Service de Cachet Electronique de La Poste

Politique de Signature

Résumé

Le présent document constitue la Politique de Signature électronique de La Poste et définit les exigences techniques, organisationnelles et juridiques de La Poste. L'objet de la présente Politique de Signature est de formaliser les engagements de La Poste. Cette Politique de Signature, qui définit donc les « objectifs et les engagements » de La Poste pour assurer la fiabilité des services de signature Cachet Serveur fournis, est un document public accessible librement par les services demandeurs et les utilisateurs finaux. La Politique de Signature fait partie du référentiel documentaire de la Politique de Sécurité des Systèmes d'Information de La Poste (PSSI-G).

Version

Statut	Approuvée
Version	3.0
Date d'enregistrement	13/12/2018
Responsable du document	Direction des Systèmes d'Information Groupe (DSI-G)
Valideur (s)	Direction des Systèmes d'Information Groupe (DSI-G) Direction des Systèmes d'Information Branche Service Colis Courrier (DSI-BSCC)
Approbateur (s)	Comité d'Approbation des Politiques (CAP)
Nom fonctionnel	Politique de signature de La Poste

© La Poste, tous droits réservés

Diffusion : Publique

SOMMAIRE

Copyright © 2017 La Poste

Copyright © 2018 La Poste

Copyright © 2018 La Poste

Copyright © 2018 La Poste

AVERTISSEMENT

Le présent document est une œuvre protégée par les dispositions du Code de la Propriété Intellectuelle du 1er juillet 1992, notamment par celles relatives à la propriété littéraire et artistique et aux droits d'auteur, ainsi que par toutes les conventions internationales applicables (notamment la convention de Berne de 1886). Ces droits sont la propriété exclusive de La Poste. La reproduction, la représentation (y compris la publication et la diffusion), intégrale ou partielle, par quelque moyen que ce soit (notamment, électronique, mécanique, optique, photocopie, enregistrement informatique), non autorisée préalablement par écrit par La Poste ou ses ayants droit, sont strictement interdites.

Le Code de la Propriété Intellectuelle n'autorise, aux termes de l'article L.122-5, d'une part, que « les copies ou reproductions strictement réservées à l'usage privé du copiste et non destinés à une utilisation collective » et, d'autre part, que les analyses et les courtes citations dans un but d'exemple et d'illustration, « toute représentation ou reproduction intégrale ou partielle faite sans le consentement de l'auteur ou de ses ayants droit ou ayants cause est illicite » (article L.122-4 du Code de la Propriété Intellectuelle).

Cette représentation ou reproduction, par quelque procédé que ce soit, constituerait une contrefaçon sanctionnée notamment par les articles L. 335-2 et suivants du Code de la Propriété Intellectuelle.

Copyright © 2017 La Poste

1. INTRODUCTION

Ce document décrit les différentes politiques de signature des Services Électroniques de Confiance de La Poste. Il y sera fait référence, dans la suite de ce document, sous le nom « Politique de Signature » (PS), lorsqu'aucune confusion n'est à craindre.

1.1. PRESENTATION GENERALE

Une politique de signature est identifiée par un identifiant unique (OID ou *Object IDentifier*). Elle est composée d'un ensemble de règles et de dispositions définissant les exigences auxquelles chacun des acteurs impliqués se conforme et qui régit la génération de signatures électroniques et la vérification de leur validité.

Une PS est définie indépendamment des modalités de mise en œuvre des composants auxquels elle s'applique.

La structure de ce document est conforme aux documents normatifs suivants :

- *ETSI TR 102 041 V1.1.1 (2002-02) : Signature Policies Report*
- *RFC 3125 - Electronic Signature Policies*

1.2. IDENTIFICATION

Les trois politiques de signature décrites dans le présent document sont identifiées par les OID suivants :

{iso(1) member-body(2) france(250) type-org(1) la poste(8) courrier-services électroniques de confiance (1) Services de Cachet Électronique(1) document(3) politique (1) ps cep (4) version (1)}	1.2.250.1.8.1.1.3.1.4.1
{iso(1) member-body(2) france(250) type-org(1) la poste(8) courrier-services électroniques de confiance (1) Services de Cachet Électronique(1) document(3) politique (1) ps cep r (5) version (1)}	1.2.250.1.8.1.1.3.1.5.1
{iso(1) member-body(2) france(250) type-org(1) la poste(8) courrier-services électroniques de confiance (1) Services de Cachet Électronique(1) document(3) politique (1) ps la-lre (6) version (1)}	1.2.250.1.8.1.1.3.1.6.1

1.3. CHAMP D'APPLICATION DES POLITIQUES

La Poste fournit les mécanismes et les dispositifs cryptographiques utilisés par certains Services Électroniques de Confiance de La Poste et Applications Postales pour signer des éléments de preuve de ses services (attestations électroniques, cachets électroniques de La Poste, marque d'affranchissement). Il s'agit de la signature électronique apposée par La Poste sur les données des éléments de preuve délivrés aux clients du Cachet Électronique de La Poste (C.E.P.) et aux services internes du C.E.P.

Ce processus est toujours réalisé sous la responsabilité de La Poste qui peut le sous-traiter auprès d'opérateurs techniques.

Copyright © 2018 La Poste

Les signatures électroniques produites le sont avec des clés privées de signature appartenant à La Poste. Les parties publiques des bi-clés correspondantes sont certifiées par des A.C. choisies par La Poste en fonction de critères et spécifications techniques qui sont périodiquement audités par la Commission d'Approbation des Politiques de La Poste (*cf.* chapitre 6).

1.4. APPLICATIONS UTILISATRICES DU SERVICE DE SIGNATURE

Seules les requêtes émises par les Applications utilisatrices ayant suivi le processus de souscription au service décrit au chapitre 4 sont autorisées à faire appel aux services de signature de La Poste.

1.5. PUBLICATION DE LA POLITIQUE DE SIGNATURE

Avant toute publication, la politique de signature est validée par l'entité responsable identifiée en 1.8. Les modifications définitives ayant des impacts sensibles au niveau des Applications Utilisatrices leur sont présentées avant publication.

La présente politique de signature est publiée à l'adresse suivante : http://www.laposte.fr/cachet

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

- Document au format PDF
- OID des politiques
- Empreinte du document
- Algorithme de hachage utilisé (condensat SHA-256 pour cette version)
- Date et heure exacte d'entrée en vigueur

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

1.6. ENTREE EN VIGUEUR DE LA NOUVELLE VERSION ET PERIODE DE VALIDITE

La nouvelle version de la politique de signature entre en vigueur 15 jours ouvrés après sa mise en ligne et reste valide jusqu'à la publication d'une nouvelle version.

1.7. MODIFICATIONS ET APPLICATION DE LA POLITIQUE DE SIGNATURE

La mise à jour d'une politique de signature est une procédure impliquant tous les acteurs et faisant l'objet d'une démarche rigoureuse, essentiellement pour procéder à des modifications importantes, pour prendre en compte de nouveaux besoins, de nouveaux acteurs, améliorer le cadre juridique ou combler des lacunes.

Copyright © 2018 La Poste

Cette Politique de Signature sera revue périodiquement par l'entité responsable identifiée en 1.8, notamment pour :

- mettre à jour le domaine d'application du document,
- s'adapter aux évolutions technologiques.

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

Direction des Systèmes d'information Courrier

111 bd Brune 75014 Paris

ld-cachet-mco@laposte.fr

Ces remarques et souhaits d'évolution sont examinés la CAP qui engage, si nécessaire, le processus de mise à jour de la présente politique de signature.

Le tableau suivant indique les principales modifications de ce document en comparaison à la version antérieure.

Version	Date d'entrée en vigueur	Principaux points de modification
1.0	6 avril 2006	Création
2.0	16 Juillet 2014	Mise à jour multi politique Intégration du suivi de version dans SharePoint
2.0a	26 Janvier 2017	Révision pour publication – OID de la PH mis à jour
3.0	13 décembre 2018	Révision pour publication – OID PS LRTE ajouté (1.2) + Mise à jour des références (1.9) + Edition des obligations (2.2) + Ajout eIDAS et RGSv2 (3.1) + Remplacement de SSL par TLS (3.2) + ajout du support du format PaDeS (3.4) + Ajout d'un email de contact (4.4) + Ajouts des sources de synchronisation du temps (5.4)

Tableau 1: Historique de la Politique de Signature

La présente version de la Politique de Signature s'applique à l'ensemble des opérations de signature effectuées par le service de signature dans le cadre énoncé au paragraphe 1.3, pour le compte d'une Application Utilisatrice (cf. paragraphe 1.4) à compter de la date notifiée aux clients ayant souscrit au service.

1.8. COORDONNEES DES ENTITES RESPONSABLES DE LA POLITIQUE DE SIGNATURE

L'organisme responsable de cette Politique de Signature est la CAP.

Copyright © 2018 La Poste

La Commission d'Approbation des Politiques (CAP) de La Poste pour les Services Électroniques de Confiance de La Poste est constituée de représentants désignés par La Poste pour créer, contrôler le respect et faire évoluer la documentation des politiques régissant l'infrastructure des Services Électroniques de Confiance de La Poste.

Les principales fonctions de la CAP sont de :

- Maintenir, corriger, faire évoluer, clarifier et remplacer les politiques en usage au sein des Services Électroniques de Confiance de La Poste ;
- Approuver les nouvelles politiques ;
- Publier les politiques.

La CAP a également pour rôle d'approuver la façon dont la sécurité a été prise en compte et mise en œuvre au sein de l'infrastructure. À ce titre, elle valide ou fait valider par une entité qu'elle désigne, la conformité des pratiques des opérateurs à la présente PS.

La CAP se réunit aussi souvent que nécessaire, afin de valider toute nouvelle version d'un document de politique, et au moins une fois par an pour passer en revue les contrôles réalisés et s'assurer de la conformité des pratiques des différents opérateurs.

1.9. REFERENCES

- [PH]

  Politique d'Horodatage de La Poste, v. 5.32, OID : 1.2.250.1.8.1.1.1.1.6

- [PC Standard]

  Politique de certification certificat de serveur Cachet, réf. DT-FL-1310/020, version 1.8, OID : 1.2.250.1.86.2.3.2.22.1

- [PC Standard G2]

  Politique de certification certificat de serveur Cachet, réf. DT-FL-1310/020, version 1.8, OID : 1.2.250.1.86.2.6.2.22.1

- [PC Prime]

  Politique de certification certificat de serveur Cachet, réf. DT-FL-1310/020, version 1.8, OID : 1.2.250.1.86.2.3.3.22.1

- [PC Prime G2]

  Politique de certification certificat de serveur Cachet, réf. DT-FL-1310/020, version 1.8, OID : 1.2.250.1.86.2.6.3.22.1

Copyright © 2018 La Poste

1.10. LISTE DES ACRONYMES UTILISES

Acronyme	Signification
AC	Autorité de Certification
CAP	Commission d'Approbation des Politiques
CEP	Cachet Électronique de La Poste
CRL	*Certificate Revocation List*, ou LCR
ICP	Infrastructure à Clés Publiques, ou PKI
LCR	Liste des Certificats Révoqués, ou CRL
OID	*Object Identifier*
PC	Politique de Certification
PKI	*Public Key Infrastructure*, ou ICP
PS	Politique de Signature
RGS	Référentiel Général de Sécurité
UTC	*Coordinated Universal Time ou Temps Universel Coordonné*

1.11. DEFINITIONS

- **Application Utilisatrice** : processus automatique (« applicatif ») utilisateur du service de signature opéré sous la responsabilité du client, clients et services du CEP.
- **Application Postale** : processus automatique (« applicatif ») utilisateur du service de signature opéré par La Poste.
- **Authentification :** vérification de l'identité d'une personne ou d'une application.

  L'authentification est l'un des services rendus par une PKI grâce à l'utilisation conjointe d'un certificat et de la clé privée associée : un porteur peut s'authentifier par exemple pour accéder à la plate-forme d'une application en présentant son certificat et par le biais d'un mécanisme de signature numérique.
- **Autorité de Certification (AC)** : entité, composante de base de la PKI, qui délivre des certificats à une population de porteurs ou à d'autres composants d'infrastructure. L'Autorité de Certification sert de caution morale en s'engageant sur l'identité d'une personne au travers du certificat qu'elle lui délivre et qu'elle signe à l'aide de sa clé privée.

  Elle regroupe l'ensemble des composants d'infrastructure qui opèrent et distribuent les services spécifiquement rendus aux titulaires de certificats (émission des certificats porteurs et gestion du cycle de vie, assistance, etc.).

Copyright © 2018 La Poste

- **Bi-clé** : couple de clés cryptographiques, composé d'une clé privée (devant être conservée secrète) et d'une clé publique (largement diffusée par le biais du certificat). Ce couple de clés permet, par le biais de divers mécanismes, de rendre des services de sécurité comme la non-répudiation, l'authentification, la confidentialité et l'intégrité.

- **Certificat (numérique) d'identité** : pièce d'identité électronique dont le contenu est garanti par une Autorité de Certification. Il permet dans les transactions électroniques d'attester de la correspondance entre une clé publique et l'identité de son titulaire (et éventuellement de son propriétaire si celui-ci est différent du titulaire). Il contient donc l'ensemble des informations qui permettent cette identification (nom, éventuellement entreprise, adresse, etc.).

- **Chaîne de confiance (chemin de certification)** : ensemble ordonné des certificats nécessaires pour vérifier la filiation d'un certificat donné.

- **Commission d'Approbation des Politiques (CAP)** : entité constituée de représentants désignés par La Poste pour créer, contrôler le respect et faire évoluer la documentation des politiques régissant l'infrastructure des Services Électroniques de Confiance. Cette documentation inclut la Politique de Signature.

  La CAP a également pour rôle d'approuver la façon dont la sécurité a été prise en compte et mise en œuvre au sein de l'infrastructure. À ce titre, elle valide ou fait valider par une entité qu'elle désigne, la conformité des pratiques des opérateurs à la présente PS.

- **Compromission** : une clé privée est dite compromise lorsqu'elle est potentiellement utilisable ou a été utilisée par d'autres personnes que celles habilitées à la mettre en œuvre.

- **Contremarque de temps** : donnée qui lie une représentation d'une donnée à un temps particulier, exprimé en heure UTC, établissant ainsi la preuve que la donnée existait à cet instant-là. Le tout étant signé électroniquement par l'Autorité d'Horodatage.

- **Demandeur (de Signature)** : personne physique ou morale demandant la signature de données à l'Autorité de Signature.

- **Données d'activation** : données privées associées à un titulaire de certificat permettant de mettre en œuvre sa clé privée.

- **Entité finale :** entité utilisatrice des services de la PKI. Une entité finale peut être titulaire de certificat, accepteur de certificat, ou les deux simultanément.

- **Infrastructure à Clé Publique (ICP ou PKI – *Public Key Infrastructure*)** : ensemble de composants, fonctions et procédures dédiés à la gestion de clés et de certificats utilisés par des services de sécurité basés sur la cryptographie à clé publique.

- **Jeton d'horodatage** : voir Contremarque de temps.

- **Liste de Certificats Révoqués (LCR ou CRL)** : liste de numéros de certificats ayant fait l'objet d'une révocation.

- ***Object IDentifier* (ou OID)** : identifiant alphanumérique unique enregistré conformément à la norme d'enregistrement ISO pour désigner un objet ou une classe d'objets spécifiques.

Copyright © 2018 La Poste

- **Politique de Certification (PC)** : ensemble de règles définissant les exigences auxquelles chacun des acteurs impliqués se conforme et qui indique le niveau de sécurité commun accordé aux certificats.

- **Politique de Signature (PS)** : ensemble de règles et dispositions définissant les exigences auxquelles chacun des acteurs impliqués se conforme et qui régit la génération des signatures électroniques et la vérification de leur validité.

- **Politique de Validation de Signature (PVS)** : ensemble de règles et dispositions définissant les exigences auxquelles chacun des acteurs impliqués se conforme et qui régit la vérification de la validité des signatures électroniques.

- **Porteur (de certificat)** : personne physique utilisatrice d'un certificat. On peut distinguer le porteur de certificat (*certificate holder*) du propriétaire du certificat (*certificate owner) :* le porteur utilisera le certificat en qualité de représentant du propriétaire du certificat.

- **Propriétaire de certificat** : personne, morale ou physique, qui a souscrit un certificat d'identité auprès d'une Autorité de Certification. Le propriétaire du certificat se distingue du porteur de certificat. Le propriétaire de certificat est en réalité le propriétaire d'une licence d'utilisation du certificat, et le porteur utilise ce dernier au titre de sa mission professionnelle.

- **Révocation (d'un certificat)** : opération de mise en opposition effectuée à la demande du porteur ou de toute autre personne autorisée, qui entraîne la suppression de la caution apportée par l'Autorité de Certification sur un certificat donné avant la fin de sa période de validité. Par exemple, la compromission, la destruction d'une clé privée, le changement d'informations contenues dans un certificat ou encore le non-respect des règles d'utilisation du certificat doivent conduire à la révocation du certificat.

- ***Secure Socket Layer* (ou SSL)** : obsolète. Cf : TLS

- **Services Électroniques de Confiance de La Poste** : composante de l'infrastructure de La Poste auprès de laquelle un utilisateur peut solliciter, entre autres, la signature de données.

- **Signature** : les définitions fonctionnelle et technique de la signature seront distinguées dans ce document en utilisant respectivement les termes de **signature électronique** et de **signature numérique** (voir les définitions ci-après).

- **Signature électronique** : donnée qui résulte de l'usage d'un procédé répondant aux conditions définies à l'article 1316-4 du code civil. En particulier et comme indiqué dans ce même article, la signature électronique manifeste le consentement des parties aux obligations qui découlent de l'acte de signature (à l'instar de la signature manuscrite).

Copyright © 2018 La Poste

- **Signature numérique** : cryptogramme issu du chiffrement d'une empreinte de données à l'aide d'une clé privée, cette empreinte étant obtenue par application d'une fonction de hachage (algorithme de codage irréversible) sur lesdites données. Le terme signature numérique désigne indifféremment le cryptogramme et le mécanisme permettant de l'obtenir. Une signature numérique peut accompagner les données qui ont été signées et en garantir l'intégrité et la non-répudiation par l'émetteur. Le mécanisme de signature numérique peut également être utilisé pour authentifier dynamiquement un titulaire de certificat.

- **Titulaire de certificat** : sujet qui s'est vu délivrer un certificat par une AC. Lorsque le titulaire est une personne physique, cette dernière est appelée « porteur ».

- ***Transport Layer Security* (ou TLS)** : protocole de sécurisation couramment utilisé sur Internet (notamment pour sécuriser HTTP). TLS offre notamment des services d'authentification, d'intégrité, et de confidentialité.

- **Utilisateur (de certificat)** : tiers destinataire d'un certificat, qui agit en faisant confiance à ce certificat et/ou à une signature numérique vérifiée grâce à ce certificat. Ce peut être une entité responsable d'une application utilisant les services de certification, ou une personne physique. Les qualités d'utilisateur de certificat et de porteur de certificat ne sont pas forcément mutuellement exclusives : une application pourra éventuellement dans le même temps être utilisatrice et porteuse de certificat.

  Bien qu'un porteur puisse être utilisateur de certificat (par exemple dans le cadre de la vérification d'une signature de courriel ou d'un accusé de réception émis par une application), il est considéré dans le reste de ce document que seules les applications (processus automatiques) peuvent tenir le rôle d'utilisateur. Il sera alors question d'Applications Utilisatrices. La présente politique fera l'objet d'une mise à jour lorsque des personnes physiques pourront tenir le rôle d'utilisateur.

- **Vérification de validité d'un certificat** : opération de contrôle du statut d'un certificat (ou d'une chaîne de certification). Un certificat référencé peut être dans l'un des trois états suivants : valide, expiré ou révoqué.

- **Vérification de validité d'une signature** : opérations de contrôle, permettant de s'assurer que la signature et le certificat associé sont cryptographiquement valides.

Copyright © 2018 La Poste

2. DISPOSITIONS DE PORTEE GENERALE

2.1. INTERVENANTS ET ROLES

2.1.1. Services Électroniques de Confiance

La Poste distribue et opère pour le compte de ses clients un service de signature. Ce service fait l'objet de la présente politique.

La Poste porte la responsabilité des opérations qu'elle réalise vis-à-vis de certains Services Électroniques de Confiance de La Poste et Applications Postales.

La Poste porte la responsabilité des opérations qu'elle réalise vis-à-vis de ses clients Applications utilisatrices. Elle est notamment l'interlocuteur unique du client pour résoudre tout litige né de l'utilisation du service de signature.

La Poste opère pour son propre compte une plate-forme technique qui réalise les opérations nécessaires à la signature de données. La Poste s'engage notamment sur la valeur des signatures que produites par cette plate-forme.

2.1.2. Application Utilisatrice

Une Application utilisatrice est un applicatif sous la responsabilité du client qui fait appel au service de signature de La Poste afin d'obtenir la signature de données. Cette signature permet à l'application utilisatrice de garantir l'intégrité des données qu'elle transmet à ses utilisateurs.

2.1.3. Destinataires des signatures

Les destinataires sont des personnes morales ou physiques, ou des applicatifs tiers, chargés de traiter les données signées.

2.2. OBLIGATIONS

La Poste s'oblige à :

- opérer ou faire opérer une plate-forme technique mettant en œuvre des moyens adaptés au niveau de risque, conformes aux règles de l'art et aux dispositions stipulées dans le présent document,
- garantir la confidentialité des informations qu'elle détient conformément aux dispositions du paragraphe 7.4.

Copyright © 2018 La Poste

2.2.1. Applications utilisatrices

Il incombe aux applications utilisatrices :

- d'accéder au service selon les moyens d'accès définis dans les documents techniques de la plate-forme, conformément aux tests de qualification (cf. 4.1)
- de se conformer aux règles édictées par La Poste quant à la mise en œuvre d'un dispositif de sécurité permettant d'assurer l'authentification, la confidentialité et l'intégrité des échanges avec le service de signature
- de mettre en œuvre des moyens adaptés au niveau de risque pour sécuriser sa propre plate-forme technique,
- de conserver par des moyens adaptés les données signées.

L'Application Utilisatrice et ses représentants sont seuls responsables de l'utilisation qu'ils font du service de signature et de la non compromission des clés privées leur permettant de s'authentifier auprès de ce dernier. Ils font notamment leur affaire personnelle de la réparation de tous dommages éventuellement subis par eux-mêmes ou des tiers en cas :

- de mauvaise utilisation du service
- de mauvaise utilisation ou compromission des certificats leur permettant de s'authentifier auprès de celui-ci.

2.2.2. Destinataires des signatures

Il incombe aux destinataires de vérifier les signatures électroniques, conformément aux exigences de la section 3.7.

2.3. UTILISATION HORS DU CADRE DE LA POLITIQUE DE SIGNATURE

La Poste ne saurait être tenue pour responsable en cas de litige lié à une utilisation des services offerts non normée par la présente Politique de Signature.

2.4. RESPECT ET INTERPRETATION DES DISPOSITIONS JURIDIQUES

2.4.1. Droit applicable

Le présent document est régi par la loi française.

2.4.2. Règlement des différends

Tout litige qui surviendrait concernant l'interprétation et l'exécution de la présente politique devra faire l'objet d'une tentative de règlement amiable. À défaut de règlement amiable, le litige sera soumis au droit français, et porté devant le tribunal compétent dans le ressort de la cour d'appel de Paris statuant en droit français.

Copyright © 2018 La Poste

2.5. AUDITS DE CONFORMITE ET AUTRES CONTROLES

Les mesures de contrôle décrites dans le présent paragraphe s'appliquent aux composants sur lesquels La Poste s'appuie dans le cadre de la fourniture des Services Électroniques de Confiance. Les contrôles de conformité sont réalisés périodiquement. La CAP de La Poste désigne un organisme d'audit afin de procéder au contrôle de conformité. La CAP prend les mesures adaptées au résultat de l'audit, à savoir :

- **En cas d'échec**, et selon l'importance des non-conformités, elle prend des sanctions. Les sanctions peuvent aller de la mise en demeure à effectuer immédiatement les modifications nécessaires, à la résiliation du contrat qui la lie à ses opérateurs.
- **En cas de résultat « À confirmer »,** elle remet à la composante en cause un avis précisant sous quel délai les non conformités doivent être réparées. Puis, un contrôle de « Confirmation » permettra de vérifier que tous les points critiques ont bien été résolus.
- **En cas de réussite**, elle remet à la composante contrôlée un avis d'autorisation d'exercice de sa fonction.

Copyright © 2018 La Poste

3. SIGNATURE ELECTRONIQUE ET VALIDATION

3.1. DESCRIPTION GENERALE DU SERVICE

La Poste offre un service de signature électronique avancée au sens de la directive 1999/93/CE du Parlement européen. Cette directive est abrogée et remplacée par le règlement eIDAS.

Ce service est construit et opéré dans le respect des exigences du Règlement Général de Sécurité (RGS) v2.

Le service de signature est mis à disposition des Applications Utilisatrices au travers du service de Cachet Électronique de La Poste.

Une requête de signature ne peut avoir que l'un des résultats suivants :

- Réussite de l'opération de signature, avec retour de la signature.
- Anomalies lors de l'opération de signature, avec retour de la signature.
- Erreur lors de l'opération de signature, sans retour de signature.

3.2. SECURITE DES ECHANGES

Le service de signature est mis à disposition des Applications Utilisatrices au travers du service de Cachet Électronique de La Poste. Les moyens d'accès au service du Cachet Électronique de La Poste permettent de répondre aux exigences suivantes.

Toute transaction de signature s'effectue via un canal chiffré avec authentification mutuelle des parties (SSL).

Sont considérées comme critiques :

- l'authentification du service
- l'intégrité des données échangées,
- la disponibilité du service.

Sont considérées comme sensibles :

- l'authentification de l'Application Utilisatrice,
- la confidentialité des échanges.

Le service s'authentifie fortement auprès des applications utilisatrices, c'est-à-dire que :

- l'authentification est non-rejouable,
- l'observation de la communication ne compromet pas les conventions secrètes utilisées,
- cette authentification s'appuie sur des mécanismes de cryptographie asymétrique.

Copyright © 2018 La Poste

Les plates-formes des Applications Utilisatrices s'authentifient quant à elles de manière renforcée :

- l'authentification est non-rejouable,
- l'observation de la communication ne compromet pas les conventions secrètes utilisées.

De plus amples dispositions quant à la gestion des données d'authentification sont exprimées dans le chapitre 6.

3.3. HORODATAGE

Dans le cadre du service de Cachet Électronique de La Poste, l'Application Utilisatrice peut demander ou non l'horodatage de la signature. Si elle a fait cette demande, c'est la date et l'heure de l'Autorité d'Horodatage de La Poste qui est utilisée.

La date considérée pour la transaction correspond donc à la contremarque de temps incluse dans la réponse de signature.

Dans le cas où cette information d'horodatage serait perdue ou inexploitable, la date et l'heure qui font foi sont extraites des journaux d'événements de la plate-forme du service, alors utilisés comme « **traces de temps** ».

3.4. CARACTERISTIQUES DES SIGNATURES

Les signatures produites par l'AS sont au format XAdES ou PAdES selon le client.

La signature est attachée ou détachée, selon l'option demandée par l'Application utilisatrice.

Si l'horodatage est demandé, une contremarque de temps conforme au standard *RFC 3161*, est intégrée dans les attributs non signés de la signature. La contremarque de temps est générée en conformité à la politique d'horodatage de La Poste.

3.5. ALGORITHMES UTILISABLES POUR LA SIGNATURE

3.5.1. Algorithme d'empreinte

L'algorithme d'empreinte est SHA256.

3.5.2. Algorithme de chiffrement

L'algorithme de chiffrement utilisé est *RSA Encryption.*

3.6. CONVENTION DE PREUVE

Le Client et l'Autorité de Signature conviennent de la valeur probante des éléments suivants **pour résoudre tout litige relatif à la fourniture et à l'utilisation du service de signature** :

- Seules les traces techniques du service font foi pour connaître les volumes d'utilisation du service par les Applications Utilisatrices (les demandes de signature sont authentifiées, notamment pour permettre la facturation du service).

Copyright © 2018 La Poste

3.7. CONDITIONS DE VALIDITE D'UNE SIGNATURE

Une signature sera considérée comme valide si et seulement si elle vérifie les trois assertions suivantes :

- Validité du certificat (syntaxe, signature, chaîne de certification, dates de début et de fin de validité, non révocation du certificat).
- Intégrité des données signée (calcul de l'empreinte et comparaison avec celle incluse dans la signature).
- Validité cryptographique de la signature (utilisation de la clef publique contenue dans le certificat).

De plus, si une contremarque de temps se trouve dans la signature, les vérifications suivantes sont réalisées sur la contremarque :

- Validité de la contremarque.
- Validité du certificat de signature de la contremarque.
- Lien avec le contenu de la signature.

Le cas échéant, elle peut porter sur :

- la vérification du respect de la norme de signature
- la vérification de l'appartenance du certificat du signataire à une famille de certificat donnée (p. ex., qualifiée RGS ou certifiée ETSI)
- la vérification de l'identifiant de la politique de signature référencée

Néanmoins, ces vérifications supplémentaires sortent du cadre de la présente politique.

Copyright © 2018 La Poste

4. BESOINS OPERATIONNELS LIES AU SERVICE

4.1. PROCESSUS DE SOUSCRIPTION AU SERVICE

Le service de signature est ouvert aux clients de La Poste et aux services internes suite à l'établissement d'un contrat ou d'un accord établi entre les parties.

En outre, afin de prévenir une utilisation de ses services qui soit inadaptée, frauduleuse ou non-conforme à l'état de l'art et de nature à compromettre la sécurité ou le bon fonctionnement de ces mêmes services, La Poste réalise des tests de qualification avec les plates-formes opérationnelles du Client avant la connexion au service.

4.2. INSTALLATION DES CHAINES DE CERTIFICATION

Le certificat de signature est généré en conformité avec une politique de certification dépendant de l'OID concernée :

1.2.250.1.86.2.3.2.22.1	[PC Standard]
1.2.250.1.86.2.3.3.22.1	- [PC Standard G2] *Politique de certification certificat de serveur Cachet,* réf. DT-FL-1310/020, version 1.8, OID : 1.2.250.1.86.2.6.2.22.1 [PC Prime]
1.2.250.1.86.2.6.2.22.1	[PC Standard]
1.2.250.1.86.2.6.3.22.1	- [PC Standard G2] *Politique de certification certificat de serveur Cachet,* réf. DT-FL-1310/020, version 1.8, OID : 1.2.250.1.86.2.6.2.22.1 [PC Prime]

Le Client se réfère à cette politique de certification pour se procurer la chaîne de certification correspondante.

4.3. SYNCHRONISATION AVEC L'INFRASTRUCTURE

La présente politique n'impose aucune obligation particulière. Il est néanmoins conseillé à l'Application Utilisatrice de maîtriser les écarts entre l'heure de son système et l'heure UTC.

4.4. COMPROMISSION DE LA CLE PRIVEE D'AUTHENTIFICATION DES APPLICATIONS UTILISATRICES

Les Applications Utilisatrices sont tenues de prévenir La Poste (ld-cachet-mco@laposte.fr) au plus tôt en cas de compromission de leur clé privée d'authentification, réelle ou supposée.

Copyright © 2018 La Poste

4.5. RENOUVELLEMENT DES CLES DES APPLICATIONS UTILISATRICES

Sans objet

4.6. RENOUVELLEMENT DES CLES DU SERVICE

Le service de signature dispose d'une clé d'authentification (pour l'établissement du canal d'interrogation sécurisé) et d'une clé de signature.

Les conditions de renouvellement de la clé d'authentification et du certificat associé sont précisées par la Politique de Certification de l'Autorité de Certification pour ce certificat.

La durée de vie des clés de signature et la période d'activité de ces clés privées sont définies dans la Politique de Certification associée (voir 4.2).

Le renouvellement des clés (d'authentification ou de signature) suppose la transmission du nouveau certificat à l'Application Utilisatrice par un moyen sûr, conformément aux dispositions du paragraphe 6.1.3.

Copyright © 2018 La Poste

5. REGLES OPERATIONNELLES DE SECURITE RELATIVES AU SERVICE DE SIGNATURE

5.1. CONTROLES DE SECURITE PHYSIQUE

5.1.1. Situation géographique et construction de sites

Les composantes du service sont hébergées dans des sites non susceptibles d'être menacés par des événements naturels.

5.1.2. Zonage des locaux

Les locaux d'exploitation du service sont découpés en zones concentriques d'accès contrôlés. Les équipements opérationnels contenant des clés de signature sont situés dans la zone réputée la plus sensible. L'accès à une zone de plus grande sensibilité ne peut se faire que par une zone de sensibilité immédiatement inférieure.

5.1.3. Accès physique

L'accès physique à chacune des composantes du service est protégé contre tout accès non autorisé.

En outre, l'accès physique aux dispositifs contenant les clés privées de signature fait l'objet d'une protection particulière. Un accès contrôlé renforcé est mis en place pour abriter :

- l'activité de gestion des clients et utilisateurs finaux,
- le cycle de vie des clés privées associées aux Services Électroniques de Confiance
- les opérations de signature,
- la génération et la signature des contremarques de temps, conformément à la [PH].

La sécurité est renforcée par la mise en œuvre de moyens de détection d'intrusion physique fonctionnant également en dehors des heures ouvrables.

5.1.4. Électricité et air conditionné

Les installations électriques et la climatisation des locaux d'exploitation sont conformes aux recommandations des fournisseurs de ces matériels de manière à garantir un bon fonctionnement des systèmes utilisés par le service de signature.

5.1.5. Dégâts des eaux

Les locaux d'exploitation sont équipés de système de protection contre les accidents de type dégâts des eaux afin d'assurer le bon fonctionnement des composantes du service de signature.

5.1.6. Prévention et protection contre le feu

Les composantes du service de signature sont hébergées dans des locaux protégés contre les incendies par un système de prévention et de protection adéquat.

Copyright © 2018 La Poste

5.1.7. Conservation des médias

Les media sont conservés dans des enceintes sécurisées dont l'accès est contrôlé.

En outre, les supports de stockage d'information utilisés par les systèmes du service de signature sont protégés contre les excès de :

- température,
- humidité,
- magnétisme.

5.1.8. Destruction des supports

Les systèmes du service de signature utilisent des mécanismes de destruction des supports papiers et des supports magnétiques. De plus, la réforme des matériels ayant appartenu aux plates-formes du service de signature assure que les informations qu'elles contiennent sont non réutilisables.

5.1.9. Site de recouvrement

Les installations de sauvegarde à l'extérieur des locaux de La Poste affectées au service de signature offrent le même niveau de sécurité que les locaux principaux, dans le cadre du plan de secours et de continuité.

5.2. CONTROLES DE SECURITE ORGANISATIONNELLE

5.2.1. Rôles de confiance

Au sein de l'environnement des Services Électroniques de Confiance de La Poste les quatre rôles suivants sont définis :

- ingénieur système,
- administrateur,
- opérateur,
- responsable sécurité.

Les attributions associées à chacun de ces rôles sont décrites dans le tableau suivant :

Rôles	Attributions
Opérateur	Responsabilité des opérations. Exploitation des services délivrés. Initialisation des fonctions cryptographiques. Remontée des incidents de sécurité à l'administrateur.

Copyright © 2018 La Poste

Rôles	Attributions
Ingénieur système	Mise en route du système (initialisation). Configuration du système. Administration du système et du réseau. Maintenance du système. Remontée des incidents de sécurité à l'administrateur.
Administrateur	Mise en route (initialisation) des services La Poste. Responsabilité des services délivrés. Supervision des actions des opérateurs. Configuration des journaux. Remontée des incidents au responsable de sécurité.
Responsable sécurité	Contrôle de la sécurité physique et logique (gestion des contrôles d'accès physique, etc.). Participation à l'initialisation des fonctions cryptographiques. Mise en œuvre de la politique de sécurité. Analyse des journaux d'événements. Remontée des incidents à l'autorité de sécurité compétente.

5.2.2. Nombre de personnes requises pour les tâches sensibles

Il est préférable d'appliquer le principe fondamental de sécurité qui repose sur la séparation des pouvoirs, c'est-à-dire associer chacun des rôles à un exploitant distinct.

Cependant, en cas de manque de ressources humaines, plusieurs rôles peuvent être attribués à une même personne dans la mesure où cela ne dégrade pas la sécurité des services offerts.

En revanche, l'ensemble des tâches sensibles effectuées dans l'environnement du service de signature telles que les initialisations cryptographiques des équipements, nécessitent le concours d'au moins deux exploitants ;

- l'un, exécutant l'opération,
- l'autre, contrôlant son déroulement et son résultat.

Copyright © 2018 La Poste

De plus, quatre règles de sécurité sont à respecter :

1. Un ingénieur système ne peut être opérateur.
2. L'opérateur ne peut être responsable de sécurité.
3. L'opérateur ne peut être administrateur.
4. L'ingénieur système ne peut être administrateur.

Note : administrateur et responsable de sécurité peuvent être confondus.

5.2.3. Identification et authentification pour chaque rôle

Tous les membres du personnel intervenant sur le service de signature font vérifier leur identité et leurs autorisations avant :

- que leur nom ne soit ajouté à la liste de contrôle d'accès à l'emplacement de l'environnement de signature concerné ;
- que leur nom ne soit ajouté à la liste des personnes autorisées à accéder physiquement aux systèmes de l'environnement de signature concerné ;
- qu'un compte ne soit ouvert en leur nom dans les systèmes de l'environnement de signature concerné.

5.3. CONTROLE DU PERSONNEL

5.3.1. Passé professionnel, qualifications, expérience et exigences d'habilitations

L'embauche de tous les intervenants du service de signature fait l'objet de la signature d'un contrat de travail présentant ses attributions et comportant une clause de confidentialité avec leur employeur.

En outre, La Poste s'engage à ce que les compétences professionnelles de son personnel correspondent à leurs attributions.

Pour atteindre un niveau élevé, l'honnêteté des personnels de La Poste est prouvée par leur employeur par tous les moyens légaux disponibles.

5.3.2. Procédures de contrôle du passé professionnel

Le recrutement des employés fait l'objet d'une procédure de contrôle portant sur :

- le passé professionnel des personnels intervenant pour l'accomplissement des tâches associées à l'exploitation dans l'environnement de signature de La Poste
- l'honnêteté des personnels par tous les moyens légaux disponibles.

5.3.3. Exigences de formation

Le personnel d'exploitation est formé aux logiciels, matériels et procédures internes de fonctionnement de la composante pour laquelle il opère dans l'environnement du service de signature.

Copyright © 2018 La Poste

5.3.4. Fréquence des formations

Tout nouvel employé reçoit une formation initiale :

- au système,
- aux politiques de sécurité,
- au plan de secours,
- aux logiciels et opérations,

qu'il met en œuvre.

En outre, chaque employé assiste à une formation de « contrôle » régulièrement ainsi qu'après toute évolution importante du système.

5.3.5. Gestion des métiers

Les règles de gestion de carrière de chacune des professions au sein du service de signature sont celles de l'organisme employeur.

5.3.6. Sanctions pour des actions non autorisées

La Poste décide des sanctions prévues à l'encontre d'un opérateur technique abusant de ses droits ou effectuant une opération non conforme à ses attributions. Pour sanctionner, La Poste met en œuvre les pénalités stipulées dans le contrat qui la lie à cet opérateur.

5.3.7. Contrôle des personnels contractants

Le personnel contractant suit les mêmes règles que celles énoncées dans tout le paragraphe 5.3. Ces règles sont applicables par l'ensemble du personnel de l'environnement du service de signature.

5.3.8. Documentation fournie au personnel

Le personnel dispose de l'ensemble des documents comportant des éléments de sécurité relatifs à ses activités. Cela inclut entre autres :

- le présent document
- les procédures internes de fonctionnement
- les documents constructeurs des matériels et logiciels utilisés.

5.4. SYNCHRONISATION DU SERVICE DE SIGNATURE

Le service de signature maîtrise les écarts entre l'heure de son système et l'heure UTC via 4 sources de références de type GPS, RADIO et 30 sources IP de Stratum 1.

Copyright © 2018 La Poste

5.5. JOURNALISATION DES EVENEMENTS

5.5.1. Objectifs

La journalisation des événements concerne tous les événements ayant trait à la sécurité des systèmes informatiques utilisés. Elle permet de garantir l'imputabilité, la traçabilité et l'auditabilité de toutes les actions réalisées sur ou par le service de signature. Elle permet, en outre, de collecter des preuves et de détecter des anomalies.

À cet effet, les journaux contiennent notamment la trace des demandes de signature et la trace des réponses à ces requêtes.

5.5.2. Politiques de journalisation

Les politiques de journalisation abordent notamment les thèmes suivants :

- Événements enregistrés.
- Contenu des événements enregistrés.
- Support des enregistrements (document papier, journaux informatiques...)
- Fréquence d'exploitation des journaux.
- Durée de conservation.
- Protection des journaux.
- Processus de remontée d'alerte.

5.5.3. Processus de journalisation

Le processus de journalisation est effectué en tâche de fond, et garantit un enregistrement immédiat des opérations effectuées.

5.5.4. Conservation des journaux

Les journaux sont périodiquement sauvegardés selon les modalités définies dans la politique de sauvegarde (cf. paragraphe 5.6).

5.5.5. Protection des journaux d'événements

L'écriture dans les journaux d'événements est conditionnée par des contrôles de droits d'accès. Par ailleurs, les enregistrements ne sont pas modifiables *a posteriori*

Les journaux d'événements du service de signature sont protégés en confidentialité, en intégrité, en disponibilité (sauvegardes), et font l'objet de règles d'exploitation strictes.

5.5.6. Système de collecte des journaux d'événements

La collecte des journaux commence au démarrage du service de signature et se termine à l'arrêt de celui-ci.

5.5.7. Imputabilité

L'imputabilité d'une action revient à la personne ou au système l'ayant exécutée et dont l'identifiant doit être inscrit dans les journaux d'événements.

Copyright © 2018 La Poste

5.5.8. Anomalies et audits

La Poste est attentive à toute violation de l'intégrité du service de signature, y compris :

- les équipements physiques,
- l'environnement d'exploitation,
- le personnel.

Les journaux d'événements sont contrôlés pour identifier des anomalies liées à des tentatives en échec.

5.6. POLITIQUE DE SAUVEGARDE

5.6.1. Types de données sauvegardées

Les données sauvegardées sont au moins les suivantes :

- les fichiers de configuration du service de signature
- les journaux du service de signature
- le contenu des bases de données sur lesquelles s'appuie le service de signature

5.6.2. Fréquence des sauvegardes

Les fréquences des sauvegardes incrémentales et complètes sont définies dans la politique de sauvegarde.

5.6.3. Période de rétention des sauvegardes

Les données sauvegardées sont conservées pendant au moins six (6) mois.

5.6.4. Protection des sauvegardes

Pendant toute la durée de leur conservation les sauvegardes :

- sont protégées en intégrité,
- sont disponibles pour les personnes habilitées,
- peuvent être relues et exploitées.

5.6.5. Procédure de sauvegarde

La procédure de sauvegarde n'est pas publique.

Copyright © 2018 La Poste

5.7. ARCHIVAGE SECURISE

5.7.1. Types de données à archiver

Les données archivées sont au moins les suivantes :

- les documents contractuels,
- les traces des requêtes de signature et les traces des réponses,
- les différentes versions des PS,
- les journaux d'événements du service de signature
- les fichiers de configuration du service de signature
- Les certificats de signature

5.7.2. Durée de conservation des archives

Les requêtes de signature et les réponses sont conservées pendant au minimum cinq (5) ans.

5.7.3. Protection des archives

Pendant toute la durée de leur conservation les archives :

- sont protégées en intégrité,
- sont disponibles pour les personnes habilitées,
- peuvent être relues et exploitées.

5.7.4. Horodatage des archives

Les enregistrements des archives (numériques) sont horodatés avec l'heure de référence du service de signature.

5.7.5. Système de collecte des archives

Le système de collecte des archives est décrit dans la documentation interne de La Poste et de ses sous-traitants éventuels.

5.7.6. Procédures de restitution des archives

L'accès aux archives fait l'objet d'une demande auprès de La Poste.

5.8. CONTROLES TECHNIQUES DU SYSTEME DURANT SON CYCLE DE VIE

5.8.1. Contrôles de la gestion de la sécurité

La traçabilité et l'imputabilité de toutes les actions réalisées sur le service de signature sont assurées notamment par l'enregistrement des actions et événements liés à l'exploitation et à l'utilisation des services de signature (cf. 5.5).

Il appartient par ailleurs à l'Application Utilisatrice d'assurer les contrôles nécessaires à la gestion de la sécurité de sa plate-forme technique.

Copyright © 2018 La Poste

5.8.2. Contrôles de la sécurité logicielle du système durant son cycle de vie

Les logiciels utilisés pour la mise en œuvre du service de signature subissent un audit régulier de contrôle de sécurité logicielle.

5.8.3. Contrôles de la sécurité réseau

Le réseau interne du service de signature est protégé suivant les règles de l'art contre les accès extérieurs non autorisés, notamment par l'installation de dispositifs de sécurité de type pare-feu.

5.9. CAS DE SINISTRE, DE COMPROMISSION, OU DE FIN DU SERVICE DE SIGNATURE

En cas d'événement affectant la sécurité des services de signature, comme la compromission des clés privées, La Poste s'assure que l'information appropriée est fournie aux entités responsables des services demandeurs.

Les thèmes suivants sont traités dans les procédures de sécurité :

- Compromission ou corruption des ressources informatiques, logicielles et/ou des données.
- Corruption des ressources cryptographiques du service de signature.
- Révocation du certificat d'authentification ou de signature dans les cas suivants :
    - forte suspicion de compromission ou compromission avérée de la clé privée,
    - vol, destruction ou perte de la clé privée,
    - vol, destruction totale ou partielle de son support de stockage,
    - les contrats ou agréments applicables sont dénoncés, périmés, ou nuls,
    - révocation du certificat d'une AC supérieure (émettrice, intermédiaire ou racine),
    - cessation d'activité de l'entité qui opère le service de signature
- Spécificités de la révocation pour cause de compromission de la clé privée d'une composante de l'infrastructure.

5.10. CESSATION OU TRANSFERT D'ACTIVITE DU SERVICE DE SIGNATURE

En cas de transfert ou de cessation d'activité du service de signature, La Poste :

- prévient tous les Clients et partenaires concernés, par un moyen à sa discrétion
- révoque ou fait révoquer les certificats du service de signature et détruit les clés privées d'authentification et de signature.

Copyright © 2018 La Poste

Avant de fermer ses services, La Poste applique les procédures suivantes :

- Rendre disponible aux entités responsables des services demandeurs toute modalité concernant la fin de ses activités (date prévue de fin d'activité, etc.).
- Les autorisations données aux sous-traitants intervenant dans le processus de signature sont révoquées.
- Prendre les mesures nécessaires afin de :
  - soit continuer à assurer les fonctions de vérification de signature
  - soit transférer contractuellement les fonctions permettant cette vérification

La Poste prend les dispositions financières permettant de couvrir les frais relatifs à ces exigences

Copyright © 2018 La Poste

6. REGLES TECHNIQUES DE SECURITE

6.1. GENERATION ET INSTALLATION DES BI-CLES

6.1.1. Génération et support des bi-clés

6.1.1.1. Concernant les clés de l'Autorité de Signature

Les clés privées de signature du service sont générées, opérées et stockées sur un dispositif cryptographique matériel (HSM, soit *Hardware Security Module*, ou module de sécurité matériel).

La clé privée d'authentification est générée, opérée et stockée sur un dispositif cryptographique logiciel.

Par ailleurs, la génération, le clonage (copie de sauvegarde) et la certification des clés font l'objet d'une sécurité organisationnelle rigoureuse, formalisée dans des procédures de *Key Ceremony*.

6.1.1.2. Concernant les clés des Applications Utilisatrices

Il appartient à l'Application Utilisatrice de générer ou obtenir, et protéger sa clé privée d'authentification par des mécanismes de sécurité adaptés.

6.1.2. Transmission de la clé publique d'une Application Utilisatrice au service de signature

Cette transmission est effectuée par un moyen quelconque ; la validation de la clé publique transmise est effectuée durant les tests de qualification réalisés entre le client et le service.

6.1.3. Transmission des clés publiques du service de signature aux Applications Utilisatrices

Le moyen mis en œuvre doit assurer l'authentification de l'expéditeur. Il peut s'agir par exemple d'une remise en main propre, d'un transfert par messagerie sécurisée ou de tout autre moyen permettant l'authentification de l'expéditeur.

6.1.4. Algorithmes et tailles de clé

Les clés associées aux certificats d'authentification sont des clés RSA de 2048 bits.

Les clés associées aux certificats de signature sont des clés RSA de 2048 bits.

6.1.5. Usage de la clé publique

Les champs *keyUsage* et *extendedKeyUsage* des certificats du service de signature stipulent les usages auxquels chaque certificat (authentification et signature) est réservé.

Copyright © 2018 La Poste

6.2. PROTECTION DE LA CLE PRIVEE

6.2.1. Normes pour les modules cryptographiques

Les modules cryptographiques utilisés pour la génération, l'opération et le stockage des clés privées de signature du service ont été évalués EAL 4+ *Common Criteria.*

Les clés privées d'authentification étant stockées sur support logiciel, l'évaluation d'un module cryptographique les concernant est sans objet.

6.2.2. Activation des clés privées de signature

Un contrôle de type « *2 sur 2* » est mis en œuvre sur les clés privées de signature du service.

6.2.3. Protection des clés privées d'authentification

Les clés privées d'authentification sont du service sont gérées en conformité avec la PSSI de La Poste.

6.2.4. Séquestre de clé privée

Les clés privées du service de signature ne sont pas utilisées à des fins de confidentialité et ne font donc pas l'objet d'un séquestre.

6.2.5. Sauvegarde de clé privée

Les clés privées du service de signature sont dupliquées pour garantir une restauration du service dans les meilleurs délais et la (ou les) copie(s) sont stockées avec un niveau de sécurité au moins équivalent à celui utilisé pour le stockage des clés en production.

6.2.6. Archivage de clé privée

Les clés privées du service ne sont pas et ne doivent pas être archivées.

6.2.7. Méthodes de destruction de clé privée

Les clés privées du service de signature sont détruites à la fin de leur période d'utilisation, cf. le paragraphe 6.3.2 à ce sujet.

6.3. AUTRES ASPECTS DE LA GESTION DES BI-CLES

6.3.1. Archivage des clés publiques

Les clés publiques de signature et les certificats associés sont archivés durant trois (3) ans après la fin d'utilisation de la clé privée.

Copyright © 2018 La Poste

6.3.2. Durée de vie des certificats et des clés privées

6.3.2.1. Certificats de signature

La durée de vie des certificats de signature est donnée au paragraphe 4.6.

Remarque : l'utilisation de la clé privée associée est plus réduite (cf. paragraphe 4.6).

6.3.2.2. Certificats d'authentification

La durée de vie des clés privées d'authentification et des certificats associés est de 2 ans.

Copyright © 2018 La Poste

7. DISPOSITIONS JURIDIQUES

7.1. DROIT APPLICABLE

Le présent document est régi par la loi française.

7.2. REGLEMENT DES DIFFERENDS

Toutes contestations et litiges survenant dans l'interprétation et la mise en œuvre du présent document seront soumis à la juridiction des tribunaux de Paris.

7.3. DONNEES NOMINATIVES

En conformité avec les dispositions de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, le traitement automatisé des données nominatives réalisé par les services électroniques de confiance ont fait l'objet d'une déclaration auprès de la Commission Nationale de l'Informatique et des Libertés (CNIL).

Le signataire est informé qu'il dispose d'un droit d'accès, de rectification et d'opposition portant sur les données le concernant en écrivant à La Poste.

7.4. POLITIQUE DE CONFIDENTIALITE

7.4.1. Informations échangées entre les parties

Sans objet.

7.4.2. Informations propres à l'infrastructure

Les informations suivantes sont considérées comme confidentielles :

- les clés privées du service de signature, et leurs données d'activation,
- les journaux d'événements, sauvegardes et archives du service de signature,
- les rapports d'audit,
- l'architecture réseau supportant le service de signature.

Cette liste n'est pas exhaustive. La protection de ces informations fait l'objet de mesures documentées.

7.5. DROITS DE PROPRIETE INTELLECTUELLE

Voir p. 6.

Copyright © 2018 La Poste