DOC 50 **0322/001**

BELGISCHE KAMER VAN VOLKSVERTEGENWOORDIGERS

16 december 1999

WETSONTWERP

betreffende de werking van de certificatiedienstverleners met het oog op het gebruik van elektronische handtekeningen

---

CHAMBRE DES REPRÉSENTANTS DE BELGIQUE

16 décembre 1999

PROJET DE LOI

relatif à l'activité des prestataires de service de certification en vue de l'utilisation de signatures électroniques

---

AGALEV-ECOLO	:	*Anders Gaan Leven / Écologistes Confédérés pour l'Organisation de luttes originales*
CVP	:	*Christelijke Volkspartij*
FN	:	*Front national*
PRL FDF MCC	:	*Parti Réformateur libéral - Front démocratique francophone-Mouvement des Citoyens pour le Changement*
PS	:	*Parti socialiste*
PSC	:	*Parti social-chrétien*
SP	:	*Socialistische Partij*
VLAAMS BLOK	:	*Vlaams Blok*
VLD	:	*Vlaamse Liberalen en Democraten*
VU&ID	:	*Volksunie&ID21*

Afkortingen bij de nummering van de publicaties :

DOC 50 0000/000	:	*Parlementair document van de 50e zittingsperiode + het nummer en het volgnummer*
QRVA	:	*Schriftelijke Vragen en Antwoorden*
HA	:	*Handelingen (Integraal Verslag)*
BV	:	*Beknopt Verslag*
PLEN	:	*Plenum*
COM	:	*Commissievergadering*

Abréviations dans la numérotation des publications :

DOC 50 0000/000	:	*Document parlementaire de la 50e législature, suivi du n° et du n° consécutif*
QRVA	:	*Questions et Réponses écrites*
HA	:	*Annales (Compte Rendu Intégral)*
CRA	:	*Compte Rendu Analytique*
PLEN	:	*Séance plénière*
COM	:	*Réunion de commission*

Officiële publicaties, uitgegeven door de Kamer van volksvertegenwoordigers
Bestellingen :
Natieplein 2
1008 Brussel
Tel. : 02/ 549 81 60
Fax : 02/549 82 74
www.deKamer.be
e-mail : alg.zaken@deKamer.be

Publications officielles éditées par la Chambre des représentants
Commandes :
Place de la Nation 2
1008 Bruxelles
Tél. : 02/ 549 81 60
Fax : 02/549 82 74
www.laChambre.be
e-mail : aff.generales@laChambre.be

MEMORIE VAN TOELICHTING

DAMES EN HEREN,

1. **Algemene context**

Meer en meer worden rechtshandelingen wereldwijd en ook in ons land via elektronische weg verricht. De informatica- en telecommunicatietechnologieën creëren, zowel in de private als in de publieke sector, mogelijkheden om sneller en efficiënter te werken. Contracten kunnen worden opgemaakt aan de hand van een computer en vervolgens via netwerken ter goedkeuring doorgestuurd naar de contracterende partij, waarna ze in een elektronische vorm kunnen worden opgeslagen. Zo is er heel wat minder plaats nodig om ze te archiveren en kunnen ze sneller worden geraadpleegd.

Het is inderdaad zo dat de zakenwereld reeds geruime tijd telematische systemen aanwendt voor de automatisering van bepaalde juridische transacties, EDI genaamd (*Electronic Data Interchange*). De bankwereld heeft eveneens een interbancair net opgericht, Isabel, dat het de klanten mogelijk maakt om elektronisch te bankieren en te communiceren met andere gebruikers van het Isabelnet. Het gaat hier evenwel om gesloten netwerken, die uiterst beveiligd zijn en waarvan de gebruikers voorafgaand en fysiek zijn geïdentificeerd. Daarenboven zijn het netwerken waarbij de partijen de kans hebben mekaar op voorhand te ontmoeten om een contract op papier te ondertekenen zodat het juridisch stelsel voor de toekomstige transacties kan worden vastgelegd. Met de nieuwe toepassingen wordt die voorafgaande ontmoeting steeds minder mogelijk. Dit ligt namelijk niet voor de hand als transacties met een handelaar slechts sporadisch plaatsvinden. Ze is nog minder waarschijnlijk wanneer de transactie gebeurt via een open netwerk, zoals het Internet, dat het voordeel biedt vlug en op afstand te kunnen communiceren, zonder voorafgaande fysieke ontmoeting. Welnu, die transacties worden steeds talrijker : het is mogelijk reizen te boeken en kleding, *software*, boeken en zelfs wagens en aandelen te bestellen via het Internet. In de toekomst zouden tevens talrijke raadplegingen mogelijk worden via het netwerk. Op administratief vlak kan het voor een privé-persoon of een onderneming interessant zijn de belastingaangifte elektronisch te versturen. Hetzelfde geldt voor de aangiften die naar de RSZ ([1]) moeten worden gestuurd en, in het algemeen, voor alle soorten betrekkingen met de administratie (aanvraag van stede-

EXPOSÉ DES MOTIFS

MESDAMES, MESSIEURS,

1. **Contexte général**

Dans le monde et notamment dans notre pays, de plus en plus d'actes juridiques sont accomplis par voie électronique. Les technologies de l'informatique et des télécommunications créent, tant dans le secteur privé que dans le secteur public, des possibilités permettant de travailler plus vite et plus efficacement. Des contrats peuvent être établis au moyen d'un ordinateur et ensuite être transmis pour approbation au contractant par le biais de réseaux, après quoi ils pourront être stockés sous une forme électronique. Ils occuperont ainsi un espace d'archivage moins important et pourront être consultés plus rapidement.

Il est vrai que le monde des affaires a déjà intégré depuis un certain temps des systèmes télématiques permettant d'effectuer automatiquement certaines transactions juridiques, appelés EDI (*Electronic Data Interchange*). Le monde bancaire a également mis en place un réseau interbancaire, Isabel, qui permet notamment aux clients d'effectuer des transactions bancaires par voie électronique et de communiquer avec d'autres utilisateurs du réseau Isabel. Mais il s'agit ici de réseaux fermés, fortement sécurisés, dont les utilisateurs sont préalablement et physiquement identifiés et surtout dans lesquels les parties ont l'occasion de se rencontrer auparavant pour signer un contrat papier en vue notamment de fixer le régime juridique qui s'appliquera aux transactions futures. Avec les nouvelles applications, cette rencontre préalable est de moins en moins possible. En effet, elle s'envisage difficilement lorsque l'on ne passe une transaction avec un commerçant que de manière sporadique. Elle s'envisage encore moins lorsque la transaction s'effectue par le biais d'un réseau ouvert, tel Internet, dont l'intérêt est justement de pouvoir communiquer rapidement et à distance, sans rencontre physique préalable. Or, ces transactions sont de plus en plus fréquentes : il est possible de réserver des voyages, de commander des livres, des vêtements, des logiciels, voire des voitures et des actions par le biais d'Internet. D'une manière plus prospective, de nombreuses consultances pourraient également s'opérer par le réseau. Sur le plan administratif, un particulier ou une entreprise peuvent être intéressés par l'envoi de leur déclaration au bureau des contributions par un moyen électronique. Il en est de même pour les déclarations à

bouwkundige vergunningen, verzoek om allerhande machtigingen, …).

Een belangrijke hinderpaal bij de ontwikkeling van de zopas geschetste toepassingen is het gebrek aan een juridische regeling betreffende de digitale handtekening. De Europese Unie en talrijke landen zijn zich ervan bewust dat de wetgeving, die wordt toegepast als niets anders overeengekomen is, soms een rem vormt voor de ontwikkeling van elektronische transacties. Zo hebben veel juridische handelingen, die elektronisch worden verricht, zelden of nooit bewijskracht, want het merendeel van de rechters eist nog steeds een met de hand ondertekend document of papier.

Op het ontbreken van een dergelijke regeling in de Lidstaten van de Europese Unie werd onder meer gewezen in twee Mededelingen van de Europese Commissie (COM(97)157 : Naar een Europees initiatief betreffende het elektronisch handelsverkeer, Mededeling van de Commissie aan het Europees Parlement, de Raad, het Economisch en Sociaal Comité en het Comité van de Regio's, 15 april 1997, § 36), (COM(97)503 : Naar een Europees kader voor numerieke handtekeningen en encryptie. Zorgen voor veiligheid van en vertrouwen in elektronische communicatie. Mededeling van de Commissie aan het Europees Parlement, de Raad, het Economisch en Sociaal Comité en het Comité van de Regio's, 8 oktober 1997). Op 1 december 1997 heeft de Raad die laatste mededeling gunstig onthaald en de Commissie verzocht om zo spoedig mogelijk een voorstel van richtlijn voor te leggen aan het Europees Parlement en aan de Raad betreffende de numerieke handtekeningen. Op 16 juni 1998 heeft de Europese Commissie een eerste voorstel van richtlijn voorgelegd betreffende een gemeenschappelijk kader voor de elektronische handtekeningen (2). Na enkele geanimeerde gesprekken werd een nieuwe versie voorgelegd aan de Europese Ministerraad van 22 april 1999, waarover op 28 juni 1999 (3) een gemeenschappelijk standpunt werd ingenomen. De wet, zoals hier voorgesteld, vormt een *omzetting* van dit gemeenschappelijk standpunt.

Ook op internationaal niveau wordt het probleem ernstig genomen. De Commissie van de Verenigde Naties voor het Internationaal Handelsrecht houdt zich namelijk bezig met de uitwerking van uniforme regels voor de elektronische handtekeningen (4).

De meerderheid van de staten van de Verenigde Staten hebben de jongste jaren een wetgeving over de juridische geldigheid en over het gebruik van elektronische handtekeningen uitgevaardigd. In de schoot van de Europese Unie hebben Duitsland (5) en Italië (6) reeds een wet op dit vlak goedgekeurd. Vergelijkbare wetsontwerpen worden voorbereid in andere lidstaten (Nederland, Oostenrijk, Luxemburg (7), Denemarken en Frankrijk).

envoyer à l'ONSS (1), et d'une manière générale, pour tout type de relation avec l'administration (introduction du permis d'urbanisme, demande d'autorisations diverses, …).

L'absence de réglementation juridique en matière de signature électronique constitue un obstacle au développement des applications précitées. L'Union européenne ainsi que de nombreux États ont pris conscience que la législation s'appliquant par défaut, c'est-à-dire en l'absence de convention contraire, constitue parfois un frein au développement de transactions électroniques. Il est par exemple encore difficile, voire impossible, de prouver un grand nombre d'actes juridiques passés par voie électronique car la plupart des juges exigent toujours un écrit papier signé manuscritement.

Deux communications de la Commission européenne ont souligné l'absence de pareille réglementation au sein des États membres de l'Union européenne (COM(97)157 : Vers une initiative européenne en matière de commerce électronique, Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social et au Comité des Régions, 15 avril 1997, § 36), (COM(97)503 : Vers un Cadre européen pour les signatures numériques et le chiffrement : Assurer la sécurité et la confiance dans la communication électronique, Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social et au Comité des Régions, 8 octobre 1997). Le 1er décembre 1997, le Conseil a accueilli favorablement cette dernière communication et a invité la Commission à soumettre dès que possible une proposition de directive au Parlement européen et au Conseil sur les signatures numériques. Le 16 juin 1998, la Commission européenne a présenté une première proposition de directive sur un cadre commun pour les signatures électroniques (2). Suite aux quelques discussions animées, une nouvelle version a été présentée au Conseil des ministres européen du 22 avril 1999 et a fait l'objet d'une position commune le 28 juin 1999 (3). Le projet de loi, ici proposé, constitue une *transposition* de cette position commune.

La question est également prise très au sérieux au niveau international. En effet, la Commission des Nations Unies pour le Droit commercial international (CNUDCI) travaille sur l'élaboration de règles uniformes pour les signatures électroniques (4).

Au cours des dernières années, la majorité des états des États-Unis ont édicté une législation concernant la valeur juridique et l'usage des signatures électroniques. Au sein de l'Union européenne, l'Allemagne (5) et l'Italie (6) ont déjà adopté une loi dans ce domaine. Des projets de loi comparables sont en préparation dans d'autres États Membres (Pays-Bas, Autriche, Luxembourg (7), Danemark, France).

In België werden er initiatieven genomen om de juridische erkenning ([8]) van de elektronische handtekening te garanderen. De Ministerraad heeft immers op 12 juni 1998 in eerste lezing twee voorontwerpen van wet in die zin goedgekeurd. Het eerste is gericht op de wijziging van sommige bepalingen van het Burgerlijk Wetboek inzake het bewijs van de verbintenissen. Het tweede wenst een juridische regeling in te voeren, die kan worden toegepast op de activiteiten van de erkende certificatie-autoriteiten bij gebruik van digitale handtekeningen.

Naast het verzoek om advies van de sectie wetgeving van de Raad van State werden beide teksten besproken in de schoot van Agora 98 ([9]), officieel discussieforum inzake de informatiemaatschappij in België, opgericht op initiatief van de toenmalige minister van Economische Zaken ([10]).

Die besprekingen hebben geleid tot een degelijk verslag en tot aanbevelingen aan de minister ([11]). De Ministerraad van 26 maart 1999 heeft het ontwerp betreffende de certificatie-autoriteiten in tweede lezing goedgekeurd. Het werd evenwel niet ingediend bij de Kamer voor de ontbinding ervan. Het proefontwerp daarentegen werd op 14 april 1999 ([12]) ingediend bij het Parlement.

Al deze initiatieven hebben tot doel de onzekerheid over het juridisch statuut van elektronische handtekeningen weg te nemen en zodoende de ontwikkeling van het elektronisch rechtsverkeer in de private en de publieke sector te bevorderen. Vanzelfsprekend kan ons land hierin niet achterblijven.

Om verschillende redenen is het noodzakelijk dat in België op korte termijn een juridisch kader wordt geschapen voor het gebruik van elektronische handtekeningen en de activiteiten van de certificatiedienstverleners. De belangrijkste redenen zijn de volgende :

— het gebrek aan een juridisch kader is een belangrijke rem op de ontwikkeling van elektronische diensten in ons land;

— een juridisch kader is eveneens noodzakelijk om een betere bescherming van de consument, en meer in het algemeen van de zwakke partij, die steeds meer in contact komt met de nieuwe informatie- en communicatietechnologie, te waarborgen. Dit fenomeen breidt zich de jongste maanden trouwens uit doordat er *providers* op de markt verschijnen die gratis toegang verlenen;

— de introductie van telematica in de overheidssector wordt afgeremd door de onzekerheid over het statuut van de elektronische handtekening in administratieve procedures;

— uiteenlopende initiatieven om het gebruik van een elektronische handtekening (en meestal de digitale

En Belgique, des initiatives ont été prises afin d'assurer une reconnaissance juridique de la signature électronique ([8]). En effet, le 12 juin 1998, le Conseil des ministres a adopté, en première lecture, deux avant-projets de loi allant dans ce sens. Le premier vise à modifier certaines dispositions du Code civil relatives à la preuve des obligations. Le second vise à mettre en place un régime juridique applicable aux activités des autorités de certification agréées, et cela dans le cadre de l'utilisation de signatures digitales.

En sus de la demande d'avis de la section de législation du Conseil d'État, ces deux textes ont été discuté au sein d'Agora 98 ([9]), forum de discussion officiel à propos de la société de l'information en Belgique, créé à l'initiative du ministre des Affaires économiques d'alors ([10]). Ces discussions ont débouché sur un rapport de grande qualité et sur des recommandations remises au ministre ([11]).

Le projet sur les autorités de certification a été adopté en seconde lecture par le Conseil des ministres du 26 mars 1999. Il n'a toutefois pas été déposé devant la Chambre avant sa dissolution. Par contre, le projet preuve a été déposé au Parlement le 14 avril 1999 ([12]).

Toutes ces initiatives ont pour objectif d'éliminer l'insécurité liée au statut juridique des signatures électroniques, afin de promouvoir l'accomplissement d'actes juridiques par voie électronique dans les secteurs privé et public. Notre pays ne peut évidemment se laisser distancer dans ce domaine.

Il est nécessaire pour diverses raisons que soit créé à court terme en Belgique un cadre juridique pour l'emploi de signatures électroniques et les activités des prestataires de service de certification. Les raisons les plus importantes sont les suivantes :

— l'absence de cadre juridique constitue un frein important au développement de services électroniques dans notre pays;

— un cadre juridique est également nécessaire pour assurer une meilleure protection du consommateur et d'une manière plus générale de la partie faible, qui est de plus en plus en contact avec les nouvelles technologies en matière d'information et de communication. Ce phénomène est d'ailleurs amplifié ces derniers mois par l'apparition sur le marché de fournisseurs d'accès gratuits;

— l'introduction de la télématique dans le secteur public est ralentie par l'incertitude relative au statut de la signature électronique dans les procédures administratives;

— des initiatives divergentes visant à permettre l'emploi d'une signature électronique (et le plus souvent, la

handtekening gebaseerd op de asymmetrische cryptografie) voor beperkte toepassingen mogelijk te maken, zullen op korte termijn leiden tot wildgroei en onderlinge incompatibiliteit;

— het is noodzakelijk aan te sluiten bij het koninklijk besluit van 16 oktober 1998 (« houdende bepalingen betreffende de elektronische handtekening, geldend voor de sociale zekerheid, met toepassing van artikel 38 van de wet van 26 juli 1996 tot modernisering van de sociale zekerheid en tot vrijwaring van de leefbaarheid van de wettelijke pensioenstelsels », *Belgische Staatsblad* van 7 november 1998), dat een voorlopig systeem van elektronische handtekening invoert voor de sociale zekerheid. Het beperkt zich namelijk tot de sociale zekerheid, terwijl de elektronische handtekening in talrijke andere sectoren wordt gebruikt. Vervolgens wijst de commentaar van het koninklijk besluit er duidelijk op dat het om een voorlopig systeem gaat, waartoe werd besloten in afwachting van een algemene juridische oplossing. Ten slotte blijkt het koninklijk besluit duidelijk in strijd met artikel 3, 7° van het voorstel van richtlijn dat bepaalt dat « de lidstaten voor het gebruik van elektronische handtekeningen in de openbare sector eventuele aanvullende eisen kunnen stellen, voor zover die objectief, transparant, evenredig en niet-discriminerend zijn ». Vanzelfsprekend voldoet het koninklijk besluit niet aan deze voorwaarden daar noch de procedure, noch de accreditatievoorwaarden zijn vastgelegd.

De voorgestelde wet wenst een duidelijk antwoord te verschaffen op de grote juridische onzekerheid en onveiligheid, inzonderheid door de nauwkeurige omschrijving van de accreditatievoorwaarden. Het steunt grotendeels op het gemeenschappelijk standpunt over het voorstel van richtlijn betreffende de elektronische handtekeningen en neemt de grote principes van die tekst over (technologische neutraliteit, vrijwillig accreditatiesysteem, juridisch gevolg van de elektronische handtekening enz.).

2. **Elektronische handtekening en certificatiedienstverlener**

De specialisten gaan er over het algemeen mee akkoord dat het begrip *elektronische handtekening* een algemeen begrip is waaronder verscheidene technische mechanismen vallen die als handtekeningen kunnen worden beschouwd, voor zover zij, apart of in combinatie met andere elementen, het mogelijk maken bepaalde functies te verwezenlijken (identificatie van de auteur van de akte, uiting van instemming met de inhoud van de akte enz.) die essentieel zijn voor deze juridische instelling ([13]). Deze mechanismen kunnen in verscheidene categorieën worden gegroepeerd : de gedi-

signature digitale basée sur la cryptographie asymétrique) dans des applications limitées risquent d'être adoptées et mener à court terme, à une prolifération incontrôlée et à des incompatibilités;

— il est nécessaire de prendre le relais de l'arrêté royal du 16 octobre 1998 (« portant des dispositions relatives à la signature électronique, qui s'applique à la sécurité sociale, en application de l'article 38 de la loi du 26 juillet 1996 portant modernisation de la sécurité sociale et assurant la viabilité des régimes légaux des pensions », *Moniteur belge* du 7 novembre 1998) qui met en place un système provisoire de signature électronique pour la sécurité sociale. En effet, celui-ci se limite au secteur de la sécurité sociale alors que la signature électronique est utilisée dans de nombreux autres secteurs. Ensuite, le commentaire de l'arrêté royal indique clairement que le système est provisoire et pris dans l'attente d'une solution juridique globale. Enfin, l'arrêté royal paraît contraire à l'article 3, 7° de la proposition de directive qui stipule que « Les États membres peuvent soumettre l'usage des signatures électroniques dans le secteur public à des exigences supplémentaires pour autant que ces dernières soient objectives, transparentes, proportionnées et non discriminatoires » dans la mesure où il ne fixe ni la procédure ni les conditions de l'accréditation ne sont fixées.

Le projet de loi proposé entend apporter une réponse claire à ces différentes incertitudes et insécurités juridiques notamment en fixant de manière précise les conditions d'accréditation. Il s'inspire globalement de la position commune sur la proposition de directive sur les signatures électroniques et reprend les grands principes de ce texte (neutralité technologique, système volontaire d'accréditation, effet juridique de la signature électronique, etc.).

2. **Signature électronique et prestataire de service de certification**

Les spécialistes s'accordent généralement pour considérer que le terme de *signature électronique* désigne une notion générique englobant divers mécanismes techniques méritant d'être tenus pour des signatures dans la mesure où ils permettent, à eux seuls ou en combinaison, de réaliser certaines fonctions essentielles (identification de l'auteur de l'acte, manifestation du consentement au contenu de l'acte, etc.) à cette institution juridique ([13]). Ces mécanismes peuvent être regroupés en plusieurs catégories : la signature manuscrite numérisée, la signature biométrique, le code secret as-

gitaliseerde met de hand geplaatste handtekening, de biometrische handtekening, de geheime code gekoppeld aan het gebruik van een kaart, de digitale (of numerieke) handtekening en andere toekomstige mechanismen.

Overeenkomstig het voorstel van de richtlijn blijft dit ontwerp neutraal op het vlak van de technologie. De definities zijn immers zo ruim mogelijk om zich niet te beperken tot een bijzondere techniek van de elektronische handtekening. Er moet echter worden vastgesteld dat de technologische neutraliteit van deze definitie slechts mogelijk is als er geen twijfel over bestaat dat thans enkel de techniek van de digitale (of numerieke) handtekening, gesteund op de asymmetrische encryptie, beantwoordt aan de definitie van de geavanceerde elektronische handtekening, vermeld in dit wetsontwerp ([14]). De inhoud van de bijlagen laat hierover geen enkele onzekerheid bestaan. Bovendien is de digitale handtekening voor het ogenblik de meest ontwikkelde techniek, die zich opdringt op de markt en die de meeste waarborgen biedt voor de uitwisseling van gegevens op een open netwerk.

Om die redenen en zonder de andere mechanismen van de elektronische handtekening ([15]) te willen verwaarlozen, lijkt het belangrijk om in enkele woorden het mechanisme van de digitale handtekening uiteen te zetten, hoe het werkt en de rol die de certificatiedienstverlener speelt bij het gebruik ervan.

2.1. *De digitale handtekening*

De digitale handtekening steunt op de asymmetrische encryptie, de zogenaamde « publieke sleutel ».

Dit mechanisme van handtekeningen beantwoordt ongetwijfeld aan de definitie van de geavanceerde elektronische handtekening in de zin van het voorstel van richtlijn en in de zin van deze wet.

In een systeem van publieke sleutel veronderstelt de realisatie van de identificeringsfunctie dat een persoon beschikt over twee complementaire wiskundige sleutels : een private sleutel, (eveneens gennaamd « gegevens voor het aanmaken van een handtekening ») waarvan het geheime karakter ook effectief moet bewaard blijven, en een publieke sleutel, (eveneens genaamd « gegevens voor het verifiëren van een handtekening ») die vrij kan worden verdeeld. De publieke sleutel is zodanig opgesteld dat hij gemakkelijk op basis van de corresponderende private sleutel te berekenen is en het materieel onmogelijk is de private sleutel af te leiden van de publieke sleutel. Daarom moet de publieke sleutel een onomkeerbare functie vertegenwoordigen van de private sleutel. Met de private sleutel kan een boodschap worden ondertekend. De decodering gebeurt dan volsocié à l'utilisation d'une carte, la signature digitale (ou numérique) et autres mécanismes futurs.

Conformément à la proposition de directive, ce projet adopte une approche neutre sur le plan de la technologie. En effet, les définitions se veulent le plus large possible afin de ne pas se limiter à une technique particulière de signature électronique. Toutefois, force est de constater que la neutralité technologique de cette définition n'est que potentielle dans la mesure où il ne fait pas de doute qu'actuellement, seule la technique de signature digitale (ou numérique), fondée sur la cryptographie asymétrique, répond à la définition de la signature électronique avancée reprise dans ce projet de loi ([14]). Le contenu des annexes ne laisse planer aucune incertitude à ce sujet. De plus, la signature digitale constitue pour l'instant la technique la plus mûre, qui s'impose sur le marché et qui présente le plus haut degré de sécurité pour les échanges de données en réseau ouvert.

Pour ces raisons et sans vouloir écarter les autres mécanismes de signature électronique ([15]), il apparaît important d'expliquer en quelques mots le mécanisme de signature digitale, la manière dont il fonctionne et le rôle que joue le prestataire de service de certification dans l'utilisation de celui-ci.

2.1. *La signature digitale*

La signature digitale est fondée sur la cryptographie asymétrique, dite « à clé publique ».

Sans conteste, ce mécanisme de signature répond à la définition de signature électronique avancée au sens de la proposition de directive ainsi que de ce projet de loi.

Dans un système à clé publique, la réalisation de la fonction d'identification suppose qu'une personne dispose de deux clés mathématiques complémentaires : une clé privée (aussi appelée données afférentes à la création de signature), dont le caractère secret doit effectivement être préservé, et une clé publique (aussi appelée données afférentes à la vérification de signature), qui peut être librement distribuée. La clé publique est une fonction telle de la clé privée qu'il doit être aisé de calculer la clé publique à partir de la clé privée et matériellement impossible de déduire de la clé publique la clé privée correspondante. La clé publique doit dès lors représenter une fonction irréversible de la clé privée. La clé privée permet de signer le message. L'opération de décodage s'effectue, quant à elle, selon le principe de la complémentarité des clés : un message en-

gens het principe van de complementariteit van de sleutels : een boodschap die werd gecodeerd met een private sleutel kan enkel worden gedecodeerd met de overeenkomstige publieke sleutel.

Het volgende voorbeeld toont aan hoe de digitale handtekening werkt.

Alice wil een elektronisch ondertekend computerbericht sturen naar Marc. Na het schrijven ervan zal Alice eerst door middel van een wiskundige bewerking het bericht comprimeren. Het comprimeren is het resultaat van een onomkeerbare zogenaamde « *hash-code* »-techniek. Deze functie maakt het mogelijk op beknopte wijze een keten van gegevens te genereren die de boodschap in kwestie vertegenwoordigt. Deze vertegenwoordiging is veilig, zeer precies en biedt de mogelijkheid elke verandering op te sporen die in de boodschap werd aangebracht. Het volstaat immers dat de bestemmeling het « *hash-code* » programma toepast op het ontvangen bericht en het aldus verkregen gecomprimeerd bestand vergelijkt met hetgeen door de afzender wordt verstuurd. Elk verschil tussen de gecomprimeerde bestanden betekent dat de boodschap tijdens de verzending werd gewijzigd.

Dit gecomprimeerd bestand wordt vervolgens gecodeerd (onleesbaar en ontoegankelijk gemaakt) met behulp van de private sleutel van Alice. Dit gecodeerd gecomprimeerd bestand is de digitale handtekening. Daarna stuurt Alice haar boodschap naar Marc (in klare tekst) samen met de digitale handtekening.

Wanneer Marc de boodschap samen met de digitale handtekening ontvangt, decodeert hij deze laatste met behulp van een wiskundige bewerking met de bijbehorende publieke sleutel van Alice. Als hij de handtekening kan decoderen, is Marc er zeker van dat deze vooraf werd gemaakt met de bijbehorende private sleutel van Alice : hij weet dan ook met zekerheid dat zij de auteur is van deze boodschap indien een derde partij (een certificatiedienstverlener eveneens genoemd een certificatie-autoriteit) erkent dat deze publieke sleutel wel degelijk Alice toebehoort. Dankzij de « *hash-code* » techniek is hij er ook van verzekerd dat aan de boodschap van Alice niets werd gewijzigd.

Wij willen er wel de aandacht op vestigen dat het comprimeren van de boodschap met behulp van een onomkeerbare « *hash-code* » techniek niet noodzakelijk is. De afzender van de boodschap kan immers de boodschap rechtstreeks coderen met behulp van zijn private sleutel zonder deze eerst te comprimeren. Nochtans wordt de functie van de onomkeerbare « *hash-code* » techniek vaak gebruikt om technische redenen en om tijd te winnen : het gaat immers vlugger een gecomprimeerd bestand (kleiner bestand) te versleutelen dan een bestand in klare tekst te coderen (groter bestand).

Wij stellen vast dat de certificatiedienstverlener een belangrijke rol speelt en dat men zich moeilijk het gecodé avec une clé privée ne peut être décodé qu'avec sa clé publique complémentaire.

L'exemple suivant illustre le fonctionnement de la signature digitale.

Alice désire envoyer à Marc un message informatisé signé de façon électronique. Après avoir écrit son message, Alice réalise un condensé de ce message au moyen d'une opération mathématique. Ce condensé est le résultat d'une fonction appelée fonction de hachage irréversible. Cette fonction permet de générer de façon concise une chaîne de données qui représente le message en question. Cette représentation est sécuritaire, très précise et permet de détecter tout changement apporté au message. En effet il suffit au destinataire d'appliquer la fonction de hachage au message reçu et de comparer le condensé ainsi obtenu avec celui transmis par l'émetteur. Toute différence entre les condensés signifie que le message a été altéré en cour de transmission.

Ce condensé est par la suite encodé (rendu illisible et inaccessible) à l'aide de la clé privée d'Alice. Ce condensé encodé constitue la signature digitale. Alice envoie alors à Marc son message (en clair) accompagné de la signature digitale.

Lorsque Marc reçoit le message et la signature digitale, il décode cette dernière en effectuant une opération mathématique impliquant la clé publique complémentaire d'Alice. S'il parvient à décoder la signature, Marc est assuré que celle-ci a préalablement été réalisée avec la clé privée complémentaire d'Alice : il sait alors de manière certaine qu'elle est l'auteur du message pour autant qu'un partie tierce (un prestataire de service de certification, aussi appelée autorité de certification) certifie que cette clé publique est bien celle d'Alice. Grâce à la fonction de hachage, il est par ailleurs assuré de l'intégrité du message d'Alice.

Remarquons toutefois que la réalisation d'un condensé du message à l'aide de la fonction de hachage irréversible n'est pas indispensable. En effet l'émetteur du message pourrait directement encoder le message avec sa clé privée sans nécessairement passer par la production du condensé. Néanmoins la fonction de hachage irréversible sera souvent utilisée pour des raisons techniques et dans un souci de gagner du temps : encoder avec la clé privée un condensé (fichier de petite taille) est plus rapide que l'encodage du message en clair (fichier de plus grosse taille).

On constate que le prestataire de service de certification joue un rôle important et que l'utilisation de la

bruik van een digitale handtekening kan voorstellen zonder zijn toedoen.

2.2. *De rol van de certificatiedienstverlener*

De belangrijkste rol van een certificatiedienstverlener in het kader van het gebruik van een digitale handtekening bestaat erin in te staan voor het formeel verband tussen de persoon en zijn publieke sleutel. Dit verband zal worden bevestigd in een digitaal certificaat afgegeven door deze dienstverlener.

Dit certificaat bevat tevens allerlei informatie betreffende onder andere de identiteit van de houder van het certificaat (diegene die wil tekenen en zich aldus wil identificeren), zijn publieke sleutel en betreffende de identiteit van de certificatiedienstverlener. Dit certificaat wordt aangemaakt en ondertekend door de certificatiedienstverlener met behulp van zijn eigen private sleutel en is, als dusdanig, beschermd tegen wijzigingen.

Het volgende voorbeeld toont het mogelijke gebruik aan van certificaten. Alice stuurt Marc een boodschap samen met haar digitale handtekening die werd opgemaakt met behulp van haar private sleutel. Na ontvangst van de documenten verifieert Marc eerst het certificaat (dat hij ofwel heeft ontvangen van Alice, ofwel heeft opgezocht in het register van certificaten) met behulp van de publieke sleutel van de certificatiedienstverlener. Indien de verificatie positief is, is hij zeker van de integriteit van de informatie opgenomen in het certificaat, dit wil zeggen de identiteit van Alice, van haar publieke sleutel en van de identiteit van de certificatiedienstverlener. Hij kan daarna de publieke sleutel van Alice gebruiken om de handtekening van haar boodschap te verifiëren.

Er valt op te merken dat zo de afgifte van het certificaat de belangrijkste functie van de certificatiedienstverlener vormt, deze laatste eveneens andere diensten kan bieden, met name inzake registratie, registratieklokken, registers, informatica of adviezen die verband houden met de elektronische handtekeningen.

Zoals men kan zien, is de rol van de certificatiedienstverlener niet onbelangrijk. Hij moet een infrastructuur tot stand brengen om in alle veiligheid de informatie te verzamelen en de integriteit ervan te verzekeren. De doeltreffendheid van het identificatieproces is een bepalend element waarvan de verantwoordelijkheid van de certificatiedienstverlener afhangt.

Daarom en overeenkomstig het voorstel van Europese richtlijn zullen de activiteiten van de certificatiedienstverleners in bepaalde gevallen en in zekere mate moeten worden gereglementeerd.

signature digitale s'envisage difficilement sans son intervention.

2.2. *Le rôle du prestataire de service de certification*

La principale fonction d'un prestataire de service de certification dans le cadre de l'utilisation d'une signature digitale est d'assurer un lien formel entre une personne et sa clé publique. Ce lien sera confirmé dans un certificat digital émis par ce prestataire.

Ce certificat contient ainsi différentes informations relatives notamment à l'identité du titulaire du certificat (celui qui veut signer et s'identifier comme tel), sa clé publique et relatives à l'identité du prestataire de service de certification. Le certificat est créé et signé par le prestataire de service de certification à l'aide de sa propre clé privée et est, de ce fait, protégé contre les altérations.

L'exemple suivant illustre l'utilisation possible de certificats. Alice transmet à Marc un message ainsi que sa signature digitale réalisée à l'aide de sa clé privée. Après avoir reçu ces documents, Marc commence par vérifier le certificat (qu'il aura soit reçu d'Alice soit été chercher dans un annuaire électronique de certificats) à l'aide de la clé publique du prestataire de service de certification. Si la vérification s'avère concluante, il est assuré de l'intégrité des informations contenues dans le certificat, soit l'identité d'Alice, de sa clé publique ainsi que de l'identité du prestataire. Il peut ensuite utiliser la clé publique d'Alice pour vérifier la signature du message transmis par celle-ci.

Notons que si la délivrance de certificat constitue la fonction principale du prestataire de service de certification, celui-ci peut également offrir d'autres services tels que services d'enregistrement, les services horodateurs, les services d'annuaires, les services informatiques ou les services de consultation liée aux signatures électroniques.

On le voit, le rôle du prestataire de service de certification n'est pas minime. Il doit mettre en place une infrastructure qui permette de collecter et d'assurer l'intégrité des informations en toute sécurité. L'efficacité du processus d'identification représente un élément déterminant dont la responsabilité du prestataire de service de certification dépendra.

Pour ces raisons et conformément à la proposition de directive européenne, les activités des prestataires de service de certification doivent, dans certains cas et dans une certaine mesure, être réglementées.

3. Krachtlijnen van de wet

Het huidige wetsontwerp omvat vijf hoofdstukken. Het eerste bevat definities en bepaalt de doelstelling en het toepassingsgebied van de wet. Het tweede legt de algemene principes vast. Het derde legt het juridisch stelsel vast dat van toepassing is op de certificatiedienstverleners. Het maakt hierbij een onderscheid enerzijds tussen de verplichtingen van de geaccrediteerde certificatiedienstverleners en anderzijds die van de al of niet geaccrediteerde certificatiedienstverleners. Het vierde hoofdstuk is gewijd aan de verplichtingen van de gebruikers van het certificaat. Het vijfde en laatste hoofdstuk handelt over de controle op de certificatiedienstverleners en de sancties.

De krachtlijnen van dit wetsontwerp steunen op die welke zijn voorgeschreven door het voorstel van richtlijn inzake de elektronische handtekeningen.

3.1. *Doelstelling van de wet*

De belangrijkste doelstelling van dit wetsontwerp bestaat erin de veiligheid van en het vertrouwen in het gebruik van de digitale handtekening te versterken en een juridische erkenning ervan te waarborgen. Het systeem wil voldoende flexibel zijn om te beantwoorden aan de vraag van de markt maar tegelijkertijd strikte criteria vastleggen om een hoge graad van bescherming te bieden.

Vooral in de open netwerken wordt de elektronische uitwisseling geremd door onzekerheden die inherent zijn aan het systeem : de berichten kunnen worden onderschept en gemanipuleerd, de geldigheid van documenten kan worden betwist, de identiteit van de afzender kan worden in vraag gesteld …

Een meer veilige omgeving is dus noodzakelijk voor een beter gebruik van commerciële en niet-commerciële mogelijkheden die worden geboden door elektronische communicatie via netwerken. Een geavanceerde elektronische handtekening gecombineerd met een certificatie, afgegeven door een certificatiedienstverlener, vertegenwoordigt een voldoende erkende techniek om de veiligheid van en het vertrouwen in de netwerken te garanderen. Nochtans kan dit doel enkel worden bereikt indien de gebruikers van de geavanceerde elektronische handtekeningen vertrouwen hebben in het gebruik ervan en in de certificatiedienstverleners.

Het vastleggen van een duidelijk juridisch kader dat de rechten en plichten van de daaraan onderworpen certificatiedienstverleners bepaalt, is een manier waarop dit vertrouwen kan worden gecreëerd en versterkt. Daarenboven zal een geavanceerde elektronische handtekening een grotere juridische waarde verkrijgen indien zij wordt gecombineerd met een certificaat uitgegeven door een geaccrediteerde certificatiedienstverlener. Terzelfder tijd wordt evenwel, overeenkomstig artikel 5, 2°

3. Lignes directrices du projet de loi

Le présent projet de loi comporte cinq chapitres. Le premier contient des définitions et détermine l'objectif et le champ d'application de la loi. Le second fixe les principes généraux. Le troisième établit le régime juridique applicable aux prestataires de service de certification en distinguant d'une part, les obligations qui sont à charge des prestataires de service de certification accrédités et d'autre part, celles qui sont à charge des prestataires de service de certification accrédités ou non. Le quatrième chapitre consacre les obligations à charge des utilisateurs de certificat. Le cinquième et dernier chapitre traite du contrôle des prestataires de service de certification et des sanctions.

Les lignes directrices de ce projet de loi s'inspirent de celles dictées par la proposition de directive sur les signatures électroniques.

3.1. *Objectif de la loi*

L'objectif principal de ce projet de loi est de renforcer la sécurité et la confiance dans l'utilisation de la signature électronique avancée ainsi que d'assurer une reconnaissance juridique de celle-ci. Le système adopté tend à être suffisamment souple afin de répondre à la demande du marché tout en adoptant des critères stricts pour offrir un niveau de protection élevé.

Surtout dans les réseaux ouverts, le développement des échanges électroniques est freiné par les incertitudes inhérentes à ces réseaux : les messages peuvent être interceptés et manipulés, la validité des documents peut être contestée, l'identité de l'émetteur peut être mis en cause, …

Un environnement plus sûr est donc nécessaire pour permettre un bon usage des possibilités commerciales et non commerciales offertes par la communication électronique sur les réseaux. La signature électronique avancée combinée à un certificat émis par un prestataire de service de certification constitue une technique largement reconnue pour assurer la sécurité et la confiance sur les réseaux. Toutefois, ce but ne peut être atteint que si les utilisateurs de signatures électroniques avancées peuvent avoir confiance dans l'utilisation de celles-ci ainsi que dans les prestataires de service de certification.

Un moyen de créer et de renforcer cette confiance est d'établir un cadre juridique clair qui détermine les droits et obligations des prestataires de service de certification qui y sont soumis. De plus, une plus grande valeur juridique sera accordée à une signature électronique avancée si elle est combinée à un certificat émis par un prestataire de service de certification accrédité, tout en reconnaissant néanmoins, et conformément à l'article 5, 2° de la proposition de directive, une certaine

van het voorstel van richtlijn, een bepaalde juridische waarde toegekend — een waarde die door de rechter moet worden beoordeeld — aan een al of niet geavanceerde elektronische handtekening die wordt gecombineerd met een certificaat afgegeven door een niet-geaccrediteerde certificatiedienstverlener.

3.2. *Een vrij accreditatiesysteem*

Overeenkomstig het voorstel van richtlijn brengt het wetsontwerp een vrijwillig systeem van accreditatie tot stand.

Het accreditatiesysteem is vrij. Een certificatiedienstverlener is dus niet verplicht een accreditatie aan te vragen om zijn activiteiten uit te oefenen. Hij kan aldus zijn diensten verlenen zonder voorafgaande machtiging. Op de markt kunnen dus geaccrediteerde en niet-geaccrediteerde certificatiedienstverleners bestaan.

Indien een certificatiedienstverlener een accreditatie wenst te bekomen, moet hij daartoe een aanvraag indienen bij het bestuur … De accreditatie zal enkel worden verleend indien de certificatiedienstverlener beantwoordt aan de accreditatievoorwaarden vastgelegd in of krachtens de wet, beoordeeld door het bestuur of een door haar aangeduide entiteit. Deze voorwaarden hebben tot doel een geheel aan vereisten te waarborgen die het vertrouwen moeten versterken in de certificatiedienstverleners die hieraan voldoen (erkende certificatiedienstverleners).

Zowel het verkrijgen als het behoud van de accreditatie is onderworpen aan de naleving van de door of krachtens de wet vastgelegde voorwaarden.

Het verkrijgen en het behoud van de accreditatie heeft tot gevolg dat de geaccrediteerde certificatiedienstverleners worden onderworpen aan bijkomende voorwaarden ten opzichte van die welke gelden voor het geheel van de certificatiedienstverleners (geaccrediteerd of niet).

Laten wij niet vergeten dat, ofschoon de bijkomende voorwaarden niet van toepassing zijn op de niet-geaccrediteerde certificatiedienstverleners, de rechter zich in geval van geschil toch op die bijkomende voorwaarden zal kunnen steunen, zonder ze echter te moeten toepassen.

3.3. *Een neutraal kader vanuit technologisch oogpunt*

In tegenstelling tot het eerste wetsontwerp en in overeenstemming met het voorstel van richtlijn is dit wetsontwerp niet meer beperkt tot het mechanisme van de digitale handtekening, gebaseerd op de asymmetrische cryptografie. Gelet op de snelheid van de technische vooruitgang en op het belang van Internet op wereldvlak, wordt in dit ontwerp immers gepoogd om rekening

valeur juridique, qui devra être appréciée par le juge, à une signature électronique avancée ou non et combinée à un certificat émis par un prestataire de service de certification non accrédité.

3.2. *Un système libre d'accréditation*

Conformément à la proposition de directive, le projet de loi met en place un système volontaire d'accréditation.

Le système d'accréditation est libre. Un prestataire de service de certification n'a donc pas l'obligation de demander une accréditation pour exercer ses activités et peut ainsi offrir ses services sans autorisation préalable. Dès lors, il peut coexister sur le marché des prestataires de service de certification accrédités et non accrédités.

Si un prestataire de service de certification désire obtenir une accréditation, il pourra introduire sa demande auprès de l'administration. L'accréditation ne sera accordée que si le prestataire de service de certification répond aux conditions d'accréditation stipulées par ou en vertu de la loi, et appréciées par l'administration ou une entité désignée par elle. Ces conditions ont pour objectif de garantir un ensemble d'impératifs de nature à accroître la confiance dans les prestataires de service de certification qui répondent à celles-ci (prestataires accrédités).

Comme pour l'obtention, le maintien de l'accréditation est également subordonné au respect des conditions fixées par ou en vertu de la loi.

L'obtention et le maintien de l'accréditation a pour conséquence de soumettre les prestataires de service de certification accrédités à des obligations supplémentaires de celles qui sont applicables à l'ensemble des prestataires de service de certification (accrédités ou non).

Notons que si les obligations supplémentaires ne s'appliquent pas aux prestataires de service de certification non accrédités, le juge pourra néanmoins en cas de litige s'inspirer de celles-ci sans qu'il ne soit cependant tenu de les appliquer.

3.3. *Un cadre neutre du point de vue de la technologie*

Contrairement au premier projet de loi et conformément à la proposition de directive, ce projet de loi ne se limite plus au mécanisme de signature digitale, fondé sur la cryptographie asymétrique. En effet, eu égard à la rapidité des progrès techniques et à la dimension mondiale d'Internet, ce projet adopte une approche qui essaye de prendre en compte les diverses technolo-

te houden met de verschillende actuele en toekomstige technologieën, die authentificatie van gegevens via elektronische weg mogelijk maken. Daarom zijn deze definities zo ruim mogelijk om zich niet te beperken en geen welbepaalde techniek van elektronische handtekening te bevoordelen, ook al weet men vandaag dat de digitale (of numerieke) handtekening de meest geschikte schijnt te zijn.

3.4. *Juridische erkenning van de geavanceerde elektronische handtekeningen*

De bedoeling van deze wet is enkel de juridische erkenning te waarborgen van sommige geavanceerde elektronische handtekeningen, namelijk dewelke die worden aangemaakt door een veilig middel voor het aanmaken van een handtekening en die gepaard gaan met een gekwalificeerd certificaat (dit wil zeggen met een bepaalde inhoud en afgegeven door een geaccrediteerde certificatiedienstverlener) (artikel 4, § 4). De juridische erkenning van de andere geavanceerde elektronische handtekeningen evenals van de (niet-geavanceerde) elektronische handtekeningen in de zin van artikel 2, 1) van het voorstel van richtlijn wordt gewaarborgd door het wetsontwerp (vgl. *supra*) betreffende het bewijsrecht waarbij een functionele definitie van de handtekening in het Burgerlijk Wetboek wordt ingevoerd.

Die twee wetsontwerpen zijn dus complementair. De combinatie van beide teksten maakt het mogelijk om de vereisten van artikel 5 van het voorstel van richtlijn in Belgisch recht om te zetten.

Teneinde inzicht te krijgen in de band tussen die twee teksten, dient te worden herinnerd aan het onderscheid dat bestaat tussen ontvankelijkheid, bewijswaarde en bewijskracht van een bewijsmiddel (in onderhavig geval van een ondertekend geschrift). Er moet een duidelijk onderscheid tussen deze drie begrippen worden gemaakt, want dat onderscheid zal aantonen hoe de twee respectieve wetsontwerpen een bijdrage leveren tot de erkenning van de elektronische handtekening.

De *ontvankelijkheid* is het « in aanmerking nemen door de rechter van bewijskrachtige elementen, die door de wet zijn toegelaten gelet op het voorwerp van het geschil » ([16]). Dat betekent dus niet dat het zogenaamde ontvankelijke element noodzakelijkerwijs enige invloed zal hebben op de beslissing van de rechter; hij kan uiteraard oordelen dat het bewuste element niets bewijst. Hij heeft maar een verplichting : het element in kwestie onderzoeken. Opdat er sprake van ontvankelijkheid zou zijn, moet er een wettelijk voorschrift in die zin zijn. In artikel 25, eerste lid van het Wetboek van Koophandel wordt bijvoorbeeld bepaald dat wat de handel betreft, het getuigenbewijs ontvankelijk is. In artikel 1341 van het Burgerlijk Wetboek daarentegen wordt

gies actuelles ou futures permettant d'authentifier des données par voie électronique. Ainsi, les définitions adoptées se veulent le plus large possible afin de ne pas se limiter et de ne pas privilégier une technique particulière de signature électronique, même si on sait qu'actuellement la signature digitale (ou numérique) semble la plus mûre.

3.4. *Reconnaissance juridique des signatures électroniques avancées*

Ce projet de loi se limite à assurer la reconnaissance juridique de certaines signatures électroniques avancées à savoir celles créées par un dispositif sécurisé de création de signature et combinées à un certificat qualifié (c'est-à-dire ayant un certain contenu et émis par un prestataire de service de certification accrédité) (article 4, § 4). La reconnaissance juridique des autres signatures électroniques avancées ainsi que des signatures électroniques (non avancées) au sens de l'article 2, 1) de la proposition de directive est assurée par le projet de loi (cf. *supra*) relatif au droit de la preuve qui introduit une définition fonctionnelle de la signature dans le Code civil.

Ces deux projets de loi sont donc complémentaires. C'est la combinaison de ces deux textes qui permet de transposer en droit belge les exigences de l'article 5 de la proposition de directive.

Afin de bien comprendre le lien entre ces deux textes, il convient de rappeler la distinction qui existe entre recevabilité, valeur probante et force probante d'un moyen de preuve (en l'occurrence ici d'un écrit signé). Ces trois notions sont à bien distinguer, car cette distinction va permettre de montrer en quoi les deux projets de loi respectifs constituent un apport quant à la reconnaissance de la signature électronique.

La *recevabilité* est la « prise en considération, par le juge, d'éléments probatoires déclarés admissibles par la loi eu égard à l'objet du litige » ([16]). Cela ne signifie donc pas que l'élément dit recevable aura forcément une influence sur la décision du juge; celui-ci peut parfaitement considérer que ledit élément ne prouve rien. Il n'a qu'une seule obligation : étudier l'élément en question. Pour qu'il y ait recevabilité, il faut qu'il y ait un prescrit légal allant dans ce sens. L'article 25, alinéa premier du Code de commerce déclare par exemple qu'en matière commerciale, la preuve testimoniale est recevable. À l'inverse, l'article 1341 du Code civil stipule que la preuve testimoniale est irrecevable lorsqu'existe un acte écrit. Ces deux exemples montrent les deux types

gesteld dat het bewijs door getuigen onontvankelijk is als er een geschreven akte bestaat. Deze twee voorbeelden illustreren de twee wettelijke voorschriften inzake ontvankelijkheid van bewijzen : het ene waarbij ontvankelijkheid wordt toegekend, het andere waarbij ze niet wordt toegelaten.

We hebben gezien dat een ontvankelijk bewijs de rechter niet noodzakelijkerwijs zal overtuigen. Het probleem van hoe de rechter te overtuigen is dan ook dat van de *bewijswaarde*. Als de rechter oordeelt dat het aangevoerde element het probleem dat hem is voorgelegd kan helpen oplossen, anders gezegd als hij vindt dat het element een betrouwbare weergave van de realiteit is, zegt men dat hij een bewijswaarde toekent aan het element. Het is pas vanaf het moment dat de rechter aan iets een bewijswaarde heeft toegekend dat echt van een bewijs kan worden gesproken. Elke redenering die hier tegen ingaat is absurd. Spreekt men van een bewijs aangaande een element waaraan de rechter geen bewijswaarde heeft toegekend, dan spreekt men van een bewijs dat niets bewijst.

Tot slot kent de wet soms zelf een *bewijskracht*, (die verschillende stadia heeft), toe aan elementen die als bewijs in aanmerking kunnen komen. De idee die aan de basis van die werkwijze ligt is inderdaad het hiërarchisch indelen van de verschillende wijzen van bewijslevering. Als twee contradictorische elementen, die aanspraak kunnen maken op het statuut van bewijs, met elkaar worden geconfronteerd, dan wordt datgene waaraan de wet de grootste bewijskracht hecht in aanmerking genomen. Zo heeft een geschreven stuk een grotere bewijskracht dan bijvoorbeeld die van een getuigenis ([17]). Die bewijskracht hangt logischerwijze af van de betrouwbaarheidsgraad die van een bewijsmethode kan worden verwacht. De wet zal enkel bewijskracht toekennen aan de bewijsmiddelen die een voldoende betrouwbaarheidsgraad bieden, want zo wordt de rechter zijn beoordelingsmacht ontnomen. Zo ontneemt de bewijskracht de beoordelingskracht van de rechter, terwijl de ontvankelijkheid veronderstelt dat de rechter de bewijswaarde van een bewijsmiddel nog moet beoordelen.

Heeft men het over juridische erkenning van de elektronische handtekening, dan moet hierbij nog worden gepreciseerd of het gaat om een gewone juridische ontvankelijkheid van het bewijs dan wel of de wet bewijskracht toekent. Om de band tussen de twee wetsontwerpen samen te vatten, kan worden gesteld dat het huidige ontwerp bewijskracht toekent aan de geavanceerde elektronische handtekeningen aangemaakt door een beveiligd middel voor het aanmaken van een handtekening en die gepaard gaan met een gekwalificeerd certificaat (artikel 4, § 4). Deze handtekeningen hebben dus dezelfde juridische gevolgen als de handgeschrede prescrits légaux en matière de recevabilité des preuves : l'une attribuant la recevabilité, l'autre la déniant.

Nous avons vu qu'une preuve recevable n'emporte pas forcément la conviction du juge. Cette question de la conviction du juge est celle de la *valeur probante*. Lorsque le juge considère que l'élément apporté peut aider à résoudre le problème qui se pose à lui, autrement dit lorsqu'il trouve que l'élément est une manifestation fiable de la réalité, on dit qu'il accorde à l'élément une valeur probante. Ce n'est qu'à partir du moment où le juge a accordé une valeur probante à quelque chose que l'on peut véritablement parler de preuve. Tout raisonnement contraire est absurde. Si l'on parle de preuve à propos d'un élément auquel le juge a dénié valeur probante, on parle d'une preuve qui ne prouve rien.

Enfin, la loi elle-même accorde parfois aux éléments susceptibles d'être des preuves une *force probante*, laquelle connaît plusieurs degrés. En effet, l'idée qui sous-tend ce procédé est de hiérarchiser les différents modes de preuve. Si deux éléments contradictoires pouvant prétendre au statut de preuve sont mis en présence, c'est celui auquel la loi attache la plus grande force probante qui sera pris en compte. Ainsi, un écrit a généralement une force probante supérieure à celle d'un témoignage par exemple ([17]). Cette force probante est très logiquement fonction du degré de fiabilité qu'on peut attendre d'un mode de preuve. Force probante ne sera reconnue par la loi qu'aux moyens de preuve qui offrent un degré de fiabilité suffisant car en se faisant on enlève le pouvoir d'appréciation du juge. Ainsi, la force probante enlève le pouvoir d'appréciation du juge alors que la recevabilité suppose que le juge doive encore apprécier la valeur probante d'un moyen de preuve.

Quand on parle de reconnaissance juridique de la signature électronique, encore faut-il préciser s'il s'agit d'une simple recevabilité en droit de la preuve ou si la loi accorde force probante. Pour résumer le lien entre les deux projets de loi, on peut dire que le présent projet accorde force probante aux signatures électroniques avancées créées par un dispositif sécurisé de création de signature et combinées à un certificat qualifié (article 4, § 4). Ces signatures bénéficient ainsi des mêmes effets juridiques que ceux qui sont reconnus aux signatures manuscrites. On estime que la signature est créée dans des conditions de sécurité qui sont telles qu'il n'est

ven handtekeningen. Men is van oordeel dat de handtekening wordt aangemaakt in dusdanige veiligheidsomstandigheden dat het niet langer nodig is om ze aan de voorafgaande controle van de rechter te onderwerpen.

Het ontwerp betreffende het bewijsrecht is daarentegen beperkt tot het invoeren van het principe van de *ontvankelijkheid* van elk type van handtekening, zelfs de elektronische, waarbij de rechter dan vrij is om te oordelen over de bewijswaarde die eraan moet worden gehecht (hij zou heel goed een bewijswaarde kunnen toekennen die gelijkwaardig is aan die van de handgeschreven handtekening als hij oordeelt dat de verschillende functies van de handtekening verricht worden met een redelijke zekerheid). Dat laatste ontwerp voert dus vernieuwingen in ten opzichte van de huidige situatie aangezien de rechter een document onontvankelijk kan verklaren alleen omdat het elektronisch ondertekend is (voor zover het een burgerrechtelijke aangelegenheid betreft en het bedrag van de transactie meer dan 15 000 Belgische frank bedraagt).

Die benadering is in overeenstemming met artikel 5 van het voorstel van richtlijn dat eveneens een duidelijk onderscheid maakt tussen de bewijskracht en de ontvankelijkheid. Om juridische waarde toe te kennen aan de elektronische handtekening, bevat dit artikel twee clausules : de ene over assimilatie en de andere over niet-discriminatie. De *assimilatieclausule* (artikel 5.1) bestaat in het gelijkstellen van de elektronische handtekening met de handgeschreven handtekening als bepaalde voorwaarden zijn vervuld ([18]), dit wil zeggen oordelen dat ze aanvaardbaar is als bewijsmiddel voor het gerecht en dat ze de bewijskracht moet krijgen die wordt toegekend aan de handgeschreven handtekening. De *niet-discriminatieclausule* (artikel 5.2) is van toepassing als aan de voorwaarden bepaald in artikel 5.1 om te genieten van de assimilatieclausule niet is voldaan. In dat geval moeten de lidstaten erop toezien dat de *ontvankelijkheid* als bewijsmiddel voor het gerecht van een elektronische handtekening niet wordt betwist enkel en alleen omdat de handtekening elektronisch is, of omdat ze niet op een gekwalificeerd certificaat is gebaseerd, of nog omdat ze niet is gebaseerd op een certificaat afgeleverd door een geaccrediteerde certificatiedienstverlener in de zin van het voorstel van richtlijn. Het in dat artikel aangehaalde principe moet worden opgevat als dat van de ontvankelijkheid van de *lato sensu* elektronische handtekeningen. Als echter niet beantwoord wordt aan de specificaties van artikel 5.1, moet degene die zich erop beroept de rechter overtuigen van de bewijswaarde terzake.

plus nécessaire qu'elle soit soumise au contrôle préalable du juge.

Par contre, le projet relatif au droit de la preuve se limite à créer le principe de la *recevabilité* de tout type de signature, même électronique, le juge étant alors libre d'apprécier la valeur probante à accorder à celle-ci (il pourrait très bien accorder une valeur probante équivalente à celle de la signature manuscrite s'il estime que les différentes fonctions de la signature sont réalisées avec une certitude raisonnable). Ce dernier projet innove donc par rapport à la situation actuelle puisqu'un juge peut déclarer irrecevable un document au seul motif qu'il est signé électroniquement (pour autant que l'on soit en matière civile et que le montant de la transaction dépasse 15 000 francs belges).

Cette approche est conforme à l'article 5 de la proposition de directive qui fait également une distinction claire entre force probante et recevabilité. En effet, afin de reconnaître une valeur juridique à la signature électronique, cet article contient deux clauses : l'une d'assimilation et l'autre de non discrimination. La *clause d'assimilation* (article 5.1.) consiste à assimiler la signature électronique à la signature manuscrite lorsque certaines conditions sont remplies ([18]), c'est-à-dire à considérer qu'elle doit être admissible comme preuve en justice et qu'elle doit bénéficier de la force probante accordée à la signature manuscrite. La *clause de non discrimination* (article 5.2.) s'applique lorsque les conditions prévues à l'article 5.1. ne sont pas remplies pour bénéficier de la clause d'assimilation. Dans ce cas, les États membres doivent veiller à ce que la *recevabilité* comme preuve en justice d'une signature électronique ne soit pas contestée au seul motif que la signature se présente sous forme électronique, ou qu'elle ne repose pas sur un certificat qualifié, ou encore qu'elle ne repose pas sur un certificat délivré par un prestataire de service de certification accrédité au sens de la proposition de directive. Le principe énoncé dans cet article doit être entendu comme celui de la recevabilité des signatures électroniques *lato sensu*. Toutefois, à défaut de répondre aux spécifications de l'article 5.1, il appartient à celui qui s'en prévaut de convaincre le juge de sa valeur probante.

3.5. *Aflevering van gekwalificeerde certificaten aan natuurlijke personen en rechtspersonen en erkenning van de handtekeningen van rechtspersonen*

De aflevering van gekwalificeerde certificaten beperkt zich niet tot natuurlijke personen. Elke persoon die al dan niet de rechtspersoonlijkheid heeft, heeft het recht een gekwalificeerd certificaat aan te vragen en te verkrijgen. Als gevolg daarvan kan een burger, een handelsvennootschap, een VZW, een GBS, de Staat, een parastatale instelling, een EPA, … houder worden van een certificaat.

Entiteiten zonder rechtspersoonlijkheid kunnen dus geen gekwalificeerd certificaat bekomen. De reden van deze keuze is dat het voor een certificatiedienstverlener moeilijk is om de identiteit na te gaan en te bevestigen van een entiteit die juridisch niet bestaat, terwijl die taak gemakkelijker is voor personen met een rechtspersoonlijkheid (een natuurlijk persoon kan worden geïdentificeerd door middel van een officieel document, de gegevens om een rechtspersoon of een privaatrechtelijke persoon te identificeren worden gepubliceerd in het *Belgisch Staatsblad* en er bestaat een nationaal register van de rechtspersonen).

De mogelijkheid voor een rechtspersoon om een certificaat aan te vragen is logisch omdat de elektronische communicatie zich niet beperkt tot communicatie tussen natuurlijke personen. Integendeel, de enorme groei van het aantal *sites* op het Internet van rechtspersonen is verbazingwekkend. Het merendeel van deze sites geven geen enkele referentie naar natuurlijke personen en de communicatie komt rechtstreeks tot stand met de rechtspersoon. Deze evolutie toont duidelijk aan hoe deze laatste zich als dusdanig wil identificeren, zonder de tussenkomst van een natuurlijke persoon. Daarenboven valt het hoogst waarschijnlijk te verwachten dat de ontwikkeling van de elektronische handel vooral een zaak wordt van rechtspersonen. Ten slotte is het van het grootste belang dat de gebruiker die elektronische transacties verricht, zeker kan zijn van de juiste identiteit van de rechtspersoon waarmee hij handelt, want hij is uiteindelijk diegene die zich financieel verbindt. Het zou dan ook uiterst onredelijk zijn om de afgifte van certificaten te beperken tot natuurlijke personen.

Deze oplossing werd al naar voren gebracht door de Europese Commissie in haar mededeling van 8 oktober 1997 (COM(97)503 : Naar een Europees kader voor digitale handtekeningen en encryptie. Zorgen voor veiligheid van en vertrouwen in elektronische communicatie. Mededeling van de Commissie aan het Europees Parlement, de Raad, het Economisch en Sociaal Comité en het Comité der Regio's, 8 oktober 1997) in punt 2.3., (i) aanduidt dat : « De sleutels (en dus ook de certificaten) kunnen worden toegekend aan natuurlijke

3.5. *Délivrance de certificats qualifiés aux personnes physique et morale et reconnaissance de la signature des personnes morales*

La délivrance de certificats qualifiés ne se limite pas aux personnes physiques. Toute personne ayant la personnalité juridique a le droit de demander et obtenir un certificat qualifié. Il en résulte qu'un citoyen, une société commerciale, une ASBL, un GIE, l'État, un parastatal, une EPA, … peut devenir titulaire d'un tel certificat.

Ne peuvent donc pas obtenir de certificat qualifié les entités sans personnalité juridique. La raison de ce choix réside dans la difficulté pour un prestataire de service de certification de vérifier et confirmer l'identité d'une entité qui n'existe pas juridiquement alors que cette tâche s'avère plus aisée pour les personnes ayant une personnalité juridique (une personne physique peut être identifiée au moyen d'un document officiel, les données d'identification d'une personne morale ou de droit public sont publiées au *Moniteur Belge* et un registre national des personnes morales existe).

La possibilité pour une personne morale de demander un certificat est logique dans la mesure où la communication électronique ne se limite pas à une communication entre personnes physiques. Bien au contraire, il est stupéfiant par exemple de voir la croissance du nombre de sites sur Internet appartenant à une personne morale. La plupart de ces sites ne contiennent aucune référence à des personnes physiques et la communication est directement établie avec la personne morale. Cette évolution démontre bien la volonté de cette dernière de s'identifier en tant que telle, sans passer par l'intermédiaire d'une personne physique. De plus, on peut très probablement s'attendre à ce que le développement du commerce électronique soit essentiellement le fait de personnes morales. Enfin il est primordial que le consommateur qui effectue des transactions électroniques puisse s'assurer de l'identité exacte de la personne morale avec laquelle il traite, puisque qu'en définitive celle-ci sera engagée financièrement. Il eut dès lors été déraisonnable de réserver la délivrance de certificats uniquement à des personnes physiques.

Cette solution était déjà préconisée par la Commission Européenne qui, dans sa communication du 8 octobre 1997 (COM(97)503 : Vers un Cadre Européen pour les signatures numériques et le chiffrement : Assurer la sécurité et la confiance dans la communication électronique, Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social et au Comité des Régions, 8 octobre 1997) indique dans le point 2.3., (i) que « *Les clés (et par conséquent les certificats)* peuvent être allouées à des personnes pri-

personen of rechtspersonen (bijvoorbeeld een vennootschap met beperkte aansprakelijkheid) … ».

De werkzaamheden van de VNCIH van de Verenigde Naties gaan ook in die richting. Inderdaad, in haar rapport van de werkgroep voor elektronische handel (Verenigde Naties Commissie inzake Internationaal Handelsrecht, Rapport van de werkgroep voor elektronische handel over de werkzaamheden van haar eenendertigste sessie (New York, 18-28 februari 1997), A/CN.9/437, 12 maart 1997) analyseert de VNCIH het ontwerp van artikel D dat uitdrukkelijk de mogelijkheid erkent voor een rechtspersoon om de certificatie van publieke sleutels te verkrijgen. De tekst voegt eraan toe dat het : « niet opportuun zou zijn om een onderscheid te maken tussen natuurlijke personen en rechtspersonen met betrekking tot numerieke handtekeningen ». Dit standpunt is vooral gebaseerd op de typewet van de VNCIH over elektronische handel « waar het begrip persoon zowel slaat op natuurlijke personen als op rechtspersonen ».

Ten slotte zien wij dat in de praktijk de certificatieautoriteiten in België of elders duidelijk die richting uitgaan : Belsign, Isabel en Verisign bijvoorbeeld leveren certificaten zowel aan natuurlijke personen als aan rechtspersonen.

Het ontwerp gaat zelfs nog verder, daar het ook *de handtekening van rechtspersonen* erkent.

Daaruit volgt dat het verband dat in artikel 4, § 4 wordt gelegd met het ontwerp, zowel voor natuurlijke als voor rechtspersonen geldt. Met andere woorden, een elektronisch document waarvan de geavanceerde elektronische handtekening zou worden gecombineerd met een gekwalificeerd certificaat afgegeven op naam van een rechtspersoon, zonder enige verwijzing naar een natuurlijk persoon, zou worden beschouwd als een onderhandse akte en evenveel bewijskracht zou hebben als een schriftelijk stuk ondertekend door een natuurlijke persoon. Zulks zou ook inhouden dat rechtspersonen geldige overeenkomsten zouden kunnen afsluiten via elektronische berichten die door hen werden ondertekend (kwestie van de vertegenwoordiging).

Er bestaat duidelijk geen juridisch bezwaar om te erkennen dat een rechtspersoon het recht heeft om een handtekening te plaatsen. Dit wordt categoriek bevestigd in een studie die voor rekening van het ministerie van Economische Zaken door de dienst handelsrecht van de rechtsfaculteit van de Luikse universiteit werd uitgevoerd. Uit deze studie blijkt enerzijds dat het wenselijk, logisch en coherent zou zijn om de handtekening van rechtspersonen te erkennen en dat zulks geen enkel probleem inzake vennootschaprecht stelt, en anderzijds dat zoiets bovendien een grotere rechtszekerheid biedt en een oplossing vormt voor bepaalde problemen inzake tegenstelbaarheid tegenover derden van daden gesteld door de instellingen van de rechtspersoon.

vées ou juridiques (par exemple une société à responsabilité limitée) … ».

Les travaux de la CNUDCI des Nations Unies se dirigent également dans ce sens. En effet dans son rapport du groupe de travail sur le commerce électronique (Commission des Nations Unies pour le Droit commercial international, Rapport du groupe de travail sur le commerce électronique sur les travaux de sa trente et unième session (New York, 18-28 février 1997), A/CN.9/437, 12 mars 1997), la CNUDCI analyse le projet d'article D qui reconnaît expressément la possibilité pour une personne morale d'obtenir la certification de clés publiques. Le texte ajoute qu'il « était inopportun d'établir une distinction entre personne morale et personne physique aux fins des signatures numériques ». Cette prise de position se fonde notamment sur la loi type de la CNUDCI sur le commerce électronique « où la notion de personne recouvrait aussi bien les personnes physiques que les personnes morales ».

Enfin on constate que la pratique actuelle des autorités de certification en Belgique ou ailleurs va clairement dans ce sens : Belsign, Isabel et Verisign, par exemple, délivrent des certificats aussi bien à des personnes physiques qu'à des personnes morales.

Le projet va même plus loin puisqu'il reconnaît *la signature des personnes morales*.

Cela signifie que le lien établi par l'article 4, § 4 avec le projet preuve vaut tant pour les personnes physiques que pour les personnes morales. En d'autres termes, un document électronique dont la signature électronique avancée serait combinée à un certificat qualifié émis au nom d'une personne morale, sans aucune référence à une personne physique, serait considéré comme un acte sous seing privé et permettrait de faire preuve au même titre qu'un écrit signé par une personne physique. De plus, cela signifierait aussi que les personnes morales pourraient conclure valablement via les messages électroniques signés par elles (question de la représentation).

D'un point de vue juridique, il n'y a manifestement aucun obstacle à reconnaître le droit pour une personne morale de signer. Une étude réalisée pour le compte du ministère des Affaires économiques par le service de droit commercial de la faculté de droit de l'université de Liège confirme cet élément de manière catégorique. Cette étude conclut que d'une part, il est souhaitable, logique et cohérent de reconnaître la signature aux personnes morales et que cela ne pose aucun problème en droit des sociétés et que d'autre part, cela présente en outre d'avantage de sécurité juridique et résout certains problèmes d'opposabilité aux tiers d'actes posés par les organes de la personne morale.

Laten wij overigens opmerken dat in het Burgerlijk Wetboek nergens de handtekening wordt voorbehouden aan natuurlijke personen. Tot nog toe stelde de vraag zich eenvoudig niet, omdat een handtekening *de facto* met de was hand geschreven. Een rechtspersoon, die geen materieel bestaan heeft, kon in praktijk moeilijk een met de hand geschreven handtekening aanbrengen. In de elektronische wereld daarentegen, die in essentie immaterieel is, gaat het er anders aan toe. De handtekening blijft immers niet langer beperkt tot een merkteken dat met de hand wordt aangebracht, maar kan voortaan ook door middel van een informaticatechniek worden tot stand gebracht, die zowel door een natuurlijke persoon als door en rechtspersoon kan worden geïmplementeerd en die een identificatie van deze laatste mogelijk maakt.

Bekijkt men de juridische gevolgen, dan lijkt het bovendien logisch om de handtekening van rechtspersonen te erkennen. De rechtspersoon heeft weliswaar geen materieel bestaan, maar wel een juridisch, en als dusdanig kan zij rechten en verplichtingen hebben, en dus ook haar vermogen op het spel zetten. Men mag bijgevolg aannemen dat een rechtspersoon, die juridisch kan worden geïdentificeerd en verantwoordelijk gesteld, een handtekening kan plaatsen, vermits de handtekening geen ander doel heeft dan het bewijs leveren van de wil van de ondertekenaar om zich te verbinden.

3.6. *Bepalingen met het oog op het verzekeren van een betere bescherming van de zwakke partij*

Sommige bepalingen volgen de eerste doelstelling voor het verzekeren en het versterken van de bescherming van de zwakke partij in haar relaties met de certificatiedienstverlener :

— de toepassing van de wet van 11 december 1998 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens en het vrije verkeer van deze gegevens;

— de verplichting voor de certificatiedienstverlener om de gebruiker de nodige informatie te verschaffen met betrekking tot het juiste en veilige gebruik van zijn diensten;

— de verplichting voor de certificatiedienstverlener om *in het certificaat* de grenzen van zijn aansprakelijkheid aan te geven;

— om de schadevergoeding aan de benadeelde persoon te verzekeren, is de certificatiedienstverlener ver-

Notons d'ailleurs que le Code civil ne réserve nullement la signature aux personnes physiques. Il est vrai que jusque maintenant la question ne s'était pas posée car la signature était manuscrite. En pratique, une personne morale, qui n'a pas d'existence matérielle, pouvait difficilement signer manuscritement. Dans le monde électronique, par essence immatériel, il en va différemment. En effet, la signature ne se réduit plus à une marque apposée de manière manuscrite mais peut désormais être réalisée au moyen d'une technique informatique qui peut être mise en œuvre aussi bien par une personne physique que par une personne morale et qui permet d'identifier cette dernière.

Du point de vue des conséquences juridiques, il paraît d'ailleurs logique qu'on puisse reconnaître la signature aux personnes morales. Si elle n'existe pas matériellement, la personne morale existe juridiquement et à ce titre elle est apte à être titulaire de droits et obligations ainsi qu'elle est susceptible de voir son patrimoine engagé. Dès lors, on peut admettre qu'une personne morale, qui peut être identifiée et engagée juridiquement, puisse signer puisque la signature n'a d'autres buts que de prouver la volonté du signataire d'être engagé.

3.6. *Dispositions ayant pour but d'assurer une meilleure protection de la partie faible*

Certaines dispositions poursuivent l'objectif premier d'assurer et de renforcer la protection de la partie faible dans ses relations avec le prestataire de service de certification :

— l'application de la loi du 11 décembre 1998 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et à la libre circulation de ces données;

— l'obligation pour le prestataire de service de certification de fournir à l'utilisateur toute information nécessaire à l'utilisation correcte et sûre de ses services;

— l'obligation pour le prestataire de service de certification d'indiquer *dans le certificat* les limites de sa responsabilité;

— pour assurer l'indemnisation des personnes préjudiciées, le prestataire de service de certification est

plicht een verzekering af te sluiten die zijn beroepsaansprakelijkheid dekt.

COMMENTAAR BIJ DE ARTIKELEN

Art. 2

Het tweede artikel geeft een lijst van de definities die de juiste draagwijdte bepalen van de termen die in deze wet worden gebruikt. Die definities steunen rechtstreeks op het gemeenschappelijk standpunt over het voorstel van richtlijn voor elektronische handtekeningen.

De definitie van de geavanceerde elektronische handtekening is vrij ruim opgesteld opdat ze niet beperkt zou blijven tot het bijzonder mechanisme van de numerieke handtekening en aldus het principe van de technologische neutraliteit zou eerbiedigen. Hiermee worden evenwel enkel de handtekeningmechanismen met een zekere graad van betrouwbaarheid bedoeld, vermits zij moeten voldoen aan de vier eisen van de definitie. Een zogenaamde geavanceerde elektronische handtekening moet het immers mogelijk maken de ondertekenaar te identificeren en moet op unieke wijze aan de ondertekenaar verbonden zijn — een voorwaarde die eigenlijk geïmpliceerd wordt door de voorgaande — zij moet op zodanige wijze verbonden zijn aan de gegevens waarop zij betrekking heeft dat elke latere wijziging van de gegevens kan worden opgespoord — een voorwaarde die rechtstreeks van de voorgestelde definitie is overgenomen — en ten slotte moet zij zijn aangemaakt met middelen die de ondertekenaar onder zijn uitsluitende controle kan houden — een onontbeerlijke voorwaarde om te vermijden dat iemand anders zich de handtekening onrechtmatig toe-eigent.

Het ontwerp van richtlijn bevat ook een minder dwingende definitie van de gewone elektronische handtekening, namelijk « elektronische gegevens die zijn vastgehecht aan of logisch geassocieerd zijn met andere elektronische gegevens die worden gebruikt als middel voor authentificatie ». Buiten de verwijzing naar de veiligheid van de gegevens voor het aanmaken van een handtekening die, voor de zogenaamde geavanceerde handtekening, onder de uitsluitende controle van de ondertekenaar moeten blijven, onderscheiden zich beide soorten handtekening vooral daardoor dat de gewone handtekening opgevat is als een authentificatiemiddel zonder als dusdanig te moeten dienen als middel om de ondertekenaar te identificeren (de authentificatie zou immers kunnen worden beperkt tot de inhoud van de boodschap). Zo'n onderscheid lijkt op zijn minst subtiel en moeilijk verenigbaar met onze traditionele opvatting van de handtekening die, hoe dan ook, onderstelt dat zij het mogelijk maakt de ondertekenaar te identificeren.

tenu de souscrire une assurance capable de couvrir sa responsabilité professionnelle.

COMMENTAIRE DES ARTICLES

Art. 2

L'article 2 donne une liste de définitions qui précisent la portée exacte des termes qui sont utilisés dans cette loi. Ces définitions sont directement inspirées de la position commune sur la proposition de directive pour les signatures électroniques.

La définition de la signature électronique avancée est libellée de manière relativement large afin de ne pas se limiter au mécanisme particulier de signature numérique et de respecter ainsi le principe de neutralité technologique, tout en n'admettant toutefois que les mécanismes de signature qui offrent un certain niveau de fiabilité puisque ces derniers doivent répondrent aux quatre exigences de cette définition. En effet, une signature électronique dite avancée, doit permettre d'identifier le signataire et être liée uniquement à celui-ci — ce qui n'est, pour l'essentiel, qu'une condition impliquée par la précédente — elle doit être liée aux données auxquelles elle se rapporte de telle sorte que toute modification ultérieure des données soit détectée — condition directement reprise dans la définition proposée — et, enfin, qu'elle soit créée par des moyens que le signataire puisse garder sous son contrôle exclusif — condition indispensable afin d'éviter l'usurpation de la signature d'autrui.

Le projet de directive comporte, par ailleurs, une définition moins contraignante de la signature électronique ordinaire, envisagée comme « une donnée sous forme numérique jointe ou liée logiquement à d'autres données électroniques et servant de méthode d'authentification ». Outre la référence à la sécurité des données afférentes à la création de la signature qui, pour la signature dite avancée, doivent demeurer sous le contrôle exclusif du signataire, les deux types de signature se distinguent essentiellement par le fait que la signature ordinaire est conçue comme une méthode d'authentification sans devoir satisfaire, en tant que telle, à la fonction d'identification du signataire (l'authentification pourrait en effet se limiter au contenu du message). La distinction paraît pour le moins subtile et difficilement compatible avec notre conception traditionnelle de la signature qui, en tout état de cause, suppose que celle-ci puisse identifier le signataire. Elle ne semble, par ailleurs, pas indispensable dans la mesure où d'une part,

ren. Dat onderscheid lijkt overigens niet onontbeerlijk, enerzijds, omdat in het ontwerp van richtlijn uiteindelijk wordt gesteld dat dit onderscheid slechts geringe gevolgen kan hebben op de regels in verband met de erkenning van elektronische handtekeningen (artikel 5,2° van het ontwerp), en anderzijds, omdat het *a contrario* voortvloeit uit de definitie van de geavanceerde elektronische handtekening, vermits de elektronische handtekening noodzakelijkerwijze wordt beschouwd als niet-geavanceerd ingeval er niet is voldaan aan een of meer van de vier eisen. Er werd dan ook voor gekozen dat onderscheid als dusdanig niet te maken in dit stadium, maar het nodige verschil in te bouwen in de erkenningsmethoden. Op die manier geniet enkel de geavanceerde elektronische handtekening de bewijskracht die wordt geïmpliceerd door artikel 4, § 4. De elektronische handtekening die als niet-geavanceerd wordt beschouwd geniet enkel het ontvankelijkheidsprincipe en het staat de rechter vrij te oordelen over de bewijskracht ervan. In dat opzicht lijken zowel de geest als de letter van de richtlijn volkomen geëerbiedigd.

Het begrip « certificaat » is fundamenteel in de context van de elektronische certificatie aangezien het een verband legt tussen een natuurlijke persoon of een rechtspersoon en gegevens met betrekking tot het verifiëren van een handtekening. Door het afgeven van het certificaat « certificeert » de certificatiedienstverlener dat verband; met andere woorden, hij bevestigt publiekelijk de juistheid van de daarin vervatte informatie. De informatie wordt beveiligd door de elektronische handtekening van de certificatiedienstverlener die deze handtekening plaatst. Dit betekent dat de dienstverlener het certificaat tekent met zijn eigen gegevens voor de aanmaak van een handtekening zodat de gebruiker van het certificaat zich ervan kan vergewissen dat de informatie werd gecertificeerd door deze of gene dienstverlener en dat de integriteit van die informatie gevrijwaard is.

Het gekwalificeerd certificaat is een speciaal soort certificaat. Overeenkomstig het voorstel van richtlijn wordt een certificaat slechts beschouwd als « gekwalificeerd » als het, enerzijds, een minimum aan informatie bevat zoals bepaald in artikel 12 (men bedoelt duidelijk het identiteits-certificaat) en het, anderzijds, afgegeven werd onder zekere voorwaarden. Dit laatste element onderstelt dat het afgegeven werd door een geaccrediteerde certificatiedienstverlener, namelijk een dienstverlener die voldoet aan de eisen van bijlage II van het voorstel van richtlijn. Alle in deze bijlage II vermelde eisen werden namelijk overgenomen in de accreditatievoorwaarden van deze wet.

De houder van het certificaat kan zowel een natuurlijke persoon als een rechtspersoon zijn. Deze definitie steunt op het principe dat een certificaat aan alle soorten personen met rechtspersoonlijkheid kan afgegeven worden (een burger, een handelsvennootschap, een

le projet de directive ne lui attache, en définitive, que des effets limités au niveau des modalités de reconnaissance des signatures électroniques (article 5,2° du projet) et d'autre part, elle découle *a contrario* de la définition de signature électronique avancée puisque si une ou plusieurs des quatre exigences ne sont pas remplies, la signature électronique sera nécessairement considérée comme non avancée. Aussi, le parti a été pris de ne pas l'intégrer telle quelle à ce stade mais de prévoir la différenciation nécessaire à propos des modes de reconnaissance. Ainsi, seule la signature électronique avancée bénéficie de la force probante impliquée par l'article 4, § 4. La signature électronique considérée comme non avancée ne bénéficie que du principe de la recevabilité, le juge restant libre d'en apprécier la valeur probante. L'esprit autant que la lettre de la directive nous semblent à cet égard parfaitement respectés.

La notion de « certificat » est fondamentale dans le contexte de la certification électronique puisque celui-ci établit le lien entre une personne, qu'elle soit physique ou morale, et ses données afférentes à la vérification de signature. Par l'émission du certificat, le prestataire de service de certification « certifie » ce lien, c'est-à-dire affirme publiquement l'exactitude des informations qu'il contient. Les informations seront sécurisées par la signature électronique du prestataire de service de certification qui l'émet. Cela signifie que le prestataire va signer le certificat avec ses propres données afférentes à la création de signature afin que l'utilisateur du certificat puisse s'assurer que les informations ont été certifiées par tel ou tel prestataire et que l'intégrité de ces informations est sauvegardée.

Le certificat qualifié est un type particulier de certificat. Conformément à la proposition de directive, un certificat n'est considéré comme « qualifié » qu'à la condition, d'une part, qu'il contienne un minimum d'informations tel que c'est prévu à l'article 12 (on vise manifestement le certificat d'identité) et, d'autre part, qu'il ait été émis dans des conditions sûres. Ce dernier élément suppose qu'il ait été émis par un prestataire de service de certification accrédité c'est-à-dire un prestataire qui satisfait aux exigences de l'annexe II de la proposition de directive. En effet, les conditions d'accréditation de cette loi reprennent l'ensemble des exigences de cette annexe II.

Le titulaire de certificat peut aussi bien être une personne physique que morale. Cette définition constitue la consécration du principe selon lequel un certificat peut être délivré à tout type de personne ayant la personnalité juridique (un citoyen, une société commerciale, une

VZW, een GBS, de Staat, een parastatale instelling, een EPA, …). Overigens kan een natuurlijke persoon of rechtspersoon verschillende gegevens voor het verifiëren van een handtekening laten certificeren en als dusdanig houder worden van meerdere certificaten.

De houder van een certificaat is de persoon zoals die geïdentificeerd wordt in het certificaat. Aldus zijn de vermeldingen met betrekking tot de identiteit, de gegevens voor het verifiëren van een handtekening, de kenmerken vermeld in het certificaat, vermeldingen verbonden met de persoon die houder is van het certificaat. Deze zal over alle rechten en verplichtingen beschikken zoals vermeld in de wet. Hij zal tevens volledig verantwoordelijk zijn voor het beheer en het gebruik dat zal worden gemaakt van zijn certificaat en zijn gegevens voor het aanmaken van een handtekening.

Het begrip houder van een certificaat, een begrip dat juridische implicaties heeft omdat het onderworpen is aan de toepassing van de wet, mag niet worden verward met het begrip bezitter van de gegevens voor het aanmaken van een handtekening (niet gebruikt in deze wet) dat eerder een materieel begrip lijkt te zijn. De gegevens voor het aanmaken van een handtekening worden immers vaak op een materiële hulpbron zoals een chipkaart opgeslagen. Dus, de houder van een certificaat, die tevens de houder is van deze gegevens, kan de bezitter ervan zijn, maar is dat niet altijd. Bijvoorbeeld, een rechtspersoon is houder van een certificaat maar is niet de bezitter van de gegevens voor het aanmaken van een handtekening, want, aangezien hij materieel niet bestaat, kan hij ook niet de bezitter zijn van de gegevens op deze chipkaart. Een natuurlijke persoon (die bevoegd is om een maatschappij te vertegenwoordigen) is dus noodzakelijkerwijze de bezitter van deze gegevens.

De rechten en plichten bepaald in of krachtens deze wet zijn enkel van toepassing op de houder van het certificaat en in geen geval op de bezitter van het certificaat. Dit betekent ook dat een handtekening afkomstig kan zijn van zowel een natuurlijke als een rechtspersoon, zelfs indien, uiteraard, in het tweede geval, deze noodzakelijkerwijze handelt door bemiddeling van een natuurlijke persoon die gemachtigd is om in zijn plaats een verbintenis aan te gaan. De juridische gevolgen van de handtekening zijn dus dezelfde, of de handtekening nu afkomstig is van een natuurlijke persoon of een rechtspersoon.

De begrippen gegevens voor het aanmaken van een handtekening en gegevens voor het verifiëren van een handtekening zijn rechtstreeks ontleend aan het voorstel van richtlijn. Hoewel voor het ogenblik alleen de technologie van de asymmetrische cryptografie lijkt te voldoen aan de voorwaarden die door deze wet gesteld worden, zal het beroep op bovengenoemde begrippen

ASBL, un GIE, l'État, un parastatal, une EPA, …). Par ailleurs, une personne physique ou morale peut faire certifier plusieurs données afférentes à la vérification de signature et devenir ainsi titulaire de plusieurs certificats.

Le titulaire de certificat est la personne telle qu'identifiée dans le certificat. Il en résulte que les mentions relatives à l'identité, aux données afférentes à la vérification de signature, à l'attribut contenues dans le certificat sont des mentions liées à la personne qui est titulaire du certificat. Celui-ci jouira des droits et obligations inscrits dans la loi. Il sera également pleinement responsable de la gestion et de l'utilisation qui sera faite de son certificat et de ses données afférentes à la création de signature.

La notion de titulaire de certificat, notion qui a des conséquences juridiques car celui-ci est soumis à l'application de la loi, ne doit pas être confondue avec la notion de détenteur des données afférentes à la création de signature (non utilisée dans cette loi) qui apparaît plus comme une notion matérielle. En effet les données afférentes à la création de signature seront souvent stockées sur un support matériel telle qu'une carte à puce. Or le titulaire de certificat, qui est également titulaire de ces données, peut être mais ne sera pas toujours détenteur de celles-ci. Par exemple une personne morale est titulaire de certificat mais ne sera pas détentrice des données afférentes à la création de signature car n'existant pas matériellement, elle n'est pas capable de détenir celles-ci (cette carte à puce). Une personne physique (habilitée à représenter la société) sera donc nécessairement détentrice de ces données.

Les droits et obligations stipulés par ou en vertu de cette loi ne s'appliquent qu'au titulaire de certificat et en aucun cas au détenteur de certificat. Cela signifie aussi qu'une signature peut émaner tant d'une personne physique que d'une personne morale, même si bien entendu dans le second cas, celle-ci agit nécessairement par l'intermédiaire d'une personne physique habilitée à l'engager. Dès lors, les conséquences juridiques attachées à la signature sont identiques, que la signature émane d'une personne physique ou morale.

Les concepts de données afférentes à la création de signature et de données afférentes à la vérification de signature sont directement empruntés à la proposition de directive. Bien qu'à l'heure actuelle seule la technologie de la cryptographie asymétrique paraît satisfaire aux conditions posées par cette loi, le recours aux concepts susvisés permettra, le cas échéant, l'emploi

het mogelijk maken, in voorkomend geval, andere technologieën te gebruiken die niet noodzakelijk steunen op het gebruik van asymmetrische sleutels, maar wel beantwoorden aan de voorwaarden van de definitie.

De codes of sleutels die door de ondertekenaar gebruikt worden zijn noodzakelijkerwijze uniek, zoals ook de handgeschreven handtekening van een persoon uniek is. Het is dus de taak van de certificatiedienstverlener (zie bovengenoemde definitie) te verifiëren of een sleutel of code reeds werd toegekend alsook of de gegevens voor het aanmaken van een handtekening en de gegevens voor het verifiëren van een handtekening complementair zijn.

De begrippen veilig middel voor het aanmaken van een handtekening en veilig middel voor het verifiëren van een handtekening vereisen geen commentaar. Zij slaan bijvoorbeeld op de software die de gegevens voor het aanmaken van een handtekening en de gegevens voor het verifiëren van een handtekening genereert, op de browser die het mogelijk maakt een elektronische handtekening aan te maken of te verifiëren, op de chipkaart waarop de gegevens voor het aanmaken van een handtekening opgeslagen zijn, op de lezer van de chipkaart, enz. Er valt alleen op te merken dat het middel voor het aanmaken van een handtekening veilig moet zijn, dat het moet voldoen aan de eisen van artikel 11.

De certificatiedienstverlener kan zowel een natuurlijke persoon als een rechtspersoon zijn. In de praktijk gaat het vaak om een rechtspersoon.

De belangrijkste opdrachten van de certificatiedienstverlener zijn het aanmaken, het afgeven en het beheren van certificaten. De certificatiedienstverlener maakt een certificaat aan op aanvraag van een natuurlijke persoon of een rechtspersoon. Eens het certificaat aangemaakt is, geeft hij het af aan de persoon die de aanvraag gedaan heeft en schrijft het, na toestemming van de houder, in in het elektronisch register dat daartoe gecreëerd werd. In geval van noodzaak, herroept hij het certificaat. De certificatiedienstverlener is niet verplicht om zelf te zorgen voor alle etappes van het certificatieproces. Voor het verzamelen van informatie kan hij immers gebruik maken van de inlichtingen waarover de registratieoverheid beschikt. Hij is echter aansprakelijk, ten opzichte van de certificaatgebruikers, voor de schade die voortvloeit uit de verplichtingen die door of krachtens deze wet worden opgelegd.

De functie van de certificatiedienstverlener beperkt zich niet alleen tot het afgeven en beheren van certificaten; zij omvat eveneens andere diensten die in verband staan met het gebruik van elektronische handtekeningen (datum- en uurvermelding, archivering, enz.).

Het begrip product voor elektronische handtekeningen is zeer ruim. Het omvat niet alleen de begrippen veilig middel voor het aanmaken van een handtekening en voor het verifiëren van een handtekening maar ook

d'autres technologies ne reposant pas nécessairement sur l'utilisation de clés asymétriques, mais répondant aux conditions de la définition.

Les codes ou clés utilisés par le signataire sont nécessairement uniques, de même qu'est unique la signature manuscrite d'une personne. Il incombera donc au prestataire de service de certification (voir définition ci-dessous) de vérifier que telle clé ou tel code n'a pas déjà été attribué ainsi que la complémentarité des données afférentes à la création et à la vérification de signature.

Les notions de dispositif sécurisé de création de signature et de dispositif de vérification de signature n'appellent pas de commentaires. Cela vise par exemple le logiciel qui génère les données afférentes à la création et vérification de signature, le *browser* qui permet de créer ou de vérifier une signature électronique, la carte à puce sur laquelle sont stockées les données afférentes à la création de signature, le lecteur de carte à puce, etc. Notons simplement que le dispositif de création de signature doit être sécurisé c'est-à-dire qu'il doit satisfaire aux exigences de l'article 11.

Le prestataire de service de certification peut aussi bien être une personne physique que morale. Dans la pratique, il s'agira souvent d'une personne morale.

Le prestataire de service de certification a comme missions principales la création, la délivrance et la gestion de certificats. Sur demande d'une personne physique ou morale, le prestataire de service de certification crée un certificat. Une fois ce certificat créé, il le délivre à la personne qui en a fait la demande et l'inscrit, après consentement du titulaire, dans l'annuaire électronique créé à cet effet. En cas de nécessité, il procède à sa révocation. Le prestataire de service de certification n'est pas tenu d'assurer seul toutes les étapes du processus de certification. En effet, il peut se référer, pour la collecte des informations, aux renseignements détenus par les autorités d'enregistrement. Toutefois, il répond, à l'égard des utilisateurs des certificats, du dommage qui est la conséquence des obligations qui lui sont imposées par ou en vertu de la présente loi.

La fonction du prestataire de service de certification n'est pas limitée à délivrance et à la gestion des certificats; il couvre également d'autres services connexes à l'utilisation des signatures électroniques (horodatage, archivage, etc.).

La notion de produit de signature électronique est très large. Elle englobe non seulement les notions de dispositifs de création et de vérification de signature mais également tout autre produit lié à la signature électroni-

elk ander product dat verband houdt met een elektronische handtekening. Volgens het voorstel van richtlijn mag de definitie van deze producten namelijk niet worden beperkt tot de afgifte of het beheer van certificaten maar slaat zij ook op elk ander product dat gebruikt wordt voor elektronische handtekeningen of hiermee in verband staat, zoals producten die gebruikt worden voor registratiediensten, registratieklokdiensten, registerdiensten of andere informaticadiensten. De definitie van het product voor elektronische handtekeningen moet samen met artikel 11 en artikel 17 gelezen worden waarin bepaald wordt dat deze producten betrouwbaar moeten zijn.

Het Bestuur gaat een belangrijke rol spelen. Het is belast met het ontvangen van de accreditatie- aanvragen, het naleven van de accreditatievoorwaarden en, eventueel, het verlenen van de accreditatie. Om dit te doen, kan het de hulp inroepen van een entiteit, zoals bedoeld in artikel 2, 12°.

Het is tevens belast met de controle van de geaccrediteerde certificatiedienstverleners en met het waken over de certificatiemarkt (artikel 6 en 22). Te dien einde controleert het of deze de accreditatievoorwaarden evenals de bepalingen vastgelegd door of krachtens de wet naleven.

Ten slotte bevestigt het Bestuur het verband tussen een geaccrediteerde certificatiedienstverlener en zijn gegevens voor het verifiëren van een handtekening.

De verschillende opdrachten worden nader bepaald in artikel 6.

Art. 3

Artikel 3 verduidelijkt het toepassingsgebied van de wet.

Paragraaf 1 definieert het toepassingsgebied van de wet aan de hand van de belangrijkste doelstelling die door de wet wordt nagestreefd, namelijk het versterken van de garantie van en het vertrouwen in het gebruik van de elektronische handtekening.

Om deze doelstelling te bereiken, creëert de wet een duidelijk juridisch kader dat het volgende vastlegt :

— de algemene voorwaarden voor de accreditatie van de certificatiedienstverleners;

— het juridisch stelsel van toepassing op de verrichtingen uitgevoerd door de certificatiedienstverleners;

— de regels die door de certificatiedienstverleners en door de certificaatgebruikers moeten worden nageleefd. Onder certificaatgebruikers verstaat men zowel de houders van door een certificatiedienstverlener gecreëerde en afgegeven certificaten als de bestemmelingen van elekronisch ondertekende berichten.

que. En effet, selon la proposition de directive, il convient que la définition de ces produits ne soit pas limitée à la délivrance ou à la gestion de certificats mais couvre également tout autre produit utilisant des signatures électroniques ou connexe à celles-ci, tels ceux utilisés pour les services d'enregistrement, les services horodateurs, les services d'annuaires ou autres services informatiques. La définition de produit de signature électronique doit être lu en parallèle avec l'article 11 ainsi qu'avec l'article 17 qui prévoit que ces produits doivent être fiables.

L'Administration va jouer un rôle important. Elle est chargée de recevoir les demandes d'accréditation, de vérifier le respect des conditions d'accréditation et, le cas échéant, de délivrer l'accréditation. Pour ce faire, elle peut s'adjoindre l'aide d'une entité visée à l'article 2, 12°.

Elle est également chargée de la surveillance des prestataires de service de certification accrédités et d'effectuer une veille sur le marché de la certification (articles 6 et 22). À cet effet, elle vérifie si ceux-ci se conforment aux conditions d'accréditation ainsi qu'aux dispositions stipulées par ou en vertu de la loi.

Enfin, l'Administration confirme le lien entre un prestataire de service de certification accrédité et ses données afférentes à la vérification de signature.

Ces différentes missions sont précisées dans l'article 6.

Art. 3

L'article 3 précise le champ d'application de la loi.

Le paragraphe 1er définit le champ d'application de la loi en fonction de l'objectif principal poursuivi par la loi qui est de renforcer la sécurité et la confiance dans l'utilisation de la signature électronique.

Afin de réaliser cet objectif, la loi met en place un cadre juridique clair qui fixe :

— les conditions générales d'accréditation des prestataires de service de certification;

— le régime juridique applicable aux opérations effectuées par les prestataires de service de certification;

— les règles que les prestataires de service de certification ainsi que les utilisateurs de certificats doivent respecter. On entend par utilisateurs de certificats aussi bien les titulaires de certificats créés et délivrés par un prestataire de service de certification que les destinataires de messages signés électroniquement.

Paragraaf 2 stelt dat de wet enkel bedoeld is voor certificatiedienstverleners die hun activiteiten uitoefenen in een open netwerk. Voor elektronische handtekeningen die in een gesloten netwerk worden gebruikt, is het principe van de contractuele vrijheid doorslaggevend. Niets belet evenwel dat de overeenkomsten over aangelegenheden in verband met het bewijs in een gesloten netwerk verwijzen naar de bepalingen van deze wet. Het Belgisch interbancair net, Isabel, is bijvoorbeeld een gesloten netwerk want de certificaten worden voor welbepaalde toepassingen gebruikt, het aantal gebruikers is relatief klein en hun onderlinge juridische betrekkingen alsook hun relaties met de dienstverlener worden bij overeenkomst geregeld.

Art. 4

Volgens paragraaf 1 « kan een certificatiedienstverlener niet verplicht worden een accreditatie aan te vragen voor de uitoefening van zijn activiteiten ». Deze paragraaf bevestigt het principe van het vrije accreditatiesysteem op grond waarvan het een certificatiedienstverlener vrij staat al dan niet een accreditatie aan te vragen.

Een certificatiedienstverlener kan slechts een accreditatie verkrijgen en behouden als hij voldoet aan de voorwaarden bepaald in artikel 5 van de wet en als hij bovendien in staat is alle verplichtingen opgelegd in de rest van de wet na te komen. Het Bestuur waakt over de naleving van deze voorwaarden.

Volgens paragraaf 2 kan « niemand verplicht worden een elektronische handtekening te gebruiken ». Aan eenieder moet dus de keuze worden gelaten om met de hand te ondertekenen of om een elektronische handtekening te gebruiken.

Krachtens § 3 is « de keuze een beroep te doen op een geaccrediteerde certificatiedienstverlener vrij ». Een persoon die beslist een beroep te doen op een elektronische handtekening moet vrij gelaten worden om een certificaat te ontvangen van een al dan niet geaccrediteerde certificatiedienstverlener. Het kan echter gebeuren dat sommige relaties of verrichtingen een zekere graad van veiligheid en betrouwbaarheid vereisen, bijvoorbeeld bij de overdracht van gegevens tussen burgers en het Bestuur of tussen consumenten en verkopers. In dergelijke gevallen zou een persoon die elektronisch wenst te ondertekenen, door of krachtens een wet, een decreet of een ordonnantie, kunnen worden verplicht een beroep te doen op een handtekening, dit wil zeggen een geavanceerde elektronische handtekening gecombineerd met een gekwalificeerd certificaat afgegeven door een geaccrediteerde certificatiedienstverlener.

Le paragraphe 2 précise que la loi ne s'adresse qu'aux prestataires de service de certification qui exercent leurs activités en réseaux ouverts. Pour les signatures électroniques utilisées en réseaux fermés, le principe de la liberté contractuelle prévaut. Rien n'empêche toutefois que les conventions régissant les questions relatives à la preuve en réseau fermé renvoient aux dispositions de la présente loi. Le réseau interbancaire belge, Isabel, constitue par exemple un réseau fermé dans la mesure où les certificats font l'objet d'applications déterminées, le nombre d'utilisateurs est relativement limité et ceux-ci voient leur relation juridique entre eux ainsi qu'avec le prestataire réglée par convention.

Art. 4

Selon le premier paragraphe, « nul prestataire de service de certification ne peut être contraint de demander une accréditation pour exercer ses activités ». Ce paragraphe consacre le principe du système libre d'accréditation selon lequel un prestataire de service de certification doit être libre de demander ou pas une accréditation.

Un prestataire de service de certification ne pourra obtenir et maintenir une accréditation que s'il respecte les conditions fixées par l'article 5 de la loi ainsi que s'il est en mesure de satisfaire à l'ensemble des obligations stipulées par le reste de la loi. L'Administration exerce la surveillance du respect de ces conditions.

Selon le paragraphe 2, « Nul ne peut être contraint de signer électroniquement ». Dès lors toute personne doit garder le libre choix d'utiliser sa signature manuscrite ou de recourir à une signature électronique.

En vertu du § 3, « le choix de recourir à un prestataire de service de certification accrédité ou non est libre ». La personne qui décide de recourir à une signature électronique doit rester libre de se faire délivrer un certificat par un prestataire de service de certification accrédité ou non. Toutefois il peut arriver que certaines relations ou transactions exigent un certain niveau de sécurité et de fiabilité. Tel pourrait être le cas du transfert de données entre citoyen et administration ou entre consommateur et vendeur. Dans de telles hypothèses, il pourrait être possible d'obliger, par ou en vertu d'une loi, d'un décret ou d'une ordonnance, une personne désirant signer électroniquement, de recourir à une signature soit une signature électronique avancée combinée à un certificat qualifié émis par un prestataire de service de certification accrédité.

Paragraaf 4 wil een verband leggen tussen, enerzijds, de hervorming van de regels over het bewijs zoals bepaald in het Burgerlijk Wetboek, meer bepaald de invoering van de open en functionele definitie van het begrip handtekening en, anderzijds, deze wet. Immers, elke geavanceerde elektronische handtekening gecombineerd met een gekwalificeerd certificaat — en dus afgegeven door een geaccrediteerde certificatiedienstverlener en aangemaakt door een veilig middel voor het aanmaken van een handtekening — is een handtekening in de zin van artikel 1322, 2e lid van het Burgerlijk Wetboek en voldoet dus aan de diverse eisen die aan een handtekening worden gesteld, zelfs indien een rechter zich over deze laatste niet kan uitspreken. Er kan worden gesteld dat de beveiliging die voor de certificatiedienstverleners is opgezet de geavanceerde elektronische handtekening een veiligheids- en betrouwbaarheidsgraad verschaft die minstens gelijk is aan die van een handgeschreven handtekening.

In dit stadium moet worden onderstreept dat een certificaat met de bij artikel 12 bepaalde inhoud (bijlage I bij het voorstel van richtlijn), behoudens artikel 12, 1°, kan worden afgegeven zowel door een geaccrediteerd certificatiedienstverlener als door een niet-geaccrediteerd certificatiedienstverlener die evenwel zou bewerken dat hij voldoet aan de accreditatievoorwaarden (zie bijlage II van het ontwerp van richtlijn) zonder daarvoor een aanvraag te hebben ingediend. Wel blijft er een fundamenteel verschil bestaan tussen die twee hypotheses omdat enkel een elektronische handtekening die steunt op een certificaat waarvan de inhoud overeenstemt met artikel 12 en dat is afgegeven door een geaccrediteerd certificatiedienstverlener automatisch zal worden gelijkgeschakeld met een handgeschreven handtekening zoals bepaald bij artikel 4 § 4, en zulks door de uiterst beveiligde omstandigheden die gepaard gaan met de aanmaak ervan. Dat wil niet zeggen dat een elektronische handtekening die steunt op een certificaat waarvan de inhoud beantwoordt aan artikel 12 en die is afgegeven door een niet-geaccrediteerde certificatiedienstverlener maar die desondanks toch voldoet aan de eisen in verband met de accreditatie (zie bijlage II van het ontwerp van richtlijn) geen enkele juridische erkenning zou genieten (in dit geval wat de ontvankelijkheid betreft). Ze wordt echter niet automatisch gelijkgeschakeld met een handgeschreven handtekening, maar er wordt verondersteld dat daadwerkelijk is bewezen dat aan de voorwaarden is voldaan.

Die verschillende behandeling is te verklaren door praktische en veiligheidsoverwegingen. De geaccrediteerde certificatiedienstverleners worden voortdurend door het Bestuur gecontroleerd en verrichten hun werk in optimale betrouwbaarheids- en veiligheidsomstandigheden. Een dienstverlener die zich beroept op een certificaat afgegeven door een geaccrediteerd

Le paragraphe 4 poursuit l'objectif d'établir un lien entre d'une part, la réforme des règles de preuve du Code civil et plus spécifiquement l'introduction de la définition ouverte et fonctionnelle du concept de signature et d'autre part, la présente loi. En effet, constitue une signature au sens de l'article 1322, alinéa 2 du Code civil et donc remplit les différentes fonctions assignées à la signature sans que le juge ne puisse apprécier ces dernières, toute signature électronique avancée combinée à un certificat qualifié, et donc émis par un prestataire de service de certification accrédité et créée par un dispositif sécurisé de création de signature. On peut considérer que le dispositif sécuritaire qui entoure les prestataires de service de certification accrédités confère à la signature électronique avancée un niveau de sécurité et de fiabilité au moins équivalent à la signature manuscrite.

Il convient de préciser à ce stade que un certificat ayant le contenu prévu à l'article 12 (annexe I de la proposition de directive), hormis l'article 12, 1°, peut être délivré tant par un prestataire de service de certification accrédité que par un prestataire de service de certification non accrédité qui prétendrait toutefois satisfaire aux conditions d'accréditation (Cf. annexe II du projet de directive) mais sans avoir fait la demande de cette dernière. Il n'en demeure pas moins une différence fondamentale entre ces deux hypothèses dans la mesure où seule une signature électronique reposant sur un certificat ayant un contenu conforme à l'article 12 émis par un prestataire de service de certification accrédité bénéficiera de l'assimilation automatique à la signature manuscrite prévue à l'article 4, § 4, et ce en raison de l'environnement extrêmement sécurisé qui entoure sa création. Ceci ne veut pas dire qu'une signature électronique reposant sur un certificat ayant un contenu conforme à l'article 12 et émis par un prestataire de service de certification non accrédité mais qui satisfait néanmoins aux exigences relatives à l'accréditation (Cf. annexe II du projet de directive) ne puisse pas bénéficier d'une certaine reconnaissance juridique (en l'occurrence sur le plan de la recevabilité), mais l'assimilation à une signature manuscrite ne sera pas automatique mais supposera que la preuve du respect des dites conditions ait été effectivement rapportée.

La distinction de traitement répond à des considérations pratiques et de sécurité. Soumises au contrôle permanent de l'Administration, les prestataires de service de certification accrédités opèrent dans des conditions de fiabilité et de sécurité optimales. Celui qui se prévaut d'un certificat émis par un prestataire de service accrédité peut de ce fait être dispensé d'apporter

certificatiedienstverlener kan dus worden vrijgesteld van de verplichting om het bewijs van zijn kwaliteit te leveren. Dat geldt niet als het certificaat werd afgegeven door een dienstverlener die zich niet heeft willen onderwerpen aan de controle die gepaard gaat met de accreditatie. In dat geval wordt door niemand meer geverifieerd noch geattesteerd dat aan de eisen in verband met het afgeven van certificaten is voldaan. Om de rechter hiervan eventueel te overtuigen, moet daarvan dus het bewijs worden geleverd.

Meer algemeen moet voorts worden vermeld dat, ook al komt een « gewone » elektronische handtekening die niet voldoet aan de eisen van artikel 4 § 4 niet in aanmerking voor de assimilatieclausule, zij toch niet kan worden verworpen louter en alleen omdat zij een elektronische vorm aanneemt, of omdat zij niet gebaseerd is op een gekwalificeerd certificaat afgegeven door een geaccrediteerde certificatiedienstverlener, of nog omdat zij niet is aangemaakt door een veilig middel voor het aanmaken van een handtekening. Elke elektronische handtekening is dus ontvankelijk in geval van betwisting. Om evenwel te voldoen aan de eisen van artikel 4 § 4 moet de persoon die zich beroept op een elektronisch ondertekend document de rechter overtuigen van de bewijskracht ervan. Er bestaat een parallellisme met het begrip « begin van bewijs door geschrift », waarvan sprake is in artikel 1347 van het Burgerlijk Wetboek. Het geschrift bedoeld in artikel 1347 voldoet niet aan de vereisten om te worden beschouwd als een bewijsstuk in de zin van artikel 1341 van het Burgerlijk Wetboek, doch beantwoordt aan sommige specifieke kenmerken inzake vorm, oorsprong en inhoud. Hiervoor verwijzen wij naar de overvloedige rechtsleer terzake.

Art. 5

Er moet onmiddellijk duidelijk gemaakt worden dat afdeling 1 betrekking heeft op geaccrediteerde certificatiedienstverleners. Daaruit volgt dat de artikelen 5 tot 17 slechts op hen van toepassing zijn. Niet-geaccrediteerde certificatiedienstverleners zijn dus niet strikt onderworpen aan deze bepalingen.

Artikel 5 legt de voorwaarden vast waaraan een certificatiedienstverlener verplicht is te voldoen om een accreditatie te verkrijgen en te behouden.

Paragraaf 1 bepaalt in algemene termen deze voorwaarden. Deze kunnen gepreciseerd worden door het koninklijk besluit bedoeld in paragraaf 2. Deze voorwaarden zijn in grote mate geïnspireerd op bijlage II van het voorstel van richtlijn.

Door aan deze voorwaarden te voldoen en door zich te onderwerpen aan een controle, toont de certificatiedienstverlener publiekelijk dat de gebruikers in hem geloof kunnen stellen en dat ze hem kunnen vertrouwen.

la preuve de sa qualité. Il n'en va plus de même, lorsque que le certificat a été émis par un prestataire de service qui n'a pas voulu se soumettre au contrôle lié à l'accréditation. La conformité aux exigences posées relativement à la délivrance des certificats n'est dans ce cas plus vérifiée ni attestée par personne. Afin d'en convaincre, le cas échéant, le juge, il appartiendra donc d'en faire la preuve.

Soulignons également et plus largement que si une signature électronique « ordinaire » qui ne satisfait pas aux conditions requises par l'article 4 § 4 ne peut bénéficier de la clause d'assimilation, elle ne pourra pas pour autant être rejetée pour le seul motif qu'elle se présente sous forme électronique, ou qu'elle ne repose pas sur un certificat qualifié délivré par un prestataire de service de certification accrédité, ou qu'elle n'est pas créée par un dispositif sécurisé de création de signature. Toute signature électronique est donc recevable en cas de litige. Toutefois, à défaut de répondre aux spécifications légales de l'article 4 § 4, il appartiendra à celui qui se prévaut du document signé électroniquement de convaincre le juge de sa valeur probante. Un parallélisme doit être établi avec la notion de commencement de preuve par écrit dont question à l'article 1347 du Code civil. L'écrit dont il est question à l'article 1347 ne présente pas les conditions requises pour être un acte probatoire au sens de l'article 1341 du Code civil, mais répond à certaines caractéristiques propres quant à sa forme, à son origine et à son contenu. Nous renvoyons à la doctrine abondante à ce sujet.

Art. 5

Il convient d'emblée de préciser que la section 1re est relative aux prestataires de service de certification accrédités. Il en résulte que les articles 5 à 17 ne s'appliquent qu'à ceux-ci. Les prestataires de service de certification non accrédités ne sont donc pas strictement soumis à ces dispositions.

L'article 5 fixe les conditions qui doivent impérativement être remplies par un prestataire de service de certification pour obtenir et conserver une accréditation.

Le paragraphe 1er détermine en termes généraux ces conditions. Celles-ci pourront être précisées par l'arrêté royal visé au paragraphe 2. Ces conditions sont en grande partie inspirées de l'annexe II de la proposition de directive.

En répondant à ces conditions et en acceptant de se soumettre à un contrôle, un prestataire de service de certification démontre publiquement la crédibilité et la confiance que les utilisateurs peuvent avoir en lui. Le

wen. Overwegende (11) van het voorstel van richtlijn toont aan dat het accreditatiesysteem (dat vrijwillig moet blijven) het mogelijk maakt de kwaliteit van de dienstverlening te verbeteren : « de vrijwillige-accreditatieregelingen, die beogen de dienstverlening te verbeteren, certificatiedienstverleners een passend kader kunnen bieden om hun diensten verder te ontwikkelen en het door de markt verlangde niveau van vertrouwen, veiligheid en kwaliteit te bereiken ». Dit betekent niet automatisch dat er geen vertrouwen kan gesteld worden in een niet-geaccrediteerde certificatiedienstverlener maar dan moet hij dit wel op een andere manier aantonen.

Om een accreditatie te verkrijgen moet een certificatiedienstverlener onder andere aantonen dat hij in staat is de eisen voorgeschreven door de wet na te leven (de informatie in artikel 8 verschaffen, een elektronisch register bijhouden dat permanent toegankelijk is en beantwoordt aan de eisen van artikel 10, op elk ogenblik gevolg geven aan een aanvraag tot herroeping, de eisen met betrekking tot het privé-leven eerbiedigen, enz.) en bewijs leveren dat hij voldoende betrouwbaar is om certificatiediensten te leveren, inzonderheid door een veiligheidsplan voor te leggen zoals bedoeld in punt 4.

Hij moet voldoende waarborgen leveren voor zijn integriteit en beschikbaarheid en de deskundigheid bezitten om zijn certificatie-activiteiten uit te oefenen.

Aangezien het vooral gaat om waarborgen voor zijn integriteit en beschikbaarheid moet de certificatiedienstverlener inzonderheid een betrouwbaar informaticasysteem en betrouwbare producten voor elektronische handtekening gebruiken (artikel 17). Dit impliceert ook dat de dienstverlener een elektronisch register bijhoudt dat voor iedereen permanent toegankelijk is en dat dit register beveiligd wordt tegen elke ongeoorloofde wijziging (artikel 10). Bovendien moet de certificatiedienstverlener proberen de vertrouwelijkheid van zijn gegevens voor het aanmaken van een handtekening die gebruikt worden om de afgegeven certificaten te tekenen, behoorlijk te beschermen. De certificatiedienstverlener moet vervolgens over de nodige deskundigheid beschikken om certificatie-activiteiten te verrichten. Daartoe stelt hij personeel tewerk dat beschikt over de specifieke kennis, ervaring en kwalificaties nodig voor het verlenen van diensten en, in het bijzonder, over de competentie op het vlak van het beheer, de gespecialiseerde kennis en de technologie van elektronische handtekeningen en een goede praktische kennis van de gepaste veiligheidsprocedures.

Hij moet over een onafhankelijk beheer beschikken ten opzichte van de gebruikers van de diensten. Als de certificatiedienstverlener het vertrouwen van het publiek wil behouden en versterken, moet hij zo onafhankelijk mogelijk zijn van de invloed van commerciële bedrijven of specifieke organisaties die zelf klant kunnen zijn bij een dienstverlener. Deze onafhankelijkheidsvoorwaarde

considérant (11) de la proposition de directive montre que le système d'accréditation (qui doit rester volontaire) permettra d'améliorer la qualité du service fourni : « les régimes volontaires d'accréditation visant à assurer un meilleur service fourni peuvent constituer pour les prestataires de service de certification le cadre propice à l'amélioration de leurs services afin d'atteindre le degré de confiance, de sécurité et de qualité exigés par l'évolution du marché ». Ceci ne signifie pas automatiquement que toute confiance doit être déniée à un prestataire de service de certification non accrédité mais encore faudra-t-il qu'il la démontre d'une autre manière.

Afin d'obtenir une accréditation, un prestataire de service de certification doit notamment montrer qu'il est capable de respecter les exigences prévues par la loi (fournir les informations de l'article 8, tenir un annuaire électronique accessible en permanence et répondant aux exigences de l'article 10, répondre en permanence à une demande de révocation, respecter les exigences relatives à la vie privée, etc.) et faire la preuve qu'il est suffisamment fiable pour fournir des services de certification, notamment en présentant un plan de sécurité tel que visé au point 4.

Il doit présenter des garanties d'intégrité et de disponibilité suffisantes et posséder l'expertise pour exercer ses activités de certification.

S'agissant tout d'abord des garanties d'intégrité et de disponibilité, le prestataire de service de certification doit notamment utiliser un système informatique et des produits de signature électronique fiables (article 17). Cela implique aussi que le prestataire tienne un annuaire électronique accessible en permanence à toute personne et que cet annuaire soit protégé contre toute modification non autorisée (article 10). En outre, le prestataire de service de certification doit faire en sorte de protéger adéquatement la confidentialité de ses données afférentes à la création de signature utilisées afin de signer les certificats qu'il émet. Le prestataire de service de certification doit ensuite posséder l'expertise nécessaire pour assurer ses activités de certification. À cette fin, il emploie du personnel ayant les connaissances spécifiques, l'expérience et les qualifications nécessaires à la fourniture des services et, en particulier, des compétences au niveau de la gestion, des connaissances spécialisées en technologie des signatures électroniques et une bonne pratique des procédures de sécurité appropriées.

Il doit disposer d'une gestion indépendante vis-à-vis des utilisateurs du service. Si il veut maintenir et renforcer la confiance que le public a en lui, le prestataire de service de certification doit être le plus indépendant possible de l'influence d'entreprises commerciales ou d'organisations spécifiques, qui pourraient elles mêmes être clientes du prestataire. Toutefois, cette condition

moet echter soepel toegepast worden. Zij moet niet noodzakelijk financieel zijn, een organisatorische onafhankelijkheid zou moeten volstaan.

De voorwaarden om de interne werking van de certificatiesystemen te garanderen zullen nader worden bepaald door het koninklijk besluit bedoeld in de tweede paragraaf.

Hij moet ook een infrastructuur opstellen die een geschikt veiligheids- en betrouwbaarheidsniveau verschaft. Deze eis zal het onderwerp zijn van een veiligheidsplan dat zal worden onderzocht en geverifieerd door het Bestuur of door een entiteit die over de nodige competentie beschikt zoals hierboven vermeld.

De certificatiedienstverlener moet over voldoende financiële waarborgen beschikken om zijn activiteiten uit te oefenen en, in voorkomend geval, de gebruikers schadeloosstellen die schade geleden hebben ten gevolge van de verplichtingen die hem werden opgelegd door of krachtens deze wet. Ten dien einde zal hij zich laten dekken door een geschikte verzekering.

De door de dienstverlener toegepaste tarieven moeten duidelijk worden vermeld en mogen in geen geval discriminerend zijn.

Ten slotte moet de dienstverlener de minimale normen naleven met betrekking tot de vertrouwelijkheid en de integriteit van de door de certificaathouder verstrekte informatie en de voorwaarden met betrekking tot de dienst voor het behandelen van klachten van klanten. De certificatiedienstverlener moet ook de regels naleven betreffende de informatie die hij over zijn diensten en over de door hem afgegeven certificaten moet bijhouden.

Het koninklijk besluit bedoeld in paragraaf 2 preciseert, in voorkomend geval, de voorwaarden bedoeld in § 1 en bepaalt de technische regels voor de afgifte van de accreditatie.

Art. 6

Artikel 6 vereist geen commentaar.

Art. 7

§ 1. De certificatiedienstverlener moet de overeenstemming nagaan tussen de gegevens voor het aanmaken en het verifiëren van de handtekening van de kandidaat-houder. Vooraleer hij de dienstverlener het certificaat afgeeft, moet hij de complementariteit van deze gegevens nagaan. Door de afgifte van het certificaat waarborgt de dienstverlener het bestaan van het verband tussen de gegevens voor het aanmaken en het verifiëren van de handtekening van de houder en bevestigt hij dat zij bij elkaar passen.

d'indépendance doit être appréciée souplement. Elle ne doit pas nécessairement être financière, une indépendance organisationnelle devrait suffire.

Les conditions visant à assurer l'interopérabilité des systèmes de certification seront précisément fixées par l'arrêté royal visé au deuxième paragraphe.

Il doit également mettre en place une infrastructure qui présente un niveau de sécurité et de fiabilité adéquat. Cette exigence fera l'objet d'un plan de sécurité qui sera examiné et vérifié par l'Administration ou par une entité qui dispose des compétences nécessaires, comme évoqué ci-dessus.

Le prestataire de service de certification doit posséder des garanties financières suffisantes pour exercer ses activités et, le cas échéant, indemniser les utilisateurs ayant subi un dommage suite à l'inexécution des obligations qui lui sont imposées par ou en vertu de la présente loi. À cet effet, il se couvrira par une assurance appropriée.

Les tarifs appliqués par le prestataire doivent être exprimés de manière claire et ne peuvent en aucun cas être discriminatoires.

Enfin, le prestataire doit respecter les normes minimales relatives à la confidentialité et à l'intégrité des informations procurées par le titulaire de certificat et les conditions concernant le service du traitement de plaintes émanant de clients. Il doit également respecter les règles relatives à l'information que le prestataire de service de certification est tenu de conserver concernant ses services et les certificats délivrés par lui.

L'arrêté royal visé au paragraphe 2 précise, le cas échéant, les conditions visées au § 1er et fixe les modalités techniques relatives à la délivrance de l'accréditation.

Art. 6

L'article 6 ne nécessite pas de commentaires.

Art. 7

§ 1er. Le prestataire de service de certification est tenu de vérifier la concordance entre les données afférentes à la création et à la vérification de signature du candidat-titulaire. Préalablement à la délivrance du certificat, le prestataire est tenu de tester la complémentarité de ces données. Par la délivrance du certificat, le prestataire garantit l'existence du lien entre les données afférentes à la création et à la vérification de signature du titulaire et confirme ainsi qu'elles sont appariées.

§ 2. De gegevens voor het aanmaken en het verifiëren van een handtekening mogen door de kandidaat-houder worden verschaft of door de certificatiedienstverlener worden gegenereerd. In beide gevallen moet — bij het genereren van die gegevens — een betrouwbaar systeem als bedoeld in de artikelen 11 en 17 worden gebruikt, om te zorgen voor de vertrouwelijkheid, de integriteit, de beschikbaarheid en het rechtmatig gebruik van die gegevens.

Bovendien mag de certificatiedienstverlener, bij het genereren, de gegevens voor het aanmaken van een handtekening niet registreren, bewaren of opnieuw samenstellen, om te vermijden dat hij de niet-gemachtigde houder of bewaarder van deze gegevens wordt.

§ 3. Zodra een natuurlijke persoon of een rechtspersoon erom vraagt, moet de certificatiedienstverlener een of meer gekwalificeerde certificaten afgeven. Aangezien de voornaamste rol van de geaccrediteerde dienstverlener erin bestaat gekwalificeerde certificaten af te geven, zou het onredelijk geweest zijn hem de bevoegdheid te geven die afgifte naar goeddunken te weigeren of niet. Hierdoor wil men het elke burger mogelijk maken een gekwalificeerd certificaat te bekomen.

Dit veronderstelt dat de dienstverlener vooraf de identiteit van de persoon — of het nu een natuurlijk persoon dan wel een rechtspersoon is — die de aanvraag indient en, in voorkomend geval, de specifieke hoedanigheden van die persoon nagaat. Die controle moet gebeuren met geschikte middelen : dit impliceert dat de dienstverlener steunt op een moeilijk te vervalsen document of op het toetsen van verschillende documenten. Daartoe kan hij een beroep doen op de hulp van registratie-overheden (gemeenten, De Post, kamers van koophandel, orden van vrije beroepen, enz.).

Indien het certificaat aan een rechtspersoon wordt afgegeven, onderzoekt de dienstverlener vooraf de identiteit van de rechtspersoon, zoals hierboven aangegeven, maar ook de identiteit en de vertegenwoordigingsbevoegdheid van de natuurlijke persoon of personen die zich bij hem aanmelden. Op grond van de wet mag een rechtspersoon immers certificaathouder worden. Aangezien rechtspersonen evenwel niet materieel bestaan, kunnen zij ook geen concrete stappen doen om een certificaat aan te vragen. Die stappen worden dan gedaan door een (of meer) natuurlijke personen die handelen in naam en voor rekening van de rechtspersoon. Om misbruiken en fraude te vermijden, moet de dienstverlener uiteraard controle uitoefenen over de identiteit van deze natuurlijke persoon en diens bevoegdheid om de rechtspersoon die certificaathouder wenst te zijn, te vertegenwoordigen. De informatie over de identiteit en vertegenwoordigingsbevoegdheid van de natuurlijke persoon is niet bestemd om op het certificaat te worden vermeld.

Die verplichting tot afgifte valt echter weg wanneer de certificatiedienstverlener ernstig twijfelt aan de identiteit en/of aan een specifieke hoedanigheid van de natuurlijke of rechtspersoon en hij dit niet kan verifiëren aan de hand van rede-

§ 2. Les données afférentes à la création et à la vérification de signature peuvent être fournies par le candidat titulaire ou générées par le prestataire de service de certification. Dans ces deux cas, un système fiable, tel que visé aux articles 11 et 17, doit être utilisé lors de la génération de ces données afin d'assurer la confidentialité, l'intégrité, la disponibilité et l'utilisation légitime de celles-ci.

Lors du processus de génération, le prestataire de service de certification ne peut par ailleurs enregistrer, conserver ou reconstituer les données afférentes à la création de signature de façon à ne pas devenir le détenteur ou le dépositaire non autorisé de ces données.

§ 3. Dès qu'une personne physique ou morale en fait la demande, le prestataire de service de certification est tenu de délivrer un ou plusieurs certificats qualifiés. En effet, le rôle principal du prestataire accrédité étant de délivrer des certificats qualifiés, il eut été déraisonnable de lui laisser le pouvoir discrétionnaire de refuser ou non cette délivrance. On veut ainsi permettre à tout citoyen d'obtenir un certificat qualifié.

Cela suppose que le prestataire vérifie préalablement l'identité de la personne, qu'elle soit physique ou morale, qui effectue la demande ainsi que, le cas échéant, les qualités spécifiques de cette personne. Cette vérification doit se faire par des moyens appropriés : cela implique que le prestataire se base sur un document difficilement falsifiable ou sur le recoupement de différents documents. Il peut pour se faire s'adjoindre l'aide d'autorités d'enregistrement (Communes, La Poste, chambres de commerce, ordres professionnels, etc.).

Si le certificat est délivré à une personne morale, le prestataire vérifie préalablement l'identité de la personne morale comme prévu ci-dessus mais aussi l'identité et le pouvoir de représentation de la (ou des) personne(s) physique(s) qui se présente(nt) à lui. En effet, la loi autorise une personne morale à devenir titulaire de certificat. Toutefois, ces dernières n'ayant pas d'existence matérielle, elles ne sont pas capables d'effectuer concrètement la démarche de demande d'un certificat. Cette démarche sera accomplie par une (ou plusieurs) personne physique qui agit au nom et pour le compte de la personne morale. Il est évident que, pour éviter les abus ou les fraudes, le prestataire doit vérifier l'identité de cette personne physique et son pouvoir de représenter la personne morale qui désire être titulaire du certificat. Cependant, les informations relatives à l'identité et au pouvoir de représentation de la personne physique ne sont pas destinées à être inscrites sur le certificat.

Toutefois cette obligation de délivrance est levée lorsque le prestataire de service de certification a de sérieux doutes quant à l'identité ou/et une qualité spécifique de la personne physique ou morale et qu'il ne peut

lijke middelen. Voor een dienstverlener kan het bijvoorbeeld moeilijk zijn het bestaan en de identiteit te controleren van een vennootschap die haar zetel heeft in een derde land met een juridisch stelsel volledig verschillend van het onze of de identiteit van een natuurlijk persoon te verifiëren indien hij weigert de bewijskrachtige documenten te bezorgen om deze controle te verrichten.

In de andere gevallen zou een dienstverlener zich moeilijk kunnen beroepen op het feit dat hij over geen redelijke middelen beschikt om enkel de identiteit na te gaan van een natuurlijke persoon. De verplichting een certificaat zonder specifieke hoedanigheid af te geven aan een natuurlijke persoon is dus bijna absoluut.

Deze afzwakking van de verplichting tot afgifte is verantwoord door het feit dat men een dienstverlener niet kon verplichten een certificaat af te geven, de inhoud ervan te bevestigen en hem aldus aansprakelijk te stellen indien hij er niet toe in staat is de in het certificaat vermelde informatie correct te controleren.

§ 4. De certificatiedienstverlener treft maatregelen tegen het namaken van certificaten. Die verplichting is vanzelfsprekend en er wordt van ambtswege aan voldaan omdat een certificaat noodzakelijkerwijze moet worden ondertekend door de dienstverlener, waardoor het beveiligd is en beschermd tegen namaak of tegen elke ongeoorloofde wijziging (artikel 2, 2° en 12).

Art. 8

Ter herinnering : de wet wil het vertrouwen in de geavanceerde elektronische handtekening versterken en het gebruik ervan bevorderen. Het correct informeren van de gebruiker van de diensten draagt bij tot het bereiken van dat doel. De geaccrediteerde certificatiedienstverlener moet aldus alle informatie bezorgen die noodzakelijk is voor het correct en veilig gebruik van zijn diensten.

Die verplichting vormt in zekere zin een wettelijke bevestiging van de verplichting van de handelaar om advies te verstrekken. Zij is des te meer verantwoord omdat de elektronische handtekening een technische en ingewikkelde zaak is.

De informatie die de dienstverlener moet bezorgen, is vermeld in artikel 8 en vergt geen commentaar. Laten wij gewoon noteren dat die informatie in een « gemakkelijk verstaanbare taal » moet worden verstrekt. Dit impliceert niet dat de dienstverlener die informatie in alle talen moet geven, maar wel in de taal of talen van het land waar hij gevestigd is, alsmede in een of meer internationale talen (Engels, Frans en Spaans bijvoorbeeld). Het is immers moeilijk denkbaar dat een in België gevestigde certificatiedienstverlener zich ertoe beperkt die informatie in het Engels mee te delen. Die informatie moet ook in het Frans, in het Nederlands en in het

le vérifier par des moyens raisonnables. Par exemple, il peut être difficile pour un prestataire de vérifier l'existence et l'identité d'une société ayant son siège social dans un pays tiers ayant un régime juridique totalement différent du nôtre ou de vérifier l'identité d'une personne physique si celle-ci refuse de lui communiquer les documents probants pour effectuer cette vérification.

Notons néanmoins que dans les autres cas, un prestataire pourrait difficilement se prévaloir du fait qu'il ne dispose pas de moyens raisonnables pour vérifier la seule identité d'une personne physique. L'obligation de délivrance d'un certificat sans qualité spécifique à une personne physique est donc presque absolue.

Ce tempérament à l'obligation de délivrance se justifie par le fait qu'on ne pouvait obliger un prestataire à délivrer un certificat, confirmer son contenu et engager ainsi sa responsabilité si il n'est pas en mesure de vérifier correctement les informations obligatoires contenues dans le certificat.

§ 4. Le prestataire de service de certification prend des mesures contre la contrefaçon des certificats. Cette obligation va de soi et est d'office satisfaite dans la mesure où un certificat doit nécessairement être signé par le prestataire et est ainsi sécurisé et protégé contre la contrefaçon ou toute modification non autorisée (article 2, 2° et 12).

Art. 8

Rappelons que l'objectif de la loi est de renforcer la confiance et de promouvoir l'utilisation de la signature électronique avancée. L'information correcte de l'utilisateur des services contribue à la réalisation de cet objectif. Le prestataire de service de certification accrédité a ainsi l'obligation de procurer toute information nécessaire à l'utilisation correcte et sûre de ses services.

Cette obligation constitue en quelque sorte une consécration légale de l'obligation de conseil qui pèse sur le professionnel. Elle se justifie d'autant plus que la signature électronique est une matière technique et complexe.

Les informations que le prestataire doit fournir sont indiquées à l'article 8 et ne nécessitent pas de commentaires. Notons simplement que ces informations doivent être procurées dans une « langue aisément compréhensible ». Cela n'implique pas que le prestataire doivent fournir ces informations dans toutes les langues mais doivent au moins les fournir dans la ou les langues du pays dans lequel il est établi ainsi que dans une ou plusieurs langues internationales (anglais, français et espagnol par exemple). On imagine mal en effet qu'un prestataire de service de certification établi en Belgique se li-

Duits worden gegeven, maar men kan niet eisen dat zij ook in het Pools of in het Japans wordt verstrekt.

Bovendien moet die informatie worden verstrekt door middel van een duurzame mededeling of een duurzame drager. Men beoogt met die bewoordingen, overgenomen uit het voorstel van richtlijn, nieuwe vormen van communicatie, die de traditionele geschriften kunnen vervangen. Die nieuwe vormen van communicatie kunnen rechtsgeldig de plaats innemen van een geschrift, op voorwaarde dat het gebruikte instrument voldoende waarborgen inzake betrouwbaarheid biedt en de geadresseerde probleemloos kennis kan nemen van de aldus verspreide informatie. Het voorstel van richtlijn betreffende de commercialisering op afstand van financiële diensten bij consumenten omschrijft het begrip duurzame drager bijvoorbeeld als « elk instrument dat het de consument mogelijk maakt informatie te bewaren, zonder dat hij die informatie zelf moet registreren; in de zin van die richtlijn zijn inzonderheid duurzame dragers bedoeld : computerdiskettes, CD-ROM's, alsmede de harde schijf van de computer van de consument waarop *e-mails* zijn opgeslagen ».

Overigens beklemtoont het voorstel van richtlijn dat de gegevens die op een duurzame drager zijn opgeslagen toegankelijk moeten zijn, dat wil zeggen dat de geadresseerde gemakkelijk kennis moet kunnen nemen van die gegevens en ze gemakkelijk moet kunnen bewaren. Men kan het dus niet over een duurzame drager hebben indien de informatie via een webpagina wordt meegedeeld, vooral wanneer er niets wordt gedownload.

De certificatiedienstverlener moet, om de in artikel 8 vermelde verplichting na te leven, een nuttig, duidelijk en verstaanbaar gebruikershandboek opstellen, op papier en/of elektronisch (opgeslagen op een diskette, een CD-ROM enz.) dat hij systematisch aan de gebruikers van zijn diensten moet overhandigen.

Art. 9

De certificatiedienstverlener verschaft een exemplaar van het certificaat aan de kandidaat-houder, die — voor hij het aanvaardt — de inhoud ervan controleert.

Wanneer het certificaat is aanvaard :

— wordt de kandidaat-houder houder van het certificaat;

— schrijft de certificatiedienstverlener het certificaat in het elektronisch register in.

Vanaf dat ogenblik is het certificaat tegenstelbaar aan derden.

mite à communiquer ces informations en anglais. Elles doivent en outre être fournies en français, néerlandais ainsi qu'en allemand mais on ne peut exiger qu'elles soient fournies en polonais ou japonais.

De plus, ces informations doivent être procurées par un moyen de communication durable ou support durable. On vise par ces termes, repris de la proposition de directive, de nouvelles formes de communication susceptibles de remplacer l'écrit traditionnel. Ces nouvelles formes de communication peuvent valablement se substituer à un écrit pourvu que l'instrument utilisé présente des garanties de fiabilité suffisantes, et que son destinataire puisse prendre connaissance sans difficulté des informations ainsi diffusées. La proposition de directive concernant la commercialisation à distance des services financiers auprès des consommateurs définit par exemple la notion de support durable comme « tout instrument permettant au consommateur de conserver des informations, sans qu'il soit tenu de procéder lui même à l'enregistrement de ces informations; sont notamment des supports durables au sens de cette directive les disquettes informatiques, les CD-ROM, ainsi que le disque dur de l'ordinateur du consommateur stockant des courriers électroniques ».

Par ailleurs, la proposition de directive insiste sur le fait que les données stockées sur support durable doivent être accessibles, c'est-à-dire que leur destinataire doit être en mesure d'en prendre connaissance aisément et de les conserver. On ne parlera donc pas de support durable si les informations sont communiquées par le biais d'une page web, spécialement s'il n'y a aucun téléchargement.

Afin de satisfaire à son obligation de l'article 8, le prestataire de service de certification rédigera utilement un manuel d'utilisation clair et compréhensible, en version papier et/ou électronique (stocké sur une disquette, un CD-ROM, etc.), qu'il remettra systématiquement aux utilisateurs de ses services.

Art. 9

Le prestataire de service de certification fournit un exemplaire du certificat au candidat titulaire pour acceptation de celui-ci notamment pour en vérifier le contenu.

Une fois le certificat accepté :

— le candidat titulaire devient titulaire de certificat;

— le prestataire de service de certification inscrit le certificat dans l'annuaire électronique.

Le certificat est, dès ce moment, opposable aux tiers.

Art. 10

De certificatiedienstverlener moet een elektronisch register bijhouden dat ten minste vermeldt :

— de afgegeven certificaten en het tijdstip waarop zij werden afgegeven;
— het tijdstip waarop zij aflopen;
— in voorkomend geval, het tijdstip waarop zij worden herroepen.

Het elektronisch register moet :
— bijgewerkt worden;
— snel en voor iedereen permanent toegankelijk zijn, en dit langs elektronische weg;
— beschermd zijn tegen iedere ongeoorloofde wijziging.

Het tweede lid van artikel 10 is rechtstreeks overgenomen van bijlage II van het voorstel van richtlijn en preciseert het laatste punt dat hierboven werd behandeld (beschermd zijn tegen iedere ongeoorloofde wijziging). Dit tweede lid voegt een eis toe betreffende de persoonlijke levenssfeer : « de certificaten moeten uitsluitend publiekelijk beschikbaar zijn *voor onderzoek* in die gevallen waarvoor de certificaathouder toestemming heeft gegeven ». Er bestaat een analogie met de telefoongids : een abonnee moet kunnen weigeren dat iedereen via opzoekingen toegang kan hebben tot het geheel van de certificaten en aldus tot gegevens met een persoonlijk karakter, zonder de toestemming van de titularis. Het spreekt echter voor zich dat de geadresseerde van een elektronisch ondertekende boodschap altijd toegang moet kunnen hebben tot het register om een specifiek certificaat op te zoeken en na te gaan of dat certificaat niet is herroepen of afgelopen. Uiteraard kan dit gebeuren zonder een algemeen onderzoek, maar door het reeksnummer van het certificaat op te geven. Het reeksnummer werd vooraf meegedeeld door de afzender, waardoor wordt vermeden dat men toegang moet kunnen hebben tot de andere certificaten die geen enkel verband hebben met de toegestuurde boodschap.

Art. 11

Artikel 11 bepaalt de vereisten betreffende de veilige middelen voor het aanmaken van een elektronische handtekening, die rechtstreeks zijn overgenomen uit bijlage III van het voorstel van richtlijn. Die vereisten zijn in zeer algemene termen uitgedrukt en het is thans niet gemakkelijk middelen te bepalen voor het aanmaken van een elektronische handtekening die voldoen aan die eisen. Volgens artikel 3, punt 5 van het voorstel van richtlijn zal de commissie evenwel referentienummers van algemeen erkende normen voor producten voor elektronische handtekeningen vaststellen en in het publicatieblad van de Europese Gemeenschappen bekendmaken. Dat zal tot gevolg hebben dat, wanneer een product voor elektronische handtekening — en dus een middel voor het aanmaken van een elektronische handtekening

Art. 10

Le prestataire de service de certification a l'obligation de conserver un annuaire électronique qui énumère au moins :
— les certificats délivrés ainsi que le moment de leur émission;
— le moment de leur expiration;
— le cas échéant, le moment de leur révocation.

Le registre électronique doit impérativement :
— être tenu à jour;
— être accessible rapidement et en permanence à toute personne, et ce par voie électronique;
— être protégé contre toute altération ou modification non autorisée.

Le deuxième alinéa de l'article 10 est directement repris de l'annexe II de la proposition de directive et précise le dernier point évoqué ci-dessus (être protégé contre toute altération ou modification non autorisée). Ce deuxième alinéa ajoute une exigence relative à la vie privée : « les certificats ne doivent être disponibles au public *pour des recherches* que dans les cas où le titulaire du certificat a donné son consentement ». Une analogie peut être faite avec l'annuaire téléphonique : un abonné doit pouvoir refuser que toute personne puisse accéder par des recherches à l'ensemble des certificats et ainsi à des données à caractère personnel sans le consentement du titulaire. Toutefois, il est évident que le destinataire d'un message signé électroniquement doit pouvoir accéder à tout moment à l'annuaire pour rechercher un certificat précis et vérifier si celui-ci n'est pas révoqué ou expiré. Il est vrai que cela peut se faire sans effectuer de recherche généralisée mais en indiquant le numéro de série du certificat, préalablement communiqué par l'émetteur du message, ce qui évite de pouvoir accéder aux autres certificats n'ayant aucun lien avec le message envoyé.

Art. 11

L'article 11 stipule les exigences relatives aux dispositifs sécurisés de création de signature électronique, qui sont directement reprises de l'annexe III de la proposition de directive. Ces exigences sont libellées en termes très généraux et il n'est pas aisé de déterminer aujourd'hui les dispositifs de création de signature électronique qui satisfont à ces exigences. Toutefois, selon l'article 3, point 5 de la proposition de directive, la commission attribuera, et publiera au « *Journal officiel des commerçants européens* », des numéros de référence de normes généralement admises pour des produits de signature électronique. Cela aura pour effet que lorsqu'un produit de signature électronique, et donc un dispositif de création de signature électronique, sont con-

— in overeenstemming is met die normen, dit product verondersteld wordt te voldoen aan de eisen van bijlage III, dat wil zeggen aan de eisen van artikel 11 van deze wet. Het bestuur is belast met het volgen van de werkzaamheden op Europees niveau, opdat de in België gebruikte middelen voor het aanmaken van een handtekening aan die normen zouden beantwoorden. Anderzijds kan een Belgische certificatiedienstverlener pogen — in het kader van zijn accreditatieaanvraag — het bewijs te leveren dat de middelen die hij gebruikt voor het aanmaken van een handtekening aan die eisen voldoen.

Art. 12

Het certificaat bestaat uit de bevestiging van een of meer gegevens, voornamelijk het verband tussen de certificaathouder en de gegevens voor het verifiëren van een handtekening die overeenstemmen met de gegevens voor het aanmaken van een handtekening onder toezicht van de ondertekenaar. Ter herinnering : deze wet heeft tot doel de veiligheid van en het vertrouwen in het gebruik van de geavanceerde elektronische handtekening in een open netwerk te versterken (artikel 3). Gelet op het door de wet nagestreefde doel was het dus onontbeerlijk dat de wet de minimale informatie opsomde die in elk certificaat vermeld moet zijn tot staving van geavanceerde elektronische handtekeningen. In navolging van de richtlijn kwalificeert de wet die certificaten als « gekwalificeerde certificaten ».

Men vroeg zich af of elke certificatiedienstverlener dan wel enkel geaccrediteerde certificatiedienstverleners dergelijke certificaten mochten afgeven. Bijlage 2 van de richtlijn somt de eisen op waaraan de certificatiedienstverleners die gekwalificeerde certificaten afgeven, moeten voldoen. De Belgische wetgever maakt van die eisen voorwaarden voor de accreditatie van de dienstverleners. Het voorstel van richtlijn is enkel belangrijk en kan maar vertrouwen inboezemen indien de lidstaten, met inachtneming van het principe van de vrijheid om de certificatieactiviteit uit te oefenen, ook nog voor twee andere zaken zorgen. Enerzijds moeten de lidstaten zorgen voor een stelsel van accreditatie van certificatiedienstverleners, waarbij het toekennen van een accreditatie afhankelijk wordt gemaakt van het naleven van de voorwaarden vermeld in bijlage 2 van het voorstel van richtlijn. Anderzijds moeten zij de activiteit van die geaccrediteerde certificatieautoriteiten onderwerpen aan het naleven van de voorwaarden vermeld in bijlage 1 en het aanmaken van handtekeningen aan de voorschriften van bijlage 3 van het voorstel van richtlijn. Natuurlijk belet niets een niet-geaccrediteerde certificatiedienstverlener certificaten af te geven waarvan de inhoud in overeenstemming is met artikel 12 en de eisen van bijlage II van het voorstel van richtlijn na te leven (zie hierboven artikel 4). Hij mag echter in het certificaat niet vermelden dat het afgegeven is als gekwalificeerd certificaat, want de dienstverlener is niet geaccrediteerd en werd vooraf dan ook niet gecontroleerd. Aannemen dat elke dienstverlener kan

formes à ces normes, ceux-ci seront *présumés satisfaire* aux exigences de l'annexe III c'est-à-dire aux exigences de l'article 11 de cette loi. L'administration est chargée de suivre les travaux au niveau européen afin que les dispositifs de création de signature utilisés en Belgique correspondent à ces normes. D'autre part, un prestataire de service de certification belge peut essayer de faire la preuve dans le cadre de sa demande d'accréditation que les dispositifs de création de signature qu'il utilise sont conformes à ces exigences.

Art. 12

Le certificat consiste en la confirmation d'une ou plusieurs informations, principalement du lien entre le titulaire du certificat et les données afférentes à la vérification de signature qui correspondent aux données afférentes à la création de signature sous le contrôle du signataire. L'objectif de la présente loi est, pour rappel, de renforcer la sécurité et la confiance dans l'utilisation de la signature électronique avancée en réseau ouvert (article 3). En raison de l'objectif poursuivi par la loi, il était donc indispensable que la loi énumère les informations minimales devant figurer sur tout certificat à l'appui de signatures électroniques avancées. La loi, à l'instar de la directive, qualifie ces certificats de « certificats qualifiés ».

La question s'est posée de savoir si tout prestataire de service de certification pouvait délivrer de tels certificats ou si seuls les prestataires accrédités pouvaient les émettre. L'annexe 2 de la directive énumère les exigences concernant les prestataires de service de certification délivrant des certificats qualifiés. Le législateur belge fait de ces exigences des conditions d'accréditation des prestataires. En effet, la proposition de directive ne revêt d'intérêt et n'est de nature à susciter la confiance que si les États membres, tout en respectant le principe de la liberté d'exercice de l'activité de certification, d'une part, mettent sur pied un régime d'accréditation des prestataires de service de certification, subordonnant l'octroi d'une accréditation au respect des conditions prévues à l'annexe 2 de la proposition de directive, d'autre part, soumettent l'activité de ces autorités de certification accréditées au respect des conditions prévues à l'annexe 1 et la création de signatures aux prescriptions de l'annexe 3 de la proposition de directive. Evidemment, rien n'empêche un prestataire de service de certification non accrédité d'émettre des certificats ayant un contenu conforme à l'article 12 et à respecter les exigences de l'annexe II de la proposition de directive (cf. *supra* article 4). Mais il ne pourra pas inscrire dans le certificat que celui-ci est émis au titre de certificat qualifié car le prestataire n'est pas accrédité et n'a donc fait l'objet d'aucun contrôle préala-

beweren dat hij de eisen van bijlage II naleeft, zonder dat er een voorafgaande controle is geweest, en dat hij in aanmerking komt voor de assimilatieclausule van artikel 4, § 4, zou een ramp zijn geweest op het vlak van de rechtszekerheid.

Het standpunt van de Belgische wetgever ligt in dat verband volledig in de lijn van de richtlijn omdat die richtlijn, in artikel 3, punt 2 bepaalt dat de lidstaten, met inachtneming van het principe van de vrijheid om de certificatieactiviteit uit te oefenen, « vrijwillige accreditatieregelingen mogen invoeren of handhaven die op verbetering van de certificatiediensten zijn gericht », voor zover de criteria betreffende die regelingen « objectief, transparant, evenredig en niet-discriminerend zijn ».

Artikel 12 van deze wet vermeldt de informatie die op gekwalificeerde certificaten moet voorkomen. De certificatiedienstverlener moet de nodige maatregelen treffen om na te gaan of die informatie correct is. Op grond van clausules over de aansprakelijkheid zou hij geen certificaten mogen afgeven die minder gegevens bevatten dan de minimaal vereiste informatie of niet mogen bepalen dat hij de echtheid van een deel van die informatie niet heeft kunnen controleren (zie in dat verband artikel 15 van deze wet).

Het gekwalificeerd certificaat moet de volgende informatie bevatten :

— een vermelding waaruit blijkt dat het certificaat als gekwalificeerd certificaat wordt afgegeven. Die vermelding is belangrijk, want de gebruiker van het certificaat, geadresseerde van een — door middel van een geavanceerde elektronische handtekening — elektronisch ondertekende boodschap, moet de waarborg kunnen hebben dat het certificaat waarop de elektronische handtekening steunt « gekwalificeerd » is en dat die handtekening dus in aanmerking kan komen voor de assimilatieclausule (artikel 4, § 4);

— de gegevens met betrekking tot de identificatie en de erkenning van de certificatiedienstverlener, en het land waar deze is gevestigd. Aan de hand van de gegevens over de identificatie en de erkenning van de certificatiedienstverlener kan de geadresseerde van een elektronisch ondertekende boodschap nagaan of het certificaat wel degelijk werd afgegeven door een geaccrediteerde certificatiedienstverlener (zie in dat verband de juridische gevolgen van elektronische handtekeningen die steunen op gekwalificeerde certificaten afgegeven door dergelijke certificatiedienstverleners). De nationaliteit van de certificatiedienstverlener is erg belangrijk (zie artikel 19 van deze wet);

— de identificatiegegevens van de certificaathouder of, zo hij dat verlangt, een pseudoniem dat als dusdanig is geïdentificeerd. De wet biedt de certificaathouder de mogelijkheid als dusdanig of via een pseudoniem te worden geïdentificeerd. Er werd reeds onderstreept dat de belangrijkste functie van het certificaat erin bestaat het verband te bevestigen tussen een persoon en de gegevens voor het verifiëren van de handtekening van die persoon. In verband met het identi-

ble. Admettre que tout prestataire puisse prétendre qu'il respecte les exigences de l'annexe II, sans qu'un contrôle préalable ne soit effectué, et bénéficier ainsi de la clause d'assimilation de l'article 4, § 4 aurait été catastrophique sur le plan de la sécurité juridique.

La position du législateur belge est à ce propos dans la droite ligne de la directive puisque celle-ci prévoit en son article 3, point 2 que, tout en respectant le principe de la liberté d'exercice de l'activité de certification, « les États membres peuvent instaurer ou maintenir des régimes volontaires d'accréditation visant à améliorer le niveau de service fourni » pour autant que les critères relatifs à ces régimes soient « objectifs, transparents, proportionnés et non discriminatoires ».

L'article 12 de la présente loi énumère un certain nombre d'informations obligatoires devant figurer sur les certificats qualifiés. Soulignons que le prestataire de service de certification doit prendre les mesures nécessaires afin d'établir l'exactitude de ces informations. Il ne pourrait, par le biais de clauses relatives à la responsabilité délivrer des certificats qui contiendraient moins que les informations minimales requises ou stipuler qu'elle n'a pu vérifier la véracité d'une de ces informations (voir à ce propos l'article 15 de la présente loi).

Le certificat qualifié doit contenir les informations suivantes :

— une mention indiquant qu'il est délivré à titre de certificat qualifié. Cette mention est importante car l'utilisateur du certificat, destinataire d'un message signé électroniquement, à l'aide d'une signature électronique avancée, doit pouvoir avoir la garantie que le certificat sur lequel se fonde la signature électronique est « qualifié » et donc que cette signature peut bénéficier de la clause d'assimilation (article 4, § 4);

— les données d'identification et d'agrément du prestataire de service de certification ainsi que le pays dans lequel il est établi. Les données d'identification et d'agrément du prestataire de service de certification permettent au destinataire d'un message signé électroniquement de vérifier si le certificat a bien été délivré par un prestataire de service de certification accrédité (voir à ce propos les conséquences juridiques attribuées aux signatures électroniques se fondant sur des certificats qualifiés émis par de tels prestataires de service de certification). Quant à la nationalité du prestataire de service de certification, celle-ci revêt une grande importance (voir article 19 de la présente loi);

— les données d'identification du titulaire de certificat ou, à sa demande, un pseudonyme identifié comme tel. La loi réserve au titulaire du certificat la possibilité d'être identifié comme tel ou par un pseudonyme. Ainsi que cela a déjà été souligné, la fonction principale du certificat est de confirmer le lien entre une personne et ses données afférentes à la vérification de signature. À propos de l'identification du titulaire du certificat, il convient de sou-

ficeren van de certificaathouder moet worden onderstreept dat de wet hem de mogelijkheid biedt anoniem te blijven door het gebruik van een pseudoniem (onverminderd de toepassing van artikel 18, § 2 van deze wet). Deze bepaling sluit aan bij de richtlijn 95/46/EG van 24 oktober 1995 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens en het vrije verkeer van deze gegevens (zie in dat verband artikel 18 van deze wet). Wanneer een pseudoniem wordt gebruikt, moet dat pseudoniem worden voorafgegaan door de vermelding dat het een pseudoniem betreft. Met deze eis wil men vermijden dat een persoon als pseudoniem de identiteit van iemand anders zou kiezen, met alle dubbelzinnigheden waartoe een dergelijke situatie zou kunnen leiden;

— in voorkomend geval een specifieke eigenschap van de certificaathouder, afhankelijk van de bestemming van het certificaat. Bijvoorbeeld een functie in een vennootschap of bij de Staat of nog een titel als notaris, architect enz.;

— de gegevens voor het verifiëren van een handtekening die overeenkomen met de gegevens voor het aanmaken van een handtekening onder toezicht van de ondertekenaar;

— vermelding van begin en einde van de geldigheid van het certificaat. Zij maakt het mogelijk de geldigheidsperiode van het certificaat af te bakenen. Buiten die periode zou de certificatiedienstverlener niet aansprakelijk kunnen worden gesteld voor schade veroorzaakt door het gebruik van het certificaat;

— de identificatiecode van het certificaat. Dat nummer is bedoeld om het certificaat te identificeren;

— in voorkomend geval de beperkingen van het gebruik van het certificaat en/of de beperking van het bedrag van de verrichtingen waarvoor het certificaat mag worden gebruikt (zie in dat verband artikel 15 van deze wet).

Art. 13

Zodra de gegevens voor het aanmaken en het verifiëren van een handtekening zijn aangemaakt, moet de persoon op wie zij van toepassing zijn alles in het werk stellen opdat de vertrouwelijkheid van de gegevens voor het aanmaken van een handtekening en de integriteit ervan zouden worden gevrijwaard.

Om de veiligheid van de elektronische handel te waarborgen, is het strikt noodzakelijk te beschouwen dat een elektronisch ondertekend bericht (door middel van een geavanceerde elektronische handtekening), waarvan de handtekening kon worden gecontroleerd door middel van een certificaat afgegeven door een geaccrediteerde certificatiedienstverlener, geacht wordt uit te gaan van de certificaathouder.

Om talrijke redenen zou de vertrouwelijkheid van de gegevens voor het aanmaken van een handtekening in het gedrang kunnen zijn gebracht of zou de certificaathouder kunnen vrezen dat dit zo is.

ligner que la loi lui réserve la possibilité de conserver l'anonymat par l'utilisation d'un pseudonyme (sans préjudice de l'application de l'article 18, § 2 de la présente loi). Cette disposition fait écho à la Directive 95/46/CE du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation des personnes (voir à ce propos l'article 18 de la présente loi). Dans le cas de l'utilisation d'un pseudonyme, celui-ci doit être précédé de la mention qu'il s'agit d'un pseudonyme. Cette exigence existe afin d'éviter qu'une personne choisisse comme pseudonyme l'identité d'une autre personne, avec toutes les ambiguïtés qu'une telle situation pourrait engendrer;

— le cas échéant, une qualité spécifique du titulaire de certificat, en fonction de l'usage auquel celui-ci est destiné. Par exemple, une fonction dans une société ou au sein de l'État ou encore un attribut tel que notaire, architecte, etc.;

— les données afférentes à la vérification de signature qui correspondent aux données afférentes à la création de signature sous le contrôle du signataire;

— l'indication du début et de la fin de la période de validité du certificat. Elle permet de délimiter la période de validité du certificat. En-dehors de celle-ci, la responsabilité du prestataire de service de certification ne pourrait être engagée en cas de dommage causé par l'utilisation du certificat;

— le code d'identification du certificat. Ce numéro est destiné à identifier le certificat;

— le cas échéant, les limites à l'utilisation du certificat et/ou à la valeur des transactions pour lesquelles le certificat peut être utilisé (voir à ce propos l'article 15 de la présente loi).

Art. 13

Dès lors que des données afférentes à la création et à la vérification de signature ont été créées, la personne à laquelle elles sont associées a l'obligation de tout mettre en œuvre afin que la confidentialité des données afférentes à la création de signature et leur intégrité soient préservées.

Afin de garantir la sécurité du commerce électronique, il est impératif de considérer qu'un message signé électroniquement (au moyen d'une signature électronique avancée) dont la signature a pu être vérifiée au moyen d'un certificat émis par un prestataire de service de certification accrédité, est réputé émaner du titulaire du certificat.

Pour de multiples raisons, il pourrait se faire que la confidentialité des données afférentes à la création de signature soit compromise ou que le titulaire du certificat craigne qu'il en soit ainsi.

Deze wet voorziet in een procedure tot herroeping om op die eventualiteit voorbereid te zijn. Zo kan aan het certificaat een einde worden gemaakt nog voor het verstrijkt. De certificatiedienstverlener die het certificaat heeft afgegeven zorgt voor de procedure, ofwel op verzoek van de certificaathouder, ofwel van ambtswege.

Wanneer zij plaats heeft op aanvraag van de certificaathouder, of deze aanvraag nu al dan niet gemotiveerd is, moet de certificatiedienstverlener het herroepingsbevel onmiddellijk uitvoeren. De certificaathouder moet die procedure altijd toepassen bij de geringste twijfel in verband met het handhaven van de vertrouwelijkheid van de gegevens voor het aanmaken van een handtekening. De herroepingsprocedure is ook van toepassing wanneer een van de vermeldingen waarin in artikel 12 is voorzien niet meer aan de werkelijkheid zou beantwoorden.

Wanneer het certificaat op initiatief van de certificatiedienstverlener wordt herroepen, moet die dienstverlener de certificaathouder onmiddellijk op de hoogte brengen en zijn beslissing motiveren. Het certificaat kan enkel worden herroepen onder de voorwaarden die in paragraaf 2 zijn bepaald.

De beslissing tot herroeping is definitief en dus onomkeerbaar. Of het nu na het verstrijken van het certificaat is of in geval van herroeping ervan, mag de certificaathouder de overeenkomstige gegevens voor het aanmaken van een handtekening niet gebruiken om een elektronische handtekening te genereren. De certificatiedienstverlener zou niet aansprakelijk kunnen worden gesteld mocht de certificaathouder die verplichting niet naleven. Laten wij in dat verband onderstrepen dat de geadresseerde van een elektronisch ondertekend bericht moet controleren of het certificaat niet verstreken of herroepen is.

Art. 14

De certificatiedienstverlener moet permanent (vierentwintig uur op vierentwintig) de aanvragen tot herroeping kunnen behandelen en er onmiddellijk gevolg aan geven. Daartoe zorgt de certificatiedienstverlener ervoor dat de certificaathouder over gepaste middelen beschikt om een herroeping aan te vragen.

De herroeping kan worden tegengesteld zodra zij in het elektronisch register is ingeschreven. Het is namelijk zo dat, zodra de inschrijving is gebeurd, de certificaathouder en de certificatiedienstverlener zich kunnen beroepen op het feit dat het certificaat herroepen is ten opzichte van derden en in het bijzonder ten opzichte van de geadresseerde van het elektronisch ondertekend bericht. Op grond van artikel 21, moet die geadresseerde controleren of het certificaat niet is herroepen.

Wat gebeurt er indien een elektronisch document elektronisch wordt ondertekend tussen het ogenblik van de aanvraag en het ogenblik van de inschrijving ? In principe zou deze periode niet mogen bestaan, want de certificatie-

Une procédure de révocation est prévue par la présente loi afin de parer à cette éventualité. Elle vise à mettre fin au certificat avant son terme. Elle est assurée par le prestataire de service de certification qui a délivré le certificat, soit à la demande de son titulaire, soit d'office.

Lorsqu'elle a lieu à la demande du titulaire, que cette demande soit ou non motivée, le prestataire de service de certification a l'obligation de procéder immédiatement à l'ordre de révocation. En toute hypothèse, le titulaire du certificat a l'obligation de la mettre en œuvre au moindre doute relatif au maintien de la confidentialité des données afférentes à la création de signature. La procédure de révocation est également applicable dans l'hypothèse où l'une des mentions prévues à l'article 12 ne serait plus conforme à la réalité.

Lorsque la révocation du certificat a lieu à l'initiative du prestataire de service de certification, celui-ci a l'obligation d'en avertir immédiatement le titulaire et de motiver sa décision. Elle ne peut avoir lieu que dans les conditions prévues au paragraphe 2.

La décision de révocation est définitive et donc irréversible. Que ce soit après l'expiration du certificat ou en cas de révocation de celui-ci, le titulaire ne peut utiliser les données afférentes à la création de signature correspondantes pour générer une signature électronique. La responsabilité de l'autorité de certification ne pourrait être engagée si le titulaire contrevenait à cette obligation. Soulignons à ce propos que le destinataire d'un message signé électroniquement est tenu de vérifier que le certificat n'est ni expiré ni révoqué.

Art. 14

Le prestataire de service de certification doit être en mesure de traiter en permanence (vingt-quatre heures sur vingt-quatre) les demandes de révocation et d'y donner suite immédiatement. À cet effet, le prestataire de service de certification assure que des moyens appropriés sont à la disposition du titulaire pour effectuer une demande de révocation.

La révocation est opposable à partir du moment de l'inscription de la révocation dans l'annuaire électronique. En effet, dès cette inscription, le titulaire de certificat et le prestataire de service de certification pourront se prévaloir du fait que le certificat est révoqué vis-à-vis des tiers, et particulièrement du destinataire du message signé électroniquement qui, rappelons-le, est tenu en vertu de l'article 21 de vérifier que le certificat n'est pas révoqué.

Que se passe-t-il si un document électronique est signé électroniquement entre le moment de la demande et le moment de l'inscription ? En principe, cet intervalle de temps ne devrait pas exister car le prestataire de

dienstverlener moet het herroepen certificaat onmiddellijk inschrijven in het elektronisch register. Nochtans kan men twee hypotheses onderscheiden :

— ofwel wordt het document elektronisch ondertekend door de certificaathouder : in dat geval is hij voor die handeling aansprakelijk, want de certificaathouder mag de gegevens voor het aanmaken van een handtekening niet meer gebruiken zodra hij de herroeping heeft aangevraagd;

— ofwel wordt het document ondertekend door een derde persoon die daartoe niet is gemachtigd : in dat geval is de certificatiedienstverlener normaal aansprakelijk tegenover de geadresseerde van het elektronisch ondertekende bericht, want hij moet onmiddellijk voor de inschrijving zorgen, wat technisch gemakkelijk is.

De certificatiedienstverlener moet alle relevante informatie over gekwalificeerde certificaten gedurende 20 jaar bewaren, voornamelijk om aan de rechtbank een bewijs van de certificatie te bezorgen. Die eis moet worden begrepen in het licht van artikel 4, § 4 van deze wet. Geavanceerde elektronische handtekeningen worden gelijkgesteld aan met de hand geschreven handtekeningen — wat de juridische gevolgen ervan betreft — op voorwaarde dat zij steunen op een gekwalificeerd certificaat afgegeven door een certificatiedienstverlener die aan de eisen van deze wet voldoet. Het is dus noodzakelijk dat de relevante informatie over de certificaten tot staving van dergelijke handtekeningen worden bewaard opdat, in geval van geschil, kan worden aangetoond dat aan de vereiste voorwaarden om in aanmerking te komen voor de assimilatieclausule, was voldaan.

Art. 15

Deze wet behandelt de kwesties in verband met de aansprakelijkheid enkel met betrekking tot certificaten afgegeven door certificatiedienstverleners die aan het publiek certificaten afgeven die als gekwalificeerd worden voorgesteld of die dergelijke certificaten in het openbaar waarborgen. Voor certificatiedienstverleners die gewone certificaten afgeven (die niet als gekwalificeerd worden voorgesteld) is het gemeenrecht van toepassing.

Voor gekwalificeerde certificaten voorziet deze wet in een specifieke regeling inzake aansprakelijkheid, en zij volgt hiervoor het voorstel van richtlijn. Door die regeling wordt gepoogd een evenwicht te creëeren tussen de belangen van de certificatiedienstverleners en die van de gebruikers van certificaten opdat de tot stand gebrachte certificatieregeling zeer betrouwbaar en geloofwaardig zou zijn, zonder daarom de ontwikkeling van de certificatie en bijgevolg de elektronische handel te belemmeren.

service de certification a l'obligation d'inscrire immédiatement le certificat révoqué dans l'annuaire électronique. Néanmoins, on peut envisager deux hypothèses :

— soit le document est signé électroniquement par le titulaire de certificat : dans ce cas, il est responsable de cet acte car celui-ci ne peut utiliser les données afférentes à la création de signature dès qu'il a effectué sa demande de révocation;

— soit le document est signé par un tiers non autorisé : dans ce cas, le prestataire de service de certification sera normalement responsable vis-à-vis du destinataire du message signé électroniquement car il a l'obligation de procéder immédiatement à l'inscription, ce qui est techniquement aisé.

Le prestataire de service de certification doit conserver toutes les informations pertinentes concernant les certificats qualifiés pendant une durée de 20 ans, essentiellement pour fournir une preuve de la certification en justice. Cette exigence doit être comprise à la lumière de l'article 4, § 4 de la présente loi. Les signatures électroniques avancées sont assimilées aux signatures manuscrites pour ce qui est de leurs conséquences juridiques si toutefois elles reposent sur un certificat qualifié émis par un prestataire de service de certification satisfaisant aux exigences de la présente loi. Il est donc nécessaire que les informations pertinentes concernant les certificats à l'appui de telles signatures soient conservées afin, qu'en cas de litige, il puisse être démontré que les conditions requises pour pouvoir bénéficier de la clause d'assimilation étaient respectées.

Art. 15

La présente loi ne traite des questions relatives à la responsabilité qu'à propos des certificats émis par les prestataires de service de certification qui délivrent au public des certificats présentés comme qualifiés ou qui garantissent publiquement de tels certificats. Dès lors, pour les prestataires de services de certification qui délivrent des certificats ordinaires (qui ne sont pas présentés comme qualifiés), le droit commun de la responsabilité trouve à s'appliquer.

Pour les certificats qualifiés, la présente loi établit un régime spécifique de responsabilité, suivant sur ce point la proposition de directive. Celui-ci tente d'établir un équilibre entre les intérêts des prestataires de service de certification et des utilisateurs de certificats afin que le régime de certification établi présente un haut degré de fiabilité et, par là même de crédibilité, sans qu'il entrave pour autant le développement de la certification et, par conséquent, le commerce électronique.

De geaccrediteerde certificatiedienstverlener die een certificaat afgeeft dat als gekwalificeerd wordt voorgesteld en die een certificaat in het openbaar waarborgt, moet ook de volgende zaken waarborgen :

— de juistheid van de informatie vermeld in het gekwalificeerd certificaat op de datum waarop het is gepubliceerd in het elektronisch register bedoeld in artikel 10;

— de verzekering dat, op het ogenblik waarop het certificaat wordt afgegeven, de persoon die in het gekwalificeerd certificaat werd geïdentificeerd de gegevens voor het aanmaken van een handtekening bezat conform de gegevens voor het verifiëren van een handtekening vermeld in het certificaat;

— de verzekering dat de gegevens voor het aanmaken van een handtekening en de gegevens voor het verifiëren van een handtekening complementair kunnen worden gebruikt;

— de geldigheid van het certificaat : dit element komt tot uiting in de eerste paragraaf van artikel 6 van het voorstel van richtlijn. Op grond hiervan moet de certificatiedienstverlener het certificaat onmiddellijk herroepen wanneer de gekwalificeerde certificaathouder het vraagt.

De hierboven opgesomde verplichtingen zijn alle bedoeld om te zorgen voor de juistheid van de informatie die ter beschikking van de gebruikers wordt gesteld. In werkelijkheid is de juistheid de essentie zelf van de certificatie : zij is een voorwaarde voor het vertrouwen dat de gebruikers kunnen stellen in een certificatiemechanisme.

De certificatiedienstverlener is dus aansprakelijk voor de schade veroorzaakt aan iedereen die rechtmatig vertrouwt op het certificaat en die voortvloeit uit het niet naleven van een van de hierboven opgesomde verplichtingen, tenzij hij bewijst dat hij niets heeft verwaarloosd.

De certificatiedienstverlener kan zijn aansprakelijkheid beperken. Twee types van clausules betreffende de aansprakelijkheid van de certificatiedienstverlener kunnen worden overwogen. De certificatiedienstverlener kan eerst en vooral de grenzen bepalen voor het gebruik van het certificaat. In die veronderstelling mag hij niet aansprakelijk worden gesteld voor de schade die voortvloeit uit het onrechtmatig gebruik van het certificaat waarvan het gebruik beperkt is. Daarna kan hij de bovengrens bepalen van de transacties waarvoor het certificaat kan worden gebruikt. Die clausules moeten duidelijk *op het certificaat* voorkomen, en niet op een ander document, en door derden kunnen worden onderscheiden.

Elke overeenkomst die in strijd is met artikel 15, inzonderheid die welke de certificatiedienstverlener zou ontheffen van een van zijn essentiële verplichtingen vermeld in de paragrafen 1 en 2 van artikel 15, wordt beschouwd als niet geschreven.

De certificatiedienstverlener zou zich bijvoorbeeld niet kunnen laten ontheffen van zijn aansprakelijkheid om de reden dat hij het verkeerde karakter van de informatie niet kende enkel en alleen omdat het inwinnen van de informatie werd toevertrouwd aan de registratieoverheid. Als certificatie-

Le prestataire de service de certification accrédité qui délivre un certificat présenté comme qualifié ou qui garantit publiquement un certificat doit garantir :

— l'exactitude des informations contenues dans le certificat qualifié à la date où il a été publié dans l'annuaire électronique visé à l'article 10;

— l'assurance que, au moment de la délivrance du certificat, la personne identifiée dans le certificat qualifié détenait les données afférentes à la création de signature correspondant aux données afférentes à la vérification de signature figurant dans le certificat;

— l'assurance que les données afférentes à la création de signature et celles afférentes à la vérification de signature puissent être utilisées de façon complémentaire;

— la validité du certificat : cet élément se dégage du premier paragraphe de l'article 6 de la proposition de directive en vertu duquel le prestataire de service de certification a l'obligation de révoquer immédiatement un certificat lorsque le titulaire de certificat qualifié en fait la demande.

Les obligations énumérées ci-dessus visent toutes à assurer l'exactitude des informations mises à la disposition des utilisateurs. En réalité, l'exactitude constitue l'essence même de la fonction de certification : elle conditionne la confiance que les utilisateurs peuvent placer dans un mécanisme de certification.

Le prestataire de service de certification est donc responsable de tout préjudice causé à toute personne qui se fie légitimement au certificat et qui découle du manquement à une des obligations énumérées ci-dessus sauf si elle prouve qu'elle n'a commis aucune négligence.

Le prestataire de service de certification peut limiter sa responsabilité. Deux types de clauses relatives à la responsabilité du prestataire de service de certification sont envisageables. Le prestataire de service de certification peut tout d'abord fixer des limites à l'utilisation du certificat. Dans cette hypothèse, il ne doit pas être tenu responsable du préjudice résultant de l'usage abusif du certificat qui contient des limites à son utilisation. Il peut ensuite fixer dans la valeur limite des transactions pour lesquelles le certificat peut être utilisé. Ces clauses doivent obligatoirement figurer clairement *sur le certificat*, et non sur un autre document, et être discernables par des tiers.

Toute convention contraire à l'article 15, notamment celle qui libérerait le prestataire de service de certification d'une des obligations essentielles prévues aux paragraphes 1er et 2 de l'article 15 doit être réputée non écrite.

Le prestataire de service de certification ne pourrait par exemple s'exonérer de sa responsabilité pour le motif qu'il ne connaissait pas le caractère erroné des informations du seul fait que la collecte de celles-ci a été confiée à une autorité d'enregistrement. En sa qualité

dienstverlener moet hij controleren of de informatie geloofwaardig is.

Art. 16

Indien een geaccrediteerde certificatiedienstverlener vrijwillig beslist zijn activiteiten stop te zetten, moet hij het bestuur hiervan binnen een redelijke termijn op de hoogte brengen, om verrassingen te vermijden en om het bestuur de kans te geven de operatie te controleren. Om te zorgen voor de continuïteit van de dienstverlening moet de dienstverlener alles in het werk stellen opdat zijn activiteiten zouden worden overgenomen door een andere geaccrediteerde dienstverlener. Wanneer hij geen overnemer vindt, herroept hij de certificaten twee maanden na de certificaathouders te hebben ingelicht.

Indien de geaccrediteerde certificatiedienstverlener onvrijwillig zijn activiteiten stopzet (bijvoorbeeld bij faillissement) moet hij het Bestuur hiervan onmiddellijk op de hoogte brengen. In die veronderstelling vreest men dat de certificatiedienstverlener niet meer efficiënt kan handelen. Daarom vertrouwt men aan het bestuur de herroeping van de certificaten toe, indien de dienstverlener dat niet reeds heeft gedaan, en moet het bestuur alle relevante informatie over het gekwalificeerd certificaat bewaren, zoals bepaald in artikel 14, § 3. Daartoe moet de dienstverlener meewerken en alle nuttige informatie overzenden aan het bestuur.

Art. 17

Het samenstellen van de gegevens voor het aanmaken en voor het verifiëren van handtekeningen, het aanmaken, afgeven en bijhouden van certificaten alsook de veilige middelen voor het aanmaken van elektronische handtekeningen gebeurt door middel van betrouwbare systemen en producten die tegen wijzigingen beschermd moeten zijn en die de technische en cryptografische veiligheid van hun functies waarborgen. Die systemen en producten maken het inzonderheid mogelijk elke aanslag te vermijden of op te sporen met betrekking tot de integriteit van een elektronisch ondertekend bericht of van een certificaat. Zij maken het ook mogelijk het niet-toegestane gebruik van de gegevens voor het aanmaken van een handtekening te vermijden of op te sporen. De betrouwbaarheid van de systemen en van de producten wordt dus beschouwd op basis van de risico's die men wenst te vermijden en van de gevaren die men wil elimineren.

Om soepel te blijven ten opzichte van de technologische evolutie worden de betrouwbaarheid van de technische middelen en het veiligheidsniveau beoordeeld op basis van de stand van de techniek op het ogenblik van de beoordeling. Om de certificatiedienstverleners de nodige aanwijzingen in verband met de stand van de techniek wordt die regelmatig

de prestataire de service de certification, une obligation de contrôle de vraisemblance pèse sur lui.

Art. 16

Si un prestataire de service de certification accrédité décide volontairement de mettre fin à ses activités, il est tenu d'en avertir l'administration dans un délai raisonnable pour éviter tout effet de surprise et pour permettre à l'administration de contrôler l'opération. En vue d'assurer la continuité du service, le prestataire doit tout mettre en œuvre pour que ses activités soient reprises par un autre prestataire accrédité. Si il ne trouve pas de repreneur, le prestataire procède à la révocation des certificats deux mois après en avoir averti les titulaires.

Si le prestataire de service de certification accrédité arrête involontairement ses activités (par exemple en cas de faillite), il doit en informer immédiatement l'administration. Dans cette hypothèse, on craint que le prestataire ne soit plus en mesure d'agir efficacement. Dès lors on confie à l'administration la tâche de procéder à la révocation des certificats, si le prestataire ne l'a pas déjà fait, et de conserver toutes les informations pertinentes concernant le certificat qualifié comme prévu à l'article 14, § 3. À cet effet, le prestataire est tenu de collaborer et de transmettre toute information utile à l'administration.

Art. 17

La création des données afférentes à la création et à la vérification de signature, la création, la délivrance et la conservation des certificats ainsi que les dispositifs sécurisés de création de signature électronique sont réalisés par des systèmes et des produits fiables qui doivent être protégés contre les modifications et assurer la sécurité technique et cryptographique des fonctions qu'ils assument, et qui permettent notamment d'éviter ou de détecter toute atteinte à l'intégrité d'un message signé électroniquement ou d'un certificat et toute utilisation non autorisée de données afférentes à la création de signature. La fiabilité des systèmes et des produits est donc envisagée sur la base des risques que l'on désire éviter et des dangers que l'on veut écarter.

En vue de rester souple par rapport aux évolutions technologiques, la fiabilité des moyens techniques ainsi que le niveau de sécurité sont appréciés en fonction de l'état de la technique au moment où cette appréciation est faite. Afin de donner aux prestataires de service de certification des indications quant à cet état de la tech-

door het bestuur vastgelegd. Het bestuur zal namelijk kunnen steunen op de normen die in het publicatieblad van de Europese Gemeenschappen zullen worden gepubliceerd, zoals bedoeld in artikel 3, 5) van het voorstel van richtlijn.

Art. 18

De certificatiedienstverlener die wordt belast met het opmaken van een certificaat, moet de identiteit van de kandidaat-houder met zekerheid en op ondubbelzinnige wijze kunnen vaststellen. Hij zal daartoe verschillende inlichtingen over de kandidaat inwinnen. Persoonlijke gegevens kan hij krachtens onderhavige wet enkel opvragen hetzij bij de betrokken persoon zelf, hetzij met diens uitdrukkelijke toestemming, en enkel wanneer die gegevens nodig zijn voor de afgifte en het beheer van het certificaat. Een identiteitscontrole via het rijksregister der natuurlijke personen is derhalve niet mogelijk, zoals het advies van de Raad van State bevestigt. Bovendien mogen deze gegevens niet worden opgevraagd of verwerkt zonder uitdrukkelijke toestemming van de betrokken persoon.

De kandidaat-houder die niet met zijn eigen naam wenst te ondertekenen, en daartoe ook niet wettelijk verplicht is, kan een pseudoniem kiezen om anoniem te blijven. Deze bepaling spruit rechtstreeks voort uit de mededeling van de Europese Commissie van 8 oktober 1997 (COM(97)503 : « Zorgen voor veiligheid en vertrouwen in elektronische communicatie — naar een Europees kader voor digitale handtekeningen en encryptie », Mededeling van de Commissie aan het Europees Parlement, de Raad, het Economisch en Sociaal Comité en het Comité van de Regio's, 8 oktober 1997).

Er dient hierbij te worden opgemerkt dat de ondertekenaar, niettegenstaande de anonimiteitsgarantie, bij de certificatiedienstverlener bekend is. Deze laatste moet krachtens onderhavige wet alle inlichtingen verstrekken waarmee de identiteit van de certificaathouder kan worden vastgesteld in de gevallen omschreven door de wet van 30 juni 1994 tot bescherming van de persoonlijke levenssfeer tegen het afluisteren, kennisnemen en opnemen van privé-communicatie en -telecommunicatie, waarbij artikelen 90*ter* en volgende in het Wetboek van Strafvordering worden ingevoegd.

Deze bepaling is zowel van toepassing op de geaccrediteerde certificatiedienstverleners als op de niet-geaccrediteerde certificatiedienstverleners.

Art. 19

Om werkelijk tot nut te strekken, dienen alle op nationaal vlak goedgekeurde certificatievoorzieningen in een internationaal perspectief te worden geplaatst. Artikel 19 van onderhavige wet, dat over de grensoverschrijdende

nique, celui-ci est arrêté régulièrement par l'administration. Elle pourra notamment se référer aux normes qui seront publiées au JOCE tel que visé à l'article 3, 5) de la proposition de directive.

Art. 18

Le prestataire de service de certification, qui est chargé d'établir un certificat, doit être en mesure de vérifier de manière certaine et non équivoque l'identité du candidat titulaire. À cette fin, il est amené à collecter diverses informations sur celui-ci. En vertu de la présente loi, il ne peut recueillir les données personnelles que directement auprès de la personne concernée ou avec son consentement explicite et uniquement dans la mesure où les informations sont nécessaires à la délivrance et à la gestion du certificat. Ceci exclut une vérification de l'identité auprès du registre national des personnes physiques comme le confirme l'avis du Conseil d'État. En outre, ces données ne peuvent être ni recueillies ni traitées à d'autres fins sans le consentement explicite de la personne intéressée.

Le candidat titulaire ne désirant pas et n'étant pas légalement obligé de signer sous son nom peut choisir un pseudonyme qui lui permettra de garder l'anonymat. Cette disposition s'inspire directement de la Communication de la Commission européenne du 8 octobre 1997 (COM(97)503 : Vers un Cadre Européen pour les signatures numériques et le chiffrement : assurer la sécurité et la confiance dans la communication électronique, Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social et au Comité des Régions, 8 octobre 1997).

Il convient de souligner que, bien que l'anonymat soit garanti, le signataire est identifié auprès du prestataire de service de certification. Celui-ci est tenu de communiquer, en vertu de la présente loi toute information permettant d'identifier le titulaire du certificat dans les conditions prévues par la loi du 30 juin 1994 relative à la protection de la vie privée contre les écoutes, la prise de connaissance et l'enregistrement de communications et de télécommunications privées qui introduit les articles 90*ter* et suivants dans le Code d'instruction criminel.

Cette disposition s'applique tant aux prestataires de service de certification accrédités qu'aux prestataires de service de certification non accrédités.

Art. 19

Afin de revêtir une réelle utilité, toute infrastructure de certification adoptée à un niveau national doit être envisagée dans une perspective internationale. L'article 19 de la présente loi, en traitant de la reconnais-

erkenning van certificaten handelt, geeft uiting aan dit streven.

Onderhavige wet maakt een onderscheid tussen voor het publiek bestemde gekwalificeerde certificaten die werden afgegeven door een in een lidstaat van de Europese Unie gevestigde en geaccrediteerde certificatiedienstverlener en certificaten die door een in een derde land gevestigde certificatiedienstverlener werden afgegeven.

In het eerste geval worden ze door artikel 19, §1 gelijkgesteld met gekwalificeerde certificaten afgegeven door een in België gevestigde certificatiedienstverlener.

In het tweede geval worden ze door artikel 19, § 2, slechts gelijkgesteld met gekwalificeerde certificaten afgegeven door een in België gevestigde certificatiedienstverlener wanneer aan een van volgende voorwaarden wordt voldaan :

— de certificatiedienstverlener voldoet aan de in onderhavige wet bedoelde voorwaarden en werd geaccrediteerd volgens een in een lidstaat van de Europese Unie opgericht vrijwillig accreditatiestelsel;

— het certificaat wordt gewaarborgd door een in de Europese Gemeenschap gevestigde, geaccrediteerde certificatiedienstverlener;

— het certificaat of de certificatiedienstverlener wordt erkend op basis van een bilaterale of multilaterale overeenkomst tussen de Europese Gemeenschap en derde landen of internationale organisaties.

Voor geavanceerde elektronische handtekeningen die overeenkomstig artikel 19 worden aangemaakt op basis van door buitenlandse certificatiedienstverleners afgegeven certificaten geldt derhalve de gelijkstellingsclausule van artikel 4, § 4.

Met deze bepaling wil onderhavige wet het vertrouwen van de gebruikers wekken en de deuren openzetten naar de internationale handel.

Art. 20

Op de schouders van de certificaathouder rusten een aantal verplichtingen. Hij kan verantwoordelijk worden gesteld voor het niet-naleven van een van de verplichtingen die hem door of krachtens onderhavige wet worden opgelegd, onder meer wanneer hij valse inlichtingen heeft verstrekt aan de certificatiedienstverlener, de vertrouwelijkheid van de gegevens voor het aanmaken van een handtekening in gevaar heeft gebracht, het certificaat niet heeft laten herroepen wanneer de omstandigheden dat vereisten, of de gegevens voor het

sance transfrontière des certificats, fait écho à cette préoccupation.

La présente loi établit une distinction entre les certificats qualifiés délivrés à l'intention du public par un prestataire de service de certification établi et accrédité dans un État membre de l'Union européenne et les certificats délivrés par un prestataire de service de certification établi dans un pays tiers.

En ce qui concerne les premiers, l'article 19, §1 les assimile aux certificats qualifiés délivrés par un prestataire de service de certification établi en Belgique.

En ce qui concerne les seconds, l'article 19, § 2, ne les assimile aux certificats qualifiés délivrés par un prestataire de service de certification établi en Belgique que si une des conditions suivantes est remplie :

— le prestataire de service de certification remplit les conditions visées dans la présente loi et a été accrédité dans le cadre d'un régime volontaire d'accréditation établi dans un État membre de l'Union européenne;

— un prestataire de service de certification accrédité établi dans la Communauté européenne garantit le certificat;

— le certificat ou le prestataire de service de certification est reconnu dans le cadre d'un accord bilatéral ou multilatéral entre la Communauté européenne et des pays tiers ou des organisations internationales.

Les signatures électroniques avancées réalisées sur la base de certificats délivrés par des prestataires de service de certification étrangers conformément à l'article 19 pourront donc bénéficier de la clause d'assimilation prévue à l'article 4, § 4.

Par cette disposition, la présente loi entend susciter la confiance des utilisateurs et ouvrir les portes au commerce international.

Art. 20

Différentes obligations pèsent sur le titulaire de certificat. Sa responsabilité pourrait être engagée en cas de manquement à une des obligations qui lui sont imposées par ou en vertu de la présente loi et notamment s'il a fourni des informations erronées au prestataire de service de certification, mis en péril la confidentialité des données afférentes à la création de signature, n'a pas fait procéder à la révocation du certificat dans les conditions requises ou s'il a utilisé les données afférentes à la création de signature pour générer une signature alors

aanmaken van een handtekening heeft gebruikt om een handtekening aan te maken op een moment dat het certificaat voor deze gegevens was herroepen of vervallen.

Art. 21

Krachtens artikel 21 heeft de ontvanger van een elektronisch ondertekende boodschap de plicht tot verificatie. De ontvanger dient enerzijds de handtekening te verifiëren met behulp van het corresponderende certificaat en moet anderzijds ook controleren of het certificaat niet vervallen of herroepen is.

Zoals reeds vermeld, moet een geavanceerde elektronische handtekening, om onder de gelijkstellingsclausule van artikel 4, § 4 te kunnen vallen, steunen op een gekwalificeerd certificaat dat werd afgegeven door een geaccrediteerde certificatiedienstverlener, overeenkomstig onderhavige wet. De ontvanger van een elektronisch ondertekend bericht moet dus controleren of het certificaat waarmee hij de handtekening verifieert, afgegeven werd door een geaccrediteerde certificatiedienstverlener of door een buitenlandse certificatiedienstverlener overeenkomstig artikel 19 van onderhavige wet.

Aan de ontvanger kan de schade ten laste gelegd worden die het gevolg is van de niet-naleving van een hem toekomende verplichting.

Art. 22

Aangezien het bestuur controle moet uitoefenen over de geaccrediteerde certificatiedienstverleners, moet het de middelen krijgen om te kunnen optreden wanneer het vaststelt dat deze laatsten zich niet aan de door of krachtens onderhavige wet opgelegde voorwaarden of verplichtingen houden. Wanneer het bestuur vaststelt dat een geaccrediteerd certificatiedienstverlener zich niet aan de voorschriften van de wet houdt, kan het een termijn opleggen waarbinnen de dienstverlener de toestand regulariseert. Deze termijn kan door het bestuur vrij worden vastgelegd al naar gelang het geval. Indien de certificatiedienstverlener na afloop van de termijn de toestand niet heeft geregulariseerd, trekt het bestuur de accreditatie in.

Om redenen van rechtszekerheid is de certificatiedienstverlener verplicht de intrekking van de accreditatie onmiddellijk in zijn register te vermelden en de certificaathouders onverwijld op de hoogte te brengen.

même que le certificat relatif à ces données était révoqué ou expiré.

Art. 21

En vertu de l'article 21, une obligation de vérification pèse sur le destinataire d'un message signé électroniquement. Celui-ci est tenu de vérifier d'une part la signature au moyen du certificat correspondant et d'autre part que le certificat n'est ni expiré ni révoqué.

Rappelons que pour bénéficier de la clause d'assimilation de l'article 4, § 4, toute signature électronique avancée doit être fondée sur un certificat qualifié délivré par un prestataire de service de certification accrédité conformément à la présente loi. Il appartient donc au destinataire d'un message signé électroniquement de vérifier que le certificat lui permettant de procéder à la vérification de la signature du message a été délivré par un prestataire de service de certification accrédité ou par un prestataire de service de certification étranger conformément à l'article 19 de la présente loi.

Le dommage qui est la conséquence de l'inexécution d'une obligation incombant au destinataire peut lui être imputable.

Art. 22

Puisque l'administration est chargée de la surveillance des prestataires de service de certification accrédités, il est nécessaire de lui procurer les moyens d'agir dans les cas où elle constaterait le non respect par ces dernières des conditions et obligations prescrites par ou en vertu de la présente loi. Si l'administration constate qu'un prestataire de service de certification accrédité ne se conforme pas aux prescriptions de la loi, elle peut fixer un délai pour que ce prestataire régularise sa situation. Ce délai est fixé discrétionnairement par l'administration en fonction du cas d'espèce. Si après, l'écoulement de ce délai, le prestataire de service de certification n'a pas régularisé sa situation, l'administration procède au retrait de l'accréditation.

Pour des raisons de sécurité juridique, le prestataire de service de certification est tenu de mentionner immédiatement dans son annuaire le retrait de l'accréditation et d'en informer immédiatement les titulaires de certificat.

Art. 23

De bedoeling van de wet, namelijk het vertrouwen van de gebruikers versterken, zou in het gedrang komen wanneer een certificatiedienstverlener de indruk geeft een geaccrediteerd certificatiedienstverlener te zijn, terwijl hij aan geen enkele accreditatievoorwaarde voldoet of er geen enkele controle op de naleving van deze voorwaarden bestaat, zodat hij niet aan de toepassing van de wet is onderworpen. Om die reden wordt het onrechtmatig gebruik van de titel van geaccrediteerd certificatiedienstverlener bij wijze van afschrikking strafrechtelijk vervolgd.

De tweede paragraaf moet ervoor zorgen dat deze sanctie in de praktijk effect heeft.

De minister van Justitie,

Marc VERWILGHEN

De minister van Telecommunicatie, en Overheidsbedrijven en Participaties

Rik DAEMS

De minister van Economie,

Rudy DEMOTTE

(1) Vanaf nu moeten de ondernemingen van de bouw- en vervoersector, behoudens afwijkingen, hun onmiddellijke aangiften van tewerkstelling via elektronische weg doen (koninklijk besluit van 22 februari 1998 « tot invoering van een onmiddellijke aangifte van tewerkstelling, met toepassing van artikel 38 van de wet van 26 juli 1996 tot modernisering van de sociale zekerheid en tot vrijwaring van de leefbaarheid van de wettelijke pensioenstelsels, » *Belgisch Staatsblad* van 18 maart 1998). Daartoe voert het koninklijk besluit van 16 oktober 1998 (« houdende bepalingen betreffende de elektronische handtekening, geldend voor de sociale zekerheid, met toepassing van artikel 38 van de wet van 26 juli 1996 tot modernisering van de sociale zekerheid en tot vrijwaring van de leefbaarheid van de wettelijke pensioenstelsels », *Belgische Staatsblad* van 7 november 1998) een voorlopig systeem van elektronische handtekening in voor de sociale zekerheid en inzonderheid voor de onmiddellijke aangiften van tewerkstelling.

(2) Voorstel van richtlijn van het Europees Parlement en van de Raad betreffende een gemeenschappelijk kader voor de elektronische handtekeningen, COM (98) 297 eindtekst, 13 juni 1998, PBEG, C 325/5-11 van 23 oktober 1998 of http://www.ispo.cec.e/eif/*policy*/com98297fr.doc

(3) Gemeenschappelijk standpunt EG nr 28/1999 bepaald door de Raad van 28 juni 1999 met het oog op de goedkeuring van de richtlijn 1999/…/EG van het Europees Parlement en van de Raad van … betreffende een gemeenschappelijk kader voor de elektronische handtekeningen, PBEG, C 243/33-46 van 27 augustus 1999 of de volgende URL : http:/europa.eu.int/comm/dg15/fr/media/*sign*/index.htm

Art. 23

L'objectif de la loi, qui est de renforcer la confiance des utilisateurs, serait compromis si un prestataire de service de certification donne l'impression qu'il a la qualité de prestataire de service de certification accrédité alors qu'il ne répond à aucune condition d'accréditation ou que le respect de ces conditions ne fait l'objet d'aucun contrôle et qu'il n'est pas soumis à l'application de la loi. Pour cette raison, toute usurpation de la qualité de prestataire de service de certification accrédité est punie pénalement. Cette sanction entend jouer un rôle dissuasif.

Le deuxième paragraphe vise à assurer l'effectivité pratique de cette sanction.

Le ministre de la Justice,

Marc VERWILGHEN

Le ministre des Télécommunications, et des Entreprises et Participations publiques

Rik DAEMS

Le ministre de l'Économie,

Rudy DEMOTTE

(1) Dès à présent, les entreprises des secteurs de la construction et du transport doivent, sauf dérogation, effectuer leurs déclarations immédiates d'emploi par voie électronique (arrêté royal du 22 février 1998 « instaurant une déclaration immédiate de l'emploi, en application de l'article 38 de la loi du 26 juillet 1996 portant modernisation de la sécurité sociale et assurant la viabilité des régimes légaux des pensions », *Moniteur belge* du 18 mars 1998). Pour ce faire, l'arrêté royal du 16 octobre 1998 (« portant des dispositions relatives à la signature électronique, qui s'applique à la sécurité sociale, en application de l'article 38 de la loi du 26 juillet 1996 portant modernisation de la sécurité sociale et assurant la viabilité des régimes légaux des pensions », *Moniteur belge* du 7 novembre 1998) met en place un système provisoire de signature électronique pour la sécurité sociale, et notamment pour les déclarations immédiates d'emploi.

(2) Proposition de directive du Parlement européen et du Conseil sur un cadre commun pour les signatures électroniques, COM (98) 297 final, 13 juin 1998, *J.O.C.E.*, C 325/5-11 du 23 octobre 1998 ou http://www.ispo.cec.be/eif/*policy*/com98297fr.doc

(3) Position commune CE n° 28/1999 arrêtée par le Conseil le 28 juin 1999 en vue de l'adoption de la directive 1999/…/CE du Parlement européen et du Conseil du … sur un cadre communautaire pour les signatures électroniques, *J.O.C.E.*, C 243/33-46 du 27 août 1999 ou l'URL suivant : http://europa.eu.int/comm/dg15/fr/media/*sign*/index.htm

(4) Zie bijvoorbeeld de Commissie van de Verenigde Naties voor het Internationaal Handelsrecht, Verslag van de werkgroep voor de elektronische handel over de werkzaamheden van de eenendertigste zitting (New York, 18-28 februari 1997), A/CN.9/437, 12 maart 1997; commissie van de Verenigde Naties voor het Internationaal Handelsrecht, Verslag van de werkgroep voor de elektronische handel over de werkzaamheden van de drieëndertigste zitting (New York, 29 juni-10 juli 1998), A/CN.9/454, 21 augustus 1998. Zie ook http://www.un.or.at/uncitral/fr-index.htm

(5) Duitse wet betreffende de multimedia van 13 juni 1997, artikel 3 (betreffende de digitale handtekening), Officieel Duits Publicatieblad van 22 juli 1997 (BGB1, IS, 1870), in werking getreden op 1 augustus 1997, http://www.iid.de/iukdg/iukdge.html

(6) Italiaans presidentieel decreet van 10 november 1997, nr. 513 over « *Regulations establishing criteria and means for implementing Section 15 (2) of Law n°59 of 15 March 1997 concerning the creation, storage and transmission of documents by means op computer-based or telematic systems* », gepubliceerd in Gazzetta Ufficiale, 13 maart 1998, nr.60, http://www.aipa.it/english/law(2/pdecree51397.asp

(7) Deze tekst is beschikbaar op volgend adres : http;//www.etat.lu/ECO/

(8) D. GOBERT, « *La sécurisation des échanges par la reconnaissance de la signature électronique : condition d'existence des réseaux d'avocats* », in *Multimédia. Le cyberavocat*, Formation permanente CUP, Volume XXIX, Luik-Namen, februari 1999, blz.173

(9) http://www.agora98.org/

(10) Die teksten werden meer bepaald besproken in atelier 1 van de tak « Verbruikers », wat betreft de elektronische handtekening en de certificatie van de *sites*, voorgezeten door Professor Yves Poullet. Dit atelier omvatte deskundigen en mensen die zich voor het thema interesseren, zowel uit de private als de publieke sector, de balie, het notariaat, de academische wereld enz.

(11) Het verslag (*Position Paper*) is beschikbaar op het volgend adres : http://www.agora98.org/fr/conso/fconso.html

(12) Parl. Besch., Kam. Volksvert., gew. Zitt. 14 april 1999, nr 214/1

(13) E. DAVIO, « *Certification, signature et cryptographie* », in E. MONTERO (ed.), *Internet face au droit*, *Cahiers du C.R.I.D.*, nr 12, E. Story-Scientia,1997, blz. 80 en volgende; M. ANTOINE en D. GOBERT, « *Pistes de réflexion pour une législation relative à la signature digitale et au régime des autorités de certification* », R.G.D.C., juli-oktober 1998, nr. 4/5, blz. 285-310.

(14) M. ANTOINE, D. GOBERT en A. SALAUN, « *Le développement du commerce électronique : les nouveaux métiers de la confiance* », in een collectief te verschijnen werk, Cahiers du CRID, nr 16, Brussel,. Bruylant, 1999.

(15) Een overzicht ervan vindt u bij D. MOUGENOT, « *Droit de la preuve et technologies nouvelles : synthèse et perspectives* », *Droit de la preuve-Formation permanente CUP,* Volume XIX, oktober 1997, blz. 45-105.

(16) M. ANTOINE, J.-F. BRAKELAND, M. ELOY, *Droit de la preuve face aux nouvelles technologies de l'information, Cahiers du CRID n°7,* Brussel, Story-Scientia, 1991, blz. 55 en volgende.

(17) Het is niet altijd gemakkelijk om de relatieve bewijskrachten van twee bewijsmethoden te kennen omdat de wet ze niet systematisch op expliciete wijze bepaalt. Ons voorbeeld is gebaseerd op de onontvankelijkheid van het getuigenbewijs als er een schriftelijk bewijs voorhanden is; als de wetgever er zo over beslist, is dat omdat hij een geringere bewijskracht toekent aan het getuigenbewijs.

(18) De elektronische handtekening moet worden geavanceerd in de zin van artikel 2, 1*bis*, ze moet gebaseerd zijn op een gekwalificeerd certificaat als bepaald in artikel 2,5 en tot slot moet ze aangemaakt zijn door een veilig middel voor het aanmaken van een handtekening als bepaald in bijlage 3 van het voorstel.

(4) Voir par exemple Commission des Nations Unies pour le Droit commercial international, Rapport du groupe de travail sur le commerce électronique sur les travaux de sa trente et unième session (New York, 18-28 février 1997), A/CN.9/437, 12 mars 1997; Commission des Nations Unies pour le Droit commercial international, Rapport du groupe de travail sur le commerce électronique sur les travaux de sa trente troisième session (New York, 29 juin-10 juillet 1998), A/CN.9/454, 21août 1998. Voir aussi http://www.un.or.at/uncitral/fr-index.htm

(5) Loi allemande sur le multimédia du 13 juin 1997, article 3 (sur la signature digitale), Journal officiel allemand du 22 juillet 1997 (BGBl, IS, 1870), entrée en vigueur le 1er août 1997, http://www.iid.de/iukdg/iukdge.html

(6) Décret présidentiel italien du 10 novembre 1997, n° 513 *in* « *Regulations establishing criteria and means for implementing Section 15 (2) of Law N° 59 of 15 March 1997 concerning the creation, storage and transmission of documents by means of computer-based or telematic systems* », publiée in Gazzetta Ufficiale, 13 mars 1998, n° 60, http://www.aipa.it/english/law[2/pdecree51397.asp

(7) Ce texte est disponible à l'adresse suivante : http://www.etat.lu/ECO/

(8) D. GOBERT, « La sécurisation des échanges par la reconnaissance de la signature électronique : condition d'existence des réseaux d'avocats », in *Multimédia. Le cyberavocat*, Formation permanente CUP, Volume XXIX, Liège-Namur, février 1999, p 173.

(9) http://www.agora98.org/

(10) Plus exactement, ces textes ont été discutés dans l'atelier 1 de la branche « Consommateurs », relatif à la signature électronique et à la certification des sites, présidé par le Professeur Yves Poullet. Cet atelier regroupait des experts et personnes intéressées par le sujet issus du secteur tant privé que public, du barreau, du notariat, du monde universitaire, etc.

(11) Le rapport (*Position Paper*) est disponible à l'adresse suivante : http://www.agora98.org/fr/conso/fconso.html

(12) *Doc. parl.*, Ch. Repr., sess. ord. 14 avril 1999, n° 2141/1.

(13) E. DAVIO, « Certification, signature et cryptographie », in E. MONTERO (éd.), *Internet face au droit*, Cahiers du C.R.I.D., n° 12, E. Story-Scientia, 1997, pp. 80 et suivantes; M. ANTOINE et D. GOBERT, « Pistes de réflexion pour une législation relative à la signature digitale et au régime des autorités de certification », *R.G.D.C.*, juillet-octobre 1998, n° 4/5, pp. 285-310 .

(14) M. ANTOINE, D. GOBERT et A. SALAUN, « Le développement du commerce électronique : les nouveaux métiers de la confiance », dans un ouvrage collectif à paraître, Cahiers du CRID, n° 16, Bruxelles, Bruylant, 1999.

(15) Pour un aperçu de ceux-ci, voyons D. MOUGENOT, « Droit de la preuve et technologies nouvelles : synthèse et perspectives », *Droit de la preuve-Formation permanente CUP*, Volume XIX, octobre 1997, pp. 45-105.

(16) M. ANTOINE, J.-F. BRAKELAND, M. ELOY, *Droit de la preuve face aux nouvelles technologies de l'information*, Cahiers du CRID n°7, Bruxelles, Story-Scientia, 1991, p.55 et suivantes.

(17) Il n'est pas toujours aisé de connaître les forces probantes relatives de deux modes de preuve, car la loi ne les détermine pas systématiquement de manière explicite. Notre exemple se fonde sur l'irrecevabilité de la preuve testimoniale lorsqu'est constituée une preuve par écrit : si le législateur en dispose ainsi, c'est qu'il accorde une force probante moindre à la preuve par témoins.

(18) La signature électronique doit être avancée au sens de l'article 2, 1*bis*, elle doit reposer sur un certificat agréé tel que défini à l'article 2, 5, et enfin elle doit être créée par un dispositif sécurisé de création de signature tel que décrit à l'annexe 3 de la proposition.

VOORONTWERP VAN WET

onderworpen aan het advies van de Raad van State

_____

Voorontwerp van wet betreffende de werking van erkende certificatie-autoriteiten met het oog op het gebruik van digitale handtekeningen

_____

Artikel 1

Deze wet regelt een materie bedoeld in artikel 78 van de Grondwet.

HOOFDSTUK I

Definities, doelstelling en toepassingsgebied van de wet

Art. 2

In deze wet verstaat men onder :

1° digitale handtekening : het resultaat van de omzetting van een digitale gegevensverzameling met behulp van een private sleutel, derwijze dat de identiteit van de titularis van de private sleutel en de integriteit van de digitale gegevens nagegaan kunnen worden met behulp van een overeenkomstige publieke sleutel vergezeld van het certificaat van een certificatie-autoriteit;

2° certificaat : een bevestiging, verzekerd door de digitale handtekening van een certificatie-autoriteit, van een of meer informatiegegevens die door haar zijn vastgesteld, onder meer van het verband tussen een natuurlijke persoon, een privaat- of publiekrechtelijke rechtspersoon, een overheidsbestuur of een feitelijke vereniging en de publieke sleutel ervan;

3° certificatie-autoriteit : een natuurlijke persoon of een rechtspersoon die de certificaten opmaakt, aflevert en beheert;

4° certificaathouder : een natuurlijke, een privaat- of publiekrechtelijke rechtspersoon, een overheidsbestuur of een feitelijke vereniging aan wie een certificatie-autoriteit een certificaat heeft afgeleverd;

5° minister : de minister tot wiens bevoegdheid de Economische Zaken en de Telecommunicatie behoren;

6° administratie : de administratieve dienst die door de Koning is belast met de administratieve taken betreffende de aflevering, de schorsing en de intrekking

AVANT-PROJET DE LOI

soumis à l'avis du Conseil d'État

_____

Avant-projet de loi relative à l'activité d'autorités de certification agréées en vue de l'utilisation de signatures digitales

_____

Article 1er

La présente loi règle une matière visée à l'article 78 de la Constitution.

CHAPITRE Ier

Définitions, objectif et champ d'application de la loi

Art. 2

Aux fins de la présente loi on entend par :

1° signature digitale : le résultat de la transformation d'un ensemble de données digitales à l'aide d'une clé privée, de telle façon que l'identité du titulaire de la clé privée et l'intégrité des données digitales peuvent être vérifiées à l'aide d'une clé publique correspondante, accompagnée du certificat d'une autorité de certification;

2° certificat : une confirmation, sécurisée par la signature digitale d'une autorité de certification, d'une ou plusieurs informations constatées par elle, notamment le lien entre une personne physique, morale de droit privé ou de droit public, une administration publique ou une association de fait et sa clé publique;

3° autorité de certification : une personne physique ou morale qui crée, délivre et gère des certificats;

4° titulaire de certificat : une personne physique, morale de droit privé ou de droit public, une administration publique ou une association de fait à laquelle une autorité de certification a délivré un certificat;

5° ministre : le ministre qui a les Affaires économiques et les Télécommunications dans ses attributions;

6° administration : le service administratif que le Roi charge des tâches administratives relatives à la délivrance, la suspension et au retrait d'agréation des auto-

van de erkenning van de certificatie-autoriteiten evenals met de controle hierop;

7° entiteit : instelling die haar bevoegdheid aantoont op grond van een certificaat afgeleverd door het Belgische accreditatiesysteem conform de wet van 20 juli 1990 betreffende de accreditatie van certificatie- en keuringsinstellingen alsmede van beproevingslaboratoria.

Art. 3

§ 1. Deze wet bepaalt de algemene voorwaarden van de erkenning van de certificatie-autoriteiten, het juridisch regime van toepassing op de activiteiten van de erkende certificatie-autoriteiten evenals de door deze laatsten en de certificaatgebruikers na te leven regels, teneinde de veiligheid van en het vertrouwen in het gebruik van de digitale handtekening te versterken.

§ 2. Een certificatie-autoriteit kan niet worden verplicht een erkenning aan te vragen.

De verkrijging en het behoud van een erkenning zijn onderworpen aan de naleving van de voorwaarden vastgelegd door of krachtens deze wet.

§ 3. De erkenning houdt de aflevering in van certificaten met betrekking tot de identiteit en eventueel, op afzonderlijke wijze, het beroep of elk ander duurzaam kenmerk van de certificaathouder. De certificatie-autoriteit kan de erkenning vragen voor een of meer van deze elementen en ten opzichte van de ene of de andere van deze categorieën van houders.

§ 4. De keuze een beroep te doen op een erkende certificatie-autoriteit is vrij.

Het is evenwel mogelijk door of krachtens een wet, een decreet of een ordonnantie de gevallen te bepalen waarin een digitale handtekening op grond van een door een erkende certificatie-autoriteit uitgegeven certificaat, moet worden gebruikt.

§ 5. Onverminderd de artikelen 1323 en volgende van het Burgerlijk Wetboek is een digitale handtekening, gerealiseerd op grond van een certificaat uitgegeven onder de door deze wet vastgestelde voorwaarden, een handtekening in de zin van artikel 1322 van het Burgerlijk Wetboek wanneer zij door een natuurlijke persoon voor dat doel wordt aangebracht.

rités de certification ainsi qu'à la surveillance de celles-ci;

7° entité : organisme qui démontre sa compétence sur la base d'un certificat délivré par le système belge d'accréditation conformément à la loi du 20 juillet 1990 concernant l'accréditation des organismes de certification et de contrôle, ainsi que les laboratoires d'essais.

Art. 3

§ 1er. La présente loi fixe les conditions générales d'agréation des autorités de certification, le régime juridique applicable aux opérations effectuées par les autorités de certification agréées ainsi que les règles à respecter par ces dernières et les utilisateurs de certificats afin de renforcer la sécurité et la confiance dans l'utilisation de la signature digitale.

§ 2. Une autorité de certification ne peut être obligée de demander une agréation.

L'obtention et le maintien de l'agréation sont subordonnés au respect des conditions fixées par ou en vertu de la présente loi.

§ 3. L'agréation couvre la délivrance de certificats relatifs à l'identité et éventuellement, de façon séparée, à la profession ou tout autre attribut durable du titulaire du certificat. L'autorité de certification peut demander l'agréation pour un ou plusieurs de ces éléments et vis-à-vis de l'une ou l'autre de ces catégories de titulaires.

§ 4. Le choix de recourir à une autorité de certification agréée est libre.

Il est néanmoins possible de fixer par ou en vertu d'une loi, d'un décret ou d'une ordonnance les cas dans lesquels une signature digitale doit être utilisée sur la base d'un certificat émis par une autorité de certification agréée.

§ 5. Sans préjudice des articles 1323 et suivants du Code civil, une signature digitale réalisée sur la base d'un certificat émis dans les conditions fixées par la présente loi constitue une signature au sens de l'article 1322 du Code civil lorsqu'elle est appliquée à cette fin par une personne physique.

HOOFDSTUK II

Erkenningsvoorwaarden

Art. 4

De Koning bepaalt bij een in Ministerraad overlegd besluit de voorwaarden waaronder een certificatie-autoriteit een erkenning verkrijgt en behoudt.

Te dien einde bepaalt hij in het bijzonder :

a) de voldoende waarborgen voor integriteit, beschikbaarheid en veiligheid en de deskundigheid en de voldoende financiële middelen om haar certificatie-activiteiten te kunnen uitoefenen;

b) de waarborgen van onafhankelijkheid ten opzichte van de gebruikers van de dienst;

c) de minimumvoorwaarden inzake de beroepsaansprakelijkheid van de certificatie-autoriteit;

d) de voorwaarden om de interoperabiliteit van de certificatiesystemen te waarborgen;

e) de reikwijdte van de erkenning;

f) de procedure voor de aflevering, uitbreiding, schorsing en intrekking van de erkenning;

g) de verschuldigde bijdragen voor het afleveren, het beheren en het controleren van de erkenning;

h) de onderzoekstermijnen voor de aanvraag;

i) de voorwaarden die de veiligheid, de interne werking van de certificatiesystemen en de uitwisseling van de noodzakelijke gegevens tussen de erkende certificatie-autoriteiten waarborgen;

j) de inzake tarieven toe te passen principes;

k) de minimale normen met betrekking tot de vertrouwelijkheid en de integriteit van de door de certificaathouder verstrekte informatie, de voorwaarden met betrekking tot de werknemers van de certificatie-autoriteit en de voorwaarden met betrekking tot de dienst voor het behandelen van klachten vanwege de klanten;

l) de regels betreffende de informatie die de certificatie-autoriteit over haar diensten en over de door haar uitgereikte certificaten moet bijhouden;

m) de controlemodaliteiten door het bestuur bedoeld in artikel 2, 6°. Het bestuur kan daarbij een beroep doen op de entiteit bedoeld in artikel 2, 7°.

CHAPITRE II

Conditions d'agréation

Art. 4

Le Roi fixe par arrêté délibéré en Conseil des ministres les conditions dans lesquelles une autorité de certification obtient et conserve une agréation.

À cette fin, il fixe notamment :

a) les garanties d'intégrité, de disponibilité et de sécurité suffisantes et l'expertise et les garanties financières suffisantes pour exercer ses activités de certification;

b) les garanties d'indépendance par rapport aux utllisateurs du service;

c) les conditions minimales relatives à la responsabilité professionnelle de l'autorité de certification;

d) les conditions visant à assurer l'intéropabilité des systèmes de certification;

e) la portée de l'agréation;

f) la procédure de délivrance, d'extension, de suspension et de retrait de l'agréation;

g) les redevances dues pour la délivrance, la gestion et le contrôle de l'agréation;

h) les délais d'examen de la demande;

i) les conditions visant à assurer la sécurité, l'intéropabilité des systèmes de certification et à l'échange de données indispensables entre les autorités de certification agréées;

j) les principes tarifaires;

k) les normes minimales relatives à la confidentialité et à l'intégrité de l'information procurée par le titulaire de certificat, les conditions concernant les employés de l'autorité de certification et les conditions concernant le service du traitement de plaintes de la part des clients;

l) les règles relatives à l'information que l'autorité de certification est tenue de conserver concernant ses services et les certificats délivrés par elle;

m) les modalités de contrôle par l'administration visée à l'article 2, 6°. L'administration peut faire appel à l'entité visée à l'article 2, 7°.

HOOFDSTUK III

Regels bettreffende erkende certificatie-autoriteitengel

Afdeling 1

Taken van de erkende certificatie-autoriteit

Art. 5

§ 1. Alvorens de aanvraag voor het certificaat in te dienen, creëert de kandidaat-houder door technische middelen één of meer sleutelparen die bestaan uit een private sleutel en een bijhorende publieke sleutel.

Deze sleutelparen kunnen door technische middelen, die door de certificatie-autoriteit ter beschikking van de kandidaat-houder worden gesteld, worden gecreëerd of, op aanvraag van de kandidaat-houder, rechtstreeks door de certificatie-autoriteit.

De certificatie-autoriteit kan de private sleutel niet registreren, behouden of opnieuw samenstellen.

§ 2. De certificatie-autoriteit creëert één of meer certificaten en levert die af aan elke kandidaat-houder die erom vraagt.

De certificatie-autoriteit weigert een of meer certificaten te maken en af te leveren wanneer zij niet over de nodige middelen beschikt om aan de haar door artikel 7 opgelegde verplichtingen te voldoen.

§ 3. De Koning bepaalt bij een in Ministerraad overlegd besluit de nadere regels voor de toepassing van dit artikel op de rechtspersonen, de feitelijke verenigingen en de openbare besturen, alsook de bijzondere regels die van toepassing zijn op de attributen die de natuurlijke personen in hun certificaat wensen opgenomen te zien.

Art. 6

De certificatie-autoriteit verschaft aan de kandidaat-houder de informatie die noodzakelijk is voor een correct en veilig gebruik van haar diensten.

Deze informatie heeft minstens betrekking op :

a) de verplichting van de certificaat-houder om de vertrouwelijkheid van de private sleutel te verzekeren;

b) de werkwijze die de certificaat-houder dient te volgen om een digitale handtekening te produceren en te verifiëren;

c) de precieze waarborgen die door de diensten van de certificatie-autoriteit worden geboden;

d) de noodzaak om digitaal gehandtekende gegevens te onderwerpen aan een nieuwe handtekening

CHAPITRE III

Régime juridique des autorités de certification agréées

Section 1re

Missions de l'autorité de certification agréée

Art. 5

§ 1er. Préalablement à l'introduction de sa demande de certificat, le candidat titulaire crée par des moyens techniques une ou plusieurs paires de clés comportant une clé privée et une clé publique complémentaires.

Ces paires de clés peuvent être créées par des moyens techniques mis à la disposition du candidat titulaire par l'autorité de certification ou, à la demande du candidat titulaire, directement par celle-ci.

L'autorité de certification ne peut ni enregistrer, ni conserver, ni reconstituer la clé privée.

§ 2. L'autorité de certification crée et délivre un ou plusieurs certificats à tout candidat titulaire qui en fait la demande.

L'autorité de certification refuse la création et la délivrance d'un ou plusieurs certificats lorsqu'elle ne dispose pas des moyens nécessaires pour satisfaire aux obligations qui lui sont imposées par l'article 7.

§ 3. Le Roi fixe par arrêté délibéré en Conseil des ministres, les modalités d'application du présent article aux personnes morales, aux associations de fait et aux administrations publiques ainsi que les règles particulières applicables aux attributs que les personnes physiques veulent voir figurer sur leur certificat.

Art. 6

L'autorité de certification procure au candidat titulaire les informations nécessaires à l'utilisation correcte et sûre de ces services.

Cette information se rapporte au moins :

a) à l'obligation du titulaire de certificat de maintenir le caractère confidentiel de la clé privée;

b) à la procédure que le titulaire d'un certificat doit suivre afin de produire et de vérifier une signature digitale;

c) aux garanties précises qu'offrent les services de l'autorité de certification;

d) à la nécessité de soumettre des données signées digitalement à une nouvelle signature lorsque, après un

wanneer de veiligheid van de bestaande digitale handtekening na verloop van tijd niet meer is gewaarborgd.

Art. 7

Door aan een kandidaathouder een certificaat af te leveren, bevestigt de certificatie-autoriteit het verband tussen de kandidaathouder en zijn publieke sleutel evenals de vermeldingen bedoeld in artikel 10, 1° tot 6° en, in voorkomend geval, in artikel 10, § 2.

Wanneer het certificaat wordt afgeleverd aan een natuurlijke persoon gaat de certificatie-autoriteit de identiteit van de persoon vooraf na volgens de door de Koning vastgelegde voorwaarden.

Wanneer het certificaat wordt afgeleverd aan een privaat- of publiekrechtelijke rechtspersoon, feitelijke vereniging of overheidsbestuur, gaat de certificatie-autoriteit op voorhand de identiteit en de vertegenwoordigingsbevoegdheid na van de natuurlijke persoon die zich hiervoor bij haar aanbiedt, volgens de nadere regels vastgesteld door de Koning.

Onverminderd de toepassing van artikel 5 van de wet van 8 augustus 1983 betreffende het Rijksregister, indien het certificaat wordt afgeleverd aan een kandidaat-titularis met het oog op het gebruik van digitale handtekeningen in de contacten met de overheid, verifiëert de certificatie-autoriteit op voorhand de identiteit van de kandidaat-titularis na raadpleging van het Rijksregister of van andere door de Koning aangeduide registers.

De Koning stelt de nadere regels vast voor het gebruik van digitale handtekeningen in de contacten met de overheid.

Bovendien dient de certificatie-autoriteit de nodige maatregelen te nemen om te na te gaan dat de publieke sleutel die de kandidaat-houder aanbiedt met het oog op certificatie, daadwerkelijk overeenstemt met de private sleutel die de aanvrager beweert te willen gebruiken voor het produceren van digitale handtekeningen.

Art. 8

De certificatie-autoriteit verschaft een exemplaar van het certificaat aan de kandidaat-houder.

Zodra de kandidaat-houder het certificaat heeft aanvaard, schrijft de certificatie-autoriteit dit in, in het elektronische register bedoeld in artikel 9.

Art. 9

De certificatie-autoriteit houdt een elektronisch register bij dat voor iedereen via elektronische weg permanent toegankelijk is. Dit register omvat de door de

certain temps, la sécurité de la signature digitale existante n'est plus garantie.

Art. 7

En délivrant un certificat à un candidat titulaire, l'autorité de certification confirme le lien entre ce dernier et sa clé publique ainsi que les mentions visées à l'article 10, 1° à 6° et, le cas échéant, à l'article 10, § 2.

Si le certificat est délivré à une personne physique, l'autorité de certification vérifie préalablement l'identité de la personne selon les modalités fixées par le Roi.

Si le certificat est délivré à une personne morale de droit privé ou de droit public ou à une administration publique, l'autorité de certification vérifie préalablement l'identité et le pouvoir de représentation de la ou des personne(s) physique(s) qui se présente(nt) à elle selon les modalités fixées par le Roi.

Sans préjudice de l'article 5 de la loi du 8 août 1983 relative au registre national, si le certificat est délivré à un titulaire en vue de l'utilisation de la signature digitale dans les échanges avec les autorités publiques, l'autorité de certification vérifie préalablement l'identité du candidat titulaire en consultant le registre national ou d'autres registres désignés par le Roi.

Le Roi fixe les modalités pour l'utilisation de la signature digitale dans les échanges avec les autorités publiques.

En outre, l'autorité de certification doit prendre les mesures nécessaires afin de vérifier que la clé publique, que le candidat-titulaire présente en vue de la certification, corresponde effectivement à la clé privée que le candidat-titulaire confirme vouloir employer pour produire des signatures digitales.

Art. 8

L'autorité de certification fournit un exemplaire du certificat au candidat-titulaire.

Dès son acceptation par le candidat-titulaire, l'autorité de certification inscrit le certificat dans le registre électronique visé à l'article 9.

Art. 9

L'autorité de certification conserve un registre électronique accessible en permanence à toute personne par voie électronique. Ce registre comprend les certifi-

certificatie-autoriteit afgeleverde certificaten en, in voorkomend geval, het ogenblik van de schorsing of herroeping ervan.

Dit register dient tegen elke niet toegelaten wijziging te worden beschermd.

Onverminderd de toepassing van de artikelen 8 en 9 van de wet van 8 augustus 1983, bevat het register, voor de certificaten die worden afgeleverd onder meer met het oog op de uitwisseling met de overheid, het identificatienummer van de houder bij het nationaal register. Dit identificatienummer kan slechts toegankelijk zijn voor de autoriteiten die gemachtigd zijn om het te gebruiken.

Afdeling 2

Inhoud van het certificaat

Art. 10

§ 1. Een certificaat bevat minstens onderstaande informatie :

1) de naam en voornaam, elk ander pertinent gegeven dat toelaat om de titularis te identificeren, of, in voorkomend geval, het pseudoniem van de natuurlijke persoon die het certificaat aanvraagt, voorafgegaan door de vermelding dat het om een « pseudoniem » gaat;

2) de publieke sleutel van de houder;

3) de referentie naar de algoritmen noodzakelijk voor het gebruik van de publieke sleutel van de certificaathouder evenals de publieke sleutel van de certificatie-autoriteit;

4) de identificatiecode van het certificaat;

5) de datum van uitgifte en de datum van afloop van het certificaat;

6) de gegevens met betrekking tot de identificatie en de erkenning van de certificatie-autoriteit.

§ 2. Bovendien kan het certificaat nog andere informatie bevatten. De certificatie-autoriteit is evenwel niet verplicht deze laatste te bevestigen. Zij vermeldt in het certificaat de al dan niet bevestigde aard van elke informatie.

cats délivrés par l'autorité de certification et, le cas échéant, le moment de leur suspension ou de leur révocation.

Ce registre doit être protégé contre toute modification non autorisée.

Sans préjudice des articles 8 et 9 de la loi du 8 août 1983 relative au registre national, pour les certificats qui sont délivrés en vue notamment des échanges avec une autorité publique, le registre comporte le numéro d'identification du titulaire au registre national. Ce numéro d'identification ne peut être accessible qu'aux autorités habilitées à l'utiliser.

Section 2

Contenu du certificat

Art. 10

§ 1er. Un certificat contient au moins les informations suivantes :

1) les nom et prénom, tout autre renseignement pertinent permettant d'identifier le titulaire du certificat ou, le cas échéant, le pseudonyme de la personne physique qui en fait la demande, précédé de l'indication qu'il s'agit d'un « pseudonyme »;

2) la clé publique du titulaire;

3) la référence aux algorithmes nécessaires pour utiliser la clé publique du titulaire du certificat ainsi que la clé publique de l'autorité de certification;

4) le code d'identification du certificat;

5) la date d'émission et la date d'expiration du certificat;

6) les données d'identification et d'agréation de l'autorité de certification.

§ 2. En outre, le certificat peut contenir d'autres informations. L'autorité de certification n'est cependant pas tenue de confirmer ces dernières. Elle indique dans le certificat le caractère confirmé ou non de chaque information.

Afdeling 3

Verplichtingen van de certificaathouder

Art. 11

§ 1. Vanaf de creatie van het sleutelpaar is de certificaathouder de enige verantwoordelijke voor de vertrouwelijkheid en de integriteit van de private sleutel.

Elk gebruik ervan wordt, behoudens tegenbewijs, geacht een daad te zijn van diens houder.

§ 2. In geval van twijfel betreffende het behoud van de vertrouwelijkheid van de private sleutel of het verlies aan overeenstemming met de realiteit van de gegevens opgenomen in het certificaat, is de houder ertoe gehouden het certificaat krachtens de artikelen 12 en 13 van deze wet te doen schorsen, of zelfs te doen herroepen.

§ 3. Wanneer een certificaat vervalt, werd geschorst of herroepen, kan de houder ervan, na de afloop van het certificaat, gedurende de periode van schorsing of na de herroeping, de overeenstemmende private sleutel niet gebruiken voor een digitale handtekening, noch het sleutelpaar door een andere certificatie-autoriteit doen certifiëren.

Section 3

Obligations du titulaire de certificat

Art. 11

§ 1er. Dès la création de la paire de clés, le titulaire du certificat est seul responsable de la confidentialité et de l'intégrité de la clé privée.

Toute utilisation de celle-ci est réputée, sauf preuve contraire, être le fait de son titulaire.

§ 2. En cas de doute quant au maintien de la confidentialité de la clé privée ou de perte de conformité à la réalité des informations contenues dans le certificat, le titulaire est tenu de faire suspendre, voire révoquer, le certificat conformément aux articles 12 et 13 de la présente loi.

§ 3. Lorsqu'un certificat est arrivé à échéance, a été suspendu ou révoqué, le titulaire de celui-ci ne peut, après l'expiration du certificat, pendant la période de suspension ou après révocation, utiliser la clé privée correspondante pour générer une signature digitale ou faire certifier la paire de clés par une autre autorité de certification.

Afdeling 4

Schorsing of herroeping van het certificaat

Art. 12

§ 1. Op aanvraag van de vooraf geïdentificeerde certificaathouder of op aanvraag van de persoon waarvan de gegevens op het certificaat zijn vermeld, schorst de certificatie-autoriteit onmiddellijk het certificaat.

Onder dezelfde omstandigheden heft zij de schorsing terug op.

§ 2. De certificatie-autoriteit schorst het certificaat eveneens wanneer er ernstige en gemotiveerde redenen bestaan om aan te nemen dat het certificaat werd afgeleverd op basis van foutieve of vervalste informatie, dat de in het certificaat opgenomen informatie niet meer overeenstemt met de werkelijkheid of dat de vertrouwelijkheid van de private sleutel werd geschonden.

In deze gevallen brengt de certificatie-autoriteit de certificaathouder hiervan op de hoogte en motiveert zij haar beslissing tot schorsing.

De schorsing moet onmiddellijk worden opgeheven wanneer een meer diepgaand onderzoek de correcte aard van de informatie of de niet-schending van de vertrouwelijkheid van de private sleutel aantoont.

Section 4

Suspension et révocation de certificat

Art. 12

§ 1er. À la demande du titulaire de certificat préalablement identifié ou à la demande de la personne dont les données figurent sur le certificat, l'autorité de certification suspend immédiatement le certificat.

Elle lève cette suspension dans les mêmes conditions.

§ 2. L'autorité de certification suspend également le certificat lorsqu'il existe des raisons sérieuses et motivées pour admettre que le certificat a été délivré sur la base d'informations erronées ou falsifiées, que les informations contenues dans le certificat ne sont plus conformes à la réalité ou que la confidentialité de la clé privée a été violée.

Dans ces cas, l'autorité de certification informe le titulaire du certificat et motive sa décision de suspension.

La suspension doit immédiatement être levée lorsqu'un examen plus approfondi démontre le caractère correct de l'information ou la non violation de la confidentialité de la clé privée.

Art. 13

§ 1. Op aanvraag van de vooraf geïdentificeerde certificaathouder herroept de certificatie-autoriteit onmiddellijk het certificaat.

§ 2. De certificatie-autoriteit herroept eveneens een certificaat wanneer :

a) na de schorsing een meer diepgaand onderzoek de foutieve of valse aard van de informatie bedoeld door artikel 12, § 2, de niet-overeenkomstigheid met de werkelijkheid of de schending van de vertrouwelijkheid van de private sleutel aantoont;

b) de administratie de herroeping beveelt zoals bepaald in artikel 15;

c) de certificatie-autoriteit haar activiteiten stopzet zonder dat deze worden overgenomen door een andere certificatie-autoriteit;

d) het certificaat afloopt; de certificatie-autoriteit brengt de houder een maand voor de herroeping hiervan op de hoogte;

e) zij op de hoogte wordt gebracht van het overlijden van de natuurlijke persoon of van de vereffening van de rechtspersoon die er certificaathouder van is.

De certificatie-autoriteit brengt de certificaathouder hiervan op de hoogte en motiveert haar beslissing tot herroeping.

§ 3. De herroeping van een certificaat is definitief.

Art. 14

§ 1. De certificatie-autoriteit treft de nodige maatregelen om op elk ogenblik en onverwijld gevolg te geven aan een aanvraag tot schorsing of herroeping.

§ 2. Onmiddellijk na de beslissing tot schorsing of herroeping neemt de certificatie-autoriteit de vermelding van de schorsing of de herroeping op in het elektronische register bedoeld in artikel 9.

Vanaf deze inschrijving zijn de schorsing en de herroeping tegenstelbaar ten aanzien van derden.

§ 3. De certificatie-autoriteit bewaart de in het certificaat opgenomen vermeldingen gedurende 20 jaar na de datum van afloop, schorsing of herroeping van het certificaat.

Deze gegevens moeten toegankelijk zijn voor elke persoon een belang aantoont.

Art. 13

§ 1er. À la demande du titulaire de certificat préalablement identifié, l'autorité de certification révoque immédiatement le certificat.

§ 2. L'autorité de certification révoque également un certificat lorsque :

a) après suspension, un examen plus approfondi démontre le caractère erroné ou falsifié des informations visées à l'article 12, § 2, leur non conformité à la réalité ou la violation de la confidentialité de la clé privée;

b) l'administration ordonne la révocation comme prévu à l'article 15;

c) l'autorité de certification arrête ses activités sans qu'il n'y ait reprise de celles-ci par une autre autorité de certification;

d) le certificat arrive à échéance; l'autorité de certification en informe le titulaire un mois avant la révocation;

e) elle est informée du décès de la personne physique ou de la liquidation de la personne morale qui en est le titulaire.

L'autorité de certification en informe le titulaire de certificat et motive sa décision de révocation.

§ 3. La révocation d'un certificat est définitive.

Art. 14

§ 1er. L'autorité de certification prend les mesures nécessaires afin de répondre à tout moment et sans délai à une demande de suspension ou de révocation.

§ 2. Immédiatement après la décision de suspension ou de révocation, l'autorité de certification inscrit la mention de la suspension ou de la révocation du certificat dans le registre électronique visé à l'article 9.

La suspension et la révocation sont opposables aux tiers à partir de cette inscription.

§ 3. L'autorité de certification conserve les mentions reprises dans le certificat pendant une durée de 20 ans à dater de l'expiration, de la suspension ou de la révocation du certificat.

Ces données doivent être accessibles à toute personne justifiant d'un intérêt.

Afdeling 5

Stopzetting van de activiteiten

Art. 15

§ 1. De certificatie-autoriteit brengt binnen een redelijke termijn de administratie op de hoogte dat zij van plan is haar activiteiten stop te zetten. In dit geval, dient zij zich te vergewissen van de overname ervan door een andere erkende certificatie-autoriteit en, indien zij dit niet kan, herroept zij de certificaten twee maanden na de houders ervan op de hoogte te hebben gebracht.

§ 2. De certificatie-autoriteit die haar activiteiten stopzet om redenen buiten haar wil om, brengt de administratie hiervan onmiddellijk op de hoogte. Deze vergewist zich van de herroeping van de certificaten en treft de nodige maatregelen om te voldoen aan de in artikel 14, § 3 bepaalde verplichting. Daartoe verschaft de certificatie-autoriteit de administratie alle nuttige informatie.

Afdeling 6

Bescherming van de persoonlijke levenssfeer

Art. 16

§ 1. De certificatie-autoriteit kan enkel de persoonlijke gegevens verzamelen die noodzakelijk zijn om haar opdrachten uit te voeren. Ze kunnen enkel worden gebruikt in het kader van certificatie-activiteiten. Het inwinnen van informatie bij derden kan enkel gebeuren met de instemming van de kandidaat-houder of de certificaathouder.

§ 2. Wanneer de houder van het certifcaat een pseudoniem gebruikt en het strafrechtelijk onderzoek dit vereist, is de certificatie-autoriteit die het certificaat heeft afgeleverd, ertoe gehouden elke informatie over de identiteit van de houder mee te delen in de omstandigheden en onder de voorwaarden bedoeld in de artikelen 90*ter* en volgende van het Wetboek van strafvordering.

Section 5

Arrêt des activités

Art. 15

§ 1er. L'autorité de certification informe dans un délai raisonnable l'administration de son intention de mettre fin à ses activités. Dans ce cas, elle doit s'assurer de la reprise de celles-ci par une autre autorité de certification agréée et à défaut, révoque les certificats deux mois après en avoir averti les titulaires.

§ 2. L'autorité de certification qui arrête ses activités pour des raisons indépendantes de sa volonté en informe immédiatement l'administration. Celle-ci s'assure de la révocation des certificats et prend les mesures nécessaires pour satisfaire à l'obligation prévue à l'article 14, § 3. À cet effet l'autorité de certification transmet toute information utile à l'administration.

Section 6

Protection de la vie privée

Art. 16

§ 1er. L'autorité de certification peut uniquement collecter les données à caractère personnel nécessaires à l'exercice de ses missions. Elles ne peuvent être utilisées que dans le cadre des activités de certification. La collecte d'informations auprès de tierces personnes peut uniquement avoir lieu avec le consentement du candidat titulaire ou du titulaire de certificat.

§ 2. Lorsque le titulaire du certificat utilise un pseudonyme et lorsque les nécessités de l'instruction l'exigent, l'autorité de certification ayant délivré le certificat est tenue de communiquer toute donnée relative à l'identité du titulaire dans les circonstances et selon les conditions prévues par les articles 90*ter* et suivants du Code d'instruction criminelle.

Afdeling 7

Certificaat afgeleverd door een buitenlandse certificatie-autoriteit

Art. 17

Een certificaat afgeleverd door een buitenlandse certificatie-autoriteit die is gevestigd in een van de Lidstaten van de Europese Unie of in een staat die het Verdrag voor de Europese Economische Ruimte heeft ondertekend, wordt, bij toepassing van deze wet, gelijkgesteld met certificaten afgeleverd door een erkende certificatie-autoriteit wanneer het hetzelfde veiligheidsniveau biedt.

De administratie maakt een lijst op van de buitenlandse certificatie-autoriteiten die certificaten afleveren met dezelfde veiligheidsgraad, zoals vermeld in het vorige lid van dit artikel.

Het bepaalde in dit artikel is eveneens van toepassing op andere staten voor zover deze staten met België of met de Europese Unie overeenkomsten hebben gesloten met betrekking tot de wederzijdse erkenning van certificaten.

Afdeling 8

Betrouwbaarheid van de technische middelen

Art. 18

§ 1. Het creëren van het sleutelpaar, het maken, afleveren en bijhouden van de certificaten evenals het maken en het verifiëren van de digitale handtekening gebeuren door middel van betrouwbare technische middelen met een adequaat veiligsheidniveau om met name elke schending van de integriteit van een digitaal ondertekend bericht of een certificaat en elk niet-toegelaten gebruik van de private sleutel, te voorkomen of op te sporen.

§ 2. De betrouwbaarheid en het adequaat karakter van het veiligheidsniveau worden beoordeeld volgens de stand van de techniek zoals vastgesteld en openbaar gemaakt door de administratie of elke door haar aangewezen entiteit.

Section 7

Certificat délivré par une autorité de certification étrangère

Art. 17

Un certificat délivré par une autorité de certification qui a son domicile dans un État-membre de l'Union européenne ou dans un état ayant signé la Convention de l'Espace Économique Européen, est assimilé aux certificats délivrés par une autorité de certification agréée, en application de la présente loi, lorsqu'il présente le même niveau de sécurité.

L'administration dresse une liste où figurent les autorités de certification étrangères qui délivrent des certificats qui atteignent le même niveau de sécurité, comme mentionné dans l'alinéa précédent du présent l'article.

Ce qui a été stipulé dans le présent article est également d'application à d'autres états dans la mesure où ces états ont conclu avec la Belgique ou avec l'Union européenne des conventions relatives à la reconnaissance mutuelle de certificats.

Section 8

Fiabilité des moyens techniques

Art. 18

§ 1er. La création de la paire de clés, la création, la délivrance et la conservation des certificats ainsi que la production et la vérification de la signature digitale sont réalisées par des moyens techniques fiables et présentant un niveau de sécurité adéquat afin, notamment, d'éviter ou de détecter toute atteinte à l'intégrité d'un message signé digitalement ou d'un certificat et toute utilisation non autorisée d'une clé privée.

§ 2. La fiabilité et l'adéquation du niveau de sécurité sont appréciées en fonction de l'état de la technique tel qu'arrêté et rendu public par l'administration ou toute entité désignée par elle.

Afdeling 9

Aansprakelijkheid

Art. 19

§ 1. Onverminderd de wettelijke bepalingen betreffende de burgerlijke aansprakelijkheid staat de certificatie-autoriteit in voor de schade die het gevolg is van de niet-uitvoering van de verplichtingen die haar zijn opgelegd door of krachtens deze wet.

§ 2. De Koning stelt de minimum- en maximumbedragen vast waaronder en waarboven de partijen de aansprakelijkheid van de certificatie-autoriteit niet mogen beperken of uitbreiden.

§ 3. Elke overeenkomst die in strijd is met de bepalingen van dit artikel wordt beschouwd als niet-geschreven.

Art. 20

Onverminderd de andere wettelijke bepalingen betreffende de burgerlijke aansprakelijkheid staat de certificaathouder in voor de schade die het gevolg is van de niet-uitvoering van de verplichtingen die hem door of krachtens deze wet zijn opgelegd.

Afdeling 10

Controle en sancties

Art. 21

Wanneer de administratie vaststelt dat een erkende certificatie-autoriteit zich niet aan de voorschriften van deze wet houdt, stelt ze een termijn vast om de toestand te regulariseren.

Wanneer na afloop van die termijn de erkende certificatie-autoriteit haar toestand niet heeft geregulariseerd, trekt de minister de erkenning in.

De certificatie-autoriteit is ertoe gehouden de intrekking van erkenning in haar register te vermelden en de houders onverwijld hiervan op de hoogte te brengen.

Art. 22

§ 1. Wie misbruik maakt van de hoedanigheid van erkende certificatie-autoriteit, wordt bestraft met een gevangenisstraf van 8 dagen tot 3 maanden en met een boete van 1 000 tot 10 000 Belgische frank, of met

Section 9

Responsabilités

Art. 19

§ 1er. Sans préjudice des dispositions légales relatives à la responsabilité civile, l'autorité de certification répond du dommage qui est la conséquence de l'inexécution des obligations qui lui sont imposées par ou en vertu de la présente loi.

§ 2. Le Roi fixe les montants minimal et maximal endeçà et au-delà desquels les parties ne peuvent limiter ou étendre la responsabilité de l'autorité de certification.

§ 3. Toute convention contraire aux dispositions du présent article est réputée non écrite.

Art. 20

Sans préjudice des autres dispositions légales relatives à la responsabilité civile, le titulaire du certificat répond du dommage qui est la conséquence de l'inexécution des obligations qui lui sont imposées par ou en vertu de la présente loi.

Section 10

Contrôle et sanctions

Art. 21

Lorsque l'administration constate qu'une autorité de certification agréée ne se conforme pas aux prescriptions de la présente loi, elle fixe un délai pour régulariser la situation.

Si, après l'écoulement de ce délai, l'autorité de certification agréée n'a pas régularisé sa situation, le ministre procède au retrait de l'agréation.

L'autorité de certification est tenue de mentionner dans son registre le retrait de l'agréation et d'en informer sans délai les titulaires.

Art. 22

§ 1er. Sera puni d'une peine de 8 jours à 3 mois de prison et d'une amende de 1 000 à 10 000 francs belges, ou d'une de ces peines seulement, quiconque aura usurpé la qualité d'autorité de certification agréée. Ce-

slechts een van deze straffen. Hij die artikel 4, a), b) of k) schendt, wordt bestraft met dezelfde straffen.

§ 2. Door te veroordelen op grond van de in paragraaf 1 bedoelde overtreding, kan de bevoegde rechtbank de volledige of gedeeltelijke opneming van het vonnis in een of meerdere dagbladen bevelen, onder de door haar bepaalde voowaarden en op kosten van de veroordeelde.

§ 3. De certificatie-autoriteit is burgerlijk aansprakelijk voor de betaling van de boetes waartoe haar beambte of mandataris is veroordeeld.

Art. 22

In artikel 5, lid 1, van de wet van 8 augustus 1983 worden de woorden « de erkende certificatie-autoriteiten bedoeld in de wet van (...) betreffende de werking van erkende certificatie-autoriteiten met het oog op het gebruik van digitale handtekeningen », gevoegd tussen de woorden « de notarissen en gerechtsdeurwaarders » en de woorden « voor de informatie die zij krachtens een wet of een decreet bevoegd zijn te kennen ».

lui qui aura violé l'article 4 a), b) ou k) sera puni des mêmes peines.

§ 2. En condamnant du chef d'infraction visé au paragraphe 1er, la juridiction compétente peut ordonner l'insertion du jugement, intégralement ou par extraits, dans un ou plusieurs journaux, dans les conditions qu'elle détermine, aux frais du condamné.

§ 3. L'autorité de certification est civilement responsable du paiement des amendes auxquelles son préposé ou mandataire a été condamné.

Art. 22

À l'article 5, alinéa 1er, de la loi du 8 août 1983 relative au registre national, les mots « aux autorités de certification agrées, visées par la loi du (...) relative à l'activité d'autorité de certification agrée en vue de l'utisation de signatures digitales » sont insérés entre les motifs « aux notaires et huissiers de justice » et les mots « pour les informations qu'ils sont habilités à connaître en vertu d'une loi ou d'un décret ».

ADVIES VAN DE RAAD VAN STATE

De RAAD VAN STATE, afdeling wetgeving, vierde kamer, op 18 juni 1998 door de Minister van Economie en Telecommunicatie verzocht hem, binnen een termijn van ten hoogste een maand, van advies te dienen over een voorontwerp van wet « betreffende de werking van erkende certificatie-autoriteiten met het oog op het gebruik van digitale handtekeningen », heeft op 16 september 1998 het volgende advies gegeven :

ALGEMENE OPMERKINGEN

1. Op 13 mei 1998 heeft de Europese Commissie aan het Europees Parlement, de Raad, het Economisch en Sociaal Comité en het Comité van de Regio's een voorstel voor een richtlijn van het Europees Parlement en van de Raad betreffende een gemeenschappelijk kader voor elektronische handtekeningen (1) bezorgd.

Met dat voorstel voor een richtlijn wil men het gebruik van elektronische handtekeningen bevorderen en de wettelijke erkenning ervan waarborgen. Het voorstel heeft het volgende tot doel : « (Het) biedt voor bepaalde certificatiediensten die het publiek worden aangeboden, een wettelijk kader teneinde het goed functioneren van de interne markt op het gebied van elektronische handtekeningen te waarborgen » (artikel 1).

Net als het onderhavige voorontwerp gaat het voorstel uit van het principe dat de markt van de verlening van certificatiediensten vrij toegankelijk moet zijn (2) en biedt het de lidstaten tegelijk de mogelijkheid om « vrijwillige accreditatieregelingen in te voeren of te behouden die op verbetering van het certificatiedienstverleningsniveau zijn gericht » (artikel 3).

Het voorstel voor een richtlijn wijkt evenwel op een belangrijk punt van het onderzochte voorontwerp af.

Terwijl het voorontwerp immers alleen aan erkende « certificatie-autoriteiten » en houders van certificaten die door die autoriteiten zijn afgegeven een reeks verplichtingen oplegt en ook alleen aan handtekeningen vergezeld van een door een « erkende certificatie-autoriteit » uitgegeven certificaat een bijzondere juridische waarde hecht (3), bepaalt het voorstel voor een richtlijn

(1) Doc COM (1998) 297 definitief van 13 mei 1998 « Voorstel voor een richtlijn van het Europees Parlement en van de Raad betreffende een gemeenschappelijk kader voor elektronische handtekeningen » (Voor de EER relevante richtlijn).

(2) Het begrip « certificatiedienstverlener » stemt overeen met wat in het voorontwerp van wet « certificatie-autoriteit » wordt genoemd. De EG-terminologie verdient de voorkeur, om duidelijk aan te geven dat certificatie een privé-activiteit is.

(3) Zie ook artikel 3, § 4, van het voorontwerp.

AVIS DU CONSEIL D'ÉTAT

Le CONSEIL D'ÉTAT, section de législation, quatrième chambre, saisi par le ministre de l'Économie et des Télécommunications, le 18 juin 1998, d'une demande d'avis, dans un délai ne dépassant pas un mois, sur un avant-projet de loi « relative à l'activité d'autorités de certification agréées en vue de l'utilisation de signatures digitales », a donné le 16 septembre 1998 l'avis suivant :

OBSERVATIONS GÉNÉRALES

1. Le 13 mai 1998, la Commission européenne a communiqué au Parlement européen, au Conseil, au Comité économique et social et au Comité des Régions une proposition de directive du Parlement européen et du Conseil sur un cadre commun pour les signatures électroniques (1).

Cette proposition de directive vise à faciliter l'utilisation des signatures électroniques et à assurer leur reconnaissance juridique. Elle tend à « instituer un cadre juridique pour certains services de certification accessibles au public, afin d'assurer le bon fonctionnement du marché intérieur dans le domaine des signatures électroniques » (article 1er).

Tout comme le présent avant-projet, la proposition retient comme principe le libre accès au marché de la fourniture des services de certification (2), tout en autorisant les États membres à « instaurer ou maintenir des régimes volontaires d'accréditation visant à élever le niveau du service de certification fourni » (article 3).

La proposition de directive s'écarte toutefois sur un point essentiel de l'avant-projet à l'examen.

En effet, alors que l'avant-projet ne soumet à une série d'obligations que les « autorités de certification » agréées et les titulaires des certificats délivrés par ces autorités et, en contrepartie, attribue une valeur juridique particulière aux seules signatures accompagnées d'un certificat délivré par une « autorité de certification agréée » (3), la proposition de directive prévoit, d'une

(1) Doc. Com (1998) 297 final du 13 mai 1998 « Proposition de directive du Parlement européen et du Conseil sur un cadre commun pour les signatures électroniques (Directive présentant de l'intérêt pour l'EEE).

(2) La définition donnée par la directive des « prestataires de services de certification » correspond à ce que l'avant-projet de loi appelle « autorité de certification ». La terminologie communautaire doit être préférée, afin de ne pas induire en erreur sur la nature privée de l'activité de certification.

(3) Voir également l'article 3, § 4, de l'avant-projet.

enerzijds dat de bepalingen die de lidstaten krachtens deze richtlijn vaststellen, van toepassing zijn op alle certificatiedienstverleners die op hun grondgebied gevestigd zijn (artikel 4, lid 1), ongeacht of ze geaccrediteerd zijn zijn of niet, en anderzijds dat de lidstaten er zorg voor dragen dat de elektronische handtekeningen die gebaseerd zijn op een gekwalificeerd certificaat dat door een certificatiedienstverlener is afgegeven die aan de vereisten van de richtlijn voldoet, dezelfde juridische waarde als een handgeschreven handtekening hebben en op dezelfde wijze als een handgeschreven handtekening in rechte aanvaardbaar zijn (artikel 5, lid 2).

Er zijn nog andere grote verschillen tussen het voorontwerp van wet en het voorstel voor een richtlijn.

Zo bijvoorbeeld blijft het begrip elektronische handtekening, aangezien die met een handgeschreven handtekening kan worden gelijkgesteld, in het voorstel voor een richtlijn neutraal ten aanzien van de gebruikte technologie en is dat begrip dus niet strikt beperkt tot asymmetrische cryptografie, zoals in het voorontwerp het geval is.

Een ander voorbeeld : in het voorstel voor een richtlijn kan de certificatiedienstverlener zich aan zijn aansprakelijkheid voor fouten in de gegevens op het certificaat onttrekken als hij aantoont dat hij alle in redelijkheid mogelijke maatregelen heeft getroffen om die gegevens te verifiëren (artikel 6, lid 2) en mag hij een grens stellen aan de waarde van de transacties waarvoor het certificaat geldig is (artikel 6, lid 4). In het voorontwerp zijn zulke bepalingen niet terug te vinden, maar wordt daarentegen voorzien in een beperking van de contractbepalingen tot begrenzing van aansprakelijkheid.

Nog een ander voorbeeld : artikel 8, lid 2, van de richtlijn bepaalt dat een certificatiedienstverlener persoonlijke gegevens slechts rechtstreeks van het datasubject kan verkrijgen, wat inhoudt dat de identiteit niet bij het Rijksregister van de natuurlijke personen kan worden nagegaan, zoals artikel 7, vierde lid, van het voorontwerp bepaalt voor handtekeningen die in betrekkingen met de overheid gebezigd worden.

Gelet op die verschillen staat het aan de steller van het voorontwerp te oordelen of het niet wenselijk is te wachten tot de Europese richtlijn is aangenomen alvorens die aangelegenheid bij wet te regelen, om te voorkomen dat de wet kort na de inwerkingtreding ervan grondig moet worden gewijzigd.

Immers, in ieder geval lijkt het dat nu al, zonder groot gevaar om zich te vergissen, mag worden aangenomen dat de federale wetgever een algemene regeling voor certificatiedienstverlening in verband met elektronische handtekeningen zal moeten opstellen en zich niet tot een regeling van de rechten en plichten van louter de erkende dienstverleners zal mogen beperken. Het is weinig waarschijnlijk dat de richtlijn die weg opgaat, die

part, que les dispositions que les États membres adoptent conformément à elle, s'appliquent à tous les prestataires de services de certification établis sur leur territoire (article 4, paragraphe 1er), qu'ils soient ou non accrédités et, d'autre part, que 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 de la directive, aient la même valeur juridique d'une signature manuscrite et soient admissibles en justice de la même façon que les signatures manuscrites (article 5, paragraphe 2).

D'autres différences significatives apparaissent entre l'avant-projet de loi et la proposition de directive.

Ainsi, par exemple, dans cette dernière, la notion de signature électronique pouvant être assimilée à une signature manuscrite, reste neutre par rapport à la technologie utilisée et n'est donc pas strictement limitée, comme dans l'avant-projet, à la cryptographie asymétrique.

Autre exemple : dans la proposition de directive, le prestataire de services de certification peut s'exonérer de sa responsabilité en cas d'erreur dans les informations contenues dans le certificat s'il démontre qu'il a pris toutes les mesures raisonnablement applicables pour vérifier les informations (article 6, paragraphe 2), et il peut indiquer une valeur limite des transactions pour lesquelles le certificat est valable (article 6, paragraphe 4). Quant à lui, l'avant-projet ne contient pas de telles dispositions, mais prévoit par contre une limitation des clauses contractuelles restrictives de responsabilité.

Autre exemple encore : l'article 8, paragraphe 2, de la directive indique qu'un prestataire de services de certification ne peut recueillir des données personnelles que directement auprès de la personne qui en fait l'objet, ce qui exclut une vérification de l'identité auprès du registre national des personnes physiques, ainsi que le prévoit l'article 7, alinéa 4, de l'avant-projet pour les signatures utilisées dans les relations avec les autorités publiques.

Au vu de ces divergences, il appartiendra à l'auteur de l'avant-projet d'apprécier s'il n'est pas souhaitable d'attendre que la directive européenne soit adoptée, avant de légiférer dans cette matière, afin d'éviter de devoir modifier considérablement la loi peu de temps après son entrée en vigueur.

En effet, il semble en tout cas que l'on puisse d'ores et déjà considérer, sans grand risque de se tromper, que le législateur fédéral devra réglementer, de manière générale, la prestation de services de certification de signatures électroniques, et ne pas se limiter à prévoir des droits et des obligations pour les seuls prestataires agréés. Il est peu probable que la directive s'engage dans cette voie, qui est susceptible de ne pas assurer

van die aard is dat de vrije verlening van die diensten in de Europese Unie en de Europese Economische Ruimte niet gewaarborgd zou worden.

2. De erkenningsregeling die in het voorontwerp wordt gepland, beperkt het vrij verrichten van diensten, daar artikel 17 van dat voorontwerp bepaalt dat certificaten die worden afgegeven door een « certificatie-autoriteit » die in een andere lidstaat van de Europese Unie gevestigd is of in een staat die partij is bij het Verdrag voor de Europese Economische Ruimte, alleen worden gelijkgesteld met certificaten die overeenkomstig het wetsontwerp worden afgegeven als die « autoriteit » op een lijst voorkomt opgesteld door de « administratie » die de « veiligheidsgraad » van de certificaten zal beoordelen.

Ook artikel 3, § 4, tweede lid, van het voorontwerp is strijdig met het vrij verrichten van diensten.

3. Artikel 3, § 5, van het onderzochte voorontwerp bepaalt dat « een digitale handtekening, gerealiseerd op grond van een certificaat uitgegeven onder de door deze wet vastgestelde voorwaarden, een handtekening (is) in de zin van artikel 1322 van het burgerlijk wetboek wanneer zij door een natuurlijke persoon voor dat doel aangebracht wordt ».

Er wordt verwezen naar het huidige artikel 1322 van het Burgerlijk Wetboek.

Er dient evenwel rekening mee te worden gehouden dat artikel 3 van het voorontwerp van wet « tot wijziging van sommige bepalingen van het Burgerlijk Wetboek met betrekking tot het bewijs van verbintenissen », dat thans ter fine van advies aan de Raad van State voorgelegd is onder het nummer L. 27.982/2, tot doel heeft het genoemde artikel 1322 van het Burgerlijk Wetboek aan te vullen met de volgende leden :

« Wordt gelijkgesteld met de eigenhandig geschreven handtekening, de gegevensverzameling die ontstaat uit de transformatie van het geschrift en waaruit met zekerheid de identiteit van de auteur en zijn instemming met de inhoud van het geschrift blijkt.

Bij toepassing van vorige alinea wordt het ondertekende geschrift waarvan het behoud van de integriteit van de inhoud met zekerheid vaststaat, gelijkgesteld met een originele onderhandse akte. ».

De strekking van die wijziging is ruimer dan die van het onderzochte artikel 3, § 5, aangezien in de memorie van toelichting bij het voorontwerp van wet met kenmerk L. 27.982/2 het volgende staat :

« De omschrijving — « gegevensverzameling die ontstaat uit de transformatie van het geschrift » — is dermate ruim dat ze niet beperkt blijft tot de momenteel bestaande technische procédés van « digitale » handtekening. ».

Er zijn nog andere verschillen tussen de beide teksten : het onderzochte artikel 3, § 5, is alleen van toepassing op handtekeningen die door een natuurlijke persoon geplaatst zijn en bevat de woorden « (is) een

la libre prestation de ces services dans l'Union européenne et l'Espace économique européen.

2. Le système d'agrément envisagé par l'avant-projet constitue une entrave à la libre prestation de services dans la mesure où son article 17 prévoit que les certificats délivrés par les « autorités de certification » domiciliées dans d'autres États membres de l'Union européenne ou parties à la Convention sur l'Espace économique européen, ne sont assimilés à des certificats délivrés conformément au projet de loi que si ces « autorités » figurent sur une liste dressée par « l'administration », qui appréciera le « niveau de sécurité » des certificats.

L'article 3, § 4, alinéa 2, de l'avant-projet est également contraire à la libre prestation des services.

3. L'article 3, § 5, de l'avant-projet à l'examen dispose qu'« une signature digitale, réalisée sur la base d'un certificat émis dans les conditions fixées par la loi en projet, constitue une signature au sens de l'article 1322 du Code civil lorsqu'elle est appliquée à cette fin par une personne physique ».

La référence est faite à l'article 1322 actuel du Code civil.

Il convient cependant de tenir compte du fait que l'article 3 de l'avant-projet de loi « visant à modifier certaines dispositions du Code civil relatives à la preuve des obligations », actuellement soumis à l'avis du Conseil d'État sous le n° L. 27.982/2, tend à compléter ledit article 1322 du Code civil par les alinéas suivants :

« Est assimilé à une signature manuscrite l'ensemble de données issues de la transformation de l'écrit et dont ressort avec certitude l'identité de l'auteur et son adhésion au contenu de l'écrit.

En cas d'application de l'alinéa précédent, est assimilé à un acte sous seing privé original l'écrit signé dont le maintien de l'intégrité du contenu est établi avec certitude. ».

La portée de cette modification est plus large que celle de l'article 3, § 5, à l'examen puisque, selon l'exposé des motifs, de l'avant-projet de loi référencé L. 27.982/2 :

« La définition — ensemble de données issues de la transformation de l'écrit — est tellement large qu'elle ne se limite pas aux procédés techniques de signature « digitale » existant pour le moment. ».

D'autres différences existent également entre les deux textes : l'article 3, § 5, à l'examen ne s'applique qu'aux signatures appliquées par une personne physique et utilise l'expression « constitue une signature au sens

handtekening in de zin van artikel 1322 van het burgerlijk wetboek », terwijl in artikel 1322, tweede lid, dat in het andere voorontwerp wordt ontworpen, niet wordt bepaald dat de ondertekenaar een natuurlijke persoon of een rechtspersoon moet zijn en de woorden « wordt gelijkgesteld met de eigenhandig geschreven handtekening » worden gebruikt.

De bewijskracht van de digitale handtekening behoort louter in artikel 1322 van het Burgerlijk Wetboek te worden geregeld, zo niet wordt eenzelfde situatie in twee verschillende teksten geregeld.

4. Met een digitale handtekening kan men de steller van een akte identificeren en de integriteit van die akte waarborgen, maar ze biedt toch niet dezelfde waarborgen tegen vervalsing als een handgeschreven handtekening.

Hoewel een derde een handgeschreven handtekening met bedrieglijk opzet kan namaken, kan degene aan wie een aldus ondertekende akte wordt tegengeworpen zijn schrift altijd ontkennen en een gerechtelijk onderzoek naar de echtheid ervan laten instellen (artikel 1324 van het Burgerlijk Wetboek). Via grafologisch onderzoek kan hij gelijk krijgen.

De authenticiteit van een digitale handtekening daarentegen wordt uitsluitend gewaarborgd door de geheime privésleutel van de ondertekenaar. Als een derde die geheime sleutel vindt en de digitale handtekening met bedrieglijk opzet gebruikt, moet de houder bewijzen dat hij niet de gebruiker van zijn eigen sleutel is geweest (1). In veel gevallen zal dat bewijs evenwel onmogelijk kunnen worden geleverd.

De houder van een privésleutel loopt in feite twee risico's : dat zijn sleutel toevallig openbaar raakt en dat zijn sleutel met bedrieglijk opzet wordt ontcijferd. Hij is volledig aansprakelijk voor de gevolgen van die risico's (2).

Die vaststelling leidt tot de volgende overwegingen :

1° zou het niet raadzaam zijn ook bepalingen over de afgifte van sleutelparen voor encryptie op te stellen ? De veiligheid van het systeem hangt immers af van de betrouwbaarheid van de gebruikte cryptogrammen. Is er, aangezien het gebruik van digitale handtekeningen zal toenemen, geen gevaar dat encryptiesleutels op de markt zullen komen die niet alle waarborgen voor veiligheid bieden ?

2° door de technische vooruitgang kan een sleutel die vandaag niet te ontcijferen is, dat snel niet meer zijn. Dat is trouwens één van de redenen waarom de

(1) Zie artikel 11 van het voorontwerp.

(2) Zie in die zin E. Davio, *Questions de certification, signature et cryptographie, in Internet face au droit, Cahiers du Centre de Recherches Informatique et Droit*, n° 12, Brussel, Story Scientia, 1997, blz. 80 en de auteurs die door E. Davio in de voetnoten worden vermeld.

de l'article 1322 du Code civil », tandis que dans l'autre avant-projet, l'article 1322, alinéa 2, en projet, ne prévoit rien quant à la personnalité physique ou morale du signataire et emploie l'expression « est assimilé à une signature manuscrite ».

Il conviendrait de régler dans le seul article 1322 du Code civil la force probante de la signature numérique, faute de quoi deux textes différents régiraient une même situation.

4. La signature digitale, si elle permet d'identifier l'auteur d'un acte et de garantir l'intégrité de cet acte, ne présente toutefois pas les mêmes garanties contre la falsification qu'une signature manuscrite.

Si celle-ci peut être imitée frauduleusement par un tiers, la personne à qui on opposerait un acte ainsi signé peut toujours désavouer son écriture et en demander la vérification en justice (article 1324 du Code civil). Le recours à l'expertise graphologique pourra lui donner raison.

Par contre, la garantie d'authenticité de la signature digitale repose entièrement sur le caractère secret de la clé privée du signataire. Si un tiers venait à percer ce secret et à utiliser frauduleusement la signature digitale, le titulaire devra prouver qu'il n'a pas été l'utilisateur de sa propre clé (1). Cette preuve risque toutefois d'être dans bien des cas impossible à apporter.

Le titulaire d'une clé privée est en fait soumis à un double risque, la divulgation accidentelle de sa clé et le déchiffrement frauduleux de celle-ci. Il doit supporter l'entière responsabilité de ce risque (2).

Cette constatation amène aux considérations suivantes :

1° ne conviendrait-il pas de prévoir également des dispositions relatives à la fourniture de paires de clés de chiffrement ? La sécurité du système repose en effet sur la fiabilité des cryptogrammes utilisés. L'utilisation de la signature digitale étant appelée à se développer, ne court-on pas le risque de voir apparaître sur le marché des clés de chiffrement n'offrant pas toutes les garanties de sécurité ?

2° en raison des progrès de la technique, une clé indéchiffrable aujourd'hui pourrait rapidement ne plus l'être. C'est d'ailleurs pour cette raison, entre autres, que

(1) Voir l'article 11 de l'avant-projet.

(2) Voir en ce sens E. Davio, Questions de certification, signature et cryptographie, in Internet face au droit, Cahiers du Centre de Recherches Informatique et Droit, n° 12, Bruxelles, Story Scientia, 1997, p. 80 et les auteurs cités en note, par cet auteur.

geldigheidsduur van de certificaten beperkt is. Die beperking lost evenwel lang niet alle problemen op.

Zo schrijft E. Davio ([1]) het volgende :

« Une clé réputée indéchiffrable à ce jour pourrait ne plus l'être dans 5 ou 10 ans. Quelle valeur pourra-t-on reconnaître alors aux éléments de preuve constitués aujourd'hui ? … ».

In het voorontwerp wordt alleen bepaald dat de informatie die de certificatie-autoriteit aan de kandidaat-houder bezorgt, betrekking moet hebben op « de noodzaak om digitaal gehandtekende gegevens te onderwerpen aan een nieuwe handtekening wanneer de veiligheid van de bestaande digitale handtekening na verloop van tijd niet meer gewaarborgd is ».

Die bepaling is kennelijk ontoereikend ([2]) om een antwoord te geven op de talrijke praktische vragen die ongetwijfeld zullen rijzen.

5. Artikel 2, 4°, van het voorontwerp bepaalt dat de certificaathouder « een natuurlijke, een privaat- of publiekrechtelijke rechtspersoon, een overheidsbestuur of een feitelijke vereniging » kan zijn.

Een rechtspersoon kan als zodanig geen stuk ondertekenen. Hij drukt zijn wil uit via natuurlijke personen die gerechtigd zijn om hem te vertegenwoordigen. Niets staat evenwel eraan in de weg dat aan een rechtspersoon een certificaat wordt afgegeven. Dat certificaat waarborgt dat de natuurlijke persoon die een privésleutel gebruikt, gerechtigd is om de rechtspersoon te vertegenwoordigen. Hoewel het aldus ondertekende stuk, overeenkomstig het Burgerlijk Wetboek geen onderhandse akte kan zijn — in artikel 3, § 5, wordt die mogelijkheid trouwens uitdrukkelijk uitgesloten — kan het echter wel een belangrijk bewijsstuk zijn, inzonderheid in handelsbetrekkingen. De rechtspersoon kan bovendien perfect geïdentificeerd worden en de verplichtingen nakomen die de wet aan certificaathouders oplegt.

Dat geldt evenwel niet voor een feitelijke vereniging. Hoewel die in sommige gevallen rechten kan hebben, zoals het recht om in rechte op te treden, heeft ze echter geen rechtspersoonlijkheid om overeenkomsten te sluiten die rechten en verplichtingen met zich meebrengen en kan haar « identiteit » onmogelijk voor waar worden verklaard.

Wat de « overheidsbesturen » betreft, is het óf het een, óf het ander : ofwel hebben ze rechtspersoonlijkheid (Staat, gemeenschappen en gewesten, instellingen van openbaar nut, …) en vallen ze dus al onder de categorie van de (publiekrechtelijke) rechtspersonen,

(1) E. Davio, *Preuve et certification sur Internet*, TBH, 1997, blz. 660 en volgende.

(2) Men kan zich zelfs afvragen of een maatregel die erin bestaat stukken van jaren geleden opnieuw te ondertekenen, wel haalbaar en nuttig is.

la durée de validité des certificats est limitée. Mais cette limitation ne résout pas, loin s'en faut, tous les problèmes.

Ainsi, selon E. Davio ([1]),

« Une clé réputée indéchiffrable à ce jour pourrait ne plus l'être dans 5 ou 10 ans. Quelle valeur pourra-t-on reconnaître alors aux éléments de preuve constitués aujourd'hui ? … ».

L'avant-projet se limite à prévoir que l'information fournie par l'autorité de certification au candidat titulaire doit se rapporter « à la nécessité de soumettre des données signées digitalement à une nouvelle signature lorsque, après un certain temps, la sécurité de la signature digitale existante n'est plus garantie ».

Cette disposition est manifestement insuffisante ([2]) pour répondre aux nombreuses questions pratiques qui ne manqueront pas de se poser.

5. L'article 2, 4°, de l'avant-projet prévoit que le titulaire du certificat peut être « une personne physique, morale de droit privé ou de droit public, une administration publique ou une association de fait ».

Une personne morale ne peut, en tant que telle, signer un document. Sa volonté s'exprime au travers des personnes physiques habilitées à la représenter. Rien ne s'oppose toutefois à ce qu'un certificat lui soit délivré. Ce dernier garantira que la personne physique qui utilise une clé privée est habilitée à la représenter. Si le document ainsi signé ne pourra, conformément au Code civil, constituer un acte sous seing privé — l'article 3, § 5, l'exclut d'ailleurs expressément —, il pourra toutefois constituer un élément de preuve important, notamment dans les relations entre commerçants. La personne morale peut en outre parfaitement être identifiée et assumer les obligations que la loi impose aux titulaires d'un certificat.

Il en va tout autrement d'une association de fait. Si celle-ci peut, dans certaines hypothèses, être titulaire de droits, tels que celui d'agir en justice, elle ne dispose toutefois pas de la personnalité juridique lui permettant de contracter des droits et des obligations et son « identité » est impossible à certifier.

En ce qui concerne les « administrations publiques », de deux choses l'une : ou bien elles ont la personnalité juridique (État, communautés et régions, organismes d'intérêt public, …) et sont dès lors déjà visées par la catégorie des personnes morales (de droit public), ou

(1) E. Davio, Preuve et certification sur Internet, RDC, 1997, p. 660 et suivantes.

(2) On peut même douter du caractère réalisable et utile d'une mesure qui consisterait à signer à nouveau des documents remontant à plusieurs années.

ofwel zijn ze geen rechtspersonen die los staan van de overheid waartoe ze behoren en in dat geval kunnen ze niet het subject van de rechten en plichten van een certificaathouder zijn (1).

De woorden « feitelijke vereniging, feitelijke verenigingen » en « overheidsbestuur, openbare besturen » moeten dus vervallen in artikel 2, 2° en 4°, en in de overige bepalingen van het voorontwerp waar ze eveneens voorkomen.

BIJZONDERE OPMERKINGEN

Opschrift

Voorgesteld wordt het opschrift als volgt te stellen :

« Ontwerp van wet betreffende de erkende certificatieautoriteiten met het oog op het gebruik van digitale handtekeningen » (2).

De tekst van het voorontwerp die ter *fine* van onderzoek is overgelegd bevat geen begroeting, vermeldt niet wie de voordragende minister is en bevat geen indieningsbesluit.

Die leemten moeten verholpen worden.

HOOFDSTUK I

Het woord « doelstelling » moet vervallen, aangezien de doelstellingen van een wet in de memorie van toelichting moeten staan en niet in het dispositief, dat alleen regelgevende bepalingen mag bevatten.

Artikel 3, § 1, moet om dezelfde reden vervallen.

Art. 2

1. In punt 1° schrijve men in het Frans *« signature numérique : … »*.

2. In punt 2° is de formulering « privaat- of publiekrechtelijke rechtspersoon » onnodig lang.

(1) Niets staat eraan in de weg, en in het voorontwerp wordt dit trouwens uitdrukkelijk bepaald, dat de Staat bijvoorbeeld over verschillende elektronische handtekeningen beschikt die elk door een certificaat worden gewaarborgd en die elk door verschillende diensten van de Staat worden gebruikt. De Staat blijft hoe dan ook de houder van die certificaten.

(2) In het Frans is alleen de benaming *« signatures numériques »* taalkundig correct; het is de benaming die door de Europese Commissie is gebruikt in haar mededeling van 8 oktober 1997 « Zorgen voor veiligheid van en vertrouwen in elektronische communicatie. Naar een Europees kader voor digitale handtekeningen en encryptie. » (Cf. memorie van toelichting, punt 1).

bien elles ne constituent pas des personnalités juridiques distinctes de l'autorité dont elles font partie, et dans cette hypothèse, elles ne peuvent être le sujet des droits et obligations du titulaire d'un certificat (1).

Les mots « association de fait » et « administrations publiques » seront dès lors omis de l'article 2, 2° et 4° et des autres dispositions de l'avant-projet où on les rencontre également.

OBSERVATIONS PARTICULIÈRES

Intitulé

Il est suggéré de rédiger l'intitulé comme suit :

« Projet de loi relative aux autorités de certification agréées en vue de l'utilisation de signatures numériques » (2).

Le texte de l'avant-projet soumis à l'examen est dépourvu de salutation, d'indication du ministre proposant et d'arrêté de présentation.

Il y a lieu de remédier à ces lacunes.

CHAPITRE Ier

Le mot « objectif » sera omis, les objectifs d'une loi devant être indiqués dans l'exposé des motifs et non dans le dispositif qui ne doit contenir que des dispositions normatives.

Pour la même raison l'article 3, § 1er, sera omis.

Art. 2

1. Au 1°, on écrira « signature numérique : … ».

2. En ce qui concerne le 2°, l'expression « personne morale de droit privé ou de droit public » est inutilement longue.

(1) Rien ne s'oppose, et l'avant-projet le prévoit d'ailleurs expressément, que l'État, par exemple, dispose de plusieurs signatures électroniques garanties par autant de certificats et utilisés chacune par différents services de l'État. Ce dernier restera en tout état de cause le titulaire de ces certificats.

(2) L'expression « signatures numériques » est la seule correcte du point de vue de la langue; elle est celle utilisée par la Commission européenne dans sa communication du 8 octobre 1997 « Vers un Cadre européen pour les Signatures Numériques et le Chiffrement : Assurer la sécurité et la confiance dans la communication électronique » (Cf. exposé des motifs, point 1).

Een rechtspersoon is immers sowieso een privaat- of publiekrechtelijke rechtspersoon.

Aangezien beide soorten rechtspersonen worden bedoeld, kan ermee worden volstaan « rechtspersoon » te schrijven.

Dezelfde opmerking geldt voor artikel 7, derde lid.

3. In punt 5° schrijve men « De minister die bevoegd is voor Economische Zaken ».

4. Wat punt 6° betreft, wordt opgemerkt dat de wetgever niet gerechtigd is uitvoeringstaken rechtstreeks toe te vertrouwen aan een administratieve dienst, zoals hij in punt 6° doet. Dat is immers een prerogatief van de uitvoerende macht.

Bovendien schrijve men in de Franse tekst *« agrément »* in plaats van *« agréation »*.

Deze opmerking geldt voor het hele voorontwerp.

Art. 3

Het zou beter zijn paragraaf 4, eerste lid, als volgt te stellen :

« § 4. Niemand is verplicht een beroep te doen op een erkende certificatieautoriteit. ».

Art. 4

1. In het tweede lid wordt met de woorden « in het bijzonder » een te ruime bevoegdheid verleend aan de Koning; deze woorden moeten vervallen.

2. Is er behoefte aan genummerde onderdelen in een volzin, dan gebruike men daarvoor de tekens 1°, 2°, 3°, enz.

Dezelfde opmerking geldt voor de artikelen 6 en 13, § 2.

3. Een aantal voorwaarden die in artikel 4, tweede lid, worden opgesomd, lijken elkaar te overlappen. Het gaat om de punten d) en i).

4. In de Franse tekst dient wellicht *« interopérabilité »* gelezen te worden in plaats van *« intéropabilité »*.

5. De structuur van artikel 4 zou moeten worden herzien om een onderscheid te maken tussen de voorwaarden die vervuld moeten zijn om te worden erkend, de procedureregels en de verplichtingen die in acht moeten worden genomen om de erkenning te behouden.

Ook dient een onderscheid te worden gemaakt tussen de voorwaarden die betrekking hebben op de certificatieautoriteit en de voorwaarden die betrekking hebben op het personeel daarvan.

En effet, une personne morale est nécessairement de droit public ou de droit privé.

Dès lors que les deux types de personnes morales sont visés, il suffit d'écrire « personne morale ».

La même observation vaut pour l'article 7, alinéa 3.

3. Au 5°, on écrira « Le ministre qui a les Affaires économiques dans ses attributions ».

4. Au 6°, il n'appartient pas au législateur de confier directement des tâches d'exécution à un service administratif. Il s'agit en effet d'une prérogative du pouvoir exécutif.

Par ailleurs, il y a lieu d'utiliser le mot « agrément » au lieu du mot « agréation ».

Cette observation vaut pour l'ensemble de l'avant-projet.

Art. 3

Le paragraphe 4, alinéa 1er, serait mieux rédigé comme suit :

« § 4. Nul n'est tenu de recourir à une autorité de certification agréée. ».

Art. 4

1. À l'alinéa 2, le mot « notamment » confère une habilitation trop large au Roi; il sera omis.

2. Lorsque, à l'intérieur d'une phrase, des subdivisions numérotées s'imposent, le numérotage s'effectue par 1°, 2°, 3°, etc.

La même observation vaut pour les articles 6 et 13, § 2.

3. Certaines des conditions énumérées à l'article 4, alinéa 2 semblent faire double emploi. Il s'agit des points d) et i).

4. Dans le texte français, il faut sans doute lire « interopérabilité » au lieu de « intéropabilité ».

5. La structure de l'article 4 devrait être revue de manière à distinguer les conditions qui doivent être remplies préalablement à l'agrément, les règles de procédure et les obligations dont le respect est une condition du maintien de l'agrément.

Il y a également lieu de distinguer les conditions relatives à l'autorité de certification et celles qui concernent son personnel.

Art. 5

Het zou beter zijn paragraaf 1, eerste en tweede lid, als volgt te stellen :

« Art. 5. — § 1. Alvorens zijn aanvraag om een certificaat in te dienen, maakt de kandidaat met behulp van technische middelen een sleutelpaar bestaande uit een privésleutel en een overeenkomstige publieke sleutel.

Dit sleutelpaar kan worden gemaakt met technische middelen die hem door de certificatieautoriteit ter beschikking worden gesteld, of kan op zijn verzoek rechtstreeks door die autoriteit worden gemaakt.

… ».

Art. 6

Wat het tweede lid, d), betreft, wordt verwezen naar algemene opmerking nr 4.

Art. 7

1. Artikel 8, lid 2, van het genoemde voorstel van richtlijn luidt als volgt :

« De lidstaten dragen ervoor zorg dat een certificatiedienstverlener persoonlijke gegevens slechts rechtstreeks van het datasubject kan verkrijgen en bovendien slechts in de mate die voor de afgifte van het certificaat is vereist.

De gegevens mogen niet zonder toestemming van het datasubject voor andere doeleinden worden verzameld of verwerkt. ».

De tekst van artikel 7 van het voorontwerp moet worden herzien om rekening te houden met de genoemde bepaling van het voorstel van richtlijn. Dat geldt in het bijzonder voor het vierde lid (1).

2. In het derde lid dient bepaald te worden dat de certificatieautoriteit de identiteit van de rechtspersoon (2) nagaat en niet alleen de identiteit en de bevoegdheid van de vertegenwoordigers ervan.

3. Het vijfde lid, dat betrekking heeft op de nadere regels voor het gebruik van de digitale handtekening in contacten met overheidsdiensten, hoort niet thuis in een artikel dat gaat over de verplichtingen van de certificatieautoriteit.

In de Franse tekst schrijve men bovendien : « *modalités d'utilisation* ».

4. In het laatste lid schrijve men :

« De certificatieautoriteit neemt … maatregelen om na te gaan of de publieke sleutel die de kandidaat-houder met het oog op … aanbiedt, daadwerkelijk overeenstemt met de privésleutel … handtekeningen. ».

(1) Zie algemene opmerking nr 1.
(2) Bijvoorbeeld de juiste naam en de rechtsvorm ervan.

Art. 5

Le paragraphe 1er, alinéas 1er et 2, sera mieux rédigé comme suit :

« Art. 5. — § 1er. Préalablement à l'introduction de sa demande de certificat, le candidat crée par des moyens techniques une paire de clés comportant une clé privée et une clé publique correspondante.

Cette paire de clés peut être créée par des moyens techniques mis à sa disposition par l'autorité de certification, ou, à sa demande, directement par cette autorité.

… ».

Art. 6

Concernant l'alinéa 2, d), il est renvoyé à l'observation générale n° 4.

Art. 7

1. Selon l'article 8, paragraphe 2, de la proposition de directive précitée,

« 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 en fait l'objet 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. ».

Le texte de l'article 7 de l'avant-projet doit être revu pour tenir compte de la disposition précitée de la proposition de directive. Ceci vaut en particulier pour l'alinéa 4 (1).

2. À l'alinéa 3, il convient de prévoir que l'autorité de certification vérifie l'identité de la personne morale (2) et non uniquement l'identité et le pouvoir de ses représentants.

3. L'alinéa 5, qui concerne les modalités d'utilisation de la signature numérique dans les échanges avec les administrations, n'a pas sa place dans un article qui traite des obligations de l'autorité de certification.

Il y a lieu, en outre, d'écrire : « modalités d'utilisation ».

4. Au dernier alinéa, il y a lieu d'écrire :

« L'autorité de certification prend … ».

(1) Voir l'observation générale n° 1.
(2) Par exemple sa dénomination exacte et sa forme juridique.

Art. 9

In het tweede lid schrijve men : « Dit register wordt tegen … niet-toegelaten wijziging beschermd ».

Art. 11

Het tweede lid van paragraaf 1 bepaalt dat de privésleutel, behoudens tegenbewijs, geacht wordt te zijn gebruikt door diegene aan wie die sleutel toebehoort.

Artikel 3, § 5, stelt een digitale handtekening gemaakt overeenkomstig het voorliggende voorontwerp echter gelijk met een handgeschreven handtekening.

De formulering « behoudens tegenbewijs » laat in het ongewisseg of men aldus met deze bepaling wil afwijken van artikel 1324 van het Burgerlijk Wetboek, dat bepaalt dat ingeval een partij haar schrift of haar handtekening ontkent, en ingeval haar erfgenamen of rechtverkijgenden verklaren dat zij dat schrift of die handtekening niet kennen, een gerechtelijk onderzoek naar de echtheid ervan wordt bevolen.

Deze kwestie moet in het Burgerlijk Wetboek zelf worden geregeld.

2. In paragraaf 2, moeten de woorden « van deze wet », die overbodig zijn, vervallen.

3. Het zou beter zijn in paragraaf 3 het volgende te schrijven :

« Wanneer een certificaat vervalt, geschorst wordt of wordt herroepen, kan de houder ervan de overeenkomstige privésleutel niet meer gebruiken om te ondertekenen … ».

Art. 12

1. In paragraaf 1, eerste lid, dienen de woorden « vooraf geïdentificeerde » te vervallen. De gemachtigde ambtenaar is het daarmee eens.

Bovendien schrijve men « houder van het certificaat » in plaats van « certificaathouder ».

Laatstgenoemde opmerking geldt ook voor het opschrift van afdeling 3 en voor artikel 13, § 1.

2. In paragraaf 2, eerste lid, zijn de woorden « en gemotiveerde » overbodig; ze moeten vervallen.

In het tweede lid van dezelfde paragraaf schrijve men : « De schorsing wordt onmiddellijk opgeheven … ».

Art. 15

De gemachtigde ambtenaar is het ermee eens dat ook uitdrukkelijk moet worden voorzien in het geval dat de certificatieautoriteit failliet gaat.

Art. 9

À l'alinéa 2, il y a lieu d'écrire : « ce registre est protégé … ».

Art. 11

L'alinéa 2 du paragraphe 1er prévoit que l'utilisation de la clé privée est réputée, sauf preuve contraire, être le fait de son titulaire.

Or l'article 3, § 5, assimile une signature numérique établie conformément au présent avant-projet à une signature manuscrite.

La formulation « sauf preuve contraire » laisse dans l'incertitude la question de savoir si cette disposition entend ainsi déroger à l'article 1324 du Code civil qui dispose que dans les cas où la partie désavoue son écriture ou sa signature, et dans les cas où ses héritiers ou ayants cause déclarent ne les point connaître, la vérification en est ordonnée en justice.

Cette question devrait être réglée dans le Code civil lui-même.

2. Au paragraphe 2, *in fine*, les mots « de la présente loi » sont inutiles et seront omis.

3. Au paragraphe 3, il serait préférable d'écrire :

« Lorsqu'un certificat est arrivé à échéance, est suspendu ou révoqué, son titulaire ne peut plus utiliser la clé privée correspondante pour signer … ».

Art. 12

1. De l'accord du fonctionnaire délégué, il y a lieu au paragraphe 1er, alinéa 1er, de supprimer les mots « préalablement identifié ».

En outre, il y a lieu d'écrire « titulaire du certificat » et non « titulaire de certificat ».

Cette dernière observation vaut également pour l'intitulé de la section 3 et pour l'article 13, § 1er.

2. Au paragraphe 2, alinéa 1er, les mots « et motivées » sont inutiles et seront omis.

À l'alinéa 2 du même paragraphe, on écrira : « La suspension est immédiatement levée … ».

Art. 15

Ainsi qu'en a convenu le fonctionnaire délégué, il convient également de viser expressément l'hypothèse de la faillite de l'autorité de certification.

Art. 19

1. Zoals artikel 19, § 1, gesteld is, is het slechts een parafrase van artikel 1382 van het Burgerlijk Wetboek; het is dus overbodig.

Dezelfde opmerking geldt voor artikel 20.

2. De paragrafen 2 en 3 wijken af van het voorstel voor een communautaire richtlijn. Wat dat betreft wordt verwezen naar algemene opmerking nr 1.

SLOTOPMERKINGEN

De afdeling wetgeving van de Raad van State wijst erop dat er een aantal discrepanties zijn tussen de tekst van het voorontwerp van wet en de memorie van toelichting. Die behoren te worden weggewerkt.

Enkele voorbeelden :

1. In tegenstelling tot wat gezegd wordt in de memorie van toelichting (blz. 6), komen in artikel 3, § 2, nergens de woorden « behoudens in de door de wet voorziene gevallen » voor.

Zo ook wordt in de memorie van toelichting verwezen naar een artikel 3, § 4, derde lid, dat niet bestaat, aangezien artikel 3, § 4, maar twee leden omvat.

2. Luidens artikel 3, § 3, houdt de erkenning in alle gevallen ten minste de afgifte van certificaten in met betrekking tot de identiteit van de houder van het certificaat.

Volgens de gemachtigde ambtenaar houdt die minimale erkenning de afgifte in van certificaten met betrekking tot de identiteit van natuurlijke personen en rechtspersonen, in tegenstelling tot wat blijkt uit punt 3.3 van de memorie van toelichting.

3. Artikel 13, § 2, b), verwijst naar artikel 15, waarvan paragraaf 2 bepaalt dat de « administratie » zich ervan vergewist dat de certificaten herroepen zijn wanneer de certificatieautoriteit haar activiteiten stopzet om redenen buiten haar wil.

In de memorie van toelichting staat dat in dat geval « aan de Administratie de taak (wordt) toevertrouwd om over te gaan tot de herroeping van de certificaten. Daartoe moet de CA samenwerken met de Administratie en haar de nodige informatie verschaffen ».

Volgens de gemachtigde ambtenaar herroept « de administratie » alleen zelf de certificaten wanneer de certificatieautoriteit dat niet uit eigen beweging doet.

Die discrepanties moeten worden weggewerkt.

4. De Nederlandse tekst van het ontwerp is uit een oogpunt van correct taalgebruik onzorgvuldig gesteld. Zo bevat hij niet alleen niet-correcte termen (bijvoorbeeld « afleveren » wanneer bedoeld wordt de afgifte van bescheiden, « toelaten » in de betekenis van « in staat stellen »), maar is de terminologie in die tekst ook niet-consequent (bijvoorbeeld het correcte « houder » naast het

Art. 19

1. Tel que rédigé, l'article 19, § 1er, ne fait que paraphraser l'article 1382 du Code civil; il est donc inutile.

La même observation vaut pour l'article 20.

2. Quant aux paragraphes 2 et 3, ils s'écartent de la proposition de directive communautaire. Il est renvoyé, à cet égard, à l'observation générale n° 1.

OBSERVATION FINALE

La section de législation du Conseil d'État observe qu'il y a un certain nombre de discordances entre le texte de l'avant-projet de loi et l'exposé des motifs. Il y a lieu de les lever.

On citera à titre d'exemples :

1. Contrairement à ce qu'indique l'exposé des motifs (p. 6), l'article 3, § 2, ne comprend pas les mots « sauf les cas prévus par la loi ».

De même l'exposé des motifs fait référence à un article 3, § 4, alinéa 3, qui n'existe pas, l'article 3, § 4 ne comportant que deux alinéas.

2. Selon l'article 3, § 3, l'agrément couvre, dans tous les cas, au moins la délivrance de certificats relatifs à l'identité du titulaire du certificat.

Selon le fonctionnaire délégué, cet agrément minimal couvre la délivrance de certificats relatifs à l'identité des personnes physiques et des personnes morales, contrairement à ce que semble indiquer le point 3.3 de l'exposé des motifs.

3. L'article 13, § 2, b), renvoie à l'article 15 dont le paragraphe 2 dispose que l'administration s'assure de la révocation des certificats lorsque l'autorité de certification arrête ses activités pour des raisons indépendantes de sa volonté.

L'exposé des motifs précise que dans cette hypothèse, « on confie à l'Administration la tâche de procéder à la révocation des certificats. À cet effet, l'AC est tenue de collaborer et de transmettre toute information utile à l'Administration ».

Selon le fonctionnaire délégué l'administration ne révoque elle même les certificats que si l'autorité de certification ne le fait pas spontanément.

Ces discordances doivent être supprimées.

4. Le texte néerlandais du projet devrait être rédigé en tenant compte des observations faites dans la version néerlandaise, *in fine*, du présent avis.

niet-correcte « titularis », « Rijksregister » doch ook « nationaal register », « overheidsbestuur » maar ook « openbare besturen »). Ook wordt nodeloos van de ontworpen EG-terminologie afgeweken (bijvoorbeeld « private sleutel » in de ontworpen wet tegenover « privésleutel » in het voorstel voor een richtlijn). Ten overvloede worden hierna enige tekstvoorstellen gedaan.

Art. 2

In 1° zou « houder » geschreven moeten worden in plaats van « titularis » en « privésleutel » in plaats van « private sleutel ». Deze opmerkingen gelden voor heel het ontwerp. In 3° zou « afgeeft » of « uitreikt » geschreven moeten worden in plaats van « aflevert ». Deze opmerking geldt *mutatis mutandis* voor heel het ontwerp.

Art. 3

Het tweede lid van paragraaf 2 is slaafs uit het Frans vertaald en derhalve zulk een stuntelig Nederlands dat de tekst vast onbegrijpelijk is. Een soortgelijke opmerking geldt voor artikel 6, tweede lid, d); artikel 7, vierde lid; artikel 11, paragraaf 2.

Art. 4

In het tweede lid, m), schrijve men « wijze van controle » in plaats van « controlemodaliteiten ». Voorts wordt erop gewezen dat hier opeens sprake is van « het bestuur bedoeld in artikel 2, 6° », ofschoon in artikel 2, 6°, een definitie gegeven wordt van « administratie », waar beter « overheidsdienst » of « overheidsbestuur » had gestaan.

HOOFDSTUK 3 (dat hoofdstuk III wordt)

Het opschrift bevat verschrijvingen die het onleesbaar maken.

Art. 11

In paragraaf 2 zou het correcter zijn « laten schorsen » en « laten herroepen » te schrijven in plaats van « doen schorsen » en « doen herroepen ». Een soortgelijke opmerking geldt voor paragraaf 3.

Art. 12

In paragraaf 1 zou het woord « terug », dat niet alleen overtollig is maar *in casu* ook verkeerd gebruikt is in de betekenis van « weer », moeten vervallen.

Art. 14

In paragraaf 2, tweede lid, schrijve men « tegenwerpbaar » in plaats van « tegenstelbaar » en in paragraaf 3, tweede lid, « die een belang aantoont » in plaats van « een belang aantoont ».

Het gehele ontwerp zou verder van alle taalongerechtigheden moeten worden gezuiverd.

De kamer was samengesteld uit

HH. :

R. ANDERSEN, *kamervoorzitter;*

C. WETTINCK,
P. LIENARDY, *staatsraden;*

F. DELPEREE,
J. KIRKPATRICK, *assessoren van de afdeling wetgeving;*

Mevr. :

M. PROOST, *griffier.*

Het verslag werd uitgebracht door de heer L. DETROUX, adjunct-auditeur. De nota van het Coördinatiebureau werd opgesteld door de heer A. LEFEBVRE en toegelicht door de heer C. NIKIS, adjunct-referendarissen.

De overeenstemming tussen de Nederlandse en de Franse tekst werd nagezien onder toezicht van de heer R. ANDERSEN.

De griffier, *De voorzitter,*

M. PROOST R. ANDERSEN

La chambre était composée de

MM. :

R. ANDERSEN, *président de chambre;*

C. WETTINCK,
P. LIENARDY, *conseillers d'État;*

F. DELPEREE,
J. KIRKPATRICK, *assesseurs de la section de législation;*

Mme :

M. PROOST, *greffier.*

Le rapport a été présenté par M. L. DETROUX, auditeur adjoint. La note du Bureau de coordination a été rédigée par M. A. LEFEBVRE et exposée par M. C. NIKIS, référendaires adjoints.

La concordance entre la version française et la version néerlandaise a été vérifiée sous le contrôle de M. R. ANDERSEN.

Le greffier, *Le président,*

M. PROOST R. ANDERSEN

WETSONTWERP

ALBERT II, KONING DER BELGEN

Aan allen die nu zijn en hierna wezen zullen,
ONZE GROET.

Op de voordracht van Onze ministers van Justitie, van Telecommunicatie en van Economie,

HEBBEN WIJ BESLOTEN EN BESLUITEN WIJ :

Onze ministers van Justitie, van Telecommunicatie et van Economie zijn ermee belast in Onze naam het ontwerp van wet waarvan de tekst hierna volgt aan de Wetgevende Kamers voor te leggen en bij de Kamer van volksvertegenwoordigers in te dienen :

Artikel 1

Deze wet regelt een materie bedoeld in artikel 78 van de Grondwet.

HOOFDSTUK 1

Definities en toepassingsgebied van de wet

Afdeling 1

Definities

Art. 2

Voor de toepassing van deze wet en de uitvoeringsbesluiten ervan wordt verstaan onder :

1° « geavanceerde elektronische handtekening » : elektronische gegevens vastgehecht aan of logisch geassocieerd met andere elektronische gegevens, die worden gebruikt als middel voor authentificatie en aan de volgende eisen voldoen :

a) zij is op unieke wijze aan de ondertekenaar verbonden;

b) zij maakt het mogelijk de ondertekenaar te identificeren;

c) zij wordt aangemaakt met middelen die de ondertekenaar onder zijn uitsluitende controle kan houden;

d) zij is op zodanige wijze aan de gegevens waarop zij betrekking heeft verbonden, dat elke latere wijziging van de gegevens kan worden opgespoord;

PROJET DE LOI

ALBERT II, ROI DES BELGES

À tous, présents et à venir,
SALUT.

Sur la proposition de Nos ministres de la Justice, des Télécommunications et de l'Économie,

NOUS AVONS ARRÊTÉ ET ARRÊTONS :

Nos ministres de la Justice, des Télécommunications et de l'Économie sont chargés de présenter en Notre nom aux Chambres législatives et de déposer à la Chambre des représentants le projet de loi dont la teneur suit :

Article 1er

La présente loi règle une matière visée à l'article 78 de la Constitution.

CHAPITRE 1er

Définitions et champ d'application de la loi

Section 1re

Définitions

Art. 2

Pour l'application de la présente loi et ses arrêtés d'exécution, on entend par :

1° « signature électronique avancée » : une donnée électronique, jointe ou liée logiquement à d'autres données électroniques, servant de méthode d'authentification et satisfaisant aux exigences suivantes :

a) être liée uniquement au signataire;

b) permettre l'identification du signataire;

c) être créée par des moyens que le signataire puisse garder sous son contrôle exclusif;

d) être liée aux données auxquelles elle se rapporte de telle sorte que toute modification ultérieure des données soit détectée;

2° « certificaat » : een elektronisch attest, verzekerd door de geavanceerde elektronische handtekening van een certificatiedienstverlener, dat inzonderheid het verband bevestigt tussen een natuurlijke persoon of een rechtspersoon en de gegevens over het verifiëren van de handtekening van deze persoon;

3° « gekwalificeerd certificaat » : een certificaat dat voldoet aan de eisen bedoeld in artikel 12 van deze wet en dat wordt afgegeven door een geaccrediteerde certificatiedienstverlener;

4° « certificaathouder » : een natuurlijke persoon of rechtspersoon aan wie een certificatiedienstverlener een certificaat heeft afgegeven;

5° « gegevens voor het aanmaken van een handtekening » : unieke gegevens, zoals codes of cryptografische privé-sleutels, die door de ondertekenaar worden gebruikt om een geavanceerde elektronische handtekening aan te maken;

6° « veilig middel voor het aanmaken van een handtekening » : geconfigureerde *software* of *hardware* die wordt gebruikt om de gegevens voor het aanmaken van een handtekening te implementeren en die voldoet aan de eisen van artikel 11 van deze wet;

7° « gegevens voor het verifiëren van een handtekening » : gegevens, zoals codes of cryptografische openbare sleutels, die worden gebruikt voor het verifiëren van een geavanceerde elektronische handtekening;

8° « middel voor het verifiëren van een handtekening » : geconfigureerde *software* of *hardware* die wordt gebruikt om de gegevens voor het verifiëren van een handtekening te implementeren;

9° « certificatiedienstverlener » : elke natuurlijke persoon of rechtspersoon die certificaten afgeeft en beheert of andere diensten in verband met elektronische handtekeningen verleent;

10° « product voor elektronische handtekeningen » : elke *software* of *hardware*, of relevante componenten daarvan, die door certificatiedienstverleners kunnen worden gebruikt om diensten op het gebied van elektronische handtekeningen te verlenen of om elektronische handtekeningen aan te maken of te verifiëren;

11° « bestuur » : het bestuur Kwaliteit en Veiligheid van het ministerie van Economische Zaken dat belast is met de taken betreffende de afgifte, de schorsing en de intrekking van de accreditatie van de certificatiedienstverleners evenals met de controle hiervan;

12° « entiteit » : instelling die haar bevoegdheid aantoont op grond van een certificaat afgegeven door het Belgische accreditatiesysteem conform de wet van 20 juli 1990 betreffende de accreditatie van certificatie- en keuringsinstellingen alsmede van beproevingslaboratoria.

2° « certificat » : une attestation électronique sécurisée par la signature électronique avancée d'un prestataire de service de certification qui confirme notamment le lien entre une personne physique ou morale et les données afférentes à la vérification de la signature de celle-ci;

3° « certificat qualifié » : un certificat qui satisfait aux exigences visées à l'article 12 de la présente loi et qui est fourni par un prestataire de service de certification accrédité;

4° « titulaire de certificat » : une personne physique ou morale à laquelle un prestataire de service de certification a délivré un certificat;

5° « données afférentes à la création de signature » : des données uniques, telles que des codes ou des clés cryptographiques privées, que le signataire utilise pour créer une signature électronique avancée;

6° « dispositif sécurisé de création de signature » : un dispositif logiciel ou matériel configuré pour mettre en application les données afférentes à la création de signature qui satisfait aux exigences de l'article 11 de la présente loi;

7° « données afférentes à la vérification de signature » : des données, telles que des codes ou des clés cryptographiques publiques, qui sont utilisées pour vérifier une signature électronique avancée;

8° « dispositif de vérification de signature » : un dispositif logiciel ou matériel configuré pour mettre en application les données afférentes à la vérification de signature

9° « prestataire de service de certification » : toute personne physique ou morale qui délivre et gère des certificats ou fournit d'autres services liés aux signatures électroniques;

10° « produit de signature électronique » : tout produit matériel ou logiciel, ou élément spécifique de ce produit, destiné à être utilisé par un prestataire de service de certification pour la fourniture de services de signature électronique ou pour la création ou la vérification de signatures électroniques;

11° « administration » : l'administration de la qualité et sécurité du ministère des Affaires économiques qui est chargée des tâches relatives à la délivrance, la suspension et au retrait de l'accréditation des prestataires de service de certification ainsi qu'à la surveillance de ceux-ci;

12° « entité » : organisme qui démontre sa compétence sur la base d'un certificat délivré par le système belge d'accréditation conformément à la loi du 20 juillet 1990 concernant l'accréditation des organismes de certification et de contrôle, ainsi que les laboratoires d'essais.

Afdeling 2

Toepassingsgebied

Art. 3

§ 1. Deze wet bepaalt de algemene voorwaarden voor de accreditatie van certificatiedienstverleners, het juridische stelsel van toepassing op de activiteiten van de certificatiedienstverleners evenals de door deze laatste en de certificaatgebruikers na te leven regels.

§ 2. Deze wet is van toepassing op de certificatiedienstverleners die hun activiteiten uitoefenen in een open netwerk.

HOOFDSTUK 2

Algemene principes

Art. 4

§ 1. Een certificatiedienstverlener kan niet worden verplicht een accreditatie aan te vragen voor de uitoefening van zijn activiteiten.

De verkrijging en het behoud van een accreditatie zijn onderworpen aan de naleving van de voorwaarden vastgelegd door of krachtens deze wet.

§ 2. Behoudens uitzondering voorzien door een wet, een decreet of een ordonnantie kan niemand worden verplicht een elektronische handtekening te gebruiken.

§ 3. De keuze een beroep te doen op een geaccrediteerde certificatiedienstverlener is vrij.

Het is evenwel mogelijk door of krachtens een wet, een decreet of een ordonnantie de gevallen te bepalen waarin een elektronische handtekening gesteund moet worden door een gekwalificeerd certificaat.

§ 4. Onverminderd de artikelen 1323 en volgende van het Burgerlijk Wetboek is een geavanceerde elektronische handtekening, gerealiseerd op grond van een gekwalificeerd certificaat en aangemaakt door een veilig middel voor het aanmaken van een handtekening, gelijkgesteld met een handtekening in de zin van artikel 1322 van het Burgerlijk Wetboek, of deze nu wordt gerealiseerd door een natuurlijke dan wel door een rechtspersoon.

Section 2

Champ d'application

Art. 3

§ 1er. La présente loi fixe les conditions générales d'accréditation des prestataires de service de certification, le régime juridique applicable aux opérations effectuées par les prestataires de service de certification ainsi que les règles à respecter par ces derniers et les utilisateurs de certificats.

§ 2. La présente loi s'applique aux prestataires de service de certification exerçant leurs activités en réseaux ouverts.

CHAPITRE 2

Principes généraux

Art. 4

§ 1er. Nul prestataire de service de certification ne peut être contraint de demander une accréditation pour exercer ses activités.

L'obtention et le maintien de l'accréditation sont subordonnés au respect des conditions fixées par ou en vertu de la présente loi.

§ 2. Sauf exception prévue par une loi, un décret ou une ordonnance, nul ne peut être contraint de signer électroniquement.

§ 3. Le choix de recourir à un prestataire de services de certification accrédité est libre.

Il est néanmoins possible de fixer par ou en vertu d'une loi, d'un décret ou d'une ordonnance les cas dans lesquels une signature électronique doit être appuyée par un certificat qualifié.

§ 4. Sans préjudice des articles 1323 et suivants du Code civil, une signature électronique avancée réalisée sur la base d'un certificat qualifié et créée par un dispositif sécurisé de création de signature est assimilée à une signature au sens de l'article 1322 du Code civil, que celle-ci soit réalisée par une personne physique ou morale.

HOOFDSTUK 3

Certificatiedienstverleners

Afdeling 1

Geaccrediteerde certificatiedienstverleners

Onderafdeling 1

Accreditatie

Art. 5

§ 1. Een certificatiedienstverlener verkrijgt en behoudt een accreditatie onder de volgende voorwaarden :

1° hij leeft de door of krachtens deze wet vastgelegde eisen na;

2° hij levert het bewijs dat hij voldoende betrouwbaar is om certificatiediensten te verlenen;

3° hij levert voldoende waarborgen voor integriteit en beschikbaarheid evenals de deskundigheid om zijn certificatie-activiteiten te kunnen uitoefenen;

4° hij stelt een nauwkeurig veiligheidsplan op dat voldoet aan de eisen van artikel 17. Dit plan wordt onderzocht en geverifieerd door het bestuur of door een entiteit die hij zelf aanstelt;

5° hij stelt personeel tewerk dat beschikt over de specifieke kennis, ervaring en kwalificaties nodig voor het verlenen van diensten en, in het bijzonder, over de competentie op het vlak van het beheer, de gespecialiseerde kennis en de technologie van elektronische handtekeningen en een goede praktische kennis van de toegepaste beveiligingsmethodes; hij moet eveneens administratieve en beheersprocedures en -methodes gebruiken die aangepast aan en conform de erkende normen zijn;

6° hij beschikt over een onafhankelijk beheer ten opzichte van de gebruikers van de dienst;

7° het laat toe om de bestemming van een boodschap voorzien van een geavanceerd elektronisch jaarboek, zonder het certificaat te kunnen registreren, of de ondertekenaar op dat ogenblik certificaathouder was;

8° hij beschikt over voldoende financiële middelen om te functioneren volgens de eisen van deze wet, in het bijzonder, om de verantwoordelijkheid te nemen voor schade, door, bijvoorbeeld, een aangepaste verzekering te sluiten;

9° hij publiceert zijn voorwaarden inzake tarieven;

10° hij leeft de minimale normen na met betrekking tot de vertrouwelijkheid en de integriteit van de door de

CHAPITRE 3

Des prestataires de service de certification

Section 1re

Des prestataires de service de certification accrédités

Sous-section 1re

De l'accréditation

Art. 5

§ 1er. Un prestataire de service de certification obtient et conserve une accréditation aux conditions suivantes :

1° il respecte les exigences fixées par ou en vertu de cette loi;

2° il fait la preuve qu'il est suffisamment fiable pour fournir des services de certification;

3° il présente des garanties d'intégrité et de disponibilité suffisantes ainsi que l'expertise pour exercer ses activités de certification;

4° il présente un plan de sécurité précis qui répond aux exigences de l'article 17. Ce plan est examiné et vérifié par l'administration ou par une entité désignée par elle;

5° il emploie du personnel ayant les connaissances spécifiques, l'expérience et les qualifications nécessaires à la fourniture des services et, en particulier, des compétences au niveau de la gestion, des connaissances spécialisées en technologie des signatures électroniques et une bonne pratique des procédures de sécurité appropriées; ils doivent également appliquer des procédures et méthodes administratives et de gestion qui soient adaptées et conformes à des normes reconnues;

6° il dispose d'une gestion indépendante par rapport aux utilisateurs du service;

7° il autorise le destinataire de message doté d'une signature électronique avancée de vérifier dans son annuaire électronique, sans pouvoir enregistrer le certificat, si le signataire était à ce moment titulaire d'un certificat;

8° il dispose des ressources financières suffisantes pour fonctionner conformément aux exigences prévues par la présente loi, en particulier pour endosser la responsabilité de dommages, en contractant, par exemple, une assurance appropriée;

9° il publie ses conditions tarifaires;

10° il respecte les normes minimales relatives à la confidentialité et à l'intégrité des informations procurées par

certificaathouder verstrekte informatie en de voorwaarden met betrekking tot de dienst voor het behandelen van klachten van klanten;

11° hij leeft de regels na betreffende de informatie die de certificatiedienstverlener over zijn diensten en over de door hem afgegeven certificaten moet bijhouden.

§ 2. De Koning preciseert de voorwaarden bedoeld in §1 en bepaalt :

1° de procedure voor de toekenning, schorsing en intrekking van de accreditatie;

2° de verschuldigde bijdragen voor het afleveren, het beheren en het controleren van de accreditatie;

3° de onderzoekstermijnen voor de aanvraag;

4° de regels voor de controle van de certificatiedienstverleners;

5° de prijzen et de voorwaarden van de afgifte van een certificaat aan een natuurlijke persoon.

Art. 6

Het bestuur :

1. Kent toe en trekt accreditaties in.

2. Coördineert de coherente en transparante toepassing van de accreditatieprincipes en -procedures bij toepassing van deze wet.

3. Heeft het toezicht op de auditprocedures bedoeld in artikel 2 , 12°) van deze wet, evenals op de activiteiten van deze entiteiten in het kader van de accreditatieprocedures.

4. Verzamelt, verspreidt en publiceert informatie over de activiteiten op het vlak van de geavanceerde elektronische handtekening verzekert en garandeert dat alle geïnteresseerde partijen deelnemen aan deze activiteiten.

5. Brengt adviezen uit in de Europese en internationale debatten met het oog op de daadwerkelijke toepassing van de internationale normen en akkoorden van toepassing op de certifcatiedienstverleners.

6. Brengt adviezen uit over alle aspecten van de elektronische handtekening.

Onderafdeling 2

Opdrachten

Art. 7

§ 1. Vooraleer een certificaat af te geven, onderzoekt de certificatiedienstverlener de complementariteit van de gegevens voor het aanmaken en het verifiëren van de handtekening.

le titulaire de certificat et les conditions concernant le service du traitement de plaintes émanant de clients;

11° il respecte les règles relatives à l'information que le prestataire de service de certification est tenu de conserver concernant ses services et les certificats délivrés par lui.

§ 2. Le Roi précise les conditions visées au § 1er et fixe :

1° la procédure de délivrance, de suspension et de retrait de l'accréditation;

2° les redevances dues pour la délivrance, la gestion et le contrôle de l'accréditation;

3° les délais d'examen de la demande;

4° les modalités de contrôle des prestataires de service de certification;

5° les prix et les conditions pour la délivrance d'un certificat à une personne physique.

Art. 6

L'administration :

1. Octroie et de retire les accréditations.

2. Coordonne l'application cohérente et transparente des principes et procédures d'accréditation en application de la présente loi.

3. Supervise les procédures d'audit des entités visées à l'article 2 , 12°) de la présente loi ainsi que les activités de ces entités dans le cadre des procédures d'accréditation.

4. Assure la collecte, la circulation et la publication d'informations relatives aux activités dans le domaine de la signature électronique avancée, et d'assurer que toutes les parties intéressées soient associées à ces activités.

5. Remet des avis dans les débats européens et internationaux menant à la mise en œuvre effective de normes et d'accords internationaux applicables aux prestataires de service de certification.

6. Remet des avis sur tous les aspects de la signature électronique.

Sous-section 2

Des missions

Art. 7

§ 1er. Préalablement à la délivrance d'un certificat, le prestataire de service de certification vérifie la complémentarité des données afférentes à la création et à la vérification de signature.

§ 2. De certificatiedienstverlener mag de gegevens voor het aanmaken van de handtekening niet registreren, behouden of opnieuw samenstellen.

Ingeval de certificatiedienstverlener gegevens voor het aanmaken van de handtekening genereert, waarborgt hij de vertrouwelijkheid bij de verwerking van de gegevens.

§ 3. Na de identiteit en, in voorkomend geval, de specifieke hoedanigheden te hebben geverifiëerd, geeft de certificatiedienstverlener één of meer gekwalificeerde certificaten af aan elke persoon die daarom verzoekt.

De identificatie van een natuurlijke persoon impliceert tenminste de ontmoeting tussen deze persoon en de certificatiedienstverlener of de afgevaardigde van deze laatste.

Elke natuurlijke persoon is in recht om van de certificatiedienstverlener een certificaat te verkrijgen, die hem toelaat om uitwisselingen met de overheid en ook handelstransacties te verrichten.

De Koning stelt de uitvoeringsmodaliteiten van de voorafgaande alinea vast.

Indien het certificaat aan een rechtspersoon wordt afgegeven, verifieert de certificatiedienstverlener eerst de identiteit en de vertegenwoordigingsbevoegdheid van de natuurlijke persoon of de personen die zich hiervoor aanbiedt of aanbieden.

De certificatiedienstverlener weigert één of meer gekwalificeerde certificaten af te geven indien hij niet over de nodige middelen beschikt om de in artikel 12 bedoelde informatie te verifiëren.

§ 4. De certificatiedienstverlener treft maatregelen tegen het namaken van de certificaten.

Art. 8

Vóór elke contractuele relatie met een persoon die een gekwalificeerd certificaat vraagt of voor elk verzoek van een derde die zich beroept op zulk certificaat, verstrekt de certificatiedienstverlener, door middel van een duurzame mededeling in een gemakkelijk verstaanbare taal, de nodige informatie voor een correct en veilig gebruik van zijn diensten.

Deze informatie heeft minstens betrekking op :

1° de te volgen procedure om een elektronische handtekening aan te maken en te verifiëren;

2° de nauwkeurige regels en voorwaarden voor het gebruik van de certificaten, met inbegrip van de voor het gebruik ervan opgelegde grenzen;

3° de verplichtingen voor de gebruikers van het certificaat;

4° het bestaan van een vrijwillig accreditatiesysteem en van de juridische gevolgen verbonden aan de elektronische handtekeningen gesteund door een gekwalificeerd certificaat;

§ 2. Le prestataire de service de certification ne peut ni enregistrer, ni conserver, ni reconstituer les données afférentes à la création de signature.

Dans le cas où il génère des données afférentes à la création de signature, le prestataire de service de certification garantit la confidentialité au cours du processus de génération des données.

§ 3. Après avoir vérifié son identité et, le cas échéant, ses qualités spécifiques, le prestataire de service de certification délivre un ou plusieurs certificats qualifiés à toute personne qui en fait la demande.

L'identification d'une personne physique implique au moins la rencontre de celle-ci et du prestataire de service de certification ou le mandataire de ce dernier.

Toute personne physique est en droit d'obtenir du prestataire de service de certification un certificat qui lui permette d'effectuer des échanges avec les autorités publiques et d'effectuer des transactions commerciales.

Le Roi fixe les modalités d'exécution de l'alinéa qui précède.

Si le certificat est délivré à une personne morale, le prestataire de service de certification vérifie préalablement l'identité et le pouvoir de représentation de la ou des personnes physiques qui se présentent à lui.

Le prestataire de service de certification refuse la délivrance d'un ou plusieurs certificats qualifiés lorsqu'il ne dispose pas des moyens nécessaires pour vérifier les informations visées à l'article 12.

§ 4. Le prestataire de service de certification prend des mesures contre la contrefaçon des certificats.

Art. 8

Préalablement à toute relation contractuelle avec une personne demandant un certificat qualifié ou à la demande d'un tiers qui se prévaut d'un tel certificat, le prestataire de service de certification procure, par un moyen de communication durable et dans une langue aisément compréhensible, les informations nécessaires à l'utilisation correcte et sûre de ses services.

Ces informations se rapportent au moins :

1° à la procédure à suivre afin de créer et de vérifier une signature électronique;

2° aux modalités et conditions précises d'utilisation des certificats, y compris les limites imposées à leur utilisation;

3° aux obligations qui sont à la charge des utilisateurs de certificat;

4° à l'existence d'un régime volontaire d'accréditation et des conséquences juridiques attachées aux signatures électroniques appuyées par un certificat qualifié;

5° de regels betreffende de bescherming van de persoonsgegevens bedoeld in artikel 18;

6° de regels betreffende de certificaten afgegeven door de buitenlandse certificatiedienstverleners bedoeld in artikel 19;

7° de procedures voor het indienen van klacht en voor het regelen van geschillen.

Art. 9

De certificatiedienstverlener verschaft een exemplaar van het certificaat aan de kandidaat-houder.

Zodra de kandidaat-houder het certificaat heeft aanvaard, schrijft de certificatiedienstverlener dit in in het elektronisch register bedoeld in artikel 10.

Art. 10

De certificatiedienstverlener houdt een elektronisch register bij met de certificaten die hij afgeeft en het tijdstip waarop zij aflopen. Deze registerdienst moet snel en veilig werken en voor iedereen langs elektronische weg permanent toegankelijk zijn. De certificatiedienstverlener waakt erover dat de datum en het uur van de afgifte en, in voorkomend geval, van de herroeping van een gekwalificeerd certificaat nauwkeurig kunnen worden bepaald.

Dit register bestaat uit betrouwbare systemen om de informatie in verifieerbare vorm op te slaan, zodat :

1. enkel gemachtigde personen gegevens kunnen invoeren en wijzigen;

2. de authenticiteit van de informatie kan worden geverifieerd;

3. de certificaten voor het publiek slechts beschikbaar zijn voor onderzoek in de gevallen waarin de houder van het certificaat hiermee heeft ingestemd; en

4. elke technische wijziging die deze veiligheidsvereisten in gevaar brengt, voor de operateur duidelijk zichtbaar wordt.

Onderafdeling 3

Vereisten betreffende de veilige middelen voor het aanmaken van een elektronische handtekening

Art. 11

De certificatiedienstverlener gebruikt of verschaft aan de gebruikers slechts veilige middelen voor het aanma-

5° aux règles relatives à la protection des données à caractère personnel visée à l'article 18;

6° aux règles relatives aux certificats délivrés par des prestataires de service de certification étrangers visées à l'article 19;

7° aux procédures de réclamation et de règlement des litiges.

Art. 9

Le prestataire de service de certification fournit un exemplaire du certificat au candidat titulaire.

Dès son acceptation par le candidat titulaire, le prestataire de service de certification inscrit le certificat dans l'annuaire électronique visé à l'article 10.

Art. 10

Le prestataire de service de certification conserve un annuaire électronique comprenant les certificats qu'il délivre et le moment de leur expiration. Le fonctionnement de ce service d'annuaire doit être rapide, sûr et accessible en permanence à toute personne par voie électronique. Le prestataire de service de certification veille à ce que la date et l'heure d'émission et, le cas échéant, de révocation d'un certificat qualifié puissent être déterminées avec précision.

Cet annuaire est constitué par des systèmes fiables pour stocker l'information sous une forme vérifiable de sorte que :

1. seules les personnes autorisées puissent introduire et modifier des données;

2. l'information puisse être contrôlée quant à son authenticité;

3. les certificats ne soient disponibles au public pour des recherches que dans les cas où le titulaire du certificat a donné son consentement; et

4. toute modification technique mettant en péril ces exigences de sécurité soit apparente pour l'opérateur.

Sous-section 3

Exigences relatives aux dispositifs sécurisés de création de signature électronique

Art. 11

Le prestataire de service de certification n'utilise ou ne met à disposition des utilisateurs que des dispositifs sécurisés de

ken van een elektronische handtekening die, via passende technische middelen en procedures, waarborgen dat :

1. de gebruikte gegevens voor het aanmaken van een elektronische handtekening in de praktijk slechts één keer kunnen voorkomen en hun vertrouwelijkheid op redelijke wijze verzekerd is;

2. men de voldoende zekerheid heeft dat de voor het aanmaken van een elektronische handtekening gebruikte gegevens niet door deductie kunnen worden gevonden en dat een handtekening met de momenteel beschikbare technische middelen beschermd is tegen vervalsing;

3. de voor het aanmaken van een elektronische handtekening gebruikte gegevens door de wettige ondertekenaar op betrouwbare wijze kunnen worden beschermd tegen het gebruik door anderen.

De veilige middelen voor het aanmaken van een elektronische handtekening mogen de te ondertekenen gegevens niet wijzigen en niet beletten dat deze gegevens de ondertekenaar worden voorgelegd vóór het ondertekeningsproces.

Onderafdeling 4

Gekwalificeerd certificaat

Art. 12

Een gekwalificeerd certificaat bevat minstens de volgende gegevens :

1° een vermelding waaruit blijkt dat het certificaat als gekwalificeerd certificaat wordt afgegeven;

2° de gegevens met betrekking tot de identificatie en de erkenning van de certificatiedienstverlener, en het land waar deze is gevestigd;

3° de identificatiegegevens van de certificaathouder of, zo hij dat verlangt, een pseudoniem dat als dusdanig is geïdentificeerd;

4° in voorkomend geval een specifieke eigenschap van de certificaathouder, afhankelijk van de bestemming van het certificaat;

5° de gegevens voor het verifiëren van een handtekening, die overeenkomen met de gegevens voor het aanmaken van een handtekening onder toezicht van de titularis;

6° vermelding van het begin en het einde van de geldigheid van het certificaat;

7° de identificatiecode van het certificaat;

8° in voorkomend geval de beperkingen bij het gebruik van het certificaat en/of de beperking op het bedrag van de verrichtingen waarvoor het certificaat mag worden gebruikt.

création de signature électronique qui garantissent, par les moyens techniques et procédures appropriés, que :

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

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

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

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

Sous-section 4

Du certificat qualifié

Art. 12

Un certificat qualifié contient au moins les informations suivantes :

1° une mention indiquant que le certificat est délivré à titre de certificat qualifié;

2° les données d'identification et d'agrément du prestataire de service de certification ainsi que le pays dans lequel il est établi;

3° les données d'identification du titulaire de certificat ou, à sa demande, un pseudonyme identifié comme tel;

4° le cas échéant, une qualité spécifique du titulaire de certificat, en fonction de l'usage auquel celui-ci est destiné;

5° les données afférentes à la vérification de signature qui correspondent aux données afférentes à la création de signature sous le contrôle du signataire;

6° l'indication du début et de la fin de la période de validité du certificat;

7° le code d'identification du certificat;

8° le cas échéant, les limites à l'utilisation du certificat et/ou à la valeur des transactions pour lesquelles le certificat peut être utilisé.

Het gekwalificeerde certificaat dient te worden beveiligd met de geavanceerde elektronische handtekening van de certificatiedienstverlener die het certificaat afgeeft.

Onderafdeling 5

Herroeping van certificaten

Art. 13

§ 1. Op aanvraag van de vooraf geïdentificeerde certificaathouder herroept de certificatiedienstverlener onmiddellijk het certificaat.

§ 2. De certificatiedienstverlener herroept eveneens een gekwalificeerd certificaat indien :

1° er ernstige redenen bestaan om aan te nemen dat het certificaat werd afgegeven op basis van foutieve of vervalste gegevens, dat de in het certificaat opgenomen informatie niet meer met de werkelijkheid overeenstemt of dat de vertrouwelijkheid van de gegevens voor het aanmaken van een handtekening werd geschonden;

2° het bestuur de herroeping gelast zoals bepaald in artikel 16;

3° de certificatiedienstverlener zijn activiteiten stopzet zonder dat deze worden overgenomen door een andere certificatiedienstverlener;

4° de certificatiedienstverlener op de hoogte wordt gebracht van het overlijden van de natuurlijke persoon of van de vereffening van de rechtspersoon die er certificaathouder van is.

De certificatiedienstverlener brengt de certificaathouder op de hoogte van de herroeping en motiveert zijn beslissing. Een maand voor afloop van een certificaat brengt de certificatiedienstverlener de certificaathouder hiervan op de hoogte.

§ 3. De herroeping van een gekwalificeerd certificaat is definitief.

Art. 14

§ 1. De certificatiedienstverlener treft de nodige maatregelen om op elk ogenblik en onverwijld gevolg te kunnen geven aan een aanvraag tot herroeping.

§ 2. Onmiddellijk na de beslissing tot herroeping neemt de certificatiedienstverlener de vermelding van de herroeping op in het elektronisch register zoals bedoeld in artikel 10.

Vanaf deze inschrijving is de herroeping tegenstelbaar ten aanzien van derden.

Le certificat qualifié doit être sécurisé par la signature électronique avancée du prestataire de service de certification qui le délivre.

Sous-section 5

De la révocation des certificats

Art. 13

§ 1er. À la demande du titulaire du certificat qualifié, préalablement identifié, le prestataire de service de certification révoque immédiatement le certificat.

§ 2. Le prestataire de service de certification révoque également un certificat qualifié lorsque :

1° il existe des raisons sérieuses pour admettre que le certificat a été délivré sur la base d'informations erronées ou falsifiées, que les informations contenues dans le certificat ne sont plus conformes à la réalité ou que la confidentialité des données afférentes à la création de signature a été violée ;

2° l'administration ordonne la révocation comme prévu à l'article 16;

3° le prestataire de service de certification arrête ses activités sans qu'il n'y ait reprise de celles-ci par un autre prestataire de service de certification;

4° le prestataire de service de certification est informé du décès de la personne physique ou de la dissolution de la personne morale qui en est le titulaire.

Le prestataire de service de certification informe le titulaire de certificat de la révocation et motive sa décision. Un mois avant l'expiration d'un certificat, le prestataire de service de certification informe son titulaire de celle-ci.

§ 3. La révocation d'un certificat qualifié est définitive.

Art. 14

§ 1er. Le prestataire de service de certification prend les mesures nécessaires afin de répondre à tout moment et sans délai à une demande de révocation.

§ 2. Immédiatement après la décision de révocation, le prestataire de service de certification inscrit la mention de la révocation du certificat dans l'annuaire électronique visé à l'article 10.

La révocation est opposable aux tiers à partir de cette inscription.

§ 3. De certificatiedienstverlener bewaart alle relevante informatie met betrekking tot het gekwalificeerde certificaat gedurende 20 jaar na de datum van afgifte, met name om voor het gerecht een bewijs van certificatie te kunnen voorleggen. Deze gegevens mogen met elektronische middelen worden opgeslagen.

De gegevens moeten toegankelijk zijn voor eenieder die een belang aantoont.

Onderafdeling 6

Aansprakelijkheid

Art. 15

§ 1. Een certificatiedienstverlener die een voor het publiek bedoeld gekwalificeerd certificaat afgeeft of een dergelijk certificaat publiekelijk waarborgt, is, tenzij hij bewijst dat er van geen enkele onachtzaamheid sprake is, aansprakelijk voor de schade die hij toebrengt aan elke persoon die op redelijke wijze vertrouwen in het certificaat stelt, met name wat betreft :

1. de juistheid van alle erin opgenomen gegevens sinds de verschijning in het elektronisch register zoals bedoeld in artikel 10;

2. de zekerheid dat de in het gekwalificeerde certificaat geïdentificeerde persoon op het moment van de afgifte van het certificaat het gebruik beheerste van de gegevens voor het aanmaken van een handtekening, overeenstemmend met de gegevens voor het verifiëren van een handtekening zoals vermeld in het certificaat;

3. de zekerheid dat de gegevens voor het aanmaken en het verifiëren van een handtekening aanvullend kunnen worden gebruikt;

4. de integriteit van de gegevens voor het aanmaken van de handtekening.

§ 2. Een certificatiedienstverlener die een voor het publiek bedoeld gekwalificeerd certificaat afgeeft of een dergelijk certificaat in het publiek waarborgt, is, tenzij hij bewijst dat er van geen enkele onachtzaamheid sprake is, aansprakelijk voor de schade die hij toebrengt aan elke persoon die op redelijke wijze vertrouwen in het certificaat stelt, wanneer werd nagelaten de herroeping van het certificaat te laten inschrijven.

§ 3. Een certificatiedienstverlener is niet aansprakelijk voor de schade die voortvloeit uit het misbruik van een gekwalificeerd certificaat bij overschrijding van de beperkingen op het gebruik van het certificaat en/of van het bedrag van de verrichtingen waarvoor het certificaat kan worden gebruikt, op voorwaarde dat deze beperkingen in het certificaat werden opgenomen en voor derden herkenbaar zijn.

§ 3. Le prestataire de service de certification conserve toutes les informations pertinentes concernant le certificat qualifié pendant une durée de 20 ans à dater de sa délivrance, en particulier, pour pouvoir fournir une preuve de la certification en justice. Ces enregistrements peuvent être effectués par des moyens électroniques.

Ces données doivent être accessibles à toute personne justifiant d'un intérêt.

Sous-section 6

De la responsabilité

Art. 15

§ 1er. Sauf s'il prouve qu'il n'a commis aucune négligence, un prestataire de service de certification qui délivre à l'intention du public un certificat qualifié ou qui garantit publiquement un tel certificat est responsable du préjudice causé à toute personne qui se fie raisonnablement à ce certificat pour ce qui est de :

1. l'exactitude de toutes les informations qui y sont contenues à dater de sa publication dans l'annuaire électronique visé à l'article 10;

2. l'assurance que, au moment de la délivrance du certificat, la personne identifiée dans le certificat qualifié avait la maîtrise des données afférentes à la création de signature correspondant aux données afférentes à la vérification de signature figurant dans le certificat;

3. l'assurance que les données afférentes à la création et à la vérification de signature puissent être utilisées de façon complémentaire;

4. l'intégrité des données afférentes à la création de la signature.

§ 2. Sauf s'il prouve qu'il n'a commis aucune négligence, un prestataire de service de certification qui délivre à l'intention du public un certificat qualifié ou qui garantit publiquement un tel certificat est responsable du préjudice causé à toute personne qui se fie raisonnablement à ce certificat, pour avoir omis de faire enregistrer la révocation du certificat.

§ 3. Un prestataire de service de certification n'est pas responsable du préjudice résultant de l'usage abusif d'un certificat qualifié qui dépasse les limites fixées à son utilisation et/ou la valeur limite des transactions pour lesquelles le certificat peut être utilisé, pour autant que ces limites soient inscrites dans le certificat et qu'elles soient discernables par les tiers.

§ 4. Elke overeenkomst die in strijd is met de bepalingen van dit artikel wordt beschouwd als zijnde niet geschreven.

Onderafdeling 7

Stopzetting van de activiteiten

Art. 16

§ 1. De certificatiedienstverlener brengt binnen een redelijke termijn het bestuur op de hoogte van zijn bedoeling om zijn activiteiten stop te zetten alsook van elke maatregel die de stopzetting van zijn activiteiten tot gevolg kan hebben. In dit geval dient hij zich te vergewissen van de overname ervan door een andere erkende certificatiedienstverlener. Wanneer dit niet mogelijk is, herroept hij de certificaten twee maanden na de houders ervan te hebben ingelicht.

§ 2. De certificatiedienstverlener die zijn activiteiten stopzet om redenen buiten zijn wil of in geval van faillissement, brengt het bestuur daarvan onmiddellijk op de hoogte. Deze zorgt in voorkomend geval voor de herroeping van de certificaten en treft de nodige maatregelen om te voldoen aan de in artikel 14, § 3 bepaalde verplichting. Daartoe verschaft de certificatiedienstverlener het bestuur alle nuttige informatie.

Onderafdeling 8

Betrouwbaarheid van de technische middelen

Art. 17

§ 1. Het samenstellen van de gegevens voor het aanmaken en verifiëren van handtekeningen, het aanmaken, afgeven en bijhouden van certificaten alsook de veilige middelen voor het aanmaken van elektronische handtekeningen gebeurt door middel van betrouwbare systemen en producten die tegen wijzigingen beschermd moeten zijn en die de technische en cryptografische veiligheid van hun functies waarborgen.

§ 2. De betrouwbaarheid van de beveiligingen wordt beoordeeld volgens de stand van de techniek.

§ 4. Toute convention contraire aux dispositions du présent article est réputée non écrite.

Sous-section 7

De l'arrêt des activités

Art. 16

§ 1er. Le prestataire de service de certification informe l'administration dans un délai raisonnable de son intention de mettre fin à ses activités ainsi que de toute action qui pourrait conduire à la cessation de ses activités. Dans ce cas, il doit s'assurer de la reprise de celles-ci par un autre prestataire de service de certification accrédité ou à défaut, révoque les certificats deux mois après en avoir averti les titulaires.

§ 2. Le prestataire de service de certification qui arrête ses activités pour des raisons indépendantes de sa volonté ou en cas de faillite en informe immédiatement l'administration. Celle-ci procède, le cas échéant, à la révocation des certificats et prend les mesures nécessaires pour satisfaire à l'obligation prévue à l'article 14, § 3. À cet effet le prestataire de service de certification transmet toute information utile à l'administration.

Sous-section 8

De la fiabilité des moyens techniques

Art. 17

§ 1er. La création des données afférentes à la création et à la vérification de signature, la création, la délivrance et la conservation des certificats ainsi que les dispositifs sécurisés de création de signature électronique sont réalisés par des systèmes et des produits fiables qui doivent être protégés contre les modifications et assurer la sécurité technique et cryptographique des fonctions qu'ils assument.

§ 2. La fiabilité du niveau de sécurité est appréciée en fonction de l'état de la technique.

Afdeling 2

Certificatiedienstverleners

Onderafdeling 1

Bescherming van de persoonsgegevens

Art. 18

§ 1. Onverminderd de wet van 11 december 1998 tot omzetting van richtlijn 95/46/EG van 24 oktober 1995 van het Europees Parlement en van de Raad betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens en het vrije verkeer van deze gegevens, mag een certificatiedienstverlener die voor het publiek bestemde certificaten afgeeft, persoonsgegevens enkel verzamelen, hetzij rechtstreeks bij de betrokken persoon zelf, hetzij met diens expliciete toestemming, en enkel indien dat nodig is voor het afgeven en bijhouden van het certificaat. De gegevens mogen niet worden verzameld of gebruikt voor andere doeleinden zonder expliciete instemming van de betrokken persoon.

§ 2. Wanneer de certificaathouder een pseudoniem gebruikt en het strafrechtelijk onderzoek dit vereist, is de certificatiedienstverlener die het certificaat heeft afgegeven, verplicht alle gegevens met betrekking tot de identiteit van de houder te verstrekken in de omstandigheden en onder de voorwaarden bedoeld in artikelen 90*ter* tot 90*decies* van het Wetboek van Strafvordering.

Onderafdeling 2

Certificaten afgegeven door buitenlandse certificatiedienstverleners

Art. 19

§ 1. Een voor het publiek bestemd gekwalificeerd certificaat afgegeven door een certificatiedienstverlener gevestigd in een Lidstaat van de Europese Unie, en door deze laatste geaccrediteerd, wordt gelijkgesteld met de gekwalificeerde certificaten afgegeven door een in België gevestigde certificatiedienstverlener.

§ 2. Een voor het publiek bestemd gekwalificeerd certificaat afgegeven door een certificatiedienstverlener gevestigd in een derde land wordt gelijkgesteld met de gekwalificeerde certificaten afgegeven door een in België gevestigde certificatiedienstverlener :

1. indien de certificatiedienstverlener aan de in deze wet bedoelde voorwaarden voldoet en geaccrediteerd

Section 2

Des prestataires de service de certification

Sous-section 1re

Protection des données à caractère personnel

Art. 18

§ 1er. Sans préjudice de la loi du 11 décembre 1998 transposant la directive 95/46/CE du 24 octobre 1995 du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et à la libre circulation de ces données, un prestataire de service de certification qui délivre des certificats à l'intention du public ne peut recueillir des données personnelles que directement auprès de la personne concernée ou avec le consentement explicite de celle-ci et uniquement dans la mesure où cela est nécessaire à la délivrance et à la conservation du certificat. Les données ne peuvent être recueillies ni traitées à d'autres fins sans le consentement explicite de la personne intéressée.

§ 2. Lorsque le titulaire du certificat utilise un pseudonyme et lorsque les nécessités de l'instruction l'exigent, le prestataire de service de certification ayant délivré le certificat est tenu de communiquer toute donnée relative à l'identité du titulaire dans les circonstances et selon les conditions prévues par les articles 90*ter* à 90*decies* du Code d'instruction criminelle.

Sous-section 2

Certificats délivrés par des prestataires de service de certification étrangers

Art. 19

§ 1er. Un certificat qualifié délivré à l'intention du public par un prestataire de service de certification qui est établi dans un État membre de l'Union européenne, et qui est accrédité par ce dernier, est assimilé aux certificats qualifiés délivrés par un prestataire de service de certification établi en Belgique.

§ 2. Un certificat délivré à l'intention du public par un prestataire de service de certification qui est établi dans un pays tiers est assimilé aux certificats qualifiés délivrés par un prestataire de service de certification établi en Belgique :

1. si le prestataire de service de certification remplit les conditions visées dans la présente loi et a été accrédité dans

werd op basis van een vrijwillig accreditatiesysteem door een Lidstaat van de Europese Unie; of

2. indien een in de Europese Unie gevestigde geaccrediteerde certificatiedienstverlener het certificaat waarborgt; of

3. indien het certificaat of de certificatiedienstverlener erkend wordt door toepassing van een bilaterale of multilaterale overeenkomst tussen de Europese Unie en derde landen of internationale organisaties.

HOOFDSTUK 4

Certificaatgebruikers

Afdeling 1

Certificaathouders

Art. 20

§ 1. Vanaf het moment van de samenstelling van de gegevens voor het aanmaken van een handtekening, is de certificaathouder alleen verantwoordelijk voor de vertrouwelijkheid van deze gegevens.

§ 2. Wanneer er twijfel bestaat over het behoud van de vertrouwelijkheid van de gegevens voor het aanmaken van een handtekening of wanneer de in het certificaat opgenomen gegevens niet meer met de werkelijkheid overeenstemmen, dient de houder het certificaat te laten herroepen.

§ 3. Wanneer een certificaat vervalt of wordt herroepen, mag de houder na de vervaldatum van het certificaat of na herroeping geen gebruik meer maken van de overeenkomstige gegevens voor het aanmaken van een handtekening om deze gegevens te ondertekenen of te laten certificeren door een andere certificatiedienstverlener.

Afdeling 2

Ontvanger van een bericht

Art. 21

De ontvanger van een elektronisch ondertekend bericht dient de elektronische handtekening te controleren door middel van de gegevens voor het verifiëren van handtekeningen of certificaten. De ontvanger controleert ook of het certificaat niet vervallen of herroepen is.

le cadre d'un régime volontaire d'accréditation par un État membre de l'Union européenne; ou

2. si un prestataire de service de certification accrédité établi dans l'Union européenne garantit le certificat; ou

3. si le certificat ou le prestataire de service de certification est reconnu en application d'un accord bilatéral ou multilatéral entre l'Union européenne et des pays tiers ou des organisations internationales.

CHAPITRE 4

Des utilisateurs de certificat

Section 1re

Des titulaires de certificat

Art. 20

§ 1er. Dès le moment de la création des données afférentes à la création de signature, le titulaire du certificat est seul responsable de la confidentialité de ces données.

§ 2. En cas de doute quant au maintien de la confidentialité des données afférentes à la création de signature ou de perte de conformité à la réalité des informations contenues dans le certificat, le titulaire est tenu de faire révoquer le certificat.

§ 3. Lorsqu'un certificat est arrivé à échéance ou a été révoqué, le titulaire de celui-ci ne peut, après l'expiration du certificat ou après révocation, utiliser les données afférentes à la création de signature correspondantes pour signer ou faire certifier ces données par un autre prestataire de service de certification.

Section 2

Des destinataires de message

Art. 21

Le destinataire d'un message signé électroniquement est tenu de vérifier la signature électronique au moyen des données afférentes à la vérification de signature et du certificat. Le destinataire vérifie également que le certificat n'est ni expiré ni révoqué.

HOOFDSTUK 5

Controle en sancties

Art. 22

§ 1. Wanner het bestuur vaststelt dat een geaccrediteerde certificatiedienstverlener zich niet aan de voorschriften van deze wet houdt, stelt het een termijn vast om de toestand te regulariseren.

§ 2. Wanneer, na afloop van die termijn, de geaccrediteerde certificatiedienstverlener de toestand niet heeft geregulariseerd, trekt het bestuur de accreditatie in.

§ 3. De certificatiedienstverlener is verplicht de intrekking van de accreditatie in zijn elektronisch register te vermelden en de certificaathouders daarvan onverwijld op de hoogte te brengen.

Art. 23

§ 1. Wie misbruik maakt van de hoedanigheid van geaccrediteerd certificatiedienstverlener wordt bestraft met een gevangenisstraf van 8 dagen tot 3 maanden en met een boete van 1 000 tot 10 000 Belgische frank, of met een van beide straffen.

§ 2. Bij veroordeling op grond van de in paragraaf 1 bedoelde overtreding kan de bevoegde rechtbank de volledige of gedeeltelijke opneming van het vonnis in een of meerdere dagbladen bevelen, onder de door haar bepaalde voorwaarden en op kosten van de veroordeelde.

Gegeven te Brussel, 7 december 1999.

ALBERT

VAN KONINGSWEGE :

De minister van Justitie,

Marc VERWILGHEN

De minister van Telecommunicatie, en Overheidsbedrijven en Participaties

Rik DAEMS

De minister van Economie,

Rudy DEMOTTE

CHAPITRE 5

Du contrôle et des sanctions

Art. 22

§ 1er. Lorsque l'administration constate qu'un prestataire de service de certification accrédité ne se conforme pas aux prescriptions de la présente loi, elle fixe un délai pour régulariser la situation.

§ 2. Si, après l'écoulement de ce délai, le prestataire de service de certification accrédité n'a pas régularisé sa situation, l'administration procède au retrait de l'accréditation.

§ 3. Le prestataire de service de certification est tenu de mentionner dans son annuaire électronique le retrait de l'accréditation et d'en informer sans délai les titulaires de certificat.

Art. 23

§ 1er. Sera puni d'une peine de 8 jours à 3 mois de prison et d'une amende de 1 000 à 10 000 francs belges, ou d'une de ces peines seulement, quiconque aura usurpé la qualité de prestataire de service de certification accrédité.

§ 2. En condamnant du chef d'infraction visé au paragraphe 1er, la juridiction compétente peut ordonner l'insertion du jugement, intégralement ou par extraits, dans un ou plusieurs journaux, dans les conditions qu'elle détermine, aux frais du condamné.

Donné à Bruxelles, le 7 décembre 1999.

ALBERT

PAR LE ROI :

Le ministre de la Justice,

Marc VERWILGHEN

Le ministre des Télécommunications, et des Entreprises et Participations publiques

Rik DAEMS

Le ministre de l'Économie,

Rudy DEMOTTE

Drukkerij-Imprimerie SCHAUBROECK — 9810 NAZARETH