Politique de signature

relative à la signature électronique en matière pénale

des personnels de la police et de la gendarmerie nationales

Références du présent document

OID : 1.2.250.1.152.6.1.4.5 Date : 17/04/2019

Version 1

APPROUVÉE

Table des matières

1. Contexte et objectif

Dans le cadre de sa stratégie de transformation numérique, l'Etat a décidé de dématérialiser les procédures pénales et de permettre aux personnels de la police et de la gendarmerie nationales de procéder à la signature électronique des documents transmis aux magistrats.

Il est important que tous les acteurs aient connaissance du contexte dans lequel cette signature électronique est produite, des rôles obligatoires que chaque acteur endosse et des conditions dans lesquelles cette signature sera ultérieurement traitée, conservée et disponible pour vérification.

L'application de signature utilisée dans le cadre de la présente politique de signature permet aux personnels de la police et de la gendarmerie nationales en charge d'une procédure pénale ou y concourant de signer au format « pdf » tous les actes la constituant.

L'objectif de la présente politique de signature est de décrire :

- les conditions dans lesquelles sont réalisées, traitées et conservées ces signatures électroniques personnelles,
- les conditions et contextes dans lesquels ces signatures électroniques seront ultérieurement consultables, utilisables et vérifiables.

Ce document est destiné aux :

- signataires, pour leur permettre de comprendre la portée et le sens de l'engagement pris en signant,
- destinataires des documents signés, qui doivent non seulement s'assurer du sens de ces signatures, mais aussi avoir les moyens de s'assurer de leur validité et recevabilité,
- directions qui s'appuient sur la solution objet de la présente politique, pour leur permettre de comprendre leurs obligations et responsabilités dans les processus de signature.

2. Politique de signature

2.1. Champ d'application

La présente politique de signature s'applique à la signature électronique des personnels des services de police nationale et des unités de gendarmerie nationale en matière pénale.

Contexte fonctionnel

La signature électronique permet l'authentification et le consentement, tels qu'ils étaient assurés précédemment par la signature manuscrite des procédures ; elle bénéficie d'une garantie de fiabilité (procédure fiable garantissant le lien entre la signature et l'acte auquel elle s'attache).

Cette signature est réalisée à partir d'un certificat qualifié RGS deux étoiles et eIDAS. La signature est confortée par un horodatage qualifié eIDAS et une validation.

Contexte légal et réglementaire

La politique de signature des éléments de procédure pénale s'inscrit dans le cade légal et réglementaire suivant :

- code de procédure pénale, notamment article 801-1,
- loi n°2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice,
- arrêté du 21 juin 2011 relatif à la signature électronique ou numérique en matière pénale,
- circulaire du 19 juillet 2010 relative à la présentation des dispositions de nature pénales de la loi n° 2009-526 du 12 mai 2009 de simplification et de clarification du droit et d'allègement des procédures et du décret n° 2010-671 du 18 juin 2010 relatif à la signature électronique et numérique en matière pénale et modifiant certaines dispositions de droit pénal et de procédure pénale (NOR : JUSD1019268C).

Les personnes habilitées à signer électroniquement ces documents dans le cadre de la présente politique sont les personnels de la police et de la gendarmerie nationales en charge des procédures pénales ou y concourant.

La présente politique est portée à la connaissance des signataires, qui doivent l'attester lors d'une signature (case à cocher). Un lien vers la politique est présent dans l'application de signature.

Le destinataire a accès à la politique de signature sur le site du ministère de l'intérieur.

La présente politique ne s'applique pas dans les hypothèses d'anonymisation prévues par le code de procédure pénale.

2.2. Identification du présent document

La présente politique est identifiée par l'OID **1.2.250.1.152.6.1.4.5**.

2.3. Période de validité du présent document

Le présent document entre en vigueur 3 jours ouvrés après la date de distribution ou de mise en ligne.

2.4. Mise à jour du présent document

2.4.1. Point de contact

Le présent document est mis à jour par les directions désignées ci-dessous.

Elles peuvent être contactées aux adresses suivantes :

Direction Générale de la Police Nationale

Place Beauvau

75800 PARIS

Mail : cabdgpn-em@interieur.gouv.fr

Tél. : 01 49 27 49 27

Direction générale de la gendarmerie nationale

4, Rue Claude Bernard

92130 ISSY-LES-MOULINEAUX

Tél : 01 84 22 41 05

2.4.2. Responsable de la présente politique

Ce document est sous la responsabilité des directions d'application. Elles peuvent être amenées à demander un rapport d'audit sur l'application de la présente politique.

Les directions en charge de l'application métier et le ST(SI)², en tant que maître d'œuvre, sont les porteurs des conditions de mise en œuvre des signatures des procédures.

Dans ce cadre, les directions (maîtrise d'ouvrage) des LRP, le SHFD, la DSIC et le ST(SI)² (maîtrise d'œuvre) mettent en œuvre les moyens permettant de garantir la validité des signatures électroniques produites par les signataires, avant transmission au ministère de la justice.

Cela concerne notamment :

- la mise à disposition des signataires de l'outil de signature fournis par la DSIC,
- la demande d'une contremarque de temps à l'issue de chaque signature,
- la demande de validation des données de signature.

Les maîtrises d'ouvrage et la maîtrise d'œuvre se doivent d'afficher les mentions légales, les conditions générales d'utilisation du service de signature, lesquelles doivent reprendre les rôles et obligations contenues dans la présente politique de signature, ainsi que les informations relatives aux données personnelles.

2.4.3. Procédure d'évolution et de mise à jour de la politique

La présente politique est réexaminée :

- lors de toute évolution du contexte fonctionnel ou juridique,
- lors d'un changement de procédure technique de signature ou de consolidation de preuve,
- lors de toute modification majeure de l'infrastructure de confiance du Ministère exploitée par la DSIC,
- sur demande du Haut-Fonctionnaire de Défense du Ministère,
- pour prendre en compte de nouvelles préconisations de l'Agence Nationale de la Sécurité des Systèmes d'Information et d'évolutions des règlements RGS ou eIDAS.

La mise à jour de la politique est un processus impliquant tous les acteurs et doit faire l'objet d'une démarche rigoureuse. Ce processus est engagé essentiellement pour procéder à des modifications importantes.

Les versions publiées du présent document peuvent être signées par (au moins) l'une des personnes physiques responsables du document. Cette signature est effectuée à l'aide du certificat personnel de la personne physique responsable et le document signé est au format PDF.

Toute publication d'une nouvelle version du document consiste à archiver l'ancienne version distribuée et mettre en ligne les éléments suivants :

- document au format PDF,
- OID du document,
- date et heure exacte d'entrée en vigueur.

La nouvelle version du document entre en vigueur 3 jours ouvrés après la date de distribution ou de mise en ligne.

2.4.4. Cohérence documentaire

Le document décrit le contexte de production des signatures dans le cadre des procédures pénales.

Il revient au comité d'approbation, composé d'un représentant du Haut-Fonctionnaire de Défense, de faire en sorte que ce document reste cohérent vis-à-vis des politiques sur lesquelles il s'appuie :

- la politique de certification de l'autorité de certification de type « personne » des certificats utilisés par les fonctionnaires de police, disponible à l'adresse : http://www.interieur.gouv.fr/IGC/PC/PC
- la politique de certification de l'autorité de certification de type « personne » des certificats utilisés par les militaires de la gendarmerie, disponible à l'adresse : igc.gendarmerie.fr.
- la politique d'horodatage qui décrit le contexte de production des contremarques de temps accessible à l'adresse : http://www.interieur.gouv.fr/IGC

2.4.5. Publication et consultation

Le Ministère se doit de tenir la présente politique de signature consultable.

Cette politique est publiée par la DICOM à l'adresse ***https://www.interieur.gouv.fr/IGC/Politique-de-signature-electronique-procedure-penale*.**

Cette page contient les différentes versions de la présente politique (par OID), avec *les empreintes SHA-256 de ces documents.*

Les informations relatives à la version courante du document et aux versions antérieures sont disponibles, pour les personnes autorisées aux adresses suivantes, où une rubrique documentaire référence toutes les versions précédentes de ce document :

Direction Générale de la Police Nationale

Place Beauvau

75800 PARIS

Mail : cabdgpn.dgpnsec@interieur.gouv.fr

Tél. : 01 49 27 49 27

Direction Générale de la Gendarmerie Nationale

4 Rue Claude Bernard
92130 ISSY-LES-MOULINEAUX

Mail : stsisi@gendarmerie.interieur.gouv.fr

Tél. : 01 84 22 41 05

3. Acteurs et rôles

3.1. Rôles et responsabilité des acteurs

Les rôles et obligations des acteurs dépendent fortement du cas d'usage. Selon les cas, les obligations peuvent être de nature opérationnelle ou légale et réglementaire.

Les rôles et responsabilité se limitent à la création ou la vérification de la signature électronique (si option prise par l'application métier). Les éléments techniques (certificat, format de signature) sont détaillés dans la suite de cette section.

Concernant la création de la signature, les obligations doivent permettre avant tout de déterminer qui est responsable et qui contrôle la clé privée de signature.

Concernant la vérification de la signature, les exigences sont similaires : les obligations doivent identifier qui vérifie les signatures et sur quelles bases.

3.2. Rôles et responsabilités du signataire

3.2.1. Environnement du signataire

Le signataire des documents est une personne physique (personnel de la police nationale ou de la gendarmerie nationale), disposant d'un certificat de signature et d'une application de signature (client lourd).

L'opération de création de la signature doit être réalisée sur l'environnement de travail du signataire.

Le signataire ne doit utiliser que les postes de travail et équipements autorisés dans le cadre de cet usage de la signature électronique conformément à la politique de sécurité des systèmes d'information du Ministère et sa déclinaison dans l'entité d'emploi.

Les directions (maîtrise d'ouvrage) en charge des LRP doivent mettre à disposition des signataires la politique de sécurité des systèmes d'information qui s'appliquent à chaque application.

Préalablement à toute signature, le signataire doit accepter formellement les conditions d'utilisation du service de signature. Le recueil de l'acceptation se fait par l'interface du client de signature.

3.2.2. Outils de signature et de validation utilisé

Le signataire doit impérativement utiliser l'outil de signature « Adsigner Standalone » ou une autre solution validée par la DSIC et le ST(SI)² et déployé sur son poste de travail, tel que diffusé par le ST(SI)^2 , sans en avoir préalablement modifié la configuration.

Cet outil présente le contenu du document « pdf » à signer. Le signataire doit en contrôler les données avant d'y apposer sa signature.

L'outil de signature fait appel à l'horodatage puis au service de validation du Ministère. Après la signature, il doit sauvegarder le fichier PDF signé.

3.2.3. Type de certificat utilisé

Le signataire doit utiliser le certificat de signature délivré par l'autorité de certification qualifiée R.G.S**/eIDAS et disponible sur sa carte agent. À ce titre, il doit respecter les obligations qui lui incombent telles que définies dans la politique de certification des autorités de certification listées au chapitre 8.18.1 de ce document.

3.2.3.1. Multi-signataires

La présente politique n'autorise pas les cosignatures.

3.2.3.2. Visuel d'information de signature

Selon son paramétrage général, l'outil de signature peut insérer une information de signature dans le document pdf. Le paramétrage est effectué de manière uniforme pour tous les utilisateurs des deux entités. Ce visuel est « informatif » et ne remplace pas la vérification technique de la signature.

Dans le cadre de cette politique, les documents « PDF» signés comportent une mention visuelle de signature.

Ce visuel est affiché dans un rectangle en bas de la dernière page du document pdf signé. Il comporte les informations extraites du champ « CN » du certificat du signataire :

- pour les personnels de la police nationale : le prénom, le nom,
- pour les personnels de la gendarmerie nationale : le nom issu de l'annuaire identifiant le signataire.

3.2.3.3. Information de contexte de signature

L'outil de signature insère des informations de détails de signature dans le document « pdf » signé. Il s'agit de métadonnées qui sont affichées dans les outils de lecture « pdf » en contrôle de signature. Elles sont définies par défaut dans l'outil.

Dans le cas d'usage de la présente politique, par défaut, les champs optionnels ne sont pas renseignés. Le motif de signature est clairement défini dans le corps du document avant signature.

3.2.4. Conservation des preuves

Les responsables des traitements de rédaction sont responsables de la conservation des preuves avant la transmission au ministère de la justice. Cela concerne :

- le fichier « pdf » signé, auto-porteur de la preuve,

3.3. Rôles et responsabilités des destinataires.

Les destinataires sont des personnes physiques ou morales qui reçoivent ou peuvent consulter les documents signés par les signataires.

Les destinataires doivent intégrer, le cas échéant, l'autorité de certification du signataire à la liste des autorités de confiance de leur outil de vérification de signature.

3.3.1. Journalisation

La DSIC s'assure de la conservation des traces relatives :

- aux preuves des traitements des services de son infrastructure de confiance (horodatage, service de validation),
- à la circulation des échanges au sein des réseaux et des équipements informatiques de son périmètre de responsabilité.

3.3.2. Contenu des données signées

Les signataires sont responsables des données signées et de la bonne utilisation des certificats.

Dans le cadre de la présente politique, le responsable de la présente politique n'est pas responsable :

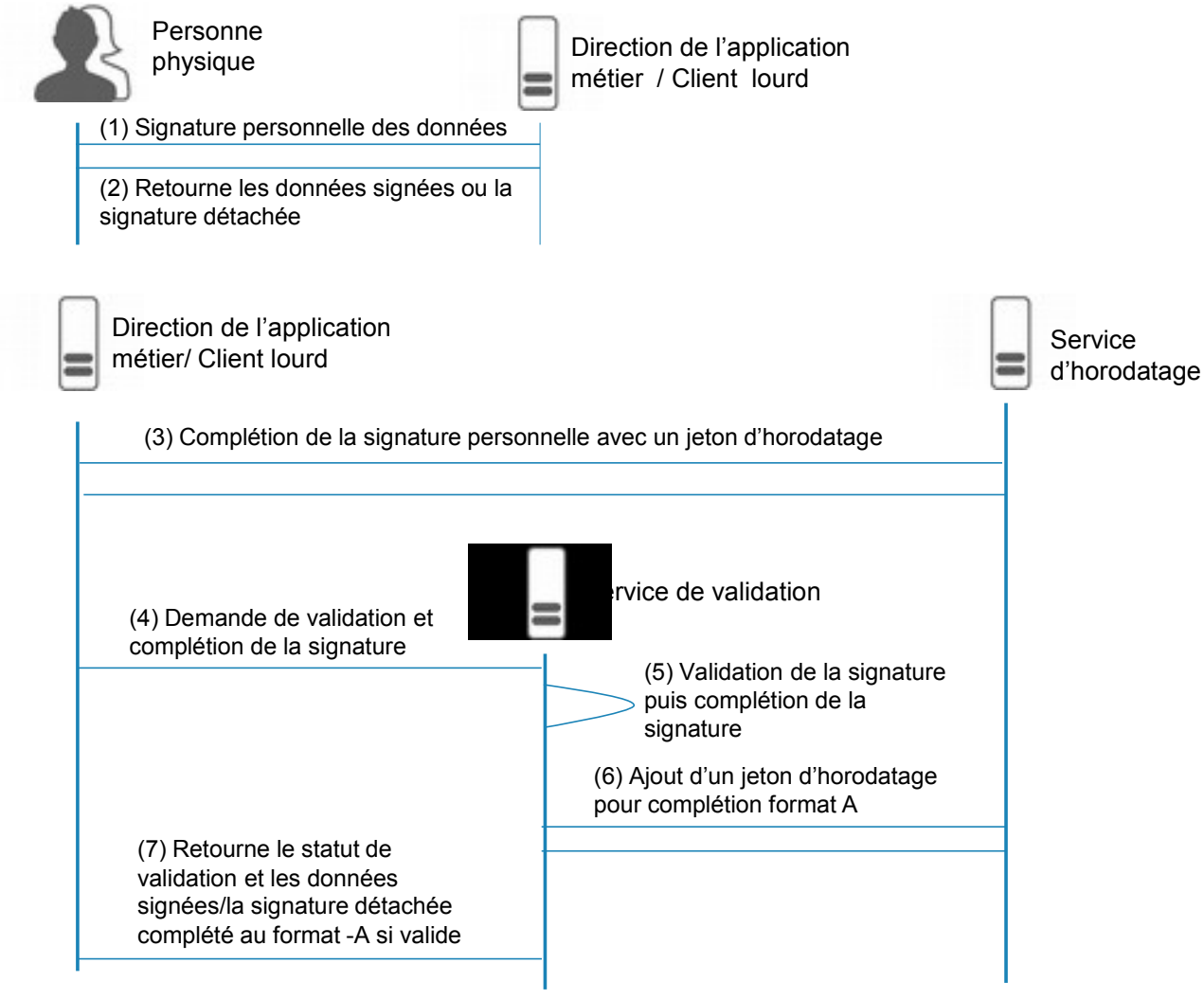
- du contenu des informations signées,
- d'une mauvaise utilisation des certificats par le signataire,
- d'une mauvaise utilisation de la plate-forme par le signataire ou la direction des applications métier pouvant entraîner une indisponibilité des services de validation de signature.

4. Signature électronique et preuves

4.1. Solution mise en œuvre dans le cadre de la présente politique

La signature personne physique, à partir de certificat RGS**/eIDAS sur carte agent, est mise en œuvre dans le cadre de cette politique. L'outil de signature est installé sur le poste de travail du signataire et mis en œuvre sous son contrôle. Pour la complétude des signatures, l'outil de signature est interfacé avec la plateforme de preuve du Ministère de l'Intérieur.

4.2. Processus de signature



La cinématique ci-dessus représente l'ensemble des opérations effectuées par le signataire porteur de certificat et les appels effectués par l'outil de signature ainsi que les appels internes aux services de confiance :

1. L'utilisateur final effectue une signature au travers du client lourd de signature sur son environnement de travail :

- Présentation du document à signer : le signataire doit visualiser les informations qu'il s'apprête à signer
- Présentation des attributs de la signature au signataire : le signataire doit visualiser son certificat de signature
- Consentement explicite et possibilité d'arrêt du processus de signature : Le signataire doit pouvoir arrêter le processus de signature et donner son consentement explicite avant signature.

2. Le client lourd renvoie à l'utilisateur (après étapes 3 à 6)
3. Le client lourd effectue un appel au service d'horodatage en transmettant la donnée signée (condensé) pour que la signature soit complétée d'un jeton d'horodatage.
4. Le client lourd effectue un appel au service de validation pour valider les données signées compléter la signature dans un format avancé (XML) permettant la conservation longue durée.
5. Le service de validation effectue l'ensemble des contrôles nécessaires pour valider la signature et complète la signature (en ajoutant des éléments requis) pour avoir une signature dans un format avancé.
6. Lors de la procédure de complétion, un appel au service d'horodatage est effectué par le service de validation pour finaliser la complétion au format A.

Si les contrôles effectués par le service de validation et l'ensemble des opérations sont réussis alors les données de signature sont affichées et le document signé peut être sauvegardé (point 2).

4.3. Caractéristiques des signatures

4.3.1. Type et norme de signature

Les signatures apposées par les signataires sont des signatures PDF.

La signature mise en œuvre est basée sur la norme PaDES.

4.3.2. Algorithmes

L'algorithme de condensation est SHA256.

L'algorithme de chiffrement est RSA Encryption.

4.3.3. Autre caractéristique

Dans le cas d'une signature au PDF visible dans le document lui-même, la présente politique ne prend pas en compte le rendu visuel de la validité de la signature par le lecteur de document. Elle n'impose pas une inscription au programme Adobe AATL.

4.3.4. Conditions pour déclarer valide le fichier signé

Un fichier signé est considéré comme valide par les directions lorsque la condition suivante est remplie :

- vérification positive de la signature électronique du signataire,

4.3.4.1. Vérification de la signature

Une signature électronique est déclarée valide par le Ministère lorsque :

- le format de la signature est conforme à la norme de signature,
- le certificat de signature est délivré par l'une des autorités de certification précisée au chapitre 8.1

- Le certificat de signature et sa chaîne de certification sont valides à l'instant « T ».
  - Validité temporelle,
  - Le certificat n'est pas révoqué,
  - La signature cryptographique est techniquement valide.
- La vérification cryptographique de la signature conformément à la norme de signature utilisée donne un résultat positif.
- Le jeton d'horodatage, si présent dans la signature ou accompagnant celle-ci, est valide.

4.3.4.2. Vérification des droits du signataire

L'utilisation du dispositif de signature mis en œuvre dans le cadre de cette politique n'est pas soumise à une authentification et un contrôle des droits par l'application LRP.

La liste des acteurs autorisés dans la cadre de la présente politique est maintenue par le Ministère. Elle est disponible auprès des directions,

Les conditions générales d'utilisation des certificats agent sont décrites dans le cadre de la politique de certification accessible à l'adresse http://www.interieur.gouv.fr/IGC/PC et http://igc.gendarmerie.fr

5. Politique de confidentialité

Les informations suivantes auxquelles il peut être fait référence dans le présent document sont considérées confidentielles :

- les données secrètes associées au certificat (clé privée, mot de passe),
- les journaux des composantes de l'application (traces d'activité),
- les procédures internes permettant d'assurer la disponibilité du service de signatures des procédures pénales et de complétude des preuves,
- les rapports d'audit.

La diffusion de ces informations à des tiers ne peut intervenir qu'après acceptation des entités responsables des éléments concernés et du Haut-Fonctionnaire de Défense du Ministère de l'Intérieur.

6. Qualification et cadre législatif

6.1. Droit applicable

Le présent document est régi par la législation française.

6.2. Règlement des différends

La résolution des litiges entre les parties découlant de l'interprétation, l'application ou l'exécution de la présente Politique de Signature, à défaut d'accord amiable entre les parties, est du ressort du tribunal administratif de Paris.

6.3. Données nominatives

Il est entendu que les collectes et usages de données à caractère personnel sont réalisés dans le strict respect de la législation et de la réglementation en vigueur sur le territoire français, en particulier de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés .

Aucune donnée à caractère personnelle n'est transmise aux services de la plateforme de preuves (horodatage et validation). Seules des empreintes numériques et des métadonnées y sont transmises.

7. Obligations et recommandations générales

7.1. Obligations appliquées aux signataires

7.1.1. Sécurité du poste client ou serveur

Le poste de travail ou le serveur à partir duquel une signature est produite ou demandée doit être protégé contre les virus, chevaux de Troie et autres logiciels malicieux susceptibles d'altérer le processus de signature (modification des données signées à l'insu du signataire, etc.).

Les déclinaisons de la politique de sécurité des systèmes d'informations du Ministère sont applicables.

7.1.2. Sécurité des clés de signature personnelle

Les clés de signature sont stockées sur support physique. Les clés de signature et leurs données d'activation sont gérées en conformité avec la politique de certification de l'autorité associée.

Les autorités de certification sont listées au chapitre 8.1 de ce document.

En cas de compromission, le signataire doit immédiatement en avertir les responsables du service de signature afin que son accès à celui-ci soit fermé et/ou le certificat révoqué conformément aux politiques de certification associées.

7.1.3. Publication des CRL (Certificate Revocation List)

Certaines données, notamment les listes de révocations, ne peuvent être mises à jour en temps réel et il s'écoule plusieurs heures avant la publication de ces données par l'entité responsable (l'autorité de certification, dans le cas d'une liste de révocation).

Dans ces conditions, il se peut qu'une signature soit déclarée valide si les données ont été signées 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 service.

La publication des CRLs est décrite dans les politiques de certification listées au chapitre 8.1de ce document.

7.1.4. Limites de responsabilités des directions et du ST(SI)²

Dans le cadre de la présente politique, les directions d'application des LRP ne sont pas responsables du contenu des données signées. Seuls les personnels signataires le sont.

7.2. Garanties apportées par les services de la plateforme de confiance

La plateforme de confiance couvre les services d'horodatage, de validation et de visualisation de preuves. Les mesures prises sont conformes à la politique de sécurité des systèmes d'information de la DSIC, à savoir :

- la protection des accès physiques aux serveurs,
- le choix d'un environnement d'hébergement adapté en termes de disponibilité aux exigences des applications clientes du Ministère (réseaux de climatisation et d'alimentation électrique secourus, systèmes de détection et d'extinction automatique de départs de feu, etc.),
- l'accès aux services de signature et de validation de signature est restreint aux seules personnes habilitées. Le nombre de personnes ayant accès aux serveurs de validation est strictement limité et ces personnes sont identifiées et authentifiées,
- la surveillance des services de confiance du Ministère est assurée en vue de prévenir les tentatives de compromission, d'intrusion physique ou par les réseaux de télécommunications,

- le stockage des clés de signature des services de confiance du Ministère est effectué sur un boîtier cryptographique.

7.2.1. Administration de la plateforme de confiance

Les administrateurs de la DSIC de la plate-forme de confiance du Ministère et de ses composants doivent s'assurer que les données qu'ils utilisent pour s'authentifier auprès du service de validation restent sous leur contrôle exclusif (confidentialité). En cas d'atteintes à ces données, ils doivent immédiatement en avertir les correspondants identifiés dans le plan de gestion de crise du Ministère.

Il leur est également demandé de révoquer immédiatement leur certificat d'authentification et/ou de signature et de procéder à une nouvelle demande.

7.2.2. Homologation et qualification des services de confiance du Ministère de l'Intérieur

La solution d'horodatage de la DSIC a fait l'objet d'une analyse de risque. Elle est homologuée SSI et qualifiée RGS et eIDAS.

La solution de validation et de consultation des preuves a fait l'objet d'une analyse de risque. Elle est homologuée SSI.

7.3. Recommandations aux destinataires

7.3.1. Vérifications complémentaires

S'il est sollicité, le service de validation vérifie la validité des signatures des documents lorsque celles-ci sont produites avant transmission au destinataire.

Néanmoins, il appartient aussi au destinataire du document signé de vérifier la validité de la signature électronique conformément à ce document.

7.3.2. Période de grâce

Compte tenu des délais de publication des CRLs, le présent document recommande au destinataire d'attendre le temps nécessaire avant de déclarer une signature valide pour son usage.

8. Politique de validation de signature

Ce chapitre de la politique de signature précise les détails techniques de sa création et de sa vérification.

8.1. Certificats de signature autorisés

La présente politique de signature impose d'utiliser les certificats émis par les autorités de certification suivantes.

Autorité de certification	Certificat de signature	URL de publication des politiques de certification
Autorité de certification Déléguée RGS** /eIDAS Police	Signature personnelle sur carte agent	http://www.interieur.gouv.fr/IGC/PC
Autorité de certification Déléguée RGS** /eIDAS Gendarmerie	Signature personnelle sur carte agent	http://igc.gendarmerie.fr

8.2. Horodatage de la preuve

Le service d'horodatage du Ministère appose une contremarque de temps sur les signatures réalisées. L'heure du serveur du service d'horodatage du Ministère repose sur des serveurs de temps précisés dans la politique d'horodatage associée.

La politique d'horodatage est disponible sur : https://www.interieur.gouv.fr/IGC/

8.3. Constitution de la preuve

8.3.1. Création des preuves de validation de signature

Une preuve est générée par le service de validation du Ministère à chaque opération de validation réalisée. La preuve de validation est signée électroniquement par le service de validation opéré par la DSIC.

8.3.2. Signature des preuves

8.3.2.1. Gabarit du certificat de preuves de signature

Le gabarit du certificat de preuves de signature est conforme au RGS. Ce certificat est émis par l'autorité de certification de Certigna. La politique de certification est disponible sur : https://certigna.fr/autorites/ et la liste de révocation sur : http://crl.certigna.fr.

8.3.2.2. Caractéristiques de la signature

La signature de la preuve respecte la norme suivantes XAdES (ETSI TS 101 093), en version 1.1.1 ou supérieure.

8.3.2.3. Algorithme de signature

L'algorithme de signature est SHA256withRSAEncryption.

8.3.3. Conservation des preuves de validation

La preuve de validation n'est pas conservée dans le cadre de la présente politique.

Le service de validation de signature s'engage à ne conserver aucune copie des données soumises pour validation de signature. En particulier, les journaux d'événements (traces d'activité) du service ne contiennent aucune copie de ces données.

****

9. Références

9.1. Réglementation

Réglementation (renvoi)	Description
[CNIL]	Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n°2018-493 du 20 juin 2018 relative à la protection des données personnelles
[RÈGLEMENT (UE)] [eIDAS]	RÈGLEMENT (UE) No 910/2014 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE
[Ordonnance]	Ordonnance n°2005-1516 du 8 décembre 2015 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives (version consolidée du 05/02/2019).
	Décret n° 2017-1416 du 28 septembre 2017 relatif à la signature électronique
[Décret RGS]	Décret n° 2010-112 du 2 février 2010 pris pour l'application des articles 9, 10 et 12 de l'ordonnance n°2005-1516 du 8 décembre 2015.
[Arrêté RGS]	Arrêté du 13 juin 2014 portant approbation du référentiel général de sécurité et précisant les modalités de mise en œuvre de la procédure de validation des certificats électroniques.

9.2. Références juridiques

Domaine	Description
Code civil	Code civil, et notamment ses articles 1316-1 et 1316-4
Code de procédure pénale	Code de procédure pénale, notamment ses articles 801-1, 16 à 20, 45 à 48, R. 49-1, R. 249-9 à R. 249-12, A. 37-14 et A. 37-15
Signature électronique en matière pénale	Arrêté du 21 juin 2011 relatif à la signature électronique ou numérique en matière pénale (article A 53-2 à . 53-4 du CPP)

10. Glossaire

10.1. Définitions

Agent
Personne physique agissant pour le compte d'une autorité administrative.

Algorithme de calcul d'empreinte numérique
Désigne l'algorithme utilisé pour calculer l'empreinte numérique du document à horodater. L'empreinte numérique est communément appelée « hash ».

Autorités administratives
Ce terme générique, défini à l'article 1 de l'ordonnance n°2005-1516 du 8 décembre 2015, désigne les administrations de l'État, les collectivités territoriales, les établissements publics à caractère administratif, les organismes gérant des régimes de protection sociale et les autres organismes chargés de la gestion d'un service public administratif.

Autorité de Certification (AC)
Désigne l'entité émettrice des certificats. C'est elle qui est garante de la gestion du cycle de vie des certificats d'UH, conformément à la PC rattachée à ses certificats.

Autorité d'Horodatage (AH)
Au sein d'un PSHE, une autorité d'Horodatage a en charge, au nom et sous la responsabilité de ce PSHE, l'application d'au moins une politique d'horodatage en s'appuyant sur une ou plusieurs Unités d'Horodatage.

Certificat électronique
Fichier électronique attestant qu'une bi-clé appartient à la personne physique ou à l'élément matériel ou logiciel identifié, directement ou indirectement (pseudonyme), dans le certificat. Il est délivré par une AC.

Condensé
(voir empreinte numérique)

CN (Common Nane : nom commun du porteur du certificat.)
Dans le cadre du RGS, ce champ doit comporter les informations d'état civil, au minimum le 1er prénom et le nom de famille, éventuellement des informations permettant de traiter les cas d'homonymie (n° RIO pour les policiers)

CRL (Certificate Revocation List) :
Désigne la liste des certificats révoqués d'une autorité de certification.

Directions
Le terme « directions », utilisé sans autre précision dans ce présent document, désigne les entités citées au § 2.4.1.

Dispositif de création de signature
Il s'agit du dispositif matériel et/ou logiciel utilisé par le porteur pour mettre en oeuvre et stocker sa clé privée de signature.

Empreinte numérique (ou hash)
Désigne l'empreinte d'un document calculée à partir d'un algorithme de calcul d'empreinte numérique.

Infrastructure de gestion de clés
Ensemble de composantes, fonctions et procédures dédiées à la gestion de clés cryptographiques et de leurs certificats utilisés par des services de confiance.

PDF (*Portable Document Format)* :
Désigne un format de fichier informatique conforme à la norme ISO 32000 et dont la spécificité est de préserver la mise en forme (polices d'écritures, images, objets graphiques...) telle que définie par son auteur, et ce quelles que soient l'application et la plate-forme utilisées pour lire ledit fichier PDF.

Politique de certification
Ensembles de règles, identifiés chacun par un nom (OID), définissant les exigences auxquelles une AC se conforme dans la mise en place et la fourniture de ses prestations et indiquant l'applicabilité d'un certificat à une communauté particulière et/ou à une classe d'applications avec des exigences de sécurité communes. Une PC peut également, si nécessaire, identifier les obligations et exigences portant sur les autres intervenants, notamment les porteurs et les utilisateurs de certificats.

Politique de Signature et de gestion de preuve
Désigne un ensemble de règles établies et les processus techniques utilisés par les utilisateurs d'une entité, pour la signature de documents métiers, la création et la conservation des preuves. Elle définit les conditions pour lesquelles une signature électronique peut être déterminée comme valide, aussi bien pour les signataires que pour les destinataires des documents.

Prestataire de service de confiance (PSCo)
Désigne toute personne ou entité offrant des services consistant en la mise en œuvre de fonctions qui contribuent à la sécurité des informations échangées par voie électronique.

Service d'horodatage
Désigne l'ensemble des prestations mise en œuvre pour générer des Contremarques de temps associées aux Fichiers de preuve, en application de la Politique d'horodatage.

10.2. Abréviations

AC	Autorité de Certification
AH	Autorité d'Horodatage
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
CGU	Conditions Générales d'Utilisation
DPH	Déclaration des Pratiques d'Horodatage
DSIC	Direction des Systèmes d'Information et de Communication du Ministère de l'Intérieur
ETSI	European Telecommunications Standards Institute
IGCMI	Infrastructure de Gestion des Clés du Ministère de l'Intérieur
LCR	Liste des Certificats Révoqués
LRP	Logiciel de rédaction de procédures (PN : Police Nationale, GN : Gendarmerie Nationale)
MI	Ministère de l'Intérieur
OID	Object Identifier (Identifiant d'Objet)
PC	Politique de Certification
PH	Politique d'Horodatage
PSCO	Prestataire de service de confiance
PSHE	Prestataire de Service d'Horodatage Electronique
RFC	Request For Comments
RGS	Référentiel Général de Sécurité

RIO	Référentiel des Identités et des Organisations
SHA	Secure Hash Algorithm (algorithme de hachage)
SHFD	Service du Haut-Fonctionnaire de Défense
ST(SI)^2	Service des technologies et des systèmes d'information de la sécurité intérieure
UH	Unité d'Horodatage
URC	Universal Time Coordinated (temps universel coordonné)

Approuvé par :

Le Préfet, Directeur général de la police nationale

Signé Eric MORVAN

Le Général d'armée, Directeur général de la gendarmerie nationale

Signé Richard LIZUREY