Een open tunnelvisie

Evaluatie van het TTP-beleid

Eindrapport

Universiteit van Tilburg/Ordina Public Management Consulting

30 juni 2004

Dr. mr. S. Zouridis
Dr. M. Thaens
Dr. J. Kielema
Dr. S. van der Hof

m.m.v. S. Tinnemans en A.J.D. Dijkshoorn

'Voorspellingen doen is erg moeilijk. Vooral over de toekomst.'
Niels Bohr

Inhoud

Samenvatting

Uitvoering van het TTP-beleid
Na enkele jaren voorbereiding kondigt het Ministerie van Economische Zaken in juni 1999 beleid af dat de totstandkoming van openbare TTP-dienstverlening beoogt te stimuleren. Tijdens de uitvoering van dat beleid worden de beleidsmakers geconfronteerd met een Europese richtlijn over elektronische handtekeningen. De uitvoering van het TTP-beleid staat vanaf dat moment in het teken van implementatie van deze richtlijn. De juridische verankering van de elektronische handtekening gaat samen met een arrangement voor vrijwillige certificering van aanbieders (een certificatieschema in combinatie met een audit-, respectievelijk toezichtsstructuur). Feitelijk is daarmee een deel van het TTP-beleid uitgevoerd, namelijk dat deel dat zich richt op de elektronische handtekening. Intussen is in de afgelopen jaren de doelstelling van dat beleid, bloeiende elektronische handel, vooral los van het beleid gerealiseerd, wellicht minder dan verwacht als gevolg van de conjuncturele inzinking.

Huidige situatie?
Het TTP-beleid heeft zich in de praktijk ontwikkeld van een set van minimumvoorwaarden voor betrouwbare elektronische handel tot een arrangement dat garant staat voor een hoog niveau van veiligheid. Aan dat hoge niveau is vooralsnog weinig behoefte in de markt; zowel de overheid als het bedrijfsleven gebruiken momenteel voor elektronische handel en dienstverlening vooral lagere niveaus van beveiliging. Op deze niveaus heeft (nog) geen standaardisatie plaatsgevonden. Deze huidige situatie wordt, zo blijkt uit het onderzoek, op verschillende manieren geduid: (1) het TTP-beleid is goed opgezet en uitgevoerd, maar het duurt iets langer voordat het succes heeft, (2) er is door de beleidsmakers op het verkeerde (want te hoog beveiligde) paard gewed of (3) het oorspronkelijke beleid berustte niet op valide veronderstellingen, maar er is op tijd bijgestuurd als gevolg van de Europese richtlijn.

Hoe verder?
De keuze voor de toekomst van het TTP-beleid hangt mede af van de waardering van de huidige situatie. Ook is van belang welke inschatting wordt gemaakt van de ontwikkelingen die we de komende jaren kunnen verwachten. We hebben in het onderzoek drie handelingsperspectieven aangetroffen:

1. Doorgaan op de huidige weg en beleidsmatig inzetten op het stimuleren van het gebruik van het gerealiseerde hoge niveau. Sommigen verwachten sowieso een beweging in de markt naar hogere niveaus van beveiliging, zodat wat nu tot stand is gebracht in de (nabije) toekomst in een (meer of minder grootschalige) behoefte gaat voorzien. Bovendien zou de introductie van een elektronisch identiteitsdocument (eNIK) een nieuwe situatie kunnen creëren, omdat daarop een elektronische handtekening conform de huidige standaarden kan worden aangebracht. In dit perspectief kan het TTP-beleid nog wat extra stimulansen geven aan de markt: bijvoorbeeld door het verlagen van de kosten van certificering en/of registratie (door een tegemoetkoming in de kosten te bieden), door applicaties te bevorderen die gebruik maken van gekwalificeerde certificaten (bijvoorbeeld door stimuleringssubsidies of –kredieten) of door meer voorlichting en onderwijs.
2. Stoppen met het TTP-beleid zoals dat oorspronkelijk is geformuleerd en terugbrengen van de overheidsbemoeienis tot het onderhouden van de door de Europese richtlijn voorgeschreven wet- en regelgeving. In dit perspectief kan ook het huidige

arrangement worden vereenvoudigd door bijvoorbeeld de vrijwillige certificering uit het systeem te verwijderen. Voor dit perspectief pleiten diegenen die uit de huidige situatie aflezen dat het TTP-beleid op het verkeerde paard heeft gewed. Betrouwbare elektronische communicatie via TTP is volgens hen immers geen voorwaarde gebleken voor het opbloeien van elektronische handel en elektronische overheidsdienstverlening. Aan het huidige, hoge niveau is geen behoefte, aldus de voorstanders van dit handelingsperspectief.

3. Verbreden van het beleid op basis van het oorspronkelijke TTP-concept. Op twee manieren is een verbreding mogelijk: verbreding van de TTP-diensten die onder het beleid vallen (naast elektronische handtekening ook andere diensten met betrekking tot authenticiteit, integriteit en vertrouwelijkheid van het berichtenverkeer) en/of verbreding van het betrouwbaarheidsniveau (dus ook standaardisatie van lagere niveaus). In beide gevallen betekent dit voor het beleid dat het huidige certificatieschema wordt uitgebreid of dat gewerkt wordt aan een of meer nieuwe schema's voor certificering.

In een toekomstworkshop die we in het kader van het evaluatieonderzoek hebben georganiseerd sprak een meerderheid van de deelnemers zich uit voor een combinatie van 'doorgaan' en 'verbreden'. Deze deelnemers zijn van mening dat het gebruik van de gekwalificeerde certificaten gestimuleerd moet worden. Tevens zien zij mogelijkheden om het versmalde concept aan te passen. Deze verbreding, zo werd opgemerkt, moet wel aansluiten bij daadwerkelijke behoeften van potentiële gebruikers van de voorziening (bijvoorbeeld banken en grote bedrijven). Overigens is deze behoefte verre van statisch: het 'meten' ervan op een specifiek moment zegt daarom niet zo veel. Mede daarom zou volgens de pleitbezorgers van de combinatie 'doorgaan' en 'verbreden' eerst moeten worden ingezet op het stimuleren van het gebruik van de huidige voorziening; daarna is verbreden aan de orde. Een kleine minderheid sprak zich tijdens de toekomstworkshop uit voor het perspectief 'stoppen'.

Overigens leveren de interviews met marktpartijen nog wat extra overwegingen op. Enkele marktpartijen verwachten dat de eventuele invoering van de elektronische identiteitskaart niet vanzelfsprekend zal leiden tot gebruik. Er zijn immers nog geen toepassingen voorzien, stellen ze, en omdat er van een eventueel op de kaart aangebrachte gekwalificeerd certificaat weinig meerwaarde kan worden verwacht zijn er op korte termijn weinig toepassingen te verwachten, aldus deze marktpartijen. Zij geven wel aan dat het al dan niet gebruiken van de gekwalificeerde certificaten afhangt van de prijs. Omdat we in het kader van het evaluatieonderzoek een beperkt aantal marktpartijen hebben gesproken, dienen deze conclusies met enige voorzichtigheid te worden geïnterpreteerd.

1. Inleiding

1.1 TTP-beleid: achtergrond en betekenis

Virtuele identiteit en fysieke identiteit: een fluïde relatie
Sinds de exponentiële toename van elektronische communicatie staan vraagstukken van identiteit en identiteitsmanagement op de bestuurlijke en wetenschappelijke agenda. Omdat de directe relatie met een fysieke verschijning bij elektronische communicatie verdwijnt, heeft iemands identiteit in de virtuele wereld een meer fluïde en vluchtig karakter gekregen. De korte geschiedenis van het internet laat in tal van verhalen zien welke vragen deze vluchtigheid oproept. De verhalen variëren van jarenlange intensieve deelname aan een virtuele gemeenschap op basis van een schijnidentiteit tot het anoniem verspreiden van een wereldwijd computervirus. Wetenschappelijk doet zich de interessante vraag voor naar het ontstaan en de aard van sociale relaties. Zo lijkt het voor veel mensen makkelijker persoonlijke vragen in een grote groep aan de orde te stellen als ze zich kunnen verschuilen achter een virtuele identiteit. Vanuit het openbaar bestuur bekeken gaat het vooral om vraagstukken van identificatie in het publieke domein. Levert de vloeibare relatie tussen virtuele identiteit en fysieke identiteit bijvoorbeeld problemen op voor veiligheid en criminaliteitsbestrijding, elektronische handel of elektronisch bestuur? Zakelijke transacties komen bij voorkeur tot stand als er sprake is van onderling vertrouwen: het vertrouwen dat het beloofde aanbod zal worden geleverd en aan de andere kant het vertrouwen dat de andere partij daarvoor zal betalen. Het kunnen vaststellen van iemands identiteit kan een voorwaarde zijn voor het totstandkomen van onderling vertrouwen, simpelweg vanwege het feit dat als iemands identiteit bekend is de wet in stelling kan worden gebracht om contractuele afspraken af te dwingen.

ACHTERGROND TTP-BELEID

- Fluïde relatie fysieke en elektronische identiteit
- Belemmering voor elektronische handel en overheidsdienstverlening?
- Technische oplossing: PKI en TTP

Op zoek naar betrouwbare elektronische communicatie
In de loop van de jaren negentig wordt voor het realiseren van betrouwbare elektronische communicatie steeds vaker gekeken naar de overheid. Het ontbreken van een betrouwbare infrastructuur voor elektronische communicatie zou een belemmering zijn voor elektronische handel (en later ook voor elektronisch bestuur). De onbetrouwbaarheid van de infrastructuur had op dat moment te maken met vraagstukken van identiteit, maar ook met onzekerheid bijvoorbeeld over de precieze verzending (en afkomst) van elektronische berichten. Overigens wordt de onbetrouwbaarheid door sommigen in die tijd vooral geweten aan het gedrag van de internetgebruikers. Als we het gemiddeld internetgedrag van gebruikers zouden vertalen naar de fysieke wereld, zou dat er volgens Esther Dyson op neerkomen dat de auto niet wordt afgesloten en zelfs uitnodigend met de sleutels op het contactslot zou worden achtergelaten (Dyson, 1998). In het algemeen omvat betrouwbaarheid van gegevens in het handelsverkeer volgens Koops, Van Kralingen en Van der Wees (1998) vier aspecten:

- de authenticiteit van gegevens: zekerheid over de identiteit van de afzender en over de herkomst van berichten;

- de integriteit van gegevens: zekerheid dat gegevens volledig zijn en niet door onbevoegden zijn gewijzigd;
- de vertrouwelijkheid van gegevens: zekerheid dat gegevens niet ingezien kunnen worden door personen die daartoe niet bevoegd zijn;
- de beschikbaarheid van gegevens: zekerheid dat gegevens op het juiste moment voor de rechthebbenden toegankelijk zijn.

Vanuit deze aspecten (informatiebeveiliging) wordt halverwege de jaren negentig veel onderzoek gedaan naar mogelijkheden voor veilige en betrouwbare elektronische communicatie. Op dat moment wordt de zogenaamde Public Key Infrastructure (PKI) gezien als een technische oplossing. Het gaat bij PKI om een variant van de klassieke op cryptografie gebaseerde systemen die we uit spionageromans kennen. De klassieke systemen gebruiken voor versleutelen en ontsleutelen dezelfde sleutel. Publieke-sleutelsystemen zijn gebaseerd op een sleutelpaar, dat uit een publieke en private sleutel bestaat. Wat met de publieke sleutel is versleuteld, kan met de private sleutel worden ontsleuteld. Of andersom: met de private sleutel kan een bericht worden versleuteld dat met de publieke sleutel te ontsleutelen is. Door deze a-symmetrische cryptografie is het mogelijk geworden om vertrouwelijk te communiceren zonder eerst de (geheime) sleutel uit te wisselen. Daarnaast is het tevens mogelijk om de authenticiteit van een bericht te waarborgen. Dat laatste gebeurt door met een private sleutel bij verzending een uittreksel van het bericht (de zogeheten 'hash') te versleutelen en dat aan het bericht toe te voegen, waarna iedere ontvanger van het bericht de toegevoegde 'hash' met de publieke sleutel kan ontsleutelen. De authenticiteit van het bericht is aldus gewaarborgd, omdat alleen diegene die over de private sleutel beschikt het bericht kan hebben verzonden. Tevens kan op die manier de integriteit van het bericht worden gewaarborgd, want de 'hash' is een soort vingerafdruk van het bericht: verandert het bericht onderweg dan komt de oorspronkelijk toegevoegde 'hash' niet overeen met de 'hash' van het veranderde bericht.

PKI-technologie

PKI-technologie maakt in het algemeen drie functies mogelijk die als belangrijk worden beschouwd voor elektronische communicatie en transacties in het zakelijke verkeer of met de overheid (PKIoverheid, 2002):

- Elektronische identificatie: de identiteit van de persoon met wie wordt gecommuniceerd kan worden vastgesteld. Dit is een functie waarbij het met 'grote zekerheid duidelijk wordt wie de communicatiepartner aan de 'andere' kant van het netwerk is.'
- Elektronische handtekening: 'de (juridische) zekerheid dat een bericht door een bepaalde persoon is verzonden of een document door een bepaalde persoon is ondertekend en dit ook niet achteraf kan worden ontkend (elektronische handtekening en onweerlegbaarheid).'
- Vertrouwelijkheid: 'de mogelijkheid om communicatie te beschermen tegen ongewenste inzage (vertrouwelijkheid, privacy) of wijziging (integriteit) door derden.'

Voor het vertrouwen in dit type cryptografie is het certificeren van sleutels belangrijk, omdat gebruikers ervan op aan moeten kunnen dat de openbare sleutel waarmee een vertrouwelijk bericht wordt versleuteld ook daadwerkelijk toebehoort aan de ontvanger. Voor het certificeren wordt bij PKI een zogenaamde certificaatinfrastructuur gecreëerd. Die zorgt voor het genereren, uitgeven, laten gebruiken, beheren en controleren van certificaten of sleutelparen. Hoewel het niet noodzakelijk is dat certificatie plaatsvindt door een derde –

onafhankelijke - partij (een van de communicatiepartners kan ook als certificatie-autoriteit fungeren), is voor zogenaamde 'openbare' communicatie (waarbij iedereen met iedereen communiceert) al snel het concept van de 'trusted third party' (TTP) bedacht. Deze derde partij kan als certificatie-autoriteit optreden, maar ook andere (al dan niet op cryptografie gebaseerde) diensten kan leveren.

Elektronische handtekening c.s.

PKI staat dus voor de technische omgeving waarin met een publieke en een private sleutel wordt gewerkt. Hoewel de elektronische handtekening als een van de functies van PKI wordt genoemd, bestaat er over het begrip elektronische handtekening veel spraakverwarring. Juridisch gesproken is een *elektronische handtekening* de elektronische variant van een gewone handtekening, een benaming voor elektronische gegevens die zijn vastgehecht aan of logisch verbonden zijn met een elektronisch document. Dat betekent dat een ingescande handtekening van een papieren drager ook als elektronische handtekening wordt beschouwd. De elektronische handtekening staat daarmee los van een bepaalde techniek, zoals PKI. Elektronische handtekeningen kunnen dus met een PKI worden gegenereerd, maar ook met andere technologieën.

Een verbijzondering van de elektronische handtekening is de *digitale handtekening*: dit is een versleuteltechniek die met een publieke en een private sleutel werkt.
In het recht is een bepaald soort elektronische handtekeningen gecreëerd, de *geavanceerde elektronische handtekening*. Deze:

EEN WOUD VAN BEGRIPPEN

- Elektronische handtekening
- Digitale handtekening
- Geavanceerde elektronische handtekening
- Gekwalificeerde elektronische handtekening

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

Een deel van de geavanceerde elektronische handtekeningen stelt de wet gelijk aan de handgeschreven handtekening. Daarvoor moet de geavanceerde elektronische handtekening:

- gebaseerd zijn op een gekwalificeerd certificaat;
- gegenereerd zijn met een veilig middel voor het aanmaken van elektronische handtekeningen.

Hoewel de wet het begrip niet kent, wordt voor deze handtekening in de praktijk wel het begrip *gekwalificeerde handtekening* gebruikt.

TTP-beleid

Om elektronische handel (en elektronische overheidsdienstverlening) te bevorderen is in de tweede helft van de jaren negentig een zogenaamd TTP-beleid ingezet door de overheid.[1] Het beleid beoogde de totstandkoming van openbare TTP-dienstverlening te stimuleren. Daarbij gaat het om TTP-diensten die als zodanig worden aangeboden op een markt; deze diensten

[1] *Kamerstukken II* 1998-1999, 26 851, nr. 1

kunnen betrekking hebben op het waarborgen van de authenticiteit, integriteit en vertrouwelijkheid van berichten en dus ook op elektronische handtekeningen. Zowel nationaal als internationaal beschouwen in die tijd veel juristen, beleidsmakers en standaardisatie-organisaties deze TTP als een veilige 'stop' voor het vertrouwenslek dat het internet veroorzaakt. Omdat openbare TTP een cruciale positie zouden krijgen in het elektronische handelsverkeer, achtten Nederlandse beleidsmakers het verstandig om goed na te denken over de randvoorwaarden en criteria voor TTP-diensten. In 1999 start dan ook een nationaal project dat erop gericht is een toetsingskader te ontwerpen voor openbare TTP-dienstverlening. Het voorstel hiervoor is op 3 juni 1999 aan de Tweede Kamer aangeboden, maar reeds ruim een jaar daarvoor al op hoofdlijnen gereed gekomen.

1.2 Benadering en opzet van het evaluatieonderzoek

Het evaluatieonderzoek

In het voorliggende evaluatieonderzoek proberen we vast te stellen of de in het genoemde voorstel genoemde doelen zijn bereikt en in welke mate dat aan het beleid kan worden gerelateerd. Het TTP-beleid is echter niet een statisch geheel dat op een moment is bedacht en vervolgens precies zo is uitgevoerd (zie Van Rij en Van Eeten, 2003; Van Rij, 2002). De voortdurende verandering van de beleidsrelevante omgeving is door de beleidsmakers aangegrepen om naar kansen voor realisatie van het beleid te zoeken en in het beleid in te spelen op nieuwe ontwikkelingen.

HET EVALUATIEONDERZOEK

- Greep krijgen op dynamiek en omgeving TTP-beleid
- Inzicht in strategische keuzes bij ontwerp en uitvoering van beleid
- Houvast: congruentie keuzes met achterliggend beleidsdoel en ontwikkelingen in de omgeving

Twee uitgangspunten staan daarom in de evaluatie centraal:

1. De dynamiek van het beleid sinds 1999 wordt niet weggewerkt door voor het beleid als geheel achteraf een zuiver 'doel-middel' schema vast te stellen en dat met de feitelijke situatie van nu te confronteren. Integendeel, de dynamiek wordt expliciet tot onderwerp van evaluatie gemaakt. Daarmee ontleden we het complex van keuzes welke op verschillende momenten door de overheid zijn gemaakt.
2. We beschouwen het TTP-beleid niet als een geïsoleerd geheel, maar plaatsen de keuzes die op specifieke momenten zijn gemaakt en de veronderstellingen die daaraan ten grondslag liggen in het licht van de toenmalige omstandigheden en ontwikkelingen. Daarbij concentreren we ons op maatschappelijke, technologische en juridisch-beleidmatige ontwikkelingen op het moment dat de keuze gemaakt werd.

Vraagstelling voor het evaluatieonderzoek

We vertrekken in het onderzoek vanuit het oorspronkelijk geformuleerde doel van het TTP-beleid. In het voorstel aan de Kamer is dat doel omschreven als het 'ervoor zorgen dat binnen het private alsmede het publieke domein een infrastructuur voor betrouwbare elektronische communicatie zou ontstaan. Deze infrastructuur zou zich moeten kenmerken door een brede beschikbaarheid en laagdrempelige toegang.'

Vanuit dit doel richt het onderzoek zich op de volgende vragen, die ontleend zijn aan de projectbeschrijving voor het evaluatieonderzoek van het Ministerie van Economische Zaken.

- Allereerst moet worden vastgesteld of de invulling van het beleidsdoel uit de notitie van 1999 is gehaald, in het bijzonder:
  - Is er een markt voor TTP-dienstverlening ontstaan?
  - In hoeverre heeft TTP-dienstverlening aantoonbaar bijgedragen aan betrouwbare elektronische communicatie ter ondersteuning van e-business en e-government?

- Het beleidsdoel wordt vervolgens in de beleidscontext (maatschappelijk, technologisch, juridisch-beleidsmatig) geplaatst om de resultaten van het beleid te toetsen op congruentie met de toenmalige situatie in het beleidsveld en ontwikkelingen die zich daarin sindsdien hebben voorgedaan. Dus:
  - In hoeverre is er in de markt behoefte aan die betrouwbaarheid die TTP-dienstverlening mogelijk maakt in elektronische communicatie?
  - In hoeverre is tot op heden betrouwbare elektronische communicatie voor e-business en e-government zonder tussenkomst van een TTP-dienst door alternatieve technieken en diensten ondersteund en in hoeverre is te verwachten dat dit in de voorzienbare toekomst zal plaatsvinden c.q. in omvang zal toenemen?
  - In hoeverre past het TTP-beleid bij technologische, maatschappelijke en juridisch-beleidsmatige ontwikkelingen en in hoeverre vormt het arrangement als geheel (en het TTP-beleid daarbinnen) een consistent geheel?

HET EVALUATIEONDERZOEK

- Beleidsdoel gehaald?
- Opzet en uitvoering congruent met ontwikkelingen in de beleidsrelevante omgeving?
- Bijdrage van het beleid aan halen doel?
- Beleid efficiënt geweest?
- Handelingsperspectieven voor de toekomst?

- Vervolgens moet worden vastgesteld wat de *bijdrage van het TTP-beleid* is geweest aan het (geheel of ten dele) behalen van het beleidsdoel. Dus:
  - In welke mate heeft het gevoerde beleid bijgedragen aan het proces van marktvorming?
  - In hoeverre heeft het gevoerde beleidsinstrument van een vrijwillige certificatieregeling (TTP.NL) bijgedragen aan en geleid tot de doelen als de vorming van een TTP-infrastructuur, kwaliteit van dienstverlening, vertrouwen van het betreffende publiek in die dienstverlening alsmede transparantie van de TTP-markt?
  - In hoeverre heeft het wettelijk toezicht door de OPTA bijgedragen aan en geleid tot de verwezenlijking van de doelstelling?

- Het min of meer 'droog' vaststellen van de bijdrage van het TTP-beleid aan de genoemde doelstelling wordt gevolgd door een analyse van de *oorzaken* van effectiviteit. Dat komt neer op de volgende vragen:
  - In hoeverre waren de oorspronkelijke assumpties waarop het TTP-beleid is gebaseerd valide (de beleidstheorie)? Deze assumpties hebben betrekking op (1) technologische ontwikkelingen, (2) het beleidsregime (marktomstandigheden en marktwerking), (3) de effecten en mechanismen die

inzet van het beleidsinstrumentarium zou veroorzaken, (4) de strategische voor- en nadelen van het koploperschap van Nederland, (5) de voor- en nadelen van de hoge mate van uniformiteit die in het TTP-beleid is gerealiseerd.
  - De manier waarop is ingespeeld op veranderingen in de beleidsomgeving. In een statische omgeving is de *validiteit van de oorspronkelijke beleidstheorie* de belangrijkste, wellicht zelfs enige oorzaak van effectiviteit. In een dynamische omgeving komt daar ook de *responsiviteit van het beleid* bij: in hoeverre zijn bij de inzet van het instrumentarium, het aanpassen daarvan en het opnieuw doordenken van het beleidsdoel veranderende omstandigheden geïncorporeerd (maatschappelijk, juridisch-beleidsmatig en technologisch). De inzet van beleidsinstrumenten komt doorgaans terecht in een reflexieve werkelijkheid. Actoren spelen strategisch in op het beleid, zoeken naar mogelijkheden om hun belang te koppelen aan het beleid, wegen om ongewenst beleid te omzeilen, enzovoort. Daarmee zouden ze een oorspronkelijk valide beleidstheorie in de uitvoering kunnen ontkrachten en de effectiviteit bedreigen. Het evaluatieonderzoek zal zich dan ook mede moeten richten op de manier waarop het TTP-beleid sinds 1997 is aangepast en geherdefinieerd.

- Het evaluatieonderzoek beoogt niet alleen vast te stellen of het beleidsdoel is gerealiseerd en in welke mate het beleid daaraan heeft bijgedragen (effectiviteit), maar ook inzicht te geven in de verhouding tussen kosten en baten die het beleid veroorzaakt (*efficiëntie*). De daarbij behorende onderzoeksvraag luidt:
  - Zijn de kosten die worden veroorzaakt door het TTP-beleid (inclusief het bijbehorende instrumentarium) bij alle betrokken actoren (waaronder de TTP-dienstverlener en de afnemers van deze dienstverlening) in verhouding met de verkregen baten?

- Tenslotte komt het erop aan met het evaluatieonderzoek aanknopingspunten te formuleren voor de toekomst van het TTP-beleid. Daarvoor hanteren we de volgende onderzoeksvragen:
  - Wat zou, naar mening van de markt (zowel aanbod- als vraagzijde), de rol van de overheid in het vervolg moeten zijn?
  - Op welke punten en in hoeverre is bijstelling van het beleid en het gehanteerde instrumentarium noodzakelijk of wenselijk?
  - Kunnen de gestelde beleidsdoelen, gegeven het wettelijk kader, in de toekomst ook tegen lagere kosten worden bereikt en zo ja, hoe?

Het antwoord op deze vragen is samengevat in paragraaf 6.2.

Ontwerp en methode van onderzoek

Er is bij de start van het TTP-beleid geen nulmeting verricht waarmee we de huidige toestand kunnen vergelijken om de precieze effecten van het beleid vast te stellen. Evenmin is een controlegroep beschikbaar om te analyseren wat er zonder het TTP-beleid zou zijn gebeurd. Daarom is voor een ander onderzoeksontwerp gekozen. We baseren de evaluatie primair op een analyse van de huidige toestand, alsmede reconstructies van de beleidstheorie en van de uitvoering (en bijstelling) van het TTP-beleid.
Daarbij geldt dat de omvang van het onderzoek beperkt is geweest en de doorlooptijd betrekkelijk kort. Dat betekent dat het antwoord op een deel van de gestelde vragen noodzakelijkerwijs een exploratief karakter heeft. Daarvoor is gekozen vanuit de overweging

dat het belangrijker is dat de evaluatie lessen oplevert voor de toekomst van het TTP-beleid dan een compleet beeld van bijvoorbeeld de beschikbare technieken voor betrouwbare elektronische communicatie. Het evaluatieonderzoek bestaat op basis van de beschreven vraagstelling uit de volgende onderdelen:

1. Reconstructie van de oorspronkelijke beleidstheorie (doel, instrumenten, analyse beleidsveld, assumpties ten aanzien van technologische, maatschappelijke en juridisch-beleidsmatige ontwikkeling). Daarvoor hebben we een literatuurscan uitgevoerd, alsmede een analyse gemaakt van de documenten waarop het TTP-beleid is gebaseerd. Enkele interviews met beleidsmakers en een toets van de reconstructie in een expertmeeting (met deskundigen en beleidsmakers) hebben het beeld gecompleteerd.
2. Reconstructie van de uitvoering van het TTP-beleid en de manier waarop beleidsmakers in hun strategische keuzen sinds de totstandkoming van het oorspronkelijke beleid hebben ingespeeld op relevante ontwikkelingen en krachten die op het beleid inwerken. Voor deze reconstructie zijn de data verzameld door (a) een literatuurscan naar voor het TTP-beleid relevante juridisch-beleidsmatige, technologische en maatschappelijke ontwikkelingen, (b) analyse van beleidsdossiers, (c) secundaire analyse van reeds verricht onderzoek naar (de uitvoering van) het TTP-beleid, (d) informantinterviews met beleidsmakers, marktpartijen en deskundigen.

   HET EVALUATIEONDERZOEK

   - Reconstructie oorspronkelijke beleidstheorie
   - Reconstructie responsiviteit en strategische keuzen
   - Analyse effectiviteit en efficiëntie
   - Verkenning toekomst
3. Analyse (op basis van beide reconstructies) van de effectiviteit en de efficiëntie van het beleid en de manier waarop beleidsmakers met de dilemma's in het beleid zijn omgegaan. Deze analyse vindt plaats op basis van de reconstructies onder (1) en (2). Bij effectiviteit gaat het om doelrealisatie (feitelijk resultaat), kwaliteit van de beleidstheorie en responsiviteit van de uitvoering; bij efficiëntie om de relatie tussen het doel en de ingezette middelen. Omdat het grootste deel van de voor het bepalen van de efficiëntie noodzakelijke gegevens in het onderzoek niet konden worden bemachtigd, is de analyse van de efficiëntie beperkt gehouden.
4. Verkenning van de huidige situatie, relevante ontwikkelingen, de behoefte aan TTP-dienstverlening en verwachtingen ten aanzien van de rol van de overheid en het overheidsbeleid. Naast de ideeën, vraagstukken en perspectieven voor de toekomst van het TTP-beleid die we in de literatuur, documenten en interviews verzamelen, is in het kader van het evaluatieonderzoek een zogenaamde toekomstworkshop georganiseerd met marktpartijen, deskundigen en beleidsmakers.

Overzichten van de gebruikte documenten en literatuur, alsmede van gesprekspartners voor het evaluatieonderzoek (interviews, expertmeeting en toekomstworkshop) zijn opgenomen in de bijlage bij dit rapport. Zowel voor de interviews als voor de expertmeeting en de toekomstworkshop zijn intensieve pogingen ondernomen om marktpartijen te betrekken, zowel (potentiële) gebruikers van TTP-dienstverlening en (potentiële) aanbieders van TTP-dienstverlening. Het is maar ten dele gelukt hen bij het evaluatieonderzoek te betrekken. De korte doorlooptijd van het onderzoek heeft daarbij mogelijk een rol gespeeld, maar opvallend is ook dat we in de markt weinig kennis van en animo voor het TTP-beleid hebben aangetroffen.

Deze constatering is vooral relevant met het oog op de toekomst van het beleid. De onderzoeksvraag met betrekking tot de toekomst van het TTP-beleid richt zich expliciet op de ideeën en behoeften van marktpartijen. Ter beantwoording van deze vraag hebben we drie handelingsperspectieven voor de toekomst onderscheiden, waarbij we aangeven welke keuze de (meerderheid van de) deelnemers aan ons onderzoek maken. Omdat dat maar een beperkt deel van 'de markt' betreft, is enige voorzichtigheid bij het waarderen van deze keuze op zijn plaats.

1.3 Leeswijzer

Dit rapport, waarin we verslag doen van het evaluatieonderzoek, is als volgt opgebouwd. In hoofdstuk 2 analyseren we de beleidstheorie die aan het oorspronkelijke TTP-beleid ten grondslag lag (doelen, instrumenten, impliciete en expliciete assumpties). De beleidstheorie plaatsen we in de toenmalige maatschappelijke, technologische en juridisch-beleidsmatige context; op basis hiervan analyseren we de congruentie tussen beleidstheorie en toenmalige beleidsrelevante omgeving. Het komt er immers niet alleen op aan vast te stellen of het beleid met de wijsheid van nu verstandig was, maar ook om te toetsen of het beleid de toets der kritiek kan doorstaan met de wijsheid van toen.

In hoofdstuk 3 beschrijven en analyseren we de responsiviteit van het TTP-beleid. Met andere woorden, hoe is ingespeeld op ontwikkelingen en veranderingen in de technologische, juridisch-beleidsmatige en maatschappelijke omgeving, inclusief de 'reactie' van het beleidsveld op het beleid? Wederom staat in de analyse een toets op congruentie tussen handelen van de overheid en (ontwikkelingen in) de beleidsrelevante omgeving centraal; bovendien geldt in deze fase dat de beleidsdoelen een extra toetsingscriterium vormen. Het gaat er in deze fase niet alleen om of effectief ingespeeld is op ontwikkelingen en veranderingen in de omgeving (al dan niet als gevolg van het beleid), maar ook of dat inspelen is gebeurd met het oog op het eerder geformuleerde beleidsdoel.

In hoofdstuk 4 vatten we de belangrijkste conclusies ten aanzien van de effectiviteit nog eens samen. Daartoe beschrijven we in dat hoofdstuk eerst de feitelijke resultaten van het TTP-beleid op dit moment (juni 2004); vervolgens analyseren we de effectiviteit en de efficiëntie.

Hoofdstuk 5 bevat aanknopingspunten voor de toekomst van het TTP-beleid. Deze hebben we in drie handelingsperspectieven of scenario's samengevat, waarbinnen overigens tal van combinaties mogelijk zijn.

Een overzicht van de conclusies is opgenomen in hoofdstuk 6.

2. Het TTP-beleid 'technisch probleem, dus technische oplossing'

2.1 Inleiding

In dit hoofdstuk analyseren we het TTP-beleid ten tijde van de aanbieding van het beleid aan de Tweede Kamer in 1999. Verschillende overwegingen liggen aan de keuze voor dit moment als startpunt voor de evaluatie ten grondslag. Vanaf de eerste gedachten over TTP (halverwege de jaren negentig) vindt met het aanbieden van het nationaal TTP-project aan de Tweede Kamer formeel politiek-bestuurlijke besluitvorming plaats op basis van een uitgekristalliseerd idee. Daarnaast bekrachtigt het project in zekere zin de (definitieve) keuze voor TTP als middel om tot betrouwbare elektronische communicatie te komen. Ten derde is er op dat moment sprake van een beleidstheorie, waarin een helder doel is omschreven en het instrumentarium is uitgewerkt om dat doel te realiseren.

Centraal in dit hoofdstuk staan de maatschappelijke, technologische en juridisch-beleidsmatige omgeving van het TTP-beleid (2.2) en het beleidsproces dat uitmondde in het Nationaal TTP-project (2.3). Ook analyseren we de beleidstheorie (probleemdefinitie, doel, instrumenten en assumpties) die aan het TTP-beleid ten grondslag ligt (2.4). We sluiten het hoofdstuk af met een evaluatief oordeel daarover (2.5)

2.2 De maatschappelijke, technologische en juridisch-beleidsmatige context

2.2.1 Het maatschappelijk decor

De nieuwe economie
In 1993 vindt de lancering van Mosaic plaats, de eerste browser voor het World Wide Web. Hiermee werd het mogelijk om zonder ingewikkelde commando's en diepgaande kennis van programmeertalen het internet te gebruiken. Toen in 1995 Bill Gates in een rede aangaf dat Microsoft het internet zou 'accepteren en uitbreiden' en kwam met een eigen browser, leidde dat tot een explosieve groei van het aantal mensen dat toegang kreeg tot het internet (zie Berners-Lee, 2000: 112).

> Ter illustratie: voor Nederland geldt bijvoorbeeld dat in de periode juni 1997 tot en met december 1998 het aantal huishoudens met een internetaansluiting verdubbelde van 8% naar 16%. Uitgedrukt in absolute aantallen hadden eind 1998 ruim 1.000.000 huishoudens een Internetaansluiting. In 1999 was dit aantal gegroeid tot 1,2 miljoen huishoudens (Kabinet, 1999: 40). Voor bedrijven gold op dat moment dat van de 75.000 bedrijven met meer dan vijf werknemers ruim 75% beschikte over tenminste één PC. Bij deze bedrijven groeide het gebruik van het internet aan het eind van de jaren negentig hard. Eind 1999 maakte 50% gebruik van het Internet (tegen 33% in 1997). Bovendien boden eind 1999 bijna 22.000 bedrijven hun producten of diensten aan via het Internet, een toename van 70% ten opzichte van 1997 (Kabinet, 1999).

De tweede helft van de jaren negentig is door deze revolutionaire ontwikkeling een tijd van techno-optimisme. Er zijn hooggespannen verwachtingen over wat er allemaal mogelijk zou zijn met ICT en het Internet. Terugkijkend op de periode 1998-2000 spreken Pieper, Kouwenhoven en Hamminga (2002) van 'extreme euphoria and collective madness' die het hoogtepunt bereikte in maart 2000. Een eerste regel uit het boek *Business @ the speed of thought* van Bill Gates drukt deze verwachtingen goed uit. Hij stelt:

> 'Business is going to change more in the next ten years than it has in the last fifty' (Gates, 1999: xvii).

Min of meer hetzelfde werd toen geconcludeerd door wetenschappers, adviseurs, beleidsmakers en bestuurders over het functioneren van de overheid. Exemplarisch voor het denken over de betekenis van nieuwe technologie in die jaren zijn de denkbeelden van goeroes als Kevin Kelly (1999). Hij sprak van een 'nieuwe economie' met permanente groei, die in het leven wordt geroepen door steeds kleiner wordende computers en zich steeds uitbreidende onderlinge netwerken ('zwermen'). Deze nieuwe economie is mondiaal, is immateriële zaken gunstig gezind en in sterke mate onderling verbonden. De nieuwe economie vormt een ware 'aardverschuiving' in onze wereld, aldus Kelly (1999: 1 en 2). Nieuwe regels in de zin van nieuwe essentiële dynamische mechanismen die als fundamentele principes verankerd zijn in het territorium van de nieuwe economie zijn volgens hem van toepassing op alle bedrijven en bedrijfstakken. Een van de aanleidingen hiervoor is dat door technologische ontwikkelingen communicatie niet langer een van de sectoren van de economie vormt. Communicatie is de economie, aldus Kelly (1999: 6).

HET MAATSCHAPPELIJK DECOR

- Exponentiële groei internetgebruik
- Nieuwe economie

Internetgebruik en -handel

In deze tijd wordt het internet steeds belangrijker als platform voor communicatie. In 1998 heeft Nederland, in vergelijking met andere landen, een redelijk kwaliteitsniveau voor wat betreft de infrastructuren voor internettoegang en -backbone. Nederland heeft, na de VS en Zweden, op dat moment de hoogste penetratie van internet-hosts (computers zichtbaar op het Internet). Ook scoort Nederland goed met het aantal particuliere internetaansluitingen. Onderzoek toont in die periode aan dat Nederland de hoogste internetpenetratie in Europa kent (Kabinet, 1998). Tegelijkertijd is de markt voor elektronische diensten in Nederland dan nog erg klein. De bestedingen per capita aan elektronische diensten zijn in 1997 lager dan die van Duitsland, het Verenigd Koninkrijk, Zweden, Frankrijk en de VS. Daar staat echter tegenover dat de groei van deze markt in Nederland wel bijna het hoogst is. Het kabinet trekt hieruit de conclusie dat Nederland dus nog aan het begin van de ontwikkeling van deze markt staat (Kabinet, 1998).

Als belangrijkste voorwaarde voor het 'uit de startblokken' komen van de elektronische dienstverlening in Nederland ziet het kabinet het realiseren van de toegang tot netwerken voor een groot deel van de bevolking. Hoewel deze voorwaarde in Nederland beter vervuld lijkt te zijn dan in veel van de andere onderzochte landen, constateert het kabinet toch dat de ontwikkeling aan zowel vraag- als aanbodzijde in de markt achterblijft bij de mogelijkheden. (Kabinet, 1998: 11). De behoefte aan beter beveiligde transacties voor elektronische dienstverlening en handel wordt in algemene analyses en beleidsdocumenten in die tijd nauwelijks gesignaleerd. Dat een dergelijke behoefte wel bestaat, blijkt later onder andere uit

een onderzoek dat in 2001 door Ernst & Young is uitgevoerd. Als grootste rem op de groei van het succes van e-commerce wordt door ruim 40 procent van de onderzochte Nederlandse bedrijven de (on)veiligheid en (on)beheersbaarheid van de ICT aangegeven. Veertig procent ziet daarnaast het betalingsverkeer via internet als niet betrouwbaar.

De behoefte aan betrouwbare elektronische communicatie geldt vooral voor open netwerken, zoals het internet. Open verwijst naar het feit dat elke natuurlijke en/of rechtspersoon in principe toegang kan krijgen tot het desbetreffende netwerk. Daarnaast zijn in de jaren tachtig en negentig reeds gesloten netwerken tussen bedrijven en instellingen tot stand gekomen waarlangs elektronische communicatie en handel plaatsvinden. Door standaardisatie (bijvoorbeeld ten aanzien van de uitwisseling van gegevens, zoals EDI) nemen de handel en het berichtenverkeer binnen deze gesloten netwerken in de jaren negentig sterk toe. Het gaat hier vrijwel uitsluitend om 'business-to-business' contacten en dus niet om contacten tussen organisaties en consumenten/burgers.

Om de ontwikkeling van het gebruik van Internet als open netwerk te stimuleren en ervoor te zorgen dat Nederland optimaal inspeelt op de mogelijkheden die nieuwe ICT biedt, vormt dit thema sinds 1994 een apart aandachtsveld in het beleid van het kabinet.

2.2.2 Het juridisch-beleidsmatig decor

Zelfsturing en marktwerking
De kiem voor het latere TTP-beleid is te vinden in het *Nationaal Actieprogramma Elektronische Snelwegen (NAP)* uit 1994 (Kabinet, 1994). Met het NAP wil Nederland zijn positie als *Gateway to Europe* versterken door informatie te benutten als bron van hoogwaardige economische activiteit. De benadering die ten aanzien van de ontwikkeling van de elektronische snelwegen is gekozen is er een waarbij wordt verwacht dat de private sector het initiatief neemt. Deze benadering van zelforganisatie en marktwerking staat niet alleen centraal in het NAP, maar wordt ook in latere nota's betrekkelijk consistent doorgetrokken als het gaat om het beleid ten aanzien van de elektronische snelweg.

In het *Actieprogramma Elektronische Overheid* (Ministerie van BZK, 1998) wordt gesproken over een zich voltrekkende ICT-revolutie die de vier traditionele overheidsfuncties (de ordenende, sturende, presterende en verzorgende functie) in volle omvang raakt. Voor wat betreft de ordenende en de sturende rol geldt dat deze met name door regulering en stimulering wordt ingevuld. Conform de bij het NAP ingezette lijn, gaat het bij dit laatste om het idee dat marktwerking het elektronische verkeer moet bevorderen. In de nota *Boven NAP* (Kabinet, 1998) wordt wel een accentverschuiving aangegeven. Waar het in het NAP vooral ging om het *tot stand brengen* van elektronische snelwegen, gaat het er in de vervolgfase vooral om het *gebruik ervan* door burgers, bedrijven en overheden te stimuleren (Kabinet, 1998: 18).

HET JURIDISCH-BELEIDSMATIG DECOR

- Zelfsturing en marktwerking
- Betrouwbare handel en communicatie (met rechtmatige toegang)
- Standaardisatie en informatiebeveiliging

In de in 1999 verschenen nota '*Digitale Delta. Nederland Online*' (Kabinet, 1999) spreekt het kabinet de ambitie uit om Nederland tot de Europese kopgroep te laten behoren op de elektronische snelweg. In feite komt dit neer op dezelfde doelstelling als die in het NAP werd gehanteerd. Nederland dient volgens het kabinet een excellente ICT-basis te realiseren en wel langs verschillende pijlers: telecommunicatie-infrastructuur, kennis en innovatie, toegang en vaardigheid, regelgeving en de toepassing van ICT in de publieke sector. Conform het geloof in marktwerking als ontwikkelingsmechanisme hanteert het kabinet hierbij het uitgangspunt dat de overheid de randvoorwaarden op orde brengt en resterende belemmeringen, voor zover aanbieders en afnemers deze niet zelf kunnen oplossen, helpt wegnemen. Het ontwikkelen door de markt blijft dus voorop staan. Voor de overheid is geen trekkende, maar een ondersteunende rol weggelegd.

Veiligheid van de infrastructuur

Al in 1994 wordt in het NAP aandacht besteed aan de beveiliging van elektronische gegevensuitwisseling. Dit wordt dan beschouwd als een belangrijk aspect in de ontwikkeling van elektronische snelwegen. Het NAP stelt dat het in de rede ligt om bescherming van het elektronische berichtenverkeer naar analogie van het briefgeheim te realiseren. Aangegeven wordt dat in de praktijk vertrouwelijkheid meestal met behulp van cryptografie wordt bereikt. Echter, 'waar cryptografie opsporing en rechtshandhaving in gevaar brengt' dienen passende voorzieningen te worden getroffen (Kabinet, 1994: 17). Een belangrijk element bij het nadenken over beveiliging door middel van cryptografie is op dat moment het vanuit het oogpunt van handhaving en opsporing ingegeven belang van de overheid bij 'rechtmatige toegang'. In beleidsmatige stukken verdwijnt deze invalshoek later volledig ten gunste van het inzetten van cryptografie als middel om de veiligheid van transacties te waarborgen en daardoor elektronische handel te stimuleren.

Dit blijkt bijvoorbeeld in 1998, wanneer betrouwbare elektronische communicatie door het *Actieprogramma elektronische Overheid* wordt gepositioneerd als een belangrijk aandachtspunt. Een voorziening voor betrouwbare communicatie wordt dan als noodzakelijk beschouwd voor de ontwikkeling van de elektronische overheid. Cryptografie wordt als zodanig niet meer aan de orde gesteld, maar is ondergebracht in het TTP-concept. Het doel van TTP is niet alleen beveiliging van informatiestromen, maar ook het verlenen van ondersteunende diensten, zoals het aantonen van verzending en ontvangst, het plaatsen en verifiëren van digitale handtekeningen, het verstrekken van digitale certificaten en sleutelbeheer. Het belang van de overheid met betrekking tot opsporing en handhaving wordt niet expliciet meer genoemd.

De koers gericht op ontwikkeling van TTP wordt doorgetrokken in de nota's *Boven NAP* en *Digitale Delta*. In *Digitale Delta* worden TTP genoemd als de partijen die een intermediaire rol kunnen vervullen bij het garanderen van de juridische betrouwbaarheid van het elektronische berichtenverkeer. Dit is nodig, zo wordt gesteld, omdat het voor het tot ontwikkeling komen van elektronisch zakendoen van groot belang is dat het vertrouwen in elektronische handelingen sterk wordt vergroot. Deze nota geeft tevens aan dat het bedrijfsleven – in samenwerking met de overheid – reeds is gestart met het vormgeven van de implementatie van een (nationale) TTP-infrastructuur om tegemoet te komen aan de behoefte daaromtrent in de markt. De keuze voor openbare TTP-dienstverlening wordt hiermee bevestigd.

In vergelijking met eerdere nota's is er met het verschijnen van de nota *Digitale Delta* wel een verschil waar te nemen voor wat betreft de omschrijving van de TTP. Waar het in het

Actieprogramma Elektronische Overheid ging om de beveiliging van informatiestromen en het verlenen van ondersteunende diensten, lijkt het TTP-concept in de nota *Digitale Delta* vooral in het teken te staan van het garanderen van juridische betrouwbaarheid. De eerdere brede insteek van het concept inclusief diverse andere ondersteunende diensten was niet primair gericht op juridische verankering, maar het ondersteunen van vertrouwen in TTP-dienstverleners door een keurmerk.

Standaardisatie
Passend bij het streven om via marktwerking het elektronische zakendoen te stimuleren is het toepassen van het instrument van standaardisatie dat ook ten aanzien van beveiligingskwesties naar voren wordt geschoven. In de nota *Digitale Delta* bijvoorbeeld wordt het stimuleren en ontwikkelen van standaarden gezien als een mogelijke manier om de kwetsbaarheid van de infrastructuur te verminderen. Standaardisatie leidt, zo stelt de nota, tot kostenverlaging, het bevorderen van concurrentie en daarmee dus ook ruimere keuzemogelijkheden voor consumenten. Bij de ontwikkeling van standaarden heeft de industrie een belangrijke rol (denk bijvoorbeeld aan het toenmalige EDIFORUM) en soms speelt de overheid een bemiddelende rol (bijvoorbeeld ten aanzien van ETSI).

Het juridisch kader rondom het TTP-beleid anno 1999
In 1999 bestond er geen specifiek juridisch kader voor TTP of gerelateerde onderwerpen als technieken voor elektronische authenticatie.[2] Dat betekende dat (de betrouwbaarheid van) elektronische communicatie viel onder de algemene regels van het burgerlijk recht en bestuursrecht en de juridische status (en met name bewijskracht) van elektronische documenten en elektronische handtekeningen uitsluitend aan de hand daarvan beoordeeld kon worden. Begin 1998 wordt in de nota *Wetgeving voor de Elektronische Snelweg* (WES) in het kader van de juridische betrouwbaarheid van het elektronische rechtsverkeer opgemerkt dat de algemene infrastructuur van het burgerlijk recht in principe toereikend is, maar dat voor de communicatie tussen overheid en burger nadere eisen noodzakelijk zijn. Tegelijkertijd onderstreept de nota WES het belang van TTP voor de betrouwbaarheid van het gehele elektronisch maatschappelijk verkeer en ofschoon in de eerste plaats regulering door de markt zelf (voor minimumeisen voldoet de Telecommunicatiewet) wordt voorgestaan, zou er toch een juridisch kader voor TTP dienen te komen met het oog op ondersteuning van het materiële recht en het bewijsrecht.[3]

In hetzelfde jaar merkt de Commissie Huls in het kader van het MDW-project 'elektronisch verrichten van rechtshandelingen' op dat de wetgever 'niet achter de techniek aan (moet hollen), maar een aantal principes (dient te formuleren) voor een betrouwbaar elektronisch rechtsverkeer. In dit proces is een belangrijke rol weggelegd voor TTP. In een volgende fase kunnen vervolgens de door de maatschappelijke realiteit gewenste uitgangspunten in wetgeving worden neergelegd. Daarbij dient aangesloten te worden bij internationale ontwikkelingen.'[4] De thematiek van de oprichting van en randvoorwaarden voor TTP zal vervolgens verder in de vorm van co-regulering door overheid en bedrijfsleven (in het publiek-private samenwerkingsproject TTP.NL) worden uitgewerkt in het kader van het in de Nota WES reeds aangekondigde Nationale TTP-project.[5]

---

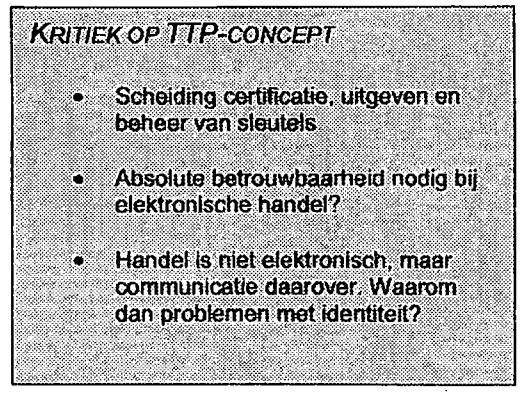
[2] Wel werd in een enkel geval – bijvoorbeeld artikel 2:10 BW – reeds gerefereerd aan de toepassing van andere dan papieren gegevensdragers.
[3] *Kamerstukken II* 1997/98, 25 880, nr. 2.
[4] Beschikbaar op: <www.ez.nl/publicaties/pdfs/MDW012.pdf>. Zie ook *Kamerstukken II* 1997/98, 24 036, nr. 84.
[5] *Kamerstukken II* 1998/99, 26 581, nr. 1.

Overigens woedt er op dat moment internationaal een discussie over het al dan niet toestaan van cryptografie. In sommige landen is het gebruik van cryptografie zelfs verboden, maar in Nederland heeft een voorstel daartoe enkele jaren eerder onvoldoende steun gekregen en is daardoor afgeketst. In de discussie staat het belang van opsporing en handhaving ('rechtmatige toegang') tegenover het belang van de bescherming van de persoonlijke levenssfeer (of een '(grond)recht op vertrouwelijke communicatie') geplaatst. Deze discussie, die Koops beschrijft als 'cryptocontroverse', raakt het TTP-beleid omdat in dat beleid het brede concept van TTP-dienstverlening ook diensten voor vertrouwelijkheid omvat en de PKI-technologie gebaseerd is op cryptografie (zie voor de beschrijving van de controverse Koops, 1999).

TTP niet onomstreden

Overigens zijn het TTP-concept en de juridisch-beleidsmatige uitwerking daarvan niet onomstreden. Zo worden naar aanleiding van het preadvies *De notaris en het elektronisch rechtsverkeer* kritische kanttekeningen geplaatst bij het beheer van de private sleutel door notarissen. Waarom, zo vraagt Koops zich in het tijdschrift Computerrecht af (Koops, 1997), is het eigenlijk nodig en zinvol dat private sleutels door de notaris worden beheerd als gebruikers dat ook zelf kunnen (of zelf maatregelen treffen voor eventueel verlies). Hij bepleit een scheiding van de certificatie van sleutels, het uitgeven van sleutels en het beheer van sleutels, activiteiten die de preadviseurs van de Koninklijk Notarieel Beroepsorganisatie Franken en Lekkerkerker in elkaars verlengde zien (zie Franken e.a., 1996).

In hetzelfde tijdschrift verschijnt een jaar later een speciaal dossier over Trusted Third Parties, waaraan de Nederlandse Vereniging voor Informatietechnologie en Recht haar najaarsvergadering van 1998 heeft gewijd. Koops, Van Kralingen en Van der Wees erkennen in hun artikel in dat dossier dat betrouwbaarheid een belangrijke voorwaarde is voor het ontstaan van vertrouwen en dat betrouwbaarheid in een elektronische omgeving wordt bereikt door het toepassen van beveiligingsmethoden. Wel beschouwen zij het als een misverstand dat in elektronische omgevingen een niveau van 'absolute betrouwbaarheid' nodig zou zijn, een niveau dat zij kennelijk impliciet met TTP associëren. TTP is volgens hen vooral een uitkomst in een omgeving waarin veel gestandaardiseerd berichtenverkeer plaatsvindt waarbij grote belangen spelen. In de meeste situaties vormen TTP-diensten een 'tamelijk zware' oplossing (...), die in veel gevallen kan worden aangemerkt als 'overkill' (Koops, Van Kralingen en Van der Wees, 1998: 208).



In hetzelfde dossier stelt Pieter Kleve zich, getuige de titel van zijn artikel ('Zijn TTP's nuttig?'), ook af wat het nut van TTP is. Hij formuleert zijn vraag scherp:

> 'De handel is niet elektronisch, maar de communicatie daarover. 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?' (Kleve, 1998: 211)

Zijn conclusie is dat het nut of de toegevoegde waarde van een TTP 'niet evident' is:

> '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 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.' (Kleve, 1998: 213)

2.2.3 Het technologisch decor

Informatiebeveiliging als focus

Om een beeld te krijgen van de stand van de technologie in de tweede helft van de jaren negentig kunnen we enkele voorbeelden van uitspraken als illustratie gebruiken die direct of indirect raken aan betrouwbare elektronische communicatie. Ze zijn ontleend aan een bundel die aansluit op de tijdgeest van dat moment (Van der Vlist en Noordam, 1997).

> Het gebruik van e-mail wordt in 1997 niet als een trend gezien, maar als gevestigde technologie. Wel wordt e-mail vanaf dat jaar steeds vaker gecombineerd met andere functionaliteiten, zoals het elektronische equivalent van aangetekende post (elektronische handtekening en bevestiging van ontvangst).
>
> De smartcard staat volop in de aandacht (bij met name financiële instellingen). Het probleem dat verdere uitbreiding in de weg staat is een gebrek aan standaardisatie. Het ideaal is een pas voor alle toepassingen. De chipkaart is 'proven technology' geworden, maar de investeringen voor een chipkaart zijn enorm hoog. Toepassingen lonen alleen als grote consortia worden gevormd die gezamenlijk de kosten dragen en gezamenlijk zorgen voor een grootschalig gebruik van de kaart.
>
> Internet expandeert snel en lijkt tegen de grenzen van zijn mogelijkheden aan te lopen. Daaraan debet zijn de snelle toename van het aantal gebruikers en het daarbij achterblijvende tempo van infrastructurele voorzieningen. Er is veel aandacht voor mogelijkheden om diensten via het internet commercieel exploiteerbaar te maken. Zo worden betalingssystemen ontwikkeld voor de afname van internetdiensten en wordt veel onderzoek gedaan naar de beveiliging van via het internet getransporteerde informatie. Tevens bestaat er behoefte aan gegarandeerde bandbreedte op het internet.

De verwachting die Van der Vlist en Noordam in 1997 uitspreken is dat voor de beveiliging van over het internet verstuurde informatie een bevredigende regeling wordt gevonden (Van der Vlist en Noordam, 1997: 69). In 2001 blijkt uit een onderzoek van Ernst & Young onder Nederlandse bedrijven dat deze verwachting niet is uitgekomen. In het onderzoek wordt aandacht besteed aan factoren die het vertrouwen in internet kunnen vergroten. Bovenaan de lijst staat meer aandacht van organisaties voor ICT-beveiliging in het algemeen en in het bijzonder veilige methoden voor betalen via het internet. Als derde factor wordt de verbetering van authenticatiemechanismen genoemd, gevolgd door het treffen van juridische maatregelen. Zeventig procent van de bedrijven geeft in 2001 aan bezig te zijn met het zoeken

naar oplossingen voor deze vraagstukken. De onderzoekers vragen zich overigens af of het onveilige imago van internet wellicht niet slechts een communicatieprobleem is (Ernst & Young, 2001: 19).

Als antwoord op de vragen die rijzen rondom beveiliging en authenticatie wordt in de jaren negentig het TTP-concept ontwikkeld. In een onderzoek uit 1999 naar de bruikbaarheid van dit concept voor de rijksoverheid wordt de conclusie getrokken dat TTP-diensten een elegante oplossing bieden voor het bewijzen van de identiteit van personen. Het brede scala aan gebruiksmogelijkheden maakt TTP-diensten, volgens Hardam (1999), aantrekkelijk in vergelijking met diverse andere op dat moment beschikbare technieken voor het bewijzen van identiteit (zoals wachtwoordsystemen, pincodes, kerberos authenticatie, PGP voor beveiligde e-mail en gesloten gebruikersgroepen) (Hardam 1999: 12). Ook blijken TTP-diensten zowel in open als in gesloten netwerken toepasbaar. In 1999 zijn dit soort diensten te vinden in min of meer gesloten vertrouwensdomeinen als dealernetwerken, bij Internet Service Providers (SURFnet), multinationals (Shell), banken en zelfs overheden (Canada en Australië). Daarnaast zijn publieke TTP-diensten ontstaan die voor elke burger en rechtspersoon toegankelijk zijn. Voorbeelden op dat moment zijn PTT Post met Keymail, een elektronische variant van de aangetekende post, KPN Telecom en Roccade die samen de diensten van het Amerikaanse VeriSign in Nederland willen leveren en Enschedé/SDU dat TTP-diensten wil aanbieden in combinatie met chipkaarten (Hardam, 1999).

2.2.4 Het decor samengevat

De belangrijkste elementen van het geschetste decor waarin het TTP-beleid is ontstaan, kunnen als volgt worden samengevat:

- Er bestaan grootse verwachtingen van de mogelijkheden van elektronische handel. Indicaties voor onveilige communicatie en onveilig betalingsverkeer als een belemmering daarvoor zijn er ook, hoewel sommigen daar vragen bij stellen.
- Het dominante beleidsparadigma wordt vooral gekenmerkt door marktwerking en deregulering. Regulering komt in die tijd vooral neer op standaardiseren en (licht) stimuleren.
- Er is geen directe juridische noodzaak voor TTP-beleid of -regelgeving; er is wel een Europese richtlijn ten aanzien van de elektronische handtekening in het vooruitzicht. Ook wordt gediscussieerd over het al dan niet toestaan van het gebruik van cryptografie.
- Er is ervaring met TTP-diensten in besloten netwerken; ook verschijnen de eerste ondernemers die marktkansen zien in het concept van open TTP-diensten.

2.3 Het beleidsproces

Ontstaan van een behoefte

Het Nederlandse TTP-beleid is ergens in het midden van de jaren negentig geboren. Met gegevensuitwisseling langs elektronische weg was op dat moment door grote organisaties al jaren ervaring opgedaan. Denk bijvoorbeeld aan EDIFACT, een standaard voor 'Electronic Data Interchange (EDI)'. In het platform EDIFORUM werken verschillende partijen (voornamelijk uit de logistieke distributieketens) samen aan verbetering en invulling van standaarden voor elektronische gegevensuitwisseling. Digitale handtekeningen en

versleuteling als technieken om veilige communicatie te waarborgen worden in dit verband ook besproken. Bij besloten netwerken voor elektronische communicatie tussen overwegend duurzame handels- en distributierelaties spelen deze onderwerpen nog geen belangrijke rol. Dat wordt anders als de verbreding naar de consumentenmarkt gaat spelen en authenticatie en vertrouwelijkheid nieuwe vragen oproepen.

In de jaren 1993-1997 wordt in Europees verband het InfoSec ('Information Security') onderzoeksprogramma uitgevoerd. Een van de lijnen in dit programma is het gebruik van encryptie voor het beveiligen van elektronische gegevensuitwisseling, waarover op dat moment verschillend wordt gedacht. Enerzijds bestond ook toen reeds de behoefte om de elektronische handel te stimuleren door het bieden van oplossingen voor beveiliging en authenticatie; anderzijds bestond er (met name bij sommige EU-lidstaten) de behoefte om de weg vrij te houden voor 'rechtmatige toegang' in het kader van strafrechtelijke opsporing en nationale veiligheid. Het gebruik van encryptie was op dat moment een omstreden onderwerp, iets dat doorwerkte in het in het kader van het InfoSec programma uitgevoerde onderzoek naar het TTP-concept. Het TTP-concept bood bedrijven technisch gezien de beveiliging waar men behoefte aan had; tevens kon het voorzien in de behoefte van de overheid om zich – als dat noodzakelijk werd geacht – toegang te verschaffen tot de inhoud van de communicatie.

De keuze voor het TTP-concept

Nog los van de onzekerheid over de ontwikkeling van de elektronische handel, kwam het TTP-concept (waarbij van PKI-technologie gebruik wordt gemaakt) op dat moment aan meerdere eisen, behoeften en zorgen tegemoet:

DE STERREN STAAN GOED VOOR TTP

- Technisch betrouwbare oplossing
- Open concept: diensten, beveiligingsniveaus en handelspartners
- Betrouwbare communicatie, en toch rechtmatige toegang mogelijk

- Het TTP-concept werd gezien als een open concept dat zich voor tal van applicaties zou lenen en uiteenlopende beveiligingsniveaus zou toelaten. Tegelijkertijd werd het als veilig beschouwd en voor authenticatie geschikt geacht.
- Het TTP-concept bood een oplossing voor elektronische handel tussen contractpartners die onbekend met elkaar zijn en maakte in dit opzicht open handel mogelijk. Op dat moment was vertrouwen nog vooral aanwezig in bilaterale relaties en 'rings of trust'.
- Bij het ontwikkelen van TTP-beleid worden in principe weinig opties afgesloten. Ook in deze zin is het een open concept. Het kan gebruikt worden voor elektronische en digitale handtekeningen, voor vertrouwensdiensten als 'time-stamping' enzovoort. Het afbreukrisico ervan is derhalve beperkt.
- Voor het probleem van de onbetrouwbare elektronische communicatie was het TTP-concept een geschikte oplossing. In technisch opzicht werd met TTP-dienstverlening de elektronische communicatie (over het internet) veilig.
- Het hanteren van een (hoog) niveau van beveiliging is aantrekkelijk omdat zo overzichtelijkheid wordt geboden. Verschillende niveaus van beveiliging zouden de complexiteit vergroten; verondersteld werd dat dit een drempel voor het gebruik zou opwerpen.

- De technische alternatieven voor PKI (als technische basis voor het TTP-concept) waren halverwege de jaren negentig beperkt en boden niet het scala aan gebruiksmogelijkheden dat PKI bood.
- Het vooruitzicht bestond dat de elektronische identiteitskaart (eNIK) in Nederland zou worden ingevoerd. Op dat moment zou dus een massaal uitgifteproces plaatsvinden aan alle Nederlanders.
- Als gevolg van het uitgevoerde InfoSec onderzoeksprogramma was veel kennis over PKI beschikbaar en was het vertrouwen erin hoog.
- Praktisch was het TTP-concept ook handig omdat het de mogelijkheid bood om de elektronische handel te stimuleren door het realiseren van betrouwbare elektronische communicatie, terwijl het tegelijkertijd tegemoet kon komen aan de behoefte aan rechtmatige toegang. Aan uiteenlopende departementale wensen kon dus tegemoet worden gekomen met het TTP-concept.
- Het TTP-concept is naar aard een hiërarchisch concept voor het regelen van vertrouwen wat aansluit bij de wijze waarop vertrouwen vaak in de fysieke wereld wordt georganiseerd (via bijvoorbeeld een notaris). Een alternatief zoals PGP, wat niet hiërarchisch is maar veel meer een netwerk van vertrouwen, staat daar verder vanaf.

Nogal wat signalen wezen halverwege de jaren negentig dus in de richting van TTP-dienstverlening als oplossing voor onveilige of onbetrouwbare elektronische communicatie. Daarbij kwam dat er op dat moment reeds enkele openbare TTP-diensten in Nederland actief waren, waaronder die van het toenmalige – vlak daarvoor verzelfstandigde – PTT Post (nu TPG). Deze onderneming had een digitale variant had ontwikkeld voor aangetekende stukken, het zogenaamde Keymail. In dit kader werden ook aanvullende diensten verwacht, zoals 'time-stamping'. Om het vertrouwen van consumenten in deze dienst te versterken, werd een door de overheid gestimuleerd of ontwikkeld certificatiesysteem of keurmerk wenselijk geacht.

Behalve TPG waren op dat moment ook andere partijen geïnteresseerd in het TTP-concept, dat zich kennelijk eenvoudig naar verschillende posities en 'metaforen' liet vertalen:

- Het notariaat was in TTP geïnteresseerd, omdat notarissen in de fysieke wereld reeds een rol spelen als 'trusted third party'. Het lag dan vanuit deze positie ook voor de hand om in de virtuele wereld dezelfde rol op zich te nemen.
- Voor banken die het toenemende elektronische betalingsverkeer voor hun rekening namen, was TTP-dienstverlening ook interessant. Zij hebben een financiële vertrouwenspositie en spelen als intermediair in het betalingsverkeer een rol.
- TTP is een methode voor authenticatie en (in combinatie met specifieke technieken) ook voor identificatie. Voor bedrijven die zich hiermee reeds bezig hielden (bijvoorbeeld Eschedé/SDU) is TTP dus ook een interessant concept.
- Voor ICT-dienstverleners (bijvoorbeeld RCC/PinkRoccade, maar ook telecomproviders) is het TTP-concept interessant als nieuwe 'productlijn', omdat het direct aansluit op bestaande activiteiten. ICT-dienstverleners zouden de hard- en software kunnen ontwikkelen, telecomproviders beschikten reeds over infrastructuur.

De focus op marktwerking en randvoorwaarden

Niet alleen in het algemeen is er ten tijde van de totstandkoming van het TTP-beleid een sterke voorkeur voor marktwerking, dat geldt ook voor het TTP-beleid als afzonderlijk terrein. Vanaf de start van het TTP-beleid stonden marktregulering, deregulering en stimulering van de economie voorop bij de beleidsmakers. De ministeries van V&W en EZ

stelden zich op het standpunt dat er geen financiële stimulering van TTP-diensten zou moeten plaatsvinden, anders dan een bijdrage in de ontwikkeling van het beleid en een subsidie in de eerste jaren van de toezichtkosten (die in verband met het omslagprincipe bij toezicht door de OPTA voor de eerste aanbieders anders onevenredig hoog werd geacht). TTP-diensten zijn vanaf de geboorte van het TTP-beleid beschouwd als een verantwoordelijkheid van de markt. Het beleid zou zich moeten richten op het realiseren van de randvoorwaarden.

De businesscase voor TTP: verbreding van het concept
In het prille begin leek het TTP-concept vooral een antwoord op de behoefte aan authenticatie bij elektronische gegevensuitwisseling. Voor dat doel is het TTP-concept (in een PKI-omgeving) een gedegen, maar complexe en in vergelijking met eenvoudiger beveiligingstechnieken tevens dure oplossing. Met de enkele toepassing van het TTP-concept voor authenticatiedoeleinden ter stimulering van elektronische handel was de 'overall business case' moeilijk te onderbouwen. In deze richting wijzen bijvoorbeeld signalen van marktpartijen die op dat moment TTP-diensten aanbieden en daarmee niet direct marktsucces boeken. Daarom zijn al snel de andere mogelijke diensten die het TTP-concept in principe biedt meegenomen in de keuze voor TTP. Met TTP-diensten worden aanvullende diensten als time-stamping en het versturen van verzend- en ontvangstberichten mogelijk, maar ook een hoge mate van vertrouwelijkheid van het berichtenverkeer. Voor dit bredere concept is de 'businesscase' vooral voor processen met omvangrijke documentstromen makkelijker rond te krijgen. Een breed concept maakt het voor marktpartijen dan ook aantrekkelijker zich op de markt voor TTP-dienstverlening te begeven.

Hoewel het dus moeilijk bleek om op macro niveau de 'overall business case' sluitend te krijgen, laat dit onverlet dat op onderdelen van het TTP-beleid wel degelijk 'business cases' opgesteld konden worden. De 'overall business case' was in het begin ook minder relevant, omdat alle betrokken partijen samen bij de ontwikkeling betrokken waren. Wel is het zo dat een economische invalshoek rond het denken over TTP-diensten lange tijd beperkt is ingevuld, namelijk met een Consultatiegroep Aanbieders en Gebruikers. Deze bestond uit vertegenwoordigers van departementen, koepelorganisaties (Consumentenbond, Nederlandse Vereniging van Banken, Vereniging van KvK en Fabrieken, VNO/NCW) en potentiële aanbieders en gebruikers van TTP-dienstverlening (Academisch Ziekenhuis Leiden, Enschedé/SDU, PTT post B.V., Rabobank Nederland, RCC, Shell, KEMA, enzovoort). De mogelijkheid van gericht en grootschalig marktonderzoek werd door de beleidsmakers op dat moment niet reëel geacht. De betrokken partijen richtten zich dan ook vooral op het formuleren van eisen en randvoorwaarden voor TTP-diensten. In dit opzicht, zo concludeert ook Van Rij (2002), was het TTP-beleid aanvankelijk het domein van juristen en technici, aangevuld met kennis op het terrein van auditing en PKI.

Meest waarschijnlijke aanleidingen voor de ontwikkeling van het beleid
De combinatie van hiervoor genoemde factoren heeft tot het TTP-beleid geleid. Om zicht te krijgen op een weging van deze factoren is tijdens een (in het kader van deze evaluatie gehouden) expertmeeting aan betrokkenen en experts gevraagd wat zij de meest waarschijnlijke verklaringen voor het beleid beschouwen. Zij noemden:

- Het toenemende aantal transacties dat zich in open netwerken (waarin het gaat om *many-to-many contacten*) voltrok ten opzichte van gesloten netwerken (bijvoorbeeld logistieke EDI-ketens) en hiermee samenhangend het veranderende karakter van internet als zodanig. Van vrijplaats binnen de overheersend

wetenschappelijke context werd het in de jaren negentig tot marktplaats voor e-business.
- Het geloof in marktwerking en deregulering als regulerende principes en in het verlengde hiervan de behoefte die de markt aangaf te hebben aan een keurmerk voor beveiliging van transacties.
- Het feit dat het TTP-concept lijkt op de wijze waarop zaken in de fysieke wereld zijn geregeld (alles wat offline kan moet ook online kunnen). Met name gold dit voor de robuuste hiërarchische insteek van beveiliging binnen het concept, de toekomstvaste technologie, de mogelijke grip die de overheid in principe zou kunnen houden op cryptografie (vanuit haar taak van het handhaven van openbare orde en veiligheid) en de belangen van marktpartijen.
- De heersende angst voor de virtuele wereld en het hiermee samenhangende geloof dat er een middel beschikbaar moest komen om vertrouwen in elektronische handel te creëren en te stimuleren. Hierbij gold een soort 'preoccupatie' met identiteit. Hoewel marktwerking het adagium was, werd het opbouwen van vertrouwen als een overheidstaak gezien;
- Het beleid sloot goed aan bij Europese ontwikkelingen en de ontwikkelingen rond het thema in andere landen, zoals de VS en Duitsland.

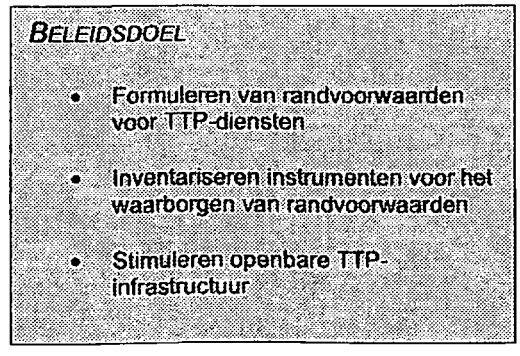
2.4 Reconstructie van de beleidstheorie

Startpunt voor evaluatie

Hoewel het besluit om het Nationaal TTP-project in het kader van het Nationaal Actieprogramma Elektronische Snelwegen te financieren (april 1997) als de formele start van het TTP-beleid kan worden gezien, is de presentatie van de resultaten van dat project aan de Tweede Kamer der Staten-Generaal (bij brief van 3 juni 1999) een geschikt startpunt voor evaluatie van het TTP-beleid. Daarom nemen we de beleidsnotitie waarin de resultaten worden gepresenteerd als uitgangspunt voor het ontrafelen van de theorie achter dat beleid. Overigens is de beleidstheorie niet uitsluitend een vrucht van beleidsmakers aan overheidszijde. In de context van het TTP-beleid is deze veeleer te beschouwen als een gedeeld beeld bij de betrokkenen bij het beleid. Over deze beleidstheorie bestond overeenstemming tussen beleidsmakers (nationaal bij de ministeries van Verkeer en Waterstaat, Economische Zaken, Binnenlandse Zaken en Justitie, internationaal vooral in Europees verband), koepelorganisaties (als de Nederlandse Vereniging van Banken, VNO/NCW), grote bedrijven en standaardisatie-organisaties als EDIFORUM (nu ECP.nl).

Beleidsdoelstellingen

De primaire invalshoek van het Nationaal TTP-project is de elektronische handel en het stimuleren daarvan. Hoewel de beleidsnotitie het belang van TTP voor elektronische communicatie aanvankelijk in algemene zin formuleert ('Vertrouwen en veiligheid bij het opslaan van gegevens en het uitwisselen van berichten worden (...) steeds belangrijker'), richt de aandacht zich direct daarna vooral op de 'kwaliteit van dienstverlening in het elektronisch handelsverkeer'. Het gaat er met andere woorden om de omstandigheden te



realiseren waaronder elektronische handel tot bloei kan komen, en niet om het stimuleren van 'vertrouwelijke communicatie' in algemene zin.

Deze abstracte doelstelling is in de beleidsnotitie wel als achtergronddoel verwoordt, maar het beleid en meer in het bijzonder het Nationaal TTP-project richt zich op concrete doelen. Deze zijn als volgt onder woorden gebracht:

1. Het formuleren van randvoorwaarden voor het aanbieden en gebruiken van TTP-diensten;
2. Het inventariseren van instrumenten waarmee deze randvoorwaarden gewaarborgd kunnen worden;
3. Het stimuleren van de ontwikkeling van een openbare Nederlandse TTP-infrastructuur.

De beleidsnotitie bevat geen uitgebreide en transparante beschrijving van de weg die is gevolgd om tot deze doelstellingen te komen, met andere woorden hoe het hoofddoel ('betrouwbare elektronische communicatie') zich laat vertalen in het 'formuleren van randvoorwaarden voor het aanbieden en gebruiken van TTP-diensten'. De logische ruimte hiertussen laat zich evenmin makkelijk reconstrueren en vullen. De beleidstheorie achter het TTP-beleid in 1999 is dan ook een betrekkelijk ingewikkeld geheel van doelen, middelen en veronderstellingen. Op basis van de omschrijving van het hoofddoel en de concrete doelstellingen laat de kernredenering van het TTP-project zich in de volgende ringen onderscheiden:

- Het doel is om elektronische handel in Nederland te stimuleren, daarvoor is betrouwbare communicatie nodig.
- Betrouwbare communicatie in een *many-to-many* omgeving laat zich technisch organiseren met TTP.
- TTP komen niet vanzelf tot stand. Omdat elektronische handel pas opbloeit als er TTP zijn en er pas een levensvatbare markt voor TTP-dienstverlening ontstaat als elektronische handel opbloeit, is een beleidsmatige stimulans nodig waarmee de bedoelde betrouwbare TTP-infrastructuur tot stand komt. Het middel daarvoor is het formuleren van randvoorwaarden voor het aanbieden en gebruiken van TTP-diensten.
- TTP zullen alleen bijdragen aan de elektronische handel als ze op het vertrouwen kunnen rekenen van marktpartijen. Dat betekent dat het erom gaat vertrouwen in TTP te realiseren. Daarvoor staan in hoofdzaak twee middelen ter beschikking: een TTP-kamer en een certificatieschema.

Het beleid gaat er vanuit dat TTP de ontwikkeling van de elektronische handel stimuleren en dat een betrouwbare TTP-infrastructuur tot stand komt door een 'reguleringsregime' op te zetten van randvoorwaarden, geoperationaliseerd in een certificatieschema, alsmede door een mechanisme (de TTP-kamer) te creëren dat voor de handhaving daarvan zorgdraagt. Stimuleren en reguleren van een TTP-infrastructuur zijn in het beleid direct met elkaar verbonden en worden in dienst van elkaar gesteld. Kort gezegd: stimuleren door (zelf)reguleren.

Beleidsinstrumentarium
Ook al is het achterliggende doel van het TTP-beleid het bevorderen van elektronische handel, het directe resultaat van het beleid zou een betrouwbare TTP-infrastructuur moeten zijn. Deze is immers geformuleerd als de primaire doelstelling van het TTP-beleid. Om tot een betrouwbare TTP-infrastructuur te komen worden verschillende instrumenten ingezet:

1. In de eerste plaats zijn in de beleidsnotitie randvoorwaarden voor TTP opgesomd en uitgewerkt. Deze hebben betrekking op twee typen TTP-diensten:

   a. Diensten voor authenticiteit en integriteit: het verstrekken van digitale certificaten, het plaatsen en verifiëren van digitale handtekeningen, het onweerlegbaar aantonen van verzending en ontvangst van elektronische berichten, het beheer van cryptografisch sleutelmateriaal voor authenticiteit en integriteit (met uitzondering van de opslag van geheim sleutelmateriaal) en het tijdstempelen van elektronische berichten. De randvoorwaarden voor dit type TTP-diensten hebben betrekking op de organisatie van de dienstverlener (organisatorische waarborgen voor betrouwbare dienstverlening), de gebruikte technologie (met name beveiliging en sleutelbeheer) en regelingen voor bijvoorbeeld bezwaar en aansprakelijkheid.

   BELEIDSINSTRUMENTEN

   - Certificatieschema en TTP-kamer voor TTP-diensten
   - Stimulerende rol overheid bij gebruik TTP-dienstverlening
   - Partnership approach voor rechtmatige toegang

   b. Diensten voor vertrouwelijkheid: het vercijferen van elektronisch berichtenverkeer en het beheer van cryptografisch sleutelmateriaal voor vertrouwelijkheid. De randvoorwaarden voor deze diensten zijn niet uitsluitend ingegeven door het oogmerk dat elektronische handel bevorderd moet worden. Uiteraard geldt voor deze diensten dat een betrouwbare infrastructuur een wezenlijke randvoorwaarde is, maar daarnaast wordt rechtmatige toegang als belangrijke randvoorwaarde gezien, evenals exportcontrole en (nationale en internationale) interoperabiliteit. Met rechtmatige toegang wordt bedoeld dat partijen die een wettelijke bevoegdheid hebben tot het verkrijgen van bepaalde elektronische gegevens (bijvoorbeeld in het kader van strafrechtelijke opsporing of nationale veiligheid) deze ook de facto moeten kunnen bemachtigen. Ten dele sluit deze randvoorwaarde aan op de belangen van marktpartijen en het doel bevordering van elektronische handel. Zo zullen partijen bij sleutelverlies behoefte hebben aan het bewaren van reservekopieën van sleutels ('key escrow') of het kunnen herleiden van sleutelmateriaal ('key recovery'). Toch wordt met rechtmatige toegang ook een nieuw belang in het TTP-beleid geïntroduceerd, evenals enkele nieuwe partijen (het Ministerie van Justitie en dat van Binnenlandse Zaken en Koninkrijksrelaties). Het gaat niet meer primair om het bevorderen van de elektronische handel, maar ook om een keuze in de afweging tussen het 'grondrecht op vertrouwelijke communicatie' (volgens de voorstanders van cryptografie) en 'het kunnen handhaven van wet- en regelgeving' (vanuit het perspectief van strafrechtelijke opsporing en nationale veiligheid).

2. De beleidsnotitie noemt naast de geformuleerde randvoorwaarden nog enkele andere instrumenten, waarmee een betrouwbare TTP-infrastructuur moet worden gerealiseerd. Het gaat daarbij in de woorden van de notitie om 'instrumenten voor het waarborgen van randvoorwaarden'. Ten eerste is dat de totstandkoming van een TTP-kamer als onafhankelijke landelijke organisatie voor TTP. Zowel de overheid als marktpartijen zouden zitting moeten nemen in deze kamer, zij het dat aansluiting door marktpartijen op vrijwillige basis moet plaatsvinden. Er is met andere woorden sprake van zelfregulering, waarbij de markt betrouwbaarheid genereert met behulp van de TTP-kamer. Deze kamer ziet toe op de mate waarin de geregistreerde TTP (blijven) voldoen aan de geformuleerde randvoorwaarden (technisch en organisatorisch, maar ook bijvoorbeeld ten aanzien van interoperabiliteit). Om dit toezicht effectief te kunnen uitoefenen en dus feitelijk als instrument te kunnen fungeren voor het waarborgen van randvoorwaarden, zet de overheid de volgende instrumenten in:

    a. De overheid stimuleert de totstandkoming van een certificatieschema waarin de randvoorwaarden zijn vertaald naar hanteerbare certificatiecriteria waarop de TTP-kamer toezicht kan uitoefenen.
    b. De overheid stimuleert TTP actief om zich aan te sluiten bij de TTP-kamer, door subsidies of kredieten beschikbaar te stellen.
    c. De overheid speelt een actieve rol op het gebied van voorlichting en onderwijs.
    d. De overheid stelt in principe aansluiting bij de TTP-kamer als eis aan TTP die diensten aan de overheid leveren.
    e. De overheid stimuleert de ontwikkeling van specifieke apparatuur en programmatuur die voldoet aan de gestelde randvoorwaarden.
    f. De overheid evalueert het functioneren van een aldus op te richten TTP-kamer na een periode van twee jaar.

3. De beleidsnotitie noemt nog een specifiek instrument om rechtmatige toegang te realiseren. Mede omdat de bewaring en herleidbaarheid van sleutelmateriaal door TTP nog steeds 'onderwerp zijn van internationale controverse', zijn deze eisen niet als randvoorwaarden voor TTP geformuleerd. Bovendien wordt er expliciet voor gekozen de techniek of methodiek om versleutelde gegevens te ontcijferen open te laten in verband met de snelheid en veranderlijkheid van de technologische ontwikkeling. Een 'voor alle partijen aanvaardbaar instrumentarium' zal dan ook nader worden ontwikkeld, en het instrument daarvoor is de 'partnership approach', aldus de beleidsnotitie.

De keuze voor dit instrumentarium ter realisering van de eerder genoemde doelstellingen wordt op verschillende plaatsen nader beargumenteerd. In het algemeen bevat de beleidsnotitie een combinatie van twee overwegingen:

- Er zijn verschillende publieke belangen in het geding, waarvan de belangrijkste zijn het bevorderen van elektronische handel en het realiseren van rechtmatige toegang. Deze belangen pleiten ervoor om ter realisatie van het doel expliciet beleidsinstrumenten in te zetten en de overheid daarin ook een actieve rol te laten spelen: als 'bevorderaar' van de economie, als 'regulator' van kwetsbare infrastructuren en als handhaver van wet- en regelgeving (rechtmatige toegang).
- Voor wetgeving wordt expliciet niet gekozen, omdat dat 'relatief kostbaar en weinig flexibel is', terwijl 'flexibiliteit in de zich nog sterk ontwikkelende TTP-markt een noodzakelijke vereiste is', aldus de notitie.

Veronderstellingen en keuzen
De formulering van de beleidsdoelstellingen en de keuze voor de genoemde 'instrumentenmix' zijn gebaseerd op een aantal expliciet in de beleidsnotitie omschreven veronderstellingen en keuzen. Deze verklaren echter niet volledig de doelen en instrumenten; daarvoor zijn tenminste enkele niet in de beleidsnotitie genoemde veronderstellingen en keuzen nodig. Laten we echter eerst de belangrijkste expliciete veronderstellingen uit de beleidsnotitie onder de loep nemen:

1. Voor het waarborgen van de kwaliteitsaspecten authenticiteit, integriteit en vertrouwelijkheid van gegevens, berichten en transacties bestaan volgens de notitie tal van technische, organisatorische en juridische maatregelen. Expliciet wordt verondersteld dat '(i)n de nabije toekomst (...)een belangrijke rol (kan) zijn weggelegd voor derde partijen die de betrouwbaarheid van het elektronisch berichtenverkeer verhogen door het leveren van specifieke diensten terzake.'
2. De notitie gaat ervan uit dat TTP-diensten voor integriteit en authenticatie en TTP-diensten voor vertrouwelijkheid zowel gecombineerd kunnen worden aangeboden als gescheiden. In de mede aan de nota ten grondslag liggende proefprojecten ging het overigens om gecombineerd aanbod.
3. De beleidsnotitie gaat ervan uit dat 'TTP-diensten (...) voor verschillende toepassingen (kunnen) worden aangewend' en noemt expliciet de financiële sector, de dienstensector, de zorgsector, de accountancy, de overheid, de detailhandel en het notariaat. 'Elke toepassing', aldus de notitie, 'zal (...) specifieke eisen aan de gebruikte TTP-dienst stellen, waardoor uiteenlopende TTP-diensten zullen ontstaan. (...) De differentiatie naar toepassingsgebieden van TTP roept vragen op omtrent de haalbaarheid en wenselijkheid van het formuleren van een algemeen geldend stelsel van randvoorwaarden dat zowel noodzakelijk als voldoende is voor elke mogelijk denkbare TTP-dienst. Hierbij zijn twee factoren van belang. In de eerste plaats zullen naast algemene wettelijke en overige randvoorwaarden ook specifieke eisen op een TTP-dienst van toepassing zijn, die voortvloeien uit specifieke wet- en regelgeving voor de door de TTP-dienst ondersteunde maatschappelijke functie. (...) In de tweede plaats speelt het kostenaspect een rol.' Twee veronderstellingen zijn uit deze passage te distilleren: (1) dat TTP-diensten voor verschillende applicaties zullen worden gebruikt, is geen belemmering om TTP-dienstverlening (in de brede zin van het concept, dus zowel diensten voor authenticiteit en integriteit als diensten voor vertrouwelijkheid) los van deze applicaties op te zetten[6], (2) de genoemde randvoorwaarden zijn minimale voorwaarden voor TTP-dienstverlening en markeren in deze zin een ondergrens.

EXPLICIETE VERONDERSTELLINGEN

- TTP gaan een belangrijke rol spelen bij waarborgen authenticiteit, integriteit en vertrouwelijkheid
- Diensten voor integriteit/authenticiteit en vertrouwelijkheid kunnen gecombineerd worden aangeboden
- De randvoorwaarden zijn minimale voorwaarden (ondergrens)

[6] In deze zin vervult een betrouwbare TTP-infrastructuur dezelfde functie als het bestaan van geld als voorwaarde voor een goed functionerend handelsverkeer.

Naast deze veronderstellingen worden in de beleidsnotitie expliciet enkele keuzen gemaakt ten aanzien van de inrichting van het TTP-beleid:

1. In verband met het 'inherent mondiale karakter van elektronische dienstverlening in het algemeen en elektronische handel in het bijzonder' wordt ervoor gekozen het beleid af te stemmen op internationale ontwikkelingen. Dat komt in het Nationaal TTP-project neer op het aansluiten bij internationale standaardisatieprocessen.
2. Zowel bij de totstandkoming van de randvoorwaarden als bij de verdere uitwerking ervan in een certificatieschema en een TTP-kamer is ervoor gekozen 'gebruikers en belangen aan vraag- en aanbodzijde van de markt' te betrekken. Naast het begeleiden en evalueren van enkele proefprojecten is dat gebeurd door een Consultatiegroep Aanbieders en Gebruikers samen te stellen.
3. Expliciet is de keuze gemaakt 'het realiseren van een TTP-infrastructuur' als 'een verantwoordelijkheid van de markt' te beschouwen. Er is in de ogen van de beleidsmakers weliswaar sprake van publieke belangen, maar de rol van de overheid en het beleid strekt niet verder dan het genoemde instrumentarium. De verantwoordelijkheid van de overheid definieert de beleidsnotitie als volgt: 'samenleving en burgers (te) beschermen door onder meer het waarborgen van de betrouwbaarheid van de TTP-dienst, het bevorderen van de nationale en internationale interoperabiliteit, het beschermen van de persoonlijke levenssfeer van de gebruikers van een TTP-dienst en het waarborgen van de rechtmatige toegang tot elektronische gegevens.' Daarnaast kan de overheid een betrouwbare TTP-infrastructuur stimuleren, aldus de beleidsnotitie. Tenslotte kan de overheid als marktpartij operen – als afnemer, maar ook als aanbieder van TTP-diensten.
4. De beleidsnotitie kiest ervoor om het waarborgen van de randvoorwaarden binnen een zich ontwikkelende TTP-infrastructuur primair haar grondvesten te laten vinden in bestaande wet- en regelgeving. Pas als deze onvoldoende blijken, dienen aanvullende oplossingen te worden overwogen.

De direct uit de beleidsnotitie gedistilleerde veronderstellingen en keuzes verklaren voor een belangrijk deel de geformuleerde beleidsdoelstellingen en de inzet van instrumenten. Toch zijn er nog enkele 'lacunes' in de redenering, die met de volgende – niet onbelangrijke - impliciete veronderstellingen en keuzes kunnen worden benoemd:

IMPLICIETE VERONDERSTELLINGEN

- TTP-infrastructuur stimuleert elektronische handel
- Formuleren randvoorwaarden leidt tot een markt
- Randvoorwaarden en toezicht leiden tot vertrouwen van handelspartners

- De totstandkoming van een betrouwbare TTP-infrastructuur zal elektronische handel stimuleren omdat daarmee het 'vertrouwenslek' in de infrastructuur van het Internet wordt gedicht (onveiligheid ten aanzien van identiteit en authenticatie, maar ook vertrouwelijkheid).
- Het formuleren van randvoorwaarden voor TTP-dienstverlening en TTP-dienstverleners zal, in combinatie met een reeks direct stimulerende maatregelen, leiden tot de totstandkoming van een betrouwbare TTP-infrastructuur.
- Door randvoorwaarden (concreet gemaakt in een certificatieschema) en toezicht op handhaving daarvan (door de TTP-kamer) zullen TTP op het vertrouwen kunnen rekenen van marktpartijen, inclusief de overheid als marktpartij.

Framing van het beleidsprobleem
De vraag kan worden gesteld voor welk probleem het TTP-beleid in 1999 eigenlijk precies een oplossing was. Deze vraag is van belang omdat de logische afstand tussen probleem en oplossing inzicht kan geven in de keuzes en veronderstellingen waarop het beleid is gestoeld. TTP is bijvoorbeeld een manier om tot betrouwbare elektronische communicatie te komen op het Internet, maar omgekeerd mondt betrouwbare elektronische communicatie logisch gezien niet per definitie in TTP uit. Daarom is het belangrijk de zogenaamde 'framing' van het beleidsprobleem te traceren: hoe is het probleem geformuleerd?

In het geval van het TTP-beleid in de notitie van 1999 treffen we tenminste vier onderling verstrengelde formuleringen van het beleidsprobleem aan (vier 'frames'), die zich vanwege de onderlinge verstrengeling niet eenvoudig laten ontrafelen:

1. Het beleidsprobleem is dat communicatie via de infrastructuur van het Internet niet betrouwbaar is. Er doen zich authenticatie- en integriteitsproblemen voor, maar ook vertrouwelijkheidsproblemen. Elektronische handel komt niet van de grond, omdat elektronische handel betrouwbare communicatie veronderstelt. Het TTP-concept lost dit probleem op zonder rechtmatige toegang te bedreigen.
2. Het probleem is dat TTP-diensten niet vanzelf tot stand komen zonder een 'minimum' aan elektronische handel en een minimum aan elektronische handel komt niet tot stand zonder een betrouwbare TTP-infrastructuur. Daarom is een betrouwbare TTP-infrastructuur nodig.
3. Het probleem is dat de nu (in 1999) beproefde technieken voor authenticatie, identificatie en vertrouwelijkheid beperkt zijn tot besloten netwerken voor 'business-to-business' elektronische handel. Voor de consumentenmarkt zijn daarom openbare voorzieningen nodig in de vorm van TTP-dienstverlening.
4. Het probleem is dat vrij aangeboden en in de markt ontwikkelde TTP-diensten (nationaal of internationaal) geen vertrouwen van marktpartijen genereren en dus op zichzelf elektronische handel niet zullen bevorderen. Aan (al dan niet zelf opgestelde) regels en toezicht gebonden TTP-diensten genieten dit vertrouwen wel en daarom moet het beleid erop gericht zijn dit type diensten te realiseren.

2.5 Een evaluatief oordeel

TTP-beleid als 'resultante'
Voor de evaluatie van het TTP-beleid is het om verschillende redenen belangrijk om de genese van dat beleid te kennen. Ten eerste wordt op die manier inzicht verkregen in de achterliggende doelstellingen van het beleid, waarmee in de evaluatie de effectiviteit kan worden beoordeeld. De feitelijk geformuleerde beleidsdoelen zijn daarvoor een geschikt aanknopingspunt, maar krijgen pas betekenis in het licht van de situatie waarin ze zijn geformuleerd. Daarnaast kan een evaluatie, zeker in een turbulente technologische, maatschappelijke en juridisch-beleidsmatige omgeving, zich niet uitsluitend richten op een confrontatie van de huidige situatie met de toenmalige doelstellingen en instrumenten. Er zal tenminste aandacht moeten zijn voor de toenmalige situatie als context waarin doelen en instrumenten zijn bepaald, maar

VERKLARINGEN VOOR TTP-BELEID

- Macro-context: nieuwe wereld en nieuwe economie
- Micro-context: druk op overheid en informatiebeveiliging
- Beleidsframe: technisch probleem, dus technische oplossing

ook is inzicht nodig in de keuzes die daarna zijn gemaakt en de manier waarop is ingespeeld op ontwikkelingen in de beleidsrelevante omgeving. In dit hoofdstuk hebben we ons geconcentreerd op reconstructie van de oorspronkelijke beleidstheorie en het plaatsen van deze theorie in de toenmalige situatie. Daartoe is de genese van het TTP-beleid ontrafeld, hetgeen een scala aan verklaringen voor de keuzes, doelen en instrumenten heeft opgeleverd. We hebben deze in drie hoofdcategorieën ondergebracht:

- De 'macro-context': maatschappelijk is er sprake van het ontstaan van een 'nieuwe economie', een sterk toenemend gebruik van het Internet, en een klimaat dat bol staat van de (economische) beloften van een nieuwe, virtuele wereld. Deze ontwikkelingen hebben op dat moment nog sterk het karakter van ideeën; praktijken blijven achter en onzekerheid over de feitelijke ontwikkelingen is troef. Het beleid dat zich op deze nieuwe wereld richt is vooral stimulerend, met veel aandacht voor zelfsturing, zelfregulering en marktwerking. Juridisch is er nog weinig houvast. In de technologie gaat de aandacht in die tijd vooral uit naar informatiebeveiliging, een ontwikkeling die sterk wordt gestimuleerd door Europees onderzoek. Sommige methoden daarvoor zijn juridisch omstreden, zoals het gebruik van cryptografie.
- De 'micro-context': in het beleidsnetwerk rondom elektronische handel (beleidsmakers op nationaal en internationaal niveau, juristen, informatici, koepelorganisaties, - grote - bedrijven, standaardisatie-organisaties en adviseurs) is een brede consensus over de toekomst van het TTP-concept. Overigens zijn er in vakkringen wel vragen bij het nut van TTP en de keuze voor het TTP-concept, maar deze dringen niet zichtbaar door in het beleidsproces. Bovendien komt het concept tegemoet aan verschillende belangen: het stimuleren van elektronische handel, zelfregulering en marktwerking, veilige en betrouwbare elektronische communicatie en rechtmatige toegang.
- Het beleidsframe: er doet zich een ogenschijnlijk 'technisch' probleem voor (gebrekkige betrouwbaarheid van elektronische communicatie), waarvoor op dat moment een technische oplossing beschikbaar is (PKI technologie). Voor het probleem van de inactie (zonder bloeiende elektronische handel geen levensvatbare markt voor TTP-dienstverlening, zonder TTP-diensten geen bloeiende elektronische handel) dient zich eveneens een haalbare oplossing aan: zelfregulering (een TTP-kamer) en het formuleren van een set van randvoorwaarden voor TTP-diensten, gecombineerd met enkele (lichte) stimuleringsmaatregelen.

De TTP-beleidstheorie: een beoordeling

Het is gemakkelijk de theorie achter het TTP-beleid in 1999 te beoordelen met de wijsheid van nu. We zullen in de volgende hoofdstukken zien dat dan blijkt dat de doelen, instrumenten en veronderstellingen deels terecht zijn gebleken en voor een ander deel niet zijn bewaarheid. Dit oordeel is echter uiterst relatief. Ten eerste is het TTP-beleid in de beschreven vorm niet uitgevoerd, dus komt het erop aan nader te onderzoeken hoe in de uitvoering (en bijstelling) van het TTP-beleid is ingespeeld op de dynamiek in en rondom het beleid (we noemen dit de responsiviteit van het TTP-beleid). Dat doen we in hoofdstuk drie. Ten tweede gaat het er niet alleen om de situatie van nu te vergelijken met de keuzes en doelstellingen van toen, maar de keuzes en doelstellingen van toen in het licht van de toenmalige situatie te beoordelen.

Deze beoordeling hangt overigens volledig af van het perspectief waarmee het oorspronkelijke TTP-beleid wordt benaderd. Wij maken een onderscheid tussen een oordeel binnen het toen gekozen paradigma en een beoordeling van het destijds gekozen paradigma. Binnen het paradigma laat het oordeel zich als volgt samenvatten:

- Het TTP-beleid bevat een degelijk uitgewerkte set randvoorwaarden. Er is niet alleen aandacht voor technische garanties voor een betrouwbare TTP-infrastructuur (bijvoorbeeld PKI technologie), maar ook voor organisatorische en 'systemische' waarborgen (van functiescheiding bij de TTP-dienstverlener tot en met bezwaar- en beroepsprocedures). De randvoorwaarden zijn in de beleidsnotitie uit 1999 nog algemeen geformuleerd, maar met het expliciete doel om in een certificatieschema te worden uitgewerkt dat zich leent voor toezicht door een TTP-kamer.
- Het beleid laat TTP-dienstverleners veel ruimte om de randvoorwaarden op een eigen manier in te vullen en hun 'maatschappelijke rol' zelf op de door hen verstandig geachte manier vorm te geven. Authenticatie-, integriteits- en vertrouwensdiensten mogen afzonderlijk op de markt worden aangeboden, maar ook in combinatie. Combinaties met andere diensten – zoals betalingsverkeer of post – zijn eveneens mogelijk volgens het TTP-beleid, mits de onafhankelijkheid van de TTP-dienstverlener ten opzichte van de marktpartijen is gewaarborgd. Deze open benadering is geschikt voor een markt die zich nog moet ontwikkelen; zo wordt immers veel ruimte gegeven aan potentiële TTP-dienstverleners om die diensten te ontwikkelen waarvoor koopkrachtige vraag bestaat. Ook worden op deze manier leerprocessen bevorderd door variatie toe te staan.

BINNEN HET TTP-PARADIGMA

- Degelijk uitgewerkte set randvoorwaarden
- Veel ruimte voor eigen invulling dienstverleners
- Publieke belangen in zelfregulering verankerd
- In flankerend beleid is voorzien

- Het beleid voorziet in een systeem van zelfregulering. De publieke belangen zijn in het systeem verankerd (variërend van bescherming van marktpartijen en min of meer waterdichte betrouwbaarheid tot interoperabiliteit, bescherming van de persoonlijke levenssfeer en rechtmatige toegang).
- Hoewel het beleid is gebouwd op de veronderstelling dat 'regulering' (door randvoorwaarden te benoemen, deze uit te werken in een certificatieschema en daarop toezicht te laten houden door een TTP-kamer) als vanzelf een 'betrouwbare TTP-infrastructuur' stimuleert, wordt daar door de beleidsmakers niet volledig op vertrouwd. Daarom zijn enkele extra stimuleringsmaatregelen voor de overheid aangebracht met een 'licht' karakter, zoals subsidies, kredieten en voorlichting. Bovendien wordt de overheid als 'marktpartij' gemobiliseerd door aan TTP-dienstverleners waarmee de overheid zaken doet de eis te stellen dat ze zijn aangesloten bij de TTP-kamer.

Naast de beoordeling van de beleidstheorie binnen het gekozen paradigma kan het paradigma van het TTP-beleid als zodanig worden beoordeeld in het licht van de toenmalige situatie. Dit oordeel laat zich samenvatten in de volgende punten:

- De keuze voor TTP past naadloos in het tijdsbeeld van de tweede helft van de jaren negentig. Het is een tijd van grote beloften ten aanzien van de interneteconomie en de potentie van het Internet als 'handelsplaats'. Bovendien sluit de keuze voor zelfregulering aan op het politiek-bestuurlijke klimaat van toen en de aard van regulering in de virtuele wereld. Ook sluit de keuze voor TTP aan op ontwikkelingen op Europees niveau en druk vanuit potentiële TTP-dienstverleners die om een 'kwaliteitskeurmerk' vragen waarmee ze het vertrouwen van marktpartijen willen winnen.
- De stelligheid waarmee voor TTP als oplossing wordt gekozen is niet congruent met de toenmalige onzekerheid ten aanzien van maatschappelijke ontwikkelingen (de interneteconomie) en de technologische ontwikkeling (PKI technologie als een van de manieren om betrouwbare communicatie te creëren). Ondanks de niet altijd even positieve voortekenen (waarop ook de beleidsnotitie uit 1999 wijst), is nergens in het beleid voorzien in een voorbehoud voor het geval dat TTP niet de primaire voorwaarde zal blijken te zijn voor het opbloeien van elektronische handel. Toch zijn er wel signalen dat het nut van TTP niet a priori mag worden verondersteld, hoewel deze niet sterk in het beleidsproces doorklinken. In het geval TTP niet 'nuttig' zouden zijn, zou immers een robuust en goed uitgewerkt raamwerk van voorwaarden zoals dat in het TTP-beleid is ontwikkeld een relatief grote inspanning zijn ten opzichte van de noodzaak of het beleidsprobleem. In een uiterst onzekere en dynamische context is onomwonden en zonder voorbehoud voor één route naar betrouwbare communicatie gekozen.

HET TTP-PARADIGMA BEOORDEELD

- Paradigma past in tijdsbeeld
- Stelligheid is niet congruent met onzekerheid en dynamiek
- Niet expliciet op aantal inschattingen gereflecteerd
- Enkelvoudig probleemframe

- We hebben gezien dat de theorie achter het TTP-beleid nogal wat veronderstellingen en probleemdefinities bevat. Deze hebben deels een feitelijke basis: zo is er technisch en juridisch onderzoek op Europees niveau beschikbaar, er zijn enkele proefprojecten uitgevoerd en geëvalueerd die laten zien dat de technologie werkt en er is een gebruikersgroep gemobiliseerd (bestaande uit marktpartijen en potentiële dienstverleners). Ook is er de feitelijke ontwikkeling van het algemene beleid ten aanzien van wat toen de elektronische snelweg werd genoemd, met de uitgangspunten van zelfregulering en marktwerking. Daarnaast zijn er ook inschattingen gemaakt die destijds een feitelijke basis ontbeerden: denk bijvoorbeeld aan de veronderstelling dat marktpartijen behoefte hebben de mate van betrouwbaarheid die het TTP-beleid creëert. Of feitelijke toetsing van deze veronderstellingen destijds mogelijk of realistisch was (niet alles laat zich immers op elk moment onderzoeken en in harde conclusies vertalen), is achteraf niet te beoordelen. Wel kan worden vastgesteld dat de inschattingen niet expliciet in het beleid als zodanig (dus als inschatting) zijn gepresenteerd en op hun betrouwbaarheid zijn beoordeeld. Aan deze inschattingen is in vakkringen wel getwijfeld, zij het dat ook daar niet direct een wenkend alternatief voor TTP werd gepresenteerd (dat tegemoet kwam aan de oplossing van het informatiebeveiligingsprobleem en tegelijkertijd aan de behoefte aan rechtmatige

toegang). Toch zijn deze inschattingen geen onderwerp geworden van publiek debat of publieke toetsing; evenmin zijn er aanwijzingen dat ze wel expliciet en grondig binnen het beleidsnetwerk ter discussie zijn gesteld en geanalyseerd.

- Hoewel binnen het TTP-paradigma de probleemdefinitie achter het beleid zoals we hebben gezien meervoudig van karakter was (verschillende 'probleemframes' tegelijkertijd), gold dat niet voor de probleemdefinitie van het TTP-paradigma als zodanig. Het paradigma is primair gebaseerd op een technologische probleemdefinitie: de infrastructuur van het internet roept vragen op rondom authenticatie, integriteit en vertrouwelijkheid, en dus is er sprake van een informatiebeveiligingsprobleem. Dat probleem ligt ten grondslag aan het gebrekkige vertrouwen van marktpartijen in elektronische handel. Nog los van de toenmalige mogelijkheid of onmogelijkheid om de validiteit van deze probleemdefinitie te onderzoeken is de eenduidigheid opvallend. Deze wordt wel geweten aan de dominante 'coalitie van juristen en techneuten', die beiden dit probleem als relatief 'behapbaar' beschouwen omdat het met regels en standaarden kan worden opgelost (zie Van Rij, 2002; Van Rij en Van Eeten, 2003). Misschien is de aandacht daardoor te snel of te veel op 'randvoorwaarden' en een 'certificatieschema' gericht, zoals Van Rij in haar scriptie over het TTP-beleid concludeert. Vastgesteld kan worden dat er in ieder geval eenduidig voor is gekozen zonder de betrekkelijkheid ervan expliciet te benoemen of er andere benaderingen of ingangen naast te plaatsen.

3. De responsiviteit van het TTP-beleid 'kansen zoeken en grijpen'

3.1 Inleiding

In de in juni 1999 aan de Tweede Kamer aangeboden notitie wordt het Nationaal TTP-project aangekondigd. Zoals in de Kamernotitie vermeld, is reeds begin 1999 gestart met uitvoering van dat project onder de noemer TTP.NL. Geheel in lijn met de strategie van zelfregulering en marktwerking is het project ondergebracht bij het Electronic Commerce Platform Nederland (ECP.NL), een publiek-privaat samenwerkingsverband dat zich richt op het bevorderen van elektronische handel ter verbetering van de concurrentiepositie van Nederland. De uitvoering van het TTP-beleid komt in de praktijk vooral neer op uitvoering van het project TTP.NL. Dit project wordt op hoofdlijnen beschreven en geanalyseerd in paragraaf 3.2.
Op verschillende momenten, zo blijkt uit eerdere analyses van het TTP-beleid (Van Rij, 2002; Van Rij en Van Eeten, 2003), is er in de uitvoering van het TTP.NL-project voor gekozen een koppeling te maken met ontwikkelingen in de (directe) omgeving van het TTP-beleid. In paragraaf 3.3 gaan we uitgebreider in op de achtergrond van twee cruciale keuzes die in de uitvoering van het TTP-beleid zijn gemaakt en de consequenties daarvan: de aansluiting op de implementatie van de in de Europese richtlijn genoemde (geavanceerde) elektronische handtekening en op het beleidsproject PKI-overheid. Andere krachten die op het TTP-beleid hebben ingewerkt beschrijven we in paragraaf 3.4. In de laatste paragraaf beoordelen we de uitvoering van het TTP-beleid en de manier waarop is ingespeeld op (veranderingen en ontwikkelingen) in de omgeving. Het oordeel komt tot stand door de feitelijke keuzes en ontwikkeling van de uitvoering van het TTP-beleid te beschouwen in het licht van (1) congruentie met ontwikkelingen en bewegingen in de omgeving van dat beleid en (2) de oorspronkelijk geformuleerde beleidsdoelstellingen.

3.2 Uitvoering van het Nationaal TTP-project

De uitvoering van het Nationaal TTP-project (TTP.NL) sluit aan op een reeks van activiteiten die met het Nationaal Actieprogramma Elektronische Snelwegen (NAP) zijn gestart. De voorloper van TTP.NL vond plaats in de periode april 1997 en maart 1999 onder gemeenschappelijk opdrachtgeverschap van het Ministerie van Economische Zaken en het Ministerie van Verkeer en Waterstaat[7]. Het project kent vier hoofdfasen, te weten het opstellen van het projectplan, de formulering van randvoorwaarden voor het aanbieden van TTP-diensten, de begeleiding en beoordeling van pilotprojecten en het opstellen van de beleidsnotitie (Nationaal TTP-project).

Gesteld werd dat het invullen van de randvoorwaarden in belangrijke mate door de marktpartijen zelf diende te geschieden. Hiertoe is het zogenaamde TTP.NL-project eind 1998 van start gegaan. Het ingezette zelfreguleringspoor was een initiatief van marktpartijen en werd gestimuleerd door de overheid.[8]

---

[7] Tijdens dat project is gewerkt met een breed samengestelde Consultatiegroep Aanbieders en Gebruikers (CAG).

[8] *Kamerstukken II*, 1998-1999, nr 26.851

3.2.1 Opzet van het project TTP.NL

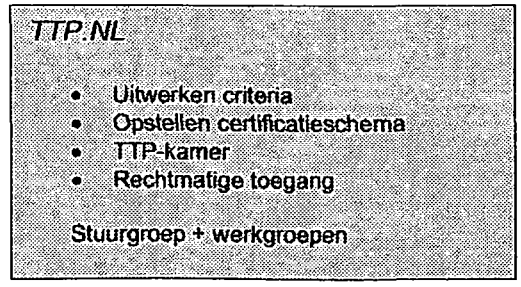
Doel van het project TTP.NL, dat formeel is gestart in 1998 en materieel in 1999, was het geven van invulling aan de in de beleidsnotitie Nationaal TTP-project geformuleerde randvoorwaarden voor het aanbieden van TTP-diensten. TTP.NL is een samenwerkingsverband van overheid, marktpartijen en onafhankelijke deskundigen en wordt gefaciliteerd door ECP.NL, het platform voor elektronisch zakendoen. In de uitvoering van het TTP.NL project zijn experts bijeengebracht in werkgroepen, zodat kennis voor handen was over zaken als PKI, auditing, juridische aspecten en technische mogelijkheden.

Bij de start van TTP.NL kende het project de volgende deelnemers (* = stuurgroeplid).

ECP.NL
Abz Holding
Consumentenbond *
EAN Nederland
DSEMCO (Data Security Management Consult)
Enschedé/Sdu
ICIT (Instituut voor keuring en certificatie van IT)
Interpay
Kamer van Koophandel Amsterdam
Kennedy Van der Laan Advocaten
Koninklijk Notarieel Beroepsorganisatie
KPMG
KPN
Ministerie van Binnenlandse Zaken *
Ministerie van Algemene Zaken *
Ministerie van Economische Zaken *
Ministerie van Justitie *
Ministerie van Verkeer en Waterstaat *
NL Sign
Kema
PriceWaterhouseCoopers
PTT Post
Rabobank
Rijksuniversiteit Leiden
Roccade
Shell
Vereniging van KvK's
VNO-NCW *
VIFKA

Het project TTP.NL is van start gegaan in een constructie met een stuurgroep en werkgroepen:

Stuurgroep: de stuurgroep coördineert de werkzaamheden van de verschillende werkgroepen met als doel de voortgang te bewaken. Ze treedt tevens vanuit het project op formele momenten naar buiten. Daarnaast heeft de stuurgroep de taak constant te bewaken of de resultaten van het project wel aan blijven sluiten bij de reële behoefte van de markt. Ook het bewaken van internationale ontwikkelingen ligt in handen van de stuurgroep. In de stuurgroep is het bedrijfsleven vertegenwoordigd door koepelorganisaties (in de werkgroepen hebben tevens individuele bedrijven zitting). Voorzitter van de stuurgroep is professor Franken van de Universiteit Leiden.



Werkgroep Accreditatie en Certificatie: deze werkgroep heeft de taak om een infrastructuur op te zetten voor het accrediteren en certificeren van TTP in Nederland.

Werkgroep Certificate Policy (later geworden Werkgroep Criteria): deze werkgroep werkt aan een set van criteria waaraan TTP in Nederland moeten voldoen. Met behulp van deze criteria heeft de werkgroep ACT een accreditatie- en certificatieschema opgesteld.

Werkgroep TTP-Kamer: de werkgroep TTP-kamer onderzoekt de institutionele en operationele aspecten van het inrichten van een TTP-kamer. Onderwerpen die hierbij aan de orde komen, zijn onder meer het opstellen van een advies inzake de institutionele aspecten, het waarborgen van internationale interoperabiliteit en het creëren van mogelijkheden voor geschillenbeslechting.

Naast deze stuur- en werkgroepen zijn nog twee actoren belangrijk: de Coördinatiegroep en het Centraal College van Deskundigen voor Informatiebeveiliging. De Coördinatiegroep is tot stand gekomen gedurende de looptijd van TTP.NL. In de groep hebben belangstellende partijen uit eerdere actieve werkgroepen van TTP.NL zitting (bijvoorbeeld uit de werkgroep criteria die eerder gereed zijn dan de werkgroep ACT), evenals partijen die later actief zijn geworden in het beleidsveld. In principe staat deze coördinatiegroep open voor alle partijen.

De inspanningen van TTP.NL hebben onder andere geleid tot een certificatieschema voor TTP (zie hoofdstuk vier). Het onderhoud en het beheer van dit schema, alsmede het certificeringsproces is in handen gelegd van het Centraal College van Deskundigen voor Informatiebeveiliging (CCvD-IB) dat is ondergebracht bij ECP.NL.[9]

3.2.2 Uitwerking van de criteria

De uitwerking van criteria is uitgevoerd door een werkgroep Certificate Policy (CP). Deze werkgroep is breed samengesteld en bestaat uit vertegenwoordigers van Abz Holding, Cordemeyer en Slager Advocaten & Procureurs, DSEMCO, ECP.NL, ENSCHEDE/SDU, Interpay Nederland, Kennedy van der Laan Advocaten, KPMG TTP Services, KPN Research, Kamer van Koophandel Amsterdam, Ministerie van Economische Zaken, NL Sign, Pricewaterhouse Coopers, Rabobank Nederland en VNO-NCW. Tijdens de eerste vergadering van de werkgroep CP ontstaat een discussie over de werkzaamheden van de werkgroep. Hierbij is een aantal essentiële vragen opgeworpen over de beoogde taken van de werkgroep CP en de relatie met andere werkgroepen binnen het project TTP.NL. Het gaat daarbij om vragen als:

- Op welk type TTP richt het project TTP.NL zich: publieke TTP, branche-TTP, bedrijfs-TTP?
- Voor welke diensten binnen de TTP zal de Certificate Policy worden opgesteld?
- Welke diepgang dient de Certificate Policy die door de werkgroep wordt opgesteld te hebben?
- Op welke wijze kunnen de werkzaamheden van de werkgroep Certificate Policy zo optimaal mogelijk in de werkzaamheden van de andere werkgroepen worden gepast?

[9] Tot het einde van de Stichting ICIT per 31 maart 2000 was het CCvD-IB ondergebracht bij deze stichting.

Nadat de stuurgroep deze vragen in de ogen van de werkgroep afdoende heeft beantwoord, is de werkgroep vervolgens daadwerkelijk gestart met de uitwerking van criteria.

Door de werkgroep is in het tweede kwartaal van 1999 een set criteria ontwikkeld voor de beoordeling van CSP. Deze criteria hebben Annex II van de Europese Richtlijn als uitgangspunt. De criteria kunnen globaal in drie groepen worden ingedeeld. Het gaat om criteria voor achtereenvolgens:

- de elektronische verwerkingsprocessen in de CSP,
- het management van de informatiebeveiliging van de CSP, en
- de maatschappelijke aspecten van de CSP.

Deze criteria worden aangeduid als de TTP.NL Criteria deel 1, 2 en 3. De beschrijvingen ervan zijn verschenen als afzonderlijke rapporten.

In de periode september tot en met november 1999 zijn proefaudits uitgevoerd bij een aantal CSP die zich hebben gemeld bij TTP.NL. Het ging om Roccade Megasign, PTT Post Keymail en Diginotar. Hoofddoel van deze audits is het onderzoeken van de praktische toepasbaarheid van de opgestelde conceptcriteria.

Na een start van TTP.NL als een initiatief in het kader van zelfregulering is de EU Richtlijn met betrekking tot elektronische handtekeningen vanaf 2000 mede als uitgangspunt voor het werk van TTP.NL genomen. TTP.NL heeft zich hierbij met name gericht op de eisen die aan TTP worden gesteld voor het uitgeven van certificaten voor de gekwalificeerde elektronische handtekening. Om de nog tamelijk abstracte eisen in de Richtlijn nader uit te werken is het European Electronic Signature Standardization Initiative (EESSI)) in het leven geroepen. Verschillende betrokken partijen (industrie, gebruikers en overheid) werkten samen in een standaardisatieproces opdat nog in 2000 standaarden beschikbaar zouden komen waarmee voldaan kon worden aan het gestelde in de Richtlijn. EESSI wordt gefaciliteerd met de standaardisatieprocessen van ETSI en CEN, waarbij het tempo hoog is gehouden door de inzet van betaalde experts. Ook TTP.NL is in EESSI op een aantal plaatsen vertegenwoordigd, onder meer om de resultaten van TTP.NL op de geëigende plaatsen in EESSI in te brengen.

3.2.3 Opstellen certificatieschema

De ontwikkeling van een schema is in handen gegeven van de werkgroep Accreditatie en Certificatie van TTP (ACT). Bij de start hiervan in 1999 bestaat deze werkgroep uit vertegenwoordigers van Shell (voorzitter), Roccade, PTT Post, Diginotar, PPT Telecom, Interpay, KEMA, KPMG, PriceWaterhouseCoopers, Rabobank Nederland, Ministerie van Economische Zaken, ECP.NL, Raad voor de Accreditatie en ICIT. Taak van de werkgroep is het opstellen van een raamwerk voor certificatie en accreditatie van CSP.

In 1999 had men de beschikking over zowel de criteria Part 1, 2 en 3 als een raamwerk voor de certificatie en accreditatie van CSP. In 2000 is besloten om het commentaar van marktpartijen (onder andere de Vereniging van Banken en de Taskforce PKI Overheid) hierop te verwerken en om aan te sluiten bij de ontwikkelingen in Europa en wel binnen het (EESSI, zie eerder). Binnen het TTP.NL project is vervolgens een ad hoc werkgroep ingesteld om te

komen tot aanpassing/verscherping van het schema (deelnemers: CSP, gebruikers, audit organisaties en de Raad voor de Accreditatie).

Naast de publicatie van de EU richtlijn met betrekking tot elektronische handtekeningen, doen zich vanaf de start van het Nationaal TTP-project twee andere belangrijke ontwikkelingen voor die (in potentie) de uitwerking van de criteria en het certificatieschema kunnen beïnvloeden. Het gaat hierbij om de relatie vanuit TTP.NL met de Taskforce PKIoverheid en de Stuurgroep Rechtmatige Toegang.[10]

Relatie met PKIoverheid
In het begin van TTP.NL nemen vertegenwoordigers van gebruikers, zoals de Consumentenbond en VNO-NCW, deel in het project. Vanaf januari 2000 schuift de overheid als gebruiker aan, gebundeld in de Taskforce PKIoverheid (zie daarvoor uitgebreid paragraaf 3.3.2). Het idee dat de overheid als 'launching customer' zou gaan optreden, sprak tot de verbeelding. Hoewel op vele punten overeenstemming bestond tussen PKIoverheid en TTP.NL waren er gelijktijdig ook verschillen. Deze hadden met name betrekking op de invulling van de eisen uit de richtlijn. In een notitie van PKIoverheid over de relatie tussen PKIoverheid en TTP.NL wordt in mei 2000 geconstateerd dat accreditatie volgens de TTP.NL criteria niet die waarborgen kunnen bieden die PKI overheid stelt aangezien de criteria, conform de Europese richtlijn, zowel geschikt zijn voor CSP die gekwalificeerde certificaten uitgeven als overige CSP. TTP.NL is slechts de invulling van een van de mogelijkheden die de richtlijn biedt aan de lidstaten om het vertrouwen in CSP te verhogen, namelijk het invoeren van een vrijwillig accreditatieschema, aldus PKIoverheid.

In april 2001 vindt overleg plaats tussen auditors en deskundigen waarbij ook de TTP zijn uitgenodigd, alsmede de OPTA als toehoorder. Hierin geeft de Taskforce PKIoverheid aan dat er nog een aantal aspecten is dat verder belicht zou moeten worden voor een grootschalige invoering / toepassing van PKI feitelijk mogelijk is. Hierbij wordt gedacht aan het ontbreken van standaarden voor trustworthy systems voor CA's en invulling van het begrip continuïteit van dienstverlening. In overleg tussen TTP.NL en PKIoverheid in de jaren 2000 en 2001 is vele malen gesproken over interoperabiliteit en de vraag hoe belangrijk dit is. PKIoverheid is van mening dat dit in de toekomst zeer belangrijk gaat worden. Als TTP.NL deze invulling niet regelt, gaat PKIoverheid het zelf doen. TTP.NL geeft aan te streven naar samenwerking, maar moet wel kijken op welk terrein dat kan. In een TTP.NL stuurgroepvergadering van 20 december 2001 is opnieuw over deze kwestie gesproken. Vanuit het bedrijfsleven wordt aangegeven dat men zich afvraagt of PKIoverheid niet een te hoog betrouwbaarheidsniveau gaat neerzetten waar in veel kringen weinig behoefte aan is. Men geeft aan dat men het van belang acht dat TTP.NL als startpunt dient, maar dat de eisen van PKIoverheid niet de norm gaan worden.

Relatie met rechtmatige toegang
In de beleidsnotitie Nationaal TTP-project is in 1999 besloten om de eisen op het gebied van rechtmatige toegang (vertrouwelijkheidsdiensten) niet als randvoorwaarden mee te nemen maar in een 'partnership approach' verder uit te werken. TTP.NL neemt de uitwerking van deze randvoorwaarden dan ook niet mee in haar werkzaamheden, maar laat dit over aan een ingestelde Stuurgroep Rechtmatige Toegang. In een stuurgroepvergadering van TTP.NL van 15 maart 2001 wordt melding gemaakt van het feit dat deze stuurgroep heeft besloten om aan te haken bij TTP.NL en criteria en een schema op te stellen voor TTP die

[10] In de volgende paragraaf wordt uitgebreider stilgestaan bij de invloed van de EU Richtlijn en PKI Overheid op TTP.NL.

vertrouwelijkheidsdiensten aanbieden. Wanneer TTP vertrouwelijkheidsdiensten willen aanbieden zullen zij moeten voldoen aan de criteria die daarvoor gelden, dat wil zeggen dat zij hun diensten zo moeten inrichten dat zij in staat zijn rechtmatige toegang te verlenen door middel van key-escrow of key-recovery. Men geeft aan dat het verwerven van de medewerking van TTP.NL voorop staat bij de Stuurgroep Rechtmatige toegang waarbij benadrukt wordt dat het koppelen van rechtmatige toegang aan TTP.NL geen belemmering mag vormen voor de ontwikkelingen bij TTP.NL. Deze koers van de Stuurgroep Rechtmatige Toegang wordt niet onmiddellijk door de Stuurgroep TTP.NL omarmd. De vraagpunt die deze laatste stuurgroep stelt, betreft de internationale economische effecten van de verplichting om rechtmatige toegang te verlenen. Men besluit aan de Stuurgroep Rechtmatige Toegang een brief te sturen waarin de opdracht wordt geformuleerd om een onderzoek te doen naar het inzichtelijk maken van deze effecten. In de TTP.NL stuurgroepvergadering van 17 september 2002 wordt aangegeven dat het door het College van Deskundigen raadzaam wordt geacht voorzichtigheid te betrachten bij het eventueel uitbreiden van het schema zodat certificering van vertrouwelijkheidsdiensten mogelijk wordt. Vertrouwelijkheidsdiensten zijn anders dan elektronische handtekeningen en bovendien is het verstandig het schema niet aan te passen nog voordat het eerste certificaat is verstrekt. Als gevolg van deze overweging wordt besloten de uitbreiding als bedoeld voorlopig op de lange baan te schuiven (in elk geval tot 2003).

Het schema in concept

Het resultaat van dit proces is dat het project TTP.NL in 2001 een vrijwillig certificatieschema voor TTP heeft opgeleverd. Het betreft een schema op basis waarvan een CSP gecertificeerd kan worden. Het TTP.NL schema is gebaseerd op de Europese Richtlijn en de Europese Technische specificatie ETSI TS 101 456 die op zijn beurt weer de TTP.NL Criteria 1, 2 en 3 omvat.
Om te kijken of het ontwikkelde certificatieschema in de praktijk ook werkt voor de betrokken partijen, zijn in 2001 vijf grote TTP in Nederland benaderd voor de noodzakelijke business case. Om gecertificeerd te kunnen worden is het volgende traject noodzakelijk: de organisatie die TTP wil certificeren (auditen) moet daarvoor eerst geaccrediteerd worden. Bij accreditatie moet er een 'witness' van de Raad voor Accreditatie mee met de audit. Het is een vrij subtiel proces, dat discreet moet gebeuren (omdat accreditatie niet zeker is). Om de business cases op te stellen heeft men dus een auditor en een potentiële dienstverlener (TTP) nodig die dit traject willen ingaan. Deze zijn niet eenvoudig te vinden; met name het vinden van auditors blijkt lastig. Zo geeft KEMA met betrekking tot PKI aan geen mogelijke klanten te zien en heeft ook KPMG vragen rondom de business case. Naast KPMG toonden PriceSaterhouseCoopers en Deloitte & Touche belangstelling. TTP.NL streeft ernaar partijen 'het laatste duwtje te geven'.

Interpretatie van de criteria: de Guidance

Niet alleen het rondmaken van de business case voor auditing blijkt lastig bij het toepassen van het schema in de praktijk. Ook de interpretatie van de criteria levert problemen op. De ontwikkelde Europese criteria (ETSI TS 101 456) zijn van een dermate hoog abstractieniveau dat het gevaar bestaat dat in de praktijk meerdere interpretaties hiervan zouden worden gehanteerd. Bovendien leidt de noodzakelijke interpretatie ertoe dat partijen die een voortrekkersrol vervullen, worden geconfronteerd met extra werkzaamheden waarmee andere marktpartijen, die later gaan certificeren, niet te maken krijgen. Interpretatie van de ontwikkelde standaard voor TTP en afstemming hierover vraagt dus een extra, onvoorziene inspanning. Deze inspanning is echter essentieel voor het waarborgen van de eenduidigheid van audits en daarmee de waarde van een TTP.NL certificaat. Door de ontwikkeling van het

guidancedocument en de financiering hiervan door het ministerie van EZ wordt voorkomen dat de eerste dienstverleners kosten moeten maken die latere toetreders niet hebben.
Om aan dit bezwaar tegemoet te komen, wordt opdracht gegeven om op basis van een eenmalige doelbeschikking van het ministerie van Economische Zaken een Guidance document te laten schrijven waarin concrete interpretaties van begrippen uit de criteria worden gegeven. Deze interpretaties zijn bindend voor certificerende instellingen die bij het Centraal College van Deskundigen voor Informatiebeveiliging (CCvD) zijn aangesloten. De werkgroep van de CCvD bestaat uit vertegenwoordigers van KPN, Diginotar, PinkRoccade Megaplex, KPMG, PriceWaterhouseCoopers en ECP.NL (tevens voorzitter).
Het Guidance document verschijnt onder de titel *TTP.NL Guidance on ETSI TS 101 456* in mei 2002. ECP.NL heeft vervolgens gezorgd voor een rapportage waarin de tijdens certificatietraject opgedane vakkennis en ervaringen vastgelegd worden. Dit rapport kan dienen als leidraad bij volgende certificaties.

3.2.4 De TTP-kamer

De start
Het idee bij aanvang van het TTP.NL project was dat het toezicht op de TTP-infrastructuur in handen zou komen van een zogenaamde TTP-kamer. In de geest van zelfregulering en het streven naar een vrijwillig certificatiesysteem, is het op dat moment de bedoeling dat de marktpartijen en overheid samen zitting nemen in de TTP-kamer. De uitwerking van dit idee is in handen gegeven van de werkgroep TTP-kamer, met daarin de Registratiekamer, NVB, VNO-NCW, Stichting Rinis, KNB, Ministerie van Verkeer en Waterstaat en SVB. De werkgroep onderzoekt de institutionele en operationele aspecten van het inrichten van een TTP-kamer. Onderwerpen die hierbij aan de orde komen, zijn:

- het beheer van de Certificate Policy/lijst van Criteria en de subsets voor de specifieke TTP-diensten,
- het opstellen van een advies inzake de institutionele aspecten,
- het waarborgen van interoperabiliteit,
- het creëren van mogelijkheden voor geschillenbeslechting, en
- de financiële inrichting van een TTP-kamer.

De oorspronkelijke uitgangspunten
De uitgangspunten voor een TTP-kamer worden in een werkgroepvergadering van 13 juli 1999 vastgesteld:

1. De TTP-kamer moet worden gezien als kenniscentrum, een 'brancheverenigingplus'. De ondergrens voor de positionering is het zijn van een brancheverenigingde bovengrens is die van toezichthouder.
2. Wettelijke verankering is een aandachtspunt. Dit kan nodig blijken om de TTP-Kamer in internationaal verband als centraal nationaal orgaan te kunnen positioneren. Dit zal primair door de overheidspartijen worden bekeken.
3. Bij de uitwerking van het business plan zal voorop staan dat de TTP-Kamer 'lean & mean' zal moeten worden ingericht.
4. Primair zullen door PWC de taken in de TTP-Kamer worden uitgewerkt, met de noodzakelijke randvoorwaarden. Daarbij zal ook aangegeven worden welke 'witte vlekken' nog bestaan. Dit overzicht zal door ECP.NL worden toegestuurd aan de leden van de werkgroep, met het verzoek om commentaar. Indien de lijst met taken en

randvoorwaarden volledig is gemaakt, vangt PWC aan met het opzetten van de structuur van het Business Plan. In dit stadium zal nog geen uitwerking gegeven worden aan de inrichting van de organisatie van de TTP-Kamer.

Uit het bovenstaande blijkt de behoefte van de partijen om de TTP-kamer qua structuur zou eenvoudig en transparant mogelijk te houden. Daarom streeft men er zoveel mogelijk naar een bestaande organisatie te benutten voor TTP. Ten tijde van de ontwikkeling van de TTP-kamer bestaat reeds een organisatie, bestaande uit twee certificerende instellingen voor het certificeren van dienstverleners (op basis van de norm BS 7799).

Van TTP-kamer naar OPTA-toezicht

Naarmate de werkgroep verder komt met haar werkzaamheden, blijkt dat de beoogde organisatie niet zonder meer te gebruiken is voor het certificeren van TTP. KEMA, een van de twee certificerende instellingen, laat weten moeite te hebben met een certificerende rol met betrekking tot TTP op grond van de mogelijkheid dat TTP zichzelf zouden kunnen certificeren. Op dat moment (2000) komt de overheid als mogelijke toezichthouder als idee naar voren. Het belangrijkste punt is een voldoende mate van adequaat toezicht, aldus de werkgroep. Het is daarbij belangrijk, zo wordt gesteld, dat klachten niet tussen wal en schip terechtkomen. Iemand zal dus hoe dan ook toezicht moeten houden. Dat kan de overheid zijn, maar ook een andere instantie die volgens bepaalde regels handelt. Een argument voor toezicht door de overheid is dat de overheid sancties kan toepassen, aldus een verslag van de stuurgroep TTP.NL uit april 2000.

Dat de overheid wellicht een grotere rol in het toezicht zou krijgen dan aanvankelijk voorzien, wordt mede gestimuleerd door de eerder reeds genoemde EU Richtlijn. Deze wordt zo geïnterpreteerd dat vrijwillige certificering onvoldoende als onvoldoende wordt beschouwd. Daarom volgt nader beraad over de inrichting van een toezichtstructuur. Uiteindelijk gaat de keuze tussen positionering van een TTP-Kamer bij de OPTA of in de vorm van een nieuwe stichting. In de stuurgroepvergadering van 5 juli 2000 wordt aangegeven dat het wetsvoorstel als volgt wordt ingevuld:

> 'Het toezicht wordt op lichte manier ingevuld middels registratie. Deze rol zal worden vervuld door de OPTA. Men denkt dan aan een openbaar register waar ook vermeld zal staan of het al dan niet een geaccrediteerde TTP betreft. Wanneer de OPTA een gegrond vermoeden heeft dat de TTP niet voldoet aan de criteria volgt een onderzoek, in afstemming met TTP.NL indien het een TTP is die onder TTP.NL geaccrediteerd is. Het toezicht wordt onder andere bij de OPTA gelegd omdat men het bij een bestaande organisatiestructuur wilde plaatsen. Het lichte toezicht moet wel goed gecommuniceerd worden naar de markt. De richtlijn zelf staat overigens preventief toezicht in de weg.'

De manier waarop OPTA het toezicht invult, wordt bijna een jaar later nog eens kort en bondig opgesomd in een stuurgroepvergadering van maart 2001. Gesteld wordt dat de OPTA alleen naar uitgevers van gekwalificeerde certificaten kijkt. De OPTA houdt van al deze TTP een register bij, ongeacht of ze al dan niet bij TTP.NL aangesloten zijn. De OPTA werkt klachtgestuurd. Het onderzoek is onafhankelijk. Indien er een klacht is over de markt streeft TTP.NL ernaar dat de OPTA niet meteen tot handhaving zal overgaan, maar eerst met TTP.NL zal afstemmen: een partnership approach.

3.2.5 TTP.NL: een samenvatting

Gestart vanuit marktbehoeften
In TTP.NL werken marktpartijen en overheid samen, mede omdat er ook concrete behoeften ten aanzien van certificering en accreditatie bij marktpartijen bestaan. In de notulen van een van de vergaderingen van de stuurgroep komt deze behoefte pregnant naar voren. Een van de marktpartijen (een beoogde TTP) vraagt of er geen deadline aan het TTP.NL traject kan worden gesteld. De vertegenwoordiger van deze marktpartij geeft aan dat zijn organisatie behoefte heeft aan snelle accreditatie omdat er vraag naar is in de markt. Hij respecteert het dynamische proces en het gewenste brede draagvlak maar vraagt om een indicatie van een tijdstip waarop accreditatie kan plaatsvinden.

Opgeleverde resultaten
Tijdens de looptijd van het TTP.NL-project en in nauwe samenwerking tussen overheid en marktpartijen zijn de volgende concrete resultaten opgeleverd:

- Criteria: 3 sets, achtereenvolgend betrekking hebbend op:
  - PKI processen en techniek
  - Algemene beveiliging
  - Maatschappelijke criteria

- Een TTP.NL-schema, dat bestaat uit procedures voor toepassing van de criteria bij:
  - Certificatie
  - Accreditatie, en
  - Auditing.

- Een Guidance Document waarin de criteria eenduidig worden geïnterpreteerd.

- Een toezichtstructuur, neergelegd bij de OPTA.

Een presentatie van de eerste resultaten
Op 13 januari 2000 is door ECP.NL een bijeenkomst georganiseerd waarin de eindresultaten van het project TTP.NL (op dat moment) aan belanghebbende partijen zijn gepresenteerd en bediscussieerd. Zo'n 120 vertegenwoordigers van TTP, overheid, bedrijfsleven en andere stakeholders wonen deze middag bij. Dat er op dat moment breed draagvlak voor de resultaten van TTP.NL bestaat, blijkt uit het verslag van deze bijeenkomst. Hierin valt te lezen:

> 'Op de vraag of de aanwezigen achter de gepresenteerde resultaten staan, kwam een bevestigend antwoord. Dit heeft tot gevolg dat de ontwikkelde infrastructuur ook daadwerkelijk ingevuld zal gaan worden. ECP.NL zal in overleg met de stuurgroep uitwerken hoe zo snel mogelijk tot een invulling van de TTP-infrastructuur kan worden gekomen.'

Sinds 2000 heeft nog aanpassing en aanscherping van de criteria en het schema plaatsgevonden als gevolg van binnengekomen opmerkingen op de criteria, de ontwikkelingen rond de EU Richtlijn en de introductie van PKIoverheid als mogelijke gebruiker. Ook verschijnt in januari 2001 de rapportage van de Technische werkgroep Instrumentarium Rechtmatige Toegang. Hierin wordt gekozen voor aansluiting bij het dan reeds opgestelde TTP-certificatieschema zodat 'de benodigde technische standaarden voor het

verlenen van rechtmatige toegang onderdeel gaan vormen van de TTP-normen en TTP-certificatiecriteria.

Communicatie over resultaten en (tussen)producten
Om bekendheid te genereren met betrekking tot resultaten en de (tussen)producten heeft TTP.NL, vaak in samenwerking met andere organisaties en instellingen, diverse malen bijeenkomsten georganiseerd. In december 2000 bijvoorbeeld organiseert TTP.NL een seminar bij VNO-NCW met als titel 'Trusted Third Parties in Europees Perspectief. De laatste ontwikkelingen rond het project TTP.NL'. Ook is in april 2001 een themamiddag georganiseerd waarin de stand van zaken rondom het project TTP.NL wordt toegelicht en het rapport 'Sleutels van Vertrouwen' van de Registratiekamer werd gepresenteerd. In december 2001 volgt dan nog in samenwerking met de Europese Commissie het seminar 'De elektronische handtekening en Trusted Third Parties in Nederland' met als spreker de toenmalige staatssecretaris van het Ministerie van Verkeer en Waterstaat.

Na alle inspanningen in de werkgroepen op de verschillende deelterreinen lijkt in juni 2002 het omslagpunt in het project bereikt. De stuurgroep meldt in haar vergadering dat een TTP op het punt staat zich te laten certificeren en één organisatie zich bij de Raad voor Accreditatie heeft gemeld om zich te laten accrediteren.

3.3 Cruciale keuzes: de elektronische handtekening en PKI-overheid

3.3.1 De Richtlijn 1999/93/EG

Een verwachte verrassing
Bij de aanbieding van het Nationaal TTP-project aan de Tweede Kamer is Nederland een voorloper in Europees verband. Er wordt in andere landen wel nagedacht over TTP en het 'stoppen' van het vertrouwenslek in elektronische communicatie, maar dat is vooral gericht op het beheersen van elektronische communicatie, rechtmatige toegang en regulering van cryptografie. Ook zijn er in andere landen certificatenaanbieders actief die het gebruik van elektronische handtekeningen ondersteunen. Het Amerikaanse VeriSign, de eerste en grootste certificatenaanbieder, is op de Europese markt actief, en in België opereert bijvoorbeeld ten tijde van de totstandkoming van het Nederlandse TTP-beleid de certificatenaanbieder BelSign. In Nederland zijn in 1998 twee certificatenaanbieders: NLSign en de digitale notaris Batenburg (Van den Hof en Huydecoper, 1998).

Hoewel de (handtekening)diensten binnen de Europese Unie op dat moment verwant zijn, ziet het er dan naar uit dat de regulering van elektronische handtekeningen in de unie uiteen gaat lopen. Waar Nederland en het Verenigd Koninkrijk (waar rechtmatige toegang aan een publieke discussie wordt onderworpen) kiezen voor zelfregulering, maakt bijvoorbeeld Duitsland de keuze om als overheid zelf een PKI op te zetten en de wet aan te passen. Als gemeenschappelijk kader voor de elektronische handtekening vaardigt de Europese Commissie in het najaar van 1999 de Richtlijn 1999/93/EG uit. Ter implementatie van deze richtlijn start Nederland met de voorbereiding van een Wet elektronische handtekeningen. De uitvoerders van het TTP-beleid kunnen hier niet aan voorbij en sluiten de activiteiten van het Nationaal TTP-project (werkgroepen ter realisatie van randvoorwaarden, certificatieschema en TTP-kamer) aan op uitvoering van de richtlijn (gericht op een Wet elektronische handtekeningen).

Elektronische handtekeningen in de richtlijn
De Europese richtlijn in kwestie beoogt het gebruik van elektronische handtekeningen te vergemakkelijken en tot de wettelijke erkenning ervan bij te dragen. Door het bieden van rechtszekerheid over de juridische status van de elektronische handtekening wordt het vertrouwen in dit middel gestimuleerd, aldus de veronderstelling achter de richtlijn. Omdat uiteenlopende regels voor de wettelijke erkenning van elektronische handtekeningen en voor de accreditatie van certificatiedienstverleners belemmeringen kunnen opwerpen voor het vrije verkeer van diensten langs elektronische weg, acht de Europese Commissie geharmoniseerde regulering noodzakelijk.

EUROPESE RICHTLIJN

- Geen regulering TTP in het algemeen, maar elektronische handtekening
- Gewone en geavanceerde handtekeningen
- Juridische consequenties: geavanceerde handtekening met gekwalificeerd certificaat aangemaakt met een veilig middel

Binnen het TTP-beleid is de elektronische handtekening een van de diensten van TTP. Mede om vraagstukken rondom rechtmatige toegang (waarover de lidstaten van mening verschillen) te voorkomen en sterk ingegeven door de behoefte om belemmeringen voor een vrij verkeer van diensten te verwijderen, kiest de Europese Commissie er expliciet voor haar regulering te beperken tot de elektronische handtekening. Voor Nederland is dat niet vanzelfsprekend, omdat het bewijsrecht in Nederland een open stelsel kent waarbij de rechter bewijsmiddelen inclusief elektronische middelen beoordeelt op hun bewijskracht. Daarom zag de Nederlandse wetgever aanvankelijk de noodzaak niet om een regeling van de elektronische handtekening in de wet vast te leggen. Met de richtlijn werd Nederland echter gedwongen om de rechtsgevolgen van elektronische handtekeningen wettelijk te regelen.

Gewone en geavanceerde handtekeningen
De richtlijn onderscheidt gewone elektronische handtekeningen van geavanceerde elektronische handtekeningen en verbindt verschillende juridische consequenties aan dat onderscheid. De geavanceerde elektronische handtekening die aan bepaalde eisen voldoet (gebaseerd op gekwalificeerd certificaat, aangemaakt met een veilig middel) dient door lidstaten volledig te worden gelijkgesteld met een handgeschreven handtekening en moet in gerechtelijke procedures worden toegelaten (artikel 5 lid 1). Overige (gewone) elektronische handtekeningen mogen geen rechtsgeldigheid worden ontzegd en niet in gerechtelijke procedures worden geweigerd op grond van het enkele feit dat ze in elektronische vorm gesteld zijn, niet zijn gebaseerd op een gekwalificeerd certificaat, niet gebaseerd op een door een geaccrediteerde certificatiedienstverlener afgegeven certificaat en niet met een veilig middel zijn aangemaakt (artikel 5 lid 2). De 'gewone' elektronische handtekening omschrijft de richtlijn als elektronische gegevens die zijn vastgehecht aan of logisch zijn geassocieerd met andere elektronische gegevens en die worden gebruikt als middel voor authenticatie. Van de geavanceerde, met meer waarborgen omklede elektronische handtekening is sprake als de elektronische handtekening op unieke wijze aan de ondertekenaar is verbonden, zij het mogelijk maakt de ondertekenaar te identificeren, zij tot stand is gekomen met middelen die de ondertekenaar onder zijn uitsluitende controle kan houden en zij op zodanige wijze aan de gegevens waarop zij betrekking heeft is verbonden, dat elke wijziging achteraf van gegevens kan worden opgespoord (artikel 2, tweede lid van de richtlijn). De techniekonafhankelijke formulering is bewust gekozen om technologische ontwikkeling mogelijk te maken.

Ondanks deze techniekonafhankelijke formulering kiest de richtlijn feitelijk voor de digitale handtekening met certificaten en certificatenaanbieders, gebaseerd op a-symmetrische cryptografie. Om de private sleutel geheim te houden zijn er, volgens de Memorie van Toelichting bij de Wet elektronische handtekeningen, verschillende (combinaties van) mogelijkheden: kennis (bijvoorbeeld een pincode), bezit (smartcard met daarop de private sleutel) of een lichaamskenmerk (vingerafdruk of irisscan).

Gewone en gekwalificeerde certificaten

Een gewoon certificaat is een elektronische bevestiging die gegevens voor het verifiëren van een handtekening aan een bepaalde persoon verbindt en de identiteit van die persoon bevestigt. De hiervoor reeds genoemde gekwalificeerde certificaten zijn met meer waarborgen omkleed. In bijlage I vermeldt de richtlijn welke informatie in een certificaat moet worden opgenomen om het predikaat 'gekwalificeerd' te krijgen. Het gaat dan bijvoorbeeld om de vermelding dat het certificaat als gekwalificeerd wordt uitgegeven, identificatie en het land van vestiging van de afgevende certificatenaanbieder, de geldigheidsduur van het certificaat en eventuele beperkingen betreffende het gebruik van het certificaat. Bovendien moet de certificatenaanbieder aan bepaalde eisen voldoen die in bijlage II van de richtlijn zijn vermeld. Deze betreffen onder meer de plicht voor certificatenaanbieders om aan te tonen dat zij voldoen aan de betrouwbaarheidseisen voor het aanbieden van certificatiediensten, de plicht om veilige en betrouwbare procedures, systemen en producten te gebruiken, een informatieplicht, een bewaarplicht alsmede organisatorische en financiële eisen. Daarnaast moet een certificatenaanbieder de identiteit van de persoon voor wie een gekwalificeerd certificaat wordt afgegeven controleren en het resultaat hiervan op verifieerbare wijze vastleggen. De Europese Standaardisatie Organisaties (European Telecommunication Standards Institute – ETSI – en Comité Europeén de Normalisation – CEN -) hebben deze normen nader gepreciseerd.

Toezicht op certificatenaanbieders

De richtlijn spreekt over certificatiedienstverleners of Certification Service Providers (CSP). Dat hoeven niet perse (onafhankelijke) derde partijen te zijn, maar ook een van de handelspartijen kan certificaten uitgeven (bijvoorbeeld een groothandel), eventueel door gebruik te maken van de diensten van een TTP-dienstverlener (bijvoorbeeld een telecomprovider). Volgens artikel 3, derde lid van de richtlijn dient elke lidstaat te zorgen voor een passend systeem van toezicht op de op zijn grondgebied gevestigde certificatiedienstverleners die gekwalificeerde certificaten aan het publiek afgeven. Het verlenen van certificatiediensten mag overigens niet aan een voorafgaande machtiging worden onderworpen. Certificatiedienstverleners mogen hun diensten vrij, zonder voorafgaande machtiging, aanbieden ter bevordering van het leveren van certificatiediensten via open netwerken in de hele Gemeenschap. Volgens de Memorie van Toelichting bij de Wet elektronische handtekeningen wordt wel 'erkend dat privaatrechtelijke organisaties die initiatieven nemen en regelingen toepassen die beogen de dienstverlening te verbeteren, aan certificatiedienstverleners een passend kader kunnen bieden om hun diensten verder te ontwikkelen en het door de markt verlangde niveau van vertrouwen, veiligheid en kwaliteit te bereiken.' Voor het door Nederland ingezette beleid van vrijwillige certificering van TTP-dienstverleners is deze bepaling bij uitstek relevant. Daarbij geldt wel dat van 'deze regelingen waarbij een door de overheid geautoriseerde instantie formeel erkent dat een certificatiedienstverlener voldoet aan bepaalde eisen' gebruik mag worden gemaakt, onder voorwaarde dat dit op vrijwillige basis geschiedt. Vrijwillige accreditatieregelingen mogen worden ingevoerd en gehandhaafd, mits de voorwaarden objectief, transparant, evenredig en niet-discriminerend zijn.

Zoals hiervoor beschreven, ging het oorspronkelijke TTP-beleid nog uit van een TTP-kamer voor de vrijwillige certificering van certificatiedienstverleners en het toezicht daarop. De richtlijn doorkruist dit beleid omdat de bevoegdheden die de toezichthouder in het licht van de richtlijn krijgt volgens de Nederlandse interpretatie door een (onafhankelijke) publieke instantie moeten worden uitgeoefend. Bovendien strekt het toezicht dat de richtlijn eist zich verder uit dan de TTP-kamer, die namelijk toezicht moest gaan uitoefenen op de bij deze kamer aangemelde TTP-dienstverleners. De richtlijn eist toezicht op alle certificatiedienstverleners die certificaten afgeven aan het publiek, ongeacht de vraag of zij zich al dan niet hebben aangemeld bij een vrijwillige regeling. Omdat certificatiedienstverleners volgens de Nederlandse wetgever diensten verrichten die vaak gekoppeld zijn aan het gebruik van openbare telecommunicatienetwerken en -diensten, is het toezicht geregeld in de Telecommunicatiewet. Als instantie voor de registratie van certificatiedienstverleners wordt de OPTA aangewezen.

Betekenis voor het TTP-beleid

Bij de implementatie van de richtlijn zijn in het Nederlandse beleid keuzes gemaakt die het TTP-beleid raken. De belangrijkste daarvan zijn:

- De ETSI-standaarden voor de gekwalificeerde elektronische handtekening worden opgenomen in het TTP.NL-schema.
- Naast registratie door aanbieders van gekwalificeerde certificaten bij de OPTA blijft het beleid uitgaan van zelfregulering en vrijwillige certificatie volgens het TTP.NL-schema. Voor dat laatste wordt uitgegaan van aansluiting bij de al bestaande certificatie- en accreditatiestructuur, waarbij auditors de certificatiedienstverleners certificeren en zelf geaccrediteerd worden door de Raad voor de accreditatie.

CONSEQUENTIES RICHTLIJN

- Toezicht bij OPTA en vrijwillige certificering
- Aansluiting op internationale – Europese – normen
- Uitvoering TTP-beleid beperkt tot gekwalificeerde certificaten
- Juridische steun in de rug

Naast de keuzes die door de beleidsmakers worden gemaakt heeft de richtlijn ook meer dwingende consequenties die weinig ruimte voor keuze laten. Zo moet de elektronische handtekening wettelijk worden verankerd, waardoor de 'logica van wetgeving' zijn intrede doet in de uitvoering van het TTP-beleid. Deze logica dwingt tot het expliciet en consistent vastleggen van criteria en systemen, omdat op basis van de wet aanspraken kunnen worden gedaan. Daarnaast moeten registratie en toezicht gezien worden als de uitoefening van openbaar gezag, waardoor wordt uitgeweken naar een overheidsorganisatie.

De consequenties van de richtlijn voor het TTP-beleid, in combinatie met de keuzes die de beleidsmakers zijn gemaakt, zijn aanzienlijk:

- Door registratie bij de OPTA worden naast elkaar een systeem van toezicht en vrijwillige certificering gecreëerd. De meerwaarde van vrijwillige certificering, zeker op een Europese markt voor geavanceerde elektronische handtekeningen, vervaagt door de richtlijn. Bovendien worden de (financiële) drempels voor toegang tot de certificatiemarkt verhoogd, omdat naast de investeringen in het proces van vrijwillige certificering ook voor registratie bij de OPTA moet worden betaald als aanbieders van gekwalificeerde certificaten kiezen voor certificering.

- Er is sprake van aansluiting op internationale normen en in zekere zin ook Europese harmonisatie. Voor Nederlandse TTP-dienstverleners is de markt daardoor ineens groter geworden, maar omgekeerd hebben certificatiedienstverleners uit andere Europese lidstaten ook toegang tot de Nederlandse markt.
- Het TTP-beleid wordt in deze fase van uitvoering sterk gericht op de gekwalificeerde certificaten, de zwaarst beveiligde variant. Het TTP-beleid dat in oorsprong was opgezet als set van minimumvoorwaarden, wordt daardoor steeds meer een arrangement voor regulering van de 'maximale vorm van beveiliging'. Ook de 'logica van wetgeving', waartoe de richtlijn dwingt, draagt bij aan deze ontwikkeling.
- De (geavanceerde) elektronische handtekening wordt in de uitvoering van het TTP-beleid opgepakt als kans of breekijzer ('killer application') voor realisatie van TTP-dienstverlening. Deze heeft nu een juridische steun in de rug, is internationaal erkend en sluit sterk aan op het TTP.NL-schema. Dat de eisen of voorwaarden iets moeten worden 'opgeschroefd', is een consequentie die de beleidsmakers voor lief nemen.
- De aandacht van beleidsmakers, juristen en van het TTP.NL-project richt zich sterk op de (regelgeving rondom de) elektronische handtekening, in het bijzonder de geavanceerde variant daarvan. Van het brede TTP-concept is in deze periode weinig terug te vinden.

3.3.2 PKIoverheid

Nieuwe kansen...
Op 17 december 1999 stemt de Ministerraad in met de oprichting van de Taskforce PKIoverheid door de Minister van Grote Steden- en Integratiebeleid. Deze taskforce is interdepartementaal samengesteld en aangestuurd, met een heldere en eenduidige doelstelling:

> 'Het realiseren van een werkbare en betrouwbare infrastructuur voor PKI-diensten die voorziet in een vastgesteld beveiligingsniveau voor de communicatiebehoefte van de overheid en transparant is voor de gebruikers.'

De taskforce is onderdeel van ICTU (ICT-Uitvoeringsorganisatie) en maakt als zodanig deel uit van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, vanuit het idee dat deze de afnemers van PKI binnen de overheid coördineert en vertegenwoordigt. Het algemene doel van de taskforce is ook concreter geformuleerd in het instellingsbesluit. Zo wordt in 2002 een vanzelfsprekend gebruik beoogd van elektronische handtekeningen met een hoge graad van betrouwbaarheid voor communicatie door en met de overheid. Voor 2000 zou een beperkte PKI moeten worden ingericht voor laag-risico communicatie en transacties. Volgens datzelfde instellingsbesluit spreekt het daarbij vanzelf dat de beoogde PKI-infrastructuur voldoet aan de randvoorwaarden in de notitie TTP-project. Het ligt dan ook voor de hand dat de activiteiten van de taskforce in nauwe samenhang en afstemming met het ministerie van Verkeer en Waterstaat plaatsvinden. In de beschrijving van het TTP.NL-traject in paragraaf 3.2.3 hebben we enkele belangrijke afstemmingsmomenten benoemd.

PKIoverheid kiest voor een infrastructurele aanpak om te voorkomen dat 'ongecoördineerde en inefficiënte PKI-eilanden ontstaan binnen de overheid' (Taskforce PKIoverheid, 2002). Het model van de PKI voor de overheid is volgens deze taskforce gebaseerd op een aantal uitgangspunten:

- Het aantal elektronische handtekeningen per gebruiker moet worden geminimaliseerd.
- Er moet een generiek betrouwbaarheidsniveau komen met een elektronische handtekening conform de Europese richtlijn (zodat een digitale sleutelbos wordt voorkomen).
- Certificaten zijn persoonsgebonden.
- Er wordt gebruik gemaakt van een smartcard als drager voor de certificaten en sleutels.
- De kaart is geschikt voor gebruik van de functies (1) elektronische identificatie/authenticatie, (2) zetten van een digitale handtekening, (3) verzorgen van vertrouwelijkheid. Voor elke functie wordt een eigen certificaat en sleutelpaar opgenomen zodat er drie certificaten op de kaart aanwezig zijn.
- Gebruik van een hiërarchische structuur, opgedeeld in drie domeinen, waardoor interoperabiliteit mogelijk is. Deze domeinen zijn: overheid-overheid, overheid-bedrijfsleven en overheid-burger.
- Er moet een hoogwaardig uitgifteproces worden ingericht van de PKI-kaart met persoonlijke verificatie van de identiteit van de persoon.

Dit betekent dat er een certificatie-infrastructuur moet worden gerealiseerd die zorgt voor uitgifte, controle en beheer van betrouwbare certificaten en sleutelparen. Ook moeten er PKI-aanpassingen worden gedaan bij gebruiker en ontvanger, niet alleen technisch maar ook organisatorisch en misschien zelfs juridisch. De taskforce wil zelf geen certificaten uitgeven, maar verwacht en wil dat commerciële partijen en overheidsinstellingen dit doen. PKIoverheid zet de zogenaamde 'root' op, de basis van een PKI-boomstructuur. Of overheidsinstellingen zelf als certificatiedienstverlener willen opereren (en daarbinnen taken uitbesteden) dan wel certificatiedienstverleners willen inhuren, mogen ze zelf bepalen. Een en ander moet wel passen binnen de boomstructuur en de eigen 'root' van PKIoverheid. De taskforce beschrijft dan ook aan welke eisen de 'sub-PKI-systemen' moeten voldoen.

EEN LAUNCHING CUSTOMER?

- Taskforce voor betrouwbare infrastructuur voor PKI-diensten van overheid
- Infrastructurele aanpak, voorkomen PKI-eilanden binnen overheid
- Europese richtlijn als vertrekpunt

De afstemming van het werk van de taskforce en het TTP-beleid vindt plaats in een speciaal daarvoor opgerichte werkgroep (zie paragraaf 3.2.3). In het oorspronkelijke TTP-beleid was voorzien dat de overheid aansluiting bij de vrijwillige certificatie van TTP-dienstverleners door de TTP-kamer zou bevorderen door dit als eis te stellen voor dienstverlening aan de overheid. In de uitvoering van het TTP-beleid wordt de taskforce PKI-overheid dan ook gezien als een nieuwe kans. De overheid zou als een 'launching customer' de markt voor TTP-dienstverlening een stimulans kunnen geven en tegelijkertijd de voorwaarden creëren voor e-government in een PKI-omgeving. Niet alleen sloot het PKI-initiatief aan op het TTP-beleid, ook andersom (van PKIoverheid naar TTP-beleid) is expliciet uitgegaan van aansluiting en afstemming.

...met een eigen invulling

Met de entree van de taskforce PKIoverheid in de uitvoering van het Nationaal TTP-project doet zich dus een voor de hand liggende kans voor op realisatie van een markt voor TTP-dienstverlening. Een (of een aantal) grote klant(en) dient (dienen) zich aan, met veel transacties en hoge eisen aan de veiligheid en betrouwbaarheid. Toch verloopt de afstemming niet vanzelfsprekend. Omdat op dat moment een precieze invulling van de eisen van de Europese richtlijn ontbreekt, ontstaan verschillende interpretaties en invullingen. De invulling van PKIoverheid stond overigens niet haaks op de ontwikkeling in het TTP.NL-proces, omdat beide geleid werden door de Europese richtlijn. Er zijn wel verschillen. Zo stelt PKIoverheid dat de richtlijn meerdere sleutels/certificaten afdwingt omdat de sleutel voor de elektronische handtekening alleen voor deze functie mag worden gebruikt. Dat betekent dat op de smartcard voor de afzonderlijke functies drie afzonderlijke certificaten en sleutelparen worden opgenomen. In het op dat moment gebruikelijke model moet per certificaat worden betaald, waardoor de kosten worden opgedreven. Ook wil de taskforce dat de zogenaamde 'revocation list' (de lijst van niet meer geldige certificaten) om de vier uur wordt bijgewerkt, in plaats van de gebruikelijke vierentwintig uur (zie Van Rij, 2002). Feitelijk is dit een extra eis. Hoewel de keuze voor smartcards en smartcardreaders niet in de Europese richtlijn is voorgeschreven, voldoet feitelijk alleen deze oplossing aan de eisen in de richtlijn. Dat is echter een ingrijpende en dure oplossing waardoor een grootschalige 'uitrol' van PKI niet eenvoudig te realiseren is. Tenslotte is aansluiting op de 'root' niet vanzelfsprekend, aldus Van Rij (2002). Volgens haar beschikken de meeste TTP-dienstverleners over een 'root' die volgens een eigen systeem werkt en in de meeste gevallen niet hetzelfde zal zijn als het systeem van de 'overheidsroot'. Aansluiting van de al bestaande 'sub-root' aan de 'root' van de overheid is dan lastig. De technische oplossing daarvoor (een nieuwe 'root' installeren die wel interoperabel is met de 'root' van de overheid) maakt de operatie duurder en omslachtiger.

Vooralsnog lege handen

Toen de grootschalige uitrol volgens het model PKIoverheid niet met de aangevraagde ICES-gelden kon worden gefinancierd, heeft de taskforce gezocht naar business-cases binnen de overheid (waar en onder welke omstandigheden loont invoering van een PKI-systeem?). In 2002 presenteert de taskforce haar definitieve conclusies. Dat onderzoek was gericht op de functies elektronische identificatie/authenticatie, de digitale handtekening en het verzorgen van vertrouwelijkheid. De conclusie van de taskforce is dat de businesscase voor het gebruik van PKI verschilt per functie en per domein (zie Taskforce PKIoverheid, 2002). Voor het TTP-beleid is deze conclusie bij uitstek interessant, omdat het een 'marktverkenning' betreft bij een interessante 'afnemer' met grote aantallen transacties.

De taskforce concludeert dat PKI-technologie voor verschillende functies in bepaalde omstandigheden zinvol is:

- Per PKI-functie:
    - De businesscase voor vertrouwelijkheid wordt bepaald door de uitkomsten van de risicoanalyse. Als dit wijst in de richting van de toepassing van PKI blijkt de kosten/baten afweging van minder belang.
    - De businesscase voor de elektronische handtekening wordt vooral bepaald door de baten die in de backoffice van de ontvanger kunnen worden geboekt in efficiëntie en administratieve lastenverlichting. Het breakeven-punt voor een PKI volgens het model van de PKI voor de overheid wordt bereikt bij ca. 15-20 transacties per gebruiker per jaar.

- De businesscase voor de elektronische identificatie ligt vooral in gemak en toegang tot beveiligde, privacygevoelige gegevens. Gebruikers geven aan dit een aantrekkelijke functie te vinden, maar lijken vooralsnog niet bereid hier veel geld aan te besteden en het is in 2002 nog moeilijk om voor deze functie een sluitende businesscase te maken.

- Per domein:

  - Domein overheid-overheid: PKI kan een bijdrage leveren aan veilige elektronische communicatie binnen de overheid, met name voor de departementen van Justitie, Defensie, Buitenlandse Zaken en Binnenlandse Zaken. Toch wordt bij deze ministeries het toepassen van een PKI volgens het model PKIoverheid niet overwogen 'omdat niet duidelijk is welk niveau van beveiliging hiermee kan worden behaald', aldus de taskforce.
  - Domein bedrijfsleven-overheid: met elektronische dienstverlening kunnen administratieve lasten worden bespaard, en hier ziet de taskforce dan ook de toepassing van PKI volgens het model als het meest kansrijk om tot implementatie te komen.
  - Domein burger-overheid: omdat het aantal interacties tussen 'normale' burgers en de overheid is afgenomen, is er volgens de taskforce in 2002 nauwelijks een overheidsdienstenpakket te bedenken dat voldoende elektronische transacties oplevert om een PKI volgens het voorgestane model te rechtvaardigen, nog los van de ingrijpende aanpassing die dat zou vergen van de organisaties die dit zouden introduceren. Bij grootschalig gebruik wordt dan ook doorgaans voor goedkopere, minder streng beveiligde oplossingen gekozen en 'grootschalige invoering van PKI volgens het model van de PKI voor de overheid wordt nog vrijwel niet overwogen', aldus de taskforce.

OVERHEID: VOORAL ALTERNATIEVE TECHNIEKEN

- Standaard-internetprotocol SSL
- Crypto-boxen
- PIN-codes en aangiftecode
- Varianten van gebruikersnaam/PINcode-combinatie

De alternatieven waarover de taskforce spreekt, zijn voor de afzonderlijke functies verschillend:

- Voor vertrouwelijkheid wordt volgens de taskforce door de overheid vaak het 'standaard'-internetprotocol SSL ingezet. Ook worden 'crypto-boxen' gebruikt om verbindingen tegen afluisteren te beveiligen.
- Voor de elektronische handtekening worden allerlei 'PIN-code' oplossingen toegepast, die in combinatie met een op cryptografie gebaseerd algoritme worden gebruikt. Hiermee kan de berekening van de unieke berichtcode worden uitgevoerd. Andere vormen zijn de aangiftecode-systematiek (IB-aangiftediskette), GIN/TAN-codes (Postbank) en speciale calculators.
- Voor elektronische identificatie worden veelal varianten van gebruikersnaam/PINcode-combinaties gebruikt. Ook kunnen gegevens die alleen bij

de gebruiker bekend zijn (bijvoorbeeld combinatie van SOFI-nummer en paspoortnummer of geboortedatum) als code worden gebruikt.

Recent heeft ook een aantal grote uitvoeringsorganisaties binnen de overheid van zich laten horen (Belastingdienst e.a., 2003). In het manifest *Innovatie in uitvoering* roepen ze op de uitvoering efficiënter te organiseren en meer te investeren in innovatie. Uitgangspunt daarbij is een gemeenschappelijk authenticatiemechanisme voor klantcontacten. De manifestpartijen bepleiten dan ook stapsgewijze invoering van een generiek regime voor elektronische identiteitskaarten, elektronische identificatie en elektronische handtekeningen voor burgers en bedrijven (een nationale authenticatievoorziening).

Betekenis voor het TTP-beleid

Bij de keuze voor een taskforce PKIoverheid leek het voor de hand te liggen afstemming te zoeken met het TTP-beleid. In het TTP-beleid speelde PKI immers een sleutelrol, en de overheid zou als 'launching customer' wel eens de doorbraak kunnen veroorzaken voor realisatie van een markt voor TTP-dienstverlening. Hier was een grote klant met veel transacties en (potentiële) certificaten, die hoofdzakelijk uitging van het niveau van de Europese richtlijn. Uiteindelijk bleek overigens een TTP.NL-certificatie of equivalent daarvan voldoende. Dat equivalent is van belang omdat anders belemmeringen zouden worden opgeworpen voor potentiële TTP-dienstverleners uit andere landen. Interessant is bovendien nog dat bij de aanbesteding van de 'overheidsroot' TTP.NL-certificering niet expliciet als eis is opgenomen door de taskforce, overigens tegen de wens van het Ministerie van Economische Zaken in (Van Rij, 2002). Volgens de taskforce heeft de TTP.NL-norm uitsluitend betrekking op de uitgifte en het beheer van gekwalificeerde certificaten en niet op 'roots'.

De in theorie voor de hand liggende afstemming tussen PKIoverheid en het TTP-beleid heeft in de praktijk nog geen resultaat opgeleverd. PKIoverheid bleek bij nadere analyse voor het brede TTP-concept (en daarbinnen de geavanceerde handtekening) geen 'businesscase' te kunnen ontwaren bij de overheid. Deels wordt dat geweten aan de strenge eisen en het uniforme betrouwbaarheidsniveau (Van Rij, 2002).

Voor het TTP-beleid als zodanig is de betekenis van PKIoverheid beperkt geweest. Uiteindelijk heeft PKIoverheid het TTP.NL-schema overgenomen, maar daarvoor nog geen businesscase binnen de overheid aangetroffen. Dat is een interessant gegeven. Voor het eerst is namelijk bij een grote gebruiker (de overheid) met veel certificaten (maar betrekkelijk weinig transacties per certificaat) systematisch de businesscase vanuit een breed TTP-concept onderzocht. De conclusie daaruit is dat er wel mogelijkheden zijn voor PKI-gebruik, maar die zijn beperkt tot het domein overheid-bedrijfsleven en dan ook nog tot specifieke functies. In dit opzicht is de betekenis van PKI-overheid voor het TTP-beleid vooral die van 'leerzame ervaring'. De tot dan toe ontbrekende schakel (de gebruiker) in een technisch betrouwbaar en geloofwaardig beleid is betrokken in de uitvoering ervan. Dat heeft vooralsnog niet een bloeiende markt voor TTP-dienstverlening opgeleverd met de overheid als klant. Deze leerervaring heeft volgens sommigen betrekkelijk veel tijd en moeite gekost; zij vragen zich af of in de uitvoering van het TTP-beleid de verbinding met PKIoverheid achteraf gezien wel zo gelukkig is geweest. Volgens Van Rij (2002: 81) heeft deze verbinding ertoe geleid dat het beleidsdoel van het TTP-beleid verder is verschoven. In plaats van het creëren van een set minimumvoorwaarden voor TTP-dienstverlening en een toezichtstructuur zijn het gebruik van de elektronische handtekening en certificering doelen op zich geworden. Het gaat er de beleidsmakers niet meer alleen om de randvoorwaarden te creëren waaronder de markt voor

TTP-dienstverlening tot stand kan komen, maar om de overheid als 'launching customer' in te zetten en zo de doorbraak voor de totstandkoming van deze markt te veroorzaken.

3.4 Belendende ontwikkelingen

In een brief van de Minister van Binnenlandse Zaken en Koninkrijksrelaties aan de Tweede Kamer bij het vaststellen van de begrotingsstaat van het Ministerie voor het jaar 2003 wordt melding gemaakt van twee voor het TTP-beleid relevante ontwikkelingen. Ten eerste het besluit om de elektronische identiteitskaart niet grootschalig uit te rollen en ten tweede de beperking van de uitrol van PKI naar bepaalde domeinen.[11]

Geen grootschalige uitrol eNIK
Het Ministerie van BZK werkt vanaf 2000 aan de ontwikkeling van een elektronische variant van de Nederlandse identiteitskaart (eNIK). Veel respondenten van de in het kader van dit evaluatieonderzoek gehouden interviews geven aan deze kaart te beschouwen als belangrijke ontwikkeling. Dit omdat deze op termijn zeker bijdraagt aan het vervolmaken van de TTP-infrastructuur of in ieder geval het gebruik ervan. Na uitrol zouden alle burgers immers beschikken over een drager waarmee elektronische identificatie mogelijk is.
Het ministerie heeft in 2001 en 2002 een haalbaarheidsonderzoek uitgevoerd naar mogelijke invoering van de eNIK. In dit kader zijn onder andere praktijkproeven gedaan in Delft en Amsterdam Oud Zuid. Het resultaat van dit onderzoek was dat er in onvoldoende mate elektronische diensten beschikbaar waren waarvoor elektronische identificatie noodzakelijk is. Daarnaast bleek de contactfrequentie tussen burger en overheid bij veel diensten laag. Tevens werden praktische belemmeringen geconstateerd, zoals de mate waarin burgers ondersteund moeten worden om gebruik te kunnen maken van de elektronische identiteitskaart en de relatief hoge kosten. Deze uitkomsten, gecombineerd met het feit dat de beoogde financiële dekking voor een investeringsimpuls ontbreekt, heeft tot de conclusie geleid dat een grootschalige uitrol van PKI en de elektronische identiteitskaart in het domein overheid-burger op dat moment niet haalbaar is.
Gezien de overwegingen rond de relatie overheid en burger, worden de inspanningen ten aanzien van de uitrol van PKI geconcentreerd bij de domeinen overheid-bedrijfsleven en overheid-overheid.

KWINT
Ruim een jaar na de presentatie van het Nationaal TTP-project aan de Tweede Kamer wordt in dezelfde kamer de Motie-Wijn aangenomen.[12] Deze motie sluit aan op een reeds in *De Digitale Delta* toegezegde verkenning naar de kwetsbaarheden op internet, en vraagt om daarbij ook andere vitale infrastructuren (zoals energie, financiële dienstverlening, e.d.) te betrekken. Er zou een sectoroverschrijdend plan inzake de bescherming van vitale infrastructuren opgesteld moeten worden. Reeds in juli 2001 reageert het kabinet op deze motie met de nota *Kwetsbaarheid op internet* (KWINT). Een van de kwetsbaarheden op internet betreft de integriteit van elektronische gecommuniceerde en opgeslagen informatie, waarmee in deze nota wordt gedoeld op 'de zekerheid omtrent de identiteit van de persoon of organisatie waar de informatie van afkomstig is en de correctheid van de informatie zelf (niet gewijzigd of aangevuld).' Ter waarborging van de integriteit van informatie wordt een rol gezien voor TTP, aldus de nota. Ten aanzien van TTP kunnen echter ook kwetsbaarheden bestaan. De nota wijst op een zogenaamde 'DoS-aanval' (Denial of Service) of een hack op

[11] *Kamerstukken II*, 2002-2003, 26.600 VII, nr. 7
[12] *Kamerstukken II*, 2000-2001, 26 643, nr. 20.

een TTP en het verlies aan vertrouwen in een TTP. TTP-dienstverlening met een hoog niveau van betrouwbaarheid is volgens de nota van belang om te voorkomen dat de integriteit van informatie wordt bedreigd. In dit opzicht is de TTP gekarakteriseerd als een kritische internetcomponent. De overheid heeft dan ook niet alleen belang bij TTP-dienstverlening vanuit het oogpunt van het stimuleren van e-business en e-government, maar het (oorspronkelijke) belang van informatiebeveiliging vormt ook een zelfstandig argument vóór het TTP-concept als instrument dat een van de kwetsbaarheden van het Internet kan aanpakken.

3.5 Responsiviteit van het TTP-beleid: een evaluatief oordeel

Twee verhalen

Dat het beleid responsief is geweest, gericht op het actief inspelen op ontwikkelingen die zich in het beleidsveld voordoen en op reacties in dat veld, laat zich makkelijk vaststellen. Dit hoofdstuk is daarvan getuige. De uitvoering van het TTP-beleid wordt gekenmerkt door een sterk ontwikkeld omgevingsbewustzijn, gericht op het waarnemen en benutten van kansen die zich voordoen om het TTP-beleid gerealiseerd te krijgen. Het vaststellen dat (de uitvoering van) het beleid responsief is geweest staat niet gelijk aan het beoordelen ervan. Centrale vraag voor de beoordeling is of het responsief uitvoeren (en bijstellen) ook verstandig is geweest in het licht van de ontwikkelingen en omstandigheden van toen en uiteraard in het licht van het oorspronkelijk geformuleerde beleidsdoel. In extremo laten zich twee verhalen vertellen over de aansluiting van het TTP-beleid bij de elektronische handtekening en PKIoverheid.

Richtlijn en PKIoverheid als zegen

Laten we beginnen met het positieve verhaal. In dat verhaal komt de Europese richtlijn als geroepen. Het is de juridische steun in de rug voor het beleid. In hoofdzaak sluit de richtlijn prima aan op de gekozen lijn van standaardisatie en het uitwerken van randvoorwaarden in een certificatieschema. Het wordt weliswaar wat duurder en strenger door bijvoorbeeld het toezicht van de OPTA, maar daarmee wordt alleen maar beter tegemoet gekomen aan de behoefte aan vertrouwen zoals deze in de markt leeft. Bovendien is aansluiting op internationale normen gegarandeerd en heeft Nederland een lastige richtlijn geïmplementeerd zonder het bestaande wettelijke stelsel te doorkruisen. Dat de richtlijn beperkt is tot de elektronische handtekening, is geen probleem. Zelfs al zou er voor andere vormen van TTP-dienstverlening zoals deze in het oorspronkelijke beleid werden gezien geen markt blijken te zijn, dan is het TTP-beleid in ieder geval nuttig geweest, omdat het de implementatie van Europese regelgeving heeft vergemakkelijkt. Met die implementatie was immers door de reeds in gang gezette activiteiten in het kader van TTP.NL al een start gemaakt nog voor de richtlijn werd uitgevaardigd.

Ook PKIoverheid is in dit verhaal een zegen. Het is een testcase voor de potentiële markt voor TTP-dienstverlening en voorziet in een systematische verkenning van deze markt. Omdat het vooral een 'papieren' verkenning is zonder grootschalige experimenten met PKI-systemen, was deze betrekkelijk goedkoop. Het systematische karakter van de verkenning geeft precies

aan waarom en in welke omstandigheden welke vormen van TTP-dienstverlening kans maken. Weliswaar zijn in de verkenning ook 'onderhandelingselementen' geslopen die het TTP-beleid doorkruisten, maar uiteindelijk is het effect daarvan beperkt geweest.

Richtlijn en PKIoverheid als Trojaanse paarden
Dezelfde ontwikkelingen kunnen ook anders worden geduid. In dat verhaal is met de aansluiting van het TTP-beleid op de uitvoering van de Europese richtlijn ten aanzien van de elektronische handtekening het paard van Troje binnen gehaald, omdat de eisen zo zijn opgeschroefd dat TTP-dienstverlening zich uit de markt heeft geprijsd. Bovendien is een hybride structuur van toezicht en vrijwillige certificering gecreëerd die de prijs verder heeft opgedreven en waarvan de zin betwijfeld mag worden in het licht van een Europese markt voor elektronische handtekeningen. Bovendien heeft de elektronische handtekening de uitvoering van het brede TTP-beleid versmald tot een van de mogelijke diensten, namelijk een een gekwalificeerd certificaat. De versmalling van de aandacht in het beleid heeft zich voorgedaan ten aanzien van de TTP-functies (beperkt tot elektronische handtekening) en ten aanzien van het beveiligingsniveau (het hoogste niveau). Daardoor zijn andere functies en beveiligingsniveaus naar de achtergrond van het beleid gedrongen.
Met PKIoverheid is in dit verhaal iets vergelijkbaars gebeurd. Ook hier is een kans gegrepen die zich later tegen het beleid heeft gekeerd. Hoge eisen, maar er stond geen klandizie tegenover. Met PKIoverheid is in dit verhaal een 'schijnklant' binnengehaald, die wel strenge eisen formuleerde maar niet de 'echte' klanten vertegenwoordigde en later door deze 'manifestpartijen' is gepasseerd. Veel energie en geld is door de afstemming verloren gegaan en het heeft niets opgeleverd. Bovendien heeft het de aandacht afgeleid van al die potentiële klanten van TTP-dienstverlening buiten de overheid en misschien zelfs binnen de overheid.

Het ware verhaal...?
Beide verhalen laten zich tot op zekere hoogte onderbouwen. Bezien vanuit de oorspronkelijke doelstelling van het TTP-beleid en vanuit ontwikkelingen in de omgeving is zowel de aansluiting op de implementatie van de richtlijn als de verbinding met PKIoverheid in het licht van de toenmalige omstandigheden logisch. De richtlijn moest sowieso worden geïmplementeerd en de implementatie sloot goed aan bij door het TTP-beleid ingezette lijn, namelijk standaardisatie en uitwerking van een certificatieschema. Ook de verbinding met PKIoverheid is logisch: er was immers gekozen voor de PKI-technologie ter ondersteuning van e-government en PKI was ook de techniek waarop het TTP-concept rustte. Er is dus alert gereageerd op de omstandigheden en veranderingen in de beleidsrelevante omgeving..

Toch zijn er wel enkele kanttekeningen bij beide keuzes te maken:

- De implementatie van de richtlijn en de verbinding met PKIoverheid zuigen in zekere zin de uitvoering van het hele TTP-beleid op zoals dat oorspronkelijk was uitgewerkt. Omdat de uitwerking van het TTP.NL-schema samen gaat met vormgeving van de elektronische handtekening en de invulling van PKIoverheid wordt het TTP.NL-project ook sterk door deze ontwikkelingen geleid. De oorspronkelijke beleidstheorie raakt daardoor op de achtergrond; er wordt meer prioriteit gegeven aan het boeken van concreet resultaat dan aan het neerzetten en implementeren van het oorspronkelijke TTP-concept of dit expliciet te herzien in het licht van de nieuwe ontwikkelingen. Overigens is dit voor een deel (de geavanceerde elektronische handtekening) een afgedwongen keuze geweest door de Europese richtlijn. Desondanks heeft daardoor wel 'aandachtsversmalling' plaatsgevonden, waardoor mogelijk kansrijke elementen uit het oorspronkelijke TTP-beleid (stimulering van het gebruik van TTP-

dienstverlening door voorlichting en onderwijs, private markten voor lagere beveiligingsniveaus, enzovoort) nog niet zijn verkend.
- Daarbij komt de vraag in welke mate de beide ervaringen (richtlijn en PKIoverheid) expliciet en systematisch zijn benut als leermoment voor het TTP-beleid. Voor wat betreft de richtlijn valt te denken aan de transformatie van de 'set minimumvoorwaarden' uit het oorspronkelijke TTP-beleid in 'het hoogste beveiligingsniveau' van de geavanceerde handtekening, maar ook aan de vraag of de idee van vrijwillige certificering niet een andere betekenis zou moeten krijgen in het licht van de Europese richtlijn. PKIoverheid als leermoment voor het TTP-beleid roept bijvoorbeeld de vraag op in welke omstandigheden en voor welke functies om welke redenen het oorspronkelijke (openbare) TTP-concept eigenlijk wel valide is: wat is de waarde van het TTP-concept, gezien de businesscase die de taskforce PKIoverheid heeft verkend?

Beide verhalen laten zich dus beargumenteren. Tegelijkertijd is het nog te vroeg om definitief een keuze te maken voor een van de verhalen. De businesscase voor PKI volgens het model van de taskforce kan veranderen, bijvoorbeeld als zich op grote schaal problemen voordoen met lagere beveiligingsniveaus. Bovendien kunnen zich nieuwe kansen voordoen, zoals de elektronische identiteitskaart.[13] Ook is de markt voor elektronische handtekeningen nog in ontwikkeling, neemt het aantal gebruikers geleidelijk toe en is het gebruik ervan nog maar beperkt gestimuleerd. Naarmate meer combinaties met andere applicaties (bijvoorbeeld betaling) worden ontwikkeld, zou ook de markt voor TTP-dienstverlening kunnen opleven. Of dat ook de markt is die de beleidsmakers in 1999 voor ogen stond, is de vraag. De ervaringen met PKIoverheid wijzen niet in deze richting. Welke gevolgen dit zou moeten hebben voor de toekomst van het TTP-beleid, analyseren we in hoofdstuk vijf.

[13] Zo wordt momenteel in België een elektronische identiteitskaart uitgerold met twee sleutelparen (voor authenticatie en voor de elektronische handtekening), met de expliciete bedoeling deze kaart ook voor bijvoorbeeld bancaire diensten te gebruiken.

4. Effectiviteit en efficiëntie 'beleid uitgevoerd, doel bereikt, maar toch...'

4.1 Inleiding

In hoofdstuk twee hebben we het TTP-beleid ontrafeld zoals het oorspronkelijk is opgezet. Dat beleid beoogde de totstandkoming van openbare TTP-dienstverlening te stimuleren door regulering en standaardisatie. Verondersteld werd dat deze openbare TTP-dienstverlening een hefboom zou zijn voor de verdere ontwikkeling van elektronische handel en elektronische overheidsdienstverlening. In hoofdstuk drie hebben we gezien dat de uitvoering van het beleid actief ter hand is genomen. De activiteiten die in het beleid zijn aangekondigd zijn betrekkelijk snel uitgevoerd, maar tijdens de uitvoering deden zich twee cruciale ontwikkelingen voor: de Europese richtlijn over elektronische handtekeningen en een PKI-behoefte bij de overheid. Niet alleen is in het TTP-beleid aangesloten op deze ontwikkelingen, de uitvoering is er zelfs primair door geleid. Dit heeft gevolgen voor het evaluatieonderzoek. Het eenvoudig leggen van de huidige situatie naast het oorspronkelijk geformuleerde doel om de effectiviteit van het beleid vast te stellen is immers niet meer reëel. Toch ontkomt een evaluatieonderzoek niet aan een analyse van de effectiviteit van het beleid. We beschrijven daarom in dit hoofdstuk eerst de feitelijke resultaten van het beleid zoals dat in de uitvoering gestalte heeft gekregen.

Daarna analyseren we de effectiviteit van het TTP-beleid. Dat doen we door eerst de feitelijke resultaten van het beleid in het licht te plaatsen van het oorspronkelijk geformuleerde beleid (hoe sluit het resultaat aan op het oorspronkelijk geformuleerde doel?). Vervolgens kijken we naar het oorspronkelijk geformuleerde beleidsdoel van het TTP-beleid en leggen we dit naast de huidige situatie (is het doel bereikt?). Tenslotte reflecteren we op basis hiervan op de effectiviteit (wat is de bijdrage van het beleid geweest aan doelrealisatie?) en de efficiëntie (hoe is de verhouding tussen doel en middelen?) van het TTP-beleid.

4.2 Feitelijke resultaten van het TTP-beleid

Huidige stand van zaken

Als we de huidige situatie bekijken, dan nemen we feitelijke resultaten van het TTP-beleid en de manier waarop dat in de uitvoering is opgepakt waar in tenminste drie domeinen. Ten eerste is er op het gebied van *wet- en regelgeving* inmiddels het een en ander tot stand gekomen. Daarnaast bestaat er een organisatorische infrastructuur, waarmee de wet- en regelgeving kan worden uitgevoerd. We beschrijven deze als *bestuurlijk-organisatorische infrastructuur*. Tot slot zijn er binnen deze structuur partijen actief die diensten aanbieden en afnemen. Dit is de *markt voor TTP-dienstverlening*. Deze markt bestaat slechts voor een klein deel uit gecertificeerde dienstverleners, maar voor een veel groter deel uit TTP-dienstverleners die wel passen binnen het oorspronkelijke TTP-

FEITELIJKE RESULTATEN

- Wet- en regelgeving
- Bestuurlijk-organisatorische infrastructuur
- Markt voor TTP-dienstverlening

concept maar geen gekwalificeerde certificaten aanbieden. Om een goed beeld van de huidige stand van zaken te schetsen nemen we deze wel mee in de feitelijke resultaten.

Wet- en regelgeving

Een van de belangrijkste lijnen in het oorspronkelijke TTP-beleid is het ontwikkelen van een zogenaamd certificatieschema voor openbare TTP-dienstverleners. Verondersteld werd dat met de totstandkoming van zo'n schema aanbieders zouden toetreden tot de markt voor TTP-dienstverlening omdat ze met een 'certificering op zak' de noodzakelijke betrouwbaarheid konden laten zien die klanten over de streep zou trekken. Later is het certificatieschema aangesloten op de uitvoering van de Europese richtlijn met betrekking tot elektronische handtekeningen (in het bijzonder de geavanceerde elektronische handtekening). In eerste instantie richtte de normstelling in het certificatieschema zich op nationale normen; later zijn de Europese (ETSI) normen overgenomen in het TTP.NL-schema. Dit schema is een uitwerking van hoe met de Europese normen omgegaan moet worden. Het schema is de leidraad op basis waarvan aanbieders van gekwalificeerde certificaten zich kunnen laten certificeren.[14] Ook heeft OPTA uitgesproken in het toezicht op certificatiedienstverleners rekening te houden met het certificatieschema.

Parallel aan het proces dat is uitgemond in het certificatieschema liep de totstandkoming en invoering van de wet Elektronische Handtekeningen. Met de invoering van deze wet[15] in 2003 zijn gekwalificeerde elektronische handtekeningen gelijkgesteld aan handgeschreven handtekeningen. De geavanceerde elektronische handtekening die gebaseerd is op een gekwalificeerd certificaat en is gegenereerd met een veilig middel wordt juridisch dus gelijk gesteld met een handgeschreven handtekening. De wet regelt tevens de aansprakelijkheid van certificatiedienstverleners die gekwalificeerde certificaten afgeven aan het publiek en het toezicht op deze certificatiedienstverleners. Een gewone elektronische handtekening kan door de rechter als ook worden geaccepteerd. Vanuit de wet is er is dus geen prikkel om alleen met gecertificeerde instellingen in zee te gaan.

Voor een gekwalificeerde handtekening gelden strenge normen, onder andere dat het certificaat alleen mag worden uitgereikt als de rechtmatige houder zich 'face to face' heeft geïdentificeerd, de private sleutel onuitleesbaar is opgeslagen (vaak op een smartcard maar tegenwoordig kan dit ook anders en goedkoper) en de organisatie aan een groot aantal organisatorische en technische eisen voldoet.

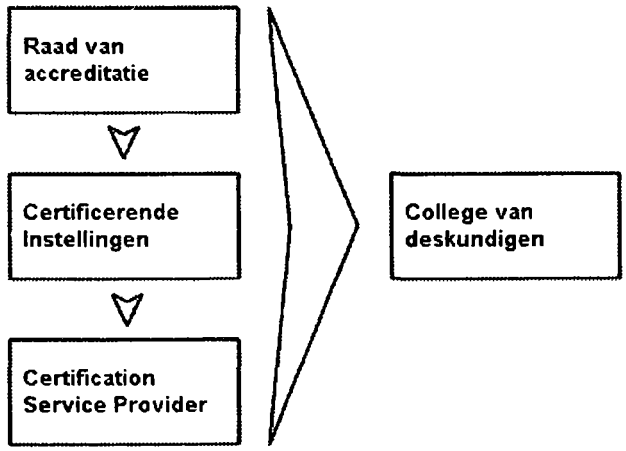
De registratie voor gecertificeerde TTP-dienstverleners gebeurt bij de OPTA. OPTA kent twee vormen van registreren. In de eerste vorm van registratie wordt er door een externe partij een audit uitgevoerd. De aanbieder kan zich dan hier laten certificeren. Als deze certificering is gedaan wordt door de OPTA slechts een marginale toets uitgevoerd. De tweede vorm van registratie is registratie zonder certificering. In dat geval dient de dienstverlener een aanvraagformulier bij de OPTA in. De OPTA controleert dan of de aanbieder aan de gestelde eisen voldoet.

[14] Dit schema staat bekend als het *Scheme for Certification of Certification Authorities against ETSI T 101 456* en wordt uitgegeven door ECP.NL.

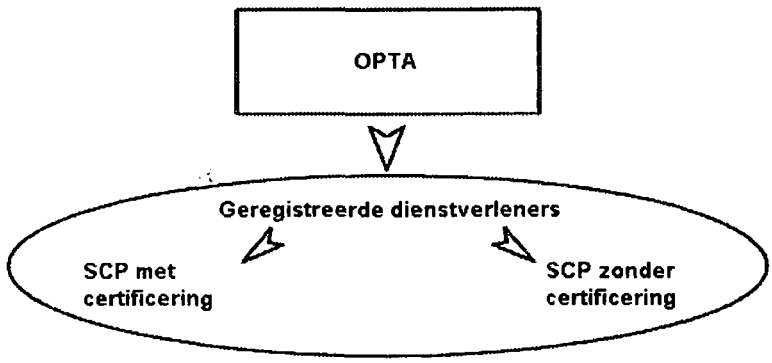
[15] Met de Wet elektronische handtekeningen gaat andere nieuwe regelgeving en veranderingen in bestaande regelgeving samen. Zo is er een *Besluit Elektronische handtekeningen* (Stb. 2003, 200), een *Ministeriële Regeling Elektronische handtekeningen* (Stcrt. Nr. 88, dd 8 mei 2003), een *Beleidsregel aanwijzing gecertificeerde instellingen* (Stcrt. Nr. 88, dd 8 mei 2003) en een *Wijziging van de Ministeriële Regeling Vergoedingen OPTA 2003* (Stcrt. Nr. 113, dd 17 juni 2003).

Bestuurlijk-organisatorische infrastructuur
Naast het certificatieschema is ook een bestuurlijk-organisatorische infrastructuur gecreëerd waarmee het TTP-beleid (in het bijzonder de Wet elektronische handtekeningen) kan worden uitgevoerd. Deze structuur is niet alleen op papier opgezet, maar door de certificering en registratie van twee aanbieders van geavanceerde elektronische handtekeningen is deze bestuurlijk-organisatorische structuur voor certificatiedienstverleners ook feitelijk operationeel. De structuur kenmerkt zich door een zekere vorm van hiërarchie. Zoals de figuren 1 en 2 laten zien, is dit niet zozeer een hiërarchie van bevoegdheden maar een hiërarchie in het proces van certificering.

Figuur 1.



Figuur 2.



De rol van de auditor in dit proces is dat zij door de Raad voor accreditatie bevoegdheden krijgt om een audit uit te voeren en daarmee de bevoegdheid om vast te stellen of de dienstverlener aan de gestelde eisen voldoet. De OPTA heeft de bevoegdheid om een dienstverlener te registreren. In het College van Deskundigen hebben tal van deskundigen zitting, zoals auditors, onafhankelijk experts en marktpartijen. Dit college maakt de code voor beveiliging. Het college heeft tevens vastgesteld hoe de audits uitgevoerd moeten worden.

Markt voor TTP-dienstverlening
De markt voor TTP-dienstverlening komt in de praktijk vooral neer op een markt voor (al dan niet gekwalificeerde) certificaten waarmee digitale handtekeningen kunnen worden geplaatst. Met de toepassing van PKI-technologie gaat het uitgeven van certificaten gepaard, waarmee wordt aangegeven dat de met de publieke sleutel 'ontsleutelbare' gegevens behoren bij een bepaald persoon. In het beleidsveld is de TTP-dienstverlener daarom naar de achtergrond gedrongen ten gunste van de zogenaamde CSP (de Certification Service Provider, oftewel de aanbieder van – al dan niet gekwalificeerde - certificaten). De praktijk is dat dienstverlening veelal niet in open, maar in gesloten netwerken plaatsvindt. In dat geval is er niet meer sprake van een openbare TTP maar wel van een CSP. Op het certificaat hoeft dan ook niet de naam van de TTP te staan. De TTP kan dan nog wel een rol in dit proces vervullen, maar die betreft dan het technisch realiseren van de certificaten. Er is geen onafhankelijke partij die een waarborg aan beide partijen geeft dat het certificaat klopt.

MARKT VOOR TTP-DIENSTVERLENING

- Veelal gesloten netwerken
- Twee aanbieders van gekwalificeerde certificaten (openbaar)
- Veel aanbieders van (niet-gekwalificeerde) certificaten
- Vooral veel andere (lagere) niveaus van beveiliging

Probleem: nog weinig applicaties

Partijen die willen communiceren op basis van gekwalificeerde certificaten kunnen terecht bij twee gecertificeerde (openbare) aanbieders: PinkRoccade CSP en Diginotar.[16] Beide aanbieders hebben een audit laten uitvoeren op basis van het certificatieschema. Dat betekent dat aanbieders de technische en organisatorische structuur hebben gecreëerd waarmee gekwalificeerde certificaten feitelijk kunnen worden geleverd. Een van de dienstverleners beschikt ook over afnemers. Deze groep afnemers is beperkt in aantal, die de handtekening bovendien vooralsnog nog vooral gebruikt voor interne berichtenuitwisseling. Er vinden wel gesprekken plaats met andere partijen. Het probleem dat zich hierbij voordoet is dat voor deze partijen vaak een PKI-oplossing binnen een 'closed user group' voldoet en men dan dus geen behoefte heeft aan het gebruik van gekwalificeerde certificaten.

Beide dienstverleners bieden overigens ook andere TTP-diensten aan, naast de gekwalificeerde elektronische handtekening. Daarnaast zijn er tal van andere organisaties actief (nationaal en in Europees verband) die fungeren als CSP en dus (met behulp van een PKI) digitale handtekeningen of andere integriteits- en authenticatiediensten aanbieden. Ook kan elders in Europa ook gebruik worden gemaakt van geavanceerde elektronische handtekeningen zoals de Europese richtlijn deze beschrijft.
De huidige CSP-dienstverlening in Nederland vindt overigens veelal plaats in gesloten gebruikersgroepen. Voorbeelden van bedrijven die deze diensten aanleveren zijn Silverback en Fox-IT. Ook overheidsorganisaties zijn actief als CSP. Zo geeft de RDW certificaten uit aan garagehouders zodat deze online APK keuringen kunnen melden en kentekens kunnen overschrijven. Dergelijke certificaten zijn wel gebaseerd op PKI technologie, maar geen gekwalificeerde handtekeningen. Er zijn daarnaast ook nog veel elektronische transacties die niet op de PKI standaarden zijn gebaseerd en die lagere niveaus van beveiliging kennen. Voorbeelden hiervan zijn combinaties van pincode en wachtwoord, zoals de elektronische handtekening van de Belastingdienst.

[16] Diginotar is nog in gesprek met OPTA en het Ministerie van Economische Zaken over de kosten van registratie.

De markt voor CSP dienstverlening is divers en groeiende, als we de aanbieders mogen geloven. Het bereik van digitale handtekeningen is beperkt, in de zin dat alle digitale handtekeningen voor een specifiek doel worden uitgegeven en gebruikt. Van openbare (en 'many-to-many') certificaten, zoals het oorspronkelijke TTP-beleid beoogde, is geen sprake. Dat heeft ook te maken met de stand van de techniek. Er zijn nog maar weinig applicaties waarmee van de CSP dienstverlening gebruik kan worden gemaakt. Verwacht wordt dat PKI faciliteiten wel meer gebruikelijk gaan worden. Zo zijn in de nieuwe versie van Microsoft Office PKI faciliteiten aanwezig.

Feitelijke resultaten: een eerste beoordeling
In het kader van het evaluatieonderzoek is een expertmeeting georganiseerd waarin we de deelnemers gevraagd hebben naar wat zij beschouwen als de belangrijkste resultaten van het TTP-beleid. Van de hiervoor genoemde feitelijke resultaten benoemden zij de volgende opbrengsten van het TTP-beleid als de belangrijkste:

- Een praktisch en inmiddels meerdere malen feitelijk beproefd model van zelfregulering in combinatie met een goed uitgewerkt stelsel van afspraken. Dit model is een drijvende kracht gebleken om te komen tot een certificatieschema dat voldoet aan internationale normen en bood houvast gedurende het gehele traject.
- Samenwerking tussen overheid en markt. Er heeft een intensieve kruisbestuiving plaatsgevonden die heeft geleid tot allerlei vormen van samenwerking, waardoor bijvoorbeeld de implementatie van de Europese richtlijn ten aanzien van elektronische handtekeningen is vergemakkelijkt. Ook is opgemerkt dat de samenwerking tussen markt en overheid en het bijeenbrengen van experts vanuit verschillende aandachtsgebieden veel kennis over PKI heeft opgeleverd. Dit niet alleen in technisch opzicht, maar ook organisatorisch en juridisch.
- Er is een voor alle partijen acceptabele oplossing gevonden voor het omgaan met het vraagstuk van 'rechtmatige toegang'. Dit thema is betrekkelijk snel na de presentatie van het oorspronkelijke TTP-beleid van de agenda verdwenen op basis van een verkenning door een daartoe speciaal ingestelde werkgroep.
- Door het ontstaan van een netwerk van betrokkenen en deskundigen werd het makkelijker na te denken over thema's en vraagstukken die ook in andere beleidsarena's spelen en waar men daar minder lang bij hoeft stil te staan. In dit verband wordt met name het vraagstuk van de aansprakelijkheid van TTP-dienstverleners en certificaataanbieders genoemd.
- Er zijn twee aanbieders en alle randvoorwaarden zijn feitelijk gecreëerd om te komen tot een toekomstige groei van TTP-diensten.
- Er is een certificatieschema dat aansluit op EU-normen.

In het verlengde van de vraag naar de belangrijkste resultaten is in dezelfde expertmeeting gevraagd naar kansen die tot op heden (nog) niet zijn geïncasseerd. Naar voren kwamen:

- De harmonisering van de 'lagere' niveaus van beveiliging, al dan niet gebaseerd op PKI. De kans die is gemist is het regelen en daarmee tegelijkertijd harmoniseren van de beveiliging op meerdere niveaus.
- De integratie van PKI/TTP in de elektronische Nederlandse Identiteits Kaart (eNIK), of breder in de Nieuwe Generatie Reisdocumenten.

- Het certificeren van vertrouwelijkheidsdiensten. Op dit moment is de aandacht ten aanzien van certificering vooral uitgegaan naar authenticatie/beveiliging, in het bijzonder de gekwalificeerde elektronische handtekening.
- De bekendheid van het grote publiek met TTP. Betrekkelijk weinig burgers en bedrijven zijn vertrouwd met de mogelijkheid van TTP-dienstverlening in het algemeen en de elektronische handtekening in het bijzonder.
- De interoperabiliteit, in de zin van het algemeen kunnen koppelen van gekwalificeerde certificaten met toepassingen. Gesteld wordt dat er richtlijnen hadden moeten komen voor het overbrengen van handtekeningen op dragers, zodat de 'digitale sleutelbos' voor burgers voorkomen was. Verder is naar voren gebracht dat de EU dit punt eigenlijk had moeten oppakken.
- Er zijn weinig applicaties die TTP-dienstverlening gebruiken en er zijn weinig gebruikers van de huidige TTP-dienstverlening.
- Een eenduidige eis voor overheidsgebruik van TTP-dienstverlening. Dit had het gebruik ervan kunnen stimuleren.

Discussie is er over de vraag of de Wet elektronische handtekeningen nu een resultaat is van het beleid of een niet-geïncasseerde kans. Door een aantal experts is er op gewezen dat met de totstandkoming van de wet Nederland beschikt over een helder kader en een stevig fundament. Aan de andere kant is het zo dat de wet, vanuit het perspectief van Nederland, wellicht helemaal niet nodig was. Het Nederlandse beleid ging verder dan wat er uiteindelijk in de wet is bepaald. Vanuit een Europees perspectief was de wet derhalve wel wenselijk, maar vanuit Nederlands standpunt niet, zo luidde de mening van een van de experts.

4.3 Beoordeling van de effectiviteit en de efficiëntie

Een doelbereikingsparadox

Deels is het oorspronkelijke TTP-beleid dus feitelijk gerealiseerd. Het destijds beoogde certificatieschema en de randvoorwaarden voor TTP-dienstverlening zijn voor wat betreft de gekwalificeerde elektronische handtekening tot stand gekomen en hebben zelfs een juridische basis gekregen; dat geldt ook voor de certificerings- en toezichtstructuur zoals die destijds werd beoogd (in ietwat geamendeerde vorm). De meningen verschillen over de vraag of met het nu feitelijk gerealiseerde (gekwalificeerde certificaten) ook de oorspronkelijk beoogde functies kunnen worden vervuld (integriteit, authenticiteit, vertrouwelijkheid en beschikbaarheid). Volgens de een is het gekwalificeerde certificaat wel geschikt voor de andere functies, een ander had een breder TTP-concept voor ogen. Voorzover de feitelijke resultaten van het beleid afwijken van het oorspronkelijke TTP-concept (bijvoorbeeld registratie bij OPTA en geen TTP-kamer), is dat een direct gevolg van dwingende Europese regelgeving.

De meningen verschillen ook of de gecreëerde randvoorwaarden wel of niet een duurzaam levensvatbare markt voor de beschikbare TTP-dienstverlening (nu feitelijk gekwalificeerde certificaten) hebben opgeleverd. Er zijn twee aanbieders van gekwalificeerde elektronische handtekeningen en er zijn afnemers. Op dit punt heeft de beleidstheorie gewerkt: het reguleren heeft enkele marktpartijen opgeleverd die het certificatieschema en de certificering kunnen gebruiken als keurmerk voor vertrouwen.

Ook het achterliggende doel van het oorspronkelijke TTP-beleid is gerealiseerd, namelijk het totstandbrengen van betrouwbare elektronische communicatie ter ondersteuning van

elektronische handel en elektronische overheidsdienstverlening. Er zijn inmiddels tal van mogelijkheden om zo'n betrouwbare elektronische communicatie te realiseren. Het project *e-OK* dat momenteel loopt, beoogt deze mogelijkheden te categoriseren. Voor elektronische handel wordt bijvoorbeeld een beveiligde verbinding gebruikt waarover creditcardgegevens kunnen worden verstuurd om de betaling te garanderen, maar er zijn ook systemen met wachtwoordbeveiliging of op PKI-technologie gebaseerde certificaten (al dan niet met hardware tokens). Zo maken banken momenteel bijvoorbeeld gebruik van calculators, tancodes en certificaten. De nieuwe generatie bankpassen, de EMV-card, zal standaard van een chip worden voorzien. Vooralsnog is het ontbreken van betrouwbare elektronische communicatie feitelijk geen belemmering voor elektronische handel en (in tal van uitvoeringscontexten) ook geen belemmering voor elektronische overheidsdienstverlening. Bovendien is met het creëren van een openbare structuur voor de geavanceerde elektronische handtekening een zodanig niveau van betrouwbaarheid gegenereerd dat elektronische handel of overheidsdienstverlening die daaraan behoefte heeft daarvan ook gebruik kan maken.

Vijf jaar na dato is het TTP-beleid dus uitgevoerd, en het achterliggende doel is gerealiseerd. Bovendien heeft een veronderstelling achter het beleid ('stimuleren door reguleren/standaardiseren') tenminste twee dienstverleners opgeleverd. Uiteraard is het de vraag of deze de vruchten zijn van het TTP-beleid dan wel van de Wet elektronische handtekeningen. Feitelijk hebben beide dienstverleners sinds de start van het TTP-beleid gewerkt aan het creëren van dienstverlening, ruim voordat de Wet elektronische handtekeningen tot stand is gekomen. Dat pleit er dus voor de nu opererende dienstverleners als vruchten van het TTP-beleid te zien.

BELEIDSRESULTAAT

- Randvoorwaarden, certificering en toezicht zijn beoogd en gerealiseerd (voor gekwalificeerde handtekening)
- Wel of niet duurzaam levensvatbare markt?
- Onbetrouwbare communicatie geen belemmering voor elektronische handel en overheidsdienstverlening
- Beleid effectief geweest?

Dat het beleid is uitgevoerd en het achterliggende doel is gerealiseerd, betekent nog niet dat het beleid effectief is geweest. Tenminste twee aanvullende overwegingen spelen bij dit oordeel een rol. Ten eerste is een groot deel van de betrouwbare elektronische communicatie niet een gevolg van het TTP-beleid, respectievelijk van het beleid inzake de elektronische handtekening. Deze mogelijkheden voor beveiliging hebben zich los van het TTP-beleid ontwikkeld en worden daar ook niet door geraakt. Soms wordt wel van PKI-technologie gebruik gemaakt en zouden de (openbare) dienstverleners formeel nog wel tot het oorspronkelijke TTP-beleid kunnen worden geregeld. Zij vallen echter niet onder het certificatieschema. Dat het achterliggende doel is gerealiseerd, is dus maar voor een klein deel toe te schrijven aan het TTP-beleid (en de uitvoering daarvan). De oorzaak daarvan is gelegen in de transformatie die het beleid heeft doorgemaakt, te karakteriseren als een dubbele versmalling. De eerste versmalling van het beleid heeft te maken met de TTP-dienstverlening. Oorspronkelijk was dat beleid opgezet als een set minimumvoorwaarden voor openbare TTP-dienstverlening voor integriteit/authenticiteit en vertrouwelijkheid (zie hoofdstuk twee). Het uitgewerkte certificatieschema en de bestuurlijk-organisatorische structuur hebben echter alleen betrekking op de gekwalificeerde certificaten. Daarmee hangt een tweede versmalling samen. Het oorspronkelijke beleid betrof openbare TTP-dienstverlening (vooral of uitsluitend met behulp van PKI technologie) en beoogde daar een set van minimumvoorwaarden voor te

creëren. In de praktijk heeft het nu gerealiseerde TTP-beleid betrekking op het hoogste niveau van betrouwbaarheid. Ten aanzien hiervan merkte een van de criticasters van het beleid in een interview op dat wanneer het goed wordt geïmplementeerd, 'het zo'n zware beveiliging betreft dat je het alleen kunt gebruiken voor zaken die je nooit elektronisch zou gaan doen'.

Een andere overweging sluit hierop aan. Er is weliswaar wetgeving gecreëerd, alsmede een bestuurlijk-organisatorische infrastructuur, maar de markt voor de nu gereguleerde geavanceerde elektronische handtekening is momenteel nog zo klein dat getwijfeld wordt aan de levensvatbaarheid ervan. Er zijn twee aanbieders en een daarvan stelt over afnemers te beschikken, maar door enkele gesprekspartners in het onderzoek wordt betoogd dat deze markt geen lang leven is beschoren. Dat wordt geweten aan de hoge eisen (in technische en organisatorische zin), maar ook aan de kosten van certificering en registratie. Daardoor zijn de kosten voor toetreding relatief hoog. Wellicht, zo wordt gesteld, zal zich een Europese markt ontwikkelen voor gekwalificeerde elektronische handtekeningen. Of Nederlandse aanbieders daarop competitief kunnen opereren, is de vraag.

Effectiviteit

De effectiviteit van het TTP-beleid laat zich dus niet eenvoudig vaststellen. Het oorspronkelijk geformuleerde doel is bereikt en het opgestelde beleid is uitgevoerd, zij het in andere vorm dan destijds werd beoogd (als gevolg van de Europese richtlijn). Toch is realisatie van het oorspronkelijk geformuleerde doel voor een klein deel direct toe te rekenen aan het TTP-beleid. Dat heeft enerzijds te maken met veronderstellingen achter het TTP-beleid die niet zijn uitgekomen. De totstandkoming van TTP is vooralsnog geen voorwaarde gebleken voor de bloei van elektronische handel en elektronische overheidsdienstverlening. Dat kan te maken hebben met een verkeerde 'framing' van het beleid. In het onderzoek is door gesprekspartners wel betoogd dat onbetrouwbare communicatie geen probleem is voor elektronische handel, omdat vertrouwen met andere dimensies te maken heeft (bijvoorbeeld kredietwaardigheid) of omdat partners aan 'risicomanagement' doen en dus een lager betrouwbaarheidsniveau accepteren. Ook de veronderstelling dat de consumentenmarkt behoefte heeft aan openbare TTP-dienstverlening is vooralsnog maar voor een klein deel juist. De veronderstelling dat reguleren en standaardiseren de markt daarvoor zal stimuleren is (nog) niet te toetsen, omdat het oorspronkelijke beleid in 'smalle' vorm is uitgevoerd, namelijk alleen voor wat betreft gekwalificeerde certificaten.
Naast onjuiste veronderstellingen is de dubbele versmalling een oorzaak voor de zwakke relatie tussen uitvoering van het TTP-beleid en het realiseren van het achterliggende doel (betrouwbare elektronische communicatie ter bevordering van elektronische handel en elektronische overheidsdienstverlening). Daardoor heeft het feitelijk uitgevoerde beleid betrekking op slechts een klein deel van het totaal aan mogelijkheden om betrouwbare elektronische communicatie te realiseren.

Efficiëntie

De efficiëntie van het beleid laat zich evenmin makkelijk vaststellen. Dat heeft primair te maken met het ontbreken van cijfers en de onmogelijkheid om deze achteraf in het kader van dit evaluatieonderzoek te reconstrueren. Vooral betrouwbare cijfers over de totale kosten van het beleid en cijfers over de investeringen door marktpartijen ontbreken. Belangrijker dan de feitelijke kosten is wellicht nog het beoordelingskader voor de efficiëntie van het beleid:

- Zo kan de efficiëntie worden beoordeeld vanuit de feitelijk gerealiseerde resultaten (wet- en regelgeving, bestuurlijk-organisatorische infrastructuur en markt voor TTP-dienstverlening). Deze resultaten zijn dan met een aantal inspanningen van de

overheid tot stand gekomen: geld voor financiering van het TTP.NL-project en de totstandkoming van het certificatieschema, ambtelijke inzet ter ondersteuning van dit project en het inzetten van ambtelijke capaciteit voor het ontwerpen van de Wet elektronische handtekeningen. Ook is (voor een periode van twee jaar) per registratie een subsidie verstrekt aan OPTA om gecertificeerde dienstverleners die zich registreren tegemoet te komen. De combinatie van beide beleidstrajecten heeft extra kosten voor uitvoering van de Europese richtlijn voorkomen. Bovendien is gebruik gemaakt van deskundigheid in het TTP.NL-project. Bezien vanuit het feitelijk gerealiseerde resultaat is met name door de keuze voor zelfregulering (de markt moet TTP-dienstverlening realiseren) en de dubbele versmalling tijdens de uitvoeringsfase de inzet van overheidsgeld beperkt.

- Ook kan de efficiëntie worden beoordeeld vanuit de feitelijke behoefte aan gekwalificeerde certificaten. Bezien vanuit de feitelijke (beperkte) behoefte is een betrekkelijk zwaar systeem opgetuigd van (opstellen en permanent onderhouden van) een certificatieschema, een certificeringsprocedure (met auditor) en een registratieprocedure (bij OPTA). Daar staat tegenover dat het systeem grotendeels pas wordt ingezet als dat aan de orde is, dat wil zeggen als een potentiële aanbieder zich wil laten certificeren. Bij beperkt gebruik (zoals nu) zijn de vaste kosten (bijvoorbeeld van expertiseontwikkeling) betrekkelijk hoog; bij veelvuldig gebruik valt deze verhouding anders uit. Daarom is twee jaar een tegemoetkoming voorzien in de registratiekosten bij OPTA. De hybride procedure van vrijwillige certificering en registratie bij OPTA is weliswaar door de genuanceerde benadering van OPTA iets minder 'dubbel' van aard, maar draagt niet bij aan de efficiëntie van het systeem. Het beperkte gebruik ervan leidt dus tot een in verhouding zware wet- en regelgeving, respectievelijk bestuurlijk-organisatorische structuur. De eis om wetgeving op te stellen is verplicht opgelegd door de Europese Unie. Vanuit de potentiële aanbieder bekeken zijn vooral de extra kosten om te komen tot gekwalificeerde certificaten relevant. Ten opzichte van het opzetten en inrichten van een PKI zijn de kosten van certificering en toezicht relatief beperkt, maar toch nog noemenswaardig. Dat geldt te meer als potentiële aanbieders reeds een PKI hebben opgezet en ingericht en de marginale kosten van certificering, toezicht en operationele uitvoering moeten worden afgezet tegen de (beperkte) marginale opbrengsten van gekwalificeerde certificaten.

EFFICIËNT VANUIT:

- **Resultaat: betrekkelijk efficiënt**
- **Behoefte: betrekkelijk inefficiënt (tenzij de behoefte sterk groeit)**
- **Oorspronkelijk beleidsdoel: betrekkelijk efficiënt door dubbele versmalling van de uitvoering**

- Tenslotte is het mogelijk de efficiëntie te beoordelen vanuit de oorspronkelijk geformuleerde beleidsdoelen. In dat licht bezien heeft met name de keuze voor zelfregulering, gecombineerd met de 'dubbele versmalling' positieve gevolgen gehad voor de efficiëntie. Daardoor is voorkomen dat een breed TTP-concept door de overheid zou zijn neergezet waar in de markt geen behoefte aan bestaat. Door gebruik te maken van de markt heeft de aandacht zich vooral gericht op mogelijke

kansen voor realisatie. Denk bijvoorbeeld aan de elektronische handtekening en de mogelijkheid om de overheid als (grote) klant te benutten om de markt tot stand te brengen ('launching customer'). Door zelfregulering en de dubbele versmalling zijn overheidsinvesteringen voorkomen.

Afsluitend

Het is makkelijker de vraag naar de effectiviteit en de efficiëntie van het TTP-beleid te stellen dan deze te beantwoorden. Dat heeft niet zozeer te maken met het kunnen vaststellen van (het bereiken van) het doel of van de feitelijk gerealiseerde resultaten van het beleid. Zoals we in dit hoofdstuk hebben gezien, laten beide zich betrekkelijk eenduidig vaststellen. De analyse van effectiviteit en efficiëntie van het TTP-beleid wordt vooral bemoeilijkt door de transformatie die het beleid in de uitvoering heeft doorgemaakt. Deze transformatie is ingegeven door ontwikkelingen en kansen die zich in de beleidsrelevante omgeving hebben voorgedaan. Wordt het oorspronkelijke beleidsontwerp centraal gesteld, dan is het beleid niet effectief geweest, maar wel betrekkelijk efficiënt (omdat extra kosten zijn voorkomen). Als daarentegen de kansen en ontwikkelingen centraal worden gesteld, dan is het beleid grotendeels wel effectief en efficiënt geweest. Kanttekeningen zijn dan nog wel aan te brengen bij bijvoorbeeld de keuze voor een hybride structuur van certificering toezicht. Daarwaar zich kansen hebben voorgedaan, zijn deze gegrepen of verkend. Dat heeft tot een 'dubbele versmalling' geleid ten opzichte van het oorspronkelijke beleidsontwerp. Het is dus de vraag hoe deze dubbele versmalling kan worden geduid, met andere woorden: hoe moeten we deze dubbele versmalling van de uitvoering van het TTP-beleid eigenlijk beoordelen? Daarop komen we in het volgende hoofdstuk uitgebreid terug bij het formuleren van de handelingsperspectieven voor de toekomst van het TTP-beleid.

5. Aanknopingspunten voor de toekomst 'slim doorgaan... of?'

5.1 Inleiding

Misschien wel de belangrijkste les uit de geschiedenis van het TTP-beleid is die dat we voorzichtig moeten zijn met uitspraken over de toekomst. Toch is het van belang een handelingsperspectief te ontwikkelen voor het TTP-beleid waarbij geleerd wordt van het verleden en rekening wordt gehouden met de (langere termijn)ontwikkelingen in de beleidsrelevante omgeving. In dit hoofdstuk reiken we daarvoor aanknopingspunten aan. We formuleren eerst enkele lessen uit het evaluatieonderzoek en de ontwikkelingsgang van het TTP-beleid tot nog toe. Vervolgens verkennen we enkele huidige en verwachte juridisch-beleidsmatige, maatschappelijke en technologische ontwikkelingen in de omgeving van het TTP-beleid. Deze ontwikkelingen zijn van belang bij het bepalen van de richting waarin het TTP-beleid zich zou moeten ontwikkeling. De richtingen waarin dat beleid zich zou kunnen ontwikkelen schetsen we in de vorm van drie handelingsperspectieven in de afsluitende paragraaf.

5.2 Lessen uit de recente TTP-geschiedenis

Een passend 'evaluatiekader': dilemma's
Van Rij en Van Eeten (2003) hebben in hun analyse van het TTP-beleid gezocht naar een passende evaluatiebenadering, een manier om naar het TTP-beleid te kijken en tot oordelen te komen. Zij stellen dat een evaluatie van dat beleid een ingewikkelde opgave is, allereerst omdat het 'beleidsterrein gezien de dynamiek en de multi-actor setting complex' is. Daarbij komen de uiteenlopende eisen aan een evaluatie: vaststellen of de beoogde doelen bereikt zijn, of adequaat is ingesprongen op kansen en bedreigingen en of goed gereageerd is op de effecten die het beleid (al dan niet) heeft veroorzaakt in het beleidsveld. Een eenvoudige doelbereikingsevaluatie volstaat niet, aldus Van Rij en Van Eeten, omdat dan geen recht wordt gedaan aan 'de doelverschuivingen in de multi-actorsetting die we hebben geconstateerd'. Een procesevaluatie is eveneens maar tot op zekere hoogte relevant. Belangrijk is volgens hen dat de evaluatie blijk geeft van de drie kerndilemma's in het TTP-beleid.

Deze drie dilemma's omschrijven Van Rij en Van Eeten als volgt:

- Ten eerste is er het dilemma overheid versus markt. Zowel de keuze voor de overheid als de keuze voor de markt kan overtuigend worden beargumenteerd. De overheid kan daadkrachtig optreden en de startkosten van een project financieren zodat net het zetje wordt gegeven dat in bepaalde omstandigheden nodig is. Ook kan de overheid partijen 'precompetitief' bijeen brengen en daarmee de markt de noodzakelijke eerste stap laten zetten. Voordeel van het overlaten aan de markt is volgens Van Rij en Van Eeten dat in dat geval de kennis in de markt beter doorklinkt in het proces en een effectieve reactie op dynamiek in de markt mogelijk is.
- Daarnaast is er het dilemma tussen daadkracht en afwachten. Er waren bij de start van het TTP-beleid volgens Van Rij en Van Eeten goede argumenten om als

marktpartijen en overheid te kiezen voor een daadkrachtig optreden in de vorm van het vroegtijdig kiezen en vaststellen van een bepaalde technische standaard om zo de Nederlandse concurrentiepositie te versterken of om versnippering tussen verschillende standaarden tegen te gaan. Het snel opstellen van een certificatieschema levert ook tastbaar resultaat op. Toch heeft het afwachten en wellicht stimuleren van een variëteit van technologische ontwikkelingen (en dus niet standaardiseren) het voordeel dat ervaring kan worden opgedaan met meerdere oplossingen, kan een concept worden 'doorontwikkeld' of kan het 'variatie- en selectieproces' van de markt worden gebruikt om tot een standaard te komen.

DILEMMA'S TTP-BELEID

- Daadkracht versus afwachten
- Markt versus overheid
- Uniformiteit versus diversiteit

- Een derde dilemma dat Van Rij en Van Eeten beschrijven is dat van uniformiteit versus diversiteit. In het TTP-beleid is vanaf de start ingezet op TTP als oplossing, op standaardisatie van de randvoorwaarden en later op een invulling van de elektronische handtekening en een betrouwbaarheidsniveau voor overheidstransacties (feitelijk overigens een keuze van PKIoverheid). Een uniform toetsingskader is helder en transparant, rechtszeker en in zekere zin stabiel. Door allerlei ontwikkelingen is de uniforme oplossing tegelijkertijd ook de 'zwaarste' of de technisch beste oplossing geworden. Daardoor bleek een universele oplossing voor veel toepassingen te duur of te zwaar in het licht van het vertrouwen waaraan behoefte bestaat.

Van Rij en Van Eeten roepen de 'evaluatoren' van het TTP-beleid op om de evaluatie niet alleen te richten op het oorspronkelijk geformuleerde doel en het proces, maar ook op de dilemma's die zich in het ontwerp en de ontwikkeling (en uitvoering) van het beleid hebben voorgedaan.

Lessen uit het voorliggende evaluatieonderzoek

Op basis van het voorliggende evaluatieonderzoek laten zich ten aanzien van drie dimensies van het TTP-beleid lessen formuleren: de context van TTP-beleid, de oorspronkelijke beleidstheorie en de responsiviteit van het beleid. Ten eerste geeft het evaluatieonderzoek, in combinatie met het eerder uitgevoerd onderzoek naar TTP-beleid, inzicht in de context waarin dat beleid wordt gemaakt en uitgevoerd.

Deze context laat zich als volgt omschrijven:

- Zowel de technologie (internet, PKI, cryptografie) als het beleidsveld (e-business, e-government, informatiebeveiliging) kennen een hoge graad van *complexiteit*. Deze heeft te maken met de variëteit aan technieken en partijen en de moeilijkheden die precieze 'framing' van het beleidsprobleem oplevert (zie hoofdstuk twee).
- Daarnaast wordt de omgeving van het TTP-beleid gekenmerkt door een hoge mate van *onzekerheid*: deze heeft ten eerste betrekking op het gedrag van (markt)aanbieders en potentiële gebruikers, bijvoorbeeld de vraag wat precies de reële behoefte aan (welk type) betrouwbare elektronische communicatie en transactie is en of in dit geval nieuw aanbod ook nieuwe vraag zal creëren. Daarnaast betreft de onzekerheid de ontwikkeling van nieuwe technologieën en de wisselwerking die deze met het beleid aangaan. Ten derde is er onzekerheid over nieuwe internationale standaarden en eisen

aan elektronische communicatie en transactie. De enige zekerheid in de omgeving van het TTP beleid lijkt te zijn dat deze omgeving turbulent is.

- Een *niet-eenduidige behoefte* aan betrouwbare elektronische communicatie en transactie bij marktpartijen. Deze behoefte hangt deels af van definieerbare categorieën: de omvang van de transactie, de vraag of partijen een duurzame relatie aangaan, het domein van de transactie (overheid-burger, overheid-bedrijfsleven, bedrijfsleven-bedrijfsleven, bedrijfsleven-consument), de betalingsgaranties (of de kredietwaardigheid van de handelspartner) en de verwachte risico's. Daarnaast zijn er ook minder goed definieerbare en voorspelbare determinanten. Als zich op een bepaald moment een grootschalige fraude voordoet, neemt de behoefte aan betrouwbaarheid toe. Of, zoals Van Rij in haar scriptie stelt, het einde van de 'dot-com-hype' leidt er min of meer onverwacht toe dat de markt voor TTP-diensten afneemt.

LESSEN CONTEXT TTP-BELEID

- Complexiteit
- Onzekerheid
- Niet-eenduidige behoefte
- Investeringsnoodzaak

- Voor welke oplossing er ook gekozen wordt, naarmate het betrouwbaarheidsniveau toeneemt neemt ook de noodzaak van aanzienlijke *financiële investeringen* in technologie en infrastructuur toe. Denk bijvoorbeeld aan het opzetten van een PKI. Deze noodzaak van financiële investeringen is relevant als kenmerk van de TTP-markt, maar ook van belang in relatie tot de voortdurend veranderende omgeving. Een turbulente omgeving die aanzienlijke investeringen van marktpartijen vergt is per definitie spanningsvol. Bovendien staat de beleidsontwikkeling en de politiek-bestuurlijke besluitvorming daardoor extra onder druk vanwege de in het geding zijnde belangen.

In theorie hoort bij deze complexiteit en onzekerheid een in sterke mate doelzoekend beleid en dus niet de standaardisatie en de uniformiteit waarvoor in het TTP-beleid is gekozen. Door de aanzienlijke investeringen die betrouwbare oplossingen op grote schaal vergen, zijn echter stabiele marktomstandigheden noodzakelijk. Het creëren van stabiliteit is niet goed mogelijk, omdat de technologische, economische en juridische omstandigheden waarin de beleidsmaker opereert veranderlijk zijn. En zo is de cirkel rond. De omgeving van het TTP-beleid dwingt daarmee dus tot uiteenlopende, spanningsvolle eisen aan het beleid.

In hoofdstuk twee heeft de beoordeling van de oorspronkelijke beleidstheorie ook enkele lessen opgeleverd:

- Binnen het gekozen 'paradigma' (marktwerking, standaardisatie, vrijwillige certificering en toezicht), zoals we dat hebben beschreven, is het TTP-beleid snel en effectief opgepakt. Het is uitgemond in een set randvoorwaarden. Op de randvoorwaarden hebben we geen kritiek aangetroffen die wijst op gebrekkige waarborgen voor veiligheid of betrouwbaarheid. De aanpak van zelfregulering, gecombineerd met stimulerende maatregelen en ondersteunende regelgeving, heeft vanuit de oorspronkelijke doelstellingen geleid tot adequaat resultaat binnen redelijke termijn. Overigens wordt door sommigen aangegeven dat het sneller had gekund, zoals ook Van Rij (2002) concludeert.
- De onzekerheid en complexiteit in het beleidsveld is in het TTP-beleid beantwoord met een stellige en enkelvoudige beleidsstrategie. Een les die zich op basis van de

'werdegang' van het TTP-beleid daarna laat formuleren is dat een onzekere en complexe omgeving om een meervoudige strategie (en probleemconceptie) vraagt of tenminste wordt nagedacht over een (of meer) alternatief (alternatieven) voor de enkelvoudige strategie waarvoor wordt gekozen.

- Een volgende les hangt hiermee samen. Juist omdat de omgeving onzeker en complex is, is het belangrijk om kritisch alle veronderstellingen en probleemdefinities achter het beleid te traceren bij het opzetten ervan en deze ook expliciet te maken. Daarmee is het mogelijk om na vaststelling van het beleid voortdurend te 'monitoren' of te verifiëren welke reacties, processen en mechanismen het beleid uitlokt in het beleidsveld en daarmee of de veronderstellingen achter het beleid ook valide blijken. Vooraf is dit immers maar tot op zekere hoogte te bepalen, zeker in een onzekere en complexe situatie als die van het TTP-beleid.

Tenslotte laten zich ten aanzien van de responsiviteit van het beleid enkele lessen formuleren:

LESSEN OORSPRONKELIJKE BELEIDSTHEORIE

- Degelijk binnen paradigma
- Stellige en enkelvoudige strategie
- Niet alle veronderstellingen expliciet gemaakt en kritisch geëvalueerd

- We hebben gezien dat in de uitvoering van het TTP-beleid alert is ingespeeld op de kansen die zich in de omgeving hebben voorgedaan. De Europese richtlijn bood de kans om een Europese juridische steun in de rug te organiseren voor een van de TTP-diensten (de elektronische handtekening) en de nationale standaarden aan te sluiten op Europese standaarden. PKIoverheid bood de kans op het forceren van een doorbraak in de markt voor TTP-dienstverlening en tegelijkertijd een belemmering weg te nemen voor een doorbraak op het terrein van e-government. KWINT laat zien dat TTP een oplossing kunnen zijn voor een reële kwetsbaarheid van het internet. Hoewel vooralsnog het inspelen op kansen maar in beperkte mate heeft geleid tot feitelijke realisatie van TTP-dienstverlening, is het ingaan op deze kansen als zodanig effectief geweest. De les die daaraan gekoppeld kan worden is dat in de complexe en dynamische omgeving van het TTP-beleid het speuren naar kansen en het daarop aansluiten effectief is: het kan bijdragen aan feitelijke realisatie van een beleidsdoel of kan een beleidsfiasco voorkomen.
- Daarop aansluitend kan een volgende les worden geformuleerd. We hebben gezien dat het aansluiten op kansrijke ontwikkelingen in de omgeving veel (uitvoerings)energie eist en soms 'aandachtsversmalling' met zich meebrengt. Daardoor wordt het bredere concept of de beleidsdoelstelling soms naar de achtergrond gedrukt. Een les die we hieraan kunnen koppelen is dat bij het 'aansluiten' op kansrijke ontwikkelingen expliciet bezien moet worden vanuit de bijdrage aan het bredere concept of de bredere doelstelling van het beleid en welke aanvullende strategieën nodig zijn om aandachtsversmalling te voorkomen.
- Een derde les sluit hierop aan. Het actief oppakken van en aansluiten op kansrijke ontwikkelingen in de omgeving van het TTP-beleid is niet alleen een mogelijkheid (delen van) het beleid te realiseren, maar telkens ook een ervaring waarvan geleerd kan worden. Dat de verbinding met PKIoverheid vooralsnog niet heeft geleid tot de langverwachte overheid als 'launching customer' kan aanleiding zijn voor teleurstelling, maar zou tegelijkertijd ook een moment van reflectie kunnen zijn. Centrale vraag zou in dat geval zijn: 'Als TTP-dienstverlening zelfs niet in deze omstandigheden (relatief hoog betrouwbaarheidsniveau en grote aantallen transacties)

een businesscase oplevert, in welke omstandigheden dan wel?' Met andere woorden, de les die zich laat formuleren is dat juist het 'opvolgen van kansen' tegelijkertijd aanleiding moet zijn om expliciet te reflecteren op de vraag of de oorspronkelijke concepten en veronderstellingen (nog) wel adequaat zijn dan wel aan herziening toe zijn.

LESSEN RESPONSIVITEIT

- Als zodanig is responsiviteit zinvol geweest (doel gerealiseerd of fiasco voorkomen)
- Voorkomen van aandachtsversmalling
- Leren van de ervaring

5.3 Huidige ontwikkelingen

Ten aanzien van de toekomst van het TTP-beleid en dan met name het gebruik van de tot stand gebrachte voorzieningen, spelen momenteel enkele relevante ontwikkelingen of zijn initiatieven aangekondigd die hierop mogelijk van invloed zijn.

Ontwikkelingen op het gebied van cryptografie: het streven naar meer veiligheid
Een aspect dat van belang is voor de toekomst van het gebruik van cryptografie is het verbeteren van bestaande en het ontwikkelen van nieuwe cryptografische algoritmen en technieken. Als opvolger van de verouderde symmetrische DES-algoritme (Data Encryption Standard) is de Advanced Encryption Standard (AES) gepresenteerd. Voordelen van deze nieuwe standaard zijn dat deze gebruik maakt van een voor de komende decennia door deskundigen veilig geacht wiskundig encryptie-algoritme, in combinatie met een hoge snelheid en een grote mate van portabiliteit. Hierdoor zijn toepassingen van AES binnen smartcard-omgevingen en draadloze datacommunicatie binnen afzienbare tijd haalbaar.
Ten aanzien van de asymmetrische encryptie geldt dat de RSA standaard er een concurrent bij heeft gekregen in de vorm van Elliptic Curve Crypthography (ECC). Deze biedt evenveel veiligheid als RSA maar heeft veel minder verwerkingsoverhead.
Een laatste ontwikkeling is dat met behulp van quantumfysica het mogelijk lijkt om een *one time pad*-methode toe te gaan passen voor sleuteldistributie. Dit betekent dat een sleutel wordt gekozen met dezelfde grootte als de te vercijferen data. Dit maakt het mogelijk rijen bits zodanig te versturen dat elke poging tot afluisteren ervan opgemerkt kan worden. (Platform Informatiebeveiliging, 2002: 120).

Ontwikkelingen ten aanzien van Ecommerce-techniek: naar mobile eCommerce
Naar verwachting zal de ontwikkeling van eCommerce zich steeds meer afspelen in de vorm van mobile eCommerce. Dit onder de voorwaarde dat de beveiliging van informatie en diensten afdoende kan worden geregeld. Met het Wireless Application Protocol (WAP) is inmiddels ervaring opgedaan maar tot een grootschalig gebruik ervan door consumenten heeft dit niet geleid. De verwachtingen ten aanzien van twee andere protocollen, General Packet Radio Services (GPRS) en Universal Mobile Telecommunication System (UMTS), liggen beduidend hoger (Platform Informatiebeveiliging, 2002: 123 e.v.).

Voor het TTP-beleid betekenen deze trends in de eerste plaats dat de gebruikte techniek in PKI toepassingen het mogelijk maakt om een nog grote mate van beveiliging te realiseren van elektronische gegevensuitwisseling. De ervaring leert dat alle algoritmen die gebruikt worden op termijn minder veilig worden omdat de technologie voortschrijdt en het makkelijker wordt om ze te 'kraken'. Met de nieuwe standaarden lijkt de beveiliging in ieder geval voor de komende decennia veiliggesteld.

De trend naar mobile eCommerce laat zien dat in de praktijk de gegevensuitwisseling via verschillende media en met verschillende soorten hardware gaat plaatsvinden. Niet alleen via pc's maar dus ook via mobiele telefoons met SIM-kaarten. Het TTP-beleid dient voldoende oog te hebben voor deze ontwikkeling om hierin kansen en beperkingen voor de toepassing van het construct in te zien.

Andere overheid
Enkele van de ontwikkelingen en initiatieven vinden plaats in het kader van het eind 2003 verschenen *Actieprogramma Andere Overheid*, waarin vier actielijnen centraal staan[17]:

- De overheid gaat haar dienstverlening aan de burger verbeteren;
- De overheid gaat minder en anders regelen;
- De rijksoverheid gaat zichzelf beter organiseren;
- De rijksoverheid gaat haar relaties met provincies en gemeenten vernieuwen.

ONTWIKKELINGEN

- Nieuwe cryptografische technieken
- Mobiele elektronische handel
- Andere overheid (en eNIK)
- Uitbreiding Nederlandse identiteitskaart en stroomlijning basisgegevens
- e-OK
- Verder met de handtekening...

In het kader van de eerste actielijn stelt het kabinet dat er voorzieningen moeten worden getroffen voor een veilig elektronisch verkeer tussen overheid en burgers of bedrijven. Belangrijk is dat zekerheid bestaat over de identiteit van degene aan wie elektronische diensten worden verleend. Om dat mogelijk te maken zal nog in 2004 een authenticatievoorziening worden ingericht, die overheidsbreed ter beschikking zal komen. Het gaat hierbij om realisatie van de *Overheidstoegangsvoorziening* (OTV), die waar mogelijk zal worden gecombineerd met de Overheidstransactiepoort (OTP). De OTV is een eerste aanzet tot een volwaardige infrastructuur voor elektronische beveiliging en identificatie waarvan een *burgerservicenummer (BSN)*, een *elektronische identiteit*, een *elektronische handtekening* en een *PKI infrastructuur* deel uitmaken. Het kabinet streeft ernaar ten behoeve daarvan zo mogelijk nog in deze kabinetsperiode een *elektronische identiteitskaart* te introduceren. Na in 2002 het besluit te hebben genomen niet over te gaan tot een grootschalige uitrol van de elektronische identiteitskaart lijkt het tij voor de eNIK dan nu te keren. Eind 2006 zou de kaart beschikbaar kunnen zijn.

In de in februari 2004 verschenen *Rijksbrede ICT-agenda* wordt gesteld dat Nederland uitblinker wil zijn in Europa. Hiervoor is een aantoonbare betere prestatie met ICT nodig, zo stelt men. De uitgangspositie hierbij is gunstig omdat onze ICT-basis grotendeels op orde is. Een betere benutting van ICT is echter urgent. Initiatieven van de overheid die bedoeld zijn om ICT te bevorderen moeten met elkaar in verband worden gebracht, zodat zij elkaar versterken. Bovendien moeten we ICT intensiever gebruiken: als er een toepassing klaar staat, er ook op toezien dat zoveel mogelijk potentiële gebruikers er ook van profiteren (Rijksbrede ICT-agenda: 2004: 2 en 3).

De relevantie voor de TTP-infrastructuur is dat het thema van beveiligde communicatie door onder andere het Actieprogramma Andere Overheid niet alleen op de agenda blijft staan, maar ook in concrete stappen wordt uitgewerkt. Naar verwachting leidt dit niet direct tot een

[17] *Kamerstukken II*, 2003-2004, 29.362, nr. 1

intensiever gebruik van de TTP-voorzieningen, maar dit zou een volgende stap kunnen zijn. Ook kan het gebruik van certificaten bijdragen aan een versnelling van de verbetering van de bedrijfsvoering (een van de thema's in Andere Overheid). Dit omdat het organisaties dwingt de overstap te maken van analoge documenten en werkstromen naar digitale vormen hiervan. Daarmee kan een certificaat dus een hefboom voor vernieuwing vormen. Juist het stimuleren van het gebruik van reeds ontwikkelde voorzieningen (benutting ICT) staat centraal in de Rijksbrede ICT-agenda.[18]

PKIoverheid
De voormalige PKI taskforce is sinds 1 januari 2003 opgesplitst in twee onderdelen. Het eerste is het Informatiecentrum PKIoverheid. Dit centrum beschikt over informatie, kennis en instrumenten ter ondersteuning van partijen die gebruik willen maken van PKI voor de overheid. Het informatiecentrum geeft hierover advies en voorlichting. Het andere onderdeel is de Policy Authority. Deze autoriteit richt zich op het beheer over de PKI voor de overheid met als doelstelling het handhaven van een werkbaar en betrouwbaar normenkader voor PKI-diensten dat voorziet in een vastgesteld beveiligingsniveau voor de communicatiebehoefte van de overheid en transparant is voor de gebruikers (zie www.PKIoverheid.nl).

Kiezen-op-Afstand
Bij de huidige opzet van verkiezingen is het stemlokaal vooraf bepaald. Het ministerie van Binnenlandse Zaken en Koninkrijksrelaties streeft ernaar om verkiezingen minder plaatsafhankelijk te maken. Onderdeel hiervan is het project Kiezen-op-Afstand: van dinsdag 1 juni tot donderdag 10 juni 2004 brachten 7200 van de twaalfduizend geregistreerde Nederlandse kiesgerechtigden in het buitenland hun stem uit via internet of de telefoon. Naast het experiment met stemmen via internet konden kiezers in vijf Nederlandse gemeenten op 10 juni hun stem uitbrengen bij een willekeurig stemlokaal in hun gemeente.

Uitbreiding Nederlandse identiteitskaart
Ter bestrijding van illegale arbeid en ontduiking van premies en heffingen in de sociale zekerheid heeft het ministerie van Sociale Zaken en Werkgelegenheid het streven geuit om gefaseerd te groeien naar een situatie waarin alle personen met toegang tot de arbeidsmarkt en sociale verzekeringen zich op eenduidige en gestandaardiseerde wijze kunnen identificeren met een Nederlands (identiteits)document voorzien van een sofi-nummer. Momenteel hebben alleen ingezetenen een document voorzien van sofi-nummer. Op termijn krijgt dit sofi-nummer de status van Burger Service Nummer.

De volgende stappen worden ten aanzien van de situatie in het sofi-domein gezet:

- Uitbreiding van de reikwijdte van de Nederlandse identiteitskaart voorzien van sofi-nummer naar vreemdelingen en EU-ingezetenen (standaardisatie);
- Bestrijding van de identiteitsfraude door opname van biometrie op deze identiteitsdocumenten;
- Met de toevoeging van certificaten voor de digitale handtekening en digitale identiteit (PKI) aan deze identiteitsdocumenten wordt de mogelijkheid gecreëerd voor een daadwerkelijke elektronische transactieverlening via internet.

[18] *Kamerstukken II*, 2003-2004, 26.643 nr. 47

Stroomlijning basisgegevens
Het ministerie van BZK heeft ICTU gevraagd een programmaplan op te stellen voor de voortzetting van het programma Stroomlijning Basisgegevens dat eind 2002 in eerste fase is afgerond. Het is de bedoeling het eventuele voortgezette programma in augustus 2004 te starten. Kern van het programma stroomlijning basisgegevens is het mogelijk maken van de gewenste eenmalige gegevensbevraging van burgers en bedrijven. Hiertoe wordt gewerkt met een aantal authentieke registraties waar alle overheidsorganisaties (verplicht) gebruik van moeten maken. Het idee is dat gegevens die in authentieke bronnen beschikbaar zijn, niet nogmaals aan burgers of bedrijven worden gevraagd. Een dergelijk stelsel vergt unieke bestanden voor bepaalde objecten (personen, percelen, dienstverbanden etc) en adequate toegankelijkheid (direct of via geautomatiseerde uitwisseling) door geautoriseerde derden. Het vervolg van de eerste fase heeft als doel om te komen tot daadwerkelijke realisatie van basisregistraties (zie www.ICTU.nl).

e-OK keurmerk
Om e-authenticatie in goede banen te leiden is samenwerking nodig tussen de verschillende initiatieven. Nederland kan hierin de leiding nemen en een voorbeeld vormen voor de rest van Europa. Om e-authenticatie in Nederland op een gecoördineerde manier van de grond te krijgen is in november 2003 het 'e-OK' initiatief door ECP.NL gelanceerd. In dit initiatief wordt een 'e-OK' keurmerk afgegeven aan aanbieders van internetdiensten op basis van het technische beveiligingsniveau van hun oplossing, gebruiksgemak (usability), interoperabiliteit (liefst op basis van Europese standaarden) en de manier waarop de aanbieder van de dienst omgaat met persoonsgegevens van gebruikers. Het 'e-OK' initiatief begint met het categoriseren van de bestaande systemen in een raamwerk en zet vervolgens een certificatieorganisatie op voor het uitgeven van het keurmerk. Het doel daarvan is samenwerking tussen de verschillende aanbieders van authenticatiediensten tot stand te brengen, zodat de eindgebruiker duidelijkheid heeft en niet overspoeld wordt door verschillende systemen.

Surf-op-safe campagne
De surf of safe campagne is een bewustwordings- en voorlichtingscampagne om internetgebruikers (burgers, bedrijven en kinderen) bewust te maken van de risico's op internet en hen erop te wijzen dat ze zelf maatregelen kunnen treffen om risico's van internetgebruik te minimaliseren. De campagne is geïnitieerd door de ministeries van Economische Zaken en Verkeer en Waterstaat. De uitwerking van de campagne is in samenwerking tussen overheid, gebruikersorganisaties en bedrijfsleven tot stand gekomen.

Verder met de handtekening...
Juridisch staat de toekomst allereerst in het teken van de invulling van vereisten waaronder de elektronische handtekening als voldoende betrouwbaar worden beschouwd voor het doel waarvoor ze worden gebruikt (zie artikel 3:15 a lid 1 BW). Deze vereisten zijn ten aanzien van de in artikel 3:15a lid 2 BW bedoelde geavanceerde elektronische handtekeningen in regelgeving reeds nader uitgewerkt (zie o.m. Besluit elektronische handtekening). Voor gewone elektronische handtekeningen is het aan de rechter om het concrete gebruik ervan als bewijsmiddel te waarderen. Toekomstige rechtspraak zal dus meer duidelijkheid moeten brengen op dit vlak.

Bij het gebruik van elektronische handtekeningen in het bestuurlijk elektronisch verkeer zal de toekomst voorts moeten uitwijzen of hier aanvullende wettelijke vereisten zullen worden gesteld, zoals artikel 2:16 uitdrukkelijk mogelijk maakt. De overweging hierachter is dat de

publieke taak kan vragen om hogere eisen aan authenticiteit van elektronische communicatie. Deze eisen mogen dan ook verdergaan dan de regeling betreffende elektronische handtekeningen in het BW, die in dezelfde bepaling van overeenkomstige toepassing op het elektronisch bestuurlijk verkeer wordt verklaard. Het stellen van aanvullende eisen in de publieke sector wordt uitdrukkelijk door artikel 3 lid 7 van richtlijn 99/93/EG betreffende elektronische handtekeningen toegestaan:

> 'De lidstaten kunnen voor het gebruik van elektronische handtekeningen in de openbare sector eventuele aanvullende eisen stellen.'

Deze eisen moeten objectief, transparant, evenredig en niet-discriminerend zijn en mogen slechts op de specifieke kenmerken van de betrokken toepassing betrekking hebben. Zij mogen geen belemmering vormen voor grensoverschrijdende diensten. Rekening houdend met de door de richtlijn genoemde voorwaarden kunnen dergelijke aanvullende eisen in een wettelijk voorschrift worden opgenomen, waarvan vervolgens niet kan worden afgeweken.[19]

Verder zal andere (naar verwachting vooral publiekrechtelijke) wetgeving worden aangepast aan het elektronisch rechtsverkeer, inclusief het gebruik van elektronische authenticatie-technieken. Zo is bijvoorbeeld de Herzieningswet Kadasterwet I in behandeling in de Tweede Kamer. Hierin wordt voorzien in aanvullende eisen voor het gebruik van elektronische handtekeningen ten behoeve van inschrijvingen in het Kadaster.[20] Een ander voorbeeld is de Experimentenwet Kiezen op Afstand, op grond waarvan kiezers via een PC moeten kunnen stemmen. De keuze voor een elektronisch identificatiemiddel ten behoeve van het elektronisch kiezen wordt uitdrukkelijk opengelaten, ofschoon de PKI van de overheid als een van de mogelijkheden wordt genoemd.[21] Ook zal in het kader van het strafrechtelijke domein afzonderlijk worden bekeken of, en zo ja in welke gevallen, elektronisch rechtsverkeer tussen overheid en burger kan plaatshebben en of daar aanvullende eisen voor nodig zijn.[22] Gedacht kan worden aan de eisen van betrouwbaarheid en vertrouwelijkheid bij het opmaken van formele stukken, zoals een elektronisch proces-verbaal. Hierbij zal tevens moeten worden onderzocht welke consequenties dergelijk elektronisch verkeer heeft voor de computersoftware en -apparatuur.[23]

Thema's die raken aan het onderwerp van evaluatie en tot juridische maatregelen aanleiding kunnen gaan geven zijn (informatie)beveiliging en beschikbaarheid van vitale infrastructuren.[24] Ofschoon de overheid in de nota KWINT aangeeft een terughoudende rol met het oog op aanvullende regelgeving te zullen innemen 'om de zich nog ontwikkelende markt niet onnodig te verstoren' is het niet ondenkbaar en mogelijk zelfs verstandig en onontkoombaar dat de overheid een actievere sturende rol op zich neemt.

---

[19] *Kamerstukken II* 2001/02, 28 483, nr. 3, p. 42.
[20] *Kamerstukken II*, 2001/02, 28 443, nrs. 1-2.
[21] *Kamerstukken II*, 2002/03, 28 664, nrs 1-2.
[22] *Kamerstukken II* 2000/01, 27 743, nr. 3, p. 11.
[23] *Kamerstukken II* 2001/02, 28 483, nr. 3, p. 4.
[24] Zie Nota KWINT (Kwetsbaarheid op Internet), *Kamerstukken II*, 2000/01 26 643, nr.30; NACOTEL, beschikbaar op: <www.ez.nl/beleid/home_ond/dgtp/veiligheid/nacotel.html>; Project Bescherming Vitale Infrastructuren, *Kamerstukken II*, 2002/03, 26 643, nr. 39.

5.4 Handelingsperspectieven voor de toekomst van het TTP-beleid

5.4.1 Interpretatie van de huidige situatie

De feiten zijn helder, maar hoe zit het met de duiding ervan?
Aan de toekomst van het TTP-beleid gaat een diagnose van de huidige situatie vooraf. Feitelijk is een deel van het oorspronkelijke TTP-beleid gerealiseerd, zij het in een andere vorm dan destijds gedacht. Er is een certificatieschema voor elektronische handtekeningen (met juridische basis), er is een adequate toezicht- en certificatiestructuur voor TTP-dienstverlening en er zijn feitelijk TTP-dienstverleners die daarvan gebruik maken. Een daarvan geeft aan ook over afnemers te beschikken. Er ligt een verkenning van de gebruiksmogelijkheden van TTP-dienstverlening voor e-government. We kunnen dat vaststellen, maar in het onderzoek hebben we sterk uiteenlopende interpretaties van deze feitelijke toestand waargenomen. Deze laten zich in drie 'interpretaties' onderbrengen.

TTP-beleid is een succes, maar het duurt iets langer
De eerste interpretatie luidt: 'Het TTP-beleid is een succes, maar het duurt alleen iets langer'. Het feitelijk gerealiseerde resultaat (certificatieschema, toezichtstructuur, deels juridische dekking) dat zich (in deze interpretatie) terecht beperkt tot de gekwalificeerde elektronische handtekening wordt positief gewaardeerd en daaraan wordt een duurzame betekenis toegekend. Verwacht wordt dat de wet- en regelgeving, de bestuurlijk-organisatorische structuur en de markt voor geavanceerde elektronische handtekeningen langere tijd zullen standhouden. Bovendien wordt in deze interpretatie verwezen naar het langzaam maar gestaag groeien van de markt voor TTP-dienstverlening. Allerlei ontwikkelingen en ervaringen met e-business en e-government, zo stelt deze interpretatie, zullen het betrouwbaarheidsniveau waaraan behoefte bestaat naar boven stuwen. In die groeiende markt zal TTP-dienstverlening kunnen voorzien. Bovendien zal de groeiende markt ertoe leiden dat de financiële drempels voor toegang aan aanbiederszijde zullen worden verlaagd, als gevolg van de lagere kosten voor toezicht. Naarmate er meer aanbieders komen, worden bijvoorbeeld de kosten voor registratie gespreid en per aanbieder dus lager. Kortom, nu het raamwerk er staat zal het gebruik vanzelf wel toenemen. Eventueel kan dat gebruik nog door de overheid worden gestimuleerd. Als de gekwalificeerde elektronische handtekening standaard op het identiteitsbewijs voor burgers wordt opgenomen, zal dat een 'push' veroorzaken omdat zowel in het publieke als in het private domein dan een authenticatievoorziening met een hoog betrouwbaarheidsniveau betrekkelijk goedkoop voorhanden is.

DE HUIDIGE SITUATIE?

- **TTP-beleid is een succes, maar het duurt iets langer**
- **TTP-beleid heeft gewed op het verkeerde paard**
- **Door bijsturing en doelverschuiving is een beleidsfiasco voorkomen**

TTP-beleid heeft gewed op het verkeerde paard
De tweede interpretatie is meer pessimistisch. Erkend wordt dat het feitelijk gerealiseerde resultaat er inderdaad is. Maar de nadruk ligt in deze interpretatie vooral op wat er niet is, en dat is een grote groep gecertificeerde TTP-dienstverleners (volgens het brede concept) met in het kielzog een nog veel grotere groep afnemers van deze diensten. De paar dienstverleners die er nu zijn, zo wordt in deze interpretatie gesteld, zullen het niet volhouden. De kosten van

het aanbod zijn immers hoog en de afnemers laten het vooralsnog massaal afweten. Een bloeiende en duurzame TTP-markt is ondanks het certificatieschema en de toezichtstructuur niet tot stand gekomen; de huidige markt is immers niet als zodanig te kwalificeren. De conclusie van deze interpretatie luidt dan ook dat het TTP-beleid op het verkeerde paard heeft gewed. Er is in de markt onvoldoende koopkrachtige vraag voor het hoge betrouwbaarheidsniveau dat het TTP-beleid waarborgt. Deels komt dat omdat er voldoende vertrouwen is in e-business met lagere veiligheidsniveaus en niet-gecertificeerde TTP-dienstverlening. Bovendien werken e-business en e-government met vormen van risicomanagement en wegen ze in dat kader de risico's van onveilige communicatie af tegen de kosten van TTP-dienstverlening en de veiligheid die dat met zich meebrengt. Of ze gaan duurzame relaties met hun consumenten of doelgroepen aan en realiseren in dat kader een eigen PKI-systeem. Daarom zal er zelden of nooit een businesscase zijn voor openbare TTP-dienstverlening.

Door transformatie van het TTP-beleid is een beleidsfiasco voorkomen
Een derde interpretatie waardeert vooral de transformaties die het TTP-beleid heeft doorgemaakt uiterst positief. Van Rij en Van Eeten (2003) analyseren de transformaties als typische vormen van 'goal displacement', het verleggen van de beleidsdoelen tijdens de uitvoering. Aanvankelijk beoogde het beleid de randvoorwaarden voor het ontstaan van een markt voor brede TTP-dienstverlening te creëren door met behulp van zelfregulering een 'kwaliteitskeurmerk' tot stand te brengen (certificatieschema en –procedure). Toen de Europese richtlijn deze beleidslijn in zekere zin doorkruiste, werd het beleidsdoel getransformeerd in het reguleren van de elektronische handtekening (wetgeving, omschrijven veiligheidsgaranties en toezichtstructuur). Bij de aansluiting op PKIoverheid veranderde het beleidsdoel wederom: het werd nu impliciet veranderd in het stimuleren van het gebruik van TTP-dienstverlening door de overheid als 'launching customer' te gebruiken. En bij de aansluiting met KWINT zou weer een verandering kunnen worden vastgesteld: nu komt het beleidsdoel neer op het benutten van TTP om kwetsbaarheden op het internet af te schermen. In deze interpretatie worden de doeltransformaties die het beleid heeft doorgemaakt positief gewaardeerd. Het feitelijk genoemde resultaat is inderdaad gerealiseerd en het oorspronkelijk geformuleerde beleidsdoel is inderdaad niet gehaald, aldus deze interpretatie, maar dat moeten we vooral opvatten als een zegen. Daarmee is immers een groot beleidsfiasco voorkomen. Volgens deze interpretatie zijn de oorspronkelijke veronderstellingen achter het TTP-beleid onjuist gebleken, maar is door alert reageren op omstandigheden het TTP-beleid zodanig veranderd dat het nu wel aansluit op de situatie in het beleidsveld.

5.4.2 Handelingsperspectieven

De handelingsperspectieven voor de toekomst van het TTP-beleid die we in het evaluatieonderzoek hebben aangetroffen, sluiten grotendeels aan op de interpretaties van de huidige situatie. In abstracto liggen voor de toekomst van het TTP-beleid drie wegen open: doorgaan met het huidige TTP-beleid (beleid ten aanzien van de geavanceerde elektronische handtekening), stoppen met het TTP-beleid of veranderen van het huidige TTP-beleid en met dat veranderde beleid doorgaan.

Concreet laten de handelingsperspectieven zich als volgt benoemen:

1. Doorgaan met huidige TTP-beleid. Dit handelingsperspectief sluit aan op de eerste, positieve diagnose. De versmalling van het oorspronkelijke TTP-concept, waardoor het zich de facto richt op de geavanceerde elektronische handtekening, staat voorop bij dit handelingsperspectief. Verondersteld wordt dat er wel een markt voor gecertificeerde TTP-dienstverlening is dan wel groeit, maar die komt langzaam op gang. De nu gecreëerde, wat afwachtende, markt kan met gerichte maatregelen, zoals destijds voorzien in het oorspronkelijke TTP-beleid, best nog een zetje worden gegeven. Het certificatieschema, alsmede de registratie- en certificatiestructuur die nu staan zijn technisch goed, sluiten aan op internationale standaarden en zijn in de praktijk beproefd. Het beleid zou zich dus moeten richten op het stimuleren van het gebruik van de geavanceerde elektronische handtekening:
   - Door 'pull-factoren' aan de zijde van de gebruikers: te denken valt aan voorlichting en onderwijs en wellicht nog eens een gericht experiment met e-government. Ook kan gedacht worden aan het bevorderen van de totstandkoming van applicaties die gekwalificeerde certificaten gebruiken, bijvoorbeeld met stimuleringssubsidies en -kredieten.
   - De markt een 'push' geven aan de zijde van de aanbieders van gecertificeerde dienstverlening. Hierbij moet vooral worden gedacht aan het verlagen van de kosten voor certificering en/of registratie. Daarnaast kan de gekwalificeerde elektronische handtekening snel op het nieuwe identiteitsdocument voor alle burgers worden opgenomen, zodat deze als authenticatiemiddel gebruikt kan worden voor applicaties voor de publieke sector en voor elektronische handel.

   Het beleid zoals zich dat in de praktijk heeft uitgekristalliseerd blijft verder onveranderd.

2. Stoppen met TTP-beleid. Dit handelingsperspectief komt erop neer dat het TTP-beleid zoals het ooit is ingezet, volledig wordt afgezworen. Het enige dat overblijft is het strikt onderhouden en uitvoeren van de wetgeving ter implementatie van de EU-richtlijn over elektronische handtekeningen. De hybride combinatie van certificering en toezicht, waarvoor nu een praktische oplossing is gevonden, kan als overblijfsel van het TTP-beleid efficiënter worden ingericht voor aanbieders van gekwalificeerde elektronische handtekeningen. Overwogen kan worden de rol van OPTA te beperken tot strikte registratie en de vrijwillige certificering uit het systeem te verwijderen. Op de vraag of het publiek toezicht door OPTA uit het systeem kan worden verwijderd en volstaan kan worden met een privaat stelsel van toezicht is geen eenduidig antwoord mogelijk. De Europese richtlijn is op dit punt namelijk niet scherp. Lidstaten hebben in het algemeen gekozen voor een stelsel van publiek toezicht, en hebben daar ook aanwijzingen in de richtlijn voor gevonden. In Nederland is bovendien aansluiting gezocht bij de bestuursrechtelijke toezichtsregeling van 5.2 Awb. Een internationaal-vergelijkend onderzoek concludeert daarentegen dat de richtlijn een privaat toezichtsregime niet verbiedt.[25] Ongeacht op welke manier het systeem 'leaner & meaner' wordt gemaakt, het brede TTP-concept met alle doelstellingen en instrumenten zoals die in 1999 zijn geformuleerd wordt in dit perspectief verlaten. De overweging hierbij is dat er kennelijk aan het betrouwbaarheidsniveau dat het TTP-concept biedt geen reële behoefte is omdat het overbodig, te duur of te complex is.

[25] http://europa.eu.int/information_society/eeurope/2005/all_about/security/electronic_sig_report.pdf

Wat resteert is een 'sober elektronisch handtekeningenbeleid', zonder overheidsbemoeienis met de uitvoering ervan.

3. Verbreden en veranderen van het TTP-beleid. Dit handelingsperspectief gaat ervan uit dat de geavanceerde elektronische handtekening de basis wordt van het TTP-beleid, maar dat het daar niet bij hoeft te blijven. In twee richtingen is een verbreding mogelijk. Ten eerste kan het oorspronkelijke TTP-concept nog eens grondig worden bekeken op kansen voor realisatie door zelfregulering en standaardisatie. Het is niet bij voorbaat uitgesloten dat delen ervan alsnog kunnen worden gerealiseerd langs deze weg. Denk bijvoorbeeld aan bepaalde integriteits-, authenticatie- en vertrouwelijkheidsdiensten. Verwacht mag worden dat certificering een zekere toegevoegde waarde (in termen van extra vertrouwen) zal blijven behouden en het is de moeite waard dat te proberen. Daarom zou het huidige TTP-beleid, dat te smal is door de concentratie op de elektronische handtekening moeten worden verbreed.

HANDELINGSPERSPECTIEVEN

- Doorgaan met gekwalificeerde handtekening (en stimuleren gebruik)
- Stoppen en minimaliseren overheidsbemoeienis
- Verbreden van de aanpak naar dienst en betrouwbaarheidsniveau

Daarnaast is nog een andere verbreding mogelijk. In het beleid is nu het 'hoogste' betrouwbaarheidsniveau gereguleerd. Er zijn allerlei vormen met een lager betrouwbaarheidsniveau waarvan het de moeite waard is te kijken of daarvoor ook een certificatieschema (met – procedure) kan worden ontwikkeld ter stimulering van het vertrouwen bij consumenten, bedrijfsleven en overheidsorganisaties. De 'TTP-manier', die gekenmerkt wordt door zelfregulering en standaardisatie, is hiervoor immers een geschikte methode gebleken. Door samenwerking van overheid, bedrijfsleven en deskundigen kan immers betrekkelijk goedkoop een betrouwbaar certificatieschema worden ontwikkeld dat helderheid biedt, uniformeert en tegelijkertijd een stimulans is voor het gebruik ervan.

Het is verleidelijk om als onderzoekers een voorkeur uit te spreken voor een van deze handelingsperspectieven. Waardevoller vanuit het evaluatieonderzoek zijn echter de aanknopingspunten en overwegingen die bij het maken van een keuze een rol spelen, althans zoals zich deze laten afleiden uit het onderzoek. Deze zijn gegrond in de lessen zoals we die hiervoor hebben geformuleerd:

- In de uitvoeringspraktijk is de situatie zo gegroeid dat de markt (zonder uniformering en standaardisatie) het overgrote deel van de zorg voor betrouwbare elektronische communicatie voor haar rekening neemt. Een vooralsnog uiterst hoog niveau van betrouwbaarheid wordt geboden door het certificatieschema. Deze 'taakverdeling' laat innovatie en diversiteit toe, maar garandeert tegelijkertijd een 'vangnet' voor het geval dat behoefte bestaat aan een hoog beveiligingsniveau. Het lijkt daarom een bevredigende uitkomst, die ruimte laat voor een marktbeweging in de richting van een hoger betrouwbaarheidsniveau als nieuwe ontwikkelingen op lagere betrouwbaarheidsniveaus (mits deze niet worden 'dichtgereguleerd'). Daarvoor is het

wel van belang dat het gebruik ervan toeneemt, omdat de kosten nu betrekkelijk hoog zijn.

- Voorspellen hoe de Europese markt voor de elektronische handtekening zich zal ontwikkelen is uiterst lastig, maar het is de vraag of de betrekkelijk dure oplossing waarvoor Nederland heeft gekozen een competitief aanbod zal genereren.
- Het oorspronkelijke beleidsontwerp dat uitgaat van brede openbare TTP-dienstverlening in een 'many-to-many-omgeving' is nooit feitelijk uitgevoerd, en daarom is het onmogelijk om zinvolle uitspraken te doen over de vraag of het feitelijk wel of niet de 'doorbraak' voor elektronische handel zal betekenen. Toch is het concept in ieder geval geen noodzakelijke voorwaarde gebleken voor het opbloeien van elektronische handel en tot op zekere hoogte ook elektronische overheidsdienstverlening. Er zijn weinig argumenten die ervoor pleiten om het oorspronkelijke concept nog eens van stal te halen. De situatie zoals deze in de praktijk is gegroeid dwingt wel tot expliciete reflectie op dat concept en de gevolgen daarvan voor het beleid zoals dat in 1999 is geformuleerd.
- Vrijwel alle gesprekspartners kijken (nog steeds) naar de overheid voor een 'doorbraak' in het beleid. De nieuwe identiteitskaart (eNIK) is daarvoor het startpunt: als deze een gekwalificeerde elektronische handtekening bevat, zal het gebruik ervan in de publieke en in de private sector toenemen, zo verwachten zij. Hoewel dit overtuigend en enthousiast wordt gebracht, dwingt de TTP-historie tot voorzichtigheid op dit punt. Aanvullend zou tenminste een strategie moeten worden gevolgd van samenwerking tussen overheid en bedrijfsleven, gericht op coördinatie en gezamenlijk gebruik van deze handtekening als authenticatiemechanisme (zoals in België op dit moment gebeurt). Ook hiervoor geldt de eerder geformuleerde les dat een enkelvoudige beleidsstrategie niet congruent is met een onzekere en turbulente context. Bovendien heeft de eNIK betrekking op burgers of consumenten, terwijl PKIoverheid de meeste mogelijkheden voor toepassing van een zwaar beveiligde PKI ziet in de relatie tussen overheid en bedrijfsleven.
- Hiermee hangt samen de vraag of er al dan niet een verdere uniformering van authenticatie- en identificatiemechanismen zal plaatsvinden. Vanuit overwegingen van kostenbesparing ligt dat, zowel binnen de overheid als tussen de publieke en private sector, wel voor de hand. De grote uitvoeringsorganisaties van de overheid hebben in hun manifest aangegeven daarnaar te streven, maar dan niet op het niveau van de gekwalificeerde elektronische handtekening. De banken hebben gekozen voor een gezamenlijke EMV-card, maar geconcludeerd dat een zware PKI niet nodig is, gezien de aard en omvang van de toepassingen.

Deze overwegingen laten zich afleiden uit het bevindingen van het evaluatieonderzoek. Interviews met marktpartijen leveren nog wat extra vragen op. De eNIK zal als geïsoleerd fenomeen niet vanzelfsprekend leiden tot gebruik, zo verwachten enkele marktpartijen. Er zijn immers nog geen toepassingen voorzien, en omdat marktpartijen in het algemeen geen meerwaarde verwachten van de gekwalificeerde handtekening ligt het niet voor de hand op korte termijn veel toepassingen te verwachten. Overigens hangt dit ook af van de prijs, zo blijkt uit de interviews met de in de bijlage genoemde marktpartijen. Het stimuleren van het gebruik zal dus in verschillende domeinen tegelijkertijd moeten plaatsvinden (overheid-overheid, overheid-bedrijfsleven, overheid-burger).
Overigens is de normatieve keuze voor een handelingsperspectief of een combinatie van de geschetste perspectieven een afweging die door beleidsmakers en politici moet worden gemaakt. Daarbij kan gebruik gemaakt worden van de gedachtewisseling in de door ons

georganiseerde toekomstworkshop, waarin de genoemde handelingsperspectieven nader zijn verkend.

In de discussie over de wenselijkheid ervan speelden de volgende argumenten een rol:

Ten aanzien van het 'stoppen'-perspectief:

- Het beleid is in principe klaar. Er moet wel duidelijkheid komen in het in de praktijk gegroeide onderscheid in identificatie- en beveiligingsniveaus, maar dit hoeft niet perse een overheidstaak te zijn en dat hoeft al helemaal niet onder de noemer TTP-beleid.
- In het huidige beleid wordt teveel gekeken naar de wijze waarop betrouwbaarheid en veiligheid op dit moment in de fysieke wereld zijn geregeld. Om deze zaken in de toekomst in de 'virtuele wereld' adequaat te regelen moeten we wellicht meer 'out of the box' denken dan het huidige TTP-beleid toelaat.
- De overheid heeft in feite geen taak in het regelen van beveiligingsniveaus voor elektronische transacties. Beleid is niet nodig omdat de markt in staat is dit op een kosteneffectieve wijze te regelen.

Ten aanzien van het perspectief van 'verbreding':

- Het is nodig om breder te kijken dan alleen naar PKI. Het oorspronkelijke TTP-concept was immers technologieonafhankelijk.
- Gezien de infrastructurele betekenis van het TTP-beleid moet dit niet geïsoleerd worden ontwikkeld, maar moet worden aangesloten bij het ICT-beleid van de overheid in het algemeen en het ICT-infrastructuurbeleid in het bijzonder.
- In de praktijk zijn inmiddels meerdere beveiligingslagen voor authenticatie tot stand gebracht. Het bestaande beleid moet op deze praktijk worden aangepast.

Ten aanzien van het perspectief van 'doorgaan':

- Het gebruik moet worden gestimuleerd door gebruikers meer (transparantie in) beveiligingsniveaus aan te bieden, bijvoorbeeld in de vorm van een ordening van deze niveaus en het door de overheid verzorgen van communicatie hierover (bijvoorbeeld in programma's als e-OK).
- Het gebruik moet ook worden gestimuleerd door het TTP-beleid meer weg te halen uit de hoek van de 'techneuten' en de focus te verschuiven naar de wereld van de managers/bestuurders. Zij beslissen tenslotte over het gebruik ervan en zij moeten dus van de meerwaarde overtuigd worden. Op dit moment wordt de discussie over elektronische handtekeningen te weinig gevoerd in termen die managers/bestuurders herkennen en aanspreken.
- Het Ministerie van Economische Zaken moet vooral inzetten op het stimuleren van de ontwikkeling van diensten op de huidige gerealiseerde infrastructuur.
- Speuren naar kansrijke initiatieven (ook in het buitenland) en het hier adequaat op inspelen biedt kansen voor intensiever gebruik van de huidige structuur. Een voorbeeld is de eventuele uitrol van de elektronische identiteitskaart zoals deze nu door ICTU wordt onderzocht.
- Het certificatieschema zoals dat er nu ligt, volstaat. Gewaakt moet worden voor nog meer normen en een eventuele verzwaring van de huidige normen (bijvoorbeeld als gevolg van verbreding van het concept). Het huidige beleid moet de kans krijgen te

groeien en volwassen te worden. Hierbij is het belangrijk om 'niet te ver voor de troepen uit te lopen'.
- Het smalle concept is voldoende omdat de markt nu kan beschikken over de gekwalificeerde handtekening, maar verder niet 'lastig wordt gevallen' met nog meer overheidsbemoeienis ten aanzien van het regelen van de betrouwbaarheid van elektronische transacties.
- Gewerkt moet worden aan de verdeeldheid van de overheid zelf ten aanzien van het gebruik van de geavanceerde elektronische handtekening. Dit zal leiden tot een stimulans voor het gebruik van de huidige voorzieningen.

Een meerderheid van de deelnemers aan de toekomstworkshop heeft zich uitgesproken voor een combinatie van 'doorgaan' en 'verbreden'. Zij zijn van mening dat het gebruik van wat nu is gerealiseerd gestimuleerd moet worden. Tevens dien zij mogelijkheden om het versmalde concept aan te passen. Deze verbreding, zo werd opgemerkt, moet wel aansluiten bij daadwerkelijke behoeften van potentiële gebruikers van de voorziening (bijvoorbeeld banken en grote bedrijven). Overigens is deze behoefte verre van statisch: het 'meten' ervan op een specifiek moment zegt daarom niet zo veel. Mede daarom zou volgens de pleitbezorgers van de combinatie 'doorgaan' en 'verbreden' eerst moeten worden ingezet op het stimuleren van het gebruik van de huidige voorziening (bijvoorbeeld gekoppeld aan eNIK en in samenwerking met banken en andere potentiële gebruikers); daarna is verbreden aan de orde.

6. De conclusies samengevat

6.1 Conclusies van het onderzoek

Uitvoering van het TTP-beleid
Na enkele jaren voorbereiding kondigt het Ministerie van Economische Zaken in juni 1999 beleid af dat de totstandkoming van openbare TTP-dienstverlening beoogt te stimuleren. Tijdens de uitvoering van dat beleid worden de beleidsmakers geconfronteerd met een Europese richtlijn over elektronische handtekeningen. De uitvoering van het TTP-beleid staat vanaf dat moment in het teken van implementatie van deze richtlijn. De juridische verankering van de elektronische handtekening gaat samen met een arrangement voor vrijwillige certificering van aanbieders (een certificatieschema in combinatie met een audit-, respectievelijk toezichtsstructuur). Feitelijk is daarmee een deel van het TTP-beleid uitgevoerd, namelijk dat deel dat zich richt op de elektronische handtekening. Intussen is in de afgelopen jaren de doelstelling van dat beleid, bloeiende elektronische handel, vooral los van het beleid gerealiseerd, wellicht minder dan verwacht als gevolg van de conjuncturele inzinking.

Huidige situatie?
Het TTP-beleid heeft zich in de praktijk ontwikkeld van een set van minimumvoorwaarden voor betrouwbare elektronische handel tot een arrangement dat garant staat voor een hoog niveau van veiligheid. Aan dat hoge niveau is vooralsnog weinig behoefte in de markt; zowel de overheid als het bedrijfsleven gebruiken momenteel voor elektronische handel en dienstverlening vooral lagere niveaus van beveiliging. Op deze niveaus heeft (nog) geen standaardisatie plaatsgevonden. Deze huidige situatie wordt, zo blijkt uit het onderzoek, op verschillende manieren geduid: (1) het TTP-beleid is goed opgezet en uitgevoerd, maar het duurt iets langer voordat het succes heeft, (2) er is door de beleidsmakers op het verkeerde (want te hoog beveiligde) paard gewed of (3) het oorspronkelijke beleid berustte niet op valide veronderstellingen, maar er is op tijd bijgestuurd als gevolg van de Europese richtlijn.

Hoe verder?
De keuze voor de toekomst van het TTP-beleid hangt mede af van de waardering van de huidige situatie. Ook is van belang welke inschatting wordt gemaakt van de ontwikkelingen die we de komende jaren kunnen verwachten. We hebben in het onderzoek drie handelingsperspectieven aangetroffen:

4. Doorgaan op de huidige weg en beleidsmatig inzetten op het stimuleren van het gebruik van het gerealiseerde hoge niveau. Sommigen verwachten sowieso een beweging in de markt naar hogere niveaus van beveiliging, zodat wat nu tot stand is gebracht in de (nabije) toekomst in een (meer of minder grootschalige) behoefte gaat voorzien. Bovendien zou de introductie van een elektronisch identiteitsdocument (eNIK) een nieuwe situatie kunnen creëren, omdat daarop een elektronische handtekening conform de huidige standaarden kan worden aangebracht. In dit perspectief kan het TTP-beleid nog wat extra stimulansen geven aan de markt: bijvoorbeeld door het verlagen van de kosten van certificering en/of registratie (door een tegemoetkoming in de kosten te bieden), door applicaties te bevorderen die gebruik maken van gekwalificeerde certificaten (bijvoorbeeld door stimuleringssubsidies of –kredieten) of door meer voorlichting en onderwijs.

5. Stoppen met het TTP-beleid zoals dat oorspronkelijk is geformuleerd en terugbrengen van de overheidsbemoeienis tot het onderhouden van de door de Europese richtlijn voorgeschreven wet- en regelgeving. In dit perspectief kan ook het huidige arrangement worden vereenvoudigd door bijvoorbeeld de vrijwillige certificering uit het systeem te verwijderen. Voor dit perspectief pleiten diegenen die uit de huidige situatie aflezen dat het TTP-beleid op het verkeerde paard heeft gewed. Betrouwbare elektronische communicatie via TTP is volgens hen immers geen voorwaarde gebleken voor het opbloeien van elektronische handel en elektronische overheidsdienstverlening. Aan het huidige, hoge niveau is geen behoefte, aldus de voorstanders van dit handelingsperspectief.
6. Verbreden van het beleid op basis van het oorspronkelijke TTP-concept. Op twee manieren is een verbreding mogelijk: verbreding van de TTP-diensten die onder het beleid vallen (naast elektronische handtekening ook andere diensten met betrekking tot authenticiteit, integriteit en vertrouwelijkheid van het berichtenverkeer) en/of verbreding van het betrouwbaarheidsniveau (dus ook standaardisatie van lagere niveaus). In beide gevallen betekent dit voor het beleid dat het huidige certificatieschema wordt uitgebreid of dat gewerkt wordt aan een of meer nieuwe schema's voor certificering.

In een toekomstworkshop die we in het kader van het evaluatieonderzoek hebben georganiseerd sprak een meerderheid van de deelnemers zich uit voor een combinatie van 'doorgaan' en 'verbreden'. Deze deelnemers zijn van mening dat het gebruik van de gekwalificeerde certificaten gestimuleerd moet worden. Tevens zien zij mogelijkheden om het versmalde concept aan te passen. Deze verbreding, zo werd opgemerkt, moet wel aansluiten bij daadwerkelijke behoeften van potentiële gebruikers van de voorziening (bijvoorbeeld banken en grote bedrijven). Overigens is deze behoefte verre van statisch: het 'meten' ervan op een specifiek moment zegt daarom niet zo veel. Mede daarom zou volgens de pleitbezorgers van de combinatie 'doorgaan' en 'verbreden' eerst moeten worden ingezet op het stimuleren van het gebruik van de huidige voorziening; daarna is verbreden aan de orde. Een kleine minderheid sprak zich tijdens de toekomstworkshop uit voor het perspectief 'stoppen'.
Overigens leveren de interviews met marktpartijen nog wat extra overwegingen op bij het maken van een keuze. Enkele marktpartijen verwachten dat de invoering van de elektronische identiteitskaart niet vanzelfsprekend zal leiden tot gebruik. Er zijn immers nog geen toepassingen voorzien, stellen ze, en omdat er van een eventueel op de kaart aangebrachte gekwalificeerd certificaat weinig meerwaarde kan worden verwacht zijn er op korte termijn weinig toepassingen te verwachten, aldus deze marktpartijen. Zij geven wel aan dat het al dan niet gebruiken van de gekwalificeerde elektronische handtekening afhangt van de prijs. Omdat we in het kader van het evaluatieonderzoek een beperkt aantal marktpartijen hebben gesproken, dienen deze conclusies met enige voorzichtigheid te worden geïnterpreteerd.

6.2 Antwoord op de vragen in de EZ-projectomschrijving

In de inleiding hebben we de vragen uit de projectomschrijving voor het evaluatieonderzoek van het Ministerie van Economische Zaken geordend en samengevat. In de hoofdstukken twee tot en met vijf zijn de bouwstenen aangedragen voor het beantwoorden van deze vragen. We vatten de antwoorden nog eens kort samen.

Doel gehaald?
Allereerst, zo schreven we in de inleiding, moet worden vastgesteld of de invulling van het beleidsdoel uit de notitie van 1999 is gehaald, in het bijzonder:

- Is er een markt voor TTP-dienstverlening ontstaan?
- In hoeverre heeft TTP-dienstverlening aantoonbaar bijgedragen aan betrouwbare elektronische communicatie ter ondersteuning van e-business en e-government?

Sinds de totstandkoming van het TTP-beleid is er inderdaad een markt voor TTP-dienstverlening ontstaan. Zowel voor integriteits- en authenticatiediensten als voor vertrouwelijkheidsdiensten is een groeiende markt. Deze markt heeft zich echter grotendeels los van de uitvoering van het TTP-beleid ontwikkeld (en deels zelfs ook los van de PKI-technologie waarop het beleid is gebaseerd). Alleen de beperkte markt voor gekwalificeerde elektronische handtekeningen is direct op uitvoering van het TTP-beleid terug te voeren. Daarmee wordt een technisch hoog betrouwbaarheidsniveau van elektronische communicatie gerealiseerd. Het gebruik van zo'n hoog niveau is in de praktijk van elektronische handel en elektronische overheidsdienstverlening nog uiterst beperkt. Elektronische handel en elektronische overheidsdienstverlening zijn vooral sterk gegroeid door alternatieve manieren om betrouwbare communicatie te realiseren. Zie verder voor effectiviteit paragraaf 4.3.

Doel congruent?
Het al dan niet realiseren van het beleidsdoel krijgt betekenis door dit in het licht te plaatsen van de beleidscontext (maatschappelijk, technologisch, juridisch-beleidsmatig). Dus:

- In hoeverre is er in de markt behoefte aan die betrouwbaarheid die TTP-dienstverlening mogelijk maakt in elektronische communicatie?
- In hoeverre is tot op heden betrouwbare elektronische communicatie voor e-business en e-government zonder tussenkomst van een TTP-dienst door alternatieve technieken en diensten ondersteund en in hoeverre is te verwachten dat dit in de voorzienbare toekomst zal plaatsvinden c.q. in omvang zal toenemen?
- In hoeverre past het TTP beleid bij technologische, maatschappelijke en juridisch-beleidsmatige ontwikkelingen en in hoeverre vormt het arrangement als geheel (en het TTP beleid daarbinnen) een consistent geheel?

Door de transformatie die het TTP-beleid in de uitvoering heeft doorgemaakt is het beleid in de praktijk veranderd van de oorspronkelijk beoogde set van minimumvoorwaarden in een regeling op een technisch hoog betrouwbaarheidsniveau, namelijk dat van de gekwalificeerde elektronische handtekening. Aan dat niveau van betrouwbaarheid blijkt in de markt nog betrekkelijk weinig behoefte. Er zijn twee aanbieders, waarvan een stelt over afnemers te beschikken. Uit het feitelijk gebruik tot nu toe laat zich dus aflezen dat de behoefte aan dit hoge niveau beperkt is. Veruit het grootste deel van de elektronische handel en elektronische overheidsdienstverlening vindt plaats door tussenkomst van alternatieve technieken en diensten. Openbare TTP-dienstverlening met behulp van PKI technologie (formeel behorend tot het oorspronkelijke TTP-beleid) maakt daarvan deel uit. De meeste betrokkenen verwachten dat de behoefte aan een hogere vorm van betrouwbare elektronische communicatie in de toekomst zal groeien, deels als gevolg van de incidenten en fraude die zij voorzien en deels als gevolg van het bundelen van de elektronische dienstverlening in de publieke sector. Zowel het TTP-beleid als de responsieve uitvoering zijn vooral ingegeven door ontwikkelingen en omstandigheden in de beleidsrelevante omgeving. In veel opzichten

zijn beleid/uitvoering en omgeving congruent; enkele kanttekeningen hierbij hebben we in de paragrafen 2.5 en 3.5 gemaakt.

Bijdrage van het beleid?
Het plaatsen van het beleid in de omgeving is niet voldoende om de effectiviteit ervan vast te stellen. Bepaald moet worden wat de *bijdrage van het TTP-beleid* is geweest aan het (geheel of ten dele) behalen van het beleidsdoel. Dus:

- In welke mate heeft het gevoerde beleid bijgedragen aan het proces van marktvorming?
- In hoeverre heeft het gevoerde beleidsinstrument van een vrijwillige certificatieregeling (TTP.nl) bijgedragen aan en geleid tot de doelen als de vorming van een TTP infrastructuur, kwaliteit van dienstverlening, vertrouwen van het betreffende publiek in die dienstverlening alsmede transparantie van de TTP markt?
- In hoeverre heeft het wettelijk toezicht door de OPTA bijgedragen aan en geleid tot de verwezenlijking van de doelstelling?

Het antwoord op deze vragen hangt af van de definitie en afbakening van TTP-beleid. Als het beleid beperkt wordt tot de geavanceerde elektronische handtekening, dan heeft het gevoerde beleid wel bijgedragen aan het proces van marktvorming, draagt de vrijwillige certificatie wel bij aan de feitelijke betrouwbaarheid van de TTP-dienstverlening (uiteraard voor zover potentiële aanbieders daarvan gebruik maken) en is het wettelijk toezicht door OPTA dwingend voorgeschreven door de Europese richtlijn. Als daarentegen het brede TTP-concept uit het oorspronkelijke beleidsontwerp als uitgangspunt wordt genomen, is de bijdrage van het beleid beperkt geweest. Slechts een klein deel van de TTP-dienstverlening wordt immers geraakt door het beleid, vanwege de dubbele versmalling die in de uitvoering heeft plaatsgevonden (geen brede TTP-dienstverlening, maar gekwalificeerde elektronische handtekening, geen PKI-technologie in algemene zin maar alleen de gekwalificeerde certificaten). De overige TTP-dienstverlening voltrekt zich buiten het beleid. Zie verder paragraaf 4.3.

Oorzaken van effectiviteit?
Het min of meer 'droog' vaststellen van de bijdrage van het TTP-beleid aan de genoemde doelstelling wordt gevolgd door een analyse van de *oorzaken* van effectiviteit. Dat komt neer op de volgende vragen:

- In hoeverre waren de oorspronkelijke assumpties waarop het TTP-beleid is gebaseerd valide (de beleidstheorie)?
- In hoeverre is effectief ingespeeld op veranderingen in de beleidsomgeving?

De volgende assumpties van het oorspronkelijke TTP-beleid zijn niet valide gebleken:

- Openbare TTP-dienstverlening is niet een belangrijke voorwaarde gebleken voor de ontwikkeling van elektronische handel en elektronische overheidsdienstverlening. Immers, elektronische handel en dito overheidsdienstverlening bloeien vooral buiten de reikwijdte van het TTP-beleid.
- Het reguleren en standaardiseren van het aanbod zal leiden tot een bloeiende markt voor TTP-dienstverlening. Immers, de behoefte aan het betrouwbaarheidsniveau dat het beleid uiteindelijk heeft gerealiseerd is tot nu toe zo beperkt gebleven dat getwijfeld wordt aan de levensvatbaarheid van de markt.

De volgende assumpties zijn wel valide gebleken:

- Het formuleren van randvoorwaarden en het realiseren van een toezichtstructuur hebben wel bijgedragen aan de feitelijke betrouwbaarheid van TTP-dienstverlening. De waarborgen voor veilige dienstverlening zijn immers hoger indien aan de eisen in het certificatieschema wordt voldaan.
- Ook werd terecht verondersteld dat regulering en standaardisatie het aanbod kunnen stimuleren (zie de geavanceerde elektronische handtekening). Eveneens is terecht van de veronderstelling uitgegaan dat het juist is om aan te sluiten op Europese ontwikkelingen; door vanaf de start voor aansluiting te kiezen is implementatie van de Europese richtlijn vergemakkelijkt.

Op belangrijke ontwikkelingen is in de uitvoering van het TTP-beleid snel en direct ingespeeld. Daardoor is de gekwalificeerde elektronische handtekening gerealiseerd en zijn de marktkansen voor TTP-dienstverlening aan de publieke sector verkend. Het zoeken van een verbinding met deze cruciale ontwikkelingen in de beleidsrelevante omgeving was dus logisch. Kanttekeningen daarbij zijn dat de uitvoering van het TTP-beleid daardoor is versmald en dat de beide ervaringen niet zichtbaar expliciet en systematisch zijn benut als leermoment voor het oorspronkelijke TTP-beleid. Zie verder paragraaf 3.5.

Efficiënt geweest?
Het evaluatieonderzoek beoogt niet alleen vast te stellen of het beleidsdoel is gerealiseerd en in welke mate het beleid daaraan heeft bijgedragen (effectiviteit), maar ook inzicht te geven in de verhouding tussen kosten en baten die het beleid veroorzaakt (*efficiëntie*). De daarbij behorende onderzoeksvraag luidt:

- Zijn de kosten die worden veroorzaakt door het TTP beleid (inclusief het bijbehorende instrumentarium) bij alle betrokken actoren (waaronder de TTP dienstverlener en de afnemers van deze dienstverlening) in verhouding met de verkregen baten?

We hebben geconcludeerd dat het vaststellen van de efficiëntie van het beleid op grote problemen stuit. Dat heeft primair te maken met het ontbreken van cijfers en de onmogelijkheid om deze achteraf in het kader van dit evaluatieonderzoek te reconstrueren. Vooral betrouwbare cijfers over de totale kosten van het beleid en cijfers over de verrichte investeringen door marktpartijen ontbreken. De efficiëntie van het beleid hangt overigens af van het beoordelingskader dat wordt gehanteerd. Gezien het feitelijk resultaat is het beleid betrekkelijk efficiënt geweest, maar bezien vanuit de feitelijke behoefte aan de gekwalificeerde elektronische handtekening op dit moment is het beleid betrekkelijk inefficiënt (lees: duur). Als het oorspronkelijke beleidsontwerp als vertrekpunt wordt gekozen, heeft vooral de transformatie die het beleid in de uitvoering heeft doorgemaakt bijgedragen aan de efficiëntie. Zie verder paragraaf 4.3.

Toekomst van het beleid?
Tenslotte komt het erop aan met het evaluatieonderzoek aanknopingspunten te formuleren voor de toekomst van het TTP beleid. Daarvoor hanteren we de volgende onderzoeksvragen:

- Wat zou, naar mening van de markt (zowel aanbod- als vraagzijde), de rol van de overheid in het vervolg moeten zijn?
- Op welke punten en in hoeverre is bijstelling van het beleid en het gehanteerde instrumentarium noodzakelijk of wenselijk?

- Kunnen de gestelde beleidsdoelen, gegeven het wettelijk kader, in de toekomst ook tegen lagere kosten worden bereikt en zo ja, hoe?

Op dit moment richt de bemoeienis van de overheid zich op 'de bovenkant' van de markt, namelijk de gekwalificeerde elektronische handtekening. Deels is deze bemoeienis voorgeschreven door de Europese richtlijn ten aanzien van de elektronische handtekening. Daarnaast komen uit het onderzoek drie mogelijke handelingsperspectieven voor de toekomst van het TTP-beleid. In het eerste perspectief wordt primair ingezet op het beleidsmatig ondersteunen en stimuleren van het gebruik van datgene dat nu is gerealiseerd (certificatieschema en certificeringsproces/toezichtstructuur). De structuur staat, nu komt het erop aan met het beleid de benutting of het gebruik daarvan te stimuleren. Het tweede perspectief komt praktisch neer op het afzweren van het TTP-beleid zoals dat oorspronkelijk is geformuleerd en het terugbrengen van de overheidsbemoeienis tot het onderhouden van de door de Europese richtlijn voorgeschreven wet- en regelgeving. Kortom een uiterst sobere bemoeienis van de overheid, beperkt tot het onderhouden van de wet- en regelgeving. Een laatste handelingsperspectief kiest het oorspronkelijke TTP-concept als uitgangspunt; gezocht zou kunnen worden naar mogelijkheden om het huidige beleid te verbreden naar het stimuleren en reguleren van uiteenlopende diensten (terug naar het oorspronkelijke TTP-concept) en uiteenlopende betrouwbaarheidsniveaus (van de elektronische handtekening). De bestuurlijk-organisatorische infrastructuur zou daarvoor kunnen worden benut; gestreefd zou kunnen worden naar uitbreiding van het huidige certificatieschema of opstellen van nieuwe certificatieschema's (al dan niet uitmondend in een juridische basis).
Het betrekken van de markt bij de keuze tussen deze handelingsperspectieven is in het onderzoek maar in beperkte mate mogelijk gebleken. In een toekomstworkshop bleek een meerderheid van de deelnemers te kiezen voor een combinatie van (eerst) doorgaan met het huidige beleid en (dan) zoeken naar mogelijkheden voor verbreding. Omdat het aantal marktpartijen in deze groep beperkt is geweëst, moet deze conclusie met de nodige voorzichtigheid worden geïnterpreteerd, zo leert de geschiedenis van het TTP-beleid. Zie verder paragraaf 5.4.

Verwijzingen

Berners-Lee, T. (2000), *De wereld van het World Wide Web*, Uitgeverij Nieuwezijds: Amsterdam.

Dyson, E. (1998), *Release 2.1. A design for living in the digital age*, Broadway Books, New York.

Ernst & Young (2001), Trends in ICT 2001 in relatie tot management en organisatie, Maarssen.

Franken, H., e.a. (1996), *De notaris en het elektronisch rechtsverkeer*, Koninklijke Vermande: Den Haag.

Gates, B. (1999), *Business @ the speed of thought. Succeeding in the digital economy*, Warner Books: New York.

Hardam, E (red.) (1999), *Trusted Third Party diensten voor de rijksoverheid. Vertrouwen in communiceren*, onderzoeksrapport in opdracht van het Ministerie van Binnenlandse Zaken, uitgevoerd door Nlsign bv., Den Haag.

Hof, S. van der, S. Huydecoper, Zwartepieten met certificatenaanbieders. De risicoverdeling in de Certification Practice Statement van BelSign, in: *Computerrecht*, 1998/5, pp. 214-221

Kabinet (1994), *Actieprogramma Elektronische Snelwegen. Van metafoor naar actie*, Den Haag.

Kabinet (1998), *Boven NAP. Herijking van het Nationaal Actieprogramma Elektronische Snelwegen (NAP)*, Den Haag.

Kabinet (1999), *De Digitale Delta. Nederland Online*, Den Haag.

Kelly, K. (1999), *Nieuwe regels voor de nieuwe economie. 10 radicale ondernemingsstrategieën in een wereld van netwerken*, Uitgeverij Nieuwezijds: Amsterdam.

Kleve, P. (1998), *Zijn TTP's nuttig?*, in: *Computerrecht*, 1998/5, pp. 211-213.

Koops, E.J. (1999), *The cryptocontroversy*, ECIS: Eindhoven.

Koops, E.J., R. van Kralingen, L. van der Wees (1998), De rol van Trusted third parties in het elektronisch handelsverkeer, in: *Computerrecht*, 1998/5, pp. 206-211.

Ministerie van Binnenlandse Zaken (1998), *Actieprogramma Elektronische Overheid*, Den Haag.

Pieper, R., V. Kouwenhoven en S. Hamminga (2002), *Beyond the Hype. E-business strategy in leading European companies*, Van Haren Publishing: Zeewolde.

Platform Informatiebeveiliging Werkgroep Encryptie, *Technische beveiligingsstudie Encryptie*, Lemma: Utrecht, 2002.

Rij, H.E. van (2002), *Evaluatiekader voor het TTP-beleid*, Delft.

Rij, H.E. van en M. van Eeten (2003), Gevangen door de markt. Evalueren van de verschuivende beleidsopgaven rond de elektronische handtekening, in: *Beleidswetenschap*, 2003/4, pp. 340-357.

Vlist, A van der en P. Noordam (1997), *Trends in IT. Op tijd investeren in de juiste technologie*, Kluwer Bedrijfsinformatie: Deventer.

Het citaat van Niels Bohr aan het begin van dit rapport is overgenomen uit het boek Breinbevingen van Jaap van Ginneken.

Bijlagen

Begrippenlijst

Accreditatie- en certificeringsysteem
Een vrijwillig systeem waarin auditors door de Raad voor Accreditatie worden geaccrediteerd voor het beoordelen van de certificatiedienstverleners. De auditors die door de Raad voor Accreditatie geaccrediteerd worden, zijn certificerende instellingen.
Certificatiedienstverleners die beoordeeld zijn door de certificerende instellingen en aan de normen voldoen, worden gecertificeerd.

Asymmetrisch sleutelpaar
Een publieke en private sleutel die wiskundig met elkaar zijn verbonden zodanig dat de publieke sleutel en de private sleutel elkaars tegenhanger zijn in de cryptografische berekening. Asymmetrische sleutelparen worden onder meer gebruikt voor het plaatsen en verifiëren van elektronische handtekeningen.

Authenticatie
Een proces waarbij de identiteit van iemand bevestigd kan worden of waarmee de integriteit van bepaalde informatie bewezen kan worden. Bij het authenticeren van berichten wordt de zender ervan bepaald en wordt nagegaan of het bericht niet gewijzigd of vervangen werd tijdens het versturen.

Certificaat
Een bericht dat ten minste de naam van de certificatieautoriteit vermeldt of deze identificeert en de abonnee identificeert. Dit certificaat bevat de publieke sleutel van de gebruiker, identificeert de operationele periode van het certificaat, bevat een certificaatserienummer en is digitaal ondertekend door de certificatieautoriteit. Een certificaat is vercijferd met de private sleutel van de certificatieautoriteit die de publieke sleutel heeft uitgegeven, waardoor het certificaat onvervalsbaar is.

Certificate Revocation List (CRL)
Een openbaar toegankelijke lijst, digitaal ondertekend door een certificatieautoriteit, met de vermelding van certificaten die vóór hun vervaldatum opgeschort of herroepen zijn. De lijst vermeldt meestal de uitgever ervan, de datum van uitgifte, de datum waarop de volgende lijst uitkomt, de serienummers van de opgeschorte of herroepen certificaten, het specifieke tijdstip van en de specifieke redenen voor de opschorting of herroeping.

Certificatiediensten
Het afgeven, beheren en intrekken van (gekwalificeerde) certificaten door certificatiedienstverleners, alsmede andere diensten die samenhangen met het gebruik van elektronische handtekeningen.

Certificatieautoriteit
Een entiteit binnen de verantwoordelijkheid van een certificatiedienstverlener die door één of meer eindgebruikers wordt vertrouwd om certificaten te maken en toe te wijzen. Een certificatieautoriteit geeft certificaten uit, schort ze op of herroept ze. Dit is de partij die feitelijk certificaten genereert. Dit betekent dat de CA niet de eindverantwoordelijkheid draagt voor de certificatiedienstverlening. De CA is een deelactiviteit die onder de verantwoordelijkheid van de CSP wordt uitgevoerd.

Elektronische handtekening
De elektronische handtekening is de elektronische variant van een gewone handtekening. Het is de benaming voor elektronische gegevens die zijn vastgehecht aan of logisch verbonden zijn met en elektronisch document. Hieronder valt bijvoorbeeld ook de ingescande handtekening van een papieren drager.

Gekwalificeerd certificaat
Een certificaat dat voldoet aan de eisen, gesteld krachtens artikel 18.15, tweede lid, van de Telecommunicatiewet en is afgegeven door een certificatiedienstverlener die voldoet aan de eisen, gesteld krachtens artikel 18.15, eerste lid van de Telecommunicatiewet.

Identificatie
Het proces waarbij de identiteit van een persoon (of een zaak) vastgesteld of bevestigd wordt.

Integriteit
De zekerheid dat gegevens volledig zijn en niet zijn gewijzigd, ongeacht of dat opzettelijk, niet opzettelijk door menselijk toedoen of anderszins is gebeurd.

Private sleutel
De sleutel van een asymmetrisch sleutelpaar die alleen bekend is bij de houder ervan.

Public Key Infrastructure - PKI
Een samenstel van architectuur, techniek, organisatie, procedures en regels, gebaseerd op public key cryptografie. Het doel is het hiermee mogelijk maken van betrouwbare elektronische communicatie en betrouwbare elektronische dienstverlening.

Publieke sleutel
De sleutel van een asymmetrisch sleutelpaar die publiekelijk bekend gemaakt kan worden.

Token
Beveiligde hardware waarop de private sleutels van de eindgebruiker opgeslagen worden. Een token kan ook cryptografische berekeningen uitvoeren. Voorbeelden van een token zijn een smartcard en een USB-token.

Vertrouwelijkheid
De garantie dat gegevens daadwerkelijk en uitsluitend terechtkomen bij degene voor wie zij zijn bedoeld, zonder dat iemand anders ze kan ontcijferen. Buiten de private sector wordt hiervoor ook wel de term exclusiviteit gebruikt.

Zie voor uitleg van deze begrippen onder andere:

http://www.silver-back.nl/definitie.php
http://www.secude.nl/secude/begrippenlijst.html
http://www.opta.nl/asp/aanbieders/elektronischehandtekeningen/begrippenlijst.asp
http://www.gea.nl/kennis/woordenboek.asp?LetterID=20&currentPage=5
http://www.referentiemodel.nl/00/begrippen/begripppen.htm

Overzicht van gesprekspartners voor het onderzoek

Geïnterviewd zijn:

R. van den Assem, VKA/Ministerie van Economische Zaken
D. Batenburg, Diginotar
T. Behre, ICTU
J. Boersma, ECP.NL
J.W. van Boven, Pink Roccade
R. de Bruin, ECP.NL
H. Dekker, PinkRoccade
R. van Eijl, OPTA
P. de Graaf, VNO/NCW
T. Hooghiemstra, NICTIZ
R. Houtsma, ICTU
B. de Jong, Interpay
F. de Jong, Silverback
A. Klein Twennaar, Rabobank
E. de Lange, Ministerie van Economische Zaken
A. van Leeuwen, Vereniging Kamers van Koophandel
R. van der Luit, Ministerie van Economische Zaken
H. Mijnheer, Ministerie van Economische Zaken –DGTP
P. Moll, KPN
P. Paling, KPMG
J. Timmermans, Ministerie van BZK
E. Verheul, PriceWaterhouseCoopers
O. Vermeulen, PriceWaterhouseCoopers
E. de Vries, Ministerie van Economische Zaken
S. de Vries, OPTA
R. Wagenaar, TU Delft
R. Weemhoff, IBM

Deelnemers aan expertmeeting/toekomstworkshop:

R. van den Assem, VKA/Ministerie van Economische Zaken
D. Batenburg, Diginotar
J. Boersma, ECP.NL
R. de Bruin, ECP.NL
C. Cuijpers, Universiteit van Tilburg
R. van Eijl, OPTA
G.J. van 't Eind, ICTU
P. de Graaf, VNO-NCW
E. Hardam, ICTU
J. Hermans, KPMG

- Is er in de markt behoefte aan TTP-dienstverlening? Zo ja, voor welke vormen van communicatie en transactie? In welke omstandigheden? Hoe schat u de omvang van deze markt in?
- Zowel door de overheid als door bedrijven worden uiteenlopende technieken gebruikt ter ondersteuning van e-business of e-government. Welke overwegingen spelen naar uw waarneming een rol bij de keuze van technieken en waarom komen deze 'gebruikers' wel of niet bij TTP-dienstverlening terecht?
- Wat zijn de kosten en baten van het TTP-beleid voor: (1) de overheid, (2) (potentiële) aanbieders van TTP-diensten? (inclusief kwantificering en onderbouwing)
- Wat is naar uw mening de bijdrage van de vrijwillige certificatieregeling geweest aan de ontwikkeling van de TTP-markt?
- In hoeverre draagt het wettelijk toezicht door de OPTA bij aan de effectiviteit van het TTP-beleid?

Toekomst van het TTP-beleid:

- Wat zijn in uw waarneming de belangrijkste (maatschappelijke, technologische en juridische) ontwikkelingen die de komende tijd zullen inwerken op het TTP-beleid en meer in algemene zin op elektronische communicatie en transactie?
- Welke elementen van het TTP-beleid zouden als gevolg daarvan ter discussie moeten worden gesteld of moeten worden veranderd?
- Hoe zou de effectiviteit van het TTP-beleid kunnen worden versterkt? En de efficiëntie?

Het gaat om semi-gestructureerde interviews.