LA POSTE

Direction de l'Innovation et du Développement des E-services

SERVICES ELECTRONIQUES DE CONFIANCE

Service de Cachet Electronique de La Poste

POLITIQUE DE VALIDATION DE SIGNATURE

Version 1.0
Date version : 16 Mars 2006
Identification du document : 1.2.250.1.8.1.1.3.1.3.1

SOMMAIRE

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.

1. INTRODUCTION

Ce document constitue la Politique de Validation de Signature inhérente à l'Autorité de Validation de Signature de La Poste. Il y sera fait référence, dans la suite de ce document, sous le nom « Politique de Validation de Signature » (PVS).

1.1. PORTEE DE LA POLITIQUE DE VALIDATION DE SIGNATURE

La Politique de Validation de Signature objet du présent document s'applique sur un service offert par La Poste dans le cadre de l'offre Cachet Electronique de La Poste. Les services de Validation de Signature sont utilisés par les applications utilisatrices via le protocole défini par la norme [S43] référencée en 1.10. Les conditions de mise en œuvre du service sont définies dans le document [CGS] référencé en 1.10.

1.2. PRESENTATION GENERALE

Une Politique de Validation 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 vérification de la validité des signatures électroniques.

Une PVS est définie indépendamment des modalités de mise en œuvre des composants auxquels est s'applique. Les procédures décrivant comment les exigences de la PVS sont atteintes en pratique sont détaillées dans un document appelé Déclaration des Pratiques de Validation de Signature (DPVS).

1.3. IDENTIFICATION

L'OID de cette Politique de Validation de Signature est :

> {iso(1) member-body(2) france(250) type-org(1) la poste(8) courrier-services electroniques de confiance (1) Services de Cachet Electronique(1) document(3) politique (1) pvs (3) version (1)}
>
> Soit : 1.2.250.1.8.1.1.3.1.3.1.

La Déclaration des Pratiques de Validation de Signature correspondante est référencée par l'OID :

> {iso(1) member-body(2) france(250) type-org(1) la poste(8) courrier-services electroniques de confiance (1) Services de Cachet Electronique(1) document(3) déclaration (2) dpvs (3) version (1)}
>
> 1.2.250.1.8.1.1.3.2.3.1.

Cette Politique de Validation de Signature définit une unique classe de service baptisée « classe de service Signature standard » par l'OID :

> {iso(1) member-body(2) france(250) type-org(1) la poste(8) courrier-services electroniques de confiance (1) Services de Cachet Electronique(1) document(3) classe de service (3) signature standard (1) version (1)}
>
> 1.2.250.1.8.1.1.3.3.1.1

1.4. LISTE DES ACRONYMES UTILISES

Acronyme	Signification
AC	Autorité de Certification
AVS	Autorité de Validation de Signature
AVT	Autorité de Validation Technique
CAP	Commission d'Approbation des Politiques
CRL	*Certificate Revocation List*, ou LCR
DPVS	Déclaration des Pratiques de Validation de Signature.
S43	Norme du Cachet Postal Electronique définie par l'UPU, Universal Postal Union
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
PVS	Politique de Validation de Signature
UTC	*Coordinated Universal Time*

1.5. DEFINITIONS

- **Application Utilisatrice** : processus automatique (« applicatif ») demandeur d'une validation de signature.

- **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.).

- **Autorité de Validation de Signature (AVS)** : composante de l'infrastructure de La Poste à qui un Utilisateur peut déléguer la validation des certificats qui lui sont présentés. Il incombe alors à l'Autorité de Validation de Signature de prendre en charge l'ensemble des vérifications permettant de déterminer si l'accepteur peut ou non se fier au certificat ou à la signature qui lui est présenté(e).

- **Autorité de Validation Technique (AVT)** : il s'agit de la composante technique de l'Autorité de Validation.

- **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.

- **Certificats acceptées (famille de)** : famille de certificats numériques concernée par la présente Politique de Validation de Signature.

- **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.

- **Classe de service** : catégorie de l'offre de service de l'Autorité de Validation de Signature, désignée par un OID spécifique, et caractérisée notamment par le type et le niveau de garantie proposés.

- **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 incluant la Politique de Validation 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 PVS.

- **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.

- **Déclaration des Pratiques de Validation de Signature (DPVS)** : énoncé des procédures et pratiques appliquées par l'AVS pour mettre en œuvre la PVS.

- **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.

- **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 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 certificats numériques et/ou des signatures électroniques.

- **Porteur (de certificat)** : personne physique titulaire 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 titulaire 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)** : protocole de sécurisation couramment utilisé sur Internet (notamment pour sécuriser HTTP). SSL (comme son successeur TLS) offre notamment des services d'authentification, d'intégrité, et de confidentialité.

- **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** : une 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).

- **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)** : cf. *Secure Socket Layer*.

- **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 titulaire de certificat ne sont pas forcément mutuellement exclusives : une application pourra éventuellement dans le même temps être Utilisatrice et titulaire de certificat.

  La Figure 1 représente la relation entre porteur de certificat, utilisateur, et Autorité de Validation de Signature.

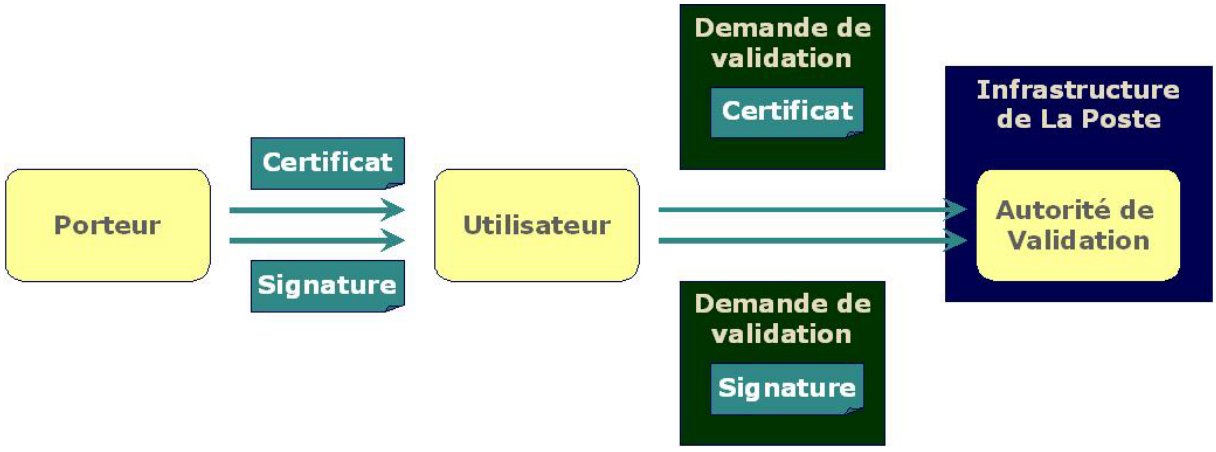

Figure 1: Fonctionnement de l'infrastructure de validation

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.

- **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.

1.6. GAMMES DE CERTIFICATS CONCERNEES PAR LA POLITIQUE DE VALIDATION DE SIGNATURE

Le service de signature électronique fournit les mécanismes et les dispositifs cryptographiques utilisés par certains Services Électroniques de Confiance de La Poste.

Trois types de signature électronique peuvent être distingués dans le cadre des Services Électroniques de Confiance de La Poste :

- La signature des contremarques de temps : il s'agit de la signature apposée par l'Autorité d'Horodatage sur une marque de temps ainsi que sur les éléments de preuve associés. Les exigences relatives à ce type de signature sont décrites dans la Politique d'Horodatage de La Poste.

- La signature des éléments de preuve de La Poste (attestations électroniques, cachets électroniques de La Poste) : il s'agit de la signature apposée par La Poste sur les données des éléments de preuve délivrés aux clients. Ce processus est toujours réalisé sous la responsabilité de La Poste qui peut le sous-traiter auprès d'opérateurs techniques.

- La signature électronique présentée par un client des Services Électroniques de Confiance.

Dans tous les cas de figure, les éléments de preuve électroniques et les contremarques de temps de La Poste comportent des signatures électroniques produites avec des clés privées de signature appartenant à La Poste. Les parties publiques des bi-clés correspondantes sont certifiées par une AC choisie par La Poste en fonction de critères et spécifications techniques qui sont périodiquement audités par la Commission d'Approbation des Politiques de La Poste.

Les signatures électroniques des clients des Services Electroniques de Confiance de La Poste sont associées à des certificats émis par des AC tierces. La Poste ne contrôle la validité de telles signatures que si elles sont produites à l'aide de clés privées associées à des certificats émis par des AC prises en compte par La Poste (cf. chapitre 2.1.1).

1.7. APPLICATIONS UTILISATRICES DU SERVICE DE VALIDATION DE SIGNATURE

Seules les requêtes émises par les Applications Utilisatrices ayant suivi le processus de souscription au service décrit au chapitre 4 sont acceptées par l'AVT.

1.8. MODIFICATIONS ET APPLICATION DE LA POLITIQUE DE VALIDATION DE SIGNATURE

Cette Politique de Validation de Signature sera revue périodiquement par l'Autorité de Validation de Signature, notamment pour :

- mettre à jour la liste des gammes de certificats concernées par la Politique de Validation de Signature,
- s'adapter aux évolutions technologiques.

La périodicité maximale de révision de cette Politique de Validation de Signature est de trois (3) ans.

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

Version	Date	Principaux points de modification
1.0	16 Mars 2006	Création

Tableau 1: Historique de la Politique de Validation de Signature

La présente version de la Politique de Validation de Signature s'applique à l'ensemble des opérations de validation effectuées sur une signature pour le compte d'une Application Utilisatrice (cf. paragraphe 1.7) à compter de la date notifiée aux clients ayant souscrit au service.

1.9. COORDONNEES DES ENTITES RESPONSABLES DE LA POLITIQUE DE VALIDATION DE SIGNATURE

1.9.1. Organisme responsable

L'organisme responsable de cette Politique de Validation de Signature est la CAP (Commission d'Approbation des Politiques).

1.9.2. Personne physique responsable

La personne physique responsable de la présente Politique de Validation de Signature est :

Le président de la CAP

1.9.3. Entité déterminant la conformité de la Déclaration des Pratiques de Validation de Signature à la Politique de Validation de Signature

La conformité de la Déclaration des Pratiques de Validation de Signature à la Politique de Validation de Signature est à la charge de la CAP, sous la responsabilité de :

Le président de la CAP

1.10. REFERENCES

- [CGS] Convention de Service du Cachet Electronique de La Poste.
- [S43] Norme S43 du Cachet Postal Electronique définie par l'UPU, Universal Postal Union, v1.15
- [PH] Politique d'Horodatage de La Poste.
- [PSign] Politique de Signature de La Poste.

2. DISPOSITIONS DE PORTEE GENERALE

2.1. INTERVENANTS ET ROLES

2.1.1. Autorités de Certification prises en compte

Le service de Validation de Signature s'applique sur les signatures réalisées par les familles de Certificats acceptées par La Poste. Les ACs concernées opèrent pour le compte de leur clients un service d'émission de certificats garantissant l'identité de leur Porteur (indépendamment de l'usage du certificat : authentification, signature, etc.). En tant qu'Autorité de Certification, il incombe notamment à l'AC :

- d'émettre, à la demande de ses clients, des certificats d'identité aux porteurs qui lui sont désignés ;
- de révoquer sans délai les certificats sur la demande de leur porteur ou dès lors qu'un élément le justifie ;
- de publier les informations de révocation à destination de l'Autorité de Validation de Signature.

2.1.2. Autorité de Validation de Signature

L'Autorité de Validation de Signature distribue et opère pour le compte de ses clients un service de validation de signatures. Ce service fait l'objet de la présente Politique.

L'Autorité de Validation de Signature porte la responsabilité des opérations qu'elle réalise vis-à-vis de ses clients Applications Utilisatrices. Elle est notamment l'interlocuteur unique d'une Application Utilisatrice pour résoudre tout litige né de l'utilisation du service de validation.

Les opérations techniques nécessaires à la vérification de la fiabilité d'un certificat ou d'une signature sont assurées par l'Autorité de Validation Technique (AVT). L'Autorité de Validation de Signature s'engage notamment sur la valeur des réponses que l'AVT fournit.

2.1.3. Applications utilisatrices du service de validation de signature

L'Application Utilisatrice offre, ou utilise, des services en ligne sécurisés à l'aide de certificats et/ou de signatures numériques. Pour savoir si elle peut raisonnablement se fier aux certificats qui lui sont présentés, elle a souscrit au service de validation distribué par l'AVS.

2.2. OBLIGATIONS

2.2.1. Obligations incombant à l'Autorité de Validation de Signature

L'Autorité de Validation de Signature s'oblige à :

- opérer une Autorité de Validation 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 et dans la DPVS,
- maintenir un niveau de qualité de service tel que stipulé au paragraphe 3.6,
- garantir la confidentialité des informations qu'elle détient conformément aux dispositions du paragraphe 2.8.

2.2.2. Obligations incombant aux Autorités de Certification

Aucune obligation n'incombe aux Autorités de Certification acceptées au regard de la présente Politique de Validation de Signature : l'Autorité de Validation de Signature est seule responsable de la validité des signatures déclarées valides par l'AVT.

2.2.3. Obligations incombant aux applications utilisatrices du service de validation de signature

Il incombe à l'Application Utilisatrice :

- d'interroger l'AVT selon les moyens d'accès définis dans [CGS],
- 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 l'AVT,
- de mettre en œuvre des moyens adaptés au niveau de risque pour sécuriser sa propre plate-forme technique,

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 et/ou le bon fonctionnement de ces mêmes services, l'AVS réalise des tests de qualification avec les plates-formes opérationnelles de l'Application Utilisatrice avant la connexion à l'AVT (cf. [CGS]).

L'Application Utilisatrice et ses représentants sont seuls responsables de l'utilisation qu'ils font du service de validation et de la non compromission des clés privées leur permettant de s'authentifier auprès de l'AVT. 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 validation,
- de mauvaise utilisation ou compromission des certificats leur permettant de s'authentifier auprès de l'AVT,
- de décision de leur part de se fier à une signature pour laquelle l'AVT a fourni une réponse autre que « Valide ».

2.3. UTILISATION HORS DU CADRE DE LA POLITIQUE DE VALIDATION DE SIGNATURE

L'Autorité de Validation de Signature ne saurait être tenue pour responsable en cas de litige lié à une utilisation des services offerts par l'AVT non normée par la présente Politique de Validation de Signature.

De la même façon, l'AVS n'est pas responsable de la nature des engagements associés à la Signature électronique, des conditions de production et d'utilisation de la Signature électronique.

2.4. RESPECT ET INTERPRETATION DES DISPOSITIONS JURIDIQUES

Voir [CGS].

2.5. PUBLICATION ET DEPOT D'INFORMATIONS

Voir [CGS]

2.6. TARIFS

Voir [CGS]

2.7. AUDITS DE CONFORMITE ET AUTRES CONTROLES

Les mesures de contrôle décrites dans le présent paragraphe s'appliquent aux composants du service de validation sur lesquels La Poste s'appuie dans le cadre de la fourniture des Services Électroniques de Confiance. Les contrôles de conformité sont réalisés annuellement. Ils visent à s'assurer du respect des pratiques énoncées dans la DPVS. La CAP de La Poste désignera 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.

2.8. POLITIQUE DE CONFIDENTIALITE

2.8.1. Informations échangées entre les parties

Voir [CGS]

2.8.2. Informations propres à l'infrastructure

Les informations suivantes sont considérées comme confidentielles :

- les clés privées de l'AVT, et leurs données d'activation,
- les journaux d'événements, sauvegardes et archives de l'Autorité de Validation de Signature,
- les rapports d'audit,
- la Déclaration des Pratiques de Validation de Signature,
- l'architecture réseau supportant l'AVT.

Cette liste n'est pas exhaustive. La protection de ces informations fait l'objet de mesures documentées. Des précisions sont indiquées dans la DPVS.

2.9. DROITS DE PROPRIETE INTELLECTUELLE

Voir [CGS]

3. DESCRIPTION DU SERVICE

3.1. DESCRIPTION GENERALE DU SERVICE

L'AVT offre un service de validation de signature

Ce service est mis à disposition des applications utilisatrices au travers du service de Cachet Electronique de La Poste. Les moyens d'accès au service du Cachet électronique de La Poste sont précisés dans [CGS].

Les données d'entrée et de sortie de cette interface sont indiquées dans la partie 7.

Une transaction de validation ne peut avoir que l'un des résultats suivants :

- Valide
- Valide avec avertissement
- Erreur : cette réponse traduit la non validité de la signature ou une impossibilité de mener à bien l'opération de vérification. Un code erreur indique la nature précise de la réponse.

Remarque importante : une réponse de validité ou de non validité constitue un engagement de la part de l'Autorité de Validation de Signature sur le statut de la signature soumise pour validation (cf. paragraphe 3.5 et à ce sujet). En revanche, toute autre réponse, est significative d'une absence de garantie, l'Application Utilisatrice étant alors libre de se fier à une signature selon sa politique de gestion des risques.

3.2. SECURITE DU CANAL D'INTERROGATION DE L'AUTORITE DE VALIDATION DE SIGNATURE TECHNIQUE

Le service de validation de signature est mis à disposition des Applications Utilisatrices au travers du service de Cachet Electronique de La Poste. Les moyens d'accès au service du Cachet Electronique de La Poste sont précisés dans [CGS].

Ces moyens d'accès permettent de satisfaire aux exigences précisées ci-après.

Toute transaction de validation s'effectue via un canal chiffré avec authentification mutuelle des parties.

Sont considérées comme critiques :

- l'authentification de l'AVT (le caractère non répudiable des réponses de validation),
- l'intégrité des données échangées,
- la disponibilité du service.

Sont considérées comme sensibles :

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

L'AVT s'authentifie fortement, 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.

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 authentifiants sont exprimées dans la partie 6.

La confidentialité des informations lors des échanges est assurée par des algorithmes de chiffrement dont la robustesse répond aux règles de l'art.

3.3. HORODATAGE

Dans le cadre du service de Cachet Electronique de La Poste, l'application utilisatrice peut demander ou non la signature de la réponse de validation de signature. Si l'application utilisatrice a fait la demande de signature de la réponse de Validation, c'est la date et l'heure de l'Autorité d'Horodatage de La Poste qui est utilisée comme heure de référence de la vérification.

Dans le cas où cette valeur serait perdue ou inexploitable, la date et l'heure qui font foi sont extraites des journaux d'événements de l'AVT, alors utilisés comme « **traces de temps** ». C'est l'heure de l'AVT qui est utilisée comme heure de référence pour les journaux d'événements.

3.4. CONVENTION DE PREUVE

L'Application Utilisatrice et l'Autorité de Validation 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 validation** :

- Seules les traces de l'AVT font foi pour connaître les volumes d'utilisation du service par les Applications Utilisatrices (les demandes de validation sont authentifiées, notamment pour permettre la facturation du service).
- Si les réponses de Validation sont signées, suite à une demande explicite de l'Application Utilisatrice dans sa requête, cette signature manifeste l'engagement de l'Autorité de Validation de Signature sur la réponse et peut être opposée à l'Autorité de Validation de Signature en cas de litige portant sur la qualité d'une signature. Une réponse « Signature Valide » a valeur de preuve de la garantie portée par l'Autorité de Validation de Signature sur une signature, à une date donnée (celle indiquée dans la signature de la réponse).

- L'AVT s'engage sur la possibilité de vérifier la signature apposées sur ses réponses de validation pendant la durée de vie du certificat de l'AVT.

- Au-delà de cette période et en dernier recours, lorsque la signature des réponses de Validation est devenue obsolète ou si elle ne peut être exhibée dans sa totale intégrité, les traces conservées par l'AVT font foi pour résoudre tout litige portant sur la qualité d'une signature.

La garantie offerte par l'Autorité de Validation de Signature porte sur la validité d'une signature à une date et heure données selon les règles définies au paragraphe « Conditions de validité d'une signature ». Lorsqu'une demande de signature de la vérification a été demandée, l'horloge faisant référence est celle de l'Autorité d'Horodatage de La Poste ; dans les autres cas c'est l'horloge de l'AVT. Les traces de l'AVT sont datées avec l'heure de l'AVT.

Remarque : il est à noter que les réponses de validation étant fournies de manière synchrone (en ligne), la vérification par l'Application Utilisatrice de la signature apposée sur les messages et de la date et heure de la réponse n'est pas requise. Il appartient à l'Application Utilisatrice de vérifier ou non ces éléments, sachant que le canal de transmission est authentifié et intègre.

3.5. CONDITIONS DE VALIDITE D'UNE SIGNATURE

3.5.1. Politique de Signature

L'ensemble des règles applicables pour la vérification des signatures est indiqué dans le présent document. Si une signature faisant référence à une Politique de Signature est soumise pour validation à l'AVT, cette dernière ignorera la référence et appliquera les règles définies pour la classe de service « Signature standard ».

De nouvelles classes de services pourront être définies sur décision de La Poste afin de prendre en compte des Politiques de Signature. Dans ce cas, les descriptions de ces classes de service préciseront quelles Politiques de Signature sont acceptées.

3.5.2. Règles pour la validation de signature pour la classe de service « Signature Standard »

3.5.2.1. Portée du service

L'Autorité de Validation de Signature s'engage à un résultat sur la qualité des signatures qu'elle valide. Ainsi, pour une réponse « valide» la portée de la garantie de l'Autorité de Validation de Signature se restreint à l'assertion suivante :

L'Autorité de Validation de Signature garantit que la signature qui fait l'objet de la requête a été effectuée à l'aide de la clé privée associée au certificat, et que ce dernier est valide.

Note : L'Autorité de Validation de Signature s'oblige à un résultat sur la qualité des réponses qu'elle fournit. La portée de cet engagement, dans le cas d'un certificat valide, se restreint à l'assertion suivante : l'**Autorité de Validation de Signature garantit l'intégrité et l'authenticité des informations contenues dans le certificat ayant fait l'objet de la requête, la nature des vérifications opérées sur le certificat est précisée au § 3.5.2.2**

La véracité de ces informations est garantie par l'AC (en particulier : l'identité du détenteur de la clé privée associée à la clé publique figurant dans le certificat est bien celle indiquée dans le champ *Subject* du certificat).

L'AVT assure la vérification de la signature à l'heure d'interrogation de l'AVT. Elle ne tient pas compte de la date de signature éventuellement attestée par une contremarque de temps.

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

- le certificat du signataire est valide (les réserves relatives à la validation des certificats, exprimées dans ce paragraphe dans la note ci-dessus, s'appliquent ici),
- le cryptogramme de signature est valide au regard des règles exprimées au paragraphe 3.5.2.3

Le service ne permet pas à ce jour la validation de signatures multiples (« parallèles » ou apposées l'une sur l'autre).

3.5.2.2. Validité du certificat du signataire

Le certificat du signataire doit vérifier les conditions exprimées dans la note du paragraphe 3.5.2. L'usage à considérer est pour une Signature Simple, *keyUsage* = *digitalSignature* ou *keyUsage* = *nonRepudiation*.

Note : la valeur du *keyUsage* indiqué dans le certificat doit autoriser au minimum ce type d'opération pour que le certificat puisse être considéré comme valide.

L'AVS propose deux niveaux de vérification du certificat :

- Le premier niveau de vérification est assuré dans tous les cas, il s'agit d'un contrôle de validité sur les points suivants :
  - Syntaxe correcte.
  - Vérification de la signature du certificat.
  - Chaîne de confiance
  - Date de début et de fin de validité du certificat. Le certificat doit être valide au moment de la vérification.
- Le second niveau de vérification est assuré sur demande de l'Application Utilisatrice et consiste en la vérification du statut de révocation du certificat, sous réserve que la date de vérification soit comprise entre les dates de début et de fin de validité du certificat.

3.5.2.3. Validité de la signature numérique

L'AVT n'autorise qu'un seul mode d'interrogation dit « mode complet », dans lequel les données envoyées à la plate-forme contiennent à la fois le document signé et la signature.

Les critères techniques de vérification de la validité de la signature sont décrits au paragraphe 8.1

Note : il appartient à l'Application Utilisatrice de comparer le document original et le document signé effectivement envoyé au service de validation de signature

3.5.2.3.1. Politique de Validation de Signature

La Politique de Validation de Signature s'articule autour des vérifications suivantes :

- Validité de la signature (cf. Chapitre Définitions)
- Validité du certificat (cf. Chapitre Définitions) si elle est demandée en paramètre de la requête.
- Correspondance entre les données passées en paramètre et la signature.

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

- Validité de la signature de la contremarque de temps.
- Validité du certificat de signature de la contremarque pour les ACs acceptées par La Poste.
- Correspondance entre la contremarque de temps et la signature sur laquelle elle porte.

3.6. QUALITE DE SERVICE

Voir [CGS].

4. BESOINS OPERATIONNELS LIES AU SERVICE

4.1. PROCESSUS DE SOUSCRIPTION AU SERVICE

Voir [CGS]

4.2. INSTALLATION DES CHAINES DE CERTIFICATION

L'AVT assure la mise en œuvre des chaînes de certification des familles de Certificats acceptées. La mise à jour est faite sur la base des informations communiquées par les ACs concernées.

4.3. SYNCHRONISATION DES APPLICATIONS UTILISATRICES AVEC L'INFRASTRUCTURE

Le [CGS] n'impose pas d'obligation. 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

Voir [CGS]

4.5. RENOUVELLEMENT DES CLES DE L'APPLICATION UTILISATRICE

Voir [CGS]

4.6. RENOUVELLEMENT DES CLES DE L'AUTORITE DE VALIDATION TECHNIQUE

L'AVT dispose de clés d'authentification (pour l'établissement du canal d'interrogation sécurisé) et de clés de signature (pour la signature des réponses de validation).

La politique de renouvellement des clés de signature est définie dans la Politique de Signature [PSign].

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

5. REGLES OPERATIONNELLES DE SECURITE RELATIVES A L'AUTORITE DE VALIDATION TECHNIQUE

5.1. CONTROLES DE SECURITE PHYSIQUE

5.1.1. Situation géographique et construction de sites

Les composantes de L'AVT sont hébergées dans des sites non susceptibles d'être menacés par des événements naturels.

5.1.2. Zonage des locaux

Les locaux d'exploitation de l'AVT 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 de l'AVT 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 et en particulier à l'AVT,
- la génération et la signature des attestations électroniques,
- la génération et la signature des contremarques de temps, conformément à la Politique d'Horodatage ([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 l'AVT.

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 de l'AVT.

5.1.6. Prévention et protection contre le feu

Les composantes de l'environnement de l'AVT sont hébergées dans des locaux protégés contre les incendies par un système de prévention et de protection adéquate.

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 de l'AVT sont protégés contre les excès de :

- température,
- humidité,
- magnétisme.

5.1.8. Destruction des supports

Les systèmes de l'AVT utilisent des mécanismes de destruction des supports papiers et des supports magnétiques. De plus, la réforme des matériels ayant appartenu aux plates-formes de l'AVT assure que les informations confidentielles 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 à l'environnement de l'AVT 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 :

- ingénieurs systèmes,
- administrateurs,
- opérateurs,
- responsables 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.
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 de l'AVT 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.

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

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 de l'environnement de l'AVT 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 chapitre 5.3. Ces règles sont applicables par l'ensemble du personnel de l'environnement de l'AVT.

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 et la DPVS associée ;
- les procédures internes de fonctionnement ;
- les documents constructeurs des matériels et logiciels utilisés.

5.4. SYNCHRONISATION DE L'AUTORITE DE VALIDATION TECHNIQUE

L'AVT maîtrise les écarts entre l'heure de son système et l'heure UTC.

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 l'AVT. 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 validation et la trace des réponses à ces requêtes.

5.5.2. Politiques de journalisation

Les dispositions relatives à la journalisation des événements sont différenciées par classe de service et par type d'événements. Les politiques de journalisation associées aux classes de service définies dans la présente PVS sont décrites précisément dans la DPVS et abordent notamment les thèmes suivants :

- Événements enregistrés.
- Contenu des événements enregistrés.
- Support des enregistrements (documents 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 DPVS et 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 de l'AVT sont protégés en confidentialité, en intégrité, en disponibilité (sauvegardes), et font l'objet de règles d'exploitation strictes.

Les mesures de protection des journaux d'événements sont décrites dans la DPVS.

5.5.6. Système de collecte des journaux d'événements

La collecte des journaux commence au démarrage de l'AVT, et se termine à l'arrêt de celle-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.

5.5.8. Anomalies et audits

L'Autorité de Validation de Signature est attentive à toute violation de l'intégrité de l'AVT, y compris :

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

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

5.6. POLITIQUE DE SAUVEGARDE

La politique de sauvegarde est définie dans la DPVS, en particulier :

- les types de données sauvegardées,
- la fréquence des sauvegardes,
- la période de rétention des sauvegardes,
- la protection des sauvegardes,
- la procédure de sauvegarde.

5.6.1. Types de données sauvegardées

Les données sauvegardées sont au moins les suivantes :

- les fichiers de configuration de l'AVT,
- les journaux de l'AVT,
- le contenu des bases de données sur lesquelles s'appuie l'AVT.

5.6.2. Fréquence des sauvegardes

Les fréquences des sauvegardes incrémentales et complètes sont définies dans la DPVS.

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 est décrite dans la DPVS.

5.7. ARCHIVAGE SECURISE

Voir [CGS]

5.7.1. Types de données à archiver

Les données archivées sont au moins les suivantes :

- les documents contractuels,
- les traces des requêtes et traces des réponses de validation,
- les différentes versions des PVS,
- les différentes versions des DPVS,
- les journaux d'événements de l'AVT,
- les fichiers de configuration de l'AVT.

5.7.2. Durée de conservation des archives

Les archives sont conservées 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 de l'AVT.

5.7.5. Système de collecte des archives

Le système de collecte des archives est décrit dans la DPVS.

5.7.6. Procédures de restitution des archives

La procédure est décrite dans la DPVS.

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 l'AVT sont assurées par des moyens décrits dans la DPVS.

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

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

Les logiciels utilisés pour la mise en œuvre de l'AVT subissent un audit régulier de contrôle de sécurité logicielle.

5.8.3. Contrôles de la sécurité réseau

Le réseau interne de l'AVT 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. Les moyens mis en œuvre sont documentés dans la DPVS.

5.8.4. Contrôles de la fabrication des modules cryptographiques

Des procédures, détaillées dans la DPVS, permettent de s'assurer de l'intégrité des modules cryptographiques matériels entre leur envoi par le fournisseur jusqu'à leur utilisation par l'AVT.

5.9. SITE DE SECOURS

Voir [CGS]

5.10. CAS DE SINISTRE, DE COMPROMISSION, OU DE FIN DE L'AUTORITE DE VALIDATION DE SIGNATURE

Les thèmes suivants sont traités dans la DPVS :

- Compromission ou corruption des ressources informatiques, logicielles et/ou des données.
- Corruption des ressources cryptographiques de l'AVT.

- Révocation du certificat d'authentification ou de signature de l'AVT, 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 l'AVT.
- Spécificités et impacts de la révocation pour cause de compromission de la clé privée d'une composante de l'infrastructure.

5.11. CESSATION OU TRANSFERT D'ACTIVITE DE L'ENTITE RESPONSABLE DE L'AUTORITE DE VALIDATION DE SIGNATURE

En cas de transfert ou de cessation d'activité de l'Autorité de Validation de Signature, cette dernière :

- prévient toutes les Applications Utilisatrices et partenaires concernés, par un moyen à sa discrétion .
- révoque le certificat de l'AVT, et détruit les clés privées d'authentification et de signature.

Les autres mesures prises en cas de cessation ou de transfert d'activité de l'Autorité de Validation de Signature sont décrites dans la DPVS, et notamment :

- la mise en œuvre de moyens adaptés pour permettre un éventuel recours juridique ultérieur.

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 Validation technique

Les clés privées de signature de l'AVT 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 générées, 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 référencées par la DPVS (procédures de *Key Ceremony*).

6.1.1.2. Concernant les clés des applications utilisatrices

Il appartient à l'Application Utilisatrice de générer/de récupérer et de protéger sa clé privée d'authentification par des mécanismes de sécurité adaptés (cf. [CGS]).

6.1.2. Transmission de la clé publique d'une application utilisatrice à l'Autorité de Validation Technique

Voir [CGS]

6.1.3. Transmission des clés publiques de l'Autorité de Validation Technique 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 et de signature sont des clés RSA de 1024 bits.

6.1.5. Usage de la clé publique

Les champs *keyUsage* et *Extended Keyusage* des certificats de l'AVT stipule les usages auxquels chaque certificat est réservé. Les clés d'authentification et de signature de l'AVT sont des clés séparées.

6.2. PROTECTION DE LA CLE PRIVEE

6.2.1. Protection de la clé privée de signature

Les informations relatives à la protection de la clé privée de signature sont précisées dans [PSign].

En particulier les informations concernant :

- les normes pour les modules cryptographiques,
- l'activation des clés privées,
- la sauvegarde de la clé privée,
- l'archivage de la clé privée,
- la méthode de destruction de la clé privée.

6.2.2. Protection de la clé privée d'authentification

Les informations relatives à la protection de la clé privée d'authentification sont précisées dans la DPVS.

6.3. AUTRES ASPECTS DE LA GESTION DES BI-CLES

Les informations concernant les bi-clés de signature telles que :

- archivage des clés publiques,
- durée de vie des certificats,

sont définies dans [PSign].

7. PROFIL DU PROTOCOLE D'INTERROGATION DE L'AUTORITE DE VALIDATION TECHNIQUE

Le service de validation de signature est mis à disposition des Applications Utilisatrices au travers du service de Cachet Electronique de La Poste. Les moyens d'accès au service du Cachet Electronique de La Poste sont précisés dans [CGS].

Les demandes de vérification de signature sont des requêtes S43 *VerifyRequest* (se reporter à [S43] pour le détail de ces requêtes).

8. CRITERES TECHNIQUES DE LA VERIFICATION DE LA VALIDITE DE LA SIGNATURE

8.1. CRITERES POUR LA CLASSE DE SERVICE « SIGNATURE STANDARD »

Ce paragraphe précise les protocoles et algorithmes supportés dans le cadre de la classe de service « signature standard ».

La vérification de signature porte sur des signatures au format PKCS#7/CMS attachées ou détachées.

Les algorithmes asymétriques reconnus par l'AVT pour ces signatures sont RSA et DSA, avec des longueurs de clés de 512, 1024 et 2048 bits.

Tels qu'indiqués dans rfc 3370 (Cryptographic Message Syntax (CMS) Algorithms), concernant RSA, il s'agit du format pkcs#1 V1.15, concernant DSA il s'agit du format FIPS 186.

Les algorithmes de hachage reconnus par l'AVT sont :

- SHA-1 pour un chiffrement avec DSA,
- MD5 et SHA-1 pour un chiffrement avec RSA.

Concernant les contremarques de temps incluses dans la signature, les formats supportés sont les suivants :

- RFC3161 draft 9
- RFC3161 final draft

9. ADMINISTRATION DES POLITIQUES

9.1. MODIFICATION DE LA POLITIQUE

Les modifications définitives ayant des impacts sensibles au niveau des Applications Utilisatrices leur sont présentées avant d'être publiées.

Les modifications des politiques sont diffusées, conformément aux chapitres 1.8 et 2.5.

L'organisme chargé de l'administration des spécifications et des politiques est la CAP (Commission d'Approbation des Procédures), dont les coordonnées figurent au chapitre 1.9. Toute modification est ordonnée et soumise à l'approbation de cette commission avant diffusion éventuelle (cf. chapitre 1.8). Les modalités du contrôle de conformité à la PVS sont précisées au chapitre 2.7.

9.2. CHANGEMENT DES COMPOSANTS DE L'AUTORITE DE VALIDATION TECHNIQUE

En cas de changement intervenant dans la composition de l'AVT, l'Autorité de Validation prévient les Applications Utilisatrices dans la mesure ou le service rendu est impacté.