Société Publique Locale Xdemat
Politique de signature

Date de rédaction	26 avril 2012
Statut du document	Approuvé par le directeur de la SPL
Identifiant	1.3.6.1.4.1.40075.1.2.1
Version	1.1
Date de validation	22 juin 2012

SOMMAIRE

1. INTRODUCTION

1.1. Présentation de l'offre de services

La Société Publique Locale (SPL) X-demat, propose des services destinés à encourager la dématérialisation des processus tout en garantissant la sécurisation des échanges.

Dans cette optique, la SPL X-demat propose un service de signature intégré aux services de dématérialisation.

1.2. Objet du document

La présente politique de signature décrit les règles auxquelles l'Autorité de signature doit se conformer pour créer et gérer des signatures électroniques et identifie les obligations et exigences portant sur les autres intervenants du dispositif de signature électronique.

La présente Politique de signature fait partie intégrante des termes des Conditions générales d'utilisation des services destinés à encourager la dématérialisation, fournis par la SPL Xdemat.

La signature électronique apposée sur un ensemble de données permet de garantir :

- l'identité du signataire,
- l'intégrité du document signé,
- le lien entre le document signé et la signature.

La signature électronique traduit ainsi la manifestation du consentement du signataire quant au contenu des données signées.

1.3. Définitions

Autorité de Certification (AC) - Autorité responsable de l'émission et la gestion des Certificats électroniques. Elle correspond à l'entité organisationnelle et technique qui reçoit les demandes de certificats, génère les certificats et les signe avec sa clé privée, selon les modalités définies dans une Politique de Certification.

Bi-clés - 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 électronique). 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 électronique - Fichier électronique attestant qu'une bi-clé appartient à la personne physique ou morale mentionnée dans le certificat. Il est géré par une Autorité de Certification. En signant le certificat, l'Autorité de certification valide le lien entre l'identité de la personne physique ou morale et la bi-clé. Le certificat est valide pendant une durée donnée précisée dans celui-ci.

Infrastructure de gestion de clés (IGC) – Ensemble de composantes, fonctions et procédures dédiées à la gestion de clés cryptographiques et de leurs certificats.

Object IDentifier (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 une Autorité de certification se conforme dans la mise en place et la fourniture des Certificats. Une Politique de certification peut également, si nécessaire, identifier les obligations et exigences portant sur les autres intervenants, notamment les Porteurs de certificats.

Politique d'Horodatage (PH) - Ensemble de règles définissant les exigences auxquelles une Autorité d'horodatage se conforme dans la mise en place et la fourniture des contremarques de temps. Une Politique d'horodatage peut également, si nécessaire, identifier les obligations et exigences portant sur les autres intervenants, notamment les abonnés et les utilisateurs de contremarques de temps.

Porteur (de certificat) - Personne physique titulaire d'un Certificat.

Signature électronique - Au plan juridique, l'article 1316-4 du Code Civil définit la signature électronique comme « l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache » : la signature identifie celui qui l'appose, et manifeste le consentement des parties aux obligations qui découlent de l'acte signé.

2. POLITIQUE DE SIGNATURE ELECTRONIQUE

2.1. Identification

La présente Politique de signature est identifiée par l'OID (Object Identifier) 1.3.6.1.4.1.40075.1.2.1

Cette référence doit figurer dans les données signées, conformément au paragraphe 6.2. de la présente Politique de signature afin d'attester du régime sous lequel est apposée la signature.

2.2. Elaboration de la Politique de signature

La présente Politique de signature est élaborée par la SPL X-demat.

2.3. Information des acteurs

La présente Politique est consultable à l'adresse suivante : http://www.spl-xdemat.fr/politiques/ps.php

2.4. Processus de mise à jour

La Politique de signature est maintenue à jour par la SPL X-demat.

2.4.1. Circonstances rendant une mise à jour nécessaire

La mise à jour de la présente Politique de signature peut avoir pour origines :

- l'évolution du droit,
- le besoin de s'adapter aux évolutions technologiques
- la mise à jour de la liste des certificats concernés par la présente politique de signature
- les observations des différents acteurs.

La périodicité minimale de révision de la présente politique de signature est fixée à 2 ans.

2.4.2. Prise en compte des remarques

Toutes les remarques concernant la présente Politique de signature sont à adresser par courriel à l'adresse : philippe.ricard@spl-xdemat.fr

Ces remarques seront examinées par la SPL X-demat qui engagera, si nécessaire, le processus de révision de la présente Politique de signature.

2.4.3. Information des acteurs

Un tableau tenu à jour et accessible et consultable à l'adresse suivante : http://www.spl-xdemat.fr/politiques/ps.php, recense les différentes versions et les principales modifications apportées, en comparaison à la version antérieure.

3. Le service de signature

Les utilisateurs de ce service de signature doivent être porteurs de :

- Certificats électroniques référencé PRIS V1, acquis auprès d'une Autorité de certification du marché
- Certificats électroniques référencés PRIS RGS, acquis auprès d'une Autorité de certification du marché
- Certificats électroniques dits internes émis par la SPL-Xdemat, dans le cadre de son infrastructure de gestion de clés

4. ACTEURS

4.1. L'Autorité de signature

L'Autorité de signature est responsable, vis-à-vis des utilisateurs, de l'ensemble des prestations rendues par les services de signature définis au paragraphe 1.1 de la présente Politique de signature.

Le rôle de l'Autorité de signature est de :

- vérifier la validité du Certificat électronique utilisé pour la signature,
- générer la signature électronique, selon les modalités définies dans la présente Politique de signature.

La fonction d'Autorité de signature est assurée par la SPL X-demat.

L'Autorité de signature peut déléguer tout ou partie de ces tâches à des prestataires de service en s'assurant de la conformité des services rendus par ces prestataires avec la présente Politique de signature.

4.2. L'Opérateur de signature

L'Autorité de signature a techniquement recours à un Opérateur de signature pour la mise en œuvre des prestations rendues par les services de signature définis au paragraphe 1.1 de la présente Politique de signature.

Le rôle de l'Opérateur de signature est de :

- fournir aux utilisateurs l'accès aux services de signature,
- s'assurer, le cas échéant, des moyens nécessaires à la protection des équipements fournissant les services de signature,
- s'assurer de la disponibilité des services de signature, en assurer le suivi et la surveillance.

La fonction d'Opérateur d'archivage est exercée par la SPL X-demat.

4.3. L'Autorité d'horodatage

L'Autorité d'horodatage assure les fonctions d'émission des contremarque de temps sur les données qui lui sont présentées afin d'attester de l'existence de ces données à la date de la contremarque de temps, selon les modalités définies dans une Politique d'horodatage.

Le rôle de l'Autorité d'horodatage est de :

- fournir une contremarque de temps à l'Autorité de signature, afin de disposer d'une date de référence pour l'opération de signature.

La fonction d'Autorité d'horodatage est assurée par le tiers horodateur Lex Personna

L'Autorité d'horodatage s'engage à informer sans délai l'Autorité de signature de toute modification de sa Politique d'horodatage ayant une incidence ou susceptible d'avoir une incidence sur les opérations de signature pratiquées en application de la présente Politique de signature.

4.4. Les utilisateurs

Les utilisateurs sont les porteurs de Certificats électroniques.

Le rôle des utilisateurs est de :

- contrôler les données avant d'y apposer leur signature,
- le cas échéant, s'assurer qu'ils sont en droit de signer, conformément à un arrêté de délégation de signature valide
- apposer leur signature.

4.5. Obligations juridiques communes

4.5.1. Secret professionnel et obligation de confidentialité

Dans la mesure où le champ d'application de la présente Politique de signature concerne à titre principal des opérations de nature confidentielle, chacun des acteurs s'engage à respecter le secret professionnel auquel il serait tenu en application des textes.

Il est rappelé que tout manquement à l'obligation de secret professionnel est susceptible de donner lieu à des sanctions pénales en vertu des dispositions de l'article 226-13 du code pénal.

Chaque acteur doit également s'assurer que les procédures et outils mis en place et utilisés par ses soins dans le cadre de la présente Politique de signature offrent des garanties suffisantes quant à la confidentialité des données traitées.

Chaque acteur s'engage à respecter les dispositions législatives et réglementaires dès lors qu'il a recours à des moyens ou prestations de cryptologie.

4.5.2. Protection des données à caractère personnel

Chaque acteur en sa qualité de responsable de traitement de données à caractère personnel au sens de la législation s'engage à respecter les dispositions législatives et réglementaires en vigueur en matière de protection des données à caractère personnel (à titre principal, cf. la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée et ses textes d'application).

4.5.3. Relation entre les utilisateurs et l'Autorité de Signature

Conformément à l'article 1316-2 du Code civil tel qu'introduit par la loi n° 2000-230 du 13 mars 2000, les acteurs s'engagent à admettre les clauses ci-après constitutives de la convention de preuve.

Les acteurs admettent la recevabilité et la force probante des données signées issues des services de signature définis au paragraphe 1.1 de la présente politique de signature, à titre de preuve pour tout litige relatif à la fourniture et à l'utilisation dudit service.

5. PRINCIPES FONCTIONNELS

- La Politique de signature est portée à la connaissance de l'utilisateur
- Les données que l'utilisateur s'apprête à signer lui sont présentées : il a la possibilité de les lire et de les sauvegarder sur son poste de travail
- Si les données à signer ont été déjà été signées par d'autres signataires, les signatures déjà réalisées sont présentées à l'utilisateur
- L'utilisateur a la possibilité de renoncer et de ne pas signer
- L'utilisateur saisit son code PIN pour déclencher la signature
- Le service de signature vérifie la validité du certificat électronique et la conformité de la signature aux standards décrits au paragraphe 6.2.
- Selon le résultat du processus de vérification, un message de confirmation ou d'erreur est adressé à l'utilisateur

6. PRINCIPES TECHNIQUES

6.1. Données signées

Les données signées sont composées des éléments suivants :

- le document original tel que présenté à la signature,
- les propriétés de signature telles que définies au paragraphe 6.2 de la présente Politique de signature,
- la Politique de signature

6.2. Caractéristiques des signatures

Les signatures respectent la norme XAdES (ETSI TS 101 903) en version v1.1.1 ou supérieure ou PAdES (ETSI TS 102 778) ou CAdES (ETSI TS 101 733).

La référence à la présente Politique de signature (OID, valeur de condensé de la Politique de signature calculé et algorithme de condensation utilisé, URL d'accès à la présente Politique de signature, OID de l'algorithme utilisé pour calculer l'empreinte de la présente Politique de signature) est embarquée soit dans les propriétés signées de la signature, soit dans les métadonnées du document signé.

6.3. Algorithmes utilisables pour la signature

6.3.1. Algorithme de condensation

Les algorithmes de condensation à utiliser sont SHA-1 et SHA256.

6.3.2. Algorithme de chiffrement

L'algorithme de chiffrement à utiliser est RSA

6.3.3. Algorithme de canonicalisation

L'algorithme de canonicalisation utilisé est le standard de canonicalisation XML exclusive défini par http://www.org/2001/10/xml-exc-c14n#

6.4. Horodatage

A la réception de la contremarque de temps délivrée par l'Autorité d'horodatage, l'Autorité de signature l'insère dans la signature.

En cas d'indisponibilité de l'Autorité d'horodatage, l'opération de signature s'effectue sans contremarque de temps.