

# Le cadre juridique de la certification

Blandine Poidevin  
Avocat au Barreau de Lille  
<http://www.jurisexpert.net>

email : [bpoidevin@jurisexpert.net](mailto:bpoidevin@jurisexpert.net)

## Introduction

Nous sommes tous convaincus de l'impact que la signature électronique peut avoir dans le cadre du commerce sur Internet.

Les autorités nationales et communautaires ont eu l'occasion d'insister à de nombreuses reprises sur l'importance de la confiance du consommateur dans le cadre d'un achat en ligne.

Cette confiance peut reposer sur l'utilisation de moyens techniques lui garantissant une sécurité optimale.

C'est dans ce cadre qu'a été votée une loi essentielle sur le sujet : la loi du 13 mars 2000, qui reconnaît la validité juridique de la signature électronique.

Cette loi a été complétée par le décret du 31 mai 2001 qui fixe les règles de certification des procédés de signature électronique. Par ce décret, il est établi que la signature électronique certifiée bénéficie d'une présomption de fiabilité. Ce dispositif législatif et réglementaire a été complété récemment par un décret du 18 avril 2002 (décret n° 2002-535, relatif au schéma d'évaluation et de certification), et par un arrêté du Ministre de l'Economie, des Finances et de l'Industrie relatif à la reconnaissance de la qualification des prestataires de certification électronique et à l'accréditation des organismes chargés de l'évaluation, signé le 31 mai 2002 (JO 132 du 8 juin 2002). Ces textes s'inscrivent dans une perspective européenne<sup>1</sup>.

## I. Le décret du 18 avril 2002 : certification de produits ou de système

### La procédure d'évaluation

Ce décret définit le cadre juridique Français de l'évaluation et de certification.

Il a pour objectif de permettre à toute entreprise de faire certifier des produits ou des systèmes relatifs aux technologies de l'information, en terme de disponibilité, de confidentialité ...

Ce décret recommande également aux administrations de recourir à des produits ou des systèmes certifiés au sens de ce décret.

La mise en œuvre de l'évaluation est confiée à la DCSSI (Direction Centrale de la Sécurité des Systèmes d'Information). Cette Direction a été créée par un décret du 31 juillet 2001 et est placée sous l'autorité du Secrétaire Général de la Défense Nationale.

La DCSSI est placée sous le contrôle du Comité Directeur de la Certification en Sécurité des Technologies de l'Information. Ce Comité Directeur a pour responsabilité la définition de la politique générale d'évaluation. En tant qu'organisme de certification, la DCSSI procède à la délivrance des certificats.

Les évaluations sont réalisées par les Centres d'Evaluation de la Sécurité des Technologies de l'Information (CESTI). Les CESTI sont agréés par la DCSSI.

L'évaluation est réalisée par le CESTI. Au terme de l'évaluation, le CESTI rédige un rapport technique d'évaluation remis à l'entreprise évaluée et à la DCSSI.

---

<sup>1</sup> Ces textes sont disponibles à l'adresse suivante : <<http://www.scssi.gouv.fr>>.

En conséquence, toute société qui souhaite obtenir un certificat doit respecter cette procédure d'évaluation.

Il est recommandé d'être vigilant sur les obligations de confidentialité des intervenants. Une fois l'évaluation réalisée, l'organisme de certification rédige un rapport décrivant l'objet des fonctions de sécurité soumises à l'évaluation, indiquant le niveau d'assurance atteint, et attestant que les critères d'évaluation ont été correctement appliqués. Ce rapport de certification peut également recommander la mise en œuvre de mesures particulières.

### **Schéma de l'évaluation et de certification**

#### **Politique Générale**

Comité Directeur de la Certification  
en sécurité des Technologies de l'information



#### **Organisme de Certification**



DCSSI  
(Direction Centrale de la Sécurité  
des Systèmes d'Information)



#### **Evaluation**

Rapport technique d'évaluation



CESTI  
(Centre d'évaluation de la Sécurité  
des Technologies de l'information)



Contrat



Rapport technique

d'évaluation

#### **Délivrance du Certificat**



Produit ou Système évalué

### **Les Centres d'Evaluation de la Sécurité des Technologies de l'Information (CESTI)**

Le CESTI est agréé par l'organisme de certification. Il se doit d'être indépendant et en conséquence ne peut être impliqué dans le développement d'un produit. Toutefois, le CESTI peut proposer des prestations de conseils, indépendantes de la mission d'évaluation, si elles ne sont pas de nature à réduire son impartialité dans ses missions.

A titre d'exemple, les organismes suivants sont agréés :

- AQL Groupe CILICOMP pour l'informatique et les réseaux
- CEACI (THALES CNES) pour les composants électroniques et les logiciels embarqués
- SERMA TECHNOLOGIES pour les composants électroniques et les logiciels embarqués

Le Centre Electronique de l'Armement (SELAR) et la DCSSI disposent également d'un Centre d'Evaluation agréé.

De même, des produits tels que des cartes à puce (porte-monnaie électronique) font également l'objet d'agrément en tant que produits.

## **II. L'arrêté du 31 mai 2002 : Accréditation des signatures électroniques**

L'arrêté du 31 mai 2002 relatif à la reconnaissance de la qualification des prestataires de certification électronique et à l'accréditation des organismes chargés de l'évaluation, instaure, quant à lui, des centres d'accréditation.

L'objet de l'accréditation est de vérifier que les services offerts par le demandeur respectent les exigences du décret du 30 mars 2001, et notamment son article 6, sur la signature électronique.

Pour être accrédité en tant que prestataire de service de certification électronique, il est nécessaire de faire une demande d'accréditation à un centre d'accréditation. Cette demande doit notamment comprendre les comptes des deux exercices précédents de la société et la description des procédures et moyens qui seront mis en œuvre par l'organisme pour évaluer les prestataires de certification électronique, en vue de reconnaître leur qualification.

Sont centre d'accréditation :

- Le Comité Français d'Accréditation (COFRAC),
- Les organismes d'accréditation signataires d'un accord Européen sur le sujet.

### **Le recours aux centres d'accréditation**

La COFRAC instruit les demandes d'accréditation. L'accréditation délivrée est accordée pour une durée de deux ans qui peut être reconduite pour une durée identique.

La liste des organismes accrédités est mise à la disposition du public à partir d'un site Internet.

L'évaluation est effectuée aux frais du demandeur.

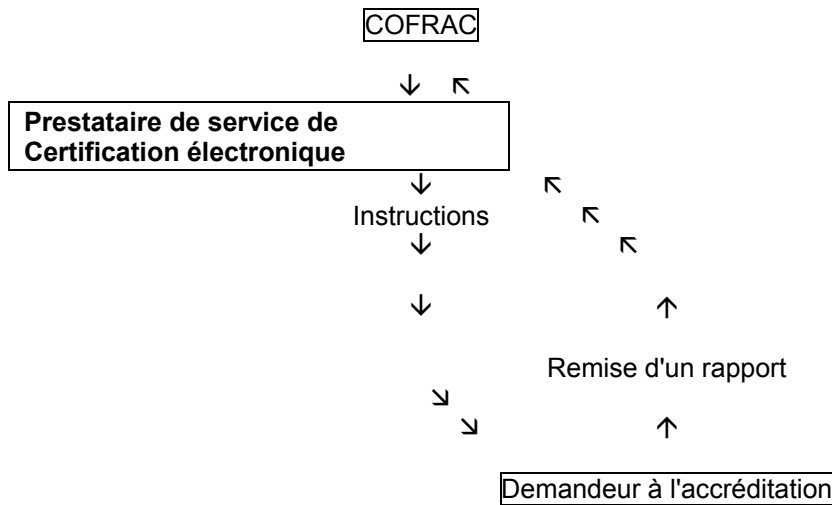
### **La procédure d'accréditation**

L'entreprise auditée doit remettre un rapport qui sera communiqué également à la DCSSI, sur demande de celle-ci.

Au vu du rapport et des éventuelles observations de l'entreprise auditée, la COFRAC reconnaît ou non la qualification du prestataire de service de certification électronique à ce dernier. Si l'accréditation est positive, la COFRAC délivre une attestation qui décrit les prestations de service couverte par la qualification, ainsi que la durée, qui ne peut excéder un an, pendant laquelle l'attestation est valable.

## Schéma d'accréditation

### Centre d'accréditation



Cet arrêté du 31 mai 2002 achève en France le dispositif de signature électronique issu de la directive Européenne de 1999.

L'accréditation du certificat électronique, selon des spécifications techniques reconnues, permettra de garantir un haut niveau de confiance auprès des utilisateurs.

Il appartiendra alors à celui qui se fie à un certificat de signature électronique, de contrôler l'accréditation du prestataire et le contenu de celle-ci.

Rappelons enfin que l'utilisation d'une signature électronique est soumise à la conclusion préalable d'un contrat d'abonnement entre l'utilisateur et le fournisseur du certificat. Les conditions générales ou les documents contractuels signés entre les parties devront intégrer une convention sur la preuve. Cette convention permettra notamment de régler les modalités d'administration de la preuve en cas de litige et leurs modalités de conservation.

Il appartiendra également au client du fournisseur de certificat de vérifier la souscription par son prestataire d'une assurance suffisante.

Une fois ces éléments contrôlés, il sera tout à fait légitime de se fier à la signature électronique, le certificat engageant la partie émettrice.

B. P.