COMPACT

TIJDSCHRIFT EDP-AUDITING

ELECTRONIC COMMERCE

1998/4

Compact ®
Jaargang 25, nummer 4
Een uitgave van KPMG EDP Auditors NV en ten Hagen & Stam BV.
Het blad verschijnt 6 x per jaar.
Redactie
Prof. A.W. Neisingh RE RA (hoofdredacteur)
Drs. P.P.M.G.G. Brouwers RE RA
Ir. J.A.M. Donkers RE
W. de Korte RE RA
J.C. van Praat RE RA
Ir.drs. J. van der Vlugt
Adviesraad
Mr. P. van Dijken
G. van Essen RA
Prof.mr. H. Franken
Dr. K.J. Mollema RA
Prof. H.B. Moonen RE RA
Prof.dr.ir. R. Paans RE
Uitgeefassistent
C.M.A. van Houtum, ten Hagen & Stam, Postbus 34, 2501 AG Den Haag
Tel.: 070 – 304 57 52
Fax: 070 – 304 58 17
e-mail: c.houtum@wkths.nl
Basisvormgeving
Bureau Karakter, Delft
Opmaak
AlphaZet bv, Waddinxveen
Abonnementen
f 165,- per jaar incl. BTW.
Losse nummers f 45,- incl. BTW.
Studentenabonnement f 95,- incl. BTW. Abonnementen kunnen schriftelijk tot uiterlijk één maand voor de aanvang van een nieuw abonnementsjaar worden opgezegd. Bij niet tijdige opzegging wordt het abonnement automatisch met een jaar verlengd.
Abonnementsadministratie
Samsom BedrijfsInformatie, Postbus 4, 2400 MA Alphen aan den Rijn
Tel.: 0172 – 466 800
Fax : 0172 – 475 933
Adreswijzigingen – ook tijdelijke – moeten minstens 8 weken voor de verschijningsdatum bekend zijn.
Overname artikelen
Het overnemen en vermenigvuldigen van artikelen en berichten is slechts geoorloofd na schriftelijke toestemming van de uitgever.
Overdrukken artikelen
Overdrukken van artikelen kunnen worden aangevraagd bij de uitgeefassistent. Prijs per overdruk per artikel (inclusief omslag) f 5,-.

Uitgever
I.J. van Haren

Nederlands Uitgeversverbond
Groep vaktijdschriften

ISSN 0920 – 1645

INHOUDSOPGAVE

REDACTIONEEL

Het blad wil een bijdrage leveren aan de ontwikkeling van het vakgebied EDP-auditing door het publiceren van actuele artikelen op deelterreinen van EDP-auditing en advies, zoals:
• beoordeling automatiseringsorganisaties en -systemen • risicobeheersing • telecommunicatie-adviezen • beveiligingsonderzoeken • quality assurance • opleidingen en trainingen • privacywetgeving • computercriminaliteit en nieuwe regelgeving.

Behalve voor EDP-auditors kan dit blad ook interessant zijn voor IT-deskundigen en gebruikers van informatiesystemen. De in dit tijdschrift weergegeven meningen mogen niet worden gezien als officiële zienswijze van KPMG EDP Auditors NV.

Het blad Compact is met de meeste zorg samengesteld. Niettemin is het niet geheel uitgesloten dat de geboden informatie enkel en alleen door tijdsverloop en/of andere oorzaken minder juist is. Noch KPMG, KPMG EDP Auditors, noch de redacteuren persoonlijk, noch uitgeverij ten Hagen & Stam BV, aanvaarden enige aansprakelijkheid, hoe ook genaamd, uit welken hoofde dan ook voor enig gevolg rechtstreeks of indirect voortvloeiend uit het gebruik van de informatie.

De redactie stelt gaarne ruimte in Compact beschikbaar voor reacties en/of ervaringen van lezers. Auteurs die overwegen een bijdrage te leveren, wordt verzocht kennis te nemen van de aanwijzing voor auteurs, die bij de uitgeef-assistent verkrijgbaar is.

Electronic commerce, te omschrijven als elektronisch zakendoen of 'het uitwisselen van digitale data voor handelsdoeleinden', staat volop in de belangstelling. Verschillende congressen zijn aan dit thema gewijd, veel artikelen zowel in dagbladen als in vaktijdschriften worden over dit thema gepubliceerd en verschillende organisaties worden opgericht om de toepassing van electronic commerce in Nederland en in Europa te bevorderen. Een voorbeeld van dit laatste is het Electronic Commerce Platform Nederland (ECP.nl). Kortom, genoeg publiciteit.

Electronic commerce biedt vele voordelen, waaronder een verhoging van de efficiency, verlaging van de kosten en vergroting van de omzet. Ondanks de grote aandacht in de media en de vele initiatieven op dit gebied komt de toepassing van electronic commerce nog niet echt van de grond, althans waren de verwachtingen hoger gespannen dan de praktijk op dit moment laat zien. Eén van de oorzaken die wordt genoemd, is dat bij veel gebruikers onzekerheid bestaat over de veiligheid van electronic commerce over het Internet. Vandaar dat wij voor dit nummer van Compact 'Secure electronic commerce' als centraal thema hebben gekozen. Vanuit diverse invalshoeken, zowel technische (artikel Moonen), juridische (artikel Kemna) als organisatorisch/beleidsmatige (artikelen Duthler/Dontje en Hermans/Bruggeman) wordt dit thema belicht.

In het eerste artikel wordt een overzicht gegeven van de ontwikkelingen op het gebied van electronic commerce, wordt aangeduid welke toepassingen van electronic commerce denkbaar zijn en worden de mogelijke voordelen van electronic commerce op een rijtje gezet.

Vervolgens wordt in het tweede artikel aandacht besteed aan oplossingen voor veilige of secure electronic commerce over Internet, vanuit een meer technische invalshoek. Verwacht wordt dat het Internet een belangrijk medium zal worden voor electronic commerce, onder andere vanwege het mondiale karakter. De verschillende netwerkbeveiligingsvereisten worden besproken, en ook wordt uitgebreid ingegaan en een toelichting gegeven op verschillende cryptografische technieken.

Voordat vervolgens wordt aangehaakt bij de netwerkbeveiligingsvereisten, die door de inzet van een zogenaamde Trusted Third Party kunnen worden gerealiseerd, wordt eerst nog ingegaan op enkele juridische aspecten van electronic commerce. De juridische aspecten betreffen het belang van contracten, het gebruik van algemene voorwaarden, het bewijs in een digitale omgeving waarbij de functie van de handtekening wordt besproken en het gebruik van e-mail. Tot slot wordt in dit artikel de suggestie gedaan om een gedragscode voor electronic commerce op te stellen. In het hierboven genoemde ECP.nl worden hier reeds aanzetten toe gegeven.
Trusted Third Parties, betrouwbare derde partijen – de betekenis ervan wordt in het artikel zelf aangegeven – kunnen worden beschouwd als een belangrijke maatregel om secure electronic commerce te realiseren. In het artikel wordt uitgelegd wat de functies van een TTP zijn, hoe een TTP 'werkt', welke diensten een TTP kan verlenen en welke eisen aan een TTP kunnen worden gesteld, wil je van een werkelijk betrouwbare partij kunnen spreken. Ook wordt in het artikel ingegaan op (internationale) ontwikkelingen op het gebied van beleid en regelgeving ten aanzien van cryptografie, vormvereisten en digitale handtekeningen, en TTP's.

Tot slot komt in het laatste artikel een praktijkvoorbeeld van electronic commerce en TTP-dienstverlening in de bouwbranche aan de orde. Aangegeven wordt hoe TTP-dienstverlening kan worden geïmplementeerd en vanuit welke invalshoeken welke onderwerpen aan bod dienen te komen.

De hooggespannen verwachtingen ten aanzien van de mogelijkheden die electronic commerce biedt zijn ons inziens terecht, mits aan de vereiste van veiligheid kan worden voldaan. De redactie heeft met dit themanummer een bijdrage willen leveren aan de realisatie van secure electronic commerce in Nederland, zodat Nederland in staat is de beoogde koppositie op de elektronische snelweg (het streven van oud-minister Wijers zoals iedereen weet) te bereiken.

Mw. mr. drs. A.W. Duthler

Stand van zaken en ontwikkelingen rond electronic commerce

Drs. A.J. Biesheuvel RA RE en drs. C.F. Olde Olthof

In vogelvlucht worden ontwikkelingen rond en toepassingen van electronic commerce behandeld. Enkele voorbeelden van toepassingen worden gegeven, alsmede worden de voordelen van en enkele voorwaarden voor electronic commerce besproken.

INLEIDING

Electronic commerce of elektronisch zakendoen heeft – als we de media moeten geloven – de toekomst. Veel ondernemers treffen voorbereidingen en investeren in deze nieuwe manier van zakendoen. Kostenbesparingen, efficiencyvoordelen en nieuwe verkoopkanalen vormen hierbij voor veel ondernemers een belangrijke drijfveer.

In dit artikel wordt aangegeven wat onder electronic commerce kan worden verstaan, wat de relatie met Internet is, welke ontwikkelingen zich op dit gebied afspelen en welke voordelen er door toepassing van electronic commerce kunnen ontstaan. Vervolgens wordt ingegaan op de grootste nog resterende barrière met betrekking tot electronic commerce, te weten het door gebruikers gestelde vertrouwen in de beveiliging van transacties en de wijze waarop deze barrière geslecht kan worden.

WAT IS ELECTRONIC COMMERCE?

Er is een groot aantal definities aangaande electronic commerce in omloop en deze variëren nogal. Enkele voorbeelden van definities zijn:

'Electronic commerce is zaken doen op afstand.' ([Louw98])

'Electronic commerce zijn alle vormen van transacties die gerelateerd zijn aan commerciële activiteiten, waarbij zowel organisaties als individuen betrokken zijn en die zijn gebaseerd op het verwerken en verzenden van gedigitaliseerde data.' ([OECD97])

'Electronic commerce is het geheel van zakelijke handelingen dat op elektronische wijze wordt uitgevoerd ter verbetering van de efficiency en de effectiviteit van bedrijfsprocessen.' ([ECPN98])

'Electronic commerce is geautomatiseerde aan commercie gerelateerde transacties.' ([Ford97])

Zoals mede uit bovenstaande blijkt bestaat er een groot aantal definities met betrekking tot electronic commerce. Het blijkt in de praktijk moeilijk om tot een eenduidige definitie van de term electronic commerce te komen. Als we uitgaan van de letterlijke vertaling van deze term komen we tot 'elektronische handel'.

We vervangen in deze vertaling de term elektronisch door digitaal omdat er over het algemeen een uitwisseling plaatsvindt van data in digitale vorm. Zodoende komen we dan tot 'het uitwisselen van digitale data voor handelsdoeleinden'; deze definitie zal in dit artikel ook als uitgangspunt worden genomen. Zij sluit ook beter aan op de voornaamste veroorzaker van de recente aandacht voor en de toename van het gebruik van de term electronic commerce, namelijk Internet.

ONTWIKKELINGEN

De toepassing en het belang van informatietechnologie (IT) in het algemeen en met name voor ondernemend Nederland neemt nog steeds toe. Dientengevolge groeit de IT-sector nog sterk. Een verdere voortzetting van deze trend wordt verwacht, voornamelijk ten aanzien van vier economische activiteiten. Het gaat om de volgende activiteiten die alle te maken hebben met of een voorbereiding zijn op de toepassing van electronic commerce ([DeCo98]).

Het bouwen aan het Internet

In 1994 maakten wereldwijd 3 miljoen mensen gebruik van Internet. In 1998 zijn dit naar verwachting 100 miljoen. De prognose is dat tegen het jaar 2005 er 1 miljard gebruikers van Internet zullen zijn. Deze groei zal een verdere verkoop van computers, software, communicatieapparatuur en de daarbij behorende dienstverlening met zich meebrengen ([IDC98]).

Omvang elektronische handel

De eerste bedrijven begonnen gemiddeld twee jaar geleden Internet te gebruiken voor commerciële transacties met zakelijke relaties. Deze eerste gebruikers meldden significante productiviteitstoenames die gerealiseerd werden door het gebruik van Internet voor het creëren, kopen, distribueren en verkopen van producten en diensten. De omvang van electronic commerce is moeilijk te meten en onvoorspelbaar mede vanwege de afbakening van het begrip zelf, de snelheid waarmee deze vorm van handel groeit en het feit dat veel ondernemingen zowel op conventionele wijze als via de digitale weg handel drijven. Verschillende prognoses wijzen echter in de richting van een wereldwijde omzet van 200 tot 300 miljard dollar rond de eeuwwisseling. Rond 2002 verwacht men dat er wereldwijd voor meer dan 300 miljard dollar verhandeld zal worden via Internet ([IDC98]).

Het digitaal leveren van goederen en diensten

Software, dagbladen, tijdschriften, muziek- en data-'cd's' hoeven niet langer gedrukt, verpakt en afgeleverd te worden bij winkels, huizen en bedrijven, maar kunnen direct in digitale vorm via het Internet geleverd worden. Ditzelfde geldt voor andere vormen van dienstverlening zoals verschillende vormen van onderwijs, medische diensten, bancaire diensten, consulting, en een grote verscheidenheid aan vormen van ontspanning via Internet.

De verkoop van tastbare goederen

Tot slot wordt het Internet ook in toenemende mate gebruikt om tastbare goederen en diensten te bestellen die – eventueel – op maat gemaakt thuis worden bezorgd via post of koerier. Ondanks het feit dat de verkoop van dit type product via Internet thans rond de één procent van de totale omzet van dit type product schommelt, toont de verkoop van deze producten via Internet een sterke groei.

Naar verwachting zal dus in de komende jaren het (zakelijk) gebruik van Internet aanzienlijk toenemen.

Alhoewel de cijfers verschillen gaan, zoals reeds vermeld, de meeste voorspellingen uit van een forse groei. Onderzoeksbureaus als Forrester, IDC en de Gartner Group voorspellen een omzet van de online verkoop tussen de 4,8 en 20 miljard dollar dit jaar. Schattingen met betrekking tot de wereldwijde electronic-commercemarkt in 2001 gaan uit van 220 miljard dollar omzet gegenereerd door 175 miljoen gebruikers. De cijfers voor Europa zijn respectievelijk 26 miljard dollar omzet bij 35 miljoen gebruikers ([IDC98]).

Ook uit trendonderzoek van KPMG in het Verenigd Koninkrijk blijkt dat zakendoen via Internet steeds meer in trek raakt bij bedrijven ([KMCU97]). Eén op de tien bedrijven maakt er inmiddels gebruik van en

Concurrentievoordeel en efficiencyverbetering worden als belangrijkste motieven voor zakendoen via Internet genoemd.

twintig procent van de bedrijven denkt erover na of experimenteert ermee. Het verwachte behalen van concurrentievoordeel en verbetering van de efficiency worden als de belangrijkste motieven gegeven.

VOORDELEN VAN ELECTRONIC COMMERCE

In het algemeen worden door bedrijven de volgende voordelen van Internet genoemd: een verbeterde informatievoorziening, een betere communicatie, een nieuwe manier van marktbenadering, een efficiëntere aflevering van het product bij de klant, en de mogelijkheid tot het benaderen van nieuwe klanten en markten.

Deze voordelen laten zich het beste toelichten aan de hand van een tweetal voorbeelden. Het eerste voorbeeld is afkomstig van de pakketdienst Federal Express (FedEx), het tweede is een voorbeeld van de computerfabrikant Dell. Van beide organisaties zal eerst een beeld geschetst worden van de electronic-commercetoepassing om vervolgens de concrete voordelen ervan aan te geven.

Federal Express

Federal Express is een internationale pakketdienst uit de Verenigde Staten. Hij gebruikt Internet in een aantal sleutelprocessen binnen zijn organisatie.

Al sinds het begin van de jaren tachtig geeft FedEx zijn klanten toegang tot zijn interne computersysteem, zodat deze zelf kunnen aangeven of er een pakket voor verzending kan worden afgehaald. Dit systeem bood later tevens een mogelijkheid tot automatisering van de aan de verzending gerelateerde documentenstroom.

In juli 1996 introduceerde FedEx InterNetShip©, waarmee een groot aantal diensten on line wordt aangeboden. Klanten kunnen een verzoek indienen om een pakket te komen afhalen, of kunnen de dichtstbijzijnde locatie traceren waar pakketten kunnen worden afgeleverd. Tevens kan men een breed scala van documenten laten printen zoals de packing-labels. Daarnaast kan men factureren en kan de status en locatie van een pakket worden opgevraagd door zowel de verzender als de ontvanger. Waar bij 'traditionele' automatisering het effectiever en efficiënter inrichten van de traditionele bedrijfsprocessen een doel op zich was, is hier sprake van externe, klantgerichte automatisering (uiteraard ook resulterend in kostenbesparing aan de zijde van FedEx) die tot wijziging in de front-office én als gevolg hiervan tot aanpassing van de back-office leidt.

De voordelen voor FedEx zijn ten eerste dat bepaalde kosten worden voorkomen doordat een groot deel van de routinewerkzaamheden is geautomatiseerd, dan wel van FedEx naar de klantzijde is verplaatst. Het afhalen van pakketten kan beter worden afgestemd op de behoefte van de klant omdat veel documenten nu door de klant zelf worden ingevuld en aangeleverd, en er is minder personeel nodig om telefonische verzoeken tot het afhalen van pakketten af te handelen.

Een tweede voordeel voor FedEx zijn de lagere kosten. Het systeem wordt door klanten van FedEx gebruikt om meer dan één miljoen pakketten per maand te traceren en het volume hiervan neemt sterk toe. Intern onderzoek van FedEx wijst uit dat bijna de helft van het traceren van deze pakketten anders door het call-center zou zijn uitgevoerd.

Een derde voordeel betreft een betere klantenservice. Klanten kunnen 24 uur per dag hun pakketten traceren en de voor hen relevante informatie opvragen. 950.000 klanten maken hier nu reeds gebruik van ([SEC98]).

Dell Computers

Dell Computers is fabrikant van desktopcomputers en gevestigd in de Verenigde Staten. Dell was één van de eerste firma's die PC's op maat bouwde en deze direct aan de eindgebruiker verkocht door gebruik te maken van telefonische verkoop en postorder.

Als één van de eerste bedrijven onderkende Dell de voordelen van Internet als retailkanaal. Klanten van Dell kunnen on-line PC's configureren en bestellen via de website van Dell ([wDell]). Daarnaast biedt de website mogelijkheden tot het verkrijgen van technische support, het downloaden van software en het door een klant zelf bekijken van de orderstatus van een bestelling.

Het merendeel van de klanten van Dell bestaat uit bedrijven. Dell maakt voor bedrijven specifieke pagina's aan op zijn site met voor dat bedrijf relevante informatie en de mogelijkheid tot het plaatsen van bestellingen.

Eén van de bedrijven die van deze service gebruikmaakt is MCI. MCI schat dat het vijftien procent heeft bespaard op de kosten die het normaal maakte bij de aanschaf van computers. Voorheen maakte MCI gebruik van zestien inkopers verspreid over vier verschillende locaties. MCI heeft alle aankopen wat betreft PC's samengevoegd en als gevolg van het volume een hogere korting weten te bedingen. Daarnaast werd de levertijd drastisch gereduceerd van vier à zes weken naar levering binnen 24 uur.

De voordelen voor Dell betreffen allereerst extra opbrengsten. Het blijkt dat zestig procent van de klanten die op de website van Dell een PC hebben besteld, nog niet eerder producten van Dell heeft afgenomen. Eén op de vier klanten geeft aan dat het bestaan van de website beslissend is geweest in het aankoopproces. Zonder deze website zouden zij dus niets van Dell hebben gekocht. Daarnaast is het bedrag dat wordt besteed aan aankopen via de website, gemiddeld hoger dan via de telefonische verkoop of postorder.

Een tweede voordeel betreft de lagere marketing- en verkoopkosten. De website van Dell biedt voldoende informatie om een klant door een aankoopproces te leiden. Als gevolg hiervan kan Dell meer verkoop genereren met minder personeel. Dell verwacht daarnaast dat ook de reclame-uitgaven voor Internet-gebruikers omlaag kunnen aangezien dertig procent van de klanten geen advertentie van Dell had gezien en toch tot aankoop overging.

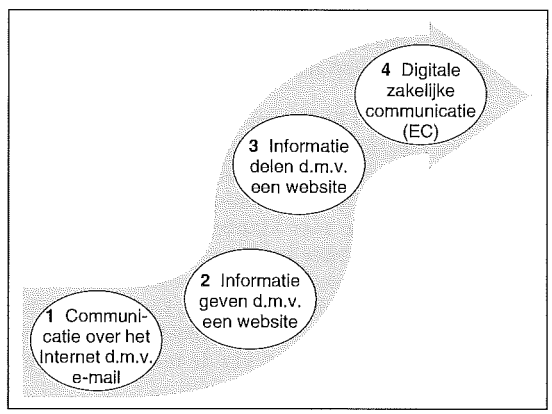
Een ander voordeel zijn de lagere servicekosten. Dell bespaart meerdere miljoenen dollars op jaarbasis door het on-line bieden van klantenservice en technische ondersteuning. Elke week wordt de status van de geplaatste order door 20.000 klanten opgevraagd. Een percentage hiervan zou normaal gesproken bij het call-center terecht zijn gekomen. Ditzelfde geldt voor de 30.000 klanten die software downloaden vanaf de website.

Een verbeterde klantenservice is een vierde voordeel. Dell ziet het Internet als middel om de relatie met de klant te verbeteren. De website maakt het op eenvoudige wijze mogelijk klanten individueel te benaderen en hierdoor de producten klantspecifiek op te leveren. De eerste keer dat de klant zijn computer opstart krijgt deze een configuratiespecifieke applicatie te zien die bedoeld is om klantspecifieke service en productaanbiedingen mogelijk te maken. Dell verwacht dat dit de tevredenheid bij klanten zal bevorderen en nieuwe verkoopmogelijkheden creëert. Voor het jaar 2000 wordt de helft van alle verkoopservice en ondersteuning on-line geleverd, zo verwacht men bij Dell.

Bovengenoemde voorbeelden illustreren de rol die Internet kan spelen bij het realiseren van efficiencyverbeteringen en het vergroten van de klantenservice. Hieronder worden zakelijke toepassingen van het Internet op een meer gestructureerde wijze weergegeven, waarbij er een ontwikkeling is waar te nemen van eenvoudige toepassingen tot een meer 'volwaardige' vorm van electronic commerce.

ZAKELIJKE TOEPASSINGEN VAN INTERNET

De ontwikkelingen die zijn te onderscheiden met betrekking tot de toepassing van Internet zijn volgens Hermans te verdelen in vier fasen. In de curve van figuur 1 worden deze weergegeven ([Herm97]).



Figuur 1. Internet-curve.

De vier fasen kunnen als volgt worden toegelicht.

Fase 1 en 2
In het algemeen starten ondernemingen met eenvoudige Internet-toepassingen als e-mail en het onderhouden van een informatieve (maar statische) website. Deze toepassingen zijn te beschouwen als 'een elektronische vertaling' van respectievelijk de fax en de productfolder.

Het merendeel van het huidige zakelijke Internetgebruik kan op dit moment worden gerangschikt onder deze eerste twee fasen.

Fase 3
In de derde fase is er sprake van het actief uitwisselen van informatie door middel van een (dynamische) website. Een voorbeeld van een dergelijke - meer innovatieve – toepassing van Internet is de dienst die vliegtuigfabrikant Boeing aanbiedt op haar website, waar klanten de beschikbaarheid van onderdelen kunnen opvragen ([Bww]).

Fase 4
Pas in de vierde fase van de ontwikkeling van Internet-toepassingen is er volgens Hermans sprake van het bedrijven van electronic commerce. In deze fase vinden er daadwerkelijk elektronische transacties plaats. Voorbeelden van toepassingen die zich in deze fase bevinden zijn naast de eerdergenoemde voorbeelden CDnow en Amazon waar respectievelijk cd's en boeken gekocht kunnen worden ([cdamw]). Interessant zijn de aanvullende diensten die op deze websites worden aangeboden. Op basis van een selectie van favoriete titels van de klant doet het systeem suggesties van titels die naar alle waarschijnlijkheid eveneens in de smaak zullen vallen. Daarnaast wordt de mogelijkheid geboden recensies van boeken te bekijken die zijn opgesteld door andere bezoekers van de site.

Het aantal concrete toepassingen in de derde en vierde fase is nog gering en het merendeel van de huidige toepassingen is afkomstig uit de Verenigde Staten. De voornaamste oorzaak voor het geringe aantal toepassingen in deze fasen ligt in het feit dat bij dit type toepassing meestal financiële transacties dienen te worden voltrokken of dat privacygevoelige of bedrijfsgevoelige informatie dient te worden verstrekt.

Het communiceren over een open netwerk als Internet, het plegen van (rechts)handelingen over het Internet en de transparantie van deze communicatie gaat op dit moment nog gepaard met de nodige argwaan en roept veel vragen op. De belangrijkste vragen houden verband met het al dan niet kunnen garanderen van betrouwbaarheid over een dergelijk netwerk. Zo komen we bij de belangrijkste voorwaarde om de potentiële voordelen van electronic commerce te kunnen benutten, de betrouwbaarheid.

VOORWAARDEN VOOR ELECTRONIC COMMERCE

In de hiervoor besproken voorbeelden komen enkele potentiële voordelen van electronic commerce naar voren, zoals kostenreductie en verbeterde service naar klanten. In veel gevallen, zoals het on line opvragen van de status van een geplaatste order bij Dell, gaat verbeterde klantenservice ook gepaard met een kostenreductie .

Om de (potentiële) voordelen die electronic commerce biedt ten volle te kunnen benutten moet echter een aantal belemmeringen worden weggenomen. Zowel op nationaal niveau als op internationaal

niveau (Organisation for Economic Co-operation and Development, Europese Unie, G7) wordt actie ondernomen om een gunstig klimaat ten behoeve van electronic commerce te scheppen. Er bestaat internationale consensus over de huidige belemmeringen aangaande electronic commerce. Voorts is de heersende mening, op zowel nationaal als internationaal niveau, dat deze belemmeringen, die in de economische, juridische en technische sfeer liggen, moeten worden weggenomen om electronic commerce verder van de grond te krijgen.

Belemmeringen van economische aard zijn bijvoorbeeld het ontbreken van een geaccepteerd betalingssysteem en de initiële investeringen en onzekerheid over de te genereren omzet aan de zijde van de aanbieder. Juridische onzekerheden betreffen zaken als cryptografie, de juridische status (inclusief bewijskracht) van digitale handtekeningen, vormvoorschriften die de toepassing van elektronische datacommunicatie kunnen belemmeren (deze onderwerpen worden behandeld in het artikel van Duthler en Dontje) en bescherming van intellectuele eigendomsrechten en privacy. Voorbeelden van technische belemmeringen ten slotte zijn technische standaardisatie en capaciteit van de infrastructuur (bandbreedte) ([MinEZ98a]).

Zoals hierboven al aangehaald is één van de belangrijkste voorwaarden waaraan electronic commerce moet voldoen, het realiseren van betrouwbare gegevensuitwisseling over Internet. De gevoeligheid voor fouten en misbruik van de elektronische systemen en infrastructuur die electronic commerce mogelijk maken, brengt een reële mogelijkheid tot schade voor de deelnemers met zich mee. Deze risico's kunnen worden voorkomen door het treffen van afdoende veiligheidsmaatregelen in combinatie met het ontwikkelen van organisatorische en juridische kaders.

Dat deze angst ook binnen het bedrijfsleven speelt blijkt onder meer uit het Electronic Research Report van KPMG uit het Verenigd Koninkrijk, waar uit een enquête onder honderd vooraanstaande bedrijven naar voren kwam dat beveiliging als grootste bedreiging c.q. belemmering voor het gebruik van Internet en dus voor de toepassing van electronic commerce werd gezien ([KMCU]).

Dat dit niet geheel ten onrechte is blijkt wel uit het feit dat tachtig procent van de door de FBI onderzochte computercriminaliteit betrekking heeft op Internet ([Icov95]).

Afdoende technische veiligheidsmaatregelen voor elektronisch berichtenverkeer zijn de afgelopen jaren ontwikkeld, zij het dat deze technieken en maatregelen voornamelijk worden gebruikt door militaire overheidsdiensten en binnen het bankwezen. Nog weinig ervaring is opgedaan met het op grote schaal invoeren van informatiebeveiligingstechnologie voor commerciële doeleinden. Daarnaast zullen er juridische en organisatorische aanpassingen en controles moeten worden ontwikkeld in samenhang met de bestaande beveiligingstechnologie.

Zoals verschillende malen in dit artikel is benadrukt, biedt electronic commerce vele voordelen, maar is het ook voor veel bedrijven en particulieren nog een

Betrouwbare gegevensuitwisseling over Internet is één van de belangrijkste voorwaarden voor electronic commerce.

relatief onbekend en onzeker verschijnsel. De deelnemer aan het elektronische verkeer zal voldoende zekerheden willen hebben ten aanzien van de betrouwbaarheid en veiligheid van deze manier van zakendoen, alvorens hij er (optimaal) gebruik van zal maken. De zakenpartner aan de andere kant van de computer is immers vaak een onbekende en hoe weet men zeker dat het verzonden bericht exclusief en integer bij de geadresseerde terechtkomt?

Betrouwbaarheid van Internet in het algemeen en electronic-commerceapplicaties in het bijzonder kan worden gerealiseerd door zogenaamde TTP-diensten. (Zie hiervoor ook het artikel van Duthler en Dontje verderop in deze Compact.) Deze TTP (Trusted Third Party)-diensten faciliteren een verdere doorbraak van electronic commerce en het wijdverspreide gebruik ervan door bedrijven en particulieren.

Een Trusted Third Party is een onafhankelijke en deskundige derde partij, die aan partijen die gebruikmaken van elektronisch dataverkeer zogenaamde betrouwbaarheidsdiensten kan aanbieden. Zij kan garanties afgeven ten aanzien van de identiteit van de verzender en de ontvanger (digitale handtekening), het tijdstip van verzending en ontvangst (tijdstempelfunctie) en de integriteit en de exclusiviteit van de berichtgeving (sleutelbeheerfunctie). Ook kan de TTP diensten verlenen ten aanzien van de bewijslevering van het bestaan van overeenkomsten (poststempelfunctie) en ten behoeve van auteursrechtelijke bescherming.

Het belang van TTP-diensten blijkt onder meer uit de Eindrapportage van het Nationaal TTP-project uitgevoerd door het Ministerie van Economische Zaken en Verkeer en Waterstaat. Hierin wordt gesteld dat de ontwikkeling van TTP-diensten lijkt te wachten op een verdere ontwikkeling van electronic commerce, terwijl een verdere groei van electronic commerce juist afhankelijk lijkt te zijn van de beschikbaarheid van een dergelijke TTP-infrastructuur ([MinEZ98b]).

De Gartner Group noemt als belangrijkste randvoorwaarden voor de ontwikkeling van electronic commerce vertrouwelijkheid, integriteit, authenticatie en onweerlegbaarheid van het elektronisch berichtenverkeer ([Gartn97]). Verwacht wordt dat de rol van Trusted Third Parties dan ook alleen maar zal toenemen, onder meer daar waar het gaat om sleutelbeheer en certificatiediensten.

Tot slot doet ook de International Data Corporation in dit kader vergelijkbare uitspraken. Een IDC-studie toonde belemmeringen aan in de groei van electronic commerce in Engeland, die met name worden veroorzaakt door een te geringe beveiligingsgraad. Hier zou een TTP uitkomst kunnen bieden. Daar-

Drs. A.J. Biesheuvel RA RE
Is directeur van KPMG TTP Services. Hij adviseert bedrijven over de toepassing van electronic commerce. Hij studeerde informatica en bedrijfseconomie aan de Rijksuniversiteit Groningen. In 1991 heeft hij zijn registeraccountancydiploma behaald.

Drs. C.F. Olde Olthof
Is sinds 1997 consultant bij KPMG TTP Services. Zijn aandachtsgebied ligt op het vlak van de verschillende vormen van informatie- en telecommunicatietechnologie in relatie tot bedrijfskundige vraagstukken. Hiervoor studeerde hij de IT-variant bedrijfskunde aan de Rijksuniversiteit Groningen.

naast voorziet IDC de noodzaak van handelsstandaarden, en ziet zij een rol weggelegd voor Trusted Third Parties daar waar het gaat om het arbitreren van de electronic-commercetransacties.

CONCLUSIE

Electronic commerce biedt een groot aantal voordelen. Het is sneller en effectiever dan de conventionele manieren van handel drijven. Electronic commerce versnelt en verbetert communicatie, het verzamelen van informatie en het drijven van handel tussen bedrijven onderling en tussen bedrijven en consumenten. Omdat de verwachte impact van electronic commerce groot zal zijn en het steeds verder doordringt in de internationale handel, kunnen bedrijven het zich amper veroorloven dit te negeren. Het gebrek aan vertrouwen, de grootste nog bestaande barrière bij het realiseren van veilige electronic commerce, kan door gebruik te maken van TTP-diensten weggenomen worden. Waardoor weinig de toekomst van veilige electronic commerce nog in de weg staat.

LITERATUUR

[Bww] Url: http://www.boeing.com

[cdamw] Url's http://www.cdnow.com en http://www.amazon.com

[DeCo98] Department of Commerce Washington, D.C., *The Emerging digital economy*, Washington 1998. Url: http://www.ecommerce.gov

[ECPN98] Electronic Commerce Platform Nederland, 1998. Url: http://www.ecp.nl

[Ford97] W.Ford en M.S. Baum, *Secure Electronic Commerce; building infrastructures for digital Signatures and Encryption*, Prentice Hall, New Jersey 1997.

[Gartn97] Gartner, *Establishing an Internet Security Plan for Electronic Commerce*, 30 oktober 1997. Url: http://www.gartner.com

[Herm97] J.A.M Hermans, *PKI for your organization*, Flyer; KPMG TTP Services, KPMG Rotterdam, 1997.

[IDC98] International Data Corporation. Cijfers zijn afkomstig uit diverse rapporten van International Data Corporation (IDC #B13855, #101DB, #H02DB) en zijn gebaseerd op het door haar ontwikkelde Internet Commerce Market Model. Url : http://www.idc.com

[Icov95] David Icove et al., *Computer Crime*: A Crimefighter's Handbook, p.129, 1995.

[KMCU97] KPMG Management Consulting UK, *Electronic Commerce Research Report 1997*, KPMG London 1997.

[Louw98] C.J.M. de Louw, *Elektronische marktplaats*, Informer, thema 'Electronic commerce', jaargang 2, nr. 1/2, februari 1998, Ten Hagen & Stam, Den Haag.

[MinEZ98a] Ministerie van Economische Zaken, *Actieplan Electronic Commerce*, maart 1998. Url: http://info.minez.nl/pdfs/05r38.pdf

[MinEZ98b] Ministerie van Economische Zaken en Ministerie van Verkeer en Waterstaat, *Eindrapportage Nationaal TTP-project*, april 1998.

[OECD97] *OECD, Policy Brief; electronic commerce, no 1, OECD 1997.* Url: http://www.oecd.org.publications/Pol_brief/9701_Pol.htm

[SEC98] Secretariat on Electronic Commerce, U.S. Department of Commerce Washington, *Electronic Commerce Between Business Analysis and Case Studies*, Washington 1998.

[wDell] Url: http://www.dell.com

Oplossingen voor veilige electronic commerce over Internet

R.L. Moonen

Vanuit een technische invalshoek worden oplossingen voor veilig elektronisch zakendoen geschetst. Platformonafhankelijke oplossingen met betrekking tot netwerkbeveiliging, continuïteit en message services. Ook wordt een overzicht gegeven van verschillende cryptografische technieken.

INLEIDING

Zoals we in het voorgaande artikel hebben kunnen lezen, staat electronic commerce (e-commerce) volop in de belangstelling. Het wordt gezien als een potentieel middel om een grotere klantenkring te benaderen, sneller en goedkoper zaken te doen en diensten te leveren die wellicht op traditionele wijze niet mogelijk zijn. Drijvende kracht achter het opkomende e-commerce is het Internet.

Met name door het mondiale karakter van Internet en de ontwikkelingen op technisch gebied wordt langzaam maar zeker duidelijk dat het Internet een belangrijk medium voor e-commerce zal worden en dat het een mooie toekomst te wachten staat.

Voordat leveranciers van goederen en diensten echter op veilige wijze handel over Internet kunnen drijven, dient aan een aantal basisbehoeften met betrekking tot netwerkbeveiliging, continuïteit en message services voldaan te worden. Message services verzorgen de vertrouwelijkheid van informatie, identificatie, authenticatie en onweerlegbaarheid.

Door een combinatie van moderne cryptografische technieken en uitgekiende netwerkkoppelingen kan aan deze voorwaarden worden voldaan. Hoewel veel van deze technieken nog in ontwikkeling zijn en standaardoplossingen niet voorhanden zijn, biedt een aantal van deze technieken uitstekende perspectieven voor het drijven van betrouwbare handel via publieke netwerken als Internet.

Met name de ontwikkelingen op het gebied van message services zijn in een stroomversnelling geraakt nu een aantal leveranciers concrete producten met ondersteuning van en aan ontwikkelaars op de markt heeft gebracht.

In de navolgende paragrafen zal worden ingegaan op een aantal platformonafhankelijke technische oplossingen met betrekking tot netwerkbeveiliging, continuïteit en message services.

NETWERKBEVEILIGING

Het versturen van informatie over Internet gebeurt door middel van de TCP/IP protocolset (zie Compact 1994/1). Deze protocolset voorziet in de basisbenodigdheden voor datacommunicatie. Zij verzorgt unieke adressen, een zekere mate van betrouwbaarheid van berichtenoverdracht, en transportcontrole. Indien echter toegang tot applicaties over Internet vereist is, zoals bij e-commerce mogelijk het geval is, spelen ook andere zaken een rol.

Ten eerste is vaak beheersbare toegang tot interne bedrijfsgegevens nodig. Omdat geen directe toegang door derden tot de interne IT-infrastructuur is gewenst, dient ter beveiliging een scheiding te worden gerealiseerd tussen het Internet en het bedrijfsnetwerk.

Ten tweede dient de gegevensoverdracht te voldoen aan hoge eisen met betrekking tot continuïteit, zekerheid van identiteit (zowel van klant als van leverancier) en vertrouwelijkheid van informatie. Bij financiële transacties is daarbij tevens de onweerlegbaarheid van de transactie van groot belang ([Duni98]).

Het implementeren van een veilige, gescheiden netwerkomgeving gebeurt in de praktijk veelal door middel van firewalls (zie Compact1994/2). Hierbij voorziet een samenstel van technische en beheersmatige beveiligingsmaatregelen in de scheiding van informatiestromen. Een combinatie van componenten als routers, mailservers en een firewall host waarop filters zijn geïmplementeerd, waarborgt dat externe toegang slechts mogelijk is van en naar specifiek toegewezen, geïsoleerde netwerkdelen waarop de applicaties draaien waartoe externe toegang dient te worden verleend.

De routers fungeren hierbij als eerste defensie en filteren ongewenst of ongeautoriseerd verkeer op basis van afkomst of bestemming. Zo mag bijvoorbeeld verkeer dat een afzendadres heeft dat binnen het interne netwerk ligt maar toch van buiten komt, niet toegelaten worden. Dergelijk verkeer bevat kennelijk een vervalst afzendadres, en de kans bestaat dat dit verkeer met kwade bedoelingen geïnjecteerd is.

De firewall host (ook wel bastion host genoemd) beschikt meestal over applicatielaagfilters die inhoudelijke filtering verzorgen (bijvoorbeeld het tegenhouden van Java-applets of e-mails die virussen bevatten). De bastion host fungeert tevens als detectiemechanisme voor ongeautoriseerd verkeer dat onverhoopt toch door de filters van de eerste router is gekomen.

Deze maatregelen zorgen ervoor dat de andere delen van het bedrijfsnetwerk zijn beschermd tegen ongeautoriseerde toegang van buitenaf. Vanuit het interne bedrijfsnetwerk is transparant toegang mogelijk tot deze geïsoleerde netwerkdelen en het Internet. Dit wil zeggen dat interne geautoriseerde gebruikers geen verschil zien tussen een directe aansluiting op het Internet en een aansluiting via een firewall.

Hiermee is echter nog niet voldaan aan de eisen met betrekking tot continuïteit en message services. De mate waarin aan deze eisen wordt voldaan, zijn van doorslaggevend belang voor het slagen van e-commercetoepassingen. Gegeven het belang van deze eisen zijn maatregelen geboden op de vlakken vertrouwelijkheid, identiteit, authenticatie en onweerlegbaarheid.

Tevens dienen additionele beschermende maatregelen te worden getroffen om de continuïteit te waarborgen. Omdat bovenstaande eisen algemeen worden beschouwd als van kritiek belang, hebben diverse leveranciers toepassingen op de markt gebracht of ondersteund die door middel van technische maatregelen pogen te voldoen aan deze eisen. Hieronder wordt per criterium ingegaan op toepassingen en mogelijke technische maatregelen.

CONTINUÏTEIT VAN BESCHIKBAARHEID

Vanwege het mondiale karakter van Internet zal een e-commercedienst bij voorkeur 24 uur per dag beschikbaar dienen te zijn. Naast goed beheer van de systemen is beveiliging tegen aanvallen die pogen diensten onbeschikbaar te maken daarom van groot belang. Laatstgenoemde aanvallen worden ook wel denial-of-service-aanvallen genoemd. Dergelijke denial-of-service-aanvallen vinden op het Internet in toenemende mate plaats.

De leveranciers van platformen treffen in voorkomende gevallen maatregelen en stellen die in de vorm van 'patches' en 'fixes' beschikbaar om apparatuur tegen zulke aanvallen te beschermen. Patches en fixes zijn tussentijdse en vaak tijdelijke verbeteringen van elementen van het besturingssysteem waar fouten in ontdekt zijn. Indien een fout ('bug') consequenties heeft voor de veiligheid van de componenten is het vaak niet mogelijk te wachten op de nieuwe versie van de software of het besturingssysteem.

Het is daarom van belang het beheer van de netwerkkoppelingen en e-commercetoepassingen zodanig in te richten dat installatie van deze patches en fixes tijdig en adequaat plaatsvindt. Daarnaast dient de filtering op de componenten van de firewall zodanig te zijn ingesteld dat dergelijke denial-of-service-aanvallen tijdig worden gedetecteerd en adequate maatregelen kunnen worden getroffen.

MESSAGE SERVICES

Onder message services wordt verstaan het verzorgen van vertrouwelijkheid, identificatie, authenticatie en onweerlegbaarheid ten behoeve van elektronisch berichtenverkeer. Met name onweerlegbaarheid is van belang bij transacties. Deze diensten zijn in de diverse verkrijgbare applicaties gebaseerd op moderne cryptografische technieken. (Zie de Toelichtingen aan het eind van dit artikel.)

Toepassing van deze technieken kan echter resulteren in schijnveiligheid, indien de implementatie niet foutvrij is. Als de implementatie niet degelijk is, kan net als bij een gammel slot op een huis alsnog rela-

tief eenvoudig ('economisch rendabel') een inbraak worden gepleegd. Fouten worden in de praktijk in de hand gewerkt door de snelle ontwikkelingen en de wens van fabrikanten om een product zo snel mogelijk op de markt te brengen. De resulterende veiligheid van de diverse specifieke implementaties is daarom van wisselend niveau.

In de volgende subparagrafen zullen de diverse message services worden toegelicht.

Vertrouwelijkheid

Vanwege het conflict tussen de publieke aard van het Internet en de vertrouwelijke aard van zakelijke transacties zijn maatregelen geboden ter bescherming van de vertrouwelijkheid van de gegevensoverdracht. Omdat het thans gebruikte TCP/IP-protocol hierin niet voorziet, dienen extra maatregelen te worden getroffen in de vorm van encryptie.

Encryptie houdt in het versleutelen van de gegevens voordat zij verstuurd worden. In het geval van e-commerce dient deze versleuteling in de meeste gevallen real-time plaats te vinden, waardoor additionele eisen met betrekking tot performance en capaciteit geïntroduceerd worden. Het opzetten van een verbinding waarbij alle gegevens van begin tot eindpunt versleuteld zijn maar de verbinding op applicatieniveau transparant is, wordt 'tunneling' genoemd.

Door tunnelingtechnieken toe te passen kunnen Virtual Private Networks (VPN's) worden gerealiseerd over publieke netwerken. Overigens wordt thans gewerkt aan de implementatie van een nieuwe set TCP/IP-protocollen waarbij encryptie wél een onderdeel is van de specificaties. Het Internet Engineering Taskforce (IETF) heeft hiertoe de IPsec-standaard ontwikkeld. Deze nieuwe standaard laat ontwikkelaars vrij om zelf de wijze van encryptie te kiezen maar voorziet in een mechanisme om op uniforme wijze versleutelde verbindingen tot stand te brengen.

Identificatie en authenticatie

Naast vertrouwelijkheid van informatie bij zakelijke transacties is zekerheid van identiteit een andere kritieke factor. Als leverancier van e-commercediensten is het noodzakelijk te weten met wie zaken gedaan worden, en als afnemer wil men zekerheid hebben over de identiteit van de leverancier. Zijn de transactiepartners wel wie zij beweren te zijn?

Om websites dit vertrouwen te geven, zijn digitale certificaten een mogelijkheid. Deze met cryptografische technieken gemerkte labels leveren zekerheid over de identiteit (en daarmee tot op zekere hoogte over de betrouwbaarheid) van de transactiepartner. Echter, deze certificaten moeten worden uitgegeven door een bron die op zich te vertrouwen is, en de overdracht moet op een veilige, niet-afluisterbare wijze plaatsvinden. Een dergelijke bron, Certification Authority (CA), levert zekerheid over de identiteit van de tegenpartij. Diverse instellingen hebben zich opgeworpen als CA, waaronder Verisign, Eurosign en CompuSource[1].

Een kanttekening hierbij is dat gebruikers die bij het bezoeken van een website een certificaat getoond krijgen, goed op de hoogte moeten zijn van de functie en inhoud ervan. Indien gebruikers hiervan niet op de hoogte zijn, is misleiding door het verstrekken van valse certificaten een reële bedreiging. Certificaten bieden naast zekerheid over de identiteit van de server ook zekerheid over de identiteit van de client. In het geval van Secure Sockets Layer (SSL) vindt tijdens de verbindingsopbouw authenticatie plaats van servers en client op basis van certificaten. Kanttekening is dat certificaten wel op een betrouwbare wijze moeten zijn uitgereikt, opdat een certificaat bindend is aan een entiteit (server én client).

Naast authenticatie door middel van certificaten bestaan ook cryptografische authenticatieprotocollen als CHAP (Challenge Handshake Authentication Protocol) en Radius. Deze protocollen voorzien in op sterke cryptografische algoritmen gebaseerde authenticatie met gebruik van wachtwoorden. Zij zijn echter minder geschikt voor het identificeren van websites, en worden in het algemeen meer gebruikt voor het identificeren van gebruikers bij het inloggen op een beveiligde server via Internet.

Een nadeel van deze technieken is dat de wachtwoorden veelal onversleuteld opgeslagen zijn aan de clientzijde, en vatbaar zijn voor woordenboekaanvallen, waarbij de tot een uitgebreide set behorende veelgebruikte wachtwoorden één voor één geprobeerd worden.

Onweerlegbaarheid en integriteit

Bij het doen van transacties is tevens de onweerlegbaarheid van de transactie van belang. Het moet niet mogelijk zijn te ontkennen dat het bericht verstuurd of ontvangen is of op andere wijze de inhoud of identiteit van afzender in twijfel te trekken. Deze onweerlegbaarheid, of non-repudiation, wordt bereikt door toepassing van asymmetrische encryptie en eventuele ontvangstbevestiging met behulp van een unieke 'vingerafdruk' van het oorspronkelijke bericht. Zie voor een nadere uitleg van deze technieken de Toelichtingen aan het eind van dit artikel.

Naast het niet kunnen ontkennen van verzending of ontvangst van een bericht, dient ook zekerheid te bestaan over de inhoud van een bericht. De inhoud mag bij aankomst niet verschillen van de inhoud zoals die is verstuurd. Deze integriteitscontrole is veelal opgenomen in de implementaties die hieronder besproken worden.

Veilige message services = veilig zakendoen op Internet

Indien de identiteit van de transactiepartner bekend is en de gegevens versleuteld worden getransporteerd, en beschermd zijn tegen invloeden van buitenaf, dan kunnen transacties met adequate zekerheid worden uitgevoerd over het Internet. Door verschillende fabrikanten worden deze message services nu gecombineerd in oplossingen die steeds meer aan invloed winnen.

Hieronder zal worden ingegaan op een aantal van de meest veelbelovende en breed inzetbare toepassingen die gebruikmaken van verschillende combinaties van authenticatie, encryptie en tunnelingprotocollen.

1 Zie ook het artikel over TTP's in deze Compact.

IMPLEMENTATIES

De navolgende implementaties verzorgen message services ten behoeve van communicatie over TCP/IP-netwerken. In de toelichting zal bij elke implementatie worden ingegaan op de specifieke message services die ondersteund worden. Merk op dat niet alle implementaties de volledige set message services ondersteunen, waardoor het toepassingsgebied van de implementaties beperkt kan zijn. Tevens is van belang op te merken dat recentelijk een aantal zwakheden geïdentificeerd is in enkele van de implementaties. Indien van toepassing zullen deze zwakheden kort worden toegelicht. De in de tabellen genoemde encryptiemethoden als RC4, DES en RSA worden in de Toelichtingen nader uitgelegd.

PPTP

Recentelijk heeft een aantal leveranciers zijn steun gegeven aan het Point-to-Point Tunneling Protocol (PPTP) ([Hamz96]). De eerste PPTP-implementaties zijn specifiek gericht op toegang tot Windows NT-servers op basis van Remote Access Server (RAS). De PPTP-implementatie grijpt binnen het OSI-lagenmodel in op het niveau tussen de sessielaag en de transportlaag. Hierdoor is transparante communicatie tussen de applicatielagen gegarandeerd. PPTP bezit de volgende karakteristieken:

Tabel 1 (links). Karakteristieken van PPTP.

Message service	Aanwezig	Implementatie
Vertrouwelijkheid	ja	Door RAS ondersteunde symmetrische encryptie, waaronder Redundant Cipher 4 (RC4).
Identificatie en authenticatie	ja	Door RAS ondersteunde protocollen, waaronder CHAP.
Onweerlegbaarheid en integriteitscontrole	nee	

Tabel 2 (rechts). Karakteristieken van SSL.

Buiten deze message services wordt betrouwbaarheid van transport verder versterkt door periodiek een nieuwe 'handshake' en authenticatieronde plaats te laten vinden.

Een mogelijke zwakheid van RC4 is de binnen PPTP vastgestelde beperkte sleutellengte. PPTP gebruikt 40-bits-sleutels waardoor export uit de Verenigde Staten is toegestaan[2], maar niet de zekerheid wordt geboden die 128-bits-implementaties van Secure Sockets Layer (SSL, zie hieronder) bijvoorbeeld wel bieden. Bovendien wordt bij veel implementaties van PPTP geen willekeurige sleutel gebruikt, waardoor het aantal potentiële sleutels significant minder is dan 2^{40} (het aantal combinaties dat met 40 bits mogelijk is). Hierdoor neemt de haalbaarheid van het 'kraken' van PPTP door uitputtende doorzoeking van alle potentiële sleutels toe.

Een verdere beperking van de bruikbaarheid van PPTP is het feit dat het om een point-to-pointverbinding gaat, waardoor koppeling van LAN's over het Internet niet mogelijk is. Desalniettemin resulteert de combinatie van de cryptografische technieken die PPTP benut in een redelijk veilige verbinding met brede ondersteuning door ontwikkelaars van applicaties. Hierbij dient opgemerkt te worden dat de momenteel meest gebruikte implementatie van PPTP een dermate grote hoeveelheid zwakheden blijkt te bevatten, dat deze voor kritische applicaties in feite onbruikbaar is geworden. De zwakheden die thans geïdentificeerd zijn, zijn niet inherent aan PPTP, maar zijn alle fouten in de implementatie ervan.

SSL v3.0

Secure Sockets Layer (SSL) versie 3.0 ([Nets96]) is het protocol dat momenteel de breedste acceptatie ondervindt in de Internet-gemeenschap, vanwege de brede ondersteuning door softwareontwikkelaars en het open karakter. SSL grijpt binnen het OSI lagenmodel in op het niveau tussen de sessielaag en de transportlaag. Hierdoor is transparante communicatie tussen de applicatielagen gegarandeerd. SSL heeft de volgende karakteristieken:

Message service	Aanwezig	Implementatie
Vertrouwelijkheid	ja	Symmetrische encryptie: DES, RC4.
Identificatie en authenticatie	ja	Asymmetrische encryptie: RSA of DSS ter uitwisseling van sleutels ten behoeve van symmetrische encryptie en verificatie van certificaten.
Onweerlegbaarheid en integriteitscontrole	ja	Integriteitscontrole door asymmetrische encryptie en MAC's op basis van MD5 of SHA. Onweerlegbaarheid is gedeeltelijk ondersteund, maar niet sterk genoeg voor kritische applicaties.

Naast het feit dat er gratis implementaties van SSL bestaan, biedt SSL de keus uit verschillende sleutellengten voor verschillende toepassingen. Naast 40-bits-sleutels is voor de Amerikaanse markt een 128-bits-versie beschikbaar. Populaire browsers ondersteunen standaard de 40-bitsversie. Ter authenticatie worden certificaten gebruikt, uitgegeven door CA's en ondertekend met behulp van cryptografische public-keytechnieken.

SSL is voorgedragen voor acceptatie door het IETF als officiële Internet-standaard en de verwachting is dat deze voordracht zal worden geaccepteerd. Daarnaast is een public domain library (SSLeay) beschikbaar voor ontwikkelaars van applicaties.

Eén van de problemen is dat SSL onvoldoende maatregelen biedt voor onweerlegbaarheid. Als sprake is van key-backup van de private keys van de gebruiker is het niet mogelijk non-repudiation te waarbor-

2 Vreemd genoeg is export van de broncode van cryptografiesoftware met implementaties met meer dan 40 bits *op papier* wel toegestaan. Op diverse Europese Internet-sites in het grijze circuit zijn daaruit ontwikkelde 128-bits-implementaties beschikbaar. Deze mogen echter weer niet worden gebruikt door organisaties die binding hebben met organisaties in de Verenigde Staten.

gen aangezien SSL gebruikmaakt van één sleutelpaar voor zowel een digitale handtekening (onweerlegbaarheid) als encryptie.

Fortezza

Fortezza is een door een Amerikaanse veiligheidsdienst (de National Security Agency) ontwikkelde toepassing, gebaseerd op het Skipjack-encryptiealgoritme ([CSRC98]) (bekend van de Clipper Chip) dat gebruikmaakt van 80-bits-sleutels. Om een zo groot mogelijke acceptatie van dit systeem te bevorderen heeft men er recentelijk voor gekozen het Skipjack algoritme vrij te geven. Tot juni 1998 was dit algoritme geheim.

Vermoed werd dat de reden voor geheimhouding was dat de Amerikaanse overheid een toegangsmogelijkheid voor justitiële en opsporingsdiensten had ingebouwd, en men niet wilde dat bekend werd hoe deze 'achterdeur' kon worden omzeild. Vele experts hebben deze beslissing echter bekritiseerd vanwege het ontbreken van controle op de intrinsieke veiligheid van het algoritme en zijn verheugd met de uiteindelijke vrijgave.
Het algoritme wordt thans door experts aan een grondig onderzoek onderworpen om inzicht te krijgen in de veiligheid van het algoritme. Skipjack is een symmetrische cipher, met 80-bits-sleutels.

Message service	Aanwezig	Implementatie
Vertrouwelijkheid	ja	Skipjack, in combinatie met het Key Exchange Algorithm.
Identificatie en authenticatie	ja	Asymmetrische encryptie: DSA.
Onweerlegbaarheid en integriteitscontrole	ja	Asymmetrische encryptie in combinatie met MAC's op basis van SHA.

Tabel 3.
Karakteristieken van Fortezza.

Fortezza is een flexibel systeem dat op veel verschillende vlakken kan worden ingezet. Momenteel worden naast Internet-gerelateerde Fortezza-applicaties tevens Fortezza-modems, netwerkkaarten, routers en mobiele telefoons ontwikkeld. Voor Internet-toepassingen geldt dat Fortezza op een aantal manieren kan worden geïmplementeerd, ieder met specifieke zwakheden en toepassingsgebieden. In tabel 4 worden deze toepassingsmogelijkheden en relatieve zwakheden weergegeven.

IPsec

IPsec ([IETF98]) is de door de IETF ontwikkelde standaard, die in de toekomst TCP/IP gedeeltelijk zal gaan vervangen. Het grote verschil met de hiervoor genoemde implementaties is dat IPsec op de netwerklaag ingrijpt en niet tussen de sessielaag en transportlaag. Hierdoor kunnen VPN's gebouwd worden door toepassing van IPsec ondersteunende communicatie-apparatuur, en behoeven de hoger gelegen protocollen geen aanpassing. Hoewel de IPsec-standaard in principe geen algoritmen voorschrijft, maar slechts een mechanisme aanbiedt waarin deze functionaliteit opgenomen kan worden, hebben de bestaande implementaties van IPsec veelal de volgende karakteristieken:

Message service	Aanwezig	Implementatie
Vertrouwelijkheid	ja	Symmetrische encryptie: DES (hoewel andere algoritmen ondersteund worden door IPsec).
Identificatie en authenticatie	ja	Asymmetrische encryptie: na uitwisseling van sleutels volgens het Internet Security Association and Key Management Protocol (ISAKMP/Oakley) volgt authenticatie door middel van certificaten.
Onweerlegbaarheid en integriteitscontrole	ja	Asymmetrische encryptie in combinatie met MAC's op basis van SHA of MD5. Onweerlegbaarheid geldt alleen voor sleuteluitwisseling, niet voor inhoud van verdere communicatie.

Tabel 5.
Karakteristieken van IPsec.

Product	Bescherming van sleutels en identiteit	Beveiligingseigenschappen	Bruikbaar in omgevingen
Software Fortezza	Zwak	Zwakke authenticatie; beperkte zekerheid over data-integriteit; beperkte zekerheid over vertrouwelijkheid.	Met weinig tot geen bedreigingen; waar authenticatie niet vereist is; waar vertrouwelijkheid van ondergeschikt belang is.
Smart Card Fortezza	Sterk, beperkt door technologie	Sterke authenticatie; zekerheid over data-integriteit; beperkte zekerheid over vertrouwelijkheid.	Met enige bedreigingen; waar zekerheid over identiteit vereist is; waar vertrouwelijkheid van ondergeschikt belang is.
Fortezza PCMCIA-card	Sterk	Sterke authenticatie; zekerheid over data-integriteit; zekerheid over vertrouwelijkheid.	Waar ernstige bedreigingen bestaan; waar zekerheid over identiteit vereist is; waar vertrouwelijkheid vereist is.

Tabel 4.
Fortezza-implementaties, eigenschappen en toepasbaarheid.

R.L. Moonen
Is als EDP-auditor werkzaam bij KPMG EDP Auditors. Zijn aandachtsgebied ligt voornamelijk bij Internet-beveiliging en Unix-systeem-beveiliging. Hij is betrokken bij audit- en adviesopdrachten inzake beveiliging en Internet-penetratietests.

Door de plaatsing in het OSI-lagenmodel is de verwachting dat IPsec met name gebruikt zal gaan worden in omgevingen waar LAN-to-LAN-verbindingen over publieke netwerken gewenst zijn. Het gebruik van IPsec ten behoeve van e-commerce zal daarom vooralsnog beperkt blijven tot gevallen waarin organisaties dermate veel samenwerken dat een VPN uitkomst biedt. IPsec wordt namelijk nog niet ondersteund door operating systemen voor PC-platformen. Wel bestaat er, net als voor SSL, een public domain library en API (in broncodevorm) waardoor ontwikkeling van IPsec-producten voor open omgevingen op vrij eenvoudige wijze mogelijk is.

TOT SLOT

De verschillen tussen de diverse protocollen en de ondersteuning ervan vanuit de markt, beperken in de praktijk de keuzemogelijkheden. Een website met een groot aantal bezoekers stelt andere eisen aan de gebruikte implementatie dan een applicatieserver met een beperkt aantal bekende gebruikers.

Daarnaast bestaan grote prijsverschillen tussen de diverse implementaties. Het is daarom van belang een gedegen analyse uit te voeren van deze factoren voordat wordt gekozen voor een specifieke implementatie. Desalniettemin kan met de geboden toepassingen in de meest voorkomende gevallen adequaat worden voldaan aan de eisen die veilige e-commerce over publieke netwerken stelt.

LITERATUUR

[CSRC98] Computer Security Resource Clearinghouse, *SKIPJACK en KEA Algorithm Specifications V2.0*, http://csrc.nist.gov/encryption/skipjack-1.pdf, Computer Security Resource Clearinghouse, mei 1998.

[Duni98] Tom Dunigan, *Tom Dunigans' security page*, http://www.epm.ornl.gov/~dunigan/security.html, Tom Dunigan, juli 1998.

[Hamz96] Hamzeh, Pall, Verthein, Taarud, Little, *Point to Point Tunneling Protocol*, http://infodeli.3com.com/infodeli/tools/remote/general/pptp/draft-00.pdf, IETF draft, juni 1996.

[IETF98] Internet Engineering Taskforce, *IP Security Protocol*, http://www.ietf.cnri.reston.va.us/html.charters/ipsec-charter.html, Internet Engineering Taskforce, april 1998.

[Nets96] Netscape Communications Corp, *SSL 3.0 SPECIFICATION*, http://home.netscape.com/eng/ssl3/index.html, Netscape Communications Corp., november 1996.

[Rain95] Rainbow Technologies, *FORTEZZA Cryptologic Interface Programmers Guide for the Fortezza Crypto Card*, http://www.rnbo.com/PROD/rmadillo/e/etoc.htm, Rainbow Technologies, mei 1995.

TOELICHTINGEN

In onderstaande kaders wordt een overzicht en uitleg gegeven van verschillende cryptografische technieken.

Toelichting 1a. Cryptografische technieken: symmetrisch.

De ontwikkeling van cryptografische technieken is de laatste jaren in een stroomversnelling gekomen. Door de toenemende kracht van computers dienen cryptografische algoritmen (ciphers) mathematisch steeds sterker te zijn. Hiermee wordt bedoeld dat decodering (decryptie) van versleutelde berichten zonder bekende sleutel een bijzondere inspanning vereist, zo niet praktisch onmogelijk is; de benodigde inspanning daalt echter snel met het voortschrijden van de techniek, waardoor de gebruikte algoritmen aan continue verandering onderhevig zijn.

Symmetrische versus asymmetrische algoritmen en hashing

Voor versleuteling (encryptie) en transport van versleutelde data zijn diverse technieken beschikbaar. Deze technieken zijn onder te verdelen in een aantal categorieën, ieder met bepaalde kenmerken.
Een versleuteling is een wiskundige functie uitgevoerd op data, zodanig dat herhaling van de functie de oorspronkelijke data oplevert. Hierbij heeft de functie één of meer parameters, keys genaamd, die de exacte werking en uitkomst van de functie bepalen.

Symmetrische encryptie

Een symmetrische cipher heeft als kenmerk dat voor encryptie en decryptie dezelfde key (sleutel) wordt gebruikt:

$F_s(M_p, \text{key}) = M_c$ en $F_s(M_c, \text{key}) = M_p$, waarbij:

F_s symmetrische cipherfunctie
M_p plaintext message (oorspronkelijk bericht)
M_c ciphertext (versleuteld bericht)
key sleutel

Goed gekozen functies zorgen in het geval van symmetrische encryptie voor uitstekende beveiliging van data, maar wanneer de ciphertext dient te worden getransporteerd, ontstaat een probleem, namelijk het distribueren van de keys. Zender en ontvanger dienen immers over dezelfde key te beschikken. Indien het transport van de sleutel via een onveilig medium zou plaatsvinden, bijvoorbeeld via het Internet, biedt symmetrische encryptie geen adequate beveiliging van gegevens vanwege het gevaar van het onderscheppen van de geheime sleutel. Dat zou te betreuren zijn vanwege de grote voordelen die symmetrische encryptie biedt, namelijk snelheid en efficiëntie. Een veilige wijze van transport van sleutels is dus geboden.

Tevens valt een onderscheid te maken tussen zogenaamde block-ciphers en stream-ciphers. Block-ciphers voeren cryptografische bewerkingen uit op een blok data met vastgestelde grootte. Stream-ciphers voeren de bewerkingen uit op een stroom van afzonderlijke bytes data. Omdat stream-ciphers niet hoeven te wachten totdat een heel blok gevuld is, zijn zij vaak nog efficiënter dan block-ciphers. Dit is in het bijzonder het geval wanneer zeer veel kleine hoeveelheden data afzonderlijk versleuteld dienen te worden.

Voorbeelden van symmetrische block-ciphers zijn Digital Encryption Standard (DES) en Blowfish. Een voorbeeld van een veelgebruikte stream-cipher is Redundant Cipher 4 (RC4).

Toelichting 1b. Cryptografische technieken: asymmetrisch.

Assymmetrische of public key encryptie

In tegenstelling tot symmetrische encryptie gebruikt asymmetrische encryptie voor de versleuteling en ontsleuteling twee verschillende keys. Hierbij hebben de keys een onderlinge wiskundige relatie, uit de ene key kan echter de andere niet worden afgeleid. De functionele relatie tussen de twee bestaat uit het feit dat slechts decryptie met één sleutel kan plaatsvinden als encryptie heeft plaatsgevonden met de andere. Het handelt dus om een sleutelpaar. De zender kan nu een sleutelpaar genereren en één van de sleutels publiek maken (public key) terwijl hij de andere sleutel (private key) geheim houdt.

$F_a(M_p, \text{key1}) = M_c$ en $F_a(M_c, \text{key2}) = M_p$, waarbij:

F_a asymmetrische cipherfunctie
M_p plaintext message
M_c ciphertext
key1 public key (of private key)
key2 private key (of public key)

Omdat de publieke sleutel niet vertrouwelijk is, kan transport van deze sleutel zonder problemen via een onveilig medium plaatsvinden. Tevens zorgt de vertrouwelijkheid van de private key ervoor dat een met de public key versleuteld bericht slechts door de houder van de private key ontsleuteld kan worden, waardoor vertrouwelijkheid van informatie gewaarborgd wordt. Een nadeel van sommige vormen van asymmetrische encryptie is echter de inefficiëntie en het gebrek aan snelheid van verwerken. Hierdoor is asymmetrische encryptie niet altijd geschikt om lange berichten (of veel kleine) in real-time te versturen.

Een mogelijke uitzondering op de inefficiëntie van huidige vormen van asymmetrische encryptie vormt de zogenaamde Elliptic Curve Cryptography (ECC), die gebruikmaakt van algoritmen die voor bepaalde toepassingen vele malen sneller zijn dan de in de genoemde applicaties gebruikte algoritmen. Helaas is de intrinsieke veiligheid van ECC nog onvoldoende onderworpen geweest aan wetenschappelijk onderzoek om te stellen dat ECC veilige, efficiënte en snelle asymmetrische encryptie biedt.

Het gebruik van asymmetrische encryptie biedt naast vertrouwelijkheid ook onweerlegbaarheid van een bericht. Immers, indien een bericht ontsleuteld kan worden met de ene helft van het sleutelpaar, dan is met zekerheid te stellen dat deze met de andere helft van het sleutelpaar is versleuteld. Indien de herkomst van de public key nu vaststaat (door middel van een Trusted Third Party (TTP) of bekendheid met de verstrekker) dan kan de houder van de private key niet ontkennen het bericht verstuurd te hebben, hij is immers de enige met deze sleutel. Deze onweerlegbaarheid is een unieke eigenschap van asymmetrische encryptie die van groot belang is bij het doen van transacties over Internet.

Voorbeelden van public key ciphers zijn RSA (naar de bedenkers Rivest, Shamir en Adleman) en Digital Signature Algorithm (DSA).

Hashing en MAC's

Een Message Authentication Code (MAC) is een door hashing berekende code die een verkorte representatie is van het oorspronkelijke bericht. Hashing behelst het berekenen van een soort samenvatting van het bericht met een zogenaamde sterke checksum, waarbij kleine veranderingen in het oorspronkelijke bericht een grote verandering in de hashingcode opleveren. Een MAC voldoet aan de volgende criteria:

- een MAC is normaliter veel korter dan het oorspronkelijke bericht;
- indien de MAC bekend is, is het uiterst moeilijk het oorspronkelijke bericht te herleiden;
- indien de MAC en het oorspronkelijke bericht bekend zijn, is het uiterst moeilijk een ander bericht te vinden dat dezelfde MAC oplevert.

Een MAC kan derhalve worden gezien als een unieke 'vingerafdruk' van een bericht. Indien een (eventueel versleutelde) MAC aan een bericht wordt gekoppeld, kan door middel van berekening van de hashingcode door de ontvanger en vergelijking met de meegestuurde MAC worden vastgesteld of het bericht integer is.

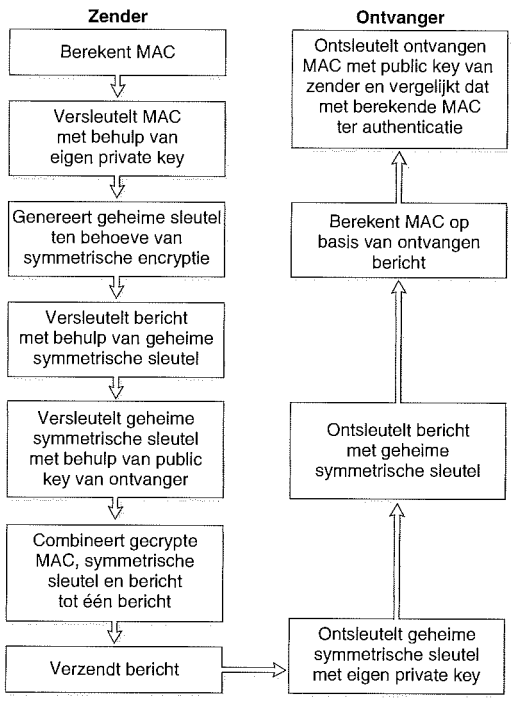
Voorbeelden van hashingalgoritmen zijn Message Digest 5 (MD5) en Secure Hashing Algorithm (SHA).

Toelichting 2. Communicatie over een onveilig kanaal.

Door een combinatie van technieken uit toelichting 1 toe te passen kan beveiligde communicatie over onveilige kanalen plaatsvinden. Omdat asymmetrische encryptie kan worden gebruikt over onveilige kanalen, kan hiermee een geheime sleutel ten behoeve van symmetrische encryptie worden uitgewisseld. Na deze uitwisseling kan verdere encryptie plaatsvinden door middel van – efficiëntere – symmetrische ciphers.

Door alle communicatie te voorzien van een MAC kan tevens worden gewaarborgd dat het bericht in oorspronkelijke staat arriveert en integer is. Door deze MAC afzonderlijk met de secret key van de verzender te versleutelen is aan te tonen dat het bericht onweerlegbaar door de houder van de secret key is verstuurd. Hiermee is in theorie aan de basisvoorwaarden van identiteit, authenticatie, vertrouwelijkheid en onweerlegbaarheid voldaan.

Figuur 1 toont een vereenvoudigde schematische weergave van de stappen die minimaal benodigd zijn om een bericht te versturen over een onveilig kanaal waarbij aan de voorwaarden van identificatie, authenticatie, vertrouwelijkheid en onweerlegbaarheid moet worden voldaan. Hierbij wordt ervan uitgegaan dat de uitwisseling van publieke sleutels tussen zender en ontvanger reeds heeft plaatsgevonden, eventueel via een Trusted Third Party (TTP).



Figuur 1. Berichtverzending over een onveilig kanaal.

Als u dan hier even wilt tekenen, op de stippellijn?

Enkele juridische aspecten van electronic commerce

Mw. mr. A.M.Ch. Kemna MBA

Hoe vertaal je de oude gang van zaken, waarbij contracten, handtekeningen, voorwaarden, bonnetjes, facturen, beslissingen, vergunningen, en wat dies meer zij, voornamelijk op papier de organisatie verlieten en binnenkwamen, naar een omgeving waarin dit medium is verdwenen, zoals bijvoorbeeld het Internet? Dit artikel geeft in vogelvlucht inzicht in een aantal van de juridische aspecten van het 'elektronisch zakendoen'.

INLEIDING

Hoe zou de wereld er uitzien zonder papier? Waarschijnlijk zullen we het antwoord daarop, ondanks de inspanningen van milieuorganisaties, vooralsnog schuldig blijven; papierloze administraties betekenden tot nu toe veelal nog geen vermindering van het papiergebruik in organisaties. De wervelende opkomst van electronic commerce in het zakelijk verkeer en de inspanningen van de overheid om te komen tot elektronische communicatie met de burger zullen wellicht voor de kentering gaan zorgen. Dat aan het verlaten van zo'n oud medium de nodige juridische consequenties kleven, is iets wat steeds meer deelnemers zich realiseren. Want hoe vertaal je de oude gang van zaken naar een omgeving waarin papier als medium is verdwenen, zoals bijvoorbeeld het Internet? Dit artikel geeft in vogelvlucht inzicht in een aantal van de juridische aspecten van het 'elektronisch zakendoen'. Ter introductie de volgende case.

De vooruitstrevende manager van mega-legbatterij Kakelvers in het midden des lands heeft met zijn afnemers besloten om op elektronische wijze de bestelling van eieren te gaan verwerken. Hij heeft daartoe met zijn afnemers een zogenaamd interchange agreement afgesloten. Tien dagen voor Pasen bestelt een dorpskruidenier in Epe elektronisch honderd dozen van tien eieren, af te leveren op Goede Vrijdag. Op die dag arriveert de vrachtwagen van Kakelvers keurig op tijd bij de dorpskruidenier in Epe en levert duizend dozen van tien eieren af. De dorpskruidenier is woedend en neemt contact op met Kakelvers. Hij beroept zich op het elektronische bericht dat hij heeft verstuurd en waarin hij honderd dozen heeft besteld. Het bericht blijkt verminkt te zijn aangekomen bij Kakelvers. In het bericht dat Kakelvers heeft ontvangen, staat een bestelling van duizend dozen.

Deze probleemstelling werd onlangs voorgelegd aan studenten post-doctoraal EDP Auditing aan de Erasmus Universiteit te Rotterdam, met het verzoek een verhandeling te geven omtrent de juridische posities van de eierhandelaar en de dorpskruidenier. De meeste studenten waren het erover eens, dat de interchange agreement, de overeenkomst die de partijen hebben afgesloten om de risico's en aansprakelijkheden ten aanzien van hun elektronische communicatie te regelen, meer duidelijkheid zou moeten verschaffen over de vraag voor wiens rekening de communicatiefout zou moeten komen.
Het belang van nadere afspraken omtrent elektronisch zakendoen, bijvoorbeeld in de vorm van algemene voorwaarden, is één van de juridische aspecten van electronic commerce die in dit artikel aan de orde komen. Daarnaast wordt gesproken over de inhoud en het kenbaarheidsvereiste van algemene voorwaarden, elektronisch bewijs en de elektronische handtekening. Er wordt ingegaan op enkele aspecten van de inzet van Trusted Third Parties voor bewijsversterking. Ook wordt nog het fenomeen e-mail behandeld, en wat de waarde daarvan kan zijn voor bewijs en bewaring. Afgesloten wordt met een uitstapje naar de activiteiten van het Ministerie van Economische Zaken en het Electronic Commerce Platform Nederland om te komen tot een gedragscode voor deelnemers aan electronic commerce.

ELECTRONIC COMMERCE EN HET BELANG VAN OVEREENKOMSTEN

Het voorbeeld van legbatterij Kakelvers en de dorpskruidenier te Epe is een gestileerde illustratie van wat er kan gebeuren als men elektronische middelen gaat toepassen in het zakelijk verkeer. Het orderformulier wordt vervangen door een e-mail en de post door de telecommunicatie- en netwerkverbinding. De afzender is niet meer te herkennen aan zijn briefpapier en handtekening, die bij de Kamer van Koophandel eventueel is te verifiëren op tekeningsbevoegdheid en de omvang daarvan. De partijen in het voorbeeld hadden een interchange agreement gesloten, waarin afspraken omtrent deze aspecten kunnen worden geregeld. Een gang van zaken die bijvoorbeeld bij Electronic Data Interchange (EDI), de vorm van elektronische handel waarbij gebruik wordt gemaakt van communicatie door middel van gestandaardiseerde en gestructureerde berichtenuitwisseling tussen de systemen van twee of meer partijen, reeds goed ingeburgerd is. Indien electronic commerce verder toeneemt, zal het echter heel wel mogelijk zijn dat wordt gecommuniceerd met partijen met wie men een dergelijke uitwisselingsovereenkomst niet heeft. Bovendien is het niet praktisch en vrijwel onmogelijk met iedereen apart een dergelijke overeenkomst te sluiten. Men gaat dan communiceren met partijen met wie voorheen nog geen (al dan niet elektronische) zakelijke relatie bestond. Daarbij zal het in de toekomst ook meer en meer om buitenlandse zakenpartners en particuliere afnemers kunnen gaan. Het grensoverschrijdende karakter van het Internet is hier bijvoorbeeld debet aan. Er kan dan onduidelijkheid ontstaan omtrent het (nationale) recht dat van toepassing dient te zijn op de desbetreffende transactie tussen partijen, een vraag van internationaal privaatrecht. Op deze laatste vraag zal in het slechts korte bestek van dit artikel niet nader worden ingegaan.[1]

Om juridische onduidelijkheden in een in beginsel open relatie het hoofd te bieden, zou men zich kunnen bedienen van algemene voorwaarden voor electronic commerce, die aan de potentiële wederpartij worden aangeboden op het moment dat men een transactie initieert.
Helaas kan juridisch gezien echter niet alles in voorwaarden worden geanticipeerd en opgelost. Van dwingendrechtelijke bepalingen in het recht kan door middel van voorwaarden of onderlinge afspraken niet worden afgeweken. Niet ieder land zal in zijn rechtsstelsel de mogelijkheid bieden om afspraken te maken omtrent de waarde van elektronische bewijsmiddelen. Ook wetsbepalingen die een bepaalde (schriftelijke) vorm dwingend voorschrijven, kunnen door voorwaarden en/of nadere afspraken niet opzij worden gezet. Een voorbeeld daarvan is de eis uit de Auteurswet 1912, dat auteursrechten slechts bij akte (een ondertekend geschrift) kunnen worden overgedragen. Auteursrechten op bijvoorbeeld publicaties of software zullen dus niet via elektronische communicatie kunnen worden overgedragen; daarvoor is papier nog steeds het verplichte medium.

Maar voor het overige geldt voor electronic commerce hetgeen voor alle vormen van zakelijk verkeer geldt: de meeste overeenkomsten kunnen vormvrij gesloten worden, dus ook mondeling en ook elektronisch.
Hierna zal nader worden ingegaan op het gebruik van algemene voorwaarden voor contracteren op het Internet.

Wetsbepalingen die een bepaalde vorm dwingend voorschrijven, kunnen door partijen niet opzij worden gezet.

ALGEMENE VOORWAARDEN EN HET INTERNET

De toepassing van het Internet wordt doorgaans gezien als één van de belangrijkste motoren van de informatiemaatschappij. Zo wordt voor Nederland bijvoorbeeld verwacht dat in 2005 25% van alle voedingswaren via het Internet zal worden besteld.[2] De enorme potentie die het Internet met betrekking tot wereldwijde informatievoorziening, teleshopping en betaling biedt, gaat vele organisaties nog de eigen verbeeldingskracht te boven.

Steeds meer organisaties bieden via Internet de mogelijkheid om diensten of producten te bestellen. De wijze waarop daarbij de algemene voorwaarden van de leverancier, die volgens hem dienen te gelden bij de transacties, aan de afnemers worden gepresenteerd, verschilt van site tot site. Soms wordt door middel van een hyperlink de mogelijkheid geboden de voorwaarden te bekijken. Niet altijd valt deze mogelijkheid bij een bezoek aan de site overigens direct op. In andere gevallen wordt men verplicht door de voorwaarden heen geleid, alvorens men bepaalde diensten of producten kan bekijken. Ook staan de voorwaarden wel eens in een klein, direct leesbaar kader op de webpagina beschreven. Op welke wijze zou het nu eigenlijk moeten volgens het Burgerlijk Wetboek (BW)?

In Boek 6, Afdeling 6.5.3 van het BW staat de regeling voor het toepassen van algemene voorwaarden beschreven. De regeling geeft aan, dat algemene voorwaarden op schrift dienen te worden gesteld ('één of meer schriftelijke bedingen') en door de wederpartij schriftelijk of op andere wijze moeten worden aanvaard.[3] De voorwaarden dienen vóór of bij het sluiten van de overeenkomst aan de wederpartij ter hand te worden gesteld. Indien dat redelijkerwijze niet mogelijk is, kan men volstaan met het aan de wederpartij mededelen dat de voorwaarden bij de gebruiker ter inzage liggen of bij een bepaalde Arrondissementsrechtbank of Kamer van Koophandel zijn gedeponeerd en op verzoek zullen worden toegezonden.
Als men de regeling sec leest, zou men geneigd kunnen zijn te concluderen dat het gebruik van algemene voorwaarden op het Internet niet mogelijk is. Deze conclusie leidt tot een juridisch niet wenselijke situatie en is naar mijn mening ook niet juist. In de literatuur gaat men er doorgaans van uit dat voorwaarden ook op niet-schriftelijke wijze mogen wor-

1 Voor een korte bespreking van aspecten van internationaal privaatrecht wordt verwezen naar [Wetg97] en [SER98].

2 Http://www.minez.nl/ecom/wpindex.htm.

3 Ten aanzien van de term 'op schrift' dienen enige kanttekeningen te worden geplaatst. Er is momenteel veel discussie in de juridische literatuur of onder een geschrift ook een niet-papieren document mag worden verstaan. Door de HR is dit voor het strafrecht al eens positief beantwoord. Voor het bestuursrecht wordt ervan uitgegaan dat de eis van een geschrift in vele bepalingen betekent: op papier.
Voor het civiele recht vindt [Pitl96] dat een elektronisch bestand niet (zonder meer) een geschrift kan zijn. [Huyd97] vinden dat dit wel het geval is, maar lijken hier later op terug te komen als het gaat om de functies van een geschrift. [MDW98] citeert hen indien het een definitie van 'geschrift' weergeeft, overigens zonder nadere nuancering, en concludeert vervolgens naar mijn mening te snel dat een geschrift *dus* ook een elektronisch stuk is. De conclusie dient genuanceerder te zijn. In het dagelijks woordgebruik is geschrift/schriftelijk: leestekens op papier.

den gepresenteerd en ook dat de letterlijke 'ter hand stelling' geen conditio sine qua non is (zie bijvoorbeeld [Nepp97]). En zelfs indien het laatstgenoemde wel het geval zou zijn, zou men er nog op de site expliciet op kunnen wijzen dat de voorwaarden elders opvraagbaar zijn en op papier, per post, kunnen worden toegestuurd. Deze laatste voorwaarde is echter voor de snelle Internet-wereld, waarin potentieel vele duizenden transacties per dag zouden kunnen worden uitgevoerd, geen aantrekkelijke (want vertragende en dure) optie.

Overigens wordt door de wet gebondenheid van de wederpartij aan algemene voorwaarden snel aangenomen: indien hij ze niet uitdrukkelijk heeft aanvaard noch heeft verworpen, terwijl een redelijke mogelijkheid is geboden om van de inhoud kennis te nemen vóór of tijdens het contracteren, zijn ze tóch van toepassing. Indien die redelijke mogelijkheid niet is geboden, kan de wederpartij echter voorwaarden die onder gegeven omstandigheden onredelijk zijn, laten vernietigen. De vraag is uiteraard: wat is een redelijke mogelijkheid op Internet? Is het via een button op de webpagina beschikbaar stellen van de voorwaarden een toereikende oplossing? Daarbij zal de afnemer dus nog een extra handeling moeten uitvoeren om de voorwaarden te lezen, een opgave waar menigeen bovendien niet met oprecht plezier aan zal beginnen. Vanuit oogpunt van consumentenbescherming lijkt het gerechtvaardigd om bij transacties tussen een consument en een niet-consument (professionele wederpartij) wel wat strengere eisen aan de kenbaarheid van de voorwaarden te stellen. Daarvan uitgaand lijkt de juridisch beste oplossing toch die waarbij de afnemer voordat de transactie is voltooid, verplicht door de voorwaarden wordt geleid en waarbij wordt aangegeven dat het vervolgen van de handelingen en aangaan van een transactie expliciet instemming met de voorwaarden inhoudt.

Inhoud algemene voorwaarden voor Internetgebruik

Ook indien men zich doorgaans reeds bedient van algemene voorwaarden, zal men bij het gebruik van Internet als verkoopkanaal in die voorwaarden bij voorkeur enige specifiek op het medium toegesneden wijzigingen en/of aanvullingen dienen door te voeren.

In het algemeen geldt dat men bij het hanteren van algemene voorwaarden jegens consumenten rekening dient te houden met de regeling voor algemene voorwaarden in het Burgerlijk Wetboek, Boek 6. Daarin is weergegeven de regeling van de zwarte lijst, met soorten voorwaarden die nietig zijn en de grijze lijst, met soorten voorwaarden die vernietigbaar zijn indien gehanteerd in consumentencontracten. Een voorbeeld uit de zwarte lijst is een beding 'dat de bevoegdheid van de wederpartij [van de voorwaardengebruiker] om bewijs te leveren uitsluit of beperkt, of dat de uit de wet voortvloeiende verdeling van de bewijslast ten nadele van de wederpartij wijzigt' (art. 6:236 onder k BW). Een voorbeeld van een voorwaarde van de grijze lijst is een beding dat de 'gebruiker of een derde geheel of ten dele bevrijdt van een wettelijke verplichting tot schadevergoeding' jegens de wederpartij (art. 6:237 onder f BW).

Daarnaast dient men rekening te houden met het eventueel van toepassing zijn van de Europese Richtlijn betreffende de bescherming van de consument bij op afstand gesloten overeenkomsten[4], welke Richtlijn uiterlijk op 20 mei 2000 in de Nederlandse wet dient te zijn doorgevoerd. Er mag van worden uitgegaan dat deze ook van toepassing is op teleshopping via het Internet. De Richtlijn geeft een aantal regels voor onder meer de informatieverplichting van aanbieders aan afnemers, het herroepingsrecht van afnemers bij het aangaan van overeenkomsten op afstand, de termijn waarbinnen de aanbieder dient te presteren, het kunnen annuleren door de afnemer van frauduleuze betalingen die zijn verricht met zijn creditcard en het vrijgesteld zijn van een tegenprestatie bij het leveren van onbestelde waren. De Richtlijn geeft een minimumkader weer, de nationale wetgever mag derhalve zwaardere eisen stellen aan consumentenovereenkomsten op afstand.

Ten aanzien van de inhoud van algemene voorwaarden op het Internet zouden de volgende (niet-uitputtende opsomming van) relevante onderwerpen kunnen worden genoemd die regeling verdienen: de toepasselijkheid van de voorwaarden, de gebondenheid van afnemer en eventuele herroepingsrechten; het gebruik van toegangscodes, (certificaten van) digitale handtekeningen, en de risico's en verantwoordelijkheden daarbij, de toegang tot eventuele andere informatie via de website van de aanbieder en diens (afwezigheid van) verantwoordelijkheid voor de kwaliteit en de inhoud daarvan; intellectuele eigendomsrechten en het gebruik van de site en de afname van diensten en producten van de aanbieder; het recht van de aanbieder gegevens van de afnemer voor bepaalde doelen te gebruiken en de wijze waarop de afnemer hiervan op de hoogte kan worden gesteld; de wijze van betaling; de bewijskracht van uitgewisselde informatie en de geautomatiseerde administratie van de aanbieder, de randvoorwaarden daarvoor en de mogelijkheid eventueel tegenbewijs te leveren; het toepasselijk recht (indien internationaal wordt aangeboden) en de forumkeuze (welke rechter is bevoegd).

Bij gebruik van Internet als verkoopkanaal zullen de voorwaarden specifiek op het medium toegesneden moeten zijn.

BEWIJS IN EEN DIGITALE OMGEVING

Het is meestal niet de bedoeling, maar het is natuurlijk mogelijk dat partijen bij een overeenkomst in een conflict tegenover elkaar komen te staan. Als het dan tot een gerechtelijke procedure komt, is het voor elk van hen van essentieel belang de juiste bewijzen op tafel te kunnen leggen om het eigen gelijk aan te kunnen tonen. Immers, ook als men ervan overtuigd is dat de eigen interpretatie van de rechtspositie de juiste is, dan nog is het zaak ook de rechter hiervan te overtuigen door het overleggen van de

De wetgever heeft ooit bedoeld papier, vanwege de daarmee gepaard gaande functionaliteiten. Als we de term 'schriftelijk' juridisch willen uitbreiden (hetgeen wenselijk lijkt), moeten we kijken naar die gewenste functionaliteiten. De drager is wel degelijk relevant naar mijn mening, alsmede de daaromheen 'gevouwen' maatregelen, die de 'papieren functionaliteiten' dienen te waarborgen. Ook de SER CCA (zie het in noot 1 aangehaalde document) concludeert dat een elektronisch document niet altijd een geschrift kan zijn, doch dat dient te worden gekeken naar de te waarborgen en gewaarborgde functionaliteiten. [MDW98] geeft overigens ook aldus een aanbeveling, en stelt enkele proefartikelen voor ten behoeve van specifieke rechtssituaties, onder meer voor het elektronisch kopen en overdragen van onroerend goed.

4 Richtlijn 97/7/EG van het Europees Parlement en de Raad, Pb. EG L 144/9.

meest geschikte bewijsmiddelen. Bewijzen in juridische, civielrechtelijke zin is het aan de rechter verschaffen van een redelijke mate van zekerheid omtrent de juiste toedracht van betwiste feiten en rechten. De rechter beslist dan of de feiten en rechten die partijen onderling in het geding hebben betwist, voldoende zijn komen vast te staan. Hij waardeert daartoe het gestelde bewijs binnen de regels die hem daartoe door het procesrecht worden gesteld.

Deze gang van zaken verandert niet indien partijen die met elkaar zakendoen gebruikmaken van moderne informatie- en communicatiemiddelen in plaats van het vertrouwde papier. Wat er wel verandert, is dat partijen (nog) beter dienen na te gaan welke bewijsmiddelen zij in geval van een conflict kunnen en willen inbrengen en wat de mogelijke bewijswaarde zal zijn van die middelen in een gerechtelijke procedure. Hoe past men digitale informatie toe als bewijs en hoe zal een rechter dergelijke vluchtige gegevens waarderen op het aspect van betrouwbaarheid?

Er ontstaat met de voortschrijdende groei van de informatie- en communicatietechnologie een steeds groter scala van mogelijkheden om alternatief bewijsmateriaal te produceren in een procedure. Dit kan variëren van het inbrengen van uitgewisselde EDI-berichten tot het gebruiken van bewijs bestaand uit een computerprogramma of informatie geproduceerd door een computersysteem (bijvoorbeeld bij Internet-bestellingen) of binnen het informatieverwerkingsproces van een organisatie (de elektronische administratie). In Nederland is er niets op tegen om elektronisch bewijsmateriaal in een juridische procedure aan te dragen: Dit vloeit voort uit het vrije bewijsstelsel dat hier te lande wordt gehanteerd. In andere landen, met name onder het Angelsaksische rechtsstelsel, levert dit nog wel eens problemen op.[5] Het bewijs van gestelde feiten kan in Nederland met alle middelen worden geleverd, tenzij de wet anders bepaalt. De rechter zal vervolgens bepalen wat de waarde is van het geleverde bewijs. Dit heeft als consequentie dat de partijen in een geding tot de uitspraak van de rechter geen zekerheid hebben over de waarde die de rechter aan hun bewijsvoering zal toekennen. Deze onzekerheid is met name in een elektronische omgeving een probleem waarvoor in de praktijk naar oplossingen wordt gezocht. Alvorens hierop in te gaan wordt allereerst een wettelijke mogelijkheid uiteengezet om het probleem van onzekerheid rondom bewijswaardering door de rechter te omzeilen: de bewijsovereenkomst.

De bewijsovereenkomst

Een bewijsovereenkomst is een afspraak tussen contractpartijen met betrekking tot hun bewijspositie in geval van een eventueel proces. Partijen kunnen daarbij een regeling treffen omtrent de (dwingende) bewijskracht van bepaalde bewijsmiddelen, de uitsluiting van bewijsmiddelen, beperking of uitsluiting van tegenbewijs of een afwijkende verdeling van bewijslast. Een bekend voorbeeld is de bepaling in algemene bankvoorwaarden, dat de administratie van de bank als (enig en) volledig bewijs zal gelden.[6] Door middel van een bewijsovereenkomst kunnen partijen derhalve (nog grotere) invloed uitoefenen op inhoud en verloop van het proces. Aan middelen waaraan onder het wettelijk bewijsrecht een mindere waarde is toegekend, kunnen partijen een dwingende bewijskracht toedichten. Voor elektronisch opererende zakenpartners is dit een belangrijke mogelijkheid.

In een aantal gevallen moeten bewijsovereenkomsten echter buiten toepassing blijven. Dit is het geval indien partijen rechtsgevolgen hebben trachten te regelen die niet ter vrije beschikking van partijen staan (met name het negeren van een dwingendrechtelijke bepaling, zoals bijvoorbeeld de eerdergenoemde eis van overdracht van auteursrechten bij akte) alsook indien het overigens in strijd zou zijn met regelingen uit het Burgerlijk Wetboek om zich op de overeenkomst te beroepen. Bij dat laatste kan men denken aan de beperkende werking van redelijkheid en billijkheid zoals neergelegd in de artikelen 6:2 lid 2 en 6:248 van het Burgerlijk Wetboek. Men zou zich kunnen voorstellen dat dit het geval is indien het bewijsproducerende communicatie- of computersysteem overduidelijke gebreken vertoont. Laat de rechter een bewijsovereenkomst buiten toepassing, dan zal men terugvallen op de wettelijke bewijsregels. Er zal dan een oplossing gezocht moeten worden in het versterken van de bewijswaarde van elektronisch bewijs.

Het probleem van onzekerheid zou aanzienlijk kleiner zijn indien partijen een bewijsmiddel zouden kunnen produceren, dat wettelijk gelijke bewijskracht zou hebben als een authentieke en een onderhandse akte. Een authentieke en een onderhandse akte zijn (handmatig) ondertekende (papieren) geschriften opgemaakt om tot bewijs te dienen. Tussen partijen leveren zij juridisch het bewijs op (bij de onderhandse akte: tot op tegenbewijs) dat de vastgelegde verklaring in de akte waar is. De rechter moet zich daar ook aan houden. Men zoekt dan ook naar mogelijkheden om de functionaliteit van dergelijke akten te vertalen naar een digitale omgeving. Aspecten die daarbij van belang zijn, zijn betrouwbaarheid, duurzaamheid, authenticiteit en identiteit. Bij het ontwikkelen van eventuele 'elektronische functionele equivalenten' van akten zijn technieken als de elektronische handtekening en de toepassing van Trusted Third Parties van essentieel belang. Op deze twee technieken wordt hierna ingegaan.

Door een bewijsovereenkomst kunnen partijen een dwingende bewijskracht toedichten aan middelen die wettelijk niet die waarde hebben.

DE HANDTEKENING

De Hoge Raad verstond in een tweetal oude arresten onder ondertekening 'het plaatsen van den naam, dien de onderteekenaar voert of draagt, met of zonder bijvoeging van den voornaam'.[7] In de juridische literatuur verstaat men er tegenwoordig gewoonlijk onder: lettertekens, gesteld in het handschrift van de ondertekenaar, die de persoon die de

5 Alhoewel getracht wordt de problemen rondom de 'admissibility of computer based evidence', dat uitsluitend als zogenaamd 'hearsay evidence' ofwel indirect bewijs kan worden ingebracht, ook onder dat rechtssysteem op te lossen. Zo is in Groot-Brittannië in 1993 een rapport verschenen van de English Law Commission dat aanbevelingen bevat om de obstakels op dat vlak voor het civiele recht op te heffen; zie ook [HMSO].

6 De zogenaamde boekenclausule, zie de Algemene Bankvoorwaarden, art. 11; zie ook Voorwaarden Gebruik Geld- en Betaalautomaten in Nederland, art. 5.3 voor een aanvulling daarop ten aanzien van de afgiftebon van geldautomaten. Ten aanzien van de Algemene Bankvoorwaarden gaf de HR in 1923 aan dat de boekenclausule niet in strijd is met de wet, de goede zeden of de openbare orde, HR 1 juni 1923, NJ 1923, pag. 947; of dit in het huidige computertijdperk nog steeds onomstotelijk zou worden aangenomen, zou kunnen worden betwijfeld.

7 HR 17 december 1885, W. 5251; HR 6 mei 1910, W. 9025.

verklaring aflegt beogen te individualiseren. Enkele lettertekens (zoals een kruisje), een vingerafdruk, of ook de elektronische handtekening kunnen volgens deze definitie niet onder het huidige begrip handtekening worden gebracht, hoezeer wellicht met de laatste twee methoden eveneens de individualisatie respectievelijk de authenticiteit kan worden gewaarborgd.

Als de functies die de handmatige handtekening vervult kunnen de volgende worden aangehaald[8]:

- *Identificatie* van de ondertekenende persoon.

- *Toerekening* van het in het geschrift gestelde aan de ondertekenende persoon; deze laatste heeft met zijn ondertekening aangegeven dat hij de inhoud voor waar aanneemt.

- Hierbij sluit de functie van vastlegging van de *wilsuiting* van de ondertekenende persoon aan.

- De *integriteit* kan worden aangenomen op grond van de ondertekening.

- Door middel van de ondertekening kan eveneens de *echtheid* van het document worden aangenomen; de ondertekenaar heeft met zijn ondertekening *authenticiteit* verleend aan het geschrift.

De definitie van handtekening/ondertekening is overigens sterk verbonden met het medium waarop de handtekening wordt gezet en daarmee met de hierboven aan dat medium toegedichte kwaliteiten.

In de elektronische communicatie stijgt het gebruik van de elektronische handtekening snel in populariteit als het gaat om versterking van de betrouwbaarheid van berichtenverkeer.
Naast de asymmetrische encryptietechnieken zijn er nog vele andere methoden in gebruik om een vorm van 'handtekening' op een elektronisch document te bewerkstelligen. In het elektronisch betalingsverkeer wordt bijvoorbeeld gebruikgemaakt van de 'pincode + ja-toets' bij pinpastransacties. Ook wordt wel symmetrische encryptie toegepast (bijvoorbeeld bij de Studentenchipkaart ([IBG96]), omdat deze sneller is dan de asymmetrische vorm. Deze andere vormen kunnen echter niet alle functies van een handtekening vervullen, die een elektronische handtekening op basis van asymmetrische encryptie wel kan vervullen.

Reeds eerder werd gesteld dat volgens huidig recht de elektronische handtekening (ook de asymmetrische) formeel juridisch geen vervanger van de 'ouderwetse' handtekening kan zijn. Een vergelijking met de functies van de handmatige handtekening geeft aan waarom. De waarborging van echtheid (in de zin van integriteit en authenticiteit) van een bericht kan wel bij uitstek door middel van een asymmetrische elektronische-handtekeningentechniek geschieden. De toerekeningsfunctie en de wilsuitingsfunctie kunnen eveneens aan deze elektronische handtekening worden toegeschreven. Het bericht wordt gecodeerd nadat het als geheel wordt opgemaakt; door middel van het uitvoeren van deze handeling kan de 'ondertekenaar' uiting geven aan zijn wil en kan het ondertekende (of eigenlijk: uniek berekende) stuk als zodanig aan hem worden toegerekend. Dit is bijvoorbeeld anders in geval van gebruik van een pincode, die weliswaar (redelijk) uniek is toegewezen, maar veeleer wordt gebruikt als toegangscode dan als authenticatiemiddel. De koppeling (verweving) tussen de inhoud van een bericht en de ondertekeningsfuncties die met een elektronische handtekening kan worden bereikt, geldt niet voor deze techniek. Datzelfde moet geconcludeerd worden ten aanzien van de procedure 'pincode + ja'. Hiermee kan weliswaar een wilsuiting aan een klant die zich tevoren heeft geïdentificeerd, worden ontlokt, doch naar mijn mening kan met de procedure onvoldoende de koppeling gemaakt worden tussen de identiteit van de ondertekenaar (mits gewaarborgd is dat de code niet door een onbevoegde is gebruikt) en integriteit en authenticiteit van het stuk als zodanig. 'Ja' zegt nog niets over de (ongewijzigde) inhoud van het verzonden stuk. Het gebruik van een tweede techniek naast de pincode (zoals ook mogelijk is bij gebruik van de Studentenchipkaart), waarbij een (unieke) berekening wordt uitgevoerd over het te ondertekenen document, geeft in die zin veel betere juridische betrouwbaarheidswaarborgen.

Het gebruik van een elektronische handtekening in een zakelijke omgeving is veelal niet aan één persoon voorbehouden.

Een probleem doet zich echter voor bij de identificerende functie van de handtekening. Het is in veel gevallen zo dat het gebruik van een bepaalde elektronische handtekening in een zakelijke omgeving niet aan één persoon is voorbehouden, hetgeen met de traditionele handtekening wel het geval is. Bovendien is het in een elektronische omgeving zeer moeilijk vast te stellen of een handtekening daadwerkelijk afkomstig is van een bepaalde persoon die zegt de afzender te zijn. Immers, zelfs indien is vast te stellen dat vanuit het systeem van een geautoriseerde handtekeninggebruiker is verzonden, wil dit nog niets zeggen over wie de handelingen daadwerkelijk heeft verricht. Dit zal mogelijk slechts anders worden indien aan de elektronische handtekening biometrische kenmerken kunnen worden toegevoegd, zoals vingerafdruk of iriskenmerken.

Bij gebruikmaking van symmetrische technieken of andere technieken waarbij de sleutel eveneens bekend is aan de ontvangende zijde is er juridisch gezien nog een additioneel identificatieprobleem. Daarbij kan het mogelijk niet onweerlegbaar worden aangetoond dat een bericht afkomstig was van de verzender; het kan in dat geval immers eveneens door de ontvanger op dezelfde wijze worden gegenereerd. Met andere woorden, non-repudiation is niet gewaarborgd. Om dit juridische probleem te ondervangen zullen aanvullende maatregelen moeten worden getroffen, waarmee de verzender van het bericht wel kan worden vastgesteld. Een goed voorbeeld van zo'n maatregel is de invoering van een zogeheten Trusted Third Party (TTP), die kan waarborgen dat verzonden berichten niet afkomstig zijn van de ontvanger zelf of van een derde-niet-geautoriseerde die de code heeft weten te bemachti-

8 [Esch96] noemt voorts nog als functies: originaliteit, bevoegdheid, kennisneming, compleetheid, overijlingsbescherming en waarschuwing aan de ondertekenaar.

gen. Ook de toevoeging van biometrische kenmerken zou hier een oplossing kunnen zijn.

Relativering waarde handmatige handtekening

Ter relativering van hetgeen hierboven gesteld is omtrent de problematiek van identiteit, integriteit en authenticiteit bij het gebruik van (diverse vormen van) de elektronische handtekening, dient te worden opgemerkt dat het tegenwoordig niet altijd meer als vaststaand wordt aangenomen, dat indien een (gewone) handtekening onder een (schriftelijk) onderhands stuk staat, alles in dat stuk ook daadwerkelijk steeds is ondertekend zoals het er staat. Op grond van gegronde vermoedens kan een rechter aan degene die zich beroept op het stuk opdragen te bewijzen dat alles op deze wijze is ondertekend. Evenzo kan de rechter aan degene die zich beroept op het stuk – terwijl de wederpartij stellig ontkent te hebben ondertekend – opdragen de echtheid van diens handtekening te bewijzen. Met andere woorden, non-repudiation is in een papieren situatie ook niet altijd vaststaand.

In de huidige situatie zal het echter nog wel steeds zo zijn, dat een rechter het traditionele stuk dat er uitziet als een echt, ondertekend document eerder voor waar zal aannemen dan een elektronisch document dat elektronisch is ondertekend. Dit vanwege de – verwachte en/of reëel – grotere kans op onzichtbare manipulaties van elektronische documenten. Veelal zal voor de versterking van de bewijswaarde tevens moeten worden aangegeven dat de beveiliging van het document en de gebruikte ICT-systemen en -technieken dusdanig was, dat aangenomen kan worden dat de betrouwbaarheid van het bewijsmiddel hoog is, iets wat in een traditionele papieren situatie toch veel sneller zal worden aangenomen.

Ook in een papieren situatie staat onweerlegbaarheid niet altijd vast.

Aan de juridische erkenning van de elektronische handtekening wordt momenteel evenwel uitgebreid aandacht besteed, zowel op nationaal niveau als op internationaal niveau. Zeer recentelijk, 13 mei van dit jaar, heeft de Europese Commissie een voorstel gedaan voor een richtlijn om te komen tot een 'common framework for electronic signatures' ([Prop98]). Hierin wordt de juridische erkenning van elektronische handtekeningen als één van de belangrijkste aspecten bestempeld.

De elektronische handtekening in de AWR

Het probleem dat de elektronische handtekening juridisch nog niet dezelfde status heeft als een schriftelijke handtekening is in een recente wijziging van de Algemene wet inzake de rijksbelastingen (AWR) voor het doen van elektronische aangifte aldus opgelost.[9] Voor het doen van elektronische aangifte is een vergunning noodzakelijk. De vergunning wordt onder een aantal voorwaarden verstrekt. Een aanvraag tot zo'n vergunning dient schriftelijk te worden gedaan (er is dus altijd een schriftelijk, ondertekend stuk van de aangifteplichtige, waarin hij zich akkoord verklaart met de te gebruiken techniek en de wijze van identificatie). De aangifte kan vervolgens, na vergunningverlening, elektronisch worden ondertekend en verzonden, waarbij de elektronische handtekening geacht wordt te kunnen worden teruggevoerd op de eerder gegeven schriftelijke handtekening. Het gebruikte systeem van de elektronische handtekening in combinatie met technische maatregelen om de integriteit van het bericht te waarborgen, biedt naar de mening van de Minister voldoende garanties voor de echtheid van het bericht. De regeling is geïnspireerd door de contractuele regeling voor het verrichten van elektronische betalingen, welke in het bankwezen wordt gebruikt. Overigens bestaat het voornemen deze werkwijze eveneens te gaan hanteren voor uitwisseling met het Kadaster van elektronische gegevens met betrekking tot voor inschrijving in de kadastrale registers bestemde feiten. Voor deze situatie wordt eveneens een wetswijziging voorzien en een vergunningenstelsel ontworpen.

DE INZET VAN TRUSTED THIRD PARTY-DIENSTEN

Het Nederlandse bewijsrecht maakt het, zoals reeds eerder aangegeven, mogelijk dat bewijs wordt geleverd met alle middelen, tenzij de wet anders bepaalt.[10] Dit betekent dat ook elektronische berichten en documenten als bewijsmiddel mogen gelden. Het komt er echter op aan de rechter te overtuigen van de waarde (de betrouwbaarheid) van het gehanteerde bewijsmiddel (bijvoorbeeld een elektronisch bericht). De terughoudendheid die op het vlak van die waardering onder juristen nog valt te bespeuren heeft met name te maken met de manipuleerbaarheid van elektronische berichten en het verdwijnen van menselijke controle. De inzet van een TTP bij electronic-commerceactiviteiten, bijvoorbeeld als Certification Authority (CA) voor de certificatie van de publieke sleutel behorend bij digitale handtekeningen, zou de waardering van de betrouwbaarheid van elektronisch bewijs wel eens kunnen verbeteren. Wellicht dat in zo'n Trusted Third Party zelfs een equivalent gevonden kan worden voor de bevoegde ambtenaar, die authentieke akten met dwingende bewijskracht kan opmaken ('de elektronische notaris').

Contractuele regelingen met TTP's

Bij de besluitvorming omtrent het verlenen of inzetten van TTP-diensten komen ook de juridische aspecten van dergelijke diensten aan de orde. Er bestaat nog een aantal onzekerheden op juridisch vlak, die vooralsnog met name contractueel zullen moeten worden opgelost tussen partijen. Slechts een aantal punten zal in het korte bestek van dit artikel worden besproken. Voor een uitgebreide verhandeling omtrent TTP's wordt verwezen naar het artikel van Duthler en Dontje in deze Compact.

Problemen zouden kunnen ontstaan indien de handtekening van de TTP zelf wordt gecompromitteerd. Alle certificaten en tijdstempels die na een be-

9 Wet van 6 december 1995 tot wijziging van de Algemene wet inzake rijksbelastingen en van enige andere wetten in verband met de invoering van de mogelijkheid tot het doen van aangifte op elektronische wijze (elektronische aangifte), Stb. 1995, 606.

10 176 en 179 lid 1 Rechtsvordering (Rv).

paald tijdstip zijn afgegeven, worden daarmee onbetrouwbaar. Alle berichten, betalingen en data die met een door de TTP gecertificeerde handtekening zijn ondertekend, verliezen daarmee mogelijk hun waarborg van integriteit. Wat betreft het risico van het valselijk gebruikmaken van een digitale handtekening heeft de Hoge Raad[11] in dit kader uitgemaakt dat voor het bewijs van een niet-handmatige handtekeningtechniek (in casu een identificatiecode) geldt, dat bij gebreke van een contractuele regeling op dit punt de vraag voor wiens rekening misbruik komt, moet worden beantwoord aan de hand van de concrete omstandigheden van het geval. Daarbij is in het bijzonder van belang aan wie valt toe te rekenen dat de code ter kennis is gekomen van de onbevoegde. Dit in tegenstelling tot het gebruik van een gewone handtekening waarbij het risico in beginsel ligt bij degene die aanneemt (en mag aannemen) dat de handtekening echt is. Een contractuele regeling op het vlak van bewijs, bewijskracht, aansprakelijkheid en risico's tussen TTP en gebruikers is dan ook ten zeerste aan te raden.

Accreditatie/certificatie

Om haar afnemers te kunnen laten bepalen of de TTP werkelijk (nog) betrouwbare diensten levert, zal deze (haar systeem alsmede haar organisatie en sleutelgebruik) bij voorkeur gecertificeerd en gecontroleerd dienen te zijn. De juridisch naar mijn mening meest optimale situatie zou die zijn, waarbij dit zou gebeuren door een specifieke, 'hogere' accreditatie-TTP.[12] Zo'n 'super-TTP' zal eisen dienen te stellen waaraan de TTP als CA minimaal moet voldoen naargelang de vorm en de zwaarte van de diensten die geleverd worden, in een bepaalde markt of omgeving. Voorts zal de super-TTP bij voorkeur controle dienen uit te voeren op de blijvende kwaliteit van diensten. Met een dergelijke accreditatie en certificatie verplicht een TTP zich mede te voldoen aan een (minimum)standaard (van bijvoorbeeld beveiliging), waardoor het voor het publiek duidelijk kan worden of er gehandeld wordt met een betrouwbare TTP. De kenbaarheid van de gehanteerde norm is dan overigens wel een noodzaak. Mogelijk dat voor het opzetten van dergelijke kwaliteitseisen een analoge regeling getroffen zou kunnen worden als voor het stelsel van eisen en controle dat wordt gehanteerd bij accreditatie van certificatie-instellingen door de Nederlandse Raad voor de Certificatie.
Het is echter zeer de vraag of een dergelijke 'super-TTP' er in de praktijk zal komen. In Denemarken is wel eens een initiatief hiertoe ontplooid, doch dit is gestrand. In Duitsland bestaat wel een dergelijke accreditatie, voor slechts specifieke doeleinden.
Het probleem van certificatie van de TTP wordt in de praktijkcases die er bestaan momenteel wel opgelost door 'zelf-certificatie'. Een andere gehanteerde methode is de 'cross-certification': hierbij certificeren TTP's als het ware elkaar.

Gezien de voortschrijdende internationalisering van de economie en de nog steeds bestaande (internationale) spraakverwarring omtrent wat een TTP is en wat de kwaliteit van TTP-diensten dient te zijn, lijkt in ieder geval de tijd rijp om tot een soort 'keurmerk' te komen voor TTP-dienstverleners, aan de hand waarvan diensten en functies van TTP's door potentiële afnemers kunnen worden 'ingeschaald'. Dit lijkt een noodzaak om een mogelijke wildgroei van diensten en daarmee mogelijk een uitholling van de begrippen 'Trusted' en 'Third' (waarmee de TTP verwordt tot een gewone 'party'!) te voorkomen. Binnen Nederland worden reeds acties op dit terrein voorbereid, onder meer door de mogelijkheid van een TTP-kamer te onderzoeken. Deze idee is voortgekomen uit het onderzoek dat de Ministeries van Verkeer en Waterstaat en Economische Zaken hebben laten uitvoeren inzake het scheppen van de randvoorwaarden voor een goede infrastructuur van TTP-dienstverleners in Nederland ([Mim98]).

HET GEBRUIK VAN E-MAIL: BEWIJS EN BEWARING

Bij het elektronisch zakelijk verkeer tussen leveranciers en afnemers (zowel ondernemingen als particulieren) en ook bij het verkeer tussen overheid en burgers wordt steeds meer gebruikgemaakt van e-mail. E-mail betreft het uitwisselen van elektronische berichten tussen twee of meer houders van elektronische postadressen (e-mailadressen), volgens een bepaald protocol, doch met een ongestructureerde berichtinhoud (dit in tegenstelling tot EDI). Nu deze vorm van communicatie zo sterk in opkomst is, worden juridische vragen als wat de bewijswaarde van e-mail berichten is of kan zijn en of e-mails ook onderworpen zijn of zouden moeten zijn aan regelgeving omtrent bewaring, steeds actueler. Voor het antwoord op die vragen is echter meer duidelijkheid vereist omtrent het daadwerkelijk gebruik van e-mail in organisaties.

Status en waarde van e-mail

De status van e-mailberichten is in veel organisaties nog onduidelijk. De vraag wat e-mail nu eigenlijk is, is ook nog niet eenvoudig te beantwoorden. E-mail wordt ervaren als de vervanger van de brief en het memo, maar ook als een soort tussenvorm tussen memo en telefoon.
De waarde ervan wordt eveneens verschillend ervaren, variërend van 'betrekkelijk vanwege de manipuleerbaarheid' tot 'essentieel voor bewijs'. Dit heeft onder meer te maken met het verschillend belang van het medium voor onderscheiden organisaties. Het ene bedrijf kan zijn werkzaamheden niet meer (efficiënt en effectief) uitvoeren zonder deze toepassing, veelal in combinatie met gebruik van het Internet en eventueel zelfs een bedrijfsintranet. Daarnaast is 'de mail' vaak een zeer intensief gebruikt middel van informele informatie-uitwisseling. Ook dit is een belangrijk aspect van e-mail: het verkort lijnen en het doorbreekt standaard-communicatiestructuren. Immers, men stuurt eenvoudiger een ongedwongen mailtje naar de hoogste baas dan dat men op bezoek gaat of de telefoon grijpt. Deze dualiteit in gebruik maakt het echter ook heel ondoorzichtig op welke wijze e-mail nu gewaardeerd en ook door wie en wanneer het gearchiveerd zou moeten worden.
In veel andere organisaties is e-mail nog een volstrekt nieuwe toepassing, die zich nog geen status heeft verworven en waarmee men zich slechts in persoonlijke of projectmatige sfeer bezighoudt.
In een recent promotieonderzoek van Van den

11 NJ 1994, 622.

12 Hier bestaat het gevaar van het 'Droste-blikje-effect': de gewaarborgde betrouwbaarheid van een CA dient gecontroleerd te kunnen worden, waarvoor weer een (certificaat van een) CA nodig is, waarvoor hetzelfde probleem geldt; op deze wijze kan de keten van benodigde CA's schier oneindig worden. Zie ook [Fran96] alsmede [Froom].

Hooff ([Hoof97]) is onderzocht wat de effecten van invoering van e-mail op de organisatie, de communicatieprocessen, de bedrijfsprocessen en de structuur van de organisatie zijn. (Zie ook [Rijks98].) Van den Hooff noemt onder meer dat door het gebruik van e-mail er een sterk verbeterde en efficiëntere communicatie kan ontstaan binnen de organisatie en een hogere kwaliteit van werk. Met een aantal effecten wordt volgens hem echter nog heel vaak geen rekening gehouden, zoals een toenemende spanning tussen de formele organisatiestructuur en hiërarchie en de dagelijkse praktijk, die directer, minder controleerbaar en informeler kan verlopen. Ook kan het aantal persoonlijke contacten afnemen. Bij het uitwisselen van e-mail ontbreekt informatie over de wijze waarop de boodschap overkomt op de ontvanger, hetgeen bij persoonlijk en ook telefonisch contact wel het geval is. Naast communicatieverbetering kan hierdoor dus ook wel degelijk communicatieverarming en -verslechtering optreden.

Omtrent de juridische bewijswaarde en de bewaarverplichtingen van e-mail kunnen nog geen eenduidige uitspraken worden gedaan.

E-mail is momenteel dus nog een complex en moeilijk te duiden medium, dat nog vele stadia van ontwikkeling en gebruik kent in de maatschappij. Ten aanzien van de juridische bewijswaarde en de bewaarverplichtingen is het dan ook nog niet mogelijk reeds vaststaande antwoorden te geven. Voor de waardering van e-mailberichten zal met name de inhoud van belang zijn, alsmede de relatie waarbinnen de e-mailberichten zijn uitgewisseld en de mate waarin de berichten betrouwbaar kunnen worden geacht.

Bewijskracht van e-mail

Over het algemeen is een e-mailbericht eenvoudig te manipuleren. Het behoeft niet zichtbaar te zijn, dat ik een ontvangen bericht aanpas alvorens ik het doorzend naar een ander. Ook kan ik een bericht dat ik eerder heb aangemaakt later verzenden, waardoor de tijdsaanduiding van de e-mail onbetrouwbaar kan zijn. Tevens kan het onduidelijk zijn van wie het bericht precies afkomstig is en welke bevoegdheden deze persoon heeft. Zodra bijvoorbeeld een e-mailbericht een veilig bedrijfsintranet verlaat om in het Internet zijn weg te vinden, kan het bericht zodanig zijn vermomd dat niet bekend hoeft te zijn dat het van een bepaald individu afkomstig is. De ontvanger van het desbetreffende bedrijfsbericht kan op deze wijze ook niet weten wat de bevoegdheden van de verzender zijn, hooguit dat het bericht van dat bedrijf afkomstig is.
Om de genoemde redenen ziet men op steeds meer (zakelijke) e-mailberichten een tekst vermeld, dat de verzendende organisatie niet instaat voor de juistheid van het bericht en dat de ontvanger er geen rechten aan kan ontlenen.

Voor het verbeteren van betrouwbaarheid (in de zin van integriteit en authenticiteit) kan men gebruikmaken van technieken als het meezenden van de met een persoonlijke sleutel van zijn digitale handtekening versleutelde hashwaarde van het bericht, waarmee de ontvanger na decryptie kan vaststellen of het bericht nog integer is en van welke sleutelgebruiker het afkomstig is, uiteraard ook weer met de inzet van de diensten van een TTP. Afhankelijk van de techniek en procedures rondom de digitale handtekening zou de identiteit van de verzendende persoon eveneens redelijk gewaarborgd kunnen worden. Een en ander is vooral van belang in het kader van het vergroten van de bewijswaarde van e-mailberichten. Het is de vraag in hoeverre dit alles zich verdraagt met de functie die e-mail uitoefent in en tussen organisaties en of een en ander in verhouding staat tot de ermee gepaard gaande kosten. Het antwoord daarop zal per organisatie en per toepassing van e-mailverkeer dienen te worden bepaald.

Bewaarverplichtingen en e-mail

Er moet juridisch onderscheid worden gemaakt tussen bewijskracht en bewaarplichten, al is er wel een nauwe band tussen die twee. Door het opnemen van bewaarplichten in de wet wordt doorgaans gewaarborgd dat er bewijsmateriaal voorhanden is en dat er controle kan worden uitgeoefend door bijvoorbeeld toezichthoudende organen. In dat kader is het dan ook wenselijk dat de juridische regels voor bewaarverplichtingen afgestemd zijn op de regels voor toelaatbaarheid en de waarde van bewijs, in bijvoorbeeld een civiele of een administratieve procedure. (Zie ook [Land97].) Voor het bewaarrecht in Nederland is dat inmiddels heel redelijk het geval. Het is toegestaan dat gegevens ook op andere media dan papieren dragers worden aangemaakt, verwerkt en bewaard. Volgens het Nederlandse bewijsrecht kunnen ook al die middelen voor bewijs worden gebruikt. Daarbij moet men dan nog wel vaststellen dat de waarde van niet-papieren, niethandmatig ondertekend bewijs doorgaans als een stuk minder wordt ervaren.

Dient e-mail om bewaarrechtelijke redenen te worden gearchiveerd? Zowel fiscaalrechtelijk als civielrechtelijk geldt een bewaarplicht van tien jaren voor bescheiden die dienen ter staving van rechten en verplichtingen.[13] Binnenkort zal deze termijn zijn teruggebracht tot zeven jaren.[14] Tot de bescheiden die dienen ter staving van rechten en verplichtingen kunnen naar mijn mening eveneens behoren de e-mailberichten die zijn uitgewisseld. Dit is wel afhankelijk van de toepassing. Wordt e-mail met een wederpartij uitgewisseld in het kader van bijvoorbeeld electronic-commerceactiviteiten of in het kader van het communiceren over de uitvoering van een order of opdracht, dan zal de e-mail zeer zeker ter staving of onderbouwing van rechten en verplichtingen kunnen dienen. In veel organisaties is de toepassing echter nog niet zover en heeft e-mail met name een interne, informatieve en/of informele communicatiefunctie. Veelal wordt dan (al dan niet daarnaast) nog gebruikgemaakt van het papieren circuit.
Echter, ook bewaring van interne e-mail kan van belang zijn voor het voldoen aan de fiscale (en civiele) bewaarplicht, indien e-mail wordt gebruikt als middel voor het uitvoeren van interne controle en het aangeven van internecontroleaantekeningen. Dit

13 Art. 2:10 lid 3 BW, art. 2:24 lid 1 BW, art. 2:394 lid 6 BW en art. 52 lid 4 AWR.

14 Wetsvoorstel nr. 25753: Wijziging van Boek 2 van het Burgerlijk Wetboek en van enige andere wetten in verband met verkorting van de bewaartermijn van boeken, bescheiden en andere gegevensdragers. Aangenomen door de Eerste Kamer in maart 1998 (EK 1997-1998, 25753, nr. 265). De termijn van zeven jaar zal hierbij eveneens worden ingevoerd in de bewaarverplichtingen in de Douanewet (art. 8 derde lid) en de Algemene wet bestuursrecht (art. 4:69, tweede lid).

kan bijvoorbeeld het geval zijn indien documenten die van belang zijn voor de administratie van de organisatie elektronisch door de organisatie reizen langs de personen die autorisatie of controle dienen uit te voeren. Worden dergelijke documenten bewaard, dan zullen ook de bijbehorende e-mailaantekeningen bewaard dienen te blijven.

Uit het bovenstaande volgt dat de beantwoording van de vraag of bewaard moet worden sterk zal afhangen van de toepassing van e-mail, en dat een algemene richtlijn ten aanzien van de bewaarverplichting van e-mail dan ook vooralsnog niet kan worden gegeven.

De Algemene wet inzake rijksbelastingen stelt als extra eis (ten opzichte van het civiele bewaarrecht), dat de informatiedragers gedurende de bewaarperiode zodanig dienen te worden bewaard en eventueel geconverteerd, dat controle daarvan door de inspecteur binnen een redelijke termijn mogelijk is.[15] Het is aan de bewaarplichtige in deze de juiste keuze te maken en hierover afspraken met de Belastingdienst te maken. Het simpelweg periodiek uitprinten van e-mailboxen zonder er verder structuur of schifting in aan te brengen zal bijvoorbeeld mogelijk een probleem vormen voor het aan de inspecteur verschaffen van inzicht binnen een redelijke termijn, doordat de gegevens ondoorzichtig qua structuur en samenhang worden.

De Archiefwet

De wet die voor de overheid van basaal belang is voor wat betreft de bewaring van documenten, al dan niet op papier, is de Archiefwet.
In de Archiefwet worden de door (semi-)overheidsorganen te bewaren gegevens omschreven als 'Archiefbescheiden, ongeacht hun vorm, door de overheidsorganen ontvangen of opgemaakt en naar hun aard bestemd daaronder te berusten.' Ook daartoe kunnen naar mijn mening e-mailberichten, uitgewisseld in het werkverkeer, behoren. Een en ander betekent dat maatregelen getroffen moeten worden om ook die digitale gegevens gedurende de vastgestelde bewaarperiode toegankelijk en ongewijzigd te houden. De criteria die gelden ten aanzien van selectie van documenten voor het papieren archief gelden ook voor e-mail. Ook die zullen moeten worden bewaard of weggegooid; de van belang zijnde berichten zullen dus uit de berichtenstroom moeten worden gefilterd ([Rijks98]). Overigens is ook in de Archiefwet conversie toegestaan: archiefbescheiden mogen onder omstandigheden worden vervangen door reproducties, waarbij eveneens geen voorschrift voor de vorm wordt gegeven.

Recente praktijkontwikkelingen

Ten aanzien van de juridische status en de wenselijkheid van het bewaren van e-mail wordt momenteel veel onderzoek gedaan en er wordt veel over gediscussieerd. Zoals gezegd hebben opvallend weinig organisaties nog beleid geformuleerd ten aanzien van het gebruik, het waarborgen van de betrouwbaarheid en de archivering van e-mail. Ook binnen organisaties waarin e-mail reeds intensief wordt gebruikt, is dit nog nauwelijks het geval. Als aanzet ziet men wel steeds vaker disclaimers verschijnen op e-mails die de organisatie verlaten.

Vele belangengroeperingen en brancheorganisaties proberen verbetering te brengen in het huidige beleid. Ook proberen zij de bewustwording omtrent de waarde van e-mail te stimuleren. Ik noem een tweetal voorbeelden.

Bewaring van interne e-mail kan van belang zijn voor het voldoen aan de fiscale en civiele bewaarplicht.

Het verbeteren van het proces rondom archivering van digitale bestanden in het algemeen is de doelstelling van een gezamenlijke werkgroep van Ediforum en het Nederlands Normalisatie Instituut, die hiervoor in overleg met bedrijfsleven en overheid een Nederlandse Praktijkrichtlijn hebben ontworpen en uitgegeven ([NNI97]).
De Praktijkrichtlijn zal eveneens kunnen worden toegepast bij e-mailarchiveringsbeleid.
Het programmabureau Digitale Duurzaamheid, een gezamenlijk initiatief van Rijk, provincies, gemeenten en waterschappen, doet onderzoek naar de archiveringseisen in overheidsorganisaties bij een toenemende digitalisering van de communicatie. Het gebruik en de archivering van e-mail is een belangrijk onderwerp voor het programmabureau. Er wordt onder andere gewerkt aan functionele en procedurele eisen voor e-mailarchivering binnen de overheid.

NAAR EEN GEDRAGSCODE VOOR ELECTRONIC COMMERCE?

Ter afsluiting van dit artikel wil ik nog kort ingaan op een recente ontwikkeling in het kader van de verdere stimulering van de toepassing van electronic commerce in Nederland.

Om in Nederland een klimaat te scheppen waarin de Nederlandse ondernemer en consument zich (nog meer) bewust worden van de mogelijkheden van electronic commerce voor economie en samenleving, heeft het Ministerie van Economische Zaken in zijn Actieplan electronic commerce een aantal activiteiten aangeduid teneinde eventuele bestaande belemmeringen weg te nemen. Belemmeringen worden ervaren op juridisch, technisch en economisch gebied.

In het Actieplan wordt geconcludeerd dat een duidelijk en adequaat juridisch kader van groot belang is voor het opbouwen van het vertrouwen van de gebruiker in electronic commerce. Uiteraard is daar een goed wettelijk kader voor nodig, ook internationaal. Ten aanzien van aspecten die als knelpunt ervaren worden, maar waarvoor een wettelijke regeling niet per se een voorwaarde is, kunnen ook andere juridische instrumenten worden toegepast. Vanuit die gedachte heeft het Ministerie aan de Stichting Ediforum in samenwerking met het Electronic Commerce Platform Nederland opdracht gegeven te onderzoeken in hoeverre een zelfreguleringsinstrument als een gedragscode zou kunnen

15 Art. 52 lid 6 AWR. Zie ook het voorbeeld omtrent het dumpen van administratieve gegevens op papier, zoals gegeven in de 4e nota van wijziging bij het Wetsontwerp ter wijziging van de AWR, nr. 17, pag. 4.

Mw. mr. A.M.Ch. Kemna MBA
Senior manager bij de Unit JURIT van KPMG EDP Auditors. Is sinds 1989 verbonden aan KPMG en betrokken bij de opbouw van de juridische dienstverlening op het gebied van de toepassing van informatie- en communicatietechnologie in organisaties. Lid van de juridische expertgroep van Ediforum/ECP Nl en uit dien hoofde onder andere betrokken bij de praktijkrichtlijn Bewaren en Bewijzen en de ontwikkeling van een gedragscode voor electronic commerce in opdracht van het Ministerie van Economische Zaken.

worden ontwikkeld om electronic commerce meer vertrouwensbasis in Nederland te geven. Aan een dergelijke gedragscode zouden electronic-commercegebruikers zich kunnen conformeren, waardoor een bepaalde standaard voor 'fatsoenlijk electronic-commercegedrag' tot stand zou kunnen worden gebracht. Als onderwerpen geschikt voor zelfregulering worden onder meer genoemd de totstandkoming van de elektronische overeenkomst, de wijze van gebruik van algemene voorwaarden, de regeling van betrouwbaar bewijs, handtekeningen en de inzet van TTP's, de vertrouwelijkheid van (persoons)gegevens en geschillenbeslechting ([Edif98]). Naar verwachting zal in de tweede helft van dit jaar de gedragscode nader vorm krijgen en in de praktijk kunnen worden getoetst.

LITERATUUR

[Edif98] Ediforum / ECP Nl, *Het Juridisch Kader voor Elektronisch Zakendoen: Zelfregulering?*, onderzoekspaper in opdracht van het Ministerie van Economische Zaken, 1998.

[Esch96] R.E. van Esch, 'Elektronische Rechtshandelingen', in: H. Franken e.a., *De notaris en het elektronisch rechtsverkeer*, Koninklijke Vermande, 1996.

[Fran96] H. Franken, m.m.v. A.M.Ch. Kemna, 'De notaris als Trusted Third Party', in: *De notaris en het elektronisch rechtsverkeer*, Koninklijke Vermande, 1996.

[Froom] A.M. Froomkin, *The essential role of Trusted Third Parties in Electronic Commerce*, http://www.law.miami.edu/~froomkin/articles/trusted.htm.

[HMSO] *The Hearsay Rule in Civil Proceedings*, Command Paper 2321, HMSO.

[Hoof97] B. van den Hooff, *Incorporating electronic mail. Adoption, use and effects of electronic mail in organizations*, proefschrift, 1997.

[Huyd97] S. Huydecoper en R.E. van Esch, *Geschriften en handtekeningen, een achterhaald concept?*, ITeR onderzoek, Samsom Bedrijfs-Informatie, Alphen aan den Rijn/Diegem, 1997.

[IBG96] Informatie Beheer Groep, 'De beveiliging van de studentenchipkaart, voor elk wat wils', *Studentenchipkaart*, nr. 4, juli 1996.

[Land97] Landsadvocaat, *Advies Digitale Duurzaamheid*, Den Haag, 28 oktober 1997.

[MDW98] Ministerie van Justitie, *Elektronisch verrichten van Rechtshandelingen*, maart 1998.

[Min98] KPMG EDP Auditors, *Eindrapportage Nationaal TTP Project*, in opdracht van het Ministerie van Economische Zaken en het Ministerie van Verkeer en Waterstaat, 1998.

[Nepp97] E.D.C. Neppelenbroek en C. Stuurman, 'Teleshopping', in: H. Franken (red.), *Recht en computer*, Kluwer, Deventer 1997.

[NNI97] Nederlands Normalisatie Instituut / Ediforum, *Bewaren en Bewijzen, deel 2*, februari 1997. Binnenkort zal een vernieuwde versie verschijnen, gecombineerd met deel 1 (Wet- en regelgeving).

[Pitl96] T.R. Hidma en G.R. Rutgers, *Bewijs*, Pitlo serie Het Nederlands burgerlijk recht, Deel 7, 1996.

[Prop98] Proposal for a European Parliament and Council Directive on a common framework for electronic signatures. Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, COM(1998)297/2, http://www.ispo.cec.be/eif/policy.

[Rijks98] Rijksarchiefdienst, *Naar een verantwoorde archivering van E-mail.* Verslag van het symposium over de invoering, het gebruik en de archivering van e-mail in (overheids)organisaties, Den Haag 1998.

[SER98] SER-advies *ICT en de consument*, SER Commissie Consumentenaangelegenheden, 98/09.

[Wetg97] Nota Wetgeving voor de elektronische snelweg, TK 1997-1998, 25 880, nrs. 1-2, http://www.minjust.nl/sdu/index.htm.

De Trusted Third Party als enabler voor electronic commerce

Mw. mr. drs. A.W. Duthler en mw. mr. M.J. Dontje

Trusted Third Parties (TTP's), organisaties die betrouwbaarheidsdiensten ten behoeve van het elektronisch berichtenverkeer leveren, kunnen worden beschouwd als een belangrijke zo niet noodzakelijke voorwaarde om de voordelen van electronic commerce ten volle te kunnen benutten. Naast een uitleg over de toepassing van cryptografie, digitale handtekeningen, de infrastructuur die nodig is om gebruik te kunnen maken van TTP-diensten, wordt een overzicht gegeven van nationale, Europese en internationale ontwikkelingen op het gebied van beleid en regelgeving.

INLEIDING

De laatste jaren is de ontwikkeling van het elektronisch berichten- en geldverkeer in een stroomversnelling geraakt. Het Internet maakt wereldwijde gegevensuitwisseling mogelijk. Om de voordelen van elektronische gegevensuitwisseling optimaal te kunnen benutten, dient bij burgers en bedrijven voldoende vertrouwen te bestaan in de betrouwbaarheid van het elektronische gegevensverkeer. Het communiceren over een open netwerk als het Internet brengt echter onzekerheid met zich mee. Pas wanneer de betrouwbaarheid van elektronische communicatie kan worden gewaarborgd, kan optimaal gebruik worden gemaakt van de voordelen en mogelijkheden van electronic commerce. Zogeheten Trusted Third Parties (TTP's) kunnen een belangrijke rol spelen bij het reduceren van die onzekerheid en het garanderen van betrouwbare gegevensuitwisseling.

Op dit moment bestaat de meerderheid van het zakelijk Internet-gebruik uit e-mailverkeer en het onderhouden van statische websites (het Internet als uithangbord).[1] Er lijkt een situatie te bestaan waarin de ontwikkeling van TTP-diensten – te omschrijven als betrouwbaarheidsdiensten door onafhankelijke derden ten behoeve van het elektronische berichtenverkeer – wacht op een verdere ontwikkeling van electronic commerce, terwijl de doorbraak van electronic commerce afhankelijk lijkt te zijn van de beschikbaarheid van een betrouwbare TTP-infrastructuur. Op overheidsniveau begint het besef te groeien dat betrouwbaarheid een essentiële voorwaarde is om elektronische handel te realiseren én tot een succes te maken. In de ontwerpbeleidsnotitie inzake het Nederlandse beleid op het gebied van Trusted Third Parties, waarover straks uitgebreider, maant de projectgroep TTP tot haast bij het nemen van een aantal maatregelen ter bevordering van een betrouwbare TTP-infrastructuur.

In dit artikel wordt allereerst de behoefte aan betrouwbaarheid op het Internet vertaald naar een vijftal beveiligingsdoelen, te weten authenticiteit, integriteit, onweerlegbaarheid, vertrouwelijkheid en autorisatie. Dan zal aandacht worden besteed aan de techniek, te weten cryptografie (inclusief de toepassing van digitale handtekeningen), die wordt gebruikt voor het realiseren van deze beveiligingsdoelen. Vervolgens wordt ingegaan op de Public Key Infrastructure (PKI), de infrastructuur die betrouwbare en veilige communicatie (door middel van e-mail, maar ook het plaatsen van gevoelige informatie op een al dan niet besloten website) mogelijk maakt. Daarna zal worden besproken op welke wijze Trusted Third Parties, als onderdeel van een PKI, kunnen bijdragen aan het realiseren van de beveiligingsdoelen. Er wordt een verbinding gelegd tussen de door TTP's te leveren diensten en de beveiligingsdoelen. Ten slotte wordt aandacht besteed aan beleid en regelgeving met betrekking tot TTP's. Hoe wordt in 'overheidsland' tegen TTP's aangekeken, wat is de stand van zaken met betrekking tot de juridische status van digitale handtekeningen en mogelijke regelgeving op het gebied van cryptografie.

1 In de bijdrage van Biesheuvel en Olde Olthof wordt ingegaan op de stand van zaken en de ontwikkelingen op het gebied van electronic commerce.

BEVEILIGINGSDOELEN

Het plegen van (rechts)handelingen over het Internet roept op dit moment een aantal vragen op. De belangrijkste vragen houden verband met het al dan niet realiseren van de (beveiligings)eisen die aan een openbaar netwerk worden gesteld indien men wil communiceren over een open netwerk.

Zo kan een leverancier die goederen aanbiedt via een website zich afvragen:
1. of de bezoeker van de site inderdaad degene is die hij beweert te zijn;
2. of het niet de concurrent is die zich voor een ander uitgeeft om informatie te krijgen over bedrijfsactiviteiten van de leverancier;
3. of de bestelling van de bezoeker tijdens transport over het Internet niet is gewijzigd;
4. of een bezoeker achteraf kan ontkennen dat hij een bestelling heeft geplaatst;
5. in hoeverre de bezoeker bevoegd is een bestelling te plaatsen.

De websitebezoeker kan zich afvragen:
6. of de leverancier wel degene is die hij beweert te zijn. Ofwel is de leverancier bonafide en levert hij datgene wat hij belooft?;
7. of de gegevens die de bezoeker verstuurt ontoegankelijk zijn voor anderen dan de leverancier (of zijn personeel);
8. of het mogelijk is dat de verstuurde gegevens tijdens transport zijn gewijzigd.

Elk van deze vragen houdt verband met het realiseren van één van de vijf vereisten die aan netwerkbeveiliging kunnen worden gesteld. Deze vereisten, ook wel beveiligingsdoelen genoemd, zijn de in de inleiding genoemde vereisten van authenticiteit, vertrouwelijkheid, integriteit, onweerlegbaarheid en autorisatie van verzender en/of informatie.

De authenticiteit van de verzender van een bericht houdt in dat de verzender ook degene is die hij beweert te zijn (vragen 1, 2 en 6). De vertrouwelijkheid (ook wel confidentialiteit of exclusiviteit) van een bericht houdt in dat het bericht tijdens transport of opslag onleesbaar is voor iedereen die niet gerechtigd is kennis te nemen van het desbetreffende bericht (vraag 7). De integriteit van een bericht houdt in dat de inhoud ervan niet is veranderd tijdens transport of opslag (vragen 3 en 8). Onweerlegbaarheid (ook wel non-repudiation) houdt in dat de verzender achteraf niet kan ontkennen een bericht te hebben verstuurd (vraag 4). Met autorisatie kan de handelingsbevoegdheid van een partij worden bedoeld (vraag 5). Onder autorisatie kan ook toegangscontrole worden verstaan, dat is de zekerheid dat alleen daartoe gerechtigden toegang hebben tot een bericht (of tot een netwerk). Het bericht wordt geopend door degene aan wie het bericht is gericht (of wie toegang heeft tot – bepaalde delen van – een netwerk; vragen 2 en 7). Zo zou een aanbieder van goederen op het Internet bijvoorbeeld de toegang tot een gedeelte van zijn website kunnen reserveren voor 'goede' klanten.

CRYPTOGRAFIE

De mechanismen die worden gebruikt bij het realiseren van deze beveiligingsdoelen zijn gebaseerd op zogeheten symmetrische en asymmetrische cryptosystemen.

Symmetrisch cryptosysteem

In een symmetrisch cryptosysteem is de sleutel die wordt gebruikt voor versleuteling gelijk aan de sleutel die wordt gebruikt voor de ontsleuteling. Voordat daadwerkelijk een bericht naar een andere partij kan worden verstuurd, moet die ontvanger beschikken over de sleutel. De noodzakelijke uitwisseling van sleutels en het feit dat voor iedere partij waarmee men veilige communicatie mogelijk wil maken, een andere sleutel moet worden aangemaakt (en verspreid), leiden ertoe dat deze vorm van cryptografie niet ideaal is. Symmetrische encryptie is wel 'sneller' en dus voornamelijk interessant ter versleuteling van grote hoeveelheden data in een besloten omgeving.

Asymmetrisch cryptosysteem

Een asymmetrisch cryptosysteem, ook wel bekend als een public key cryptosysteem, maakt gebruik van een sleutelpaar bestaande uit een vercijfer- en een ontcijfersleutel. Eén sleutel is geheim (private key) en één sleutel is openbaar (public key). De twee sleutels corresponderen op een unieke wijze met elkaar en de private sleutel is, althans volgens de huidige stand van de techniek, niet te achterhalen op grond van de publieke sleutel. Er wordt gewerkt met twee publiek-private sleutelparen. Eén sleutelpaar wordt gebruikt ter waarborging van de vertrouwelijkheid en toegangscontrole, dus voor encryptie. Het andere sleutelpaar maakt het mogelijk een zogenaamde digitale handtekening te plaatsen, zodat de authenticiteit en de onweerlegbaarheid kunnen worden gewaarborgd. De digitale handtekening maakt het mogelijk een wilsuiting, noodzakelijk voor het verrichten van rechtshandelingen, te kunnen verrichten. De integriteit kan worden gewaarborgd door een hashwaarde, een unieke waarde vergelijkbaar met een vingerafdruk, van het te verzenden bericht te bepalen en die versleuteld met het originele bericht mee te zenden, waarna de ontvanger een 'verse' hashwaarde van het originele bericht bepaalt en die vergelijkt met de ontsleutelde meegezonden hashwaarde. Daar wijzigingen in een bericht leiden tot wijziging van de berekende hashwaarde en de versleutelde hashwaarde alleen toegankelijk is voor de ontvanger, is die ontvanger er zeker van dat een bericht ongewijzigd is aangekomen indien de twee hashwaarden gelijk zijn.

Symmetrisch en asymmetrisch cryptosysteem

Een public key cryptosysteem (asymmetrische encryptie) kan worden gebruikt voor encryptie en voor het plaatsen van digitale handtekeningen. Het nadeel van asymmetrische encryptie is echter dat dit systeem vanwege mogelijke inefficiëntie minder geschikt is (dan een symmetrisch cryptosysteem) voor de encryptie van grote hoeveelheden data. Daarom wordt bij moderne data-encryptie gebruik-

gemaakt van een combinatie van symmetrische en asymmetrische encryptie.

Het systeem werkt aldus: de afzender ondertekent een bericht eerst met zijn private sleutel, met zijn digitale handtekening. Vervolgens wordt het ondertekende document versleuteld met een symmetrische sleutel (deze sleutel kan random worden gegenereerd). Deze symmetrische sleutel wordt vervolgens versleuteld met de publieke sleutel van de ontvanger. De versleutelde boodschap en de versleutelde symmetrische sleutel worden verzonden. De ontvanger gebruikt zijn private sleutel om de symmetrische sleutel te achterhalen en ontsleutelt vervolgens – met behulp van de symmetrische sleutel – het bericht. Op deze manier worden de vertrouwelijkheid, de toegangscontrole, de onweerlegbaarheid en de integriteit gewaarborgd. De authenticiteit wordt gewaarborgd doordat de ontvanger de publieke sleutel van de afzender gebruikt ter verificatie van de – unieke – digitale handtekening van de afzender. Zie voor meer technische achtergrondinformatie het in deze Compact opgenomen artikel van Moonen.

PUBLIC KEY INFRASTRUCTURE

Het voordeel van het gebruik van encryptie is duidelijk. Resteert echter het probleem van de binding tussen enerzijds de publieke sleutel van het asymmetrische sleutelpaar en anderzijds de gebruiker van de private sleutel van dat sleutelpaar. Een zogeheten Public Key Infrastructure biedt, zoals hieronder wordt uiteengezet, en oplossing voor dit 'sleutelprobleem'.

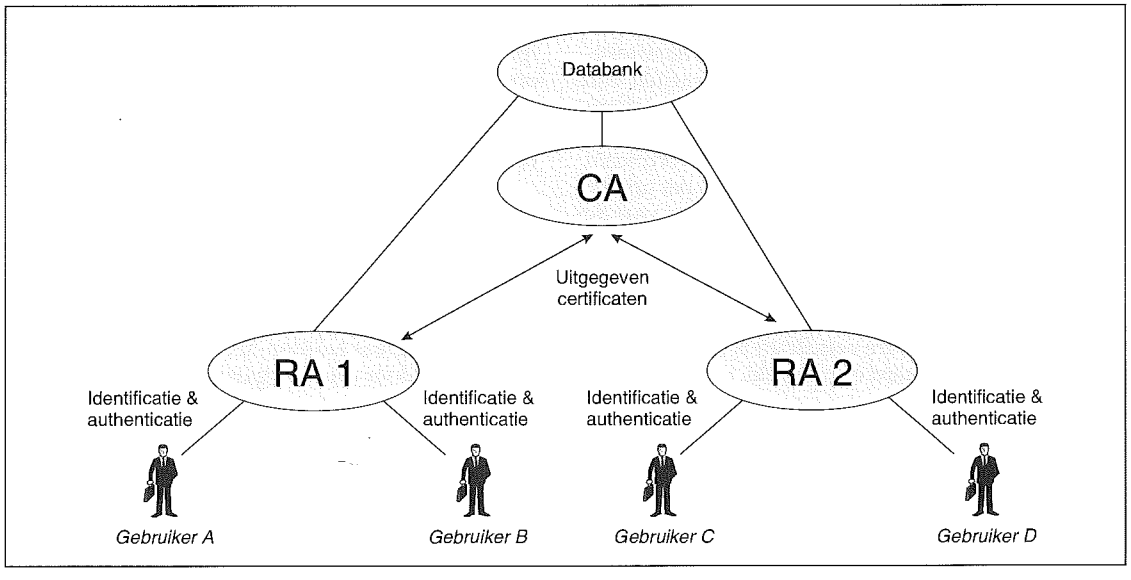
'Sleutelprobleem': gebrek aan vertrouwen

Voor het gebruik van een sleutelpaar met het oog op het realiseren van de genoemde beveiligingsvereisten is het noodzakelijk dat binding tussen enerzijds de publieke sleutel van het asymmetrische sleutelpaar en anderzijds de gebruiker van de private sleutel gegarandeerd is. In een puur digitale omgeving is die binding niet te garanderen. Door gebruik te maken van een Public Key Infrastructure (PKI), zo genoemd vanwege het feit dat de beveiliging voornamelijk gebaseerd is op het gelijknamige en hiervoor uiteengezette asymmetrische cryptosysteem, kan valselijk gebruik van sleutelparen (zowel het paar ten behoeve van encryptie als de digitale handtekening) worden tegengegaan. Met andere woorden, een PKI maakt het mogelijk sleutelparen een persoonsgebonden status te geven en wel met behulp van de Registration Authority-functie.

Een PKI is de infrastructuur waarbij gebruik wordt gemaakt van het public key cryptosysteem en door middel van de uitgifte van certificaten veilige communicatie tussen de gebruikers van die certificaten kan worden bewerkstelligd. Een PKI bestaat uit (ten minste) een Certification Authority (CA), één of meer Registration Authorities (RA's) en de gebruikers van de certificaten die worden uitgegeven. De kern van de PKI wordt gevormd door vertrouwen in de RA en de CA. Dit vertrouwen maakt dat gebruikers de certificaten waarmee ze digitale handtekeningen zetten (c.q. verifiëren) en berichten versleutelen (c.q. ontsleutelen) vertrouwen. De uitgegeven certificaten worden gepubliceerd in een openbaar toegankelijke databank. De functie van de databank is vergelijkbaar met die van een telefoonboek. De betrouwbaarheid van de identificatie en authenticatie die plaatsvond bij de RA is dus van fundamenteel belang voor de betrouwbaarheid van de certificaten opgenomen in dit 'telefoonboek'.

Om gebruikers van certificaten die door verschillende PKI's zijn uitgegeven in staat te stellen vertrouwelijk met elkaar te communiceren, kunnen afzonderlijke PKI's elkaars sleutels certificeren. We spreken dan van cross-certificering. Zo kan bijvoorbeeld een private CA (bijvoorbeeld een multinational met een eigen corporate network) worden gekoppeld aan een publieke CA, een CA die opereert in een open omgeving (waar bijvoorbeeld kleinere ondernemingen bij zijn aangesloten).

In figuur 1 zijn de verschillende componenten van een PKI weergegeven. Hoewel de databank niet als een afzonderlijke component kan worden aangemerkt, is zij vanwege het belang van haar functie



Figuur 1. Componenten binnen een PKI.

Tabel 1. Minimaal door CA en RA uit te voeren taken.

Component	Taken
Certification Authority (CA)	Uitgeven van certificaten Intrekken van certificaten Onderhouden van de directory (openbare lijst met certificaten)
Registration Authority (RA)	Registratie van de gebruikers Identificatie en authenticatie van de gebruikers

('telefoonboekfunctie') in de figuur opgenomen. In tabel 1 zijn de – minimaal uit te voeren – taken van de CA en RA weergegeven.

Toepassingen
Zoals gezegd maakt een Public Key Infrastructure het mogelijk tot betrouwbare elektronische *communicatie* te komen. De term communicatie heeft zowel betrekking op secure e-mail als op electronic commerce, maar ook op berichtenverkeer tussen burgers en bedrijven enerzijds en overheidsinstellingen anderzijds, zoals bijvoorbeeld elektronische belastingaangifte (zie hierover de bijdrage van Kemna in deze Compact), dan wel tussen overheidsinstellingen onderling. Een andere mogelijke toepassing van PKI is bijvoorbeeld beveiligd telewerken.

PKI-concept

Zoals hiervoor aangegeven wordt de kern van de PKI gevormd door vertrouwen in de Registration Authority en de Certification Authority. De Registration Authority is een organisatie die als belangrijkste taak heeft zorg te dragen voor de identificatie en authenticatie van de gebruikers die op het certificaat worden vermeld. Door gebruik te maken van een RA en een CA is het mogelijk de registratie en certificatie strikt te scheiden. Bovendien ontstaat door de instelling van meerdere RA's decentralisatie zodat het verkrijgen van certificaten eenvoudiger zal zijn.

De Certification Authority is de organisatie die de sleutels waarover hiervoor is gesproken, certificeert. Een gecertificeerde sleutel, vergezeld van de gegevens over de gebruiker (dit kan één persoon zijn, maar ook een groep personen) die met die sleutel is verbonden, wordt een certificaat genoemd. Met behulp van certificaten kunnen digitale handtekeningen worden geverifieerd, kan de integriteit van berichten worden gecontroleerd en kan de (handelings)bevoegdheid van een wederpartij worden gecontroleerd. De gegevens die op een certificaat zijn opgenomen, betreffen onder andere het unieke serienummer van het certificaat, de naam van de CA, de geldigheidsduur, de naam van de gebruiker, de handtekening van de CA, de encryptiesleutel (c.q. decryptiesleutel) of sleutel voor het zetten (c.q. verifiëren) van digitale handtekeningen en extensies. Voor de opmaak van een certificaat is de ITU-T Rec. X.509 versie 3-standaard ontwikkeld.

In een extensie op het certificaat wordt verwezen naar de toepasselijke Certificate Policy (CP). Binnen één PKI worden certificaten voor verschillende doeleinden gebruikt. Verschillende doeleinden zullen verschillende niveaus van vertrouwen – en dus beveiliging – eisen. Een CP bevat het geheel van regels waarin de toepassing van een certificaat voor een bepaalde toepasselijke gebruikersgroep, in overeenstemming met bepaalde beveiligingseisen (dus het noodzakelijke vertrouwen) wordt uiteengezet. Het geheel van die regels heeft een gestandaardiseerde opmaak (een standaard is bijvoorbeeld die van de PKIX Working Group van de Internet Engineering Task Force; de American Bar Association bereidt een standaard voor); dit maakt het mogelijk dat de Certificate Policies die binnen andere PKI's worden gehanteerd op eenvoudige wijze met de eigen policy kunnen worden vergeleken.

Een ander belangrijk document is de zogeheten Certificate Practice Statement (CPS). In de Certificate Practice Statement is het gehele proces van certificatie alsmede de wijze van beheer van certificaten beschreven. De CPS is als het ware de blauwdruk van de betrouwbaarheid van een CA. Een CA ondersteunt dus slechts één CPS, maar kan meerdere CP's ondersteunen. Een Certificate Practice Statement bevat juridische aspecten (rechten en verplichtingen van CA, RA en gebruikers en aansprakelijkheden van de verschillende partijen), organisatorische aspecten (sleutelbeheer, toegankelijkheid van directory met certificaten), procedurele aspecten (identificatie en authenticatie van gebruikers, procedures voor key escrow en revocation) en ten slotte beveiligingsaspecten (beveiliging bij de aanmaak van sleutels). De CPS heeft dezelfde gestandaardiseerde opmaak als de CP, maar beschrijft de elementen op een meer gedetailleerd niveau. Een voorwaarde voor cross-certificatie is dat de cross-certificerende CA's vertrouwen hebben in elkaars CPS, vandaar dat standaarden hier een nuttige rol kunnen vervullen (standaarden zijn bijvoorbeeld PKIX en SEIS; ook hiervoor bereidt de American Bar Association een standaard voor).

Van de twee sleutelparen per gebruiker worden dus in totaal twee certificaten aangemaakt: één voor het zetten c.q. verifiëren van digitale handtekeningen en één voor encryptie c.q. decryptie. De publieke certificaten zijn opgenomen in een voor iedere gebruiker toegankelijke lijst (directory). Door virtueel een certificaat van de beoogde communicatiepartij op te halen (downloaden) en de boodschap met de sleutel op het certificaat te encrypten kan betrouwbaar met die wederpartij worden gecommuniceerd. Een CA kan operationeel zijn binnen de eigen organisatie (private CA) of kan operationeel zijn binnen een open omgeving (publieke CA). Indien een publieke CA door een gehele gemeenschap gezien wordt als een onafhankelijke, onpartijdige betrouwbare autoriteit is sprake van een Trusted Third Party.

TTP-DIENSTEN

In deze paragraaf worden het begrip Trusted Third Party en de door een TTP geleverde diensten toegelicht.

TTP

Een Trusted Third Party is de partij die een faciliterende rol in het elektronische communicatieverkeer vervult. Met het begrip TTP wordt vaak de hierbo-

ven genoemde CA en/of RA bedoeld, maar een TTP kan ook andere functies vervullen. Hieronder worden eerst de kerndiensten en daarna een aantal aanvullende diensten aangegeven.

Kerndiensten

De te leveren kerndiensten zijn de volgende:

- Identificatie en authenticatie van gebruikers.

- Het uitgeven van certificaten.

- Het verzekeren van de integriteit van een bestand of boodschap.

- Het bieden van zekerheid omtrent de authenticiteit van de wederpartij: doordat de identiteit van de gebruiker van een certificaat is gecontroleerd door de RA, hebben partijen over en weer zekerheid dat zij te doen hebben met degene met wie zij denken te doen te hebben.

- Het bieden van zekerheid omtrent de vertrouwelijkheid van communicatie: door certificering van de publieke sleutel van het sleutelpaar dat wordt gebruikt voor encryptie en opname van dat certificaat in een zogeheten Certification List (CL) kan eenieder die vertrouwelijk met een andere partij wil communiceren de publieke (encryptie)sleutel van die wederpartij opvragen via de CL en met de sleutel op het certificaat zijn bericht encrypten.

- Beheren van certificaten: dit is de registerfunctie van een TTP. De TTP beheert een lijst met publieke certificaten, de Certification List, waarin de publieke sleutels ten behoeve van encryptie zijn opgenomen en de sleutels voor het verifiëren van digitale handtekeningen zijn opgenomen.

- Het intrekken van certificaten: bijvoorbeeld bij vermeend misbruik of in geval van verlies. De TTP geeft een zogenaamde Certification Revocation List (CRL) uit zodat bekend is welke certificaten – om welke reden dan ook – niet meer geldig zijn en wordt voorkomen dat alsnog (rechts)handelingen met die ongeldige certificaten kunnen worden verricht.

- Het beheren van encryptiesleutels (key escrow): er kan behoefte zijn aan een reserve-exemplaar van de (private) encryptiesleutel. Dit is bijvoorbeeld het geval indien een werknemer van werkgever wisselt en zijn private encryptiesleutel niet inlevert. De werkgever kan in een dergelijk geval de TTP verzoeken over te gaan tot key recovery, dus om hem het reserve-exemplaar te geven, zodat de werkgever de aan de werknemer gerichte berichten kan openen. Het bewaren van een reserve-exemplaar van de private sleutel voor het zetten van digitale handtekeningen stelt zeer hoge beveiligingseisen aan een TTP, omdat een ander bij doorbreking van de beveiliging van de TTP rechtshandelingen zou kunnen verrichten op valse naam en onweerlegbaarheid dan niet is gewaarborgd.

- Het 'updaten' van certificaten: indien een certificaat – bijna – verlopen is, of bijvoorbeeld de gegevens (autorisatie bijvoorbeeld) van de gebruiker zijn veranderd.

Een Trusted Third Party vervult een faciliterende rol in het elektronische communicatieverkeer.

Aanvullende diensten

Aanvullende diensten die door een TTP kunnen worden geleverd en waarmee zij toegevoegde waarde biedt, zijn onder andere de volgende:

- Time-stamping: is een bericht verzonden of opgeslagen op het tijdstip waarop een partij zegt dat dit is gebeurd? Deze dienst zal een belangrijke rol gaan vervullen in verband met de bewijskracht (onweerlegbaarheid) van digitaal ondertekende documenten (poststempelfunctie).

- Het digitaal verwerken van contracten met een digitale handtekening: is een contract ondertekend, gezien en akkoord verklaard? Een TTP kan een waarmerk verbinden aan een contract en zo de bewijskracht (onweerlegbaarheid) vergroten (notarisfunctie).

- Het bieden van informatie omtrent de autorisatie van een bepaalde gebruiker: in het door de TTP uitgegeven certificaat kan informatie worden opgenomen over de handelingsbevoegdheid van de houder (tot welk bedrag mag een persoon of een entiteit bijvoorbeeld transacties aangaan). Dit kan in business-to-business electronic commerce van grote waarde zijn (autorisatiecontrole-functie).

Een TTP kan als onderdeel van een Public Key Infrastructure in de vijf beveiligingsdoelen authenticiteit, integriteit, vertrouwelijkheid, onweerlegbaarheid en autorisatie voorzien. Het instellen van een TTP kan daarom als een belangrijke maatregel worden opgevat om betrouwbare electronic commerce te realiseren.

EISEN TE STELLEN AAN EEN TTP

Om te garanderen dat een TTP ook werkelijk trusted, betrouwbaar, is zal een TTP aan een aantal eisen moeten voldoen. De eisen hebben onder andere betrekking op:

- onpartijdigheid: een TTP mag geen der betrokken partijen bevoor- of benadelen;
- onafhankelijkheid: een TTP mag voor haar voortbestaan niet afhankelijk zijn van één of enkele partijen;
- continuïteit: het voortbestaan van de TTP moet zijn gegarandeerd om de beschikbaarheid van de dienstverlening te waarborgen;
- beveiliging: de computersystemen van een TTP moeten enerzijds zeer goed beveiligd zijn tegen aanvallen van buiten en van binnen, maar het systeem moet anderzijds ook transparant zijn, omdat de werking nauwgezet moet kunnen worden gecontroleerd (periodieke audit);
- deskundig personeel: het personeel moet aan bepaalde, hoge opleidings- en ervaringsvereisten voldoen.

Uiteraard zal er een verschil zijn in de eisen die worden gesteld aan TTP's die opereren in een privaat domein en TTP's die een publieke functie vervullen.

BELEID EN REGELGEVING

Er is ten aanzien van electronic commerce een aantal belemmeringen te onderkennen ([EUR97a], [MinEZ98a]). Belemmeringen die veelal onder te verdelen zijn in economische, technische en juridische belemmeringen. Hieronder zal worden ingegaan op beleid en regelgeving ten aanzien van een drietal juridische factoren die een negatieve invloed kunnen hebben op de ontwikkeling van electronic commerce. Ten eerste zal aandacht worden besteed aan cryptografie. Het door middel van encryptie vertrouwelijk kunnen verzenden van gegevens over het Internet wordt als een belangrijke voorwaarde gezien voor de succesvolle ontwikkeling van electronic commerce. In veel landen wordt echter, vanwege de vrees voor 'onzichtbaarheid' van criminele activiteiten, getracht export en/of het binnenlands gebruik van cryptografische producten te controleren. Vervolgens wordt ingegaan op vormvereisten in wet- en regelgeving die het gebruik van *elektronisch* dataverkeer ten behoeve van het verrichten van (rechts)handelingen kunnen belemmeren. Ten slotte wordt aandacht besteed aan digitale handtekeningen en – vanwege de in regelgeving veelal bestaande relatie tussen deze twee – daaraan gekoppeld TTP's.

Cryptografie

Cryptografische hardware en software is, zoals hiervoor uiteengezet, een noodzakelijk onderdeel van een PKI en aldus een noodzakelijke voorwaarde voor secure electronic commerce. Veel landen kennen exportbeperkingen ten aanzien van cryptografische producten en in sommige landen bestaat of wordt gesproken over een verplichting om, in verband met opsporingsonderzoek, in bepaalde gevallen (private) encryptiesleutels over te dragen aan de nationale (opsporings)autoriteiten.

Cryptografische hardware en software is een noodzakelijke voorwaarde voor secure electronic commerce.

Ingegaan zal worden op het beleid en de regelgeving inzake cryptografie in Frankrijk respectievelijk Duitsland, het Verenigd Koninkrijk en de Verenigde Staten. Tevens worden de Nederlandse situatie en de OECD-richtlijnen toegelicht.

Frankrijk
In Frankrijk bestaat al tientallen jaren wetgeving die encryptie reguleert. Op 27 juli 1996 is een nieuwe telecommunicatiewet aangenomen die de regulering van encryptie versoepelt. Nieuwe elektronische ontwikkelingen maken dit noodzakelijk. Handhaafbaarheid van het verbod is problematisch: encryptiemiddelen zijn – mede via het Internet – steeds eenvoudiger toegankelijk. Bovendien worden authenticatie en integriteit (bijvoorbeeld door middel van een digitale handtekening) als noodzakelijke voorwaarden gezien voor het slagen van electronic commerce; encryptie die wordt gebruikt voor digitale handtekeningen zal dan ook worden vrijgegeven. Andere cryptografische doelen zullen aan een vergunningenstelsel worden gebonden: een vergunning wordt afgegeven indien de private sleutel in beheer wordt gegeven bij een officieel erkende TTP. In de licentieovereenkomst met die TTP wordt opgenomen dat de TTP in bij de wet voorziene gevallen de sleutels over moet dragen aan de autoriteiten. De nieuwe wet is geïmplementeerd op 24 februari 1998 (decreten nr. 98-101 en nr. 98-102).

Duitsland, Verenigd Koninkrijk en Verenigde Staten
In verschillende landen bestaat wetgeving ten aanzien van de export van cryptografische producten. Dat betekent dat voor de export van dergelijke producten een vergunning vereist is. In bijvoorbeeld Duitsland, het Verenigd Koninkrijk en de Verenigde Staten is dit het geval.

In Duitsland bestaat over de wenselijkheid en de mogelijke vorm van regulering – naast de huidige exportbeperkingen – ten aanzien van cryptografische producten verschil van mening. In het bekende beleidsdocument 'Info 2000: Deutschlands Weg in die Informationsgesellschaft' ([Bund96]) wordt het aan encryptie verbonden gevaar van negatieve gevolgen ten aanzien van de opsporing van criminele activiteiten weliswaar onderkend, maar concrete oplossingen worden niet aangedragen.

Zoals hiervoor gezegd, bestaan in het Verenigd Koninkrijk exportbeperkingen ten aanzien van cryptografische middelen. Voor het overige is cryptografie in het Verenigd Koninkrijk – nog – ongereguleerd. De meest recente beleidsvisie is te vinden in een consultatiedocument 'Licensing of Trusted Third Parties for the Provision of Encryption Services' ([Dep97]) uit maart 1997 van het Department of Trade and Industry. Hierin wordt voorgesteld om TTP's die cryptografische diensten aanbieden, te binden aan een vergunningenstelsel. CA's zouden alleen een certificaat mogen afgeven indien de gebruiker de sleutel heeft gedeponeerd bij een officieel erkende key-escroworganisatie (een TTP). Het gebruik van cryptografie zou onder dit voorstel vrij blijven. De wisseling van de regering in het Verenigd Koninkrijk lijkt een remmend effect te hebben op de ontwikkelingen op het gebied van encryptie en TTP's. Labour is geen voorstander van de key-escrowoplossing en stelt voor om bij rechterlijke autorisatie verdachten te gebieden tot ontsleuteling over te gaan.

De Verenigde Staten kennen een exportverbod voor elektronische cryptografische middelen. Bij export is altijd een vergunning noodzakelijk. Indien het export van cryptografische producten met een sleutellengte van minder dan 56 bits betreft, volstaat een reguliere exportvergunning. Indien de sleutellengte groter is dan 56 bits is een key-recoveryfaciliteit vereist. Op nationaal niveau richten wetsvoorstellen zich met name op key escrow en key recovery. Aan de mogelijkheid van een op verdachten op te leggen

decryptiegebod wordt geen aandacht besteed, een dergelijk gebod zou in strijd kunnen zijn met het Vijfde Amendement.[2]

Nederland
In Nederland geldt, evenals in Duitsland, Frankrijk, het Verenigd Koninkrijk en de Verenigde Staten, een exportcontrole op cryptografische producten. Voor de export van cryptografische hardware en software moet een vergunning bij de Centrale Dienst voor In- en Uitvoer worden aangevraagd.

Uit een brief van de minister van Binnenlandse Zaken aan de Tweede Kamer, van februari dit jaar, blijkt dat met het oog op de toegankelijkheid van de inhoud van versleutelde berichten voor opsporings- en veiligheidsdiensten een deponeringsplicht van private cryptografische sleutels wordt overwogen ([MinBiZa98]). Dit idee strookt niet met de in het conceptwetsontwerp Computercriminaliteit II ([MinJus98a]) voorgestelde medewerkingsverplichting tot ontsleuteling van door middel van encryptie beveiligde berichten. Indien het voorstel wordt doorgevoerd, zijn de in het conceptwetsontwerp voorgestelde artikelen 126 lid 5 en 126t lid 5 Sv, respectievelijk van toepassing op de medewerking tot ontsleuteling van opgeslagen of stromende gegevens, overbodig. De Registratiekamer heeft de minister naar aanleiding van de brief aan de Tweede Kamer een advies geschreven waarin wordt verzocht het idee van een verplichte deponering van encryptiesleutels te heroverwegen.[3] De Registratiekamer stelt dat encryptie en TTP's van essentieel belang zijn voor het vertrouwen van de burger en maatschappelijke organisaties in de digitale snelweg. Bovendien is de Registratiekamer van oordeel dat betrouwbare encryptie, mede vanwege het privacybelang, onmisbaar is voor de ontwikkeling van electronic commerce. Geconcludeerd wordt dat verplichte deponering van encryptiesleutels negatieve gevolgen heeft voor de privacy en voor het vertrouwen van de markt. Het belang van opsporings- en veiligheidsdiensten weegt hier niet tegen op. In de brief aan de minister van Binnenlandse Zaken spreekt de Registratiekamer ten slotte haar zorg uit over de introductie van het onderscheid tussen zware (voor overheidsdiensten zoals ambassades of de krijgsmacht) en commerciële cryptografie door de minister van Verkeer en Waterstaat in een brief van 16 februari 1998 aan de Tweede Kamer. Ook dit onderscheid acht de Registratiekamer een onaanvaardbare belemmering van de privacy van de burger. Bovendien kan een dergelijk onderscheid, evenals de verplichte deponering van encryptiesleutels, een remmend effect hebben op de ontwikkeling van – electronic commerce op – de digitale snelweg.

OECD
De OECD (Organisation for Economic Co-operation and Development) heeft op 27 maart 1997 richtsnoeren voor cryptografie aangenomen. Het doel van de richtlijnen is het gebruik van cryptografie (bijvoorbeeld voor het gebruik van digitale handtekeningen) te stimuleren en zo de ontwikkeling van electronic commerce te bevorderen. Deze niet-bindende richtsnoeren behandelen een aantal basisonderwerpen die landen kunnen volgen bij het opzetten van wetgeving betreffende cryptografie. De richtsnoeren worden echter als vaag ervaren en geven niet voldoende aan welke richting landen kunnen volgen. Zo blijft de situatie bestaan waarin landen wachten op wat andere landen gaan ondernemen en blijft sprake van een internationale impasse.

TTP's zijn van essentieel belang voor het vertrouwen van de burger in de digitale samenleving.

Vormvereisten

In veel landen bestaan beperkingen ten aanzien van het elektronisch verrichten van rechtshandelingen en het gebruik van digitale handtekeningen. Vormvereisten zoals geschriftsvereisten, ondertekening (door partijen, notaris en getuigen) en voorlezing van een akte door de notaris kunnen een belemmering opleveren voor de ontwikkeling van electronic commerce.

Het Duitse recht bijvoorbeeld kent ongeveer 3800 geschriftsvereisten, met name in het civiele en in het handelsrecht. Deze vereisten belemmeren de erkenning van elektronisch verrichte rechtshandelingen.

Nederland
De meeste rechtshandelingen, zoals de koop van roerende zaken als een boek, zijn hier te lande vormvrij.[4] Voor bepaalde rechtshandelingen gelden echter één of meer vormvereisten. De notariële akte is bijvoorbeeld gebonden aan vormvereisten. Zo vindt de overdracht van een onroerende zaak plaats door middel van het verlijden van een geschrift, van een zogeheten transportakte door de notaris. In Nederland bevat de wet geen omschrijving van het begrip geschrift. Een veelgebruikte definitie van het begrip geschrift luidt 'iedere drager van verstaanbare leestekens die – in onderling verband – een gedachteninhoud vertolken'. Op welk materiaal deze leestekens zijn aangebracht, is irrelevant. Eveneens is het irrelevant of die leestekens bestaan in ons welbekende karakters dan wel in Chinese, in stenografische of in eigen gevormd geheimschrift. Hieruit blijkt dat een elektronisch leesbaar stuk onder de definitie van geschrift valt. Vormvereisten zijn echter opgenomen om in bepaalde waarborgen (het vereiste van schriftelijkheid heeft onder meer tot doel hetgeen is overeengekomen te bewijzen, de rechtszekerheid te dienen en fraude te voorkomen) te voorzien en het is van belang dat elektronische alternatieven ook die waarborgen bieden.

Een werkgroep heeft in het kader van de operatie Marktwerking, deregulering en wetgevingskwaliteit (MDW) onderzocht in welke mate in Nederland met betrekking tot rechtshandelingen geldende vormvereisten een belemmering vormen voor het elektronisch rechtsverkeer en of dient te worden voorzien in elektronische tegenhangers van (authentieke) akten ([MinJus98b]). 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. Besloten is om in het Burgerlijk Wetboek (BW) en in de Algemene wet bestuursrecht (Awb) experimenteerbepalingen op te

2 Het Vijfde Amendement luidt: 'No person shall be held to answer for a capital, or otherwise infamous crime, unless a presentment or indictment of a grand jury, except in cases arising in the land or naval forces, or in the militia, when in actual service in time of war or public danger; nor shall any person be subject to the same offence twice put in jeopardy of life or limb; nor shall be compelled in any criminal case to be a witness himself, nor be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation'.

3 Advies van de Registratiekamer aan de minister van Binnenlandse Zaken van 9 april 1998, kenmerk Registratiekamer 98.A.294.01. In haar advies van 9 maart 1998 (kenmerk Registratiekamer 98.A.089.01) had de Registratiekamer al uitgesproken dat het systeem van medewerkingsverplichting tot ontsleuteling van versleutelde berichten de voorkeur heeft boven een algemene deponeringsplicht voor encryptiesleutels.

4 Een rechtshandeling vereist een op een rechtsgevolg gerichte wil die zich door een verklaring heeft geopenbaard. Het openbaren van de wil (wilsuiting) verschilt in een elektronische omgeving niet van die in een fysieke omgeving. Vormvrij houdt in dat die wilsuiting in iedere vorm kan geschieden. Zo kan de wilsuiting ook in één of meer gedragingen besloten liggen.

nemen. Zo wordt de mogelijkheid gecreëerd om een elektronische variant van de – schriftelijke – transportakte te gebruiken en krijgen overheden de mogelijkheid over te gaan tot elektronische kennisgeving van besluiten, besluiten elektronisch toe te zenden en elektronisch ter inzage te leggen. Dit jaar (1998) zal een wetsvoorstel voor experimenteerbepalingen in het BW en de Awb worden voorbereid.

Digitale handtekening en TTP's

In veel landen bestaan belemmeringen voor het gebruik van digitale handtekeningen. Enerzijds als gevolg van vormvereisten, geschriftsvereisten en ondertekeningsvereisten en anderzijds als gevolg van de waardering van digitale handtekeningen als bewijs. In een groot aantal landen wordt momenteel gewerkt aan (concept)wetgeving die de digitale handtekening als elektronische equivalent van de ouderwetse geschreven handtekening erkent. Hieronder zal – in vogelvlucht – de wet- en regelgeving met betrekking tot digitale handtekeningen worden besproken. Voorts worden de initiatieven van UNCITRAL en de Europese Commissie met betrekking tot de juridische status van digitale handtekeningen aangegeven. Vaak zal de juridische status (gelijkstelling digitale handtekening aan geschreven handtekening en bewijskracht van digitale handtekeningen) van de digitale handtekening gekoppeld worden aan eisen die aan Certification Authorities (TTP's) zijn te stellen. Daarom wordt in deze subparagraaf tot slot aandacht geschonken aan het Nederlandse beleid met betrekking tot TTP's.

Wet- en regelgeving digitale handtekeningen
Op het gebied van digitale[5] handtekeningen bestaat regelgeving in onder andere Duitsland, de Verenigde Staten en Maleisië. In België, Denemarken en Zweden wordt momenteel gewerkt aan wetgeving voor digitale handtekeningen.

In de Duitse 'Gesetz zur digitalen Signaturen' (SigG), ook wel Signaturgesetz, onderdeel van de op 1 augustus 1997 in werking getreden 'Gesetz zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste' ([IuKDG97]) is de juridische status van een digitale handtekening gekoppeld aan eisen te stellen aan TTP's. Deze wet beschrijft het kader waarbinnen digitale handtekeningen op een betrouwbare wijze kunnen worden gebruikt. De wet gaat uit van een certificeringssysteem. Het is niet verplicht van gecertificeerde sleutels gebruik te maken voor het zetten van digitale handtekeningen, maar in gevallen waarin bijzondere zekerheid is gewenst, is het aan te bevelen gebruik te maken van de diensten van gecertificeerde organisaties. De rechtsgeldigheid van een digitaal ondertekende rechtshandeling wordt overigens niet met zoveel woorden door de IuKDG erkend. Het verkrijgen van een dergelijke vergunning is aan strenge eisen gebonden. Op 1 november 1997 is de 'Signaturverordnung' (SigV) ('Digital Signature Ordinance') van kracht geworden. Hierin zijn (procedurele) vereisten voor CA's opgenomen. Overeenkomstig artikel 17 lid 2 SigV is een conceptlijst met cryptografische algoritmen opgesteld waarvan het gebruik is toegestaan. Op 9 februari 1998 is deze lijst bekendgemaakt.

In de Verenigde Staten is in een groot aantal staten reeds wetgeving ingevoerd of voorgesteld op het gebied van digitale handtekeningen. De bekendste wet is de 'Utah Digital Signature Act'. Deze wet geeft een juridisch kader voor het gebruik van cryptografie voor authenticatie- en integriteitsdoeleinden. De eisen die in de wet ten aanzien van TTP's worden gesteld, zijn echter zo hoog dat sinds de invoering van de wet in 1995 slechts één TTP is opgericht. Dergelijke strenge eisen kunnen tot gevolg hebben dat een TTP zich in een gunstiger juridisch klimaat (lees: een andere staat) gaat vestigen, wat economisch gezien uiteraard ongunstig is.

UNCITRAL en Europese Commissie
De juridische status van digitale handtekeningen is momenteel onderwerp van onderzoek. Op internationaal niveau vindt beleidsvorming plaats door UNCITRAL (United Nations Commission on International Trade Law). UNCITRAL acht regelgeving op het gebied van digitale (en elektronische) handtekeningen en aspecten als CA's noodzakelijk, terwijl bestaande wetgeving dient te worden geharmoniseerd. De – niet-bindende – Model Law on Electronic Commerce fungeert als aanzet en voorbeeld voor de wijze waarop belemmeringen voor de ontwikkeling van elektronische handel kunnen worden weggenomen ([UNCI96]). Op het gebied van digitale handtekeningen is UNCITRAL in februari 1997 gestart met het ontwerpen van modelwetgeving. Dit heeft geresulteerd in Draft Uniform Rules on Electronic Signatures ([UNCI98]).

Op Europees niveau worden electronic commerce en het gebruik van digitale handtekeningen gestimuleerd. In de mededeling 'A European Initiative in Electronic Commerce' ([EUR97a]) van de Europese Commissie van 16 april 1997 erkent de Commissie dat digitale handtekeningen een noodzakelijke voorwaarde zijn om veiligheid en vertrouwen in communicatie via open netwerken te bewerkstelligen. Ook tijdens de Conferentie van Bonn ('Global Information Networks: Releasing the Potential' 6 t/m 8 juli 1997) werd de digitale handtekening als noodzakelijk voor het bedrijven van electronic commerce geoordeeld. De Commissie heeft als eerste stap een mededeling over beveiliging en vertrouwen in elektronische communicatie uitgevaardigd ([EUR97b]). In die mededeling wordt aangekondigd dat de Commissie zal bekijken of op communautair niveau in een wettelijke wederzijdse erkenning van digitale handtekeningen moet worden voorzien. Voorts wordt, gezien de uiteenlopende – concepten voor – wettelijke regelingen, overwogen gemeenschappelijke juridische randvoorwaarden voor CA's op te stellen. De Raad heeft die mededeling in december 1997 overgenomen en heeft de Commissie verzocht om een voorstel voor een richtlijn op te stellen. Recentelijk, op 13 mei 1998, heeft de Europese Commissie dit voorstel voor een 'common framework for electronic signatures' uitgevaardigd ([EUR98]). De richtlijn heeft tot doel om tot harmonisatie van de wetgeving betreffende elektronische handtekeningen op Europees niveau te komen om zo te voorkomen dat uiteenlopende wetgeving leidt tot verstoring van de interne (Europese) markt. Het verzekeren van wettelijke erkenning, in het bijzonder tussen lidstaten, van elektronische handtekeningen en TTP's[6] wordt beschouwd als het belangrijkste onderwerp. Hiertoe is het, aldus de Commissie, noodzakelijk om minimumvoorwaarden voor TTP's op te stellen.

5 Wat betreft wetgeving moet een onderscheid worden gemaakt tussen die voor elektronische handtekeningen en digitale handtekeningen. Het begrip elektronische handtekening omvat alle soorten van elektronische identificatie (waaronder de digitale handtekening). Voorbeelden zijn de pincode, gescande handtekening of biometrische technieken zoals een vingerafdruk of een scan van de iris. Wetgeving met betrekking tot elektronische handtekeningen (Florida, Texas) zal de wijze waarop 'de handtekening wordt gezet' onbepaald laten. De techniek is niet voorgeschreven, het vereiste beveiligingsniveau kan op meerdere wijzen worden bereikt. Wetgeving met betrekking tot digitale handtekeningen ziet specifiek op de techniek van encryptie. Door het opstellen van wetgeving met betrekking tot deze vorm van handtekeningen wordt aangegeven dat de techniek van digitale handtekeningen betrouwbaar wordt geacht en aldus wordt de juridische status van deze handtekening geregeld (onweerlegbaarheid, bewijskracht, mogelijkheid rechtshandelingen te verrichten).

6 Het voorstel van de Europese Commissie voor een richtlijn betreffende elektronische handtekeningen ([EUR98]) spreekt van 'certification service providers'. In art. 2 lid 6 van de conceptrichtlijn wordt een dergelijke provider gedefinieerd als 'a person who or entity which issues certificates or provides other services related to electronic signatures to the public'; deze omschrijving komt overeen met de taken die aan een Trusted Third Party kunnen worden toegekend.

Nederlands beleid ten aanzien van TTP's
Recentelijk is in Nederland op interdepartementaal niveau een aantal rapporten verschenen waarin aandacht wordt besteed aan TTP's, dan wel TTP's centraal staan. De in februari 1998 verschenen nota Wetgeving voor de elektronische snelweg ([MinJus98c]) van het Ministerie van Justitie behandelt de toepasbaarheid van het privaatrecht, het bestuursrecht en het strafrecht op de elektronische snelweg. In de nota wordt ingegaan op de rol die TTP's moeten gaan spelen in het elektronisch rechtsverkeer. Geconcludeerd wordt dat bij het garanderen van de juridische betrouwbaarheid van het elektronische verkeer een belangrijke rol voor TTP's zal zijn weggelegd. Gesteld wordt dat door middel van zelfregulering kan worden voorzien in de opstelling en naleving van eisen die aan de TTP als aanbieder van intermediaire diensten worden gesteld. Zelfregulering zou dienen te worden ondersteund door overheidstoezicht.

In de in de inleiding reeds aangehaalde ontwerpbeleidsnotitie met betrekking tot Trusted Third Parties ([MinEZ98b]), een gezamenlijke nota van het Ministerie van Economische Zaken en het Ministerie van Verkeer en Waterstaat, staan de technische inrichting en infrastructuur van TTP-diensten centraal. De definitieve nota over openbare TTP-diensten zal pas na de kabinetsformatie door het kabinet worden behandeld. Ondertussen is wel een start gemaakt met één van de aanbevelingen uit de ontwerpnota, namelijk het oprichten van een TTP-kamer ([Auto98]). De zogeheten TTP-kamer moet een waarborg vormen voor de betrouwbaarheid van zijn leden. Om voor lidmaatschap in aanmerking te komen zullen de aanbieders van TTP-diensten aan een aantal randvoorwaarden moeten voldoen. Er is een werkgroep opgericht bestaande uit de werkgeversorganisatie VNO, de Stichting Ediforum, Shell en de ministeries van Verkeer en Waterstaat, Justitie en Economische Zaken, die de oprichting van een TTP-kamer voorbereidt. In de ontwerpnota wordt voorts geconcludeerd dat er – vooralsnog – geen noodzaak tot het opstellen van wet- en regelgeving ten aanzien van TTP's bestaat.

BTW

Hoewel het onderwerp niet geheel in de context van dit artikel past, wordt vanwege de nieuwswaarde en het belang voor electronic commerce, kort stilgestaan bij de BTW-problematiek die elektronische handel met zich meebrengt. Recentelijk heeft de staatssecretaris van Financiën de notitie 'Belastingen in een wereld zonder afstand' ([MinFin98]) naar de Tweede Kamer gestuurd. In deze notitie wordt overwogen om elektronische handel drie jaar vrij te stellen van BTW-afdracht ([FinD98]). Het doel is de Nederlandse exportpositie te versterken door concurrentieverstoringen tussen binnenlandse en buitenlandse aanbieders weg te nemen en de ontwikkeling van informatie- en communicatietechnologie in Nederland te stimuleren. Een dergelijk nultarief is slechts mogelijk met unanieme toestemming binnen de EU. Nederland heeft inmiddels de introductie van een tijdelijk nultarief binnen de EU aan de orde gesteld.

Verschil in BTW-systemen kan als gevolg van het toenemende gebruik van het Internet voor commerciële activiteiten leiden tot verplaatsing van handelsstromen en zelfs tot verplaatsing van bedrijven. Op dit moment worden vanuit bijvoorbeeld de Verenigde Staten digitale goederen en diensten (zoals software en muziek die kunnen worden 'gedownload') aan afnemers in de Europese Unie verkocht. Particulieren kunnen deze producten aanschaffen zonder dat ze BTW hoeven te betalen. Dit zal de afzet van de leverancier uit de Verenigde Staten uiteraard ten goede komen, maar de afzet (export en binnenlandse afzet) van Nederlandse aanbieders van dergelijke te digitaliseren waren negatief beïnvloeden. Het gevolg is dat handelsstromen naar elders worden verplaatst. Ten tweede kan verschil in BTW-heffing tot gevolg hebben dat bedrijven zich verplaatsen naar een land waar geen BTW wordt geheven. Financiële instellingen bijvoorbeeld hebben in Nederland geen recht op vooraftrek. Dit houdt in dat dergelijke instellingen de BTW betaald over bijvoorbeeld de aanschaf van een kantoor en de meubelen niet kunnen aftrekken en dat BTW dus een kostenpost voor deze instellingen is. Door zich te vestigen in een land waar geen BTW wordt geheven, kunnen zij die kosten vermijden. De klanten kunnen via het Internet (Internet Banking) worden bediend.

Handel via Internet biedt naast commerciële pluspunten voor bepaalde producten en diensten interessante BTW-voordelen.

Vanuit instanties als de World Trade Organisation (WTO), de Organisation for Economic Co-operation and Development (OECD) en de EU wordt gezocht naar een oplossing voor de BTW-kwestie. Internationale overeenstemming zal echter nog wel even op zich laten wachten. Voorlopig biedt handel via Internet naast de commerciële pluspunten dus interessante BTW-voordelen. Gezien het feit dat BTW-vrij aangeboden diensten vanuit derde landen praktisch niet tegen te houden zijn, is het zeer de vraag of heffing van BTW ter zake van electronic commerce op langere termijn wel wenselijk is. Encryptie maakt het onmogelijk om transacties te controleren. Ook als houders van een certificaat verplicht zouden worden gesteld een kopie van de private encryptiesleutel af te staan aan de nationale overheid zal de omvang van het berichtenverkeer het onmogelijk maken ieder bericht te controleren. Indien electronic commerce wordt vrijgesteld van BTW-heffing zullen ook de 'traditionele' diensten en fysieke goederen die door electronic commerce dreigen te worden vervangen tegen een nultarief moeten worden aangeboden, willen de verkopers van de traditionele diensten en fysieke goederen kunnen overleven.

Trusted Third Parties kunnen – als onderdeel van een PKI – de identiteit van aanbieder en afnemer garanderen en zodoende op internationaal niveau secure electronic commerce mogelijk maken. Door certificaten uit te geven ontstaat zekerheid omtrent de identiteit van een natuurlijke persoon of een bedrijf. Door transacties door middel van het certificaat digitaal te ondertekenen, ontstaat een onlosmakelijke koppeling tussen de identiteit van een per-

Mw. mr. drs. A.W. Duthler Is sinds 1993 werkzaam bij KPMG EDP Auditors als adviseur informaticarecht, sinds 1997 in de functie van manager bij KPMG TTP Services in Amsterdam. Tevens is zij verbonden aan de afdeling Recht en Informatica van de Rijksuniversiteit Leiden, alwaar zij een proefschrift over de juridische aspecten van Trusted Third Parties voorbereidt. Zij studeerde Bestuurskunde aan de Technische Universiteit Twente en rechten aan de Rijksuniversiteit Leiden.

Mw. mr. M.J.Dontje Is sinds maart 1998 werkzaam bij KPMG TTP Services. Studeerde Nederlands Recht aan de Vrije Universiteit te Amsterdam. Studeerde af in de hoofdrichtingen Privaatrecht en Strafrecht. Schreef voor beide richtingen een scriptie bij de vakgroep Informatica en Recht. De privaatrechtelijke scriptie had privacybescherming en Air Miles als onderwerp en de strafrechtelijke scriptie betrof een rechtsvergelijkende studie naar uitingsdelicten op het Internet. Rondt binnenkort haar studie Bedrijfseconomie, eveneens aan de VU, af.

soon/bedrijf en de door die persoon of dat bedrijf verrichte transacties. Door inschakeling van een TTP kunnen bedrijven en particulieren op een veilige wijze electronic commerce bedrijven en eventueel profiteren van BTW-voordelen. TTP's kunnen echter ook BTW-afdracht ondersteunen: door gebruik te maken van een TTP kan wel degelijk de identiteit van aanbieder en afnemer worden gegarandeerd en kan zodoende BTW-afdracht mogelijk worden gemaakt.

CONCLUSIE

Het vertrouwen van burgers, bedrijfsleven en ook overheid dat het mogelijk is op een betrouwbare wijze elektronisch te kunnen communiceren, is noodzakelijk om toepassingen als electronic commerce en bijvoorbeeld ook elektronische verstrekking van vergunningen te realiseren en – wellicht belangrijker – tot een succes te maken. TTP's vervullen een zeer belangrijke rol in de infrastructuur (PKI) die betrouwbare elektronische communicatie mogelijk maakt. Op nationaal niveau is het initiatief om een TTP-kamer op te richten een eerste stap in de goede richting. Het opnemen van experimenteerbepalingen in het Burgerlijk Wetboek en de Algemene wet bestuursrecht teneinde vormvereisten als schriftelijkheid of een authentieke akte die het elektronisch verrichten van rechtshandelingen belemmeren op te heffen, is eveneens toe te juichen. Initiatieven om te komen tot uniforme regels betreffende de digitale (of elektronische) handtekeningen (zoals door UNCITRAL en de Europese Commissie) en de vereisten te stellen aan diensten geleverd door TTP's (aangemoedigd door de Europese Commissie), teneinde internationaal juridische erkenning te realiseren, zijn van harte te onderschrijven. Internationale overeenstemming kan baanbrekend werken op het gebied van elektronische communicatie in het algemeen en electronic commerce in het bijzonder.

LITERATUUR

[Auto98] Automatisering Gids, 1 mei 1998.

[Bund96] Bundesministerium für Wirtschaft, *Info 2000: Deutschlands Weg in die Informationsgesellschaft*, februari 1996, http://www.bmwi-info2000.de/gip/programme/info2000/index.html

[Dep97] Department of Trade and Industry, *Licensing of Trusted Third Parties for the Provision of Encryption Services*, maart 1997, http://dtiinfo1.dti.gov.uk/pubs

[EUR97a] European Commission, Communication to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, *A European Initiative in Electronic Commerce*, COM(97)157, http://www.cordis.lu/esprit/src/ecomcom.htm

[EUR97b] European Commission, Communication to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, *Towards A European Framework for Digital Signatures And Encryption*, COM (97)503, http://www.ispo.cec.be/eif/policy/97503toc.html

[EUR98] European Commission, Communication to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, *Proposal for a European Parliament and Council Directive on a common framework for electronic signatures*, COM (98)297/2, http://www.ispo.cec.be/eif/policy

[FinD98] Het Financieele Dagblad, 5 mei 1998.

[IuKDG97] Gesetz zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste (IuKDG), augustus 1997, http://www.iid.de/rahmen/iukdgebt.html

[MinBiZa98] Minister van Binnenlandse Zaken, TK, 1997-1998, 21 501-10, nr. 38.

[MinEZ98a] Ministerie van Economische Zaken, *Actieplan Electronic Commerce*, maart 1998, http://info.minez.nl/pdfs/05r38.pdf

[MinEZ98b] Ministerie van Economische Zaken en Ministerie van Verkeer en Waterstaat, *Eindrapportage Nationaal TTP-project*, april 1998.

[MinFin98] Ministerie van Financiën, *Notitie belastingen in een wereld zonder afstand*, mei 1998, http://www.minfin.nl/nieuws/AFP-224.htm

[MinJus98a] Ministerie van Justitie Directie Wetgeving, *Voorontwerp wijziging van het Wetboek van Strafrecht en het Wetboek van Strafvordering in verband met nieuwe ontwikkelingen in de informatietechnologie (Computercriminaliteit II)*, januari 1998.

[MinJus98b] 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/pb274.htm

[MinJus98c] Ministerie van Justitie, *Wetgeving voor de elektronische snelweg*, TK 1997-1998, 25 880, nrs. 1-2, http://www.minjust.nl/sdu/index.htm

[UNCI96] United Nations Commission on International Trade Law (UNCITRAL), General Assembly Resolution, *Model Law on Electronic Commerce*, December 1996, http://www.un.or.at/uncitral/texts/electcom/ml-ec.htm#TOP

[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.mbc.com/legis/uncitral-1.html

Electronic commerce en TTP-dienstverlening, een praktijkvoorbeeld uit de bouwbranche

Ing. J.A.M. Hermans en A. Bruggeman

De bouwbranche is één van de eerste branches waar een virtuele marktplaats wordt gecreëerd en electronic commerce wordt toegepast. De inzet van een Trusted Third Party wordt als essentieel gezien voor het succes.

INLEIDING

Elektronische berichtenuitwisseling is sterk in opkomst. Deze elektronische berichtenuitwisseling kan de operationele uitvoering van de dienstverlening aanzienlijk verbeteren en vergemakkelijken. Met name in de bouwbranche is een goede inrichting van de informatie- en communicatiekanalen zeer belangrijk vanwege de grote hoeveelheid betrokken partijen in de bouwnijverheid. Tijdens de uitvoer van projecten is er behoefte bij toeleverende fabrikanten, groothandels, overkoepelende organen, aannemers, architecten en installateurs om op een flexibele en betrouwbare wijze met elkaar te communiceren. Er dient bijvoorbeeld voortdurend (bouw)locatiespecifieke informatie naar hoofdkantoren en toeleveranciers van gereedschappen en materialen gecommuniceerd te worden. Het gebruik van elektronisch berichtenverkeer zal in deze context tot efficiency-verbeteringen leiden. Om dit voor de bouwbranche te bewerkstelligen heeft IntraBouw een eigen 'Internet' voor de bouw- en installatiewereld opgericht.

Naast een platform voor onderlinge communicatie biedt het IntraBouw-netwerk ook informatiediensten gericht op de bouwbranche en toegespitst op alle betrokken partijen. Andere derde partijen zoals makelaars, notarissen en het Kadaster zullen in de toekomst ook vertegenwoordigd zijn, zodat een volledige (virtuele) elektronische marktplaats kan ontstaan. Dit artikel geeft een beeld van de redenen waarom voor IntraBouw TTP-dienstverlening een cruciale factor is en op welke wijze TTP-dienstverlening is gerealiseerd.

KANSEN EN BEDREIGINGEN

Electronic commerce biedt volop kansen voor de bouwbranche. Naast kostenbesparingen die op korte termijn gerealiseerd kunnen worden, vormt elektronisch berichtenverkeer de eerste stap naar een virtuele marktplaats. Er ontstaat een geheel nieuwe dynamiek in de markt. Klant-leverancierrelaties veranderen, nieuwe samenwerkingsverbanden ontstaan en IntraBouw-deelnemers worden door de communicatie-infrastructuur in staat gesteld gezamenlijk (als virtuele organisaties) op te treden. Verder wordt door het toepassen van electronic commerce een betere en bredere benutting van informatiebronnen mogelijk.

Een voorwaarde voor het slagen van electronic commerce is te voorzien in voldoende vertrouwen. Dit vertrouwen is tweeledig en betreft:
- vertrouwen in de handelspartners op het Internet;
- vertrouwen in de juridische geldigheid van de verzonden en ontvangen berichten.

Daarnaast dient ruime aandacht te zijn geschonken aan beveiliging van het Internet en de daarover aangeboden en getransporteerde informatie. Het verkrijgen van voldoende vertrouwen kan worden gerealiseerd door gebruik te maken van een Trusted Third Party. Door het verlenen van TTP-diensten door IntraBouw kan betrouwbare digitale gegevensuitwisseling plaatsvinden en kan IntraBouw electronic commerce faciliteren.

WAT IS INTRABOUW?

IntraBouw, bijgenaamd het eigen Internet van en voor de bouw- en installatiewereld, is een zakelijk gespecialiseerd netwerk met als doel een bijdrage te leveren aan het structureel verbeteren van de informatievoorziening binnen de bouwwereld. Het verbeteren van de informatievoorziening dient uiteindelijk te leiden tot productieverbetering en kostenverlaging voor de leden van IntraBouw.

IntraBouw levert een bijdrage aan de verdere professionalisering van de bouwnijverheid. Dit doet zij door het definiëren, realiseren en exploiteren van een *infrastructuur* die communicatie, informatieontsluiting en samenwerking van groepen ondersteunt en door het opzetten van een digitale marktplaats. Het huidige platform voor deze dienstverlening is een op Internet-technologie gebaseerd netwerk (een extranet). De toegevoegde waarde wordt gerealiseerd door ten eerste de interactie tussen de leden die actuele informatie uitwisselen en waartussen (betrouwbare) transacties plaatsvinden, ten tweede de inhoud van de berichten die de deelnemende partijen aan elkaar aanbieden, ten derde de snelheid waarmee informatie gedeeld kan worden en tot slot de afspraken die direct tussen de communicerende partijen kunnen worden gemaakt. Om succesvol te kunnen zijn dient IntraBouw als facilitair bedrijf ervoor te zorgen dat haar dienstverlening ten minste de factoren afdekt die zijn weergegeven in tabel 1.

Clusters	Factoren
Infrastructuur	• snelheid • gebruiksvriendelijkheid • betrouwbaarheid • autorisatie • beveiliging
Institutioneel	• handelswetgeving • fiscale wetgeving • trust • privacy • betalingsverkeer
Bedrijfseconomisch	• omvang van de markt • investeringen

Tabel 1. Factoren voor succesvol zakelijk Internetgebruik ([Gerr97]).

Deelnemers

IntraBouw wil met haar deelnemers een afspiegeling van de gehele bouw- en installatiewereld vormen. Het streven is te komen tot een evenwichtige opbouw van maatschappelijke organisaties, toeleverende fabrikanten, groothandels, overkoepelende organen, aannemers, architecten, installateurs, dienstenleveranciers, etc. Om succesvol te kunnen zijn is het noodzakelijk dat alle partijen die actief zijn in de bouwnijverheid, op termijn gebruik kunnen maken van dit netwerk.

Doelstellingen

IntraBouw heeft als doelstelling dé electronic-commerceprovider in de bouw- en installatiebranche te worden. Zij wil haar leden de gelegenheid bieden de mogelijkheden van de elektronische snelweg optimaal te benutten. In een vroeg stadium is reeds onderkend dat, wil IntraBouw deze rol kunnen vervullen, naast het bieden van een reeks faciliteiten, ook de voorwaarde 'trust' moet zijn ingevuld. Deze voorwaarde kan worden ingevuld door de inzet van een Trusted Third Party. Een dergelijke onafhankelijke derde partij kan voorzien in betrouwbaarheidsdiensten (verzekeren van de identiteit van handelspartners alsmede de integriteit, vertrouwelijkheid en onweerlegbaarheid van berichtenverkeer en bijvoorbeeld het registreren van tijdstip van verzending en ontvangst) die noodzakelijk zijn om electronic commerce binnen de bouwwereld tot een succes te maken.
Dit is de reden waarom binnen het gehele IntraBouw-concept TTP-dienstverlening een cruciale rol speelt. Zonder TTP-dienstverlening zal het gehele IntraBouw-concept niet boven het niveau van een kleine Internet-serviceprovider kunnen uitgroeien.

ROADMAP VOOR TTP-DIENSTVERLENING

Het opzetten van TTP-dienstverlening en zeker de inbedding in het bestaande IntraBouw-concept is geen sinecure. Dit is dan ook de reden dat bij het vormgeven van de benodigde TTP-dienstverlening gestart is met het opstellen van een zogenaamde 'Roadmap'.

Deze roadmap kan gekenschetst worden als een richtinggevend document waarin het concept TTP-dienstverlening wordt beschreven, alsmede de impact van TTP-dienstverlening op het IntraBouw-concept. Verder beschrijft de roadmap een mogelijke strategie voor de realisatie van TTP-dienstverlening. Verschillende stappen worden gedefinieerd om te komen tot de uiteindelijke vorm van TTP-dienstverlening, die het meest geschikt is voor IntraBouw en haar leden.

Voor wie was deze roadmap nu eigenlijk bedoeld? Aangezien het concept TTP een relatief nieuw concept is en nog niet bekend is bij het merendeel van de beslissers van een organisatie, is deze roadmap met name bedoeld voor het management van een organisatie. Enerzijds om gevoel te krijgen voor de materie en anderzijds om besluitvorming hieromtrent mogelijk te maken.

Veel TTP-trajecten zijn ten onrechte te vaak gericht op technische aspecten, terwijl aspecten zoals organisatie, processen, procedures en wetgeving veelal onderbelicht blijven. De realisatie van TTP-dienstverlening is geen puur 'IT-oriented'-traject, maar voor een veel belangrijker deel een 'Business oriented'-traject. De implementatie van een Public Key Infrastructure zal invloed hebben op de gehele organisatie.[1] Het business Performance Model, zoals dat hieronder wordt toegelicht, geeft weer welke aandachtsgebieden invloed hebben op de prestatie van een organisatie. Daarbij wordt dit model gesplitst in twee delen, te weten het 'business oriented'-deel en het 'IT-oriented'-deel. Beide delen belichten de diverse onderdelen van het TTP-traject.

BUSINESS PERFORMANCE MODEL

Binnen het Business Performance Model zijn vier aandachtsgebieden te onderkennen, die de prestatie van een organisatie beïnvloeden. Dit zijn de volgende:

- Management & organisatie;
- IT-infrastructuur;
- Bedrijfsprocessen;
- Personeel & cultuur.

Deze vier aandachtsgebieden komen terug in het 'Business oriented'-deel en het 'IT-oriented'-deel van het model. In de toelichting van deze beide delen worden deze vier aandachtsgebieden dan ook nader uitgelegd. Ieder van de aandachtsgebieden uit het Business Performance Model dient voldoende belicht te worden. Tevens dienen de afzonderlijke aandachtsgebieden met elkaar in balans te zijn. Indien TTP-dienstverlening niet op een evenwichtige en volledige manier is geïmplementeerd, kan de 'performance' van de organisatie negatief worden beïnvloed.

Hieronder wordt ingegaan op het 'business oriented'-deel van de TTP-dienstverlening, daarna op het 'IT-oriented'-deel.

'Business-oriented'-deel

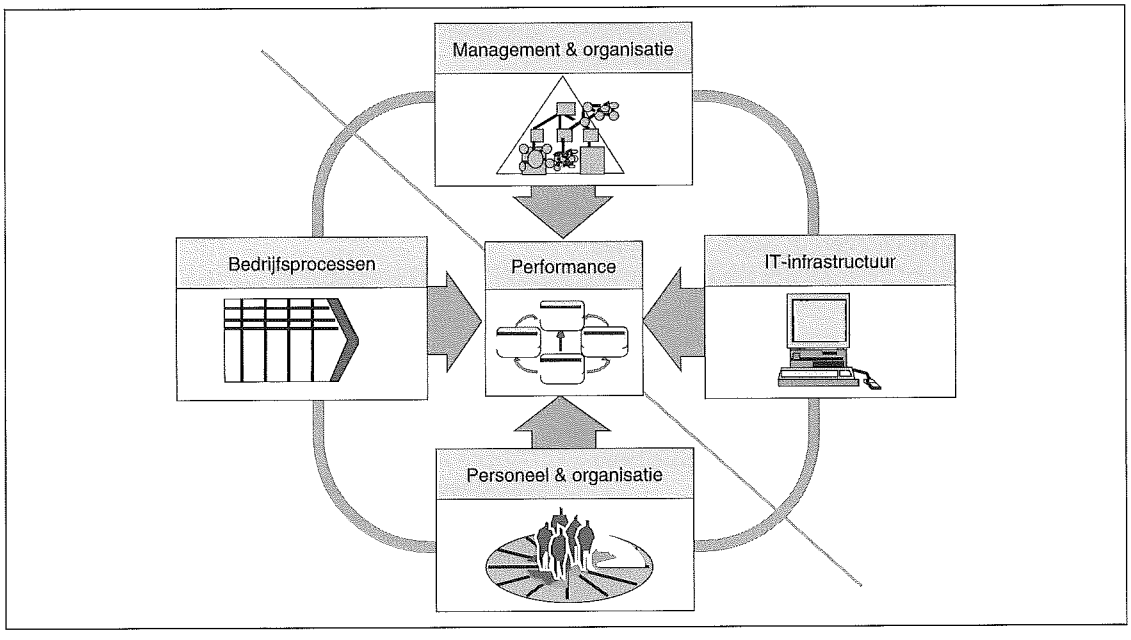
Aandachtsgebieden binnen het 'business oriented'-deel worden beschreven in een organisatorische architectuur. De in figuur 2 weergegeven aandachtsgebieden zijn :

- *Infrastructuur:* de langetermijn-faciliterende structuur van de organisatie, te weten: overeenkomsten, contracten, juridisch kader, informatietechnologie, gebouwen, etc.

- *Management & organisatie:* de organisatiestructuur, planning & control mechanismen en managementstijlen van een organisatie.

- *Processen & services:* de processen (primaire en ondersteunende) en services die een toegevoegde waarde vormen voor de organisatie.

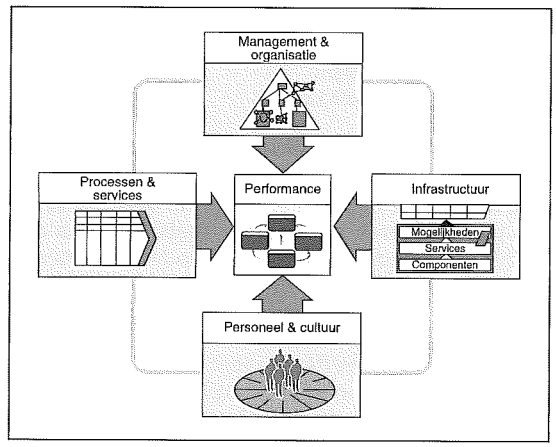
- *Personeel & cultuur:* de verwachtingen ten aanzien van het personeel en zijn capaciteiten, de benodigde communicatie.



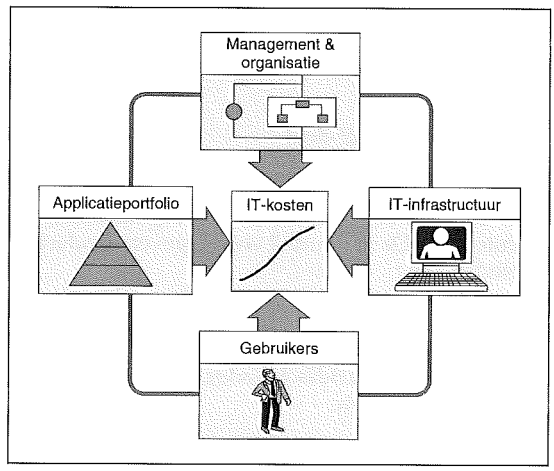
Figuur 1.
De vier aandachtsgebieden van het BPM.

1 In het artikel van Duthler en Dontje wordt het begrip PKI nader uitgelegd.

Figuur 2.
'Business oriented'-aspecten.



Figuur 3.
'IT-oriented'-aspecten.



Deze aandachtsgebieden, die een directe invloed hebben op de operationele uitvoering van de TTP-dienstverlening, dienen beschreven te zijn in een zogenaamde Certification Practice Statement (CPS). Een CPS kan worden beschreven als de tekstuele representatie van de betrouwbaarheid van de door een TTP verleende diensten. In het artikel van Duthler en Dontje in deze Compact wordt hier meer over gezegd. Zoals vermeld wordt in het 'Business oriented'-gedeelte de organisatorische architectuur vastgelegd. Met name worden beschreven de introductie en inbedding van de TTP-dienstverlening binnen de organisatie zelf. De volgende documenten dienen te worden opgeleverd:

Businessplan
De TTP-dienstverlening heeft impact op het totale dienstverleningspakket van de organisatie die deze diensten gaat verlenen. Derhalve zal deze nieuwe dienstverlening, beschreven in een businessplan, getoetst dienen te worden aan de strategie van de organisatie.

Personeelsplan
De benodigde organisatorische veranderingen dienen beschreven te worden in een personeelsplan. Zo zullen functiebeschrijvingen aangepast dienen te worden aan de voor de TTP-dienstverlening benodigde functies.

Communicatie- & marketingplan
De TTP-dienstverlening dient gecommuniceerd en ge-'market' te worden naar afnemers en gebruikers om een groot draagvlak te creëren.

Handboek Administratieve Organisatie
Het uitvoeren van TTP-dienstverlening dient op een beheersbare en gecontroleerde wijze te geschieden. Zo zullen de procedures en controlemaatregelen in detail beschreven dienen te zijn in de Administratieve Organisatie. Een groot deel wordt reeds beschreven in de Certification Practice Statement. De procedures en maatregelen die voor TTP-dienstverlening nodig zijn, dienen ingebed te worden in de bestaande procedures.

'IT-ORIENTED'-DEEL

Binnen het 'IT-oriented'-deel kunnen de vier aandachtsgebieden als volgt gedefinieerd worden:

- *IT-infrastructuur:* de resources in termen van IT-personeel, hardware, software en netwerken welke noodzakelijk zijn voor het opzetten en beheren van de applicatieportfolio noodzakelijk voor TTP-dienstverlening.

- *Management & organisatie:* de organisatiestructuur, planning & control, en managementprincipes van de IT-organisatie.

- *Gebruikers:* de gebruikersomgeving die noodzakelijk is voor het optimaal, effectief en efficiënt gebruik van de applicatieportfolio om de bedrijfsdoelstellingen te bereiken.

- *Applicatieportfolio:* de geautomatiseerde hulpmiddelen die voor de gebruikers noodzakelijk zijn om de bedrijfsdoelstellingen te behalen.

Ook voor de IT-architectuur geldt dat de IT-maatregelen benodigd voor de beheersing en operationele uitvoering van de TTP-dienstverlening beschreven staan in de Certification Practice Statement (CPS).

In het 'IT-oriented'-gedeelte wordt hoofdzakelijk de inbedding in de bestaande IT-omgeving van de organisatie beschreven. De hierbij van belang zijnde documenten en activiteiten zijn:

Informatie- en automatiseringsplan
De voor TTP-dienstverlening benodigde IT-middelen zullen hun weerslag hebben op de bestaande informatie- en automatiseringsomgeving, zoals deze staat beschreven in het informatie- en automatiseringsplan.

(Informatie)beveiligingsplan
TTP-dienstverlening kan pas vertrouwen genieten, indien voldoende beveiligingsmaatregelen zijn getroffen. Het samenstel van beveiligingsmaatregelen dient beschreven te worden in het informatiebeveiligingsplan.

IT-beheersomgeving
TTP-dienstverlening dient ingebed te worden in de bestaande IT-beheersorganisatie. Zo dienen de beheersprocessen rondom de TTP-dienstverlening ingevuld en geïntegreerd te worden in de bestaande processen.

Automatiseringscontracten
Indien sprake is van automatiseringscontracten (outsourcing, onderhoud, etc.) zullen deze beoordeeld dienen te worden in het licht van de TTP-dienstverlening. Door het vertrouwelijke karakter van deze dienstverlening zullen vaak striktere eisen benodigd zijn.

Gebruikerstrainingen
Om tot effectief en efficiënt gebruik te komen van de Public Key Infrastructure is het van belang dat alle gebruikers bekend zijn met de mogelijkheden van het systeem. Effectief en efficiënt gebruik zal de performance van de organisatie sterk verbeteren.

Applicatieportfolio
De IntraBouw-site gaat uit van het web-based concept, waarbij de gebruikers via het Internet de site kunnen benaderen. Daarbij zal de site enerzijds publiek, anderzijds alleen voor leden toegankelijk zijn. Binnen het afgesloten gebied kunnen gebruikers op basis van het door de TTP uitgegeven certificaat (waarbij de TTP een unieke koppeling tussen gebruiker en certificaat verzekert) toegang verkrijgen tot diverse applicaties van het Sociaal Fonds Bouwnijverheid. Verder kunnen ze toegang verkrijgen tot de Bomatelboulevard, alwaar ze bestellingen kunnen doen of informatie kunnen opvragen bij de verschillende onderliggende organisaties. Het gevolg van het web-based concept is dat de diverse applicaties aangepast dienen te worden aan dit concept.

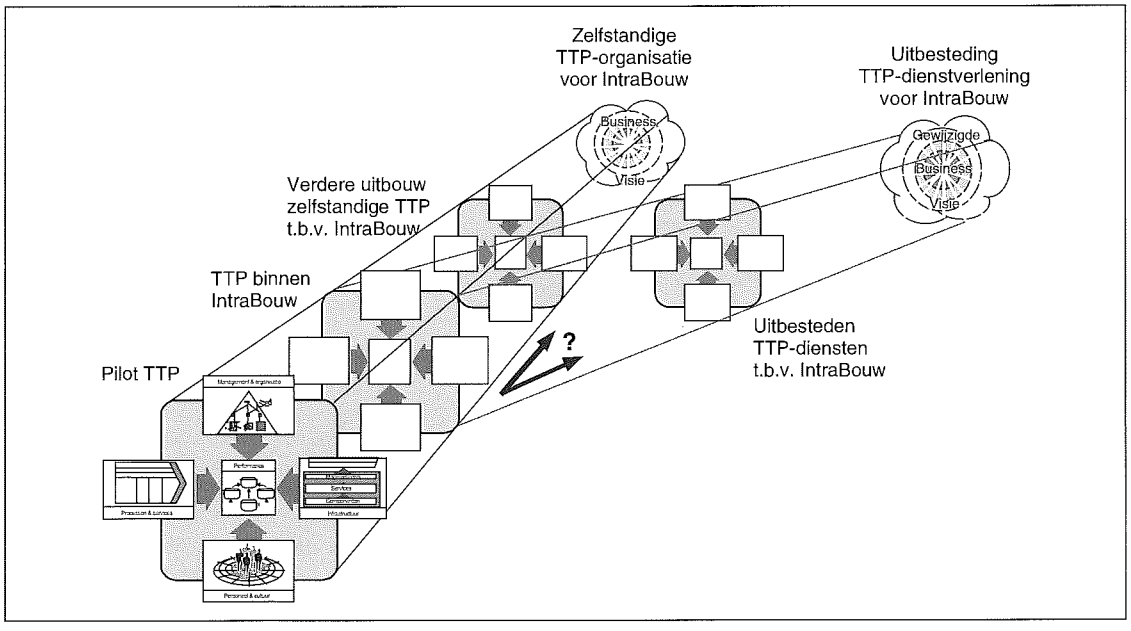
GEFASEERDE TOEPASSING ROADMAP VOOR INTRABOUW

De Roadmap voor TTP-dienstverlening wordt voor Intrabouw gefaseerd toegepast, om eventuele risico's zo beheersbaar mogelijk te houden. In figuur 4 wordt deze gefaseerde aanpak weergegeven.
Gestart wordt met het uitvoeren van een pilot binnen een kleine, afgebakende omgeving. Aangezien gebruik wordt gemaakt van een nieuwe technologie, die bovendien voor de meeste mensen onbekend is, en de taakstelling en het toekomstbeeld door de voortschrijdende inzichten nog te veel aan verandering onderhevig zijn, wordt gestart met een pilot. Een pilot waarin op heel pragmatische wijze de diverse aspecten, zoals hiervoor beschreven, worden geadresseerd. Op basis van deze pilot kunnen de diverse deelgebieden verder worden uitgewerkt. Vervolgens wordt in de tweede fase een TTP voor de deelnemers van IntraBouw geïmplementeerd. Hierna wordt een beslissing genomen over het verder uitbouwen van de TTP ten behoeve van Intrabouw door een aparte entiteit (een apart organisatieonderdeel van IntraBouw) dan wel over het uitbesteden van de TTP-functie aan een externe organisatie. Pas zodra duidelijk is hoe de TTP goed kan functioneren en aan welke randvoorwaarden zij dient te voldoen, kan deze beslissing worden genomen. In de laatste fase wordt volledige TTP-dienstverlening gerealiseerd door een aparte entiteit dan wel een externe TTP-organisatie.

Hoewel een aantal operationele applicaties op IntraBouw reeds vraagt om toepassing van een volledige TTP, vereist de realiteit echter bovengenoemde aanpak. Zo dient de inrichting van de technische beheerorganisatie te worden aangepast om tegemoet te komen aan een hogere beschikbaarheidseis. In de eerste twee maanden wordt aandacht besteed aan de technische beheerorganisatie en het implementeren en testen van de techniek in een pilotproject. Parallel hieraan wordt in deze twee maanden de administratieve organisatie voor de TTP-functies opgesteld en ingevoerd. Naar schatting zal het totale project (tot en met de laatste fase) ruim een half jaar in beslag nemen.

EERSTE BEVINDINGEN

Op dit moment wordt de eerste fase, de pilot voor TTP-dienstverlening, uitgevoerd. Het creëren van draagvlak bij de dragende en ondersteunende orga-



Figuur 4. Gefaseerde toepassing Roadmap voor IntraBouw.

Ing. J.A.M. Hermans
Is sinds 1996 werkzaam bij KPMG. Eerst als EDP-auditing supervisor bij KPMG EDP Auditors en later als manager bij KPMG TTP Services. Hij voert opdrachten uit op het gebied van secure electronic commerce en TTP-dienstverlening, onder andere bij (semi-)overheden en brancheorganisaties. Verder is hij voorzitter van ECAF (European Certification Authority Forum), een onafhankelijk platform waarin op dit moment 200 organisaties zijn vertegenwoordigd met als doelstelling het opzetten van een marktplaats voor informatie omtrent TTP-dienstverlening.

A. Bruggeman
Zelfstandig adviseur en interim-manager. Is sinds april 1997 verantwoordelijk voor de technische en commerciële gang van zaken bij IntraBouw, de Electronic Commerce Service Provider voor de Bouwnijverheid. Daarnaast geeft hij vorm aan de Intranet & extranet beheerafdeling binnen de SFB-groep. Neemt namens IntraBouw deel aan het bestuur van ECP NL en participeert in BAS, de stichting Bouw Afspraken Stelsel. Direct voorafgaand aan deze periode heeft hij bij Cap Gemini een beheerorganisatie voor Internet, intranet en extranet opgezet.

nisaties van IntraBouw kost relatief veel energie, met name doordat het gehele fenomeen TTP voor veel betrokkenen nieuw is en het nut niet direct wordt ingezien. De implementatie wordt door de gebruikers, omdat een goede ondersteuning wordt geboden, niet als knelpunt ervaren. De gebruiker ondervindt nu al een aantal voordelen, zoals een versimpelde, eenduidige aanlogprocedure voor verschillende applicatiegebieden en een verhoogd gevoel van veiligheid.

AFSLUITEND

In dit artikel is een beeld geschetst van de implementatie van TTP-dienstverlening bij IntraBouw. We hebben laten zien hoe de Roadmap voor TTP-dienstverlening er uitziet, welke modellen worden gehanteerd ('business oriented'-model en 'IT-oriented'-model), welke producten dienen te worden opgeleverd en activiteiten uitgevoerd, en hoe de gefaseerde aanpak voor de toepassing van de Roadmap voor Intrabouw er uitziet.

Hoewel de TTP-dienstverlening nog niet volledig is gerealiseerd, kunnen we toch reeds een aantal voorzichtige conclusies trekken. Een algemene conclusie die we kunnen trekken uit de pilot van TTP-dienstverlening binnen een electronic-commercetoepassing, zoals IntraBouw, is dat de voordelen voor de gebruikers en informatieleveranciers direct merkbaar kunnen zijn (single sign-on, centrale beveiligingsconcepten). Het direct merkbaar zijn van deze voordelen is zeer wenselijk zo niet noodzakelijk voor het verkrijgen van het gewenste draagvlak, aangezien de gebruikers wel de lasten van het gebruik van TTP-diensten op zich moeten willen nemen.

Verder kunnen we concluderen dat de invoering van de specifieke PKI-technologie geen drempel vormt voor het succesvol invoeren van TTP-dienstverlening. Doordat gebruik wordt gemaakt van standaardproducten in een standaardomgeving wordt de invoering sterk vereenvoudigd. Vanuit technologisch oogpunt onderscheidt de implementatie van TTP-diensten zich niet van reguliere IT-trajecten.

Tot slot willen we benadrukken dat hoewel bij een diversiteit van toepassingen volledige TTP-dienstverlening uitkomst biedt, het naar onze mening verstandig is klein te beginnen door middel van een afgebakende pilot. Omdat we te maken hebben met nieuwe technologie kan op basis van deze pilot de benodigde ervaring worden opgedaan. Na het doorlopen van een pilot kan een organisatie geleidelijk doorgroeien naar de uiteindelijk gewenste vorm van TTP-dienstverlening.

LITERATUUR

[Gerr97] J.W.M. Gerrits, K.R. Jonkheer en M. van der Linden, *De elektronische snelweg en het MKB, implicaties van Internetgebruik voor het MKB*, EIM/Vrije Universiteit, Amsterdam 1997.

Bent u al voorbereid op het jaar 2000?

Millennium Monitor

JA ik probeer vrijblijvend 2 nummers van Millennium Monitor voor ƒ 58,-*

NAAM: .....M/V

NAAM BEDRIJF: .....

BEDRIJFS-/PRIVÉ-ADRES: .....

POSTCODE: .....PLAATS: .....

TEL.: .....

FUNCTIE: .....

DATUM: .....HANDTEKENING: .....

☐ HOUDER VAN DE AG-PRIVILEGEPAS PASNR.: .....

(*) excl. 6% btw

Tot een maand na ontvangst van het tweede nummer kunt u opzeggen. Bij geen bericht abonneert u zich automatisch. Verstuur deze bon in een envelop zonder postzegel naar: ten Hagen & Stam, antwoordnummer 1557, 2501 VC DEN HAAG. Faxen kan ook: 070-3045813

Het jaar 2000 nadert sneller dan u denkt. Alleen een goede voorbereiding kan u redden. Ongetwijfeld zullen ook binnen uw organisatie verschillende facetten van het jaar 2000-probleem de revue passeren. De nieuwsbrief Millennium Monitor helpt u daarbij. U leest over verschillende aspecten van het jaar 2000, zoals: technische, strategische, management, juridische en financiële aspecten. Daarnaast vindt u in elk nummer cases, die betrekking hebben op één of meerdere van deze onderwerpen. Verder wordt aandacht besteed aan de personele gevolgen en is er een servicerubriek met onder meer discussie-punten, agenda en websites.

Millennium Monitor is naast een onafhankelijke nieuwsbrief tevens het officiële orgaan van het Millennium Platform. De nieuwsbrief verschijnt 6 keer per jaar. Een jaarabonnement kost ƒ 345,- en voor houders van een AG-PrivilegePas ƒ 295,-. U kunt eerst vrijblijvend twee nummers proberen door middel van een proefabonnement voor ƒ 58,-.

Wees het jaar 2000 te slim af en stuur bijgaande bon vandaag nog in.

Genoemde prijzen zijn exclusief 6% btw

tenHagenStam UITGEVERS

Wie waakt er over de vitale informatie

IN UW BEDRIJF?

Gaat u dit voorkomen... of gaat het u overkomen?

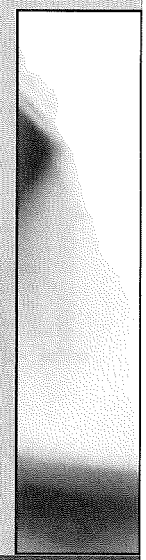
DE NIET opgehaalde tekst op de printer bevatte geheime reorganisatievoorstellen voor het komende jaar. Kopieën voor alle medewerkers waren snel gemaakt. Met als gevolg een enorme personeelsonrust.

PRECIES EEN week nadat de vertegenwoordiger een laptop had gekregen werd die uit zijn auto gestolen. Inclusief de opgeslagen orders van de hele week.

NA DE zoveelste avond overwerk had het verkoop-team de mammoet-offerte eindelijk klaar. Vermoeid sloeg de binnendienstmedewerker de tekst op... onder een verkeerde opslagcode, die de volgende dag gewist werd. Helaas voorzag ook het back-up systeem niet in dergelijke situaties.

Informatie-beveiliging Praktijkjournaal

Informatiestromen vormen de bloedsomloop van uw organisatie. Het lekken van die informatie kan ernstige gevolgen hebben voor vitale delen ervan, of zelfs voor het voortbestaan van uw bedrijf. Denk aan kostbare marketinginformatie die verloren gaat, product- en researchgegevens die bij de concurrentie terecht komen, of financiële autorisatiecodes in verkeerde handen.
Maar hoe beveilig je deze 'gevoelige' bedrijfsinformatie? Het antwoord op die vraag verandert met de dag.
Want met de Informatietechnologie groeit ook het aantal nieuwe beveiligingssystemen. En de enige manier om voortdurend over álle ontwikkelingen op dit gebied geïnformeerd te blijven is een abonnement nemen op het nieuwe vakblad Informatiebeveiliging Praktijkjournaal.



Begin met 'n half jaar voor de halve prijs

Het eerste nummer van Informatiebeveiliging Praktijkjournaal is verschenen in de maand juli 1998. Als u zich nu abonneert, krijgt u het eerste half jaar voor minder dan de halve prijs: 5 nummers voor f 49,-. Pas daarna gaat uw jaarabonnement in à f 210,-. (Of f 190,- voor AG-PrivilegePashouders en NGI-leden) Aarzel niet en verstuur vandaag nog de antwoordbon. Juist bij beveiliging komt twijfel vaak te laat !

Ja **ik wil mijn vitale bedrijfsinformatie beter gaan beveiligen....**

en abonneer mij tot wederopzegging op het 10x per jaar verschijnende, nieuwe vakblad Informatie-beveiliging Praktijkjournaal. Voor het eerste half jaar betaal ik slechts f 49,-, daarna gaat het abonnement in à

- ☐ f 210,- per jaar.
- ☐ f 190,- per jaar omdat ik AG-PrivilegePashouder ben.
- ☐ f 190,- per jaar omdat ik NGI-lid ben.

(genoemde prijzen zijn exclusief BTW)

U kunt deze bon ook per post versturen aan:
tenHagen&Stam bv, t.a.v. Klantenservice Lezersmarkt,
Antwoordnummer 1557, 2501 VC Den Haag.

Fax: 070 - 304 58 13
Meer informatie
Tel. 070 - 3045888

tenHagenStam UITGEVERS

Naam bedrijf: .....

Naam besteller: ..... M/V

Adres: .....

PC/Plaats: .....

Functie: .....

Tel.: ..... Fax: .....

Datum: ..... Handtekening: .....

KPMG EDP Auditors
ten Hagen & Stam Uitgevers