Politique de signature électronique simple de personne physique du ministère de la Justice

TABLE DES MATIÈRES

Diffusion	Publique	Contrôlée exemplaire n°
Pour action		

HISTORIQUE DES MODIFICATIONS

Date application	Version	Objet	Rédaction	Vérification	Approbation
09/2021	0.1	Première version	SEM/DEPM/		

I. OBJET DU DOCUMENT

La signature électronique apposée sur un ensemble de données permet de garantir leur intégrité, leur non répudiation et leur authenticité compte tenu du lien univoque entre la signature et son signataire.

Une politique de signature est un document qui fait partie intégrante de la chaîne de confiance du traitement d'une procédure dématérialisée. En effet, la politique de signature précise le contexte dans lequel la signature électronique est produite, le rôle et les obligations de chacun et les conditions dans lesquelles cette signature sera ultérieurement traitée, conservée et disponible pour vérification.

Les objectifs visés d'une politique de signature sont ainsi :

- de prendre conscience de l'acte de signature,
- de connaître le processus de signature,
- de définir un cadre harmonisé pour l'ensemble du ministère.

Le présent document « Politique de signature électronique simple du ministère de la justice », décrit ces conditions dans le cadre des documents ne nécessitant pas un niveau de signature qualifiée, signés par les magistrats et agents du ministère de la justice, des juridictions et des services déconcentrés et le cas échéant les autres porteurs de certificats qui participent au fonctionnement de la justice[1] et possèdent un compte dans l'annuaire du système d'information du ministère.

En effet, la signature électronique simple permet de garantir un niveau de confiance conforme avec l'absence de nécessité d'une signature présentant un très haut niveau de sécurité.

La signature électronique de chaque document assure l'intégrité du document et l'identification de son signataire.

Le présent document est destiné :

- aux signataires, pour leur permettre de comprendre la portée et le sens de l'engagement pris en signant ;
- aux destinataires des documents signés, pour leur permettre de s'assurer de leur validité (technique) et du sens des signatures ;
- aux éventuels prestataires participant au processus de signature électronique ;
- aux services et personnes désirant vérifier l'authenticité des documents dématérialisés signés à l'aide d'une signature électronique simple..

[1] Les porteurs de certificats peuvent être soit des internes au ministère de la justice en tant qu'agent de l'Etat ; soit des externes au ministère de la justice en tant que personnel d'un autre ministère ou prestataire d'une société. Tout porteur possède un dossier administratif (personnel interne) ou un dossier d'habilitation (personnel externe)

II. POLITIQUE DE SIGNATURE ELECTRONIQUE

II.1. CHAMP D'APPLICATION

La présente politique de signature électronique s'applique à tout document dont la signature ne nécessite pas une signature électronique de niveau qualifié, c'est-à-dire dont aucune disposition législative ou réglementaire n'impose un tel niveau et dont la nature ne requiert pas de bénéficier de la présomption de fiabilité attachée à la signature électronique qualifiée.

Les documents concernés pourront notamment comprendre :

- les décisions prises et les documents signés dans le cadre du traitement des demandes d'aide juridictionnelle ;
- les mesures d'administration judiciaires;
- les convocations ;
- les conventions conclues entre le ministère et les magistrats ou agents.

La présente signature électronique répond aux exigences :

- du règlement eIDAS - règl. 910/2014/UE sur l'identification électronique et les services de confiance pour les transactions électroniques
- de la décision d'exécution (UE) 2015/1506 de la commission du 8 septembre 2015
- des articles 1366 et 1367 du code civil.

II.2. IDENTIFICATION

La présente politique de signature est identifiée par l'OID (Object IDentifier) 1.2.250.1.120.100.7.1.1. Cette référence figure dans les données signées conformément au paragraphe IV.2 de ce document afin d'attester du régime sous lequel le document a été signé.

II.3. GESTION DE LA POLITIQUE

La présente politique est validée par la secrétaire générale du ministère de la justice après avis du comité d'approbation.

COMITE D'APPROBATION

Le comité d'approbation est composé de représentants :

- des services concernés au sein du secrétariat général du ministère de la justice ;
- de la cellule d'appui HFDS ;
- de la direction des services judiciaires ;
- de la direction des affaires civiles et du Sceau ;
- de la direction des affaires criminelles et des grâces ;
- de la direction de l'administration pénitentiaire ;
- de la direction de la protection judiciaire de la jeunesse ;

Ce comité est placé sous la responsabilité de la secrétaire générale du ministère de la justice.

PUBLICATION DU DOCUMENT

La présente politique, soumise au comité d'approbation pour avis, est publiée après validation de la secrétaire générale du ministère de la justice.

La présente politique de signature est publiée à l'adresse suivante :

http://www.justice.gouv.fr/igc/ants/politiquesignaturesimple.pdf

PROCESSUS DE MISE A JOUR

La mise à jour d'une politique de signature est un processus impliquant tous les acteurs du comité d'approbation.

CIRCONSTANCES RENDANT UNE MISE A JOUR NECESSAIRE

Le processus de mise à jour est enclenché notamment en vue de l'amélioration et de l'optimisation du dispositif institué, de la prise en compte d'évolutions techniques ou organisationnelles ou de nouveaux besoins ou de mise en conformité avec le cadre juridique et technique.

PRISE EN COMPTE DES REMARQUES

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

depm.sem-sg@justice.gouv.fr

Ces remarques et souhaits d'évolution sont examinés par le service de l'expertise et de la modernisation au sein du secrétariat général après consultation des acteurs concernés, qui engage si nécessaire le processus de mise à jour de la présente politique de signature.

INFORMATION DES ACTEURS

Lorsqu'une mise à jour est intervenue, les informations relatives à cette évolution sont mises en ligne sur l'espace de publication. Indépendamment de ce mode de communication, les acteurs peuvent à tout moment se renseigner auprès du service de l'expertise et de la modernisation pour obtenir plus d'informations.

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

- document au format PDF ;
- OID du document ;
- 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 caduc ».

ENTREE EN VIGUEUR DE LA NOUVELLE VERSION ET PERIODE DE VALIDITE

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

III. ACTEURS ET ROLES

III.1. LE SIGNATAIRE APPOSANT SA SIGNATURE ÉLECTRONIQUE

Le signataire apposant sa signature électronique est un magistrat ou agent du ministère de la justice ou de ses services déconcentrés ou tout autre porteur de certificat qui participe au fonctionnement de la justice[2] et possède un compte dans l'annuaire du système d'information du ministère.

Dans la suite du document, le terme SSE (signataire signature électronique) désignera ce signataire. Son rôle est d'apposer sa signature électronique sur des documents numériques.

III.2. LE MINISTÈRE DE LA JUSTICE

Le rôle du ministère de la justice, consiste à :

- vérifier la validité du processus technique de signature ;
- vérifier la validité du certificat ayant servi à la signature électronique ;
- vérifier que le certificat électronique de signature électronique a bien été délivré par le ministère de la justice ;
- mettre à disposition des signataires les dispositifs techniques de création de signature électronique.

III.3. OBLIGATIONS DU SIGNATAIRE APPOSANT UNE SIGNATURE NUMERIQUE (SSE)

DISPOSITIF TECHNIQUE DE SIGNATURE

Seuls les dispositifs techniques autorisés par le ministère de la justice doivent être utilisés pour l'apposition de la signature électronique.

Le SSE doit utiliser l'environnement technique de signature mis à sa disposition par le ministère de la justice.

VERIFICATION DES DONNEES A SIGNER

Le SSE vérifie le document qu'il va signer avant d'y apposer sa signature.

TYPE DE CERTIFICAT UTILISE

Le SSE doit utiliser le certificat de signature délivré par une autorité interne du ministère de la justice.

PROTECTION DU SUPPORT DU CERTIFICAT

Le SSE doit prendre toutes les mesures nécessaires pour protéger l'accès à la clé privée associée à son certificat de signature.

[2] Les porteurs de certificats peuvent être soit des internes au ministère de la justice en tant qu'agent de l'Etat ; soit des externes au ministère de la justice en tant que personnel d'un autre ministère ou prestataire d'une société. Tout porteur possède un dossier administratif (personnel interne) ou un dossier d'habilitation (personnel externe)

REVOCATION DU CERTIFICAT

Considérant la nature du certificat (éphémère), la révocation de certificat n'est pas applicable.

III.4. OBLIGATIONS DU MINISTÈRE DE LA JUSTICE

ENVIRONNEMENT TECHNIQUE DE SIGNATURE

Le ministère de la justice s'engage à utiliser un environnement technique de signature conforme à la réglementation en vigueur.

Le ministère de la justice s'engage à ce que le dispositif technique de signature ne présente pas de faille logicielle connue de nature à permettre une quelconque modification des contenus validés par les signataires lors de l'apposition de leur signature électronique.

DONNEES DE VALIDATION

Pour effectuer les vérifications, le service de validation utilisé par le ministère de la justice doit utiliser les données publiques relatives aux certificats des SSE.

PROTECTION DES MOYENS

Le ministère de la justice s'assure de la mise en œuvre des moyens nécessaires à la protection des équipements fournissant les services de validation.
Les mesures prises concernent à la fois :

- la protection des accès physiques et logiques aux équipements aux seules personnes habilitées ;
- la disponibilité du service ;
- la surveillance et le suivi du service.

JOURNALISATION

Le ministère de la justice s'assure de la conservation des traces relatives au traitement des données signées conformément à la réglementation en vigueur.

IV. SIGNATURE ELECTRONIQUE ET VALIDATION

IV.1. SIGNATURE ÉLECTRONIQUE

DONNEES SIGNEES

Au moment de la signature électronique, le SSE signe électroniquement l'intégralité des données (non réencodées) constituant l'acte, ainsi que les propriétés de la signature électronique telles que définies dans le paragraphe « Norme de signature ».

PROCESSUS DE SIGNATURE

PRESENTATION DU DOCUMENT A SIGNER

Le SSE doit avoir la possibilité de parcourir et prendre connaissance de l'ensemble du document avant de de signer.
Les prénom et nom du SSE sont intégrés définitivement au document à la signature.
Le SSE a la possibilité de positionner un visuel ou d'apposer une signature manuscrite numérique.

PRESENTATION DES ATTRIBUTS DE LA SIGNATURE AU SSE

Avant de signer, le SSE doit avoir la possibilité d'accéder à la politique de signature qui encadre sa signature ainsi qu'aux paramètres de celle-ci (niveau de signature, algorithme de chiffrement, etc.).

POSSIBILITE D'ARRET DU PROCESSUS DE SIGNATURE

À tout moment, il doit pouvoir interrompre le processus de signature.

TYPE DE SIGNATURE

Les signatures électroniques apposées par les SSE sont de niveau simple au sens du règlement eIDAS (règlement UE n°910/2014 du 23 juillet 2014).

Ce sont des signatures enveloppées, également désignées sous le terme « signature embarquée ». Ces signatures contiennent :

- une identification du SSE ;
- un jeton d'horodatage garantissant l'intégrité du document et la date de signature.

Cette politique de signature impose l'utilisation de positions de signature permettant d'avoir le contenu et l'enveloppe de signature dans un même document.

NORME DE SIGNATURE

Les signatures doivent respecter la norme PAdES (ETSI EN 319 142) en version v1.1.1 ou supérieure.

Conformément à la norme PAdES, les propriétés signées doivent contenir les éléments suivants :

- le certificat du SSE (SigningCertificate) ;
- la date et l'heure de signature présumé (heure délivrée par le serveur de signature, SigningTime) ;
- la référence au présent document (SigningPolicyIdentifier / SigPolicyIdType) ;
- l'OID de la présente politique de signature (SigPolicyId) ;
- la valeur de condensé de la politique de signature calculée et algorithme de condensation utilisé (SigPolicyHash).

Le document signé doit être immédiatement validé, horodaté et complété par l'usage du niveau de signature PAdES-T, intégrant la signature électronique et un jeton d'horodatage, permettant de conserver la date et l'heure de la signature et la liste de révocation de la chaîne de certification de l'unité d'horodatage à cette date.

DATE ET HEURE DE SIGNATURE

La date et l'heure de signature sont établies pour chaque signature par l'intégration à la signature embarquée dans le document d'une contremarque de temps émise par une autorité d'horodatage.

ALGORITHMES UTILISABLES POUR LA SIGNATURE

ALGORITHME D'EMPREINTE

L'empreinte des données signées doit être effectuée avec l'algorithme SHA-256 ou plus.

ALGORITHME DE CHIFFREMENT

Les algorithmes de chiffrement à utiliser sont :

- RSA Encryption avec une taille de clé au minimum de 2048 bits ;
- par courbe elliptique (ECDSA avec la courbe nommée secp256r1)

IV.2. AUTRES CARACTÉRISTIQUES

La signature électronique d'un document intègre dans celui-ci un visuel composé notamment d'éléments d'identification du SSE et de la date de signature.

IV.3. CONDITIONS TECHNIQUES POUR DÉCLARER VALIDE LE DOCUMENT SIGNÉ

Un document signé est considéré comme valide techniquement par le ministère de la justice lorsque les conditions suivantes sont remplies :

- validation positive de la signature électronique du SSE :
  - vérification du respect de la norme de signature ;
  - vérification du certificat du SSE et de tous les certificats de la chaîne de certification :
    - validité temporelle ;

- signature cryptographique ;
- vérification de la non révocation pour la chaîne d'horodatage ;

  - vérification de l'intégrité des données transmises par calcul de l'empreinte et comparaison avec l'empreinte reçue ;
  - validation de la signature électronique apposée sur le document en utilisant la clé publique du SSE contenue dans le certificat transmis.

- appartenance du certificat de signature utilisé par le SSE à la liste des certificats référencés dans cette politique de signature ;
- correspondance entre les données signées reçues et les données envoyées par l'environnement technique de signature au SSE : cette étape permet de vérifier que les données présentées au SSE n'ont pas été modifiées durant leur transmission.

V. AUTRES ASPECTS DE LA POLITIQUE

V.1. POLITIQUE DE CONFIDENTIALITÉ

CLASSIFICATION DES INFORMATIONS

Les journaux des différents environnements techniques sont considérés comme confidentiels.

COMMUNICATION DES INFORMATIONS A DES TIERS

On entend par tiers, tout organisme n'étant pas dans la chaîne de traitement des informations du ministère de la justice.

La diffusion des informations à un tiers ne peut intervenir qu'après acceptation du ministère de la justice.

V.2. DISPOSITIONS JURIDIQUES

DROIT APPLICABLE

Le présent document est régi par la loi française.

DONNEES A CARACTERE PERSONNEL

Les données à caractère personnel contenues dans les documents signés ou résultant du procédé de signature décrit ci-dessus relèvent de traitements placés sous la responsabilité du ministère de la Justice conformément au règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et les dispositions légales et réglementaires françaises, notamment la loi n°78-17 du 6 janvier 1978 modifiée (dite loi « Informatique et Libertés »).

Signé par
Catherine PIGNON L0007752
le 16/02/2022