



COMMISSION DES COMMUNAUTÉS EUROPÉENNES

Bruxelles, le 29.04.1999

COM(1999) 195 final

98/0191(COD)

Proposition modifiée de

**DIRECTIVE DU PARLEMENT EUROPÉEN ET DU CONSEIL**

**sur un cadre commun pour les signatures électroniques**

(présentée par la Commission conformément à l'article 189 B,  
paragraphe 2 du traité CE)

## RÉSUMÉ

Le 13 janvier 1999, le Parlement européen a adopté une résolution législative approuvant, sous réserve des amendements contenus dans ladite résolution, la proposition de directive du Parlement européen et du Conseil sur un cadre commun pour les signatures électroniques (COM(98)297 final - C4-0376/98 - 98/0191(COD) présentée par la Commission, et invitant la Commission à modifier sa proposition en conséquence.

La directive vise à assurer le bon fonctionnement du marché intérieur dans le domaine des signatures électroniques en instituant un cadre juridique homogène et approprié à l'utilisation des signatures électroniques dans la Communauté. Elle établit un ensemble de critères devant servir de base à la reconnaissance juridique des signatures électroniques. **La proposition a pour base juridique l'article 57, paragraphe 2, et les articles 66 et 100A du traité.**

La directive institue un cadre juridique pour certains services de certification accessibles au public. Elle met l'accent en particulier sur les services de certification et établit des critères communs pour les prestataires de service de certification et les certificats afin de garantir la reconnaissance transfrontalière des signatures et des certificats dans la Communauté européenne. En couvrant un large spectre de "signatures électroniques", la directive affirme sa neutralité sur le plan technologique. **La directive repose sur un double concept: les prestataires de services de certification sont, en règle générale, libres d'offrir leurs services sans autorisation préalable. Parallèlement, les États membres sont autorisés à mettre en place des régimes d'accréditation volontaires reposant sur des exigences communes et visant à améliorer le niveau de sécurité. La directive vise à contribuer à l'établissement d'un cadre juridique harmonisé à l'intérieur de la Communauté en garantissant aux signatures électroniques la reconnaissance juridique. Afin de soutenir la confiance des consommateurs et des entrepreneurs qui utilisent les certificats, la proposition établit des règles de responsabilité pour les prestataires de services de certification. La directive prévoit des mécanismes de coopération avec les pays tiers afin de contribuer à la reconnaissance des certificats au niveau mondial.**

Sur les 32 amendements adoptés par le Parlement européen en première lecture, la Commission en a accepté 22, certains dans leur intégralité (amendements 3, 11, 12, 14, 18, 20, 27, 30, 31, 32, 33 et 34), et d'autres en partie ou en principe (amendements 2, 4, 5, 9, 13, 16, 17, 21, 22 et 25).

La Commission ne peut pas accepter dix des amendements proposés, soit pour des motifs juridiques (amendements 1, 10, 24, 28, 29), soit parce qu'ils contiennent des dispositions superflues (amendements 6 and 7), soit parce que leur mise en œuvre poserait des problèmes (amendements 15, 23 et 26).

## **EXPOSÉ DES MOTIFS**

La Commission présente ci-après une proposition modifiée de directive du Parlement européen et du Conseil sur un cadre commun pour les signatures électroniques. La proposition modifiée incorpore les amendements proposés par le Parlement européen en première lecture qui peuvent être acceptés par la Commission.

### **1) INTRODUCTION**

#### **a) Historique**

La Commission a tout d'abord présenté, le 8 octobre 1997, une communication intitulée "Assurer la sécurité et la confiance dans la communication électronique - Vers un cadre européen pour les signatures numériques et le chiffrement" (COM(97)503 final - C4-0648/97), qui soulignait la nécessité d'adopter une approche cohérente dans ce domaine. Le 1er décembre 1997, le Conseil a accueilli favorablement cette communication et a invité la Commission à présenter dès que possible une proposition de directive sur les signatures numériques. Dans sa résolution du 17 juillet 1998 (A4-0189/98), le Parlement européen a insisté sur la nécessité de créer un cadre juridique au niveau européen visant à garantir la confiance mutuelle dans les signatures numériques et à encourager le développement du commerce électronique et de la communication électronique.

Le 13 mai 1998, la Commission a adopté une proposition de directive du Parlement européen et du Conseil sur un cadre commun pour les signatures électroniques (COM(1998)297 final - C4-0376/98 - 98/0191(COD)). La proposition de directive précède les initiatives de plusieurs États membres de l'Union européenne visant à élaborer un cadre juridique pour les signatures électroniques. La directive est donc considérée comme une mesure préventive visant à créer un cadre homogène pour les services d'authentification en Europe. Elle prend en considération le caractère global de la communication électronique. La proposition a pour base juridique l'article 57, paragraphe 2, et les articles 66 et 100A du traité.

La proposition a été officiellement transmise au Parlement européen et au Conseil le 16 juin 1998. Le Comité économique et social a émis son avis les 2/3 décembre 1998 et le Comité des régions les 13/14 janvier 1999. Le Parlement européen a adopté une résolution favorable en première lecture le 13 janvier 1999 et a formulé 32 propositions d'amendements au texte présenté par la Commission.

#### **b) Objectif de la directive**

La directive vise à assurer le bon fonctionnement du marché intérieur dans le domaine des signatures électroniques en instituant un cadre juridique harmonisé et approprié permettant l'utilisation des signatures électroniques dans la Communauté. Elle établit un ensemble de critères devant servir de base à la reconnaissance juridique des signatures électroniques. Les communications et le commerce électroniques mondiaux dépendent de l'adaptation progressive des législations nationales et internationales à l'évolution rapide de l'infrastructure technique. Il faut s'occuper de ces questions si l'on veut que les

consommateurs et les entreprises en Europe puissent profiter pleinement des possibilités offertes par les communications électroniques.

### **c) Grands principes de la directive**

#### **- Portée**

La directive institue un cadre juridique pour certains services de certification accessibles au public. Elle est centrée en particulier sur les services de certification et établit des critères communs pour les prestataires de service de certification et les certificats afin de garantir la reconnaissance transfrontalière des signatures et des certificats dans la Communauté européenne. La technologie des signatures électroniques a des applications évidentes dans les environnements fermés, comme un réseau local d'entreprises ou un système bancaire. Les certificats et les signatures électroniques ont également une fonction d'autorisation, par exemple, pour accéder à un compte privé. Dans ce cas, la Commission ne voit pas la nécessité d'une harmonisation.

#### **- Neutralité technologique**

On peut s'attendre au développement d'une série de mécanismes d'authentification. C'est pourquoi le champ d'application de la directive doit être suffisamment large pour s'appliquer à tout l'éventail des signatures électroniques. Bien que l'importance des signatures numériques utilisant les techniques de la cryptographie soient aujourd'hui reconnues, la proposition souligne qu'un cadre réglementaire européen doit être suffisamment souple pour englober d'autres techniques qui peuvent être utilisées à des fins d'authentification.

#### **- Double approche**

La directive repose sur un double concept. Elle a pour objectif principal d'encourager l'utilisation au niveau communautaire des services de certification sur les réseaux ouverts. Étant donné la diversité des services et leurs possibilités d'application, les prestataires de services de certification devraient, en règle générale, être libres d'offrir leurs services sans autorisation préalable. Dans ce secteur, le marché doit pouvoir se développer librement. Parallèlement, les États membres seront autorisés à mettre en place des régimes d'accréditation volontaires reposant sur des exigences communes et visant à améliorer le niveau de sécurité. Ces régimes offrent aux prestataires de service de certification le cadre approprié au perfectionnement de leurs services sur le plan de la confiance, de la sécurité et de la qualité exigée par le marché, les consommateurs et les citoyens.

#### **- Exigences essentielles**

La proposition de directive établit des exigences concernant les certificats et les prestataires de service de certification visant à créer un cadre harmonisé au niveau européen. Ces exigences ne sont pas très détaillées et sont exclusivement liées à la reconnaissance juridique des signatures électroniques.

#### **- Reconnaissance juridique des signatures électroniques**

La directive vise à contribuer à l'établissement d'un cadre juridique harmonisé à l'intérieur de la Communauté en garantissant aux signatures électroniques la reconnaissance juridique. La reconnaissance juridique signifie que les signatures électroniques reposant

sur un certificat agréé délivré par un prestataire de service de certification qui satisfait aux exigences prévues à l'annexe II sont, d'une part, reconnues comme conformes aux exigences légales relatives à une signature manuscrite et, d'autre part, admises comme preuve en justice de la même façon que les signatures manuscrites.

#### - Responsabilité

Afin de soutenir la confiance des consommateurs et des entrepreneurs qui utilisent les certificats, la proposition établit des règles de responsabilité pour les prestataires de services de certification. Sur la base de la proposition, ceux-ci sont en particulier responsables de la validité du contenu d'un certificat.

#### - Aspects internationaux

La directive prévoit des mécanismes de coopération avec les pays tiers afin de contribuer à la reconnaissance des certificats au niveau mondial. Ils visent en particulier à garantir la reconnaissance par les États membres, dans des conditions claires, de certificats de pays tiers et à envisager la négociation par la Commission d'accords bilatéraux et multilatéraux. Il s'agit là d'un élément important pour le développement du commerce électronique au niveau international.

#### - Protection des données

La directive vise à harmoniser les dispositions nationales visant à assurer la protection de l'intérêt public, telles que celles qui doivent assurer le respect de la vie privée et la protection des données personnelles dans le cadre particulier des signatures électroniques. En outre, la directive fournit l'instrument nécessaire pour que les consommateurs puissent garder leur anonymat dans les transactions en ligne (certificats indiquant un pseudonyme au lieu du nom du signataire).

## **2) AMENDEMENTS DU PE ACCEPTÉS PAR LA COMMISSION**

Sur les 32 amendements adoptés par le Parlement européen en première lecture, la Commission en a accepté 22 intégralement, partiellement ou en principe.

Amendements acceptés dans leur intégralité : 3, 11, 12, 14, 18, 20, 27, 30, 31, 32, 33 et 34.

Amendements acceptés en partie ou en principe : 2, 4, 5, 9, 13, 16, 17, 21, 22 et 25.

La Commission a accepté les amendements qui :

- rendent le texte plus clair et plus complet (amendements 2, 3, 5, 9, 11 - 14, 16 - 18, 20 - 22, 25, 27, 30 - 34),
- donnent des indications utiles sur le sens dans lequel la directive devra être revue à la fin de 2002 (amendement 4).

Dans sa proposition modifiée, la Commission a inséré les amendements dans la formulation proposée par le Parlement européen, et a apporté certains ajouts pour assurer la cohérence de l'ensemble.

### 3) AMENDEMENTS DU PE NON ACCEPTÉS PAR LA COMMISSION

Dix amendements proposés n'ont pas été acceptés :

- soit pour des motifs juridiques, notamment parce qu'ils ne s'accordaient pas avec des règles communautaires existantes ;
- soit parce qu'ils contenaient des dispositions jugées superflues ;
- soit parce que leur mise en œuvre poserait des problèmes.

#### a) Motifs juridiques

- Le Parlement propose que, dans le troisième considérant, on parle de signatures *électroniques* au lieu de signatures numériques (amendement 1). La Commission est d'accord avec la démarche globale du Parlement européen qui consiste à ce que le texte soit exclusivement concentré sur les signatures électroniques parce que c'est effectivement le domaine régi par la directive, mais le troisième considérant cite le texte d'une conclusion du Conseil du 1<sup>er</sup> décembre 1997. Changer le texte n'aurait donc aucun sens.
- Le Parlement propose de changer le "comité de caractère consultatif" en un "comité de contact" (amendements 10 et 28) et d'imposer quelques obligations de consultation et d'information supplémentaires (amendement 28). Cette proposition n'est pas conforme à la procédure des comités ("comitologie") établie par la décision 87/373/CEE du Conseil, du 13 juillet 1987. Cette décision institue différents types de comités. Les obligations de consultation et d'information proposées ne correspondent pas aux procédures prévues et ne reflètent pas la façon de faire actuelle des groupes de travail existants. La Commission peut garantir qu'elle se mettra en rapport avec l'industrie, les utilisateurs et les associations de consommateurs sur une base volontaire.

La tâche du comité doit être de clarifier les exigences fixées aux annexes I et II ainsi qu'en matière de normalisation et non d'élaborer ces exigences, faute de quoi ce comité aurait un caractère quasi législatif.

- La distinction faite entre le type de comité et la procédure à l'article 9, et la fonction du comité à l'article 10 rend le texte plus clair. C'est pourquoi la Commission juge préférable de ne pas supprimer l'article 10 (amendement 29).
- Dans l'amendement 24, le Parlement propose que les propositions de mandats de négociation d'accords bilatéraux et multilatéraux soient soumises non seulement au Conseil mais *aussi au Parlement européen*. Cette disposition serait contraire à l'article 113 du traité CEE, qui prévoit que la Commission soumet des propositions au Conseil exclusivement, et non au Parlement européen.
- Le Parlement propose d'ajouter un membre de phrase indiquant que le prestataire de service de certification indique un pseudonyme *pour autant que cela soit autorisé par les dispositions juridiques nationales concernant les opérations commerciales non électroniques* (amendement 26). Il n'existe pas de règles générales nationales sur les pseudonymes dans les transactions autres que les opérations "en ligne" pour la simple raison qu'elles ne sont pas nécessaires. En principe, les consommateurs peuvent choisir de garder l'anonymat. Le but de l'article 8, paragraphe 3, est de créer l'outil nécessaire pour permettre que les transactions en ligne puissent se faire de la même manière que les transactions non électroniques.

## **b) Dispositions superflues**

- Le Parlement propose d'ajouter un considérant indiquant que les accords internationaux ne doivent pas empêcher l'Union européenne de maintenir et de continuer à développer les règles concernant la protection des données (amendement 6). C'est un fait que les règles existantes concernant la protection des données doivent être respectées et que les accords dans le domaine des signatures électroniques devront respecter le droit de maintenir et de continuer à développer les règles existantes concernant la protection des données. Il est donc inutile d'ajouter une telle disposition.
- Le Parlement propose d'ajouter un considérant indiquant que les accords dans le domaine des signatures électroniques doivent également porter sur la protection des données et le respect de la vie privée (amendement 7). Il est clair que dans le cadre d'un tel accord, il faudra tenir compte des règles existantes concernant la protection des données, et en particulier des dispositions relatives aux flux de données internationaux. C'est pourquoi la Commission estime qu'une telle disposition serait superflue.

## **c) Problèmes de mise en œuvre**

- L'ajout du mot *indépendant* dans la définition du prestataire de service de certification donnée à l'article 2, paragraphe 6, (amendement 15) poserait des problèmes de mise en œuvre. Le sens de cette exigence ne serait en effet pas clair, puisque cela pourrait viser l'indépendance financière, l'indépendance sur le plan de l'organisation, ou encore autre chose. En outre, il serait préférable de faire figurer cette exigence dans l'annexe II, au lieu de l'ajouter dans la définition.
- L'amendement 23 ne peut être accepté pour des raisons semblables. Le Parlement propose d'ajouter à l'article 6 un paragraphe indiquant que le prestataire de service de certification doit restreindre ses activités aux tâches fixées dans ses statuts. Tout d'abord, on ne voit pas très bien quel serait le but exact de cette disposition. Deuxièmement, les prestataires de services de certification ne sont pas tenus d'établir des statuts; de plus, le sens juridique qu'il faut attribuer à ce terme de statuts n'est pas précisé. Enfin, il y a lieu de se demander si un prestataire de service de certification pourrait être en mesure d'assurer qu'il n'est pas soumis à un quelconque contrôle administratif. En tout état de cause, cette disposition ne doit pas figurer à l'article 6, car le texte proposé ne se rapporte pas aux questions de responsabilité.

## **4) CONCLUSIONS**

La Commission a accepté, en tout ou en partie, 22 des 32 amendements proposés par le Parlement européen en première lecture.

Conformément à l'article 189B, paragraphe 2, du traité CE, la Commission modifie sa proposition initiale en y incorporant lesdits amendements.

Proposition modifiée de

**DIRECTIVE DU PARLEMENT EUROPÉEN ET DU CONSEIL**

**sur un cadre commun pour les signatures électroniques**

**(Texte présentant de l'intérêt pour l'EEE)**

Texte original	Texte modifié
----------------	---------------

Quatrième considérant  
(basé sur l'amendement 2)

<p>(4) considérant que les communications et le commerce électroniques nécessitent des signatures électroniques et des services connexes permettant d'authentifier les données; que toute divergence dans les règles relatives à la reconnaissance juridique des signatures électroniques et à l'accréditation des "prestataires de service de certification" dans les États membres risque de constituer un sérieux obstacle à l'utilisation des communications électroniques et au commerce électronique, <u>et donc d'entraver le développement du marché intérieur</u>; que la diversité des activités menées dans les États membres <u>met en évidence le besoin d'harmonisation au niveau communautaire</u>;</p>	<p>(4) considérant que les communications et le commerce électroniques nécessitent des signatures électroniques et des services connexes permettant d'authentifier les données; que toute divergence dans les règles relatives à la reconnaissance juridique des signatures électroniques et à l'accréditation des "prestataires de service de certification" dans les États membres risque de constituer un sérieux obstacle à l'utilisation des communications électroniques et au commerce électronique; <u>que des conditions cadres communes, claires, pour les signatures électroniques renforcent par contre la confiance dans les nouvelles technologies et l'acceptation générale de celles-ci</u>; que la diversité des activités menées dans les États membres <u>ne doit pas entraver la libre circulation des marchandises et des services au sein du marché intérieur</u>;</p>
--	--

Sixième considérant  
(basé sur l'amendement 3)

<p>(6) considérant que, eu égard à la rapidité des progrès techniques et à la dimension mondiale d'Internet, il convient d'adopter une approche qui prenne en compte les diverses technologies et services permettant d'authentifier des données électroniquement; <u>que, toutefois, les «signatures numériques» reposant sur la cryptographie à clé publique constituent actuellement la forme la plus reconnue de signature électronique;</u></p>	<p>(6) considérant que, eu égard à la rapidité des progrès techniques et à la dimension mondiale d'Internet, il convient d'adopter une approche qui prenne en compte les diverses technologies et services permettant d'authentifier des données électroniquement;</p>
--	--

Sixième considérant bis (nouveau)  
(basé sur l'amendement 4)

	<p><u>considérant que la Commission procédera à un réexamen de la présente directive avant 2003, en partie pour s'assurer que les progrès techniques ou les changements intervenus dans l'environnement juridique n'ont pas créé d'obstacles à la réalisation des objectifs énoncés dans la présente directive; qu'elle examinera les incidences d'aspects techniques connexes, tels que la confidentialité, et qu'elle présentera un rapport à ce sujet au Parlement et au Conseil;</u></p>
--	--

Considérant 10 bis (nouveau)  
(basé sur l'amendement 5)

	<p>(10 bis) <u>considérant que le marché intérieur comprend également la libre circulation des personnes, ce qui implique que les citoyens et les résidents de l'Union européenne ont nécessairement de plus en plus de contacts avec les autorités d'États membres autres que celui dans lequel ils résident; considérant que, pour ces raisons, le Parlement européen a décidé d'approuver le traitement électronique des pétitions; considérant que la disponibilité des communications électroniques pourrait s'avérer très utile dans ce domaine, pour autant que les réglementations nationales concernant des exigences supplémentaires ne constituent pas un obstacle à des possibilités d'accès plus aisées à l'administration.</u></p>
--	--

Considérant 13 bis (nouveau)  
(basé sur l'amendement 9)

	<p>(13 bis) <u>considérant que la présente directive ne porte pas atteinte aux dispositions nationales existantes concernant l'ordre ou la sécurité publics ou relatives à la fourniture de services à caractère confidentiel;</u></p>
--	--

Article premier  
(basé sur l'amendement 11)

<p>Article premier La présente directive porte sur l'utilisation et la reconnaissance juridique des signatures électroniques. Elle ne couvre pas d'autres aspects liés à la conclusion et à la validité des contrats ou d'autres formalités non contractuelles nécessitant signature. <u>Elle institue un cadre juridique pour certains services de certification accessibles au public.</u></p>	<p>Article premier La présente directive porte sur l'utilisation et la reconnaissance juridique des signatures électroniques. <u>Elle institue un cadre juridique pour certains services de certification accessibles au public.</u> Elle ne couvre pas d'autres aspects liés à la conclusion et à la validité des contrats ou d'autres formalités non contractuelles nécessitant signature.</p>
--	--

Article 2, paragraphe 1  
(basé sur l'amendement 12)

<p>1. «signature électronique», une signature sous forme numérique intégrée, jointe ou liée logiquement à des données, utilisée par un signataire pour signifier son acceptation du contenu des données, et qui satisfait aux exigences suivantes:</p>	<p>1. «signature électronique», une signature sous forme <u>électronique</u> intégrée, jointe ou liée logiquement à des données, utilisée par un signataire pour signifier son acceptation du contenu des données, et qui satisfait aux exigences suivantes:</p>
--	--

Article 2, paragraphe 2  
(basé sur l'amendement 13)

<p>2. «signataire», toute personne qui crée une signature électronique;</p>	<p>2. «signataire», toute personne <u>physique</u>, qui, <u>en son nom propre ou au nom de la personne ou de l'entité qu'elle représente</u>, crée une signature électronique;</p>
---	--

Article 2, paragraphe 5  
(basé sur l'amendement 14)

<p>5. «certificat agréé», une attestation numérique qui lie un dispositif de vérification de signature à une personne, confirme l'identité de cette personne et satisfait aux exigences prévues à l'annexe I;</p>	<p>5. «certificat agréé», une attestation <u>électronique</u> qui lie un dispositif de vérification de signature à une personne, confirme l'identité de cette personne et satisfait aux exigences prévues à l'annexe I;</p>
---	---

Article 3, paragraphe 2  
(basé sur l'amendement 16)

<p>2. Sans préjudice des dispositions du paragraphe 1, les États membres peuvent instaurer ou maintenir des régimes volontaires d'accréditation visant à élever le niveau du service de certification fourni. Tous les critères relatifs à ces régimes doivent être objectifs, transparents, proportionnés et non discriminatoires. Les États membres ne peuvent limiter le nombre de prestataires de service de certification pour des motifs relevant du champ d'application de la présente directive.</p>	<p>2. Sans préjudice des dispositions du paragraphe 1, les États membres peuvent instaurer ou maintenir des régimes volontaires d'accréditation visant à élever le niveau du service de certification fourni. <u>Les États membres peuvent également reconnaître des régimes d'accréditation gérés par des organisations indépendantes des administrations des États membres dont l'objectif consiste à améliorer les niveaux des services de certification.</u> Tous les critères relatifs à ces régimes doivent être objectifs, transparents, proportionnés et non discriminatoires. Les États membres ne peuvent limiter le nombre de prestataires de service de certification pour des motifs relevant du champ d'application de la présente directive.</p>
--	---

Article 3, paragraphe 4  
(basé sur l'amendement 17)

<p>4. Les États membres peuvent admettre l'usage des signatures électroniques dans le secteur public sous réserve d'exigences supplémentaires. Ces exigences doivent être objectives, transparentes, proportionnées et non discriminatoires, et ne s'appliquer qu'aux caractéristiques spécifiques de l'application concernée.</p>	<p>4. Les États membres peuvent admettre l'usage des signatures électroniques dans le secteur public sous réserve d'exigences supplémentaires. Ces exigences doivent être objectives, transparentes, proportionnées et non discriminatoires, et ne s'appliquer qu'aux caractéristiques spécifiques de l'application concernée. <u>Ces exigences ne doivent pas constituer un obstacle aux services transfrontaliers pour le citoyen, notamment en ce qui concerne les prestations sociales ou les pensions.</u></p>
--	---

Article 5  
(basé sur l'amendement 18)

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

Article 6, paragraphe 1, point (b)  
(basé sur l'amendement 20)

<p>b) la conformité à toutes les exigences de la présente directive pour ce qui est de la délivrance du certificat agréé;</p>	<p>b) la conformité à toutes les exigences de <u>l'annexe I</u> de la présente directive pour ce qui est de la délivrance du certificat agréé;</p>
---	--

Article 6, paragraphe 3  
(basé sur l'amendement 21)

<p>3. Les États membres veillent à ce qu'un prestataire de service de certification puisse indiquer, dans un certificat agréé particulier, les limites fixées à son utilisation. Le prestataire de service de certification ne doit pas être tenu pour responsable des dommages résultant de l'usage d'un certificat agréé en dehors des limites fixées à son utilisation.</p>	<p>3. Les États membres veillent à ce qu'un prestataire de service de certification puisse indiquer, dans un certificat agréé particulier, les limites fixées à son utilisation. <u>Cette valeur limite doit être suffisamment évidente pour les tiers.</u> Le prestataire de service de certification ne doit pas être tenu pour responsable des dommages résultant de l'usage d'un certificat agréé en dehors des limites fixées à son utilisation.</p>
--	---

Article 6, paragraphe 4  
(basé sur l'amendement 22)

<p>4. Les États membres veillent à ce qu'un prestataire de service de certification puisse indiquer, dans un certificat agréé, la valeur limite des transactions pour lesquelles le certificat est valable. Le prestataire de service de certification ne doit pas être tenu pour responsable des dommages résultant du dépassement de cette valeur limite.</p>	<p>4. Les États membres veillent à ce qu'un prestataire de service de certification puisse indiquer, dans un certificat agréé, la valeur limite des transactions pour lesquelles le certificat est valable. <u>Cette valeur limite doit être suffisamment évidente pour les tiers.</u> Le prestataire de service de certification ne doit pas être tenu pour responsable des dommages résultant du dépassement de cette valeur limite.</p>
---	--

Article 8, paragraphe 2  
(basé sur l'amendement 25)

<p>2. Les États membres veillent à ce qu'un prestataire de service de certification ne puisse recueillir des données personnelles que directement auprès de la personne qui fait l'objet des données et uniquement dans la mesure où cela est nécessaire à la délivrance d'un certificat. Les données ne peuvent être recueillies ou traitées à d'autres fins sans le consentement de la personne qui en fait l'objet.</p>	<p>2. Les États membres veillent à ce qu'un prestataire de service de certification ne puisse recueillir des données personnelles que directement auprès de la personne qui fait l'objet des données, <u>ou avec le consentement explicite de cette personne,</u> et uniquement dans la mesure où cela est nécessaire à la délivrance d'un certificat. Les données ne peuvent être recueillies ou traitées à d'autres fins sans le consentement de la personne qui en fait l'objet.</p>
--	---

Article 8, paragraphe 4  
(basé sur l'amendement 27)

<p>4. <u>Dans le cas de personnes utilisant un pseudonyme, les États membres veillent à ce que le prestataire de service de certification transmette les données concernant l'identité de ces personnes avec leur consentement aux pouvoirs publics qui en font la demande.</u> Si la législation nationale exige, aux fins d'une enquête pénale concernant l'utilisation de la signature électronique <u>sous un pseudonyme</u>, de transférer les données révélant l'identité de la personne qui en fait l'objet, le transfert est consigné et la personne faisant l'objet des données est informée du transfert <u>des données la concernant dans les meilleurs délais après la conclusion de l'enquête.</u></p>	<p>4. Si la <u>directive 95/46/CE</u> et la législation nationale exigent de transférer les données révélant l'identité de la personne qui en fait l'objet/<u>du signataire aux pouvoirs publics</u>, aux fins d'une enquête pénale concernant l'utilisation de la signature électronique <u>accompagnée d'un certificat du pseudonyme ou nécessaire aux demandes en justice liées aux transactions effectuées en recourant à la signature électronique accompagnée d'un certificat du pseudonyme</u>, le transfert est consigné et la personne faisant l'objet des données est informée du transfert.</p>
---	--

Article 11  
(basé sur l'amendement 30)

<p>1. Les États membres communiquent à la Commission les informations suivantes:</p> <p>a) des informations sur les régimes volontaires d'accréditation, ainsi que toute exigence supplémentaire visée à l'article 3, paragraphe 4;</p> <p>b) les noms et adresses des organismes nationaux responsables de l'accréditation et de la supervision; et</p> <p>c) les noms et adresses des prestataires de service de certification nationaux accrédités.</p> <p>2. Les informations fournies en application du paragraphe 1 et les changements concernant ces informations sont notifiés dans les meilleurs délais par les États membres.</p>	<p>1. Les États membres communiquent à la Commission les informations suivantes:</p> <p>a) des informations sur les régimes volontaires d'accréditation, ainsi que toute exigence supplémentaire visée à l'article 3, paragraphe 4;</p> <p>b) les noms et adresses des organismes nationaux <u>reconnus</u> qui sont responsables de l'accréditation et de la supervision; et</p> <p>c) les noms et adresses des prestataires de service de certification nationaux accrédités.</p> <p>2. Les informations fournies en application du paragraphe 1 et les changements concernant ces informations sont notifiés <u>dans un délai d'un mois</u> par les États membres <u>et par des organismes reconnus</u>.</p>
---	---

Annexe I, point b)  
(basé sur l'amendement 31)

<p>b) le nom <u>indiscutable</u> du titulaire ou un pseudonyme <u>ne prêtant pas à confusion</u> et identifié comme tel;</p>	<p>b) le nom du titulaire ou un pseudonyme identifié comme tel;</p>
--	---

Annexe I, point f)  
(basé sur l'amendement 32)

<p>f) le code d'identification <u>unique</u> du certificat;</p>	<p>f) le code d'identification du certificat;</p>
---	---

Annexe I, point i)  
(basé sur l'amendement 33)

<p>i) les limites à la <u>responsabilité du prestataire de service de certification</u> et la valeur des transactions pour lesquelles le certificat est valable, le cas échéant.</p>	<p>i) les limites à <u>l'utilisation du certificat</u> et à la valeur des transactions pour lesquelles le certificat est valable, le cas échéant.</p>
--	---

Annexe II, point e)  
(basé sur l'amendement 34)

<p>e) utiliser des systèmes fiables et des produits de signature électronique qui assurent une protection contre toute modification non autorisée desdits produits <u>pour qu'ils ne puissent être utilisés à des fins autres que celles pour lesquelles ils ont été conçus</u>; ils doivent également utiliser des produits de signature électronique qui assurent la sécurité technique et cryptographique des processus de certification pris en charge par lesdits produits;</p>	<p>e) utiliser des systèmes fiables et des produits de signature électronique qui assurent une protection contre toute modification non autorisée desdits produits; ils doivent également utiliser des produits de signature électronique qui assurent la sécurité technique et cryptographique des processus de certification pris en charge par lesdits produits;</p>
--	---