

Citation : Régime juridique du Prestataire de services de confiance au regard de la directive du 13 décembre 1999, <http://www.caprioli-avocats.com>

Date de la mise à jour : mai 2003.

Régime juridique du Prestataire de services de confiance au regard de la directive du 13 décembre 1999

email : contact@caprioli-avocats.com

Plan

I/ Les signatures électroniques

II/ Obligations et responsabilités des Prestataires de services de certification

A) Obligations du P.S.C.E.

B) Responsabilité du P.S.C.E.

La société de l'information et plus particulièrement le développement du commerce électronique reposent sur la confiance. La sécurité juridique et technique constitue un point crucial. Dans cette optique, les interrogations liées à la force probante des écrits électroniques se posaient avec de plus en plus d'acuité. La preuve dont la finalité est toujours la même et vise directement le juge puisqu'elle doit le convaincre de la vérité rapportée est un élément essentiel dans tous les systèmes juridiques.

De façon plus précise, l'inadaptation du système probatoire français quant à la force probante des écrits électroniques constituait un obstacle fondé sur la prééminence de l'écrit papier ainsi qu'un frein à la confiance attendue par les acteurs de la société de l'information. Au niveau international, la Commission des Nations Unies pour le Droit du Commerce International adoptait en 1996 une loi-type et une autre loi type sur les signatures électroniques a été adoptée par la CNUDCI en juillet 2001. Au niveau communautaire, la directive pour un cadre commun sur les signatures électroniques (directive 1999/93/CE du 13 décembre 1999, JOCE n° L 13, 19 janvier 2000, p. 12 s.) facilite l'usage des signatures électroniques et consacrent leur reconnaissance juridique. En France, la loi du 13 mars 2000 définit désormais la preuve par écrit sous forme électronique ainsi que le régime de la signature électronique (V. notamment E. A. Caprioli, *La loi française sur la preuve et la signature électroniques dans la perspective européenne*, J.C.P. éd. G, 2000, I, 224 et *Ecrit et preuve électroniques dans la loi n°2000-230 du 13 mars 2000*, J.C.P. 2000, éd. E, Cah. Dr. Entr. n°2, Suppl. au n°30, p.1- 11). Les décrets n° 2001-272 du 30 mars 2001 (J.O., 31 mars 2001, p. 5070) et n° 2002-535 du 18 avril 2002 (J.O., 19 avril 2002, p. 6944) ainsi que l'arrêté du 31 mai 2002 (J.O. n° 132 du 8 juin 2002, p. 10223, v. à cet égard, D &P, février 2003, p. 116, obs. E. Caprioli) complètent les dispositions adoptées par le législateur. La reconnaissance juridique des signatures électroniques (I) s'accompagne ainsi de règles juridiques propres aux prestataires de services de certification électronique (II).

I/ Les signatures électroniques

Alors que le code civil vise souvent la signature, aucune définition n'en était donnée jusqu'à la loi du 13 mars 2000. Le juge et la doctrine, en revanche, s'étaient penchés sur cette question et pour l'essentiel, le législateur a repris fidèlement les principes qu'ils avaient dégagés. En ce sens, l'art. 1316-4 alinéa 1 c. civ. donne une définition fonctionnelle de la signature en général. Ainsi, la signature (qu'elle soit électronique ou manuscrite) remplit deux fonctions juridiques de base : l'identification de l'auteur de l'acte et l'expression du consentement du signataire au contenu de l'acte. La définition des signatures électroniques et surtout les conditions légales posées pour cette catégorie de signature sont données à l'article 1316-4, al. 2 c. civ. qui dispose : « *Lorsqu'elle est électronique, elle (la signature) consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache. La fiabilité de ce procédé est présumée, jusqu'à preuve contraire, lorsque la signature électronique est créée, l'identité du signataire assurée et l'intégrité de l'acte garantie, dans des conditions fixées par décret en Conseil d'Etat.* » Le procédé de signature électronique doit donc identifier le signataire, garantir le lien entre l'acte et la personne dont il émane et assurer l'intégrité de l'écrit signé. A

l'heure actuelle, seules les signatures électroniques basées sur la cryptologie à clé publique (à savoir les signatures numériques) répondent aux exigences légales et plus particulièrement à la garantie de la solidité du lien entre la signature et le message. En effet, ce procédé assure l'intégrité du message signé grâce à la fonction "hash" ou "contrôle" qui consiste à faire avec un logiciel intégré dans le dispositif de signature un abrégé du message ("condensé") que l'on chiffre à l'aide de la clé privée de signature (connue du seul signataire pour des raisons de sécurité évidente) et qui est logiquement lié au message électronique ("empreinte"). Ce procédé a été retenu par la directive européenne sous l'appellation « *signatures électroniques avancées* » et par le décret du 30 mars 2001 pris en application de l'article 1316-4 du code civil qui reprend 80% du texte communautaire. La directive reconnaît que la signature électronique équivaut à la signature manuscrite si elle repose sur un certificat agréé conformément à l'annexe I et créé par un dispositif sécurisé de création de signature tel que décrit à l'annexe III. Ainsi, l'originalité de la signature numérique vient du fait que trois parties jouent trois rôles distincts qui contribuent à la confiance : le signataire, le prestataire de service de certification électronique (P.S.C.E.), le destinataire (« *la partie qui se fie* »). Compte tenu du fait que ce sont les signatures numériques qui sont indirectement visées, c'est grâce d'une part, à la fonction de "hachage" (abrégé ou "contrôle") que l'intégrité de l'acte est préservée, et d'autre part au certificat numérique contenant la clé publique du signataire que son identification est ainsi garantie et peut être vérifiée. La sécurité dépend de la politique de certification de l'Autorité de certification (P.S.C.E.) qui décrit les niveaux de confiance souhaités et de la Déclaration des pratiques de certification qui énonce les modalités concrètes pour y parvenir. Ces documents de nature juridique et technique s'inspirent largement, pour la plupart, des travaux internationaux réalisés à l'IETF (Internet Engineering Task Force). Ce processus de normalisation s'inscrit résolument dans une perspective technique et il s'apparente à l'élaboration de véritables codes de conduite privée. Ces documents - types, politique de certification (P.C.) et "certification practices statement" ("C.P.S." ou D.P.C.), proviennent "d'ordres spontanés et mûris" et sont les instruments de régulation de l'activité de P.S.C.E.

Conformément à la directive, il est prévu un régime d'accréditation volontaire des P.S.C.E.. L'obtention de l'accréditation sera valable pour une durée définie dans le décret. Cette accréditation emportera reconnaissance de la force probante de l'écrit électronique, le procédé de signature utilisé étant présumé fiable. Or, le décret n'établit pas un lien direct entre la présomption et l'accréditation. Ceci étant, le décret, conformément à la directive, traite principalement des certificats et des obligations générales qui pèsent sur les P.S.C.E..

II / Obligations et responsabilités des Prestataires de services de certification

Le certificat (art. 6 du décret relatif aux certificats qualifiés) fait apparaître diverses indications relatives au P.S.C.E., au signataire et à des données qui lui sont propres (début et fin de validité, limites d'utilisation et limites à la valeur des transactions pour lesquelles il peut être utilisé, ...). La loi sur la société de l'information devrait quant à elle compléter la loi du 13 mars 2000, car outre une réforme du régime de la cryptographie (déjà modifié par la loi n° 2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne, J.O., 16 novembre 2001, p. 18215), elle devrait prévoir notamment le régime de limitation de la responsabilité civile des P.S.C.E.E.

Pour émettre des « *certificats qualifiés* », les « *prestataires de services de certification* » doivent fournir un certain nombre de garanties dont les exigences sont prévues à l'annexe II de la directive. Peu importe que le P.S.C.E. bénéficie d'une accréditation volontaire ou qu'il se conforme à la directive sans passer par le régime d'accréditation. Sans entrer dans le détail des prescriptions de l'annexe II, nous signalerons que le P.S.C.E. doit utiliser des systèmes et produits fiables tant pour leur fonctionnement que pour la conservation des certificats (annexe II, f et l) et employer du personnel qualifié (annexe II, e). Ces dispositions sont reprises à l'article 6 du décret du 30 mars 2001.

En cas de litige, ils auront également à faire la preuve qu'ils sont suffisamment fiables pour fournir des services de certification (annexe II, a). Les P.S.C.E. doivent disposer des garanties financières suffisantes pour fonctionner en permettant l'indemnisation des utilisateurs autant que de besoin et notamment par le biais de souscription d'une police d'assurance appropriée. S'agissant de la communication et de la reconnaissance avec d'autres P.S.C.E., il conviendra que l'interopérabilité des systèmes de signatures électroniques soit garantie, par exemple en respectant les normes et les standards en vigueur. Pour que toutes les parties intéressées aux services de certification (ex : les abonnés, les tierces parties au contrat d'abonnement qui se fient aux certificats) puissent être en mesure de les utiliser dans leurs opérations en ligne, il est nécessaire que le P.S.C.E. leur procure une information correcte "par un moyen de communication durable" sur l'ensemble des services qu'il propose et dans une langue compréhensible (en principe, au moins trois langues communautaires) (annexe II, k). Cette information doit être faite par écrit (elle peut être transmise par voie électronique) et doit également porter sur les termes et conditions contractuels, spécialement les procédures de réclamations et de règlement des litiges. L'existence d'un régime d'accréditation volontaire doit figurer sur le site. De la sorte, à notre avis, les personnes qui demandent un certificat seront informées de la situation du P.S.C.E. (titulaire ou non de l'accréditation).

Lorsque le P.S.C.E. fournit à son client des services de gestion de clés, il ne doit ni stocker, ni copier les données afférentes à la création de signature de celui-ci (Annexe II, j). Cette exigence découle directement

d'un principe de sécurité en vertu duquel il faut disposer de deux paires de clés distinctes lorsque l'on entend signer et chiffrer des messages. L'usage d'une seule paire de clés à la fois pour la signature et pour le chiffrement des messages aurait pour conséquence de créer le risque de voir un tiers s'approprier ou reconstituer la clé privée de signature d'une personne et qu'elle se fasse passer pour elle. Dans le cas de signature numérique, la clé privée doit rester secrète et sous le " *contrôle exclusif*" du signataire (art. 2-2 du décret du 30 mars 2001). Pour les clés de confidentialité, en revanche, le P.S.C.E. peut être conduit à les conserver dans l'hypothèse où un client, suite à la perte de sa clé, demanderait au P.S.C.E. de la reconstituer (service de recouvrement de clé de confidentialité) pour être en mesure d'accéder à l'ensemble des fichiers qu'il aurait antérieurement chiffrés.

Dans toute Infrastructure à clé publique (I.C.P.), l'enregistrement des abonnés aux services de certification s'effectue par l'entremise d'Autorités d'enregistrement (A.E.). L'enregistrement peut s'effectuer soit en ligne et les pièces justificatives de l'identité sont envoyées par la Poste (pièces d'identité, Extrait K-Bis, et autres quittances attestant du domicile), soit de visu aux guichets prévus à cet effet (sur présentation des pièces justificatives). Cette opération est très importante car elle permet de vérifier l'identité conformément au droit national (annexe II, d), la capacité et les pouvoirs des personnes, de manière " *à enregistrer toutes les informations pertinentes concernant un certificat qualifié*" (annexe II, i). Cette entité ne souscrit pas d'engagement juridique envers les clients, elle est uniquement en relation contractuelle avec l'A.C. Cette dernière génère le certificat numérique d'identification sous sa seule responsabilité et à ce titre elle s'engage à remplir certaines obligations essentielles (art. 6 § 1 et § 2), c'est à dire établir et garantir le lien qui existe entre une personne et une paire de clés asymétriques dont elle est titulaire. En outre, le P.S.C.E. crée et assure, sous sa responsabilité, le fonctionnement d'un service d'annuaire (rapide et sûr) et d'un service de révocation (sûr et immédiat) (annexe II, b).

En France, le schéma d'accréditation et les conditions à remplir découlent directement de la directive et de ses annexes ; ils sont mis en œuvre dans le cadre du décret du 30 mars 2001 pris en application de l'article 1316-4, al.2 c. civ. Et du décret du 18 avril 2002.

Les États peuvent au demeurant contrôler les P.S.C.E. basés sur leur territoire qui délivreront des certificats qualifiés (article 6 § 3). Mais sur quoi portera ce contrôle dans la mesure où tout système d'autorisation obligatoire est prohibé ? On peut soutenir qu'un tel pouvoir relevant des États consiste en la connaissance de l'existence de la personne qui exerce une activité de P.S.C.E. et en l'imposition d'une déclaration de fournitures de services de certification auprès d'un organisme d'État (ex : en France, la D.C.S.S.I.). Ces modalités, particulières à chaque État, sont dans un pays comme la France fixées par voie réglementaire.

A) Obligations du P.S.C.E.

Il convient de signaler que les dispositions de la directive 93/13/CEE du Conseil du 5 avril 1993 relatives aux clauses abusives dans les contrats conclus avec les consommateurs s'appliquent aux relations entre les P.S.C.E. et les " *abonnés*" (article 3, § 5).

Aux termes de l'article 8 de la directive, les États membres doivent veiller à ce que les P.S.C.E. et les organismes responsables de l'accréditation et du contrôle honorent les exigences posées par la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative au traitement des données à caractère personnel.

La directive prévoit des règles de responsabilité pour les P.S.C.E. notamment eu égard au contenu des certificats (article 6). Cette partie de la directive doit encore faire l'objet, en France, d'une loi de transposition. En cas de préjudice, le P.S.C.E. doit être responsable de l'exactitude des informations qu'il inscrit dans le certificat au moment de sa date d'émission, du lien entre le signataire et un bi-clé et enfin, de toute omission d'enregistrement et de publication de la révocation du certificat sur ses listes accessibles en ligne. Concernant l'exactitude des informations que le certificat doit contenir, il faut reconnaître qu'elles ne peuvent que résulter des pièces fournies lors de l'enregistrement (ex : pièce d'identité, quittance). En cas de falsification, tant matérielle qu'intellectuelle, du ou des document(s), ou d'informations obsolètes, le P.S.C.E. ne devrait pas être responsable des informations inscrites dans le certificat. En effet, actuellement les enregistrements s'effectuent le plus souvent en ligne et par l'envoi des pièces justificatives par courrier. Mais ce problème de faux documents serait le même dans le cadre des procédures d'enregistrement en face à face. Le P.S.C.E. ne peut garantir que l'exactitude formelle des informations au vu des pièces transmises et non leur exactitude sur le fond. Dès lors, sa responsabilité ne peut être liée qu'à l'exacte transcription dans le certificat des informations fournies par l'abonné. Le titulaire du certificat devra, par conséquent, communiquer au P.S.C.E. tous les changements affectant les informations contenues dans le certificat. Le P.S.C.E. aura de la sorte la possibilité d'établir toute inexactitude et être déchargé, le cas échéant, de sa responsabilité.

En outre, comme le souligne une doctrine autorisée, " *puisque une obligation d'exactitude pèse sur le prestataire à ce moment précis (la date de délivrance, art. 6 § 1, a), il (le P.S.C.E.) doit veiller à ce que la date et l'heure d'émission puissent être déterminées avec précision (annexe II, b de la directive)* ». Cette disposition suppose que des services d'horodatage soient opérationnels.

S'agissant à présent de la personne physique ou morale ou de l'entité qui se fie *raisonnablement* au certificat (ou qui s'en prévaut) (art. 6 § 1 et § 2), il faut comprendre que le tiers doit vérifier non seulement la validité du certificat mais aussi celle de la signature. Dans cette perspective, une partie qui se fierait à un certificat sans consulter notamment la Liste de révocation des certificats (annuaire publié en ligne) ou les restrictions d'usage ou les valeurs limites contenues dans le certificat n'aura pas le droit d'engager la responsabilité du P.S.C.E.

B) Responsabilité du P.S.C.E.

Selon l'article 6 § 3 "*Les Etats membres veillent à ce qu'un Prestataire de services de certification puisse indiquer, dans un certificat qualifié, les limites fixées à son utilisation, à condition que ces limites soient discernables par des tiers. Le Prestataire de services de certification ne doit pas être tenu responsable du préjudice résultant de l'usage abusif d'un certificat qualifié qui dépasse les limites fixées à son utilisation*" et selon l'article 6 § 4 "*dans un certificat qualifié, la valeur limite des transactions pour lesquelles le certificat peut être utilisé, à condition que cette limite soit discernable par des tiers. Le Prestataire de services de certification n'est pas responsable des dommages qui résultent du dépassement de cette limite maximale.*". Le terme « *discernable* » utilisé dans ces deux paragraphes peut surprendre le juriste, voire le laisser perplexe. Il signifie que les limites d'utilisation (ex : engageant l'entreprise à l'exclusion de son employé en son nom personnel) du certificat doivent être perçues de façon à éviter toute confusion. Ainsi, il suffira que l'attention de la personne qui reçoit un certificat et un message signé soit attirée par une indication selon laquelle l'utilisation du certificat est limité, sans qu'il soit nécessaire que ce soit tout le contenu de cette limite lui-même qui soit affiché. Ensuite (art. 6 § 4), les Etats devront exclure toute responsabilité du prestataire qui pourrait survenir à la suite d'une utilisation du certificat au delà de la valeur limite des transactions (montants maximum) établie selon le certificat. Ces deux paragraphes doivent s'entendre comme étant une exclusion de tous les préjudices tant directs qu'indirects.

En réalité, les P.S.C.E. se situent au cœur d'une Infrastructure à clé publique (I.C.P.). Cette I.C.P. comprend plusieurs entités qui ont des fonctions et des responsabilités distinctes. Plusieurs métiers coexistent : Autorité de certification (A.C.), Opérateur de certification et Autorité d'enregistrement, Services de publication (annuaire ou liste de révocation des certificats ou des autorités de certification reconnues). Il ressort de ce système que la confiance dépend de l'ensemble des composantes de l'I.C.P. Néanmoins, en cas de préjudice, c'est l'A.C. (le P.S.C.E.) qui sera responsable vis à vis de ses clients et des personnes qui se fie à la signature électronique. De la sorte, elle ne pourra exonérer sa responsabilité en soutenant qu'une autre entité est responsable (ex : l'A.E. pour la collecte des données relatives à l'enregistrement ou l'opérateur pour les services de certification). Elle pourra toutefois engager la responsabilité de cette dernière sur la base des engagements contractuels souscrits entre elles au sein de l'I.C.P.

La transposition des dispositions de l'article 6 de la Directive a été prévue dans le projet de L.S.I. et, après modifications, elle sera intégrée, en vue de son adoption par l'Assemblée, à l'article 21 du projet de loi pour la confiance dans l'économie numérique (v. l'avis n° 608 de Mme Michèle Tabarot, fait au nom de la commission des lois, 11 février 2003, disponible sur le site <http://www.assemblee-nationale.fr>). Le nouveau texte, contrairement aux précédents, s'applique exclusivement aux certificats présentés comme qualifiés et non à tous les certificats électroniques.