Politique de Traçabilité et de Gestion de Preuves

OID	1.3.6.1.4.1.36513.2.4.2		
Version	2	Date	31 juillet 2015

1 Introduction

1.1 Identification du document

La présente Politique de Gestion de Preuves est identifiée de manière unique par l'OID suivant :

1.3.6.1.4.1.36513.2.4.2

1.2 Contexte

Le présent document est la Politique de Traçabilité et de Gestion de Preuves 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 conservée dans un dispositif de traçabilité 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 La traçabilité des services de SOGELINK

En validant les Conditions Générales d'Utilisation des services de SOGELINK, dont la présente Politique de Traçabilité et de Gestion de Preuves fait partie intégrante, chaque utilisateur reconnaît la validité à titre de preuve des preuves générées par ces services, conformément à la Convention de Preuve de ces services, rédigée et acceptée par tous en vertu de l'article 1316-2 du Code civil.

Ce sont ces preuves, décrites dans la présente Politique de Traçabilité et de Gestion de Preuves, qui font foi du bon déroulement des événements qui se déroulent au sein des services de SOGELINK, et des paramètres pris en compte dans leur réalisation.

2.2 Traces applicatives

Les événements qui se déroulent au sein des services de SOGELINK sont de deux natures :

- les événements automatiques, réalisés par le système régulièrement à date programmée, ou ponctuellement en fonction de l'état des données ;
- les actions des utilisateurs : création ou modification de compte, validation des Conditions Générales, etc.

Chacun de ces événements donne lieu à la création de traces conservées par Sogelink. Ces traces peuvent être stockées sur un système de fichier ou en base de données. Le présent document ne décrit pas la liste des traces applicatives.

2.3 Preuves cryptographiques

Certains événements à forte implication juridique donnent lieu, en plus des traces applicatives, à la génération d'une unité de traçabilité autonome, scellée cryptographiquement par un horodatage. Le présent document décrit la liste de ces preuves cryptographiques et des paramètres qui les composent, ainsi que la manière de les interpréter.

2.4 Politiques applicables

Les preuves cryptographiques sont générées et conservées conformément à :

- la Politique d'Horodatage de SOGELINK ;
- la Politique d'Archivage Électronique de SOGELINK.

Ces documents font partie intégrante des Conditions Générales d'Utilisation des services de SOGELINK.

2.5 Ordre de priorité des traces

La traçabilité des événements des services de SOGELINK sera systématiquement interprétée à partir des éléments suivants, dans cet ordre de priorité :

1. la ou les preuves cryptographiques correspondantes ;
2. la ou les traces applicatives correspondantes ;
3. en l'absence de ces éléments de preuve, tout autre élément de preuve pertinent pouvant être présenté par une des parties.

2.6 Conservation et consultation de la traçabilité

Les traces applicatives sont conservées au moins un an au sein des services de SOGELINK.

Les preuves cryptographiques sont conservées 5 ans au sein du coffre-fort d'archivage électronique de SOGELINK.

L'accès aux éléments de traçabilité est réalisé par un administrateur de SOGELINK.

Afin que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité, chaque preuve fera l'objet d'un scellement cryptographique et d'un archivage auprès d'un tiers archiveur, dans le respect de la norme NF/Z 42-013 et conformément à la Politique d'Archivage de SOGELINK.

3 Les preuves cryptographiques

3.1 Format des traces applicatives

Les traces applicatives pour lesquelles le service doit générer une preuve sont enregistrées en base de données. Elles comportent :

- un identifiant unique de preuve, croissant et sans interruption ;
- une date et heure système de réalisation de la trace ;
- une identification du service au sein duquel la trace est générée ;
- un identifiant de type d'événement ;
- un enregistrement de l'événement concerné et de ses paramètres pertinents sous la forme d'un fichier descriptif.

Chaque preuve cryptographique est constituée d'un fichier archive contenant :

- un fichier descriptif reprenant les éléments de la trace correspondante ;
- un horodatage réalisée conformément à la Politique d'Horodatage de SOGELINK.

3.2 Valeurs des champs

Certains champs comportent une valeur dont la teneur est évidente (par exemple, le champ « nom » comportera le nom de la personne).

D'autres champs comportent un code dont la valeur renvoie à une liste d'items possibles.

Pour les champs contenant des codes, la liste des valeurs et de leurs correspondances n'est pas incluse dans le présent document mais est disponible sur demande motivée.

3.3 Liste et interprétation des traces applicatives

Les événements donnant lieu à la génération d'une preuve cryptographique sont décrits ci-dessous. Sur demande motivée SOGELINK pourra présenter un devis à la charge exclusive du demandeur pour la fourniture du descriptif des preuves cryptographique et la sémantique des champs utilisés.

3.3.1 Validation des CGU et CPU

Lors de la validation des Conditions Générales d'Utilisation (CGU) ou des Conditions Particulières d'Utilisation (CPU), une preuve est générée indiquant l'application utilisée, le ou les documents validés ainsi que l'identification de l'utilisateur.

3.3.2 Etat du référencement au moment de la validation d'une demande dans DICT.fr

Lors de la validation d'une demande utilisant une liste de référencement, une preuve est créée indiquant l'état du référencement (grâce au dossier de consultation concerné) ainsi que les listes des destinataires sélectionnés (cochés) et ignorés (décochés) par l'utilisateur.

3.4 Vérification et interprétation des preuves cryptographiques

Les preuves cryptographiques peuvent être vérifiées par les opérations suivantes :

Les étapes de la vérification d'une preuve sont les suivantes :

- vérification du format de la preuve :
  - il s'agit d'une archive,
  - il contient un horodatage et un fichier descriptif ;
- extraction de l'archive des deux fichiers qu'il contient ;
- vérification du fichier descriptif :
  - il est bien formé,
  - il s'agit bien d'une preuve générée par l'application ;
- vérification du jeton d'horodatage :
  - il est bien formé,
  - il est généré par l'Autorité d'Horodatage SOGELINK HORODATAGE,
  - sa signature est valable,
  - sa signature porte bien sur le hash du fichier descriptif.
- interprétation du contenu du fichier descriptif conformément à la description faite plus haut dans le présent document.

Les vérifications cryptographiques peuvent être réalisées avec tout outil implémentant la norme publique employée pour réaliser les horodatages. Il existe des implémentations open source de tels outils, librement disponibles.

L'horodatage apposé sur la preuve cryptographique doit être interprété comme suit : au jour et à l'heure indiqués dans le jeton d'horodatage, interprété conformément à la Politique d'Horodatage de SOGELINK, SOGELINK certifie que l'événement décrit dans le fichier descriptif a bien eu lieu.

4 Obligations

4.1 Obligation de SOGELINK

4.1.1 Génération

SOGELINK s'engage à ce que les services soumis à la présente Politique de Traçabilité et de Gestion de Preuves procèdent à la génération des preuves cryptographiques décrites dans la présente Politique lors du déroulement des événements correspondants.

SOGELINK s'engage à mettre en œuvre les corrections nécessaires dans des délais raisonnables en cas d'incident ou d'erreur empêchant la génération des preuves cryptographiques.

SOGELINK s'engage à ce que ses services ne procèdent jamais à la génération de preuves cryptographiques décrites dans la présente Politique hors du déroulement des événements correspondants.

SOGELINK garantit l'exactitude des données contenues dans les traces et les preuves cryptographiques, dans la limite de la sincérité des Utilisateurs pour les données transmises de manière déclarative.

SOGELINK garantit l'unicité et la séquentialité des identifiants de traces.

SOGELINK garantit le maintien à l'heure de serveurs avec une dérive par rapport à l'heure de référence ne pouvant pas dépasser une minute.

L'unicité et la séquentialité de l'identifiant de trace sont garanties par l'utilisation d'un mécanisme natif de la base de données.

La date et l'heure système sont maintenues grâce à l'utilisation du protocole NTP.

4.1.2 Conservation

SOGELINK s'engage à conserver les traces et les preuves cryptographiques réalisées en respect de la présente Politique dans des conditions de nature à en garantir la provenance et l'intégrité.

Cette conservation est réalisée conformément à la Politique d'Archivage Électronique de SOGELINK.

4.1.3 Présentation

SOGELINK s'engage à présenter aux Utilisateurs les traces et preuves cryptographiques générées au cours des événements qui les concernent. Sur demande motivée SOGELINK pourra présenter un devis pour la présentation de ces traces et preuves à la charge exclusive du demandeur.

4.2 Obligation des Utilisateurs

4.2.1 Respect de la Politique de Traçabilité et de Gestion de Preuves

Les Utilisateurs reconnaissent la validité de la présente Politique.

Les Utilisateurs reconnaissent la mise en œuvre diligente et sincère de la présente Politique par SOGELINK. En particulier, les Utilisateurs reconnaissent l'exhaustivité et la pertinence des traces et preuves cryptographiques générées en vertu de la présente Politique et acceptent que ces éléments tiennent lieu de preuves et fassent foi dans la résolution d'éventuels litiges.

Les Utilisateurs s'engagent à respecter les termes de la présente Politique, notamment en termes d'interprétation des traces et preuves cryptographiques générées par SOGELINK.

4.3 Contacts et organisation dédiée à la Politique de Traçabilité et de Gestion de Preuves

4.3.1 Organisation dédiée

SOGELINK est responsable de l'élaboration, du suivi et de la modification dès que nécessaire de la présente Politique. A cette fin elle a mis en œuvre une organisation dédiée coordonnée par un Responsable de la Certification. L'organisation dédiée statue sur toute modification nécessaire à apporter à la Politique.

4.3.2 Contact

Le Responsable de la Certification est le seul contact habilité vis-à-vis des organisations extérieures à SOGELINK.

Coordonnées :

SOGELINK

M. le Responsable de la Certification

131 Chemin du Bac a Traille - Les Portes du Rhône - 69647 CALUIRE ET CUIRE CEDEX

4.4 Dispositions applicables et règlement des litiges

4.4.1 Dispositions applicables

Il est expressément entendu qu'en l'état de la pratique et des textes législatifs et réglementaires en vigueur, la présente Politique constitue une convention de preuve valide au sens de l'article 1316-2 du Code civil.

La présente Politique est susceptible d'être adaptée, si nécessaire, en fonction de toute évolution législative et réglementaire qui pourra avoir un impact sur les conditions d'émission, de gestion des traces applicatives et des preuves cryptographiques ou sur les obligations respectives des intervenants.

Les relations entre SOGELINK et l'Utilisateur sont régies par les dispositions de la présente Politique, les Conditions Générales et Particulières d'Utilisation (CGU et CPU) des services de SOGELINK.

4.4.2 Loi applicable et résolution des litiges

La présente Politique est soumise au droit français.

Tout litige relatif à la validité, l'interprétation, l'exécution de la présente Politique sera porté devant la juridiction compétente pour connaître de ce litige.

4.5 Modifications des spécifications et des composantes de l'AC

SOGELINK procède à toute modification des spécifications stipulées dans la présente Politique et/ou des composantes de l'infrastructure de traçabilité correspondante qui lui apparaît nécessaire pour l'amélioration de la qualité des services et de la sécurité des processus.

SOGELINK procède également à toute modification des spécifications stipulées dans la présente Politique et/ou des composantes de l'infrastructure de traçabilité correspondante 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.