Politique et pratiques du service de confiance

Recommandé électronique qualifié AR24

1.3.6.1.4.1.50034.1.1.1

Historique

Version	Date	Rédigé par	Mise à jour
1.0.0	07/08/2017	AR24	Version initiale
1.0.1	10/08/2018	AR24	Corrections mineures

Table des matières

1 Introduction

1.1 Présentation générale

AR24 est une société de services informatiques commercialisant principalement un service de Lettres Recommandées Électroniques (LRE). Ce service a pour vocation d'être qualifié au sens de l'article 44 du règlement européen eIDAS, faisant d'AR24 un Prestataire de Services de Confiance qualifié eIDAS.

L'organisation adoptée pour cela est présentée dans la section 1.4.

La présente Politique définit les engagements d'AR24 dans le cadre de la fourniture de services de lettres recommandées électroniques qualifiées au sens de l'article 44 du règlement européen eIDAS et dans l'objectif d'être référencé dans la liste de confiance (*Trusted List*) des prestataires de service de confiance européens.

1.2 Identification du document

La présente politique est identifiée par l'OID suivant : 1.3.6.1.4.1.50034.1.1.1

1.3 Date d'entrée en vigueur

La présente politique entre en vigueur le : 21 novembre 2017.

1.4 Gestion de la politique

1.4.1 Entité gérant la politique

La politique est gérée par les membres du comité de pilotage d'AR24.

1.4.2 Point de contact

AR24 SAS

85, Boulevard de Courcelles

75008 Paris

1.4.3 Procédure d'approbation de la politique

La politique est approuvée après examen et relecture par membres du comité de pilotage, 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 AR24 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

AR24 contrôle que tout projet de modification de sa politique reste conforme aux exigences réglementaires et normatives applicables.

1.4.4.1 Procédures d'amendement

Hormis les corrections induites par les audits (voir 6.14, p. 32) ou des corrections mineures (erreurs, oublis, précisions supplémentaires…), les amendements pressentis à la présente politique portent sur :

- L'extension du service de recommandé électronique qualifié à d'autres catégories d'utilisateurs et d'autres modalités d'identification (3, p. 10)
- L'acceptation ou la mise en œuvre de nouveaux moyens d'identification électronique (4.5)
- Des changements d'ordre technique (mise en œuvre, partenaires/fournisseurs, etc.)

Avant tout changement effectif du service (passage en production), AR24 réalise une analyse d'impact afin de déterminer si les évolutions ont une incidence sur la conformité de l'offre qualifiée, et si celle-ci est majeure (impliquant un changement d'OID). L'analyse d'impact peut, à cette occasion, être soumise à l'ANSSI et à l'organisme de certification pour avis ou commentaire.

Le cas échéant, la politique est mise à jour, approuvée (1.4.3) et publiée avant toute mise en œuvre. Les CGU (1.5.4) sont amendées concomitamment si besoin.

1.4.4.2 Mécanisme et période d'information sur les amendements

AR24 adressera annuellement 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.

En cas de changement de la présente politique ou des CGU (1.5.4), les utilisateurs en sont avertis par un message sur leur espace personnel.

1.4.4.3 Circonstances selon lesquelles l'OID doit être changé

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

1.5 Documents associés

1.5.1 Politique d'horodatage

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

Politique d'horodatage en vigueur : *Universign Timestamping Service,*
OID : 1.3.6.1.4.1.15819.5.2.2

1.5.2 Politique de certification du cachet électronique

Les certificats de cachet électronique utilisés par AR24 pour sceller les données sont des certificats *Certigna Entity* (OID : 1.2.250.1.177.2.6.1.4.1).

1.5.3 Politique de scellement électronique

La politique de scellement électronique applicable aux cachets apposés sur les données du service (4.4, p. 14) a pour OID : 1.3.6.1.4.1.50034.1.2.1.0. Cette politique est disponible sur le site d'AR24.

1.5.4 Conditions générales d'utilisation

Les CGU applicables (et leurs versions précédentes) sont disponibles sur le site d'AR24.

1.5.5 Documents normatifs

[ANSSI_LRE]	*Services d'envoi recommandé électronique qualifiés – Critères d'évaluation de la conformité au règlement eIDAS,* Version 1.0 du 3 janvier 2017 https://www.ssi.gouv.fr/uploads/2016/06/eidas_envoi-recommande-electronique-qualifie_v1.0_anssi.pdf
[ANSSI_PSCO]	*Prestataires de services de confiance qualifiés – Critères d'évaluation de la conformité au règlement eIDAS,* Version 1.1 du 3 janvier 2017 https://www.ssi.gouv.fr/uploads/2016/06/eidas_psc-qualifies_v1.1_anssi.pdf
[EN_319401]	*ETSI EN 319 401 V2.1.1 (2016-02) Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.*
[TS_102640-3]	*ETSI TS 102 640-3 V2.1.2, Registered Electronic Mail (REM) ; Information Security Policy Requirements for REM Management Domains*
[GDPR]	*Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016* https://www.cnil.fr/fr/reglement-europeen-protection-donnees
[RGS]	*Référentiel général de sécurité,* Version 1.0 du 6 mai 2010

1.6 Entités intervenant dans le service de recommandé électronique

Concernant les prestataires devant fournir un service qualifié, AR24 surveille régulièrement (procédure automatique) le statut du service correspondant à travers la liste de confiance nationale.

1.6.1 Prestataire du service de recommandé électronique (PSRE)

Le PSRE est AR24.

1.6.2 Opérateur du service de recommandé électronique (OSRE)

L'opérateur du service de recommandé est AR24, assisté par la société Euskill pour la fourniture du S.I.

1.6.3 Prestataire d'horodatage électronique (PSHE)

Les jetons d'horodatage utilisés par le service de recommandé sont émis par Universign (OID: 1.3.6.1.4.1.15819.5.2.2).

1.6.4 Fournisseur de certificat de cachet électronique (PSCE)

Le certificat utilisé par AR24 (cf. 1.5.3) pour apposer ses cachets est fourni par Dhimyotis (cf. 1.5.2). Ce fournisseur est indépendant d'AR24.

1.6.5 Utilisateurs

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

1.6.6 Expéditeur

Dans le cadre de la présente politique, les expéditeurs de recommandés électroniques appartiennent à l'une des catégories de population suivantes :

- notaires ou des clercs de notaires possédant une clé REAL (et donc un certificat émis par l'AC REALAUTH (OID 1.2.250.1.78.2.1.3.2.1.1) ou REAL (OID:1.2.250.1.78.1.1.3.1.3.1.1.22) http://www.preuve-electronique.org/), ainsi que toute personne dont l'identité a été vérifiée par l'un d'eux.
  Seuls les expéditeurs (dits « expéditeurs REAL ») possédant une clé REAL sont habilités à procéder à l'identification des destinataires en face-à-face (3.2.1).
- toute personne possédant un certificat électronique de signature ou d'authentification de niveau [RGS] (★★) ou (★★★)[1].

1.6.7 Destinataire

Les destinataires sont :

- Soit des personnes morales ou physiques en relation avec un office notarial ;
- Soit des personnes possédant un certificat électronique de signature ou d'authentification de niveau [RGS] (★★) ou (★★★).

[1] Deux ou trois étoiles.

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

2.1 Entités chargées de la mise à disposition des informations

La mise à disposition des informations devant être publiées à destination des utilisateurs du service (expéditeurs et destinataires) et des tiers ayant à déterminer la validité des preuves produites est réalisée par l'équipe en charge du site web https://www.ar24.fr.

2.2 Informations devant être publiées

AR24 s'engage à publier au minimum les informations suivantes à destination des utilisateurs du service et des tiers ayant à déterminer la validité des preuves produites par celui-ci :

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

2.3 Délais et fréquences de publication

Les informations liées au service (nouvelle version des présentes, etc.) sont 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 AR24. En particulier, toute nouvelle version est communiquée aux clients et, le cas échéant, faire l'objet d'un nouvel accord.

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

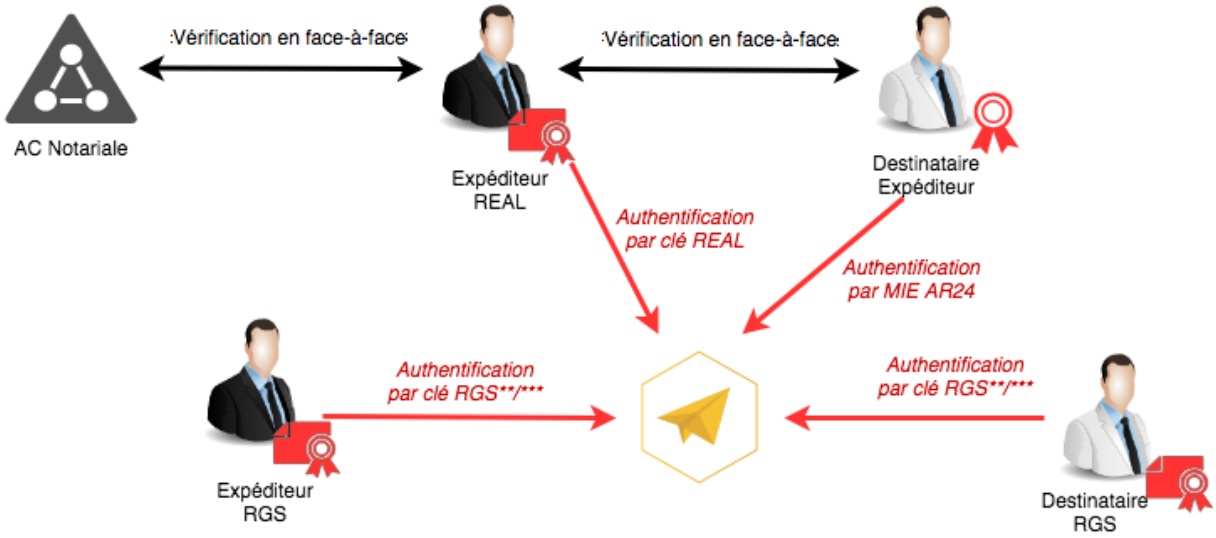
Il est à noter qu'une perte d'intégrité d'une information mise à disposition (présence de l'information et intégrité de son contenu) est considérée comme une indisponibilité de cette information.

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 AR24, 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



3.1 Identification de l'expéditeur

Le service d'envoi recommandé électronique qualifié garantit l'identification de l'expéditeur avec un degré de confiance élevé par l'un des moyens suivants :

- par la présence en personne de l'expéditeur (ou du représentant autorisé de la personne morale) ; ou
- à distance, à l'aide d'un moyen d'identification électronique pour lequel la personne physique ou un représentant autorisé de la personne morale s'est présenté en personne et qui satisfait aux exigences des niveaux de garantie substantiel ou élevé ; ou
- au moyen d'un certificat de signature électronique qualifié pour une personne physique ou d'un certificat de cachet électronique qualifié pour une personne morale, délivré conformément à l'un des deux cas ci-dessus.

3.1.1 Validation initiale de l'identité

3.1.1.1 Expéditeur REAL

L'identité de l'expéditeur REAL est vérifiée en face-à-face dans le cadre de la délivrance de sa clé REAL (1.6.6). Du point de vue d'AR24, l'expéditeur possède donc déjà un moyen d'authentification forte garantissant son identité avec un degré de confiance élevé.

3.1.1.2 Expéditeur (ex-destinataire)

Il s'agit d'un expéditeur dont l'identité est vérifiée en face-à-face par un expéditeur REAL lors d'un envoi précédent, envoi dont il était destinataire.

3.1.1.3 Expéditeur RGS

Il s'agit d'un expéditeur dont l'identité est vérifiée en face-à-face dans le cadre de la délivrance d'un certificat [RGS] de niveau [RGS] (**) ou (***).

3.1.2 Informations non vérifiées

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

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

Avant toute opération relative à l'envoi d'un recommandé électronique, l'expéditeur s'authentifie en ligne avec une clé REAL (1.6.6), un certificat RGS ou un MIE fourni par AR24 (3.2.4) . Suite à cette authentification, il peut bien sûr réaliser plusieurs opérations dans le cadre de sa session.

3.2 Identification du destinataire

Le service d'envoi recommandé électronique qualifié garantit l'identification du destinataire avant la fourniture des données.

3.2.1 Validation initiale de l'identité

L'identité du destinataire est vérifiée en face-à-face par un expéditeur REAL (cf. 1.6.6). Pour cela, l'expéditeur s'authentifie fortement (3.1.3) dans son espace personnel sur le site *ar24.fr* et saisit les informations suivantes :

Personne physique

- Nom et prénoms d'état civil, tels qu'apparaissant sur la pièce d'identité (en cours de validité) présentée par le destinataire
- Date et lieu de naissance, tels qu'apparaissant sur la pièce d'identité (en cours de validité) présentée par le destinataire
- statut du destinataire (particulier ou professionnel[2])

Personne morale

- Adresse courriel de contact (p.ex. *…@societe.fr*)
- Copie d'un K-bis de moins d'un an
- Copie de pièce d'identité d'un responsable légal
- Optionnellement : mandat signé + pièce d'identité du mandataire

- numéro de téléphone du destinataire (facultatif)
- Adresse courriel du destinataire

Le site vérifie alors qu'aucun compte n'existe déjà pour cette adresse courriel.

- Si aucun compte n'existe pour cette adresse courriel, le compte est créé (sans mot de passe) et ne sera activable qu'à l'aide des codes de vérification automatiquement produits (3.2.4).
- Si un compte existe déjà pour cette adresse courriel, le site signale simplement qu'une identité a déjà été validée pour cette adresse courriel. Il n'est alors pas nécessaire de produire des codes de vérification (3.2.4), mais cela reste possible.

Suite à ces vérifications, le cas échéant, de nouveaux codes de vérification (3.2.4) sont affichés par le site, avec possibilité de les imprimer.

3.2.2 Informations non vérifiées

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

[2] Le statut du destinataire sert à déterminer la nécessité éventuelle de recueillir le consentement du destinataire à recevoir des LRE.

3.2.3 Validation par certificat RGS

Pour les porteurs d'un certificat [RGS] de niveau [RGS] (★★) ou (★★★), la validation de l'identité est réalisée dans le cadre de la délivrance du certificat.

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

Le destinataire doit disposer de « codes de vérification » pour s'authentifier fortement sur le site. Cette authentification est nécessaire à la création initiale du compte (si celle-ci a eu lieu suite à l'envoi d'un recommandé) et pour retirer un pli recommandé.

Ces codes sont des mots de passe à usage unique (HOTP), séquentiellement produits par le site *ar24.fr* : lors de la vérification d'identité initiale, une suite de 20 (vingt) HOTP sont produits. L'utilisateur peut s'en servir pour :

- S'authentifier fortement pour retirer ou refuser un recommandé
- Enrôler un autre moyen d'identification électronique ; dans le cadre de la présente politique, les seuls MIE alternatifs enrôlables sont des TOTP (voir § 4.5).
- Générer une nouvelle séquence (HOTP)

4 Exigences opérationnelles

4.1 Processus d'envoi

4.1.1 Processus et responsabilités pour le dépôt d'une LRE

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

- D'un compte (identifiant/mot de passe) sur le site *ar24.fr*
- D'un MIE reconnu (3.1.3)

4.1.2 Traitement du dépôt d'une LRE

Pour déposer une LRE, l'expéditeur doit s'authentifier fortement sur le *ar24.fr* et en sélectionner le ou les destinataires. S'il n'y a pas eu de vérification d'identité pour un des destinataires, l'expéditeur doit alors l'effectuer, tel que décrit en 3.2.1.

Une fois tous les destinataires identifiés, l'expéditeur peut rédiger la LRE et y ajouter des pièces jointes.

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

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

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

Une fois le dépôt terminé, la LRE (c'est-à-dire le message et ses pièces jointes) sont scellées par AR24 et horodatées.

4.1.4 Acceptation ou rejet du dépôt

Les dépôts sont considérés acceptés lorsque l'expéditeur termine son envoi et le valide.

4.1.5 Remise de la preuve de dépôt

Une preuve de dépôt sur laquelle est apposée le jeton d'horodatage est produite et mise à disposition de l'utilisateur. Si ce dernier a autorisé la réception de preuve de dépôt par courriel dans son profil AR24, il recevra aussi la preuve par ce biais.

Dans tous les cas, il peut visualiser la preuve dans la rubrique « Mes envois » de son espace personnel. Si une erreur survenait lors du processus d'enregistrement du courrier, l'utilisateur serait notifié immédiatement de l'échec de son courrier.

4.2 Processus de remise

4.2.1 Information du destinataire

Le destinataire est informé par courriel à l'adresse indiquée par l'expéditeur du dépôt d'une LRE.

La notification apparaît aussi dans l'espace personnel du destinataire, sur le site *ar24.fr*.

AR24 vérifie que l'envoi de la notification (courriel) s'est bien déroulé, faute de quoi un message d'erreur est retourné à l'expéditeur, lui indiquant que l'envoi de son courrier a échoué. Si ce processus est effectué correctement, une preuve de « première présentation » est mise à disposition de l'expéditeur.

Si AR24 est notifié par le serveur du domaine de l'adresse courriel de l'expéditeur d'une impossibilité de délivrer le courrier (utilisateur inexistant, boite pleine, redirection non conforme à la politique de SPF…), AR24 avertit l'expéditeur de la non délivrance de la LRE

dans un délai maximum de 5 minutes après réception de la notification du serveur du domaine du destinataire.

4.2.2 Exécution des processus d'identification du destinataire

Le courriel de notification contient un lien direct (URL unique) lui permettant d'accepter et de consulter la LRE, sur le site *ar24.fr*, ainsi qu'un lien direct lui permettant de la refuser.

Le destinataire peut aussi effectuer ces deux actions depuis son espace personnel.

4.2.3 Acceptation ou rejet de la LRE

L'acceptation et le rejet se font en accédant au lien direct correspondant dans le message de notification (cf. ci-dessus) ou par le biais de l'interface Web de son espace personnel. Si le destinataire ne s'est pas fortement identifié par l'un des moyens reconnus (3.2.3, 3.2.4), l'authentification a lieu à ce moment.

L'activation du compte du destinataire peut aussi être déclenchée par la première acceptation (ou rejet), si celui-ci ne disposait pas de compte sur le site *ar24.fr*.

4.2.4 Délai d'acceptation de la LRE

Le destinataire dispose d'un délai de 15 jours, à compter du lendemain de la première notification, pour accepter ou refuser la LRE.

4.2.5 Transmission de la LRE

Si le destinataire accepte la LRE, son contenu est présenté dans le navigateur, et une copie est transmise par courriel à son adresse.

4.2.6 Remise de la preuve de réception

En cas d'acceptation, une preuve de réception est générée et mise à disposition de l'expéditeur. Si ce dernier a activé l'option de notification par courriel des preuves de réception dans son profil, il recevra instantanément cette preuve sur sa boite courriel.

4.2.7 Remise de la preuve de refus

En cas de refus, une preuve de refus est générée et mise à disposition de l'expéditeur.

Si ce dernier a activé l'option de notification par courriel des preuves de refus dans son profil, il recevra instantanément cette preuve sur sa boite courriel.

4.2.8 Remise de la preuve de non-réclamation

Si le destinataire n'entreprend aucune action lors du délai d'acceptation (4.2.4) et ce, malgré les deux relances hebdomadaires faites par AR24, la LRE est considérée comme non réclamée. Une preuve de non réclamation est générée et mise à disposition de l'expéditeur.

Si ce dernier a activé l'option de notification par courriel des preuves de non réclamation dans son profil, il recevra également cette preuve sur sa boite courriel.

4.3 Modification des données

Les données des LRE (message et pièces jointes) ne font l'objet d'aucune modification dans le cadre de leur acheminement.

4.4 Description des preuves

Toutes les preuves produites par le service sont au format PDF et sont scellées par un cachet électronique respectant le standard *PAdES Baseline Profile*, ETSI TS 103172, v.2.2.2, (niveau B) conformément à *Décision d'exécution (UE) 2015/1506 de la Commission du 8*

septembre 2015 établissant les spécifications relatives aux formats des signatures électroniques avancées et des cachets électroniques avancés du règlement (UE) nº 910/2014.

Ces cachets sont apposés conformément à la politique mentionnée en 1.5.3.

4.4.1 Preuve de dépôt

La preuve de dépôt est un fichier au format PDF reprenant les éléments suivants.

Donnée	Précisions
Nom et prénom ou raison sociale de l'expéditeur	-
Adresse électronique de l'expéditeur	-
Nom et prénom ou raison sociale du destinataire	-
Adresse électronique du destinataire	-
Niveau de garantie	Les preuves émises au titre de l'article 44 du Règlement eIDAS se distinguent par la mention de l'OID de la politique applicable et la présence de la *EU Trust Mark*[3]
Numéro d'identification unique de l'envoi	-
Jeton d'horodatage qualifié	La date et heure de l'envoi sont présentées lisiblement dans la preuve, au même titre que les autres informations. L'heure affichée est au fuseau CET (UTC+1). Elles proviennent du jeton d'horodatage qualifié apposé sur les données transmises, qui est lui-même inclus dans la preuve (encodé en base64).
Cachet électronique avancé	Cachet apposé sur les données (contenu du pli) pour les protéger contre toute modification. Il s'agit du cachet PAdES apposé sur le fichier preuve lui-même.

Remarque : l'intégrité des données est assurée par le cachet apposé sur la preuve, puisque celle-ci contient une empreinte des données (provenant du jeton d'horodatage). L'algorithme d'empreinte est le SHA-256.

[3] https://ec.europa.eu/digital-single-market/en/eu-trust-mark

4.4.2 Preuve de réception

La preuve de réception contient :

Donnée	Précisions
Les données de la preuve de dépôt (4.4.1)	La preuve de réception en reprend les données suivantes : • Nom et prénom ou raison sociale de l'expéditeur • Adresse électronique de l'expéditeur • Nom et prénom ou raison sociale du destinataire • Adresse électronique du destinataire • Niveau de garantie • Numéro d'identification unique de l'envoi
Identité du récepteur	Il s'agit du destinataire.
Référence à l'identification préalable du récepteur	Cette information est présentée sous la forme d'une référence au moyen d'identification utilisé par le destinataire.
Jeton d'horodatage qualifié	Cf. preuve de dépôt pour le format. Le jeton d'horodatage est spécifique à la preuve de réception. L'algorithme d'empreinte est le SHA-256, l'heure affichée est au fuseau CET (UTC+1).

4.4.3 Preuve de refus

La preuve de refus contient :

Donnée	Précisions
Les données de la preuve de dépôt (4.4.1)	*Idem.* preuve de réception
Jeton d'horodatage qualifié	Indique la date et heure de refus. Cf. preuve de dépôt pour le format. L'algorithme d'empreinte est le SHA-256, l'heure affichée est au fuseau CET (UTC+1).

4.4.4 Preuve de non-réclamation

La preuve de non-réclamation contient :

Donnée	Précisions
Les données de la preuve de dépôt (4.4.1)	*Idem.* preuve de réception

Donnée	Précisions
Date de production de la preuve	Indique la date et heure de non-réclamation. L'algorithme d'empreinte est le SHA-256, l'heure affichée est au fuseau CET (UTC+1).

4.5 Cycle de vie des MIE

Dans le cadre de la présente politique, les MIE reconnus dépendent du type d'utilisateur :

Expéditeur REAL (cf. 1.6.6)	– Clé REAL
Expéditeur	– HOTP – TOTP
Expéditeur RGS	– Certificat RGS
Destinataire	– HOTP – TOTP – Certificat RGS

Le cycle de vie des clés REAL ne dépend pas d'AR24 et est décrit dans la politique de certification associée (voir 1.6.6). Il en est de même pour les certificats RGS. La présente politique ne traite donc que des MIE suivants dont le cycle de vie est géré par AR24 :

- HOTP : Il s'agit d'OTP basés sur la RFC4225 (OTP produits à partir d'un compteur).
- TOTP : Il s'agit d'OTP basés sur la RFC6238 (OTP à durée de vie limitée produits en fonction du temps).

4.5.1 Remise à l'expéditeur

Les MIE remis à un expéditeur sont les mêmes que ceux remis à un destinataire.

4.5.2 Remise au destinataire

Le destinataire reçoit une liste d'HOTP en mains propres lors de la validation initiale de son identité (3.2.1).

Il peut aussi générer une nouvelle liste depuis son espace personnel en ligne (*ar24.fr*). Cette génération requiert une authentification forte par le biais d'un OTP valide (de la liste précédente).

4.5.3 Révocation du MIE

La révocation des clés REAL ne dépend pas d'AR24 et est décrit dans la politique de certification associée (voir 1.6.6).

La fonction de révocation est disponible 24h/24h, avec une durée maximale d'indisponibilité de 96h (quatre-vingt seize heures).

4.5.3.1 Origine d'une demande

Les demandes de révocation d'un MIE sont effectuées par le porteur du MIE lui-même.

4.5.3.2 Validation de la demande

Pour révoquer son MIE, le porteur s'authentifie sur son espace personnel avec son login et son mot de passe.

4.5.3.3 Traitement d'une demande

La révocation est gérée automatiquement depuis l'interface utilisateur.

4.5.3.4 Délai de traitement d'une demande

Le MIE est révoqué dans les secondes qui suivent la demande du porteur.

4.5.3.5 Notification de la révocation au porteur du MIE

Le nouveau statut du MIE est affiché dans l’espace du porteur.

5 Gestion des risques

5.1 Analyse de risques

Avant le lancement du service qualifié, AR24 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.

AR24 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, AR24 procèdera à l'homologation du service. Cette homologation est réalisée préalablement à la fourniture du service de confiance qualifié puis révisée au moins tous les deux ans.

5.3 PSSI

AR24 dispose d'une politique de sécurité du système d'information (PSSI) du service. Cette PSSI est approuvée par la direction.

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

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

AR24 conserve la responsabilité globale de la conformité avec les procédures prévues dans sa PSSI, même lorsque certaines fonctions sont mises en œuvres par des sous-traitants. En particulier, AR24 s'assure de la mise en œuvre effective des mesures prévues dans la PSSI.

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

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

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

5.4 Déclaration d'applicabilité

La liste suivante associe les documents applicables aux clauses issue de la norme *ISO 27002 : 2005* mentionnées au point 5 de *[TS_102640-3]* :

- 5 - Politique de sécurité : clause applicable, voir 5.3 de la politique du service

- 6.1 - Organisation interne : clause applicable, voir chapitre 6 et 5.2 de la politique du service
- 6.2.1 - Identification des risques provenant des tiers : clause applicable, voir 5.1 de la politique du service
- 6.2.2 - La sécurité et les clients : clause applicable, voir 5.1 de la politique du service
- 7 - Gestion des biens : clause applicable, voir 6.3, 6.4 de la politique du service
- 8 - Sécurité liée aux ressources humaines : clause applicable, voir 6.2 de la politique du service
- 9 - Sécurité physique et environnementale : clause applicable, voir 6.6 de la politique du service
- 10 - Gestion de l'exploitation et des télécommunications : clause applicable, voir 6 de la politique du service
- 11 - Contrôle d'accès : clause applicable, voir 6.4, 6.8 de la politique du service

6 Gestion et exploitation du PSRE

6.1 Organisation interne

6.1.1 Fiabilité

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

6.1.2 Rôles de confiance

Les rôles de confiance identifiés sont les suivants :

- **Responsable du cachet :** Le cachet utilisé pour sceller les données (4.4), même opéré par un tiers, reste sous la responsabilité de AR24. À ce titre, une ou plusieurs personnes sont responsables du cachet vis-à-vis de AR24, mais aussi de l'autorité de certification qui l'a émis.
- **Responsable sécurité :** Le responsable de sécurité est chargé de la mise en œuvre de la politique de sécurité de la composante. Il gère notamment les contrôles d'accès physiques aux équipements des systèmes sensibles.
- **Administrateur système :** 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).
- **Opérateur :** Les opérateurs sont les personnes en charge du fonctionnement quotidien du service (cf. chapitre 4) : support client, gestion éventuelle du MIE, etc.
- **Contrôleur :** Personne autorisée à accéder aux archives du service.
- **Porteurs de secrets :** Personne en charge d'un des secrets des HSM.

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, les cumuls suivants sont interdits :

- Responsable sécurité et administrateur système ou opérateur
- Contrôleur et tout autre rôle
- Administrateur système et opérateur.

6.2 Ressources humaines

6.2.1 Qualifications, compétences et habilitations requises

AR24 s'assure de la compétence et de l'adéquation des personnels employés.

6.2.2 Procédures de vérification des antécédents

AR24 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.

Par ailleurs, AR24 vérifie l'absence de conflit d'intérêt avant toute attribution d'un rôle de confiance.

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 Fréquence et séquence de rotation entre différentes attributions

La présente politique ne formule aucune exigence sur le sujet.

6.2.6 Sanctions en cas d'actions non autorisées

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

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

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

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

6.2.8 Documentation fournie au personnel

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

6.3 Gestion des biens

6.3.1 Généralités

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

6.3.2 Supports

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

6.4 Contrôle d'accès

AR24 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 (cf. 5.1).

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

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

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

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

Voir 6.8 pour le contrôle d'accès au niveau réseau.

6.5 Cryptographie

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

6.6 Sécurité physique et environnementale

6.6.1 Situation géographique 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). AR24 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 AR24 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.

6.6.8 Sauvegardes hors site

Des sauvegardes hors site sont effectuées quotidiennement.

6.7 Sécurité opérationnelle

6.7.1 Mesures de sécurité des systèmes informatiques

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

6.7.1.1 Exigences de sécurité technique spécifiques aux systèmes informatiques

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

- identification et authentification 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.

6.7.1.2 Niveau de qualification des systèmes informatiques

Voir 6.5.

6.7.1.3 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.

AR24 garantit que les objectifs de sécurité sont définis lors des phases de spécification et de conception.

AR24 utilise des systèmes et des produits fiables qui sont protégés contre toute modification.

Conformément au [GDPR], AR24 met en œuvre toutes les mesures techniques et organisationnelles nécessaires au respect de la protection des données personnelles, à la fois dès la conception des produits et des services, en veillant notamment à limiter la quantité de données traitée dès le départ (principe dit de « minimisation »).

6.7.2 Mesures liées à la gestion de la sécurité

Toute évolution significative d'une composante du système est signalée à l'entité identifiée en 1.4.1 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.

6.7.3 Évaluation des vulnérabilités

Les procédures d'exploitation du SI incluent la veille sécuritaire de ses composants. Ces procédures assurent que les correctifs de sécurité sont appliqués, au plus tard 2 mois après leur publication. 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≥9), l'analyse d'impact est effectuée dans les 48 heures suivant la publication de la vulnérabilité.

6.7.4 Horodatage / Système de datation

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

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

6.8 Sécurité réseau

Le réseau et ses systèmes sont protégés contre les attaques. 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.
AR24 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 (cf. 5.1) sont isolés dans une ou plusieurs zones sécurisées.

d) L'exploitation des systèmes est réalisée à travers un réseau d'administration dédié et cloisonné. Les systèmes utilisés pour l'administration de la mise en œuvre de la politique de sécurité ne 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 et privées du service, identifiées par TSP, 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.

6.9 Gestion des incidents et supervision

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

AR24 réagit de manière coordonnée afin de répondre rapidement aux incidents et de limiter l'impact des violations de la sécurité. La responsabilité d'assurer le suivi des alertes sur les événements de sécurité potentiellement critiques et de veiller à ce que les incidents pertinents soient signalés conformément aux procédures est attribuée à des personnels de confiance.

Les procédures de déclaration et d'intervention d'incident minimisent 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

AR24 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, AR24 informe sans délai la personne physique ou morale concernée.

6.9.2 Supervision des services partenaires

Le service de la LRE s'appuie sur un ou plusieurs prestataires d'horodatage, et un fournisseur de certificat de cachet électronique (1.5). La documentation interne d'AR24 décrit les mesures mises en œuvre pour vérifier de façon régulière la conformité de ces services tiers aux exigences de la présente politique, et notamment : la qualification des services d'horodatage et la non-révocation du certificat de cachet électronique.

6.10 Gestion des traces

6.10.1 Type d'événements à enregistrer

Concernant les systèmes liés aux fonctions qui sont mises en œuvre dans le cadre du service, chaque entité en opérant une composante 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.

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

D'autres événements 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	Contrôle d'accès au centre de données Enregistrement vidéo de l'accès à la salle d'hébergement
Les actions de maintenance et de changements de la configuration des systèmes	Tracé par les intervenants dans l'outil de gestion des traces
Les actions de destruction et de réinitialisation des supports contenant des informations confidentielles (clés, données d'activation, renseignements personnels sur les utilisateurs...).	HSM : Tracés dans le cadre des procédures de gestion interne

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

Validation de l'identité de l'expéditeur et du destinataire d'une LRE, et la preuve de validation associée.	Expéditeur : processus notarial Destinataire : trace technique de l'engagement par l'expéditeur REAL sur le portail lors de la production des OTP remis au destinataire.
Validation ou échec de l'identification de l'expéditeur ou du destinataire via leur MIE	Trace technique de validation des OTP Trace métier dans le portail de gestion LRE
Événements liés au cycle de vie des clés et des certificats cryptographiques (cachet et horodatage) : génération (cérémonie des clés), sauvegarde et récupération, révocation, renouvellement, destruction, etc. Remarque : ces événements peuvent être journalisés par les prestataires ou sous-traitants en charge de la gestion de ces clés et services (horodatage et apposition du cachet).	Tracés dans le cadre des procédures de gestion interne
Génération des preuves produites par le service (4.4)	Traces techniques
Publication et mise à jour des informations liées au service (politique, conditions générales d'utilisation, etc.) (2.4)	Traces techniques des outils de gestion de contenu du portail
(le cas échéant) remise du MIE à son porteur (4.5)	OTP : traces techniques
(le cas échéant) Réception d'une demande de révocation d'un MIE (4.5.3)	Trace technique du système de gestion des OTP
(le cas échéant) Validation ou rejet d'une demande de révocation d'un MIE (4.5.3)	Pas de rejet. La révocation effective est tracée techniquement par le système de gestion des OTP

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

- Type de l'événement
- Nom de l'exécutant ou référence du système déclenchant l'événement
- Date et heure de l'événement
- Résultat de l'événement (échec ou réussite).

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

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

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

- Toute information caractérisant l'événement

Les opérations de journalisation sont effectuées au cours du processus.

En cas de saisie manuelle, l'écriture est faite, sauf exception, le même jour ouvré que l'événement. Les événements et données spécifiques à journaliser sont documentés par AR24.

6.10.2 Fréquence de traitement des journaux d'événements

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

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

Par ailleurs, un rapprochement entre les différents journaux d'événements de fonctions qui interagissent entre elles est périodiquement effectué afin de vérifier la concordance entre événements dépendants et contribuer ainsi à révéler toute anomalie.

6.10.3 Période de conservation des journaux d'événements

Les journaux d'événements sont conservés sur site pendant au moins 1 (un) mois. Ils sont archivés le plus rapidement possible et au plus tard 15 (quinze) jours après leur génération.

6.10.4 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 6.7.4.

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.

6.10.5 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.

6.10.6 Notification de l'enregistrement d'un événement au responsable de l'événement

Aucune exigence spécifique.

6.11 Archivage des données

6.11.1 Types de données à archiver

AR24 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 à fin 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 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).

Remarque : toutes ces informations sont contenues dans les preuves (4.4) produites tout au long du cycle de vie des LRE. La conservation des preuves suffit à répondre à cette exigence.

6.11.2 Période de conservation des archives

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

Les journaux d'événements sont archivés pendant 10 ans après leur génération.

6.11.3 Protection des archives

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

Pendant tout le temps de leur conservation, les archives sont :

- protégées en intégrité ;
- accessibles aux personnes autorisées ;
- lisibles et exploitables.

6.11.4 Exigences d'horodatage des données

Voir 6.7.4.

6.11.5 Procédures de récupération et de vérification des archives

Seul AR24 a accès aux archives.

6.12 Continuité d'activité

6.12.1 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 (6.9), notamment au travers de la sensibilisation et de la formation de ses personnels et au travers de l'analyse des différents journaux d'événements (6.10.2).

Dans le cas d'un incident majeur, tel que la perte, la suspicion de compromission, la compromission, le vol de données critiques (p. ex., clés privées), l'événement déclencheur est la constatation de cet incident au niveau de la composante concernée, qui doit en informer immédiatement AR24. Le cas de l'incident majeur est impérativement traité dès détection et traité dans la plus grande urgence, voire immédiatement, par tout moyen utile

et disponible (presse, site Internet, récépissé…). AR24 prévient directement et sans délai l'ANSSI, conformément au § 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 AR24 :

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

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

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

Ce plan est testé annuellement.

6.12.3 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 est traité dans le plan de continuité de la composante en tant que sinistre.

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

En outre, AR24 informe au minimum 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 disposent des moyens nécessaires permettant d'assurer la continuité de leurs activités en conformité avec les exigences de la présente politique.

6.13 Fin d'activité

AR24 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, AR24 s'engage à transférer l'activité 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 AR24, 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, AR24 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, AR24 s'engage à transférer l'activité 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 AR24 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 d'AR24 seront transférées soit au tiers archiveur, soit à un tiers sous contrat, soit à un prestataire qualifié.

Les obligations transférées comprendront au moins les points suivants :

- Les preuves des envois recommandés électronique devront être conservée durant la durée légale nécessaire
- Les données personnelles ne pourront être exploitée à d'autres fins que celles mentionnées dans la présente politique

AR24 informera ses utilisateurs de l'arrêt d'activité et procèdera à la révocation des MIE, 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 AR24 réalise, ou fait 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, AR24 procèdera à un contrôle de conformité de cette composante.

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

6.14.2 Identités et qualifications des évaluateurs

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

6.14.3 Relations entre évaluateurs et entités évaluées

L'équipe d'audit 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 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.

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 sont tenus à la disposition de l'organisme de qualification en charge de la qualification du service.

7 Autres problématiques métiers et légales

7.1 Responsabilité financière

7.1.1 Couverture par les assurances

AR24 a contracté une assurance Responsabilité Civile Professionnelle auprès de Syntec Numérique Assurances. AR24 est assuré contre :

- toutes les conséquences pécuniaires,
    - résultant de tout fondement en responsabilité civile,
    - lui incombant dans l'exercice de l'ensemble de ses activités (définies à l'article 3 des conditions particulières),
- à raison de tous dommages (corporels, matériels et immatériels),
    - dans le monde entier, sous réserve des dispositions de l'article 2.2 des conventions spéciales,
    - quelle que soit la juridiction qui les apprécie,
    - dès lors que le risque n'est pas expressément visé dans une des exclusions (article 1.4 des conventions spéciales).

Sont notamment couvertes les conséquences des risques suivants, spécifiques au secteur les nouvelles technologies :

- Faute, erreur, omission, négligence, inobservation des règles de l'art, défaut de conseil (inadéquation entre la solution proposée et les besoins du client, spécifications insuffisantes)
- Obligation de résultat
- Engagement de performance et de délai
- Dysfonctionnements (ex. bug)
- Interruption de service dans les contrats d'hébergement (de données ou d'applicatif), d'infogérance ou de prestation en mode Saas ou l'équivalent
- Inexécution partielle ou totale (ex : déni de service), mauvaise exécution d'une obligation contractuelle (ex : mauvaise conduite de projet)
- Retard (même si la cause n'est pas accidentelle)
- Atteinte aux droits de propriété intellectuelle et/ou industrielle (contrefaçon de brevets et droits d'auteurs, concurrence déloyale, parasitisme économique, etc.)
- Divulgation d'information(s) confidentielle(s)
- Engagements et modifications contractuels non formalisés par écrit (y compris cahier des charges)
- Pertes de données clients et altérations ou destructions de biens confiés
- Volet RC des Cyber Risques (virus, données personnelles, fraude informatique)
- Volet Gestion de Crise des Cyber Risque

- Acte(s) de malveillance / faute intentionnelle des salariés
- Garantie de bonne fin et frais de retrait, remboursement des factures, pénalités de retard dans les marchés publics, frais de gestion des dossiers en crise

7.1.2 Autres ressources

Sans objet.

7.1.3 Couverture et garantie concernant les entités utilisatrices

Se référer aux sections afférentes au garanties pécuniaires décrites dans les *Conditions Générales d'Utilisation* (1.5.4).

7.2 Confidentialité des données professionnelles

7.2.1 Périmètre des informations confidentielles

Les informations considérées comme confidentielles sont au minimum les suivantes :

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

7.2.2 Informations hors du périmètre des informations confidentielles

Pas d'exigence.

7.2.3 Responsabilités en termes de protection des informations confidentielles

AR24 respecte la législation et la réglementation en vigueur sur le territoire français. En particulier, AR24 peut devoir mettre à disposition les données dont il dispose à des tiers dans le cadre de procédures légales. Elle doit également donner l'accès à ces informations à ses clients.

7.3 Protection des données personnelles

7.3.1 Politique de protection des données personnelles

Toute collecte et tout usage de données à caractère personnel par AR24 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).

7.3.2 Informations à caractère personnel

Les informations considérées comme personnelles sont au minimum les suivantes :

- Le cas échéant, les données d'identité des clients et les pièces associées utilisées pour vérifier leur identité[4] ;
- Les adresses IP, *hostname* et les *UserAgents* des navigateurs utilisés par les clients pour accéder au service

7.3.3 Informations à caractère non personnel

La présente politique ne formule aucune exigence sur ce point.

[4] À ce jour, AR24 ne manipule aucune pièce ni copie de pièce justificative de l'identité de ses utilisateurs.

7.3.4 Responsabilité en termes de protection des données personnelles

Voir 7.3.1.

7.3.5 Notification et consentement d'utilisation des données personnelles

Conformément à la législation et réglementation en vigueur sur le territoire français, les informations personnelles transmises à AR24 par les utilisateurs du service ne doivent ni être divulguées, ni transférées à un tiers, sauf dans les cas suivants : consentement préalable du porteur, décision judiciaire ou autre autorisation légale.

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

Sur ce point, AR24 agit dans le respect de la législation et réglementation en vigueur sur le territoire français.

7.3.7 Autres circonstances de divulgation d'informations personnelles

La présente politique ne formule aucune exigence sur ce point.

7.4 Obligations des utilisateurs

7.4.1 Expéditeurs

Les Expéditeurs garantissent :

- qu'ils ont, lors du dépôt d'une LRE, transmis à AR24, conformément au Décret, les informations suivantes :

(i) leurs nom et prénom s'il s'agit de personnes physiques, leur raison sociale s'il s'agit de personnes morales, ainsi que leur adresse électronique et, le cas échéant, leur adresse postale ;

(ii) Les nom et prénom ou la raison sociale du Destinataire, ainsi que son adresse électronique ;

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

- qu'ils ont préalablement obtenu l'accord du Destinataire, lorsque celui-ci est un non professionnel, pour lui adresser une LRE et qu'ils sont en mesure de prouver, par tous moyens, qu'ils ont obtenu le consentement du Destinataire ;
- l'identité du Destinataire, la validité de l'adresse électronique de contact à laquelle la LRE sera adressée et la qualité de consommateur ou de professionnel du Destinataire ;
- ne pas porter atteinte à leurs obligations contractuelles ou légales et à ne pas introduire lors de leur Dépôts tout virus, vers, bombe logique ou tout contenu pouvant être assimilés à du courrier non désiré.

7.4.2 Utilisation des MIE

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

- Protéger celui-ci de toute perte ou divulgation
- Révoquer (4.5.3) sans délai le MIE en cas de perte, vol, compromission ou de suspicion de compromission des moyens fournis

Les MIE sont strictement personnels et ne doivent pas être communiqués ou transmis à des tiers. L'utilisateur est responsable de l'utilisation qui est faite du MIE qui lui a été remis.

7.4.3 Utilisation des LRE

Le service de LRE entièrement électronique produit des preuves de Dépôt, d'Acceptation, de Refus et de Non-Réclamation (4.4) qui sont opposables en justice. Leur authenticité est garantie par le jeton d'horodatage qualifié qu'elles contiennent et le cachet électronique avancé d'AR24 qui est apposé dessus.

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

- Vérifier la validité du jeton d'horodatage, conformément aux procédures décrites dans la politique correspondante (1.5.1)
- Vérifier la validité du certificat utilisé pour le cachet électronique, conformément aux procédures décrites dans la politique correspondante (1.5.2)
- Vérifier la validité du cachet électronique (en utilisant par exemple un logiciel de lecture des fichiers PDF sachant interpréter les signatures électroniques, p. ex., *Acrobat Reader*)

7.5 Droits sur la propriété intellectuelle et industrielle

La présente politique ne formule aucune exigence sur ce point.

7.6 Interprétations contractuelles et garanties

La présente politique ne formule aucune exigence sur ce point.

7.7 Durée et fin anticipée de validité de la politique

7.7.1 Durée de validité

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

7.7.2 Fin anticipée de validité

L'adoption d'actes d'exécution ou délégués du règlement eIDAS peut entraîner, en fonction des évolutions apportées, la nécessité pour AR24 de faire évoluer la présente politique (pour la gestion de la politique, voir 1.3, p. 5).

AR24 se réserve aussi le droit d'étendre les moyens d'identification techniques et organisationnels des expéditeurs et destinataires, et le périmètre des populations concernées par la présente politique.

7.7.3 Effets de la fin de validité et clauses restant applicables

Dans tous les cas, AR24 respectera les exigences réglementaires qui lui incombent.

7.8 Conformité aux législations et réglementations

Les pratiques de AR24 sont non-discriminatoires.

La conception et la mise en œuvre des services, logiciels et procédures de AR24 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/).

7.9 Force majeure

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