Politique de Certification

Sogelink Racine

OID	1.3.6.1.4.1.36513.2.1.2		
Version	2	Date	31 juillet 2015

1 Introduction

1.1 Identification du document

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

1.3.6.1.4.1.36513.2.1.2

1.2 Contexte

Le présent document est la Politique de Certification de l'Autorité de Certification SOGELINK RACINE.

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.

1.4 Avertissement

Lorsqu'une Autorité de Certification (AC) émet un Certificat, elle indique de ce fait à l'Utilisateur de Certificat qu'une clef publique spécifique est associée à un Porteur de Certificat spécifique, identifié par le Distinguished Name (DN) du Certificat.

Un Certificat peut être émis selon des pratiques et des procédures différentes, et peut convenir à des applications et/ou des fins diverses.

Et, conformément à la norme X.509, une Politique de Certification (PC) constitue un ensemble de règles qui prescrivent l'applicabilité d'un Certificat à une collectivité et/ou à une classe d'applications particulières ayant des exigences communes en matière de sécurité.

En conséquence et compte tenu de la grande importance des PC pour établir la confiance à l'égard d'un Certificat, il est primordial que la présente PC soit bien comprise et soit consultée non seulement par les Porteurs de Certificat, mais également par tout Utilisateur de Certificat.

L'attention du lecteur est attirée sur le fait que la compréhension de la présente PC suppose que le lecteur soit familiarisé avec les notions liées à la technologie des Infrastructures à Clefs Publiques (ICP).

2 Règles générales

2.1 Infrastructure à Clefs Publiques mise en oeuvre

L'ICP SOGELINK, dont la racine SOGELINK RACINE est régie par la présente PC, est constituée de la racine autosignée, des certificats d'Autorité d'Horodatage qu'elle émet, d'un certificat d'Autorité de Certification SOGELINK SIGNATURE subordonné à SOGELINK RACINE, et des certificats émis par SOGELINK SIGNATURE pour les utilisateurs.

Sogelink joue à la fois les rôles d'AC, d'OC et d'AE.

2.2 Domaines d'application

L'ICP SOGELINK et en particulier la racine SOGELINK RACINE ne sont destinées à être employées que dans le cadre des services de SOGELINK.

2.3 Nommage

Le CN de la racine SOGELINK est nommé comme suit :

CN=SOGELINK Racine
O=SOGELINK
C=FR

Le certificat racine est publié dans le fichier nommé : SOGELINKRacine.cer

La LCR correspondante est publiée dans le fichier nommé : SOGELINKRacine.crl

2.4 Publication

La dernière version de la présente PC est publiée sur le site institutionnel de SOGELINK.

L'historique des versions de la présente PC est conservé au sein d'un dispositif d'archivage électronique à valeur probatoire et est disponible sur demande motivée auprès de SOGELINK.

La dernière version de la LCR est accessible sur le site de SOGELINK à l'URL désignée dans le champ CRLDP des certificats émis.

Le certificat racine de l'ICP SOGELINK est mis à disposition sur le site institutionnel de SOGELINK.

L'historique des certificats racine successifs est conservé au sein d'un dispositif d'archivage électronique à valeur probatoire et est disponible sur demande motivée auprès de SOGELINK.

2.5 Conservation

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

3 Règles de gestion du cycle de vie des certificats

3.1 Intervenants

3.1.1 L'Autorité de Certification

L'AC responsable de la présente PC est SOGELINK.

L'AC est responsable de l'ensemble de l'Infrastructure à Clef Publique qu'elle a mise en place. Pour les Certificats signés en son nom, l'AC assure les fonctions suivantes :

- gestion de l'ensemble de l'Infrastructure à Clef Publique qu'elle a mise en place ;
- mise en application de la présente PC ;
- émission des Certificats ;
- gestion de la révocation des certificats ;
- gestion des Certificats.

L'AC assure ces fonctions directement ou en les sous-traitant, tout ou partie. Dans tous les cas, l'AC en garde la responsabilité.

3.1.2 L'Autorité d'Enregistrement

Les fonctions suivantes sont constitutives du rôle d'AE :

- gestion des demandes de Certificats ;
- vérification de l'Identité du Porteur de Certificat ;
- enregistrement des Porteurs de Certificats ;
- information du Porteur de Certificat sur les contraintes liées à l'usage d'un Certificat ;
- traçabilité des demandes de Certificats ;
- vérification des demandes de Révocation de Certificats.

3.1.3 L'Opérateur de Certification

L'OC est responsable vis-à-vis de l'AC de l'exploitation technique du service de génération des certificats et de leur acheminement vers les Porteurs de Certificats. Ses rôles sont les suivants :

- garantir la sécurité des clefs d'AC ;
- recevoir les demandes de certificats ;
- s'assurer du bon format de ces demandes ;
- procéder à la génération des certificats dans les conditions prévues par la présente PC ;
- procéder à la révocation des certificats à la demande de l'AE et tenir à jour la LCR.

Sogelink assure les fonctions d'Opérateur de Certification, et se réserve la faculté de sous-traiter l'hébergement et l'exploitation technique des composantes de l'ICP.

3.1.4 Le Porteur de Certificat

Les certificats délivrés par SOGELINK RACINE sont de deux natures :

- des certificats d'Autorité d'Horodatage, destinés à être employés conformément à la Politique d'Horodatage de Sogelink ;

- des certificats d'Autorité de Certification subordonnée, destinés à être employés conformément à la Politique de Certification SOGELINK SIGNATURE et à la Politique de Signature Électronique de SOGELINK.

Pour ces deux types de certificats, le porteur de certificat est SOGELINK.

Le porteur a les responsabilités suivantes :
- conserver secrète et garder sous son contrôle exclusif la clef privée correspondant à son Certificat ;
- conserver secrètes et garder sous son contrôle exclusif les données d'activation de cette clef privée.

3.1.5 L'Utilisateur de Certificat

L'Utilisateur de Certificat est toute personne qui utilise un certificat émis par l'ICP SOGELINK pour vérifier une signature électronique ou un horodatage. Il est de la responsabilité de l'Utilisateur de Certificat de n'utiliser ce certificat que dans le cadre applicatif défini par la présente Politique de Certification et par les Conditions Générales d'Utilisation des services de SOGELINK.

3.2 Les types d'applications et les fournisseurs de services

Il est expressément entendu que la présente PC n'autorise l'utilisation des Certificats émis en vertu de cette PC qu'à des fins de génération de certificats d'Autorités d'Horodatage ou d'Autorités de Certification subordonnées dans le cadre des services de SOGELINK.

3.2.1 Fournisseurs de service

Le fournisseur de service est l'entité qui fournit un service nécessitant l'usage des Certificats. Un tel service est appelé Application. Une Application cible est une application dans le cadre de laquelle l'usage des Certificats émis au titre de la présente PC est autorisé. Le seul Fournisseur de service habilité à employer les certificats émis au titre de la présente PC au sein de l'Application qu'il fournit est SOGELINK.

3.2.2 Application cible

Les seules Applications cibles sont les services rendus par SOGELINK.

3.2.3 Applications hors cibles

Il s'agit de toute Application qui ne figure pas dans la liste des Applications cibles.

En tant qu'Autorité de Certification, SOGELINK ne saurait être responsable de l'utilisation d'un Certificat dans le cadre d'une Application hors cible. Étant rappelé que tout Utilisateur a, conformément aux usages en la matière, l'obligation d'identifier et contrôler la PC en vertu de laquelle le Certificat qu'il utilise est émis, et en particulier la liste des applications cibles.

3.3 Obligations

3.3.1 Obligations de l'AC

L'AC s'engage à mettre en œuvre les moyens décrits dans la présente PC afin de permettre d'assurer :
- la qualité et sécurité des prestations auxquelles elle s'engage ;
- la définition d'un cadre contractuel entre elle et chaque Porteur de Certificat par lequel notamment seront définis les droits et obligations de l'AC et du Porteur de Certificat concerné ;
- le respect des dispositions contractuelles susvisées ;
- l'utilisation de sa clef privée de signature de Certificat aux seules fins de signature des Certificats, des jetons d'horodatage et des LCR ;
- la protection de ses clefs privées et ses Données d'Activation.

3.3.1.1 S'agissant des fonctions de gestion des Certificats

L'AC s'engage à mettre en œuvre les moyens décrits dans la présente PC afin de permettre d'assurer :
- l'émission et la délivrance du Certificat au Porteur de Certificat ;
- la conformité des informations contenues dans le Certificat avec les informations recueillies aux fins de délivrance de Certificats ;
- la mise en œuvre des procédures de Renouvellement des Certificats conformément à la présente PC ;
- la mise en œuvre des procédures de Révocation des Certificats conformément à la présente PC.

3.3.1.2 S'agissant de la fonction de publication

L'AC s'engage à mettre en œuvre les moyens décrits dans la présente PC afin d'assurer la publication et l'accès à la présente Politique de Certification, au certificat racine et à la LCR.

3.3.2 Obligations de l'OC

L'OC s'engage à ne transmettre les bi-clefs et certificats émis au titre de la présente PC qu'aux seuls destinataires dont les coordonnées ont été transmises par l'AC dans les requêtes de certification.

L'OC s'engage à ne jamais procéder, pour son propre compte ou pour le compte d'un tiers autre que le Porteur de Certificat, de copie de bi-clef ou de moyens d'activation de bi-clef.

L'OC s'engage à ne jamais procéder ou tenter de procéder, pour son compte ou pour le compte d'un tiers, à la génération d'un certificat par SOGELINK RACINE en-dehors du cadre de la présente PC et des demandes légitimes validées par l'AC.

3.3.3 Obligations de l'AE

L'AE s'engage à mettre en œuvre les moyens décrits dans la présente PC afin de permettre d'assurer :

- la vérification de la compatibilité des informations recueillies avec celles exigées par la présente PC pour la délivrance de Certificats ;
- la conformité des informations contenues dans le Certificat avec les informations recueillies aux fins de délivrance de Certificats ;
- la vérification de l'authenticité d'une demande de Révocation qui lui est soumis conformément à la présente PC.

3.3.4 Obligations du Porteur de Certificat

L'AC est liée contractuellement avec chaque Porteur de Certificat pour l'émission de Certificats.

Le Porteur de Certificat est responsable des obligations ci-après mentionnées :

- garantir l'authenticité, le caractère complet et à jour des informations communiquées lors de la demande de Certificat ainsi que des documents qui accompagnent ces informations ;
- informer sans délai l'AE et l'AC de toute modification relative à ces informations et/ou documents ;
- assurer l'information des personnes mandatées pour l'utilisation des certificats dans le cadre des Applications Cibles sur les conditions d'utilisation des Certificats, de la gestion des clefs ou encore de l'équipement et des logiciels permettant de les utiliser ;
- faire protéger la clef privée de chaque Certificat par des moyens appropriés à son environnement ;
- faire protéger les Données d'Activation de chaque Certificat par des moyens appropriés à leur environnement ;
- faire respecter les conditions d'utilisation de la clef privée et du Certificat correspondant, notamment l'utilisation dans le strict cadre des applications décrites par la présente PC ;
- faire demander la Révocation d'un Certificat dès lors qu'elle est nécessaire ;
- faire informer sans délai l'AE ou l'AC en cas de compromission ou de suspicion de compromission de la clef privée.

3.3.5 Obligations des Utilisateurs de Certificats

Pour permettre une utilisation d'un Certificat, dans des conditions optimales de sécurité, il est rappelé que l'Utilisateur doit :

- avoir pris connaissance de la PC en vertu de laquelle le Certificat qui lui est adressé est émis afin de lui permettre notamment :
  - de refuser un Certificat qui ne serait pas utilisé conformément à la présente PC et notamment qui serait utilisé hors du champ des Applications cibles définies par la présente PC,
  - de vérifier l'objet pour lequel le Certificat est émis ;
- contrôler ou avoir connaissance de la validité de la signature électronique de l'AC émettrice du Certificat ;
- contrôler la validité des Certificats en vérifiant la date de validité du Certificat et la LCR, afin de lui permettre de refuser tout Certificat révoqué ou ayant expiré.

L'AC n'est pas responsable des conséquences dommageables qui seraient dues au non respect par les Utilisateurs des contrôles ci-dessus rappelés.

3.3.6 Obligations du Fournisseur de Service

En tant que fournisseur de services, SOGELINK s'engage à publier sur son site le certificat racine de l'ICP SOGELINK.

3.4 Processus du cycle de vie des certificats

3.4.1 Génération des certificats émis par SOGELINK RACINE

La génération ou le renouvellement d'un certificat racine, d'un certificat d'AC subordonnée ou d'un certificat d'AH est un processus interne à SOGELINK qui sera mené en fonction des besoins identifiés au fur et à mesure de la vie des services et de l'ICP de SOGELINK.

Toute génération d'un certificat donne lieu à la tenue d'une Cérémonie de Génération de Certificat au cours de laquelle, en présence de témoins, ont lieu les opérations suivantes :

- vérification de la demande réalisée, dont les données sont fonction du rôle dévolu au nouveau certificat ;
- s'il s'agit d'un certificat secondaire : vérification que la durée de vie de l'AC racine est suffisante pour couvrir la durée de vie du certificat secondaire ;
- génération de la bi-clef ;
- génération des moyens d'activation ;
- protection de la bi-clef par les moyens d'activation ;
- génération du certificat correspondant ;
- si le certificat est lui-même destiné à générer d'autres certificats :
  - contrôle de l'existence de la PC correspondante,
  - génération de la LCR correspondante ;
- dans tous les cas, contrôle de l'existence des documents contractuels régissant l'usage du certificat (Politique d'Horodatage par exemple) ;
- publication des informations sur le site de SOGELINK.

La Cérémonie de Génération des Certificats a lieu sous la responsabilité de SOGELINK.

3.4.2 Révocation d'un certificat émis par SOGELINK RACINE

Lorsque l'une des circonstances ci-dessous se produit, le Certificat concerné doit être révoqué et inscrit dans la LCR ; il cesse également d'être utilisé dans le cadre des services de SOGELINK :

- changement dans les informations et/ou documents communiqués lors de la demande de Certificat avant l'expiration normale du Certificat,
- non respect par le Porteur de Certificat des modalités applicables à l'utilisation du Certificat ;
- perte, vol, compromission ou suspicion de compromission de la clef privée associée à la clef publique certifiée ;
- demande de Révocation émanant du Porteur de Certificat ;
- révocation du Certificat de l'AC (ce qui entraîne la Révocation des Certificats signés par la clef privée correspondante) ;
- cessation d'activité du Porteur de Certificat ;
- évolution de l'état de l'art cryptographique : par exemple lorsque la taille des clefs ou les algorithmes de chiffrement deviennent obsolètes ;
- il a été démontré une fraude dans le dossier de demande de Certificat.

S'agissant d'une ICP à usage interne à SOGELINK, les modalités de demande de révocation seront gérées selon les règles en vigueur au sein de SOGELINK.

La révocation sera effective lorsque la LCR incluant le numéro de série du certificat incriminé aura été publiée et que le certificat correspondant aura été retiré de la base de certificats utilisés par les services de SOGELINK.

3.4.3 Renouvellement du certificat racine

Le renouvellement est réalisé avant l'expiration du certificat. Il s'effectue de la même manière que l'émission d'origine.

3.5 Profil des certificats

Les Certificats produits par l'ICP sont conformes au standard ITU-T Recommandation X.509 V3.

3.5.1 Certificat racine

Le certificat racine de l'ICP SOGELINK comprend les champs suivants :

Élément	Valeur
Version	V3
Numéro de série	Numéro unique
Algorithme de signature	sha1RSA
Émetteur	CN=SOGELINK Racine,O=SOGELINK,C=FR
Valide à partir de	Date de génération de certificat
Valide jusqu'à	Date de génération + 5 ans
Sujet	CN=SOGELINK Racine,O=SOGELINK,C=FR
Clef publique	2048 bits
AKI	Empreinte SHA1 de la clef publique
SKI	Empreinte SHA1 de la clef publique
Stratégie de certificat	1.3.6.1.4.1.36513.2.1.1

Point de distribution de la CRL	http://www.dict.fr/SOGELINKRacine.crl
Key usage	Signature du certificat, Signature de la liste de révocation de certificats hors connexion, Signature de la liste de révocation de certificats
Contraintes de base	Type d'objet = AC,
Contrainte de longueur de chemin d'accès	2
Algorithme de hash	sha1

3.5.2 Certificat d'Autorité de Certification subordonnée

Les certificats d'AC subordonnées émis par SOGELINK RACINE comprennent les champs suivants :

Élément	Valeur
Version	V3
Numéro de série	Numéro unique
Algorithme de signature	sha1RSA
Émetteur	CN=SOGELINK Racine,O=SOGELINK,C=FR
Valide à partir de	Date de génération de certificat
Valide jusqu'à	Date de génération + 1825 jours ou date d'expiration du certificat RACINE
Sujet	CN=SOGELINK Signature,O=SOGELINK,C=FR
Clef publique	2048 bits
AKI	Empreinte SHA1 de la clef publique de SOGELINK RACINE
SKI	Empreinte SHA1 de la clef publique
Stratégie de certificat	1.3.6.1.4.1.36513.2.1.1
Point de distribution de la CRL	http://www.dict.fr/SOGELINKRacine.crl
Key usage	Signature du certificat, Signature de la liste de révocation de certificats hors connexion, Signature de la liste de révocation de certificats
Contraintes de base	Type d'objet = AC
Contrainte de longueur de chemin d'accès	1
Algorithme de hash	sha1

3.5.3 Certificats d'Autorité d'Horodatage

Les certificats d'Autorité d'Horodatage signés par SOGELINK RACINE comprennent les champs suivants :

Élément	Valeur
Version	V3
Numéro de série	Numéro unique
Algorithme de signature	sha1RSA
Émetteur	CN=SOGELINK Racine,O=SOGELINK,C=FR
Valide à partir de	Date de génération de certificat
Valide jusqu'à	Date de génération + 1825 jours ou date d'expiration du certification RACINE
Objet	CN=SOGELINK Horodatage,O=SOGELINK,C=FR
Clef publique	2048 bits
AKI	Empreinte SHA1 de la clef publique de SOGELINK RACINE

SKI	Empreinte SHA1 de la clé publique
Stratégie de certificat	1.3.6.1.4.1.36513.2.1.1
Point de distribution de la CRL	http://www.dict.fr/SOGELINKRacine.crl
Key usage	Signature électronique, Non répudiation
Extended Key Usage	Horodatage
Contraintes de base	Type d'objet = entité finale
Contrainte de longueur de chemin d'accès :	0
Algorithme de hash	sha1

3.6 Sécurité physique de l'ICP

Des contrôles sont effectués sur les équipements de l'OC, sur les points suivants :

- situation géographique et construction de sites ;
- accès physique ;
- énergie et air conditionné ;
- exposition aux liquides ;
- sécurité incendie ;
- conservation des médias.

Le certificat racine de l'ICP SOGELINK est exploité en ligne sur un serveur protégé. La clef privée est stockée de façon cryptée sur le serveur. La version non cryptée est uniquement conservée en mémoire et détruite en cas de panne du serveur ou de l'application.

SOGELINK s'engage à exploiter les clefs privées nécessaires à ses services selon les pratiques de l'état de l'art relatif à l'exploitation de tels services.

SOGELINK s'engage à être auditable de manière à pouvoir fournir une mesure objective de la qualité de la gestion de ses clefs privées. Sur demande motivée SOGELINK pourra présenter un devis pour l'accompagnement d'un audit réalisé par un organisme indépendant et à la charge exclusive du demandeur.

3.7 Contacts et organisation dédiée à la PC

3.7.1 Organisation dédiée à la PC

SOGELINK est responsable de l'élaboration, du suivi et de la modification dès que nécessaire de la présente PC. 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 PC.

3.7.2 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

3.8 Dispositions applicables et règlement des litiges

3.8.1 Dispositions applicables

Il est expressément entendu qu'en l'état de la pratique et des textes législatifs et réglementaires en vigueur, les Certificats émis en vertu de la présente PC sont des Certificats simples dont les conditions d'utilisation sont définies par la présente PC et/ou par le contrat d'abonnement aux services de certification définissant les relations entre l'AC et un Porteur de Certificat.

La présente PC 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 Certificats ou sur les obligations respectives des intervenants.

Les relations entre l'AC d'une part et les Porteurs de Certificats d'autre part sont régies par un contrat d'abonnement au service de certification entre l'AC et le Porteur de Certificat et par les dispositions de la présente PC.

Les relations entre l'AC et l'Utilisateur sont régies par les dispositions de la présente PC et les Conditions Générales d'Utilisation des services de SOGELINK.

3.8.2 Loi applicable et résolution des litiges

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

3.9 Modifications des spécifications et des composantes de l'AC

L'AC procède à toute modification des spécifications stipulées dans la PC et/ou des composantes de l'ICP qui lui apparaît nécessaire pour l'amélioration de la qualité des services de Certification et de la sécurité des processus.

L'AC procède également à toute modification des spécifications stipulées dans la PC et/ou des composantes de l'AC qui est rendue nécessaire par une législation ou réglementation en vigueur.

L'AC informera les Applications cibles et/ou les Porteurs de telles modifications dès lors qu'il s'agit de modifications majeures ayant un impact déterminant.

L'information sera effectuée par l'AC par tout moyen, notamment à l'aide de message électronique spécifique ou via la publication de l'information sur son site web.