

Introduction à la notion de signature électronique



Par

Guenièvre Bordinat *

gbordinat@yahoo.fr

DESS droit du multimédia et de l'informatique Paris

Mastère spécialisé ESSEC Droit des Affaires Internationales et Management.

Le développement du commerce électronique demande l'existence d'une sécurité pour la transmission de données et les paiements en ligne. Grâce à un système de chiffrement, appliqué à l'abrégé du message transmis, la signature électronique peut être une réponse à ce besoin car elle assure plusieurs fonctions - dont celles de garantir l'authenticité et l'intégrité des données, ainsi que l'identité du signataire. Or l'écrit électronique, conçu comme preuve juridique, s'appuie avant tout sur la signature électronique dans le domaine du multimédia.

Bien sur, pour que la signature électronique soit réellement une garantie, il faut que tout son environnement contractuel, tant au niveau utilisateur que prestataire, soit sécurisé. De même, un bon contrat, la caution de l'Etat ainsi que l'existence de groupements de professionnels, sont des gages de confiance dans la certification externe de l'entreprise. Cependant, comme le précise Isabelle Renard "les implications juridiques de ces montages sont nombreuses et complexes, tant à raison de la nouveauté de l'environnement légal que des schémas contractuels mis en oeuvre." D'où l'importance d'apporter un cadre législatif et réglementaire à la signature électronique.

Le système légal en France est avant tout décrit par la loi du 13 mars 2000 qui affirme la valeur juridique de la signature électronique mais sous certaines conditions. Cette loi s'inscrit dans un contexte européen (Directive du 30 novembre 1999) et est complétée par un texte réglementaire (décret du 13 décembre 2001). Il faut aussi évoquer le rôle espéré du projet de loi sur la société de l'information (projet LSI) qui pose le principe de l'équivalence de la signature électronique et manuscrite, même dans le cas où cette dernière est exigée ad validitatem (comme condition de validité de l'acte) ce qui n'est pas le cas actuellement en France contrairement aux souhaits européens (article 9 de la Directive du 8 juin 2000).

1. Un phénomène mondial

La plupart des pays développés sont en train d'adapter leur cadre législatif à la signature électronique.

En Europe, la directive européenne du 13 décembre 1999 définit le cadre dans lequel doivent s'inscrire les lois nationales : l'Italie et l'Allemagne ont déjà modifié leur législation ; la France le fait, tout comme la plupart des autres pays européens (Espagne, Luxembourg, Royaume-Uni, Belgique, Danemark).

Aux Etats-Unis, la situation diffère d'un Etat à l'autre, et plusieurs projets concurrents de lois fédérales sur le cyberparaphe sont en projet.

2. La directive européenne du 13 décembre 1999

La Commission estimait que les réseaux ouverts comme Internet n'étaient pas suffisamment sécurisés pour les affaires et voulait instaurer un environnement sûr en ce qui concerne l'authentification électronique : d'où la directive.

Le but de la directive est d'aboutir à ce qu'en droit interne les Etats membres reconnaissent à la signature électronique la "valeur juridique d'une signature manuscrite". Et plus, les signatures électroniques doivent être "admissibles comme preuves en justice de la même façon que les signatures manuscrites" (art.5.2.).

La Directive européenne du 13 décembre 1999 sur la signature électronique définit la signature électronique par deux notions.

- D'abord une définition générale de signature électronique (article 2-1 de la Directive) : " la signature électronique correspond à une donnée sous forme électronique, qui est jointe ou liée logiquement à d'autres données électroniques et qui sert de méthode d'authentification ".
- Ensuite, (article 2-2) la signature électronique avancée qui est définie comme devant satisfaire aux exigences suivantes : " être liée uniquement au signataire ; permettre d'identifier le signataire ; être créée par des moyens que le signataire puisse garder sous son contrôle exclusif ; être liée aux données auxquelles elle se rapporte de telle sorte que toute modification ultérieure des données soit détectable ". Cette dernière serait plus à proprement parler la signature électronique telle qu'on l'entend : c'est à dire celle qui identifie l'auteur et garantit l'intégrité.

Ces définitions sont plus d'ordre technique que d'ordre fonctionnel. En effet pour définir la signature électronique la Commission a préféré un système technique sans faire de référence directe à la cryptographie asymétrique bien que s'en inspirant fortement (neutralité technologique oblige). Or la directive associe la signature à deux notions : celle de "certificat de signature" et de "prestataire de service de certification".

Selon la directive l'accréditation n'est pas obligatoire et on ne sait pas si elle doit être publique (par l'Etat) ou privée. Ainsi une signature électronique qui serait garantie par un certificat non qualifié émis par un prestataire de certification non accrédité devrait avoir la valeur juridique d'une signature manuscrite ce qui est problématique.

De plus, la directive ne couvre pas les autres aspects du contrat en ligne, liés à la conclusion et à la validité du contrat. C'est donc au droit applicable qu'il faudra se référer.

3. Préliminaires sur le droit français de la preuve

Le principe en droit français est celui du consensualisme mais il s'organise en fait autour de l'écrit : même si le contrat est valablement formé sans écrit du seul fait de l'échange des consentements des parties (principe du consensualisme), la nécessité pour les parties de prouver leur contrat leur impose le recours à un écrit.

L'"écrit" au sens traditionnel est le titre original revêtu d'une signature manuscrite et matérialisé dans un document papier. Un écrit est exigé pour toute convention dont l'objet vaut plus de 800 euros. De plus, quand un écrit a été rédigé, on ne peut apporter la preuve contraire que par un autre écrit.

La signature remplit deux fonctions juridiques essentielles : identification de l'auteur et manifestation de sa volonté, adhésion personnelle du signataire au contenu du document.

Toutes fois, la signature n'était pas définie par la loi, même si le Code civil mentionne à plusieurs reprises l'obligation d'une signature : article 1322 sur les actes sous seing privé, article 1325 sur le contrat synallagmatique et la formalité du double original, article 1326 sur la reconnaissance de dette.

Ce principe de la preuve écrite comporte un certain nombre d'exceptions. Par exemple, les conventions de preuve sont valables car les dispositions relatives à la preuve ne sont pas d'ordre public. Il est possible pour les parties de prévoir dans un contrat les questions relatives à la valeur probante des documents numériques.

La doctrine d'abord puis la jurisprudence ont reconnu la validité de telles conventions en matière de paiement par cartes bancaires (affaire Crédicas, 8 novembre 1989, D. 1990, 369).

Cependant, la validité de la preuve électronique restait contestable. De même, la liberté contractuelle n'est pas absolue :

Entre professionnel et consommateurs : la convention sur la preuve ne doit pas constituer une clause dite abusive (Article L 132-1 du Code de la consommation ; Directive 93/13 du 5 avril 1993). Une recommandation de la commission des clauses abusives demande notamment que soient éliminées des contrats proposés par les émetteurs de cartes, les clauses ayant pour objet de conférer aux enregistrements magnétiques des établissements financiers une valeur probante tout en dispensant ces derniers de prouver que l'opération contestée a été correctement enregistrée (Recommandation n° 94-02 relative aux contrats porteurs des cartes de paiement, BOCCRF 30 mai 1995, p. 182).

De plus, le cadre de la convention sur la preuve nécessite que les parties aient une relation préexistante. Or, on assiste à une dématérialisation du processus contractuel, le contrat naît du simple échange de consentements. Face à cela le problème de la preuve du contrat et de l'étendue du consentement reste entier.

En outre, les conventions sur la preuve ne sont pas opposables aux tiers (effet relatif du contrat).

Enfin, certains textes imposent des conditions de forme faisant une référence explicite à l'écrit. Ex : La directive sur les contrats à distance, qui inclut les contrats conclus sur Internet, prévoit la confirmation par écrit, ou sur un autre support durable, de certaines informations relatives au contrat (article 5 de la Directive sur le Commerce Electronique). On peut citer également le formalisme du droit cambiaire (Cass. Com. 26 novembre 1996, JCP E 97, II, 906).

Une réforme du cadre juridique pour l'adapter aux nouvelles technologies apparaissait inéluctable.

4. La modification du code civil par la loi du 13 mars 2000

La loi du 13 mars 2000 est venue modifier le droit français relatif à la preuve, en reconnaissant l'équivalence du support papier et du support numérique dès lors qu'un certain nombre de conditions sont respectées. Dans ce cadre, le Code civil énonce désormais (article 1316-4) : " La signature nécessaire à la perfection d'un acte juridique identifie celui qui l'appose. Elle manifeste le consentement des parties aux obligations qui découlent de cet acte. Quand elle est apposée par un officier public, elle confère l'authenticité à l'acte. Lorsqu'elle est électronique, elle consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache. La fiabilité de ce procédé est présumée, jusqu'à preuve contraire, lorsque la signature électronique est créée, l'identité du signataire assurée et l'intégrité de l'acte garantie, dans des conditions fixées par décret en Conseil d'État".

Le texte se veut indépendant de toute technologie et définit la signature par rapport à ses fonctionnalités (contrairement à la directive). La loi réfute donc désormais toute hiérarchie entre les supports, considérant que l'écrit sous forme électronique doit avoir la même force probante que l'écrit sur support papier.

Cependant, cette règle s'applique sous réserve que soient remplies des conditions de nature à en garantir l'intégrité. Les modalités sont définies par le décret en Conseil d'Etat, et le Code civil. Il y a quatre conditions pour l'équivalence :support électronique / support papier dans le Code :

- 1 - pouvoir identifier la personne dont émane l'écrit électronique au moyen d'un procédé fiable
- 2 - l'écrit électronique a été créé dans des conditions de nature à en garantir l'intégrité
- 3 - l'écrit électronique est conservé dans des conditions de nature à en garantir l'intégrité
- 4 - utiliser un procédé fiable garantissant le lien de la signature électronique avec l'acte auquel elle s'attache.

Si les quatre conditions précédentes sont remplies, selon les modalités du décret du 30 mars 2001, il y a alors présomption de fiabilité du dispositif et présomption simple de validité de la signature électronique. Ceci est une innovation importante de la loi. Cela ne signifie pas qu'une signature qui ne respecte pas les conditions du décret ne soit pas valable. En fait, s'il y a contestation, celui qui se prévaut de la fiabilité ou non de la signature électronique devra en apporter la preuve. C'est ce qui se passe aujourd'hui pour les tiers certificateurs de confiance qui doivent prouver la fiabilité de la signature notamment, puisque les arrêtés n'en sont qu'à l'état de projet en ce qui concerne leur accréditation.

Portée du nouveau dispositif français.

Il va plus loin que la norme européenne puisqu'il vise également les actes authentiques dressés sur un support électronique, qu'ils soient accomplis par des notaires, des officiers de l'état civil, des magistrats, des huissiers, ou encore des commissaires-priseurs. En revanche, la loi du 13 mars 2000 ne concerne pas tous les actes juridiques, ceux pour lesquels l'écrit est requis

à titre de validité, et non pas à titre de simple preuve, étant écartés. Ainsi, seuls les contrats dont l'écrit n'est pas une condition de validité pourront être conclus via l'Internet, ce qui exclut par exemple certains contrats régis par le Code de la consommation, le contrat de démarchage par exemple, ou certains contrats bancaires devant comporter des mentions relatives au taux d'intérêt conventionnel. Ceci devrait être supprimé avec le projet de loi sur la société de l'information.

Désormais si deux modes probatoires ayant la même force coexistent, comment régler les conflits entre eux ?

Si une convention de preuve prévoit la supériorité d'une forme sur l'autre (écrit / électronique), le juge sera tenu de l'appliquer. A défaut, la loi précise qu'un juge devra régler le conflit " en déterminant par tous les moyens le titre le plus vraisemblable, quel qu'en soit le support ". Il est bien entendu difficile de déterminer par avance ce que le juge entend par "vraisemblable".

NB : Signature électronique et contrats

L'article 1316-4 du Code civil, dispose que "la signature nécessaire à la perfection d'un acte juridique identifie celui qui l'appose. Elle manifeste le consentement des parties aux obligations qui découlent de cet acte". L'emploi d'une signature électronique dans le cadre d'une vente en ligne engage donc les signataires, commerçants et internautes, comme le ferait un contrat sous forme papier. Non seulement la signature électronique accompagnant l'acte identifiera celui dont il émane et lui conférera une valeur probatoire équivalente à celle d'un écrit papier, mais elle permettra également de clarifier la valeur juridique des contrats passés en ligne, en encadrant la manifestation du consentement.

Deux limites subsistent cependant : premièrement, la mise en conformité des législations au sein de l'Union européenne va demander un certain délai, et deuxièmement, les divergences législatives entre l'Union européenne et les Etats-Unis restreignent la possibilité pour les internautes d'employer ce système hors des frontières des Etats membres.

5. Qu'apportent les décrets ?

La loi du 13 mars 2000 et ses décrets d'application confèrent un cadre juridique à la signature électronique. En particulier, une signature électronique sera recevable comme preuve en justice, dans les conditions du décret du 30 mars 2001 qui transpose la directive sur la signature électronique. Il distingue ainsi la signature électronique (qui respecte les conditions du Code civil) et la signature électronique "sécurisée" qui est présumée fiable si elle est conforme aux conditions du décret. Le décret du 18 avril 2002 est relatif à l'évaluation et à la certification des produits offerts par les PSCE notamment.

Décret du 30 mars 2001 pris en Conseil d'Etat

La fiabilité d'un procédé de signature électronique sera présumée, jusqu'à preuve du contraire sous les conditions données à l'article 2 du décret du 30 mars 2001 : dès lors qu'une signature électronique sécurisée est mise en oeuvre :

- elle doit être établie grâce à un dispositif sécurisé de création de signature électronique,

- la vérification de cette signature doit reposer sur l'utilisation d'un certificat électronique qualifié.

Le décret du 30 mars 2001 précise les conditions techniques qui doivent être réunies :

> en précisant les notions de.

- signature sécurisée
- dispositif sécurisé de création de signature électronique
- certificat électronique qualifié

> en prévoyant un contrôle des prestataires délivrant des certificats électroniques qualifiés

> en prévoyant un schéma de certification volontaire des prestataires délivrant des certificats électroniques qualifiés.

> La certification leur vaudra présomption de conformité aux exigences du décret.

NB : Ce décret prévoit les conditions de reconnaissance des certificats qualifiés émis par des prestataires étrangers, ouvrant ainsi la voie à la reconnaissance de signatures électroniques " de ", ou " vers ", l'étranger. Cependant, ce dispositif n'est pas encore prêt semble t-il.

De plus, si le texte ne touche pas directement l'administration, celle-ci compte suivre et a même parfois anticipé le mouvement, comme le prouvent les annonces de Bercy quant à la prochaine télédéclaration d'impôts. Il devrait aussi toucher rapidement les actes "authentiques" (contrats de mariage, actes immobiliers...), établie par les notaires, et qui pourront eux aussi se traiter à distance.

Ce décret faisait référence à cinq arrêtés qui se résumeront en fait au décret du 18 avril 2002:

- [arrêté A] arrêté du Premier ministre relatif au schéma d'évaluation des dispositifs de création de signature électronique (mentionné dans l'article 4 du décret) ;
- [arrêté B] arrêté du Premier ministre relatif au référentiel d'évaluation des dispositifs de création de signature électronique (mentionné dans l'article 3 du décret);
- [arrêté C] arrêté du ministre chargé de l'industrie relatif au schéma de qualification des prestataires de services de certification électronique (mentionné dans l'article 7 du décret);
- [arrêté D] arrêté du Premier ministre relatif au référentiel de qualification des prestataires de services de certification électronique (mentionné dans l'article 7 du décret);
- [arrêté E] arrêté du Premier ministre relatif au contrôle des prestataires de services de certification électronique(mentionné dans l'article 9 du décret).

Décret du 18 avril 2002 pris en Conseil des ministres

Le décret du 18 avril est relatif à l'évaluation et à la certification de la sécurité des produits et les systèmes des technologies de l'information. Ce décret supprime les arrêtés prévus dans le décret de mars 2001. Il a, notamment, pour finalité de créer une superstructure administrative qui encadre les technologies de l'information : la DCSSI ou Direction centrale de sécurité des

systèmes d'information (ainsi qu'un comité directeur de certification ou de sécurité des systèmes d'information par un arrêté du Premier ministre qui se fait attendre).

Le système est assez compliqué :

- L'Etat agréé le Cofrac (Comité Français de Certification) qui a été créé par une loi de 1994 dans le cadre du schéma d'accréditation en France (Code de la Consommation). C'est un schéma général de certification qui comprend les systèmes d'information.
- Le COFRAC évalue et accrédite les commanditaires dits CESTI (des cabinets d'audit).
- Ceux-ci certifient les autorités de certification et les dispositifs de signature électronique.

Le problème est que cette évaluation se fait selon un référentiel de critères techniques et organisationnels qui n'est pas unique et homologué (comme le souhaitait le MINEFI) mais qui est présenté par le PSCE lui-même, ce qui laisse présager de sa fiabilité relative. La DCSSI intervient dans tout ce processus.

Les CESTI sont accrédités pour 2 ans et les PSCE sont certifiés pour 1 an.

6. Définition technique de la signature électronique

La signature est un concept qui peut recouvrir deux fonctions : identification du signataire et validation du document (intégrité par rapport à ce que le signataire a signé). La loi donne deux définitions qui, bien qu'ayant le même nom juridique dans la directive, ne recouvrent pas la même réalité.

- La signature électronique et sa valeur juridique.

La loi du 13 mars 2000 précise : toutes les signatures électroniques sont recevables en justice dès lors qu'elles assurent l'identification du signataire et la garantie de l'intégrité de l'acte. Si les conditions nécessaires à la présomption de fiabilité ne sont pas réalisées, alors la fiabilité du procédé devra être démontrée à la charge du signataire.

- La signature électronique "sécurisée" et sa valeur juridique.

Selon l'article 1er - 2, il s'agit d'une signature électronique qui est "propre au signataire", qui est créée par des "moyens que le signataire puisse garder sous son contrôle exclusif" et qui garantit avec l'acte auquel elle s'attache "un lien tel que toute modification ultérieure de l'acte soit détectable". La signature électronique sécurisée est recevable comme preuve en justice mais la fiabilité du procédé devra être démontrée par le signataire ou le prestataire de certification si les conditions nécessaires à la présomption de fiabilité ne sont pas réalisées. La notion de lien tient en fait à la facilité de modifier les données sur Internet, ainsi la solution est de créer un lien unique entre le document et la signature de l'expéditeur qui permettra de l'identifier.

a. Chiffrement, notion d'empreinte et certificat

Une signature électronique fait intervenir les trois éléments: un chiffrement, l'empreinte d'un document et un certificat.

- Le **chiffrement**, est un processus qui applique un algorithme à un message afin d'en coder la signification. L'algorithme utilise une clé de chiffrement qui empêche de décrypter le message.

La force de cette clé dépend de deux facteurs : la nature de l'algorithme (chiffrement symétrique ou asymétrique) et la taille de la clé (la loi française autorise une clé limitée à 128 bits mais le projet de loi LSI va sans doute libéraliser le cryptage et ses applications).

- La signature électronique fait ensuite référence à l'**empreinte** ("hash" en anglais). L'empreinte d'un texte est la forme abrégée de ce texte obtenue à l'aide d'une fonction de hachage. C'est donc une version synthétique et unique du document d'origine. L'intérêt est que les différences entre deux textes sont immédiatement décelées en comparant leurs empreintes ou condensés.

- Enfin, la signature électronique est liée à la notion de **certificat** électronique (ou passeport électronique est un petit fichier de 8 à 10 Ko qui voyage avec tous les envois certifiés et qui est public). Il identifie l'émetteur en fournissant le nom de la personne (physique, morale) associé à une clé publique.

Pour utiliser en confiance la clé publique d'un interlocuteur, il faut qu'elle soit certifiée par une autorité de confiance, appelé "Prestataire de Service de Certification Electronique" (PSCE) par les textes. En effet, contrairement à la signature manuscrite, la signature électronique ne comporte aucun élément permettant de l'attribuer à une personne donnée. C'est pourquoi on recourt à des services de certification qui garantissent l'appartenance d'une signature à une personne.

La signature s'envisage complétée d'un test d'identification liant le signataire à ce code, comme celui que fournissent les PSCE. Parfois, il suffit d'un simple code confidentiel, comme dans le cas des cartes à puce, ou d'une reconnaissance de l'iris ou des empreintes digitales grâce à une machine branchée sur l'ordinateur...etc.

La clé privée si elle est fournie par les PSCE doit être remise, depuis la loi concernant la sécurité quotidienne, au Ministère de l'intérieur, sauf si le PSCE peut prouver qu'il ne l'a jamais eue (comme, par exemple, quand c'est la personne certifiée elle-même qui crée ses clés et n'envoie que la clé publique au PSCE).

Un point est à souligner ici. Le décret parle des '**prestataires de services de certification**' en général, sans distinguer entre leurs différentes fonctions. Néanmoins, en pratique s'opère une distinction entre ces prestataires selon leurs fonctionnalités. Il y a d'une part : l'autorité de certification sur laquelle repose la confiance et qui, en principe, est responsable de l'ensemble de la prestation. D'autre part : l'autorité d'enregistrement vérifie l'identité. L'opérateur de certification qui est le prestataire technique.

Cependant, il n'y a pas de liste officielle et une banque, un greffe, une assurance, peuvent être des PSCE. La principale difficulté qui en découle est qu'un certificateur ne peut pas être utilisé universellement. Ainsi, chaque entreprise ou particulier aura plusieurs certificats ce qui promet une certaine complexité en pratique. Il faut espérer que les arrêtés simplifieront la donne.

b. Cas des clés asymétriques

L'inconvénient principal de cryptologie symétrique réside dans le fait que l'expéditeur et le destinataire doivent convenir à l'avance de la clé et doivent disposer d'un canal sûr pour l'échanger.

C'est pourquoi les systèmes de signature électronique qui se développent depuis quelques années reposent sur des algorithmes de chiffrement asymétriques, où, de plus, chaque utilisateur dispose de deux clés. Le chiffrement asymétrique utilise donc deux clés qui sont liées mathématiquement. La première est la clé "privée", qui n'est jamais révélée, et la seconde est la clé "publique" qui est divulguée à tous les correspondants (elle est contenu dans le certificat ou accessible sur Internet par exemple).

C'est donc le fait que les deux clés (privée et publique) d'une même personne soient liées entre elles, qui va permettre de vérifier l'authenticité de la signature. Un message chiffré à l'aide d'une clé privée, ne peut être déchiffré qu'avec la clé publique correspondante, et inversement. La clé publique doit donc être connue de tous, tandis que la clé privée reste secrète.

c. Sécurité et authentification

La légalité des signatures électroniques va autoriser le développement de tous les échanges électroniques grâce à l'authentification des parties. La signature électronique s'annonce pour certains plus sûre que la signature manuscrite. Elle ne peut être produite que par une unique personne, le détenteur de la clé privée correspondant à la clé publique utilisée pour la vérification si tant est que l'enregistrement a été correctement réalisé (ex: face à face). De plus, si le document numérique a été modifié pendant son transport, la vérification de la signature donnera un résultat négatif.

Cependant, il existe plusieurs moyens de démontrer la faiblesse de cette signature électronique, comme par exemple exhiber la clé privée d'un signataire sans accord, se faire passer pour le signataire sans pour autant disposer de sa clé privée ou exhiber deux messages distincts ayant la même signature.

NB : Pour résumer, il y a une même technique pour deux fonctions différentes.

- Si j'encode avec ma clé privée et que je décode avec ma clé publique, personne d'autre que moi ne peut avoir codé, signé le document. Dans ce cas la fonction de la cryptologie asymétrique est d'identifier ou de signer.
- Si j'encode avec ma clé publique et que je décode avec ma clé privée, la fonction voulue est alors la confidentialité.

d. Les usages de la signature électronique

Les usages professionnels

- TVA : (est obligatoire pour les entreprises réalisant plus de 100 millions de francs de chiffre d'affaire annuel)
- Gestion de l'entreprise et dématérialisation des documents
- Actes médicaux : carte Santé Professionnelle (www.santé.fr et www.gip-cps.fr)
- Achats en ligne
- Actes authentiques
- Transferts financiers, actes de commerce...

Les usages pour les particuliers

Les mails

Les actes notariés

Achat en ligne : carte EMVcarte bancaire

La télédéclaration d'impôts (cf. www.finances.gouv.fr) cf. Télé IR

Le coût final de la signature électronique devrait s'élever à "50 à 250 francs par an pour les particuliers", selon Eric Caprioli, avocat au barreau de Nice et expert aux Nations unies sur le e-commerce.

Conclusion

En somme, la signature est un code numérique qui doit donner des garanties sur l'authentification du signataire et sur l'intégrité de la signature pendant son transport électronique. La signature est apposée automatiquement sur un document électronique par un logiciel ad hoc mais activée par le seul titulaire de la clé privée, sans autre indication des méthodes de chiffrement à utiliser.

Annexes :

1. sur le certificat

a. Les règles minimales de garantie de fiabilité concernant les PSC - cf. article 6 II du décret dont :

- un prestataire doit faire la preuve de la fiabilité des services de certification électronique qu'il fournit.
- un prestataire doit fournir aux personnes qui se fondent sur un certificat électronique au moins certains éléments d'information.
- un prestataire de services de certification engage sa responsabilité sur la validité et les règles de sécurité liées à la mise à disposition d'un certificat électronique sur le réseau, à la fois vis à vis du signataire et vis à vis de la personne qui se fie au certificat.

b. Informations que doit présenter le certificat :

Il doit contenir au minimum : la version du certificat ; un numéro de série ; le nom du porteur et sa clef publique ; l'algorithme utilisé; les dates de validité ; le nom de l'émetteur, l'identification de la politique de certification et la signature de l'émetteur.

c. La responsabilité de quelqu'un qui se fie à un certificat erroné

- Votre responsabilité sera vraisemblablement engagée si vous avez accepté une signature non conforme aux engagements maximaux portés sur le certificat, ou émise après la date de validité du certificat. Idem si le certificat a été révoqué avant la création de signature.
- En revanche, elle ne sera en principe pas engagée si vous prouvez que le PSC n'a pas enregistré une révocation en temps voulu, ou s'il a émis un certificat en se fondant sur des informations insuffisantes (photocopie de pièce d'identité, inscription en ligne, etc).

d. Cycle de vie

Le cycle de vie d'un certificat commence par la création des deux clefs publique et privée. Il se poursuit par la demande de certificat de la part du détenteur des clefs, puis par la validation des justificatifs apportés. Viennent ensuite les étapes d'émission du certificat et de son acceptation. La phase suivante comporte l'utilisation des clefs et du certificat, la validation du

certificat, sa suspension ou sa révocation. Le cycle s'achève à l'expiration des clefs et du certificat et recommence à la phase première.

2. Les technologiques du cyberparaphe (signature électronique).

a) Cryptographie

Il faut un logiciel spécifique, fondé sur la cryptographie. Malgré les réticences des militaires, le gouvernement a dû assouplir le régime de la cryptographie en vigueur. La signature électronique est d'utilisation libre depuis 1996 en ce qui concerne l'identification et l'intégrité et d'utilisation restreinte pour la confidentialité (inférieur ou égal à 128 bits). Le gouvernement a prévu d'en libéraliser encore plus l'usage avec la loi sur la "société de l'information".

Malgré ces techniques de faibles risques subsistent car la clef est sur le disque dur et un intrus pourra profiter de l'absence de l'internaute devant sa machine pour envoyer un message signé à sa place. Un hacker doué pourra s'introduire illégalement dans l'ordinateur via l'Internet et voler la clef. Il pourra aussi enregistrer des données de la clé avec un logiciel espion

b) Le modèle de la carte bancaire.

Afin de protéger la clef, des dispositifs bâtis sur le modèle de la carte bancaire française sont à l'étude: un boîtier branché sur l'ordinateur ou intégré à celui-ci, accueille une carte à puce où se trouve la clef privée et le certificat. Pour signer l'internaute tape un code confidentiel. Comme chez les commerçants. L'intérêt est que la clé privée est sur la carte et pas sur l'ordinateur ou internet.

La frappe d'un code peut être combinée avec des techniques de reconnaissance de l'iris (avec laser dans l'œil) ou des empreintes digitales, ce sont les données biométriques qui entrent ici en jeu.

c) Système garantie par un organisme identifié

Dans le cas des Carte bleue en France aujourd'hui, c'est le GIE Carte bancaire qui sert de caution aux transactions. Les intervenants ont confiance, car la sécurité est garantie par un organisme identifié, habilité à distribuer les lecteurs. C'est ce qui est utilisé avec les PSC sauf que ceux ci sont très nombreux. Une procédure d'agrément définit quelles entreprises ou associations pourront distribuer les technologies utilisées. Dans le cas des particuliers, des entreprises (ex : télé TVA), les banques, la Poste, les assureurs et certaines administrations sont présents comme on l'a vu.

(*) Cet article à fait l'objet d'une première publication le **6 mars 2002** sur le site <http://www.u-paris2.fr/dess-dmi/>

(**) Les opinions exprimées dans cet article sont propres à leur auteur qui ne saurait être responsable du contenu en cas d'erreurs, d'évolution du droit, ni pour tout contenu, futur ou présent figurant sur signelec.com ou y étant référencé de quelque manière que ce soit.