Projet ICare

La Directive Européenne Signature Electronique

Référence : ICARE/CAB/TPC/DOC_31/v1
Type : Document
Diffusion : Diffusion limitée aux membres du consortium

Date : 05/05/2003
Titre : **ICare – La Directive Européenne sur la Signature Electronique**

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

Résumé :
Cette note décrit et commente la base juridique de la législation française en matière de signature électronique, la Directive 1999/93.

TABLE DES MATIERES

1 Introduction

La législation française en matière de signature électronique trouve ses fondements dans la transposition de la *Directive 1999/93/CE sur un cadre communautaire pour les signatures électroniques*. Ce texte suprême pose les bases pour le droit interne de chaque Etat membre de l'Union Européenne. Aussi l'étude de ce texte est-il indispensable d'une part, pour comprendre quels sont les choix juridiques et technologiques du droit français et d'autre part, pour comprendre les bases qui sont communes à la France et aux autres pays de l'Union. Ces bases permettent d'augurer de l'interopérabilité des produits et services et de la liberté de diffusion et de commercialisation de ceux-ci.

En conséquence, la note est consacrée à la présentation et au commentaire de la Directive Signature Electronique.

Le 13 mai 1998, la Commission a présenté la proposition de directive sur un cadre commun pour les signatures électroniques. Le Parlement européen l'a approuvée le 13 janvier 1999, après avoir introduit quelques amendements. La Commission a donc présenté une proposition modifiée le 29 avril 1999, sur laquelle le Conseil a adopté une position commune. Le 27 octobre 1999, le Parlement européen a adopté quelques amendements formels à ce texte, sur lequel le Conseil s'est prononcé le 29 novembre 1999. Le texte définitif est la Directive 1999/93/CE du Parlement européen et du Conseil du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques.

La Directive énonce tout d'abord ses motifs sous 28 *considérants* qui situent le texte dans la politique de l'Union Européenne dans les Techniques de l'Information et de la Communication. La Directive est encore composée de 4 annexes, précédées de 15 articles dont la teneur est la suivante :

- L'*article 1 Champ d'application* fixe le périmètre de la Directive : reconnaissance juridique de la signature électronique, strictement sans empiétement sur le formalisme juridique documentaire prévu dans le droit interne des Etats membres.
- L'*article 2 Définitions* identifie et définit les termes techniques employés dans le texte.
- L'*article 3 Accès au marché* prévoit que tous les composants techniques de la SE peuvent faire l'objet d'un système de contrôle non obligatoire des Etats membres qui ne doit pas restreindre la liberté des prestataires.
- L'*article 4 Principes du marché intérieur* rappelle que le principe de liberté de l'article précédent s'applique lorsque les composants et les prestataires sont originaires d'un autre Etat membre de l'Union.
- L'*article 5 Effets juridiques des signatures électroniques* établit le régime juridique basique de la SE, le cœur de la Directive.
- L'*article 6 Responsabilité* traite de la responsabilité des prestataires de certification (les autorités de certification de la technique) à l'égard des utilisateurs de certificats électroniques.
- L'*article 7 Aspects internationaux* pose les conditions auxquelles un prestataire de services de certification appartenant à un pays extérieur à l'Union verra ses certificats reconnus valides.
- L'*article 8 Protection des données* rappelle que la certification électronique est soumise à la réglementation européenne en matière de protection des données personnelles.
- L'*article 9 Comité* instaure un comité de suivi de la mise en application des dispositions de la Directive et est complété par l'*article 10 Tâches du comité.*
- L'*article 11 Notification* créée une obligation d'information de la Commission à la charge des Etats membres en matière de système de contrôle des certificateurs (régimes d'accréditation).
- Les articles 12 à 14 sont des articles de service[1].
- L'*annexe I* liste les exigences concernant les certificats qualifiés.
- L'*annexe II* établit les exigences concernant les prestataires de service de certification délivrant des certificats qualifiés.
- L'*annexe III* décline la liste des exigences pour les dispositifs sécurisés de création de signature électronique (outil de signature)
- *L'annexe IV* émet des recommandations pour la vérification sécurisée de la signature (applicables aux outils de vérification de signature).

[1] *article 12 Examen* (audit de la Commission et compte-rendu au Parlement européen), *article 13 Mise en œuvre* (de la Directive), *article 14 Entrée en vigueur*, *article 15 Destinataires* (Les Etats membres).

2 La dimension juridique europeenne de la signature électronique

Cette section situe la Directive dans l'ensemble des textes juridiques européens, en particulier par rapport aux notions techniques et juridiques proches dans les nouvelles technologies de l'information et de la communication. Ce positionnement fait, il est possible d'envisager les effets juridiques de cet instrument typique des relations juridiques, la signature électronique.

2.1 Le périmètre juridique de la signature

211 La signature de la Directive est intra-européenne

Comme l'indique son titre, la *Directive 1999/93/CE du parlement européen et du conseil du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques* (JOCE du 17.1.2002 n°L 15/24) le texte vise le "cadre commun pour la signature électronique". Les principes juridiques posés sont minimaux et visent une utilisation intra-européenne, ce qui conduit aux conséquences suivantes :

- Ils doivent être adoptés par la législation des Etats membres de l'Union Européenne au moment de la transposition de la Directive. Ainsi le ressortissant d'un Etat pourra signer un message électronique selon des conditions et des modalités et avec des effets acceptés par un destinataire de message situé dans un autre pays de l'Union.
- Les Etats membres transposent le texte en l'enrichissant éventuellement selon leur génie juridique, ce qui explique que les législations sont souvent dissemblables quoiqu'elles reconnaissent toutes la validité juridique de la signature électronique.
- Les Etats membres n'imposent pas leur législation interne pour les utilisations spécifiques de signature électronique à des communautés fermées d'utilisateur.

On peut voir à ce sujet le considérant 16 de la Directive :

(16) la présente directive favorise l'utilisation et la reconnaissance juridique des signatures électroniques dans la Communauté ; un cadre réglementaire n'est pas nécessaire pour les signatures électroniques utilisées exclusivement à l'intérieur de systèmes résultant d'accords volontaires de droit privé entre un nombre défini de participants ; il est nécessaire que la liberté des parties de convenir entre elles des modalités et conditions dans lesquelles elles acceptent les données signées électroniquement soit respectée dans les limites autorisées par le droit national ; il convient de reconnaître l'efficacité juridique des signatures électroniques utilisées dans de tels systèmes et leur recevabilité comme preuves en justice ;

212 La signature et non le chiffrement

Le marché intérieur européen nécessite la sécurisation des échanges électroniques. A cet égard, la Commission de Bruxelles a fait le pari que la signature électronique participerait à la validité des échanges électroniques, en particulier dans le Commerce Electronique, en apportant des assurances en termes d'origine des messages et d'intégrité dans les transmissions. Cet objectif rentre dans la mission générale de l'Union Européenne pour le bénéfice des Etats-membres. A l'opposé en prétendant réguler la confidentialité des échanges électroniques, elle rencontrerait l'opposition de certains Etats-membres qui mettraient en avant les impératifs de la sûreté intérieure et de la défense nationale qui peuvent être opposés à ceux du Commerce Electronique. C'est un point important de l'auto-limitation que se donne la Commission en distinguant la distinction la signature électronique du chiffrement. Cette situation explique que la Commission est prête à participer à la régulation des infrastructures, sous réserve de la compétence de normalisation technique des organisations internationale, largement en matière de signature électronique mais plus prudemment en matière de chiffrement. Comme exposé dans un document COM503[2] :

> *Le Traité CEE et le Traité de l'Union européenne respectent pleinement la compétence des Etats membres dans les domaines de la sécurité nationale et de l'application du droit. Si des restrictions nationales sont établies, elles doivent rester compatibles avec la législation communautaire. La Commission va examiner si des restrictions nationales peuvent être totalement ou partiellement justifiées, en particulier au vu des dispositions du Traité en matière de libre circulation et des dispositions de la Directive communautaire sur la protection des données.*

[2] COM(97)503, projet de communication de la Commission : *Assurer la sécurité et la confiance dans la communication électronique - vers un Cadre Européen Pour Les Signatures Numériques et la Cryptographie"*

Le principe est repris dans la Directive[3] sur un cadre communautaire pour les signatures électroniques dans son considérant n°6 :

> *"La présente directive n'harmonise pas la fourniture de services en ce qui concerne la confidentialité de l'information quand ils sont couverts par des dispositions nationales relatives à l'ordre public ou à la sécurité publique."*

213 La Directive n'empiète pas sur le droit des contrats

Le Commerce est l'affaire des Etats et dans les Etats, l'affaire des particuliers, Commerce Electronique compris. Aussi la signature de la Directive n'est pas un point de passage obligé pour des contrats qui seraient formés et exécutés électroniquement[4]. Ce point est précisé dans le considérant 17 de la Directive :

> *"La présente directive ne vise pas à harmoniser les règles nationales concernant le droit des contrats, en particulier la formation et l'exécution des contrats, ou d'autres formalités de nature non contractuelle concernant les signatures ; pour cette raison, il est nécessaire que les dispositions concernant les effets juridiques des signatures électroniques ne portent pas atteinte aux obligations d'ordre formel instituées par le droit national pour la conclusion de contrats ni aux règles déterminant le lieu où un contrat est conclu ;"*

2.2 Les effets des signatures électroniques

Le but principal de la Directive est d'aboutir à une reconnaissance juridique de la Signature Electronique dans le système juridique de chacun des Etats membres. Cette reconnaissance devrait permettre à la Signature Electronique de présenter les mêmes effets que la signature (manuscrite) sur un document papier. Mais ces effets varient selon le type de signature envisagé par la Directive.

221 La signature avancée comme moyen de preuve

La *Signature Electronique Avancée* n'est pas seulement un sur-ensemble de la signature ordinaire de la Directive. Elle est la signature pleine et entière des juristes, celle qui est permet les effets juridiques de l'article 5.1. :

> *"Les Etats membres veillent à ce que les signatures électroniques avancées basées sur un certificat qualifié et créées par un dispositif sécurisé de création de signature :*
> *a) répondent aux exigences légales d'une signature à l'égard de données électroniques de la même manière qu'une signature manuscrite répond à ces exigences à l'égard de données manuscrites ou imprimées sur papier,*
> *et b) soient recevables comme preuves en justice".*

Le point b sur la *preuve* de l'article est la conséquence la plus attendue de la reconnaissance de la validité juridique de la signature électronique. La formulation du point a permet d'élargir les objectifs juridiques potentiels : dans chaque pays de l'Union, la signature électronique sur un message électronique doit présenter les mêmes caractéristiques qu'une signature manuscrite sur un document papier de même nature. Au total, la *Signature Electronique Avancée* garantit l'identification et l'intégrité. Elle est admise en justice et possède une force probante maximale. Mais elle n'apporte aucun certitude en matière de consentement du signataire sur le contenu du fichier signé (cf. infra)

222 La prise en compte juridique des signature non avancées

A contrario, la signature électronique ordinaire de la Directive n'a pas la perfection accordée à la signature électronique avancée. Pour en apprécier les effets juridiques, il est nécessaire d'interpréter l'article 5.2. de la Directive qui déclare :

---

[3] Directive 1999/93/CE du parlement européen et du conseil du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques (JOCE du 17.1.2002 n°L 15/24) ;

[4] La formation des contrats en ligne, par exemple par une succession de messages alternatifs entre les parties, est délicat à règle au regard du droit. Le sujet est traité dans une autre directive, 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") (JOCE du 17 juillet 2000 p. L.178/1).

"*Les Etats membres veillent à ce que l'efficacité juridique et la recevabilité comme preuve en justice ne soient pas refusées à une signature électronique au seul motif que :*

- *la signature se présente sous forme électronique*
- *Ou, qu'elle ne repose pas sur un certificat qualifié*
- *ou qu'elle ne repose pas sur un certificat qualifié délivré par un prestataire accrédité de service de certification*
- *qu'elle n'est pas créée par un dispositif sécurisé de création de signature".*

Les différents cas listés par le texte caractérisent une signature qui ne posséderait pas la totalité des caractéristiques attendues : certificat qualifié, prestataire accrédité, dispositif sécurisé de création de signature. Ainsi la *signature numérique* qui garantit l'identification et l'intégrité pourrait rentrer dans la sphère juridique, par exemple, si le signataire est un être humain. Ce qui ne lui donne pas nécessairement pas un caractère juridique, si elle n'est pas apposée sur un acte juridique sous forme électronique[5]. La réflexion est de même nature pour une signature qu'on aurait voulu *avancée* mais qui à l'expérience aurait été créé par un système quelconque c'est-à-dire non sécurisé ou qui ferait l'objet d'un certificat non qualifié ou encore d'un certificat certes qualifié mais émis par un PSC non qualifié. Bref, cette signature imparfaite aurait tout d'une signature avancée *dégradée.*

La directive prévoit ici qu'on ne peut répudier ce type de signature de façon générale. On doit la considérer même si elle est imparfaite. Sa dégradation ne suffit pas pour l'exclure des instruments juridiques. Par application de l'article 5.2., la Signature Electronique ordinaire serait *admissible* aux fins de preuve, quoiqu'on puisse s'interroger sur sa *portée* exacte[6].

Enfin on ne voit pas comment la Signature Electronique ordinaire serait en mesure de fournir quelque assurance que ce soit en matière de consentement du signataire. La question du consentement, typique des pays de droit civil[7], est d'ailleurs absente de la Directive européenne qui ne l'inclut pas dans les caractéristiques de la signature, au contraire de la *Loi type de la CNUDCI.*

223 Le consentement, cet inconnu

L'article 2 de la loi type de la CNUDCI sur les signatures électroniques[8] présente en effet la définition suivante :

> *"a) Le terme "signature électronique" désigne des données sous forme électronique contenues dans un message de données ou jointes ou logiquement associées audit message, pouvant être utilisées pour identifier le signataire dans le cadre du message de données et indiquer qu'il approuve l'information qui y est contenue".*

Cette définition indique comme caractéristique de la signature électronique l'identification et le consentement à l'information. Il est vrai que dans la plupart des systèmes juridiques, la signature est une marque personnelle de l'auteur du texte, au point que la forme la plus élémentaire de la signature s'appuie sur la transcription graphique du nom du signataire. Il en va tout autrement de la signature électronique dont la base est le message ou le fichier électronique[9].

Dans cette définition, on ne voit nulle trace de la question de l'intégrité. La notion n'est toutefois pas totalement absente : on la retrouve sous le couvert de la notion de fiabilité dans l'article 6 "Satisfaction de l'exigence de signature" :

---

[5] On ne peut se contenter d'étudier la signature électronique, prise isolément. Il faut considérer sur quoi elle s'applique. Puisque cette signature est de nature juridique, elle est apposée sur un document électronique de nature juridique c.a.d. un document qui contient des obligations ou des droits.

[6] L'*admissibilité* est la possibilité de produire un moyen en justice aux fins de preuve, car certains moyens peuvent être refusés. La *portée* traduit l'efficacité du moyen (surtout en face de moyen de preuve contraire opposé par un adversaire).

[7] Les pays dits de *droit civil* présentent un système juridique qui résulte de textes législatifs. A l'inverse, les pays dits de *common law* possèdent un système juridique qui se réfère à la pratique des juridictions .

[8] Rapport de la Commission des Nations Unies sur le droit commercial international sur les travaux de sa trente-quatrième session, tenue à Vienne du 25 juin au 13 juillet 2001, adopté le 5 juillet 2001. Disponible au service des publications de la CNUDCI ou sur son site Web : www.uncitral.org .

[9] La signature électronique n'est pas un signe propre au signataire, mais un condensé du message à signer, calculé par un algorithme de hachage et chiffré par un algorithme cryptographique initialisé par la clé privée du signataire.

> *1.Lorsque la loi exige la signature d'une certaine personne, cette exigence est satisfaite dans le cas d'un message de données s'il est fait usage d'une signature électronique dont la fiabilité est suffisante au regard de l'objet pour lequel le message de données a été créé ou communiqué, compte tenu de toutes les circonstances, y compris toute convention en la matière.*

L'article 6-3 indique ce qu'on peut entendre par fiabilité :

> *Une signature électronique est considérée fiable en ce qu'elle satisfait à l'exigence indiquée au paragraphe 1 si : ...*
> *d) Dans le cas où l'exigence légale de signature a pour but de garantir l'intégrité de l'information à laquelle elle se rapporte, toute modification apportée à cette information après le moment de la signature est décelable.*

Ainsi la Loi type vise expressément l'identification et tacitement l'intégrité. Elle mentionne encore l'approbation sur l'information contenue dans le document signé, c.a.d. le consentement sur le contenu juridique. Le consentement doit être manifeste selon la loi, ce qui s'analyse sur les deux éléments suivants :

- Le consentement porte sur le contenu d'un acte juridique. Pour s'assurer de la concordance d'un contenu juridique avec sa volonté, le (futur) signataire doit préalablement lire le document avant de procéder à sa signature.
- Pour que le consentement soit manifeste, il faut le... manifester de façon volontaire. Ce qui exclut tout traitement automatique. Il est bon de rappeler que certains serveurs d'entreprise sont susceptibles de signer à la volée tous les messages électroniques qui en sortent sans intervention humaine.

224 La responsabilité des PSC

La directive prévoit la responsabilité des tiers de certification pour tout préjudice causé par l'utilisation d'un certificat inexact ou invalide. Ils peuvent cependant dégager leur responsabilité en prouvant qu'ils n'ont commis aucune négligence. Qui est responsable si la vérification de la signature électronique ne rend pas un résultat satisfaisant ? Par exemple, si le certificat et consécutivement la clé publique ne permettent pas de déchiffrer la signature, la signature ne correspond pas à l'expéditeur du message, les effets juridiques du message deviennent incertains. La question est posée de la responsabilité du PSC. La position qui consiste à rendre le PSC pleinement responsable doit être nuancée.

Outre le cadre contractuel général, d'autres éléments sur la responsabilité peuvent être tirés des dispositions de la Directive Signature Electronique. Selon le texte, la responsabilité du PSC est raisonnablement limitée :

- La responsabilité ne porte que sur les certificats agréés. Ainsi la responsabilité en cascade se trouve désactivée. Même si les utilisateurs tirent la responsabilité du PSC sur le terrain de la signature électronique et de sa validité, les conséquences juridiques ne doivent pas aller plus loin. La Directive limite d'ailleurs d'elle-même son champ d'application, puisqu'elle *"ne couvre pas les aspects liés à la conclusion et à la validité des contrats"*[10].
- La responsabilité du PSC couvre l'exactitude et la pertinence des informations contenues dans le certificat agréé sauf si le PSC prouve qu'il n'a commis nulle négligence. S'il a limité sa responsabilité, par exemple sur la valeur limite des transactions pour lesquels le certificat est utilisé, elle doit être discernable par les Tiers[11].
- La responsabilité peut être cantonnée dans les limites d'utilisation du certificat spécifiées dans celui-ci. Dans la certification électronique classique, ces restrictions d'utilisation sont généralement fixées par les Politiques de Certification.
- La responsabilité peut être cantonnée à une valeur financière limite des transactions pour lesquelles le certificat est valable.

Pour disposer ainsi du "crédit" des utilisateurs, le PSC devra disposer de garanties financières. Outre sa surface financière, il devra posséder une Assurance Professionnelle. L'Annexe II indique qu'il devra *"disposer des ressources financières suffisantes pour fonctionner conformément aux exigences prévues par la présente directive, en particulier pour endosser la responsabilité de dommages, en contractant, par exemple, une assurance appropriée."*

[10] La question des contrats en ligne est cependant traitée par un autre texte communautaire en cours d'élaboration au moment de la rédaction de cet ouvrage, la Directive sur certains aspects juridiques sur commerce électronique. Y est notamment posé le principe de la validité de la conclusion des contrats en ligne.

[11] Application de la réglementation communautaire des clauses abusives dans les contrats conclu avec les consommateurs - Directive 93/13CEE du 5 avril 1993.

L'annexe II de la Directive "*Exigences concernant les prestations de service de certification délivrant des certificats agréés*" pose que les relations entre le PSC et ses clients doit faire l'objet d'un contrat transmis par un *"moyen de communication durable"* c.à.d. par écrit ou par voie électronique (sic !) qui sera remis à ceux-ci préalablement à l'engagement des relations. Certaines clauses sont suggérées, en particulier :

- les conditions d'utilisation des certificats,
- les limites de la responsabilité du prestataire,
- l'existence d'un régime volontaire d'accréditation,
- l'existence de procédures de réclamation et de règlement des litiges.

La Directive fixe certains points relatifs aux certificats et à leur gestion technique. Le service doit présenter les spécificités suivantes :

- Il doit comporter un service de révocation.
- Il doit vérifier la qualité du destinataire du certificat.
- Toutes les mesures utiles doivent être prises afin de pouvoir, le moment venu, administrer la preuve en justice, notamment par l'enregistrement électronique des informations pertinentes.
- Si le PSC tire les clés privées de son client, il ne stocke pas ces dernières, sauf si cela fait l'objet d'un service optionnel aux clients. Il devra garantir la confidentialité pendant la génération des clés.
- Le PSC doit prendre toutes les mesures pour éviter la "contrefaçon" de certificats.

La pérennité des PSC ou la durabilité de la certification n'est pas actuellement envisagée. Elle pourrait l'être dans les législations nationales.

3 Les bases techniques de la Directive

La Signature Electronique de la Directive est une construction juridique plaquée sur la réalité de la signature numérique des techniciens. Aussi ne sera-t-on pas surpris d'y trouver une certaine prise en compte des composants techniques habituels de la signature numérique : moyens de cryptographie asymétrique et prestation de certification électronique. La prise en compte est cependant limitée puisque la Directive se veut technologiquement neutre, ce qui n'empêche pas par ailleurs les organismes de normalisation technique européen d'apporter leur support en termes de normes, protocoles et standards.

3.1 Deux types de signature

La Directive 1999/93/CE du parlement européen et du conseil du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques reconnaît deux types de signatures électroniques. L'attention du juriste est immédiatement attiré par la *signature électronique avancée* qui est l'instrument prévu pour rendre dans le monde électronique les mêmes services que la signature manuscrite dans le monde de l'écrit-papier. Cependant la signature avancée ne doit pas venir éclipser l'autre signature qui ne doit pas être pour autant minimisée.

311 La Signature Electronique "ordinaire" de la Directive

L'article 2 de la Directive précise : *"on entend par «signature électronique», une donnée sous forme électronique, qui est jointe ou liée logiquement à d'autres données électroniques et qui sert de méthode d'authentification"*. Nous la désignerons ici sous le nom de *signature électronique ordinaire*. Cette signature n'assure qu'un niveau de sécurité incomplet : si elle prend en compte l'authentification, elle ne donne aucune garantie en ce qui concerne l'intégrité[12]. De plus, elle ne semble pas présenter une caractéristique universelle du Droit, tout au moins dans les pays de droit civil[13], le consentement du signataire. On peut d'ailleurs douter que la

[12] La signature électronique est d'abord une invention des techniciens avant d'être la découverte des juristes. La signature garantit d'abord l'identification de l'expéditeur mais également l'intégrité du message. Standardisée au niveau international, la "*digital signature*" est définie par la norme ISO 7498-2 de la façon suivante : "*Données ajoutées à une unité de données, ou transformation cryptographique d'une unité de données permettant à un destinataire de prouver la source et l'intégrité de cette unité en la protégeant contre la contrefaçon (par le destinataire par exemple)*".

[13] La solution est moins nette dans les "pays de common law"

Signature Electronique ordinaire soit créée par un être humain, tandis que la Directive envisage une signature avancée qui, elle, est précisément rattachée à un signataire.

La Signature Electronique ordinaire ne prétend pas assurer l'intégrité. Elle ne fera pas appel à un algorithme de hachage permettant d'obtenir un condensât du texte, parade sécuritaire habituelle pour vérifier l'intégrité d'un texte signé arrivé à destination. La définition générale est susceptible de s'appliquer à de nombreux types de signatures technologiques : mesures biométriques, signatures graphiques, voire certificats seuls et signatures numériques. Les mesures biométriques semblent évidement visées par cette définition. Les mesures telles que le fond de l'œil, l'empreinte digitale ou le code génétique, permettent bien d'identifier un individu avec une faible marge d'erreur. Mais elles s'intéressent à un individu et non à un message électronique. On comprend qu'il soit impossible d'appliquer une garantie d'intégrité. Les signatures graphiques sont basées sur la reproduction du tracé de la signature manuscrite.
Aujourd'hui, les plus performantes ne s'arrêtent pas au seul dessin et prennent également en compte la vitesse, les accélérations et la pression exercée par la main qui signe. Ces signatures s'attachent réellement à la signature et à l'être humain qui la trace, mais pas au document signé. En général, elles ne contrôlent pas l'intégrité.

Dans le processus de signature électronique, l'authentification repose sur la clé publique de l'émetteur de message certifiée par le certificateur. Dans ce cas, en considérant le certificat seul, celui-ci ne répond-il pas aux termes de la définition de la Directive ? Il semble que oui. Une semblable interprétation est mise en avant par certains produits et services du marché qui affirment travailler avec une signature électronique (ou numérique), alors que seul le certificat est visible[14].

312 La Signature Electronique Avancée de la Directive

La Directive envisage dans ses définitions une seconde variété de signature, la *Signature Electronique Avancée* . Le texte définit ainsi cette nouvelle variété : "*une signature électronique[15] 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 garder sous son contrôle exclusif
et d) être liée aux données auxquelles elle se rapporte de telle sorte que toute modification ultérieure des données soit détectable ;

Par opposition avec la Signature Electronique ordinaire, cette définition mentionne un être humain, le signataire. Comme cette signature identifie le signataire (point c), elle peut constituer une véritable signature sous forme électronique pour les juristes. Et le point d demande la mise en place d'une garantie d'intégrité. Les a, b et c peuvent être commentés sous différents points de vue juridique :

- Liée uniquement au signataire, la *Signature Electronique Avancée* lui est personnelle.
- Comme la *Signature Electronique Avancée* est propre au signataire, elle permettra de l'identifier[16] par le biais de la clé publique certifiée par le PSC.
- Les moyens de signature devront être mis en œuvre par le signataire, ce qui rappelle que la signature juridique est un acte volontaire.
- La délégation de signature n'est pas possible[17]. La clé privée doit rester confidentielle et sous le contrôle du signataire.

La signature électronique avancée est un ensemble technique complexe. Basée sur la signature des techniciens, elle comprend les composants techniques habituels de la signature électronique avec Infrastructure à clés

[14] Face à un doute de ce genre, il faut rechercher s'il existe vraiment dans cette offre de service le module de signature à proprement parler que le droit nomme "dispositif de création de signature".
[15] C'est une définition cumulative : une signature électronique, comme la précédente (signature électronique ordinaire) mais avec des exigences supplémentaires.
[16] Au point de vue technique (de la signature électronique), l'identification est la pratique par laquelle une entité fait part de son nom ou d'une appellation, l'authentification est la manière le moyen par lequel l'entité confirme son identification. En droit, l'identification d'une personne suppose qu'on établisse avec des moyens (de preuve) suffisants son identité. Aussi peut-on en assimiler l'authentification de la technique avec l'identification du droit.
[17] En matière de délégation de signature, c'est l'acte de signer qui est délégué et non pas la signature elle-même : le délégué appose sa propre marque ; il n'imite pas le tracé du délégataire.

publiques (ICP)[18] vus sous un angle et une appellation juridiques : dispositif de création de signature électronique (logiciel de signature), dispositif de vérification (logiciel de vérification de signature), certificat, données afférentes à la création (clé privée) et à la vérification de signature (clé publique), prestataire de services de certification (autorité de certification).

3.2 Les outils logiciels de signature

321 Le Dispositif de Création de Signature

Pour désigner l'outil logiciel qui sert à générer la signature électronique, la Directive emploie la périphrase *dispositif de création de signature (DCS)* qu'elle définit dans son article 2.5° : "*un dispositif logiciel ou matériel configuré pour mettre en application les données afférentes à la création de signature*" c'est-à-dire la clé privée.

Caractéristiques techniques

Pour donner au DCS une dimension pleinement juridique (signature avancée), le DCS doit devenir un *Dispositif sécurisé de création de signature*. Ce DCS renforcé est également configuré pour mettre en œuvre la clé privée, mais la Directive lui impose des sujétions techniques particulières énoncées dans l'annexe III. Les sujétions sont les suivantes :

Annexe III – Exigences pour les dispositifs sécurisés de création de signature électronique

1. *Les dispositifs sécurisés de création de signature doivent au moins garantir, par les moyens techniques et procédures appropriés, que :*

a) les données utilisées pour la création de la signature ne puissent, pratiquement, se rencontrer qu'une seule fois et que leur confidentialité soit raisonnablement assurée ;

b) l'on puisse avoir l'assurance suffisante que les données utilisées pour la création de la signature ne puissent être trouvées par déduction et que la signature soit protégée contre toute falsification par les moyens techniques actuellement disponibles ;

c) les données utilisées pour la création de la signature puissent être protégées de manière fiable par le signataire légitime contre leur utilisation par d'autres.

2. *Les dispositifs sécurisés de création de signature ne doivent pas modifier les données à signer ni empêcher que ces données soient soumises au signataire avant le processus de signature*

On voit que les sujétions du premier alinéa visent à insister et garantir que la clé privée est aussi proche que possible du signataire. Elle est placée sous son contrôle direct ; son utilisation par des personnes non-autorisées doit être impossible. On se rappelle que le bi-clé, et en particulier la clé privée, est le composant technique sur lequel est basée l'identification du signataire réclamé par le droit. Le DCS doit être conforme à l'état de l'art au niveau technologique : la clé privée ne doit pas pouvoir être tirée deux fois pour et par un produit disponible sur le marché. L'algorithme de tirage des clés doit être tel qu'il soit impossible de calculer la clé privée à partir d'une clé publique facilement disponible.

Le deuxième alinéa n'est pas si anodin qu'il y paraît. D'une part, il crée un principe qui pourrait devenir célèbre auprès des praticiens : *What you sign is what you see*, c'est ce que vous voyez que vous signez ! D'autre part, la signature ne doit pas mettre à mal l'intégrité du message. Elle est elle-même une donnée qui vient s'attacher à d'autres données (celles qui sont signées) ; elle doit être présentée d'une façon non ambiguë comme signature électronique

La validation du DCS par la procédure d'évaluation-certification

Comment être sûr que le dispositif de création de signature est bien ce qu'il doit être et qu'il est conforme à ce que le droit en attend ? L'assurance sera apportée par la procédure d'*évaluation - certification*. Pour satisfaire au besoin général de sécurité rencontré par le commerce électronique et l'utilisation d'Internet, la commission européenne a publié dès 1991 les critères d'évaluation ITSEC (Information Technologies Security Evaluation Criteria). Ces critères sont largement utilisés en Europe pour évaluer les produits qui mettent en avant les

[18] Sur la notion d'Infrastructure à Clé Publique (ICP ou PKI en anglais), voir par exemple "*Sécuriser ses échanges électronique avec une PKI*" Th. Autret et M.-L. Oble-Laffaire, chez Eyrolles, janvier 2002 ou notre ouvrage, "*Echanges Electroniques - Certification et sécurité*", aux éditions Droit@Litec, mars 2000.

mécanismes de sécurité matériels et logiciels. La France, comme l'Allemagne et le Royaume-Uni, disposent d'une structure nationale dite "*schéma d'évaluation et de certification*" pour la délivrance de certificats, véritables labels officiels qui attestent de la réussite d'une évaluation. Les certificats émis en France sont reconnus par les partenaires allemands et britanniques avec lesquels des accords de reconnaissance mutuelle ont été négociés. L'évaluation, effectuée par une tierce partie indépendante, couvre aussi bien à la qualité du développement que l'efficacité des mesures de sécurité. Réalisée par des experts selon des méthodes éprouvées, elle est confirmée par un certificat officiel.

Ce système d'évaluation-certification ne sera peut-être pas l'unique procédé pour contrôler la conformité des dispositifs de création de signature. La réglementation, applicable en cas de litige par le juge, ne doit pas empêcher d'autres organisations, françaises, européennes ou internationales, de procéder à un contrôle de conformité, sans que ce contrôle soit nécessairement validé par une certification provenant de l'Etat. Quel que soit le systèmes choisi, il devra cependant prendre en compte les règles établies par la Commission sur cette question spécifique[19].

322 Le Dispositif de Vérification de Signature

L'annexe IV formule quelques "recommandations" portant sur la moulinette qui va opérer la vérification. Le "*dispositif de vérification de signature"* (DVS) est défini comme "*un dispositif logiciel ou matériel configuré pour mettre en application les données afférentes à la vérification de signature"* (c'est-à-dire la clé publique). Voici les recommandations de la directive :

Annexe IV Recommandations pour la vérification sécurisée de la signature
Durant le processus de vérification de la signature, il convient de veiller, avec une marge de sécurité suffisante, à ce que :

a) les données utilisées pour vérifier la signature correspondent aux données affichées à l'intention du vérificateur ;
b) la signature soit vérifiée de manière sûre et que le résultat de cette vérification soit correctement affiché ;
c) le vérificateur puisse, si nécessaire, déterminer de manière sûre le contenu des données signées ;
d) l'authenticité et la validité du certificat requis lors de la vérification de la signature soient vérifiées de manière sûre ;
e) le résultat de la vérification ainsi que l'identité du signataire soient correctement affichés ;
f) l'utilisation d'un pseudonyme soit clairement indiquée et
g) tout changement ayant une influence sur la sécurité puisse être détecté.

3.3 La prestation de certification électronique

331 L'ICP, cette inconnue

Les juristes américains de l'American Bar Association aux Etats-Unis se sont les premiers saisis de la Signature Electronique; L'ABA a publié en 1995 les *Signature Guidelines* accompagnés de l'*US Model Digital Signature Law*. Cette Loi modèle ensuite portée à la CNUDCI (Commission des Nations Unies pour le Droit Commercial International est devenue une des bases pour la préparation de sa *Loi-Modèle pour le Commerce Electronique*. La CNUDCI a continué ses travaux sur ce thème dans une *Loi-type sur la signature électronique*[20]. Il est remarquable que tous ces éléments et travaux concourent à la satisfaction des mêmes besoins, bien qu'il manque un modèle général permettant de les intégrer, aussi bien au plus haut niveau qu'à celui des utilisateurs de base.

[19] Il est paru une *Décision de la commission du 6 novembre 2000 relative aux critères minimaux devant être pris en compte par les Etats membres lors de la désignation des organismes visés à l'article 3, paragraphe 4. de la directive 1999193/CE du Parlement européen et du Conseil sur un cadre communautaire pour les signatures électroniques*. Cette décision a pour but d'énoncer les critères auxquels les Etats membres doivent se référer pour désigner les organismes nationaux chargés d'évaluer la conformité des dispositifs sécurisés de création de signature.

[20] Rapport de la Commission des Nations Unies sur le droit commercial international sur les travaux de sa trente-quatrième session, tenue à Vienne du 25 juin au 13 juillet 2001, adopté le 5 juillet 2001. Disponible au service des publications de la CNUDCI ou sur son site Web : www.uncitral.org .

Des réflexions ont été menées sur cette question en plusieurs endroits du monde et un modèle de management pratique a été défini s'appliquant tant aux travaux des groupes nationaux ou internationaux qu'aux PSCs : l'Infrastructure à clé publique ou ICP (Public Key Infrastructure ou PKI, en anglais). La réponse aux besoins exprimés par les utilisateurs est de créer une structure spéciale apte à inclure tous les certificateurs et autres autorités techniques. L'ICP favorise l'émergence de la signature électronique : sans préjuger des effets juridiques finaux de la signature électronique, cette dernière doit rester conforme aux règles et normes tout au long de l'échange électronique, tant au niveau de l'authentification que de l'intégrité. La cryptographie joue sur ces points un rôle essentiel.

Le document technique fondamental dans le domaine des certificats électronique est la recommandation X.509 de l'Union Internationale des Télécommunications, sans oublier les développements spécifiques de l'IETF sur les ICP dans les protocoles de la famille des *PKIX*. Cette base fondamentale laisse difficilement appréhender le concept d'ICP et son contenu, tous deux faisant l'objet d'évolutions successives. La notion d'infrastructure est pourtant inhérente au dispositif technique décrit par la Recommandation. Dans le schéma le plus simple, un utilisateur final s'authentifie auprès d'un autre utilisateur final en lui fournissant sa clé publique. Mais pour des raisons de confiance et de sécurité, la clé publique est plus sure s'il elle est certifiée au moyen du certificat électronique fourni par un prestataire spécialisé, le PSC. La Recommandation X.509 conseille de s'en remettre à une structure générale hiérarchique des AC[21].

Une ICP est un système de gestion de clés de chiffrement et de délivrance de certificats qui permet les transactions commerciales et financières en toute sécurité. Une ICP offre des services de protection de la vie privée, contrôle d'accès, d'intégrité, d'authentification et de non-répudiation pour les applications informatiques et les transactions de commerce électronique. Pour tenter de synthétiser le tout, une ICP est un ensemble cohérent de matériel, logiciel, base de données, réseaux, procédures de sécurité et d'exigences légales. Les ICP sont aujourd'hui dessinées et réalisées dans ce cadre de la signature électronique. La dimension technique a été déclinée et traduite en solution pour l'utilisateur final. Avec les aspects juridiques auxquels font appel la signature électronique, on s'éloigne encore un peu de la sphère technique. Aussi les ICP sont plus strictes dans leur fonctionnement technique ainsi que dans les exigences qui pèsent sur les prestataires, les PSC.

Même si certains des éléments d'une ICP sont présents dans la proposition de Directive sur la signature électronique, la notion d'ICP n'est pas imposée, ni même suggérée. Ce qu'on peut trouver étrange ou regrettable compte tenu des aspects juridiques particulièrement significatifs de cette Directive. La Commission ne renvoie pas au standard X.509 v.3. mais préfère un système technique plus vague comportant tout de même des certificats, mais sans faire référence à la cryptographie à clé publique. La proposition ne considère pas la collectivité des prestataires réunis dans l'Infrastructure à clé publique.

332 Le certificat électronique qualifié

La Directive européenne prévoit l'utilisation d'un certificat en support de la signature électronique qu'elle définit de la façon suivante (article 2) : *une attestation électronique qui lie des données afférentes à la vérification de signature à une personne et confirme l'identité de cette personne*. Tel quel le concept cité par la Directive rencontre le certificat technique dont le modèle est décrit par la norme internationale nommée *Recommandation X.509 v.3* de l'Union Internationale des Télécommunications. Cette norme a été reprise et développée par l'organisation de normalisation du monde Internet, l'Internet Engineering Task Force (IETF) qui l'a déclinée certificats pour l'appliquer à la technologie de signature numérique (sécurité des échanges électroniques) et a développé le concept d'*Infrastructure à clés publiques*. Le certificat électronique possède un véritable *cycle de vie* qui comprend des étapes successives de demande de certificat, émission de certificat, suspension ou révocation de certificat. Toutes ces étapes demandent à être précisées pour des processus de certification un peu complexes.

La qualification du certificat

[21] La recommandation X.509 a été mise en pratique pour la première fois par le département américain de la Défense (DOD) : une infrastructure à clé publique hiérarchique de type "top-down" fut créée pour assurer la sécurité dans les messageries électroniques militaires. Dès 1993, la communauté Internet a développé le concept d'infrastructure dans le monde TCP-IP avec P.E.M. (Privacy Enhanced Mail). Au fur et à mesure du développement du concept, l'infrastructure a acquis une nature de moins en moins technique. Déjà la multiplication des TC posait aux utilisateurs un problème non technique, celui de la confiance à leur accorder. La notion de confiance devant à son tour entraîner une réflexion de nature juridique.

Toutefois il ne suffit pas d'employer un certificat électronique de type X.509 pour répondre à la finalité juridique de la Directive. La *signature électronique avancée* réclame sur un *certificat* dit *qualifié*, "*un certificat qui satisfait aux exigences visées à l'annexe I et qui est fourni par un prestataire de service de certification satisfaisant aux exigences visées à l'annexe II*" (selon la définition donnée par la Directive). L'annexe I fixe une liste de spécification techniques qui viennent limiter les choix possibles en matière de contenu du certificat électroniques. Ce sont les suivantes :

ANNEXE I Exigences concernant les certificats qualifiés

Tout certificat qualifié doit comporter :
- *une mention indiquant que le certificat est délivré à titre de certificat qualifié ;*
- *l'identification du prestataire de service de certification ainsi que le pays dans lequel il est établi ;*
- *le nom du signataire ou un pseudonyme qui est identifié comme tel ;*
- *la possibilité d'inclure, le cas échéant, une qualité spécifique du signataire, en fonction de l'usage auquel le certificat est destiné ;*
- *des données afférentes à la vérification de signature qui correspondent aux données pour la création de signature sous le contrôle du signataire ;*
- *l'indication du début et de la fin de la période de validité du certificat ;*
- *le code d'identité du certificat ;*
- *la signature électronique avancée du prestataire de service de certification qui délivre le certificat ;*
- *les limites à l'utilisation du certificat, le cas échéant et,*
- *les limites à la valeur des transactions pour lesquelles le certificat peut être utilisé, le cas échéant.*

On retrouvera naturellement dans le contenu obligatoire du certificat la clé publique du signataire (e) ainsi que le nom (b) et la signature électronique (h) du certificateur, répondant au nom de "*prestataire de service de certification*". On peut ajouter en cas de besoin une qualité spécifique du signataire (d). Les titulaires des certificats sont des personnes physiques qui peuvent, le cas échéant, agir pour le compte d'une personne morale. A noter, la possibilité d'employer un pseudonyme pour le signataire. Enfin le certificat dispose d'une certaine durée de vie.

C'est au moment de la transposition de cette disposition dans le droit interne que les Etats membres prévoient l'intervention de systèmes de contrôle rattachés à leurs administrations. Selon l'article *3.3 accès au marché* de la Directive, "*chaque Etat membre veille à instaurer un système adéquat permettant de contrôler des prestataires de services de certifications établies sur son territoire et délivrant des certificats qualifiés au public*". Cette disposition complète ce qui est déjà prévu dans l'article 3.2. de la directive relativement à l'instauration des *régimes volontaires d'accréditation*. Ces systèmes de contrôle permettront aux utilisateurs d'avoir confiance dans les certificats qualifiés du prestataire de certification qu'ils auront choisis. Cependant les systèmes de contrôle restent facultatifs.

La reconnaissance mutuelle des certificats

Pour autoriser l'interopérabilité, la Commission Européenne encourage la reconnaissance mutuelle des certificats. La Commission dans son document COM503 insiste sur la nécessité d'instaurer une reconnaissance mutuelle en matière de certificat :
"Reconnaissance mutuelle - Dans un cadre réellement international pour le commerce électronique, les certificats alloués par des AC étrangères doivent être reconnus mutuellement dans différents pays, de manière à permettre une vérification rapide et efficace de chaque certificat international. Les structures nationales pourraient être complétées par un mécanisme de coordination au niveau européen. Un tel concept serait cohérent avec la stratégie de négociation communautaire existante en matière de reconnaissance mutuelle, et pourrait encourager le développement de services de certification en Europe. Des accords avec des pays tiers seront à la fois plus faciles à conclure et économiquement plus avantageux s'ils sont basés sur un régime commun au niveau communautaire".

Et plus loin, dans les orientations de travail, la Commission fixe des objectifs précis pour aboutir à la reconnaissance mutuelle :
Orientations : ... (iv) Compte tenu de la nature universelle de la communication et du commerce électroniques, des accords internationaux pourraient s'avérer nécessaires entre la Communauté et d'autres pays, une fois qu'un système harmonisé aura été mis en place. Le but doit être de lever les obstacles existants de manière à créer un cadre international compatible pour le commerce électronique, en particulier pour l'établissement de normes techniques communes et pour la reconnaissance mutuelle des certificats.

333 Le Prestataire des Services de Certification

Le certificat électronique qualifié indispensable pour la vérification de la signature électronique avancée est émis par un *prestataire de services de certification* (PSC) qui est constitué, selon la définition de la Directive, par "*toute entité ou personne physique ou morale qui délivre des certificats ou fournit d'autres services liés aux signatures électroniques*". Dans une logique identique à celle du certificat, le PSC doit donner des gages de la qualité de sa prestation, en particulier en respectant les exigences techniques listées dans l'annexe II.

Au titre des exigences les plus importantes, le PSC doit :
- employer du personnel ayant l'expérience et les qualifications nécessaires disposer des ressources financières suffisantes pour endosser la responsabilité de dommages, en contractant, par exemple, une assurance appropriée ;
- informer les personnes des modalités et conditions d'utilisation des certificats, de l'existence d'un régime volontaire d'accréditation et des procédures de réclamation et de règlement des litiges
- vérifier par des moyens appropriés et conformes au droit national, l'identité et le cas échéant, les qualités spécifiques de la personne à laquelle un certificat qualifié est délivré ;
- prendre des mesures contre la contrefaçon des certificats ; veiller à ce que la date et l'heure d'émission et de révocation d'un certificat puissent être déterminées avec précision ;
- enregistrer toutes les informations pertinentes concernant un certificat qualifié pendant le délai utile, en particulier pour pouvoir fournir une preuve de la certification en justice ;
- assurer le fonctionnement d'un service d'annuaire rapide et sûr et d'un service de révocation sûr et immédiat ;
- utiliser des systèmes fiables pour stocker les certificats sous une forme vérifiable.
- ne pas stocker ni copier les clés privées s'il les tire ;

Pour sécuriser les utilisateurs, les PSC pourront suivre un processus d'*accréditation*. La Directive renvoie aux Etats-membres pour la définition d'une politique nationale d'accréditation. Pour des motifs autant inspirés par le respect de la concurrence que par la crainte de l'obsolescence rapide des technologies, la Directive ouvre le cadre de l'accréditation. Des systèmes d'accréditation seront créés ; ils seront volontaires pour les Prestataires de Services de Certification. L'accréditation est une procédure créée par l'ISO, une 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 dans la perspective de l'ISO 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 dans la plupart des pays développés par un organisme spécialisé. Il n'y a qu'un organisme d'accréditation par pays intervenant dans ce domaine. 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 certificats 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. Chaque organisme national est membre d'E.A. (European Co-operation for Accreditation) et signataire du M.L.A (Accord multilatéral Européen d'Accréditation) pour les essais, les étalonnages et la certification. L'accréditation est la reconnaissance de la compétence, processus qui se poursuit par une certification qui est la reconnaissance de la conformité par rapport à un référentiel.

3.4 La normalisation en soutien du montage juridique

La position de l'Union Européenne en matière de normalisation pour ce qui concerne la signature électronique est exprimée dans sa Communication COM503 :

> *"La Commission encourage l'industrie et les organisations internationales de normalisation à développer des normes techniques et d'infrastructure pour les signatures numériques et le chiffrement, afin d'assurer un usage sûr et en confiance des réseaux, et de respecter les obligations en matière de protection de la vie privée et des données. La Commission va réfléchir à des mandats spécifiques ou des obligations en matière de normalisation, et proposer, en étroite collaboration avec les Etats membres, l'industrie et la communauté des usagers (entreprises, consommateurs, citoyens), des mesures permettant de soutenir les travaux dans ce domaine."*

La Commission ne se reconnaît pas un pouvoir d'action directe en la matière. Classiquement pour tout ce qui concerne les normes techniques, elle renvoie aux organisations spécialisées, UIT (Union Internationale des Télécommunications) ou ISO (Organisation Internationale de Normalisation) au niveau international ou le CEN-CENELEC (Centre Européen de Normalisation) ou l'ETSI (organisme européen de normalisation des télécommunications) au niveau européen. Elle peut par contre soutenir les projets techniques directement initiés par l'industrie européenne. Suite à la parution de la Directive, les industries européennes et les organismes de normalisation ont lancé une *Initiative de Standardisation Européenne de la signature électronique* (EESSI)[22] avec l'objectif d'analyser d'une façon cohérente les besoins futurs des activités de normalisation pour le soutien de la Directive Européenne sur les signatures électroniques, particulièrement dans un environnement d'affaires.

Une équipe d'experts nommée par EESSI a produit un premier rapport dès juillet 1999. Ce rapport a été préparé avec l'intention de proposer des normes sur la base d'un cadre ouvert de mise en œuvre des signatures électroniques face aux exigences d'utilisateurs en conformité avec la Directive proposée. Mettant en œuvre les recommandations des experts, les normalisateurs se sont penchés sur les normes internationales adoptées et/ou développées par l'industrie pour autant que possible écarter le besoin de règles nationales détaillées. Un profil technique, décrivant un premier ensemble de technologies et de mécanismes spécifiques à employer pour des signatures électroniques qualifiées a été défini, basé sur la cryptographique asymétrique et sur des certificats dont la vérification serait effectuée par des dispositifs fiables d'équipement comme des cartes à puce. Pour les fournisseurs de service de certification, les standards relatifs à la sécurité conseillés par l'EESSI sont les suivants :

- Pour les codes de bonnes pratiques relatifs à la gestion générale de la sécurité, voir la recommandation européenne BS 7799 parties 1 et 2.
- Pour la spécification des exigences de sécurité pour des systèmes fiables employées par les prestataires : des modules cryptographiques FIPS 140-1 ou équivalents ou un profil convenable de protection basé sur les Critères Communs (ISO 15408).
- En matière de Politique de Certification (PC) pour les fournisseurs de service émettant des certificats qualifiés, l'utilisations du RFC 2527 de l'IETF PKIX

Dans le domaine de l'interopérabilité, les normes suivantes sont requises :

- Une norme technique pour la syntaxe et l'encodage des signatures électroniques, supportant signataires multiples et signatures de rôle, et qui soient vérifiables longtemps après leur emploi initial. L'EESSI recommande que cela soit basé sur un profil et les extensions à la norme CMS (pour remplacer le RFC 2315).
- Des profils pour protocoles opérationnels de gestion de PKI basés sur les RFC.
- Un profil pour des certificats qualifiés basé sur X.509.

Les travaux de normalisation ont trouvé leur aboutissement par des documents normatifs à haute valeur ajoutée dont les principaux sont listés en annexe 2 de ce texte.

[22] cf. le site http://www.ict.etsi.fr/eessi/EESSI-homepage.htm

Annexe I- documents et travaux normatifs

1 Le CEN-CENELEC

Outre les travaux sur les certificateurs et les certificateurs, le CEN-CENELEC encourage l'emploi de la carte à puce cryptographique pour le stockage des certificats comme pour le tirage du bi-clé (voir le site spécialisé http://www.cenorm.be/isss/CWAs/cwalist.htm). La section Signature Electronique contient les documents suivants :

- CWA14365, Guide on the use of Electronic Signatures
- CWA 14355, Guidelines for the implementation of Secure Signature-Creation Devices
- CWA 14172, CWA14172-1 EESSI Conformity Assessment Guidance - Part:1: General
- CWA14172-2, EESSI Conformity Assessment Guidance - Part 2: Certification Authority services and processes
- CWA 14172-3, EESSI Conformity Assessment Guidance - Part 3: Trustworthy systems managing certificates for electronic signatures
- CWA 14172-4, EESSI Conformity Assessment Guidance - Part 4: Signature Creation Applications and Procedures for Electronic Signature Verification
- CWA 14172-5, EESSI Conformity Assessment Guidance - Part 5: Secure signature creation devices
- CWA 14171, Procedures for Electronic Signature Verification
- CWA 14170, Security Requirements for Signature Creation Systems
- CWA 14169, Secure Signature-Creation Devices, version 'EAL 4+'
- CWA 14168, Secure Signature-Creation Devices, version 'EAL 4'
- CWA 14167, CWA 14167-1, Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements
- CWA14167-2, Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 2 Cryptographic Module for CSP Signing Operations - Protection Profile (MCSO-PP)

2 L'ETSI

L'ETSI approfondit divers sujets complémentaires à la signature (spécifications des certificats, horodatage, notarisation), notamment :

- Policy requirements for time-stamping authorities TR 102 023 (January 2003)
- Electronic Signature formats version TS 101 733 v 1.4.0 (September 2002)
- XML format for signature policies - TR 102 038 (April 2002)
- Policy requirements for time-stamping authorities - TS 102 023 (April 2002)
- Policy requirements for certification authorities issuing public key certificates - TS 102 042 (April 2002)
- Policy requirements for certification authorities issuing qualified certificates - TS 101 456 v 1.2.1 (April 2002)
- Provision of harmonized Trust Service Provider status information - TR 102 030 (April 2002)
- FAQ (March 2002)
- International Harmonization of Policy Requirements for CAs issuing Certificates - TR 102 040 (March 2002)
- Signature Policies Report - TR 102 041 (February 2002)
- XML Advanced Electronic Signatures (XAdES) - TS 101 903 (February 2002)
- Electronic Signature Formats - TS 101 733 v 1.3.1 (February 2002)

Annexe II- Législation europenne comparee (Synthese)

Avertissement : on prendra garde au fait que l'actualité juridique en matière de signature électronique est en évolution constante dans les pays membres de l'Union Européenne. Le panorama ci-dessous, déjà remis à jour par nos soins, est tiré d'une étude réalisée par le Sénat[23] français au moment de l'adoption de la loi française sur la signature électronique (1er semestre 2000). Toute recherche sur le droit positif d'un pays de l'Union en la matière ne peut se suffire de ce texte qui devra être actualisé, par exemple au moyens des informations disponibles sur le Web[24].

1 Ressemblances et différences sur les formes de signature et leurs effets en Allemagne et en Italie

Les textes allemand et italien[25] ne reconnaissent que certaines formes de signature électronique et leur accordent des effets différents :

- *La loi allemande et le décret italien ne traitent que de la signature électronique fondée sur un système de chiffrement asymétrique*. Le domaine d'application des deux textes est limité aux signatures numériques, c'est-à-dire aux signatures électroniques créées à l'aide d'un procédé de chiffrement asymétrique. Aucun de ces textes n'évoque les autres signatures électroniques, dont la valeur est donc laissée à l'appréciation du juge.
- *Les deux textes n'accordent pas les mêmes effets juridiques à la signature numérique*. Le décret italien confère à la signature numérique les mêmes effets juridiques qu'à la signature manuscrite et prévoit qu'elle puisse remplacer n'importe quel signe, sceau, cachet, poinçon... Il prévoit même que, à l'image de la signature manuscrite, elle puisse être authentifiée par un officier ministériel. En revanche, la loi allemande ne contient aucune disposition explicite sur la recevabilité en justice et sur la valeur probante de la signature numérique. Elle ne remet pas non plus en cause la liberté qu'a le juge d'apprécier les éléments de preuve qui lui sont soumis. Elle définit seulement les conditions dans lesquelles le destinataire peut être sûr de l'identité de l'émetteur et de l'intégrité des données transmises. Il paraît donc probable que, sauf dans les cas où une signature manuscrite est expressément exigée, le juge admettra la valeur probante des signatures numériques.

2 Ressemblances et différences sur les effets dans les autres pays

Les lois espagnole et luxembourgeoise, ainsi que les textes anglais, belge et danois, visent toutes les formes de signature électronique, mais divergent dans les effets qu'ils leur reconnaissent :

- *Les cinq pays s'appliquent à toutes les formes de signature électronique, indépendamment de la technologie retenue...* Reprenant plus ou moins fidèlement la formulation de la directive, les cinq textes définissent la signature électronique comme une donnée électronique qui sert de méthode d'authentification. Même s'ils paraissent avoir été rédigés pour s'appliquer aux signatures électroniques créées grâce à un procédé de chiffrement asymétrique, ils n'excluent *a priori* aucune autre forme de signature électronique et respectent donc le principe de neutralité technologique qui sous-tend la directive. Malgré ce principe, certains textes ne sont pas destinés à s'appliquer à toutes les signatures électroniques. En effet, la loi belge ne traite que de la signature électronique "avancée", c'est-à-dire la signature électronique produite grâce à un dispositif qui est lié de manière unique et certaine au signataire et qu'il peut garder sous son contrôle exclusif. Il en va de même du texte danois, qui, sans se référer explicitement à la signature électronique "avancée", ne s'applique qu'aux signatures électroniques les plus fiables. Par ailleurs, à l'image de la directive, les lois espagnole et luxembourgeoise établissent une distinction en fonction du degré de fiabilité des signatures électroniques : ils opposent en effet la signature électronique et la signature électronique "avancée". En droit français, le

[23] Un des deux chambres du Parlement français (avec l'Assemblée Nationale).

[24] Par exemple, The Digital Signature Law Survey http://rechten.uvt.nl/simone/ds-lawsu.htm

[25] Ces deux pays étaient en effet précurseurs en matières de signature électronique. En Allemagne, la reconnaissance de la signature électronique a été approuvée par le parlement le 13 juin 1997 dans un article 3 de la loi multimédia, entrée en application le 1er août 1997. En Italie, une Loi n°59 du 15 mars 1997 sur la simplification de l'administration publique a disposé dans son article 15 que l'usage de procédés électroniques était légalement valide. Puis un Décret Présidentiel n°513 du 10 novembre 1997 élaboré comme texte d'application a établi la reconnaissance légale des documents électroniques, des signatures électroniques, des contrats électroniques et des paiements électroniques.

Code civil a adopté la signature électronique à côté de la traditionnelle signature manuscrite. Un décret d'application prévoit l'existence d'une signature électronique "sécurisée" qui se rapproche des caractéristiques de la signature "avancée" de la Directive. Ce décret prévoit également une autre "signature électronique", sans autre qualification, qui peut comme la "sécurisée" servir de moyen de preuve du Code civil et se différencie de la "signature électronique" de la Directive.

- *... sans leur reconnaître la même valeur juridique*[26]. Comme la directive, les textes belge, espagnol et luxembourgeois considèrent comme équivalentes aux signatures manuscrites les signatures électroniques créées dans des conditions de sécurité optimales, c'est-à-dire les signatures électroniques "avancées" qui, de plus, sont associées à un certificat particulièrement fiable et sont créées par un dispositif sécurisé. En revanche, ils ne reconnaissent aucun effet juridique particulier aux autres signatures électroniques. Cependant, les projets espagnol et luxembourgeois précisent explicitement, tout comme la directive, qu'elles seront recevables en justice. Les textes anglais et danois ne comportent pas la notion de signature électronique "avancée". Le premier prévoit, de façon générale, la recevabilité des signatures électroniques, quelles qu'elles soient, mais laisse au juge le soin d'apprécier leur valeur probante, tandis que le second détermine seulement les conditions dans lesquelles les signatures électroniques peuvent être considérées comme sûres, sans remettre en cause la totale liberté du juge pour évaluer leur recevabilité et leur valeur probante. La loi française sur la signature électronique ne prévoit qu'une "présomption" de preuve à condition, toutefois, que la signature électronique soit "sécurisée", le certificat "qualifié" et le dispositif de création de signature "sécurisé". A défaut d'un de ces éléments, le signataire pourrait avoir à prouver qu'il a mis en œuvre un dispositif technique fiable. La loi française n'est pas complète puisqu'elle vise la signature électronique uniquement comme un moyen de preuve. A l'occasion de la transposition de la Directive européenne 2000/31/CE du 8 juin 2000 sur le Commerce Electronique, la signature sera reconnue comme un élément fondamental de la dématérialisation des actes juridiques : tout acte obligatoirement créé sur papier pourra être dématérialisé à condition d'être validé par une signature électronique.

[26] Outre ces divergences importantes dans son régime même, il faut souligner que les conditions de validité de la signature électronique, notamment celles qui se rapportent aux tiers de certification, sont assez différentes d'un pays à l'autre. La loi allemande et le décret italien ne contiennent aucune disposition sur leur responsabilité et le texte anglais est particulièrement libéral. La loi française instaurera un régime de responsabilité des certificateurs (celui de la Directive Signature) à l'occasion de la transposition de la Directive Commerce Electronique.