Projet ICare

La signature électronique - Régime juridique

Référence : ICARE/CAB/TPC/DOC_28/v1
Type : Document
Diffusion : Membres du consortium

Date : 04/03/2003
Titre : **ICare – La signature électronique - Régime juridique**

Sous-Projet :
Auteur(s) : Thierry Piette-Coudol, avocat

Résumé :
En complément du DOC_1, cette note présente le régime juridique de la signature électronique.

TABLE DES MATIERES

1 Introduction

Cette note a pour objectif de présenter au lecteur le régime juridique de la signature électronique c'est-à-dire de montrer quelles sont les exigences que le Droit a imposé à une réalité technique préexistante, la signature numérique ou électronique.

Ce document remet en perspective les différents textes juridiques, en commençant par le niveau européen.

Ce document est à utiliser en complément du *DOC_1 Recueil des textes juridiques applicables à la signature électronique* qui recense les textes juridiques et les reproduit en intégralité.

2 La référence européenne : la directive signature électronique

Dans les années 1990, la Commission de Bruxelles a insisté sur le développement du Commerce Electronique dans les télécommunications dérégulées : "*le Commerce Electronique offre à l'Union Européenne une excellente occasion de poursuivre son intégration économique. Néanmoins la Commission observe que les réseaux ouverts comme Internet ne sont pas suffisamment sécurisés pour les affaires. Elle estime nécessaire d'instaurer un environnement sûr en ce qui concerne l'authentification électronique."* Comme le moyen le plus efficace pour assurer l'authentification des partenaires à un échange électronique est la signature électronique, sans compter les incidences possibles au niveau juridique, la Commission a préparé une proposition de "*Directive sur un cadre commun pour les signatures électroniques"*. Ce texte offrait l'opportunité de replacer la question de la signature électronique dans le contexte technique le plus ample, qui intégrait de nombreuses notions autant transversales que complémentaires. Le caractère innovant de la Directive par rapport aux standards technologiques est le suivant : le texte construit un dispositif intégré nécessaire pour fonder des conséquences juridiques de première grandeur, la reconnaissance juridique de la signature électronique.

La proposition de Directive de la Commission sur un cadre commun pour les signatures électroniques a été publiée le 13 mai 1998. La proposition a fait l'objet de nombreuses critiques et demandes de modifications. Une version amendée a été rejetée par le Conseil des ministres télécommunications le 27 novembre 1998. De novembre 1998 au printemps 1999, les experts ont mis au point une version nouvelle chaque mois. Enfin une version de consensus a été acceptée par le Conseil télécommunications d'avril 1999 et la proposition a pu être discutée par le Parlement européen.

2.1 Les composants de la signature

2.1.1. La signature électronique

Avec cette seconde version, la proposition de directive envisageait dans son article 2 deux types de signature électronique, dont une est qualifiée d'*avancée*. Une première signature semble englober tout type de moyen d'authentification dont les mesures biométriques. Elle est définie ainsi qu'il suit : "*Signature électronique : une donnée sous forme numérique jointe ou liée logiquement à d'autres données électroniques et servant de méthode d'authentification*". On trouve ensuite la signature avancée qui profitera de la reconnaissance juridique, la finalité de la Directive. Cette dernière est ainsi définie :

> *"Signature électronique avancée : une signature électronique qui satisfait aux exigences suivantes :*
> *a) être liée uniquement au signataire ;*
> *b) permettre d'identifier le signataire ;*
> *c) être créée par des moyens que le signataire puisse passer sous son contrôle exclusif ; et*
> *d) être liée aux données auxquelles elle se rapporte de telle sorte que toute modification ultérieure des données soit détectée."*

Les juristes français ont critiqué cette dernière définition parce qu'elle ne correspondait qu'aux garanties de la signature électronique technique, authentification et intégrité. Mais promise à une reconnaissance juridique, sa

définition ne présentait aucune des caractéristiques juridiques de la signature manuscrite : identification du signataire et appropriation du contenu du document signé.

2.1.2. Le certificat qualifié

La directive prévoit que les Prestataires de Services de Certification (PSC) utiliseront des certificats électroniques, mais sans référence à la recommandation X.509 du CCITT. La raison en est la suivante : si l'usage de procédés cryptographiques est connu de la Directive, celle-ci ne veut en aucune manière privilégier la cryptographie asymétrique à clés publiques. Cette absence de référence à la norme fondamentale du domaine, X.509, peut sembler gênante puisque la directive ouvre des effets juridiques maximaux sur des instruments techniques aux exigences minimales. D'où sans doute, l'invention du certificat *qualifié*. Quoique la chose ne soit pas précisément exprimée, le certificat renvoie à la clé publique du signataire. On le comprend en cheminant dans les termes de la définition qui renvoient eux-mêmes à d'autres définitions. Ainsi le certificat lie l'identité de la personne signataire avec un *"dispositif de vérification de signature"* qui doit être compris comme "*un dispositif logiciel ou matériel configuré pour mettre en application les données afférentes à la vérification de signature*". Quant aux "*données afférentes à la vérification de signature"*, on doit les considérer comme étant "*des données, telles que des codes ou des clés cryptographiques publiques, qui sont utilisées pour vérifier la signature électronique"*.

L'annexe I également mentionné ne crée pas à proprement parler un régime administratif d'*agrément* mais fait un choix parmi les contenus optionnels du certificat de la recommandation X.509 (sans le mentionner).

2.2 Les acteurs

La Directive ne mentionne que trois acteurs : le signataire, le prestataire de services de certification (l'AC de la technique) et le vérificateur, destinataire du message signé qui n'est que mentionné.

2.2.1. Le signataire

La directive définit ainsi le signataire : *"toute personne qui détient un dispositif de création de signature et qui agit soit pour son propre compte, soit pour celui de la personne ou de l'entité qu'elle représente.* Elle précise ainsi que le signataire est une personne physique et non pas une personne morale. Par contre, elle fait toujours l'impasse sur une différence fondamentale entre signature électronique et signature manuscrite : c'est l'opérateur sur machine qui appose une signature électronique avant la transmission, alors que le signataire d'un document écrit est celui qui est maître des effets juridiques dans l'entreprise. Par exemple, c'est le chef d'entreprise qui est signataire des actes et des contrats et non la secrétaire ou le vaguemestre.

2.2.2. Le Prestataire de Service de Certification

Le PSC est selon la directive le professionnel qui exerce la mission d'autorité de certification (AC) dans le cadre des signatures électroniques. L'article 2.6 des définitions la présentait dans la première version de la Directive comme *"Toute personne physique ou morale qui délivre des certificats au public pour vérifier la signature électronique."* Cette définition pouvait être considérée comme fausse puisque le certificat électronique garantit l'adéquation entre l'identité du signataire et sa clé publique. Le certificat sert à mettre en œuvre les prestations cryptographiques qui protègent le dispositif de vérification de signature. La nouvelle définition dans sa généralité est plus proche de la vérité : "*toute personne physique ou morale qui délivre des certificats ou fournit d'autres services liés aux signatures électroniques"*. Les PSC peuvent être accrédités, cette procédure nécessitant un développement particulier.

2.3 L'accréditation et la liberté d'établissement dans les services de confiance

Selon une appellation synonyme, les PSC sont également des Tierces Parties de Confiance. Comment la confiance peut-elle naître et durer ? La confiance naît du fait que les utilisateurs des services de certification leur font crédit sur ce point. D'où l'appellation d'origine anglo-saxonne d'*accréditation*. L'accréditation est d'abord le fait de l'organisme de gestion de l'infrastructure à clés publiques (ICP) susceptible d'accréditer les offres de service de prestataires, en particulier si leur offre est compatible avec les Politiques de Certification correspondantes. La Directive parle d'accréditation en lui donnant un sens quelque peu différent. La conséquence en est une plus grande tranquillité pour l'utilisateur qui pourrait utiliser sans autres soucis (sur la compétence

technique de son prestataire) les services d'un PSC accrédité. A noter cependant que l'accréditation n'est pas obligatoire pour les PSC. Mais l'utilisateur devra se déterminer par lui-même face à un PSC non accrédité.

2.3.1. L'accréditation dans la Directive

La Directive formule cette définition de l'accréditation : "*toute autorisation, indiquant les droits et obligations spécifiques à la fourniture de services de certification, à accorder sur demande du prestataire de service de certification concerné par l'autorité publique*…". Les rédacteurs de la Directive ont considéré que les régimes volontaires d'accréditation doivent permettre d'élever le niveau du service fourni. Ils constitueront pour les prestataires de service de certification le cadre propice au perfectionnement de leurs services pour atteindre les niveaux de confiance, de sécurité et de qualité exigés par l'évolution du marché. L'accréditation reste cependant facultative. En conséquence :

- Les PSC doivent rester libres de souscrire à ces régimes d'accréditation et d'en bénéficier.
- Les PSC ne seront pas obligés de demander à être contrôlés dans le cadre de tout accord d'accréditation applicable ;
- Les Etats membres ne doivent pas interdire aux prestataires de service de certification d'opérer en marge de ces régimes d'accréditation.
- Les régimes d'accréditation ne doivent pas limiter la concurrence dans le secteur des services de certification. Tous les critères relatifs à ces régimes doivent être objectifs, transparents, proportionnés et non discriminatoires.
- Les Etats membres ne peuvent limiter le nombre de prestataires de service de certification agréés pour des motifs relevant du champ d'application de la directive.

Les Etats membres peuvent décider de la façon dont ils assurent le contrôle du respect des dispositions prévues par la Directive. Cette dernière n'exclut pas la mise en place de systèmes de contrôle faisant intervenir le secteur privé. Les services de certification peuvent être proposés soit par une entité publique soit par une personne morale ou physique, à condition que cette entité ou cette personne soit établie conformément au droit national. On constate cependant que l'accréditation est un régime procédant de l'Etat et non de la communauté des utilisateurs, réunis dans l'ICP. Ceci constitue un changement d'orientation pour l'accréditation par rapport à une exigence fondamentale des utilisateurs des ICP : la vérification de l'aptitude des PSC à respecter les Politiques de Certification.

2.3.2. L'accréditation selon l'ISO

Le concept d'accréditation n'est donc pas apparu pour la première fois dans la directive, le groupe de travail américain spécialisé sur les autorités de certification et les ICP, le groupe l'ISC de l'American Bar Association, l'utilise depuis plusieurs années. L'Union Européenne devra cependant composer car l'accréditation est d'abord un concept issu de l'ISO et qui fait l'objet en Europe d'une Infrastructure de travail.

L'accréditation répond à la définition suivante : "*Procédure par laquelle un organisme faisant autorité reconnaît formellement qu'un organisme ou un individu est compétent pour effectuer des tâches spécifiques*". Le but de l'accréditation est de favoriser les échanges commerciaux en supprimant toute entrave technique, le terme "technique" étant entendu au sens le plus large. Cette libéralisation des aléas techniques est obtenue à partir de la reconnaissance des essais, étalonnages, audits, inspections et autres types de contrôles techniques, dès lors qu'ils ont été réalisés par des organismes respectant les critères définis au niveau international (série des normes EN 45000, guides ISO/CEI...). L'accréditation est décernée par un organisme spécialisé. Il n'y a qu'un organisme d'accréditation par pays intervenant dans les domaines réglementaire et volontaire.

2.4 Les effets juridiques de la directive

La conséquence annoncée du système établi par la Directive est d'obtenir la reconnaissance juridique de la signature électronique. La nouvelle formulation de la définition est susceptible d'écarter une reconnaissance juridique quasi-automatique de la signature électronique. Il faut en effet conserver deux aspects d'une signature purement électronique (c.a.d. sans dimension juridique) : d'une part, pour des "signatures" appliquées sur des objets autres que des messages électroniques (ex.: signature et/ou certification de centre serveur), d'autre part, lorsque les effets juridiques ne sont pas recherchés (cas de la facture électronique).

Les effets juridiques finaux sont énoncés dans l'article 5 de la Directive :

> *1. Les Etats membres veillent à ce que les signatures électroniques reposant sur un certificat agréé et délivré par un prestataire de service de certification qui satisfait aux exigences prévues à l'annexe II soient, d'une part, reconnues comme conformes aux exigences légales relatives à une signature manuscrites et d'autre part, admises comme preuve en justice de la même façon que les signatures manuscrites.*
>
> *2. Les Etats membres veillent à ce qu'une signature électronique ne soit pas considérée comme dépourvue d'effet ou de validité juridique, ou de force exécutoire, au seul motif que la signature se présente sous forme électronique, ou qu'elle ne repose pas sur un certificat agréé, ou qu'elle ne repose pas sur un certificat délivré par un prestataire de service de certification accrédité.*

Le texte est sur ce point difficile à saisir. En prévoyant une signature reposant sur un certificat pas nécessairement agréé délivré par un PSC pas nécessairement accrédité, on multiplie les cas de figure. On peut atteindre une compréhension satisfaisante en considérant les deux faces de certains concepts juridiques : l'admissibilité de la preuve et la force probante. Par exemple en matière de preuve, l'admissibilité est la qualité d'un moyen quelconque d'être admis en justice comme preuve ; certains moyens ne sont pas admis. Une fois admis, le moyen peut se trouver contredit par un autre moyen. La force d'un moyen de preuve est fonction de son classement parmi la typologie des moyens établis par le Code Civil. La typologie va de l'écrit original au simple indice, en passant par la copie et le témoignage.

L'alinéa 2 de la Directive fixe une admissibilité générale de toutes les signatures électroniques, quand bien même, elles reposeraient sur un certificat non qualifié émis par un PSC non accrédité. Cette admissibilité joue pour la preuve et même en situation hors contentieux. Dans le cas de deux partenaires en échanges électronique, aucun des deux ne pourrait répudier la signature électronique au motif précisément de sa forme électronique. L'alinéa 1 est d'un effet supérieur puisqu'il vise la force de la signature électronique. Il s'agit naturellement d'une signature électronique "maximale" c.a.d. reposant sur un certificat agréé émis par un PSC accrédité. Dans ce cas aussi, l'admissibilité est générale. Mais la force de la signature électronique est maximale puisqu'elle se situe au niveau de la signature manuscrite. Cette force sans discussion possible est opposable à tous : aux utilisateurs concernés, au tiers et au juge qui devra lui reconnaître la force d'une signature manuscrite.

3 La transposition dans le droit français

3.1 L'intégration dans le Code civil : la loi n°2000-230 du 13 mars 2000

La Loi n°2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique apporte d'importantes modifications au Code Civil en ce qui concerne la notion de signature et l'écrit pour preuve. Pour la première fois, le Code Civil dans l'article 1316-4 nouveau énonce une définition de la signature dont on peut tirer deux caractéristiques présentées par toutes les signatures : la signature identifie le signataire et manifeste son consentement au contenu du document signé. Cette définition est valable pour tous types de signature. Par analogie avec l'écrit défini dans un autre article de la loi, la signature, jusqu'ici uniquement *manuscrite*, pourra adopter la modalité électronique. La signature électronique répondra naturellement à la même définition mais des précisions sont apportées sur la façon dont elle est réalisée. En effet, toute signature répond ainsi pour sa création à un véritable processus. Si la signature manuscrite est le résultat d'un procédé manuel, qui n'a généralement pas besoin d'être organisé, la signature électronique est produite par un procédé informatique d'identification fiable.

3.1.1. Signature et écrit électronique

Le procédé de signature doit présenter un lien avec l'acte auquel la signature s'attache. Cette précision est inutile dans le cas de la signature manuscrite dont on dit qu'elle est *apposée* sur le support papier. Mais l'électronique ne possède pas de support, c'est seulement une forme. Aussi la signature électronique doit donner une assurance qu'elle correspond bien à un message électronique déterminé. D'où l'idée du *lien* puisque de plus, la signature électronique peut voyager indépendamment des données concernées. Mais surtout le procédé technique doit être fiable. Les éléments qui concourront à cette fiabilité sont déterminés par un Décret en Conseil d'Etat. Cependant la loi liste les points à couvrir : création de la signature, assurance de l'identité du signataire et garantie de l'intégrité.

La garantie d'intégrité mentionnée par l'article 1316-4 est traitée d'une façon non satisfaisante, car elle est susceptible d'entraîner une discrimination injustifiée à l'encontre de certaines technologies de signatures électroniques, comme la signature graphique. La garantie d'intégrité s'applique en effet au message électronique. C'est lui qui doit rester intègre tout au long de l'échange électronique puis ultérieurement dans l'étape d'archivage (cf. article 1316-1 nouveau). La garantie d'intégrité semble bien indispensable. Mais pourquoi la rendre indissociable de la signature alors que d'autres procédés techniques existent apportant la même garantie ?

Autre point à signaler, le respect des exigences formulées par le Décret en Conseil d'Etat ne permettra que de donner une "présomption" de fiabilité au procédé. En effet, dans tous les cas, il sera nécessaire d'être en mesure de démontrer que le procédé technique est fiable :

- Si les exigences du décret sont respectées (et peut être constatées par une "accréditation"), il y a aura présomption simple c.a.d. pas de charge de la preuve, mais seulement jusqu'à preuve contraire,
- Si les exigences du décret ne sont pas respectées, les utilisateurs devront supporter la charge de la preuve en cas de contestation et se disposer à démontrer par tout moyen la fiabilité du procédé.

Enfin par rapport au texte originel du projet de loi, les sénateurs qui ont été saisis du projet de loi avant les députés ont introduit dans l'article 1316-4 un amendement concernant les officiers publics. Dans tous les cas, la signature apposée par un officier public est un brevet d'authenticité, qu'elle soit manuscrite ou électronique. Une signature électronique issue d'un procédé d'identification fiable ne lui donnera qu'une présomption simple. Peu de choses à côté de la force et de la portée de la signature d'un officier public. L'amendement des sénateurs est à double détente : si les officiers publics peuvent signer électroniquement, c'est parce qu'ils peuvent également passer leurs écrits à la forme électronique. La loi leur ouvre la voie aux actes authentiques électroniques. Un amendement bien anodin dont on n'a pas fini de mesurer toutes les conséquences…

3.1.2. La preuve en contexte électronique

Le Code Civil connaît avec cette loi une innovation fondamentale autant que de bon sens : l'ouverture aux formes électroniques de l'informatique. Le législateur a décidé d'intégrer les donnés dans les moyens sans les subordonner à la primauté de l'écrit. Au contraire, l'écrit comprend désormais deux modalités : le support écrit comme traditionnellement et la forme électronique. Pour la première fois aussi, le Code définit la notion d'écrit dans l'article 1316 nouveau : *une suite de lettres, de caractères, de chiffres ou de tous autres signes ou symboles dotés d'une signification intelligible.* L'écrit reste comme auparavant le moyen dominant d'apporter la preuve et l'écrit électronique bénéficie désormais du même pouvoir. Mais comme pour la signature électronique, l'écrit de forme électronique doit être accompagné de certaines caractéristiques qui vont de soi dans l'écrit-papier traditionnel mais qui devront être vérifiés dans le contexte électronique, selon l'article 1316-1.

Pour l'écrit traditionnel, il peut être simple de déterminer son origine : papier à entête, indication de l'auteur en toutes lettres, éléments postaux, etc. La chose est plus délicate en électronique surtout s'il y a télétransmission. Il y a aussi la pérennité du support : malgré une apparente fragilité, le papier peut se conserver plusieurs siècles. Quant à l'écrit électronique, il ne possède pas de support et n'est constitué que d'informations élémentaires qui peuvent cheminer par des voies différentes et donc se perdre pendant les télétransmissions. D'où une exigence d'intégrité à respecter.

Il est exigé de l'écrit électronique qu'il garantisse authentification ("*la personne dont il émane*") et intégrité (dans l'établissement et la conservation). Toute mesure de sécurité permettant de garantir ces points permettra à tout message et fichier de données d'obtenir la qualification d'*écrit sous forme électronique* et d'être un bon moyen de preuve. Naturellement on aura remarqué que l'écrit électronique exige des garanties... caractéristiques de la signature électronique. On en tirera deux conclusions fondamentales :

- une signature électronique valide permettra efficacement à tout ensemble de données d'acquérir la qualité d'écrit et la force probante ;
- la signature électronique montre un intérêt a posteriori pour l'administration de la preuve et non a priori pour la validité de l'écrit électronique, une signature hautement technologique qui est *ad probationem* (c'est-à-dire pour le preuve) et non *ad validitatem* (c'est-à-dire pour la validité du document). Cette conclusion est à considérer dans les processus de dématérialisation documentaire. Lorsqu'un texte juridique exige un support écrit pour un acte juridique, la dématérialisation sauvage ne sera par valide même en prenant la précaution de munir la forme dématérialisée d'une signature électronique.

3.2 Des exigences techniques fixées par le Droit de la signature électronique

3.2.1. Le Décret n°2001-272 du 30 mars 2001

L'article 1316-4 du Code Civil stipule que la signature électronique "*consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache"*. Il ajoute qu'un décret en Conseil d'Etat fixera les conditions dans lesquelles *"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"*. Il s'agit du Décret n°2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du Code Civil et relatif à la signature électronique.

La signature électronique était un moyen de sécurité des échanges électroniques bien avant que les juristes ne s'en emparent pour lui donner une valeur juridique. Pour atteindre des objectifs sécuritaires, les techniciens avaient le choix dans une large palette de paramètres techniques. Lorsqu'il s'agit d'atteindre un objectif juridique déterminé (l'équivalence avec une signature manuscrite), le législateur limite la liberté des techniciens en leur imposant des exigences techniques précises. Ces exigences sont listées dans le décret d'application qui transpose les annexes techniques de la Directive européenne sur la signature électronique. Lorsqu'une signature respecte la totalité des impératifs techniques du Décret, elle prend le nom de *signature électronique sécurisée* (SES). Seul ce type de signature bénéficie de la présomption de fiabilité instaurée par le Code Civil, ce qui lui permet de jouer sur un message électronique le même rôle qu'une signature manuscrite sur papier.

Quelques rappels sont nécessaires en ce qui concerne les composants de la signature électronique :
- La signature électronique est générée par un logiciel qui prend le nom de "*Dispositif de création de signature*" (DCS),
- La signature électronique dans le message arrivé à destination doit être vérifiée par un logiciel appelé "*Dispositif de vérification de signature*" (DVS).
- Le DVS doit disposer de certaines informations (la clé publique du signataire) contenue dans un *certificat électronique*.
- Le certificat électronique est préparé, vérifié et diffusé par un *Prestataire de Services de Certification Electronique* (PSC).

Le décret impose à chacun de ces composants un supplément de rigueur et de précision par rapport à l'utilisation purement technique de la signature. La SES comprend un DCS *sécurisé* et met en œuvre un certificat électronique *qualifié* délivré par un PSC également *qualifié* :

S.E.S. = Dispositif **SECURISE** de création de signature + certificat électronique **QUALIFIE**	
⇓	⇓
le DCS est sécurisé si :	Le certificat est QUALIFIE si
1) Exigences techniques remplies	1) certificat conforme
2) Certification du DCS	2) un PSC **QUALIFIE**

La difficulté est quasi insurmontable pour les utilisateurs de juger par eux-mêmes de la conformité des spécifications techniques aux exigences réglementaires. Aussi le décret établit-il des systèmes de contrôles sanctionnés par divers agréments :
- Pour se présenter comme "*sécurisé*", un DCS doit respecter les exigences techniques de l'article 5.-I et se faire contrôler et *certifier* par les services spécialisés du Premier Ministre (le SCSSI) (art. 5.-II).
- Pour se présenter comme "*qualifié*", un certificat doit être conforme aux prescriptions de l'article 6.-I. Le certificat est émis par un PSC qui répond quant à son organisation et son fonctionnement aux stipulations de l'article 6.-II.
- En cas de doute ou d'incertitude sur la qualification du certificat, l'utilisateur pourra se tourner vers le SCSSI qui auditera certificats et prestataire et en rendra publics les résultats (art. 9).
- Les PSC pourront faire constater l'excellence de leurs prestations en sollicitant une *qualification* de leur activité auprès du Ministre chargé de l'Industrie (art. 7).
- Les Dispositifs de vérification de signature, qui doivent être compatibles avec les DCS pourront être *évalués* par le SCSSI, s'ils répondent aux exigences de l'article 5.

3.2.2. Le décret 2002-535

Un an après la parution du Décret d'application (n°2001-272) de l'article 1316-4 du Code Civil sur la signature électronique, les cinq arrêtés d'application annoncés par ledit décret ont été suppléés par un *Décret n°2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes*

des technologies de l'information[1]. Ce nouveau décret modifie l'ancien et prévoit que la reconnaissance de conformité des composants de signature électroniques aux exigences techniques du décret 2001-272 passe par une procédure d'agrément – évaluation – certification :

- Les centres techniques chargés de l'audit des composants doivent être agréés. La demande d'agrément est formulée auprès de la DCSSI et précise le domaine dans lequel l'organisme demandeur entend exercer son activité. L'agrément est délivré par le Premier Ministre, après avis d'un Comité directeur de la certification. Il est valable pour une durée de deux ans renouvelable.
- Tout candidat à la certification d'un composant doit d'abord le faire évaluer. Pour cela, il adresse à la DCSSI un dossier d'évaluation qui comporte la description du système de sécurité à évaluer, les dispositions prévues pour lui conférer sa pleine efficacité ainsi que le programme de travail prévisionnel. Avant le début des travaux, il détermine avec le centre d'évaluation le produit ou le système à évaluer ainsi que les objectifs de sécurité, le coût et les modalités de paiement de l'évaluation, le programme de travail et les délais prévus pour l'évaluation.
- Au terme des travaux d'évaluation, l'évaluateur remet un rapport d'évaluation au demandeur et à la DCSSI. Le candidat et la DCSSI valident les rapports d'évaluation en liaison avec le centre d'évaluation. Puis la DCSSI élabore un rapport de certification dans un délai d'un mois. Ce dernier conclut soit à la délivrance d'un certificat, soit au refus de la certification.
- Le certificat est délivré par le Premier ministre. Il atteste que l'exemplaire du produit ou du système soumis à évaluation répond aux caractéristiques de sécurité spécifiées. Il atteste également que l'évaluation a été conduite conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises.

3.3 La compétence et la qualité exigées chez les prestataires

La procédure et les modalités de la qualification des Prestataires de Services de Certification Electronique (PSCE) sont désormais connus depuis un *Arrêté du 31 mai 2002 relatif à la reconnaissance de la qualification des PSCE et à l'accréditation des organismes chargés de l'évaluation* [2]. La qualification d'un PSCE est prononcée après une évaluation de sa pratique professionnelle et des certificats émis. L'évaluation des PSCE est effectuée par un *organisme accrédité* et aux frais du PSCE. L'objet de l'évaluation porte sur le respect des exigences techniques et organisationnelles de l'article 6 du Décret 2001-272 ainsi que les normes, les prescriptions techniques et les règles de bonne pratique applicables en matière de certification électronique.

A l'issue des contrôles, l'organisme accrédité établit un rapport qui est notifié au prestataire afin que celui-ci puisse, le cas échéant, formuler des observations sur son contenu. En conclusion de l'évaluation, l'organisme accrédité reconnaît ou non la qualification du prestataire de services de certification électronique à partir de son rapport et des éventuelles observations du prestataire. Lorsqu'il reconnaît la qualification d'un prestataire, l'organisme accrédité produit une *attestation* décrivant les prestations de services couvertes par la qualification ainsi que la durée, qui ne peut excéder un an, pendant laquelle elle est valable. A titre d'application de l'article 6-II-o du Décret[3], les prestataires dont la qualification est reconnue communiquent à toute personne qui en fait la demande une copie de l'attestation délivrée par l'organisme accrédité.

Le processus de qualification dépend d'organismes accrédités[4]. Le Comité français d'accréditation (COFRAC), association déclarée le 4 mai 1994, est chargé d'accréditer les organismes qui procéderont à l'évaluation des prestataires de services de certification électronique en vue de reconnaître leur qualification. Selon la procédure ISO d'accréditation, il n'y a un organisme d'accréditation par pays. Au niveau international existe un système d'audits croisés entre les différents pays afin d'assurer la reconnaissance mutuelle, dans tout l'Espace Economique Européen, des attestations émanant d'organismes accrédités. L'accréditation permet d'harmoniser, dans un contexte européen et international, les pratiques des organismes en mettant en œuvre des règles, des critères et des processus de décision communs à tous les secteurs. Aussi le COFRAC est-il membre de l'*European Co-operation for Accreditation* et signataire de l'*Accord multilatéral Européen d'Accréditation* pour les essais, les étalonnages et la certification.

---

1 Pour de plus amples informations, voir notre *DOC_9 le Décret 2002-535.*

2 Pour de plus amples informations, voir notre *DOC_12 La qualification des PSCE – l'arrêté du 31 mai 2002*

3 Selon l'article 6-II-o du Décret, avant la conclusion d'un contrat de prestation de services de certification électronique, le PSCE doit informer par écrit la personne demandant la délivrance d'un certificat électronique du fait qu'il s'est soumis ou non au processus de qualification volontaire des prestataires de services de certification électronique de l'article 7 du Décret.

4 C'est par erreur que la Directive 1999/93/CE sur un cadre communautaire pour les signatures électroniques parle d'*accréditation des PSC(E)* (cf. art. 3 de la Directive). Il s'agit en fait d'*accréditation* de l'organisme de contrôle qui procédera à la *qualification* des PSCE.

Dans le droit interne, la demande d'accréditation adressée par un organisme au COFRAC doit comprendre un certain nombre d'informations élémentaires sur le demandeur (voir l'article 2 de l'arrêté pour le détail), notamment la description des activités de l'organisme, de sa structure et de ses moyens techniques. Il y joindra la description des procédures et des moyens qui seront mis en œuvre pour évaluer les PSCE en vue de reconnaître leur qualification, compte tenu des normes ou prescriptions techniques en vigueur. L'organisme demandeur doit signaler au centre d'accréditation les liens éventuels qu'il a avec des prestataires de services de certification électronique. En ce cas, il doit préciser les mesures qu'il compte mettre en œuvre pour éviter tout conflit d'intérêts. Le COFRAC instruira la demande d'accréditation. Il pourra solliciter tous renseignements complémentaires de l'organisme demandeur et effectuer des vérifications dans les locaux de l'organisme demandeur. A l'issue de l'instruction, le centre d'accréditation prend une décision motivée qu'il notifie à l'organisme demandeur. L'accréditation est accordée pour une durée de deux ans. Elle peut être renouvelée pour une durée identique.