Projet ICare

Responsabilité et assurances des certificateurs

Référence : ICARE/CAB/TPC/DOC_14/v1
Type : Note de travail
Diffusion : Générale

Date : 12/09/2002
Titre : **ICare – Responsabilité et assurances des certificateurs**

Auteur(s) : Thierry Piette-Coudol, avocat

Résumé :
Cette note identifie les principes juridiques qui doivent permettre de définir le périmètre du régime de responsabilité civile professionnelle (RCP) des prestataires de services de certification.

TABLE DES MATIERES

1 Introduction

La Directive 1999/93/CE du parlement européen et du conseil du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques a fixé dans son article 6 le régime de la responsabilité des Prestataires de Services de Certification (PSC) (voir ci-dessous en annexe).

Au moment de la transposition en droit interne français, les Pouvoirs Publics ont décidé d'intégrer la signature électronique dans le Code Civil au chapitre de la preuve. Or la logique du chapitre responsabilité (article 1382 et suiv.) n'offrait pas l'opportunité d'intégrer un régime de responsabilité pour une entité commerciale aussi spécifique. D'autre part, la répartition des compétences issue de l'article 34 de la Constitution ne permettait pas d'établir le régime de responsabilité des PSC dans le Décret d'application de l'article 1316-4. Aussi les Pouvoirs Publics ont-ils décidé d'inclure le régime des PSC dans le projet de Loi sur la Société de l'Information.

La LSI assurera la transposition dans le droit interne de la Directive 2000/31/CE du Parlement Européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique dans le marché intérieur ("directive sur le commerce électronique"). D'autre part, la LSI comble un manque important de l'article 1316-4 en autorisant l'usage *ad validatem*[1] de la signature électronique pour les écrits sous forme électronique. Le projet de loi LSI a été arrêté par le Conseil des Ministres le 13 juin dernier.

Le projet de LSI réalisant pour sa plus grande part la transposition de la Directive Commerce Electronique, il est possible de baser une analyse juridique sur ce texte qui ne deviendra définitif qu'après adoption par le Parlement. Ce que nous faisons ci-après.

2 Responsabilité et assurances dans la prestation de certification

2.1. La nécessité d'une assurance RCP

Toute société commerciale ou tout prestataire de service est responsable du service fourni. Aussi il peut être judicieux de souscrire une assurance responsabilité civile professionnelle (RCP), même s'il ne s'agit pas d'une obligation légale.

Pour les PSC[2], la loi reprenant les prescriptions de la Directive exige la couverture financière des risques pesant sur les prestations de certification. L'article 39, 3ème alinéa du projet de LSI pose le principe d'une assurance de type RCP :

> *"[Les PSC] doivent justifier d'une garantie financière suffisante, spécialement affectée au paiement des sommes qu'elles pourraient devoir aux personnes s'étant fiées raisonnablement aux certificats qu'elles délivrent, ou d'une assurance garantissant les conséquences pécuniaires de leur responsabilité civile professionnelle.*

Dans le monde de la confiance, le PSC est responsable de la confiance qu'on peut légitement avoir dans le certificat émis. Le PSC est ainsi responsable contractuellement du certificat émis face à son client. Mais il est aussi responsable délictuellement du certificat émis face aux utilisateurs, en particulier au "vérificateur" de signature électronique. Comme l'indique le 1er alinéa de l'article 39 :

[1] Ce qui signifie que lorsqu'un acte juridique doit être créé sur un support papier (par suite d'une texte juridique spécifique), il sera possible de passer outre, d'en faire un message électronique à condition de le re-valider par une signature électronique.
[2] Rappel : PSC, appellation juridique pour AC.

> *"Sauf à démontrer qu'elles n'ont commis aucune faute intentionnelle ou négligence, les personnes physiques ou morales prestataires de services de certification électronique ou fournissant d'autres services liés aux signatures électroniques sont présumées responsables du préjudice causé aux personnes qui se sont fiées raisonnablement aux certificats qu'elles délivrent."*

2.2. Les risques

Outre la responsabilité professionnelle générale supportée par le PSC sur son cœur de métier, la gestion de certificat, certains risques spécifiques peuvent être identifiés quant au certificat et à son contenu.

2.2.1. Limitations dans l'utilisation du certificat

Le certificat peut mentionner dans ses rubriques une limitation à l'utilisation du certificat (article 6.-I. i) du Décret d'application). Le PSC n'est pas responsable si cette limitation apparaît clairement et de façon non ambiguë. Comme l'indique le second alinéa de l'article 39 du projet de LSI :

> *"[Les PSC] ne sont pas responsables du préjudice causé par un usage du certificat dépassant les limites fixées à son utilisation ou à la valeur des transactions pour lesquelles il peut être utilisé, à condition que ces limites aient été clairement portées à la connaissance des utilisateurs dans le certificat.*

En conséquence, le PSC devrait :
- prévoir les limitations de l'utilisation du certificat dans le rubriquage de ce certificat, l'indiquer dans la Politique de Certification et/ou sa DPC, ainsi que dans sa documentation commerciale,
- inscrire les limitations de l'utilisation du certificat dans le contrat de prestation de service qu'il propose à ses abonnés,
- éventuellement, proposer ou mettre à disposition de l'abonné, directement ou indirectement, un système de garantie et/ou d'assurance qui le couvrirait de tout recours introduit par les utilisateurs de certificats
- se garantir par une assurance de tout recours introduit par l'abonné mécontent.

2.2.2. Limitations dans l'utilisation du certificat

Le certificat peut mentionner dans ses rubriques une valeur maximale pour les transactions utilisant le certificat émis (même article 6.-I. i) du Décret d'application). Le PSC n'est pas responsable si cette valeur limite apparaît clairement et de façon non ambiguë. Le second alinéa de l'article 39 du projet de LSI l'indique (voir ci-dessus).

En conséquence, le PSC devrait :
- prévoir la valeur maximale de la transaction considérée dans le rubriquage de ce certificat, l'indiquer dans la Politique de Certification et/ou sa DPC, ainsi que dans sa documentation commerciale,
- mentionner la valeur maximale de la transaction considérée dans le contrat de prestation de service qu'il propose à ses abonnés,
- éventuellement, proposer ou mettre à disposition de l'abonné, directement ou indirectement, un système de garantie et/ou d'assurance qui le couvrirait de tout recours introduit par les utilisateurs de certificats
- se garantir par une assurance de tout recours introduit par l'abonné mécontent.

2.2.3. L'exactitude des informations contenues dans le certificat

Le PSC assure la responsabilité de la présence et de l'exactitude des informations contenues dans le certificat. Ce risque apparaît dans le texte de la Directive (article 6.-I a), même si le droit interne ne le mentionne pas expressément. Le PSC est responsable de "*l'exactitude de toutes les informations contenues dans le certificat qualifié à la date où il a été délivré et la présence, dans ce certificat, de toutes les données prescrites pour un certificat qualifié"*

La responsabilité du PSC peut être mise en jeu par les utilisateurs qui se seraient fiés au certificat, alors que des informations seraient absentes ou fausses. Ce risque devrait être inclus nommément dans les garanties couvertes dans sa RCP.

2.2.4. La concordance de la clé publique contenue dans le certificat avec la clé privée

Le certificat a pour but d'établir une liaison entre une identification de personne ou d'entité et la clé publique correspondante. Dans la cryptographie asymétrique, une clé privée correspond à cette la clé publique, les deux formant un bi-clé cryptographique.

Pour satisfaire un besoin d'identification fort exigé par le droit, le bi-clé est tiré par l'abonné face à l'autorité d'enregistrement (par exemple, le greffier) (le bi-clé pourrait également être tiré chez le PSC). Aussi le PSC se trouve en possession d'une clé publique sans être sûr qu'il existe chez l'abonné la clé privée complémentaire. Or selon l'article 6.I. b), le PSC doit donner toute "*assurance que, au moment de la délivrance du certificat, le signataire identifié dans le certificat qualifié détenait les données afférentes à la création de signature [c'est-à-dire la clé privée] correspondant aux données afférentes à la vérification de signature fournies ou identifiées [c'est-à-dire la clé publique] dans le certificat*".

La responsabilité du PSC peut être mise en jeu par les utilisateurs qui se seraient fiés au certificat, alors que la clé privée n'existerait pas ou serait fausse (cas d'une "mascarade" avec une vrai-fausse clé) ou ne serait pas complémentaire (non-conformité du dispositif cryptographique à l'état de l'art, défaut de conformité aux ITSEC et Critères Communs). Ce risque devrait être inclus nommément dans les garanties couvertes dans sa RCP.

2.3. Le titulaire de la responsabilité

Comme on l'a vu dans la directive européenne ou dans le droit interne, la responsabilité pèse sur le PSC. Or dans les architectures de système de signature en cours d'élaboration en France, le PSC ne procède pas en personne aux traitements techniques des certificats qui sont effectués par un Opérateur de Services de Certification (OSC), disposant des ressources techniques nécessaires. Or le Droit ne connaît pas l'OSC.

2.3.1. Le partage de responsabilité entre le PSC et l'OSC

Ainsi le fait générateur de toute mise en jeu de la responsabilité du PSC sur les certificats ne peut apparaître que là où les certificats sont opérés c'est-à-dire chez l'OSC ! En cas de litige, le PSC endosse toute la responsabilité, même si l'OSC est en faute ou a été négligent. En, conséquence, il faut se préoccuper de la responsabilité de l'OSC et de la couverture des risques :

- l'OSC doit disposer d'une assurance RCP...
- ... mentionnant expressément la couverture de l'appel en garantie que le PSC ne manquerait d'actionner si sa responsabilité était mise en jeu pour un préjudice subi par l'abonné ou les utilisateurs du fait d'un certificat "défectueux".

Ces principes devraient être intégrés dans le contrat liant le PSC à son OSC.

2.3.2. La responsabilité des AE

Il faut aussi compter avec la présence dans l'architecture du système des autorités d'enregistrement (AE). Dans les scénarios de certification courants, les AE ne sont pas des employés du PSC, mais simplement des délégués. Pour eux, la mission d'AE est peut-être tout à fait ponctuelle.

L'AE est le seul à pouvoir contrôler de visu le tirage du bi-clé par l'abonné (pas le PSC) et donc, à pouvoir constater la concordance entre la clé privée, gardée par l'abonné, et la clé publique, envoyée au PSC. Si le PSC était surpris quant à l'inexistence d'une clé privée ou de sa non-concordance avec la clé publique du certificat (voir SUPRA), il pourrait tenter de dégager sa responsabilité en la reportant sur l'AE. Ce qui serait totalement inéquitable, compte tenu de la nature professionnelle de l'AE.

Aussi il semble que le PSC devrait être assuré sur le risque que l'AE soit surprise par un dysfonctionnement technique ou par la conduite de l'abonné et qu'il en résulte pour lui (le PSC) une mise en jeu de sa RCP, alors qu'il ne pourrait pas se retourner contra l'AE !

A cela, on ajoutera que les doutes du PSC sur l'hypothétique clé privée ne sont en réalité pas ressentis par lui, mais par l'OSC ! Dans l'architecture retenue, il est probable que les relations électroniques seront directes entre l'AE et l'OSC, sans passer par le PSC, qui sur ce point n'est pas en ligne. De sorte que le PSC reste intégralement responsable selon la loi, alors que les flux ne passent pas par lui.

3 Annexes

1. PROJET DE LOI SUR LA SOCIETE DE L'INFORMATION (LSI)
arrêté par le Conseil des Ministres du 13 juin 2001

Article 39

Sauf à démontrer qu'elles n'ont commis aucune faute intentionnelle ou négligence, les personnes physiques ou morales fournissant des prestations de cryptologie à des fins de confidentialité sont présumées responsables, nonobstant toute stipulation contractuelle contraire, du préjudice causé aux personnes leur confiant la gestion de leurs conventions secrètes en cas d'atteinte à l'intégrité, à la confidentialité ou à la disponibilité des données transformées à l'aide de ces conventions.

Article 40

Sauf à démontrer qu'elles n'ont commis aucune faute intentionnelle ou négligence, les personnes physiques ou morales prestataires de services de certification électronique ou fournissant d'autres services liés aux signatures électroniques sont présumées responsables du préjudice causé aux personnes qui se sont fiées raisonnablement aux certificats qu'elles délivrent.

Elles ne sont pas responsables du préjudice causé par un usage du certificat dépassant les limites fixées à son utilisation ou à la valeur des transactions pour lesquelles il peut être utilisé, à condition que ces limites aient été clairement portées à la connaissance des utilisateurs dans le certificat.
Elles doivent justifier d'une garantie financière suffisante, spécialement affectée au paiement des sommes qu'elles pourraient devoir aux personnes s'étant fiées raisonnablement aux certificats qu'elles délivrent, ou d'une assurance garantissant les conséquences pécuniaires de leur responsabilité civile professionnelle.

2. Directive 1999/93/CE du Parlement Européen et du Conseil du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques

Article 6 - Responsabilité

1. Les Etats membres veillent au moins à ce qu'un prestataire de service de certification qui délivre à l'intention du public un certificat présenté comme qualifié ou qui garantit au public un tel certificat soit responsable du préjudice causé à toute entité ou personne physique ou morale qui se fie raisonnablement à ce certificat pour ce qui est de :
l'exactitude de toutes les informations contenues dans le certificat qualifié à la date où il a été délivré et la présence, dans ce certificat, de toutes les données prescrites pour un certificat qualifié ;
l'assurance que, au moment de la délivrance du certificat, le signataire identifié dans le certificat qualifié détenait les données afférentes à la création de signature correspondant aux données afférentes à la vérification de signature fournies ou identifiées dans le certificat ;
l'assurance que les données afférentes à la création de signature et celles afférentes à la vérification de signature puissent être utilisées de façon complémentaire, dans le cas où le prestataire de service de certification générerait ces deux types de données, sauf si le prestataire de service de certification prouve qu'il n'a commis aucune négligence.
2. Les Etats membres veillent au moins à ce qu'un prestataire de service de certification qui a délivré à l'intention du public un certificat présenté comme qualifié soit responsable du préjudice causé à une entité ou personne physique ou morale qui se prévaut raisonnablement du certificat, pour avoir omis de faire enregistrer la révocation du certificat, sauf si le prestataire de service de certification prouve qu'il n'a commis aucune négligence.

3. Les Etats membres veillent à ce qu'un prestataire de service 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 service 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.
4. Les Etats membres veillent à ce qu'un prestataire de service de certification puisse indiquer, 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 service de certification n'est pas responsable des dommages qui résultent du dépassement de cette limite maximale.
5. Les dispositions des paragraphes 1 à 4 s'appliquent sans préjudice de la directive 93/13/CEE du Conseil du 5 avril 1993 concernant les clauses abusives dans les contrats conclus avec les consommateurs.