eurosign

Politique de signature

Version 1.0 - 20.10.2020

VERSION	DATE	DESCRIPTION	AUTEURS	SOCIÉTÉ
V. 1.0	20.10.2020	Création du document	Emmanuel MATHIEU	Eurosign

ETAT DU DOCUMENT - CLASSIFICATION	RÉFÉRENCE
Diffusion publique	1.3.6.1.4.1.55276.1.1.1.0

Table des matières

1. Contexte et objectifs

La société EUROSIGN met à disposition de ses clients un service de signature électronique permettant à toute personne ayant souscrit au service, de signer électroniquement des documents (ex : contrats, …) à distance.

Le présent document constitue la Politique de Signature d'EUROSIGN applicable aux documents signés sur le service de signature d'EUROSIGN.

Le niveau de signature utilisé dans le cadre de la présente Politique de Signature est dit « simple » au sens de la définition de la « signature électronique » stipulée à l'article 3 du règlement européen 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 (aussi appelé Règlement eIDAS).

L'objet de la Politique de Signature d'EUROSIGN est de décrire :

- Les conditions dans lesquelles sont réalisées, traitées, conservées ces signatures électroniques,
- Les conditions et le contexte dans lesquels ces signatures électroniques seront ultérieurement consultables, utilisables, vérifiables.

Ce document est destiné aux :

- Signataires des documents,
- Destinataires et lecteurs ultérieurs de ces documents signés, qui auront nécessairement besoin d'avoir connaissance des conditions dans lesquelles ces signatures électroniques auront été réalisées.

2. Politique de signature

2.1 Champ d'application

La présente Politique de Signature, s'applique aux transactions électroniques produites au sein du service de signature électronique d'EUROSIGN et ne fait aucune distinction sur le contexte de la signature qu'elle soit réalisée en face-à-face ou à distance.

2.2 Identification

La présente Politique de Signature est identifiée par l'OID 1.3.6.1.4.1.55276.1.1.1.1.0.

Cette référence, ainsi que le numéro de version de la Politique de Signature utilisée, doit obligatoirement figurer dans les données signées, afin d'attester du régime sous lequel chacun des signataires a produit sa signature électronique.

Lors de toute communication ultérieure, pour référencer la présente Politique de Signature, on utilisera l'OID accompagné de l'empreinte de ce document et de la mention de l'algorithme utilisé pour produire cette empreinte.

2.3 Publication de document

Avant toute publication officielle, la Politique de Signature est validée par le Comité d'Approbation d'EUROSIGN.

La présente Politique de Signature est :

- Disponible sur le service de signature et accessible par le signataire au moment de la signature électronique,
- Et publiée sur l'URL suivante : https://www.eurosign.com/fr/docs/certifications-eurosign/

2.4 Processus de mise à jour

2.4.1 Circonstances rendant une mise à jour nécessaire

La mise à jour d'une Politique de Signature est une procédure impliquant tous les acteurs et faisant l'objet d'une démarche rigoureuse. Il est enclenché essentiellement pour procéder à des modifications importantes, pour prendre en compte de nouveaux besoins, de nouveaux acteurs, améliorer le cadre juridique ou combler des lacunes.

La présente politique est réexaminée lors de toute modification majeure de l'application.

2.4.2 Prise en compte des mises à jour

Toutes les remarques ou demandes d'information sur la présente Politique de Signature sont à adresser par courriel à l'adresse suivante : certification@eurosign.com

Ces remarques et demandes d'information sont examinées par le Comité d'Approbation qui engage, si nécessaire, le processus de mise à jour de la présente Politique de Signature.

Une signature électronique est toujours valide au regard de la Politique de Signature qui s'appliquait au moment de la signature électronique. Toutes les versions des Politiques de Signature et leur durée respective de validité sont donc conservées par EUROSIGN et accessibles sur demande.

2.4.3 Information des acteurs

Lorsqu'une mise à jour a été planifiée, les informations relatives à cette évolution sont mises en ligne sur les lieux de publication précisés au chapitre 2.3. Indépendamment de ce mode de communication, les acteurs (cf. définition au chapitre 3.1) peuvent à tout moment se renseigner auprès d'EUROSIGN, au point de contact précisé au chapitre 2.4.2, pour obtenir plus d'informations.

La publication d'une nouvelle version de la Politique de Signature consiste à archiver la version précédente et à 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),
- Signature Technique du document,
- Algorithme de signature utilisé (algorithme SHA256WithRSAEncryption pour cette version),
- Date et heure exacte d'entrée en vigueur.

2.5 Entrée en vigueur de la nouvelle version et période de validité

Lorsqu'une nouvelle version de la Politique de Signature est mise en ligne, celle-ci est systématiquement présentée et mise à disposition des signataires lors des transactions électroniques suivant la publication.

La date et l'heure exacte d'entrée en vigueur de la nouvelle Politique de Signature sont précisées sur le site de publication.

La nouvelle version de la Politique de Signature entre en vigueur dès sa publication sur le lieu de publication identifié au chapitre 2.3 et reste valide jusqu'à la publication d'une nouvelle version.

3. Acteurs et rôles

3.1 Les acteurs

3.1.1 Signataires

Les signataires des documents sont des personnes physiques clients du service de signature électronique d'EUROSIGN, disposant de l'autorisation de l'entité qu'elles représentent le cas échéant pour signer des documents.

Le client dispose de deux niveaux d'identification avant d'entamer le processus de signature :

- Identification de niveau 1 : l'identité du signataire est contrôlée sur la base d'informations déclaratives.

- Identification de niveau 2 : l'identité du signataire est contrôlée sur la base d'informations déclaratives et de la fourniture d'une pièce justificative d'identité (carte nationale d'identité, passeport, titre de séjour).

Dans le cadre de la présente Politique de Signature, aucun certificat électronique de signature n'est délivré au signataire.

3.1.2 Eurosign

EUROSIGN développe et opère le service de signature utilisé par les signataires.

EUROSIGN et ses sous-traitants réalisent, hébergent et maintiennent le service de signature mis à disposition des signataires.

Par ailleurs, EUROSIGN :

- Dispose d'un certificat de cachet lui permettant de réaliser un scellement technique des documents en apposant un cachet électronique pour toute signature électronique « simple » réalisée par un signataire. Ce cachet électronique permet de protéger en intégrité le document signé.
- Utilise ce certificat de cachet à la fin de chaque transaction (lorsque tous les signataires ont signé) pour réaliser un dernier scellement qui est horodaté de manière à dater le document et mettre en capacité le signataire ou une tierce personne de vérifier la qualité de la signature électronique a posteriori.
- Conserve le document électronique signé dans des conditions de sécurité permettant de garantir sa confidentialité et son intégrité dans le temps.

3.1.3 Destinataire

Les destinataires des documents signés électroniquement sont les clients eux-mêmes qui conservent ces documents dont la signature électronique matérialise leur consentement par rapport au contenu des documents.

3.2 Rôles et obligations du signataire

3.2.1 Environnement du signataire

L'opération de création de la signature doit être réalisée sur un équipement informatique (ordinateur, tablette, smartphone) connecté au réseau internet.

Le processus de signature ne dépend pas de l'équipement du client, par conséquent, aucun outil lié aux opérations de signature n'est à installer sur l'équipement informatique des signataires.

Le signataire doit toutefois s'assurer que cet équipement est protégé, notamment contre l'utilisation frauduleuse de son identité.

Il est donc nécessaire de protéger l'accès physique et technique à ce poste et aux informations confidentielles qui s'y trouvent.

3.2.2 Outil de signature utilisé

Les clients doivent contrôler les données qu'ils vont signer avant d'y apposer leur signature électronique. Ils utilisent pour cela le service de signature mis à disposition par EUROSIGN et dont les différentes étapes du processus de signature les amènent à :

- Contrôler les éléments du document à signer,
- Accepter les Conditions Générales du Service,
- Accepter explicitement l'opération de signature.

3.2.3 Type de certificat utilisé

Aucun certificat électronique n'est délivré au signataire pour réaliser l'opération de signature.

La signature électronique réalisée par le signataire est de niveau « simple » au sens de la définition de la « signature électronique » stipulée à l'article 3 du règlement eIDAS.

Toutefois, un scellement électronique est réalisé par EUROSIGN pour toute signature électronique « simple » réalisée par un signataire et permet ainsi de garantir l'intégrité du document.

3.2.4 Protection du support du certificat

Non applicable. Aucun certificat n'est délivré au signataire.

3.2.5 Révocation du certificat

Non applicable. Aucun certificat n'est délivré au signataire.

3.3 Rôles et obligations d'EUROSIGN

3.3.1 Environnement technique

Le service de signature est installé sur le site d'hébergement d'EUROSIGN.

Des mesures de sécurité permettant de protéger l'accès au service de signature sont mises en œuvre, notamment :

- La surveillance de l'accès physique et logique au système et la protection contre les intrusions,
- Une limitation d'accès et d'administration du service à un minimum de personnes de confiance, ayant les compétences nécessaires.

3.3.2 Outil de signature utilisé

EUROSIGN s'appuie sur son service de signature :

- Pour réaliser un scellement pour chaque signature électronique « simple » réalisée,
- Pour réaliser un dernier scellement horodaté à la fin de la transaction.

3.3.3 Type de certificat utilisé

EUROSIGN utilise un certificat de scellement qualifié délivré par l'Autorité de Certification de Certinomis conformément à la Politique de Certification identifiée par l'OID suivant : 1.2.250.1.86.2.3.3.22.1

3.3.4 Protection du support du certificat

EUROSIGN se conforme à l'usage décrit dans les Conditions Générales d'Utilisation de Certinomis. À ce titre, le certificat électronique est stocké sur un dispositif cryptographique qui doit être qualifié au minimum au niveau FIPS 140-2 Level 2 ou CWA 14169 (SSCD), et être conforme aux exigences du chapitre 12.1 de la politique de certification Certinomis.

3.3.5 Révocation du certificat

EUROSIGN s'engage à demander la révocation de son certificat de scellement en cas de perte, de vol, de compromission ou de simple suspicion de compromission de sa clé privée et se conformer ainsi aux Conditions Générales d'Utilisation émises par l'Autorité de Certification de Certinomis.

3.3.6 Données de vérification de signature

EUROSIGN effectue une vérification de la qualité de la signature électronique préalablement à l'archivage du document signé.

Pour effectuer des vérifications des signatures/scellements électroniques, EUROSIGN utilise les données à sa disposition notamment les données publiques relatives au certificat d'EUROSIGN, telles que les listes de révocation ou encore le certificat de l'Autorité de Certification ayant délivré son certificat.

Tous les documents signés peuvent faire l'objet d'un horodatage en fin de transaction permettant :

- De s'assurer de la traçabilité des informations de date et heure de signature de ces transactions,
- De déterminer la liste de révocation à utiliser pour valider cette transaction.

En cas d'arrêt de la vérification de la signature, l'archivage électronique du document est temporairement suspendu mais n'impacte en rien la validité du document signé et horodaté.

EUROSIGN s'assure de mettre en œuvre les procédures et dispositifs techniques permettant de lancer automatiquement une nouvelle vérification du document signé lorsque le service sera de nouveau disponible.

3.3.7 Protection des moyens

EUROSIGN s'assure de la mise en œuvre des moyens nécessaires à la protection des équipements fournissant le service de signature.

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.

3.3.8 Journalisation

EUROSIGN s'assure de la conservation des traces relatives :

- A la circulation des échanges au sein des réseaux et des équipements informatiques,
- Au traitement des données échangées.

EUROSIGN s'assure que les preuves de traitement relatives à la vérification des signatures électroniques sont conservées pendant toute la durée règlementaire.

3.3.9 Reprise en cas d'interruption de service

EUROSIGN s'assure de la mise en œuvre des moyens nécessaires à la reprise d'activité en cas d'interruption de service d'un des composants nécessaires aux tâches dont il a la responsabilité.

Il s'assure en particulier que ces moyens font l'objet de tests à intervalles réguliers.

3.3.10 Assistance aux utilisateurs

Les signataires peuvent s'adresser à EUROSIGN pour toute information complémentaire ou pour signaler tout dysfonctionnement à l'adresse indiquée au chapitre 2.4.2.

3.4 Rôles et obligations des destinataires

3.4.1 Limitation des responsabilités d'EUROSIGN

3.4.1.1 Mise à jour des informations utilisées

Certaines données, notamment les listes de révocations, ne peuvent être mises à jour en temps réel et il s'écoule plusieurs heures (24 au maximum) avant la publication de ces données par l'Autorité de Certification.

Dans ces conditions, il se peut qu'une signature électronique soit déclarée valide si elle est réalisée 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 EUROSIGN.

EUROSIGN ne peut être alors tenue responsable de cet état de fait considérant cette « période de caution » inhérente à ce type de système.

3.4.1.2 Contenu des documents signés

Les clients sont responsables du contenu des informations présentes dans le document signé.

4. Signature électronique et validation

4.1 Caractéristiques de l'équipement du signataire

L'équipement informatique du signataire (ordinateur, tablette, smartphone) fonctionne dans un environnement sous le contrôle du client.

Le processus de signature ne dépend pas de l'équipement du client.

Le certificat utilisé par EUROSIGN pour la signature du client est un certificat qualifié de cachet.

Ce certificat est délivré par une Autorité de Certification : Certinomis.

4.2 Données signées

Les données signées sont des documents convertis au format PDF préalablement à leur signature.
La signature est visuellement intégrée dans les documents PDF.

4.3 Opération de signature électronique

Au préalable du processus de signature électronique, le client accède à un ou plusieurs moyens d'authentification suivant le processus d'enrôlement en vigueur.

Au préalable du processus de signature électronique, l'émetteur du document à signer définit le niveau d'authentification des signataires attendu parmi les niveaux suivants :

- **Authentification de niveau 1 :** l'identité du signataire est contrôlée sur la base d'informations déclaratives**.**
- **Authentification de niveau 2 :** l'identité du signataire est contrôlée sur la base d'informations déclaratives et de la fourniture d'une pièce justificative d'identité (carte nationale d'identité, passeport, titre de séjour).

L'opération de signature électronique peut avoir lieu dans différents environnements, selon l'équipement dont dispose le signataire.

Les fonctionnalités minimales suivantes sont assurées par le service de signature, pour permettre au signataire d'avoir connaissance et conscience de l'action qu'il est sur le point d'effectuer :

- **Présentation des documents à signer.**
  Les documents à signer sont présentés à l'écran en séquence. Le signataire doit volontairement dérouler l'ensemble du ou des documents à signer pour accéder à la phase de signature.

- **Présentation des attributs de la signature au signataire**
  Les « attributs » de la signature suivants sont affichés au signataire pour lui permettre d'avoir connaissance des conditions dans lesquelles sa signature électronique sera réalisée et traitée :
  - Lien vers la politique de signature,
  - Lien vers les Conditions Générales du Service,

  Le signataire doit confirmer qu'il a pris connaissance des Conditions Générales du Service et de la Politique de Signature du service d'EUROSIGN.

- **Interaction avec le signataire : consentement explicite et possibilité d'arrêt du processus de signature**
  Le signataire a les moyens d'exprimer explicitement (c'est-à-dire, de manière volontaire et non ambiguë) son consentement pour déclencher le processus de signature des documents sélectionnés.

  Le signataire doit volontairement dérouler l'ensemble du ou des documents à signer. Il ne peut donc en aucun cas contester que ces informations lui ont été présentées lors de la transaction dématérialisée.

- **Authentification**
  En fonction du niveau d'authentification souhaité par l'émetteur du document à signer, le client est authentifié soit sur la base de ses informations déclaratives (Niveau 1) soit via la fourniture d'une pièce justificative de son identité (Niveau 2).

  Une authentification non rejouable par SMS peut être réalisée si elle a été spécifiée par l'expéditeur. Le client reçoit alors un code à usage unique sur son mobile dont le numéro a été déclaré soit par lui-même soit par l'émetteur du document à signer.
  Il est invité à saisir ce code à l'écran pour s'authentifier puis passer à l'étape de signature.

- **Signature**
  Une fois signés, les documents sont mis à disposition du client et archivés.

4.4 Caractéristiques des signatures

Les signatures électroniques apposées par les clients sont des signatures PDF. La signature mise en œuvre est basée sur la norme PaDES (ETSI EN 319 412-1).

Le certificat utilisé pour réaliser cette signature est le certificat de cachet d'EUROSIGN.

A l'issue de la transaction, un dernier scellement peut être réalisé et peut faire l'objet d'un horodatage, produit par une Autorité d'Horodatage qualifiée au sens du règlement eIDAS. Dans ce cas, le jeton d'horodatage sera également contenu dans le document PDF.

4.5 Algorithmes utilisables pour la signature

4.5.1 Algorithme de condensation

Les algorithmes de condensation supportés sont SHA-256.

4.5.2 Algorithme de chiffrement

L'algorithme de chiffrement à utiliser est RSA Encryption.

4.6 Vérification de la signature

La vérification de la signature est possible pour les destinataires et lecteurs des documents signés.

Le cas échéant, elle porte sur :

- La vérification du respect de la norme de signature,

- La vérification de l'appartenance du certificat d'EUROSIGN à une famille de certificat qualifiée au sens du règlement eIDAS ou certifiée ETSI 319 411-1 niveau NCP a minima,
- La vérification du certificat d'EUROSIGN et de tous les certificats de la chaîne de certification :
    - Validité temporelle,
    - Statut,
    - Signature cryptographique,
    - La vérification de l'intégrité des données transmises par calcul de l'empreinte et comparaison avec l'empreinte reçue,
- La vérification de la signature électronique apposée sur le fichier en utilisant la clé publique d'EUROSIGN contenue dans le certificat transmis,
- La vérification des données d'horodatage apposées sur le dernier scellement électronique réalisé par EUROSIGN le cas échéant,
- La vérification que le certificat utilisé au moment de la signature n'était pas dans une Liste de Certificats Révoqués. Cela concerne le certificat de cachet d'EUROSIGN,
- La vérification de l'identifiant de la Politique de Signature référencée.

4.7 Gestion de la preuve

Pour conserver une trace de chaque validation de signature, EUROSIGN constitue une preuve électronique signée, qui recense les éléments associés à la validation de signature effectuée :

- Document signé par l'ensemble des clients,
- Certificat de cachet utilisé par EUROSIGN pour le compte des clients,
- Résultat de la validation,
- Statut de contrôle de la Liste de Certificats Révoqués,
- L'ensemble des chaînes de certification mises en œuvre,
- Trace d'audit générée par le serveur de signature.

Cette preuve peut être rejouée (par la validation de la signature de la preuve) ultérieurement en cas de litige et restitue exactement les informations utilisées lors de la validation.

5. Politique de confidentialité

5.1 Classification des informations

Les informations suivantes sont considérées comme confidentielles :

- Les clés privées du service de cachet d'EUROSIGN et des composantes du service de signature d'EUROSIGN (clés privées des Autorités de Certification, clés privées des Unités d'Horodatage)
- Les données d'activation associées à la clé privée d'EUROSIGN,
- Les informations personnelles des utilisateurs renseignées sur la plateforme de signature,
- Les pièces justificatives d'identité des utilisateurs déposées sur la plateforme de signature,
- Les contrats et autres documents manipulés sur la plateforme de signature,
- Les preuves constituées et leur contenu,
- Les journaux de l'application de signature,
- Les procédures internes de gestion des preuves d'EUROSIGN,
- Les rapports d'audit sur l'application de signature d'EUROSIGN et sur les différents composants de l'infrastructure s'il en existe.

Les informations confidentielles sont protégées, et donc non accessibles publiquement.

5.2 Communication des informations à un tiers

On entend par tiers, tout organisme n'étant pas dans la chaîne de traitement des informations d'EUROSIGN.

La diffusion des informations à un tiers ne peut intervenir que si EUROSIGN en reçoit la demande formelle et accepte la communication (notamment dans le cadre d'un litige et si un juge en formule une demande).

6. Dispositions juridiques

6.1 Droit applicable

La présente politique de signature est régie par le droit français.

6.2 Règlement des différends

Toutes contestations et litiges survenant dans l'interprétation et la mise en œuvre du présent document seront soumis à la juridiction des tribunaux de Paris.

6.3 Propriété intellectuelle de l'infrastructure de création et de validation des signataires

EUROSIGN dispose des droits de propriété intellectuelle des services mis en œuvre dans le cadre de son service de signature.

Les signataires ne disposent d'aucun droit de propriété intellectuelle sur les documents signés.

Toute utilisation ou reproduction, totale ou partielle, de ces éléments et/ou des informations qu'ils contiennent, par quelque procédé que ce soit, est strictement interdite et constitue une contrefaçon sanctionnée par le Code de la propriété intellectuelle.
EUROSIGN est propriétaire de la politique de signature.

6.4 Données personnelles

Les données personnelles au sens de l'article 4 du règlement européen sur la protection des données considérées dans le cadre du service de signature d'EUROSIGN sont :

- Le prénom et le nom du signataire,
- L'adresse email du signataire,
- Le numéro de mobile du signataire,
- La pièce justificative d'identité du signataire.

La collecte et l'usage de données personnelles par EUROSIGN et l'ensemble de ses composantes sont réalisés dans le strict respect de la législation et de la réglementation en vigueur sur le territoire français, en particulier du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 applicable à compter du 25 mai 2018 (règlement général sur la protection des données – RGPD) et de la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés.

En conformité avec les dispositions précitées, le traitement automatisé des données nominatives réalisé par EUROSIGN ont fait l'objet d'une déclaration auprès de la Commission Nationale de l'Informatique et des Libertés (CNIL).

Le signataire est informé qu'il dispose d'un droit d'accès, de rectification et d'opposition portant sur les données le concernant en écrivant à EUROSIGN.

Les signataires sont tenus de respecter les dispositions de la loi relative à l'informatique, aux fichiers et aux libertés, dont la violation est passible de sanctions pénales.
Ils doivent notamment s'abstenir, s'agissant des informations nominatives auxquelles ils accèdent, de toute collecte, de toute utilisation détournée et, d'une manière générale, de tout acte susceptible de porter atteinte à la vie privée ou à la réputation des personnes.