Politique de cachet électronique 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
06/2019	1.0	Première version	Équipe MOE		
08/07/2019	1.1	Version revue et consolidée	Équipe MOA	Déborah QUIRANT-PIDET	Antoine MEISSONNIER
13/09/2019	1.2	Version modifiée	Equipe MOE SIGNA	Julien MARGINIER	Julien MARGINIER
13/09/2019	1.3	Version modifiée	Equipe MOA PPN OJI4	Jennifer GAULUPEAU	Charlène WANPOUILLE
13/09/2019	2	Version consolidée	Équipe MOA	Antoine MEISSONNIER	Antoine MEISSONNIER
04/12/2019	3	Version consolidée	Équipe MOA	Antoine MEISSONNIER	Antoine MEISSONNIER
04/12/2019	3.1	Version consolidée	Équipe MOA	Antoine MEISSONNIER	Antoine MEISSONNIER
06/01/2020	3.2	Version consolidée	Équipe MOA	Antoine MEISSONNIER	Antoine MEISSONNIER
06/01/2020	3.3	Version consolidée	Équipe MOA	Antoine MEISSONNIER	Antoine MEISSONNIER
05/05/2020	3.6	Version consolidée	Antoine MEISSONNIER		
06/05/2020	3.7	Version consolidée	J. MARGINIER		
02/12/2021	3.8	Ajout du format JADES	Jennifer GAULUPEAU Coralie FOURNIAT	Antoine MEISSONNIER	Antoine MEISSONNIER

I. OBJET DU DOCUMENT

Le cachet électronique apposé sur un ensemble de données permet de garantir leur origine et leur intégrité.

Une politique de cachet électronique est un document décrivant les conditions de recevabilité d'un document sur lequel sont apposés un ou plusieurs cachets électroniques dans le cadre d'échanges électroniques prédéfinis.

Le présent document « Politique de cachet électronique du ministère de la justice » décrit ces conditions dans le cadre de l'utilisation d'un service de création de cachet électronique (SCCe) avancé ou qualifié par toute entité du ministère de la justice souhaitant sécuriser et garantir la valeur des documents et données produits dans le cadre de son activité, à des fins de stockage dans l'application de production, dans le coffre-fort électronique du ministère ou dans son système d'archivage électronique (SAE). Ces conditions s'appliquent également dans le cadre de l'utilisation du service de vérification de cachet, principalement lors d'un transfert de documents signés par cachet d'une application de production ou du coffre-fort électronique vers le SAE. Le cachet électronique apposé assure la valeur probante des documents. Aussi, l'intégrité d'une pièce et son origine sont garanties par le cachet électronique.

Ce 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 juridique) et du sens des cachets ;
- au département des archives, de la documentation et du patrimoine, pour lui permettre de documenter la procédure de signature des documents qui intègreront le système d'archivage électronique.

Le ministère de la justice s'est doté d'un service de création de cachet électronique avancé ou qualifié et d'un service de vérification de cachets permettant de :

- garantir l'intégrité d'un document électronique et d'authentifier l'organisation ou l'entité émettrice du document.
- de vérifier l'intégrité et la validité des cachets électroniques internes et externes.

II. POLITIQUE DE SIGNATURE « CACHET »

II.1. CHAMP D'APPLICATION

La présente politique de cachet électronique s'applique à tout document signé électroniquement, dans le cadre d'un stockage dans l'application de production, dans le coffre-fort électronique du ministère de la justice ou dans son SAE.

II.2. IDENTIFICATION

La présente politique de signature est identifiée par l'OID (Object IDentifier) 1.2.250.1.120.100.3.1.1.

Cette référence figure dans les données signées conformément au paragraphe IV.1 de ce document afin d'attester du régime sous lequel le document a été signé.

II.3. GESTION DE LA POLITIQUE

Cette présente politique est validée par la secrétaire générale du ministère de la justice sur proposition 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 ;
- du département des archives et de la documentation et du patrimoine (DADP) ;
- de l'ensemble des directions du ministère de la justice utilisant le service de Cachet ou de Vérification de Signature.

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

PUBLICATION DU DOCUMENT

La présente politique est publiée après validation formelle de la secrétaire générale du ministère de la justice et apposition de sa signature électronique.

La présente politique de signature « cachet » est publiée à l'adresse suivante : http://www.justice.gouv.fr/igc/ants/.

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 pour prendre en compte de nouveaux acteurs, de nouveaux besoins ou mettre 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 :

projae.sg@justice.gouv.fr

Ces remarques et souhaits d'évolution sont examinés par le SEM/DADP 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 des services du secrétariat général compétents pour obtenir plus d'informations.

La publication d'une nouvelle version de la politique de signature « cachet » 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 caduque ».

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 SERVICE DEMANDEUR DU CACHET ELECTRONIQUE

Dans la suite du document, le terme SDC désignera le service demandeur de cachet. Il s'agit d'un service du ministère de la justice, d'une Direction du ministère ou d'un programme du ministère.
Son rôle est d'apposer un cachet 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 des cachets ;
- vérifier la validité du certificat ayant servi au cachet électronique ;
- vérifier que le certificat de cachet électronique est conforme au règlement e-IDAS et a bien été délivré pour le ministère de la justice ;
- mettre à disposition des signataires les dispositifs techniques de création de cachet et de vérification des cachets.

III.3. OBLIGATIONS DU SERVICE DE CRÉATION DE CACHET ÉLECTRONIQUE AVANCÉ OU QUALIFIÉ

Dans la suite du document, le terme SCCe désignera le service de création de cachet électronique avancé ou qualifié, qui utilise un dispositif qualifié de création de cachet électronique et une application de création de cachet électronique.

ENVIRONNEMENT TECHNIQUE

La création du cachet doit être réalisée sur un serveur du ministère de la justice par le SCCe. Les applications signataires ne doivent utiliser que les postes de travail et les serveurs autorisés dans le cadre de cet usage du cachet.
Les accès physiques et techniques aux équipements permettant le cachet et aux informations confidentielles qui s'y trouvent sont protégés.

DISPOSITIFS TECHNIQUES DE SIGNATURE DU CACHET ET DE VERIFICATION

Seuls les dispositifs techniques autorisés par le ministère de la justice doivent être utilisés par le SCCe pour l'apposition du cachet.
La fonction respecte les exigences réglementaires en vigueur pour chacun des composants suivants :

- le dispositif de création de cachet électronique qualifié ;

- le module de vérification d'un cachet.

TYPE DE CERTIFICAT UTILISE

Le SCCe doit utiliser un certificat avancé ou qualifié de cachet électronique au sens du règlement eIDAS (règlement UE n°910/2014 du 23 juillet 2014) délivré pour le ministère de la justice.
À ce titre, il doit respecter les obligations qui lui incombent telles que définies dans la politique de certification idoine.

PROTECTION DU CERTIFICAT DE CACHET

Le SCCe doit intégrer toutes les mesures nécessaires pour protéger l'accès au certificat de cachet et aux données secrètes (clé privé et code d'activation) associées.

REVOCATION DU CERTIFICAT

En cas de perte, de vol, de compromission ou de simple suspicion de compromission de la clé privée, le responsable de certificat de cachet doit demander la révocation dans les plus brefs délais du certificat.

III.4. OBLIGATIONS DU MINISTÈRE DE LA JUSTICE

VERIFICATION DES DONNEES A SIGNER

Le SDC doit contrôler les données qu'il va signer avant d'y apposer un cachet.

ENVIRONNEMENT TECHNIQUE DE SIGNATURE

Le ministère de la justice s'engage à utiliser un environnement technique de signature conforme à l'état de l'art.

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

DONNEES DE VALIDATION

Pour effectuer les vérifications, le service de validation du ministère de la justice doit utiliser les données publiques relatives aux certificats de cachet utilisées par les SCCe, telles que les listes de révocations.
Un délai existe entre le moment où est demandée la révocation d'un certificat et le moment où la liste des certificats révoqués est publiée. Si une signature a été effectuée pendant ce délai de latence, cette signature est nulle.

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.

III.5. OBLIGATIONS DES DESTINATAIRES DES INFORMATIONS AVEC APPOSITION DE CACHET

Les destinataires doivent intégrer, le cas échéant, l'autorité de certification du cachet électronique de l'application utilisatrice à la liste des autorités de confiance de leur outil de vérification de signature en se fondant sur les Trusted Lists publiées par l'Union européenne à l'adresse : https://webgate.ec.europa.eu/tl-browser/#/tl/FR.

Les destinataires peuvent mettre par eux-mêmes des moyens de vérification des cachets électroniques des informations reçues en s'appuyant sur les informations contenues dans la présente politique.

Certaines données, notamment les listes de révocation, sont mises à jour quotidiennement. Par conséquent, il se peut qu'un cachet électronique soit déclarée valide s'il est réalisé entre le moment où le certificat a été révoqué et le moment où sa révocation a été publiée par l'autorité de certification et prise en compte par le SCCe et par les outils utilisés par les destinataires pour vérifier les cachets électroniques. Le SCCe ne peut être par conséquent tenu responsable de cet état de fait.

IV. SIGNATURE ELECTRONIQUE ET VALIDATION

IV.1. CACHET ÉLECTRONIQUE

DONNEES SIGNEES

Au moment de l'apposition du cachet électronique, le SCCe signe électroniquement l'intégralité des données constituant le document et contient les métadonnées définies dans le paragraphe « Configuration technique de cachet électronique ».

PROCESSUS DE SIGNATURE

AUTHENTIFICATION

Le SCCe s'identifie auprès du SDC. Cette identification se fait par le biais d'un certificat qui est vérifié, ainsi que toute la chaine de certification, en s'appuyant sur la liste CRL émise par le ministère de la justice.

PRESENTATION DU DOCUMENT ET DES ATTRIBUTS DU CACHET AU SCCE

Lorsque cette authentification mutuelle (via des certificats client et serveur) est effectuée, le SCCe présente le document au SDC, l'identification de la signature voulue et les paramètres qui seront appliqués.

Avant de signer, le SDC doit avoir la possibilité d'accéder à la politique de cachet électronique du ministère de la justice qui encadre sa signature ainsi qu'aux paramètres de celui-ci (niveau de cachet, algorithme de chiffrement, etc.).

SIGNATURE ET MISE A DISPOSITION DU DOCUMENT SIGNE

Le SCCe appose le cachet sur le document pour :

- sceller électroniquement son contenu ;
- certifier sa provenance.

Le SCCe met à disposition du SDC le document dans l'un des environnements suivants selon les besoins :

- dans l'application de production ;
- dans le coffre-fort électronique ;
- dans le système d'archivage électronique.

TYPE DE CACHET

Les cachets électroniques apposées par les SCCe sont de niveau avancé ou qualifié au sens du règlement eIDAS (règlement UE n°910/2014 du 23 juillet 2014).

Ce sont des signatures uniquement détachées, enveloppées et enveloppantes suivant le type de documents à signer. Ces signatures contiennent :

- une identification du certificat utilisé par le Cachet ;
- un jeton d'horodatage garantissant l'intégrité du document et la date de signature, en fonction du besoin.

Les documents concernés par le cachet électronique sont de type PDF, XML, JSON ou autres. Les documents auront une signature au format :

- PADES, XADES,CADES ou JADES.

CONFIGURATION TECHNIQUE DE CACHET

Les cachets électroniques doivent respecter les normes suivantes :

- PADES (ETSI EN 319 142 part 1-2) avec une position de signature : enveloppée.
- XADES (ETSI EN 319 132 part 1-2) au niveau LT ou LTA : les trois positions de signature sont autorisées : détachée, enveloppée et enveloppante.
- CADES (ETSI EN 319 122-1) les deux positions de signature sont autorisées : détachée et enveloppante.
- JADES (ETSI TS 119 182-1) les deux positions de signature sont autorisées : enveloppée et enveloppante.

Le document signé doit être immédiatement validé, horodaté et complété par l'usage du niveau de signature LT ou LTA, intégrant la signature électronique et un jeton d'horodatage, permettant de conserver la date, l'heure et la liste de non-révocation à cette date.

Les propriétés signées doivent contenir les éléments suivants :

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

Les données signées doivent être immédiatement validées, et complétées par l'usage du niveau de signature, intégrant la signature électronique voire un jeton d'horodatage, permettant de conserver la date et l'heure de la signature et la liste de révocation à cette date.

DATE ET HEURE DU CACHET ELECTRONIQUE

La date et l'heure du cachet sont établies pour chaque cachet, par l'intégration au cachet d'une contremarque de temps émise par une Autorité d'Horodatage, en fonction du format de cachet électronique utilisé.

Dans le cadre de la vérification du cachet électronique, la validité du certificat du cachet et le certificat du jeton d'horodatage sont vérifiés.

ALGORITHMES UTILISABLES POUR LE CACHET

ALGORITHME D'EMPREINTE

L'empreinte des données signées doit être effectuée avec l'algorithme SHA-256 ou plus, conformément à l'état de l'art.

ALGORITHME DE CHIFFREMENT

L'algorithme de chiffrement à utiliser est RSA Encryption avec une taille de clé au minimum de 2048 bits, conformément à l'état de l'art.

IV.2. 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 du cachet électronique :
  - vérification du respect de la norme de signature ;
  - vérification du certificat du SCCe et de tous les certificats de la chaîne de certification (s'appuyant sur les CRL) :
    - validité temporelle,
    - statut,
    - signature cryptographique ;
  - vérification de l'intégrité des données transmises par calcul de l'empreinte et comparaison avec l'empreinte reçue ;
  - validation du cachet électronique apposé sur le document en utilisant la clé publique du SCCe contenue dans le certificat transmis.
- appartenance du certificat de cachet utilisé par le SCCe 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 SCCe : cette étape permet de vérifier que les données n'ont pas été modifiées durant leur transmission.

V. AUTRES ASPECTS DE LA POLITIQUE

V.1. POLITIQUE DE CONFIDENTIALITÉ

CLASSIFICATION DES INFORMATIONS

Les informations suivantes sont considérées comme confidentielles :

- les données secrètes associées au certificat (clé privée et code d'activation) ;
- les journaux des différents environnements techniques ;
- les rapports de contrôle de conformité et les plans d'action référents.

La confidentialité des documents signés est régie par les dispositions légales et réglementaires en vigueur.

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 des procédés de signature décrits 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 abrogeant la directive 95/46/CE, à la directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, ainsi qu'aux dispositions légales et réglementaires françaises, notamment la loi n°78-17 du 6 janvier 1978 modifiée (dite loi « Informatique et Libertés »).

6LJQp SDU &DWKHULQH 3,*121 / OH