Projet ICare

Le Décret n°2002-535 et la signature électronique

Référence : ICARE/CAB/TPC/DOC_9/v1
Type : Note d'information
Diffusion : Générale

Date : 02/05/2002
Titre : **ICare – Le Décret n°2002-535 et la signature électronique.**

Auteur(s) : Thierry Piette-Coudol, avocat

Résumé :
Le Décret d'application sur la signature électronique vient d'être modifié par un nouveau décret n°2002-535 du 18 avril 2002, dernièrement sorti et qui est *relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information*. Cette note d'information fait le point sur le droit applicable.

1 Préambule

Un an après la parution du Décret d'application (n°2001-272) de l'article 1316-4 du Code Civil[1] sur la signature électronique, nous étions encore dans l'attente de cinq arrêtés d'application annoncés par ledit décret. Mais c'est une norme juridique de même nature que nous apporté la livraison du 19 avril 2002 du Journal Officiel : un *Décret n°2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information*. Ce texte ne modifie pas de façon fondamentale ce que le décret 2001-272 avait annoncé. Toutefois sa parution fournit l'opportunité de faire le point sur les textes fondateurs de la signature électronique.

Le document ICARE/CAB/TPC/DOC_1/v1.0, "Recueil des textes juridiques applicables à la signature électronique", sera révisé en conséquence.

2 Un Décret en remplacement des arrêtés d'application

Le premier Décret 2001-272 liste les exigences techniques et organisationnelles qu'une signature électronique doit respecter pour emporter la présomption de fiabilité de l'article 1316-4. Les exigences (issues de la Directive signature électronique) portent sur les principaux composants de la signature électronique :

- le dispositif de création de signature (le logiciel qui signe) et le dispositif de vérification (le logiciel qui vérifie),
- le certificat électronique qui contient la clé publique du signataire (nécessaire au dispositif de vérification),
- et le prestataire de services de certification électronique (qui certifie la provenance de la clé publique sous sa propre responsabilité).

Sans que cela soit obligation[2], il est possible de se tourner vers des organismes d'audit et de contrôle techniques qui vérifieront la conformité de ces composants aux exigences citées. La signature électronique prend alors le nom de *signature électronique sécurisée*. Les arrêtés d'application devaient indiquer quels étaient les organismes susceptibles d'intervenir et avec quelle méthodologie de contrôle. La FAQ (Foire-Aux-Questions) sur la signature électronique du site de la Direction Centrale de la Sécurité des Systèmes d'Information (DCSSI) auprès du Premier Ministre (http://www.scssi.gouv.fr/fr/faq/faq_sigelec2.html) emploie les lettres de l'alphabet pour identifier les arrêtés. Ce sont les suivants :

- [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).

La préparation des arrêtés a rencontré un obstacle juridique inattendu : les textes relatifs à la déconcentration administrative. Parmi diverses mesures, le Décret n°97-1184 du 19 décembre 1997 relatif à la déconcentration

---

[1] Rappel : " *Art. 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'Etat.* "

[2] L'article 1 du nouveau décret précise que la sécurité offerte par des produits ou des systèmes des technologies de l'information, au regard notamment de leur aptitude à assurer la disponibilité, l'intégrité ou la confidentialité de l'information traitée face aux menaces dues en particulier à la malveillance PEUT être certifiée.

des décisions administratives individuelles[3], cité dans les motifs du décret, ventile entre les différentes autorités étatiques les décisions administratives individuelles. Or plusieurs dispositions de ce type appartenaient au Premier Ministre dans le décret d'application de l'article 1316-4. Pour suivre dans la lettre comme dans l'esprit le texte de 1997, il a fallu se résoudre à passer par le biais d'un nouveau décret[4] pour appliquer le décret d'application sur la signature électronique. Le nouveau texte réglementaire vise la sécurité des systèmes d'information et s'applique du même coup (et pas uniquement) à la signature électronique. Il vient se substituer aux arrêtés A, B, D et E ; l'arrêté C subsiste sous la responsabilité du Ministre de l'Industrie.

3 Le contenu du décret

En ce qui concerne la signature électronique et le décret n°2001-272, l'article 20 du nouveau décret apporte les modifications suivantes :

Le décret du 30 mars 2001 susvisé est ainsi modifié :
I. - Le 1o du II de l'article 3 est remplacé par les dispositions suivantes :
« *1o Soit par le Premier ministre, dans les conditions prévues par le décret no 2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information. La délivrance du certificat de conformité est rendue publique.* »
II. - L'article 4 est remplacé par les dispositions suivantes :
« *Art. 4. - La mise en oeuvre des procédures d'évaluation et de certification prévues au 1o du II de l'article 3 est assurée dans les conditions prévues par le décret no 2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information.* »
III. - Au premier alinéa de l'article 5, les mots : « *l'arrêté* » sont remplacés par les mots : « *le décret* ».
IV. - Au deuxième alinéa de l'article 7, les mots : « *selon des règles définies par arrêté du Premier ministre*» sont supprimés.
V. - Au premier alinéa du II de l'article 9, les mots : « par des organismes publics désignés par arrêté du Premier ministre et agissant sous l'autorité des services du Premier ministre chargés de la sécurité des systèmes d'information » sont remplacés par les mots : « *par la direction centrale de la sécurité des systèmes d'information*».

En résumé, la reconnaissance de conformité des composants de signature électroniques aux exigences techniques du décret 2001-272 passe par une procédure d'agrément – évaluation – certification :

- Les centres techniques chargés de l'audit des composants doivent être agréés. La demande d'agrément est formulée auprès de la DCSSI et précise le domaine dans lequel l'organisme demandeur entend exercer son activité. L'agrément est délivré par le Premier Ministre, après avis d'un Comité directeur de la certification. Il est valable pour une durée de deux ans renouvelable.
- Tout candidat à la certification d'un composant doit d'abord le faire évaluer. Pour cela, il adresse à la DCSSI un dossier d'évaluation qui comporte la description du système de sécurité à évaluer, les dispositions prévues pour lui conférer sa pleine efficacité ainsi que le programme de travail prévisionnel. Le candidat choisit un ou plusieurs centres d'évaluation agréés pour procéder à celle-ci. Avant le début des travaux, il détermine avec chacun de ces centres le produit ou le système à évaluer ainsi que les objectifs de sécurité, le coût et les modalités de paiement de l'évaluation, le programme de travail et les délais prévus pour l'évaluation.
- Au terme des travaux d'évaluation, l'évaluateur remet un rapport d'évaluation au demandeur et à la DCSSI. Ce rapport est un document confidentiel dont les informations sont couvertes par le secret industriel et commercial.
- Le candidat et la DCSSI valident les rapports d'évaluation en liaison avec le centre d'évaluation intervenant. Puis la DCSSI élabore un rapport de certification dans un délai d'un mois. Ce dernier conclut soit à la délivrance d'un certificat, soit au refus de la certification.

[3] Décret no 97-1184 du 19 décembre 1997 pris pour l'application au Premier ministre du o de l'article 2 du décret no 97-34 du 15 janvier 1997 relatif à la déconcentration des décisions administratives individuelles.
[4] Selon l'article 1 du Décret no 97-1184 du 19 décembre 1997 précité : *Les décisions administratives individuelles dont la liste figure en annexe sont prises soit par le Premier ministre, seul ou conjointement avec d'autres ministres, soit par décret selon que les dispositions en vigueur donnent compétence aux uns ou à l'autre (...)*. L'annexe vise expressément dans la catégorie des "*décisions administratives individuelles prises par le Premier ministre*", la sécurité et la défense nationale.

- Le certificat est délivré par le Premier ministre. Il atteste que l'exemplaire du produit ou du système soumis à évaluation répond aux caractéristiques de sécurité spécifiées. Il atteste également que l'évaluation a été conduite conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises.

Le nouveau décret installe auprès de la DCSSI un *Comité directeur de la certification en sécurité des technologies de l'information*. Le Comité a notamment pour mission de formuler des avis ou des propositions sur la politique de certification, sur les règles et normes utilisées pour les procédures d'évaluation et de certification et sur les guides techniques mis à la disposition du public. Lorsque le Comité, composé de 13 membres représentants les ministères, examinera des questions concernant les dispositifs de création et de vérification de signature électronique, il s'adjoindra 12 personnalités qualifiées nommées pour trois ans par arrêté du Premier ministre.

Enfin le décret s'intéresse aux certificats délivrés par les organismes ayant leur siège dans un Etat membre de la Communauté européenne : le Premier ministre leur reconnaîtra, dans le cadre de procédures comparables présentant des garanties équivalentes, la même valeur qu'aux certificats délivrés en application du décret,

4 Annexe 1 – Le décret

Décret no 2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information
NOR : PRMX0100183D

Le Président de la République,
Sur le rapport du Premier ministre, du ministre de l'économie, des finances et de l'industrie et du ministre délégué à l'industrie, aux petites et moyennes entreprises, au commerce, à l'artisanat et à la consommation,
Vu la directive 98/34/CE du 22 juin 1998, modifiée par la directive 98/48/CE du 20 juillet 1998, prévoyant une procédure d'information dans le domaine des normes et réglementations techniques et des règles relatives aux services de la société de l'information ;
Vu le code de la consommation, notamment son article R. 115-6 ;
Vu le décret no 97-34 du 15 janvier 1997, modifié par le décret no 97-463 du 9 mai 1997 et par le décret no 97-1205 du 19 décembre 1997, relatif à la déconcentration des décisions administratives individuelles ;
Vu le décret no 97-1184 du 19 décembre 1997, modifié par le décret no 2001-143 du 15 février 2001, pris pour l'application au Premier ministre du 1o de l'article 2 du décret no 97-34 du 15 janvier 1997 relatif à la déconcentration des décisions administratives individuelles ;
Vu le décret no 2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique ;

Le Conseil d'Etat (section de l'intérieur) entendu ;
Le conseil des ministres entendu,

Décrète :

Art. 1er. - La sécurité offerte par des produits ou des systèmes des technologies de l'information, au regard notamment de leur aptitude à assurer la disponibilité, l'intégrité ou la confidentialité de l'information traitée face aux menaces dues en particulier à la malveillance peut être certifiée dans les conditions prévues au présent décret.
Les administrations de l'Etat recourent, dans la mesure du possible et en fonction de leurs besoins de sécurité, à des produits ou des systèmes des technologies de l'information certifiés suivant la procédure prévue au présent décret.

Chapitre Ier
Procédure d'évaluation et de certification
Section 1
Evaluation

Art. 2. - Une évaluation en vue de la certification prévue à l'article 1er est effectuée à la demande d'un commanditaire qui adresse à la direction centrale de la sécurité des systèmes d'information un dossier d'évaluation. Le dossier comporte notamment la description du système de sécurité à évaluer, les dispositions prévues pour lui conférer sa pleine efficacité ainsi que le programme de travail prévisionnel permettant une évaluation.
Dès réception de ce dossier, la direction centrale de la sécurité des systèmes d'information si elle estime que les objectifs de sécurité ne sont pas définis de manière pertinente au regard des normes, prescriptions techniques ou règles de bonne pratique applicables au moment où commence l'évaluation, notifie au commanditaire qu'elle ne pourra pas en l'état du dossier procéder à la certification envisagée.

Art. 3. - Le commanditaire de l'évaluation choisit un ou plusieurs centres d'évaluation, agréés dans les conditions prévues au chapitre II, pour procéder à celle-ci. Avant le début des travaux, il détermine avec chacun de ces centres :
a) Le produit ou le système à évaluer ainsi que les objectifs de sécurité ;
b) Les conditions de protection de la confidentialité des informations qui seront traitées dans le cadre de l'évaluation ;
c) Le coût et les modalités de paiement de l'évaluation ;
d) Le programme de travail et les délais prévus pour l'évaluation.

Le commanditaire est tenu d'assurer la mise à la disposition des centres d'évaluation qu'il a choisis et de la direction centrale de la sécurité des systèmes d'information, si elle en fait la demande, de tous les éléments nécessaires au bon accomplissement de leurs travaux, le cas échéant après accord des fabricants concernés.

Art. 4. - Le commanditaire peut décider à tout moment de mettre fin à une évaluation.
Il est décidé entre les parties du dédommagement éventuellement dû au centre d'évaluation.

Art. 5. - La direction centrale de la sécurité des systèmes d'information veille à la bonne exécution des travaux d'évaluation. Elle peut à tout moment demander à assister à ces travaux ou à obtenir des informations sur leur déroulement.

Art. 6. - Au terme des travaux d'évaluation, chaque centre remet un rapport d'évaluation au commanditaire et à la direction centrale de la sécurité des systèmes d'information. Ce rapport est un document confidentiel dont les informations sont couvertes par le secret industriel et commercial.

Section 2
Certification

Art. 7. - Le commanditaire et la direction centrale de la sécurité des systèmes d'information valident les rapports d'évaluation en liaison avec le centre d'évaluation intervenant. Lorsque l'ensemble des rapports prévus a été validé, la direction centrale de la sécurité des systèmes d'information élabore un rapport de certification dans un délai d'un mois. Ce rapport, qui précise les caractéristiques des objectifs de sécurité proposés, conclut soit à la délivrance d'un certificat, soit au refus de la certification.

Le rapport de certification peut comporter tout avertissement que ses rédacteurs estiment utile de mentionner pour des raisons de sécurité. Il est, au choix du commanditaire, communiqué ou non à des tiers ou rendu public.

Art. 8. - Le certificat est délivré par le Premier ministre.
Il atteste que l'exemplaire du produit ou du système soumis à évaluation répond aux caractéristiques de sécurité spécifiées. Il atteste également que l'évaluation a été conduite conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises.

Art. 9. - La direction centrale de la sécurité des systèmes d'information peut passer, après avis du comité directeur de la certification, des accords de reconnaissance mutuelle avec des organismes étrangers homologues, ayant leur siège en dehors des Etats membres de la Communauté européenne.
Ces accords peuvent prévoir que les certificats délivrés par les organismes étrangers cosignataires, dans le cadre de procédures comparables à celle prévue au présent chapitre, sont reconnus comme ayant la même valeur que les certificats délivrés en application du présent décret. La reconnaissance mutuelle des certificats peut être limitée à un niveau d'assurance déterminé.
Sans préjudice des règles régissant la certification des dispositifs sécurisés de création de signature électronique mentionnées au 2o du II de l'article 3 du décret du 30 mars 2001 susvisé, le Premier ministre reconnaît aux certificats délivrés par les organismes ayant leur siège dans un Etat membre de la Communauté européenne, dans le cadre de procédures comparables présentant des garanties équivalentes, la même valeur qu'aux certificats délivrés en application du présent décret.

Chapitre II
Agrément des centres d'évaluation

Art. 10. - Les centres d'évaluation chargés de procéder à l'évaluation prévue au présent décret sont agréés dans les conditions fixées par le présent chapitre.

Art. 11. - I. - La demande d'agrément est formulée auprès de la direction centrale de la sécurité des systèmes d'information. Cette demande précise le domaine dans lequel l'organisme demandeur entend exercer son activité.
II. - L'organisme demandeur doit faire la preuve :
a) De sa conformité aux critères de qualité selon les règles et normes d'accréditation en vigueur ;
b) De son aptitude à appliquer les critères d'évaluation en vigueur et la méthodologie correspondante ainsi qu'à assurer la confidentialité requise par l'évaluation ;
c) De sa compétence technique à conduire une évaluation.
La conformité mentionnée au a et l'aptitude mentionnée au b sont attestées par une accréditation délivrée par une instance reconnue dans les conditions prévues à l'article R. 115-6 du code de la consommation ou délivrée par une instance étrangère équivalente.

La compétence technique mentionnée au c est appréciée par la direction centrale de la sécurité des systèmes d'information, notamment à partir des moyens, des ressources et de l'expérience du centre d'évaluation.

Art. 12. - L'agrément est délivré par le Premier ministre, après avis du comité directeur de la certification. Il peut énoncer les obligations particulières auxquelles est soumis le centre d'évaluation. Il est valable pour une durée de deux ans renouvelable.

Art. 13. - Lorsqu'un centre d'évaluation situé hors du territoire national ou d'un autre Etat membre de la Communauté européenne a déjà fait l'objet d'un agrément par les autorités de son pays d'installation dans le cadre d'une procédure homologue, le Premier ministre peut, après avis du comité directeur de la certification, le déclarer agréé au titre du présent décret. Cet agrément, qui est accordé pour une durée de deux ans renouvelable, peut être limité à un niveau d'assurance déterminé.
Lorsqu'un centre d'évaluation situé dans un Etat membre de la Communauté européenne a déjà fait l'objet d'un agrément par les autorités de cet Etat dans le cadre d'une procédure équivalente, le Premier ministre, après avis du comité directeur de la certification, le déclare agréé au titre du présent décret.

Art. 14. - La direction centrale de la sécurité des systèmes d'information peut s'assurer à tout moment que les centres d'évaluation continuent à satisfaire aux critères au vu desquels ils ont été agréés. Lorsqu'un centre ne satisfait plus aux exigences mentionnées à l'article 11 ou qu'il manque aux obligations fixées par la décision d'agrément, l'agrément peut être retiré par le Premier ministre, après avis du comité directeur de la certification. Le retrait ne peut être prononcé qu'après que le représentant du centre d'évaluation a été mis à même de faire valoir ses observations devant le comité directeur de la certification.

Chapitre III
Comité directeur de la certification en sécurité des technologies de l'information

Art. 15. - Le comité directeur de la certification en sécurité des technologies de l'information a notamment pour mission :
a) De formuler des avis ou des propositions sur la politique de certification, sur les règles et normes utilisées pour les procédures d'évaluation et de certification et sur les guides techniques mis à la disposition du public ;
b) D'émettre un avis sur la délivrance et le retrait des agréments aux centres d'évaluation ;
d) D'examiner, à des fins de conciliation, tout litige relatif aux procédures d'évaluation organisées par le présent décret qui lui est soumis par les parties ;
e) D'émettre un avis sur les accords de reconnaissance mutuelle conclus avec des organismes étrangers en application de l'article 9.
La mission prévue au c ci-dessus peut être déléguée par le comité à l'un de ses membres, elle comporte obligatoirement l'audition des parties.

Art. 16. - Le comité directeur de la certification en sécurité des technologies de l'information est présidé par le secrétaire général de la défense nationale ou son représentant. Outre son président, il comprend :
a) Un représentant du ministre de la justice ;
b) Un représentant du ministre de l'intérieur ;
c) Un représentant du ministre des affaires étrangères ;
d) Un représentant du ministre de la défense ;
f) Un représentant du ministre chargé de l'industrie ;
g) Un représentant du ministre chargé de l'économie ;
h) Un représentant du ministre chargé de l'emploi ;
i) Un représentant du ministre chargé de la santé ;
j) Un représentant du ministre chargé de l'éducation nationale ;
k) Un représentant du ministre chargé de la communication ;
l) Un représentant du ministre chargé de la réforme de l'Etat ;
m) Un représentant du ministre chargé des transports ;
n) Un représentant du ministre chargé de la recherche.
Lorsque le comité directeur examine des questions concernant les dispositifs de création et de vérification de signature électronique, tels que définis à l'article 1er du décret du 30 mars 2001 susvisé, il comprend en outre douze personnalités qualifiées nommées pour trois ans par arrêté du Premier ministre.
Le secrétariat du comité directeur est assuré par la direction centrale de la sécurité des systèmes d'information.

Art. 17. - Le comité directeur se réunit sur convocation de son président qui en fixe l'ordre du jour.

Le président peut inviter tout expert ou personne qualifiée dont la participation aux débats lui paraît nécessaire. Le comité rend compte de ses travaux au Premier ministre.

Art. 18. - La direction centrale de la sécurité des systèmes d'information fait annuellement rapport au comité directeur de la certification de l'activité qu'elle exerce dans le cadre de la mise en oeuvre du présent décret.

Chapitre IV
Dispositions diverses et transitoires

Art. 19. - Dans la partie « Sécurité et défense nationale » du paragraphe 2 de l'annexe au décret no 97-1184 du 19 décembre 1997 susvisé, il est ajouté, à la suite du tableau relatif au décret no 2001-143 du 15 février 2001, les mots et le tableau suivants :
« Décret no 2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information.

Vous pouvez consulter le tableau dans le JO
n° 92 du 19/04/2002 page 6944 à 6946

Art. 20. - Le décret du 30 mars 2001 susvisé est ainsi modifié :
I. - Le 1o du II de l'article 3 est remplacé par les dispositions suivantes :
« 1o Soit par le Premier ministre, dans les conditions prévues par le décret no 2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information. La délivrance du certificat de conformité est rendue publique. »
II. - L'article 4 est remplacé par les dispositions suivantes :
« Art. 4. - La mise en oeuvre des procédures d'évaluation et de certification prévues au 1o du II de l'article 3 est assurée dans les conditions prévues par le décret no 2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information. »
III. - Au premier alinéa de l'article 5, les mots : « l'arrêté » sont remplacés par les mots : « le décret ».
IV. - Au deuxième alinéa de l'article 7, les mots : « selon des règles définies par arrêté du Premier ministre » sont supprimés.
V. - Au premier alinéa du II de l'article 9, les mots : « par des organismes publics désignés par arrêté du Premier ministre et agissant sous l'autorité des services du Premier ministre chargés de la sécurité des systèmes d'information » sont remplacés par les mots : « par la direction centrale de la sécurité des systèmes d'information».

Art. 21. - Les certificats et les agréments des centres d'évaluation délivrés avant la date d'entrée en vigueur du présent décret, en application des dispositions de l'avis du Premier ministre relatif à la délivrance de certificats pour la sécurité offerte par les produits informatiques vis-à-vis de la malveillance, publié au Journal officiel de la République française du 1er septembre 1995, sont reconnus comme délivrés au titre du présent décret.

Art. 22. - Le présent décret est applicable :
a) En Nouvelle-Calédonie et en Polynésie française, en tant qu'il concerne la signature électronique ;
b) Dans les îles Wallis et Futuna et à Mayotte.

Art. 23. - Les dispositions du présent décret pourront être ultérieurement modifiées par décret, à l'exception :
a) Du premier alinéa des articles 8 et 12, du deuxième alinéa de l'article 14 et de l'article 19 dont la modification s'effectuera, le cas échéant, dans les conditions prévues à l'article 2 du décret du 15 janvier 1997 susvisé ;
b) De l'article 20.

Art. 24. - Le présent décret sera publié au Journal officiel de la République française.

Fait à Paris, le 18 avril 2002.

Jacques Chirac
Par le Président de la République :
Le Premier ministre,
Lionel Jospin
.../...

5 Annexe 2 - Récapitulation des textes relatifs à la signature électronique

On trouvera ci-dessous le rappel des textes qui s'appliquent directement à la signature électronique, à l'exception de la réglementation de la cryptologie ou des télécommunications :

- Directive 1999/93/CE du parlement européen et du conseil du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques[5] ;
- Décision 2000/709/CE 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[6] ;
- Loi n°2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relatif à la signature électronique[7] ;
- Décret n°2001-272 du 30 mars 2001 modifié pris pour l'application de l'article 1316-4 du Code Civil et relatif à la signature électronique[8] ;
- Arrêté du 15 mars 2002 portant organisation de la direction centrale de la sécurité des systèmes d'information[9] ;
- Arrêté du 15 mars 2002 relatif à l'organisation en bureaux des sous-directions de la direction centrale de la sécurité des systèmes d'information[10] ;
- Décret n°2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information[11].

On peut s'attendre à la parution des textes suivants (à une date cependant indéterminée) :

- L'arrêté [arrêté C] 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);
- Le décret en Conseil d'Etat relatif aux actes authentiques électroniques, prévu par l'article 1 bis de la loi du 13 mars 2000[12].
- La loi sur la Société de l'Information (LSI) qui doit transposer la Directive sur le commerce électronique[13]. Ce texte, dont une première mouture a été rendue publique en avril 2001, devrait d'une part, permettre l'emploi de la signature électronique *ad solemnitatem* pour satisfaire le formalisme juridique s'opposant à la dématérialisation documentaire et d'autre part, poser les principes de la responsabilité professionnelle des Prestataires des Services de Certification Electronique.

---

5 JOCE du 17.1.2002 n°L 15/24.

6 JOCE du 16 novembre 2000 p. L.289/42

7 JO du 14 mars 2000 p. 3968

8 JO du 31 mars 2001 p. 5070

9 JO Numéro 65 du 17 mars 2002 page 4838

10 JO Numéro 65 du 17 mars 2002 page 4839

11 JO Numéro 92 du 19 Avril 2002 page 6944

12 Selon l'article 1 bis de la loi du 13 mars 2000, l'article 1317 du code civil est complété par un alinéa ainsi rédigé : "*Il [l'acte authentique électronique] peut être dressé sur support électronique s'il est établi et conservé dans des conditions fixées par Décret en Conseil d'Etat.*"

13 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.