No trade without trust

Mw. mr. drs. M.J. Dontje

Vertrouwen in een digitale omgeving, meer in het bijzonder vertrouwen bij e-commerce, staat centraal in dit artikel. De nadruk ligt op consumenten-vertrouwen, maar ook business-to-business e-commerce komt aan bod. Er wordt ingegaan op de vraag waar vertrouwen in een digitale omgeving op gebaseerd is en hoe het vertrouwen in elektronische handel kan worden vergroot. Tevens worden (inter)nationale beleids- en wetgevende initiatieven en zelfregulerende en commerciële initiatieven besproken. Hoe belangrijk vertrouwen bij Internet-handel is, blijkt bijvoorbeeld uit het feit dat in een in 1998 verricht onderzoek[1] beveiliging als grootste belemmering voor de toepassing van electronic commerce werd aangewezen ([KMCU98]). Terwijl een ander onderzoek heeft uitgewezen dat ruim tachtig procent van de Internet-gebruikers zich zorgen maakt over zijn privacy en dat ongerustheid over privacy en veiligheid aanleiding is om geen aankopen te doen via het web. Reden genoeg om na te gaan hoe vertrouwen in een elektronische omgeving kan worden vergroot.

1) Het betreft een in 1998 door KPMG Verenigd Koninkrijk verrichte enquête onder ruim 450 vooraanstaande bedrijven.

2) Zie voor een uitgebreide uiteenzetting over het gebruik van digitale certificaten om vertrouwelijkheid, authenticiteit, integriteit en onweerlegbaarheid van berichten-uitwisseling te realiseren de bijdrage van Dontje en Olde Olthof in het Compact Jubileumboek.

Inleiding

Het Internet roept vragen op. Veel van die vragen hebben te maken met vertrouwen en veiligheid. Veiligheid is een middel om vertrouwen te realiseren, maar vertrouwen is meer dan veiligheid alleen. Een voorbeeld ter verduidelijking. Door gebruik te maken van digitale (server) certificaten[2] kan een consument erop vertrouwen dat communicatie met een bepaalde website (en daarmee met een bepaald bedrijf) niet onderschept kan worden en ongewijzigd bij de beoogde ontvanger aankomt. De consument weet dat de communicatie veilig geschiedt, maar als deze er niet op vertrouwt dat het bedrijf achter de website zorgvuldig met de door hem verstrekte gegevens omgaat, zal hij geen gegevens willen verstrekken. Ook als een afnemer geen vertrouwen heeft in de dienstverlening van een leverancier, waar het bijvoorbeeld gaat om de vraag of de leverancier op tijd het juiste product zal kunnen leveren, zal die afnemer niet met die leverancier in zee willen gaan.

Onduidelijkheid en bedreigingen zijn er genoeg op Internet. Met behulp van cookies kan (muis)klik- of surfgedrag worden gevolgd, om toegang tot bepaalde sites te krijgen moet vaak allerlei persoonlijke informatie worden verstrekt, bij het kopen van een cd van een onbekende aanbieder op het net blijft onduidelijk of de verkoper bonafide is en bij een koop over de landsgrenzen heen is meestal niet duidelijk welk recht van toepassing is op de gesloten overeenkomst, laat staan welke bescherming dat recht de consument biedt. Al deze zaken maken dat veel Internet-gebruikers zich wel twee keer achter de oren krabben voordat ze persoonsgegevens verstrekken of een handelstransactie aangaan. Om het vertrouwen te vergroten, en aldus business-to-consumer e-commerce een impuls te geven, wordt vanuit verschillende invalshoeken en door verschillende instanties actie ondernomen.

Vertrouwen in elektronisch zakendoen kan onder meer ontstaan door het verschaffen van een duidelijk juridisch kader. Verschillende relevante actuele (internationale en nationale) beleids- en wetgevingsinitiatieven worden kort toegelicht. Naast (supranationale) overheidsinitiatieven zijn echter ook zelfregulerende en commerciële initiatieven van belang. Indien regels (mede) door partijen zelf zijn opgesteld, is de betrokkenheid – en daarmee de bereidheid tot naleving – groter dan bij regels die 'van boven af' zijn opgelegd. Naast gedragscodes op brancheniveau kan bij zelfregulering bijvoorbeeld ook worden gedacht aan het opstellen van een privacy statement door een individuele organisatie. Een commercieel initiatief dat het vertrouwen – en daarmee de bereidheid om online te winkelen – vergroot zijn privacy- en webseals, een soort elektronische stempels van goedkeuring vergelijkbaar met bijvoorbeeld het Kema-keur in de fysieke wereld. Daarom worden ook deze initiatieven behandeld. Aan de hand van de resultaten van een onderzoek naar vertrouwen in e-commerce wordt toegelicht welke factoren bepalend zijn voor het vertrouwen dat Internet-gebruikers in websites stellen. Allereerst wordt echter aan de hand van de resultaten van een onderzoek van Consumers International uiteengezet wat allemaal mis kan gaan bij het online aanschaffen van producten en diensten. De belangrijkste uitkomsten en aanbevelingen uit het onderzoek worden besproken.

Onderzoek consumentenorganisaties

Dat de schroom van veel consumenten online aankopen te doen niet onterecht is, blijkt uit de resultaten van het onderzoek 'Consumers@shopping: An international comparative study of electronic commerce' ([Cons99c]) van Consumers International. Consumentenorganisaties uit elf landen wereldwijd kochten via het Internet 151 producten en diensten in zeventien landen. Een aantal zaken die in een fysieke omgeving als vanzelfsprekend worden ervaren en goed geregeld zijn, bleken dit in een digitale omgeving niet te zijn.

Eén op de tien online bestelde producten kwam nooit aan en in maar liefst 25 procent van de gevallen bestond geen duidelijkheid over de totaalprijs (inclusief handling/shipping en eventueel verschuldigde BTW) van aangeschafte goederen. Ook was de identiteit van de aanbieder niet altijd duidelijk (de naam van de website hoeft niet overeen te stemmen met het bedrijf achter de site) en

ontbraken in veel gevallen gegevens (adres, telefoonnummer, e-mailadres) om met de aanbieder contact op te kunnen nemen.

Voorts viel in veel gevallen nogal wat aan te merken op het bestelproces. Vaak ontbrak een uitleg en in 36 procent van de gevallen werd geen bevestiging van de bestelling verstuurd. Op de overeenkomst toepasselijke voorwaarden, bijvoorbeeld betreffende betaling, bezorging, garantie en afkoelmogelijkheid, ontbraken in veertig procent van de gevallen en in bijna eenderde (29 procent) van de gevallen vonden de onderzoekers de voorwaarden pas na actief de website te hebben afgezocht. Ten slotte beschikte slechts 21 procent van de onderzochte websites over een vastgelegd privacybeleid met informatie over de wijze van omgang met de persoonlijke gegevens van de consument en werd slechts in één op de tien gevallen informatie verstrekt over het op de overeenkomst toepasselijke recht.

In het onderzoek van Consumers International waren geen Nederlandse sites betrokken; onderzoek van de Nederlandse Consumentenbond onder 150 Nederlandse websites bevestigt echter het hiervoor geschetste beeld. Zo blijken ook door Nederlandse webwinkels verkochte producten bijvoorbeeld niet of veel te laat aan te komen en ontbreekt in de meeste gevallen een klachtenregeling ([Cons99a]).

Consumers International heeft de volgende aspecten geïnventariseerd waarover verkopers (potentiële) klanten ten minste van informatie dienen te voorzien c.q. welke garanties verkopers ten minste dienen te bieden:

1. identiteit, fysieke adresgegevens, telefoonnummer, e-mailadres van de leverancier, zodat de klant – bijvoorbeeld bij klachten – contact kan opnemen met de leverancier;
2. informatie over de landen waar goederen worden bezorgd en wel voorafgaand aan het bestelproces, zodat wordt voorkomen dat een klant het gehele bestelproces doorloopt om vervolgens tot de conclusie te komen dat niet wordt bezorgd in het land waar hij woonachtig is;
3. prijsinformatie inclusief eventuele bezorgkosten en/of verschuldigde BTW en de mogelijkheid om de prijs in de valuta van het land waar de klant woont om te rekenen;
4. de op de overeenkomst toepasselijke voorwaarden, bijvoorbeeld betreffende mogelijkheid tot annulering en retourneren, betalings- en bezorgtermijnen en geschillenoplossing en wel voordat de klant zijn bestelling heeft geplaatst;
5. het op de overeenkomst toepasselijke recht;
6. toegankelijk en helder bestelproces;
7. het privacybeleid van de leverancier, inclusief informatie over eventueel gebruik van cookies;
8. het veiligheidsbeleid van de leverancier;
9. de mogelijkheid om goederen te retourneren;
10. een heldere klachtenprocedure;
11. informatie over de voortgang van de bestelling: zijn goederen in voorraad, zo niet een indicatie of en zo ja, wanneer de voorraad wordt aangevuld en hoe de klant hierover wordt geïnformeerd, alsmede een bevestiging van de ontvangst van de bestelling;
12. berichtgeving dat een goed is verzonden plus een indicatie van de verwachte bezorgtermijn;
13. geen debitering van het verschuldigde aankoopbedrag voordat de bestelling is afgeleverd.

Het zal duidelijk zijn dat de geschetste tekortkomingen in de voorlichting van consumenten de bereidheid om via Internet aankopen te doen niet ten goede komen. Er zijn verschillende initiatieven (regelgeving, maar ook zelfreguleringsinitiatieven) die voorzien in oplossingen voor de geconstateerde tekortkomingen. Die initiatieven komen verderop aan bod. Allereerst wordt echter ingegaan op de factoren die in de ogen van consumenten bepalend zijn voor het vertrouwen dat zij stellen in online goederen- en dienstenaanbieders.

Consumentenvertrouwen

Door Cheskin Research is een onderzoek, genaamd ‘eCommerce Trust Study’, verricht met als doel het identificeren van de factoren die bepalend zijn voor het vertrouwen dat in e-commerce websites wordt gesteld ([Ches99]). Uit het onderzoek zijn zes aspecten naar voren gekomen die bepalend zijn voor het vertrouwen dat bezoekers in een bepaalde website stellen. Dat zijn: merk (bekendheid met en vertrouwen in), eenvoud van navigatie (de weg vinden op een website), beleid (informatie over verwerking bestelling en voorwaarden als garantie, mogelijkheid tot retourneren, klachtenprocedure), presentatie (ontwerp van een site: heeft de site een professionele en verzorgde uitstraling en ondersteunt het ontwerp de boodschap van de site), moderne technologie (worden pagina’s bijvoorbeeld snel ingeladen) en de aanwezigheid van beeldmerken van bedrijven die veiligheid garanderen (zowel webseals als logo’s van creditcardorganisaties).

Het onderzoek wijst ten aanzien van logo’s uit dat de aanwezige creditcardbeeldmerken wel worden herkend, maar weinig effect hebben op het vertrouwen dat in een website wordt gesteld. Zogenaamde web-based merken als VeriSign of TRUSTe die worden herkend, blijken juist wel een positieve invloed te hebben op het vertrouwen. Hieruit blijkt dat een web-based merknaam, die in de fysieke wereld niet wordt gebruikt, wel degelijk vertrouwen kan uitstralen. Een voorbeeld uit de Nederlandse e-commercepraktijk bevestigt dat de aanwezigheid van logo’s een positief effect heeft op het vertrouwen in een website. De CD Teleshop (www.cdteleshop.nl), een cd-winkel op Internet gericht op de Europese markt, merkte dat na de implementatie van het I-Pay systeem van Interpay het aantal creditcardbetalingen steeg. Navraag bij de klantenkring leerde dat bezoekers van de website door de vermelding van het Interpay/I-Pay logo vertrouwen kregen in de CD Teleshop ([Door99]).

Uit het onderzoek blijkt verder dat bezoekers veel waarde hechten aan het gebruik van technologie, zoals cryptografie, ter beveiliging van communicatie. Vermelding van de toegepaste technologie blijkt zelf meer vertrouwen op te wekken dan de naam van de partij die de betreffende techniek levert.

Dat een merknaam niet noodzakelijkerwijs bekend hoeft te zijn uit de fysieke wereld wil hij vertrouwen opwekken, blijkt uit het feit dat zeven van de twaalf merknamen die door de respondenten als meest vertrouwenwekkend werden aangemerkt, niet afkomstig zijn uit de fysieke wereld maar hun oorsprong hebben op het web. Ten slotte stelt de studie dat veiligheid en privacy de twee aspecten zijn waarin een Internet-aanbieder als eerste moet voorzien in het proces van het opbouwen van vertrouwen bij websitebezoekers. Door deze twee zaken te adresseren, krijgen bezoekers namelijk het gevoel controle te hebben over hun gegevens. Het informeren van bezoekers over security policies (inclusief gebruik van cryptografie) en hen niet meer gegevens te laten verstrekken dan noodzakelijk is, zijn twee manieren om te helpen dit vertrouwen op te bouwen.

Let wel, bovenstaande betreft één onderzoek, het is mogelijk dat andere studies andere uitkomsten opleveren. De zes geïdentificeerde factoren zijn naar mijn mening echter zeker relevant voor het vertrouwen dat een website bij een (potentiële) klant opwekt.

Beleid en regelgeving

Zowel op nationaal als op supranationaal niveau (Europese Unie, Wereld Handelsorganisatie, Verenigde Naties en de Organisatie voor Economische Samenwerking en Ontwikkeling (OESO)) is vertrouwen van burgers in de digitale maatschappij in het algemeen en electronic commerce meer in het bijzonder een belangrijk onderwerp. Electronic commerce bevordert immers de economische groei en het concurrentievermogen.

Beleid en regelgeving internationaal

OESO
De OESO heeft een aantal rapporten geschreven waarin aandacht wordt besteed aan belemmeringen voor e-commerce. Gebrek aan vertrouwen is met technische beperkingen als beperkte toegang tot Internet, te weinig bandbreedte en beperkte mogelijkheden tot elektronisch betalen één van de grootste belemmeringen voor elektronische handel. 'Dismantling the Barriers to Global Electronic Commerce' ([OESO97b]) gaat uit van het principe dat vertrouwen centraal staat in iedere commerciële transactie. De ontwikkeling van commerciële activiteiten in een elektronische omgeving vergt bijvoorbeeld dat transacties veilig zijn en dat belangrijke informatie met betrekking tot een transactie (integriteit van gegevens) en de tegenpartij (zoals identiteit) bekend is. Het gebruik van cryptografie en digitale certificaten om vertrouwelijkheid en integriteit van berichtenuitwisseling te waarborgen en de identiteit van handelspartijen te garanderen, privacybescherming en consumentenbescherming worden genoemd als middelen om dit vertrouwen te vergroten.

'Business-to-Consumer Electronic Commerce, Survey of Status and Issues' ([OESO97a]) behandelt, zo blijkt ook uit de titel, een aantal aspecten die van belang zijn voor elektronische handel tussen bedrijven en consumenten. Het rapport identificeert een aantal vertrouwengerelateerde zaken die geadresseerd dienen te worden als voorwaarde voor het uitvoeren van dergelijke transacties. Dit zijn onder meer zekerheid omtrent de identiteit van de handelspartner en de rechtsgeldigheid van elektronisch afgesloten en ondertekende contracten en andere documenten, privacy, betaling (betalingssystemen en elektronisch geld) en beveiliging van netwerken en informatiesystemen tegen inbraak en fraude.

> Zonder vertrouwen kan e-commerce nimmer zijn volle potentieel bereiken.

UNCITRAL
UNCITRAL (United Nations Commission on International Trade Law), een commissie van de Verenigde Naties die zich met het handelsrecht bezighoudt, heeft een 'Model Law on Electronic Commerce' vastgesteld ([UNCI96]). Deze – niet-bindende – modelwet beoogt nationale wetgevers te voorzien van een set internationaal geaccepteerde (model)regels gericht op het wegnemen van wettelijke belemmeringen en het scheppen van juridische zekerheid voor elektronische handel. De modelwet is gericht op de totstandbrenging van een technologieonafhankelijke juridische infrastructuur, waarbij als uitgangspunt geldt dat het langs elektronische weg verrichten van rechtshandelingen in beginsel niet mag leiden tot oneigenlijke voor- of nadelen ten opzichte van de fysieke wereld. Om deze non-discriminatie te realiseren wordt voor iedere belemmering, bijvoorbeeld het vereiste van schriftelijkheid, bepaald wat het doel en de functie van het betreffende vereiste zijn, waarna doel en functie worden 'vertaald' naar criteria die toepasbaar zijn in een elektronische omgeving. In Nederland is deze zogeheten 'functional equivalence approach' toegepast door de werkgroep 'elektronisch verrichten van rechtshandelingen' (zie hierna de subparagraaf 'Beleid en regelgeving nationaal'). De modelwet is tot dusverre de enige mondiaal totstandgekomen regeling betreffende de juridische aspecten van elektronisch zakendoen. De regeling wordt breed gedragen en is in diverse landen gebruikt bij het opstellen van nationale wetgeving. Bij de totstandkoming van enkele algemene bepalingen omtrent het vermogensrechtelijke rechtsverkeer in het Burgerlijk Wetboek zal de modelwet ook als inspiratiebron worden gebruikt (zie hierna de subparagraaf 'Beleid en regelgeving nationaal'). Voorts werkt UNCITRAL aan mondiale regels voor elektronische handtekeningen en certificerende instellingen. Dit heeft geresulteerd in Draft Uniform Rules on Electronic Signatures ([UNCI98]).

Europese Unie
Het beleid van de Europese Unie ten aanzien van Internet legt de nadruk op zelfregulering en voorziet slechts in minimumregels, zodat aan de ene kant wordt voorzien in noodzakelijke waarborgen ter stimulering van elektronische handel en aan de andere kant marktpartijen voldoende ruimte wordt gelaten en de interne markt niet wordt verstoord. Een tweetal ontwerprichtlijnen die (onder meer) tot doel hebben elektronische handel te stimuleren en te faciliteren worden hier besproken. Dit zijn de ontwerprichtlijn inzake elektronische handtekeningen

([EuCO99b])[3] en de ontwerprichtlijn betreffende juridische aspecten van elektronische handel ([EuCO99a]).[4]

Richtlijn betreffende bepaalde juridische aspecten van elektronische handel
Eind 1998 heeft de Europese Commissie een voorstel voor een richtlijn inzake enkele juridische aspecten van het elektronisch zakendoen aangenomen en aangeboden aan de Raad van de Europese Unie ([EuCO98a]). Dit voorstel heeft na amendementen van het Europees Parlement geresulteerd in een gewijzigd voorstel ([EuCO99a]). Een gemeenschappelijk standpunt van het Europees Parlement en de Raad wordt voor het einde van dit jaar verwacht. Eén van de vier onderkende redenen om een wettelijke regeling te ontwikkelen betreft het gebrek aan vertrouwen bij afnemers. Een onduidelijke en verwarrende omgeving met weinig garanties voor een goede bescherming kan afnemers ertoe doen besluiten af te zien van het aangaan van online-contracten. Met de richtlijn wil de Commissie voorzien in een geharmoniseerd juridisch kader van minimumnormen op terreinen waar rechtsonzekerheid bestaat voor elektronische handel. De ontwerprichtlijn heeft uitsluitend betrekking op de elektronische transactie zelf en dus niet op de levering van producten of diensten, tenzij aflevering daarvan elektronisch plaatsvindt (overweging 6). De conceptrichtlijn behandelt een aantal uiteenlopende onderwerpen. De onderwerpen die het vertrouwen van afnemers in elektronisch zakendoen beïnvloeden worden hier behandeld.

Country of origin-principe
Een belangrijk artikel van de richtlijn is artikel 3 dat bepaalt dat in beginsel het zogenaamde *country of origin*-principe van toepassing is op elektronische handel: leveranciers dienen in principe de nationale bepalingen van het land waar zij zijn gevestigd[5] na te leven. Een belangrijke uitzondering (genoemd in bijlage II) heeft betrekking op contractuele verplichtingen betreffende met consumenten gesloten contracten. In de contractuele fase van business-to-consumer transacties geldt derhalve het recht van de consument. Op business-to-business transacties is op grond van de richtlijn zowel in de precontractuele als de contractuele fase het recht van de leverancier van toepassing.

Vestigings- en informatieregeling
Artikel 5 van de conceptrichtlijn bepaalt dat dienstverleners aan afnemers (en bevoegde autoriteiten) ten minste de volgende informatie moeten verschaffen: naam, vestigingsadres, e-mailadres, gegevens over (eventuele) inschrijving in handelsregister (inclusief inschrijvingsnummer), informatie over eventueel toepasselijke vergunningen, voor gereglementeerde beroepen informatie over de orde/instelling waar de dienstverlener bij is aangesloten alsmede toepasselijke beroepsregels, indien toepasselijk BTW-nummer, een nauwkeurige en ondubbelzinnige prijsaanduiding inclusief aanduiding van alle aanvullende kosten en informatie over belangrijke voorwaarden en condities. Aldus wordt ten dele invulling gegeven aan de door Consumers International geformuleerde vereisten opgesomd in de paragraaf 'Onderzoek consumentenorganisaties' ten aanzien van informatieverschaffing aan afnemers.

De ontwerprichtlijn heeft uitsluitend betrekking op de elektronische transactie zelf.

Commerciële communicatie
Voorts bevat de richtlijn een aantal aanwijzingen ten aanzien van elektronische reclame. Artikel 6 bepaalt dat reclame duidelijk als zodanig herkenbaar dient te zijn, dat de verantwoordelijke (rechts)persoon duidelijk te identificeren moet zijn en dat eventuele verkoopbevorderende aanbiedingen (kortingen, geschenken) of wedstrijden als zodanig herkenbaar moeten zijn en de op de aanbieding/wedstrijd toepasselijke voorwaarden eenvoudig te vervullen moeten zijn en nauwkeurig en ondubbelzinnig moeten worden weergegeven. Ook ongevraagde reclame via e-mail dient bij ontvangst door de ontvanger duidelijk als zodanig herkenbaar te zijn (art. 7(a)). Dit kan door een aanduiding op te nemen in de header van een bericht. Bovendien verplicht de richtlijn aanbieders van dergelijke reclameboodschappen ontvangers de mogelijkheid te bieden in een centraal register aan te geven dat zij die berichten niet willen ontvangen. Een regeling die vergelijkbaar is met het gebruik van de 'nee-nee sticker' om in de fysieke wereld ongeadresseerd reclamedrukwerk en huis-aan-huisbladen te weren.

Contracten langs elektronische weg
Ten slotte is de voorgestelde regeling voor het langs elektronische weg totstandkomen van overeenkomsten van belang. Allereerst verplicht de richtlijn lidstaten hun wetgeving (behoudens enkele uitzonderingen) waar nodig aan te passen zodat het sluiten van contracten langs elektronische weg mogelijk wordt gemaakt (art. 9). Ten tweede legt artikel 10 leveranciers de verplichting op om afnemers te informeren over de verschillende stappen van de totstandkoming van de overeenkomst en wel voordat een (elektronische) overeenkomst totstandkomt. Ten slotte voorziet de conceptrichtlijn in een regeling betreffende het tijdstip van de totstandkoming van de overeenkomst (art. 11). Als tijdstip van het sluiten van een contract geldt het moment waarop de afnemer van een dienst van de dienstverlener langs elektronische weg het bewijs van ontvangst van de akkoordverklaring (met de overeenkomst) van de afnemer heeft ontvangen.

Richtlijn inzake elektronische handtekeningen
De richtlijn inzake elektronische handtekeningen[6] heeft tot doel het gebruik van elektronische handtekeningen en daarmee ook het elektronische rechtsverkeer te stimuleren en beoogt bij te dragen aan een geharmoniseerd wettelijk kader binnen de EU door te waarborgen dat elektronische handtekeningen wettelijk erkend worden. Wettelijke erkenning betekent dat elektronische handtekeningen die zijn gebaseerd op een zogeheten gekwalifi-

3) Gewijzigd voorstel (n.a.v. amendementen van het Europees Parlement) voor een richtlijn van het Europees Parlement en de Raad betreffende een gemeenschappelijk kader voor elektronische handtekeningen, 29 april 1999, COM(1999) 195 def., 98/0191 (COD).

4) Gewijzigd voorstel (n.a.v. amendementen van het Europees Parlement) voor een richtlijn van het Europees Parlement en de Raad betreffende bepaalde juridische aspecten van de elektronische handel in de interne markt, COM(99) 427 def., 98/0325 (COD).

5) De richtlijn is uiteraard alleen van toepassing op dienstverleners gevestigd in één van de lidstaten van de EU. Indien een dienstverlener meerdere vestigingen heeft, is de lidstaat waar de dienstverlener het centrum van zijn activiteiten heeft, maatgevend (overweging 9).

6) Hoewel digitale handtekeningen gecreëerd met behulp van cryptografische technieken momenteel worden beschouwd als de belangrijkste soort elektronische handtekeningen is het toepassingsgebied van de conceptrichtlijn, in tegenstelling tot voorgaande versies van de richtlijn, niet beperkt tot digitale handtekeningen maar omvat deze alle soorten elektronische handtekeningen. De in de subparagraaf 'Beleid en regelgeving nationaal' toegelichte toepassing van cryptografie ten behoeve van vertrouwelijkheidsdoeleinden valt nadrukkelijk buiten de reikwijdte van de richtlijn.

ceerd certificaat[7] dat door een aan de in bijlage II genoemde eisen beantwoordende certificatiedienstverlener[8] is afgegeven, ten eerste worden erkend als beantwoordend aan de wettelijke eisen van een met de hand geschreven handtekening en ten tweede in gerechtelijke procedures op dezelfde wijze als handgeschreven handtekeningen als bewijsmiddel moeten worden toegelaten. Om vertrouwen te scheppen bij degenen (consumenten en bedrijven) die op de certificaten moeten vertrouwen, bevat het voorstel aansprakelijkheidsvoorschriften voor certificatiedienstverleners. Het gaat in het bijzonder om aansprakelijkheid voor de geldigheid van (de gegevens opgenomen in) het certificaat. Om bij te dragen aan de wereldwijde erkenning van certificaten voorziet de richtlijn in wettelijke erkenning, onder bepaalde voorwaarden, van certificaten uitgegeven door certificatiedienstverleners uit landen buiten de Unie. De richtlijn heeft geen betrekking op rechtshandelingen waarvoor in het nationale recht van de lidstaten vormvereisten gelden, zoals bijvoorbeeld een notariële akte.[9]

De richtlijn ziet alleen op certificaten uitgegeven aan het publiek en uitdrukkelijk niet op het gebruik van elektronische handtekeningen die uitsluitend in gesloten systemen worden gebruikt; op dat punt zijn partijen vrij om onderling voorwaarden overeen te komen voor het aanvaarden van elektronisch ondertekende gegevens in de mate waarin dat door het nationale recht is toegestaan. Indien elektronische handtekeningen die gebruikt worden binnen gesloten gebruikersgroepen echter aan de eisen van de richtlijn voldoen, dan zijn ook die handtekeningen wettelijk erkend.

De richtlijn is gebaseerd op een tweeledig concept: certificatiedienstverleners zijn in het algemeen vrij om hun diensten zonder voorafgaande toestemming aan te bieden. Parallel hieraan mogen de lidstaten vrijwillige accreditatieregelingen invoeren, gebaseerd op gemeenschappelijke vereisten en gericht op een hoger niveau van veiligheid. Dat een elektronische handtekening niet is gecreëerd door middel van een certificaat dat uitgegeven is door een geaccrediteerde dienstverlener betekent echter niet dat de handtekening automatisch rechtsgevolg en rechtsgeldigheid ontbeert (artikel 5 lid 2 gewijzigd conceptvoorstel). Certificaten uitgegeven door geaccrediteerde certificatiedienstverleners worden automatisch geacht rechtsgevolg te hebben en rechtsgeldig te zijn. In Nederland wordt reeds onderzoek verricht naar een dergelijk accreditatie- en certificatieschema. Zulks naar aanleiding van de uitkomsten van het 'nationaal TTP-project' (zie hierover de betreffende subparagraaf).

Wat betreft de status van conceptrichtlijn het volgende. Er heeft inmiddels een tweede lezing door het Europees Parlement plaatsgevonden waarbij een paar amendementen van de Europese Commissie zijn goedgekeurd. De aangepaste conceptrichtlijn moet nu nog worden goedgekeurd door de Raad. De richtlijn zal waarschijnlijk voor het einde van het jaar van kracht worden. Dan moeten de lidstaten de richtlijn omzetten in nationale regelgeving.

Beleid en regelgeving nationaal

Het uitgangspunt van de Nederlandse regering is dat in de elektronische omgeving dezelfde bescherming en rechtszekerheid moeten gelden als in de traditionele fysieke omgeving. Het langs elektronische weg verrichten van rechtshandelingen mag in beginsel geen oneigenlijke voor- of nadelen opleveren ten opzichte van het gebruik van de traditionele mondelinge of schriftelijke weg. Nederland sluit hiermee aan bij het beginsel dat ten grondslag ligt aan de besproken modelwet voor electronic commerce. Waar aanpassingen in de nationale wetgeving noodzakelijk zijn om dit uitgangspunt te realiseren, wordt actie ondernomen. Dit uitgangspunt vormt de kern van een belangrijk nationaal beleidsdocument, de nota 'Wetgeving voor de elektronische snelweg' van het Ministerie van Justitie ([MJus98b]). Deze nota inventariseert alle voor de elektronische snelweg relevante rechtsgebieden en behandelt voorstellen voor aanpassingen van wetgeving, alsmede initiatieven tot zelfregulering en inbreng vanuit Nederland in internationale overlegfora. Ten aanzien van het privaatrecht onderkent de nota dat zich met name waar het de vaststelling van de juistheid en daarmee de betrouwbaarheid van elektronische uitingen betreft problemen voor kunnen doen, omdat dergelijke uitingen onderschept en gewijzigd kunnen worden als hiertegen geen afdoende maatregelen (bijvoorbeeld toepassing van cryptografische technieken) worden getroffen. Voorts onderkent de regering dat de onbekendheid met de identiteit van de wederpartij waarvan in een elektronische omgeving vaak sprake is, tot belangrijke problemen kan leiden. Ten slotte kunnen specifieke vormvoorschriften als de eis van schriftelijkheid of origineel een belemmering vormen voor het elektronische rechtsverkeer ([MJus98b]).

> In de elektronische omgeving moeten dezelfde bescherming en rechtszekerheid gelden als in de traditionele fysieke omgeving.

De regering heeft een tweetal projecten geïnitieerd die verband houden met het hiervoor omschreven gebrek aan vertrouwen in een elektronische omgeving en bij het elektronisch zakendoen. Deze twee projecten, te weten het 'nationaal TTP-project' en het project 'elektronisch verrichten van rechtshandelingen', worden hierna toegelicht.

Nationaal TTP-project

Het 'nationaal TTP-project', dat heeft geresulteerd in de notitie 'Nationaal TTP-project' ([MEZ98b], [MEZ99a]), had tot doel de randvoorwaarden voor het aanbieden van Trusted Third Party-diensten te inventariseren. Trusted Third Parties (TTP's) zijn vertrouwde derde partijen die diensten aanbieden om elektronische berichtenuitwisseling betrouwbaar te maken. Betrouwbaarheid omvat dan vertrouwelijkheid (berichten worden geëncrypt verzonden), integriteit (geen gegevens toegevoegd, weggehaald of gewijzigd), authenticiteit (bericht is afkomstig van degene die zegt het te hebben verzonden) en onweerlegbaarheid (verzender kan niet ontkennen een

7) Artikel 2 lid 5 van de gewijzigde conceptrichtlijn omschrijft een gekwalificeerd certificaat als 'een elektronische verklaring die een middel voor handtekeningverifiëring met een bepaalde persoon verbindt, diens identiteit bevestigt en aan de in bijlage I vervatte eisen voldoet'. Bijlage I stelt eisen aan de inhoud van het certificaat. Geëist wordt bijvoorbeeld dat op het certificaat het begin en einde van de geldigheidsduur van het certificaat, de identiteit en het land van vestiging van de partij die het certificaat uitgeeft (in de conceptrichtlijn certificatiedienstverlener genoemd en ook wel bekend als TTP of Certification Authority) en, voorzover van toepassing, beperkingen ten aanzien van het gebruik van het betreffende certificaat staan vermeld.

8) In de conceptrichtlijn wordt een partij die digitale certificaten uitgeeft of andere diensten in verband met elektronische handtekeningen verleent, certificatiedienstverlener genoemd. Artikel 2 lid 10 van de gewijzigde conceptrichtlijn omschrijft een certificatiedienstverlener als 'een dienst of een natuurlijke of rechtspersoon die certificaten uitgeeft of andere diensten in verband met elektronische handtekeningen verleent'. Nadrukkelijk heeft de conceptrichtlijn derhalve een breder toepassingsgebied dan partijen die digitale certificaten uitgeven (Certification Authorities) of beheren alleen. De richtlijn is ook bedoeld voor dienstverleners die voorzien in diensten zoals registratiediensten (Registration Authorities), tijdstempeldiensten (bijvoorbeeld te verlenen door TTP's), directorydiensten, computerdiensten of adviesverlening inzake elektronische handtekeningen.

9) Zie overweging 17 gewijzigde conceptrichtlijn.

bericht te hebben verzonden). De TTP koppelt de identiteit van een persoon aan een publiek/privaat sleutelpaar (gebaseerd op cryptografische technieken). Het publieke deel van dit sleutelpaar wordt vastgelegd in een digitaal certificaat dat aan eenieder bekend kan worden gemaakt en het private deel is geheim en houdt de persoon voor zichzelf. Door berichten te versleutelen met het digitale certificaat van de ontvanger vindt berichtenuitwisseling vertrouwelijk plaats. Doordat de verzender een bericht met behulp van zijn private sleutel digitaal ondertekent – hij zet een zogenaamde digitale handtekening – worden de andere drie betrouwbaarheidsdoelen (zekerheid over oorsprong, integriteit en onweerlegbaarheid van een bericht) gerealiseerd. TTP's vervullen aldus een belangrijke rol in het vergroten van het vertrouwen in digitale gegevensuitwisseling, waaronder commerciële transacties.[10] De hoofdconclusies uit de TTP-beleidsnotitie zijn de volgende:

1. Overheid en bedrijfsleven dienen een aantal concrete maatregelen te treffen ter bevordering van de snelle ontwikkeling van een betrouwbare TTP-infrastructuur. Door middel van zelfregulering kan worden voorzien in de opstelling en naleving van eisen die aan de TTP-dienstverlening moeten worden gesteld. Zelfregulering dient te worden ondersteund door overheidstoezicht.
2. De overheid, aanbieders en gebruikers dienen een TTP-kamer op te richten, die waarborgt dat de in de beleidsnotitie omschreven randvoorwaarden in een bindend reglement worden opgenomen waaraan TTP's zich conformeren. In de TTP-kamer hebben, naast de overheid, zowel de aanbieders als de gebruikers van TTP-diensten op vrijwillige basis zitting. De belangrijkste beoogde taak van de TTP-kamer is het verlenen van een – niet-verplichte – goedkeuring in de vorm van een 'keurmerk' aan TTP's die aan de geformuleerde eisen voldoen door middel van een accreditatie-[11] en certificatieschema.[12]
3. De overheid dient de totstandkoming van een accreditatie- en certificatieschema te stimuleren.

Voordat de parlementaire behandeling van de definitieve nota plaatsvond, is reeds gestart met de uitwerking van de aanbevelingen uit de ontwerpnota. In het kader van TTP.nl zijn drie werkgroepen ingesteld. De werkgroep 'Certificate Policy' moet een overkoepelende CP voor de nationale TTP-infrastructuur opstellen. De 'TTP-kamer' is belast met het onderzoeken van de institutionele en operationele aspecten van het inrichten van een TTP-kamer. De werkgroep 'Accreditatie en Certificatie' ten slotte heeft als doel het opzetten van een infrastructuur voor het certificeren en accrediteren van TTP's in Nederland.

Elektronisch verrichten van rechtshandelingen

De interdepartementale werkgroep 'elektronisch verrichten van rechtshandelingen' heeft in het kader van de operatie Marktwerking, deregulering en wetgevingskwaliteit (MDW) onderzocht in hoeverre vormvereisten[13] in het Burgerlijk Wetboek (BW) en in het bestuursrecht (Algemene wet bestuursrecht) een belemmering vormen voor het elektronisch verrichten van rechtshandelingen en of dient te worden voorzien in elektronische tegenhangers van (authentieke) akten ([MJus98a]). Vormvereisten zijn verplicht gesteld om in bepaalde waarborgen te voorzien. Het vereiste van schriftelijkheid heeft onder meer tot doel hetgeen is overeengekomen te bewijzen, de rechtszekerheid te dienen en fraude te voorkomen. Het is van belang dat elektronische alternatieven ook die waarborgen bieden. De werkgroep concludeert dat, hoewel er technische vooruitgang is, bijvoorbeeld op de gebieden van encryptie, elektronische handtekeningen en TTP's, er in het algemeen op dit moment nog geen volledig gelijkwaardige elektronische alternatieven voor schriftelijke vormvereisten beschikbaar zijn in het BW en in het bestuursrecht. Overeenkomstig de aanbevelingen van de werkgroep wordt een wetsvoorstel voorbereid dat het voor consumenten mogelijk maakt om elektronisch een onroerende zaak (bijvoorbeeld een huis) te kopen, waarbij de consument ter bescherming tegen onder andere overijling een bedenktijd wordt gegund. De verwachting is dat het wetsvoorstel op korte termijn wordt ingediend.

Algemene bepalingen in het BW

Ten slotte heeft het uitgangspunt dat aan mededelingen of rechtshandelingen de geldigheid niet kan worden ontzegd vanwege het feit dat zij in elektronische vorm hebben plaatsgevonden, ertoe geleid dat besloten is om het algemene vermogensrecht geschikt te maken voor de elektronische omgeving. Concreet betekent dit dat in boek 3 van het Burgerlijk Wetboek (BW) een aantal algemene bepalingen zal worden opgenomen met als doel de rechter enkele leidende beginselen te bieden bij de toepassing van het burgerlijk recht in het elektronische rechtsverkeer. Te denken valt aan beginselen als goede trouw en redelijkheid en billijkheid. Naast houvast voor de rechter hebben deze bepalingen tevens tot gevolg dat op de rechter een zekere motiveringsplicht rust. Deze dient aan te geven in hoeverre hij gebruik heeft gemaakt van de bepalingen en zo niet, waarom niet. Het streven is voor het eind van dit jaar een wetsvoorstel gereed te hebben dat ter consultatie aan betrokken partijen kan worden voorgelegd ([MJus99a, p. 3])[14].

Gedragscode voor electronic commerce

De toenmalige Minister van Economische Zaken heeft in 1998 het 'Actieplan Electronic Commerce' ([MEZ98a]) uitgebracht waarin knelpunten voor electronic commerce en oplossingen voor die knelpunten worden aangedragen. Voor vraagstukken op het gebied van contractenrecht, bewijsrechtelijke aspecten van elektronische documenten en bescherming van persoonsgegevens beveelt het actieplan stimulering van de totstandkoming van modelovereenkomsten en/of het tot stand brengen van een uniforme commerciële gedragscode voor electronic commerce aan. Inmiddels is door verschillende partijen, onder de vlag van het Electronic Commerce Platform Nederland (ECP.nl), in overleg met onder meer de ministeries van Economische Zaken en Justitie en VNO-NCW, een Nederlandse Code of Conduct voor elektronisch zakendoen opgesteld ([ECP99]).

De code omvat 'het geheel van alle activiteiten, communicaties en transacties, met een zakelijke doelstelling of achtergrond, welke worden uitgevoerd op elektronische wijze'. De code maakt geen onderscheid tussen goederen en diensten. Zulks in tegenstelling tot de conceptrichtlijn betreffende bepaalde juridische aspecten van de elektro-

10) Zie voor uitgebreidere informatie over TTP's en de onderliggende technologie en procedures de bijdrage van Dontje en Olde Olthof in het Compact Jubileumboek.

11) Accrediteren houdt in dat een organisatie wordt erkend als een certificatie-instelling, zodat deze vervolgens weer aanvragers (TTP's) kan certificeren.

12) Certificeren houdt hier in dat een TTP wordt 'gewaarmerkt'; een onafhankelijke, onpartijdige, deskundige en betrouwbare instelling verklaart dat de TTP voldoet aan vooraf opgestelde eisen. Certificeren kan ook inhouden dat de TTP certificaten uitgeeft en beheert.

13) Een rechtshandeling vereist een op een rechtsgevolg gerichte wil die zich door een verklaring heeft geopenbaard, de wilsuiting. Vormvrij houdt in dat die wilsuiting in iedere vorm kan geschieden. Zo kan de wilsuiting bijvoorbeeld in één of meer gedragingen besloten liggen. De meeste rechtshandelingen, zoals de koop van roerende zaken als een boek, zijn in Nederland vormvrij. Voor bepaalde rechtshandelingen gelden echter één of meer vormvereisten, zoals geschriftsvereisten, ondertekening (door partijen, notaris en getuigen) en voorlezing van een akte door een notaris.

14) Afhankelijk van de voortgang van de thans lopende onderhandelingen over de EU-conceptrichtlijn betreffende enige aspecten van juridische handel wordt in de loop van 2000 een afzonderlijk wetsvoorstel dan wel een wetsvoorstel in samenhang met de uitvoering van de richtlijn ingediend.

nische handel, die uitsluitend betrekking heeft op de elektronische transactie zelf en dus niet op de levering van producten of diensten, tenzij die aflevering elektronisch plaatsvindt. De opstellers van de code achten een drietal begrippen van bijzonder belang voor het creëren van vertrouwen bij elektronische handel, te weten transparantie, betrouwbaarheid alsmede vertrouwelijkheid en privacy. De code is ingedeeld naar deze drie onderwerpen.

Onder transparantie vallen zaken als het (tijdig) inzicht verschaffen in de toepasselijke algemene voorwaarden en het kenbaar maken van de identiteit (en adresgegevens) aan de wederpartij. De opsomming van de gedragscode sluit aan bij de opsomming in de conceptrichtlijn betreffende bepaalde juridische aspecten van de elektronische handel. Ook het duidelijk als zodanig herkenbaar zijn van reclameboodschappen alsmede informatie over de afzender van dergelijke boodschappen valt onder het begrip transparantie. Betrouwbaarheid betekent bijvoorbeeld dat moet worden voorzien in betrouwbare ICT-toepassingen zowel voor communicatie tussen partijen als de afwikkeling van transacties, bijvoorbeeld door toepassing van digitale handtekeningen en servercertificaten waarbij een betrouwbare verbinding tot stand wordt gebracht tussen een cliënt en een server. Vertrouwelijkheid en privacy omvat de zorgvuldige omgang met persoonsgegevens. De verplichtingen opgenomen in de gedragscode zijn conform de toekomstige Wet bescherming persoonsgegevens. De code gebruikt eenvoudige niet-juridische bewoordingen die ook voor een leek begrijpelijk zijn. Hierdoor is de code een zeer toegankelijk document, een streven dat door de makers werd beoogd. Nadeel is dat de code niet voorziet in een handhavingsstructuur. De code is in november tijdens het Nationale Electronic Commerce Congres landelijk gelanceerd door de Minister van Economische Zaken. In oktober was de code al internationaal gepresenteerd en wel aan de OECD.

Cryptografie

Het laatste onderwerp om in het kader van nationaal beleid en regelgeving aan te stippen is het gebruik van cryptografische producten om vertrouwelijkheid te realiseren. Nationale autoriteiten vrezen dat opsporingsdiensten buitenspel worden gezet als criminelen gebruikmaken van dergelijke technieken. In sommige landen bestaat of wordt gesproken over een verplichting om, in verband met opsporingsonderzoek, (private) encryptiesleutels (waarmee vertrouwelijkheid van berichtenuitwisseling wordt gerealiseerd) over te dragen aan de nationale opsporingsautoriteiten indien die autoriteiten zulks noodzakelijk achten. In het wetsvoorstel computercriminaliteit II[15] wordt voorzien in een verplichting tot de medewerking aan ontsleuteling van in geautomatiseerde werken opgeslagen gegevens. Ook TTP's kunnen, als deze voor klanten sleutels bewaren, worden verplicht op bevel van een officier van justitie medewerking te verlenen aan het ontsleutelen van berichten, aldus de Memorie van Toelichting.[16] Er is dus geen sprake van verplichte key escrow, het verplicht deponeren van een extra exemplaar van private sleutels bij een TTP of een overheidsinstantie, maar als TTP's sleutels in escrow hebben, dan dienen zij op bevel van de officier van justitie medewerking te verlenen aan de ontsleuteling van berichten.

Webseals

Webseals, een soort keurmerk dat op een website wordt geplaatst en aangeeft dat de website zich houdt aan de regels verbonden aan het keurmerk, zijn een middel om het vertrouwen van consumenten maar ook van bedrijven in webaanbieders te bevorderen. Dat dergelijke zegels inderdaad een vertrouwensbevorderend effect hebben, blijkt bijvoorbeeld uit het besproken Cheskinonderzoek. Webseals staan de laatste tijd volop in de belangstelling. De lancering begin november van Web Trader, een elektronisch waarborgzegel van de Consumentenbond, is in de media breed uitgemeten. Hieronder volgt een bespreking van een aantal keurmerken. Alleen keurmerken die als doel hebben vertrouwen in elektronische handel te bevorderen worden besproken. Bekeken wordt welke garanties de aanwezigheid van een bepaald keurmerk nu precies biedt. Tevens wordt aangegeven waar de verschillen tussen de verschillende keurmerken uit bestaan. Er is nadrukkelijk geen sprake van een limitatieve bespreking, dat zou in het kader van dit artikel te ver strekken. Er worden twee webseals behandeld die gericht zijn op de Nederlandse markt, te weten Web Trader en het Goedgekeurd Keurmerkinstituut van het Keurmerkinstituut. Voorts worden twee keurmerken besproken die zich op de Amerikaans/Canadese markt richten, BBB*OnLine* en TRUSTe, en één keurmerk dat een internationaal karakter heeft, WebTrust. TRUSTe verleent alleen een privacyseal, BBB*OnLine* kent zowel privacyseals toe als zogeheten reliabilityseals. De andere uitgevende instanties geven een zegel uit waarbij privacy één van de onderwerpen is.

De Code of Conduct voor elektronisch zakendoen is een zeer toegankelijk document, dat echter niet in een handhavingsstructuur voorziet.

Web Trader

Web Trader bestond al langer maar begin november heeft de Consumentenbond het keurmerk landelijk gelanceerd. Dit gebeurde gelijktijdig met de bekendmaking van de teleurstellende resultaten van een onderzoek door de Consumentenbond naar de kwaliteit van de dienstverlening van 150 Nederlandse webwinkels. Web Trader is bedoeld voor aanbieders die volgens Nederlands recht leveren en waarmee consumenten in het Nederlands kunnen communiceren. De Consumentenbond publiceert op zijn site een overzicht van de bij Web Trader aangesloten winkels alsmede ervaringen van het publiek met die aanbieders. Websites die het Web Trader-logo willen voeren, moeten aan een aantal eisen voldoen. Door het doen van proefaankopen wordt gecontroleerd of de winkels zich in de praktijk aan de afgesproken regels houden.

Een aantal regels komt overeen met de eisen uit de besproken conceptrichtlijn betreffende juridische aspecten van elektronische handel. De leverancier moet zijn identiteit kenbaar maken en alle gegevens vermelden om met hem in contact te kunnen treden, alsmede zijn

15) De officiële benaming van het wetsvoorstel computercriminaliteit II is het wetsvoorstel tot wijziging van het Wetboek van Strafrecht, het Wetboek van Strafvordering en de Telecommunicatiewet in verband met nieuwe ontwikkelingen in de informatietechnologie, TK 1998-1999, 26 671. Aan art. 126m Sv wordt een nieuw lid 5 toegevoegd.

16) TK 1998-1999, 26 671, nr. 3, p. 24.

inschrijvingsnummer bij de KvK en eventueel zijn BTW-nummer vermelden. Voorts moet de totaalprijs duidelijk vermeld zijn. Er mag geen sprake zijn van verborgen aanvullende kosten zoals BTW- en verzendkosten. Indien leveringsvoorwaarden van toepassing zijn, moeten die beschikbaar worden gesteld.

De overige voorwaarden komen sterk overeen met de opsomming van verplichtingen die door Consumers International is opgesteld (zie paragraaf 'Onderzoek consumentenorganisaties'). Zo dienen aanbieders aan te geven hoe betaling plaats kan vinden (inclusief een 'stap-voor-stap'-instructie over de betreffende betalingsmethoden), via welke stappen de overeenkomst totstandkomt en moeten zij afnemers informeren over de toepasselijke garantie. Voorts mag de leveringstermijn niet langer zijn dan dertig dagen, moet een factuur worden verstuurd (bij elektronische levering van diensten ten minste een elektronische factuur), geldt dat een koop binnen zeven dagen na ontvangst van het product ongedaan gemaakt moet kunnen worden, dient een niet-goed-geld-terugbeleid te worden gevoerd en moeten veiligheidsmaatregelen worden getroffen voor wat betreft de overdracht van persoonlijke gegevens en betalingen. Webwinkels moeten ook beschikken over een klachtenprocedure, klantenservice en ze dienen aanvullend op de wettelijke verplichtingen (Wet persoonsregistraties) aan een aantal voorwaarden met betrekking tot de omgang met persoonsgegevens te voldoen.

Het Web Trader-keurmerk heeft als voordeel dat de uitgever, de Consumentenbond, een oude vertrouwde partij is die al jaren opkomt voor de rechten van de consument en ook door alle partijen als zodanig herkend zal worden. Voorts zijn er voor de leverancier geen kosten verbonden aan het keurmerk. Een derde positief aspect is dat het keurmerk niet op zichzelf staat, maar dat de Consumentenbond een platform heeft opgericht, dedigitaleconsument.nl, waar consumenten onder meer hun ervaringen kunnen delen.
Nadeel is de beperkte scope van het initiatief: Web Trader geldt alleen voor Nederlandse aanbieders (Nederlands recht is van toepassing en communicatie moet plaatsvinden in het Nederlands). Hoewel de Consumentenbond stelt dat het Web Trader-keurmerk internationaal door verschillende buitenlandse zusterorganisaties van de Nederlandse bond wordt gelanceerd, is het de vraag of dit waardevol is voor de consument. De regels waar sites aan moeten voldoen willen ze het Web Trader-logo voeren, verschillen per land; het gevaar bestaat dan ook dat consumenten ervan uit zullen gaan dat voor iedere site die het Web Trader-logo voert de Nederlandse voorwaarden gelden.
Een ander nadeel betreft het feit dat naast de proefaankopen en het delen van ervaringen van shoppers via de website van de Consumentenbond, de verplichting van leveranciers alleen een 'papieren' verplichting betreft. De Consumentenbond controleert weliswaar of de inhoud van de site voldoet aan de eisen vastgelegd in de Web Trader-code, maar er wordt niet gecontroleerd of de door de sites toegepaste beveiliging wel toereikend is. Daags na de toekenning van het logo aan twintig webwinkels werd bekend dat een kwart van de betreffende sites gekraakt was. Hackers konden zich toegang verschaffen tot bestanden met persoonlijke gegevens van klanten. Bovendien maakt de meerderheid van de twintig winkels geen gebruik van SSL (Secure Socket Layer) of een andere beveiligingsmethode, voor het versturen van klant- en betalingsgegevens, hetgeen de code wel eist (zie de paragraaf 'veiligheid' van de Web Trader-code).

Goedgekeurd Keurmerkinstituut

Het keurmerk Goedgekeurd Keurmerkinstituut is de opvolger van het keurmerk van de Nederlandse Vereniging van Huisvrouwen en Goedmerk. Deze keurmerken hebben hun basis in de fysieke wereld, maar Goedgekeurd Keurmerkinstituut richt zich ook op e-commerce. Goedgekeurd Keurmerkinstituut is gericht op de consumentenmarkt. Ook het Keurmerkinstituut vermeldt goedgekeurde producten en diensten op zijn website. Bovendien kunnen keurmerkhouders een eigen webpagina op de site van het Keurmerkinstituut krijgen om nadere informatie over het bedrijf te verstrekken.

Hoewel het onderzoek dat het Keurmerkinstituut uitvoert in het kader van een keurmerkaanvraag nadrukkelijk alle stadia (vóór, tijdens en na aankoop) en facetten van de relatie tussen consument en leverancier in acht neemt, ligt de nadruk op de kwaliteit (producteigenschappen als bruikbaarheid, duurzaamheid en veiligheid) van het product of de dienst zelf. Zo vindt onderzoek plaats in laboratoria en/of in een praktijksituatie door middel van een panel van huishoudens. Consumenten die goederen aanschaffen via Internet maken zich echter vooral zorgen of de leverancier wel betrouwbaar is en of een product überhaupt wel wordt bezorgd. Hoewel een garantie over de kwaliteit van bepaalde producten – denk met name aan producten uit het hogere prijssegment zoals audio- en videoapparatuur en computers – zeker als wenselijk wordt ervaren, zijn de meeste webshoppers primair op zoek naar informatie over de betrouwbaarheid van de dienstverlening rondom een aangeschaft product/dienst. Zonder een aan elektronische handel aangepaste strategie is niet te verwachten dat het Goedgekeurd Keurmerkinstituut-keurmerk online veel succes zal boeken.

WebTrust

WebTrust is een gezamenlijk initiatief van de Amerikaanse en Canadese beroepsinstituten voor accountants (AICPA en CICA)[17] met als doel onzekerheden bij elektronische handel weg te nemen door accountants te laten toetsen of aan de WebTrust-principes is voldaan. Accountantskantoren die over een licentie beschikken kunnen het zegel uitgeven. KPMG heeft zo'n licentie en heeft inmiddels het eerste WebTrust-zegel in Nederland toegekend. WebTrust richt zich zowel op leveranciers die zakendoen met eindgebruikers als op business-to-business toepassingen.

Het WebTrust-zegel kan worden beschouwd als een soort goedkeurende accountantsverklaring in elektronische vorm. Met het WebTrust-zegel maakt de aanbieder niet alleen kenbaar dat de informatieverstrekking via de website door een accountant is onderzocht en voldoet aan de WebTrust-principes, maar het zegel geeft tevens aan dat onderzoek is gedaan naar de IT-controls van de systemen die de e-commerceapplicatie ondersteunen en

17) American Institute of Certified Public Accountants en Canadian Institute of Certified Accountants.

naar organisatorische processen en procedures. Voorts geeft het zegel aan dat de aanbieder onder permanente controle van een accountant staat. Ten minste eenmaal per drie maanden wordt gecontroleerd of er geen wezenlijke veranderingen zijn opgetreden in de werkwijze van de aanbieder.

De WebTrust-audit richt zich in grote lijnen op drie aspecten. Deze aspecten zijn:

1. *Algemene leveringsvoorwaarden*. Op de website moeten algemene voorwaarden zijn opgenomen waarin onder andere bestelproces, retourneren van goederen, klachten en garantie worden behandeld. Tevens wordt gecontroleerd of klanten juist en volledig worden geïnformeerd over de verzameling van hun persoonlijke gegevens.
2. *Integriteit van de transactie*. Gecontroleerd wordt of er beheersingsmaatregelen zijn geïmplementeerd zodat bestellingen juist en tijdig worden afgewerkt en de juiste bedragen worden gefactureerd. Er wordt met andere woorden gecontroleerd of de organisatie haar processen zodanig heeft ingericht dat werkelijk conform de algemene voorwaarden kan worden gehandeld.
3. *Zorgvuldige omgang met gegevens*. Er dienen maatregelen te zijn getroffen om ervoor te zorgen dat gegevens van klanten zijn beveiligd tegen raadpleging door derden en gegevens niet worden gebruikt voor andere doeleinden dan waarvoor ze zijn verzameld. Voorts dient de communicatie tussen de aanbieder en (potentiële) klanten beveiligd plaats te vinden (gegevens kunnen niet worden onderschept en gewijzigd). De inrichting en het beheer van de firewall, alsmede andere beveiligingsmaatregelen worden beoordeeld.

De kracht van WebTrust zit met name in twee zaken. Ten eerste gaat de controle verder dan alleen de (tekstuele) inhoud van de website. Ook de door de organisatie achter de website gehanteerde processen en procedures en de Internet-toepassing worden gecontroleerd. Er wordt gecontroleerd of de leverancier hetgeen hij toezegt op zijn website werkelijk kan waarmaken. Ten tweede wordt het zegel afgegeven door een onafhankelijke partij met een lange historie van vertrouwen in de fysieke wereld, de accountant, die bovendien na het uitreiken van het zegel ten minste driemaandelijks controleert of zich bij de aanbieder veranderingen hebben voorgedaan.

Omdat aan de toekenning van een WebTrust-zegel niet alleen een analyse van de website voorafgaat maar ook de gehanteerde processen en procedures en de Internet-toepassing worden gecontroleerd, hangt aan WebTrust een prijskaartje van minimaal *f* 10.000 (afhankelijk van de omvang van de e-commerceorganisatie). Naast deze initiële kosten moet ook rekening worden gehouden met de kosten verbonden aan de driemaandelijkse audit en het na de audit vervangen van het webzegel door een nieuw exemplaar. Omdat het onderzoek vrij diepgaand is, is het bijvoorbeeld heel goed mogelijk het WebTrust-programma te combineren met een onderzoek naar de informatiebeveiliging. Aldus is het verkrijgen van het zegel niet meer een doel op zich maar een soort bonus na de afronding van een groter project en kunnen de kosten beter worden verantwoord.

TRUSTe

TRUSTe is een onafhankelijke non-profitorganisatie opgericht door CommerceNet en de Electronic Frontier Foundation (EFF, een bekende Amerikaanse voorvechter van privacyrechten). Het doel van TRUSTe is het vergroten van vertrouwen van gebruikers in Internet. Het zegel dat TRUSTe uitgeeft, het TRUSTe-trustmark zoals ze het zelf noemen, garandeert dat de website een privacybeleid heeft dat via het aanklikken van het TRUSTe-icoon is te raadplegen en dat wordt gecontroleerd door TRUSTe. Sites moeten ten minste de volgende informatie verschaffen: welke gegevens worden verzameld, voor welke doeleinden die gegevens worden gebruikt, aan welke partijen de gegevens (eventueel) worden verstrekt, de wijze waarop degene op wie de gegevens betrekking hebben zijn gegevens kan laten wijzigen en ten slotte de maatregelen die zijn getroffen ten behoeve van de beveiliging van de gegevens die worden verstrekt. Als websites voor betaling een creditcardnummer van een klant vragen, moet de verzending van dit nummer beveiligd, bijvoorbeeld met behulp van SSL, gebeuren.

Om voor een TRUSTe-zegel in aanmerking te komen moet een privacybeleid, vastgelegd in een privacy policy, ter goedkeuring worden voorgelegd aan TRUSTe. Na de initiële uitreiking van het zegel vindt periodieke controle van de inhoud van de privacy policy plaats door TRUSTe. Bovendien voert TRUSTe zelf steekproeven uit door gegevens te verstrekken om vervolgens te controleren of hetgeen wordt geclaimd in de privacy policy ook werkelijk wordt nageleefd. Voorts wordt de Internetgemeenschap opgeroepen om schendingen van privacy policies te melden. Ten slotte kan TRUSTe als laatste middel een website laten onderwerpen aan een accountantsonderzoek. Bedrijven die zich aansluiten bij TRUSTe onderwerpen zich aan de hiervoor genoemde controlemaatregelen. Een groot aantal Amerikaanse websites is aangesloten bij TRUSTe. De kosten liggen, afhankelijk van de omzet van het bedrijf, tussen de $ 249 en $ 4,999 per jaar.

BBB*OnLine*

Better Business Bureau OnLine is een honderd procent dochteronderneming van de Council of Better Business Bureaus (CBBB). Onder de oprichters van deze raad bevinden zich grote namen als AT&T, Hewlett-Packard, Netscape en Xerox. BBB*OnLine* heeft twee webzegelprogramma's; een gericht op privacy en een op vertrouwen in de meer brede zin.

Partijen die voor een zegel in aanmerking willen komen, moeten een privacy policy opstellen en een beveiligingsbeleid. De zaken die in de privacy policy moeten worden geadresseerd, zijn omschreven. Het betreft zaken als de doelen waarvoor gespecificeerde gegevens worden verzameld, beveiliging en de (eventuele) keuze van degene om wiens gegevens het gaat ten aanzien van het gebruik van zijn gegevens en verstrekking aan derden. Naast de meer standaardprivacyaspecten die ook bij andere zegels aan bod komen adresseert BBB*OnLine* ook een aantal aanvullende zaken. Zo zijn deelnemende organisaties verplicht toe te lichten hoe de juistheid van de opgeslagen gegevens wordt gegarandeerd en moet degene wiens gegevens worden verzameld de mogelijkheid worden

geboden om verstrekking van zijn gegevens aan derden ten behoeve van marketingdoeleinden te weigeren. Tevens moeten deelnemende organisaties beschikken over een beveiligingsbeleid en moet online verzamelde informatie worden beschermd tegen onderschepping. Voorts moeten deelnemende organisaties akkoord gaan met controlemaatregelen en de geschillenregeling, alsmede de uitkomsten van die regeling, van BBB*OnLine*. De kosten variëren, afhankelijk van de omzet van de deelnemende organisatie, van $ 150 tot $ 3,000 per jaar. Om voor een privacy webseal van BBB*OnLine* in aanmerking te komen moet de website zijn gericht op consumenten in Amerika en/of Canada. Dit vormt een belangrijke beperking van BBB*OnLine*.

Om in aanmerking te komen voor het 'BBB*OnLine* Reliability Program seal' moet een bedrijf allereerst lid worden van het Better Business Bureau (BBB). Het adres van (fysieke) vestiging moet worden opgegeven en dat wordt gecontroleerd. Voorts moet de aanvrager van het zegel minimaal een jaar zijn producten/diensten aanbieden (hierop zijn uitzonderingen mogelijk) en moet deze zich onderwerpen aan de geschillenregeling van BBB*OnLine*. Er wordt gecontroleerd of de aanvrager voldoet aan de BBB*OnLine*-standaard. Als dit zo is krijgt de aanvrager het zegel op zijn website. Klanten kunnen op het zegel klikken om informatie te raadplegen van BBB over het betreffende bedrijf.

18) De Wet persoonsregistraties, die waarschijnlijk begin volgend jaar wordt vervangen door de Wet bescherming persoonsgegevens.

Voorlichting over de inhoud van de verschillende webseals is een vereiste.

Conclusie webseals

Tussen de besproken webseals zijn duidelijke verschillen in doelgroep waar te nemen. Twee seals, Web Trader en Goedgekeurd Keurmerkinstituut, zijn duidelijk gericht op de Nederlandse markt, TRUSTe en BBB*OnLine* richten zich op de Amerikaans/Canadese markt. Alleen WebTrust is een internationaal opgezet keurmerk. Het Keurmerkinstituut-keurmerk lijkt beter geschikt voor een fysieke omgeving dan een elektronische omgeving, omdat de nadruk sterk ligt op de productkwaliteiten en er minder aandacht is voor de voorwaarden en de afhandeling van de overeenkomst. Web Trader is een goed initiatief van de Consumentenbond. Het is jammer dat de controle niet verder gaat dan een 'papieren' controle van de inhoud van de website, het doen van proefaankopen en het delen van ervaringen door het winkelend publiek. Met name de beveiliging van de site en de communicatie tussen kopers en verkopers zijn belangrijk voor e-commercetoepassingen en op dit punt vindt geen controle plaats. Het voordeel van WebTrust is juist dat de processen en procedures alsmede de Internet-toepassing aan een (periodieke) audit zijn onderworpen. Het gevolg van deze insteek is uiteraard wel dat aan dit zegel een prijskaartje hangt, in tegenstelling tot het Web Trader-zegel dat gratis wordt verstrekt. De meeste zegels richten zich op business-to-consumer e-commerce, alleen WebTrust mikt tevens op business-to-business e-commercetoepassingen. Dat Amerikaanse organisaties voorzien in een privacyseal en de Nederlandse aanbieders privacy als onderdeel in een trustseal opnemen is niet zo vreemd gezien het feit dat hier te lande uitgebreide privacywetgeving[18] bestaat, terwijl er in de Verenigde Staten eigenlijk slechts sectorale privacyregulering bestaat. Van een dreigende wildgroei aan keurmerken voor Internet waar het Nederlandse Keurmerkinstituut voor vreest ([NRC99]) is nog geen sprake. De besproken keurmerken richten zich op verschillende markten. Voorlichting, zeker voor particuliere afnemers, over de inhoud van de verschillende webseals is echter wel een vereiste. Zeker nu steeds meer mensen reeds hun eerste stappen op het net hebben gezet, met het medium vertrouwd zijn geraakt en ook geïnteresseerd raken in het online aanschaffen van producten en diensten.

Samenvatting

In dit artikel is stilgestaan bij de factoren die bepalend zijn voor het vertrouwen in elektronische handel. Het betreft vertrouwen in brede zin. Veiligheid is één van de factoren die bepalend zijn voor vertrouwen, maar het realiseren van vertrouwen vraagt meer dan beveiliging alleen. Simpel gezegd, een webaanbieder is er niet met het bieden van een goede beveiliging, hoe belangrijk ook, alleen. Een heldere en toegankelijke voorlichting over de toepasselijke voorwaarden en een klantenservice zijn andere factoren die vertrouwenwekkend zijn.

Gebrekkige informatieverstrekking door en slechte ervaringen met online-verkopers, zoals uit het onderzoek van Consumers International naar voren kwam, en niet te vergeten de verhalen die hierover de ronde doen, hebben een negatieve invloed op de bereidheid om via het Internet aankopen te doen. Online-verkopers kunnen hier iets aan doen. Zij kunnen hun voorlichting verbeteren en hun bedrijfsprocessen adequaat inrichten op het elektronisch verkoperschap. Ook kunnen ze bij de inrichting van hun site rekening houden met het vertrouwensaspect, bijvoorbeeld door de resultaten van het Cheskin-onderzoek mee te nemen. Bovendien kunnen websites zich aansluiten bij een trustseal-programma en zo meeliften op het vertrouwen dat afnemers in het betreffende zegel stellen.

Naast tekortkomingen die te wijten zijn aan leveranciers die via Internet zakendoen, zijn er ook belemmeringen die hun grondslag hebben in het feit dat regelgeving aangepast moet worden aan een elektronische handelsomgeving. Getracht is inzichtelijk te maken welke tekortkomingen zich voordoen en hoe hiervoor een oplossing wordt gezocht, zowel in nationaal als internationaal verband.

Eén ding is zeker: No trade without trust.

Literatuur

[Ches99]
Cheskin Research and Studio Archetype/Sapient, *eCommerce Trust Study*, January 1999, http://www.studioarchetype.com/cheskin/assets/images/etrust.pdf

[Cons99a]
Consumentenbond, *Consumentenbond geeft internet-winkels een zware onvoldoende, Nieuwe campagne over digitaal consumeren van start (persbericht),* 1 november 1999, http://www.consumentenbond.nl
[Cons99b]
Consumentenbond, *Veel nep-keurmerken op Internet,* 1 november 1999, http://www.consumentenbond.nl
[Cons99c]
Consumers International, *Consumers@shopping: An international comparative study of electronic commerce*, september 1999. Het rapport is in pdf-formaat beschikbaar op de site van Consumers International, http://www.consumersinternational.org/campaigns/electronic/e-comm.pdf
[Cran99]
L. Faith Cranor, J. Reagle en M.S. Ackerman, *Beyond Concern: Understanding Net Users' Attitudes About Online Privacy*, april 1999, http://www.research.att.com/library/trs/TRs/99/99.4/99.4.3/report.htm .
Een samenvatting is te lezen op: http://www.research.att.com/projects/privacystudy/
[Door99]
F. van Doorn, *De CD Teleshop*, Informatie, september 1999, p. 34-41.
[ECP99]
Electronic Commerce Platform Nederland, *ECP.NL Code of Conduct voor elektronisch zakendoen*, 1999, http://www.ecp.nl/vertrouwen/
[EuCo98a]
European Commission, *Proposal for a European Parliament and Council directive on certain legal aspects of electronic commerce in the Internal Market*, 18 November 1998, COM(98) 586 def., 98/0325 (COD), http://europa.eu.int/comm/dg15/en/media/eleccomm/com586en.pdf
Europese Commissie, *Voorstel voor een richtlijn van het Europees Parlement en de Raad betreffende bepaalde juridische aspecten van de elektronische handel in de interne markt*, 18 november 1998, COM(98) 586 def., 98/0325 (COD), http://europa.eu.int/comm/dg15/en/media/eleccomm/com586nl.pdf
[EuCo98b]
European Commission, *Proposal for a European Parliament and Council directive on a common framework for electronic signatures,* 13 May 1998, COM(1998) 297 def., 98/0191(COD), http://europa.eu.int/comm/dg15/en/media/infso/com297en.pdf
Europese Commissie, *Voorstel voor een richtlijn van het Europees Parlement en de Raad betreffende een gemeenschappelijk kader voor elektronische handtekeningen,*13 mei 1998, COM(1998) 297 def., 98/0191(COD), http://europa.eu.int/comm/dg15/en/media/infso/com297nl.pdf
[EuCo99a]
European Commission, *Amended proposal for a European Parliament and Council directive on certain legal aspects of electronic commerce in the Internal Market*, COM (99) 427 final, 98/0325(COD), http://europa.eu.int/comm/dg15/en/media/eleccomm/com427en.pdf
Europese Commissie, *Gewijzigd voorstel voor een richtlijn van het Europees Parlement en de Raad betreffende bepaalde juridische aspecten van de elektronische handel in de interne markt*, COM(99) 427 def., 98/0325 (COD), http://europa.eu.int/comm/dg15/en/media/eleccomm/com427nl.pdf
[EuCo99b]
European Commission, *Amended proposal for a European Parliament and Council directive on a common framework for electronic signatures,* 29 April 1999, COM(1999) 195 final., 98/0191(COD), http://europa.eu.int/comm/dg15/en/media/sign/signamen.pdf
Europese Commissie, *Gewijzigd voorstel voor een richtlijn van het Europees Parlement en de Raad betreffende een gemeenschappelijk kader voor elektronische handtekeningen,* 29 april 1999, COM(1999) 195 def., 98/0191(COD), http://europa.eu.int/comm/dg15/en/media/sign/signamnl.pdf
[KMCU98]
KPMG Management Consulting UK, *Electronic Commerce Research Report 1998*, KPMG London 1998.
[MEZ98a]
Ministerie van Economische Zaken, *Actieplan Electronic Commerce*, maart 1998, http://info.minez.nl/pdfs/05r38.pdf
[MEZ98b]
Ministerie van Economische Zaken en Ministerie van Verkeer en Waterstaat, *concept Eindrapportage Nationaal TTP-project*, maart 1998.
[MEZ99a]
Ministerie van Economische Zaken en Ministerie van Verkeer en Waterstaat, *notitie Nationaal TTP-project*, juni 1999, TK 1998-1999, 26 581, nr. 1, http://www.overheid.nl/op/ (definitieve versie van de rapportage uit 1998).
[MJus98a]
Ministerie van Justitie en Ministerie van Economische Zaken, *MDW-rapport Elektronisch verrichten van rechtshandelingen*, april 1998. Persbericht van het Ministerie van Justitie: http://www.minjust.nl/c_actual/persber/EINDRAP.htm
[MJus98b]
Ministerie van Justitie, *Wetgeving voor de elektronische snelweg*, februari 1998, TK 1997-1998, 25 880, nrs. 1-2, http://www.minjust.nl/sdu/index.htm
[MJus99a]
Ministerie van Justitie, brief van de Minister van Justitie met een geactualiseerde versie van het actieplan behorend bij de nota *Wetgeving voor de elektronische snelweg,* TK 1998-1999, 25 880, nr. 8, http://www.overheid.nl/op/
[NRC99]
NRC Handelsblad, *Consumentenbond: Winkels op Internet deugen niet,* 2 november 1999, http://www.nrc.nl/W2/Nieuws/1999/11/02/Eco/01.html
[OESO97a]
OESO, *Business-to-Consumer Electronic Commerce: Survey of Status and Issues*, OECD/GD(97)219, 1997, http://www.oecd.org/dsti/sti/it/ec/prod/gd97219e.pdf
[OESO97b]
OESO, *Dismantling the Barriers to Global Electronic Commerce*, 1997, 30 p., http://www.oecd.org/dsti/sti/it/ec/prod/dismantl.htm
[UNCI96]
United Nations Commission on International Trade Law (UNCITRAL), General Assembly Resolution, *Model Law on Electronic Commerce*, December 1996, http://www.uncitral.org/english/texts/electcom/ml-ec.htm
[UNCI98]
United Nations Commission on International Trade Law (UNCITRAL), Working Group on Electronic Commerce, *Draft Uniform Rules on Electronic Signatures*, 32th session, Vienna, 19-30 January 1998, http://www.uncitral.org/english/sessions/wg_ec/wp-73.htm

Mw. mr. drs. M.J.Dontje is werkzaam bij KPMG EDP Auditors Electronic Commerce te Amstelveen. Haar aandachtsgebied betreft advisering (organisatorisch alsook juridisch) op het gebied van ICT in het algemeen en e-commerce in het bijzonder. Hiervoor studeerde zij Nederlands Recht (hoofdrichtingen privaatrecht en strafrecht) en Bedrijfseconomie.