De invloed van de digitale handtekening op de elektronische aangifte van de vennootschapsbelasting

Bram LAMBRICHTS

promotor :
Prof.dr.ir Frans LEMEIRE

Eindverhandeling voorgedragen tot het bekomen van de graad
Handelsingenieur major technologie

universiteit hasselt

Voorwoord

In het kader van mijn opleiding tot licentiaat handelsingenieur koos ik digitale handtekening als onderwerp voor mijn thesis. Deze keuze is mede gebeurd op basis van mijn afstudeerrichting technologie en omwille van mijn interesse voor het onderwerp. Aangezien de digitale handtekening een recent begrip is, leek het me een uitdaging om dit onderwerp verder te onderzoeken.

Bij het schrijven van deze eindverhandeling heb ik natuurlijk hulp gekregen van verschillende mensen. Aan deze mensen wil ik mijn dank betuigen. In de eerste plaats wil ik mijn promotor Prof. Dr. ir. F. Lemeire bedanken. Zijn inzicht in de wiskundige begrippen leverden een belangrijke bijdrage aan dit onderzoek. Verder wil ik eveneens de heer S. De Prins bedanken voor zijn bereidwillige medewerking aan dit onderzoek. Zijn kennis van de vennootschapsbelasting heeft mij uitstekend geholpen bij de uitwerking van het praktijkvoorbeeld.

Tenslotte bedank ik mijn ouders van wie ik deze kans heb gekregen om opgeleid te worden tot licentiaat handelsingenieur. Ze zijn steeds in mij blijven geloven en hebben me doorheen de opleiding ten volle gesteund. Ook bedank ik mijn broer Bjorn voor zijn hulp bij de lay-out en verbetering. Als laatste wil ik mijn vriendin Andromeda bedanken voor haar onvoorwaardelijke steun.

Samenvatting

“The Internet is becoming the town square for the global village of tomorrow”, is een uitspraak van Bill Gates die de belangrijkheid van het Internet en zijn technologische mogelijkheden goed samenvat. Steeds meer zaken worden elektronisch afgehandeld via het Internet. Het probleem van het wereldwijde Web is dat het nog niet echt veilig is. Het Internet heeft een open en onbeveiligde structuur. Hierdoor is de kans op misbruik bij gegevenstransmissie groot. Berichten en informatie kunnen onderschept worden. Zo komt de informatie in verkeerde handen en kan ze misbruikt worden. Een ander probleem is dat men op het Internet moeilijk kan nagaan of men de informatie naar de juiste persoon stuurt en niet naar een andere persoon die zich uitgeeft voor deze juiste persoon.

Om deze problemen van onveilige dataverzending te verhelpen kan de informatie vercijferd worden. Dit gebeurt met behulp van cryptografie. De digitale handtekening is een andere toepassing van public-key cryptografie, waarbij de zender het bericht ondertekent met zijn private sleutel. Het is een uitstekend middel om de authenticiteit, integriteit en onweerlegbaarheid bij internettransacties te garanderen. In combinatie met een cryptosysteem kan de digitale handtekening ook garant voor confidentialiteit.

De basis van deze cryptografie vindt zijn wortels in de getallenleer. Dankzij deze wiskunde kan men de werking van cryptosystemen begrijpen. De digitale handtekening steunt op de principes van de one way functie. Deze functie is gemakkelijk te berekenen in één richting. Het is echter bijna onmogelijk om de inverse functie hiervan te achterhalen, tenzij men over extra informatie beschikt. Het RSA-algoritme steunt op dit principe. De hash functie speelt eveneens een belangrijke rol bij de digitale handtekening. Met de hash functie kan men een bericht van willekeurige grootte omzetten in een reeks met een vaste en meestal korte lengte, die toelaat om de authenticiteit van het bericht te controleren.

Wetten omtrent digitale handtekening konden niet uitblijven. Eind 1999 verscheen er eerst een Europese richtlijn betreffende elektronische handtekeningen. In België werd deze richtlijn in twee wetten uitgevoerd. De wet van 20 oktober 2000 stelt dat

elektronische geschriften gelijkwaardig zijn aan klassieke geschriften. De wet van 9 juli 2001 zorgt ervoor dat een digitale handtekening, gecreëerd met gekwalificeerde certificaten, automatisch dezelfde rechtsgeldigheid heeft als een handgeschreven handtekening.

De digitale handtekening kent ondertussen reeds verschillende toepassingsgebieden. Een eerste toepassingsgebied is e-commerce. E-commerce is de verzamelnaam van alle manieren waarop via digitale wegen handel gedreven kan worden. Er bestaan verschillende types van e-commerce. Zo heeft men business-to-business (B2B) e-commerce, business-to-consumer (B2C) e-commerce en consumer-to-consumer (C2C) e-commerce. Deze laatste vorm wordt steeds groter dankzij internetsites zoals e-bay. Om deze transacties veiliger te maken kan de digitale handtekening van belang zijn.

Een tweede toepassing vindt men terug in het bankwezen, met name e-banking. Hierbij is de digitale handtekening van groot belang. Veiligheid is immers het belangrijkste aspect bij financiële transacties. Een bank moet immers met zekerheid weten dat ze handelt met de persoon die hij beweert te zijn. Tegelijkertijd moeten sommige gegevens versleuteld verstuurd worden.

E-government is een derde toepassing van de digitale handtekening. E-government is het beleid van de overheid waarbij burgers en ondernemingen via het Internet kunnen communiceren en handelen met de overheid. Het praktijkvoorbeeld uit mijn eindverhandeling is een onderdeel van e-government. Het indienen van een aangifte van de vennootschapsbelasting via elektronische weg moet veilig gebeuren. Ook hier is de betrouwbaarheid en identiteit van het bedrijf dat de aangifte indient belangrijk. Andere onderdelen van e-government zijn bijvoorbeeld elektronische loketten, het invullen van verklaringen, sociale zekerheid, personenbelasting, …

Een laatste toepassing van de digitale handtekening vindt men in de medische wereld. Ook hier kan deze een meerwaarde bieden. Het is vaak nodig dat gegevens van patiënten uitgewisseld worden tussen ziekenhuizen en andere zorgverleners. Men zou een elektronisch patiëntendossier (EPD) kunnen gebruiken om een chaos van gegevensstromen te vermijden. Dit is een interactief systeem waarmee,

onafhankelijk van plaats en tijd, toegang tot alle medische gegevens van een patiënt verkregen kan worden. Een digitale handtekening waarborgt dat enkel bevoegden toegang hebben tot het EPD en garandeert de integriteit van de data. De combinatie met een cryptosysteem zorgt ervoor dat de privacy van de patiënt niet geschonden wordt.

Inhoudsopgave

Hoofdstuk 1 Inleiding

In dit hoofdstuk wordt er stil gestaan bij de omschrijving van het praktijkprobleem, de formulering van de onderzoeksvragen en de bespreking van de gebruikte onderzoeksmethodologische instrumenten.

1.1 Praktijkprobleem

Elektronische communicatie is één van de meest besproken onderwerpen van de laatste jaren en zit enorm in de lift. In onze maatschappij zijn begrippen zoals elektronische post niet meer weg te denken. Iedereen, zowel bedrijven als particulieren, maakt meer en meer gebruik van informatie- en communicatietechnologie. Er worden steeds meer en meer online transacties uitgevoerd. Enkele voorbeelden hiervan zijn elektronisch bankieren, online een belastingsaangifte invullen, uitwisseling van documenten … Bij deze toepassingen spelen veiligheid, vertrouwelijkheid en integriteit dikwijls een cruciale rol. Andere voorbeelden zijn terug te vinden in de medische wereld, zoals het geneeskundig dossier en het beoordelingsdossier …

De behoefte aan vertrouwen ontstaat vooral wanneer men financiële transacties uitvoert. Het is immers van groot belang dat deze veilig gebeuren. Hierdoor wordt betrouwbaarheid bij elektronische transacties een belangrijke voorwaarde. Betrouwbaarheid kan slechts ontstaan wanneer men beschikt over goede beveiligingsmethoden. Wanneer men via Internet communiceert, kan men niet met zekerheid zeggen of men te maken heeft met een bedrieger. Ook dit is een belangrijk gegeven. De digitale handtekening is een beveiligingsmethode die instaat voor de authenticiteit, betrouwbaarheid en integriteit.

De basis van de digitale handtekening vindt men terug in de cryptologie. Eén onderdeel van cryptologie is cryptografie. Dit bestaat uit verschillende technieken om teksten te coderen. Men spreekt van symmetrische encryptie als zender en

ontvanger dezelfde en dus één unieke sleutel gebruiken. Wanneer er een private sleutel en een publieke sleutel gebruikt worden, spreekt men van asymmetrische encryptie of publieke sleutel encryptie. Vooral dit laatste type wordt gebruikt bij de digitale handtekening.

Het andere onderdeel van cryptologie is crypto-analyse. Hierbij worden technieken ontwikkeld om gecodeerde berichten te decoderen. Dit kan gebeuren via goed geplande aanvallen, zoals een plaintextaanval. (zie hoofdstuk 3)

Cryptografie biedt bescherming voor gevoelige informatie. Banken gebruiken op dit moment al onrechtstreeks vormen van cryptografie om geldtransacties af te schermen voor kwaadwillige tussenkomsten. Zo beschermt cryptografie tegen vervalsingen, ongewilde wijzigingen, maar ook beveiligt het pincodes en kredietkaartnummers. Een voorbeeld hiervan is de digipass om toegang te krijgen tot online transacties.

Een digitale handtekening is zoals reeds vermeld gebaseerd op publieke sleutel encryptie. Het doel is de identiteit van de zender te garanderen net zoals bij de klassieke handgeschreven handtekening. Daarnaast verzekert ze ook de integriteit van elektronische berichten. In commerciële situaties, waar onweerlegbaarheid zeer belangrijk is, kunnen digitale handtekeningen eveneens een meerwaarde bieden. Zo wordt het met behulp van de digitale handtekening onmogelijk te ontkennen dat hij een bepaalde bestelling heeft geplaatst.

1.2 Centrale onderzoeksvraag en deelvragen

Het doel van deze eindverhandeling is om een inzicht te krijgen in de principes van de digitale handtekening. Ook wordt er kort uitgewijd over toepassingen van de digitale handtekening. In het bijzonder wordt er dieper ingegaan op de online verwerking van vennootschapsbelasting. Hierbij wordt de nadruk gelegd op de voordelen voor de overheid en voor de ondernemingen. Heel belangrijk bij de online verwerking van vennootschapsbelasting is dat het de transparantie en duidelijkheid verbetert. Zo moeten ook KMO’s geen grote inspanningen doen om hun fiscaliteit te

optimaliseren. De digitale handtekening biedt enorm veel mogelijkheden en kan daarom een belangrijk middel zijn om het vertrouwen van de internetgebruiker te winnen. Het is niet de bedoeling in deze eindverhandeling een allesomvattend onderzoek uit te voeren. Men wil zich beperken tot enkele onderdelen en deze verder uit te diepen.

Het doel van het onderzoek kan samengevat worden in onderstaande centrale onderzoeksvraag:

Wat is de invloed van de digitale handtekening in het bedrijfsleven?

Verder wordt er onderzoek verricht naar de mogelijkheden om met behulp van het interactieve Internet de vennootschapsbelasting te optimaliseren, en de plaats van de digitale handtekening hierbij, vooral voor KMO's die niet altijd over nodige knowhow beschikken om delen van de vennootschapsbelasting te ontwijken.

Om de centrale onderzoeksvraag verder uit te werken, trachten we gebruik te maken van deelvragen. Een eerste deelvraag zou kunnen zijn: **"Wat is cryptografie?"** Aangezien cryptografie de basis vormt van de digitale handtekening is het nuttig uit te zoeken wat cryptografie precies voorstelt. We trachten de soorten cryptografie te achterhalen en eveneens de werking hiervan.

Ten tweede kunnen we ons afvragen welke wiskundige hulpmiddelen gebruikt kunnen worden bij de creatie van de digitale handtekening. De vraag luidt dan ook: **"Welke wiskundige hulpmiddelen en cryptologie gebruikt de digitale handtekening?"**

Een volgende vraag in het onderzoek is: **"Wat is een digitale handtekening en hoe werkt de digitale handtekening?"** Kennis van de principes van de digitale handtekening helpen ons het vertrouwen in transacties via het Internet vergroten.

Vervolgens vragen we ons af of de digitale handtekening enkel wiskundig beschermd wordt of dat deze handtekening ook door de wet wordt beschermd. De vraag is: **"Welke wettelijke regeling bestaat er voor de digitale handtekening?"** Ook deze vraag helpt ons het vertrouwen in online transacties te vergroten.

Een laatste theoretische vraag is: **"Welke toepassingen bestaan reeds van de digitale handtekening?"** Hier wordt kort ingegaan op de mogelijke toepassingen van de digitale handtekening, zoals medische toepassingen, e-commerce, e-banking …

In het praktijkgedeelte wordt er verder ingegaan op een applicatie van e-government. We onderzoeken de mogelijkheden van het online invullen van de belastingsaangifte voor vennootschappen. Enkele deelvragen die we bij dit gedeelte kunnen stellen zijn:

- Welke systemen worden gebruikt voor belastingsaangiften?
- Hoe werken deze systemen?
- Hoe wordt de digitale handtekening geïntegreerd in deze systemen?
- Hoe veilig zijn deze systemen?
- Hoe economisch is het online indienen van de vennootschapsbelasting?

Het onderzoek werd opgezet in tien luiken die achtereenvolgens zullen besproken worden in de hoofdstukken twee tot en met tien.

1.3 Onderzoeksmethodologie

1.3.1 Literatuurstudie

Deze eindverhandeling is opgebouwd rond een literatuurstudie en een aansluitend praktijkgedeelte. Eerst werd er gezocht naar wetenschappelijke bronnen uit een aantal bibliotheken, gebruik makend van zoektermen zoals de digitale handtekening, elektronische communicatie, cryptografie, netwerkbeveiliging, e-government … . Uit de gevonden literatuur konden we verder zoeken naar nieuwe bronnen via de in de literatuur gebruikte bronnen. Eveneens werd Internet aangewend als bron. Hierdoor was het mogelijk inzichten te krijgen over de te onderzoeken materie en was het mogelijk een overzicht te krijgen van reeds gepubliceerd materiaal. Via de digitale persdatabank "Mediargus" werd het mogelijk recent gepubliceerde artikels te bestuderen.

1.3.2 Praktijkgedeelte

Om informatie te krijgen over het praktijkgedeelte werd een beroep gedaan op een vakdeskundige. Deze werd ondervraagd met behulp van half gestructureerde interviews. Als uitgangspunt werden de bevindingen uit de literatuurstudie genomen. In het praktijkgedeelte wordt er verder ook nog in het kort uitgewijd over de vennootschapsbelasting.

Hoofdstuk 2 Cryptologie

In hoofdstuk 2 wordt er dieper ingegaan op de onderliggende basis van de digitale handtekening. Er wordt getracht een beter inzicht te krijgen in cryptologie.

2.1 Wat is Cryptologie?

De term cryptologie is opgebouwd uit twee Griekse woorden: “cruptos” (verbergen) en “logos” (woord, leer). Het betekent dan ook letterlijk de leer van het verbergen. Enerzijds zal men pogen boodschappen zo goed mogelijk te beveiligen door ze met efficiënte technieken te coderen. Het onderdeel van de cryptologie dat deze doelstelling nastreeft noemt men de cryptografie. Er kan ook gepoogd worden om technieken en strategieën te ontwikkelen om gecodeerde boodschappen te ontcijferen. Het onderdeel van de cryptologie dat zich hiermee bezighoudt noemt men de crypto-analyse. (http://www.kubrussel.ac.be/WSetew/cryptotekst.html#1, 2006) In dit hoofdstuk wordt er vooral ingegaan op cryptografie. Toch zal ook crypto-analyse gedeeltelijk aan bod komen.

Een interessante noot die men hierbij kan maken houdt verband met de moeilijkheden in de taalgrammaticadialecten. Men zou kunnen veronderstellen dat er verschillende dialecten werden uitgevonden als een soort van codetaal. Bevolkingsgroepen met een verschillend dialect verstaan elkaar niet. Dit maakt het mogelijk om vreemdelingen te herkennen. Om maar een klein voorbeeld te geven. In 1302 nam het fiere Vlaanderen het op tegen de Franse koning. Er werd een wachtwoord verzonnen, “schild en vriend”. Al wie deze leuze niet deftig kon uitspreken, werd vermoord. Dit kan gezien worden als een vorm van cryptologie. (F. Lemeire, 2006)

Een ander voorbeeld dat Prof dr. ir. Lemeire (2007) aanhaalde, handelde over het Sloveens. Sloveens wil zeggen: “zij die elkaar verstaan”. Toen Slovenië tot het

Oostenrijks Keizerrijk behoorde verstonden de Oostenrijkers hen niet. De Oostenrijkers spraken immers Duits.

2.2 Geschiedenis van cryptografie

De oorsprong van cryptografie gaat waarschijnlijk terug tot de begintijd van de menselijke beschaving, vanaf het moment dat mensen leerden communiceren. Ze moesten continu zoeken naar middelen om er zeker van te zijn dat gecommuniceerde geheimen ook geheim bleven. Het eerste opzettelijke gebruik van technische middelen om berichten te coderen is terug te vinden bij de Grieken. Rond 6 jaar voor Christus werd er bij hen een stok, de "scytale" genaamd, gebruikt. De persoon die de boodschap stuurde, bond een stuk papier om de stok en schreef er in de lengterichting een bericht op. Daarna haalde hij het papier van de stok en stuurde het naar de bedoelde ontvanger.

De Romeinen maakten ook gebruik van cryptosystemen Deze zijn echter naar huidige maatstaven kinderlijk eenvoudig te kraken. Zij gebruikten encryptie bij hun militaire communicatie en deden dit door letters van het alfabet met een vaste factor te verschuiven. Julius Caesar was één van de meest prominente gebruikers van dit systeem. Deze vorm van versleutelen staat dan ook bekend als de Caesarvercijfering. Een met behulp van dit systeem geconstrueerde cijfertekst is in maximaal 26 pogingen te kraken en derhalve niet erg veilig. Cryptografie heeft zich door de eeuwen heen verder ontwikkeld en vond haar toepassingen vooral bij overheidsaangelegenheden.
(http://www.uu.nl/content/elektronischehandtekeningen.pdf, 2006)

In de volgende 19 eeuwen zijn er meer en minder geavanceerde experimentele coderings-technieken verzonnen, waarbij de veiligheid afhing van hoeveel vertrouwen de gebruiker er in had. In de 19e eeuw schreef Kerchoffs over de principes van de moderne cryptografie. Eén van deze principes zegt dat de veiligheid van een cryptografisch systeem niet afhangt van het gebruikte cryptografische proces, maar van de gebruikte sleutel. Voornamelijk diplomatieke diensten, inlichtingendiensten en defensie waren enthousiaste gebruikers van deze

technieken. Dit wil niet zeggen dat er nooit publieke belangstelling geweest is voor cryptografie. Edgar Allan Poe die een fervent amateur cryptograaf was, heeft met zijn verhaal “The Gold Bug”, waarin geheimschriften een grote rol spelen, de belangstelling voor deze materie behoorlijk aangewakkerd in de 19e eeuw. (http://www.uu.nl/content/elektronischehandtekeningen.pdf, 2006)

In tijden van oorlog en bij internationale spanningen ontwikkelde de wetenschap van de cryptografie zich versneld, terwijl er in rustigere perioden nauwelijks progressie was. In deze eeuw heeft de cryptografie zich gestaag ontwikkeld, mede gestimuleerd door de beide Wereldoorlogen en de daarop volgende Koude Oorlog. (http://www.uu.nl/content/elektronischehandtekeningen.pdf, 2006)

Vanaf de jaren '50 en '60 ging de wiskunde als hulpwetenschap bij het ontwikkelen van cryptografische algoritmen een belangrijkere rol spelen. De afgelopen twee decennia heeft de ontwikkeling van de cryptografie een grote sprong voorwaarts gemaakt. De vraag naar veilige versleutelingtechnieken in een maatschappij, die in toenemende mate automatiseerde, nam steeds meer toe. Men moest het hoofd bieden aan problemen rond de opslag van gegevens en rond de vertrouwelijkheid, exclusiviteit en betrouwbaarheid van communicatie. (http://www.uu.nl/content/elektronischehandtekeningen.pdf, 2006)

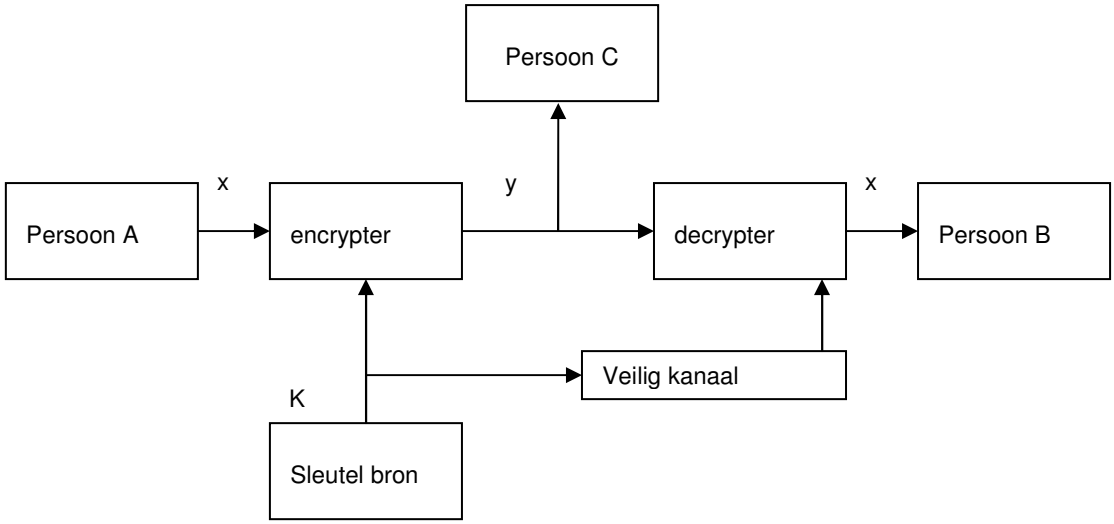
Hoofdstuk 3 Klassieke of symmetrische cryptografie

Zoals reeds eerder vermeld is het fundamentele doel van cryptografie het mogelijk maken twee mensen met elkaar te laten communiceren via een onveilig kanaal zodat een luistervink niet kan verstaan wat er gezegd wordt. Dit kanaal kan een telefoonlijn of een computernetwerk zijn. Er bestaan verschillende soorten cryptografie. Als eerste wordt het klassieke geval beschreven.

3.1 Symmetrische encryptie

Aan de hand van een eenvoudig voorbeeld tracht men het doel van klassieke cryptografie uit te leggen. Persoon A wil informatie doorgeven aan persoon B. Deze informatie kan een tekst zijn, maar het kan ook numerische data of wat dan ook zijn. Deze informatie wordt vanaf heden *plaintext* genoemd. Persoon A versleutelt deze plaintext met een vooraf bepaalde sleutel en zendt deze resulterende *ciphertext* of vercijferde tekst via een kanaal naar Persoon B. Deze laatste kent de encryptiesleutel en kan de ciphertext ontsleutelen om zo de plaintext te reconstrueren. Een derde persoon, persoon C kan slechts de ciphertext lezen omdat hij niet beschikt over de encryptiesleutel. (Stinson, 2006)

Figuur 3.1: Symmetrische encryptie



Persoon C wordt in de meeste literatuur beschreven als Persoon E. Dit is een afkorting voor Eavesdropper. Het duidt dus op een persoon die probeert mee te luisteren of af te luisteren. Meestal is er eveneens sprake van een vertrouwenspersoon of organisatie (zie paragraaf 7.4.5).

Dit voorbeeld kan worden beschreven met volgend wiskundig model:

Een cryptosysteem is 5-voudig (P,C,K,E,D) met onderstaande voldane voorwaarden:

1. P is een eindige set van mogelijke plaintexts
2. C is een eindige set van mogelijke ciphertexts
3. K, de sleutelverzameling, is een eindige set van sleutels
4. Voor elke $k \in K$ is er een encryptieregel e_k en een corresponderende decryptiesleutel $d_k \in D$. Elke e_k: P → C en d_k: C → P zijn functies zodat $d_k(e_k(x)) = x$ voor elk plaintext element $x \in P$

Deze laatste voorwaarde duidt erop dat x versleuteld wordt door e_k en de ciphertext $e_k(x)$ ontsleuteld wordt door d_k. (Stinson, 2006)

3.1.1 Shift cipher methode

Een veelgebruikte klassieke encryptiemethode is de *shift cipher* methode.

Shift cipher:
Laat $P = C = Z_{26}$. Voor $0 \leq K \leq 26$, definieer

$$e_k(x) = (x + K) \bmod 26$$

en

$$d_k(y) = (y - K) \bmod 26$$

met $x,y \in Z_{26}$

Deze methode is gebaseerd op modulaire rekenkunde. Het Shift Cipher cryptosysteem is gedefinieerd over Z_{26}, met modulus 26, omdat er 26 letters in het Alfabet zijn. Het zou evengoed voor elke modulus m mogelijk kunnen zijn. (Stinson, 2006)

We gebruiken de Shift vercijfering om een gewone Nederlandse tekst te versleutelen. Hierbij linken we alfabetische karakters en restwaarden modulo 26 als volgt: A ↔ 0, B ↔ 1, C ↔ 2, D ↔3, …, Z ↔ 25.

0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**	**21**	**22**	**23**	**24**	**25**
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Een voorbeeld:
Stel de sleutel K voor de Shift Cipher is 10, en de plaintext is

ikwachtopdebusaandehalte

Eerst zetten we de plaintext om in een volgorde van natuurlijke gehele getallen. Hierbij maken we gebruik van de gespecificeerde correspondentie. Zo bekomen we het volgende resultaat:

8 10 22 0 2 7 19 14 15 3 4 1 20 18 0 0 13 3 4 7 0 11 19 4

Vervolgens tellen we 10 op bij elke waarde, terwijl we elke som verminderen met modulo 26:

18 20 6 10 12 17 3 24 25 13 14 4 2 10 10 23 13 14 17 10 21 3 14

Uiteindelijk converteren we deze volgorde van gehele getallen in alfabetische tekens. Dit geeft het volgende resultaat:

KSUGKMRDYZNOECKKXNORKVDO

Om deze ciphertext te ontcijferen zal persoon B deze tekst omzetten in een volgorde van cijfers, dan 10 van elk cijfer aftrekken en vervolgens de volgorde van cijfers omzetten in alfabetische tekens.

Om een cryptosysteem praktisch te gebruiken moet het voldoen aan volgende voorwaarden:

1. Elke encryptiefunctie e_k en elke decryptiefunctie d_k moeten efficiënt te berekenen zijn.
2. Een tegenstander mag de sleutel K niet kunnen achterhalen als hij de ciphertext ziet.

Het nadeel van deze Shift vercijfering is echter dat men ze gemakkelijk kan kraken door gebruik te maken van de *exhaustive key search*. Er zijn slechts 26 sleutels mogelijk. Dit maakt het gemakkelijk om elke decryptieregel te proberen totdat er een beduidende plaintext verkregen wordt. (Stinson, 2006)

3.1.2 De Substitutie cipher

Een ander bekend cryptosysteem is de substitutie cipher

Substitution cipher:
Laat P = C = Z_{26}. K bestaat uit alle mogelijke permutaties van de 26 symbolen 0,1,…,25. Voor elke permutatie $\pi \in$ K, definieer

$$e_\pi(x) = \pi(x)$$

en

$$d_\pi(y) = \pi^{-1}(y)$$

met π^{-1} de inverse permutatie van π

In het geval de Substitutie cipher nemen we voor zowel P als C het alfabet. Dit doen we omdat het gemakkelijker is om encryptie en decryptie te zien als een permutatie van alfabetische tekens.

a	**b**	**c**	**d**	**e**	**f**	**g**	**h**	**i**	**j**	**k**	**l**	**m**	**n**	**o**	**p**	**q**	**r**	**s**	**t**	**u**	**v**	**w**	**x**	**y**	**z**
X	N	Y	A	H	P	O	G	Z	Q	W	B	T	S	F	L	R	C	V	M	U	E	K	J	D	I

De decryptiefunctie is de inverse permutatie.

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
d	i	r	y	v	o	h	e	z	x	w	p	t	B	g	f	j	q	n	m	U	s	k	a	c	l

De shift cipher is een speciaal geval van de substitutievercijfering.

Deze twee soorten vercijfering zijn toepassingen van monoalfabetische cryptosystemen. Dit wil zeggen dat als er een sleutel gekozen wordt, elk alfabetisch teken gelinkt wordt aan een uniek alfabetisch teken. (Stinson, 2006)

In tegenstelling tot de shiftvercijfering heeft de substitutievercijfering veel meer mogelijke sleutels. Dit is echter nog geen garantie voor een betere beveiliging aangezien deze vercijfering via andere methodes ook gemakkelijk gekraakt kan worden. (Stinson, 2006)

3.1.3 De Vigenère vercijfering

Deze soort vercijfering is niet monoalfabetisch, maar polyalfabetisch. Het is genoemd naar Blaise de Vigenère, die in de 16^{de} eeuw leefde. Nog steeds gebruiken we het volgende systeem: A ↔ 0, B ↔ 1, …, Z ↔ 25. We associëren elke sleutel K met een alfabetische rij van lengte m. Dit noemt men het *keyword* of sleutelwoord. De Vigenère cipher versleutelt m alfabetische tekens tegelijk: elk plaintext element is equivalent met m alfabetische tekens.

Vigenère cipher:
Laat m een positief geheel getal zijn. Definieer $P = C = (Z_{26})^m$. Voor een sleutel $K = (k_1, k_2, \ldots, k_m)$, definieren we

$$e_k(x_1, x_2, \ldots, x_m) = (x_1 + k_1, x_2 + k_2, \ldots, x_m + k_m)$$

en

$$d_k(y) = (y_1 - k_1, y_2 - k_2, \ldots, y_m - k_m)$$

waar alle operaties uitgevoerd worden in Z_{26}

Een voorbeeld ter verduidelijking:

Stel dat m = 4 en het sleutelwoord roos is. De numerische equivalent van dit woord is K = (17, 14, 14, 18). Stel nu dat de plaintext de volgende rij is:

Ikwachtopdebusaandehalte

We zetten de plaintextelementen om in rest modulo 26. Schrijf ze in groepen van 6 en voeg dan het sleutelwoord modulo 26 toe:

8 10 22 0 2 7 19 14 15 3 4 1 20 18 0 0 13 3 4 7 0 11 19 4

8	10	22	0	2	7	19	14	15	3	4	1	20	18	0	0	13	3	4	7	0	11	19	4
17	14	14	18	17	14	14	18	17	14	14	18	17	14	14	18	17	14	14	18	17	14	14	18
25	24	4	18	19	21	7	6	6	17	18	19	11	6	14	18	4	17	18	25	17	25	7	22

De alfabetische equivalent van deze ciphervolgorde wordt dus als volgt:

ZYESTVHGGRSTLGOSERSZRZHW

Aangezien de Vigenère vercijfering een polyalfabetisch cryptosysteem is, is het sowieso moeilijker om de plaintext hiervan te achterhalen. (Stinson, 2006)

De kracht van deze vercijfering schuilt in het feit dat er voor elk plaintextelement meerdere ciphertextletters bestaan, één voor elke unieke letter van het sleutelwoord. De informatie over de letterfrequentie wordt verborgen, maar niet alle kennis van de plaintextstructuur gaat verloren. (Stinson, 2006)

Toch is ook dit systeem kwetsbaar voor cryptoanalyse. De sleutel en de plaintext bevatten namelijk dezelfde frequentiedistributie van letters. Hierop kan dus een statistische analyse worden toegepast. (Stinson, 2006)

3.1.4 De Hill cipher

Een andere polyalfabetisch cryptosysteem is de Hillvercijfering. Deze werd uitgevonden in 1929 door Lester S. Hill. Het idee achter deze Hillvercijfering is het vastleggen van m lineaire combinaties van de m alfabetische karakters voor één plaintextelement zodat m alfabetische karakters geproduceerd worden in één ciphertextelement. Bij deze Hillvercijfering kunnen we gebruik maken van een matrixnotatie. In het algemeen nemen we een m x m matrix K als sleutel. Hierdoor kunnen we $y = e_K(x) = (y_1, y_2, \ldots, y_m)$ berekenen.

$$(y_1, y_2, \ldots, y_m) = (x_1, x_2, \ldots, x_m) \begin{pmatrix} k_{1,1} & k_{1,2} & \ldots & k_{1,m} \\ k_{2,1} & k_{2,2} & \ldots & k_{2,m} \\ \ldots & \ldots & & \ldots \\ k_{m,1} & k_{m,2} & \ldots & k_{m,m} \end{pmatrix}$$

Hieruit kunnen we opmaken dat de ciphertext door middel van een lineaire transformatie uit de plaintext achterhaald kan worden. Om de matrix K te ontsleutelen gebruiken we de inverse matrix K^{-1}. De ciphertext wordt ontsleuteld door gebruik te maken van de vergelijking $x=y\,K^{-1}$.

Deze theorie kan beter begrepen worden aan de hand van een voorbeeld.

Hill cipher:

Laat $m \geq 2$ een positief geheel getal zijn. Laat $P = C = (Z_{26})^m$ en laat

$$K = \{m \text{ x } m \text{ inverteerbare matrices in } Z_{26}\}$$

Voor een sleutel K definiëren we

$$e_k(x) = xK$$

en

$$d_k(y) = yK^{-1}$$

waar alle operaties uitgevoerd worden in Z_{26}

Stel dat

$$K = \begin{pmatrix} 10 & 5 & 12 \\ 3 & 14 & 21 \\ 8 & 9 & 11 \end{pmatrix}$$

Det K = 7 mod 26. In Z_{26} kunnen we berekenen dat 7^{-1} mod 26 = 15. De *adjoint* matrix is

$$K_a = K^* = \begin{pmatrix} 17 & 1 & 15 \\ 5 & 14 & 8 \\ 19 & 2 & 21 \end{pmatrix}$$

Hieruit berekent men uiteindelijk de inverse matrix.

$$K^{-1} = 15K^* = \begin{pmatrix} 21 & 15 & 17 \\ 23 & 2 & 16 \\ 25 & 4 & 3 \end{pmatrix} = K^{-1} \bmod 26$$

Zoals eerder vermeld werkt encryptie bij de Hillvercijfering door de plaintext te vermenigvuldigen met matrix K. De decryptie vermenigvuldigt de ciphertext met de inverse matrix K^{-1}. (Stinson, 2006)

Stel dat men volgende tekst wil versleutelen: “paymoremoney” aan de hand van de onderstaande ecryptiesleutel:

$$K = \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 9 \end{pmatrix}$$

Beschouw de eerste drie letters van de plaintext P, A, Y. Vermits P = 15, A = 0 en Y = 24, kunnen deze letters worden voorgesteld door $\begin{pmatrix} 15 \\ 0 \\ 24 \end{pmatrix}$

Dan is $C = K \times P = \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 9 \end{pmatrix} \begin{pmatrix} 15 \\ 0 \\ 24 \end{pmatrix} = \begin{pmatrix} 375 \\ 819 \\ 486 \end{pmatrix} \bmod 26 = \begin{pmatrix} 11 \\ 13 \\ 18 \end{pmatrix}$ = LNS

Als we op deze manier doorgaan voor de overige plaintext-letters, wordt de ciphertext voor de hele plaintext LNSHDLEWMTRW.

Het zwakke punt van de Hill vercijfering is de lineariteit. Hierdoor kan de vercijfering vrij gemakkelijk gebroken worden met een bekende “plaintext-aanval”. De cryptanalist is dan in staat om zowel plaintextberichten als ciphertextberichten te onderscheppen en deze te gebruiken om geheime informatie te onthullen, zoals de geheime sleutel. (Stinson, 2006)

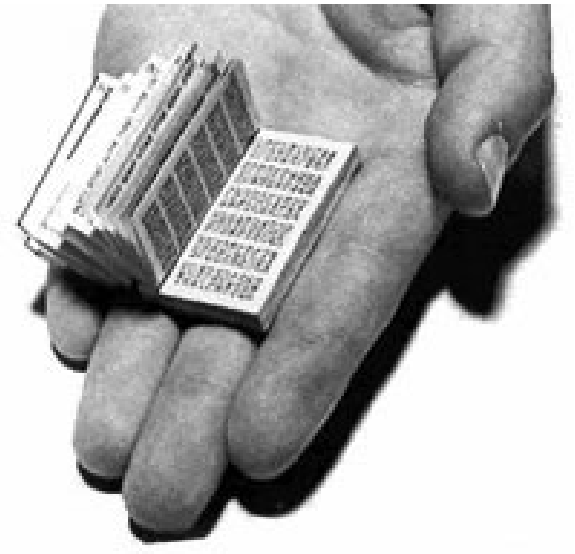
Een speciaal geval van deze Hill vercijfering is de permutatievercijfering.

3.1.5 De Vernamvercijfering

Met de technieken die voorafgingen zou men de vraag kunnen stellen of er wel veilige of onbreekbare codeermethodes bestaan. Op deze vraag moet inderdaad bevestigend geantwoord worden. De Vernamvercijfering of one time pad vercijfering is een methode die deze perfecte veiligheid bereikt. Perfecte veiligheid wil zeggen dat een luistervink geen informatie kan bekomen over de plaintext als hij enkel de ciphertext bekijkt. In 1917 werd dit one time pad beschreven door Gilbert Vernam. Het werd gebruikt in automatische encryptie en telegraafberichten. Het grote voordeel van de Vernamvercijfering is zijn eenvoud. Gilbert Vernam bedacht tijdens de 2e Wereldoorlog een versleutelingmethode die niet door de Duitsers, maar ook niet door iemand anders gekraakt kon worden. (http://www.pro-technix.com/information/crypto/pages/vernam_base.html, 2006)

Het Engelse woord "pad' staat voor een strook papier, de sleutel op het papier bestaat uit willekeurig gekozen letters of cijfers in een willekeurige volgorde, die gebruikt worden om de boodschap teken voor teken te wijzigen. Zender en ontvanger moeten dus allebei deze sleutel hebben. Elke letter uit het pad wordt maar één keer gebruikt. De zender moet letter voor letter de boodschap wijzigen, de ontvanger doet dat ook:

Figuur 3.2: Russisch one time pad, bemachtigd door de Engelse geheime dienst MI5



bron: http://www.pro-technix.com/information/crypto/pages/vernam_base.html (2006)

Bijvoorbeeld:

Klare tekst: hallolief

Sleutel: axybcyvwm

Geheim: icknrcave

Elke letter van het pad wijzigt precies een letter in de boodschap. Een a in het pad betekent dat de bijbehorende letter in de boodschap gewijzigd moet worden in de volgende letter in alfabetische volgorde, een b betekend dat de bijbehorende letter gewijzigd moet worden in de letter daaropvolgend in het alfabet, enzovoort. Omdat de letters in het pad willekeurig zijn is elk schema bruikbaar. (http://www.pro-technix.com/information/crypto/pages/vernam_base.html, 2006)

De versleutelde 'icknrcave' tekst kan dus elk negenletterig woord betekenen. Het verschil met de Caesarverschuiving is dat daar sprake is van regelmatige verschuiving: elke a wordt bijvoorbeeld een d. Bij Vernam wordt gebruik gemaakt van een eenmalige sleutel. Een a kan een d worden, maar ook een andere letter. (http://www.pro-technix.com/information/crypto/pages/vernam_base.html, 2006)

Tijdens de Eerste Wereldoorlog in 1917 nam Gilbert Vernam de taak op zich om een encryptiemethode uit te voeren die de Duitsers niet konden breken. Wat hij ontwierp is vandaag de dag nog steeds de enige bewezen onbreekbare encryptiemethode. Vergeleken met andere cryptosystemen is het heel eenvoudig. De Vernamvercijfering wordt ook wel het one time pad genoemd. Om dit one time pad te gebruiken zijn er twee kopieën van het pad of de sleutel nodig. Dit pad stelt willekeurige data voor. One time pads worden in paren gebruikt. Hoe meer kopieën van een gegeven pad, hoe groter de kans bestaat dat er één onderschept wordt. Dit eindigt vervolgens in het kraken van het systeem. (http://www.pro-technix.com/information/crypto/pages/vernam_base.html, 2006)

Eén kopie van het pad wordt bijgehouden door elke gebruiker. De sleutels moeten via een veilig kanaal uitgewisseld worden. Ze mogen slechts één keer gebruikt worden.

De boodschap en de sleutel worden gecodeerd in een binaire voorstelling. Elk karakter heeft een unieke combinatie van enen en nullen, die bits genoemd worden. Elke bit van elke letter in de plaintext wordt gecombineerd met het corresponderende bit van de letters in de sleutel. Hierbij maakt men gebruik van een transformatie die XOR (exclusie or) genoemd wordt. Dit systeem gebruikt twee bits als input. De output hiervan wordt één enkele bit volgens het volgende schema:

Tabel 3.1: XOR-tabel

Input bits		Output bit
Bericht	Pad	
0	0	0
0	1	1
1	0	1
1	1	0

Bron: http://www.pro-technix.com/information/crypto/pages/vernam_base.html (2006)

Deze operatie wordt op elke letter in de volgorde uitgevoerd.

Een klein voorbeeld:
Veronderstel dat men de volgende boodschap wil coderen: “begin at 17.30” gebruik makend van de sleutel of pad “#/KBZaF>TQV^Nc”. Eerst worden alle bits van “b” getransformeerd met alle bits van “#”. Dit produceert het binaire patroon voor karakter A:

Bit volgorde voor “b”	Bit volgorde voor “#”	XOR “A”
1	0	1
1	1	0
0	0	0
0	0	0
0	0	0
1	1	0
0	1	1

Hetzelfde proces wordt herhaald voor de volgende letters. “e” en “/” worden getransformeerd tot “J”
“g” en ”K” worden getransformeerd tot “,” enz.
De voltooide ciphertext ziet er als volgt uit: “AJ,+4A'Jt`ap}S”.

De belangrijkste eigenschap van de Vernam vercijfering is de willekeurigheid van de pad-volgorde. Een gebeurtenisvolgorde kan slechts echt willekeurig zijn als het onmogelijk is om de volgende gebeurtenis in de volgorde te kennen.

De code van Vernam is slechts perfect veilig op voorwaarde dat:

1. De sleutel volledig willekeurig gegenereerd is.
2. De sleutel even lang is als de boodschap.
3. De sleutel slechts éénmaal gebruikt wordt (*one time*).

Indien aan deze drie voorwaarden voldaan is, wordt het onmogelijk om de oorspronkelijke tekst te reconstrueren. Vandaar dat de Vernam methode een garantie is voor perfecte veiligheid. We kunnen zeggen dat het Vernam algoritme een onvoorwaardelijk veilig cryptosysteem is. Dit wil zeggen dat de door het systeem gegenereerde ciphertext onvoldoende informatie bevat om de overeenkomstige plaintext vast te stellen. Ongeacht hoeveel tijd de tegenpartij heeft, deze is niet in staat de ciphertext te ontcijferen. De meeste encryptiealgoritmen zijn niet onvoorwaardelijk veilig, maar rekenveilig. Een systeem is rekenveilig als de kosten van het breken van de code de waarde van de versleutelde informatie overstijgen en als de tijd die nodig is om de code te breken langer is dan de periode dat de informatie bruikbaar is. (Stallings, 2000)

3.1.6 DES-encryptie

DES is het meest gebruikte blokalgoritme. Dat komt vooral omdat het zowat het enige algoritme is dat vrij in en uit de VS geëxporteerd mag worden. Hoewel het algoritme al enige tijd geleden gekraakt is, wordt het nog steeds op vrij grote schaal toegepast in allerlei producten. DES is gebaseerd op het in de jaren zeventig ontwikkelde algoritme “LUCIFER” van IBM en ontwikkeld door het NIST, een

Amerikaans technologie-instituut. (http://jelmer.vernstok.nl/publications/cryptografie.pdf#search=%22Werking%20van%20DES%20algoritme%22, 2006)

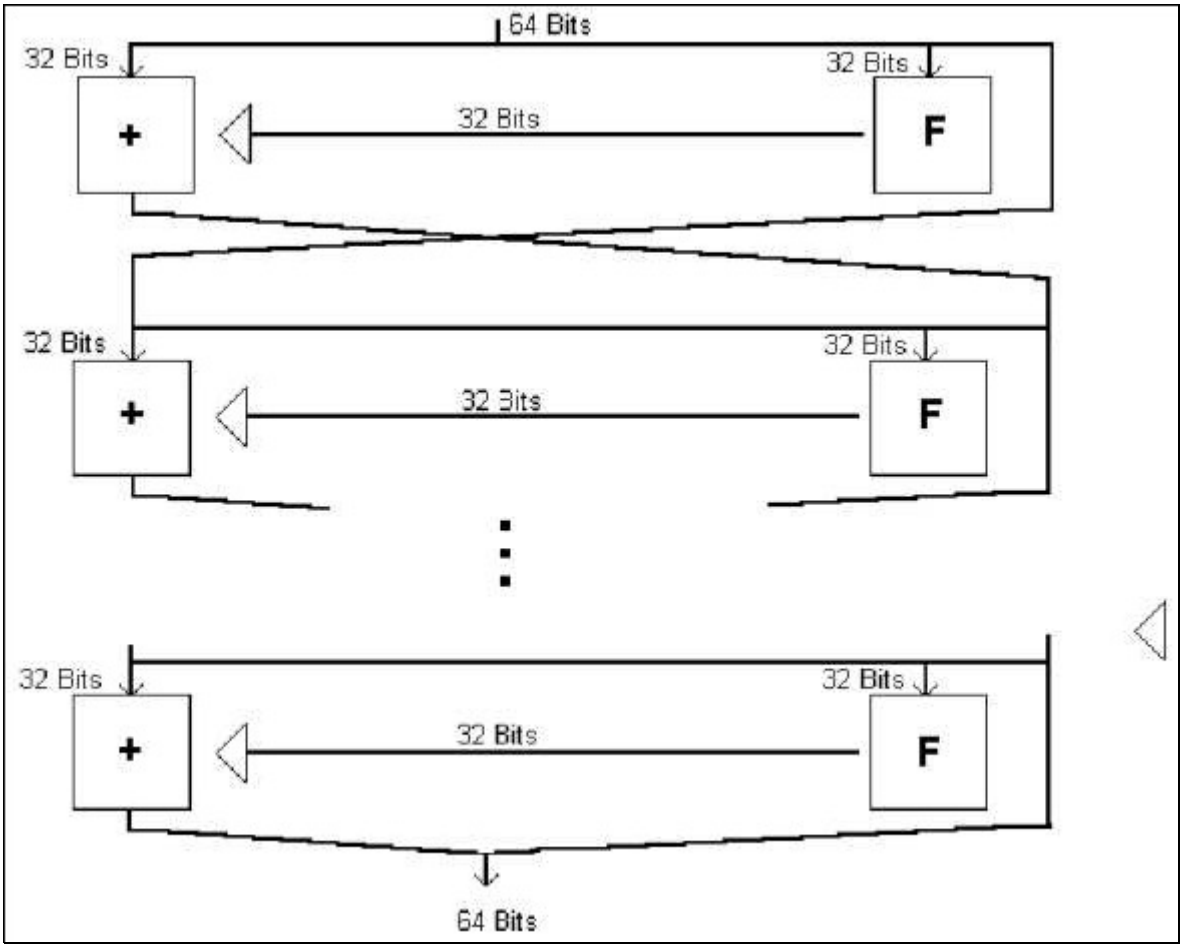
DES werkt met sleutels van 64 bits, maar elke achtste bit wordt gebruikt ter controle. Dat betekent dus dat er (264−8 = 256 =) 72057594037927936 mogelijke sleutels zijn. DES werkt, in tegenstelling tot de voorgaande algoritmes niet door de sleutel “op te tellen” bij de plaintext. DES werkt op blokken van 64 bits. DES werkt niet met optellen of aftrekken, maar met XOR(N). De XOR van twee waardes is 1 als precies één van beiden gelijk is aan 1. Wanneer beiden gelijk zijn aan 0 of beiden gelijk zijn aan 1 is de XOR van deze twee waarden 0. (Zie tabel 2.1) (http://jelmer.vernstok.nl/publications/cryptografie.pdf#search=%22Werking%20van%20DES%20algoritme%22, 2006)

DES is een algoritme dat gebruik maakt van een zogenaamd “Feistel Netwerk”. DES werkt in zestien rondes waarbij in elke ronde steeds de beide helften van het blok verwisseld wordt en waarbij op de linker encryptie toegepast wordt:

$L_i = R_i{-}1$

Voor de rechterkant gebruikt men een functie van een Feistel-netwerk: deze gebruikt een sleutel en een deel van het blok zelf:

Figuur 3.3: Uitvoeren van DES



Bron: http://jelmer.vernstok.nl/publications/cryptografie.pdf (2006)

Tabel 3.2: Opsplitsing datareeks DES

Nr.	Bits					
1	32	1	2	3	4	5
2	4	5	6	7	8	9
3	8	9	10	11	12	13
4	12	13	14	15	16	17
5	16	17	18	19	20	21
6	20	21	22	23	24	25
7	24	25	26	27	28	29
8	28	29	30	31	32	1

Bron: http://jelmer.vernstok.nl/publications/cryptografie.pdf (2006)

$$Ri = L_i \otimes f(R_{i-1}, K_i)$$

Ontcijferen van dit gedeelte kan ook weer door middel van XOR gebeuren, aangezien a $\otimes$ b $\otimes$ b = a. Wat f dus ook voor functie is, ontcijferen kan altijd met dezelfde functie als vercijferen (zolang de sleutel bekend is). (http://jelmer.vernstok.nl/publications/cryptografie.pdf#search=%22Werking%20van%20DES%20algoritme%22, 2006)

De functie f uit het bovenstaande stuk krijgt een 32-bits lange datareeks (R_i–1) en een 56-bits lange sleutelreeks (K_i) mee. De 32 bits uit de datareeks worden opgesplitst in blokjes van acht blokjes van 6 bits, met overlap. De eerste twee bits zijn steeds gemeenschappelijk met het voorgaande blokje en de laatste twee zijn steeds gemeenschappelijk met het nakomende blokje. (Zie de tabel 3.2) De 48-bits lange reeks die op deze manier ontstaat wordt ge-XOR-d met de 48 bits uit de 56-bits lange sleutel. (http://jelmer.vernstok.nl/publications/cryptografie.pdf#search=%22Werking%20van%20DES%20algoritme%22, 2006)

Nu wordt er gebruik gemaakt van de zogenaamde “S-boxen”: acht verschillende tabellen waarin de eerste en de zesde bit uitstaan tegen de tweede tot en met de vijfde bit. Wiskundig genoteerd: $S_1(b_1b_6, b_2b_3b_4b_5)$. Voor elk van bovenstaande blokjes wordt een andere tabel gebruikt.

De 32 bits die uit de acht S-boxen komen worden uiteindelijk in de volgende volgorde gezet:

16	7	20	21	29	12	28	17	1	15	23	26	5	18	31	10
2	8	24	14	32	27	3	9	19	13	30	6	22	11	4	25

Deze tabel is de zogenaamde “P-box”.

Aangezien de sleutel van DES niet zo heel erg lang is, zijn er veel bedrijven die tegenwoordig gebruik maken van “triple DES”. De DES wordt drie keer toegepast in plaats van één keer. Hiervoor zijn twee sleutels nodig, en de procedure werkt als volgt:

1. Versleutel met k_1
2. Ontcijfer met k_2
3. Versleutel met k_1

Bij het ontcijferen geldt precies de omgekeerde procedure:

1. Ontcijfer met k_1
2. Versleutel met k_2
3. Ontcijfer met k_1

(http://jelmer.vernstok.nl/publications/cryptografie.pdf#search=%22Werking%20van%20DES%20algoritme%22, 2006)

Een wenselijke eigenschap van elk encryptiealgoritme is dat een kleine verandering in de plaintext of de sleutel een grote wijziging in de ciphertext veroorzaakt. Dit wordt het *lawine-effect* genoemd. DES vertoont een sterk lawine-effect. (Stallings, 2000, p.81)

Conventionele encryptie werkt alleen als de twee partijen dezelfde sleutel gebruiken en als die sleutel wordt beveiligd tegen toegang door anderen. Bovendien is het meestal gewenst vaak van sleutel te wisselen om ervoor te zorgen dat er zo weinig mogelijk data in gevaar wordt gebracht wanneer de aanvaller de sleutel te weten is gekomen. (Stallings, 2000, p. 162)

Hoofdstuk 4 Asymmetrische encryptie

In het klassieke model van cryptografie kiezen persoon A en B hun eigen sleutel. Deze sleutel K is geheim. Een nadeel van dit cryptosysteem met symmetrische sleutel bestaat in het feit dat er al communicatie moet geweest zijn tussen persoon A en B via een veilig kanaal, alvorens men ciphertext kan uitwisselen. (Stinson, 2006)

Het idee achter een cryptosysteem met een publieke sleutel is dat het mogelijk is om een systeem te vinden waarbij het onmogelijk is om d_K te vinden als men e_K kent. Dit zou van e_K een publieke sleutel maken die gemakkelijk uitgewisseld zou kunnen worden. Het voordeel van een systeem met publieke sleutels is dat persoon A een gecodeerd bericht kan zenden naar persoon B zonder op voorhand met elkaar te communiceren door gebruik te maken van de publieke encryptie e_K. Persoon B zal de enige persoon zijn die de ciphertext kan ontcijferen met behulp van de decryptie d_K. d_K wordt de private sleutel genoemd. (Stinson, 2006)

Stallings (2006, p. 189) vermeldt dat public-key cryptografie een radicale breuk betekent met het verleden. Public-key algoritmen zijn gebaseerd op wiskundige functies in plaats van op substitutie en permutatie. Het gebruik van twee sleutels heeft diepgaande consequenties op het gebied van vertrouwelijkheid, sleuteldistributie en authenticatie.

Public-key algoritmen steunen op één sleutel voor encryptie en op een andere, maar gerelateerde sleutel voor decryptie. Een belangrijke eigenschap van deze algoritmen is dat het rekenkundig ondoenbaar is de decryptiesleutel te bepalen als alleen kennis van de cryptografische algoritmen en de encryptiesleutel aanwezig is. (Stallings, 2006, p. 191)

4.1 Het RSA-Systeem

RSA is een asymmetrisch encryptiealgoritme dat veel gebruikt wordt voor elektronische handel (zoals bijvoorbeeld de beveiliging van transacties). Het algoritme werd in 1977 ontworpen door Ron Rivest, Adi Shamir en Len Adleman (vandaar de afkorting RSA).

Clifford Cocks, een Britse wiskundige, die voor het Government Communications Headquarters werkte, heeft in 1973 een gelijkaardig algoritme beschreven in een intern document, dat pas in 1997 boven water is gekomen omdat het als top-secret geclassificeerd was.

De veiligheid van RSA steunt op het probleem van de ontbinding in factoren (bij heel grote getallen): op dit moment is het bijna onmogelijk de twee oorspronkelijke priemgetallen p en q te achterhalen als alleen p*q bekend is en p en q groot genoeg zijn. Het zou te veel tijd in beslag nemen. Nieuwe ontwikkelingen op dit gebied zouden RSA onbruikbaar kunnen maken. (http://nl.wikipedia.org, 2006)

1. Het sleutelgeneratiealgoritme

   a. Genereer twee grote willekeurige priemgetallen p en q, zodat hun product p x q = n de voorgenomen bitlengte heeft.
   b. Bereken n = p x q. n is de modulus. Bereken eveneens $\varphi(n) = (p-1)(q-1)$.
   c. Kies een geheel getal e zodat de ggd(e, φ(n)) = 1 met $1 < e < \varphi(n)$. e is de publieke component.
   d. Bereken de geheime exponent d zodat $d = e^{-1} \bmod \varphi(n)$ of $e \times d = 1 \bmod \varphi(n)$ met $1 < d < \varphi(n)$. Hierbij wordt gebruik gemaakt van het uitgebreide Euclidische algoritme om de grootste gemene deler (ggd) te berekenen
   e. De publieke sleutel wordt gegeven door (n,e) en de private sleutel door (φ(n),d). De waarden van p, q en φ(n) worden geheim gehouden.

2. Encryptie

Stel dat persoon A een bericht wil verzenden naar persoon B. Persoon A bekomt de publieke sleutel van persoon B, (n, e). Persoon A vormt de plaintext P om tot een ciphertext C aan de hand van volgende formule: $C = P^e \bmod n$. Vervolgens stuurt hij deze ciphertext C naar persoon B.

3. Decryptie

Persoon B ontvangt de door persoon A verzonden ciphertext. Hij gebruikt zijn eigen private sleutel (φ(n),d) om de plaintext te berekenen. De gebruikte formule is: $P = C^d \bmod n$. Zo bekomt hij de plaintext P.

4. Digitale ondertekening

Persoon A creëert een *message digest* m (zie paragraaf 6.3) door een hashfunctie toe te passen op de te verzenden informatie. Hij gebruikt zijn private sleutel (φ(n), d) om de handtekening te berekenen: $s = m^d \bmod n$. Vervolgens zendt hij deze digitale handtekening naar persoon B.

5. Handtekeningverificatie

Persoon B ontvangt de door A verzonden handtekening. Hij gebruikt de publieke sleutel (n,e) van persoon A om $m = s^e \bmod n$ te berekenen. Vervolgens past hij dezelfde hashfunctie toe als A op de eveneens meegezonden plaintext. Als beide message digest overeenstemmen is de handtekening juist.

6. Voorbeeld

a. Genereer priemgetallen p = 137 en q = 131.
b. n x p = 137 x 131 = 17947
   φ(n) = (p – 1)(q – 1) = 136 x 130 = 17680
c. Kies e = 3. GGD (e, p – 1) = GGD (3, 136) = 1, GGD (e, q – 1) = GGD (3, 130) = 1.
d. Bereken $d = e^{-1} \bmod \varphi(n) = 3^{-1} \bmod 17680 = 11787$
e. Dus is de publieke sleutel (17947, 3) en de private sleutel (17680, 11787).

7. Sleutellengte

De sleutellengte voor een veilige RSA transmissie is meestal 1024 bits. Indien men twijfelt aan de veiligheid kan men natuurlijk ook met nog langere sleutels werken, zoals 2048 of zelfs 4096 bits. Praktisch gezien is het tot op heden voor gewone mensen nog steeds onmogelijk om zelfs een 512 bits sleutel te kraken. Enkel met gebruik van supercomputers is het mogelijk deze codes te kraken. Deze computers worden door het NSA en nog andere veiligheidsdiensten gebruikt. Met behulp van een brute kracht aanval slagen deze computers erin de 512 bit code binnen een redelijke tijd te kraken. Hoe langer de informatie is die geheim moet gehouden worden, hoe langer de sleutel moet zijn.

8. Veiligheid

Veronderstel dat persoon C, een luistervink, de publieke sleutel (n,e), en de cijfertekst C onderschept. Hij kan niet rechtstreeks aan d geraken, omdat persoon A dat geheim houdt. De meest voor de hand liggende manier voor persoon C om n te vinden uit C, is om n in de factoren p en q te ontbinden, zodat ze $\varphi(n) = (p-1)(q-1)$ kan berekenen en d kan vinden uit e. Er is nog geen polynomische tijdmethode gevonden om getallen in factoren te ontbinden met een gewone computer (de benodigde tijd wordt veel sneller groter dan lineair bij groter wordende getallen), maar het is niet bewezen dat er geen bestaat.
(http://nl.wikipedia.org, 2006)

Het is ook niet bewezen dat de enige manier om n te uit C te berekenen, is om n in factoren te ontbinden, maar er is nog geen gemakkelijkere manier ontdekt (tenminste geen publiekelijk gekende). Daarom wordt algemeen verondersteld dat persoon C het bericht niet kan terugvinden als n groot genoeg is.
(http://nl.wikipedia.org, 2006)

Als n 256 bits of korter is, kunnen de factoren in een paar uur gevonden worden met een personal computer, gebruik makende van software die vrij toegankelijk is op het Internet. Als n 512 bits of korter is, kan de ontbinding uitgevoerd worden door enkele honderden computers (in een aanvaardbare tijd). Het is tegenwoordig aan te raden n ten minste 1024 bits lang te kiezen.
(http://nl.wikipedia.org, 2006)

In 1993 heeft Peter Shor aangetoond dat een kwantumcomputer in principe de factorisatie in polynomiale tijd zou kunnen uitvoeren. Als (of wanneer) kwantumcomputers werkelijkheid worden, zal Shors algoritme RSA en andere soortgelijke algoritmes onbruikbaar maken. Als een efficiënte methode voor ontbinding in factoren met een gewone computer zou worden gevonden, of als een kwantumcomputer zou worden gemaakt, dan kunnen nog langere sleutels een tijdelijke oplossing bieden, maar zo'n veiligheidslek in RSA zou wel retroactief zijn: de publieke sleutel en de cijfertekst kunnen worden bijgehouden totdat het mogelijk wordt om het bericht te ontcijferen. Daarom is het niet veilig om lange-termijn geheimen uit te wisselen met RSA. (http://nl.wikipedia.org, 2006)

9. Sleutelverdeling

Zoals bij alle encryptiemethoden, is het belangrijk hoe de publieke sleutels verspreid worden. We moeten ons bewust zijn van de mogelijkheid van een *man-in-the-middle attack*. Veronderstel dat persoon C de communicatie tussen persoon A en persoon B kan onderscheppen. Hij ontvangt dan een publieke sleutel van persoon A, maakt zelf een nieuwe publieke en geheime sleutel en stuurt zijn eigen publieke sleutel naar persoon B, die denkt dat hij de publieke sleutel van persoon A ontvangt. Dan kan ze verdere berichten van persoon B (vercijferd met haar publieke sleutel) ontvangen, ontcijferen met haar geheime sleutel, en (eventueel veranderd) weer geëncrypteerd met de eerder ontvangen publieke sleutel naar persoon A sturen (persoon A denkt dat het bericht rechtstreeks van persoon B komt). In principe kunnen persoon A en persoon B niet merken dat persoon C ertussen zit. Verdedigingen tegen zo'n aanval zijn meestal gebaseerd op digitale certificaten of andere onderdelen van een publieke sleutel infrastructuur. Uiteraard is de beste oplossing dat persoon A en persoon B de sleutels vergelijken tijdens een "echte" ontmoeting (als dat mogelijk is). (http://nl.wikipedia.org, 2006)

In hoofdstuk 7 wordt er verder ingegaan op de verschillende types van digitale handtekeningen. De types die besproken zullen worden:

1. Enkel betrouwbaarheid is belangrijk
2. Enkel onweerlegbaarheid is belangrijk
3. Zowel betrouwbaarheid als onweerlegbaarheid zijn belangrijk

De schema’s met asymmetrische encryptie bevinden zich in hoofdstuk zes en zeven.

Hoofdstuk 5 Vergelijking van symmetrische en asymmetrische encryptie

In hoofdstuk vijf wordt symmetrische encryptie in het kort vergeleken met asymmetrische encryptie. Vooral de verschillen in sleutelgrootte en -lengte worden aangehaald.

5.1 Algemeen

Het verschil tussen symmetrische en asymmetrische encryptie situeert zich in het aantal sleutels. Bij symmetrische encryptie gebruikt men slechts één sleutel. Bij asymmetrische encryptie gebruikt men twee sleutels, één private en één publieke sleutel.

Bij symmetrische encryptie beschikken verzender en ontvanger allebei over dezelfde sleutel. De sleutel waarmee encryptie wordt uitgevoerd, is dezelfde sleutel als waarmee decryptie wordt uitgevoerd.

Deze sessiesleutel is een geheime sleutel. In onderstaande tabel werd het aantal deelnemers aan zo een sessie vergeleken met het aantal benodigde sleutels.

Tabel 5.1: Aantal benodigde sleutels symmetrische encryptie

Symmetrische Encryptie				
Deelnemers	2	4	6	18
Sleutels	1	6	28	120

Bron: http://infolab.uvt.nl/ (2006)

Uit deze tabel kan men afleiden dat het beheer van sleutels onpraktisch wordt als het aantal deelnemers groot is. Het aantal sleutels is een kwadratische functie van het aantal deelnemers. Als n het aantal deelnemers is, is het aantal benodigde sleutels n(n-1)/2. (http://infolab.uvt.nl/, 2006)

Het probleem van deze methode is dat de veiligheid van de sleutel niet langer kan worden gegarandeerd als de sleutel niet persoonlijk overgedragen wordt. Om dit probleem op te lossen werd de asymmetrische methode ontwikkeld. (http://infolab.uvt.nl/, 2006)

Bij asymmetrische encryptie wordt gebruik gemaakt van een sleutelpaar. Hierbij wordt de publieke sleutel openbaar gemaakt. Dit heeft echter geen invloed op de veiligheid omdat het onmogelijk geacht wordt uit de publieke sleutel (public key) de private sleutel (secret key) te reconstrueren en andersom. De private sleutel is zoals het woord het zelf zegt geheim. (http://infolab.uvt.nl/, 2006)

Deze techniek wordt publieke sleutel cryptografie genoemd omdat ieder deelnemend persoon over een publieke sleutel beschikt. Het is mogelijk om een geheim bericht te sturen naar ieder persoon omdat men over zijn publieke sleutel beschikt. In onderstaande tabel wordt het aantal deelnemers vergeleken met het aantal benodigde sleutels bij asymmetrische encryptie (http://infolab.uvt.nl/, 2006):

Tabel 5.2: Aantal benodigde sleutels asymmetrische encryptie

Asymmetrische Encryptie				
Deelnemers	2	4	6	18
Sleutels	2	4	6	18

Bron: http://infolab.uvt.nl/ (2006)

De zender gebruikt de publieke sleutel van de ontvanger om het bericht te versleutelen. De ontvanger kan met zijn eigen private sleutel het bericht dan ontcijferen. (zie hoofdstuk 6) (http://infolab.uvt.nl/, 2006)

Het probleem van de sleuteldistributie is met de komst van de asymmetrische sleutel ook uit de wereld: de sleutel hoeft niet veilig overgebracht te worden; de publieke sleutels moeten juist zo bereikbaar mogelijk gemaakt worden. Tegelijkertijd geldt dat ontcijferen met een publieke sleutel niet kan omdat kennis van de publieke sleutel niet zal helpen bij het ontcijferen.

Tabel 5.3: Voor- en nadelen van symmetrische en assymetrische algoritmen

	Symmetrische algoritmen	Asymmetrische algoritmen
Voordelen	– Snelle vercijfer- en ontcijfermethode door een relatief minder rekenintensieve methode en de mogelijkheid om relatief kleinere sleutels te gebruiken. – Veelal transparant voor gebruiker. Door gebruik van slechts één en dezelfde sleutel kan dit vaak in een applicatie worden geïntegreerd. – Relatief kleine sleutellengte is voldoende voor een hoge mate van veiligheid. – Relatief eenvoudig te realiseren in hardware (cryptobox).	– Bij een grote groep gebruikers of systemen blijft het beheer van de sleutels relatief eenvoudig, schaalbaar en beheersbaar. Het aantal benodigde sleutels is recht evenredig met het aantal gebruikers of systemen. Door het public key mechanisme kan de publieke sleutel aan derden worden verzonden zonder verlies van vertrouwelijkheid en authenticiteit. – Kan eveneens worden gebruikt voor het plaatsen en verifiëren van digitale handtekening. – Digitale handtekening krijgt snel een juridisch volwaardige status.
Nadelen	– Bij een grote populatie (gebruikers of systemen) is een relatief groot aantal verschillende sleutels nodig om een voldoende hoog betrouwbaarheidsniveau te behalen. (het aantal sleutels neemt kwadratisch toe met het aantal gebruikers of systemen) – Het beheer en de distributie van deze grote aantallen sleutels (zoals hierboven omschreven) wordt al snel zeer complex. – Door minder rekenintensieve vercijfering heeft een bruteforce aanval sneller resultaat dan bij asymmetrische vercijfering.	– Rekenintensieve vercijfering (factor 1000 langzamer dan symmetrische vercijfering). – Extra maatregelen dienen te worden genomen om de authenticiteit van de eigenaar van de publieke sleutel vast te stellen. – Relatief grote sleutellengte noodzakelijk voor een hoge mate van veiligheid.

Bron: https://www.platforminformatiebeveiliging.nl/tikiwiki/ (2006)

5.2 Sleutellengte

De sleutellengte speelt een belangrijke rol in de betrouwbaarheid van de vercijfering. Een te korte sleutellengte kan de betrouwbaarheid nadelig beïnvloeden. Algemeen kan men stellen dat de inspanning die verricht moet worden om een sleutel te achterhalen exponentieel groeit met de sleutellengte. Zoals reeds eerder vermeld moet er wat betreft de sleutellengte rekening gehouden worden met de gekozen vercijfermethodes. Bij de symmetrische methodes kan de sleutellengte beduidend korter zijn (3DES bijvoorbeeld 168 bits) dan bij de asymmetrische methoden (RSA 2048 bits) om een vergelijkbare betrouwbaarheid te garanderen. De oorzaak voor dit fenomeen kan men verklaren door te kijken naar de wiskundige basis van de asymmetrische methoden. Hierbij moeten zeer grote priemgetallen gebruikt worden of beschrijvingen van grote elliptische krommen. (Schneier, 1996)

De rekenkracht die nodig is om een sleutel te kraken neemt exponentieel toe met de sleutellengte. Dit kan zeer belangrijk zijn bij de keuze van een sleutellengte. Het is dus eveneens belangrijk om de verwachte levensduur van een encryptietoepassing te kennen. Hoe langer deze verwachte levensduur is, hoe langer de gewenste sleutel dient te zijn. De schattingen van de levensduur van een bepaalde sleutellengte worden berekend op basis van de hiervoor genoemde *brute force* aanvallen (alle mogelijke sleutels worden uitgeprobeerd). Bij nieuwe wiskundige mogelijkheden of een doorbraak in de techniek kan de gekozen sleutellengte eerder te kort blijken. (Schneier, 1996)

Tabel 5.4: Sleutellengte versus bitsgrootte

Sleutellengte vs bitsgrootte					
	Aantal Bits Keylengte				
Symmetrische Encryptie	56	64	80	112	128
Asymmetrische Encryptie	384	512	768	1792	2304

bron: Schneier, Applied Cryptography, 1996

In bovenstaande tabel is duidelijk te zien dat voor dezelfde cryptografische sterkte bij

asymmetrische encryptie een veel langere sleutel nodig is dan bij symmetrische encryptie.

Hoofdstuk 6 Wiskundige achtergrond

In hoofdstuk zes worden de wiskundige begrippen beschreven die de basis vormen voor cryptologie. Deze begrippen zijn relatief eenvoudig te verstaan, maar ze zijn weinig gekend. Een bedenking hierbij is dat men deze begrippen misschien reeds in de humaniora moet invoeren.

6.1 One way function

Een one way functie is een functie die gemakkelijk te berekenen is, maar die niet te inverteren is. Dus het is eenvoudig om voor elke $x \in X$, $y = f(x)$ te berekenen. Het is echter bijna onmogelijk om vertrekkende van $y = f(x)$ en de kennis van f, voor een gegeven andere $y' \in Y$, $x' = f^{-1}(y')$ te bepalen. De inverse functie kan bijna nooit met weinig rekenwerk gevonden worden. (A.J. Menezes & P.C. Van Oorschot & S.A. Vanstone, 2001, p.9)

Een functie f is een one way functie als:

1. de beschrijving van f publiekelijk gekend is en geen geheime informatie vereist voor zijn uitvoering
2. gegeven x, f(x) gemakkelijk te berekenen is
3. gegeven y, het moeilijk is een x te vinden zodat f(x) = y

(http://mathworld.wolfram.com/, 2006)

6.1.1 Voorbeelden

1. Factorprobleem: f(p,q) = p x q voor willekeurig gekozen priemgetallen p, q

2. Discreet logaritmeprobleem: f(p,g,x) = (p, g, g^x (mod p), voor g een generator van Z^*_p, voor een willekeurig priemgetal p.

3. Discreet wortelprobleem: f(p,q,e,y) = (p x q, e, y^e (mod p x q) voor y $\in$ Z^*_{pq} , e $\in$ Z_{pq} en relatief priem voor (p – 1)(q – 1), en p en q zijn priemgetallen. Deze functie staat ook beter bekend als RSA encryptie.

Het beeld van x bij de functie f(x) = x^e (mod m) is zelfs voor grote waarden van e en m vrij eenvoudig uit te rekenen, met behulp van een computer. De inverse van f(x) = x^e (mod m) kan echter zeer moeilijk te bepalen zijn. Meestal kiest men voor m een product van twee hele grote priemgetallen. Om de inverse van f te bepalen heb je in ieder geval een ontbinding van m in priemfactoren nodig. Deze ontbinding in priemfactoren is heel erg complex en bijna onmogelijk voor hele grote priemgetallen.

One way functies kunnen enerzijds opgesplitst worden in *trapdoor* one way functies, ook wel bifuncties genoemd en anderzijds *hash* one way functies of meerduidige one way functies. Bij bifuncties is inverteren onmogelijk, tenzij men de trapdoor kent. Hash functies zijn botsingsvrij. De inverse van een hashfunctie bestaat niet.

6.2 Trapdoor one way function

Een trapdoor one way functie is een one way functie waarbij de inverse makkelijk te berekenen valt als er extra informatie gegeven wordt (de trapdoor) die het mogelijk maakt om de inverse functie te berekenen. Het wordt bijgevolg mogelijk om voor elke gegeven y $\in$ Y een x $\in$ X te vinden zodat f(x) = y. (A.J. Menezes & P.C. Van Oorschot & S.A. Vanstone, 2001)

Een functie f: $(0,1)^{l(n)}$ x $(0,1)^n$ → $(0,1)^{m(n)}$ is een trap door one way functie als:

1. het een one way functie is
2. Voor een vaste publieke sleutel y $\in$ $(0,1)^{l(n)}$, f(x,y) wordt gezien als een functie $f_y(x)$ van x die n bits voorstelt ten opzichte van m(n) bits. Hiervoor bestaat een efficiënt algoritme dat na ingave van (y, $f_y(x)$, z) een x' produceert zodat $f_y(x') = f_y(x)$ voor een trapdoor sleutel z $\in$ $(0,1)^{k(n)}$.

(http://mathworld.wolfram.com/, 2006)

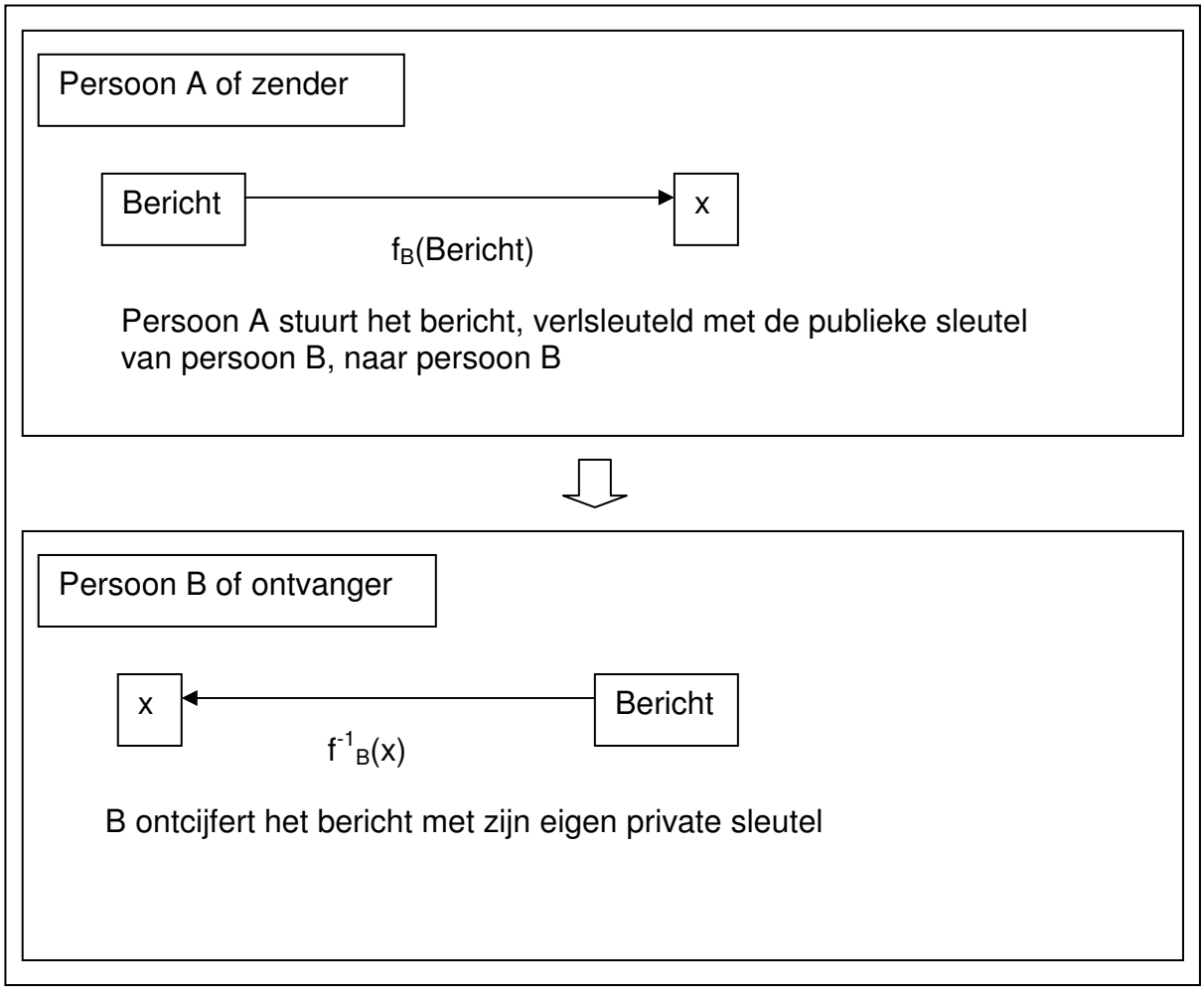
Men kan niet met zekerheid zeggen of er wel degelijk echte one way functies bestaan. Niemand heeft tot nu toe het bestaan van zulke functies bewezen. (A.J. Menezes & P.C. Van Oorschot & S.A. Vanstone, 2001, p.9)

Publieke sleutel cryptosystemen zijn gebaseerd op deze one way functies.

6.2.1 Voorbeeld

Stel dat persoon A een geheim bericht naar persoon B wil sturen. Hiervoor kiest persoon B eerst zijn one way function f_B, waarvoor hij alleen de inverse f^{-1}_B kent. Deze one way functie wordt de publieke sleutel genoemd en mag door iedereen gekend zijn. De inverse functie wordt de private sleutel genoemd en is enkel gekend door de ontwerper ervan. Persoon A kan dan met de publieke sleutel van persoon B het bericht vercijferen en versturen. Persoon A zendt dus naar persoon B: $x = f_B$ (bericht). Omdat enkel persoon B de overeenkomstige private sleutel kent, kan niemand anders dan persoon B het bericht ontcijferen. Enkel persoon B kan het bericht = f^{-1}_B (x) terugvinden. Doordat de publieke sleutel een one way functie is, kan niemand die in het bezit is van de publieke sleutel hieruit de private sleutel afleiden. De one way functie maakt het omgekeerde proces immers zeer moeilijk.

Figuur 6.1: One way functie, principe



6.3 Hash functie

Een hash functie is een transformatie die een input m (willekeurige grootte) opneemt en een reeks van vaste lengte produceert die h genoemd wordt: h = H(m) (http://www.rsasecurity.com/rsalabs/node.asp?id=2176, 2006). De hashwaarde h is dus het resultaat van het omzetten van een bericht van willekeurige grootte in een reeks met een vaste, meestal korte lengte. Men bekomt steeds hetzelfde resultaat als dezelfde hash functie wordt gebruikt op eenzelfde bericht. Als het bericht verandert, zal ook de hashwaarde veranderen. Er zijn namelijk oneindig veel berichten die dezelfde hashwaarde genereren, maar liefst zijn er geen twee zinvolle berichten bij. Uit de hashwaarde kan het bericht niet berekend worden. Een andere benaming voor de hashwaarde is message digest. Uit de message digest kan men

noch de hash functie noch het bericht afleiden. (http://www.cacr.math.uwaterloo.ca/hac/about/chap9.pdf, 2006)

Wanneer hash functies gebruikt worden in cryptosystemen moeten ze voorzien zijn van enkele extra eigenschappen:

1. De input kan een willekeurige lengte hebben
2. De output heeft een vaste lengte
3. H(x) is relatief makkelijk te berekenen voor elke x-waarde
4. H(x) is een meerduidige one-way functie
   Dit wil zeggen dat
5. $H^{-1}(x)$ bestaat zeer moeilijk te berekenen is.
6. H(x) is botsingsvrij.

Onder botsingen verstaan we twee of meer zinvolle plaintexten die dezelfde hash krijgen. (http://www.rsasecurity.com/rsalabs/node.asp?id=2176 en www.digitalehandtekening.be, 2006).

Er bestaan twee manieren om te bedriegen bij een hash functie. Een eerste geval kan men als volgt omschrijven. Stel dat persoon A een bericht wil versturen naar persoon B en hem hierbij wil bedriegen. Persoon A maakt twee verschillende berichten die eenzelfde hashwaarde geven berekend met eenzelfde hash functie. Wanneer persoon B één van de twee berichten ontvangt kan persoon A zeggen dat dit niet het juiste bericht is, aangezien hij ook nog een ander bericht heeft dat dezelfde hashwaarde uitkomt. Het tweede geval bestaat wanneer een persoon C persoon A, de verzender van het bericht, probeert om de tuin te leiden. Persoon C tracht dan een zinvol bericht te vinden dat met dezelfde hash functie eenzelfde hashwaarde uitkomt als het originele bericht. Wanneer deze twee vormen van bedrog bijna onmogelijk zijn, wordt de hash functie een sterke botsingsvrije hash functie genoemd.

Cryptografische hash functies spelen een fundamentele rol in de moderne cryptografie. De belangrijkste rol van een hash functie vinden we terug bij de creatie van een digitale handtekening. De hash functie wordt gebruikt om lange teksten te ondertekenen. Op de tekst wordt een hash functie toegepast die publiekelijk beschikbaar is en enkel de hashwaarde is gekend. Wie de boodschap ontvangt, past

de hash functie hierop toe en verifieert de hashwaarde. (http://www.x5.net/x5.html, 2006)

Er zijn verschillende soorten hash functies. Deze worden onderverdeeld in families.

MD-familie

MD is een afkorting voor message digest. In deze familie vindt men drie soorten: md2, md4, md5. Deze laatste is de bekendste en de meest gebruikte. De ontwikkelaar Ronald Rivest die in 1989 begon met md2, is ook de grote man achter de RSA-cryptografie. Echter, deze familie is minder veilig dan men oorspronkelijk dacht. Er kunnen reeds snel botsingen berekend worden. (http://www.nightkiller.net/Eindwerk_Cryptografie, 2006)

SHA-familie

SHA staat voor Secure Hash Algorithm. Deze familie bestaat momenteel uit de SHA-0, SHA-1 en SHA-2. SHA-224, SHA-256, SHA-384 en SHA-512 worden gegroepeerd onder de verzamelnaam SHA-2. Dit algoritme werd geschreven door de NSA (National Security Agency van Amerika). Bij SHA-0 en SHA-1 zijn reeds botsingen gevonden. Enkel bij SHA-2 is dit nog niet het geval. (http://www.nightkiller.net/Eindwerk_Cryptografie, 2006)

6.3.1 Voorbeeld van een hash functie

Het onderstaande voorbeeld toont het algoritme voor een MD5 hash functie. De message digest van MD5 wordt in vijf stappen berekend. De invoer is een bericht van een willekeurig aantal bits b. De afzonderlijke bits daarvan worden voorgesteld door m_0, m_1, …, m_{b-1}.

Dit voorbeeld werd overgenomen uit http://home.student.utwente.nl/b.verhaagen/cryptonet/hash/content.htm

Stap 1: Aanpassen van de lengte

De lengte van het bericht wordt aangepast tot 448 (mod 512) tekens. Hiervoor wordt eerst een 1 achteraan het bericht toegevoegd, ook als het bericht al een lengte van 448 tekens had. Vervolgens worden er nullen achteraan toegevoegd, net zolang tot de lengte 448 mod 512 is, dus een 448 plus een veelvoud van 512.

Stap 2: Lengte aanvullen

De lengte van het bericht wordt aangevuld met 64 bits. Hiervoor wordt de oorspronkelijke boodschap weergegeven als een 64-bits binair getal en achter het bericht van stap 1 gezet. Het bericht heeft nu dus een lengte van een veelvoud van 512 bits, oftewel een veelvoud van 16 bytes van 32 bits. Het bericht wordt nu geschreven als een matrix M[0,1,..,N-1], waarbij de parameters van de matrix de 32-bits bytes zijn, en N een veelvoud van 16 is.

Stap 3: Bytes A tot en met D aanmaken

Nu moeten vier bytes van elk 8 bits aangemaakt worden, samen dus 32 bits. Deze vier bytes (A, B, C en D) bestaan uit de hexadecimale getallen:

Byte A: 01 23 45 67

Byte B: 89 ab cd ef

Byte C: fe dc ba 98

Byte D: 76 54 32 10

Stap 4: Bericht verwerken

Om het bericht te verwerken, hebben we de functies F(X,Y,Z), G(X,Y,Z), H(X,Y,Z) en I(X,Y,Z) nodig. Ze hebben als invoer drie 32-bits bytes en als uitvoer één byte van 32 bits.

F(X,Y,Z) = (X AND Y) OR (not(X) AND Z)

G(X,Y,Z) = (X AND Z) OR (Y AND not(Z))

H(X,Y,Z) = X XOR Y XOR Z

I(X,Y,Z) = Y XOR (X OR not(Z))

Vervolgens heeft men een tabel T met 64 elementen nodig, dus T[1,2,..,64]. De tabel is als volgt gedefinieerd: T[i] is het i-de element van de tabel. De waarde van T[i] is de integere waarde (dus zonder decimalen) van 2^{32} keer abs(sin(i)), met i in radialen.

De tabel T:

3614090360	3905402710	606105819	3250441966	4118548399	1200080426	2821735955	4249261313
1770035416	2336552879	4294925233	2304563134	1804603682	4254626195	2792965006	1236535329
4129170786	3225465664	643717713	3921069994	3593408605	38016083	3634488961	3889429448
568446438	3275163606	4107603335	1163531501	2850285829	4243563512	1735328473	2368359562
4294588738	2272392833	1839030562	4259657740	2763975236	1272893353	4139469664	3200236656
681279174	3936430074	3572445317	76029189	3654602809	3873151461	530742520	3299628645
4096336452	1126891415	2878612391	4237533241	1700485571	2399980690	4293915773	2240044497
1873313359	4264355552	2734768916	1309151649	4149444226	3174756917	718787259	3951481745

De rest van deze stap moet net zo vaak gedaan worden tot alle blokken van 16 (32-bits) bytes van M verwerkt zijn. Dus eerst M[0,1,...,15], daarna M[16,17,...,31], etc. Dit wordt op de volgende manier genoteerd:

For i = 0 to N/16-1

i is een teller, die loopt van 0 tot het totale aantal blokken - 1, en aangeeft welk blok van 16 bytes wordt verwerkt. Dat aantal blokken is N gedeeld door 16.
Het blok van 16 bytes kopiëren we nu naar X, dus:
X[0, 1, .., 15] = M[0+i*16, 1+i*16, .., 15+i*16].

Bij M staat er steeds +i*16 tussen, om aan te geven welke waarden uit M gebruikt worden. Dit hangt af van i:

Als i = 0, dan krijgt me voor M de waarden:
M[0+0*16, 1+0*16, ..., 15+0*16] = M[0, 1, ..., 15],
als i = 1, dan krijg je voor M de waarden:
M[0+1*16, 1+1*16, ..., 15+1*16] = M[16, 17, ..., 31],
etc.

Ook moet men de bytes A, B, C en D kopiëren naar AA, BB, CC en DD:
AA = A
BB = B
CC = C
DD = D
Vervolgens komen er 4 ronden met berekeningen.

Ronde 1:

[ABCD k s i] staat voor de functie: A = B + ((A + F(B,C,D) + X[k] + T[i]) <<< s). <<< s betekent dat de byte met s bits naar links geroteerd wordt, oftewel de s bytes aan de linkerkant worden achteraan gezet.

Nu moeten de volgende 16 berekeningen gedaan worden. Eerst de 1e rij, dan de 2e, enz.. Bij elke berekening wordt de uitkomst van de vorige berekeningen gebruikt.

[ABCD 0 7 1] [DABC 1 12 2] [CDAB 2 17 3] [BCDA 3 22 4]
[ABCD 4 7 5] [DABC 5 12 6] [CDAB 6 17 7] [BCDA 7 22 8]
[ABCD 8 7 9] [DABC 9 12 10] [CDAB 10 17 11] [BCDA 11 22 12]
[ABCD 12 7 13] [DABC 13 12 14] [CDAB 14 17 15] [BCDA 15 22 16]

Ronde 2:

Deze ronde is bijna hetzelfde als de vorige, behalve dat deze keer G(B,C,D) in plaats van F(B,C,D) gebruikt wordt. Dus: [ABCD k s i] staat voor A = B + ((A + G(B,C,D) + X[k] + T[i]) <<< s).

[ABCD 1 5 17] [DABC 6 9 18] [CDAB 11 14 19] [BCDA 0 20 20]
[ABCD 5 5 21] [DABC 10 9 22] [CDAB 15 14 23] [BCDA 4 20 24]
[ABCD 9 5 25] [DABC 14 9 26] [CDAB 3 14 27] [BCDA 8 20 28]
[ABCD 13 5 29] [DABC 2 9 30] [CDAB 7 14 31] [BCDA 12 20 32]

Ronde 3:

Zie vorige ronde, deze keer met H(B,C,D).

[ABCD 5 4 33] [DABC 8 11 34] [CDAB 11 16 35] [BCDA 14 23 36]
[ABCD 1 4 37] [DABC 4 11 38] [CDAB 7 16 39] [BCDA 10 23 40]
[ABCD 13 4 41] [DABC 0 11 42] [CDAB 3 16 43] [BCDA 6 23 44]
[ABCD 9 4 45] [DABC 12 11 46] [CDAB 15 16 47] [BCDA 2 23 48]

Ronde 4:

Zie vorige ronde, deze keer met I(B,C,D).

[ABCD 0 6 49] [DABC 7 10 50] [CDAB 14 15 51] [BCDA 5 21 52]

[ABCD 12 6 53] [DABC 3 10 54] [CDAB 10 15 55] [BCDA 1 21 56]

[ABCD 8 6 57] [DABC 15 10 58] [CDAB 6 15 59] [BCDA 13 21 60]

[ABCD 4 6 61] [DABC 11 10 62] [CDAB 2 15 63] [BCDA 9 21 64]

Nu moeten de uitkomsten van A, B, C, en D nog bij hun oorspronkelijke waarden (AA, BB, CC, en DD) worden opgeteld:

A = A + AA

B = B + BB

C = C + CC

D = D + DD

Next i: nu moet het volgende blok verwerkt worden, dus i wordt eentje groter en alle berekeningen moeten weer herhaald worden, vanaf het kopieren van de blokken van M in X.

Stap 5: message digest samenstellen

De bytes A, B, C en D bestaan allen uit 32 bits. Door ze nu achter elkaar te zetten (in de volgorde A - B - C - D) krijg je een byte van 128 bits. Dit is de gehashde waarde van het oorpsronkelijke bericht.

De MD5 hash van de volgende zin "ik wacht op de bus" is: 825d737a1ea850e259642a75e3ce4c3c

6.4 Codetheorie

Bij het versturen van al dan niet geheime informatie kunnen storingen optreden. Hierdoor is het ontvangen bericht niet meer hetzelfde als het originele bericht dat verstuurd werd. De codetheorie is een tak van de wiskunde die zich bezighoudt met het ontwikkelen van methoden om uit een verstoorde boodschap toch de oorspronkelijk informatie te reconstrueren. (Buyst, 1967)

De primaire doelstellingen van codetheorie zijn:

- Efficiënt coderen van informatie
- Veilig versturen van gecodeerde berichten
- Snelle decodering van de ontvangen informatie
- Vinden en eventueel verbeteren van de fouten die zijn opgetreden tijdens de transmissie

(http://www7.tamu-commerce.edu/honors/honorsprog/Vaczlavik's%20Honors%20Proposal.doc, 2004)

Eén van de eenvoudigste methoden om fouten in een binaire boodschap te kunnen herkennen, is door gebruik te maken van de pariteitscode. Hierbij wordt een extra pariteitsbit meegestuurd die aangeeft of het aantal enen in de boodschap even of oneven is. Dit toegevoegde bit is volledig redundant. Het brengt geen informatie over, maar wordt gebruikt om fouten op te sporen. Indien één enkel bit veranderd is tijdens de transmissie, zal de pariteit van de boodschap veranderen zodat de fout gedetecteerd kan worden. Een nadeel van deze methode is dat de pariteitscode niet aangeeft welke bit de fout bevat zodat deze niet hersteld kan worden. De data moet dan telkens opnieuw verstuurd worden. Het was Richard Hamming die in 1950 de grondslag legde voor codes die fouten niet alleen kunnen detecteren, maar die ze ook kunnen verbeteren. De Hammingcode is de meest bekende foutenherkennende en foutenverbeterende code. Met behulp van de Hammingcode kunnen alle één-bit fouten gedetecteerd en gecorrigeerd worden, en alle twee-bit fouten gedetecteerd worden. Dit alles geldt voor zelfgekozen woordlengten, die het percentage aan fouten die verbeterd of gedetecteerd worden bepaalt. (http://www7.tamu-commerce.edu/honors/honorsprog/Vaczlavik's%20Honors%20Proposal.doc, 2004)

Codetheorie kent twee mogelijke toepassingen. Een eerste toepassing bestaat erin dat codetheorie de kleinst perturbatie (tot minder dan 10^{-12de}) uit een verzonden bericht kan halen en verbeteren. Een andere toepassing van codetheorie is dat men uit sterk vervormde berichten toch nog informatie kan halen. Een voorbeeld hiervan zijn de beelden van de planeet Jupiter die zeer sterk vervormd binnenstroomden bij NASA. Met behulp van codetheorie kon men hier toch nog zinnige beelden uit vormen.

Hoofdstuk 7 Digitale handtekening

In hoofdstuk zeven wordt er verder ingegaan op het principe van de digitale handtekening. Er wordt ook kort ingegaan op andere soorten digitale handtekeningen en andere aspecten van de digitale handtekening.

7.1 Inleiding

Een digitale handtekening is een handtekening die kan gebruikt worden om de identiteit van de zender van een bericht of de ondertekenaar van een document te verifiëren. Mogelijk dient ze ook nog om te verzekeren dat de originele inhoud van een bericht of document dat verzonden werd, onveranderd bleef. Digitale handtekeningen kunnen gemakkelijk overgemaakt worden. Ze kunnen niet nagemaakt worden door iemand anders en kunnen automatisch een tijdsstempel (datum en tijd) meekrijgen. De mogelijkheid om te verzekeren dat het originele ondertekende bericht aangekomen is, houdt het eveneens in dat de ontvanger het later moet erkennen. (www.digitalehandtekening.be, 2006)

Een digitale handtekening wordt gemaakt met behulp van een digitaal certificaat. Een digitaal certificaat verbindt een publieke sleutel met een individu of een organisatie. De toewijzing van de publieke sleutel aan een individu of een organisatie wordt verzorgd door een betrouwbare instantie (meestal een certificatieautoriteit of CA). Digitale certificaten zijn gebaseerd op cryptografie van de publieke sleutel. (Hier wordt verder op ingegaan in 7.4.4) Dit wil eigenlijk zeggen dat twee sleutels gebruikt worden: een publieke en een private. De private sleutel is enkel gekend door de eigenaar en wordt gebruikt om een digitale handtekening te maken. Deze sleutel moet de gebruiker natuurlijk voor zichzelf houden. De publieke sleutel is daarentegen door iedereen gekend en wordt gebruikt om de digitale handtekening te controleren. Als men een digitale handtekening controleert, weet men ook meteen wie het bericht ondertekende. Een sleutelpaar kan niet rechtstreeks geassocieerd worden met een

identiteit: het zijn immers gewoon twee getallen. De associatie wordt verkregen met het digitale certificaat dat de publieke sleutel met een identiteit verbindt. Met een digitaal certificaat kan je nagaan of iemand het recht heeft een bepaalde sleutel te gebruiken, waardoor vermeden wordt dat iemand valse sleutels gebruikt en zich als iemand anders voordoet. Versterkt door het gebruik van encryptie, bieden digitale certificaten een volledigere beveiligingsoplossing waarbij de identiteit van alle partijen in een transactie gekend is.
(http://www.isabel.be/contrib/documents/nl/signature.nl.pdf, 2006)

Hoewel het paar van sleutels wiskundig gerelateerd is, is het rekenkundig onmogelijk om de private sleutel af te leiden uit de publieke sleutel door een andere persoon. Bijgevolg kan men de private sleutel van de verzender niet ontdekken en deze gebruiken om de digitale handtekening te vervalsen ook al is de publieke sleutel door vele personen gekend en wordt deze gebruikt om de digitale handtekening van de verzender te verifiëren. Hier wordt dikwijls naar verwezen als het principe van de onomkeerbaarheid. (http://www.abanet.org, 2006)

De term "elektronische handtekening", die vaak incorrect als synoniem van een digitale handtekening wordt gebruikt, is een wettelijke definitie voor diverse, niet noodzakelijk cryptografische, methoden om de identiteit van iemand die een elektronisch bericht zendt te bevestigen. Dit omvat behalve een digitale handtekening ook bijvoorbeeld telegram- en telexadressen en een geschreven handtekening op een gefaxt document. (http://www.wikipedia.org, 2006)

Een elektronische handtekening is, per definitie, een geheel van elektronische gegevens dat vastgehecht is aan of logisch geassocieerd is met andere elektronische gegevens, en dat wordt gebruikt als middel voor authentificatie. Dergelijke handtekening kan worden gebruikt voor het identificeren van de ondertekenaar(s) van een juridische akte die via elektronische weg werd opgemaakt. Wettelijk gezien kan ze niet geweigerd worden op het stuk van haar juridische doeltreffendheid of haar ontvankelijkheid als gerechtelijk bewijsmiddel. Niettemin wordt ze enkel erkend als gelijkwaardig aan de handgeschreven handtekening wanneer ze voldoet aan een aantal technische veiligheidscriteria. In dit geval zegt

men dat de elektronische handtekening gekwalificeerd is. (http://mineco.fgov.be, 2006)

Er worden twee soorten elektronische handtekening onderscheiden: een (gewone) elektronische handtekening en een geavanceerde elektronische handtekening.

Met een gewone elektronische handtekening wordt een handtekening bedoeld waarvan de elektronische gegevens in combinatie met andere elektronische gegevens een middel zijn om de identiteit van de ondertekenaar vast te stellen. Een voorbeeld hiervan is een ingescande handtekening die aan een elektronisch document is toegevoegd.

Een geavanceerde elektronische handtekening is daarentegen met meer waarborgen omkleed en dient te voldoen aan de volgende kwaliteitseisen:

- zij is op unieke wijze aan de ondertekenaar verbonden.
- zij maakt het mogelijk de ondertekenaar te identificeren.
- zij komt tot stand met middelen die de ondertekenaar onder zijn uitsluitende controle kan houden.
- zij is op zodanige wijze verbonden aan het elektronisch bestand waarop zij betrekking heeft, dat elke wijziging van de gegevens achteraf kan worden opgespoord.

De digitale handtekening daarentegen maakt altijd gebruik van asymmetrische encryptie en digitale certificaten om de authenticiteit en de integriteit van berichten te verzekeren.

Men kan vaststellen dat tegenwoordig enkel de digitale handtekening voldoet aan dit begrip van geavanceerde elektronische handtekening. Indien een geavanceerde elektronische handtekening gebaseerd is op een gekwalificeerd certificaat, spreekt men van een gekwalificeerde elektronische handtekening. (Delbrouck, 2002)

De keuze voor een bepaalde soort van handtekening is afhankelijk van de veiligheid die men wil bekomen. De gewone elektronische handtekening is voldoende voor toepassingen die geen strenge veiligheid vereisen, zoals het verzenden van e-mail.

De geavanceerde elektronische handtekening biedt een grotere veiligheid dan de gewone elektronische handtekening. Ze is voldoende voor een toepassing die het equivalent van een handgeschreven handtekening niet noodzakelijk vereist, zoals facturatie. De gekwalificeerde elektronische handtekening biedt het hoogste veiligheidsniveau. Ze wordt gelijkgesteld aan de geschreven handtekening. Ze is dus nodig voor het ondertekenen van documenten waarvoor vroeger een handgeschreven handtekening nodig was, zoals het aanvragen van een uitreksel van je geboorteakte. (http://www.ecp.nl, 2006)

7.2 Soorten elektronische handtekeningen

Er bestaan verschillende soorten elektronische handtekeningen. Hieronder wordt een kort overzicht gegeven.

7.2.1 Biometrische methoden

Dit zijn methoden waarbij een uniek menselijk lichaamsdeel wordt gebruikt als elektronische handtekening. Gedacht kan worden aan vingerafdrukken, een scan van de iris van het menselijk oog, een DNA-test of de stem. Zowel het patroon van een vingerafdruk, als van een iris en een DNA-string zijn uniek voor ieder mens. Omdat die patronen uniek zijn kan hiermee iemands identiteit onomstotelijk worden vastgesteld. Om identificatie via deze methoden daadwerkelijk goed te laten verlopen moet aan verschillende voorwaarden voldaan worden:

1. Er moet eenvoudige apparatuur komen die een biometrische scan of afdruk kan maken;
2. Die apparatuur moet zeer toegankelijk zijn en op zeer veel plaatsen aanwezig zijn;
3. Er moet een uitgebreide databank opgesteld worden, waarin ter verificatie een kopie van de scan wordt opgeslagen.

Los van de benodigde infrastructuur die zou opgebouwd moeten worden, bevinden de meeste van deze scantechnieken zich nog in een experimenteel stadium. Eveneens is het mogelijk om verschillende biometrische handtekeningen in combinatie met elkaar te gebruiken. (http://www.wikipedia.org, 2006)

7.2.2 Gescande handtekening

Van een handgeschreven handtekening kan met behulp van scantechnieken een digitale afbeelding worden gemaakt. Dit gebeurt met behulp van een apparaat dat een zeer fijnmazig rooster over de handtekening projecteert. Het apparaat leest alle hokjes in het rooster en noteert of een hokje zwart, dan wel wit is en vertaalt dit in digitale nullen en enen. Deze gegevens worden in een computerbestandje opgeslagen. Als een handtekening onderaan een document geplaatst moet worden reproduceert de computer de handtekening door de (imaginaire) hokjes zwart te maken, dan wel wit te laten. Hierdoor wordt een kopie van de handtekening verkregen. Een handtekening onder een fax wordt op dezelfde manier gereproduceerd. Deze handtekening is oorspronkelijk gebaseerd op een ‘echte’ handtekening die maar door één persoon gemaakt kan zijn, maar als zij eenmaal in het computerbestand is opgeslagen kan iedereen die toegang heeft tot dat bestand deze handtekening zetten. Afhankelijk van de kwaliteit van de scanner is deze handtekening met het blote oog niet van echt te onderscheiden. Overigens kan worden opgemerkt dat in de praktijk in toenemende mate schriftelijke documenten inclusief handtekening worden gescand (document imaging) onder vernietiging van het origineel om kosten van bewaring te verminderen. (http://www.wikipedia.org, 2006)

7.2.3 Digitale pen

Dit apparaat ziet eruit als een gewone pen, maar is via een draad verbonden met een computer. Bij ingebruikneming van de pen wordt een bestand aangemaakt waarin in elektronische vorm de kenmerkende gegevens van de handtekening worden neergelegd zoals de vorm, de snelheid waarmee de handtekening wordt gezet alsmede met welke druk en houding van de pen dit gebeurt. De betreffende gegevens zijn het gemiddelde van een aantal handtekeningen. (http://www.wikipedia.org, 2006)

Wanneer de houder van de handtekening met een pen een nieuwe handtekening zet worden de gegevens van de betreffende handtekening vergeleken met de gegevens in het bestand. Indien deze gegevens binnen de vastgestelde marges overeenstemmen met de gegevens in het bestand wordt degene die de

handtekening heeft geplaatst geïdentificeerd als de houder van de betreffende handtekening. Omdat handtekeningen in de loop der tijd evolueren, worden telkenmale dat er een nieuwe handtekening wordt geplaatst en geaccordeerd, de gegevens van de oudste handtekening in het bestand vervangen door de gegevens van de nieuwe handtekening. (http://www.wikipedia.org, 2006)

Bij deze methode hoeft de persoon die het bericht ondertekent niet fysiek op de plaats der ondertekening te zijn, omdat de informatie via een netwerk naar elders getransporteerd kan worden. Ook deze methode bevindt zich nog in een experimentele fase. De vraag is of het systeem wel helemaal betrouwbaar is. Omdat niemand zijn handtekening tweemaal exact hetzelfde maakt moeten er afwijkingsmarges in het systeem worden ingebouwd. Het gevolg hiervan is dat de kans aanzienlijk wordt dat een valse ondertekenaar door de computer als rechtmatig wordt herkend en de rechtmatige ondertekenaar als oplichter wordt aangemerkt. (http://www.wikipedia.org, 2006)

7.2.4 Digitale handtekening (zie paragraaf 7.4)

7.3 Eigenschappen van digitale handtekeningen

Digitale handtekeningen hebben enkele belangrijke eigenschappen zoals: authenticatie, confidentialiteit, integriteit en onweerlegbaarheid.

7.3.1 Authenticatie

Authenticatie is de verificatie van de identiteit van een persoon (server, stukje software...). Het garandeert de identiteit van diegene die de informatie handtekende: zo weet men wie deelnam aan de transactie en dat het niet door anderen vervalst werd. Het laat eveneens toe de ware identiteit te achterhalen van een gebruiker die toegang probeert te verkrijgen tot een systeem. (http://www.digitalehandtekening.be, 2006)

Stallings (2000) haalt eveneens aan dat berichtauthenticatie twee partijen beveiligt tegen elke derde partij. Hij haalt echter wel aan dat het niet de twee partijen tegen elkaar beveiligt.

Een geverifieerde digitale handtekening geeft de ontvanger het vertrouwen dat de zender van het bericht inderdaad degene is wiens naam als afzender in het bericht staat. De afzender tekent het bericht met zijn geheime sleutel, de ontvanger verifieert met de publieke sleutel van de afzender. (http://www.isabel.be, 2006)

Het belang van authenticiteit is vooral duidelijk bij het gebruik van communicatie voor financiële doeleinden. Bijvoorbeeld als een bijkantoor van een bank instructies zendt naar het hoofdkantoor om een bedrag naar een rekening over te maken is het belangrijk om te kunnen bepalen of de afzender van het bericht effectief een gemachtigde zender uit het bijkantoor is. Zonder authenticatie zou een kwaadwillige gebruiker immers een bericht kunnen afluisteren, en dit bericht daarna zelf herhalen en verzenden naar het hoofdkantoor. (http://www.isabel.be, 2006)

7.3.2 Integriteit

Een digitale handtekening beschermt de integriteit van de informatie: men weet wanneer deze werd gewijzigd, zowel toevallig als kwaadwillig. Een digitale handtekening bevat een verkapte vorm van de informatie die gehandtekend wordt. Elke wijziging aan die informatie nadat het gehandtekend is, zou deze digitale verkapte vorm ongeldig maken. Ook dit aspect wordt diepgaander besproken in 7.4. (http://www.digitalehandtekening.be) De afzender en de ontvanger willen er beide zeker van zijn dat een bericht niet veranderd is tijdens de transmissie. In bijvoorbeeld een bankscenario is het belangrijk te kunnen bepalen of onderweg niet een paar nullen aan een bedrag zijn toegevoegd. Een digitale handtekening bevat onder meer een controlegetal van het originele bericht. Hier wordt verder op ingegaan in deel 7.4. Deze hash-waarde wordt ook met behulp van cryptografische technieken berekend. Bij ontvangst wordt opnieuw dezelfde controleberekening gemaakt, waarmee kan worden vastgesteld of tussen verzending en ontvangst een mutatie van het bericht heeft plaatsgevonden. (http://www.isabel.be, 2006)

7.3.3 Confidentialiteit

De confidentialiteit van de data wordt bereikt door de boodschap te encrypteren aan de hand van de 'publieke' sleutel van de ontvanger. Enkel de ontvanger kan dan het bericht lezen. (http://www.digitalehandtekening.be, 2006) De digitale handtekening op zich biedt dus geen confidentialiteit, maar wel de combinatie van digitale handtekening met een cryptosysteem.

Stallings (2000) vermeldt eveneens dat vertrouwelijkheid kan geboden worden door het hele bericht plus de handtekening verder te versleutelen met de public key van de ontvanger.

7.3.4 Onweerlegbaarheid

Een eigenschap van een digitale handtekening is het feit dat de auteur van een bericht zijn identiteit kan bewijzen. Onweerlegbaarheid laat echter ook toe om later te bewijzen wie in een transactie participeerde, wie een bericht in een transactie verzond kan niet meer ontkennen dat hij dit deed. In eenvoudige woorden, onweerlegbaarheid betekent dat een communicatie of een transactie niet meer kan ontkend worden, net zoals bij een aangetekende zending. (http://www.digitalehandtekening.be, 2006)

In tabel 7.1 wordt een vergelijkend overzicht geboden van de vier voorgaande eigenschappen bij drie soorten handtekening.

Tabel 7.1 Vergelijking eigenschappen soorten handtekeningen

Eigenschappen	**Digitale Handtekening**	**Biometrische handtekening**	**Gewone handtekening**
Authenticatie	++	+	-
Betrouwbaarheid	++	-	--
Integriteit	++	+	-
Onweerlegbaarheid	+	0	-

++ : zeer goed
+ : goed
0 : normaal
- : slecht
-- : zeer slecht

7.4 Werking van de digitale handtekening

Digitale handtekeningen worden gecreëerd en geverifieerd door cryptografie. Ze gebruiken publieke sleutel cryptografie.

7.4.1 Principe

Een digitale handtekening bestaat uit twee handelingen. Een eerste handeling wordt uitgevoerd door de verzender van de boodschap, de tweede door de ontvanger.

De eerste handeling is het aanmaken van de digitale handtekening. Het aanmaken van de digitale handtekening kan op verschillende manieren gebeuren. Dit is afhankelijk van de gewenste beveiliging. De verschillende mogelijkheden worden later in dit hoofdstuk besproken.

De handeling uitgevoerd door de ontvanger is het controleren van de digitale handtekening. De complexiteit van deze handeling is eveneens afhankelijk van de gekozen beveiligingsgraad van de zender.

Er bestaan verschillende mogelijkheden om een bericht te coderen of om een digitale handtekening te plaatsen. Deze worden hieronder besproken. Ook de schema's van deze mogelijkheden komen verder in dit hoofdstuk aan bod.

7.4.2 Slechts confidentialiteit is belangrijk

Als men enkel wenst dat de inhoud van een bericht geheim blijft, volstaat het om public key cryptografie toe te passen. Hierbij vercijfert persoon A het bericht met de publieke sleutel van B alvorens het te versturen. Stel dat f_A en f_B de publieke sleutels zijn van persoon A en persoon B en dat deze twee functies gedefinieerd worden als one way functies. Dan zendt persoon A naar persoon B: $y = f_B$ (bericht). Enkel persoon B heeft de overeenkomstige private sleutel f^{-1}_B in zijn bezit. Niemand anders dan persoon B kan het bericht ontcijferen. Enkel B kan berekenen: bericht = $f^{-1}_B(y)$. Dit systeem is identiek aan paragraaf 6.2 (zie ook het schema in figuur 6.1) Soms kunnen er fouten ontstaan bij het verzenden van het bericht. Om dit probleem vast te stellen en te vermijden, is het mogelijk gebruik te maken van de codetheorie. Aangezien het hier enkel om public key cryptografie draait, is er nog geen sprake van een digitale handtekening.

7.4.3 Slechts onweerlegbaarheid is belangrijk

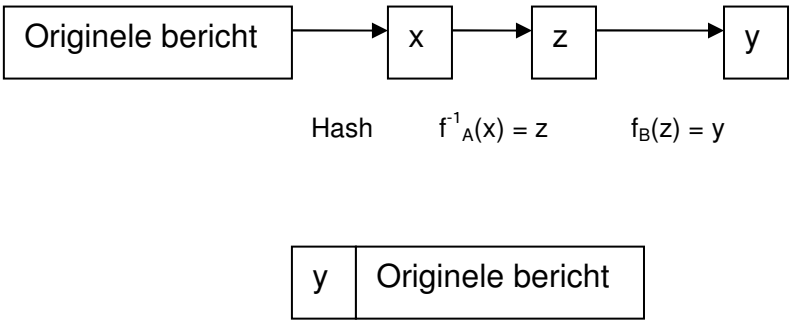
Veronderstel dat persoon A een bericht naar persoon B wil versturen zodat persoon A niet kan ontkennen dat hij het bericht verstuurd heeft en zodat persoon B zekerheid heeft dat het bericht van persoon A komt, kan deze laatste een digitale handtekening gebruiken. Om dit te bewerkstelligen ondertekent persoon A het bericht dat hij wil verzenden met zijn private sleutel f^{-1}_A. Dus $x = f^{-1}_A$(bericht). Een bijkomend probleem bij het versturen van berichten is de lengte van de berichten. Dit proces wordt dan immers een omslachtig en tijdrovend proces. Een oplossing hiervoor is dat men bij het creëren van de digitale handtekening eerst van de inhoud van het bericht een hashwaarde (x) berekent. Deze message digest (MD) of

hashwaarde wijzigt enkel als de inhoud van het bericht wijzigt. Vervolgens wordt deze message digest versleuteld met de private sleutel van persoon A. Zo wordt $z = f^{-1}_A(x)$. Dit wordt voorlopig de digitale handtekening (DS) genoemd. De geheimhouding van het bericht is bijkomstig in dit scenario, dus mag persoon A het bericht gewoon naar persoon B versturen. Enkel z wordt dan voor de betrouwbaarheid versleuteld met de publieke sleutel van persoon B alvorens het bericht te versturen. Persoon A zendt dus het originele bericht en $y = f_B(z)$ naar persoon B. Om transmissiefouten te vermijden wordt een foutenverbeterende en foutenherkennende code toegevoegd. Enkel persoon B is in het bezit van de juiste private sleutel. Dus enkel deze kan y terug ontcijferen in z. B berekent achtereenvolgens $z = f^{-1}_B(y)$ en $x = f_A(z)$. Dit levert de oorspronkelijke message digest x op. Persoon A kan bijgevolg niet ontkennen dat hij het bericht verstuurd heeft. Persoon B kan slechts met de publieke sleutel van persoon A z ontcijferen in x. Het oorspronkelijke bericht wordt bekomen door hetzelfde hashalgoritme als persoon A gebruikte. Indien deze hashwaarden overeenstemmen is persoon B zeker van de identiteit van persoon A. Hij is er eveneens zeker van dat de inhoud van het bericht niet werd gewijzigd. De digitale handtekening is dus geen fysieke handtekening, maar wel het feit dat twee hashwaarden aan elkaar gelijk zijn.

Figuur 7.1: onweerlegbaarheid is belangrijk

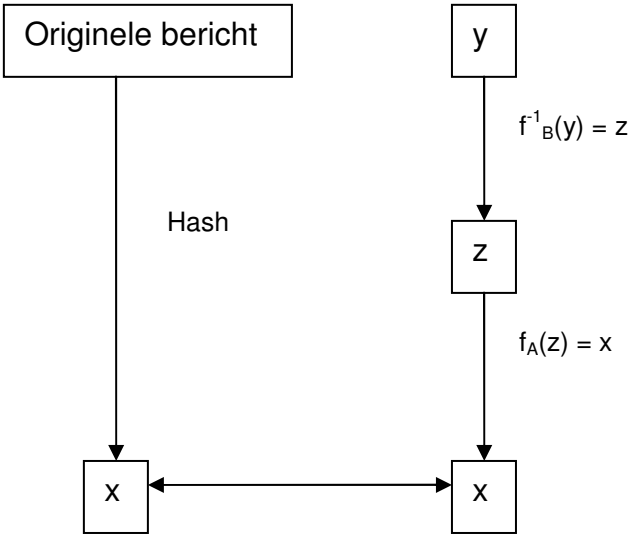
Persoon A of verzender

Persoon A verzendt zowel het originele bericht als de dubbel versleutelde hashwaarde (privaat zender, publiek ontvanger) naar een persoon B



Persoon B of ontvanger

Persoon B ontvangt het originele bericht en de dubbel versleutelde hashwaarde. Eerst ontcijfert hij met zijn eigen private sleutel y. Dit geeft z. Vervolgens ontcijfert hij z met de publieke sleutel van persoon A tot hashwaarde x. Dan past hij hetzelfde hashalgoritme als persoon A toe op het originele bericht. Deze twee hashwaardes komen slechts overeen als het bericht niet veranderd werd.

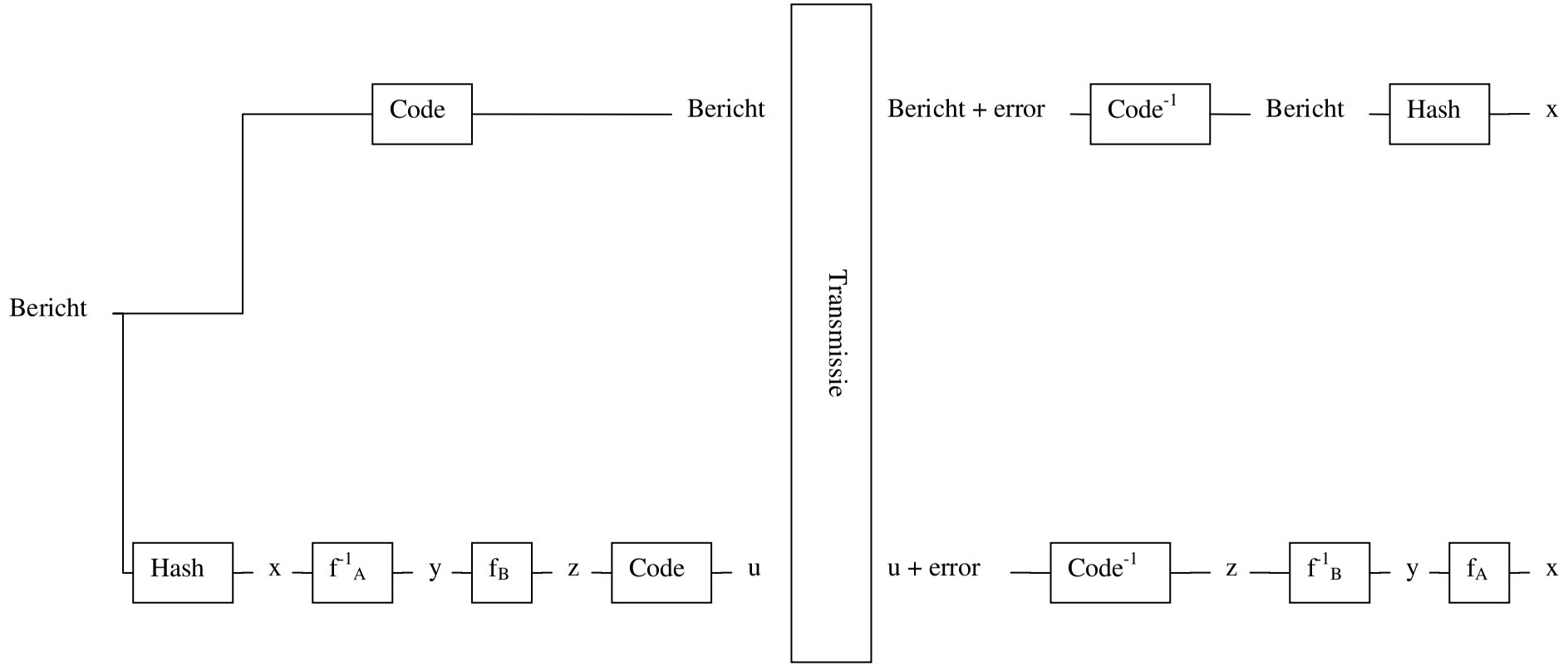


Om eventuele transmissiefouten te vermijden wordt het bericht nog voorzien van foutenherkennende en foutenverbeterende code.

Een andere mogelijke voorstelling:

f^{-1}_A : geheime sleutel van persoon A of zender, f^{-1}_B : geheime sleutel van persoon B of ontvanger

f_A : publieke sleutel van persoon A of zender, f_B : publieke sleutel van persoon B of ontvanger



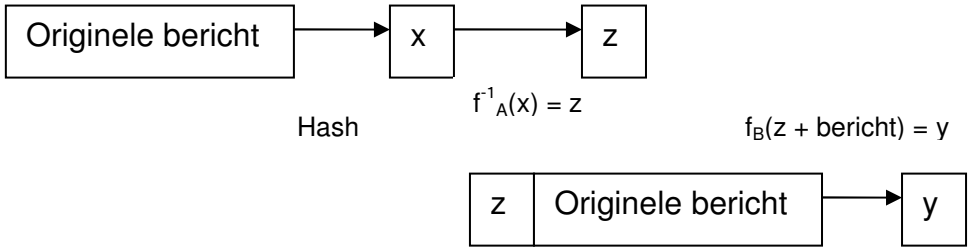
7.4.4 Onweerlegbaarheid én geheimhouding zijn belangrijk

Er is slechts een klein verschil met het vorige geval. Indien enkel onweerlegbaarheid belangrijk is, wordt de digitale handtekening vercijferd met de publieke sleutel van persoon B of de ontvanger. Als zowel onweerlegbaarheid en geheimhouding belangrijk zijn, versleutelt de zender of persoon A zowel het originele bericht als de digitale handtekening met de publieke sleutel van persoon B of de ontvanger. Y = f_B(z + origineel bericht). Hierbij wordt de geheimhouding gegarandeerd omdat alleen persoon B beschikt over de juiste private sleutel f^{-1}_B. Zo bekomt hij de digitale handtekening z en het originele bericht. Vervolgens past hij het hash algoritme toe op het originele bericht en gebruikt hij de publieke sleutel van persoon A om x te bekomen. Daarna vergelijkt hij de twee bekomen hashwaardes om het bericht te verifiëren.

Figuur 7.2: Onweerlegbaarheid en geheimhouding zijn belangrijk

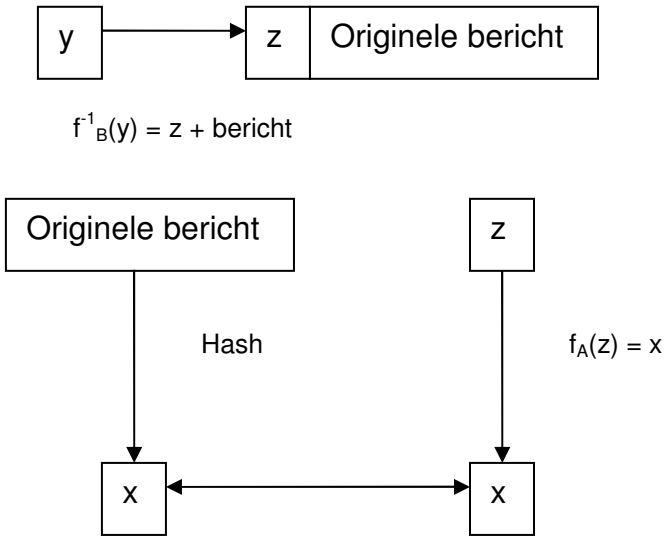
Persoon A of verzender

Persoon A versleutelt zowel het originele bericht als de reeds versleutelde hashwaarde (privaat zender) met de publieke sleutel van persoon B voor de informatie te verzenden naar persoon B



Persoon B of ontvanger

Persoon B ontvangt de met de publieke sleutel van persoon B versleutelde y. Hij ontcijfert y met zijn eigen private sleutel. Hieruit haalt hij z en het originele bericht. Z ontcijfert hij met de publieke sleutel van persoon A tot x en op het originele bericht past hij hetzelfde hashalgoritme toe als persoon A. Daarna vergelijkt hij de twee hashwaardes ter verificatie van het bericht.

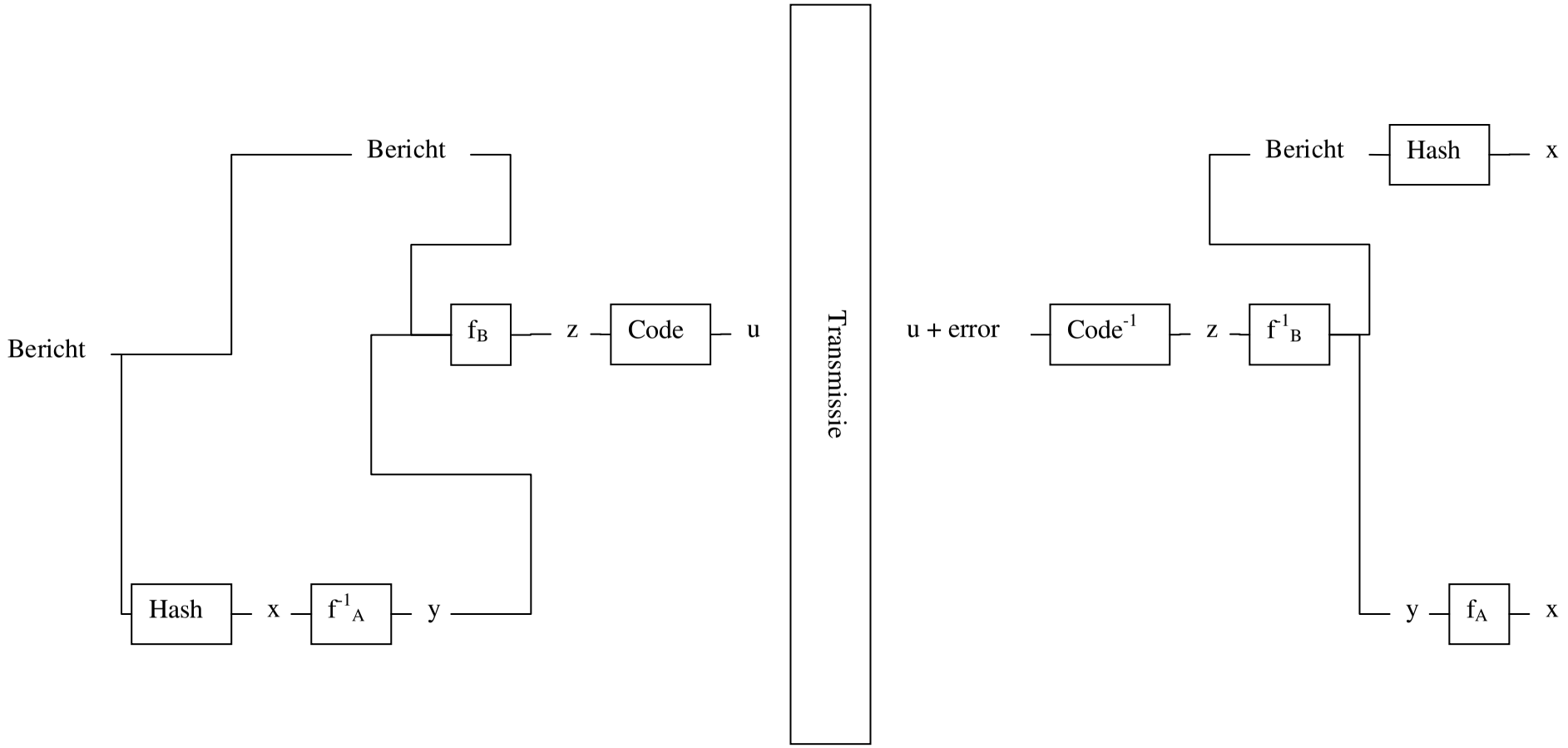


Om eventuele transmissiefouten te vermijden wordt het bericht nog voorzien van foutenherkennende en foutenverbeterende code.

Ook hier een andere voorstelling:

f^{-1}_A : geheime sleutel van persoon A of zender, f^{-1}_B : geheime sleutel van persoon B of ontvanger

f_A : publieke sleutel van persoon A of zender, f_B : publieke sleutel van persoon B of ontvanger



Deze laatste methode zorgt in de praktijk nog voor een probleem. Public key cryptografie is weinig efficiënt bij het versturen van lange berichten. Bij deze laatste methode worden zowel het originele bericht als de digitale handtekening versleuteld met de publieke sleutel van de ontvanger (persoon B). De digitale handtekening is meestal een waarde met een kleine lengte. Deze zorgt niet voor de problemen. Het bericht daarentegen heeft een veel grotere lengte. Via publieke sleutel cryptografie is het niet efficiënt deze grote lengte te versleutelen.

Panko (2005) vermeldt een oplossing voor dit probleem. Hij zegt dat men enkel de digitale handtekening moet versleutelen met de publieke sleutel van persoon B (ontvanger) zoals beschreven in paragraaf 7.4.3. Het originele bericht moet volgens hem versleuteld worden met symmetrische encryptie. Volgens mij leidt deze symmetrische encryptie tot nog grotere problemen. Bij symmetrische encryptie wordt slechts één sleutel gebruikt die beide partijen kennen. Het probleem is echter dat men voor elk verschillend koppel een nieuwe geheime sleutel moet vinden. Dus als men 100 verschillende koppels heeft, moet men ook 100 verschillende sleutels hebben.

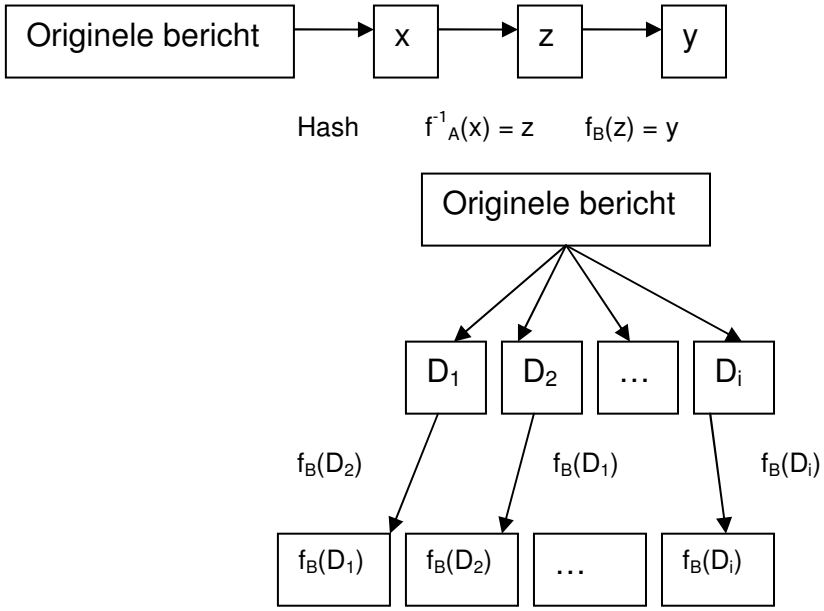
Een betere oplossing voor dit probleem is het bericht splitsen in verschillende delen. Elke deel wordt dan afzonderlijk vercijferd met de publieke sleutel van de ontvanger. Persoon A zendt dus naar persoon B: $f_B(D_i)$ en $y = f_B(z)$

Eerst wordt door deze ontvanger dan elk deel ontcijferd met zijn private sleutel. Na ontcijfering van alle delen, verkrijgt persoon B het originele bericht. Deze delen krijgen een volgnummer. Dus persoon B ontcijfert $z = f^{-1}_B(y)$ en “origineel bericht” = $\sum f^{-1}_B(D_i)$. Vervolgens berekent hij ook nog $x = f_A(z)$. Op het originele bericht past hij dezelfde hash functie toe als persoon A. De bekomen hashwaarde vergelijkt hij met x.

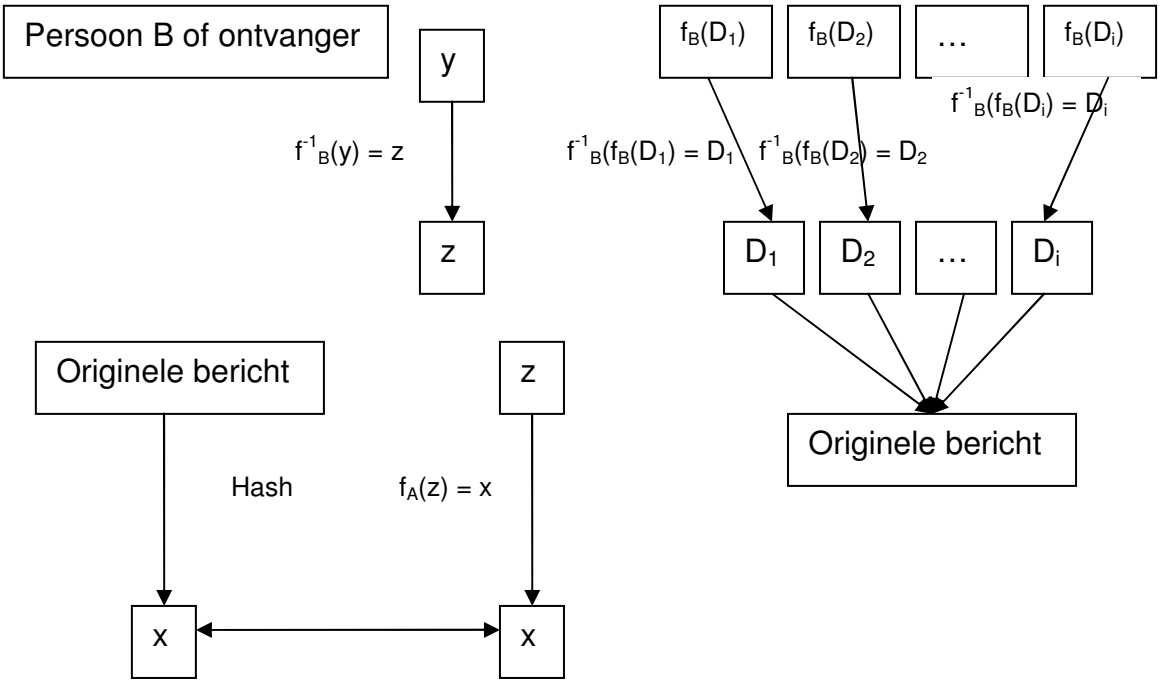
Figuur 7.3: onweerlegbaarheid en geheimhouding zijn belangrijk, praktijk

Persoon A of verzender

Persoon A splitst het originele bericht op in delen en versleutelt zowel deze delen als de reeds versleutelde hashwaarde (privaat zender) met de publieke sleutel van persoon B voor de informatie te verzenden naar persoon B



Persoon B of ontvanger



Persoon B ontvangt de met de publieke sleutel van persoon B versleutelde y en de met de publieke sleutel van persoon B versleutelde delen. Hij ontcijfert y en de versleutelde delen met zijn eigen private sleutel. Hieruit haalt hij z en de verschillende delen. Deze delen vormen samen het originele bericht. Z ontcijfert hij met de publieke sleutel van persoon A tot x en op het originele bericht past hij hetzelfde hashalgoritme toe als persoon A. Daarna vergelijkt hij de twee hashwaardes ter verificatie van het bericht.

In de praktijk is de methode die men gebruikt afhankelijk van de belangrijkheid van de inhoud van het bericht. Hoe belangrijker de inhoud van het bericht, des te belangrijker de geheimhouding is. Als geheimhouding niet belangrijk is gebruikt men de eerste methode. Als geheimhouding heel belangrijk is, gebruikt men de laatste methode. Bij deze laatste methode zijn er twee mogelijkheden. Hier kiest men in functie van de belangrijkheid van geheimhouding, maar men kijkt ook naar de lengte van het bericht. Als het bericht lang maar toch nog redelijk belangrijk is, zal men zich beroepen op de methode met symmetrische encryptie.

In tabel 7.2 wordt een kort overzicht gegeven van de verschillende soorten digitale handtekeningen.

Tabel 7.2: Soorten digitale handtekening, samenvattende tabel

Beveiligingssterkte	**Methode**
Enkel confidentialiteit	Publieke sleutel cryptografie
Enkel onweerlegbaarheid	MD versleuteld met private sleutel van zender. Enkel privaat versleutelde MD met publieke sleutel van ontvanger
Beiden	Theorie: MD versleuteld met private sleutel van zender Orig. bericht + Dig. Handtek. versleuteld met publieke sleutel van ontvanger Praktijk: in delen opgesplitst en zo versleuteld

7.4.5 Digitale certificaten

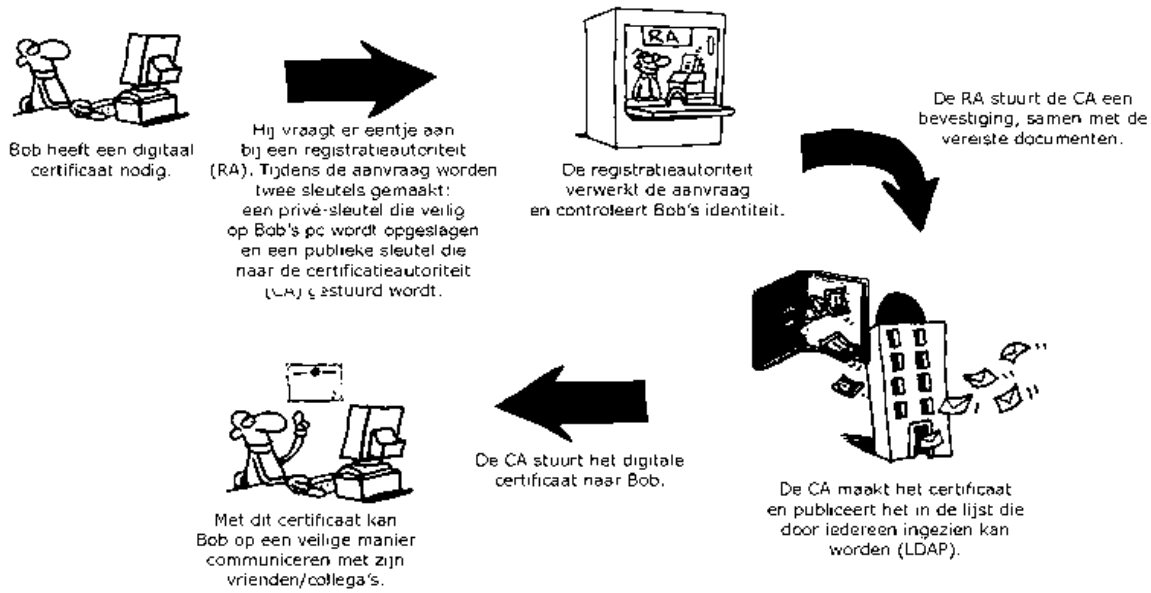
Wanneer een persoon B (ontvanger) een bericht ontvangt, ondertekend met een digitale handtekening, kan hij wel nagaan dat deze handtekening gezet is met een bepaalde geheime sleutel, maar weet hij nog steeds niet welke persoon deze handtekening gezet heeft. Hiervoor moet men zeker zijn welke naam bij de publieke sleutel hoort die hij gebruikt. Als persoon A persoon B kent, kunnen ze hun publieke sleutels uitwisselen door even bij de ander persoon langs te gaan. Maar dit kan

echter niet wanneer men te maken heeft met een groter systeem, zoals bijvoorbeeld het Internet. Het is goed mogelijk dat persoon C een publieke sleutel verspreidt die de naam van persoon B draagt, waardoor persoon A misleid wordt en denkt dat het bericht van persoon B afkomstig is. Stel dat persoon A een bedrag schuldig is aan persoon B, dan zal dit tot pijnlijke gevolgen leiden.

Om dit probleem op te lossen, maakt men gebruik van een digitaal certificaat. Een digitaal certificaat is een computerbestand dat fungeert als een digitaal paspoort voor de eigenaar van dat bestand. Een certificaat wordt gebruikt binnen de publieke sleutel infrastructuur. Het wordt uitgereikt en beheerd door een Certificatenautoriteit (CA). Een certificaat bevat de geregistreerde naam van de eigenaar, de publieke sleutel van de eigenaar, de geldigheidsduur van het certificaat en de locatie van de Certificate Revocation List (bij de uitgever van het certificaat). (www.wikipedia.org, 2006) Het bevat eveneens de handtekening van de certificatenautoriteit. Deze laatste tekent de vorige genoemde elementen en zorgt voor geloofwaardigheid.

Een digitaal certificaat zorgt er voor dat men bij een elektronische transactie de identiteit van de afzender van een bericht kan controleren. De identiteit van deze afzender is gebonden aan een publieke sleutel. Alle certificaten van een CA worden door deze CA beschikbaar gemaakt via een bestand van publieke sleutels. Zo kan iedereen publieke sleutels opvragen om een handtekening te controleren.

Figuur 7.4: Digitaal certificaat



Bron: www.digitalehandtekening.be (2006)

7.5 Juridische aspecten van de digitale handtekening

Omwille van het feit dat de digitale handtekening de mogelijkheid verschaft om de handgeschreven handtekening te vervangen, dient deze ook voorzien te zijn van een juridische achtergrond.

7.5.1 De Europese richtlijn

Eind jaren negentig ontstonden er een aantal initiatieven om een dergelijke betrouwbare keten op te zetten, maar deze systemen zijn nooit echt aangeslagen. De voornaamste reden hiervoor lijkt te zijn dat er geen duidelijkheid is over de rechtsgeldigheid van een digitale handtekening en de minimumeisen voor de te gebruiken apparatuur. Daarnaast schrijft de wet in bepaalde gevallen nog eens voor dat er schriftelijke verklaringen opgesteld moeten worden. Zelfs al zou het volkomen veilig zijn, dan nog mag een dergelijk proces verbaal simpelweg niet elektronisch opgesteld en getekend worden. Het is dan niet rechtsgeldig.

Op 19 januari 2000 werd de Richtlijn 1999/93/EG van het Europees Parlement en de Raad betreffende een gemeenschappelijk kader voor elektronische handtekeningen

verspreid in het publicatieblad van de Europese Gemeenschappen. Deze Richtlijn heeft tot doel het gebruik van elektronische handtekeningen te vergemakkelijken en tot de wettelijke erkenning ervan bij te dragen. (http://www.law.kuleuven.be/icri/publications, 2006)

De richtlijn stelt dat aan bepaalde types van elektronische handtekeningen dezelfde juridische waarde moet toegekend worden als aan de handgeschreven handtekening. Eveneens moeten de lidstaten van de Europese Unie alle soorten elektronische handtekeningen in hun wetgeving opnemen. De richtlijn is ten slotte technologie-onafhankelijk. Dit wil zeggen dat de lidstaten zowel huidige technieken als toekomstige technieken voor de elektronische handtekeningen op gelijke voet moeten behandelen als de handgeschreven elektronische handtekening. (http://www.iusmentis.com, 2006)

7.5.2 Het Belgisch juridisch kader (http://www.justfgov.be, 2006)

De Belgische wetgeving inzake elektronische handtekening is conform de richtlijn 1999/93/EG van het Europees Parlement en de Raad betreffende een gemeenschappelijk kader voor elektronische handtekeningen. De Europese richtlijn werd met behulp van twee wetten ingevoerd in de Belgische wetgeving: enerzijds de Wet Bourgeois (Wet van 20 oktober 2000) en anderzijds de wet van 9 juli 2001.

Op 22 december 2000 werd de wet van 20 oktober 2000 tot invoering van het gebruik van telecommunicatiemiddelen en van de elektronische handtekening in de gerechtelijke en de buitengerechtelijke procedure in het Belgisch Staatsblad bekendgemaakt.

De verdienste van de geamendeerde wet Bourgeois is gelegen in het feit dat daarmee het pad geëffend wordt voor het gebruik van elektronische handtekeningen, door de handtekening niet meer alleen als “met de hand geschreven” te beschouwen. Deze wijziging wordt doorgevoerd in artikel 1322 van het Burgerlijk Wetboek.

Artikel 1322 stelt dat *“Een onderhandse akte die erkend is door degenen tegen wie men zich daarop beroept, of die wettelijk voor erkend wordt gehouden, heeft tussen*

de ondertekenaars van de akte en tussen hun erfgenamen en rechtsverkrijgenden dezelfde bewijskracht als een authentieke akte." Het nieuwe tweede lid van art. 1322 luidt als volgt: "*Kan, voor de toepassing van dit artikel, voldoen aan de vereiste van een handtekening, een geheel van elektronische gegevens dat aan een bepaalde persoon kan worden toegerekend en het behoud van de integriteit van de akte aantoont*."

Dit nieuwe artikel duidt erop dat elektronische geschriften gelijkgesteld kunnen worden met klassieke geschriften als ze aan een bepaalde persoon toegerekend kunnen worden en ze het behoud van integriteit kunnen aantonen. Aan deze voorwaarden moet ook voldaan worden bij een handgeschreven handtekening.

De wet van 9 juli 2001, de tweede wet, handelde over de houdende vaststelling van bepaalde regels in verband met het juridisch kader voor elektronische handtekeningen en certificatiediensten. Deze wet wordt eveneens de wet certificatiediensten genoemd. Hierin worden de voorwaarden besproken waaraan een elektronische handtekening moet voldoen om gelijkwaardig te zijn met een handgeschreven handtekening. Net als in de Europese richtlijn spreekt men over elektronische gegevens die vastgehecht zijn aan of logisch geassocieerd zijn met andere elektronische gegevens en die gebruikt worden als middel voor authenticiteit. Er wordt eveneens vermeld dat een geavanceerde elektronische handtekening, die op een gekwalificeerd certificaat gebaseerd is en op een veilige manier gecreëerd is, dezelfde juridische gevolgen heeft als een geschreven handtekening. Een handtekening die voldoet aan deze drie voorwaarden wordt een gekwalificeerde elektronische handtekening genoemd. Daarnaast reglementeert deze wet de activiteiten van certificatiedienstverleners. Certificatiedienstverleners zijn vrij om al dan niet gekwalificeerde certificaten uit te reiken aan het publiek. Het spreekt voor zich dat de meerderheid ervoor kiest om ook gekwalificeerde certificaten uit te reiken, gezien het automatisme waarmee een gekwalificeerde elektronische handtekening als een geldige handtekening beschouwd wordt. De in België gevestigde certificaatverleners die zulke certificaten wensen uit te reiken moeten voor de aanvang van hun activiteiten een aangifte doen van hun identificatiegegevens bij het Ministerie van Economische Zaken om controle te vergemakkelijken. Voor de

certificatiedienstverleners voorziet de wet een bijzonder aansprakelijkheidsregime. (Delbrouck, 2002)

Tabel 7.3 geeft een kort schema van de besproken richtlijn en wetten.

Tabel 7.3 Schema van wetten

Wet	**Functie**
Europese richtlijn	Duidelijkheid scheppen over de rechtsgeldigheid van de digitale handtekening
Wet Bourgeois	Handtekening wordt niet enkel meer beschouwd als een met de handgeschreven handtekening
Wet certificaatdiensten	Voorwaarden opdat een elektronische handtekening evenwaardig is aan een handgeschreven handtekening

Hoofdstuk 8 Toepassingen van de digitale handtekening

In hoofdstuk acht wordt er in het kort ingegaan op de verschillende toepassingen van de digitale handtekening. Deze wordt gebruikt in e-commerce, e-banking, e-government, in de medische wereld en als e-cash.

8.1 E-Commerce

Een belangrijk verschijnsel in de 21ste eeuw is zonder twijfel e-commerce. Deze term electronic commerce vond zijn oorsprong in de jaren zeventig met innovaties zoals Electronic Fund Transfers (EFTs). Deze systemen maakten via een netwerk geld over tussen verschillende rekeningen. Door de opkomst van Electronic Data Interchange (EDI), een systeem voor data-uitwisseling tussen organisaties, breidde electronic commerce zich ook uit naar niet-financiële transacties. (http://www.wikipedia.org, 2006)

E-commerce is de laatste jaren steeds belangrijker geworden voor bedrijven. Het zorgde voor het ontstaan van verschillende telecommunicatietoepassingen, zoals digitale veilingen en ticketreserveringssystemen. Vandaar dat men e-commerce kan definiëren als een verzamelnaam voor alle manieren waarop via elektronische weg handel gedreven kan worden. (O'Brien, 1998)

Traditioneel worden er twee hoofdtypes van e-commerce onderscheiden: business-to-business (B2B) en business-to-consumer (B2C). Tegenwoordig spreekt men nog van een derde opkomende vorm van e-commerce, namelijk consumer-to-consumer (C2C). Bij deze laatste gaat het om consumenten die via het Internet aan andere consumenten verkopen. Een populair voorbeeld hiervan is e-bay. (http://www.wikipedia.org, 2006)

Veiligheid en betrouwbaarheid van transacties via het Internet zijn zeer belangrijk voor consumenten. Bij de toepassing van e-commerce kan er van alles mislopen. (W. Stallings, 2000, p. 145) Zo kan men geconfronteerd worden met technologische problemen, computerinbraken, menselijke vergissingen, … Dit zorgt ervoor dat de consument e-commerce wantrouwend bekijkt. Andere problemen die zich kunnen voordoen hebben betrekking op de privacy van de gebruiker. Online winkels nemen het vaak niet zo nauw met de privacy van de klanten. Hierdoor kan de klant ongewenste reclame ontvangen.

8.2 E-banking

Bankieren via het Internet, ook wel online bankieren of internetbankieren genoemd, maakt het heel gemakkelijk om de meest gangbare bankverrichtingen via een computer met internetverbinding te regelen. (http://www.telenet.be, 2006)

Internetbankieren is eenvoudig en gebruiksvriendelijk. Men bespaart veel tijd want men kan eenvoudig van achter het beeldscherm bankverrichtingen doen. Men kan snel en gemakkelijk rekeninginformatie opvragen, rekeningafschriften afdrukken, een overschrijving uitvoeren, beleggingen raadplegen en dergelijke in orde brengen. Men kiest zelf waar en wanneer het past en is niet langer gebonden door de openingsuren van een bank. Bovendien hoeft men zich niet meer te verplaatsen naar het bankkantoor of een automaat, maar kan men transacties uitvoeren van op de eigen stoel.

Internetbankieren is gemakkelijk en goedkoop. Men heeft enkel het softwarepakket van de bank nodig. Verrichtingen die men online doet, zijn vaak goedkoper dan verrichtingen die men in het bankkantoor uitvoert.

Veiligheid is enorm belangrijk bij internetbankieren. Mits enkele voorwaarden verloopt internetbankieren zo veilig mogelijk. Door de combinatie van een persoonlijke digitale handtekening en een wachtwoord is de toegang tot internetbankieren optimaal beschermd. Ook verrichtingen (overschrijvingen, beursorders, etc.) worden efficiënt

beveiligd door een elektronische handtekening. De digitale handtekening zorgt ervoor dat de transactie niet door anderen vervalst kan worden en garandeert de identiteit van de persoon die de transactie uitvoert. (http://www.telenet.be, 2006)

De communicatie tussen de computer van de gebruiker en de server van de bank verloopt over een beveiligde verbinding. De informatie wordt versleuteld of geëncrypteerd verzonden zodat ze niet door onbevoegden kan gelezen of gewijzigd kan worden. Enkel met behulp van de juiste sleutel, beveiligd met een geheim wachtwoord, kan de informatie ontcijferd worden.

Een bijkomende mogelijkheid die door sommige banken aangeboden wordt is de digitale kluis. In deze kluis kan men bestanden plaatsen die belangrijk zijn voor uzelf of voor uw bedrijf. Voorbeelden hiervan zijn codes van software, personeelsdossiers, juridische documenten, jaarcijfers, …

8.3 E-government

E-government wordt gedefinieerd als een fundamenteel nieuwe, geïntegreerde en permanente manier om openbare diensten te leveren via een optimaal gebruik van de informatie- en communicatietechnologie. E-Government beperkt er zich dus niet louter en alleen toe informatie op de websites van de overheidsbesturen te plaatsen, maar houdt ook een grondige reorganisatie in van de structuur en de werking van de besturen (wat men aanduidt met de term "back office"). De administratieve procedures, zoals het verzamelen, verwerken en elektronisch uitwisselen van gegevens binnen of tussen de besturen moeten aangepast worden aan de levering van elektronische overheidsdiensten die beantwoorden aan de behoeften van de burgers en de ondernemingen. Een voorbeeld hiervan is het aanvragen en invullen van formulieren via een elektronisch loket. Bovendien is het eenvoudiger voor administratieve diensten om online contacten te leggen met de burger of de onderneming en om zo procedures versnellen.
(http://www.mineco.fgov.be, 2006)

Belangrijke voordelen van e-government zijn onder andere snelheid, bereikbaarheid en doorzichtigheid. Snelheid verbetert omwille van het feit dat gebruikers zich niet meer fysiek naar het loket moeten begeven. Bereikbaarheid duidt op het feit dat de elektronische loketten zeven dagen op zeven en vierentwintig uur op vierentwintig open zijn. Aangezien de burgers en ondernemingen meer betrokken zijn bij het besluitvormingsproces van de overheid, is er sprake van meer doorzichtigheid. (http://www.mineco.fgov.be/, 2006)

Een belangrijke ontwikkeling op het gebied van e-government is het gebruik van de elektronische identiteitskaart.

8.4 Medische toepassingen

Ook in de medische sector is er sprake van informatisering. Een voordeel hiervan is dat er steeds minder op papier wordt bijgehouden. Er wordt gebruik gemaakt van gegevensuitwisseling via het EDI-systeem (Electronic Data Interchange). Hierbij worden enkelvoudige berichten verstuurd tussen twee partijen. Een probleem dat zich hier stelt, uit zich in toegang tot medische dossiers. Vaak willen meerdere zorgverleners toegang tot het medische dossier van een patiënt. Toepassing van een één-op-één gegevensuitwisseling zou hier resulteren in een chaos van gegevensstromen. Om dit probleem op te lossen, zou elke zorgverlener zich kunnen aansluiten op een netwerk, waarbij elke zorgverlener via één enkele verbinding communiceert met talloze andere partijen. Deze methode is mogelijk via het Internet. Een mogelijk hulpmiddel voor dit systeem is het elektronische patiëntendossier (EPD). Met een elektronisch patiëntendossier kan alle informatie op elke plek zowel binnen als buiten de zorginstelling direct opgeroepen en bijgewerkt worden. Het doel hiervan is dat de zorgverlening aan de patiënt efficiënter en beter wordt, omdat iedere zorgverlener in de keten van zorg rondom een patiënt met dit systeem op ieder moment kan beschikken over relevante informatie over de patiënt. Dit voorkomt dubbele onderzoeken, tijdverlies met het opvragen van gegevens, etc. Het efficiënt opslaan van en beschikken over patiëntgegevens komt ook de patiënt ten goede. Immers, samen met de informatie-uitwisseling kan ook informatie over de kwaliteit en effectiviteit van de zorgverlening worden vastgelegd. Hieruit kan de

patiënt informatie halen over instellingen en zorgverleners die het best passen bij zijn zorgvraag. Zo kan hij bijvoorbeeld bepalen waar de wachtlijst voor een bepaalde behandeling het kortst is. (http://www.vbk.nl/nl/htm/nieuws/actueel, 2006)

8.5 E-cash

Als men in de reële wereld contant betaalt, blijft men anoniem. Ook op het Internet is anonimiteit voor veel gebruikers belangrijk. Hierdoor is er een elektronische vorm van contant geld ontstaan. Elektronisch contant geld is eenvoudig te realiseren door gebruik te maken van publieke sleutel cryptografie en digitale handtekeningen. Het uitvoeren van betalingen met e-cash is gelijkaardig aan betalen met cash geld. In plaats van geld “uit de muur” te halen en het vervolgens bij de hand te hebben, installeert de klant een digitale portemonnee op zijn harde schijf. Voordat het geld op de harddisk wordt gedownload, moet het uit een digitale kluis, vergelijkbaar met een gewone bankkluis, gehaald worden. Door een versleuteld bericht van een digitale handtekening te voorzien en naar de bank te sturen geeft de klant opdracht geld van zijn bankrekening om te zetten in digitaal geld. De bank kan het bericht ontcijferen door gebruik te maken van zijn privé sleutel. Met behulp van de digitale handtekening weet de bank dat de klant toestemming geeft voor de omwisseling. Het geld wordt bijgevolg van de gewone rekening van de klant omgewisseld in digitaal geld, waarna dit in de kluis gedeponeerd wordt. Vanuit de kluis kan de klant het naar zijn harddisk halen. Voor winkeliers geldt hetzelfde verhaal. Tijdens een transactie ontvangen zij digitaal geld waaraan ze kunnen zien dat het van de bank komt. Ze nemen contact op met de bank om zeker te weten dat het digitale geld niet dubbel is uitgegeven, waarna de rekening van de winkelier wordt gecrediteerd. Met digitaal geld kan de klant zo producten kopen bij elke virtuele winkel, die digitaal geld accepteert. Digicash en Netcash zijn twee voorbeelden van e-Cash. Een andere populaire e-cash provider is PayPal. (http://www.ework.nl/struc/docs/020305.htm, 2006)

Hoofdstuk 9 Praktijk: VenSoc

Om het theoretisch onderzoek wat kracht bij te zetten, werd besloten een praktijkvoorbeeld van één van de toepassingen uit te werken. Als praktijkvoorbeeld werd gekozen voor een gedetailleerde uitwerking van aangiften in de vennootschapbelasting via het Internet.

In België wordt vennootschapsbelasting geheven op grond van het Wetboek van de Inkomensbelastingen. Vennootschapsbelasting geldt enkel voor binnenlandse vennootschappen. Voor inrichtingen in België van buitenlandse rechtspersonen geldt een vergelijkbare belasting van niet-inwoners. Vennootschappen zijn belastbaar op het bedrag van de winst, zoals die teruggevonden wordt in de gereserveerde winsten, in de uitgekeerde dividenden of in bepaalde niet aftrekbare uitgaven, de zogenaamde verworpen uitgaven. Van deze winst kunnen nog bepaalde aftrekken gebeuren, zoals de investeringsaftrek of de compenseerbare verliezen van vroegere jaren. Om dubbele belasting te vermijden zijn er ook vrijstellingen voor dividenden ontvangen van andere vennootschappen en voor meerwaarden op aandelen van andere vennootschappen.

De federale overheidsdienst financiën heeft een aparte website opgericht met een uitgebreide uitleg over aangiften in de vennootschapsbelasting via het Internet. De website is getiteld: VenSoc

9.1 VenSoc (http://minfin.fgov.be, 2006)

Met behulp van de applicatie VenSoc heeft men de mogelijkheid om de aangiften in de vennootschapsbelasting via elektronische weg op te stellen en in te dienen. Iedereen die namens een vennootschap een aangifte moet indienen, kan gebruik maken van VenSoc. Ze moeten echter wel gemachtigd zijn door de vennootschap. VenSoc vereist geen voorafgaande registratie van de volmachten en de gebruikelijke papieren volmacht volstaat.

9.1.1 Technische vereisten

Slechts indien aan een aantal technische vereisten voldaan is, kan de applicatie VenSoc gebruikt worden. Men dient over een digitaal certificaat te beschikken en de vereiste software moet op voorhand geïnstalleerd worden

Digitaal certificaat

Gegevens zoals de vennootschapsbelasting die elektronisch verstuurd worden, zijn vertrouwelijk van aard. Bijgevolg moet de elektronische verbinding beveiligd worden. Om dit te verwezenlijken, maakt men gebruik van een digitaal certificaat.

Een digitaal certificaat kan men min of meer vergelijken met een digitale identiteitskaart waarop een beperkt aantal gegevens voorkomen met betrekking tot de houder van het certificaat. Zo komen op het certificaat de identiteit van de houder, de publieke sleutel verbonden aan de houder, de geldigheidsduur en de klasse van het certificaat voor. (zie ook hoofdstuk 7)

Er zijn twee verschillende soorten certificaten die men kan gebruiken. Een eerste is de elektronische identiteitskaart (eID). Deze kan opgevraagd worden bij de dienst bevolking van de stad of gemeente waarin men woont. Vervolgens heeft men een kaartlezer nodig om de PC te laten communiceren met de eID. Er bestaan verschillende soorten kaartlezers. Meestal is er sprake van externe lezers die men via een USB-poort aansluit op de PC.

Een tweede optie is een digitaal certificaat klasse 3. Dit is te vergelijken met een elektronische identiteitskaart. Er komen heel wat gegevens voor van de houder van het certificaat, zoals de identiteit van de houder, de publieke sleutel die verbonden is met de houder van het certificaat, de geldigheidsduur en de klasse van het certificaat.

Zoals reeds vermeld dienen de gebruikers van VenSoc te beschikken over een digitaal certificaat klasse 3. Dit certificaat is het meest beveiligde certificaat. Hoe hoger de klasse, hoe meer het certificaat gecontroleerd wordt. De certificaten kan

men aanvragen bij drie erkende Certificatie Autoriteiten: Certipost, Global Sign en Isabel.

Software

Om VenSoc succesvol te kunnen gebruiken dient een gebruiker te beschikken over een internetverbinding, liefst een snelle zoals een breedband- of adsl-verbinding. Daarnaast moet hij beschikken over een browser zoals Internet Explorer. Hiervan heeft men versie 6.x nodig. Het programma Adobe Acrobat reader versie 7 of hoger moet eveneens geïnstalleerd te zijn. Indien de gebruiker kiest voor eID, moet hij eveneens in het bezit zijn van software voor het installeren van de kaartlezer en software voor het gebruik van de elektronische eID. Hij moet ook software bezitten voor de creatie van PDF-bestanden (portable document format). Een laatste voorwaarde is het aanwezig zijn van Java runtime versie 1.4.2

9.1.2 Aangiften en bijlagen

Als men een digitaal certificaat klasse 3 heeft bekomen en de benodigde software geïnstalleerd is, kan de applicatie VenSoc gebruikt worden.

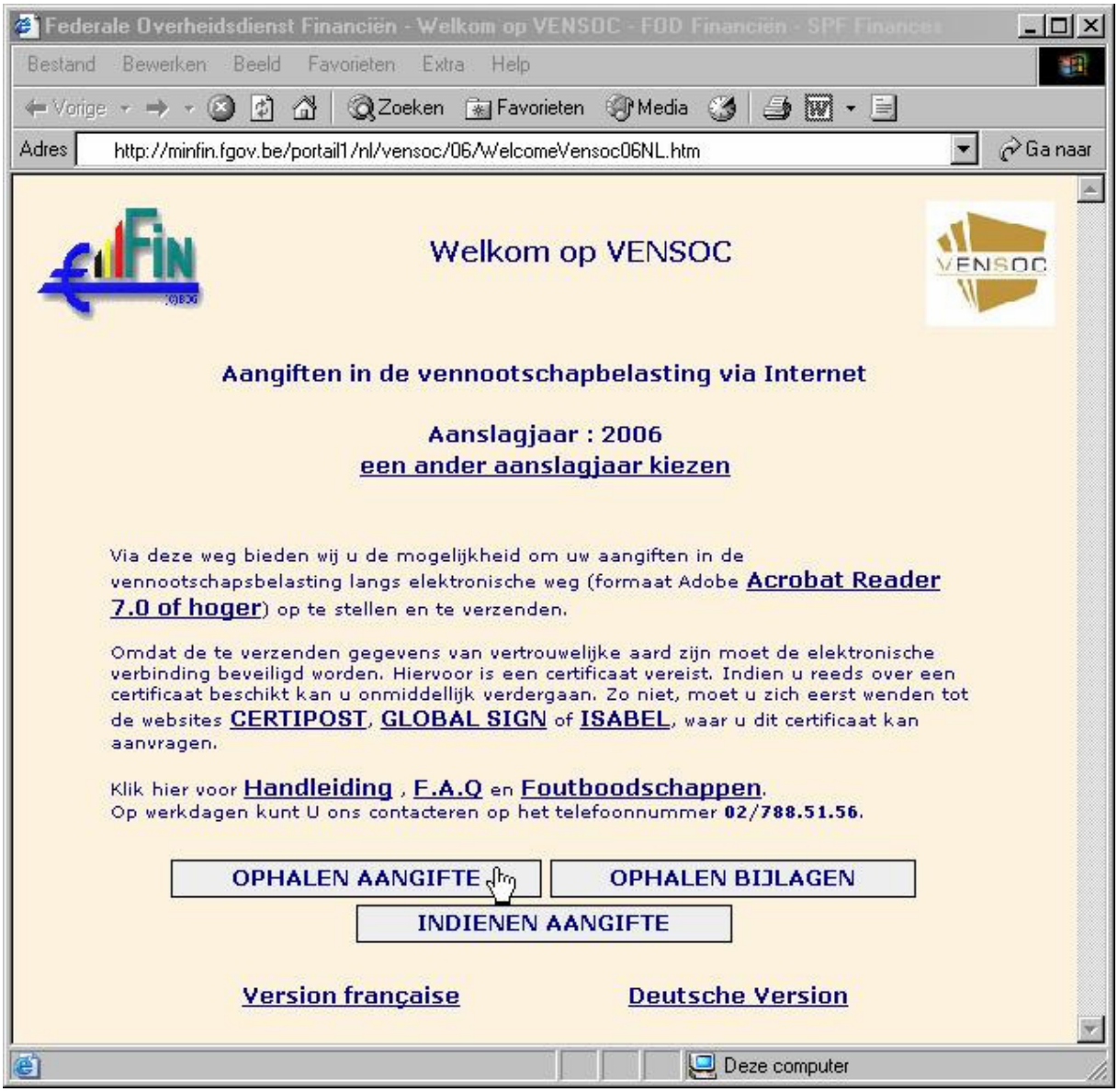
Stap 1: Creëren van een directory of map

Om de verzending succesvol te laten verlopen, is het noodzakelijk dat per aangifte die zal verzonden worden een aparte directory of map gecreëerd wordt waarin naast de elektronische aangifte ook de bijbehorende bijlagen worden opgeslagen. Het volledig te verzenden pakket moet worden samengebracht in éénzelfde map.

Stap 2: Downloaden en invullen van de VenSoc-aangifte

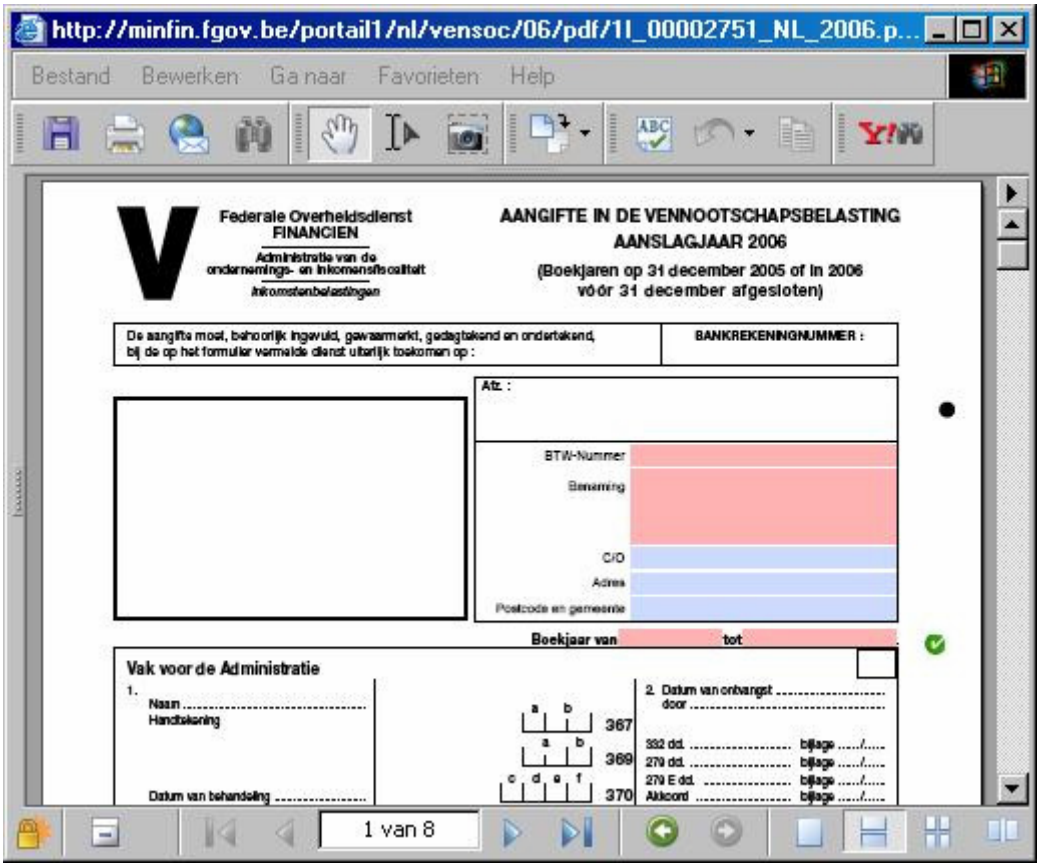
Eerst moet de gebruiker de VenSoc-aangifte ophalen. Deze aangifte is een elektronische versie van een aangifte in de vennootschapsbelasting. Het heeft dezelfde waarde als een traditionele papieren aangifte en wordt uiteraard volgens dezelfde reglementering als de papieren versie ingevuld. De opgave voor de investeringsaftrek is reeds als bijlage bij de VenSoc-aangifte toegevoegd.

Figuur 9.1: Ophalen aangifte vensoc



Bron: http://minfin.fgov.be/ (2006)

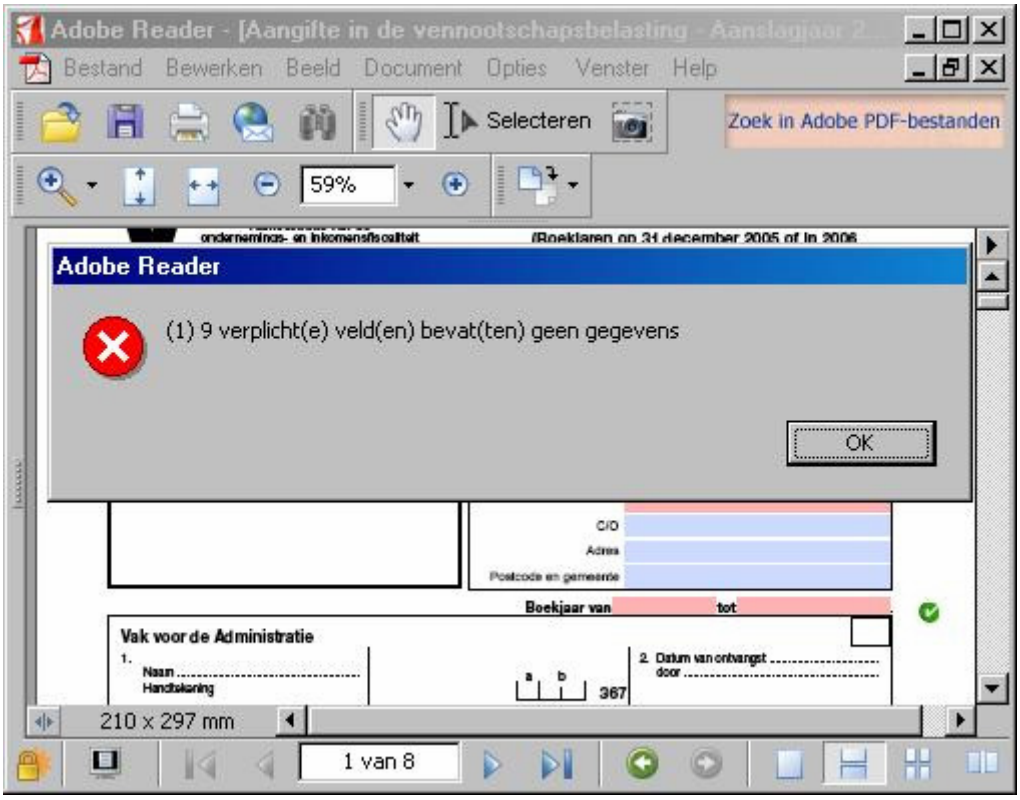
Figuur 9.2: Aangifte Vensoc



Bron: http://minfin.fgov.be/ (2006)

De VenSoc aangifte moet worden opgeslagen in de map die in de eerste stap gecreëerd werd, onder de 1I_00002751_NL_2006.pdf. Het invullen van de VenSoc-aangifte gebeurt niet online. Dit heeft als voordeel dat het invullen kan gespreid worden over de tijd. Daarnaast kan de aangifte via elektronische weg naar andere personen gestuurd worden, zoals bijvoorbeeld een financieel raadgever. Het gebruiksgemak van de VenSoc-aangifte wordt vergroot door het aanbieden van enkele hulpschermen. Ook materiële vergissingen worden vermeden door het intern inbouwen van validaties. Een voorbeeld van zo een aangifte vindt men in de bijlage.

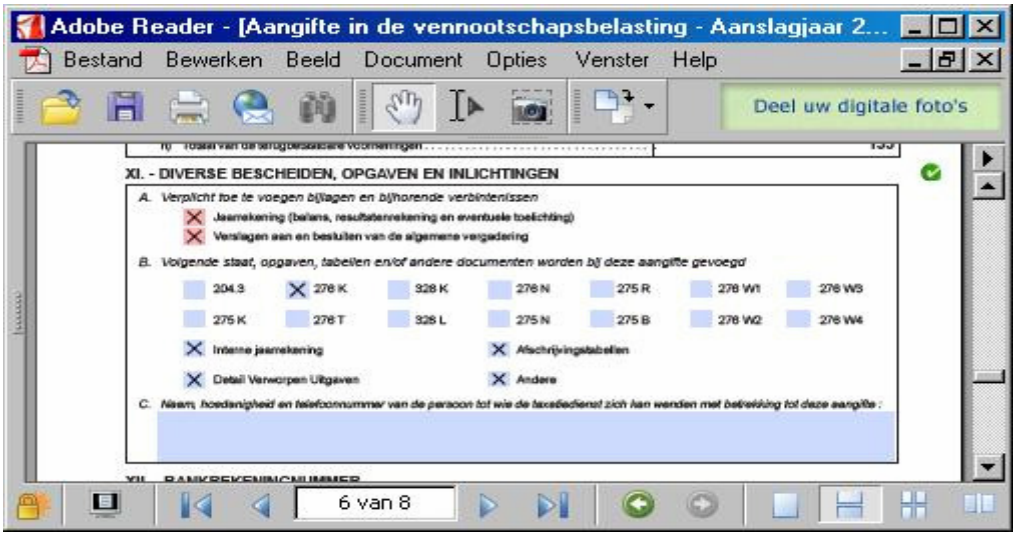
Figuur 9.3: Intern ingebouwde validaties



Bron: http://minfin.fgov.be (2006)

Indien de gebruiker nog bijlagen zal toevoegen dient hij in vak XI aan te duiden welke hij zal toevoegen. Enkele bijlagen zijn steeds verplicht zoals de neergelegde jaarrekening en het verslag van de Algemene Vergadering.

Figuur 9.4: Aanduiden bijlagen

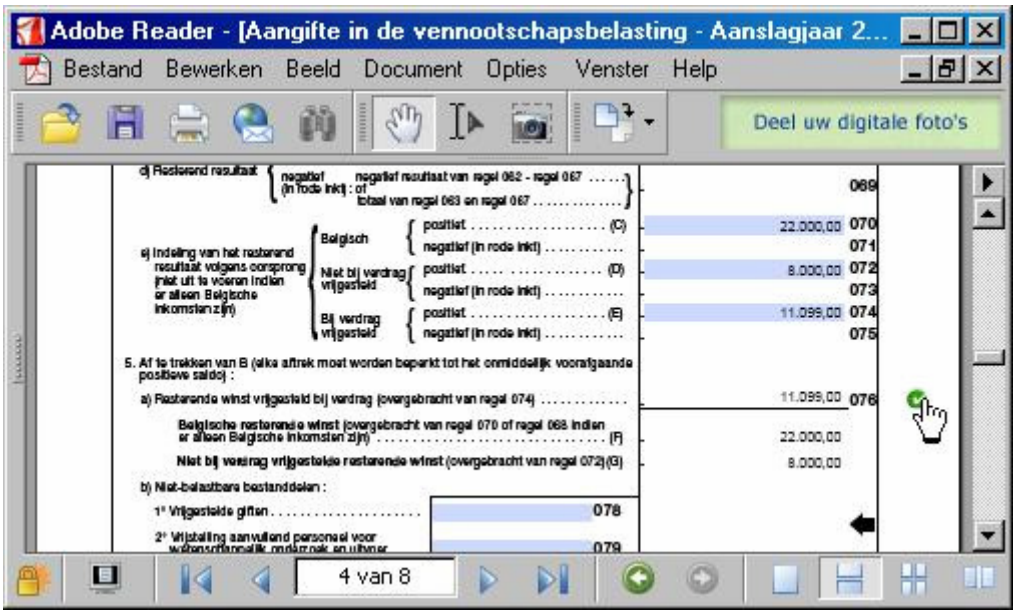


Bron: http://minfin.fgov.be (2006)

De taal van de VenSoc-aangifte moet overeenstemmen met de taal van de papieren aangifte vennootschapsbelasting die aan de vennootschap werd toegezonden.

Wanneer de aangifte volledig ingevuld is, wordt de validatieknop aangeklikt. Deze knop bevindt zich op elke pagina van de VenSoc-aangifte.

Figuur 9.5: Validatieknop



Bron: http://minfin.fgov.be (2006)

Indien er nog onvolkomenheden aanwezig zijn, dan worden deze aangegeven. Zolang er één of meer foutmeldingen verschijnen, zal het onmogelijk zijn om de aangifte elektronisch in te dienen.

Figuur 9.6: Foutmelding

Bron: http://finmin.fgov.be (2006)

Indien de aangifte geen onvolkomenheden meer bevat, krijgt men volgende melding

Figuur 9.7: Goedkeuring

Bron: http://finmin.fgov.be (2006)

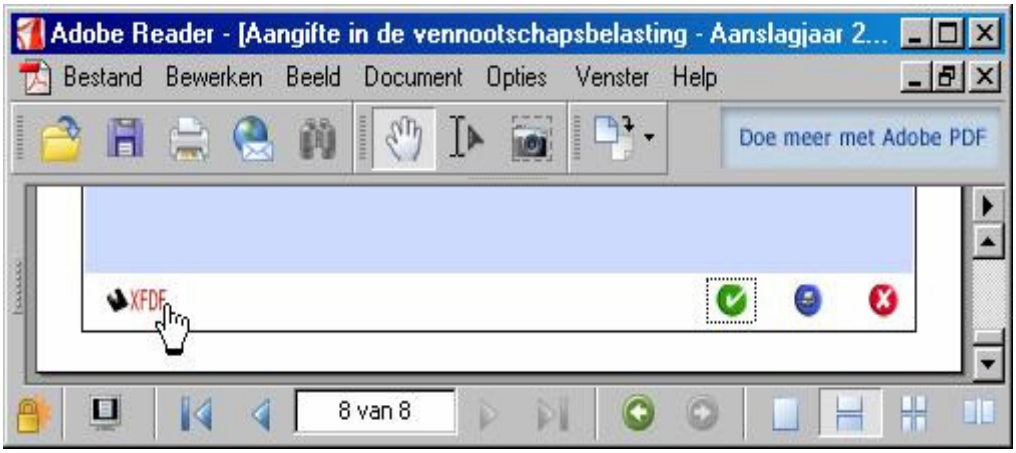
Stap 3: Creatie van het XFDF-bestand

Als de VenSoc-aangifte ingevuld en gevalideerd is, moet dit PDF-document als een XFDF-bestand opgeslagen worden. Ook dit bestand wordt opgeslagen in de map die gecreëerd werd in stap 1.

Het creëren van een XFDF-bestand kan op twee verschillende manieren gebeuren. Bij de eerste manier maakt men gebruik van de menubalk in Adobe Acrobat reader versie 7.x. Men opent de VenSoc-aangifte. Vervolgens kiest men in de menubalk van Acrobat de optie document. Daarna kiest men formulier invullen en formuliergegevens exporteren. Als laatste kiest men “opslaan data als type XFDF”. In de professionele versie van Acrobat gebeurt dit op een gelijkaardige manier.

Bij de tweede manier maakt men gebruik van de knop “opslaan XFDF-bestand” die zich onderaan links bevindt op het einde van de VenSoc-aangifte. Hierbij wordt het XFDF-bestand automatisch gecreëerd.

Figuur 9.8: XFDF creatie

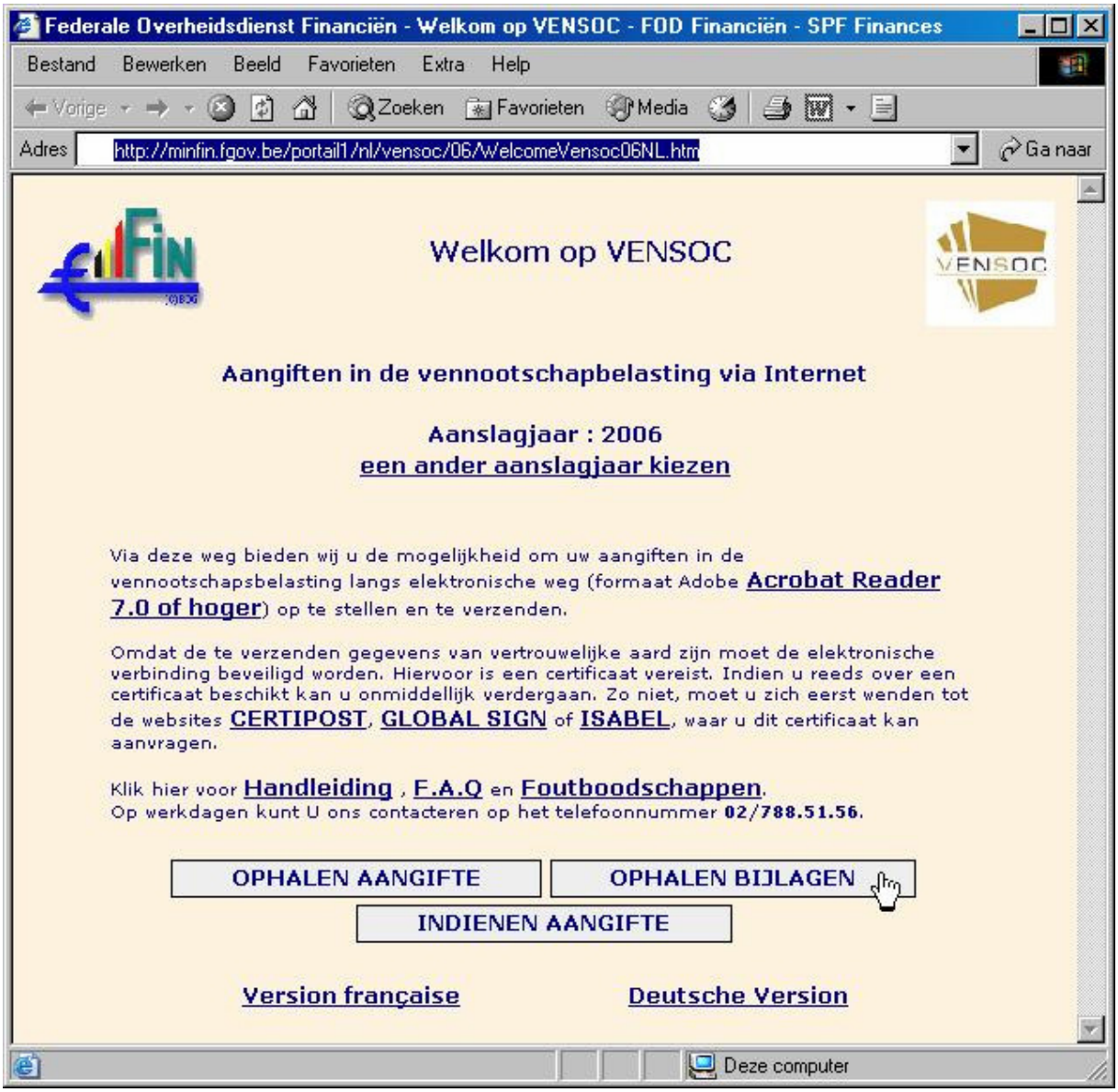


Bron: Bron: http://finmin.fgov.be (2006)

Stap 4: Ophalen van de bijlagen

Zoals reeds vermeld heeft de gebruiker in vak XI aangekruist welke bijlagen aan de aangifte zullen worden toegevoegd. Deze bijlagen zijn elektronisch beschikbaar via de Finform-website van de Financiële Overheidsdienst (FOD) Financiën. Door te klikken op “ophalen bijlagen” in het beginscherm van de VenSoc website wordt de Finform-website geopend. Hier kan men de gewenste bijlage zoeken. Ook dit formulier dient na aanvulling opgeslagen te worden in de map die gecreëerd werd in stap 1.

Figuur 9.9: Ophalen bijlagen



Bron: http://finmin.fgov.be (2006)

Bij de bijlagen is er een verschil tussen de gestandaardiseerde bijlagen en overige bijlagen. In onderstaande tabel wordt een overzicht gegeven van de gestandaardiseerde bijlagen.

Tabel 9.1: gestandaardiseerde bijlagen

Opgave	Omschrijving	Verplichte bestandsnaam
204.3	Staat van de waardeverminderingen voor waarschijnlijke verliezen en van de voorzieningen voor risico's en kosten	1I_00002043_NL_2006.pdf
275B	Vrijstelling van meerwaarden op zeeschepen	1I_0000275B_NL_2006.pdf
275K	Gespreide belasting van meerwaarden op bepaalde effecten	1I_0000275K_NL_2006.pdf
275N	Belastingkrediet	1I_0000275N_NL_2006.pdf
275R	Investeringsreserve	1I_0000275R_NL_2006.pdf
276K	Gespreide belasting meerwaarden	1I_0000276K_NL_2006.pdf
276N	Vrijstelling van meerwaarden op bedrijfsvoertuigen	1I_0000276N_NL_2006.pdf
276T	Tabel voor de berekening van de vrijstelling voor bijkomend personeel	1I_0000276T_NL_2006.pdf
276U	Investeringsaftrek	Is automatisch toegevoegd als bijlage bij de Vensoc-aangifte.
276 W1	Vrijstelling voor bijkomend personeel tewerkgesteld voor wetenschappelijk onderzoek	1I_000276W1_NL_2006.pdf
276 W2	Vrijstelling voor bijkomend personeel tewerkgesteld voor de uitbouw van het technologisch potentieel van de onderneming	1I_000276W2_NL_2006.pdf
276 W3	Vrijstelling voor bijkomend personeel tewerkgesteld als diensthoofd uitvoer	1I_000276W3_NL_2006.pdf
276 W4	Vrijstelling voor bijkomend	1I_000276W4_NL_2006.pdf

	personeel tewerkgesteld als diensthoofd van de afdeling Integrale kwaliteitszorg	
328K	Opgave van degressief af te schrijven vaste activa	1I_0000328K_NL_2006.pdf
328L	Opgave van de vaste activa waarvoor van degressieve afschrijving wordt afgezien	1I_0000328L_NL_2006.pdf

Bron: http://finmin.fgov.be (2006)

Stap 5: Creëren van overige bijlagen

De bijlagen die niet vastliggen volgens het model van de FOD Financiën dienen zelf gecreëerd te worden. Het gaat hier onder andere over de jaarrekening en het verslag van de Algemene Vergadering. Deze bijlagen moeten in PDF formaat aangemaakt worden. Ze mogen niet groter zijn dan vijf Megabyte. Tenslotte kunnen er slechts zes dergelijke bijlagen worden toegevoegd. Deze bijlagen dienen opgeslagen te worden in dezelfde map die gecreëerd werd in stap 1.

De verplichte namen van de overige bijlagen vindt men in onderstaande tabel

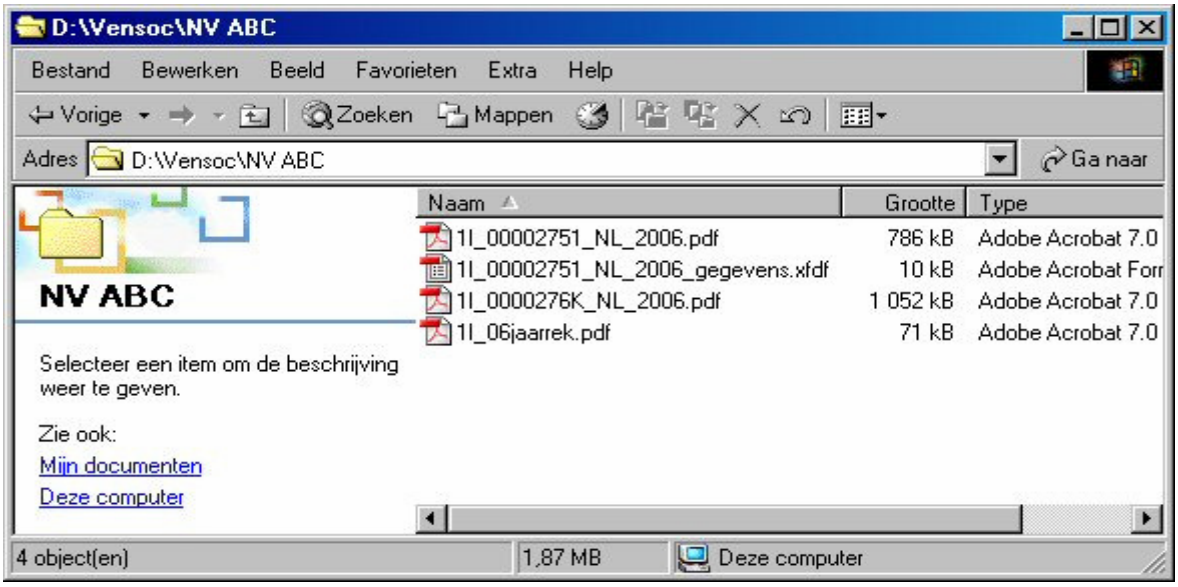
Tabel 9.2: overige bijlagen

Omschrijving	**Verplichte bestandsnaam**
1. Jaarrekening	1I_06jaarrek.pdf
2. Verslagen aan en besluiten van de algemene vergadering	1I_06versAV.pdf
3. Interne jaarrekening	1I_06intjaarrek.pdf
4. Afschrijvingstabellen	1I_06afschr.pdf
5. Detail verworpen uitgaven	1I_06detvu.pdf
6. Diverse	1I_06diversen.pdf

Bron: http://finmin.fgov.be (2006)

Uiteindelijk zal de in stap 1 gecreëerde map er als volgt uitzien.

Figuur 9.10: Gecreëerde Map of Directory

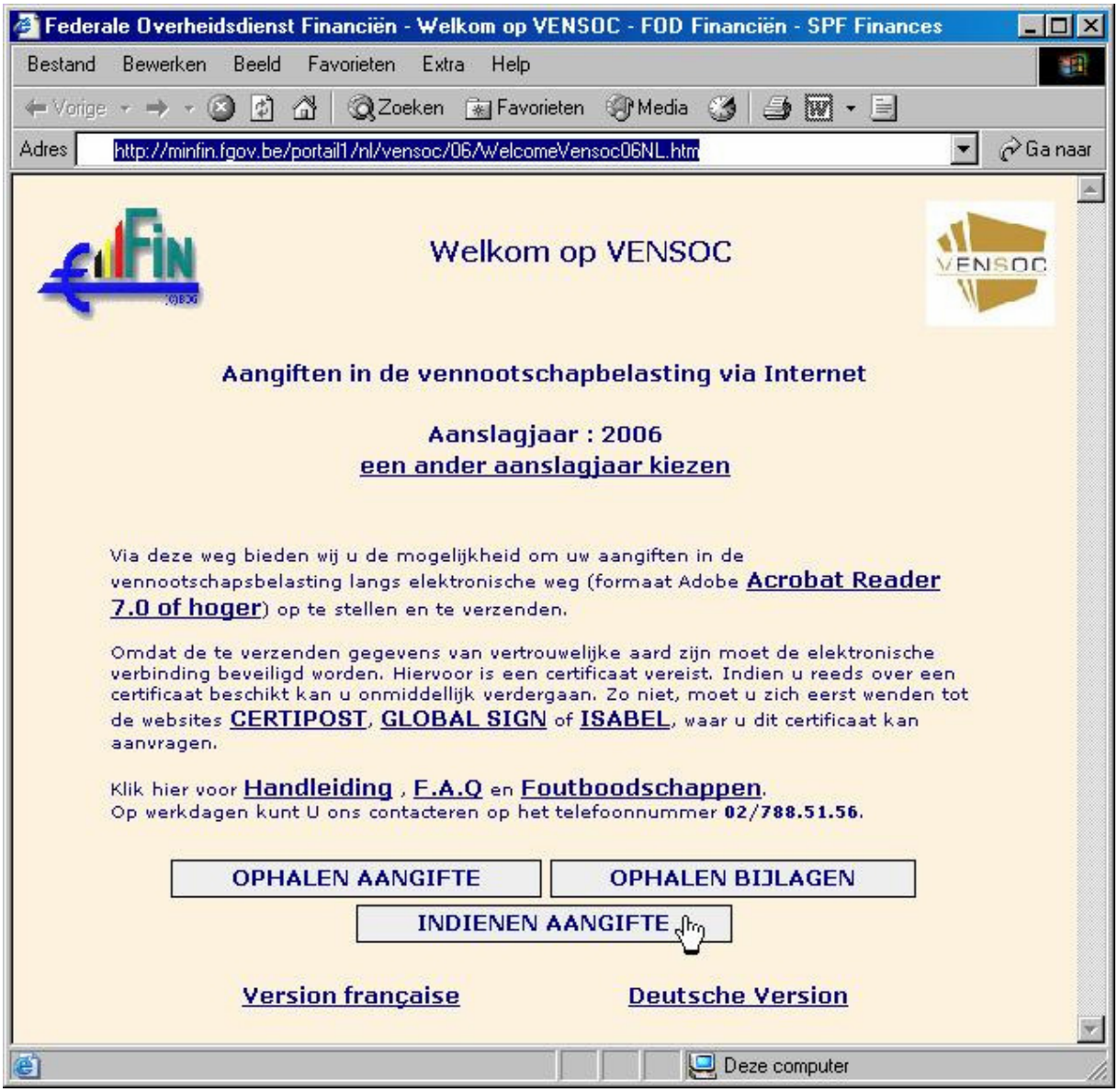


Bron: http://finmin.fgov.be (2006)

Stap 6: Indienen van de aangifte

Als de XFDF-aangifte en alle bijlagen ingevuld en samengebracht zijn in één map, kunnen ze ingediend worden. Door te klikken op “indienen aangifte” wordt een beveiligde internetverbinding tot stand gebracht en wordt de gebruiker met behulp van een digitaal certificaat klasse 3 geïdentificeerd.

Figuur 9.11: Indienen aangifte



Bron: http://finmin.fgov.be (2006)

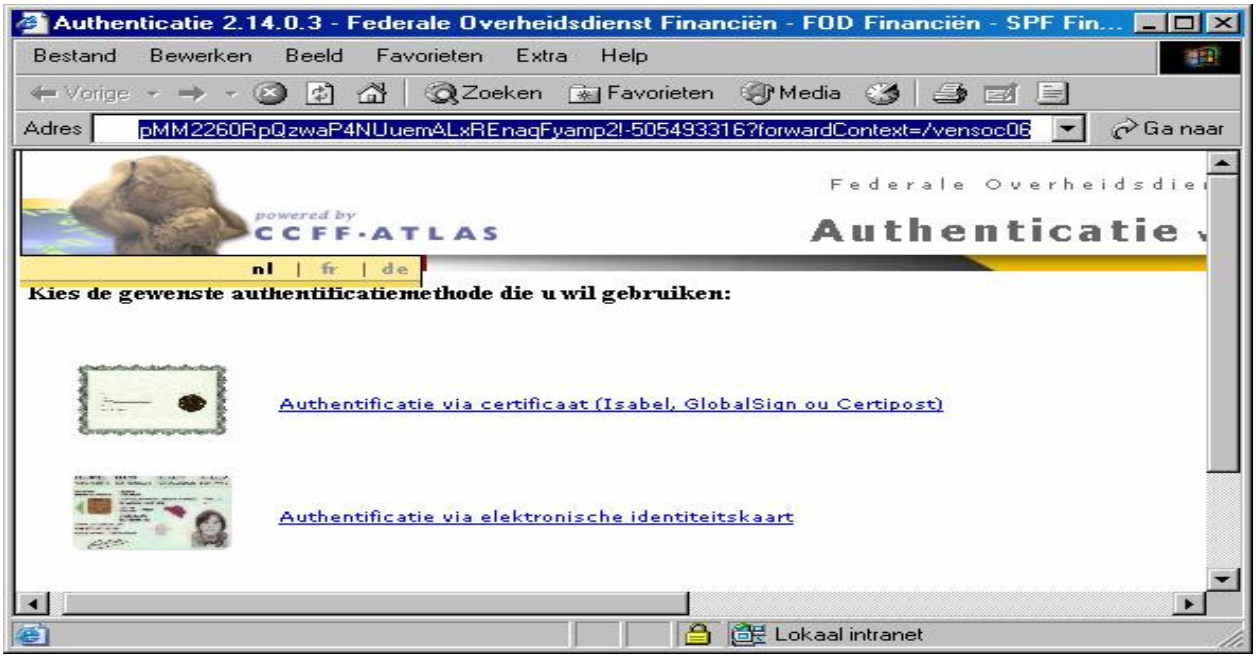
Als men VenSoc voor de eerste keer gebruikt, zal men gevraagd worden om CAPICOM te installeren.

Figuur 9.12: CAPICOM installeren

Bron: http://finmin.fgov.be (2006)

Als CAPICOM geïnstalleerd is, moet men vervolgens kiezen op welke manier men de aangifte zal indienen. Men krijgt de keuze tussen enerzijds authentificatie via certificaat en anderzijds authentificatie via elektronische identiteitskaart.

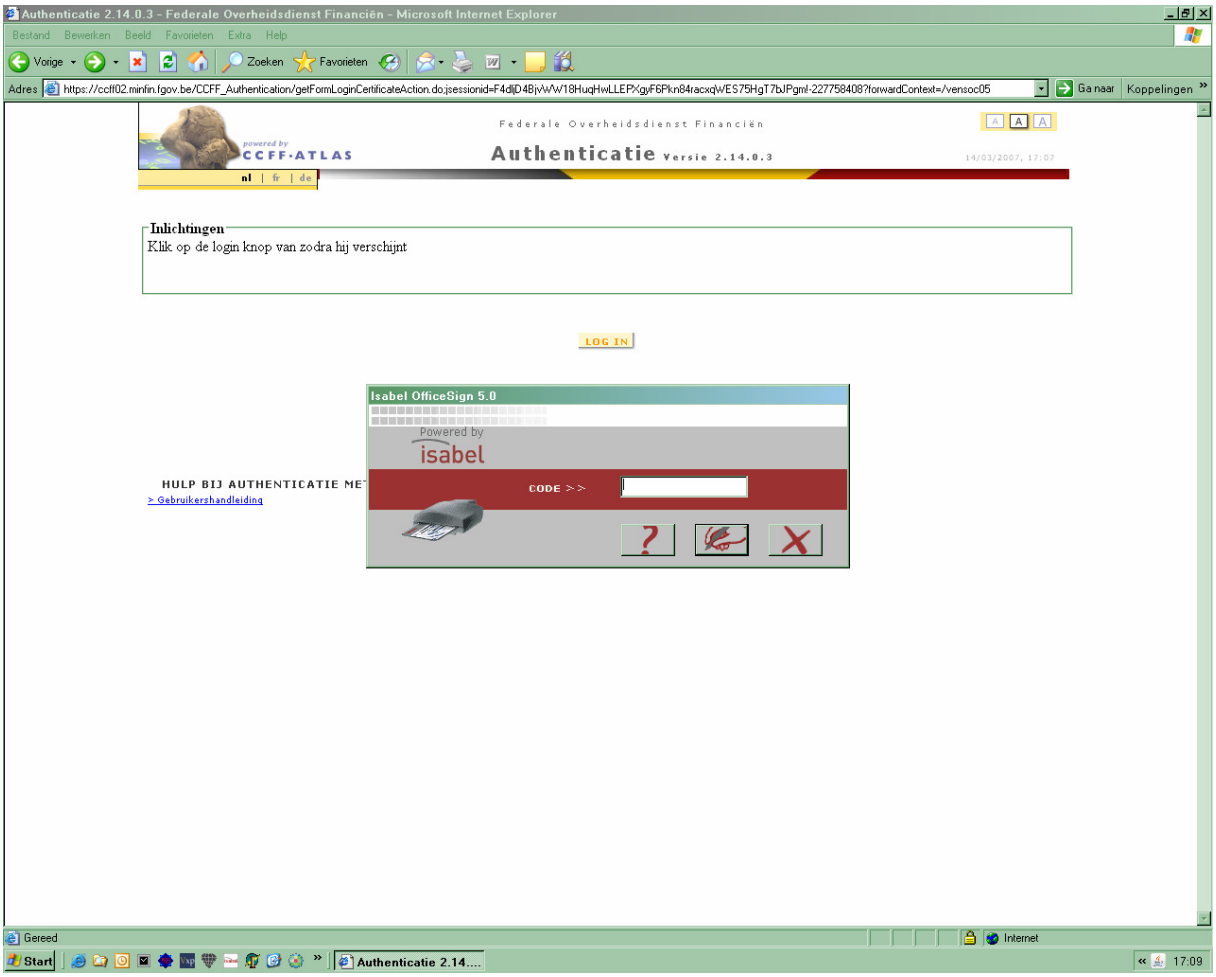
Figuur 9.13: Methode van authentificatie



Bron: http://finmin.fgov.be (2006)

Indien men gebruik maakt van een digitaal certificaat van de CA Isabel, krijgt men vervolgens volgend inlogscherm.

Figuur 9.14: inlogscherm Isabel



Bron: HLB Fineko (2007)

Bij andere certificaten of bij de eID methode bekomt men gelijkaardige beveiligingsmaatregelen.

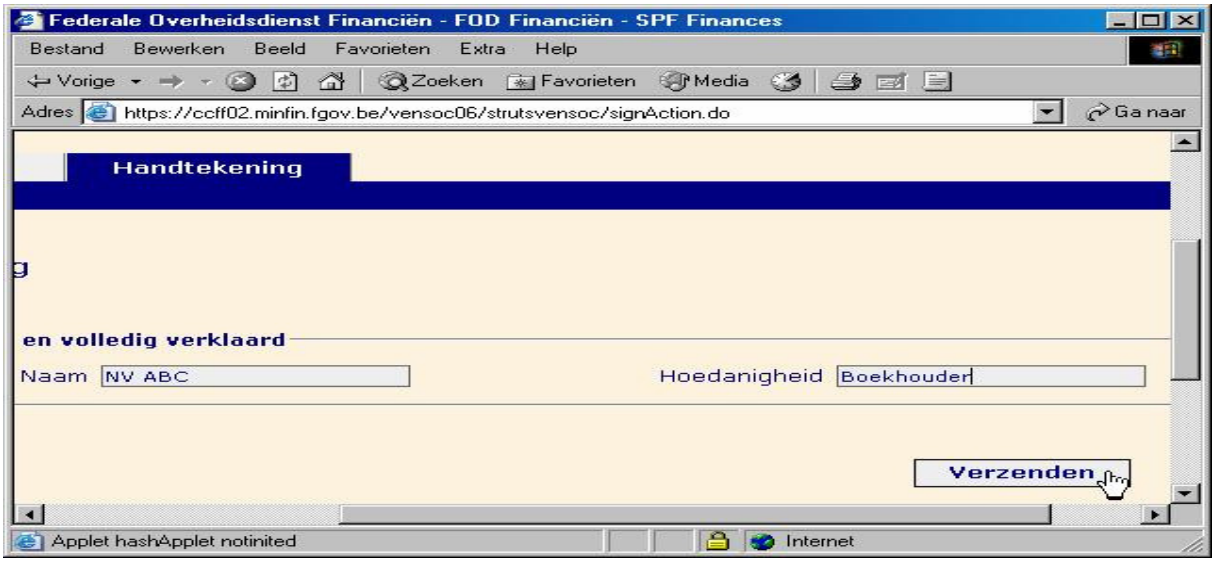
Wanneer men op het tabblad “aangifte” klikt, moet men de locatie van de XFDF-versie van de VenSoc-aangifte ingeven. Het systeem zal de aangekruiste bijlagen automatisch zoeken in dezelfde map als de aangifte en deze er ook aan toevoegen.

Figuur 9.15: Tabblad aangifte

Bron: http://finmin.fgov.be (2006)

Vervolgens kiest men het tabblad “handtekening”. De gebruiker dient zijn naam en hoedanigheid in te vullen in het daarvoor voorziene handtekeningvak.

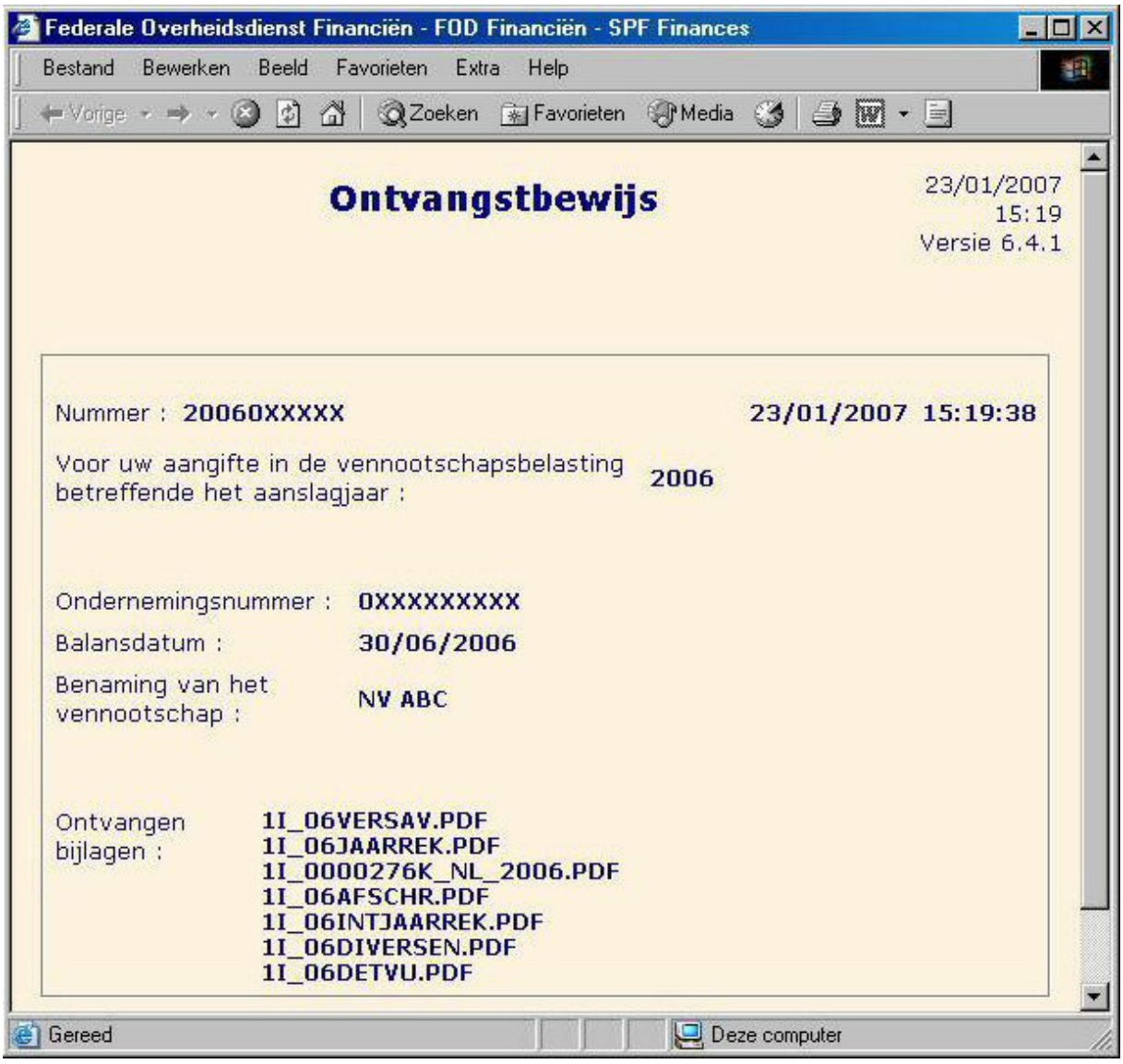
Figuur 9.16: Tabblad Handtekening



Bron: http://finmin.fgov.be (2006)

De aangifte en bijlage worden elektronisch verzonden naar FOD Financiën. De bestanden in de map worden automatisch gecomprimeerd tot één te verzenden bestand. Dit bestand blijft ook op de PC van de gebruiker bewaard. Als de verzending succesvol is verlopen, ontvangt de gebruiker een ontvangstmelding. Ook dit ontvangstbewijs wordt geplaatst in de map die in stap 1 gecreëerd werd. Het bevat een uniek volgnummer, een ondernemingsnummer, naam en balansdatum van de vennootschap, datum en uur van inzending en een lijst van meegezonden bijlagen.

Figuur 9.17: Ontvangstbewijs



Bron: http://finmin.fgov.be (2006)

9.1.3 Extra Informatie

Indien men een aangifte via elektronische weg verstuurd mag men in geen geval nog een papieren aangifte versturen voor de vennootschap. De VenSoc-aangifte kan na inzending niet meer op elektronische manier geraadpleegd of gewijzigd worden. Indien men toch wenst te wijzigen of extra bijlagen wenst in te dienen, moet men contact opnemen met de bevoegde taxatiedienst.

9.2 Papieren versus elektronische aangifte van vennootschapsbelasting

Een elektronische aangifte heeft enkele voordelen ten opzichte van de papieren aangifte van de vennootschapsbelasting. De aangifte kan sneller ingevuld worden en sneller verwerkt worden. Aan de ene kant bespaart dit tijd om zich te richten op andere belangrijke zaken binnen de vennootschap. Aan de andere kant bespaart het de FOD Financiën eveneens tijd in het controleren van de ingevulde aangiftes. Een ander voordeel is de lagere kostprijs. Een elektronische aangifte is immers goedkoper dan een papieren aangifte. Zo worden de dossier- en behandelingskosten voor de FOD Financiën een stuk goedkoper. De aangiftes moeten immers niet meer handmatig in het controleprogramma ingegeven worden, maar kunnen er rechtstreeks ingeladen worden. Een laatste voordeel is dat de beveiliging gegarandeerd is door gebruik te maken van digitale certificaten en digitale handtekeningen.

Daarnaast worden er vaak nog voordelen voor de KMO's (Kleine en Middelgrote Ondernemingen) aangehaald. Deze bedrijven hebben immers geen specialisten op het gebied van vennootschapsbelastingen. Hierdoor is het voor hen moeilijker om hun vennootschapsbelasting te verlagen. De grote bedrijven beschikken hier wel over en kunnen hun fiscaliteit optimaliseren. Er wordt gezegd dat dankzij deze elektronische aangifte de doorzichtigheid en duidelijkheid van de vennootschapsbelastingen vergroot wordt zodat ook deze KMO's hun vennootschapsbelastingen kunnen verlagen. De heer S. De Prins, accountant te HLB

Fineko ontkent dit echter. Hij vermeldt immers dat de aangifte identiek blijft zowel elektronisch als papier. De berekeningen moeten gewoon manueel gedaan en ingevuld worden. Dit zorgt ervoor dat de berekeningen voor zowel de papieren als elektronische aangifte hetzelfde blijven. Hierdoor hebben grote bedrijven nog steeds het voordeel omdat zij zich specialisten kunnen veroorloven die hun fiscaliteit kunnen bevorderen. KMO's kunnen dit echter niet.

Een eventuele opmerking die hierbij gemaakt kan worden, is dat VenSoc in de toekomst voorzien zou kunnen worden van een soort van artificiële of analytische efficiëntie. Deze toepassing zou het voor KMO's mogelijk kunnen maken om hun fiscaliteit te verbeteren. Bijgevolg hoeven zij geen "dure" expert aan te nemen die probeert hun fiscaliteit te verbeteren. Ze kunnen zich deze toch niet veroorloven, in tegenstelling tot grote bedrijven die hierdoor een voordeel behalen op het gebied van vennootschapsbelasting.

9.3 Economie en Vennootschapsbelasting

In België is er sprake van een relatie tussen vennootschapsbelasting enerzijds en tewerkstelling en groei anderzijds. Ten opzichte van andere Europese landen heeft België een hoge aanslagvoet met betrekking tot de vennootschapsbelasting. Met een percentage van 33,99 % blijft men nog steeds boven het gemiddelde van Europa (25,3 %) hangen. Voor 2002 was dit verschil vijftien procent. Toen bedroeg de aanslagvoet immers 40,17 %. Nu scheelt het slechts acht procent. Terwijl de gemiddelde aanslagvoet in Europa daalde, bleef de vennootschapsbelasting in België stabiel. Dit heeft er waarschijnlijk voor gezorgd dat het concurrentievermogen van de Belgische economie verslechterde, waardoor eveneens effecten te verwachten zijn op het proces van jobcreatie en –destructie. (Konings, 2006)

Tabel 9.3: Overzicht percentage vennootschapsbelasting

Land	Percentage
België (vóór 2002)	40,17 %
België (na 2002)	33,99 %
Europa (gemiddeld)	25,3 %

Onder jobcreatie wordt de som van alle nieuwe jobs die ontstaan in nieuwe en groeiende bedrijven in een bepaald jaar gedeeld door het totale aantal jobs in de economie verstaan. De jobdestructiegraad daarentegen is de som van alle jobs die verloren gegaan zijn door het inkrimpen van bedrijven en bedrijven die de markt verlaten gedeeld door het totaal aantal jobs in de economie. De som van jobcreatie en jobdestructie geeft een maatstaf voor de bruto jobreallocatie. (Konings, 2006)

Volgens Konings en Vandenbussche (2006) is er enerzijds een negatief verband tussen de vennootschapsbelasting en de jobreallocatiegraad en anderzijds een positief verband tussen de jobreallocatie en economische groei. België heeft een hoge gemiddelde vennootschapsbelasting en bijgevolg een relatief lage jobreallocatiegraad. Wanneer de jobreallocatiegraad laag is, is de economische groei ook lager. Als België zijn economisch beleid zou aanpassen en zijn vennootschapsbelasting zou verlagen, zou de jobreallocatie gemakkelijker moeten verlopen en zou de economische groei eveneens verhogen.

In zijn manifest heeft Verhofstadt (2006) aangehaald dat de vennootschapsbelasting afgeschaft zou kunnen worden omdat het slechts enkele procenten (3 %) van het totale inkomen van de staat vertegenwoordigt. Deze percenten zouden eventueel op andere manieren kunnen gerecupereerd worden.

9.4 Opmerking: belang van KMO's in België

De Belgische bedrijfswereld bestaat uit een reeks grote bedrijven en een zeer groot aantal KMO's. Een groot bedrijf is bijvoorbeeld Inbev, dat met behulp van de Leuvense brouwerij Stella Artois kon uitgroeien tot één van de grootste brouwerijgroepen ter wereld. Echter de meeste grote bedrijven zijn eigendom van

buitenlandse groepen. Daarnaast steunt de Belgische economie op middelgrote en kleine bedrijven. Zowat 83 procent van de Belgische bedrijven telt minder dan tien werknemers, 97 procent van de bedrijven stellen minder dan vijftig mensen tewerk. De KMO's zijn verantwoordelijk voor meer dan 70 procent van het BBP (Bruto Binnenlands Product). De Belgische KMO's zijn bovendien voor het overgrote deel familiebedrijven. Uit Europese vergelijkingen blijkt hoe speciaal deze kleine bedrijven zijn: de Belgische KMO's zijn de meest winstgevende van de EU. België is bovendien het enige Europese land waar de winstgevendheid van KMO's aanzienlijk hoger ligt dan in grote bedrijven.
(http://www.diplomatie.be/nl/belgium/belgiumdetail.asp?textID=49043, 2006)

Hoofdstuk 10 Conclusies en mogelijkheden tot verder onderzoek

Dit laatste hoofdstuk omvat een algemeen besluit waarin we de belangrijkste componenten en toepassingen kort in de verf zetten.

10.1 Conclusies

De laatste jaren zit de elektronische handel duidelijk in een groeifase. Consumenten en producenten kopen enerzijds en verkopen anderzijds steeds meer producten en diensten via elektronische weg. Dit is mede mogelijk door de opkomst en tevens permanente uitbreiding van het Internet. Het Internet is haast niet meer weg te denken in de huidige informatie- en communicatiemaatschappij. Het vindt zijn toepassingen in de bedrijfswereld, maar ook bij de gezinnen thuis. Al is het maar om op te zoeken welke programma's er 's avonds op televisie komen. Door deze groei wordt de onzekerheid van het Internet en de vraag naar de veiligheid eveneens groter. De consument heeft tot op heden nog maar weinig vertrouwen in de beveiliging van vooral financiële transacties via een publiek kanaal. Vertrouwen kan slechts gecreëerd worden indien men beschikt over betrouwbare kanalen voor transacties. Wanneer men via elektronische weg communiceert, tracht men deze betrouwbaarheid te scheppen door het gebruik van beveiligingsmethoden. Ideaal hiervoor zijn cryptografische technieken die ook tot uiting komen in de digitale handtekening.

Het wiskundige basisbegrip in de moderne cryptografie en de digitale handtekening is de trapdoor one way functie. Dit is een functie die in één richting makkelijk te berekenen is, maar waarbij de inverse functie enkel berekend kan worden als men over additionele informatie beschikt. De publieke sleutels die men gebruikt in de cryptografie, worden gedefinieerd als trapdoor one way functies. Om een geheim bericht te versturen, versleutelt de zender dit bericht met de publieke sleutel van de ontvanger. Enkel de ontvanger is in het bezit van de inverse publieke sleutel of de

overeenkomstige private sleutel en kan het bericht ontcijferen. Deze private sleutel komt overeen met de additionele informatie die nodig is om de inverse functie van de one way functie te berekenen.

De digitale handtekening maakt eveneens gebruik van de cryptografie. Hierbij wordt de functie echter omgekeerd gebruikt. De zender versleutelt het bericht met zijn inverse publieke sleutel, ook wel private sleutel genoemd. Iedere ontvanger kan het bericht vervolgens ontsleutelen met de publieke sleutel van de zender waardoor de ontvanger zeker is van de identiteit van de zender. Een eigenschap van de digitale handtekening is dat ze authenticiteit verzekert.

Als men zeker wil zijn dat de inhoud van een bericht niet gewijzigd werd, wordt het bericht eerst bewerkt met een hash functie (die publiek gekend is). Het bericht wordt vervolgens omgezet in een reeks bits van een vaste lengte. Dit wordt de hashwaarde genoemd. Wanneer het bericht onderweg kwaadwillig of toevallig veranderd werd, zal de ontvanger dit opmerken. De ontvanger zal immers bij verificatie niet twee keer dezelfde hashwaarde bekomen wanneer er met het bericht geknoeid werd.

Bij toepassing van de digitale handtekening kan een zender niet ontkennen dat hij het bericht verstuurd heeft. De eigenschap van de digitale handtekening die hiervoor zorgt is onweerlegbaarheid. Een bericht dat versleuteld is met de private sleutel van de zender kan slechts ontsleuteld worden met de publieke sleutel van deze zender. Een digitaal certificaat bindt de publieke sleutel aan de identiteit van een zender. Certificaatautoriteiten zien er op toe dat deze publieke sleutels gebonden worden aan de identiteiten van de zenders. Ook dit draagt bij tot de authenticiteit van de digitale handtekening.

Een laatste eigenschap van de digitale handtekening is confidentialiteit. In combinatie met een cryptosysteem garandeert een digitale handtekening de confidentialiteit van de inhoud van een bericht. Vooraleer men de privaat (met private sleutel van de zender) versleutelde hashwaarde van de zender naar de ontvanger verstuurt, wordt het geheel nogmaals versleuteld met de publieke sleutel van de ontvanger. Slechts de ontvanger kan vervolgens het geheel terug ontsleutelen met

zijn private sleutel. De digitale handtekening biedt op zich geen confidentialiteit, maar wel in combinatie met een cryptosysteem.

Men kan verschillende soorten digitale handtekeningen creëren naargelang de gewenste beveiliging. Men kan kiezen tussen: enkel confidentialiteit is belangrijk, enkel onweerlegbaarheid is belangrijk en zowel confidentialiteit als onweerlegbaarheid zijn belangrijk.

Sinds 9 juli 2001 bestaat in een België de wet certificatiediensten. Deze wet houdt in dat de digitale handtekening dezelfde juridische waarde heeft als de handgeschreven variant. De groei van de elektronische handel zou dankzij dit wettelijk kader moeten toenemen.

De digitale handtekening heeft eveneens impact op elektronische toepassingen zoals e-commerce, e-banking, e-government … Voor e-government, zoals bijvoorbeeld het invullen en indienen van de aangifte voor de vennootschapsbelasting, is de identificatie van de aanvrager noodzakelijk. Ook mag men achteraf niet ontkennen dat deze aangifte aan een bepaald persoon toebehoort. Voor deze problematiek kan de digitale handtekening een oplossing bieden. Via de website VenSoc kan men een aangifte van de vennootschapsbelasting elektronisch invullen en verzenden. Echter biedt dit nog steeds geen oplossing voor de KMO's die zich geen dure belastingsspecialist kunnen veroorloven. De elektronische aangifte is immers identiek aan de papieren aangifte.

10.2 Mogelijkheden tot verder onderzoek

Deze eindverhandeling heeft zeker niet als doel om een volledige bespreking van de digitale handtekening weer te geven. Zeker niet alle topics komen hierin aan bod. Er zijn bijgevolg nog andere onderwerpen die de moeite waard zijn om verder of dieper te onderzoeken. Zo kan men zich bijvoorbeeld afvragen welke systemen er bij de belangrijkste banken zoals Fortis, KBC, ING … gebruikt worden met betrekking tot e-banking. Ook kan men hier de kosten en baten van berekenen.

Een ander mogelijk onderzoek zou een studie over de kosten en baten van papieren aangifte enerzijds en de elektronische aangifte anderzijds kunnen bevatten. Men zou zich kunnen afvragen of er nu wel zo een groot verschil bestaat in de kosten en baten van deze twee mogelijkheden.

Men zou eveneens de mogelijke toepassingen van de elektronische identiteitskaart in detail kunnen onderzoeken. Wat zijn nu eigenlijk alle mogelijke toepassingen van de elektronische identiteitskaart? Kan de elektronische identiteitskaart een digitaal certificaat vervangen?

Ook zou men dieper kunnen ingaan op de certificaatautoriteiten. Hoe gaat het eigenlijk in zijn werk? Hoe moet een certificaat aangevraagd worden? Op basis waarvan worden certificaten toegekend?

Verder zou men ook nog kunnen onderzoeken hoe de digitale handtekening in andere Europese landen evolueert. Hoe ziet de wetgeving eruit in de andere Europese landen. Hoe scoort België in vergelijking met andere Europese landen? In vergelijking met de rest van de wereld?

Het praktijkvoorbeeld dat ikzelf onderzocht heb, kan ook nog verder uitgewerkt worden. Men zou kunnen onderzoeken of er eventueel een analytische intelligentie kan toegevoegd worden aan de elektronische aangifte van de vennootschapsbelasting, zodat de laagste fiscaliteit kan gewaarborgd worden. Wat zijn de voordelen voor de KMO's en de grote bedrijven? Wat zijn de kosten en baten van een dergelijke intelligentie? Voor hetzelfde praktijkvoorbeeld zou men ook kunnen nagaan of de vennootschapsbelasting kan verlaagd worden indien men enkel nog met elektronische aangiften zou werken.

Bibliografie

Boeken en syllabi

Belastingswijzer vennootschapsbelasting, Diegem

Broekmans J., *Methode van onderzoek en rapportering,* Faculteit toegepaste economische wetenschappen, Limburgs Universitair centrum, 2001

Buyst, L., *Codetheorie: toepassingen van de moderne algebra,* N.V. Scriptoria, Antwerpen, 1967, 124p

Delbrouck, C., *Handelsrecht: praktijkboek,* Faculteit toegepaste economische wetenschappen, Limburgs Universitair centrum, 2003

Lefebvre, E. R. J., *Tekst en organisatie,* derde druk, Acco, Leuven, 1997

Menezes, A. J., Oorschot, P. C. van, Vanstone, S. A., *Handbook of applied cryptography,* CRC Press LLC, Florida, 1997, 780p

O'Brien, J. A., *Leerboek ICT-toepassingen: het bedrijfsleven en het internet, intra/extranetten en electronic commerce,* derde herziene uitgave, Academic Service, Schoonhoven, 1998, 617p

Panko, R., *Datanetwerken en telecommunicatie,* vijfde editie, Pearson Education Benelux, Amsterdam, 2005, 577p

Stallings , W., *Netwerkbeveiliging en Cryptografie: Beginselen en praktijk,* Academic service, Schoonhoven, 2000, 644p

Stinson, D. R., *Cryptography: Theory and Practice,* Chapman & Hall/CRC, Florida, 2006, 593p

Websites

ABA (American Bar Association), http://www.abanet.org

Belgische economie, http://www.diplomatie.be

Certipost, http://www.certipost.be

Computer/Law institute, http://www.cli.vy

Crypto-world, http://www.crypto-world.com

De Meese, T., De elektronische handtekening, http://www.crowell.com

Digitale handtekening informatiecentrum, http://www.digitalehandtekening.be

ECP, http://www.ecp.nl

Egten, D. van, Een verbod om te fluisteren…, 1996, http://www.vanegten.net

Federale Overheidsdienst Justitie, Belgisch Staatsblad, 2006, http://www.just.fgov.be

Federale Overheidsdienst Financiën, 2006, http://minfin.fgov.be

Gastel, M. C. van, Wet elektronische handtekeningen: toetsing aan de eisen van de "papieren" handtekening, http://www.uu.nl/content/elektronischehandtekeningen.pdf

Global Sign, http://nl.globalsign.net

Infolab, http://www.uvt.nl/infolab

Isabel, http://www.isabel.be

Ius Mentis, http://www.iusmentis.com

Jelmer Vernooij, http://jelmer.vernstok.nl

Juridische aspecten van internet, http://www.javasite.nl

Katholieke universiteit Brussel, http://www.kubrussel.ac.be

Ministerie van justitie, http://www.justitie.nl

Protechnix, innovation and research, http://www.pro-technix.com

RSA Security Inc., 2006, http://www.rsasecurity.com

SG1.net, Applied cryptography, http://www.sg1.net/

Surfnet, http://www.surfnet.nl

Telenet, Internetbankieren, http://www.telenet.be

Vaczlavik, L., Coding Theory, http://www7.tamu-commerce.edu/honors

Wikipedia, de vrije encyclopedie, http://www.wikipedia.org

X5 Networks, http://www.x5.net

Geraadpleegde eindverhandelingen

Deckers, M., *De digitale handtekening als stimulans voor e-commerce en economische vooruitgang,* Limburgs Universitair Centrum, Diepenbeek, 2005, 106p

Hermans, I., *De digitale handtekening en de elektronische bedrijfsvoering,* Limburgs Universitair Centrum, Diepenbeek, 2001, 81p

Smets, E., *De digitale handtekening: principe en mogelijke toepassingen met de elektronische identiteitskaart,* Limburgs Universitair Centrum, Diepenbeek, 2005, 96p

Lijst van tabellen

Lijst van figuren

Bijlagen

Bijlage 1: Richtlijn 1999/93/EG van het Europees Parlement en de Raad betreffende een gemeenschappelijk kader voor elektronische handtekeningen

Bijlage 2: Wet van 20 oktober 2000 tot invoering van het gebruik van telecommunicatiemiddelen en van de elektronische handtekening in de gerechtelijke en buitengerechtelijke procedure

Bijlage 3: Wet van 9 juli 2001 houdende vaststelling van bepaalde regels in verband met het juridisch kader voor elektronische handtekeningen en certificatiediensten

Bijlage 4: Vragenlijst betreffende online indienen van vennootschapsbelasting ter voorbereiding van het interview met de heer S. De Prins van HLB Fineko

Bijlage 1: Richtlijn 1999/93/EG van het Europees Parlement en de Raad betreffende een gemeenschappelijk kader voor elektronische handtekeningen

RICHTLIJN 1999/93/EG VAN HET EUROPEES PARLEMENT EN DE RAAD
van 13 december 1999
betreffende een gemeenschappelijk kader voor elektronische handtekeningen

HET EUROPEES PARLEMENT EN DE RAAD VAN DE EUROPESE UNIE,

Gelet op het Verdrag tot oprichting van de Europese Gemeenschap, met name op artikel 47, lid 2, artikel 55 en artikel 95,

Gezien het voorstel van de Commissie [1],

Gezien het advies van het Economisch en Sociaal Comité [2],

Gezien het advies van het Comité van de Regio's [3],

Volgens de procedure van artikel 251 van het Verdrag [4]:

Overwegende hetgeen volgt:

(1) De Commissie heeft op 16 april 1997 bij het Europees Parlement, de Raad, het Economisch en Sociaal Comité en het Comité van de Regio's een mededeling ingediend over een Europees initiatief inzake elektronische handel.

(2) De Commissie heeft op 8 oktober 1997 bij het Europees Parlement, de Raad, het Economisch en Sociaal Comité en het Comité van de Regio's een mededeling ingediend „Zorgen voor veiligheid en vertrouwen in elektronische communicatie — Naar een Europees kader voor digitale handtekeningen en encryptie".

(3) De Raad heeft op 1 december 1997 de Commissie opgeroepen zo spoedig mogelijk een voorstel in te dienen voor een richtlijn van het Europees Parlement en de Raad betreffende digitale handtekeningen.

(4) Voor elektronische communicatie en handel zijn „elektronische handtekeningen" en daarmee verwante diensten die authentificatie mogelijk maken, vereist: uiteenlopende regels voor de wettelijke erkenning van elektronische handtekeningen en voor de accreditatie van certificatiedienstverleners kunnen in de lidstaten grote belemmeringen opwerpen voor het gebruik van elektronische communicatie en voor de elektronische handel; duidelijke gemeenschappelijke randvoorwaarden voor elektronische handtekeningen zullen anderzijds het vertrouwen in en de algemene aanvaarding van de nieuwe technologieën bevorderen; wetgeving in de lidstaten mag het vrije verkeer van goederen en diensten binnen de interne markt niet belemmeren.

(5) De interoperabiliteit van producten voor elektronische handtekeningen moet worden bevorderd; in overeenstemming met artikel 14 van het Verdrag is de interne markt een gebied zonder binnengrenzen waarin het vrije verkeer van goederen moet worden gewaarborgd; er moet worden voldaan aan essentiële eisen die specifiek zijn voor producten voor elektronische handtekeningen, zodat het vrije verkeer in de interne markt wordt gewaarborgd en het vertrouwen in elektronische handtekeningen kan worden opgebouwd, onverminderd Verordening (EEG) nr. 3381/94 van de Raad van 19 december 1994 tot instelling van een communautaire regeling voor exportcontrole op goederen voor tweeërlei gebruik [5] en Besluit 94/942/GBVB van de Raad van 19 december 1994 betreffende het gemeenschappelijke optreden door de Raad vastgesteld ten aanzien van de controle op de uitvoer uit de Gemeenschap van goederen voor tweeërlei gebruik [6].

(6) Deze richtlijn ziet niet op de harmonisatie van het leveren van diensten met betrekking tot de vertrouwelijkheid van gegevens, wanneer die diensten onder nationale regelgeving inzake de openbare orde of openbare veiligheid vallen.

(7) De interne markt verzekert ook het vrije verkeer van personen, waardoor burgers en ingezetenen van de Europese Unie steeds meer moeten omgaan met de autoriteiten van andere lidstaten dan die waar zij verblijven; de beschikbaarheid van elektronische communicatie kan in dit verband grote diensten bewijzen.

(8) De snelle technologische ontwikkelingen en de wereldwijde omvang van het Internet vereisen een aanpak die openstaat voor de verschillende technologieën en diensten die elektronische authentificatie mogelijk maken.

(9) Elektronische handtekeningen zullen in zeer uiteenlopende omstandigheden en toepassingen worden gebruikt, hetgeen zal resulteren in een breed scala van nieuwe producten en diensten die verband houden met elektronische handtekeningen; de definitie van dergelijke producten en diensten mag niet beperkt blijven tot afgifte en beheer van certificaten, maar moet ook alle andere producten en diensten omvatten die gebruikmaken van of een hulpmiddel zijn voor elektronische handtekeningen, zoals registratiediensten, tijdstempeldiensten, directorydiensten, computerdiensten of adviesverlening inzake elektronische handtekeningen.

(10) De interne markt maakt het certificatiedienstverleners mogelijk grensoverschrijdende activiteiten te ontwikkelen om hun concurrentiepositie te verbeteren, en aldus consumenten en bedrijven nieuwe mogelijkheden te bieden inzake veilige elektronische informatie-uitwisseling en handel, over de grenzen heen; teneinde in de hele Gemeenschap het leveren, via open netwerken, van certificatiediensten te bevorderen, moeten de certificatiedienstverleners hun diensten vrij zonder voorafgaande machtiging kunnen aanbieden; onder voorafgaande

---

(1) PB C 325 van 23.10.1998, blz. 5.
(2) PB C 40 van 15.2.1999, blz. 29.
(3) PB C 93 van 6.4.1999, blz. 33.
(4) Advies van het Europees Parlement van 13 januari 1999 (PB C 104 van 14.4.1999, blz. 49), gemeenschappelijk standpunt van de Raad van 28 juni 1999 (PB C 243 van 27.8.1999, blz. 33) en besluit van het Europees Parlement van 27 oktober 1999 (nog niet verschenen in het Publicatieblad). Besluit van de Raad van 30 november 1999.
(5) PB L 367 van 31.12.1994, blz. 1. Verordening gewijzigd bij Verordening (EG) nr. 837/95 (PB L 90 van 21.4.1995, blz. 1).
(6) PB L 367 van 31.12.1994, blz. 8. Besluit laatstelijk gewijzigd bij Besluit 1999/193/GBVB (PB L 73 van 19.3.1999, blz. 1).

machtiging wordt niet alleen elke vergunning verstaan waarvoor de certificatiedienstverlener een besluit van de nationale autoriteiten moet verkrijgen voordat hij zijn certificatiediensten mag verlenen, maar ook alle andere maatregelen met hetzelfde effect.

(11) Vrijwillige-accreditatieregelingen, die beogen de dienstverlening te verbeteren, kunnen certificatiedienstverleners een passend kader bieden om hun diensten verder te ontwikkelen en het door de markt verlangde niveau van vertrouwen, veiligheid en kwaliteit te bereiken; dergelijke regelingen dienen de ontwikkeling te bevorderen van beste praktijken van certificatiedienstverleners; het moet certificatiedienstverleners vrij staan zich te laten accrediteren en van dergelijke accreditatieregelingen gebruik te maken.

(12) Certificatiediensten kunnen worden aangeboden door hetzij een dienst, hetzij een natuurlijke of rechtspersoon zodra die overeenkomstig de nationale wetgeving gevestigd is; de lidstaten mogen de certificatiedienstverleners niet verbieden buiten dergelijke accreditatieregelingen te werken; er moet voor worden gezorgd dat accreditatieregelingen de concurrentie voor certificatiediensten niet beperken.

(13) De lidstaten kunnen bepalen hoe zij het toezicht op de naleving van deze richtlijn zullen waarborgen; deze richtlijn sluit niet uit dat vanuit de particuliere sector toezichtsystemen worden opgezet; deze richtlijn verplicht de certificatiedienstverleners er niet toe om toezicht in het kader van een geldende accreditatieregeling te verzoeken.

(14) Het is van belang een evenwicht te vinden tussen de behoeften van de consumenten en die van het bedrijfsleven.

(15) Bijlage III heeft betrekking op eisen voor veilige middelen voor het aanmaken van handtekeningen die moeten instaan voor de functionaliteit van geavanceerde elektronische handtekeningen; bijlage III bestrijkt niet de hele systeemomgeving waarbinnen dergelijke middelen functioneren; de werking van de interne markt vereist dat de Commissie en de lidstaten snel de aanwijzing mogelijk maken van de instanties die belast worden met de overeenstemmingsbeoordeling van veilige middelen voor het aanmaken van handtekeningen met bijlage III; de overeenstemming moet met gepaste spoed en doeltreffend worden beoordeeld teneinde te voldoen aan de behoeften van de markt.

(16) Deze richtlijn draagt bij tot het gebruik en de wettelijke erkenning van elektronische handtekeningen in de Gemeenschap; er bestaat geen behoefte aan een regelgevend kader voor elektronische handtekeningen die uitsluitend worden gebruikt in systemen die berusten op vrijwillige privaatrechtelijke overeenkomsten tussen een vastgesteld aantal deelnemers; de vrijheid van partijen om onderling voorwaarden overeen te komen voor het aanvaarden van elektronisch ondertekende gegevens moet worden geëerbiedigd in de mate die door het nationale recht wordt toegestaan; de rechtsgeldigheid en de toelaatbaarheid als bewijsmiddel in gerechtelijke procedures van in dergelijke systemen gebruikte elektronische handtekeningen mogen niet worden miskend.

(17) Deze richtlijn is niet gericht op de harmonisatie van nationale regels met betrekking tot het contractenrecht, en in het bijzonder betreffende het aangaan en uitvoeren van contracten, of andere niet-contractuele formaliteiten waarvoor handtekeningen vereist zijn; derhalve mogen de bepalingen betreffende de rechtsgevolgen van elektronische handtekeningen geen afbreuk doen aan de nationale wettelijke vormvereisten met betrekking tot het sluiten van contracten of de regels die bepalen waar een contract gesloten wordt.

(18) Het opslaan of kopiëren van gegevens voor het aanmaken van handtekeningen zou een ernstige bedreiging voor de rechtsgeldigheid van elektronische handtekeningen kunnen vormen.

(19) Elektronische handtekeningen zullen door de openbare sector worden gebruikt in de ambtelijke diensten van de lidstaten en van de Gemeenschap, alsmede bij de communicatie tussen deze diensten en met de burgers en met de economische actoren, bijvoorbeeld in het kader van overheidsopdrachten, belastingen, sociale zekerheid, gezondheid en justitie.

(20) Geharmoniseerde criteria in verband met de rechtsgevolgen van elektronische handtekeningen zullen een samenhangend wettelijk kader in de gehele Gemeenschap garanderen; de nationale wetgeving bevat verschillende voorschriften inzake de rechtsgeldigheid van handgeschreven handtekeningen; certificaten kunnen worden gebruikt om de dienst te bevestigen van een persoon die elektronisch ondertekent; geavanceerde elektronische handtekeningen die zijn gebaseerd op gekwalificeerde certificaten zijn bedoeld om de veiligheid te vergroten; geavanceerde elektronische handtekeningendie zijn gebaseerd op een gekwalificeerd certificaat en die zijn aangemaakt met een veilig middel voor het aanmaken van handtekeningen kunnen alleen als juridisch gelijkwaardig met handgeschreven handtekeningen worden beschouwd indien aan deze voorschriften voor handgeschreven handtekeningen is voldaan.

(21) Teneinde bij te dragen tot de algemene aanvaarding van elektronische authentificatiemethodes, moet ervoor worden gezorgd dat elektronische handtekeningen in alle lidstaten in rechtszaken als bewijsmiddel kunnen worden gebruikt; de wettelijke erkenning van elektronische handtekeningen moet worden gebaseerd op objectieve criteria en mag niet worden gekoppeld aan de machtiging van de betrokken dienstverlener; de nationale wetgeving bepaalt in welke rechtsgebieden elektronische documenten en elektronische handtekeningen kunnen worden gebruikt; deze richtlijn doet geen afbreuk aan de mogelijkheid voor een nationale rechtbank om uitspraak te doen over de overeenstemming met de eisen van de richtlijn en zij laat de nationale regels in verband met de vrije beoordeling van bewijsmiddelen door de rechter onverlet.

(22) Certificatiedienstverleners die aan het publiek certificatiediensten aanbieden, zijn onderworpen aan de nationale aansprakelijkheidsregels.

(23) Voor de ontwikkeling van de internationale handel zijn grensoverschrijdende afspraken met derde landen vereist; om de interoperabiliteit op mondiaal niveau te waarborgen kunnen overeenkomsten over multilaterale voorschriften met derde landen terzake van de wederzijdse erkenning van certificatiediensten nuttig zijn.

(24) Teneinde het vertrouwen van de gebruiker in elektronische communicatie en elektronische handel te bevorderen, moeten de certificatiedienstverleners de wetgeving inzake gegevensbescherming en bescherming van de persoonlijke levenssfeer naleven.

(25) De bepaling inzake het gebruik van pseudoniemen in certificaten belet de lidstaten niet op grond van de communautaire of de nationale wetgeving de identificatie van personen te eisen.

(26) De voor de uitvoering van de onderhavige richtlijn vereiste maatregelen moeten worden vastgesteld volgens Besluit 1999/468/EG van de Raad van 28 juni 1999 tot vaststelling van de voorwaarden voor de uitoefening van de aan de Commissie verleende uitvoeringsbevoegdheden (1).

(27) De Commissie zal twee jaar na de uitvoering van deze richtlijn een evaluatie daarvan uitvoeren, onder andere om te waarborgen dat de vooruitgang van de techniek of wijzigingen in het juridische kader geen belemmeringen voor de verwezenlijking van de in deze richtlijn vervatte doelstellingen hebben opgeworpen; zij moet de implicaties van verwante technische sectoren onderzoeken en daarover een verslag aan het Parlement en de Raad voorleggen.

(28) In overeenstemming met de beginselen van subsidiariteit en evenredigheid zoals bedoeld in artikel 5 van het Verdrag, kan de doelstelling een geharmoniseerd juridisch kader te creëren voor elektronische handtekeningen en daarmee verband houdende diensten niet in voldoende mate door de lidstaten worden verwezenlijkt en derhalve beter door de Gemeenschap worden verwezenlijkt; deze richtlijn gaat niet verder dan wat nodig is om deze doelstelling te verwezenlijken,

HEBBEN DE VOLGENDE RICHTLIJN VASTGESTELD:

Artikel 1

Toepassingsgebied

Deze richtlijn heeft tot doel het gebruik van elektronische handtekeningen te vergemakkelijken en tot de wettelijke erkenning ervan bij te dragen. Zij brengt een juridisch kader tot stand voor elektronische handtekeningen en voor bepaalde certificatiediensten, teneinde de goede werking vals de interne markt te garanderen.

Deze richtlijn heeft geen betrekking op aspecten die verband houden met de totstandkoming of geldigheid van contracten of andere wettelijke verbintenissen waarvoor het nationale of het Gemeenschapsrecht vormvereisten voorschrijven en laat de regels en beperkingen onverlet die het nationale of het Gemeenschapsrecht voorschrijven voor het gebruik van documenten.

Artikel 2

Definities

Voor de toepassing van deze richtlijn wordt verstaan onder:

1. „elektronische handtekening": elektronische gegevens die zijn vastgehecht aan of logisch geassocieerd zijn met andere elektronische gegevens en die worden gebruikt als middel voor authentificatie;

2. „geavanceerde elektronische handtekening": een elektronische handtekening die voldoet aan de volgende eisen:

   a) zij is op unieke wijze aan de ondertekenaar verbonden;

   b) zij maakt het mogelijk de ondertekenaar te identificeren;

   c) zij komt tot stand met middelen die de ondertekenaar onder zijn uitsluitende controle kan houden; en

   d) zij is op zodanige wijze aan de gegevens waarop zij betrekking heeft verbonden, dat elke wijziging achteraf van de gegevens kan worden opgespoord;

3. „ondertekenaar": een persoon die de beschikking heeft over een middel voor het aanmaken van handtekeningen en handelt hetzij uit eigen naam hetzij uit naam van de dienst of de natuurlijke of rechtspersoon die hij vertegenwoordigt;

4. „gegevens voor het aanmaken van handtekeningen": unieke gegevens, zoals codes of cryptografische privé-sleutels, die door de ondertekenaar worden gebruikt om een elektronische handtekening aan te maken;

5. „middel voor het aanmaken van handtekeningen": geconfigureerde software of hardware die wordt gebruikt om de gegevens voor het aanmaken van handtekeningen te implementeren;

6. „veilig middel voor het aanmaken van handtekeningen": een middel voor het aanmaken van handtekeningen dat voldoet aan de eisen van bijlage III;

7. „gegevens voor het verifiëren van een handtekening": gegevens, zoals codes of cryptografische openbare sleutels, die worden gebruikt voor het verifiëren van een 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. „certificaat": een elektronische bevestiging die gegevens voor het verifiëren van een handtekening aan een bepaalde persoon verbindt en de identiteit van die persoon bevestigt;

10. „gekwalificeerd certificaat": een certificaat dat voldoet aan de eisen van bijlage I en is afgegeven door een certificatiedienstverlener die voldoet aan de eisen van bijlage II;

11. „certificatiedienstverlener": een dienst of een natuurlijke of rechtspersoon die certificaten afgeeft of andere diensten in verband met elektronische handtekeningen verleent;

12. „product voor elektronische handtekeningen": software of hardware, of relevante componenten daarvan, die door certificatiedienstverleners kunnen worden gebruikt om diensten op het gebied van elektronische handtekeningen te verlenen of die voor het aanmaken of verifiëren van elektronische handtekeningen kunnen worden gebruikt;

13. „vrijwillige accreditatie": een vergunning waarin de rechten en verplichtingen betreffende de verlening van certificatiediensten zijn vermeld en die op verzoek van de betrokken certificatiedienstverlener wordt afgegeven door de openbare of particuliere instantie die belast is met de vastlegging en de handhaving van die rechten en verplichtingen, wanneer de certificatiedienstverlener de uit de vergunning voortvloeiende rechten niet kan uitoefenen zolang hij het besluit van die instantie niet heeft ontvangen.

(1) PB L 184 van 17.7.1999, blz. 23.

Artikel 3

Markttoegang

1. De lidstaten stellen het verlenen van certificatiediensten niet afhankelijk van voorafgaande machtiging.

2. Onverminderd het bepaalde in lid 1, mogen de lidstaten vrijwillige-accreditatieregelingen invoeren of handhaven die op verbetering van de certificatiediensten zijn gericht. Alle voorwaarden betreffende dergelijke regelingen moeten objectief, transparant, evenredig en niet-discriminerend zijn. De lidstaten mogen het aantal geaccrediteerde certificatiedienstverleners niet beperken om redenen die onder het toepassingsgebied van deze richtlijn vallen.

3. De lidstaten zorgen voor een passend systeem voor toezicht op de op hun grondgebied gevestigde certificatiedienstverleners die gekwalificeerde certificaten aan het publiek afgeven.

4. De overeenstemming van veilige middelen voor het aanmaken van handtekeningen met de eisen van bijlage III wordt vastgesteld door passende openbare of particuliere instanties die door de lidstaten worden aangewezen. De Commissie stelt volgens de procedure van artikel 9 de criteria vast aan de hand waarvan de lidstaten bepalen of een instantie voor aanwijzing geschikt is.

De bevindingen van de in de eerste alinea bedoelde instanties met betrekking tot de overeenstemming met de eisen van bijlage III worden door alle lidstaten erkend.

5. De Commissie kan, volgens de procedure van artikel 9, referentienummers van algemeenl erkende normen voor producten voor elektronische handtekeningen vaststellen en in het *Publicatieblad van de Europese Gemeenschappen* bekendmaken. Wanneer een product voor elektronische handtekeningen aan dergelijke normen voldoet, gaan de lidstaten ervan uit dat het met de eisen van bijlage II, punt f), en bijlage III, in overeenstemming is.

6. De lidstaten en de Commissie werken samen om de ontwikkeling en het gebruik van middelen voor het verifiëren van handtekeningen te bevorderen en houden daarbij de in bijlage IV opgenomen aanbevelingen voor het veilig verifiëren van handtekeningen alsmede het belang van de consument voor ogen.

7. De lidstaten kunnen voor het gebruik van elektronische handtekeningen in de openbare sector eventuele aanvullende eisen stellen. Deze eisen moeten objectief, transparant, evenredig en niet-discriminerend zijn en mogen slechts op de specifieke kenmerken van de betrokken toepassing betrekking hebben. Zij mogen geen belemmering vormen voor grensoverschrijdende diensten.

Artikel 4

Beginselen betreffende de interne markt

1. Elke lidstaat past de nationale bepalingen die hij krachtens deze richtlijn vaststelt toe ten aanzien van de op zijn grondgebied gevestigde certificatiedienstverleners en van de diensten die zij verrichten. De lidstaten mogen het verlenen van certificatiediensten vanuit een andere lidstaat op gebieden die onder deze richtlijn vallen niet beperken.

2. De lidstaten waarborgen het vrije verkeer in de interne markt van producten voor elektronische handtekeningen die aan deze richtlijn voldoen.

Artikel 5

Rechtsgevolgen van elektronische handtekeningen

1. De lidstaten zorgen ervoor dat geavanceerde elektronische handtekeningen die zijn gebaseerd op een gekwalificeerd certificaat en die door een veilig middel zijn aangemaakt:

a) ten aanzien van gegevens in elektronische vorm voldoen aan alle wettelijke eisen voor een handtekening, net zoals een handgeschreven handtekening zulks doet voor gegevens op een papieren drager, alsmede

b) als bewijsmiddel in gerechtelijke procedures worden toegelaten.

2. De lidstaten zorgen ervoor dat een elektronische handtekening geen rechtsgeldigheid wordt ontzegd en dat zij niet als bewijsmiddel in gerechtelijke procedures kan worden geweigerd louter op grond van het feit dat:

de handtekening in elektronische vorm is gesteld, of

— niet is gebaseerd op een gekwalificeerd certificaat, of

niet is gebaseerd op een door een geaccrediteerd certificatiedienstverlener afgegeven certificaat, of

zij niet met een veilig middel is aangemaakt.

Artikel 6

Aansprakelijkheid

1. De lidstaten zorgen er ten minste voor dat een certificatiedienstverlener die een certificaat als gekwalificeerd certificaat aan het publiek afgeeft, of die zich publiekelijk borg stelt voor een dergelijk certificaat, aansprakelijk is voor schade die diensten of natuurlijke of rechtspersonen die in redelijkheid op dit certificaat vertrouwen ondervinden, in samenhang met:

a) de juistheid, op het tijdstip van afgifte, van alle gegevens in het gekwalificeerde certificaat en de opneming in het gekwalificeerde certificaat van alle voor een dergelijk certificaat voorgeschreven gegevens;

b) de garantie dat de in het gekwalificeerd certificaat geïdentificeerde ondertekenaar, op het tijdstip van de afgifte van het certificaat, houder was van de gegevens voor het aanmaken van de handtekening, die met de in het certificaat gegeven of geïdentificeerde gegevens voor het verifiëren van een handtekening overeenstemmen;

c) de garantie dat de gegevens voor het aanmaken van de handtekening en die voor het verifiëren van de handtekening, — ingeval zij beide door de certificatiedienstverlener worden gegenereerd , complementair kunnen worden gebruikt;

tenzij de certificatiedienstverlener bewijst dat hij niet nalatig heeft gehandeld.

2. De lidstaten zorgen er ten minste voor dat een certificatiedienstverlener die een certificaat als gekwalificeerd certificaat aan het publiek heeft afgegeven, aansprakelijk is voor de schade die bij diensten of natuurlijke of rechtspersonen die in redelijkheid op het certificaat hebben vertrouwd, is ontstaan doordat de intrekking van het certificaat niet werd geregistreerd, tenzij de certificatiedienstverlener bewijst dat hij niet nalatig heeft gehandeld.

3. De lidstaten zorgen ervoor dat een certificatiedienstverlener in een gekwalificeerd certificaat beperkingen betreffende het gebruik van dat certificaat kan aangeven, doch met dien verstande dat die beperkingen voor derden herkenbaar moeten zijn. De certificatiedienstverlener is niet aansprakelijk voor schade die voortvloeit uit gebruik van een gekwalificeerd certificaat waarbij de op het certificaat aangegeven beperkingen worden overschreden.

4. De lidstaten zorgen ervoor dat certificatiedienstverleners in het gekwalificeerd certificaat een grens kunnen aangeven voor de waarde van de transacties waarvoor het certificaat kan worden gebruikt, doch met dien verstande dat die grens voor derden herkenbaar moet zijn.

De certificatiedienstverlener is niet aansprakelijk voor schade die voortvloeit uit overschrijding van de hierboven bedoelde grens.

5. De leden 1 tot en met 4 doen geen afbreuk aan Richtlijn 93/13/EEG van de Raad van 5 april 1993 betreffende oneerlijke bedingen in consumentenovereenkomsten (1).

Artikel 7

Internationale aspecten

1. De lidstaten zorgen ervoor, dat certificaten die door een in een derde land gevestigde certificatiedienstverlener als gekwalificeerd certificaat aan het publiek worden afgegeven, worden gelijkgesteld met certificaten die door een in de Gemeenschap gevestigde certificatiedienstverlener worden afgegeven, indien

a) de certificatiedienstverlener voldoet aan de eisen van deze richtlijn en in het kader van een in een lidstaat van de Europese Gemeenschap ingestelde vrijwillige-accreditatieregeling is geaccrediteerd; dan wel

b) een in de Gemeenschap gevestigde certificatiedienstverlener die voldoet aan de eisen van deze richtlijn, zich voor het certificaat borg stelt; dan wel

c) het certificaat of de certificatiedienstverlener is erkend in het kader van een bilaterale of multilaterale overeenkomst tussen de Gemeenschap en derde landen of internationale organisaties.

2. Teneinde grensoverschrijdende certificatiediensten waarbij derde landen zijn betrokken en de wettelijke erkenning van geavanceerde elektronische handtekeningen afkomstig uit derde landen te vergemakkelijken, doet de Commissie passende voorstellen om de effectieve uitvoering van normen en internationale overeenkomsten inzake certificatiediensten te bereiken. Met name, en indien nodig, dient zij bij de Raad voorstellen in voor passende onderhandelingsmandaten voor bilaterale en multilaterale overeenkomsten met derde landen en internationale organisaties. De Raad besluit met gekwalificeerde meerderheid van stemmen.

3. Wordt de Commissie in kennis gesteld van moeilijkheden die ondernemingen uit de Gemeenschap ondervinden om toegang te verkrijgen tot de markt van derde landen, dan kan zij zo nodig aan de Raad voorstellen doen voor een passend mandaat voor onderhandelingen over vergelijkbare rechten voor ondernemingen uit de Gemeenschap in die derde landen. De Raad besluit met gekwalificeerde meerderheid van stemmen.

Overeenkomstig dit lid genomen maatregelen laten de krachtens de toepasselijke internationale overeenkomsten op de Gemeenschap en de lidstaten rustende verplichtingen onverlet.

Artikel 8

Gegevensbescherming

1. De lidstaten zorgen ervoor dat de certificatiedienstverleners en de met accreditatie of toezicht belaste nationale instanties voldoen aan de eisen van Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (2).

2. De lidstaten zorgen ervoor dat een certificatiedienstverlener die certificaten aan het publiek afgeeft persoonsgegevens niet anders kan verkrijgen dan rechtstreeks van de betrokkene zelf of met diens uitdrukkelijke toestemming, en slechts voorzover de afgifte en het beheer van het certificaat zulks vereisen. Zonder uitdrukkelijke toestemming van de betrokkene mogen gegevens niet voor andere doeleinden worden verzameld of verwerkt.

3. Onverminderd de rechtsgevolgen van pseudoniemen in het nationale recht, mogen de lidstaten niet verhinderen dat certificatiedienstverleners op het certificaat een pseudoniem vermelden in plaats van de werkelijke naam van de ondertekenaar.

Artikel 9

Comité

1. De Commissie wordt bijgestaand door een Comité voor elektronische handtekeningen (hierna „het comité" genoemd).

2. Wanneer naar dit lid wordt verwezen, zijn de artikelen 4 en 7 van Besluit 1999/468/EG van toepassing, met inachtneming van het bepaalde in artikel 8 van dat besluit.

De in artikel 4, lid 3, van Besluit 1999/468/EG bedoelde termijn wordt vastgesteld op drie maanden.

3. Het comité stelt zijn reglement van orde vast.

Artikel 10

Taken van het comité

Het comité geeft toelichtingen bij de in de bijlagen bij deze richtlijn genoemde eisen, de in artikel 3, lid 4, bedoelde criteria en de in artikel 3, lid 5, bedoelde algemeen erkende normen voor producten voor elektronische handtekeningen; het volgt daarbij de procedure van artikel 9, lid 2.

(1) PB L 95 van 21.4.1993, blz. 29.

(2) PB L 281 van 23.11.1995, blz. 31.

Artikel 11

Kennisgeving

1. De lidstaten verstrekken de Commissie en de andere lidstaten:

a) informatie over nationale vrijwillige accreditatieregelingen, met inbegrip van eventuele aanvullende eisen overeenkomstig artikel 3, lid 7;

b) de namen en adressen van de nationale instanties die belast zijn met accreditatie en toezicht alsmede van de in artikel 3, lid 4, genoemde instanties;

c) de namen en adressen van alle geaccrediteerde nationale certificatiedienstverleners.

2. De lidstaten delen de overeenkomstig lid 1 verstrekte informatie en wijzigingen daarvan zo spoedig mogelijk mede.

Artikel 12

Beoordeling

1. De Commissie beoordeelt de werking van deze richtlijn en brengt uiterlijk op 19 juli 2003 daarover verslag uit aan het Europees Parlement en aan de Raad.

2. Bij deze beoordeling wordt onder andere bezien of, rekening houdend met de technologische, commerciële en juridische ontwikkelingen, het toepassingsgebied van de richtlijn moet worden gewijzigd. Het verslag dient met name een beoordeling te bevatten, op basis van de opgedane ervaringen, van aspecten van harmonisatie. Het verslag gaat, in voorkomend geval, vergezeld van wetgevingsvoorstellen.

Artikel 13

Omzetting

1. De lidstaten doen de nodige wettelijke en bestuursrechtelijke bepalingen in werking treden om vóór 19 juli 2001 aan deze richtlijn te voldoen en stellen de Commissie daarvan onverwijld in kennis.

Wanneer de lidstaten die bepalingen aannemen, wordt in die bepalingen zelf of bij de officiële bekendmaking daarvan naar deze richtlijn verwezen. De regels voor deze verwijzing worden vastgesteld door de lidstaten.

2. De lidstaten stellen de Commissie in kennis van alle belangrijke bepalingen van intern recht die zij op het onder deze richtlijn vallende gebied vaststellen.

Artikel 14

Inwerkingtreding

Deze richtlijn treedt in werking op de dag van haar bekendmaking in het *Publicatieblad van de Europese Gemeenschappen*.

Artikel 15

Adressaten

Deze richtlijn is gericht tot de lidstaten.

Gedaan te Brussel, 13 december 1999.

Voor het Europees Parlement	*Voor de Raad*
De Voorzitster	*De Voorzitter*
N. FONTAINE	S. HASSI

BIJLAGE I

Eisen voor gekwalificeerde certificaten

Gekwalificeerde certificaten moeten het navolgende bevatten:

a) de vermelding dat het certificaat als gekwalificeerd certificaat wordt afgegeven;

b) de identificatie en het land van vestiging van de afgevende certificatiedienstverlener;

c) de naam van de ondertekenaar of een als zodanig geïdentificeerd pseudoniem;

d) ruimte voor een specifiek attribuut van de ondertekenaar, dat indien nodig, afhankelijk van het doel van het certificaat, kan worden vermeld;

e) gegevens voor het verifiëren van de handtekening die overeenstemmen met de gegevens voor het aanmaken van de handtekening die onder controle van de houder staan;

f) begin en einde van de geldigheidsduur van het certificaat;

g) de identiteitscode van het certificaat;

h) de geavanceerde elektronische handtekening van de afgevende certificatiedienstverlener;

i) voorzover van toepassing, beperkingen betreffende het gebruik van het certificaat; en

j) voorzover van toepassing, grenzen met betrekking tot de waarde van de transacties waarvoor het certificaat kan worden gebruikt.

BIJLAGE II

Eisen ten aanzien van certificatiedienstverleners die gekwalificeerde certificaten afgeven

Certificatiedienstverleners moeten:

a) aantonen dat zij voldoen aan de betrouwbaarheidseisen voor het aanbieden van certificatiediensten;

b) zorgen voor een snelle en veilige directorydienst alsook voor prompte en veilige intrekking;

c) ervoor zorgen dat datum en tijdstip van afgifte of intrekking van een certificaat precies kunnen worden vastgesteld;

d) met daartoe geschikte middelen en overeenkomstig de nationale wetgeving, de identiteit en in voorkomend geval de specifieke attributen verifiëren van de persoon aan wie een gekwalificeerd certificaat wordt afgegeven;

e) personeel in dienst hebben dat beschikt over de deskundige kennis, ervaring en kwalificaties die noodzakelijk zijn voor de aangeboden diensten, met name competentie op het gebied van beheer, alsmede over expertise inzake technologie voor elektronische handtekeningen, en dat bekend is met goede beveiligingsprocedures; het personeel moet ook adequate procedures en processen op het gebied van administratie en beheer toepassen die voldoen aan erkende normen;

f) gebruikmaken van betrouwbare systemen en producten die beschermd zijn tegen wijziging en die de technische en cryptografische veiligheid garanderen van de processen die zij ondersteunen;

g) maatregelen nemen tegen het vervalsen van certificaten en, wanneer de certificatiedienstverlener gegevens voor het aanmaken van handtekeningen genereert, de vertrouwelijkheid van dat proces garanderen;

h) voldoende financiële middelen tot hun beschikking houden om in overeenstemming met de eisen van deze richtlijn te kunnen functioneren, met name met het oog op de gevolgen van aansprakelijkheid wegens schade, bijvoorbeeld door middel van een geëigende verzekering;

i) gedurende een gepaste periode alle relevante informatie met betrekking tot een gekwalificeerd certificaat vastleggen, met name om ten behoeve van gerechtelijke procedures de certificatie te kunnen bewijzen. Dit vastleggen mag elektronisch plaatsvinden;

j) afzien van het opslaan of copiëren van gegevens voor het aanmaken van elektronische handtekeningen van de personen aan wie de certificatiedienstverlener sleutelbeheerdiensten heeft aangeboden;

k) alvorens een contractuele verbintenis aan te gaan met een persoon die een certificaat ter ondersteuning van zijn elektronische handtekening wenst, deze met behulp van een duurzaam communicatiemiddel op de hoogte brengen van de exacte voorwaarden voor het gebruik van het certificaat, met inbegrip van eventuele beperkingen inzake dit gebruik, het bestaan van een vrijwillige accreditatie en de procedures voor klachtenbehandeling en geschillenbeslechting. Deze informatie moet schriftelijk en in gemakkelijk te begrijpen taal worden opgesteld; eventueel kan zij langs elektronische weg worden toegezonden. Relevante delen van die informatie dienen op verzoek eveneens te worden meegedeeld aan derden die op het certificaat vertrouwen;

l) gebruikmaken van betrouwbare systemen voor de opslag van certificaten in verifieerbare vorm, zodat

— alleen bevoegde personen gegevens kunnen invoeren en wijzigen;

de authenticiteit van de informatie kan worden gecontroleerd;

de certificaten uitsluitend publiekelijk beschikbaar zijn in die gevallen waarvoor de certificaathouder toestemming heeft gegeven; en

elke technische wijziging die de bovengenoemde beveiligingsvoorschriften in gevaar kan brengen, voor de gebruiker duidelijk is.

BIJLAGE III

Eisen voor veilige middelen voor het aanmaken van elektronische handtekeningen

1. Veilige middelen voor het aanmaken van elektronische handtekeningen waarborgen via passende technieken en procedures ten minste, dat

   a) de gegevens voor het aanmaken van handtekeningen in de praktijk slechts één keer kunnen voorkomen en de vertrouwelijkheid daarvan redelijkerwijs gegarandeerd is;

   b) de gegevens voor het aanmaken van handtekeningen, met redelijke zekerheid, niet kunnen worden afgeleid en dat de handtekening beschermd is tegen vervalsing met de thans beschikbare technieken;

   c) de gegevens voor het aanmaken van handtekeningen door de legitieme ondertekenaar op betrouwbare wijze kunnen worden beschermd tegen gebruik door anderen.

2. Veilige middelen voor het aanmaken van handtekeningen laten de te ondertekenen gegevens ongewijzigd en beletten niet dat die gegevens vóór de ondertekening aan de ondertekenaar worden voorgelegd.

BIJLAGE IV

Aanbevelingen voor het veilig verifiëren van handtekeningen

Tijdens het proces voor het verifiëren van handtekeningen wordt met redelijke zekerheid gewaarborgd, dat

a) de voor het verifiëren van een handtekening gebruikte gegevens overeenstemmen met de gegevens die de verifieerder te zien krijgt;

b) de handtekening op betrouwbare wijze wordt geverificerd en het resultaat daarvan correct wordt weergegeven;

c) de verificerder, zo nodig, op betrouwbare wijze de inhoud van de ondertekende gegevens kan vaststellen;

d) de authenticiteit en de geldigheid van het certificaat dat bij het verifiëren van de handtekening vereist is, op betrouwbare wijze worden gecontroleerd;

e) dat het resultaat van de verificatie en de identiteit van de ondertekenaar correct worden weergegeven;

f) het gebruik van een pseudoniem duidelijk wordt aangegeven; en

g) elke wijziging die invloed heeft op de beveiliging kan worden opgespoord.

Bijlage 2: Wet van 20 oktober 2000 tot invoering van het gebruik van telecommunicatiemiddelen en van de elektronische handtekening in de gerechtelijke en buitengerechtelijke procedure

WETTEN, DECRETEN, ORDONNANTIES EN VERORDENINGEN
LOIS, DECRETS, ORDONNANCES ET REGLEMENTS

MINISTERIE VAN JUSTITIE

N. 2000 — 3304 [2000/10017]

20 OKTOBER 2000. — Wet tot invoering van het gebruik van telecommunicatiemiddelen en van de elektronische handtekening in de gerechtelijke en de buitengerechtelijke procedure (1)

ALBERT II, Koning der Belgen,

Aan allen die nu zijn en hierna wezen zullen, Onze Groet.

De Kamers hebben aangenomen en Wij bekrachtigen hetgeen volgt :

HOOFDSTUK I. — *Algemene bepaling*

Artikel 1. Deze wet regelt een aangelegenheid als bedoeld in artikel 78 van de Grondwet.

HOOFDSTUK II. — *Wijzigingen van het Burgerlijk Wetboek*

Art. 2. Artikel 1322 van het Burgerlijk Wetboek wordt aangevuld met het volgende lid :

« Kan, voor de toepassing van dit artikel, voldoen aan de vereiste van een handtekening, een geheel van elektronische gegevens dat aan een bepaalde persoon kan worden toegerekend en het behoud van de integriteit van de inhoud van de akte aantoont. »

Art. 3. In boek III van hetzelfde Wetboek wordt, onder een titel XXI, met als opschrift « Kennisgeving », artikel 2281, opgeheven bij de wet van 15 december 1949, hersteld in de volgende lezing :

« Art. 2281. Wanneer een kennisgeving schriftelijk dient te gebeuren om door de kennisgever te kunnen worden aangevoerd, wordt ook een kennisgeving per telegram, telex, telefax, elektronische post of enig ander telecommunicatiemiddel dat resulteert in een schriftelijk stuk aan de zijde van de geadresseerde, als een schriftelijke kennisgeving beschouwd. Hetzelfde geldt wanneer de kennisgeving slechts daarom niet in een schriftelijk stuk resulteert aan de zijde van de geadresseerde omdat deze een andere wijze van ontvangst hanteert.

De kennisgeving gaat in bij ontvangst ervan in de vormen genoemd in het eerste lid.

MINISTERE DE LA JUSTICE

F. 2000 — 3304 [2000/10017]

20 OCTOBRE 2000. — Loi introduisant l'utilisation de moyens de télécommunication et de la signature électronique dans la procédure judiciaire et extrajudiciaire (1)

ALBERT II, Roi des Belges,

A tous, présents et à venir, Salut.

Les Chambres ont adopté et Nous sanctionnons ce qui suit :

CHAPITRE Ier. — *Disposition générale*

Article 1er. La présente loi règle une matière visée à l'article 78 de la Constitution.

CHAPITRE II. — *Modifications du Code civil*

Art. 2. L'article 1322 du Code civil est complété par l'alinéa suivant :

« Peut satisfaire à l'exigence d'une signature, pour l'application du présent article, un ensemble de données électroniques pouvant être imputé à une personne déterminée et établissant le maintien de l'intégrité du contenu de l'acte. »

Art. 3. Dans le livre III du même Code, sous un titre XXI, intitulé « De la notification », l'article 2281, abrogé par la loi du 15 décembre 1949, est rétabli dans la rédaction suivante :

« Art. 2281. Lorsqu'une notification doit avoir lieu par écrit pour pouvoir être invoquée par celui qui l'a faite, une notification faite par télégramme, par télex, par télécopie, par courrier électronique ou par tout autre moyen de communication, qui se matérialise par un document écrit chez le destinataire, est également considérée comme une notification écrite. La notification est également considérée comme écrite si elle ne se matérialise pas par un document écrit chez le destinataire pour la seule raison que celui-ci utilise un autre mode de réception.

La notification est accomplie dès sa réception dans les formes énumérées à l'alinéa 1er.

Ontbreekt een handtekening in de zin van artikel 1322, dan kan de geadresseerde de kennisgever zonder onnodig uitstel verzoeken om een origineel ondertekend exemplaar na te zenden. Doet hij dit niet zonder onnodig uitstel, of gaat de kennisgever zonder onnodig uitstel op dit verzoek in, dan kan de geadresseerde het ontbreken van een handtekening niet aanvoeren. »

HOOFDSTUK III. — *Wijzigingen van het Gerechtelijk Wetboek*

Art. 4. In artikel 32 van het Gerechtelijk Wetboek worden de volgende wijzigingen aangebracht :

1° in punt 2° worden tussen de woorden « post » en « of » de woorden « , per fax of per elektronische post » ingevoegd;

2° het artikel wordt aangevuld met de volgende leden :

« Een mededeling, kennisgeving of neerlegging die per gewone brief kan geschieden, kan eveneens geldig per fax of per elektronische post geschieden, voor zover de geadresseerde een faxnummer of elektronisch adres opgeeft, dan wel regelmatig gebruikt.

Een mededeling, kennisgeving of neerlegging die bij een ter post aangetekende brief dient te geschieden, kan eveneens geldig per fax of elektronische post geschieden, mits dit een ontvangstbewijs oplevert vanwege de geadresseerde. »

Art. 5. In artikel 52 van hetzelfde Wetboek worden de volgende wijzigingen aangebracht :

1° in het tweede lid worden de woorden « Een akte kan evenwel » vervangen door de woorden « Tenzij een handeling geldig per fax of per elektronische post kan worden verricht, kan zij »;

2° het artikel wordt aangevuld met het volgende lid :

« De datum van een handeling per fax of elektronische post wordt bepaald door het tijdstip van aankomst, ongeacht of de griffie op dat tijdstip toegankelijk is voor het publiek of niet. »

Art. 6. Artikel 863 van hetzelfde Wetboek, opgeheven bij de wet van 3 augustus 1992, wordt hersteld in de volgende lezing :

« Art. 863. In alle gevallen waarin de ondertekening vereist is voor de geldigheid van een proceshandeling, kan de nietigheid slechts worden uitgesproken indien de ondertekening niet wordt geregulariseerd ter zitting of binnen een door de rechter vastgestelde termijn.

Het vereiste van de ondertekening staat er niet aan in de weg dat de handeling ook geldig per fax of per elektronische post kan worden verricht, maar de rechter kan op verzoek van een partij die daar belang bij heeft de auteur van de handeling bevelen de ondertekening te bevestigen. »

HOOFDSTUK IV. — *Inwerkingtreding*

Art. 7. De Koning stelt de datum van de inwerkingtreding van de artikelen 4 tot 6 van deze wet vast.

Kondigen deze wet af, bevelen dat zij met 's Lands zegel zal worden bekleed en door het *Belgisch Staatsblad* zal worden bekendgemaakt.

Gegeven te Brussel, 20 oktober 2000.

ALBERT

Van Koningswege :

De Minister van Justitie,
M. VERWILGHEN

Met 's Lands zegel gezegeld :

De Minister van Justitie,
M. VERWILGHEN

Nota

(1) *Buitengewone zitting 1999.*
Kamer van volksvertegenwoordigers.
Parlementaire stukken. — Wetsvoorstel, nr. 38/1 van 4 augustus 1999.
Gewone zitting 1999-2000.
Kamer van volksvertegenwoordigers.
Parlementaire stukken. — Amendementen, nrs. 38/2-4. — Erratum, nr. 38/5. — Amendementen, nrs. 38/6-7. — Verslag van de heer Somers, nr. 38/8 van 30 juni 2000. — Tekst aangenomen door de commissie, nr. 38/9 van 30 juni 2000. — Tekst aangenomen in plenaire vergadering en overgezonden aan de Senaat, nr. 38/10 van 6 juli 2000.

Parlementaire Handelingen. — Bespreking en aanneming. — Vergadering van 6 juli 2000.
Senaat.
Parlementaire stukken. — Wetsontwerp overgezonden door de Kamer van volksvertegenwoordigers, nr. 2-511/1 van 7 juli 2000. — Wetsontwerp niet gevoceerd door de Senaat, nr. 2-511/2 van 12 oktober 2000.

A défaut de signature au sens de l'article 1322, le destinataire peut, sans retard injustifié, demander au notifiant de lui fournir un exemplaire original signé. S'il ne le demande pas sans retard injustifié ou si, sans retard injustifié, le notifiant fait droit à cette demande, le destinataire ne peut invoquer l'absence de signature. »

CHAPITRE III. — *Modifications du Code judiciaire*

Art. 4. A l'article 32 du Code judiciaire sont apportées les modifications suivantes :

1° au 2°, les mots « par télécopie ou par courrier électronique » sont insérés entre le mot « , poste » et le mot « ou »;

2° l'article est complété par les alinéas suivants :

« Une communication, une notification ou un dépôt qui peuvent avoir lieu par lettre ordinaire, peuvent également avoir lieu valablement par télécopie ou par courrier électronique, pour autant que le destinataire indique un numéro de téléfax ou une adresse électronique ou les utilise régulièrement.

Une communication, une notification ou un dépôt qui doivent avoir lieu par lettre recommandée à la poste, peuvent également avoir lieu valablement par télécopie ou par courrier électronique, pour autant que le destinataire fournisse un accusé de réception. »

Art. 5. A l'article 52 du même Code sont apportées les modifications suivantes :

1° dans l'alinéa 2 les mots « Un acte ne peut toutefois » sont remplacés par les mots « A moins qu'il puisse être accompli valablement par télécopie ou par courrier électronique, un acte ne peut »;

2° l'article est complété par l'alinéa suivant :

« La date d'un acte accompli par télécopie ou par courrier électronique est déterminée par le moment où il arrive, que le greffe soit ou non accessible au public à ce moment. »

Art. 6. L'article 863 du même Code, abrogé par la loi du 3 août 1992, est rétabli dans la rédaction suivante :

« Art. 863. Dans tous les cas où la signature est nécessaire pour qu'un acte de procédure soit valable, la nullité ne peut être prononcée que si la signature n'est pas régularisée à l'audience ou dans un délai fixé par le juge.

L'exigence de la signature n'empêche pas que l'acte puisse également être accompli valablement par télécopie ou par courrier électronique. Si une partie qui y a intérêt le demande, le juge peut toutefois ordonner à l'auteur de l'acte de confirmer la signature. »

CHAPITRE IV. — *Entrée en vigueur*

Art. 7. Le Roi fixe la date d'entrée en vigueur des articles 4 à 6 de la présente loi.

Promulguons la présente loi, ordonnons qu'elle soit revêtue du sceau de l'Etat et publiée par le *Moniteur belge*.

Donné à Bruxelles, le 20 octobre 2000.

ALBERT

Par le Roi :

Le Ministre de la Justice,
M. VERWILGHEN

Scellé du sceau de l'Etat :

Le Ministre de la Justice,
M. VERWILGHEN

Note

(1) *Session extraordinaire 1999.*
Chambre des représentants.
Documents parlementaires. — Proposition de loi, n° 38/1 du 4 août 1999.
Session ordinaire 1999-2000.
Chambre des représentants.
Documents parlementaires. — Amendements, n^{os} 38/2-4. — Erratum, n° 38/5. — Amendements, n^{os} 38/6-7. — Rapport de M. Somers, n° 38/8 du 30 juin 2000. — Texte adopté par la commission, n° 38/9 du 30 juin 2000. — Texte adopté en séance plénière et transmis au Sénat, n° 38/10 du 6 juillet 2000.

Annales parlementaires. — Discussion et adoption. — Séance du 6 juillet 2000.
Sénat.
Documents parlementaires. — Projet de loi transmis par la Chambre des représentants, n° 2-511/1 du 7 juillet 2000. — Projet de loi non évoqué par le Sénat, n° 2-511/2 du 12 octobre 2000.

Bijlage 3: Wet van 9 juli 2001 houdende vaststelling van bepaalde regels in verband met het juridisch kader voor elektronische handtekeningen en certificatiediensten

LOIS, DECRETS, ORDONNANCES ET REGLEMENTS
WETTEN, DECRETEN, ORDONNANTIES EN VERORDENINGEN

MINISTERE DES AFFAIRES ECONOMIQUES

F. 2001 — 2699 [2001/11298]

9 JUILLET 2001. —Loi fixant certaines règles relatives au cadre juridique pour les signatures électroniques et les services de certification

ALBERT II, Roi des Belges,
A tous, présents et à venir, Salut.

Les Chambres ont adopté et Nous sanctionnons ce qui suit :

CHAPITRE Ier. — *Disposition générale*

Article 1er. La présente loi règle une matière visée à l'article 78 de la Constitution.

CHAPITRE II. — *Définitions et champ d'application de la loi*

Section 1re. — Définitions

Art. 2. La présente loi transpose les dispositions de la directive 1999/93/CE du Parlement européen et du Conseil du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques.

Pour l'application de la présente loi et de ses arrêtés d'exécution, on entend par :

1° « signature électronique » : une donnée sous forme électronique jointe ou liée logiquement à d'autres données électroniques et servant de méthode d'authentification;

2° « 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;

3° « certificat » : une attestation électronique qui lie des données afférentes à la vérification de signature à une personne physique ou morale et confirme l'identité de cette personne;

4° « certificat qualifié » : un certificat qui satisfait aux exigences visées à l'annexe I de la présente loi et qui est fourni par un prestataire de service de certification satisfaisant aux exigences visées à l'annexe II de la présente loi;

5° « titulaire de certificat » : une personne physique ou morale à laquelle un prestataire de service de certification a délivré un certificat;

6° « 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;

7° « 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'annexe III de la présente loi;

8° « 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;

9° « dispositif de vérification de signature » : un dispositif logiciel ou matériel configuré pour mettre en application les données afférentes à la vérification de signature;

10° « 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;

MINISTERIE VAN ECONOMISCHE ZAKEN

N. 2001 — 2699 [2001/11298]

9 JULI 2001. — Wet houdende vaststelling van bepaalde regels in verband met het juridisch kader voor elektronische handtekeningen en certificatiediensten

ALBERT II, Koning der Belgen,
Aan allen die nu zijn en hierna wezen zullen, Onze Groet.

De Kamers hebben aangenomen en Wij bekrachtigen hetgeen volgt :

HOOFDSTUK I. — *Algemene bepaling*

Artikel 1. Deze wet regelt een aangelegenheid als bedoeld in artikel 78 van de Grondwet.

HOOFDSTUK II. — *Definities en toepassingsgebied van de wet*

Afdeling 1. — Definities

Art. 2. Deze wet zet de bepalingen om van de Richtlijn 1999/93/EG van het Europees Parlement en de Raad van 13 december 1999 betreffende een gemeenschappelijk kader voor elektronische handtekeningen.

Voor de toepassing van deze wet en de uitvoeringsbesluiten ervan wordt verstaan onder :

1° « elektronische handtekening » : gegevens in elektronische vorm, vastgehecht aan of logisch geassocieerd met andere elektronische gegevens, die worden gebruikt als middel voor authentificatie.

2° « 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 voldoet :

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;

3° « certificaat » : een elektronische bevestiging die de gegevens voor het verifiëren van de handtekening koppelt aan een natuurlijke persoon of een rechtspersoon en de identiteit van die persoon bevestigt;

4° « gekwalificeerd certificaat » : een certificaat dat voldoet aan de eisen van bijlage I van deze wet en dat wordt afgegeven door een certificatiedienstverlener die voldoet aan de eisen van bijlage II van deze wet;

5° « certificaathouder » : een natuurlijke persoon of rechtspersoon aan wie een certificatiedienstverlener een certificaat heeft afgegeven;

6° « 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;

7° « 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 bijlage III van deze wet;

8° « 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;

9° « 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;

10° « certificatiedienstverlener » : elke natuurlijke persoon of rechtspersoon die certificaten afgeeft en beheert of andere diensten in verband met elektronische handtekeningen verleent;

11° « 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;

12° « Administration » : l'administration du ministère des Affaires économiques qui est chargée des tâches relatives à l'accréditation et au contrôle des prestataires de service de certification délivrant des certificats qualifiés et établis en Belgique;

13° « entité » : organisme qui démontre sa compétence sur 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 des laboratoires d'essais, ou par un organisme équivalent établi dans l'Espace économique européen.

Section 2. — Champ d'application

Art. 3. La présente loi fixe certaines règles relatives au cadre juridique pour les signatures électroniques et définit 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 titulaires de certificats sans préjudice des dispositions légales concernant les règles de représentations des personnes morales.

La présente loi instaure également un régime d'accréditation volontaire.

CHAPITRE III. — *Principes généraux*

Art. 4. § 1er. A défaut de dispositions légales contraires, nul ne peut être contraint de poser un acte juridique par voie électronique.

§ 2. Nul prestataire de service de certification ne peut être contraint de demander une autorisation préalable pour exercer ses activités.

Néanmoins, les prestataires de service de certification délivrant des certificats qualifiés établis en Belgique doivent communiquer les informations suivantes à l'Administration, soit dans le mois suivant la publication de la présente loi, soit avant le début de leurs activités :

— leur nom;

— l'adresse géographique où ils sont établis;

— les coordonnées permettant de les contacter rapidement, y compris leur adresse de courrier électronique;

— le cas échéant, leur titre professionnel et leurs références et leurs numéros d'identification (registre de commerce, T.V.A.);

— la preuve qu'une assurance a été souscrite en vue de couvrir leurs obligations visées à l'article 14.

L'Administration leur délivre un récépissé dans les cinq jours ouvrables suivant la réception de leur communication.

§ 3. Le Roi peut, par arrêté délibéré en Conseil des Ministres, soumettre l'usage des signatures électroniques dans le secteur public à des exigences supplémentaires éventuelles. Ces exigences doivent être objectives, transparentes, proportionnées et non discriminatoires et ne s'appliquer qu'aux caractéristiques spécifiques de l'application concernée. Ces exigences ne peuvent pas constituer un obstacle aux services transfrontaliers pour les citoyens.

§ 4. Sans préjudice des articles 1323 et suivants du Code civil, une signature électronique avancée réalisée sur la base d'un certificat qualifié et conçue au moyen d'un dispositif sécurisé de création de signature électronique, est assimilée à une signature manuscrite, qu'elle soit réalisée par une personne physique ou morale.

§ 5. Une signature électronique ne peut être privée de son efficacité juridique et ne peut être refusée comme preuve en justice au seul motif :

— que la signature se présente sous forme électronique, ou

— qu'elle ne repose pas sur un certificat qualifié, ou

— qu'elle ne repose pas sur un certificat qualifié délivré par un prestataire accrédité de service de certification, ou

— qu'elle n'est pas créée par un dispositif sécurisé de création de signature.

11° « product voor elektronische handtekeningen » : software of hardware, of relevante componenten daarvan, die door certificatiedienstverleners kunnen worden gebruikt om diensten op het gebied van elektronische handtekeningen te verlenen of die voor het aanmaken of verifiëren van elektronische handtekeningen kunnen worden gebruikt;

12° « Bestuur » : het bestuur van het ministerie van Economische Zaken dat belast is met de taken betreffende de accreditatie en de controle van de certificatiedienstverleners die gekwalificeerde certificaten afgeven en in België gevestigd zijn;

13° « entiteit » : instelling die haar bevoegdheid aantoont op grond van een certificaat afgegeven door het Belgisch accreditatiessysteem conform de wet van 20 juli 1990 betreffende de accreditatie van certificatie- en keuringsinstellingen alsmede van beproevingslaboratoria of door een gelijkwaardige instelling opgericht binnen de Europese Economische Ruimte.

Afdeling 2. — Toepassingsgebied

Art. 3. Deze wet legt bepaalde regels vast in verband met het juridisch kader voor elektronische handtekeningen en bepaalt het juridisch stelsel van toepassing op de activiteiten van de certificatiedienstverleners evenals de door deze laatste en de certificaathouders na te leven regels, zonder afbreuk te doen aan de wettelijke bepalingen met betrekking tot de bevoegdheid tot het stellen van rechtshandelingen voor rekening van rechtspersonen.

Deze wet voert eveneens een vrijwillig accreditatiestelsel in.

HOOFDSTUK III. — *Algemene principes*

Art. 4. § 1. Behoudens andersluidende wettelijke bepalingen kan niemand verplicht worden rechtshandelingen te stellen via elektronische weg.

§ 2. Een certificatiedienstverlener kan niet verplicht worden een voorafgaande machtiging aan te vragen voor de uitoefening van zijn activiteiten.

De in België gevestigde certificatiedienstverleners die gekwalificeerde certificaten afgeven dienen niettemin, ofwel in de loop van de maand die volgt op de bekendmaking van deze wet, ofwel voor de aanvang van hun activiteiten, de volgende inlichtingen mee te delen aan het Bestuur :

— hun naam;

— het geografisch adres waar ze gevestigd zijn;

— hun coördinaten, waardoor ze gemakkelijk te bereiken zijn, met inbegrip van hun adres voor elektronische post;

— in voorkomend geval, hun beroep, referenties en identificatienummers (handelsregister, BTW);

— het bewijs dat er een verzekering onderschreven werd ter dekking van hun verplichtingen bedoeld in artikel 14.

Het Bestuur overhandigt hen een ontvangstbewijs binnen vijf werkdagen volgend op de ontvangst van hun mededeling.

§ 3. De Koning kan, bij een besluit vastgesteld na overleg in Ministerraad, voor het gebruik van elektronische handtekeningen in de openbare sector eventuele aanvullende eisen stellen. Deze eisen moeten objectief, transparant, evenredig en niet discriminerend zijn en mogen slechts op de specifieke kenmerken van de betrokken toepassing betrekking hebben. Zij mogen geen belemmering vormen voor grensoverschrijdende diensten voor de burgers.

§ 4. Onverminderd de artikelen 1323 en volgende van het Burgerlijk Wetboek wordt een geavanceerde elektronische handtekening, gerealiseerd op basis van een gekwalificeerd certificaat en aangemaakt door een veilig middel voor het aanmaken van een handtekening, geassimileerd met een handgeschreven handtekening ongeacht of deze handtekening gerealiseerd wordt door een natuurlijke dan wel door een rechtspersoon.

§ 5. Een elektronische handtekening kan geen rechtsgeldigheid worden ontzegd en niet als bewijsmiddel in gerechtelijke procedures worden geweigerd louter op grond van het feit dat :

— de handtekening in elektronische vorm is gesteld, of

— niet is gebaseerd op een gekwalificeerd certificaat, of

— niet is gebaseerd op een door een geaccrediteerd certificatiedienstverlener afgegeven certificaat, of

— zij niet met een veilig middel is aangemaakt.

Art. 5. § 1er. Sans préjudice de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, 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.

CHAPITRE IV. — *Des produits de signature électronique*

Art. 6. Lorsqu'un produit de signature électronique est conforme à des normes dont les numéros de référence sont publiés au *Journal officiel des Communautés européennes* conformément à la procédure visée par la directive 99/93/CE du Parlement et du Conseil du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques, ce produit est présumé conforme aux exigences visées à l'annexe II point *f)*, et à l'annexe III de la présente loi.

Art. 7. § 1er. Les exigences relatives aux dispositifs sécurisés de création de signature électronique sont reprises à l'annexe III de la présente loi.

§ 2. La conformité des dispositifs sécurisés de création de signature électronique par rapport aux exigences visées à l'annexe III de la présente loi est attestée par des organismes compétents désignés par l'Administration et dont la liste est communiquée à la Commission européenne.

§ 3. Le Roi détermine les conditions auxquelles doivent répondre les organismes visés au paragraphe précédent.

§ 4. La conformité établie par un organisme désigné par un autre Etat membre de l'Espace économique européen est reconnue en Belgique.

CHAPITRE V. — *Des prestataires de service de certification délivrant des certificats qualifiés*

Section 1re. — Des certificats qualifiés

Sous-section 1re. — Des missions

Art. 8. § 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. Après avoir vérifié son identité et, le cas échéant, ses qualités spécifiques, le prestataire de service de certification délivre un ou plusieurs certificats à toute personne qui en fait la demande.

§ 3. En ce qui concerne les personnes morales, le prestataire de services de certification tient un registre contenant le nom et la qualité de la personne physique qui représente la personne morale et qui fait usage de la signature liée au certificat, de telle manière qu'à chaque utilisation de cette signature, on puisse établir l'identité de la personne physique.

Art. 9. Le prestataire de service de certification fournit un exemplaire du certificat au candidat titulaire.

Art. 10. Le prestataire de service de certification conserve un annuaire électronique comprenant les certificats qu'il délivre et le moment de leur expiration.

Sous-section 2
Exigences relatives aux certificats qualifiés

Art. 11. § 1er. Les certificats qualifiés doivent satisfaire aux exigences visées à l'annexe I de la présente loi.

§ 2. Les prestataires de service de certification qui délivrent des certificats qualifiés doivent satisfaire aux exigences visées à l'annexe II de la présente loi.

Sous-section 3
De la révocation des certificats qualifiés

Art. 12. § 1er. A la demande du titulaire du certificat, préalablement identifié, le prestataire de service de certification révoque immédiatement le certificat.

Art. 5. § 1. Onverminderd de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten aanzien van de verwerking van persoonsgegevens, mag een certificatiedienstverlener die voor het publiek bestemde certificaten afgeeft enkel rechtstreeks bij de betrokken persoon of met diens uitdrukkelijke toestemming persoonlijke gegevens inwinnen en enkel indien dit noodzakelijk is voor de afgifte en de bewaring van het certificaat. De gegevens mogen niet voor andere doeleinden worden verzameld of verwerkt zonder de uitdrukkelijke toestemming van de betrokken persoon.

§ 2. Wanneer de houder van het certificaat een pseudoniem gebruikt en wanneer het onderzoek dit vereist, is de certificatiedienstverlener die het certificaat heeft afgegeven ertoe gehouden alle gegevens betreffende de identiteit van de titularis mee te delen in de omstandigheden en volgens de voorwaarden waarin de artikelen 90*ter* tot 90*decies* van het Wetboek van Strafvordering voorzien.

HOOFDSTUK IV. — *Producten voor elektronische handtekeningen*

Art. 6. Wanneer een product voor elektronische handtekeningen overeenstemt met de normen waarvan de referentienummers worden gepubliceerd in het *Publicatieblad van de Europese Gemeenschappen*, overeenkomstig de procedure bedoeld in de richtlijn 99/93/EG van het Parlement en van de Raad van 13 december 1999 betreffende een communautair kader voor de elektronische handtekeningen, wordt dit product verondersteld te voldoen aan de eisen van bijlage II, punt *f)*, en bijlage III van deze wet.

Art. 7. § 1. De eisen in verband met de veilige middelen voor het aanmaken van een elektronische handtekening zijn vermeld in bijlage III van deze wet.

§ 2. De overeenstemming van de veilige middelen voor het aanmaken van een elektronische handtekening met de eisen van bijlage III van deze wet, wordt bevestigd door de bevoegde instellingen, aangewezen door het Bestuur en waarvan de lijst wordt meegedeeld aan de Europese Commissie.

§ 3. De Koning bepaalt de voorwaarden waaraan de instellingen bedoeld in de vorige paragraaf moeten voldoen.

§ 4. De overeenstemming vastgesteld door een instelling aangewezen door een andere lidstaat van de Europese Economische Ruimte, wordt in België erkend.

HOOFDSTUK V. — *Certificatiedienstverleners die gekwalificeerde certificaten afgeven*

Afdeling 1. — Gekwalificeerde certificaten

Onderafdeling 1. — Opdrachten

Art. 8. § 1. Vooraleer een certificaat af te geven, onderzoekt de certificatiedienstverlener de complementariteit van de gegevens voor het aanmaken en het verifiëren van de handtekening.

§ 2. Na de identiteit en, in voorkomend geval, de specifieke hoedanigheden geverifieerd te hebben, geeft de certificatiedienstverlener één of meer certificaten af aan elke persoon die daarom verzoekt.

§ 3. Voor de rechtspersonen houdt de certificatiedienstverlener een register bij met de identiteit en de hoedanigheid van de natuurlijke persoon die de rechtspersoon vertegenwoordigt en die gebruik maakt van de handtekening verbonden aan het certificaat, op zo een wijze dat bij elk gebruik van deze handtekening de identiteit van de natuurlijke persoon kan achterhaald worden.

Art. 9. De certificatiedienstverlener verschaft een exemplaar van het certificaat aan de kandidaat-houder.

Art. 10. De certificatiedienstverlener houdt een elektronisch register bij met de certificaten die hij afgeeft en het tijdstip waarop ze vervallen.

Onderafdeling 2
Vereisten betreffende de gekwalificeerde certificaten

Art. 11. § 1. De gekwalificeerde certificaten moeten voldoen aan de eisen van bijlage I van deze wet.

§ 2. De certificatiedienstverleners die gekwalificeerde certificaten afgeven, moeten voldoen aan de eisen van bijlage II van deze wet.

Onderafdeling 3
Herroeping van de gekwalificeerde certificaten

Art. 12. § 1. Op aanvraag van de vooraf geïdentificeerde certificaathouder herroept de certificatiedienstverlener onmiddellijk het certificaat.

§ 2. Le prestataire de service de certification révoque également un certificat lorsque :

1° il existe des raisons sérieuses pour admettre que le certificat a été délivré sur 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° les tribunaux ont ordonné les mesures prévues à l'article 20, § 4, *b)*;

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 garantissant un niveau de qualité et de sécurité équivalent;

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, sauf en cas de décès, 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 est définitive.

Art. 13. § 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.

Sous-section 4. — De la responsabilité des prestataires de service de certification délivrant des certificats qualifiés

Art. 14. § 1er. Un prestataire de service de certification qui délivre à l'intention du public un certificat présenté comme qualifié ou qui garantit au public un tel certificat est responsable du préjudice causé à tout organisme ou personne physique ou morale qui, en bon père de famille, se fie raisonnablement à ce certificat pour ce qui est de :

a) l'exactitude de toutes les informations contenues dans le certificat qualifié à la date où il a été délivré et la présence, dans ce certificat, de toutes les données prescrites pour un certificat qualifié;

b) l'assurance que, au moment de la délivrance du certificat, le signataire identifié dans le certificat qualifié détenait les données afférentes à la création de signature correspondant aux données afférentes à la vérification de signature fournies ou identifiées dans le certificat;

c) 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, dans le cas où le prestataire de service de certification génère ces deux types de données;

sauf si le prestataire de service de certification prouve qu'il n'a commis aucune négligence.

§ 2. Un prestataire de service de certification qui a délivré à l'intention du public un certificat présenté comme qualifié est responsable du préjudice causé à un organisme ou à une personne physique ou morale qui se prévaut raisonnablement du certificat, pour avoir omis de faire enregistrer la révocation du certificat, sauf si le prestataire de service de certification prouve qu'il n'a commis aucune négligence.

§ 3. Un prestataire de service de certification peut indiquer, dans un certificat qualifié, les limites fixées à son utilisation, à condition que ces limites soient discernables par des tiers. Le prestataire de service de certification ne doit pas être tenu responsable du préjudice résultant de l'usage d'un certificat qualifié qui dépasse les limites fixées à son utilisation.

§ 4. Un prestataire de service de certification peut indiquer, dans un certificat qualifié, la valeur maximale des transactions pour lesquelles le certificat peut être utilisé, à condition que cette valeur soit discernable par des tiers. Le prestataire de service de certification n'est pas responsable des dommages qui résultent du dépassement de cette valeur maximale.

§ 2. De certificatiedienstverlener herroept eveneens een 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° de rechtbanken de maatregelen hebben bevolen waarin artikel 20, § 4, *b)*, voorziet;

3° de certificatiedienstverlener zijn activiteiten stopzet zonder dat deze worden overgenomen door een andere certificatiedienstverlener die een gelijkwaardig kwaliteits- en veiligheidsniveau waarborgt;

4° de certificatiedienstverlener op de hoogte gebracht wordt van het overlijden van de natuurlijke persoon of van de ontbinding van de rechtspersoon die certificaathouder is.

De certificatiedienstverlener brengt de certificaathouder, behalve in geval van overlijden, op de hoogte van de herroeping en motiveert zijn beslissing. Een maand voor het vervallen van een certificaat brengt de certificatiedienstverlener de certificaathouder hiervan op de hoogte.

§ 3. De herroeping van een certificaat is definitief.

Art. 13. § 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 van een certificaat schrijft de certificatiedienstverlener de vermelding van de herroeping in in het elektronisch register zoals bedoeld in artikel 10.

Vanaf deze inschrijving is de herroeping tegenstelbaar ten aanzien van derden.

Onderafdeling 4. — Aansprakelijkheid van de certificatiedienstverleners die gekwalificeerde certificaten afgeven

Art. 14. § 1. Een certificatiedienstverlener die een gekwalificeerd certificaat aan het publiek afgeeft of een dergelijk certificaat publiekelijk waarborgt, is aansprakelijk voor de schade die hij toebrengt aan elke instelling of natuurlijke persoon of rechtspersoon die, als een goede huisvader, redelijkerwijze vertrouwen stelt in dit certificaat, voor wat betreft :

a) de juistheid van alle gegevens die in het gekwalificeerd certificaat opgenomen zijn op de datum dat het werd afgegeven en de vermelding, in dit certificaat, van alle voorgeschreven gegevens voor een gekwalificeerd certificaat;

b) de garantie dat de in het gekwalificeerde certificaat geïdentificeerde ondertekenaar, op het tijdstip van de afgifte van het certificaat, de gegevens bevat voor het aanmaken van de handtekening overeenstemmend met de in het certificaat vermelde of geïdentificeerde gegevens voor het verifiëren van de handtekening;

c) de garantie dat de gegevens voor het aanmaken en die voor het verifiëren van een handtekening complementair kunnen worden gebruikt, in geval de certificatiedienstverlener beide soorten gegevens genereert;

tenzij de certificatiedienstverlener bewijst dat er van geen enkele nalatigheid sprake is.

§ 2. Een certificatiedienstverlener die aan het publiek een certificaat heeft afgegeven dat als gekwalificeerd bestempeld wordt, is aansprakelijk voor de schade die hij toebrengt aan een instelling of natuurlijke persoon of rechtspersoon die zich op redelijke wijze beroept op het certificaat, wanneer werd nagelaten de herroeping van het certificaat te laten registreren, tenzij de certificatiedienstverlener bewijst dat er van geen enkele nalatigheid sprake is.

§ 3. Een certificatiedienstverlener kan in een gekwalificeerd certificaat de beperkingen voor het gebruik ervan bepalen, op voorwaarde dat die beperkingen voor derden herkenbaar zijn. De certificatiedienstverlener is niet aansprakelijk voor de schade die voortvloeit uit het gebruik van een gekwalificeerd certificaat waarbij de aangegeven beperkingen voor het gebruik worden overschreden.

§ 4. Een certificatiedienstverlener kan in een gekwalificeerd certificaat de maximumwaarde bepalen van de transacties waarvoor het certificaat kan worden gebruikt, op voorwaarde dat die waarde voor derden herkenbaar is. De certificatiedienstverlener is niet aansprakelijk voor de schade die voortvloeit uit het overschrijden van die maximumwaarde.

Sous-section 5. — De l'arrêt des activités des prestataires de service de certification délivrant des certificats qualifiés

Art. 15. § 1er. Le prestataire de service de certification qui délivre des certificats qualifiés informe l'Administration dans un délai raisonnable de son intention de mettre fin à ses activités de prestataire de service de certification qualifiée 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 garantissant un même niveau de qualité et de sécurité, ou à défaut, révoque les certificats deux mois après en avoir averti les titulaires. Dans ce cas, le prestataire de service de certification prend les mesures nécessaires pour satisfaire à l'obligation prévue à l'Annexe II, *i)*.

§ 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. Il procède, le cas échéant, à la révocation des certificats et prend les mesures nécessaires pour satisfaire à l'obligation prévue à l'Annexe II, *i)*.

Sous-section 6. — Certificats délivrés à titre de certificats qualifiés par des prestataires de service de certification étrangers

Art. 16. § 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'Espace économique européen est assimilé aux certificats qualifiés délivrés par un prestataire de service de certification établi en Belgique.

§ 2. Les certificats délivrés à titre de certificats qualifiés à l'intention du public par un prestataire de service de certification établi dans un pays tiers sont reconnus équivalents, sur le plan juridique, aux certificats délivrés par un prestataire de service de certification établi en Belgique :

a) si le prestataire de service de certification remplit les conditions visées par sa réglementation nationale transposant la directive 99/93/CE du Parlement et du Conseil du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques et a été accrédité dans le cadre d'un régime volontaire d'accréditation établi dans un Etat membre de l'Espace économique européen;

ou

b) si un prestataire de service de certification établi dans la Communauté européenne, qui satisfait aux exigences visées par la réglementation nationale transposant la directive 99/93/CE du Parlement et du Conseil du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques, garantit le certificat;

ou

c) si le certificat ou le prestataire de service de certification est reconnu en application d'un accord bilatéral ou multilatéral entre la Communauté européenne et des pays tiers ou des organisations internationales.

Section 2. — Des prestataires de service de certification accrédités

Art. 17. § 1er. Un prestataire de service de certification qui répond aux exigences de l'annexe II, délivrant des certificats qualifiés qui répondent aux exigences de l'annexe I et qui utilise des dispositifs de création répondant aux exigences de l'annexe III, peut demander une accréditation à l'Administration.

L'accréditation prévue par la présente loi se base sur le résultat d'une évaluation, par une entité visée à l'article 2, 13°, de la conformité aux exigences des annexes I, II et III, et le cas échéant, à celles liées à d'autres services et produits délivrés par les prestataires de service de certification.

§ 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 au « Fonds pour l'accréditation » pour la délivrance, la gestion et la surveillance de l'accréditation;

3° les délais d'examen de la demande;

4° les modalités du contrôle des prestataires de service de certification accrédités.

§ 3. Le choix de recourir à un prestataire de services de certification accrédité est libre.

Art. 18. L'Administration :

1° octroie et retire les accréditations. Cette mission s'exerce selon des règles, par des services et des personnes distincts de ceux visés à l'article 20, § 2;

Onderafdeling 5. — Stopzetting van de activiteiten van de certificatiedienstverleners die gekwalificeerde certificaten afgeven

Art. 15. § 1. De certificatiedienstverlener die gekwalificeerde certificaten afgeeft, brengt binnen een redelijke termijn het Bestuur op de hoogte van zijn bedoeling om zijn activiteiten van gekwalificeerde certificatiedienstverlener 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 certificatiedienstverlener die eenzelfde kwaliteits- en veiligheidsniveau waarborgt. Wanneer dit niet mogelijk is, herroept hij de certificaten twee maanden na de houders ervan te hebben ingelicht. In dit geval treft de certificatiedienstverlener de nodige maatregelen om te voldoen aan de verplichting waarin Bijlage II, *i)*, voorziet.

§ 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. Hij zorgt in voorkomend geval voor de herroeping van de certificaten en treft de nodige maatregelen om te voldoen aan de in Bijlage II, *i)*, bepaalde verplichting.

Onderafdeling 6. — Certificaten afgegeven als gekwalificeerde certificaten door buitenlandse certificatiedienstverleners

Art. 16. § 1. Een voor het publiek bestemd gekwalificeerd certificaat afgegeven door een certificatiedienstverlener gevestigd in een lidstaat van de Europese Economische Ruimte, wordt gelijkgesteld met de gekwalificeerde certificaten afgeven door een in België gevestigde certificatiedienstverlener.

§ 2. De voor het publiek bestemde certificaten, die als gekwalificeerde certificaten worden afgegeven door een certificatiedienstverlener gevestigd in een derde land, worden op juridisch vlak gelijkgesteld met de certificaten afgegeven door een certificatiedienstverlener die in België gevestigd is :

a) indien de certificatiedienstverlener voldoet aan de voorwaarden van de nationale reglementering waarin de richtlijn 99/93/EG van het Parlement en van de Raad van 13 december 1999 betreffende een communautair kader voor de elektronische handtekeningen werd omgezet en indien hij geaccrediteerd werd op basis van een vrijwillig accreditatiesysteem ingevoerd in een lidstaat van de Europese Economische Ruimte;

of

b) indien een in de Europese Gemeenschap gevestigde certificatiedienstverlener, die voldoet aan de eisen van de nationale reglementering waarin de richtlijn 99/93/EG van het Parlement en van de Raad van 13 december 1999 betreffende een communautair kader voor de elektronische handtekeningen werd omgezet, het certificaat waarborgt;

of

c) indien het certificaat of de certificatiedienstverlener erkend wordt in het kader van de toepassing van een bilaterale of multilaterale overeenkomst tussen de Europese Gemeenschap en derde landen of internationale organisaties.

Afdeling 2. — Geaccrediteerde certificatiedienstverleners

Art. 17. § 1. Een certificatiedienstverlener die voldoet aan de eisen van bijlage II, gekwalificeerde certificaten afgeeft die overeenkomen met de eisen van bijlage I en aanmaakmiddelen gebruikt die overeenkomen met de eisen van bijlage III, kan het Bestuur om een accreditatie vragen.

De accreditatie waarin deze wet voorziet, steunt op het resultaat van een evaluatie, door een entiteit bedoeld in artikel 2, 13°, van de overeenstemming met de eisen van de bijlagen I, II en III en in voorkomend geval, met die verbonden aan andere diensten en producten afgegeven door de certificatiedienstverleners.

§ 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 aan het « Fonds voor accreditatie » verschuldigde bedragen voor het afleveren, beheren en controleren van de accreditatie;

3° de onderzoekstermijnen voor de aanvraag;

4° de regels voor de controle van de geaccrediteerde certificatiedienstverleners.

§ 3. De keuze om zich te wenden tot een geaccrediteerde certificatiedienstverlener is vrij.

Art. 18. Het Bestuur :

1° kent accreditaties toe en trekt ze in. Deze opdracht is onderworpen aan procedures en wordt uitgevoegd door personen en diensten die verschillend zijn van deze bedoeld in artikel 20, § 2:

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, 13°) ainsi que les activités de ces entités dans le cadre des procédures d'accréditation;

4° communique à la Commission et aux Etats de l'Espace économique européen :

a) les informations sur le régime volontaire d'accréditation instauré en application de la présente loi;

b) les nom et adresse de tous les prestataires de service de certification accrédités dans ce cadre;

5° exécute l'ensemble des notifications visées à l'article 11 de la directive 1999/93/CE du Parlement européen et du Conseil du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques.

CHAPITRE VI. — *Des titulaires de certificat*

Art. 19. § 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.

CHAPITRE VII. — *Du contrôle et des sanctions*

Art. 20. § 1er. Le Roi détermine, par arrêté délibéré en Conseil des Ministres, les règles relatives au contrôle des prestataires de service de certification ainsi que les moyens de droit dont l'Administration peut se prévaloir.

§ 2. L'Administration est chargée du contrôle des prestataires de service de certification qui délivrent des certificats qualifiés au public. Sous certaines conditions, fixées par le Roi, l'Administration est habilitée à demander aux prestataires de service de certification, toutes les informations nécessaires à la vérification de l'observation, par ceux-ci, de la présente loi.

§ 3. Lorsque l'Administration constate qu'un prestataire de service de certification, établi en Belgique, qui délivre des certificats qualifiés, n'observe pas les prescriptions de la présente loi, elle le met en défaut et fixe un délai raisonnable endéans lequel le prestataire de service de certification doit avoir pris les mesures nécessaires afin d'agir à nouveau en conformité avec la loi.

§ 4. Si après l'expiration de ce délai, les mesures nécessaires n'ont pas été prises, l'Administration saisira les tribunaux afin :

a) de défendre au prestataire de service de certification de continuer à délivrer des certificats qualifiés et

b) d'enjoindre au prestataire de service de certification d'informer immédiatement les titulaires des certificats qualifiés, délivrés par lui, de leur non-conformité aux prescriptions de la présente loi.

§ 5. Si, après l'écoulement du délai précité, le prestataire de service de certification accrédité en vertu de l'article 17 n'a pas régularisé sa situation, l'Administration procède au retrait d'office de son accréditation.

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 certificats.

Art. 21. § 1er. Sera puni d'une peine de huit jours à trois mois de prison et d'une amende de mille à dix mille francs, 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.

2° coördineert de coherente en transparante toepassing van de accreditatieprincipes en -procedures met toepassing van deze wet;

3° superviseert de auditprocedures van de entiteiten bedoeld in artikel 2, 13°), evenals de activiteiten van deze entiteiten in het kader van de accreditatieprocedures;

4° deelt aan de Commissie en aan de landen van de Europese Economische Ruimte het volgende mee :

a) de informatie over het vrijwillig accreditatiestelsel ingevoerd met toepassing van deze wet;

b) de naam en het adres van alle in dit kader geaccrediteerde certificatiedienstverleners;

5° voert het geheel van notificaties uit bedoeld in artikel 11 van de richtlijn 1999/93/EG van het Europees Parlement en van de Raad van 13 december 1999 betreffende een communautair kader voor de elektronische handtekeningen.

HOOFDSTUK VI. — *Certificaathouders*

Art. 19. § 1. Zodra de gegevens voor het aanmaken van een handtekening samengesteld zijn, 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 herroepen wordt, 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.

HOOFDSTUL VII. — *Controle en sancties*

Art. 20. § 1. De Koning bepaalt, bij een besluit vastgesteld na overleg in de Ministerraad, de regels betreffende de controle van de certificatiedienstverleners evenals de rechtsmiddelen die het Bestuur kan aanwenden.

§ 2. Het Bestuur is belast met de controle van de certificatiedienstverleners die gekwalificeerde certificaten afgeven aan het publiek. Onder bepaalde voorwaarden, bepaald door de Koning, is het Bestuur bevoegd om de certificatiedienstverleners alle informatie te vragen die noodzakelijk is om te controleren of zij deze wet eerbiedigen.

§ 3. Wanneer het Bestuur vaststelt dat een in België gevestigd certificatiedienstverlener, die gekwalificeerde certificaten afgeeft, zich niet houdt aan de voorschriften van deze wet, wijst het hem op die tekortkoming en stelt het een redelijke termijn vast tijdens welke de certificatiedienstverlener alle nodige maatregelen dient te hebben getroffen om opnieuw te handelen in overeenstemming met de wet.

§ 4. Indien na afloop van die termijn de nodige maatregelen niet werden getroffen, maakt het Bestuur de zaak aanhangig bij de rechtbank teneinde :

a) de certificatiedienstverlener te verbieden verder gekwalificeerde certificaten af te geven en

b) de certificatiedienstverlener te gelasten onmiddellijk de houders van gekwalificeerde certificaten, die door hem werden afgegeven, op de hoogte te brengen van het feit dat ze niet langer voldoen aan de voorschriften van deze wet.

§ 5. Wanneer, na afloop van de voormelde termijn, de certificatiedienstverlener geaccrediteerd krachtens artikel 17 de toestand niet heeft geregulariseerd, trekt het Bestuur ambtshalve zijn accreditatie in.

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. 21. § 1. Wie zich de hoedanigheid aanmatigt van geaccrediteerd certificatiedienstverlener wordt gestraft met gevangenisstraf van acht dagen tot drie maanden en met een geldboete van duizend tot tienduizend frank, of met een van die straffen alleen.

§ 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.

Promulguons la présente loi, ordonnons qu'elle soit revêtue du sceau de l'Etat et publiée par le *Moniteur belge*.

Donné à Bruxelles, le 9 juillet 2001.

ALBERT

Par le Roi :

Le Ministre de l'Economie,
Ch. PICQUE

Le Ministre de la Justice,
M. VERWILGHEN

Le Ministre des Télécommunications
et des Entreprises et Participations publiques,
R. DAEMS

Scellé du sceau de l'Etat :

Le Ministre de la Justice,
M. VERWILGHEN

Notes

(1) Chambre des Représentants :

Session ordinaire 1999-2000.

Documents parlementaires. — Projet de loi n° 322/1.

Session ordinaire 2000-2001.

Documents parlementaires. — Amendement n° 322/2 — Rapport n° 322/3 — Texte adopté par la Commission de l'Economie, de la Politique scientifique, de l'Education, des Institutions scientifiques et culturelles nationales, des Classes moyennes et de l'Agriculture n° 322/4 — Texte adopté en séance plénière et transmis au Sénat n° 322/5 — Projet amendé par le Sénat n° 322/6 — Rapport n° 322/7 — Texte adopté en séance plénière et soumis à la sanction royale n° 322/8.

Annales de la Chambre des Représentants — Compte rendu intégral : 15 février 2001. — Adoption : 14 juin 2001.

Sénat :

Session ordinaire 2000-2001.

Documents du Sénat — Projet transmis par la Chambre des Représentants n° 2-662/1 — Amendements n^{os} 2-662/2 et 3 — Rapport n° 2-662/4 — Texte amendé par la commission n° 2-662/5 — Amendements n° 2-662/6 — Texte adopté en séance plénière et renvoyé à la Chambre des Représentants n° 2-662/7.

Annales du Sénat — 17 mai 2001.

Formalités prescrites par la Directive 98/34/CE

Les formalités prescrites par la Directive 98/34/CE du 22 juin 1998 du Parlement européen et du Conseil, prévoyant une procédure d'information dans le domaine des normes et réglementations techniques et des règles relatives aux services de la société de l'information, ont été accomplies (notification 2000/0050/B).

ANNEXE I

Exigences concernant les certificats qualifiés

Tout certificat qualifié doit comporter :

a) la mention indiquant que le certificat est délivré à titre de certificat qualifié;

b) l'identification du prestataire de service de certification ainsi que le pays dans lequel il est établi;

c) le nom du signataire ou un pseudonyme qui est identifié comme tel;

d) la possibilité d'inclure, le cas échéant, une qualité spécifique du signataire, en fonction de l'usage auquel le certificat est destiné;

e) des données afférentes à la vérification de signature qui correspondent aux données pour la création de signature sous le contrôle du signataire;

f) l'indication du début et de la fin de la période de validité du certificat;

g) le code d'identité du certificat;

h) la signature électronique avancée du prestataire de service de certification qui délivre le certificat;

i) les limites à l'utilisation du certificat, le cas échéant et

j) les limites à la valeur des transactions pour lesquelles le certificat peut être utilisé, le cas échéant.

Kondigen deze wet af, bevelen dat zij met 's Lands zegel zal worden bekleed en door het *Belgisch Staatsblad* zal worden bekendgemaakt.

Gegeven te Brussel, 9 juli 2001.

ALBERT

Van Koningswege :

De Minister van Economie,
Ch. PICQUE

De Minister van Justitie,
M. VERWILGHEN

De Minister van Telecommunicatie,
en Overheidsbedrijven en Participaties,
R. DAEMS

Met 's Lands zegel gezegeld :

De Minister van Justitie,
M. VERWILGHEN

Nota's

(1) Kamer van Volksvertegenwoordigers :

Gewone zitting 1999-2000.

Parlementaire stukken. — Wetsontwerp nr. 322/1.

Gewone zitting 2000-2001.

Parlementaire stukken. — Amendement nr. 322/2 — Verslag nr. 322/3 — Tekst aangenomen door de Commissie, voor het Bedrijfsleven, het Wetenschapsbeleid, het Onderwijs, de Nationale Wetenschappelijke en Culturele Instellingen, de Middenstand en de Landbouw nr. 322/4 — Tekst aangenomen in plenaire vergadering en overgezonden aan de Senaat nr. 322/5 — Ontwerp geamendeerd door de Senaat nr. 322/6 — Verslag nr. 322/7 — Tekst aangenomen in plenaire vergadering en aan de Koning ter bekrachtiging voorgelegd nr. 322/8.

Handelingen van de Kamer van Volksvertegenwoordigers — Integraal verslag : 15 februari 2001 — Aanneming : 14 juni 2001.

Senaat :

Gewone zitting 2000-2001.

Stukken van de Senaat — Ontwerp overgezonden door de Kamer van Volksvertegenwoordigers nr. 2-662/1 — Amendementen nrs. 2-662/2 en 3 — Verslag nr. 2-662/4 — Tekst geamendeerd door de commissie nr. 2-662/5 — Amendementen nr. 2-662/6 — Tekst aangenomen in plenaire vergadering en teruggezonden naar de Kamer van Volksvertegenwoordigers nr. 2-662/7.

Handelingen van de Senaat — 17 mei 2001.

Formaliteiten voorgeschreven door de Richtlijn 98/34/EC

De formaliteiten voorgeschreven door de Richtlijn 98/34/EC van 22 juni 1998 van het Europees Parlement en de Raad betreffende een informatie-procedure op het gebied van normen en technische voorschriften en regels betreffende de diensten van de informatiemaatschappij worden vervuld (kennisgeving 2000/0050/B).

BIJLAGE I

Eisen betreffende gekwalificeerde certificaten

Elk gekwalificeerd certificaat dient het volgende te bevatten :

a) de vermelding waaruit blijkt dat het certificaat als gekwalificeerd certificaat wordt afgegeven;

b) de identificatie van de certificatiedienstverlener en het land waar hij gevestigd is;

c) de naam van de ondertekenaar of een pseudoniem dat als dusdanig is geïdentificeerd;

d) de mogelijkheid om, in voorkomend geval, een specifiek attribuut van de ondertekenaar te vermelden, rekening houdend met het gebruik waarvoor het certificaat bestemd is;

e) gegevens voor het verifiëren van de handtekening die overeenstemmen met de gegevens voor het aanmaken van de handtekening onder controle van de ondertekenaar;

f) de vermelding van het begin en het einde van de geldigheidsduur van het certificaat;

g) de identiteitscode van het certificaat;

h) de geavanceerde elektronische handtekening van de certificatiedienstverlener die het certificaat afgeeft;

i) in voorkomend geval de beperkingen op het gebruik van het certificaat, en

j) in voorkomend geval de grenzen met betrekking tot de waarde van de transacties waarvoor het certificaat kan worden gebruikt.

ANNEXE II

Exigences concernant les prestataires de service de certification délivrant des certificats qualifiés

Les prestataires de service de certification doivent :

a) faire la preuve qu'ils sont suffisamment fiables pour fournir des services de certification;

b) assurer le fonctionnement d'un service d'annuaire rapide et sûr et d'un service de révocation sûr et immédiat;

c) veiller à ce que la date et l'heure d'émission et de révocation d'un certificat puissent être déterminées avec précision;

d) vérifier, par des moyens appropriés et conformes au droit national, l'identité et, le cas échéant, les qualités spécifiques de la personne à laquelle un certificat qualifié est délivré;

e) employer 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;

f) utiliser des systèmes et des produits fiables qui sont protégés contre les modifications et qui assurent la sécurité technique et cryptographique des fonctions qu'ils assument;

g) prendre des mesures contre la contrefaçon des certificats et, dans les cas où le prestataire de service de certification génère des données afférentes à la création de signature, garantir la confidentialité au cours du processus de génération de ces données;

h) disposer 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;

i) enregistrer toutes les informations pertinentes concernant un certificat qualifié pendant le délai utile de 30 ans, en particulier pour pouvoir fournir une preuve de la certification en justice.

Ces enregistrements peuvent être effectués par des moyens électroniques;

j) ne pas stocker ni copier les données afférentes à la création de signature de la personne à laquelle le prestataire de service de certification a fourni des services de gestion de clés;

k) avant d'établir une relation contractuelle avec une personne demandant un certificat à l'appui de sa signature électronique, informer cette personne par un moyen de communication durable des modalités et conditions précises d'utilisation des certificats, y compris des limites imposées à leur utilisation, de l'existence d'un régime volontaire d'accréditation et des procédures de réclamation et de règlement des litiges. Cette information, qui peut être transmise par voie électronique, doit être faite par écrit et dans une langue aisément compréhensible. Des éléments pertinents de cette information doivent également être mis à la disposition, sur demande, de tiers qui se prévalent du certificat;

l) utiliser des systèmes fiables pour stocker les certificats sous une forme vérifiable de sorte que :

a) seules les personnes autorisées puissent introduire et modifier des données,

b) l'information puisse être contrôlée quant à son authenticité,

c) les certificats ne soient disponibles au public pour des recherches que dans les cas où le titulaire du certificat a donné son consentement et

d) toute modification technique mettant en péril ces exigences de sécurité soit apparente pour l'opérateur.

ANNEXE III

Exigences pour les dispositifs sécurisés de création de signature électronique

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

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

BIJLAGE II

Eisen betreffende certificatiedienstverleners die gekwalificeerde certificaten afgeven.

De certificatiedienstverleners dienen :

a) het bewijs te leveren dat ze voldoende betrouwbaar zijn om certificatiediensten te leveren;

b) te zorgen voor de werking van een snelle en veilige directorydienst en van een veilige en prompte herroepingsdienst;

c) erop toe te zien dat de datum en het uur van uitgifte en herroeping van een certificaat nauwkeurig kunnen worden bepaald;

d) aan de hand van passende en met het nationaal recht in overeenstemming zijnde middelen de identiteit en, in voorkomend geval, de specifieke attributen te controleren van de persoon aan wie een gekwalificeerd certificaat wordt afgegeven;

e) personeel tewerk te stellen met specifieke kennis, ervaring en kwalificaties noodzakelijk voor het verlenen van de diensten en, in het bijzonder, met beheersbekwaamheid, gespecialiseerde kennis inzake technologie van elektronische handtekeningen en een goede praktische kennis van de passende beveiligingsmethoden; ze dienen tevens administratieve en beheerprocedures en -methoden toe te passen, die aangepast zijn aan en overeenstemmen met de erkende normen;

f) betrouwbare systemen en producten te gebruiken, die beschermd zijn tegen de wijzigingen en die de technische en cryptografische veiligheid garanderen van de processen die ze ondersteunen;

g) maatregelen te treffen tegen het vervalsen van certificaten en wanneer de certificatiedienstverlener gegevens genereert in verband met het aanmaken van de handtekening, de vertrouwelijkheid van dat proces te garanderen;

h) over voldoende financiële middelen te beschikken om te functioneren overeenkomstig de vereisten van deze wet en vooral om de aansprakelijkheid te nemen voor schade, door bijvoorbeeld een passende verzekering te sluiten;

i) alle relevante informatie over een gekwalificeerd certificaat te registreren gedurende de nuttige termijn van dertig jaar, in het bijzonder om een certificatiebewijs te kunnen voorleggen bij gerechtelijke procedures.

Die registraties mogen elektronisch gebeuren;

j) de gegevens voor het aanmaken van de handtekening van de persoon waaraan de certificatiedienstverlener sleutelbeheersdiensten heeft verleend, noch op te slaan noch te kopiëren;

k) vooraleer een contractuele verbintenis tot stand te brengen met een persoon die om een certificaat verzoekt ter ondersteuning van zijn elektronische handtekening, die persoon via een duurzaam communicatiemiddel op de hoogte te brengen van de exacte gebruiksmodaliteiten en -voorwaarden van de certificaten, met inbegrip van de opgelegde beperkingen voor het gebruik ervan, van het bestaan van een vrijwillig accreditatiestelsel en van de procedures qua klachten en regeling van de geschillen. Deze informatie, die elektronisch kan worden doorgegeven, dient schriftelijk en in gemakkelijk te begrijpen woorden geformuleerd te zijn. Relevante elementen van die informatie dienen tevens, op verzoek, ter beschikking te worden gesteld van derden die zich beroepen op het certificaat;

l) betrouwbare systemen te gebruiken om de certificaten in controleerbare vorm op te slaan zodat :

a) enkel daartoe gemachtigde personen gegevens kunnen invoeren en wijzigen;

b) de authenticiteit van de informatie kan worden gecontroleerd;

c) de certificaten enkel publiekelijk beschikbaar zijn in de gevallen waarin de certificaathouder zijn toestemming heeft verleend en

d) elke technische wijziging waarbij die veiligheidsvereisten in het gedrang komen, duidelijk is voor de gebruiker.

BIJLAGE III

Eisen betreffende de veilige middelen voor het aanmaken van een elektronische handtekening

1. De veilige middelen voor het aanmaken van een handtekening dienen ten minste, via passende technische middelen en procedures, te garanderen dat :

a) de gebruikte gegevens voor het aanmaken van een handtekening in de praktijk slechts éénmaal kunnen voorkomen en de vertrouwelijkheid ervan op redelijke wijze verzekerd is;

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

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

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

ANNEXE IV

Recommandations pour la vérification sécurisée de la signature

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

a) les données utilisées pour vérifier la signature correspondent aux données affichées à l'intention du vérificateur;

b) la signature soit vérifiée de manière sûre et que le résultat de cette vérification soit correctement affiché;

c) le vérificateur puisse, si nécessaire, déterminer de manière sûre le contenu des données signées;

d) l'authenticité et la validité du certificat requis lors de la vérification de la signature soient vérifiées de manière sûre;

e) le résultat de la vérification ainsi que l'identité du signataire soient correctement affichés;

f) l'utilisation d'un pseudonyme soit clairement indiquée et

g) tout changement ayant une influence sur la sécurité puisse être détecté.

b) men redelijke zekerheid heeft dat de gebruikte gegevens voor het aanmaken van de handtekening niet door deductie kunnen worden achterhaald en dat de handtekening met de momenteel beschikbare technische middelen beschermd is tegen vervalsing;

c) de voor het aanmaken van de handtekening gebruikte gegevens door de legitieme ondertekenaar op betrouwbare wijze kunnen worden beschermd tegen het gebruik door anderen.

2. De veilige middelen voor het aanmaken van een handtekening mogen noch de te ondertekenen gegevens wijzigen noch verhinderen dat die gegevens vóór het ondertekeningsproces aan de ondertekenaar worden voorgelegd.

BIJLAGE IV

Aanbevelingen voor het veilig verifiëren van de handtekening

Tijdens het verifiëren van de handtekening dient, met een voldoende zekerheid gewaarborgd dat :

a) de gebruikte gegevens voor het verifiëren van de handtekening overeenstemmen met de gegevens die de verifieerder te zien krijgt;

b) de handtekening op betrouwbare wijze wordt geverifieerd en het resultaat van die verificatie op de correcte wijze wordt weergegeven;

c) de verifieerder, zo nodig, op betrouwbare wijze de inhoud van de ondertekende gegevens kan vaststellen;

d) de bij de verificatie van de handtekening vereiste authenticiteit en geldigheid van het certificaat op betrouwbare wijze worden gecontroleerd;

e) het resultaat van de verificatie en de identiteit van de ondertekenaar op de correcte wijze worden weergegeven;

f) het gebruik van een pseudoniem duidelijk vermeld wordt; en

g) elke verandering die de veiligheid beïnvloedt, kan worden opgespoord.

F. 2001 — 2700 [C 2001/11401]

20 SEPTEMBRE 2001. — Arrêté royal modifiant l'arrêté royal du 3 mai 1999 relatif à la composition et au fonctionnement du conseil général de la Commission de Régulation de l'Electricité et du Gaz

ALBERT II, Roi des Belges,

A tous, présents et à venir, Salut.

Vu la loi du 12 avril 1965 relative au transport de produits gazeux et autres par canalisations, notamment l'article 15/15, § 5, inséré par la loi du 29 avril 1999 relative à l'organisation du marché du gaz et au statut fiscal des producteurs d'électricité;

Vu la loi du 29 avril 1999 relative à l'organisation du marché de l'électricité, notamment l'article 24, § 3, alinéa 1er, modifié par la loi du 16 juillet 2001;

Vu l'arrêté royal du 3 mai 1999 relatif à la composition et au fonctionnement du conseil général de la Commission de Régulation de l'Electricité et du Gaz, notamment l'article 2, modifié par l'arrêté royal du 6 octobre 2000;

Vu l'avis de l'Inspecteur des Finances donné le 18 juillet 2001;

Vu la concertation avec les Gouvernements de Région;

Vu les lois sur le Conseil d'Etat, coordonnées le 12 janvier 1973, notamment l'article 3, § 1er, remplacé par la loi du 4 juillet 1989 et modifié par la loi du 4 août 1996;

Vu l'urgence;

Considérant que l'urgence est motivée par le fait que les lois du 29 avril 1999 relatives à l'organisation des marchés de l'électricité et du gaz visent à transposer en droit belge les dispositions des directives 96/92/CE et 98/30/CE du Parlement européen et du Conseil du 19 décembre 1996 et du 22 juin 1998 concernant des règles communes pour les marchés intérieurs de l'électricité et du gaz naturel; que la mise en place de la Commission de Régulation de l'Electricité et du Gaz est une étape indispensable à la mise en œuvre des dispositions des lois du 29 avril 1999 précitées; que le conseil général est l'un des deux organes de cette Commission;

Considérant qu'il convient d'adapter la composition du conseil général en vue d'y assurer la représentation des associations environnementales, comme le prévoit la loi du 16 juillet 2001 portant modification de la loi du 29 avril 1999 relative à l'organisation du marché de l'électricité; que le présent arrêté doit dès lors être pris dans les délais les plus brefs;

N. 2001 — 2700 [C 2001/11401]

20 SEPTEMBER 2001. — Koninklijk besluit tot wijziging van het koninklijk besluit van 3 mei 1999 betreffende de samenstelling en de werking van de algemene raad van de Commissie voor de Regulering van de Elektriciteit en het Gas

ALBERT II, Koning der Belgen,

Aan allen die nu zijn en hierna wezen zullen, Onze Groet.

Gelet op de wet van 12 april 1965 betreffende het vervoer van gasachtige producten en andere door middel van leidingen, inzonderheid op artikel 15/15, § 5, ingevoegd door de wet van 29 april 1999 betreffende de organisatie van de gasmarkt en het fiscaal statuut van de elektriciteitsproducenten;

Gelet op de wet van 29 april 1999 betreffende de organisatie van de elektriciteitsmarkt, inzonderheid op artikel 24, § 3, eerste lid, gewijzigd bij de wet van 16 juli 2001;

Gelet op het koninklijk besluit van 3 mei 1999 betreffende de samenstelling en de werking van de algemene raad van de Commissie voor de Regulering van de Elektriciteit en het Gas, inzonderheid op artikel 2, gewijzigd bij het koninklijk besluit van 6 oktober 2000;

Gelet op het advies van de Inspecteur van Financiën, gegeven op 18 juli 2001;

Gelet op het overleg met de Gewestregeringen;

Gelet op de wetten op de Raad van State, gecoördineerd op 12 januari 1973, inzonderheid op artikel 3, § 1, vervangen bij de wet van 4 juli 1989 en gewijzigd bij de wet van 4 augustus 1996;

Gelet op de dringende noodzakelijkheid;

Overwegende dat de dringende noodzakelijkheid gemotiveerd wordt door de omstandigheid dat voornoemde wetten van 29 april 1999 de omzetting in Belgisch recht beogen van de bepalingen van richtlijnen 96/92/EG en 98/30/EG van het Europees Parlement en van de Raad van 19 december 1996 en van 22 juni 1998 betreffende gemeenschappelijke regels voor de interne markten voor elektriciteit en dat de oprichting van de Commissie voor de Regulering van de Elektriciteit en het Gas een onmisbare schakel is voor de inwerkingstelling van de bepalingen van voornoemde wetten van 29 april 1999; dat de algemene raad één van de twee organen is van deze Commissie;

Overwegende dat het passend is de samenstelling van de algemene raad aan te passen met het oog op de vertegenwoordiging erin van de milieuverenigingen, zoals voorzien in de wet van 16 juli 2001 houdende wijziging van de wet van 29 april 1999 betreffende de organisatie van de elektriciteitsmarkt; dat dit besluit derhalve zo spoedig mogelijk moet genomen worden;

Bijlage 4: Vragenlijst online indienen vennootschapsbelasting

1. Kunt u in het kort even de vennootschapsbelasting voor bedrijven toelichten?

2. Wat is de situatie In België met betrekking tot de vennootschapsbelasting?

3. Sinds kort is er de mogelijkheid om met behulp van VenSoc de aangifte van de vennootschapsbelasting on line in te dienen. Hoe gaat dit in zijn werk?

4. Is de toevoeging van de elektronische identiteitskaart als authentificatiemiddel bij het indienen van de VenSoc aangifte een goede of slechte toevoeging van de mogelijkheden? Waarom?

5. Wat zijn de voordelen van het elektronisch indienen van de VenSoc aangifte? Zowel voor de FOD als voor de bedrijven zelf?

6. Vindt u het elektronisch indienen van de aangifte een verbetering ten opzichte van de vroegere papieren aangifte? Waarom?

7. De vennootschapsbelasting in België is eerder hoog ten opzichte van andere landen. Wat zijn de gevolgen hiervan op economisch vlak?

Auteursrechterlijke overeenkomst

Opdat de Universiteit Hasselt uw eindverhandeling wereldwijd kan reproduceren, vertalen en distribueren is uw akkoord voor deze overeenkomst noodzakelijk. Gelieve de tijd te nemen om deze overeenkomst door te nemen, de gevraagde informatie in te vullen (en de overeenkomst te ondertekenen en af te geven).

Ik/wij verlenen het wereldwijde auteursrecht voor de ingediende eindverhandeling:
De invloed van de digitale handtekening op de elektronische aangifte van de vennootschapsbelasting
Richting: **Handelsingenieur** Jaar: **2007**
in alle mogelijke mediaformaten, - bestaande en in de toekomst te ontwikkelen - , aan de Universiteit Hasselt.

Niet tegenstaand deze toekenning van het auteursrecht aan de Universiteit Hasselt behoud ik als auteur het recht om de eindverhandeling, - in zijn geheel of gedeeltelijk -, vrij te reproduceren, (her)publiceren of distribueren zonder de toelating te moeten verkrijgen van de Universiteit Hasselt.

Ik bevestig dat de eindverhandeling mijn origineel werk is, en dat ik het recht heb om de rechten te verlenen die in deze overeenkomst worden beschreven. Ik verklaar tevens dat de eindverhandeling, naar mijn weten, het auteursrecht van anderen niet overtreedt.

Ik verklaar tevens dat ik voor het materiaal in de eindverhandeling dat beschermd wordt door het auteursrecht, de nodige toelatingen heb verkregen zodat ik deze ook aan de Universiteit Hasselt kan overdragen en dat dit duidelijk in de tekst en inhoud van de eindverhandeling werd genotificeerd.

Universiteit Hasselt zal mij als auteur(s) van de eindverhandeling identificeren en zal geen wijzigingen aanbrengen aan de eindverhandeling, uitgezonderd deze toegelaten door deze overeenkomst.

Ik ga akkoord,

Bram LAMBRICHTS

Datum: **04.06.2007**