Politique de Signature Électronique

OID	1.3.6.1.4.1.36513.2.6.5		
Version	5	Date	10 aout 2020

Sogelink So easy
Les Portes du Rhône
131, chemin du Bac à Traille
69647 Caluire Cedex
T. 0 820 820 990 - F. 0 820 820 148

www.sogelink.fr

1 Introduction

1.1 Identification du document

La présente Politique de Signature Électronique est identifiée de manière unique par l'OID suivant :

1.3.6.1.4.1.36513.2.6.3

1.2 Contexte

Le présent document est la Politique de Signature Électronique de SOGELINK. Il fait partie intégrante des termes des Conditions Générales d'Utilisation des services de SOGELINK. Le présent document constitue une convention de preuve au sens de l'article 1316-2 du Code civil.

1.3 Définitions

Bi-clef : couple de clefs cryptographiques, composé d'une clef privée (devant être conservée secrète) et d'une clef publique, nécessaire à la mise en œuvre d'opérations de cryptographie basées sur des algorithmes asymétriques.

Autorité de Certification (AC) : entité responsable d'une ICP. L'AC est notamment responsable de la définition et de l'application de la Politique de Certification.

Autorité d'Enregistrement (AE) : entité responsable, au sein d'une ICP, de procéder à l'enregistrement des porteurs de certificats et à la vérification de leur identité.

Archivage électronique : conservation de documents dans un coffre-fort électronique.

Certificat : document électronique contenant la clef publique d'un Porteur de Certificat, ainsi que certaines autres informations attestées par l'Autorité de Certification qui l'a délivré. Un Certificat contient des informations telles que :

- *l'Identité du Porteur de Certificat,*
- *la clef publique du Porteur de Certificat,*
- *les dates de début et de fin de validité du Certificat,*
- *l'Identité de l'Autorité de Certification qui l'a émis,*
- *la signature de l'Autorité de Certification qui l'a émis.*

Un format standard de Certificat est normalisé dans la recommandation X509 V3.

Coffre-fort électronique : dispositif technique permettant la conservation de documents électroniques sur le long terme dans des conditions de nature à en garantir la provenance et l'intégrité. La norme française est AFNOR NF-Z 42 013.

Common Name (CN) : élément du champ 'subject' du certificat comportant l'identité du Porteur de Certificat

Composante de l'ICP : plate-forme constituée d'au moins un poste informatique, une application, un moyen de cryptographie et jouant un rôle déterminé au sein de l'ICP.

Distinguished Name (DN) : nom distinctif X.500 du Porteur de Certificat pour lequel le Certificat est émis. Il constitue le champ 'subject' du certificat et identifie le porteur de manière unique au sein de l'ICP.

Données d'Activation : données connues du Porteur de Certificat uniquement lui permettant de mettre en œuvre sa clef privée.

Empreinte d'un document : voir Hash.

Génération d'un Certificat : action réalisée par une Autorité de Certification et qui consiste à signer le gabarit d'un Certificat édité par une Autorité d'Enregistrement.

Hash d'un document : donnée de longueur fixe résultant d'un calcul mathématique prenant en compte l'ensemble des bits du document.

Horodatage : action d'associer une date à un document ou un événement.

Identité : ensemble des informations définissant un individu (nom, prénom(s)…) ou une entité (dénomination sociale, SIRET…).

Infrastructure à Clef Publique (ICP) : ensemble de composantes, fonctions et procédures dédiés à la gestion des clefs et de Certificats utilisés par des services basés sur la cryptographie à clef publique.

Jeton d'Horodatage : donnée liant de manière infalsifiable une date et un document.

Liste de Certificats Révoqués (LCR) : liste comprenant les numéros de série des Certificats ayant fait l'objet d'une Révocation, signée par l'AC émettrice.

Opérateur de Certification (OC) : entité chargée d'exploiter techniquement l'ICP pour le compte de l'Autorité de Certification.
Parties : terme générique désignant SOGELINK et les Utilisateurs.
Politique de Certification (PC) : ensemble de règles, définissant les exigences auxquelles l'Autorité de Certification se conforme pour l'émission de Certificats adaptés à certains types d'applications.
Porteur de Certificat : personne physique ou morale qui dispose de l'usage légitime du certificat et de la bi- clef associée.
Preuve cryptographique : trace faisant l'objet d'un scellement par un horodatage.
Renouvellement d'un Certificat : opération effectuée à la demande d'un Porteur de Certificat, en fin de période de validité d'un Certificat, qui consiste à générer un nouveau Certificat.
Révocation d'un Certificat : opération demandée par le Porteur de Certificat, par une AC ou une AE, et dont le résultat est la suppression de la garantie de l'AC sur un Certificat donné, avant la fin de sa période de validité. La demande peut être la conséquence de différents types d'événements tels que la compromission d'un bi-clef, le changement d'informations contenues dans un Certificat, etc.
Signature électronique : usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache.
SOGELINK : désigne la société Sogelink SAS.
Traçabilité : dispositif organisé de conservation de données permettant de faire foi des événements s'étant déroulés au sein d'un Système d'Information.
Trace : unité élémentaire d'information conservée par Sogelink.
Utilisateur de Certificat : toute entité qui utilise le Certificat d'un Porteur de Certificat, par exemple pour vérifier une signature électronique.
Utilisateurs : personnes physiques ou morales employant l'ICP dans le cadre de l'utilisation des services de SOGELINK.

2 Règles générales

2.1 Infrastructure à Clefs Publiques mise en oeuvre

Les signatures électroniques réalisées dans les services de SOGELINK s'appuient sur l'ICP SOGELINK, qui se fonde sur le certificat autosigné SOGELINK RACINE, régie par la Politique de Certification publiée sur le site Internet de SOGELINK.
Les certificats d'Autorité d'Horodatage SOGELINK HORODATAGE exploités par SOGELINK sont émis directement par SOGELINK RACINE conformément à sa PC. Ils sont employés pour délivrer des jetons d'horodatage conformément à la Politique d'Horodatage.

2.2 Domaines d'application

Les signatures électroniques réalisées dans les services de SOGELINK sont destinés à être utilisées uniquement dans le cadre des services de SOGELINK
Les signatures électroniques réalisées par les services de signature électronique de SOGELINK ne portent que sur des documents générés ou échangés via la plate-forme de services de SOGELINK dans le cadre des services offerts par SOGELINK.
SOGELINK ne saurait endosser aucune responsabilité relativement à des documents non générés, non signés ou non conservés dans le cadre des services dématérialisés de SOGELINK.
SOGELINK ne saurait endosser aucune responsabilité dans les cas où un ou des documents provenant des services dématérialisés de SOGELINK seraient employés à titre de preuve dans un contexte différent.

2.3 Publication

La dernière version de la présente Politique est publiée sur le site institutionnel de SOGELINK.
L'historique des versions de la présente Politique est conservé au sein d'un dispositif d'archivage électronique à valeur probatoire et est disponible sur demande motivée auprès de SOGELINK.

2.4 Conservation

Les versions successives des Politiques, LCR et certificats générés sont archivés par SOGELINK pour une durée de 5 ans à l'issue de leur fin de validité.

3 Signature électronique des utilisateurs

3.1 Contexte

Pour des raisons de coûts, de fluidité et de simplicité des procédures, SOGELINK a souhaité ne pas imposer à ses utilisateurs l'acquisition d'un certificat de signature électronique du marché.
La plate-forme de services de SOGELINK inclut donc un service de signature électronique à la demande, permettant à un utilisateur de signer électroniquement des documents sans disposer préalablement d'un certificat.
Le présent chapitre décrit le fonctionnement de ce service.

3.2 Gestion des comptes des établissements

Le représentant légal de tout établissement (entreprise, association ou collectivité publique) disposant d'un compte sur la plate-forme de services de SOGELINK est responsable de tenir à jour sans délai les informations et coordonnées relatives à cet établissement.
A cette fin, il peut nommer un administrateur du compte de l'établissement, qui dispose d'un accès à une interface d'administration, ou faire appel au support client de SOGELINK.
Dans tous les cas, SOGELINK n'endosse aucune responsabilité en cas d'inexactitude des informations constitutives du compte d'un établissement, cette responsabilité incombant entièrement et exclusivement au représentant légal de l'établissement.

3.3 Gestion des comptes des utilisateurs

Le représentant légal de tout établissement disposant d'un compte sur la plate-forme de services de SOGELINK peut créer des comptes sur cette plate-forme pour les membres de son établissement, appelés utilisateurs.
A cette fin, il peut nommer un administrateur du compte de l'établissement, qui dispose d'un accès à une interface d'administration, ou faire appel au support client de SOGELINK.
Le représentant légal de l'établissement est responsable de tenir à jour sans délai les informations et coordonnées relatives aux comptes des utilisateurs membres de son établissement.
Dans tous les cas, SOGELINK n'endosse aucune responsabilité en cas d'inexactitude des informations constitutives du compte d'un utilisateur membre d'un établissement, cette responsabilité incombant entièrement et exclusivement au représentant légal de l'établissement.
Les utilisateurs agissant en tant que particuliers sont responsables, entièrement et exclusivement, de tenir à jour sans délai les informations et coordonnées relatives à leur compte personnel.
Dans tous les cas, SOGELINK n'endosse aucune responsabilité en cas d'inexactitude des informations constitutives du compte d'un utilisateur individuel, cette responsabilité incombant entièrement et exclusivement à l'utilisateur.

3.4 Accès aux services de SOGELINK

Le représentant légal de tout établissement est responsable de porter à la connaissance des membres de son établissement les clauses contractuelles qui régissent les relations entre l'établissement et SOGELINK et en particulier les Conditions Générales d'Utilisation des services dématérialisés de SOGELINK et la présente Politique de Signature Électronique.
Il est responsable des actions réalisées par les membres de son établissement au sein des services dématérialisés de SOGELINK.
Il est notamment responsable de l'attribution du droit d'accès aux services et en particulier du droit de réaliser des signatures électroniques.
Ainsi toute signature électronique réalisée au sein des services dématérialisés de SOGELINK le sera par la volonté et au nom d'un utilisateur, qui sera considéré comme dûment habilité à engager l'établissement auquel il appartient et au nom duquel il agit pour l'acte sur lequel il prend un engagement via cette signature.
De la même manière, l'utilisateur individuel prend connaissance des documents contractuels régissant

sa relation avec SOGELINK, et assume seul la responsabilité des signatures électroniques qu'il réalise au sein des services dématérialisés de SOGELINK et de leurs conséquences en termes d'engagement.

3.5 Moyens d'authentification

Lors de la création de son compte, tout utilisateur se voit remettre, sous la responsabilité du représentant légal de l'établissement auquel il appartient, ou sous sa responsabilité propre pour les utilisateurs individuels, des moyens d'authentification, constitués d'un courrier électronique contenant un lien d'activation.
Lors de sa première connexion au site, l'utilisateur a l'obligation de définir son mot de passe, dont il conservera seul la connaissance et qu'il gardera sous son contrôle exclusif.

3.6 Procédé fiable d'identification

Les parties reconnaissent que l'identifiant et le mot de passe de l'utilisateur constituent un procédé fiable d'identification et d'authentification.
Toute signature électronique réalisée au sein des services de SOGELINK suite à la présentation de ces moyens d'authentification est réputée avoir été réalisée par l'utilisateur qu'ils identifient au sein des services de SOGELINK.

3.7 Déroulement fonctionnel de l'acte de signature

Au sein des services de SOGELINK, l'acte de signature est clairement mis en exergue de plusieurs manières :

- *un texte explicite est présenté au signataire pour lui expliciter la portée de l'acte qu'il s'apprête à réaliser ;*
- *le ou les documents que l'utilisateur s'apprête à signer lui sont présentés : il a la possibilité de visualiser une copie du document ou un résumé des données le constituant ;*
- *si le document à signer a déjà été signé par un ou plusieurs autres signataires, les signatures déjà réalisées sont présentées à l'utilisateur ;*
- *l'utilisateur a la possibilité de renoncer et de ne pas signer ;*
- *l'utilisateur doit cocher une case pour marquer sa volonté de signer ;*
- *l'utilisateur doit être authentifié pour accéder au service ;*
- *l'utilisateur doit activer un bouton de signature à l'intitulé explicite (« signer » par exemple). Les*

documents signés sont exclusivement au format PDF.

Une fois l'authentification réalisée, la case d'engagement cochée et le bouton de signature activé par l'utilisateur, les opérations suivantes se déroulent automatiquement :

- *le service de signature de SOGELINK vérifie qu'il existe une session active au nom de l'utilisateur, dont l'ouverture a nécessité la saisie de son mot de passe : sinon, l'opération de signature est interrompue sans qu'aucune signature n'ait été réalisée ;*
- *une bi-clef RSA de 2048 bits est générée ;*
- *un certificat de signature portant sur la clef publique de cette bi-clef est généré au nom du signataire et de l'établissement auquel il appartient, conformément à la Politique de Certification de l'Autorité de Certification SOGELINK SIGNATURE ;*
- *la clef privée de la bi-clef est utilisée pour réaliser une signature électronique SHA1-RSA sur chaque document à signer ;*
- *chaque signature est horodatée conformément à la Politique d'Horodatage de SOGELINK ;*
- *chaque signature électronique est incluse conformément au format PAdES dans le document correspondant ;*
- *les documents signés sont traités et conservés dans le cadre du service de SOGELINK.*

Dans certains des services de SOGELINK, la signature électronique des documents est subordonnée au paiement en ligne du service ou à des opérations techniques de mise en forme réalisées de manière légèrement différée dans le temps. Dans ce cas, le ou les documents à signer sont mis en attente de cet événement, et il peut exister un décalage temporel entre la validation de la demande de signature et sa réalisation effective. Les étapes du processus demeurent toutefois les mêmes.

3.8 Autorité de certification

L'Autorité de Certification qui émet les certificats de signature électronique employés par les utilisateurs sur la plate-forme de services de SOGELINK est SOGELINK SIGNATURE.
On se reportera à la Politique de Certification de SOGELINK SIGNATURE pour plus de détails.
Les parties reconnaissent avoir pris connaissance et accepter la Politique de Certification de SOGELINK SIGNATURE et les obligations qui en découlent.

3.8.1 Révocation

Du fait de la courte durée de vie des certificats générés (1 jour), la révocation des certificats n'est pas nécessaire. Une Liste de Certificats Révoqués est néanmoins émise pour des raisons techniques. Le

point de distribution de la Liste des Certificats Révoqués est indiqué dans les certificats.

3.8.2 Horodatage

Les signatures électroniques générées sont horodatées par le service de signature électronique de SOGELINK conformément à la Politique d'Horodatage de SOGELINK HORODATAGE.

4 Format des signatures électroniques

4.1.1 Stockage des signatures

Les signatures électroniques sont incluses dans les documents signés conformément au format PAdES.
Les jetons d'horodatage qui y sont inclus sont conformes à la RFC 3161 de l'IETF et leur inclusion suit les recommandations de l'APPENDIX A de cette même norme.
Lorsque plusieurs signatures portent sur le même document, ces signatures sont stockées au sein du même fichier.

4.1.2 Garantie du lien entre la signature et le document

Le protocole standard de signature SHA1-RSA garantit techniquement un lien entre la signature électronique et le document sur lequel il porte. Toute modification ultérieure du document sera détectable par l'opération de vérification de signature.

4.1.3 Mode de vérification des signatures électroniques

Les signatures électroniques réalisées au sein des services dématérialisés de SOGELINK peuvent être vérifiées en utilisant les fonctions natives de l'outil Adobe ® Reader ®, disponible gratuitement sur Internet.
Elles peuvent également être vérifiées par tout autre outil implémentant les normes SHA1-RSA, TSP et PAdES.

5 Engagement

5.1 Documents originaux faisant foi

Les documents signés via les services de SOGELINK sont des documents constitutifs des procédures métier relatives à ces services.
Ces documents étant générés, signés électroniquement et échangés via la plate-forme, les parties reconnaissent que les originaux faisant foi sont ceux qui sont conservés par SOGELINK au sein de son service.

5.2 Valeur des signatures

Les parties reconnaissent la conformité des signatures électroniques réalisées via les services de SOGELINK avec l'article 1316-4 du Code civil.
Les parties reconnaissent que la signature réalisée conformément aux protocoles décrits dans la présente Politique de Signature manifeste le consentement du signataire aux obligations qui découlent de l'acte signé.

5.3 Publication

La dernière version de la présente Politique de Signature Électronique est publiée sur le site institutionnel de SOGELINK.
L'historique des versions de la présente Politique de Signature Électronique est conservé au sein d'un dispositif d'archivage électronique à valeur probatoire et est disponible sur demande motivée auprès de SOGELINK.

6 Dispositions applicables et règlement des litiges

6.1 Dispositions applicables

Il est expressément entendu qu'en l'état de la pratique et des textes législatifs et réglementaires en vigueur, les signatures électroniques réalisées en vertu de la présente Politique de Signature Électronique sont des signatures électroniques simples dont les conditions d'utilisation sont définies par la présente Politique de Signature et par la Convention de Preuve incluse dans les Conditions Générales d'Utilisation des services de SOGELINK. La présente Politique de Signature Électronique est susceptible d'être adaptée, si nécessaire, en fonction de toute évolution législative et réglementaire qui pourra avoir un impact sur les conditions de réalisation, de vérification ou de conservation des signatures électroniques ou sur les obligations respectives des intervenants.

6.2 Loi applicable et résolution des litiges

La présente Politique de Signature Électronique est soumise au droit français. Tout litige relatif à la validité, l'interprétation, l'exécution de la présente Politique de Signature Électronique sera porté devant la juridiction compétente pour connaître de ce litige.

6.3 Modifications des spécifications et des composantes du service de signature électronique

SOGELINK procède à toute modification des spécifications de son service de signature électronique qui lui apparaît nécessaire pour l'amélioration de la qualité de ses services et de la sécurité des processus.
SOGELINK procède également à toute modification des spécifications de son service de signature électronique qui est rendue nécessaire par une législation ou réglementation en vigueur.
SOGELINK informera les utilisateurs de telles modifications dès lors qu'il s'agit de modifications majeures ayant un impact déterminant.
L'information sera effectuée par SOGELINK par tout moyen, notamment à l'aide de message électronique spécifique ou via la publication de l'information sur son site web.