

Zijn TTP's nuttig?

Mr. P. Kleve
Erasmus Universiteit Rotterdam

Abstract

In dit artikel wordt nader ingegaan op de dienstverlening van TTP's en de daarmee samenhangende juridische aspecten, op de vraag derhalve welke rol TTP's kunnen vervullen in het elektronisch handelsverkeer. De vraag of TTP's ook daadwerkelijk een rol zullen gaan vervullen is afhankelijk van het nut van die dienstverlening. Aan de vraag of de dienstverlening van TTP's nuttig is, wordt in deze paragraaf aandacht geschonken.

Te vertrouwen derden

Als het waar is dat we elkaar in het elektronisch handelsverkeer ineens zo weinig schijnen te vertrouwen dat we een beroep moeten doen op een te vertrouwen derde, kan men zich afvragen of er dan sowieso wel een basis voor een overeenkomst aanwezig is, én waarom die derde eigenlijk wél te vertrouwen zou zijn. De term 'trusted third party', is een suggestieve, en daardoor misleidende term. De indruk wordt gewekt, dat elektronische handel met behulp van zo'n 'te vertrouwen derde' wel goed zit, en dat die derde zelf te vertrouwen zou zijn. Welnu, om met dat laatste te beginnen, dat is hij niet. Mocht namelijk uw transactie, ondanks alle goede zorgen van de TTP, toch fout lopen, dan krijgt u van de TTP niet uw schade vergoed. Dat roept onmiddellijk de vraag op: "Waar in handelen ze dan?". Er wordt wel gesteld dat TTP's 'vertrouwen garanderen'. Ook dit echter is niet waar. TTP's garanderen niet, en onder vertrouwen mag men slechts verstaan dat TTP's trachten de betrouwbaarheid van de elektronische communicatie te bevorderen en/of bij te dragen tot de vaststelling van de identiteit van de deelnemers aan die communicatie. En dat brengt ons bij de hoofdvraag van deze paragraaf: "Is dát nou nuttig?".

Betrouwbaarheid van de berichten

Het verschijnsel TTP speelt in op twee veronderstellingen, namelijk dat elektronische handel met zich mee zal brengen dat vaker met onbekende partners zal worden gehandeld en dat elektronisch berichtenverkeer gevoelig is voor manipulatie. Een derde veronderstelling, dat onder invloed van internet de globalisering van het handelsverkeer zal toenemen, hangt hiermee wel samen,

doch wordt meestal niet uitdrukkelijk in verband gebracht met de dienstverlening van TTP's.

Teneinde inzicht te verkrijgen in het nut van TTP's, zullen we elektronische handel – 'ecommerce' – moeten afzetten tegen ..., ja, tegen wat eigenlijk? 'Papieren handel'? 'Digitale handel' tegenover 'analoge handel'? Waarin zitten nu de verschillen? De handel is niet elektronisch, maar de communicatie daarover¹. In plaats van een telefoontje, of een brief, sturen we tegenwoordig een email. Waarom zouden we nu ineens een probleem krijgen met de identiteit van de kopende of verkopende partij? Doorgaans zal de identiteit juist minder een probleem zijn, omdat de afzender het emailadres bekend maakt. Misverstanden zoals bij telefonische bestellingen zijn daardoor in principe uitgesloten. Is het dan wellicht zo, dat de boodschap onjuist kan aankomen? Wel, dat kan ook met papier, of met de telefoon. Maar wat is nu de kans dat een boodschap onjuist aankomt? Als we gebruik maken van versleuteltechnieken, die boodschappen 'inpakken' vóór verzending en weer 'uitpakken' ná verzending, is die kans klein, in ieder geval aanmerkelijk kleiner dan in het geval van traditionele berichtenverzending. En dan bewijs en bewaring tenslotte. In hoeverre is dat nu verschillend met ons telefoongesprek, of met de mondelinge reservering in de winkel? Het voordeel is wel dat we nu tenminste nog een bericht hebben, dat we gemakkelijk kunnen bewaren en gemakkelijk kunnen terugvinden (zelfs jaren later). En indien er gebruik wordt gemaakt van bepaalde (asymmetrische) versleuteltechnieken, dan is de bewijskracht van het bericht in niet-ontsleutelde vorm hoog, om niet te zeggen vergelijkbaar met die van een akte. En voor dit alles is geen TTP nodig. De deelnemers kunnen dit eenvoudig zelf verzorgen, met behulp van vrij verkrijgbare standaard software.

Betrouwbaarheid van de wederpartij

Door gebruik te maken van cryptografie kan dus worden voorkomen dat koper of verkoper de integriteit van de berichten in twijfel trekken. Zijn er dan misschien andersoortige problemen, b.v. met betrekking tot de integriteit van de wederpartij? Doet de verkoper zich voor als een bona fide onderneming, maar is hij in feite een oplichter? En is de koper wel kredietwaardig? Anders dan de situatie in de vorige alinea, waar we met betrouwbare partners te maken te hebben, vormen situatie als deze het echte probleem. En dat is dus niet de betrouwbaarheid van de elektronische communicatie, maar de betrouwbaarheid van de handelspartner. En dat is een probleem waar de dienstverlening van TTP's zoals deze doorgaans wordt belicht, niet aan tegemoet kan komen en dat een TTP niet gauw tot het zijne zal maken. Gelukkig hoeft dat ook niet. Het risico in het ootje te worden genomen, is in de praktijk minder groot dan in theorie. Een oplichter/verkopende partij heeft er belang bij dat er wordt vooruitbetaald; een oplichter/kopende partij heeft er juist belang bij dat er op

rekening wordt geleverd. Het ligt dan ook voor de hand dat transacties tussen partners die niet eerder zaken met elkaar hebben gedaan, onder rembours plaats vinden. In feite wordt het probleem teruggebracht tot niet meer dan een logistiek financieel probleem. En als daarin een rol voor een intermediair is weggelegd, dan zal dat moeten zijn dat deze, onder voorwaarden, bevoegd is tot het terugboeken van geldstromen.

Maar wat nu, indien de ontvanger beweert dat hij het bericht in het geheel niet heeft ontvangen? Het is maar zeer de vraag welk belang een verkopende partij daarbij zou hebben, maar niet ondenkbaar is dat hij een hoger bod heeft ontvangen en van de eerdere verkoop af wil. Met het oog op dit soort situaties is het raadzaam de ontvangst van het bericht te laten bevestigen². Wordt de bestelling niet bevestigd, dan is er geen geldige overeenkomst tot stand gekomen. Ook deze procedure is echter al geldende praktijk. In veel algemene voorwaarden wordt gesteld dat opdrachten eerst bindend zijn nadat zij door de verkopende partij (schriftelijk) zijn bevestigd. Een spiegelsituatie komen we tegen in het geval de afzender ontkent dat hij het was die het bericht heeft verzonden. Een kopende partij kan daar belang bij hebben, b.v. indien hij een voordeliger aanbod heeft gevonden. Ook deze problematiek lijkt dezelfde als in de sfeer van telefonische boekingen. Echter, de juridische positie van de verkoper kan hier aanmerkelijk sterker zijn, afhankelijk van de vraag wie het risico van misbruik van het identificatiemiddel behoort te dragen³.

Uitwisseling van identificatiecodes

Het probleem van misbruik van identificatiemiddelen legt in beginsel een zwaar accent op de toepassing van beveiligingsmaatregelen van zowel organisatorische aard als van technische aard. We moeten daarbij wel bedenken dat elektronische handel niet anders is dan elektronische communicatie. Het is natuurlijk niet zo dat de berichtenuitwisseling, vanwege de elektronische vorm, nieuwe behoeften creëert. Elektronische communicatie zal in de plaats treden van bestaande communicatiepatronen als daarmee voordeel is te behalen, dus met name in de plaats van schriftelijke en – in mindere mate – telefonische communicatie. Vanuit deze optiek is een zekere nuancering ten aanzien van de te verwachten ontwikkeling van ‘elektronische handel’ op zijn plaats. In de consumentenmarkt is het belang van telecommunicatie relatief geringer dan in de zakelijke markt. De positie van de verkopende partij evenwel blijkt onder invloed van e-commerce te verbeteren vergeleken met de situatie van telefonische bestellingen en bovendien heeft men ervaring met levering aan onbekende afnemers. In de zakelijke markt bestaan veelal reeds procedures waarin berichtenverkeer over en weer wordt bevestigd en wordt minder snel met (volledig) onbekende partners in zee gegaan. Op grond van het speltheoretische ‘prisoner’s dilemma’ kan voorts worden voorspeld dat bedriegen niet voor de

hand ligt in situaties waarin sprake is van ‘repeat play’. Een andere drempel tegen bedriegen is dat transacties toch altijd sporen nalaten, ook indien zij via internet zijn overeengekomen. Hier wordt niet alleen gedoeld op het elektronisch spoor van de internet communicatie. Ook de goederen worden ergens afgeleverd; geld wordt naar een bankrekening overgemaakt.

We zien dat de vraag of iemand wel is voor wie hij zich uitgeeft, eigenlijk opgaat in de vraag naar diens kredietwaardigheid. In een zakelijke, competitieve markt komt het bovendien praktisch niet voor dat een relatie wordt aangegaan zonder voorafgaand persoonlijk contact. In de uitwisseling van dat contact, kan ook de uitwisseling van de identificatiecodes worden overeengekomen. Daarvoor is geen instantie nodig die de echtheid van het identificatiemiddel bevestigt.

Globalisering

Nu voor het wegnemen van het veronderstelde manipulatiegevoelige karakter van elektronische berichten geen TTP noodzakelijk blijkt, en de dienstverlening van TTP's zich vooralsnog niet lijkt uit te strekken tot informatie of garanties ten aanzien van de betrouwbaarheid van onbekende handelspartners, komt de vraag naar boven of TTP's een rol spelen in de derde veronderstelling, die van de toenemende globalisering. Nemen we b.v. de situatie waarin, vanuit Nederland, bij een computer ‘mega store’ in de Verenigde Staten een modem wordt gekocht. De bestelling wordt hetzij onder opgave van een creditcardnummer uitgevoerd, hetzij na elektronische betaling. Eerst wordt het verschuldigde bedrag door de leverancier geïncasseerd, vervolgens wordt er geleverd. Althans, dat hopen we dan. Een bijkomend voordeel van kopen bij dit soort warenhuizen is dat je gerechtigd bent het product binnen een zekere termijn terug te sturen, indien je niet tevreden bent met de geleverde waar. Waar zit hier nu de bottleneck? De verkoper heeft geen probleem; hij wacht eerst betaling af. De koper evenwel moet maar afwachten of hij inderdaad geleverd krijgt, c.q. zijn geld terugkrijgt indien hij het product heeft retour gezonden. En dan is het natuurlijk wel prettig als de koper kan nagaan of bepaalde identificatiemiddelen inderdaad toebehoren aan het, hem onbekende, postorderbedrijf, maar is het niet belangrijker dat de koper zekerheid verkrijgt dat de overeenkomst correct wordt nagekomen? Een koper zal dan liever met zijn verzendbewijs naar het lokale kantoor van de intermediair toestappen, met het verzoek het bedrag terug te boeken, dan naar een advocaat om tegen het uurtarief van de prijs van een modem te trachten zijn geld terug te krijgen. Uit dit voorbeeld blijkt wederom het belang om als ‘ecommerce enabler’ te mogen ingrijpen in geldstromen, en bovendien om te kunnen optreden als bemiddelaar⁴.

Intermediaire dienstverlening

Het nut, of de toegevoegde waarde van een TTP is niet evident. De activiteiten op het terrein van de versleuteling van het datatransport, het certificeren van identificatiemiddelen en bewijs en bewaring zijn op zichzelf genomen nuttig, maar kunnen doorgaans door partijen zelf ter hand worden genomen. Vanwege het ontbreken van aanvullende garanties of andere zekerheidstellingen is uitbesteden niet aantrekkelijker. Daar komt bij dat in het algemeen bij TTP's de nadruk ligt op sleutelbeheer, certificatie en bewijs en bewaring. In het handelsverkeer lijkt echter een grotere behoefte te bestaan aan intermediaire dienstverlening met betrekking tot handelsinformatie en kredietwaardigheid, bancaire diensten en geschillenbeslechting. De afweging al dan niet gebruik te maken van de diensten van TTP's komt zo allengs meer te liggen op het vlak van algemeen bedrijfseconomische motieven aangaande 'outsourcing', dan dat juridische overwegingen ter beperking van risico's een rol blijken te spelen. De afweging, kortom, of uitbesteden goedkoper en effectiever is dan zelf doen en niet te veel verlies van greep op bedrijfsprocessen met zich meebrengt. Beide aspecten zijn niet overtuigend. Asymmetrische cryptografie software, zoals 'Pretty Good Privacy' is gratis van internet te 'downloaden' (zelfs de broncode is vrij beschikbaar!) en eenvoudig te gebruiken. Aan het uitbesteden van veiligheidsmaatregelen blijkt nogal eens een risico verbonden, niet alleen van onachtzaamheid, maar ook van lekken, misbruik en fraude. In de kracht van beveiligingen door middel van sleutels, ligt immers ook de zwakte: degene die de beschikking heeft over de sleutel, kan binnen komen.

In de overgang naar elektronische communicatie in de handelsomgeving, is het van belang 'functioneel' te denken' en niet zozeer te denken in elektronische equivalenten van papieren uitingen. Van fysiek naar virtueel heeft juist grote voordelen, niet in de laatste plaats omdat belemmeringen uit het 'papierregime' verdwijnen. Is het nu niet eerder het voordeel van elektronische communicatie dat niet meer persoonlijk een handtekening hoeft te worden gezet, dan het nadeel? Moeten notarisdiensten elektronisch worden, of kunnen we er nu juist van buiten? We zien echter dat functioneel denken wel tot een uitgebreider takenpakket – wellicht zelfs andersoortig en minder geïsoleerd – aanleiding geeft dan wat tot nog toe door TTP's wordt geboden.

Bezwaren in breder verband

In een oriëntatie op het nut van TTP's, en dan met name de diensten van beveiliging, sleutelbeheer en certificatie, is het belangrijk om ook naar mogelijke gevolgen van deze ontwikkeling te kijken. We stuiten dan op twee zeer reële bezwaren. Het eerste is het risico dat diensten als hier bedoeld door bepaalde beroepsgroepen gemonopoliseerd worden, mogelijk zelfs met

wettelijke verankering, zoals thans b.v. de accountancy en de advocatuur. Te vrezan valt voor een onaanvaardbare afhankelijkheid, bovendien voor deels nutteloze activiteiten. Het tweede bezwaar zullen we tegen komen in de houding van de overheid. Het zou in dit artikel te ver voeren om hier in detail op in te gaan, maar de wettelijke initiatieven op het gebied van cryptografie, justitiële aftapbevoegdheden van internet en medewerkingsverplichtingen van intermediairs⁵, zullen in de uitvoering een stuk eenvoudiger komen te liggen, als justitie zich tot geautoriseerde, geregistreerde en/of gecentraliseerde TTP-organisaties kan wenden.

Conclusie

Rond het fenomeen TTP spelen verschillende vraagstukken en juridische aspecten, zoals: “Wat doet een TTP precies? Hoe zit het met zijn juridische aansprakelijkheid? en Welke juridische status kan aan TTP-diensten worden toegekend?”. De belangrijke vraag evenwel die hieraan vooraf gaat is of, en zo ja welke praktijkproblemen TTP’s daadwerkelijk oplossen, en bovendien of dat efficiënter is dan andere opties. Een kanttekening die hierbij kan worden gemaakt is dat het werkelijke probleem in het elektronisch handelsverkeer is de onzekerheid omtrent de nakoming van de overeenkomst. Beveiliging van de communicatie en identificatie van de wederpartij zijn daarvan slechts ondergeschikte aspecten, die ook zonder TTP kunnen worden ingevuld. Het lijkt raadzaam alvorens tot verdere uitwerking van het TTP-concept te geraken, de uitgangspunten nog eens te bezien. En het kan geen kwaad daarbij in herinnering te brengen dat we juist zo verheugd waren dat we de afhankelijkheid van de EDP-afdelingen uit de jaren zeventig achter ons hebben.

Noten

- 1 Ook aanduidingen als ‘virtuele handel’ t.o.v. ‘fysieke handel’ zijn onzorgvuldig en verwarrend. Zo is ‘de handel’ altijd fysiek. Met het virtuele aspect wordt niet bedoeld dat er ‘schijnbaar’ of ‘denkbeeldig’ handel wordt gedreven op internet, maar slechts dat het niet nodig is dat partijen lijkfelijk op dezelfde (markt)plaats aanwezig zijn om een transactie te sluiten, communicatie dus. Wel is het zo dat bij bepaalde transacties, zoals de verzending van software, muziek of andere databestanden, internet niet alleen het communicatiemedium is, maar ook het transportmedium van de te leveren zaak(!).
- 2 Zie ook: Article 14. Acknowledgement of receipt, van de uncitral Model Law on Electronic Commerce, 1997.
- 3 Zie b.v. HR 19 november 1993, NJ 1994 nr. 622, m.nt PvS, Stg. Cova – ING.
- 4 Zie hierover b.v. P. Kleve, R.V. De Mulder en J.G.L. van der Wees, ‘Re-engineering Dispute Resolution in an EDI Environment, Law, Computers and Artificial Intelligence, volume 4 number 1 1995, pp. 25-32.
- 5 Wetsontwerp Computercriminaliteit II, Hoofdstuk 13 van het ontwerp Telecommunicatiewet en de voorgestelde wijziging van het grondwettelijk briefgeheim.