNEL.

DOCUMENT CHANNEL est une filiale de Paragon Editique. Ses activités comprennent notamment la dématérialisation des flux documentaires et des processus de souscription, la personnalisation de documents, la gestion de bases de données, la saisie de documents, coupons et courriers, et le routage.

Le service e-velop est qualifié au sens de l'article 44 du règlement européen eIDAS, faisant de DOCUMENT CHANNEL un Prestataire de Services de Confiance (PSCO) qualifié eIDAS. A ce titre, il est référencé dans la liste de confiance (Trusted List) des prestataires de services de confiance européens.

La présente politique définit les engagements de DOCUMENT CHANNEL dans le cadre de la fourniture du service de lettre recommandée électronique e-velop, ainsi que les obligations des clients, utilisateurs et tierces parties du service.

## 2. Identification du document

La présente politique est identifiée par l'OID (Object Identifier) suivant : 1.3.6.1.4.1.52671.1.1.1.4

## 3. Gestion de la politique

### *a ) Entité gérant la politique*

La politique est gérée par les membres du comité de pilotage nommé par la Direction Générale de DOCUMENT CHANNEL et présidé par le responsable du service.

DOCUMENT CHANNEL

Siège social : 2 Rue de l'Erigny, 41000 Blois

SIREN 504.259.375

### *b ) Procédure d'approbation de la politique*

La politique est approuvée après examen et relecture par le responsable du service, 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 DOCUMENT CHANNEL et ses partenaires.
- ✓ Que toute modification importante dans la fourniture du service de confiance qualifié (y compris celles entrainant des changements dans la liste de confiance) fasse l'objet d'une information de l'ANSSI selon les modalités décrites dans les procédures de qualification.

### *c ) Amendement à la politique*

DOCUMENT CHANNEL s'assure que tout projet de modification de sa politique reste conforme aux exigences réglementaires et normatives applicables.

#### *i. Procédures d'amendement*

La modification de la politique de DOCUMENT CHANNEL est soumise à l'approbation des membres du comité de pilotage.

#### *ii. Mécanisme et période d'information sur les amendements*

DOCUMENT CHANNEL adressera, dans les meilleurs délais, à l'ANSSI et à l'organisme de certification une synthèse de l'ensemble des modifications apportées à la fourniture de ses services de confiance qualifiés à savoir :

- ✓ les changements induits par une modification de la politique de service ou des conditions générales d'utilisation associées
- ✓ les changements de sous-traitants
- ✓ les modifications des conditions d'hébergement
- ✓ les changements de matériels cryptographiques
- ✓ les modifications d'architecture technique
- ✓ les changements de procédures d'enregistrement et d'identification
- ✓ les changements dans la gouvernance du PSCo.

#### *iii. Circonstances entrainant un changement d'OID*

En cas d'évolution majeure de la politique et pratiques du service, DOCUMENT CHANNEL informera l'ANSSI et procédera à un changement d'OID afin que les utilisateurs du service aient la possibilité d'identifier les exigences applicables à leurs envois.

## 4. Durée et fin anticipée de validité de la politique

### *a ) Durée de validité*

La présente politique est valable à compter du 31 mai 2025 et reste en vigueur jusqu'à ce qu'une nouvelle politique du service soit publiée. La date d'entrée en vigueur de cette nouvelle politique laisse, dans la mesure du possible, un délai suffisant aux clients pour prendre connaissance des nouvelles dispositions et adapter si besoin leurs pratiques.

### *b ) Fin anticipée de validité*

L'évolution ou l'adoption d'actes d'exécution ou délégués du règlement eIDAS peuvent entraîner le cas échéant la nécessité pour DOCUMENT CHANNEL de faire évoluer la présente politique.

DOCUMENT CHANNEL se réserve aussi le droit d'apporter des modifications techniques et organisationnelles à sa solution de recommandé électronique qualifié e-velop.

### *c ) Effets de la fin de validité et clauses restant applicables*

Dans tous les cas, DOCUMENT CHANNEL respectera les exigences réglementaires qui lui incombent notamment en matière de conservation des preuves des LRE qualifiées e-velop.

# 5. Documents associés

## *a ) Politique d'horodatage des envois et réceptions de données*

La date et l'heure d'envoi, de réception et de non-réclamation des données sont indiquées par un horodatage électronique qualifié délivré par Universign selon la politique d'horodatage identifiée par :

OID : 1.3.6.1.4.1.15819.5.2.2

La politique peut être obtenue auprès d'Universign à l'adresse indiquée dans la liste de confiance (cf. [TRUSTED_LIST]).

## *b ) Politique de certification du certificat de cachet électronique*

Les certificats de cachet électronique utilisés pour sceller les preuves sont des certificats délivrés par Universign selon la Politique de Certification identifiée par :

OID : 1.3.6.1.4.1.15819.5.1.3.5

La politique peut être obtenue auprès d'Universign à l'adresse indiquée dans la liste de confiance (cf. [TRUSTED_LIST]).

## *c ) Politique de création du cachet sur les preuves*

La politique de création des cachets apposés sur les preuves du service (cf. §III.5) est identifiée par :

OID : 1.3.6.1.4.1.52671.1.1.2.2

Cette politique est disponible sur demande à l'adresse evelop.contact@solution-paragon.fr.

## *d ) Politique de vérification du cachet sur les preuves*

La vérification des cachets apposés sur les preuves du service est réalisée par un service qualifié fourni par Docaposte Arkhineo, selon une politique de vérification identifiée par :

OID : 1.3.6.1.4.1.29371.2.3

La politique peut être obtenue auprès de Docaposte Arkhineo à l'adresse indiquée dans la liste de confiance (cf. [TRUSTED_LIST]).

## *e ) Politique d'archivage électronique*

L'archivage des LRE et des preuves est réalisé dans un SAE (Système d'Archivage Electronique) à valeur probante, certifié NF 461, fourni par Docaposte Arkhineo.

## *f ) Conditions générales d'utilisation*

Les CGU applicables (et leurs versions précédentes) sont disponibles sur le site monespace.evelop.fr ou sur demande à l'adresse evelop.contact@solution-paragon.fr.

## *g ) Documents de référence*

| Référence | Document |
|---|---|
| **[ANSSI_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 https://cyber.gouv.fr/sites/default/files/2022-09/eidas_delivrance-certificats-qualifies_v1.2_anssi.pdf |

| | |
|---|---|
| **[ANSSI_LRE]** | Services d'envoi recommandé électronique qualifiés – Critères d'évaluation de la conformité au règlement eIDAS, Version 1.0 du 3 janvier 2017<br>https://cyber.gouv.fr/sites/default/files/2022-09/eidas_envoi-recommande-electronique-qualifie_v1.0_anssi.pdf |
| **[ANSSI_PSCO]** | Prestataires de services de confiance qualifiés – Critères d'évaluation de la conformité au règlement eIDAS, Version 1.2 du 5 juillet 2017<br>https://cyber.gouv.fr/sites/default/files/2022-09/eidas_psc-qualifies_v1.2_anssi.pdf |
| **[EIDAS]** | Règlement (UE) 2014/910 du Parlement européen et du Conseil du 23 juillet 2014<br>https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32014R0910<br><br>Règlement (UE) 2024/1183 du Parlement européen et du Conseil du 11 avril 2024 modifiant le règlement (UE) n° 910/2014 en ce qui concerne l'établissement du cadre européen relatif à une identité numérique<br>https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=OJ:L_202401183 |
| **[EN_319401]** | Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers<br>https://www.etsi.org/deliver/etsi_en/319400_319499/319401/03.01.01_60/en_319401v030101p.pdf |
| **[EN_319521]** | Registered Electronic Mail (REM) ; Information Security Policy Requirements for REM Management Domains<br>https://www.etsi.org/deliver/etsi_en/319500_319599/319521/01.01.01_60/en_319521v010101p.pdf |
| **[RGPD]** | Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016<br>https://www.cnil.fr/fr/reglement-europeen-protection-donnees |
| **[RGS]** | Référentiel général de sécurité, Version 2.0 du 13 juin 2014<br>https://cyber.gouv.fr/le-referentiel-general-de-securite-version-20-les-documents |
| **[TRUSTED_LIST]** | Liste de confiance des services qualifiés au titre du règlement eIDAS<br>https://eidas.ec.europa.eu/efda/trust-services/browse/eidas/tls |

## 6. Entités intervenant dans le service de recommandé électronique

DOCUMENT CHANNEL s'assure régulièrement du statut des prestataires fournissant un service qualifié utilisé dans sa solution de lettre recommandée électronique qualifié e-velop. En cas de perte de qualification de l'un des prestataires utilisés dans la solution, le Responsable de Service et le Comité de pilotage sont immédiatement informés afin de mettre en place les actions nécessaires au remplacement de ce prestataire.

### *a ) Prestataire du service de recommandé électronique (PSRE)*

Le prestataire du service de recommandé est DOCUMENT CHANNEL.

### *b ) Opérateur du service de recommandé électronique*

L'opérateur du service de recommandé est DOCUMENT CHANNEL.

### *c ) Prestataire d'horodatage électronique*

Les jetons d'horodatage utilisés par le service de lettre recommandée sont émis par Universign selon la politique référencée au §5.a ).

### *d ) Prestataire de création du cachet électronique*

Le certificat utilisé par DOCUMENT CHANNEL pour apposer son cachet sur les preuves est fourni par Universign selon la politique référencée au §5.b ). Les cachets sont générés par Universign sur demande de DOCUMENT CHANNEL.

### *e ) Prestataire de vérification des cachets électroniques*

La vérification de la validité des cachets électroniques et de l'horodatage électronique des preuves est réalisée par Docaposte Arkhineo selon la politique référencée au 5.d ).

### *f ) Prestataire d'archivage électronique*

Les LRE et les preuves sont archivées dans un Système d'Archivage Electronique (SAE) fourni par Docaposte Arkhineo.

### *g ) Hébergement et infogérance de la solution*

L'hébergement et l'infogérance de la solution sont réalisés par Claranet selon des modalités certifiées ISO 27001.

### *h ) Utilisateurs*

Les expéditeurs et les destinataires de LRE sont uniquement des personnes morales. Les expéditeurs sont des clients du service, et peuvent envoyer des LRE à des destinataires clients ou non-clients.

Les utilisateurs du service sont des personnes physiques ou des serveurs agissant au nom et pour le compte des expéditeurs et destinataires de LRE.

## 7. Acronymes

| | |
|---|---|
| ANSSI | Agence nationale de la sécurité des systèmes d'information |
| LRE | Lettre recommandée électronique |
| OID | Object identifier |
| PAS | Plan d'assurance sécurité |
| PSCO | Prestataire de service de confiance |
| PSRE | Prestataire de service de recommandé électronique |
| RGS | Référentiel général de sécurité |
| SAE | Système d'archivage électronique |
| SIEM | Security Information and event management |
| SIRET | Système d'identification du répertoire des établissements |
| UTC | Temps Universel Coordonné |

# II. Identification

L'identification électronique d'une personne physique consiste à recueillir, et à vérifier sur la base d'un document d'identité, a minima son nom et son prénom.

L'identification électronique d'une personne morale consiste à recueillir, et à vérifier par exemple sur la base d'un Kbis, a minima sa raison sociale et son numéro d'immatriculation.

## 1. Identification de l'expéditeur

Le règlement eIDAS (cf. [EIDAS]) impose l'identification de l'expéditeur avec un « degré de confiance élevé ». Pour atteindre ce niveau de sécurité, l'ANSSI impose dans son référentiel (cf. [ANSSI_LRE]) de respecter les exigences de délivrance d'un certificat qualifié eIDAS, ce qui inclut notamment une vérification d'identité du porteur en face-à-face physique ou équivalent. La délivrance d'un certificat qualifié RGS au niveau RGS** ou RGS*** est également conforme.

### *a ) Certificats et Autorités de Certification (AC) pouvant être utilisés sur le service de recommandé qualifié e-velop*

Les certificats acceptés pour l'authentification d'un utilisateur sur le service doivent remplir l'une des deux conditions suivantes :

- ✓ Certificats d'authentification qualifiés au titre du référentiel RGS, au niveau RGS** ou RGS*** ;
- ✓ Certificats d'authentification qualifiés au titre du règlement eIDAS, c'est-à-dire dont le niveau ETSI est :
  - QCP-n ou QCP-n-qscd pour les personnes physiques ;
  - QEVCP-w (auparavant QCP-w), QNCP-w ou QNCP-w-gen pour les serveurs.

Une liste des Autorités de Certification et des offres de certificats, conformes à ces critères et acceptées sur le service, est mise à disposition des utilisateurs du service dans la FAQ accessible sur le site monespace.evelop.fr. Sur demande d'un utilisateur, Document Channel peut être amenée à ajouter de nouvelles Autorités de Certification et/ou offres de certificats si celles-ci remplissent bien les conditions exprimées ci-dessus.

### *b ) Vérification initiale de l'identité de l'expéditeur*

La vérification initiale de l'identité est réalisée par le PSCO sélectionné par l'expéditeur lors de la délivrance du certificat d'authentification de l'utilisateur. Lorsque l'expéditeur utilise un certificat d'authentification d'un serveur, un face-à-face est réalisé par l'officier de vérification d'identité et le lien avec l'expéditeur est vérifié.

### *c ) Identification et authentification de l'expéditeur*

A chaque envoi les informations relatives à l'expéditeur et à son certificat sont vérifiées afin de s'assurer de son identité :

- ✓ Niveau du certificat conforme aux exigences du service (cf. II.1.a ))
- ✓ Dates de validité
- ✓ Non révocation du certificat
- ✓ Autorité de certification émettrice du certificat
- ✓ Numéro de série et OID du certificat enregistré dans le système e-velop

Si tous les contrôles réalisés sont satisfaisants, l'expéditeur est autorisé à envoyer sa LRE e-velop.

## 2. Identification du destinataire

Le règlement eIDAS (cf. [EIDAS]) demande l'identification du destinataire avant la fourniture de la LRE. L'ANSSI, dans son référentiel (cf. [ANSSI_LRE]), recommande lorsque cela est possible d'appliquer les mêmes exigences que pour l'identification de l'expéditeur.

### *a ) Vérification initiale de l'identité du destinataire*

Le service e-velop applique au destinataire les mêmes exigences d'identification que pour l'expéditeur.

Le destinataire doit par conséquent utiliser un certificat d'authentification respectant les critères définis au § II.1.a ). Sa vérification initiale d'identité est réalisée par un PSCO lors de la délivrance du certificat. Si le destinataire utilise un certificat de type QCP-W, un vis-à-vis est réalisé par l'officier de vérification d'identité.

### *b ) Identification et authentification du destinataire*

A chaque action d'acceptation ou de refus auprès du service-e-velop, le certificat du destinataire est vérifié selon la même méthode que celle appliquée à l'expéditeur.

Si tous les contrôles réalisés sont satisfaisants, le destinataire est autorisé à accepter ou refuser sa LRE e-velop.

Le destinataire accède à ses e-velop déjà acceptées en se connectant à son compte avec ses identifiants, il n'est pas nécessaire d'utiliser son certificat pour réaliser l'action de consultation.

# III. Exigences opérationnelles

## 1. Description générale du service de recommandé électronique qualifié e-velop

Le service e-velop qualifié permet l'envoi, le suivi et la réception de recommandé électronique.

L'expéditeur, une personne morale, est enrôlé pour pouvoir utiliser le service : Création du compte expéditeur, vérification et enregistrement du certificat client. Pour envoyer des e-velop, l'expéditeur utilise les web services ou le portail mis à sa disposition.

Il se connecte sur son compte avec ses identifiants préalablement créés et renseigne ensuite les données essentielles pour la délivrance de son e-velop (coordonnées destinataire, durée d'archivage…) et transmet un ensemble de documents PDF constituant la LRE.

Lorsque l'expéditeur valide son envoi, les informations relatives à son certificat sont vérifiées. Si le certificat est inconnu (certificat non enregistré), expiré ou révoqué, l'envoi est refusé. L'expéditeur peut alors se mettre en relation avec le service client de Paragon Editique pour régulariser sa situation.

Si tous les contrôles réalisés par le service sont bien valides, le dépôt est accepté et une preuve de dépôt est générée, scellée et horodatée et mise à disposition de l'expéditeur. La preuve de dépôt, le document envoyé ainsi que les traces sont archivés dans un Service d'Archivage Electronique pendant la durée choisie par l'expéditeur (au moins pendant 7 ans jusqu'à 10 ans maximum).

Le destinataire reçoit une notification email qui l'informe de la réception d'une e-velop, il a 15 jours à compter du lendemain de l'envoi de cette notification pour accepter ou refuser l'e-velop. Passé ce délai et sans action de sa part, la lettre recommandée électronique e-velop est déclarée non réclamée. Il ne peut plus accéder à son contenu et une preuve de non-réclamation est mise à disposition de l'Expéditeur (le procédé de récupération des preuves est identique à celui de la preuve de dépôt).

Le destinataire peut utiliser les web services ou le portail web destinataire pour l'accepter ou la refuser.

Lors d'une première réception, le destinataire est invité à se créer un compte sur le site web monespace.evelop.fr pour pouvoir accéder aux e-velop qu'ils a reçues. Une fois le compte créé et le destinataire identifié avec son identifiant et son mot de passe, il accède à la liste des e-velop en attente d'action de sa part.

A chaque action d'acceptation ou de refus auprès du service-e-velop, les informations relatives au certificat du destinataire sont vérifiées afin de s'assurer de son identité. Si le certificat est inconnu (autorité de certification non enregistrée), non valide (d'un niveau non compatible avec le service) ou révoqué, la

connexion est refusée. Le destinataire peut alors se mettre en relation avec le service client de Paragon Editique pour régulariser sa situation.

S'il accepte, il accède à l'identité de l'expéditeur et au contenu de l'e-velop durant la durée d'archivage paramétrée par l'expéditeur au moment de l'envoi (minimum 7 ans jusqu'à 10 ans maximum). Une preuve d'acceptation est générée et mise à disposition de l'expéditeur.

S'il refuse la réception de l'e-velop, il n'accède ni à l'identité de l'expéditeur ni au contenu. Une preuve de refus est générée et mise à disposition de l'expéditeur.

Le destinataire accède à ses e-velop déjà acceptées en se connectant à son compte avec ses identifiants, il n'est pas nécessaire d'utiliser son certificat pour réaliser l'action de consultation.

## 2. Processus d'envoi

### *a ) Processus et responsabilités pour le dépôt d'une LRE*

L'expéditeur est seul responsable des informations concernant le destinataire de la LRE e-velop.

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

### *b ) Exécution des processus d'identification et de validation du dépôt*

Une LRE ne peut être envoyée que par une personne morale préalablement enregistrée par DOCUMENT CHANNEL, par l'intermédiaire d'un utilisateur satisfaisant aux exigences d'identification exprimées au §II.

### *c ) Traitement du dépôt d'une LRE*

A réception du fichier déposé par le client, celui-ci est archivé pendant au moins 7 ans dans un SAE (Système d'Archivage Electronique). La durée d'archivage peut être supérieure à 7 ans, si le client en fait la demande au moment de l'envoi. La preuve de dépôt est générée puis scellée avec le cachet du service qualifié e-velop, et horodatée.

### *d ) Acceptation ou rejet du dépôt*

Les dépôts sont considérés acceptés lorsque l'expéditeur termine son envoi et lorsque le cachet et l'horodatage qui protègent la preuve de dépôt sont vérifiés et validés.

La preuve de dépôt est alors archivée.

### *e ) Remise de la preuve de dépôt*

La preuve de dépôt est mise à disposition pour l'expéditeur durant toute la durée d'archivage de la LRE, soit 7 ans minimum ou pour une durée supérieure selon le choix fait par l'expéditeur au moment de l'envoi.

## 3. Processus de remise

### *a ) Information du destinataire*

Le destinataire est informé par email de la réception d'une LRE e-velop à l'adresse indiquée par l'expéditeur.

### *b ) Acceptation ou refus de la LRE*

L'acceptation ou le refus de la LRE e-velop est réalisée par un utilisateur du destinataire, via les web services pour un serveur ou via le portail web monespace.evelop.fr pour une personne physique. Cet utilisateur doit satisfaire aux exigences d'identification exprimées au §II.

La preuve d'acceptation ou de refus est générée puis scellée avec le cachet du service qualifié e-velop, horodatée, vérifiée et enfin archivée dans le SAE à valeur probante.

### *c ) Délai d'acceptation de la LRE*

Le destinataire dispose d'un délai de 15 jours, à compter du lendemain de l'envoi de la notification, pour accepter ou refuser la LRE. Passé ce délai, la preuve de non-réclamation est générée puis scellée avec le cachet du service qualifié e-velop, horodatée, vérifiée et archivée dans le SAE à valeur probante.

### *d ) Transmission de la LRE*

Si le destinataire accepte la LRE, il accède au contenu du fichier par web services ou via le portail web monespace.evelop.fr. La durée de mise à disposition de la LRE pour le destinataire est de 7 ans minimum, elle peut être supérieure selon le choix fait par l'expéditeur au moment de l'envoi.

### *e ) Remise de la preuve d'acceptation*

En cas d'acceptation, la preuve d'acceptation est mise à disposition pour l'expéditeur durant toute la durée d'archivage de la LRE, soit 7 ans minimum ou pour une durée supérieure selon le choix fait par l'expéditeur au moment de l'envoi.

### *f ) Remise de la preuve de refus*

En cas de refus, la preuve de refus est mise à disposition pour l'expéditeur durant toute la durée d'archivage de la LRE, soit 7 ans minimum ou pour une durée supérieure selon le choix fait par l'expéditeur au moment de l'envoi.

### *g ) Remise de la preuve de non-réclamation*

En cas de non-réclamation, la preuve de non-réclamation est mise à disposition pour l'expéditeur durant toute la durée d'archivage de la LRE, soit 7 ans minimum ou pour une durée supérieure selon le choix fait par l'expéditeur au moment de l'envoi.

## 4. Modification des données

Les données des LRE e-velop ne font l'objet d'aucune modification dans le cadre de leur acheminement.

## 5. Description des preuves

Toutes les preuves produites par le service sont au format PDF et scellées par un cachet électronique respectant les normes d'évaluation de la conformité au règlement eIDAS pour le recommandé électronique (cf. [ANSSI_LRE]).

Ces cachets sont apposés conformément à la politique mentionnée au §I.5.c ).

La validation des cachets apposés sur les preuves de dépôt, d'acceptation, de refus et de non-réclamation est réalisée par le prestataire identifié au §I.5.d ). Le détail des contrôles effectués est précisé dans le document référencé au §I.5.d ).

### *a ) Preuve de dépôt*

| Informations présentes sur la preuve | Commentaires |
|---|---|
| Référence à la qualification du service de recommandé électronique | Le numéro OID de la politique de service de recommandé ainsi que logo EU Trust Mark (https://ec.europa.eu/digital-single-market/en/eu-trust-mark) |
| Référence unique de la LRE | Format propre à DOCUMENT CHANNEL, sur 20 caractères générés aléatoirement |
| Raison sociale de l'expéditeur et SIRET | |
| **Adresse électronique de l'expéditeur** | |
| **Adresse postale de l'expéditeur** | Si elle est précisée. |
| Raison sociale du destinataire et SIRET | |
| **Adresse électronique du destinataire** | |
| **Adresse postale du destinataire** | Si elle est précisée. |
| Preuve de validation de l'identité de l'expéditeur | Le numéro de série et l'Autorité de Certification du certificat utilisé par l'utilisateur de l'expéditeur pour son identification électronique |
| Empreintes et noms de chacun des fichiers PDF constituant les données du courrier | Les empreintes sont calculées en SHA-256 |
| **Cachet électronique avancé** | Le cachet est apposé sur le fichier PDF de preuve. Celui-ci intégrant les empreintes des documents, il permet de détecter toute modification ultérieure des données. |
| **Jeton d'horodatage qualifié** | Le jeton d'horodatage qualifié apposé sur la preuve PDF, scellée par le cachet, indique la date et l'heure de l'envoi |

### *b ) Preuve d'acceptation*

| Informations présentes sur la preuve | Commentaires |
|---|---|
| Les éléments de la preuve de dépôt | - Numéro OID de la politique de service et logo EU Trust Mark<br>- Référence unique de la LRE<br>- Raison sociale, SIRET, adresse email, adresse postale (si présente) de l'expéditeur<br>- Raison sociale, SIRET, adresse email, adresse postale (si présente) du destinataire<br>- Preuve de validation de l'identité de l'expéditeur<br>- Empreinte et nom des fichiers constituant les données du courrier |
| Preuve de validation de l'identité du destinataire | Le numéro de série et l'Autorité de Certification du certificat utilisé par l'utilisateur du destinataire pour son identification électronique |
| **Cachet électronique avancé** | Le cachet est apposé sur le fichier PDF de preuve. Celui-ci intégrant les empreintes des documents, il permet de détecter toute modification des données. |
| **Jeton d'horodatage qualifié** | Le jeton d'horodatage qualifié apposé sur la preuve PDF, scellée par le cachet, indique la date et l'heure de l'acceptation. |

### c ) Preuve de refus

| Informations présentes sur la preuve | Commentaires |
|---|---|
| **Les éléments de la preuve de dépôt** | - Numéro OID de la politique de service et logo EU Trust Mark<br>- Référence unique de la LRE<br>- Raison sociale, SIRET, adresse email, adresse postale (si présente) de l'expéditeur<br>- Raison sociale, SIRET, adresse email, adresse postale (si présente) du destinataire<br>- Preuve de validation de l'identité de l'expéditeur<br>- Empreinte et nom des fichiers constituant les données du courrier |
| **Preuve de validation de l'identité du destinataire** | Le numéro de série et l'Autorité de certification du certificat utilisé par l'utilisateur du destinataire pour son identification électronique |
| **Cachet électronique avancé** | Le cachet est apposé sur le fichier PDF de preuve. Celui-ci intégrant les empreintes des documents, il permet de détecter toute modification des données. |
| **Jeton d'horodatage qualifié** | Le jeton d'horodatage qualifié apposé sur la preuve PDF, scellée par le cachet indique la date et l'heure de refus. |

### d ) Preuve de non-réclamation

| Informations présentes sur la preuve | Commentaires |
|---|---|
| **Les éléments de la preuve de dépôt** | - Numéro OID de la politique de service et logo EU Trust Mark[3]<br>- Référence unique de la LRE<br>- Raison sociale, SIRET, adresse email, adresse postale (si présente) de l'expéditeur<br>- Raison sociale, SIRET, adresse email, adresse postale (si présente) du destinataire<br>- Preuve de validation de l'identité de l'expéditeur<br>- Empreinte et nom des fichiers constituant les données du courrier |
| **Cachet électronique avancé** | Le cachet est apposé sur le fichier PDF de preuve. Celui-ci intégrant les empreintes des documents, il permet de détecter toute modification des données. |
| **Jeton d'horodatage qualifié** | Le jeton d'horodatage qualifié apposé sur la preuve PDF, scellée par le cachet, indique la date et l'heure de génération de la preuve de non-réclamation. |

### e ) Utilisation des preuves des LRE

Le service de LRE entièrement électronique produit des preuves de Dépôt, d'Acceptation, de Refus et de Non-Réclamation, qui sont opposables en justice. Leur authenticité est garantie par le cachet électronique avancé de DOCUMENT CHANNEL qui y est apposé.

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

- ✓ Vérifier la validité du certificat utilisé pour le cachet électronique, conformément aux procédures décrites dans la politique de certification correspondante
- ✓ Vérifier la validité du cachet électronique avancé (en utilisant par exemple un logiciel de lecture des fichiers PDF sachant interpréter les signatures électroniques, p. ex., Acrobat Reader)

# IV. Gestion des risques

## 1. Analyse de risques

Avant le lancement du service qualifié, DOCUMENT CHANNEL 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 sont prises en tenant compte du résultat de cette analyse.

DOCUMENT CHANNEL fixe, dans le Plan d'Assurance Sécurité LRE e-velop, 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.

## 2. Homologation

La direction de DOCUMENT CHANNEL procède à l'homologation de sécurité du service au sens du RGS. Cette homologation est réalisée préalablement à la fourniture du service de confiance qualifié puis révisée au moins tous les deux ans.

## 3. Plan d'Assurance Sécurité e-velop (PAS)

DOCUMENT CHANNEL dispose d'un Plan d'Assurance Sécurité du service e-velop qualifié eIDAS. Celui-ci est approuvé par la direction.

Ce document et ses différentes versions seront communiqués aux organismes d'évaluation, à l'ANSSI et aux utilisateurs du service, sur demande.

Le PAS est transmis aux employés et aux éventuels sous-traitants.

DOCUMENT CHANNEL conserve la responsabilité globale de la conformité avec les procédures prévues dans son PAS, même lorsque certaines fonctions sont mises en œuvre par des sous-traitants. En particulier, DOCUMENT CHANNEL s'assure de la mise en œuvre effective des mesures prévues dans son PAS.

Le PAS établit un inventaire des actifs du SI. Cet inventaire est revu régulièrement.

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

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

# V. Gestion et exploitation du PSRE

## 1. Organisation interne

### *a ) Fiabilité*

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

### *b ) Rôles de confiance*

Les rôles de confiance identifiés sont les suivants :

- ✓ Gestionnaire fonctionnel et officier de vérification d'identité :

  Enregistre et gère les informations des clients expéditeurs. Il gère également la création des accès au portail de gestion ainsi que le support client en lien avec le référent technique. C'est également la personne autorisée à accéder aux archives du service, c'est-à-dire aux preuves et aux archives chez le tiers archiveur électronique. Le gestionnaire fonctionnel s'assure régulièrement et pour chaque comité de pilotage de la situation légale des fournisseurs qui constituent le service e-velop (normes, certifications, audits …).

- ✓ Responsable du cachet : Le cachet utilisé pour sceller les données, même opéré par un tiers reste sous la responsabilité de DOCUMENT CHANNEL. Il est donc responsable du cachet vis-à-vis de DOCUMENT CHANNEL et également de l'Autorité de Certification (Universign).

- ✓ Responsable sécurité des SI du service e-velop qualifié eIDAS : Garantit la protection des réseaux informatiques et des informations qui transitent au sein de la solution. A ce titre, il définit une politique de sécurité à mettre en œuvre, préservant l'intégrité et la confidentialité des systèmes d'informations et transactions.

- ✓ Administrateur système : Chargé de la configuration, des mises à jour et de la supervision des plateformes. Il s'agit d'une personne physique rattachée au prestataire Claranet. Il garantit la mise en œuvre et le fonctionnement optimal des plateformes IT et le fonctionnement quotidien du service.

- ✓ Contrôleur : Le contrôleur contrôle les opérations réalisées dans les systèmes, afin de s'assurer du respect des conditions de sécurité et de la légitimité des opérations réalisées par les autres acteurs disposant d'un rôle de confiance.

### *c ) 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, les cumuls suivants sont interdits :

- ✓ Responsable sécurité des SI du service e-velop qualifié eIDAS et tout autre rôle
- ✓ Administrateur système et tout autre rôle

## 2. Ressources humaines

### *a ) Qualifications, compétences et habilitations requises*

DOCUMENT CHANNEL s'assure de la compétence et de l'adéquation des personnels employés.

### *b ) Procédures de vérification des antécédents*

DOCUMENT CHANNEL met en œuvre tous les moyens légaux dont il dispose pour s'assurer de l'honnêteté du personnel employé. 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 ses attributions.

Par ailleurs, DOCUMENT CHANNEL vérifie l'absence de conflit d'intérêt avant toute attribution d'un rôle de confiance.

Ces vérifications sont menées préalablement à l'affectation d'un rôle de confiance et revues régulièrement (au minimum tous les 3 ans).

### *c ) 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.

### *d ) 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.

### *e ) Sanctions en cas d'actions non autorisées*

En cas de non-respect des obligations, procédures ou exigences exprimées dans la présente politique ou le Plan d'Assurance Sécurité LRE e-velop, le personnel s'expose à des sanctions disciplinaires telles que prévu dans le règlement intérieur de la société.

### *f ) Exigences vis-à-vis du personnel des prestataires externes*

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

En particulier, le plan d'assurance sécurité LRE e-velop est transmis aux prestataires externes.

### *g ) 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.

### *h ) Télétravail*

Lorsque le télétravail est autorisé, des mesures de sécurité spécifiques de protection des informations sont définies et communiquées au personnel concerné.

## 3. Gestion des biens

### *a ) Généralités*

Un inventaire détaillé des biens est réalisé et tenu à jour. Les biens sont décrits, affectés à un propriétaire et gérés en adéquation avec leur classification.

L'inventaire permet d'identifier les biens sujets aux vulnérabilités identifiées par la veille de sécurité, et de vérifier que les besoins de sécurité (confidentialité, disponibilité) sont bien adressés.

### *b ) Supports*

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

## 4. Contrôle d'accès

DOCUMENT CHANNEL 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. Ces procédures assurent que l'octroi et le retrait des habilitations s'effectuent en accord avec la gestion des ressources humaines.

Tout utilisateur doit être identifié et authentifié avant de pouvoir accéder aux systèmes critiques du service.

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

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

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

La PAS e-velop décrit en détail les règles de contrôle d'accès applicables au SI du service.

Le contrôle d'accès au niveau réseau est décrit dans cette politique.

## 5. Cryptographie

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

## 6. Sécurité physique et environnementale

### *a ) 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.

### *b ) Accès physique*

Pour les systèmes critiques du service, 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.

### c ) 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.

### d ) 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.

### e ) 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.

### f ) 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). DOCUMENT CHANNEL 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 DOCUMENT CHANNEL s'engage à conserver les informations qu'ils contiennent.

### g ) 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.

### h ) Sauvegardes hors site

Des sauvegardes hors site sont effectuées quotidiennement et leur intégrité est régulièrement vérifiée.

## 7. Sécurité opérationnelle

### a ) Mesures de sécurité des systèmes informatiques

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

#### i. Exigences de sécurité technique spécifiques aux systèmes informatiques

Les systèmes informatiques permettent 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 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); éventuellement, gestion des reprises sur erreur.

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

#### *ii. Niveau de qualification des systèmes informatiques*

Voir §

#### *iii. Mesures de sécurité liées au développement des systèmes*

L'implémentation d'un système contribuant au service est documentée et respecte, 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, sont documentées et contrôlées.

DOCUMENT CHANNEL garantit que les objectifs de sécurité sont définis lors des phases de spécification et de conception.

DOCUMENT CHANNEL utilise des systèmes et des produits fiables qui sont protégés contre toute modification.

Conformément aux Règlement Général sur la Protection des Données, DOCUMENT CHANNEL met en œuvre ses traitements dans le respect du principe du Privacy By Design et prend en compte les droits des personnes concernées.

### *b ) Mesures liées à la gestion de la sécurité*

Toute évolution significative d'une composante du système est signalée pour validation. Elle est documentée et apparaît 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.

### *c ) Évaluation des vulnérabilités*

Les procédures d'exploitation du SI incluent la veille sécuritaire de ses composants. Ces procédures assurent que les correctifs de sécurité sont appliqués, au plus tard 2 mois après leur publication. 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 », l'analyse d'impact est effectuée dans les 48 heures suivant la publication de la vulnérabilité.

### *d ) 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.

## 8. Sécurité réseau

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

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

b) L'interconnexion vers des réseaux publics est protégée par des passerelles de sécurité configurées pour n'accepter que les protocoles nécessaires au fonctionnement de la composante au sein du SI du service.

DOCUMENT CHANNEL 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 sont mis en place.

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

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

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

Cela concerne, en particulier, toute connexion entre les HSM et les serveurs.

f) Une analyse de vulnérabilité régulière sur les adresses IP publiques est 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.

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

## 9. Gestion des incidents et supervision

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

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

nécessaires. Des procédures d'escalade et des plans de communication sont établis selon la typologie des incidents. Les incidents les plus critiques sont traités selon un processus formalisé de gestion de crise.

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

### *a ) Procédures de remontée et de traitement des incidents et des compromissions*

DOCUMENT CHANNEL 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, DOCUMENT CHANNEL informe sans délai l'expéditeur afin que celui-ci informe la personne physique ou morale concernée.

### *b ) Supervision des services partenaires*

Le service de la LRE s'appuie sur un ou plusieurs prestataires d'horodatage, de certificats et de cachets électroniques, de SAE (Système d'Archivage Electronique), de notifications email tracées, d'hébergement. Contractuellement, DOCUMENT CHANNEL engage ses différents prestataires à l'informer de toutes modifications relatives à la conformité de leurs services.

## 10. Gestion des traces

### *a ) Type d'événements à enregistrer*

Concernant les systèmes liés aux fonctions qui sont mises en œuvre dans le cadre du service, chaque entité en opérant une composante doit au minimum journaliser les événements décrits ci-dessous, sous forme électronique. La journalisation est automatique, dès le démarrage d'un système et sans interruption jusqu'à l'arrêt de ce système. Sont tracés à la fois, les événements valides ainsi que les événements en échec.

Les journaux archivés sont les suivants :

- ✓ Evénements d'administration
- ✓ Evénements sur les LRE
- ✓ Journaux applicatifs
  - Dont tous les appels aux services SaaS (service d'archivage, service d'horodatage et de cachet serveur, service de mail)
- ✓ Traces du frontal SSL
- ✓ Journaux de l'hébergeur
  - Journaux système : tous les événements d'administration des machines concernées par la plateforme (Connexions admin, patchs, opérations de maintenance, …)
  - Base De Données : toutes les connexions + les opérations de montée de version (Modification de structure, …)
  - Journaux des frontaux SSL
- ✓ Journaux de la base de données
- ✓ Journaux de l'ordonnanceur (lancement des traitements)

### *b ) Fréquence d'archivage*

Les journaux sont archivés au plus tard 10 jours après leur génération.

### c ) Type de conservation

Les données sont archivées :

- ✓ dans un SAE à valeur probante pour garantir leur confidentialité, intégrité, pérennité, authenticité, sécurité et traçabilité pour les événements d'administration et les événements sur les LRE
- ✓ dans un SIEM pour les journaux applicatifs, traces du frontal SSL, journaux de l'hébergeur, journaux de la base de données, journaux de l'ordonnanceur (lancement des traitements)

### d ) Durée de conservation

Les journaux sont archivés pendant une durée de 10 ans.

### e ) Fréquence de traitement des journaux d'événements

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

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

### f ) Période de conservation des journaux d'événements

Les journaux d'événements sont conservés dans le SIEM pendant 10 (dix) ans. Ils sont archivés le plus rapidement possible et au plus tard 10 (dix) jours après leur génération.

### g ) Protection des journaux d'événements

La journalisation est conçue et mise en œuvre de façon à limiter les risques de contournement, de modification ou de destruction des journaux d'événements. Des mécanismes de contrôle d'intégrité permettent de détecter toute modification, volontaire ou accidentelle, de ces journaux.

Les journaux d'événements sont protégés en disponibilité (contre la perte et la destruction partielle ou totale, volontaire ou non).

Le système de datation des événements respecte les exigences du §VI.7.4.

La définition de la sensibilité des journaux d'événements dépend de la nature des informations traitées et du métier. Elle peut entraîner un besoin de protection en confidentialité.

### h ) Procédure de sauvegarde des journaux d'événements

Chaque composante du service met en place les mesures requises afin d'assurer l'intégrité et la disponibilité de ses journaux.

### i ) Notification de l'enregistrement d'un événement au responsable de l'événement

Aucune exigence spécifique.

## 11. Archivage des données

### a ) Types de données archivées et période de conservation

Les données conservées sont les preuves, le contenu envoyé et les traces comme indiqué précédemment.

DOCUMENT CHANNEL conserve le contenu, les preuves et les traces (définies dans le PAS e-velop) pendant une durée minimale de 7 (sept) ans après la date d'envoi et de réception des données afin de pouvoir fournir des preuves en justice.

La durée de conservation et les modalités de réversibilité sont précisées dans les conditions générales d'utilisation du service.

### *b ) Protection des archives*

Les données sont archivées dans un SAE (service d'archivage électronique) à valeur probante pour garantir leur confidentialité, intégrité, pérennité, authenticité, sécurité et traçabilité.

### *c ) Exigences d'horodatage des données*

Les machines produisant les logs sont synchronisées sur l'heure UTC au moins une fois par jour.

### *d ) Procédures de récupération et de vérification des archives*

L'accès aux archives se fait via le portail de gestion evelop.fr et seuls les gestionnaires fonctionnels de niveau N2 et N3 ont accès à ce service.

Les fichiers, preuves et contenu des LRE, sont archivés dans un SAE (Système d'Archivage Electronique) en France.

La vérification des archives est, elle, réalisée par le prestataire d'archivage.

## 12. Continuité d'activité

### *a ) Reprise suite à la compromission et sinistre*

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

Les modalités de déclenchement des cellules de crise sont détaillées dans le document Plan d'Assurance Sécurité LRE e-velop, spécifique au service.

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

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

Ce plan est testé annuellement.

### *c ) Procédures de reprise en cas de compromission de la clé privée d'une composante*

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

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

DOCUMENT CHANNEL informe tous les clients, les autres entités avec lesquelles des accords ont été passés et l'ANSSI, de cette compromission.

### *d ) Capacités de continuité d'activité suite à un sinistre*

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

## 13. Fin d'activité

DOCUMENT CHANNEL a provisionné les moyens financiers nécessaires au transfert ou à la fin d'activité.

### *a ) Transfert d'activité*

En cas de transfert d'activité à un tiers, celui-ci se fera avec un préavis d'au minimum un 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 DOCUMENT CHANNEL, 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, DOCUMENT CHANNEL 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.

### *b ) Fin d'activité définitive*

En cas de fin d'activité du service, celui-ci se fera avec un préavis d'au minimum un 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 DOCUMENT CHANNEL chez un tiers archiveur afin de rester disponibles à des fins de justice durant la durée prévue en § V.11.a ).

L'ensemble des obligations de DOCUMENT CHANNEL seront transférées soit au tiers archiveur, soit à un tiers sous contrat, soit à un prestataire qualifié.

DOCUMENT CHANNEL informera ses utilisateurs de l'arrêt d'activité, la révocation de son certificat de cachet et à la destruction des clés privées et secrets utilisés par le service du recommandé électronique.

## 14. Chaîne d'approvisionnement

### *a ) Gestion des fournisseurs*

La sélection des fournisseurs prend en compte leurs capacités à satisfaire les exigences fonctionnelles et les besoins de sécurité du service, mais aussi les risques et le niveau de dépendance qu'ils induisent.

DOCUMENT CHANNEL met en œuvre des processus et des procédures de gestion des risques liés à l'utilisation des produits et services fournis par les fournisseurs.

DOCUMENT CHANNEL s'assure que l'utilisation de l'interface du composant répond aux exigences spécifiées par le fournisseur du composant de service de confiance et que la sécurité et les fonctionnalités requises par ce composant répondent aux exigences appropriées de la politique et des pratiques applicables.

DOCUMENT CHANNEL établit et tient à jour un registre des fournisseurs, des produits et services approvisionnés et des accords passés. Ce registre est revu régulièrement.

### *b ) Procédures et processus de la chaîne d'approvisionnement*

DOCUMENT CHANNEL impose à ses fournisseurs de propager ses exigences de sécurité à leurs propres chaines de sous-traitance. Les fournisseurs doivent décrire leurs produits ou services, et documenter les pratiques et configurations de sécurité pertinentes pour leur utilisation, y compris lorsque ces informations proviennent de leurs propres chaines de sous-traitance.

DOCUMENT CHANNEL met en œuvre des processus de contrôle d'authenticité, de bon fonctionnement et de sécurité, des produits ou services livrés, et ce sur toute la durée de leur utilisation. Les changements pouvant survenir sur les produits ou services des fournisseurs, ou chez ces fournisseurs eux-mêmes, font l'objet d'une obligation de déclaration et d'une analyse d'impact par DOCUMENT CHANNEL.

Les services cloud, du fait des risques spécifiques portant sur la sécurité de l'information, font l'objet de politiques de gestion des risques adaptées et de dispositions contractuelles établissant clairement les responsabilités et obligations des parties.

### *c ) Contractualisation*

DOCUMENT CHANNEL conserve la responsabilité globale de la conformité à la politique de la chaîne d'approvisionnement, à sa politique de sécurité de l'information et aux exigences définies dans la politique des services de confiance.

DOCUMENT CHANNEL formalise des contrats avec ses fournisseurs, comprenant en particulier :

- ✓ Les politiques et exigences de sécurité ;
- ✓ Les responsabilités respectives des parties ;
- ✓ Les contrôles a mettre en œuvre par chacun des parties ;
- ✓ Les obligations des deux parties en matière de respect des exigences de sécurité de l'information ;
- ✓ Les mesures planifiées cas de cessation d'utilisation de ses produits et services ;
- ✓ Des « accords de niveau de service » ;
- ✓ Des mécanismes d'audit ou de contrôle de conformité aux exigences de sécurité (production d'un certificat de conformité par un organisme tiers agréé).

## 15. 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 DOCUMENT CHANNEL réalise, ou fait réaliser, afin de s'assurer que l'ensemble de son infrastructure est bien conforme aux engagements affichés dans la présente politique.

### *a ) 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, DOCUMENT CHANNEL 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.

### *b ) Identités et qualifications des évaluateurs*

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

### *c ) 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.

### *d ) 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,

### *e ) 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 sont 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.

### *f ) 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 sont tenus à la disposition de l'organisme de qualification en charge de la qualification du service.

# VI. Autres obligations légales

## 1. Publication des informations

La publication des informations à destination des utilisateurs du service ou des tiers ayant à déterminer la validité des preuves, est réalisée sur le site web www.evelop.fr, en accès libre, 24/24/7, dont la mise à jour et la maintenance sont sous la responsabilité du comité de pilotage du service e-velop.

Seules les personnes habilitées par le comité de pilotage ont accès en écriture et modification de ces informations. Cet accès en lecture et modification est protégé par un contrôle d'accès strict basé sur un mot de passe.

Les informations publiées consistent en :

- ✓ Le présent document, décrivant la politique et les pratiques du service de recommandé électronique e-velop ;
- ✓ Les conditions générales d'utilisation du service.

Ces informations sont publiées régulièrement, en cohérence avec l'évolution de l'organisation, des moyens et des procédures mis en œuvre dans le service e-velop.

## 2. Responsabilité financière

Sauf cas de faute lourde, la responsabilité de Document Channel ne peut être engagée qu'à concurrence du montant total hors taxes de la prestation en cause et plafonnée, sur la durée du Contrat et en tout état de cause à la somme la moins importante des montants suivants :

- ✓ de 15 000 € (quinze mille euros) ;
- ✓ de 3 mois moyens de chiffre d'affaires (sur la base de la facturation des douze derniers mois).

En tout état de cause, et dans cette limite, Document Channel ne sera tenue qu'à la réparation des dommages directs

## 3. Confidentialité et protection des données

### *a ) Confidentialité des données*

#### *i. Responsabilités en termes de protection des informations confidentielles*

DOCUMENT CHANNEL s'engage à respecter la confidentialité des données traitées. Toutefois, DOCUMENT CHANNEL peut avoir à mettre à disposition les données dont elle dispose à des tiers dans le cadre de procédures légales. Dès lors, certaines données à caractère personnel pourront également être accessibles à des organismes publics, auxiliaires de justice, officiers ministériels, afin de se conformer à toute loi ou réglementation en vigueur.

Le Plan d'Assurance Sécurité (PAS) de service de recommandé électronique qualifié e-velop reprend les exigences de confidentialité des données recueillies.

### *b ) Protection des données personnelles*

#### *i. Politique de protection des données personnelles*

L'usage de données à caractère personnel par DOCUMENT CHANNEL 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, le Règlement Général sur la Protection des Données (RGPD).

#### *ii. Informations à caractère personnel*

Parmi les données collectées, les informations considérées comme personnelles sont les suivantes :

- ✓ Nom prénom et adresse e-mail des utilisateurs.
- ✓ Les adresses IP, hostname et les User Agents des navigateurs utilisés par les utilisateurs pour accéder au service.

Le contenu des LRE peut éventuellement, en cas de litige, être transmis, sur demande aux autorités, dans le cadre de nos obligations légales.

Les données sont conservées, dans l'Union européenne, pour une durée définie à l'article V.11.a ).

#### *iii. Responsabilité en termes de protection des données personnelles*

L'Utilisateur professionnel garantit qu'il dispose de tous les pouvoirs afin d'agir au nom et pour le compte de la personne morale qu'il représente. L'Utilisateur est le seul responsable des conséquences d'informations personnelles erronées.

L'Utilisateur s'engage à notifier immédiatement toute modification affectant ses informations.

#### *iv. Notification et consentement d'utilisation des données personnelles*

L'Utilisateur communique des données à caractère personnel le concernant lors de son inscription aux services, via le formulaire mis à disposition à cet effet, et ce, afin d'utiliser son compte et bénéficier des Services. Les données à caractère personnel collectées sont utilisées notamment à des fins d'administration et de gestion technique du Compte et des Services et d'exécution des Services,

Les données à caractère personnel de L'utilisateur sont destinées au personnel de DOCUMENT CHANNEL et/ou de ses sous-traitants assurant la fourniture des Services.

Conformément aux dispositions légales et réglementaires précitées, vous disposez d'un droit d'interrogation et d'accès à vos données.

Vous bénéficiez également d'un droit de rectification, d'effacement et de limitation du traitement de vos données dans une certaine mesure, ainsi que du droit à la portabilité de vos données.

Vous disposez en outre d'un droit d'opposition à ce que les données à caractère personnel vous concernant fassent l'objet d'un traitement, et d'un droit d'opposition à ce que vos données soient utilisées à des fins de prospection notamment commerciale.

Vous disposez également du droit de définir des directives générales et/ou particulières relatives au sort de vos données à caractère personnel et à la manière dont vous souhaitez que vos droits soient exercés après votre décès. A cet égard, en cas de décès qui serait porté à notre connaissance, vos données seront supprimées, sauf nécessité de conservation pendant une durée déterminée pour des motifs tenant à nos obligations légales et réglementaires et/ou aux délais légaux de prescription, et après le cas échéant avoir été communiquées à un tiers éventuellement désigné par vos soins.

Toutes demandes tendant à l'exercice de ces droits, ainsi que toutes demandes d'information concernant la protection des données à caractère personnel, doivent être effectués par mail auprès de Paragon Editique à l'adresse suivante : dpo@paragon-cc.fr

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

#### *v. Conditions de divulgation d'informations personnelles aux autorités judiciaires ou administratives*

Si ces informations devaient s'avérer fausses, incomplètes ou obsolètes, DOCUMENT CHANNEL se réserve le droit de refuser l'Inscription et/ou l'accès au Compte

## 4. Obligations des utilisateurs

Les utilisateurs sont des personnes physiques agissant au nom et pour le compte des expéditeurs et destinataires de LRE qualifiée.

Les expéditeurs garantissent ne pas porter atteinte à leurs obligations contractuelles ou légales et à ne pas introduire dans leur LRE qualifiée 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 DOCUMENT CHANNEL, si celles-ci ont changées, 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 l'adresse courriel servant à la réception des notifications qu'il a déclarées lors de la procédure d'enrôlement.

L'utilisateur s'engage à informer immédiatement DOCUMENT CHANNEL de toute utilisation non autorisée de son compte sur la plate-forme 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 moyens de connexion sera présumée avoir été effectuée par l'utilisateur concerné, sous sa seule responsabilité.

## 5. Conformité aux législations et réglementations

A défaut d'accord amiable, tout litige éventuel entre les Parties sera de la compétence exclusive du Tribunal de Commerce de Paris, qu'il s'agisse d'action en référé, de demandes incidentes, de pluralité de défendeurs, d'appel en garantie et quels que soient le mode et les modalités de paiement.

La loi applicable est la loi Française.

La conception et la mise en œuvre des services, logiciels et procédures de DOCUMENT CHANNEL 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 localisation géographique, ou leurs aptitudes physiques ou mentales » (https://www.w3.org/Translations/WCAG20-fr/).

## 6. Force majeure

Aucune Partie n'encourra de responsabilité pour un défaut d'exécution de ses obligations contractuelles si ce défaut est dû à un élément extérieur et indépendant de la volonté des Parties (ci-après « Cas de Force Majeure ») et notamment : grèves, activités terroristes, émeutes, insurrections, guerres, actions gouvernementales, catastrophes naturelles, défaut imputable à un prestataire tiers de télécommunication.

La Partie empêchée devra informer dans les meilleurs délais l'autre Partie en indiquant la nature du Cas de Force Majeure. Si le Cas de Force Majeure perdure plus de trois mois, chaque Partie pourra résilier le Contrat.

Dès cessation du Cas de Force Majeure, la Partie empêchée doit informer immédiatement l'autre Partie et reprendre l'exécution des obligations affectées. Si, à la suite d'un Cas de Force Majeure la Partie affectée est empêchée de remplir seulement une Partie de ses obligations contractuelles, elle reste responsable de l'exécution des obligations qui ne sont pas affectées par le Cas de Force Majeure ainsi que de ses obligations de paiement.