De Trusted Third Party: voorwaarde voor electronic commerce

Mw. mr. drs. M.J. Dontje en drs. C.F. Olde Olthof

Electronic commerce heeft – als we de media moeten geloven – de toekomst. Toch is de omvang van electronic commerce minder groot dan verwacht. Gebrek aan betrouwbaarheid van het medium Internet is waarschijnlijk de oorzaak van de langzame totstandkoming van een wereldwijde marktplaats. In dit artikel worden kort de ontwikkelingen rond en toepassingen van electronic commerce behandeld en zullen de voorwaarden voor electronic commerce en de rol die een Trusted Third Party hierin kan spelen, worden besproken.

Inleiding

Het Internet is een populair publicatiemedium (Internet als een wereldwijd verspreid digitaal tijdschrift) en communicatiemedium (Internet als wereldomspannende digitale communicatie- c.q. discussieplaats). Opvallend is dat het gebruik van het Internet ten behoeve van het verrichten van zakelijke transacties, het Internet als wereldomvattende virtuele marktplaats, niet zo'n stormachtige ontwikkeling doormaakt als het gebruik van het Internet ten behoeve van communicatie- en publicatiedoeleinden. Bedrijven en particulieren zijn terughoudend om het Internet te benutten voor het verrichten van zakelijke transacties. De voornaamste oorzaak van die terughoudendheid ligt waarschijnlijk in het feit dat het communiceren over een open netwerk als het Internet in het algemeen, en het verrichten van rechtshandelingen over het Internet in het bijzonder, gepaard gaan met onzekerheid. Zo zal een consument die via het Internet een boek bij Amazon.com bestelt en betaalt zeker willen weten dat niemand zijn creditcardnummer kan lezen. Een bedrijf dat een overeenkomst aangaat via het Internet wil ervan overtuigd zijn dat degene met wie de overeenkomst aangegaan wordt, de partij is voor wie hij zich uitgeeft. Ten slotte zal bijvoorbeeld een burger die zijn belastingaangifte elektronisch indient er zeker van willen zijn dat die aangifte ongewijzigd bij de Belastingdienst aankomt. Pas wanneer de betrouwbaarheid van elektronische communicatie kan worden gewaarborgd, kan het Internet als medium voor electronic commerce optimaal worden benut.

Door toepassing van een TTP kan aan vijf betrouwbaarheidsvereisten worden voldaan, te weten vertrouwelijkheid, authenticiteit, integriteit, onweerlegbaarheid en autorisatie.

Door toepassing van cryptografische technieken kan aan vijf betrouwbaarheidsvereisten, te weten vertrouwelijkheid, authenticiteit, integriteit, onweerlegbaarheid en autorisatie, worden voldaan. Er worden twee toepassingen van cryptografie gebruikt om veilige elektronische communicatie te bewerkstelligen, namelijk het versleutelen van berichten en het plaatsen van digitale handtekeningen. Toepassing van cryptografische technieken alleen is echter niet voldoende om tot betrouwbare digitale berichtenuitwisseling te komen. Cryptografie biedt geen garantie omtrent de identiteit van partijen. Er bestaat dus geen zekerheid dat een bericht werkelijk afkomstig is van degene met wie men denkt zaken te doen. Een vaststaande relatie tussen een fysieke identiteit en een digitale identiteit is echter een noodzakelijke voorwaarde voor betrouwbaar elektronisch berichtenverkeer.

Door gebruik te maken van de diensten van Trusted Third Parties (hierna: TTP's) kan die noodzakelijke koppeling tussen een fysieke en een digitale identiteit worden gerealiseerd. TTP's zijn organisaties die betrouwbaarheidsdiensten in een elektronische omgeving aanbieden. Ten gevolge van het digitale en grensoverschrijdende karakter van de elektronische snelweg gaat het verrichten van rechtshandelingen in deze omgeving met onzekerheid gepaard. Met behulp van de diensten verleend door TTP's kan de onzekerheid die gepaard gaat met elektronische berichtenuitwisseling, waaronder het verrichten van rechtshandelingen, worden gereduceerd.

Om de vijf hiervoor genoemde betrouwbaarheidsvereisten te realiseren, maakt een TTP gebruik van een Public Key Infrastructure (PKI). Dit is een infrastructuur die is gebaseerd op een zogeheten asymmetrisch cryptosysteem. TTP's verlenen een aantal kerndiensten waarmee de organisatorische, technische en juridische randvoorwaarden verbonden aan het gebruik van cryptografische technieken ten behoeve van elektronische transacties kunnen worden vervuld. Deze diensten hebben ten eerste betrekking op het identificeren/authenticeren en registreren van personen die een digitale identiteit (in de vorm van een certificaat) willen hebben, ten tweede op het beheer van cryptografische sleutels en ten derde op certificatie. Voorts kunnen TTP's een aantal aanvullende diensten leveren; hierbij kan worden gedacht aan het tijdstempelen van berichten en het waarmerken van digitale contracten. TTP's kunnen worden beschouwd als een belangrijke zo niet noodzakelijke voorwaarde om de voordelen van electronic commerce ten volle te kunnen benutten.

Ook op nationaal en internationaal overheidsniveau bestaat het besef dat TTP's een belangrijke impuls kunnen leveren aan de werkelijke groei van electronic commerce. Veel overheden willen echter een vinger in de pap houden. Gevreesd wordt dat ook criminelen gebruik

(zullen) maken van deze technieken en zo hun illegale activiteiten (zullen) afschermen van opsporingsinstanties. Vandaar dat in veel landen exportbeperkingen ten aanzien van cryptografische producten bestaan. Bovendien is de verlening van TTP-diensten, met het oog op het gebruik van cryptografische middelen, in een aantal landen reeds gebonden aan voorwaarden en overwegen ook andere landen het gebruik van cryptografische producten – al dan niet via het stellen van eisen aan TTP's – te controleren.

In dit artikel wordt allereerst aangegeven wat onder electronic commerce kan worden verstaan en wordt een aantal recente ontwikkelingen met betrekking tot Internet electronic commerce geschetst. Daarna wordt een aantal voorwaarden voor electronic commerce gesignaleerd. Eén van de voorwaarden, betrouwbare gegevensuitwisseling over het Internet, wordt in het vervolg van dit artikel verder uitgewerkt. Er zal een link worden gelegd tussen de onzekerheden die in een elektronische handelsomgeving bestaan en de verschillende diensten die TTP's kunnen verlenen. Hieruit blijkt het 'waarom' van TTP-dienstverlening. Alvorens in te gaan op de betrouwbaarheidsvereisten waaraan door middel van de diensten van een TTP kan worden voldaan, volgt eerst een introductie inzake cryptografie en wordt het begrip Public Key Infrastructure toegelicht. Ten slotte wordt ingegaan op beleidsmatige aspecten, zowel op nationaal als op internationaal niveau.

Wat is electronic commerce?

Er is een groot aantal definities van 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 nemen nog steeds toe. Dientengevolge groeit de IT-sector 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 drie miljoen mensen gebruik van Internet. In 1998 zijn dit naar verwachting honderd miljoen. De prognose is dat tegen het jaar 2005 er één 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 handeldrijven. 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, consumenten 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, consultancy, 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 tastbare goederen via Internet thans rond de één procent van de totale omzet van deze producten schommelt, vertoont de verkoop van deze producten via Internet een sterke groei.

Naar verwachting zal 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 on-lineverkoop 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 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.

Voorwaarden voor electronic commerce

Om de (potentiële) voordelen die electronic commerce biedt ten volle te kunnen benutten moeten echter enkele 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 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 ([KMCU97]).

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 informatie-beveiligingstechnologie voor commerciële doeleinden. Daarnaast zullen er juridische en organisatorische aanpassingen en controles moeten worden ontwikkeld in samenhang met de bestaande beveiligingstechnologie.

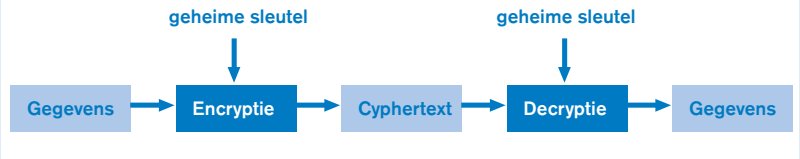
Zoals verschillende malen in dit artikel is benadrukt, biedt electronic commerce vele voordelen, maar is het ook voor veel bedrijven en particulieren nog een relatief onbekend en onzeker verschijnsel. De deelnemer aan het elektronische verkeer zal voldoende zekerheden willen hebben ten aanzien van de 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?

Concurrentievoordeel en efficiency zijn de belangrijkste motieven voor electronic commerce.

Betrouwbaarheid van Internet in het algemeen en electronic-commerceapplicaties in het bijzonder kan worden gerealiseerd door middel van de diensten verleend door TTP's. Deze TTP-diensten faciliteren een verdere doorbraak van electronic commerce en het wijdverspreide gebruik ervan door bedrijven en particulieren.

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 TTP's dan ook alleen maar zal toenemen, onder meer daar waar het gaat om sleutelbeheer en certificatiediensten.

De International Data Corporation doet in dit kader vergelijkbare uitspraken. Een IDC-studie toonde belemmeringen aan in de groei van electronic commerce in Enge-



Figuur 1.
Werking symmetrisch cryptosysteem.

land, die met name worden veroorzaakt door een te geringe beveiligingsgraad. Hier zou een TTP uitkomst kunnen bieden. Daarnaast voorziet IDC de noodzaak van handelsstandaarden en ziet zij een rol weggelegd voor TTP's daar waar het gaat om het arbiteren van de electronic-commercetransacties.

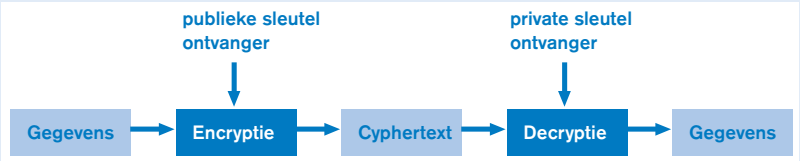
In het vervolg van dit artikel zal worden ingegaan op TTP's. Hiertoe wordt allereerst de techniek geschetst die TTP-dienstverlening mogelijk maakt, te weten cryptografie. Vervolgens wordt aandacht besteed aan de infrastructuur waarin cryptografie wordt toegepast ten behoeve van betrouwbare elektronische gegevensuitwisseling, de Public Key Infrastructure. Hierna wordt het fenomeen TTP toegelicht, waarbij uiteengezet zal worden hoe met behulp van TTP-diensten de betrouwbaarheid van het elektronisch berichtenverkeer kan worden gegarandeerd. Ten slotte wordt kort ingegaan op nationale en internationale ontwikkelingen op het gebied van TTP's.

Cryptografie

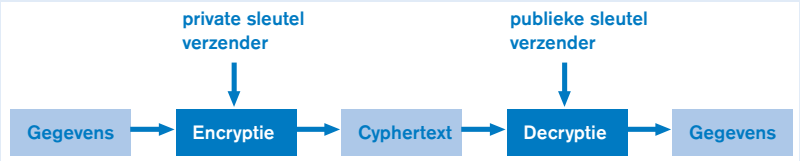
Cryptografie is geheimschrift.[1] Cryptografie is geen nieuw verschijnsel, Julius Caesar gebruikte al geheimschrift. Als tegenwoordig wordt gesproken over cryptografie denken we echter niet meer, zoals Caesar dat deed en kinderen dat nog steeds doen, aan geheimschriften waarbij de juiste letter – en zo uiteindelijk de juiste tekst – wordt gevonden door die letter te vervangen door een letter die een x-aantal posities verderop in het alfabet staat. Tegenwoordig wordt gewerkt met twee basisvormen van cryptografie: symmetrische en asymmetrische cryptografische systemen.

1) 'Cryptography is a discipline that embodies principles, means, and methods for the transformation of data in order to hide its information content, establish its authenticity, prevent its undetected modification, prevent its repudiation, and/or prevent its unauthorised use' ([OECD97], p. 1). Van Dale, *Groot Woordenboek der Nederlandse Taal*, omschrijft cryptografie als 'kunst van geheimschrift schrijven'.

2) Het product (de uitkomst van de vermenigvuldiging) van twee grote priemgetallen levert eenvoudig een derde getal op (A*B=C). Het herleiden van A en B uit C, oftewel het ontbinden in factoren van C, is zeer arbeidsintensief (vereist een krachtige computer) en hierin ligt de veiligheid van een asymmetrisch cryptosysteem. Des te groter (langer) de gebruikte sleutels (weergegeven in het aantal bits van de encryptiesleutel) des te veiliger is het systeem: het herleiden van A en B uit de openbare encryptiesleutel C zal moeilijker zijn.



Figuur 2.
Werking asymmetrisch cryptosysteem ten behoeve van vertrouwelijkheids- en integriteitsdoeleinden.



Figuur 3.
Werking asymmetrisch cryptosysteem ten behoeve van authenticatie.

Symmetrisch cryptosysteem

In een symmetrisch cryptosysteem wordt gewerkt met één sleutel, die zowel voor versleuteling (encryptie) als voor ontsleuteling (decryptie) wordt gebruikt. Vandaar dat dit systeem ook wel wordt aangeduid als secret key cryptosysteem. Voordat daadwerkelijk betrouwbare communicatie met een andere partij plaats kan vinden, moet die ander 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' dan de hierna te behandelen asymmetrische encryptie en dus voornamelijk interessant ter versleuteling van grote hoeveelheden data in een besloten omgeving. In figuur 1 is de werking van een symmetrisch cryptosysteem weergegeven. De versleutelde en dus onleesbare gegevens worden cyphertext genoemd.

Asymmetrisch cryptosysteem

Asymmetrische cryptosystemen, ook wel bekend als public key cryptosystemen, maken gebruik van sleutelparen bestaande uit één sleutel voor versleuteling en één voor ontsleuteling. De ene sleutel is geheim (private key of private sleutel) en de andere is openbaar (public key of publieke sleutel). De twee sleutels zijn uniek met elkaar verbonden. De publieke sleutel is het product van twee zeer grote priemgetallen. De private sleutel is de factorisatie van de publieke sleutel (de priemgetallen).[2] Er wordt gebruikgemaakt van steeds grotere priemgetallen, en dus ook steeds langere sleutels, om te voorkomen dat onbevoegden de sleutel kraken.

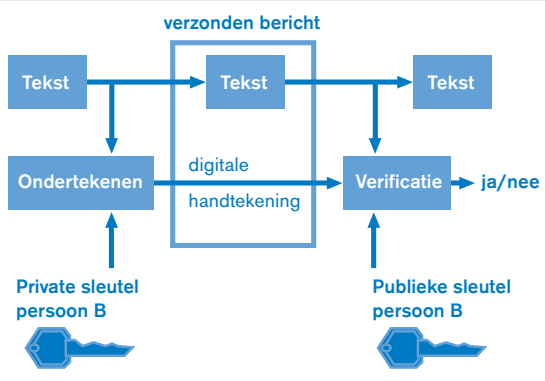
Encryptie

Een asymmetrisch cryptosysteem werkt met twee publiek-private sleutelparen. Het ene paar wordt gebruikt voor het versleutelen (c.q. ontsleutelen) van de berichten zelf (encryptie c.q. decryptie), de sleutels van dit paar worden hierna de publieke respectievelijk private encryptie/decryptiesleutel genoemd.

In figuur 2 wordt het geval geschetst waarbij asymmetrische encryptie wordt toegepast voor vertrouwelijkheids- en integriteitsdoeleinden. Het bericht wordt met de publieke sleutel van de ontvanger versleuteld en ontsleuteld met de private sleutel van de ontvanger. Vertrouwelijkheid en integriteit wordt gewaarborgd, alleen de ontvanger bezit de private sleutel noodzakelijk om het bericht te kunnen ontsleutelen.

Indien asymmetrische cryptografie wordt toegepast ten behoeve van authenticatiedoeleinden zal een bericht worden versleuteld met de private sleutel van de verzender en worden ontsleuteld met de publieke sleutel van de verzender. De werking van een asymmetrisch cryptosysteem ten behoeve van authenticatie is in figuur 3 weergegeven.

Bij asymmetrische cryptografie kunnen de publieke en de private sleutel dus zowel voor versleuteling als ontsleuteling worden toegepast. Afhankelijk van de functie, vertrouwelijkheid/integriteit dan wel authenticatie, wordt



Figuur 4.
Het digitaal ondertekenen van een bericht.

de publieke sleutel gebruikt als respectievelijk encryptie- en decryptiesleutel. Voor de private sleutel geldt uiteraard het omgekeerde. In het vervolg van dit artikel zal worden gesproken van de publieke respectievelijk private encryptie/decryptiesleutel wanneer wordt gedoeld op de sleutels ten behoeve van de encryptie en decryptie van berichten.

Digitale handtekening

Het andere sleutelpaar wordt gebruikt om digitale handtekeningen te plaatsen. De digitale handtekening maakt het mogelijk een wilsuiting, noodzakelijk voor het verrichten van een rechtshandeling, te kunnen verrichten. In figuur 4 is weergegeven hoe een bericht digitaal wordt ondertekend.

Van het te verzenden bericht wordt een hashwaarde, een uniek met het bericht corresponderende waarde vergelijkbaar met een vingerafdruk of DNA, bepaald. Die hashwaarde wordt voorzien van een digitale handtekening, dat wil zeggen de hashwaarde wordt versleuteld met de private sleutel van het sleutelpaar ten behoeve van het plaatsen c.q. verifiëren van digitale handtekeningen. De digitaal ondertekende hashwaarde wordt meegezonden met het originele bericht dat is versleuteld met de publieke encryptie/decryptiesleutel van de ontvanger. De ontvanger ontsleutelt met behulp van zijn private encryptie/decryptiesleutel het originele bericht en bepaalt de 'verse' hashwaarde van het bericht, waarna deze hash wordt vergeleken met de meegezonden hashwaarde die is ontsleuteld met de (publieke) verificatiesleutel van het sleutelpaar ten behoeve van het plaatsen c.q. verifiëren van digitale handtekeningen (hierna: verificatiesleutel). 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 niet is veranderd sinds het digitaal is ondertekend, ofwel de integriteit van het bericht staat vast, indien de twee hashwaarden gelijk zijn. Bovendien kan met behulp van een digitale handtekening de authenticiteit en de onweerlegbaarheid van de verzending van een bericht worden gewaarborgd en kan de bevoegdheid van de verzender (autorisatie) worden gecontroleerd. In figuur 5 wordt de werking van een digitale handtekening uiteengezet.

Symmetrisch en asymmetrisch cryptosysteem

Om zowel het voordeel van de hogere snelheid van het symmetrische encryptiesysteem (ten opzichte van het asymmetrische cryptosysteem) als de voordelen van de eenvoudige sleuteldistributie en de mogelijkheid om digitale handtekeningen te plaatsen van het asymmetrische encryptiesysteem te kunnen benutten, wordt bij moderne data-encryptie vaak een combinatie van beide cryptosystemen toegepast. Symmetrische encryptie wordt gebruikt voor het versleutelen van een digitaal ondertekend bericht, terwijl vervolgens asymmetrische encryptie wordt toegepast voor het versturen van de symmetrische sleutel.

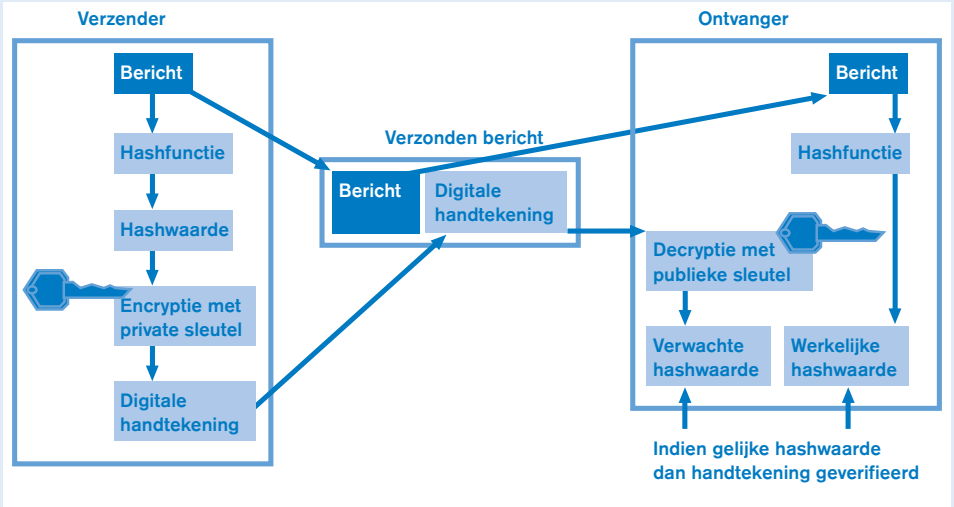
Het systeem werkt als volgt: de afzender versleutelt een bericht eerst met zijn private sleutel ten behoeve van het plaatsen van digitale handtekeningen (1) ofwel hij plaatst zijn digitale handtekening. Vervolgens wordt het ondertekende document versleuteld met een random gegenereerde symmetrische sleutel (2). Deze symmetrische sleutel wordt vervolgens versleuteld met de publieke encryptie/decryptiesleutel van de ontvanger (3). De versleutelde boodschap en de versleutelde symmetrische sleutel worden verzonden. De ontvanger gebruikt zijn private encryptie/decryptiesleutel om de symmetrische sleutel te achterhalen (3) en ontsleutelt vervolgens – met behulp van die symmetrische sleutel – het bericht (2). Op deze manier worden de vertrouwelijkheid, de toegangscontrole, de onweerlegbaarheid en de integriteit gewaarborgd. De authenticiteit wordt gewaarborgd doordat de ontvanger de – unieke – digitale handtekening van de afzender verifieert met behulp van de (publieke) verificatiesleutel (1). Zie ook het schema van figuur 6.

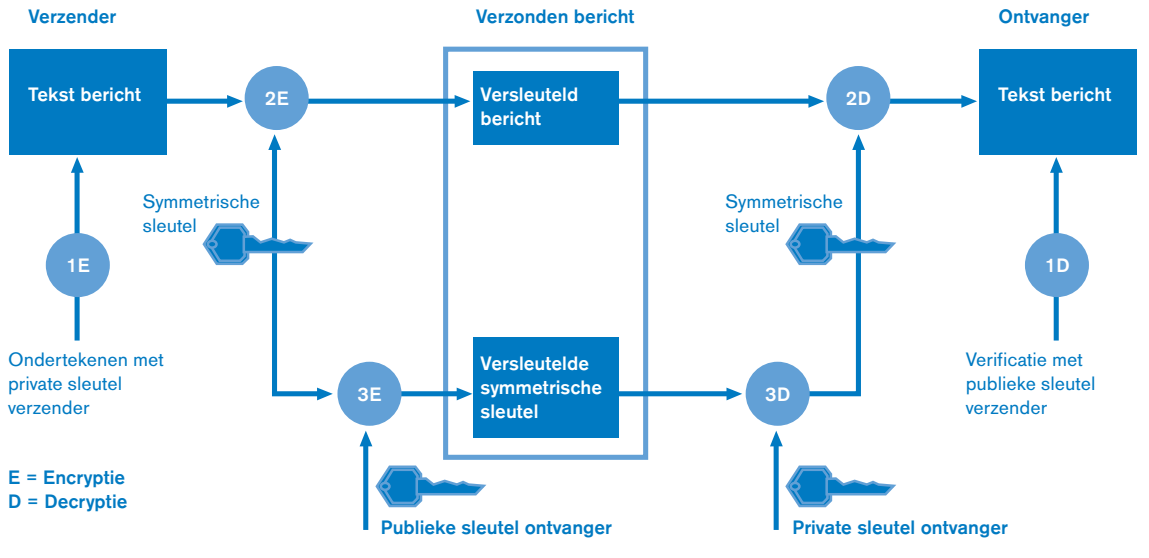
Public Key Infrastructure

Het voordeel van het gebruik van encryptie is duidelijk. Resteert echter het probleem van de binding tussen enerzijds de publieke sleutels van de twee gebruikte asymmetrische sleutelparen[3] en anderzijds de gebruiker van

3) Het ene paar ten behoeve van vertrouwelijkheid (publiek-privaat encryptie/decryptiepaar) en het andere paar ten behoeve van het plaatsen c.q. verifiëren van een digitale handtekening.

Figuur 5.
Werking digitale handtekening.





Figuur 6. Werking combinatie van symmetrisch en asymmetrisch cryptosysteem.

de private sleutel van de twee sleutelparen. In de nota *Wetgeving voor de elektronische snelweg* van het Ministerie van Justitie wordt gesteld: 'Door middel van encryptie en andere technieken is een document of transactie te waarmerken als authentiek, maar de identiteit van het rechtssubject valt niet altijd vast te stellen. Voor een betrouwbaar economisch verkeer is in veel gevallen nodig dat de ware identiteit van een partij kan worden vastgesteld' ([MinJ98], p. 141). Een zogeheten Public Key Infrastructure biedt, zoals hieronder wordt uiteengezet, een oplossing voor dit 'sleutel'probleem.

'Sleutel'probleem: gebrek aan vertrouwen

Voor het gebruik van een sleutelpaar met het oog op het realiseren van de genoemde betrouwbaarheidsvereisten dient de binding tussen enerzijds de publieke sleutel van een asymmetrisch sleutelpaar en anderzijds de gebruiker van de private sleutel gegarandeerd te zijn. In een puur digitale omgeving is die binding niet te garanderen. Een Public Key Infrastructure (PKI), zo genoemd vanwege het feit dat de beveiliging voornamelijk gebaseerd is op het gelijknamige en hiervoor uiteengezette asymmetrische cryptosysteem, maakt het mogelijk sleutelparen een persoonsgebonden status te geven, waardoor de noodzakelijke binding kan worden gerealiseerd. Door het gebruik van een PKI kan de identiteit van een persoon worden vastgesteld, waarna die identiteit door middel van een certificaat aan een sleutelpaar[4] wordt gekoppeld. Hierna wordt uiteengezet hoe die binding totstandkomt en hoe het systeem van certificaten functioneert. Allereerst wordt – aan de hand van de verschillende componenten – de structuur van een PKI toegelicht.

Structuur

Een PKI is de infrastructuur die gebruikmaakt van het public key cryptosysteem en die door middel van de uitgifte van certificaten veilige communicatie tussen de gebruikers van die certificaten kan bewerkstelligen. Een PKI bestaat uit een drietal componenten: één of meer Registration Authorities (hierna: RA's), (ten minste) één Certification Authority (hierna: CA) en de gebruikers. De gebruikers zijn te onderscheiden in twee groepen. Namelijk degene(n) bij wie het certificaat 'hoort' (certificate subject, houder of subscriber), dus de persoon of personen op wiens naam het certificaat staat, en de zogeheten relying parties, dat wil zeggen degenen die het certificaat gebruiken voor controledoeleinden, dus degenen die op het certificaat vertrouwen. Indien twee partijen bij dezelfde CA een certificaat hebben en met elkaar communiceren zijn ze beide zowel certificate subject als relying party binnen die PKI. Indien de twee partijen bij twee verschillende CA's (A en B) een certificaat hebben (en de CA's hebben elkaars certificaten gecross-certificeerd) dan is de een certificate subject in A en relying party in B en geldt voor de ander precies het omgekeerde. Indien hierna wordt gesproken over gebruikers dan worden zowel certificate subjects als relying parties bedoeld.

Indien iemand een certificaat, het beste te omschrijven als een digitaal paspoort, wil hebben, zal hij zich moeten melden bij een Registration Authority. Die RA zal de identiteit van de certificate subject vaststellen en verifiëren (identificatie en authenticatie). Ten slotte gaat de Registration Authority over tot registratie. De RA-functie vormt de voorbereiding op de CA-functie. Op grond van de gegevens van de RA zal de CA certificaten uitgeven.

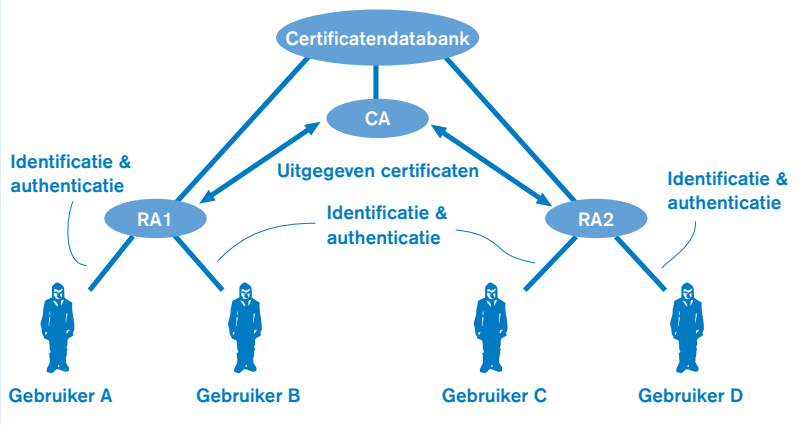
De Certification Authority is de organisatie die de sleutels waarover hiervoor is gesproken, certificeert. Een gecertificeerde sleutel, vergezeld van de gegevens over de certificate subject die met die sleutel is verbonden, wordt een certificaat genoemd. De publieke sleutels, zowel die waarmee berichten kunnen worden versleuteld dan wel ontsleuteld (de publieke encryptie/decryptiesleutel), als die waarmee digitale handtekeningen kunnen worden geverifieerd (de verificatiesleutel), worden opgenomen in een certificaat. Van de twee sleutelparen per gebruiker worden dus in totaal twee certificaten aangemaakt. De certificaten worden voorzien van de digitale handtekening van de Certification Authority. De digitale handtekening van de CA heeft tot doel gebruikers vertrouwen te geven in het certificaat.[5]

4) Zowel van het paar dat wordt gebruikt voor versleuteling c.q. ontsleuteling als van het paar dat wordt gebruikt ten behoeve van het plaatsen c.q. het verifiëren van een digitale handtekening.

5) Het is van zeer groot belang dat de private sleutel van de CA ten behoeve van het plaatsen van digitale handtekeningen niet in verkeerde handen valt. Onverlaten zouden immers 'namens' de CA (valse) certificaten kunnen genereren op naam van bepaalde natuurlijke of rechtspersonen om zich vervolgens voor te doen als die (rechts)personen. Indien de private sleutel van de CA wordt gecompromitteerd, zal de corresponderende publieke sleutel (ter verificatie van de digitale handtekening van de CA) moeten worden ingetrokken.

De door de CA uitgegeven certificaten worden gepubliceerd in een voor de gebruiker toegankelijke lijst (een certificatendatabank, Certificate List, Certificate Repository of Certificate Directory). Deze lijst is vergelijkbaar met een telefoonboek. In de databank is bovendien een lijst opgenomen met certificaten die ingetrokken of geschorst zijn, de zogeheten Certification Revocation List (CRL; zie voor de reden van intrekking of schorsing van certificaten hierna onder het kopje 'Certificatie'). Voor relying parties is het van groot belang dat een certificaat geldig is. Zij moeten kunnen controleren of een digitale handtekening nog geldig is, ofwel of die handtekening nog waarde heeft. Hetzelfde geldt voor het certificaat dat wordt gebruikt om berichten te versleutelen (ten behoeve van integriteits- en vertrouwelijkheidsdoeleinden) en voor het ontsleutelen (ten behoeve van authenticatie van de certificate subject) van berichten. Een certificaat kan verlopen zijn, maar kan bijvoorbeeld ook ingetrokken of geschorst zijn omdat (het vermoeden bestaat dat) de corresponderende private sleutel is gestolen, verloren of gecompromitteerd.

Het proces van identificatie en authenticatie dat plaatsvindt bij de RA is (mede)bepalend voor de betrouwbaarheid van de certificaten die zijn opgenomen in dit 'telefoonboek': de waarde die aan de certificaten gehecht kan worden, is afhankelijk van de zorgvuldigheid waarmee de RA voornoemd proces uitvoert. Voorts is de wijze waarop invulling wordt gegeven aan de CA-functie bepalend voor de waarde die aan certificaten kan worden gehecht. Hierbij moet gedacht worden aan de procedures voor het uitgeven en beheren van certificaten ('life-cycle management'), maar ook bijvoorbeeld aan maatregelen die deze procedures ondersteunen, zoals informatiebeveiliging. 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 een potentiële certificate subject (ervan uitgaande dat deze zich fysiek bij de RA moet melden) niet stad en land hoeft af te reizen voor een certificaat.



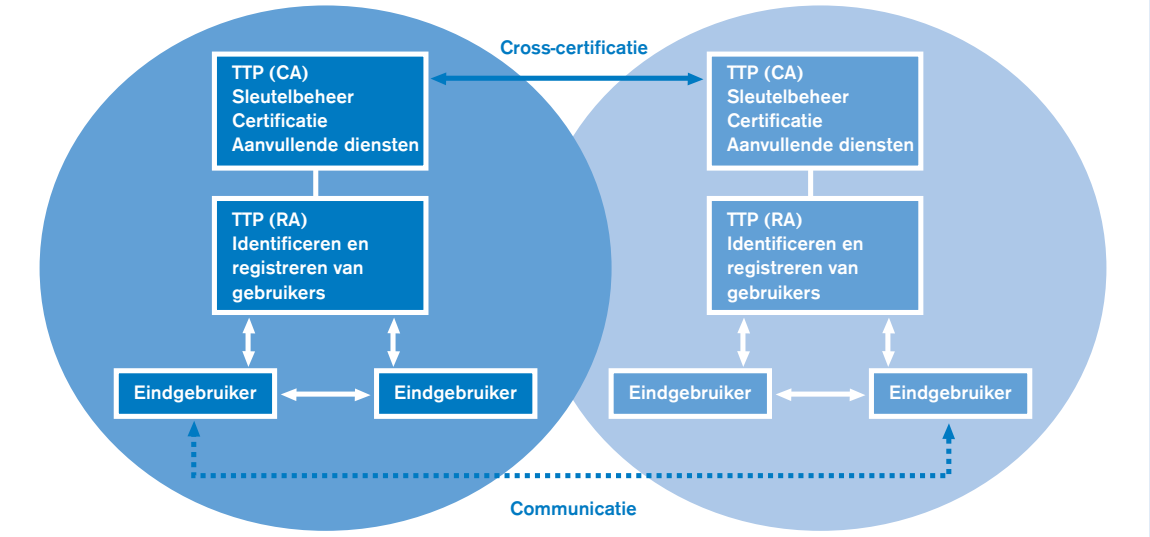
Figuur 7. Componenten binnen een Public Key Infrastructure.

De opmaak van de meeste certificaten is gebaseerd op de ITU-T Rec. X.509 versie 3-standaard. De gegevens die op een certificaat zijn opgenomen, betreffen – afhankelijk van de versie – onder andere de naam van de certificate subject, de naam van de CA, uitgifte- en vervaldatums, het unieke serienummer van het certificaat, de digitale handtekening van de CA, de publieke encryptiesleutel of de sleutel voor het verifiëren van digitale handtekeningen, extensies en de unieke naam van de bijbehorende CRL. In de bovengenoemde versie 3 van de X.509-standaard is een veld (extensie) opgenomen waarin de bevoegdheden van personen kunnen worden opgenomen.

In figuur 7 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 ('telefoonboekfunctie') in de figuur opgenomen.

Cross-certificering

Niet iedere certificate subject zal zijn certificaat van dezelfde PKI (CA) verkrijgen. Er bestaan verschillende CA's en in de toekomst zullen er ongetwijfeld nog vele bij komen. Om certificate subjects van certificaten die



Figuur 8. Werking cross-certificatie.

door verschillende CA's zijn uitgegeven in staat te stellen vertrouwelijk met elkaar te communiceren, kunnen afzonderlijke CA's elkaars sleutels certificeren. Dit proces wordt cross-certificering genoemd. Zo kan bijvoorbeeld een private infrastructuur (bijvoorbeeld een multinational of een brancheorganisatie) worden gekoppeld aan een publieke infrastructuur (een infrastructuur die opereert in een open omgeving en diensten levert waarvan eenieder in principe gebruik kan maken) of aan een andere private infrastructuur. Het concept van cross-certificering gaat ervan uit dat er niet één top-CA (of root-CA) bestaat, maar dat CA's elkaar kunnen certificeren, en aldus elkaars certificaten erkennen, en er dus geen top-CA nodig is.[6] Waarschijnlijk ontstaat in de toekomst een structuur waarbij verschillende PKI's naast elkaar bestaan, waarvan de hoogste CA's elkaars sleutels zullen certificeren. Een voorbeeld hiervan bestaat in Canada; daar ontstaan naast de PKI van de Canadese overheid ook een PKI voor de financiële sector en een PKI voor de gezondheidssector.

Certificate Policy en Certificate Practice Statement

De kern van de PKI vormt het vertrouwen dat de gebruikers stellen in de Registration Authority en de Certification Authority. Alleen indien gebruikers ervan overtuigd zijn dat de RA en CA integer zijn en zorgvuldig hun taken verrichten, bestaat vertrouwen in de certificaten die door een CA zijn uitgegeven. Met andere woorden, vertrouwt een relying party erop dat zijn wederpartij ook daadwerkelijk de persoon is op wiens naam het certificaat is gesteld. Een tweetal documenten, te weten de Certificate Policy en de Certificate Practice Statement, kan worden beschouwd als de schriftelijke weergave van de betrouwbaarheid van een PKI. Deze twee documenten worden hierna toegelicht.

In een extensie op het certificaat wordt verwezen naar de toepasselijke Certificate Policy (hierna: CP). Een CP bevat het geheel van regels waarin het gebruik van een certificaat ten behoeve van een bepaalde gebruikersgroep, in overeenstemming met bepaalde beveiligingseisen (dus het noodzakelijke vertrouwen), wordt uiteengezet. Een CP stelt een relying party, maar ook een (potentiële) certificate subject van een certificaat, in staat te bepalen hoeveel vertrouwen hij kan stellen in het verband tussen de publieke sleutel en de bijbehorende identiteit.[7] Binnen één PKI kunnen certificaten voor verschillende doeleinden worden gebruikt. Verschillende doeleinden zullen verschillende niveaus van vertrouwen – en dus beveiliging – eisen. Een PKI kan dan ook meerdere CP's ondersteunen. Het geheel van de in de CP vervatte 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). Door te werken met bepaalde standaarden is het mogelijk de CP's die binnen andere PKI's worden gehanteerd op eenvoudige wijze met de eigen policy te vergelijken. Dit is van belang bij cross-certificering tussen verschillende PKI's.

In de zogeheten Certificate Practice Statement (hierna: CPS) is het gehele proces van het genereren van certificaten, het beheer en uiteindelijk de vernietiging van certificaten beschreven (voor het proces van het genereren van certificaten tot de vernietiging: zie verder onder 'Certificatie').[8] Een CA ondersteunt dus slechts één CPS, maar kan meerdere CP's ondersteunen. Een CPS bevat juridische aspecten (rechten en verplichtingen van CA, RA, certificate subjects en relying parties en aansprakelijkheden van de verschillende partijen), organisatorische aspecten (sleutelbeheer, toegankelijkheid van certificatendatabank en Certification Revocation List), procedurele aspecten (die de RA en CA moeten volgen bij het uitoefenen van hun taken, bijvoorbeeld ten aanzien van de identificatie en authenticatie van gebruikers, en de uitgifte en intrekking van certificaten) en ten slotte beveiligingsaspecten (fysieke toegangscontrole, maar ook eisen gesteld aan personen die werkzaam zijn bij een CA of RA en beveiliging bij het genereren en het distribueren van sleutels en certificaten). De CPS heeft betrekking op de wijze waarop door de CA certificaten worden gegenereerd, uitgegeven en beheerd. Een CPS heeft dezelfde gestandaardiseerde opmaak als de CP, maar is gedetailleerder dan een CP. In de CPS wordt weergegeven hoe de vereisten opgenomen in één of meer door de CA ondersteunde CP's zullen worden gerealiseerd.[9] Aan de CPS wordt veel waarde gehecht, omdat de betrouwbaarheid van de CA uit dit stuk kan worden afgeleid. Voor cross-certificerende CA's is vertrouwen in elkaars CPS een noodzakelijke voorwaarde, 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).

Betrouwbaarheidsvereisten

Hieronder worden vijf – al eerder aangehaalde – betrouwbaarheidsvereisten besproken, vervolgens worden deze vereisten gekoppeld aan de door een TTP te leveren diensten. De betrouwbaarheidsvereisten die aan elektronisch berichtenverkeer kunnen worden gesteld, betreffen in ieder geval de volgende vijf vereisten van informatiebeveiliging.

Authenticiteit

De authenticiteit van de verzender van een bericht houdt in dat de verzender daadwerkelijk degene is die hij beweert te zijn. Gezien het feit dat elektronisch handelsverkeer zich in een open omgeving (Internet) afspeelt en de kans groot is dat de wederzijdse partijen elkaar voorafniet kennen, is het van groot belang dat zekerheid bestaat omtrent de identiteit van de wederpartij. Door het plaatsen (en verifiëren) van een digitale handtekening kan die noodzakelijke zekerheid worden verkregen. In plaats van alleen authenticatie wordt ook wel gesproken van identificatie en authenticatie. Identificatie en authenticatie zijn met elkaar verbonden. Identificatie heeft betrekking op de vraag 'Wie bent u?' en authenticatie op de vraag 'Kunt u bewijzen dat u degene bent die u zegt te zijn?' (Dit zijn de vragen die door de RA worden gesteld.) Authenticatie is het bewijs van identificatie.

Vertrouwelijkheid

De vertrouwelijkheid (ook wel confidentialiteit of exclusiviteit) van een bericht houdt in dat het bericht tijdens transport of opslag wordt beschermd tegen onbevoegde kennisneming. Met andere woorden, alleen de geadres-

6) Alleen de Duitse wet gaat op het moment uit van een hiërarchische structuur van CA's. De top-CA is een overheids-CA. Bezwaarlijk aan een dergelijke hiërarchische structuur is ten eerste de kwetsbaarheid van zo'n model. Er bestaat een zeer grote afhankelijkheid van de top-CA, waardoor de betrouwbaarheid van het gehele systeem van PKI's minder groot zal zijn. Indien de sleutel van de top-CA niet meer betrouwbaar is, is de veiligheid van alle andere (onder de top-CA hangende) CA's niet meer gegarandeerd. Ten tweede strookt dit model niet met de ontwikkelingen die zich momenteel in de praktijk voordoen.

7) Een CP kan worden gedefinieerd als 'A named set of Certificate Policy Rules relating to the use of a certificate and the certified public key, recognized by both the issuer and user of the certificate', ISO/IEC 9594-8/ITU-T Recommendation X.509, Information Technology - Open Systems Interconnection: The Directory: Authentication Framework.

8) Een CPS wordt wel omschreven als 'A statement of the practices which a CA employs in issuing certificates', American Bar Association, Section of Science and Technology, Information Security Committee, *Digital Signature Guidelines: Legal Infrastructure for CA's and Electronic Commerce*, Chicago, 1996.

seerde kan het bericht lezen. Vertrouwelijkheid wordt gerealiseerd door berichten te versleutelen met de publieke encryptie/decryptiesleutel van de beoogde ontvanger (alleen de ontvanger bezit de private sleutel noodzakelijk om het bericht te kunnen ontsleutelen).

Integriteit
Integriteit betreft de zekerheid dat de inhoud van een bericht niet is veranderd (aanvulling, verwijdering, wijziging van gegevens) tijdens transport of opslag. Die zekerheid wordt verkregen door het gebruik van een digitale handtekening (zie verder onder 'Digitale handtekening' over het vergelijken van hashwaarden).

Onweerlegbaarheid
Onweerlegbaarheid (ook wel non-repudiation) houdt in dat de verzender achteraf niet kan ontkennen een bericht te hebben verstuurd. Aan de ontvangstkant houdt onweerlegbaarheid in dat de ontvanger de ontvangst van een bericht niet kan ontkennen. Met name in het zakelijk verkeer is dit uitermate belangrijk. Indien een bericht is ondertekend met een digitale handtekening kan de verzender niet ontkennen een bericht te hebben verzonden, hij alleen immers bezit de (private) sleutel voor het plaatsen van zijn digitale handtekening. Indien de verzender bewijs (tegenover de ontvanger) wil van het feit van verzending en/of ontvangst kan hij gebruikmaken van de diensten van een TTP (zie verder onder 'Aanvullende diensten' de dienst 'Bewijs van zending en ontvangst').

Autorisatie
Autorisatie heeft zowel betrekking op de handelingsbevoegdheid van een partij als op toegangscontrole. Een voorbeeld van handelingsbevoegdheid betreft de vraag of en zo ja, tot welk bedrag iemand bevoegd is namens een onderneming overeenkomsten te sluiten. Andere voorbeelden zijn de gebondenheid van bezichtiging van sites gericht op 'entertainment' voor volwassenen aan een leeftijdsgrens of gebondenheid van de verkoop van cryptografische producten aan (rechts)personen met een bepaalde nationaliteit. Autorisatie in de zin van toegangscontrole heeft betrekking op de toegang tot berichten of tot – delen van – netwerken. Zo zou, in het kader van een loyaliteitsprogramma, een ondernemer een gedeelte van zijn website uitsluitend voor deelnemers aan dat programma toegankelijk kunnen stellen.

Een TTP kan in het kader van het elektronisch berichtenverkeer verschillende diensten aanbieden om in de vijf bovengenoemde betrouwbaarheidsvereisten te voorzien. Het instellen van een TTP kan daarom als een belangrijke maatregel worden opgevat om betrouwbare electronic commerce te realiseren.

TTP-diensten

Hieronder worden het begrip Trusted Third Party en de door een TTP geleverde diensten toegelicht. Voorts wordt aandacht besteed aan de aan een TTP te stellen eisen.

TTP

Een Trusted Third Party is een derde-partij die een faciliterende rol in het elektronisch communicatieverkeer vervult. Indien cryptografische technieken worden toegepast, kan een TTP diensten verlenen op het gebied van identificatie/authenticatie, sleutelbeheer en certificatie en kan de TTP bovendien aanvullende diensten verlenen. TTP's kunnen een belangrijke rol spelen bij het reduceren van de onzekerheid die gepaard gaat met elektronische berichtenuitwisseling in het algemeen en elektronische handel in het bijzonder. Hieronder worden eerst de kerndiensten en daarna een aantal aanvullende diensten beschreven die door TTP's kunnen worden verleend. Deze diensten maken het mogelijk de vijf hiervoor uiteengezette betrouwbaarheidsvereisten te realiseren.

Kerndiensten

De kerndiensten die door een TTP worden verleend, zijn die diensten die onder de RA-functie en de CA-functie vallen, ofwel de registrerende en de certificerende TTP. Daarnaast valt ook sleutelbeheer onder de kerndiensten van een TTP. De te leveren kerndiensten zijn dus de volgende:
1 het identificeren en registreren van partijen;
2 sleutelbeheer;
3 certificatie.

1 Het identificeren en registreren van partijen
Dit is de RA-functie van een TTP. Personen die een digitale identiteit, een certificaat, willen hebben dienen zich te identificeren en te registreren bij een TTP. Zoals vermeld, kunnen binnen één PKI certificaten voor verschillende doeleinden worden gebruikt. Deze verschillende doeleinden kunnen tot gevolg hebben dat verschillende niveaus van vertrouwen – en dus van beveiliging – bestaan, resulterend in het bestaan van meerdere CP's (Certificate Policies). De procedure van identiteitscontrole kan dus ook, afhankelijk van het vereiste beveiligingsniveau, verschillen. Zo kan een certificaat worden uitgegeven nadat daartoe via e-mail een verzoek is ingediend, maar is het voor een hoger niveau van vertrouwen in een certificaat nodig dat de gebruiker van het certificaat zich fysiek bij de RA meldt. De verwachting is dat in de toekomst alleen certificaten die zijn uitgegeven nadat de gebruiker zich in persoon heeft geïdentificeerd en geregistreerd bij een TTP, in het elektronisch handelsverkeer zullen worden gebruikt.

Voor TTP's zal een belangrijke rol zijn weggelegd bij het garanderen van betrouwbare elektronische communicatie.

De RA stuurt de gegevens die in het certificaat moeten worden opgenomen naar de CA, die vervolgens een certificaat zal uitgeven.

2 Sleutelbeheer
Indien cryptografische technieken worden toegepast, kan gebruik worden gemaakt van de door een TTP verleende diensten op het gebied van sleutelbeheer. De dienst sleutelbeheer (ook wel key management) omvat het gehele proces van het genereren van sleutels tot het intrekken van sleutels. Het gaat om de volgende diensten:

9) In de Certificate Policies for the Government of Canada Public Key Infrastructure (GOC PKI) (Working Draft) wordt het verschil tussen de CP en CPS als volgt toegelicht: een Certificate Policy is 'A named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirement. For example, a particular certificate policy might indicate applicability of a type of certificate to the authentication of electronic data interchange transactions for the trading of goods within a given price range.' Een Certificate Practice Statement is 'A statement of the practices which a certification authority employs in issuing certificates. The CPS defines the equipment, policies and procedures the CA uses to satisfy the requirements specified in the certificate policies that are supported by it.'

* *het genereren van sleutels*. Partijen die hun eigen sleutels genereren, hoeven van deze dienst geen gebruik te maken, maar kunnen hun zelf gegenereerde sleutels wel laten certificeren door een TTP als CA.
* *het distribueren van sleutels*. In het geval van toepassing van symmetrische cryptografie kan een TTP symmetrische sleutels (genereren en) distribueren voor een klant (bij asymmetrische cryptografie wordt gebruikgemaakt van publieke certificaten die toegankelijk zijn via een databank en is distributie ten behoeve van gebruikers niet nodig). Distributie van cryptografische sleutels dient veilig te gebeuren. Het is ontoelaatbaar dat onbevoegden kennisnemen van de sleutel dan wel veranderingen aanbrengen in die sleutel.
* *het opslaan van private encryptie/decryptiesleutels (key-escrow of key recovery)*. Er kan behoefte bestaan aan een reserve-exemplaar van de private encryptie-/decryptiesleutel. Indien sleutels zoekraken of beschadigd zijn, is het nuttig een reserve-exemplaar achter de hand te hebben. Veelal zal niet de sleutel zelf worden bewaard, maar heeft de TTP speciale data-recovery sleutels onder zich die toegang geven tot de 'originele' encryptie- en decryptiesleutel (key recovery).
Key-escrow is een onderwerp waarover de nodige verdeeldheid bestaat. Nationale overheden vrezen dat criminelen cryptografie gebruiken om hun activiteiten af te schermen van opsporings- en veiligheidsinstanties. Key escrow wordt door sommige overheden dan ook gezien als middel om berichtenverkeer (van criminelen) te kunnen controleren. Nadeel is echter dat de betrouwbaarheid die cryptografie biedt door key escrow vermindert. Het bewaren van een reserve-exemplaar van de private sleutel voor het zetten van digitale handtekeningen stelt zeer hoge beveiligingseisen aan een TTP. Bij doorbreking van de beveiliging van de TTP zou een onverlaat immers rechtshandelingen kunnen verrichten op een valse naam. Om deze reden is het niet raadzaam een reserve-exemplaar van deze sleutel te bewaren.
* *het schorsen of intrekken van sleutels*. Indien het vermoeden bestaat dat een sleutel is gekraakt (gecompromitteerd), kan de sleutel tijdelijk worden geschorst. Afhankelijk van het feit of dit vermoeden wordt bevestigd of ontkracht, zal de sleutel worden ingetrokken dan wel zal de schorsing worden opgeheven.

3 Certificatie

Met behulp van een certificaat kan, zoals eerder ter sprake kwam, een digitale handtekening worden geverifieerd en een bericht worden versleuteld of ontsleuteld. De TTP als CA voert het proces van certificatie uit. Certificatie omvat de volgende diensten:
* *het genereren en uitgeven van certificaten*. Doordat de identiteit van de gebruiker van een certificaat is gecontroleerd door de RA (identificatie/authenticatie) en vervolgens is gekoppeld aan 'zijn' certificaat, hebben partijen over en weer zekerheid dat zij te maken hebben met degene met wie zij denken te doen te hebben. De TTP biedt aldus zekerheid omtrent de authenticiteit van de wederpartij.
* *het opslaan van certificaten*. Dit is de registerfunctie van een TTP. De TTP beheert een lijst met publieke certificaten, de Certification List (CL), waarin de publieke sleutels ten behoeve van encryptie/decryptie en de sleutels voor het verifiëren van digitale handtekeningen zijn opgenomen. De lijst is opgenomen in de databank of directory.
* *het 'updaten' van certificaten of het uitgeven van nieuwe certificaten*. De geldigheidsduur van een certificaat wordt bij de generatie van het certificaat vastgesteld. Na het verstrijken van deze duur is het certificaat ongeldig. Indien een certificaat – bijna – verlopen is, of de gegevens (autorisatie bijvoorbeeld) van de gebruiker zijn veranderd, dan kan het certificaat worden vernieuwd of wordt een nieuw certificaat (met nieuwe publieke sleutel) uitgegeven.
* *het schorsen of intrekken van certificaten*. Indien een private sleutel is gecompromitteerd of er bestaat een vermoeden hiervan, dan zal het met deze sleutel corresponderende certificaat worden geschorst dan wel ingetrokken. Indien de geldigheidsduur van een certificaat is verlopen dan wordt het certificaat ingetrokken. De TTP geeft een Certification Revocation List (CRL) uit zodat bekend is welke certificaten geschorst of ingetrokken zijn. Zo wordt voorkomen dat (rechts)handelingen met ongeldige certificaten kunnen worden verricht. De CRL zal evenals de Certificate List moeten zijn opgenomen in een op permanente basis toegankelijke databank.

Aanvullende diensten

Met het begrip TTP wordt vaak op de hierboven uiteengezette RA- en/of CA-functie gedoeld, maar een TTP kan ook andere, aanvullende diensten verlenen. Aanvullende diensten hebben momenteel voornamelijk het karakter van bewijs- en bewaardiensten. Deze diensten komen van pas indien conflicten ontstaan. Als de ene partij bijvoorbeeld zegt dat een bepaald document is verstuurd of een bepaalde order is betaald en de wederpartij ontkent dit, dan kunnen de aanvullende, op het bewaren en bewijzen gerichte diensten van een TTP uitkomst bieden. Naast deze bewijs- en bewaardiensten (zie de hierna genoemde) is het echter ook denkbaar dat een TTP wordt ingeschakeld om bijvoorbeeld als informatiemakelaar te fungeren (bijvoorbeeld tussen werkzoekende en werkgever of tussen vrachtvervoerders en bedrijven die ladingen te vervoeren hebben of tussen overheid en burgers) of als verrekenorgaan (bijvoorbeeld op het gebied van intellectuele eigendomsrechten zoals auteursrechten). De TTP verricht in een dergelijk geval aanvullende diensten zoals toezending van informatie, facturering en overboeking van licentievergoedingen.

Aanvullende, op het bewijzen en bewaren gerichte diensten die door een TTP kunnen worden verleend zijn, zonder uitputtendheid na te streven, de volgende:

Bewijs van verzending en ontvangst
Nederland kent wat het bewijsrecht betreft een zogenaamd vrij bewijsstelsel. Art. 179 lid 1 Rv zegt dat partijen met alle middelen bewijs kunnen leveren tenzij de wet anders bepaalt. Elektronisch bewijsmateriaal kan dan ook als bewijsmateriaal worden aangevoerd. In een digitale omgeving kan behoefte bestaan aan bewijs van verzending c.q. van ontvangst. Om de bewijspositie te versterken kan gebruik worden gemaakt van de diensten van een TTP. Bewijs omtrent verzending wordt op de volgende wijze verkregen: een verzender X stuurt zijn bericht via een TTP naar ontvanger Y. De organisatie van Y kan vervolgens een bericht van ontvangst sturen

naar de TTP die het bericht, voorzien van zijn digitale handtekening, doorstuurt naar X. Het feit dat het bericht bij de organisatie van Y is aangekomen, wil nog niet zeggen dat Y zelf het bericht heeft ontvangen. Bewijs van ontvangst wordt gegenereerd doordat Y, nadat hij het bericht heeft gelezen, via de TTP (die wederom zijn digitale handtekening toevoegt), een bericht van ontvangst aan X zendt.

Tijdstempelen (time-stamping)
Onder tijdstempelen wordt verstaan dat een TTP berichten, documenten en transacties voorziet van een tijd- en datumstempel. Ook deze dienst is van belang in verband met de bewijskracht die aan elektronische documenten kan worden toegekend. Digitale handtekeningen worden wel gebruikt als tijdstempel. Door een digitale handtekening met tijdsaanduiding op een bepaald (niet noodzakelijkerwijs aan een ander verzonden) document te zetten, verklaart een TTP dat het document bestond op dat tijdstip en in die vorm.
Het systeem werkt aldus: de TTP zal de hashwaarde (zie verder onder 'Digitale handtekening') van een document voorzien van een time-stamp en digitaal ondertekenen (met zijn digitale handtekening) en dit terugsturen aan degene die de TTP om een time-stamp heeft verzocht. Er is zelfs een methode waarbij vertrouwen in de TTP niet een noodzakelijke voorwaarde is om overtuigd te zijn van de betrouwbaarheid van de time-stamp. Bij dit systeem stuurt de TTP niet alleen de hashwaarde (voorzien van time-stamp en zijn digitale handtekening) van het door een cliënt toegestuurde document terug, maar ook een aantal andere hashwaarden en e-mailadressen van andere cliënten die een document hebben laten tijdstempelen. Nu moet dus een hele groep (naast de TTP ook een aantal andere cliënten) bij een eventuele antedatering betrokken zijn ([Froo96], § I D 4).

Het bewaren van elektronische documenten
Indien partijen onenigheid vrezen over de werkelijke inhoud van een elektronisch document en dit willen voorkomen, dan kan afgesproken worden het document bij een TTP in bewaring te geven. De TTP zal het bericht, voorzien van zijn digitale handtekening en een tijdstempel, bewaren. De inhoud van het bij de TTP gedeponeerde document zal door partijen worden geaccepteerd.

Eisen te stellen aan TTP's

Hoewel het begrip TTP nog niet geheel is uitgekristalliseerd, kan er wel een aantal eisen worden geformuleerd waaraan een TTP dient te voldoen. Aan de volgende eisen dienen TTP's in ieder geval te voldoen:
* *betrouwbaarheid*. De TTP dient over een aantal eigenschappen te beschikken, waarmee ze aan haar klanten kan aantonen dat ze betrouwbaar is. De hierna genoemde eigenschappen vormen naar mijn mening samen de bouwstenen van de betrouwbaarheid van een TTP.
* *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 een 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).
* *deskundigheid*. Het personeel van een TTP dient aan bepaalde opleidings- en ervaringsvereisten te voldoen.

Regelgeving

De exacte invulling van het begrip TTP is allerminst uitgekristalliseerd. Diverse (inter)nationale organen houden zich bezig met de vraag aan welke eisen een TTP zou moeten voldoen.

Nationaal

Op nationaal niveau kan worden gewezen op de in 1997 door de overheid opgerichte projectgroep (projectgroep TTP.NL) waaraan de Ministeries van Verkeer en Waterstaat, Binnenlandse Zaken, Justitie, Economische Zaken, Defensie en Algemene Zaken deelnemen. In de eindrapportage van de projectgroep wordt geconcludeerd dat TTP's een belangrijke rol kunnen spelen bij de 'opbloei van een veilige, betrouwbare en beheersbare infrastructuur voor electronic commerce' ([MinEZ98b], p. 7). Om die reden wordt vanuit de projectgroep een snelle ontwikkeling van TTP-infrastructuren zeer wenselijk geacht. In de rapportage worden randvoorwaarden voor het aanbieden en gebruiken van TTP-diensten geformuleerd. Deze voorwaarden hebben betrekking op zaken als onafhankelijkheid (ten opzichte van andere partijen, maar ook in financieel opzicht), onpartijdigheid, continuïteit (hierbij is bijvoorbeeld de financiële positie van de TTP van groot belang), beveiliging, aansprakelijkheid, privacy en interoperabiliteit (tussen nationale en internationale TTP-infrastructuren).

Voorts adviseert de projectgroep een zogeheten TTP-kamer op te richten. Die TTP-kamer is een overkoepelende organisatie, waarin zowel de overheid als aanbieders en gebruikers van TTP-diensten op vrijwillige basis zitting hebben, die de randvoorwaarden zoals omschreven in de eindrapportage in een bindend reglement opneemt. Met de instelling van een dergelijke kamer acht de projectgroep de totstandkoming van wetgeving of andere vormen van regulering niet noodzakelijk. De belangrijkste beoogde taak van de TTP-kamer is het verlenen van een – niet verplichte – goedkeuring in de vorm van een 'keurmerk' aan TTP's die aan de geformuleerde eisen voldoen. Een dergelijk keurmerk is zeer waardevol voor (potentiële) certificate subjects en relying parties en kan bovenal een positieve bijdrage leveren aan het proces van cross-certificatie, op nationaal maar ook op internationaal niveau. Voorts zou de TTP-kamer wederzijdse erkenning tussen Nederlandse TTP's en internationale TTP-infrastructuren moeten realiseren. Om uitwerking te geven aan de door de projectgroep verrichte werkzaamheden is een vervolgtraject opgezet. Een drietal werkgroepen is ingesteld. Daarvan moet de werkgroep 'Certificate Policy' een overkoepelende CP voor de nationale TTP-infrastructuur opstellen. De werkgroep 'TTP-kamer' is belast met onderzoeken van de institutionele en operationele aspecten van het inrichten van

een TTP-kamer. En ten slotte heeft de werkgroep 'Accreditatie en Certificatie' tot doel een infrastructuur op te zetten voor het certificeren[10] en accrediteren[11] van TTP's in Nederland.

Internationaal

Uiteraard is het van het grootste belang voor de werkelijke totstandkoming van wereldwijde Internet electronic commerce dat TTP's uit verschillende landen elkaars certificaten accepteren. Hierbij is het van belang te weten welke vereisten aan digitale handtekeningen worden gesteld, maar is het bijvoorbeeld ook relevant dat richtlijnen voor accreditatie en certificatie van TTP's internationaal geaccepteerd en toegepast worden. Diverse internationale gremia zetten zich in om internationaal geaccepteerde standaarden te realiseren.

Diverse gremia zijn bezig met internationale standaarden.

De Europese Commissie heeft in haar mededeling genaamd *A European Initiative in Electronic Commerce* ([EuCo97a]) digitale handtekeningen aangewezen als een essentieel hulpmiddel om te voorzien in veiligheid en om vertrouwen op open netwerken (zoals het Internet) te ontwikkelen. Ook in de ministeriële verklaring van Bonn werd erkend dat digitale handtekeningen een sleutelelement zijn voor de elektronische handel. Als een eerste stap heeft de Commissie de mededeling *Ensuring Security and Trust in Electronic Communication – Towards a European framework for Digital Signatures and Encryption* ([EuCo97b]) ingediend. Aanbevolen wordt te komen tot een Europees raamwerk voor digitale handtekeningen en encryptie, om zowel electronic commerce en de economische groei en werkgelegenheid binnen de Gemeenschap (ofwel de concurrentiepositie van de EU) te stimuleren alsook om de – grensoverschrijdende – toepassing van digitale handtekeningen te faciliteren. Uiteindelijk heeft dit in mei 1998 geresulteerd in de 'Proposal for a European Parliament and Council Directive on a common framework for electronic signatures' ([EuCo98]). Dit voorstel heeft tot doel belemmeringen, veroorzaakt door verschillen in wettelijke erkenning van elektronische handtekeningen[12], weg te nemen om zo een goed functioneren van de interne markt te verzekeren. Dit moet gebeuren door een gemeenschappelijk juridisch kader voor elektronische handtekeningen tot stand te brengen. Juridische erkenning van elektronische handtekeningen mag volgens het voorstel niet afhankelijk zijn van het al dan niet geaccrediteerd zijn van een 'certification service provider' (ofwel een CA of een TTP in de functie van CA). Gemeenschappelijke vereisten gesteld aan certification service providers moeten de grensoverschrijdende erkenning van handtekeningen en certificaten binnen de EU ondersteunen. In april 1999 hebben de EU-ministers voor telecommunicatie de richtlijn aangenomen. Het Europees Parlement moet (ten tijde van het ter perse gaan van dit boek) de richtlijn nog goedkeuren.

Ook de Verenigde Naties heeft via haar instelling UNCITRAL (United Nations Commission on International Trade Law) activiteiten ontplooid op het gebied van elektronische handel. UNCITRAL heeft een modelwet inzake elektronische handel goedgekeurd en is begonnen met de voorbereiding van uniforme regels inzake digitale handtekeningen.
Voorts zijn de werkzaamheden van de American Bar Association (ABA) van belang. De ABA heeft reeds richtlijnen ontwikkeld die gebruikt kunnen worden bij het opstellen van regelgeving voor TTP's en ontwikkelt momenteel richtlijnen voor de accreditatie en certificatie van TTP's.

Tot slot

Uit bovenstaande blijkt dat TTP's een belangrijke bijdrage kunnen leveren aan de betrouwbaarheid (authenticiteit, integriteit, vertrouwelijkheid, onweerlegbaarheid en autorisatie) van het elektronisch berichtenverkeer, waaronder electronic commerce. Vooralsnog lijkt er echter een situatie te bestaan waarin de ontwikkeling van TTP-diensten wacht op verdere ontwikkeling van electronic commerce, terwijl de doorbraak van electronic commerce juist afhankelijk lijkt te zijn van de beschikbaarheid van een betrouwbare TTP-infrastructuur ([MinEZ98], p. 13). Zowel op nationaal als op internationaal niveau wordt het belang van TTP's onderkend en worden initiatieven ontplooid om de totstandkoming van TTP-infrastructuren te faciliteren. Wellicht dat die initiatieven een eind kunnen maken aan 'de kip-of-het-ei-situatie' die momenteel lijkt te bestaan.

10) Certificeren houdt hier in dat een TTP wordt 'gewaarmerkt'; een onafhankelijke, onpartijdige, deskundige en betrouwbare instelling verklaart dat de TTP voldoet aan vooraf opgestelde eisen. Certificeren kan ook inhouden dat de TTP een houder van een certificaat voorziet.

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

12) Een digitale handtekening is een vorm van een elektronische handtekening. Het voorstel kiest voor een technologieonafhankelijke benadering. Erkend wordt echter wel dat digitale handtekeningen die met behulp van cryptografische technieken totstandkomen, momenteel de belangrijkste categorie van elektronische handtekeningen zijn ([EuCo98], p. 4).

Literatuur

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

[EuCo97a]
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 final, 16.4.1997, http://www.cordis.lu/esprit/src/ecomcom.htm

[EuCo97b]
European Commission, Communication to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, *Ensuring Security and Trust in Electronic Communication – Towards a European framework for Digital Signatures and Encryption*, COM (97)503 final, 8.10.1997, http://www.ispo.cec.be/eif/policy/97503toc.html

[EuCo98]
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 final, 13.5.1998, http://www.ispo.cec.be/eif/policy

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

[Froo96]
A.M. Froomkin, *The essential role of trusted Third Parties in Electronic Commerce*, 1996, http://www.law.miami.edu/~froomkin/articles/trusted.htm

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

[Icov95)]
D. Icove et al., *Computer Crime: A Crimefighter's Handbook*, 1995.

[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, http://www.idc.com

[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, http://info.minez.nl/pdfs/05r38.pdf

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

[MinJ98]
Ministerie van Justitie, *Wetgeving voor de elektronische snelweg*, TK 1997-1998, 25 880, nrs. 1-2, http://www.minjust.nl/sdu/index.htm

[OECD97a]
OECD, Policy Brief; electronic commerce , no 1, OECD 1997, http://www.oecd.org.publications/Pol_brief/9701_Pol.htm

[OECD97b] OECD, *Cryptography Policy: the Guidelines and the Issues. The OECD Cryptography Policy Guidelines and the Report on Background and Issues of Cryptography Policy*, 1997, http://www.oecd.org/dsti/sti/it/secur/prod/e-crypto.htm