Tweede Kamer der Staten-Generaal

2

Vergaderjaar 1998–1999

26 581 Nationaal TTP-project

Nr. 1

BRIEF VAN DE STAATSSECRETARIS VAN VERKEER EN WATERSTAAT

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

's-Gravenhage, 3 juni 1999

Mede namens de Minister van Economische Zaken bied ik u aan de notitie «Nationaal TTP-project». Deze notitie is het resultaat van een project dat in het kader van het Nationaal Actieprogramma Elektronische Snelwegen is uitgevoerd door het Ministerie van Verkeer en Waterstaat en het Ministerie van Economische Zaken, overigens met nauwe betrokkenheid van andere departementen en marktpartijen.

Een Trusted Third Party (TTP) is een vertrouwde derde die diensten aanbiedt om elektronische gegevensuitwisseling betrouwbaar te maken en is in die zin een belangrijk middel om elektronische handel tot bloei te laten komen. Een TTP kan diensten aanbieden om de authenticiteit (oorsprong van het bericht), integriteit (volledigheid en juistheid van het bericht) en vertrouwelijkheid (vercijfering van het bericht) van elektronische gegevensuitwisseling te garanderen. De notitie beoogt de randvoorwaarden te inventariseren voor het aanbieden van dergelijke TTP-diensten. Deze randvoorwaarden zullen in belangrijke mate door marktpartijen zelf moeten worden ingevuld. Hiermee is reeds aangevangen door de start van het implementatieproject TTP.NL eind 1998. Dit ingezette zelfreguleringsspoor is een initiatief van marktpartijen en wordt gestimuleerd door de overheid.

In de beleidsnotitie is een periode van twee jaar voorzien waarin de TTP-infrastructuur zich in Nederland kan ontwikkelen. Daarna zal een evaluatie plaatsvinden waarbij wordt getoetst in hoeverre de ontwikkelingen aan de gestelde randvoorwaarden voldoen en of deze voorwaarden toereikend zijn.

De Staatssecretaris van Verkeer en Waterstaat,
J. M. de Vries

KST35668
ISSN 0921 - 7371
Sdu Uitgevers
's-Gravenhage 1999

BELEIDSNOTITIE NATIONAAL TTP-PROJECT

Inhoudsopgave

0 MANAGEMENTSAMENVATTING

Het nationaal TTP-project

Informatie- en communicatietechnologie ontwikkelt zich in een zeer hoog tempo, waarbij de maatschappelijke afhankelijkheid van deze technologie sterk toeneemt. Vertrouwen en veiligheid bij het opslaan van gegevens en het uitwisselen van berichten worden hierdoor steeds belangrijker. Een belangrijke mogelijkheid om deze aspecten te waarborgen is het gebruik van zogenaamde Trusted Third Parties (TTP's), die tezamen een TTP-infrastructuur vormen.

Mede omdat deze mogelijkheid ook internationaal sterk in de belangstelling staat, heeft de Nederlandse overheid begin 1997 besloten tot de uitvoering van het nationaal TTP-project. Deze beleidsnotitie bevat de resultaten van dit nationale TTP-project, dat is uitgevoerd onder de vlag van het Nationaal Actieplan Elektronische Snelwegen. Het project is uitgevoerd onder auspiciën van het Ministerie van Verkeer en Waterstaat en het Ministerie van Economische Zaken.

Doelstellingen, scope en uitgangspunten van het nationaal TTP-project

Het nationaal TTP-project kent drie doelstellingen:
- het formuleren van randvoorwaarden voor het aanbieden en gebruiken van TTP-diensten;
- het inventariseren van instrumenten waarmee deze randvoorwaarden gewaarborgd kunnen worden;
- het stimuleren van de ontwikkeling van een Nederlandse TTP-infrastructuur.

Het nationaal TTP-project heeft uitsluitend betrekking op openbare TTP-diensten. Dit zijn TTP-diensten die in beginsel voor alle burgers, bedrijven en instellingen toegankelijk zijn en/of worden aangeboden via een openbare infrastructuur.

Marktwerking en deregulering zijn in het nationaal TTP-project als geldende beleidsuitgangspunten gehanteerd. De ontwikkeling van een TTP-infrastructuur wordt hierbij als een primaire verantwoordelijkheid van de markt beschouwd.

Wat is een TTP?

Trusted Third Parties (TTP's) zijn organisaties die diensten aanbieden om de betrouwbaarheid van elektronische gegevensuitwisseling te bevorderen.

Onder betrouwbaarheid wordt verstaan:
- de *authenticiteit* van gegevens;
- de *integriteit,* ofwel de juistheid en de volledigheid van gegevens;
- de *vertrouwelijkheid* van gegevens.

Wat doet een TTP?

TTP's leveren uiteenlopende diensten aan burgers, bedrijven en instellingen, waaronder:
- diensten voor *authenticiteit en integriteit,* zoals het uitgeven van elektronische certificaten die worden gebruikt bij het zetten en controleren van digitale handtekeningen, waarbij de TTP de rol van

Certification Authority (CA) vervult, en het bewaren en tijdstempelen van berichten;
- diensten voor *vertrouwelijkheid,* zoals het versleutelen van berichten en transacties, en het aanmaken, verstrekken en bewaren van cryptografisch sleutelmateriaal.

Waarom zijn TTP's belangrijk?

TTP's kunnen door het leveren van specifieke diensten een centrale rol spelen bij de ontwikkeling van een betrouwbare infrastructuur voor electronic commerce. Dit geldt voor TTP's die digitale handtekeningen verzorgen, maar ook voor TTP's die gegevens versleutelen of cryptografisch sleutelmateriaal verstrekken.

Burgers, bedrijven en instellingen zullen een hoge mate van vertrouwen stellen in de diensten die door een TTP worden aangeboden. Dit vertrouwen heeft niet alleen betrekking op de betrouwbaarheid van het berichtenverkeer en opgeslagen gegevens, maar ook op zaken als privacy, aansprakelijkheid, zorgvuldigheid, rechtmatige toegang tot gegevens en internationale aansluiting.

Wat is het belang van randvoorwaarden?

Door middel van randvoorwaarden kan worden zekergesteld dat het in TTP's gestelde vertrouwen gewaarborgd is en kan worden voorkomen dat de belangen van de betrokken partijen worden geschaad. Randvoorwaarden bieden daarbij een referentiekader voor de nationale en internationale wederzijdse erkenning van TTP's, die noodzakelijk is in het kader van grensoverschrijdend elektronisch handelsverkeer.

Wie stelt de randvoorwaarden?

Randvoorwaarden kunnen worden gesteld door alle partijen die een belang hebben bij een betrouwbare TTP-infrastructuur: burgers, bedrijfsleven en overheden, zowel nationaal als internationaal. In het nationaal TTP-project is ernaar gestreefd de belangen van zoveel mogelijk betrokken partijen in overweging te nemen.

Op basis van een uitgebreid onderzoek is een verzameling van randvoorwaarden opgesteld, waaraan elke TTP naar inzicht van de projectgroep zou moeten voldoen. De randvoorwaarden zijn voorgelegd aan een breed samengestelde Consultatiegroep Aanbieders en Gebruikers (CAG) en vervolgens getoetst in een viertal proefprojecten.

Hoe kunnen randvoorwaarden in de praktijk worden gerealiseerd?

Om te bewerkstelligen dat TTP's in de toekomst ook daadwerkelijk aan de opgestelde randvoorwaarden zullen voldoen, beschikt de overheid over verschillende instrumenten, die variëren van regulering en wetgeving tot *deregulering en marktwerking. In het nationaal TTP-project zijn deregu*lering en marktwerking als uitgangspunten gekozen. Het maatschappelijk belang van een betrouwbare TTP-infrastructuur is echter zo groot, met name daar waar diensten voor vertrouwelijkheid worden aangeboden, dat voor deze laatstgenoemde diensten uitgangspunt is dat zelfregulering een wettelijke verankering krijgt.

De TTP-kamer

Concreet beveelt de projectgroep de oprichting van een TTP-kamer aan. De TTP-kamer is een overkoepelende organisatie, waarin, naast de overheid, zowel de aanbieders als de gebruikers van TTP-diensten op vrijwillige basis zitting hebben, en waarbij minimaal de in deze beleidsnotitie opgestelde randvoorwaarden worden opgenomen in een bindend reglement.

Wat zijn de voordelen van een TTP-kamer?

Aan het oprichten van een TTP-kamer zijn als belangrijkste maatschappelijke voordelen verbonden:
- het waarborgen van de belangen van de betrokken partijen;
- het bevorderen van de noodzakelijke aansluiting en wederzijdse erkenning tussen Nederlandse TTP's en internationale TTP-infrastructuren;
- het stimuleren van de ontwikkeling van een betrouwbare TTP-infrastructuur door de markt.

Om welke randvoorwaarden gaat het?

Randvoorwaarden verschillen van TTP-dienst tot TTP-dienst. Een primair onderscheid is gemaakt tussen TTP-diensten voor authenticiteit en integriteit en TTP-diensten voor vertrouwelijkheid.

a. *TTP-diensten voor authenticiteit en integriteit (digitale handtekening)*
Aan deze categorie van TTP-diensten worden onder meer randvoorwaarden gesteld die betrekking hebben op betrouwbaarheid, privacy, interoperabiliteit, onafhankelijkheid, aansprakelijkheid, bezwaar en verhaal.

b. *TTP-diensten voor vertrouwelijkheid (versleuteling)*
Aan deze categorie van TTP-diensten worden dezelfde randvoorwaarden gesteld als onder (a). Daarnaast worden aanvullende randvoorwaarden gesteld, die betrekking hebben op rechtmatige toegang en exportcontrole.

Een TTP die beide categorieën van TTP-diensten aanbiedt, zal aan beide categorieën van randvoorwaarden moeten voldoen.

Conclusies

Overheid en bedrijfsleven dienen een aantal concrete maatregelen te treffen om de snelle ontwikkeling van een betrouwbare TTP-infrastructuur te bevorderen. Daarbij zal aansluiting worden gezocht bij het zelfreguleringsmechanisme.

Overheid, aanbieders en gebruikers van TTP-diensten dienen het initiatief te nemen tot het oprichten van een TTP-kamer, die waarborgt dat aan de gestelde randvoorwaarden wordt voldaan. In de TTP-kamer hebben, naast de overheid, zowel de aanbieders als de gebruikers van TTP-diensten op vrijwillige basis zitting.

De overheid dient de oprichting van genoemde TTP-kamer te begeleiden en te stimuleren. Aan deze stimulering dient zo spoedig mogelijk invulling te worden gegeven.

De overheid dient TTP's die zich bij de TTP-kamer aansluiten te stimuleren. Aan deze stimulering dient zo spoedig mogelijk invulling te worden gegeven.

De overheid dient de totstandkoming van een certificatieschema te stimuleren, waarbij de in deze beleidsnotitie genoemde randvoorwaarden dienen te worden vertaald naar hanteerbare certificatiecriteria.

In principe dient de overheid uitsluitend diensten af te nemen van TTP's die zich bij de TTP-kamer hebben aangesloten.

De overheid dient de ontwikkeling en het gebruik van apparatuur en programmatuur die bijdraagt aan een betrouwbare TTP-infrastructuur te stimuleren.

De overheid dient het Nederlandse beleidsmodel in het kader van de wederzijdse erkenning van TTP's internationaal uit te dragen.

Terzake de in hoofdstuk 4.3 beschreven specifieke randvoorwaarde van rechtmatige toegang dient daarnaast via een partnership approach tussen de overheid en het relevante bedrijfsleven een voor alle partijen aanvaardbaar instrumentarium voor het faciliteren van de rechtmatige toegang te worden ontwikkeld. Om te waarborgen dat het relevante bedrijfsleven dit nog te ontwikkelen instrumentarium ook daadwerkelijk toepast zal ook hier aansluiting worden gezocht bij een zelfreguleringsmechanisme. Uitgangspunt hierbij zal zijn dat deze zelfregulering een wettelijke verankering krijgt.

De overheid dient na uiterlijk twee jaar de ontwikkelingen in Nederland te evalueren, waarbij wordt getoetst in hoeverre deze ontwikkelingen aan de gestelde randvoorwaarden voldoen en of de gestelde voorwaarden toereikend zijn.

1 INLEIDING

Informatie- en communicatietechnologie ontwikkelt zich in een zeer hoog tempo. De maatschappelijke afhankelijkheid van deze technologie neemt eveneens sterk toe. Vertrouwen en veiligheid bij het opslaan van gegevens en het uitwisselen van berichten worden hierdoor steeds belangrijker. Daarbij zijn drie aspecten van belang. In de eerste plaats is van belang dat een partij voldoende zekerheid heeft over de identiteit van zijn communicatiepartners en de herkomst van berichten en transacties. In de tweede plaats is van belang dat gegevens niet door onbevoegden kunnen worden gewijzigd. In de derde plaats is het van belang dat geen kennis kan worden genomen van informatie door partijen voor wie deze informatie niet bestemd is. Met andere woorden: de *authenticiteit, integriteit en vertrouwelijkheid* van gegevens, berichten en transacties dienen in voldoende mate gewaarborgd te zijn. Deze aspecten zijn in toenemende mate bepalend voor de kwaliteit van dienstverlening in het elektronisch handelsverkeer.

Voor waarborgen van deze kwaliteitsaspecten bestaan tal van technische, organisatorische en juridische maatregelen. In de nabije toekomst kan een belangrijke rol zijn weggelegd voor derde partijen die de betrouwbaarheid van het elektronisch berichtenverkeer verhogen door het leveren van specifieke ondersteunende diensten terzake. Zulke partijen worden internationaal algemeen aangeduid als Trusted Third Parties (TTP's). De door deze partijen geleverde ondersteunende diensten zijn in veel gevallen gebaseerd op het gebruik van cryptografische technieken. Zij hebben onder meer betrekking op het verstrekken van elektronische certificaten; het plaatsen en verifiëren van digitale handtekeningen; het vercijferen van elektronisch berichtenverkeer; het genereren, verstrekken, opslaan en/of vernietigen van cryptografisch sleutelmateriaal (sleutel-

beheer); het onweerlegbaar aantonen van verzending en ontvangst van elektronische berichten; en het bewaren en tijdstempelen van elektronische berichten en gegevens, al dan niet in versleutelde vorm.

Het maatschappelijk belang van TTP's bestaat primair uit het bieden van faciliteiten voor een betrouwbare en nationaal en internationaal erkende digitale handtekening, die in het elektronisch handelsverkeer noodzakelijk wordt geacht, en uit het bieden van mogelijkheden voor veilige berichtenuitwisseling voor burgers en bedrijven, waardoor de vertrouwelijkheid van het berichtenverkeer kan worden gewaarborgd. TTP's kunnen dan ook een belangrijke rol spelen bij de opbloei van een veilige, betrouwbare en beheersbare infrastructuur voor electronic commerce. Om die reden wordt een snelle ontwikkeling van TTP-infrastructuren in brede kring zeer wenselijk geacht. Het maatschappelijk belang van een dergelijke ontwikkeling vereist duidelijkheid omtrent de rol van zowel de overheid als de marktpartijen.

In het kader van het Nationaal Actieprogramma Elektronische Snelwegen (NAP) is het initiatief genomen tot het uitvoeren van het nationaal TTP-project. Dit project vindt plaats onder gemeenschappelijk opdrachtgeverschap van het Ministerie van Economische Zaken en het Ministerie van Verkeer en Waterstaat.

Doel van het project is het formuleren van randvoorwaarden voor het aanbieden en gebruiken van TTP-diensten in Nederland. Daarnaast is geïnventariseerd op welke wijze en met behulp van welke instrumenten zulke randvoorwaarden zouden kunnen worden gewaarborgd. Een andere belangrijke doelstelling van het project is het stimuleren van een verantwoorde ontwikkeling en exploitatie van een Nederlandse TTP-infrastructuur. Het project is uitgevoerd conform de door de projectgroep NAP/TTP goedgekeurde opzet en het projectplan [1,2].

Het project is opgedeeld in vier hoofdfasen, te weten:
- Fase 1 – Opstellen projectplan;
- Fase 2 – Formulering randvoorwaarden;
- Fase 3 – Begeleiding en beoordeling pilotprojecten;
- Fase 4 – Opstellen beleidsnotitie.

Het project is in april 1997 gestart en is in maart 1999 afgerond.

Hoewel het project is gericht op de nationale situatie, kan het niet los worden gezien van internationale ontwikkelingen. Als belangrijkste reden geldt het inherent mondiale karakter van elektronische dienstverlening in het algemeen en electronic commerce in het bijzonder. Daarnaast geldt de noodzaak de nationale beleidsvorming reeds in de voorbereidende fase af te stemmen op internationaal beleid, zoals dat onder meer verder wordt ontwikkeld door de EU [21] en de OECD [12,20].

Het project wordt gekenmerkt door een resultaatgerichte, pragmatische aanpak, waarbij steeds afstemming wordt gezocht met internationale ontwikkelingen. De gekozen invalshoek is niet zozeer technisch als wel bestuurlijk, beleidsmatig en juridisch van aard.

In het project is een belangrijke plaats ingeruimd voor het inventariseren van belangen en ontwikkelingen aan zowel de vraagzijde als de aanbodzijde van de markt. Hiertoe is in het kader van het project een aantal door de markt aangedragen proefprojecten begeleid en geëvalueerd. Daarnaast is een breed samengestelde Consultatiegroep Aanbieders en Gebruikers (CAG) opgericht, die bij het project is betrokken.

Ten slotte zijn marktwerking en deregulering in het nationaal TTP-project als geldende beleidsuitgangspunten gehanteerd. Dit impliceert onder meer dat de ontwikkeling van een TTP-infrastructuur als een primaire verantwoordelijkheid van de markt wordt beschouwd.

De inhoud van deze beleidsnotitie is als volgt. Sectie 2 bevat een beschrijving van het gehanteerde begrippenkader, de context en de scope van het nationaal TTP-project. Sectie 3 gaat in op de randvoorwaarden inzake TTP-diensten voor authenticiteit en integriteit van gegevens, berichten en transacties. Sectie 4 gaat in op randvoorwaarden inzake TTP-diensten voor vertrouwelijkheid van gegevens, berichten en transacties. Sectie 5 gaat in op de mogelijke instrumenten voor het waarborgen van deze randvoorwaarden. Sectie 6 bevat de conclusies en aanbevelingen van het project.

Bijlage 1 bevat de resultaten van de inventarisatie van de proefprojecten, die is uitgevoerd door de EDP AUDIT POOL. Bijlage 2 bevat een opsomming van de in dit project geraadpleegde bronnen. Bijlage 3 beschrijft de samenstelling van de projectgroep en de Consultatiegroep Aanbieders en Gebruikers.

2 OMSCHRIJVING, CONTEXT EN SCOPE

In deze sectie komen achtereenvolgens aan de orde: de betekenis die in de context van het nationaal TTP-project aan de term TTP wordt gehecht, de bij het nationaal TTP-project betrokken partijen, een classificatie van TTP-diensten op basis van verschillende criteria, de stand van zaken rond nationale en internationale beleidsontwikkeling terzake, de totstandkoming van de in deze beleidsnotitie genoemde randvoorwaarden die op TTP's en TTP-diensten van toepassing zijn, en het mogelijke instrumentarium om deze randvoorwaarden in de praktijk te waarborgen.

2.1 Omschrijving

De term Trusted Third Party (TTP) is inmiddels algemeen ingeburgerd, maar blijkt soms op uiteenlopende wijzen te worden geïnterpreteerd. In het kader van deze beleidsnotitie wordt de volgende werkdefinitie gehanteerd:

Een Trusted Third Party (TTP) is een betrouwbare derde partij die diensten aanbiedt om de betrouwbaarheid van de geautomatiseerde verwerking, uitwisseling en opslag van gegevens tussen partijen te waarborgen.

Onder betrouwbaarheid wordt verstaan:
- de *authenticiteit* van gegevens;
- de *integriteit*, ofwel de juistheid en de volledigheid van gegevens;
- de *vertrouwelijkheid* van gegevens.

Bedoelde TTP-diensten kunnen onder meer betrekking hebben op: het verstrekken van digitale certificaten; het plaatsen en verifiëren van digitale handtekeningen; het versleutelen van elektronisch berichtenverkeer en/of gegevens; het genereren, verstrekken, opslaan en/of vernietigen van cryptografisch sleutelmateriaal (sleutelbeheer); het onweerlegbaar aantonen van verzending en ontvangst van elektronische berichten; het bewaren en tijdstempelen van elektronische berichten.

2.2 Betrokken partijen

Bij de ontwikkeling en het gebruik van TTP-infrastructuren is een groot aantal nationale en internationale partijen betrokken. Hierbij kan primair onderscheid worden gemaakt tussen marktpartijen en overheid. Er geldt echter een bijzondere situatie voor partijen met een wettelijke bevoegdheid tot het verkrijgen van elektronische gegevens; het betreft hierbij zowel de marktpartijen als de overheid.

2.2.1 Marktpartijen

De belangrijkste rol is weggelegd voor de *marktpartijen*, ofwel de aanbieders en gebruikers van TTP-diensten. TTP-diensten kunnen worden aangeboden door zeer uiteenlopende commerciële en niet-commerciële organisaties die al dan niet binnen een specifiek marktsegment opereren. Anderzijds kunnen TTP-diensten worden afgenomen door bedrijven, instellingen en burgers. In het nationaal TTP-project hebben de marktpartijen hun inbreng kunnen geven via een hiertoe opgerichte Consultatiegroep Aanbieders en Gebruikers, waarvan de samenstelling is weergegeven in bijlage 3.

2.2.2 Overheid

Gezien het maatschappelijk belang zal een rol voor de overheid zijn weggelegd in de vorm van beleid, stimulering, wet- en regelgeving en/of toezicht. De algemene gedachte hierbij is dat de *overheid* tenminste tot taak heeft om, gebruikmakend van het ter beschikking staande instrumentarium, 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 de totstandkoming van een veilige en betrouwbare TTP-infrastructuur stimuleren. Ten slotte kan de overheid als marktpartij opereren – als afnemer, maar ook als aanbieder van TTP-diensten. De bij het nationaal TTP-project betrokken ministeries zijn weergegeven in Bijlage 3.

2.3 Classificatie van TTP-diensten

TTP-diensten kunnen op verschillende wijzen worden geclassificeerd. Deze classificatie is noodzakelijk, omdat het type van een TTP in veel gevallen bepalend is voor de randvoorwaarden die aan de TTP worden gesteld. Achtereenvolgens komen aan de orde: de functionaliteit van de TTP-dienst; de wijze van sleutelbeheer; de openbaarheid van de TTP-dienst; de topologie van de TTP-dienst; en het toepassingsgebied van de TTP-dienst.

2.3.1 Functionaliteit van de TTP-dienst

Zoals reeds in de hierboven gegeven werkdefinitie naar voren komt, kan een TTP-dienst uiteenlopende vormen aannemen. Hierbij bestaat een wezenlijk onderscheid tussen TTP-diensten die gericht zijn op het waarborgen van de *authenticiteit en/of integriteit van gegevens*, berichten en transacties, en TTP-diensten die gericht zijn op het waarborgen van de *vertrouwelijkheid* van gegevens, berichten en transacties:

a. *TTP-diensten voor authenticiteit en integriteit*
   Onder TTP-diensten voor authenticiteit en integriteit vallen onder meer: het verstrekken van digitale certificaten (de TTP vervult hierbij de rol van Certification Authority, CA); 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, uitgezonderd de opslag van geheim sleutelmateriaal terzake (private keys); en het tijdstempelen van elektronische berichten.

b. *TTP-diensten voor vertrouwelijkheid*
Onder TTP-diensten voor vertrouwelijkheid vallen onder meer: het versleutelen van elektronisch berichtenverkeer; en het beheer van cryptografisch sleutelmateriaal voor vertrouwelijkheid.

Het aldus gemaakte onderscheid wordt ook in internationaal verband gemaakt en is in recente internationale beleidsdocumenten van de EU, OECD en APEC [21, 12, 20] als zodanig aanvaard. Het onderscheid is in die zin fundamenteel, dat niet alleen de TTP-diensten zelf, maar ook de hierop van toepassing zijnde randvoorwaarden verschillen. Zo ligt bij TTP-diensten voor *authenticiteit en integriteit* een zware nadruk op randvoorwaarden ten aanzien van betrouwbaarheid, privacy en interoperabiliteit, zoals genoemd in sectie 3, terwijl bij TTP-diensten voor *vertrouwelijkheid* bovendien de in sectie 4 genoemde aanvullende randvoorwaarden ten aanzien van rechtmatige toegang tot gegevens en exportcontrole gelden.

Een en ander impliceert overigens niet dat een TTP zijn diensten voor authenticiteit en integriteit en zijn diensten voor vertrouwelijkheid altijd gescheiden aanbiedt; ook een combinatie van beide diensten is mogelijk. Gegeven de huidige stand van de techniek kunnen beide TTP-diensten eenvoudig en efficiënt met behulp van één enkele technische oplossing worden gerealiseerd.

Het aanbieden van gescheiden oplossingen voor de onderscheiden klassen van TTP-diensten behoort echter zeer wel tot de mogelijkheden. Zo kan een TTP-dienst voor authenticiteit en integriteit worden geboden op basis van een toegevoegde digitale handtekening, waarbij het bericht zelf onvercijferd blijft. Een aanvullende TTP-dienst voor vertrouwelijkheid kan dan bijvoorbeeld bestaan uit het aanleveren van additioneel sleutelmateriaal voor de versleuteling van het bericht zelf. Sleutelmateriaal voor authenticiteit en integriteit kan door de gebruiker eenvoudig ook voor vertrouwelijkheid worden aangewend, tenzij hiertegen door de TTP specifieke technische maatregelen zijn getroffen; voor meer details zij verwezen naar [12, 21].

De internationale aanvaarding van het beleidsmatige onderscheid tussen TTP-diensten voor authenticiteit en integriteit en TTP-diensten voor vertrouwelijkheid kan ertoe leiden dat de TTP-markt deze diensten in toenemende mate gescheiden zal aanbieden. Hoewel gescheiden oplossingen op de markt beschikbaar zijn, worden beide diensten door een aantal van de in fase 3 onderzochte proefprojecten niet gescheiden aangeboden.

2.3.2 Wijze van sleutelbeheer

Een tweede onderscheidend criterium is de wijze waarop het sleutelbeheer is ingericht. Onder sleutelbeheer wordt hierbij verstaan: het genereren, opslaan, distribueren, vernietigen en/of intrekken van sleutelmateriaal. Voor de inrichting van sleutelbeheer bestaan verschillende varianten, waarbij de TTP in meer of mindere mate bij het sleutelbeheer betrokken is.

In het ene uiterste geval zal de TTP zelf sleutelmateriaal genereren, opslaan, distribueren en na verloop van tijd vernietigen. In het andere

uiterste geval is de gebruiker zelf volledig verantwoordelijk voor het sleutelbeheer. Ook tussenvormen zijn mogelijk, zoals een vorm waarbij de gebruiker zelf het sleutelmateriaal genereert en zijn openbare sleutel bij een TTP deponeert, of zelfs een vorm waarbij de gebruiker, onder strikte voorwaarden, geheim sleutelmateriaal bij een TTP deponeert.

Bij het merendeel van de in fase 3 onderzochte proefprojecten genereert de gebruiker zelf het sleutelmateriaal, waarna hij de openbare sleutel bij een TTP deponeert. De desbetreffende aanbieders hebben geen intenties om te voorzien in de opslag van geheim sleutelmateriaal.

2.3.3 Openbaarheid van de TTP-dienst

De openbaarheid van een TTP-dienst vormt een derde belangrijk onderscheidend criterium bij het bepalen van de wenselijke en/of noodzakelijke invloed van de overheid terzake. Voor de term openbaar is aansluiting gezocht bij de Telecommunicatiewet.

Niet-openbare TTP-diensten worden hierbij gedefinieerd als TTP-diensten die uitsluitend gebruik maken van een eigen infrastructuur en uitsluitend binnen één organisatie worden gebruikt. Voorbeelden hiervan zijn TTP's binnen één bedrijf of instelling, of TTP's die exclusief worden gebruikt door een beperkt aantal bedrijven of instellingen die onderling berichten uitwisselen. Daartegenover staan *openbare TTP-diensten,* gedefinieerd als TTP-diensten die in beginsel gebruik maken van een openbare infrastructuur en/of voor alle burgers, bedrijven en instellingen toegankelijk zijn.

Het nationaal TTP-project heeft uitsluitend betrekking op openbare TTP-diensten.

2.3.4 Topologie van de TTP-dienst

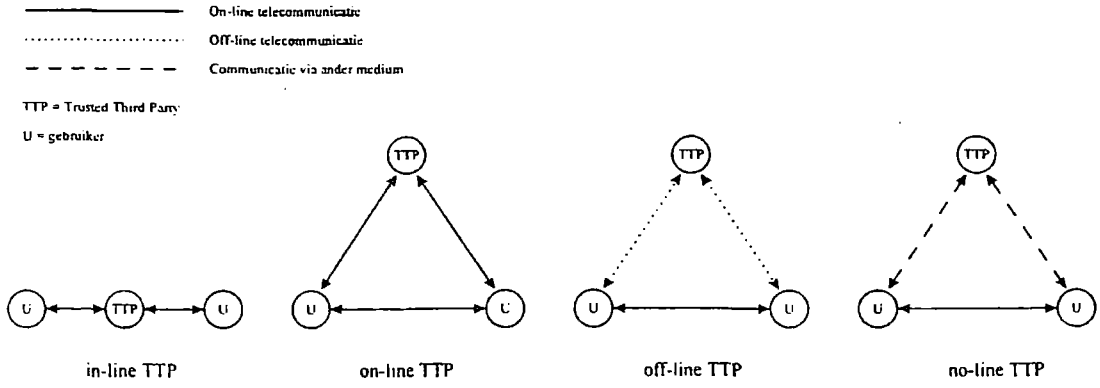
De topologie van een TTP-dienst – in het kader van het nationaal TTP-project geïnterpreteerd als: de positie die de TTP-dienst inneemt in de communicatie tussen partijen – wordt als vierde belangrijke indelingscriterium gehanteerd. Gegeven de huidige stand van de techniek kan op dit moment onderscheid worden gemaakt tussen drie TTP-topologieën, waarbij wordt aangesloten op gangbare definities van onder meer het ETSI [11] (zie figuur 1):

- de *in-line TTP,* die met elk van de aangesloten partijen een direct of indirect telecommunicatiepad onderhoudt, waarbij deze partijen onderling uitsluitend via de TTP met elkaar communiceren;
- de *on-line TTP,* die met ten minste één van de met elkaar communicerende partijen een telecommunicatiepad onderhoudt, terwijl deze partijen onderling ook een afzonderlijk telecommunicatiepad onderhouden;
- de *off-line TTP,* die gedurende de communicatie tussen twee partijen geen telecommunicatiepad met deze partijen onderhoudt, maar de benodigde communicatie op een ander tijdstip voert.

Daarnaast wordt in deze beleidsnotitie een vierde TTP-type onderscheiden, dat kan worden beschouwd als een bijzondere variant van de off-line TTP:

- de *no-line TTP,* die gebruikmaakt van andere communicatiemedia dan een telecommunicatienetwerk, zoals post.

Figuur 1 - Topologie van de TTP-dienst



Het hier gemaakte onderscheid is om twee redenen van belang. Allereerst zal de topologie van de TTP-dienst mede bepalend zijn voor mogelijke wetgeving die op de TTP van toepassing is; zo vallen in-line, on-line en off-line TTP's wel onder de Telecommunicatiewet (zie sectie 4), maar no-line TTP's niet. Daarnaast is de topologie van de TTP-dienst van invloed op specifieke problemen die optreden in het kader van rechtmatige toegang; zie hiervoor sectie 4.

2.3.5 Toepassingsgebied van de TTP-dienst

Het vijfde indelingscriterium voor TTP-diensten is het toepassingsgebied. In de toekomst kunnen TTP-diensten in uiteenlopende sectoren van de maatschappij voor verschillende toepassingen worden aangewend. Voorbeelden hiervan zijn de financiële sector, de dienstensector, de zorgsector, de accountancy, de overheidssector, de detailhandel en het notariaat.

Binnen elke sector kunnen TTP-diensten worden gebruikt voor de ondersteuning van specifieke toepassingen, producten en/of diensten. Elke toepassing zal daarbij specifieke eisen aan de gebruikte TTP-dienst stellen, waardoor uiteenlopende TTP-diensten zullen ontstaan. Een dergelijke differentiatie geldt in de huidige samenleving voor vrijwel elke technologie en elke dienst. Reeds op dit moment worden in de markt «op maat gesneden» TTP-diensten aangeboden, die zijn afgestemd op de eisen van specifieke toepassingen. Het is overigens denkbaar dat één TTP-dienst voor de ondersteuning van meerdere toepassingsgebieden zal worden aangeboden, waarbij de eisen van de hoogst geclassificeerde toepassing in de regel zullen prevaleren.

De differentiatie naar toepassingsgebieden van TTP's 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. Een voorbeeld hiervan is de vigerende wet- en regelgeving voor het bankwezen, het notariaat, de

advocatuur, de accountancy en de zorgsector, die onverkort op in deze sectoren gebruikte TTP-diensten van toepassing zal zijn.

In de tweede plaats speelt het kostenaspect een rol. Een stelsel van randvoorwaarden dat is toegesneden op toepassingen die zeer hoge eisen stellen aan een TTP-dienst is naar alle waarschijnlijkheid onnodig kostbaar voor toepassingen die lagere eisen stellen aan een TTP-dienst. De ontwikkeling van minder kostbare TTP-diensten – die een substantieel deel van het totale volume aan TTP-diensten kunnen vormen – zal door een al te stringent stelsel van randvoorwaarden niet worden gestimuleerd, maar juist worden belemmerd. Het formuleren van een te stringent stelsel van randvoorwaarden kan derhalve leiden tot een situatie die strijdig is met het doel van het nationaal TTP-project, namelijk het stimuleren van de ontwikkeling van een nationale TTP-infrastructuur.

Om bovengenoemde reden is ervoor gekozen niet zozeer een volledig en alomvattend stelsel van mogelijke randvoorwaarden voor alle mogelijke TTP-diensten te definiëren, als wel een stelsel van minimum-randvoorwaarden op te stellen dat voor alle klassen van TTP-diensten van toepassing is. Aanvullende randvoorwaarden kunnen dan door de markt worden opgesteld voor nog te onderscheiden klassen van TTP's, waarbij het toepassingsgebied of de vereiste graad van betrouwbaarheid als criteria voor classificatie zouden kunnen dienen.

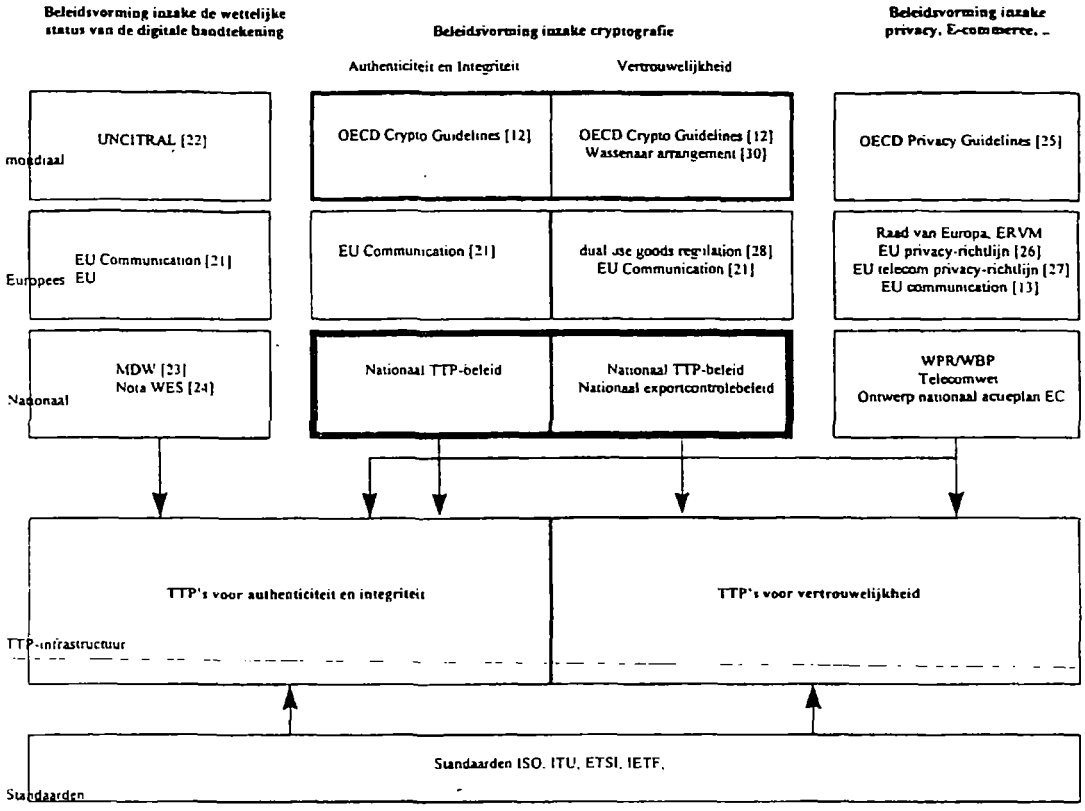
2.4 Marktontwikkeling

De markt voor TTP-diensten bevindt zich in de beginfase van zijn ontwikkeling. Deze ontwikkeling verloopt minder stormachtig dan nog maar kort geleden werd verwacht. Hetzelfde geldt voor de ontwikkeling en aanvaarding van internationale standaarden terzake. De bevindingen uit de inventarisatie van de proefprojecten onderbouwen deze stelling. Naar alle waarschijnlijkheid spelen hierbij vele factoren een rol. In elk geval lijkt de ontwikkeling van TTP-diensten te wachten op een verdere ontwikkeling van electronic commerce, terwijl de opbloei van electronic commerce afhankelijk lijkt te zijn van de beschikbaarheid van een betrouwbare TTP-infrastructuur. Het nationaal TTP-project heeft mede tot doel de ontwikkeling van een TTP-infrastructuur te stimuleren.

2.5 Beleidsontwikkeling

De nationale en internationale beleidsontwikkeling inzake TTP's staat niet op zichzelf, maar moet worden geplaatst binnen de bredere context van de ontwikkeling van internationaal en nationaal beleid inzake: cryptografie; de juridische status van digitale handtekeningen; privacy en electronic commerce. Daarnaast speelt de ontwikkeling van internationale standaarden voor TTP's, waaronder Certification Authorities (CA's). In figuur 2 is de context van het nationaal TTP-project schematisch weergegeven. Voor meer informatie zij verwezen naar de referenties in figuur 2.

Figuur 2 – Overzicht van nationale en internationale beleidsontwikkeling en standaardisatie



2.6 Totstandkoming randvoorwaarden

In het kader van het nationaal TTP-project is geïnventariseerd aan welke randvoorwaarden een TTP-infrastructuur zou moeten voldoen. Deze inventarisatie heeft als volgt plaatsgevonden:

- de betrokken ministeries hebben aangegeven welke randvoorwaarden in het kader van hun specifieke taakstelling en problematiek noodzakelijk worden geacht;
- vervolgens is een inventarisatie en analyse uitgevoerd van randvoorwaarden zoals die in nationale en internationale beleidsdocumenten, discussiestukken en standaarden naar voren komen;
- de hieruit voortvloeiende verzameling mogelijke randvoorwaarden is in conceptvorm ter commentaar voorgelegd aan de leden van de projectgroep van het nationaal TTP-project en aan de leden van de Consultatiegroep Aanbieders en Gebruikers;
- de mogelijke randvoorwaarden zijn door de EDP AUDIT POOL verder uitgewerkt in deelaspecten en gehanteerd als inventarisatiecriteria voor een viertal pilotprojecten;
- het commentaar van de leden van de projectgroep, het commentaar van de Consultatiegroep Aanbieders en Gebruikers en de resultaten van de inventarisatie van de proefprojecten zijn zoveel mogelijk in onderhavige beleidsnotitie verwerkt.

Een afsluitende analyse heeft plaatsgevonden met enkele leden van de projectgroep betreffende randvoorwaarden genoemd in sectie 4. Dit alles

heeft uiteindelijk geresulteerd in de randvoorwaarden zoals beschreven in de secties 3 en 4, waarbij primair onderscheid wordt gemaakt tussen randvoorwaarden inzake TTP's voor authenticiteit en integriteit en randvoorwaarden inzake TTP's voor vertrouwelijkheid.

2.7 Instrumenten voor het waarborgen van randvoorwaarden

Naast het formuleren van de randvoorwaarden zelf is een doelstelling van het nationaal TTP-project geweest te inventariseren op welke wijze deze randvoorwaarden binnen een zich ontwikkelende TTP-infrastructuur kunnen worden gewaarborgd.

De vereiste borging zal primair haar grondvesten moeten vinden in bestaande wet- en regelgeving. Nederland kent een uitgebreide algemene en specifieke wet- en regelgeving die mede is gericht op het beschermen van de maatschappij in het algemeen en de consument in het bijzonder. Deze bescherming wordt mede gerealiseerd door het waarborgen van de kwaliteit van de door marktpartijen geleverde diensten en het vaststellen van een vorm van toezicht daarop. Bestaande wet- en regelgeving terzake zal ook onverkort op TTP-diensten van toepassing zijn.

Pas als bestaande wet- en regelgeving onvoldoende blijkt om de noodzakelijke randvoorwaarden te kunnen waarborgen, dienen aanvullende oplossingen te worden overwogen. Overheid en bedrijfsleven beschikken hiervoor over een aantal instrumenten die variëren in de mate van regulering en overheidsinvloed. In dit geval is sprake van een spectrum, met strikte regulering aan het ene uiterste, volledige deregulering aan het andere uiterste, en tal van mengvormen daar tussenin, zoals een vergunningenstelsel, aansluiting bij een bij wet ingestelde of wettelijk erkende organisatie met zelfregulering, aansluiting bij een door de marktpartijen zelf ingestelde organisatie met zelfregulering, certificatie met overheidstoezicht, en certificatie zonder overheidstoezicht. Deze vormen zullen verder worden besproken in sectie 5.

3 RANDVOORWAARDEN INZAKE TTP-DIENSTEN VOOR AUTHENTICITEIT EN INTEGRITEIT

3.1 Inleiding

Onder TTP-diensten voor *authenticiteit en integriteit* vallen onder meer: 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 *(private keys);* en het tijdstempelen van elektronische berichten. Binnen TTP-diensten voor authenticiteit en integriteit wordt vaak onderscheid gemaakt tussen de Registration Authority (RA), die de legitimatie van aangesloten gebruikers verzorgt, en de Certification Authority (CA), die elektronische certificaten ten behoeve van deze gebruikers verstrekt.

Over de randvoorwaarden die op deze categorie van TTP's van toepassing zijn, bestaat bij de betrokken partijen een zekere consensus. Deze randvoorwaarden hebben onder meer betrekking op de wettelijke status van digitale handtekeningen, op de betrouwbaarheid van de geleverde TTP-dienst en de TTP zelf, op de bescherming van de persoonlijke levenssfeer, en op internationale interoperabiliteit.

Een groot aantal van de in het nationaal TTP-project ingebrachte

randvoorwaarden is algemeen van aard en is, als normale eisen van professionaliteit, in wezen van toepassing op elke dienst; andere randvoorwaarden zijn wel specifiek voor TTP-diensten. De in deze sectie beschreven randvoorwaarden kunnen worden beschouwd als minimum-randvoorwaarden die in feite op elke categorie van TTP-diensten van toepassing zijn, ongeacht het toepassingsgebied.

Op TTP-diensten voor authenticiteit en integriteit zijn in beginsel geen randvoorwaarden inzake rechtmatige toegang van toepassing, mits de TTP, door het treffen van specifieke maatregelen, voldoet aan de voorwaarde dat de bedoelde TTP-dienst en het desbetreffende sleutelmateriaal uitsluitend voor authenticiteit en integriteit kunnen worden gebruikt. Alvorens in te gaan op de randvoorwaarden zelf, zal eerst de juridische status van digitale handtekeningen worden besproken.

3.2 Juridische status van digitale handtekeningen

De juridische status van digitale handtekeningen is onderwerp van onderzoek. In internationaal verband vindt beleidsvorming plaats door UNCITRAL [22]. In Europees verband is een mededeling uitgevaardigd [21]. Op dit moment wordt gewerkt aan een in deze mededeling aangekondigde Europese richtlijn voor elektronische handtekeningen. Het doel van deze richtlijn is binnen de EU te komen tot harmonisatie van de rechtsgeldigheid van elektronische handtekeningen. Dit wordt ten eerste gerealiseerd doordat elektronische handtekeningen niet à priori ongeldig mogen worden verklaard puur vanwege het feit dat ze elektronisch van aard zijn en ten tweede door *gekwalificeerde* handtekeningen in principe dezelfde rechtskracht als handgeschreven handtekeningen te verlenen. Een handtekening is gekwalificeerd indien uitgegeven door organisaties (TTP's) die aan minimumeisen voldoen. Deze minimumeisen worden in de richtlijn vermeld.

Het Ministerie van Justitie en het Ministerie van Economische Zaken hebben een MDW-project omtrent de juridische status in Nederland uitgevoerd [23]. Daarnaast heeft een projectgroep onder voorzitterschap van het Ministerie van Justitie een notitie opgesteld over de uitgangspunten van wetgeving op de elektronische snelweg [24], waarbij onder meer aandacht is geschonken aan de juridische status van digitale handtekeningen.

Onderzoek naar de juridische status van digitale handtekeningen is gerelateerd aan het nationaal TTP-project, maar valt buiten de voor dit deelproject gedefinieerde scope. De onderliggende TTP-infrastructuur is geen voorwaarde voor de juridische erkenning van de digitale handtekening, maar zal wel bijdragen aan de bewijskracht ervan.

3.3 Betrouwbaarheid

Verreweg de belangrijkste randvoorwaarden die in het nationaal TTP-project naar voren zijn gekomen, hebben betrekking op de betrouwbaarheid van zowel de TTP-dienst als de organisatie die deze dienst levert: de TTP zelf. De gebruikers van een TTP-dienst zullen een hoog vertrouwen moeten kunnen stellen in de organisatie die deze TTP-dienst aanbiedt. Voor TTP's is betrouwbaarheid dan ook van essentieel belang. Deze eis beperkt zich niet tot individuele TTP's, maar heeft betrekking op de gehele internationale TTP-infrastructuur.

De ruime betekenis van het begrip betrouwbaarheid maakt een nadere opsplitsing in deelaspecten noodzakelijk, die kunnen worden onderverdeeld in eisen ten aanzien van de TTP-organisatie en eisen ten aanzien

van de TTP-dienst. In het kader van het nationaal TTP-project is een aantal betrouwbaarheidseisen geformuleerd, die navolgend zullen worden toegelicht.

3.3.1 Betrouwbaarheid van de TTP-organisatie

De volgende betrouwbaarheidseisen zijn van toepassing op de TTP:
- *rechtmatig handelen* – TTP's dienen in elke zin van het woord te handelen in overeenstemming met het nationaal en internationaal recht;
- *financiële positie* – de financiële positie van de TTP-organisatie dient voldoende waarborgen te bieden ten aanzien van de continuïteit van de TTP-dienst;
- *bedrijfscontinuïteit* – de continuïteit van TTP-diensten dient zoveel mogelijk te worden gewaarborgd, ook in geval van overname, fusie, bedrijfsstaking of faillissement;
- *beveiliging* – de vertrouwelijkheid, integriteit en beschikbaarheid van gegevens en informatiesystemen binnen de TTP-organisatie dienen door het treffen van een adequaat stelsel van beveiligingsmaatregelen te zijn gewaarborgd tegen schade voortvloeiend uit onder meer calamiteiten, storingen, alsmede opzettelijk en onopzettelijk menselijk handelen. De in 1994 door het Ministerie van Economische Zaken uitgegeven Code voor Informatiebeveiliging lijkt een goede basis te bieden voor de beveiliging van TTP-organisaties, waarbij de hoge betrouwbaarheidseisen die aan een TTP worden gesteld aanvullende maatregelen noodzakelijk kunnen maken. De Information Technology Security Evaluation Criteria (ITSEC) en daarop mede gebaseerde Common Criteria bieden hierbij wellicht een goede basis voor de evaluatie van de gebruikte IT-producten;
- *personeel* – eigenaren, aandeelhouders, directie, management en personeel van de TTP-organisatie moeten kunnen worden vertrouwd ten aanzien van de hun toevertrouwde taken;
- *authenticatie* – de TTP-organisatie dient bij het nemen van beslissingen en het uitvoeren van handelingen door management en medewerkers van de TTP-organisatie steeds ondubbelzinnig de identiteit van de hierbij betrokken personen te kunnen vaststellen. Het vaststellen van de identiteit van betrokken personen dient ook achteraf mogelijk te zijn;
- *autorisatie* – specifieke bevoegdheden dienen duidelijk en ondubbelzinnig aan specifieke functies en functionarissen binnen de TTP-organisatie te zijn toegewezen;
- *functiescheiding* – er dient een adequate controletechnische scheiding te bestaan tussen beschikkende, bewarende, uitvoerende en controlerende functies binnen de TTP-organisatie, onder meer inzake sleutelbeheer;
- *toezicht* – om de betrouwbaarheid van een TTP-organisatie te waarborgen, zal regelmatig door een onafhankelijke instantie moeten worden gecontroleerd of de TTP-organisatie voldoet aan een vooraf opgesteld pakket van eisen en randvoorwaarden, en of dit pakket van eisen en randvoorwaarden toereikend is om de gewenste graad van betrouwbaarheid te bereiken. Voor het realiseren van een dergelijke vorm van toezicht zijn verschillende modellen denkbaar, die in sectie 5 worden uitgewerkt. Tevens kan op deze plaats nogmaals worden benadrukt dat op TTP-organisaties die diensten leveren ten behoeve van specifieke maatschappelijke functies ook de bijbehorende wettelijke vereisten ten aanzien van toezicht en controle van toepassing zullen zijn;
- *zorgvuldigheid* – de TTP dient uitsluitend gegevens aan derden te verstrekken indien hiertoe een aantoonbare wettelijke grondslag bestaat. Het is van groot belang dat de gebruikers van een TTP-dienst

erop kunnen vertrouwen dat een eventuele verstrekking van gegevens uitsluitend onder strikte voorwaarden zal plaatsvinden, en dan nog alleen indien hiertoe een aantoonbare wettelijke grondslag bestaat, waarbij de TTP-organisatie zich van de rechtmatigheid van een verzoek tot medewerking zal moeten overtuigen. Geheime cryptografische sleutels die uitsluitend worden gebruikt voor authenticiteit en integriteit (private keys) zullen nooit en te nimmer aan derden mogen worden verstrekt;
- *beheer van bedrijfsmiddelen* – de ontwikkeling en het beheer van informatietechnologie en andere bedrijfsmiddelen binnen de TTP dienen te zijn ingericht volgens algemeen aanvaarde kwaliteitsnormen;
- *onafhankelijkheid* – de TTP dient niet gebonden te zijn aan één of meer bestaande partijen en geen belang te hebben bij de te beveiligen informatie;
- *transparantie* – de TTP dient inzicht te geven in de gehanteerde werkwijze, om toetsing van de TTP-organisatie en de TTP-dienst mogelijk te maken.

3.3.2 Betrouwbaarheid van de TTP-dienst

De volgende betrouwbaarheidseisen zijn van toepassing op de TTP-dienst:
- *betrouwbare technologie* – de gebruikte technologie dient voldoende betrouwbaar te zijn om de vertrouwelijkheid, integriteit en beschikbaarheid van de geautomatiseerde gegevensverwerking te waarborgen;
- *documentatie* – het ontwerp, de implementatie, het beheer en het gebruik van de TTP-dienst dienen adequaat gedocumenteerd te zijn;
- *sleutelbeheer* – sleutelbeheer dient op betrouwbare wijze te geschieden.

In tabel 1 is een overzicht van randvoorwaarden inzake betrouwbaarheid weergegeven.

Ten slotte zij opgemerkt dat de betrouwbaarheid van een TTP-dienst mede afhankelijk zal zijn van de betrouwbaarheid van de gebruikers van die dienst. Daardoor kunnen niet alleen aan de aanbieders, maar ook aan de gebruikers van een TTP-dienst eisen worden gesteld, bijvoorbeeld eisen ten aanzien van goed huisvaderschap.

Tabel 1. Overzicht van randvoorwaarden inzake betrouwbaarheid

TTP-organisatie	TTP-dienst
rechtmatig handelen	betrouwbare technologie
financiële positie	documentatie
bedrijfscontinuïteit	sleutelbeheer
beveiliging	
personeel	
authenticatie	
autorisatie	
functiescheiding	
toezicht	
zorgvuldigheid	
beheer van bedrijfsmiddelen	
transparantie	
onafhankelijkheid	

3.4 Privacy

Inzake privacy is zowel door de overheid als door enkele marktpartijen benadrukt dat de bescherming van de persoonlijke levenssfeer van de gebruikers van een TTP-dienst bijzondere aandacht behoeft. De Wet persoonsregistraties, die, onder invloed van de Europese privacyrichtlijn [26], naar verwachting in de loop van 1999 zal worden vervangen door de Wet bescherming persoonsgegevens, is vanzelfsprekend ook op TTP's van toepassing. Daarnaast is er de EU Telecommunicatie Privacy-richtlijn [27], die is geïmplementeerd in de nieuwe Telecommunicatiewet.

In het geval van TTP's valt onder de noemer privacy onder meer te denken aan de beveiliging van certificaten en/of openbare sleutels. Een certificaat heeft hierbij als primaire functie een identiteit te binden aan de publieke sleutel van een sleutelpaar. De geheime sleutel van het sleutelpaar is alleen behouden aan de eigenaar. Daarnaast kan een certificaat andere informatie bevatten. Een verzameling certificaten moet daarom worden beschouwd als een persoonsregistratie.

Om de herleidbaarheid van certificaten en sleutelmateriaal naar natuurlijke personen te beperken, kan worden overwogen gebruik te maken van privacy-enhanced technology (PET). Een voorbeeld is het gebruik van pseudo-identiteiten bij de uitwisseling van persoonsgegevens.

Aanbevolen wordt een privacygedragscode voor TTP's op te stellen, waarin het treffen van nadere maatregelen terzake verder wordt uitgewerkt. Deze gedragscode kan als randvoorwaarde in een certificeringstraject (zie sectie 5) worden ingebouwd.

3.5 Interoperabiliteit

De ontwikkeling van een betrouwbare, breed toepasbare en economisch haalbare TTP-infrastructuur voor authenticiteit en integriteit kan slechts succesvol zijn, indien nauwe aansluiting wordt gevonden bij nationale en internationale ontwikkelingen.

Deze aansluiting heeft twee aspecten.

Allereerst moeten de technische interoperabiliteit tussen nationale en internationale TTP-infrastructuren gewaarborgd zijn. De internationale situatie kent een groot aantal technische standaarden op het gebied van interfaces, protocollen en algoritmen, waartoe onder meer de standaarden van de ETSI, ITU, ISO en IETF en verschillende de-factostandaarden gerekend mogen worden. Overheden kunnen bij standaardisatie een stimulerende en activerende rol spelen.

In de tweede plaats is in het kader van interoperabiliteit wederzijdse erkenning van nationale en internationale TTP's noodzakelijk. Hierbij geldt dat wederzijdse erkenning pas mogelijk is indien deze TTP's voldoen aan een gelijkwaardig stelsel van randvoorwaarden, waarbij in het internationale geval ook moet worden gestreefd naar de wederzijdse erkenning van digitale handtekeningen in de desbetreffende landen. De Europese richtlijn voor elektronische handtekeningen is een goed voorbeeld van een initiatief dat de wederzijdse erkenning van digitale handtekeningen in de lidstaten tot doel heeft.

In enkele landen, zoals Duitsland en de Verenigde Staten, bestaat reeds wetgeving op dit vlak. Wederzijdse erkenning tussen verschillende nationale en internationale TTP's kan worden gerealiseerd op basis van overeenkomsten in combinatie met wederzijdse toetsing; het verdient

aanbeveling hiermee vanuit Nederland reeds zo snel mogelijk een aanvang te maken. Ook hierbij kan de overheid een stimulerende en activerende rol spelen. Hierbij zal rekening moeten worden gehouden met een zich snel ontwikkelend internationaal raamwerk, waarbinnen de in Nederland geldende randvoorwaarden zo efficiënt mogelijk moeten kunnen worden ingepast.

In fase 3 van het TTP-project is naar voren gekomen dat interoperabiliteit door de onderzochte TTP's van groot belang wordt geacht. Hierbij dient te worden aangetekend, dat niet is onderzocht of en in hoeverre de proefprojecten interoperabel zijn.

3.6 Overige randvoorwaarden

Naast bovengenoemde randvoorwaarden is een aantal aanvullende randvoorwaarden geformuleerd:

- *Bezwaar- en beroepsmogelijkheden* – de gebruikers van een TTP-dienst dienen in staat te worden gesteld bezwaar of beroep aan te tekenen bij een onafhankelijke beroepsinstantie. De gebruiker van een TTP dient te beschikken over laagdrempelige mogelijkheden tot het indienen en afhandelen van klachten, waarbij de mogelijkheden en termijnen voor het indienen van klachten, alsmede de termijn van behandeling duidelijk aan de gebruiker kenbaar worden gemaakt.

- *Aansprakelijkheid* – de TTP-organisatie dient, onder zekere voorwaarden, aansprakelijkheid voor de door haar geleverde diensten en/of verrichte transacties te aanvaarden. Om aansprakelijkheidsvraagstukken te kunnen beantwoorden wordt een eenduidige en onweerlegbare vastlegging van uitgevoerde activiteiten door de TTP onmisbaar geacht.

- *Klachtenregeling* – er dient een klachtenregeling te zijn, alsmede een mogelijkheid tot schadeverhaal bij, bijvoorbeeld, onrechtmatige verstrekking van sleutelmateriaal aan derden; een dergelijke compromittering dient hoe dan ook altijd onverwijld door de TTP aan de gebruiker te worden gemeld.

- *Keuzevrijheid* – ter bevordering van de vrije marktwerking en om de individuele wensen van de consument te kunnen behartigen dient de consument altijd een vrije keuze te kunnen maken bij de selectie van een TTP en van specifieke TTP-diensten. Er mag met andere woorden geen sprake zijn van «gedwongen winkelnering», bijvoorbeeld als gevolg van een monopoliepositie. Dit geldt ook voor commerciële producten die het gebruik van TTP's mogelijk maken.

- *Geen vertrouwelijkheidsfuncties* – een TTP in deze categorie mag niet willens en wetens meewerken aan het gebruiken van sleutelmateriaal, dat is bestemd voor authenticiteit en integriteit, voor de versleuteling van gegevens.

4 RANDVOORWAARDEN INZAKE TTP-DIENSTEN VOOR VERTROUWELIJKHEID

4.1 Inleiding

Onder TTP-diensten voor *vertrouwelijkheid* vallen onder meer: het *vercijferen van elektronisch berichtenverkeer; en het beheer van cryptografisch sleutelmateriaal voor vertrouwelijkheid.*

De hierbij behorende randvoorwaarden hebben onder meer betrekking op betrouwbaarheid, rechtmatige toegang, exportcontrole en interoperabiliteit.

4.2 Betrouwbaarheid

De randvoorwaarden inzake de betrouwbaarheid van TTP-diensten voor vertrouwelijkheid wijken niet af van de randvoorwaarden inzake de betrouwbaarheid van TTP-diensten voor authenticiteit en integriteit.

Aanvullend kan worden gesteld dat een TTP vertrouwelijk dient om te gaan met medewerking aan de rechtmatige verkrijging van bepaalde gegevens en/of sleutelmateriaal door hiertoe wettelijk bevoegde instanties. Evenzo dient de TTP vertrouwelijk om te gaan met de uit een dergelijke medewerking voortvloeiende informatie.

4.3 Rechtmatige toegang

Deze categorie van randvoorwaarden heeft betrekking op de rechtmatige toegang tot gegevens, zowel door de gebruiker als door andere partijen.

De *gebruiker* zal voor de toegang tot zijn gegevens altijd moeten kunnen beschikken over het geheime sleutelmateriaal waarmee de oorspronkelijke gegevens zijn versleuteld. Voor de gebruiker van een TTP-dienst voor vertrouwelijkheid is het verlies van sleutelmateriaal een reëel risico. Bij verlies of verminking van dit sleutelmateriaal zijn de oorspronkelijke gegevens immers niet langer toegankelijk. Sleutelverlies kan daarom grote gevolgen hebben voor de continuïteit van een organisatie, maar ook voor de individuele gebruiker. De risico's van sleutelverlies kunnen tot een aanvaardbaar niveau worden teruggebracht door reservekopieën van sleutels te bewaren *(key escrow)* of ervoor te zorgen dat sleutelmateriaal te herleiden is *(key recovery)*. Een TTP die zorg draagt voor sleutelbewaring en/of herleidbaarheid ontslaat zijn gebruiker van de taak deze maatregel zelf te treffen.

Niet alleen de gebruikers van een TTP-dienst, maar ook *andere partijen* met rechtmatige toegang tot *bepaalde* gegevens hebben baat bij een vorm van sleutelbewaring en/of herleidbaarheid. Voor deze partijen is of wordt de wettelijke bevoegdheid tot het verkrijgen van bepaalde elektronische gegevens op dit moment geregeld door middel van specifieke wet- en regelgeving. In een aantal gevallen kan deze specifieke wet- en regelgeving onder strikte voorwaarden het normaal geldende beroepsgeheim of een geheimhoudingsplicht ten aanzien van vertrouwelijke informatie doorbreken, behoudens situaties waarin verschoningsrecht van toepassing is. De specifieke wet- en regelgeving is onder meer van toepassing op curatoren, medische instellingen, de advocatuur, opsporingsdiensten met wettelijke bevoegdheid, zoals politie, FIOD en AID, en de inlichtingen- en veiligheidsdiensten. In de wet wordt onderscheid gemaakt tussen rechtmatige toegang tot opgeslagen gegevens en rechtmatige toegang tot telecommunicatieverkeer.

De randvoorwaarden die in dit verband op de TTP van toepassing zijn, zijn afhankelijk van de topologie van de TTP-dienst (zie 2.3.4). *In-line TTP's* kennen reeds een medewerkingsverplichting bij een rechtmatig verzoek, waarbij de in-line TTP als telecommunicatiedienst[1] wettelijk verplicht is om het oorspronkelijke signaal aan te leveren. Bij *on-line, off-line en no-line* TTP's kan, zoals beschreven in sectie 2.3, onderscheid worden gemaakt tussen de gevallen waarin sleutelmateriaal wordt opgeslagen door de gebruiker enerzijds of door de TTP anderzijds.

[1] Zie de Telecommunicatiewet, Memorie van Toelichting.

Wordt het sleutelmateriaal opgeslagen door de gebruiker zelf, dan ontstaat een situatie die voor de gebruiker vanuit het oogpunt van risicobeheersing aanvaardbaar kan zijn, maar voor andere partijen met rechtmatige toegang tot gegevens niet in alle gevallen toereikend zal zijn. Het merendeel van de in fase 3 onderzochte TTP's heeft het sleutelbeheer zodanig ingericht, dat alleen de gebruiker zelf over het geheime sleutelmateriaal beschikt (zie Bijlage 1).

Wordt sleutelmateriaal door de TTP opgeslagen, dan zijn daarmee niet *alleen de belangen van de gebruiker, maar ook de belangen van de* partijen met rechtmatige toegang tot bepaalde gegevens gediend. Rechtmatige toegang tot zulk sleutelmateriaal – en de medewerking hierbij door de TTP – zal immers geregeld zijn op grond van vigerende wet- en regelgeving. De opsporingsdiensten hebben de bevoegdheid tot het opvragen van opgeslagen gegevens en daarmee tot opgeslagen sleutelmateriaal in het kader van de WCC (art. 125k WSv). Een en ander is schematisch weergegeven in figuur 3. De inlichtingen- en veiligheidsdiensten kennen op dit moment geen bevoegdheid tot het opvragen van opgeslagen gegevens; in het ontwerp van de nieuwe Wet op de Inlichtingen en Veiligheidsdiensten (WIV) is echter voorzien in een verplichting ten aanzien van het verlenen van medewerking door degenen die kennis dragen van het ongedaan maken van de versleuteling van (a) gegevens opgeslagen of verwerkt in een geautomatiseerd werk; (b) gesprekken, telecommunicatie of gegevensoverdracht die door de dienst zijn afgetapt. Aan de medewerking door de TTP is een aantal voor de hand liggende randvoorwaarden verbonden. In de eerste plaats zal de TTP de rechtmatigheid van het verzoek tot het verstrekken van gegevens alsmede de bevoegdheid van de persoon die het verzoek tot het verlenen van medewerking doet ondubbelzinnig dienen te verifiëren. Vervolgens zal de TTP onverwijld medewerking dienen te verlenen, zal strikte geheimhouding bij het verlenen van zulke medewerking moeten worden betracht, en dient de TTP inzage te geven in de gebruikte encryptietechnieken. Ten slotte dient de TTP een vertrouwenspersoon in dienst te hebben voor de vertrouwelijke afhandeling van verzoeken tot rechtmatige toegang.

Figuur 3 – Rechtmatige toegang in het kader van opsporing en informatievergaring op basis van huidige wet- en regelgeving

gegevens / encryptie	transport rechtmatige interceptie	opslag rechtmatige toegang
encryptie door TTP	in-line TTP TTP levert oorspronkelijk signaal aftapregulering Telecomwet	on-line, off-line en no-line TTP TTP levert oorspronkelijke gegevens medewerkingsverplichting WCC
encryptie door gebruiker	on-line, off-line en no-line TTP *on-line/off-line TTP* levert sleutelmateriaal, indien beschikbaar medewerkingsverplichting WCC en Telecomwet TTP levert oorspronkelijk signaal aftapregulering Telecomwet *no-line TTP* levert sleutelmateriaal, indien beschikbaar medewerkingsverplichting WCC	on-line, off-line en no-line TTP TTP levert sleutelmateriaal, indien beschikbaar medewerkingsverplichting WCC

Bij het internationaal gebruik van TTP's doet zich een specifiek probleem voor als de betrokken partijen voor encryptie sleutelmateriaal gebruiken dat is gegenereerd door, verstrekt door en/of gedeponeerd bij een buitenlandse TTP. De Nederlandse wet- en regelgeving biedt onvoldoende aanknopingspunten om zulk sleutelmateriaal te achterhalen; de buitenlandse TTP zal niet gehouden zijn het sleutelmateriaal aan Nederlandse instanties te verstrekken. Een mogelijke maatregel om hieraan tegemoet te komen lijkt de verplichte opslag van een kopie van het geheime sleutelmateriaal door een TTP binnen de jurisdictie, met een bewaarplicht en toegang door partijen met rechtmatige toegang. Eventueel zou hiervoor een hiërarchische internationale TTP-infrastructuur kunnen worden opgezet, waarbij vertrouwelijkheidssleutels altijd worden opgeslagen door TTP's binnen de onderscheiden jurisdicties; interoperabiliteit van deze TTP's is hiervoor een noodzakelijke vereiste. Een andere mogelijkheid is het opstellen van overeenkomsten, zoals rechtshulpverdragen, tussen jurisdicties inzake het in klare tekst verstrekken van gegevens en/of sleutelmateriaal door TTP's, waarbij verzoeken hiertoe via de nationale overheidsdiensten kunnen verlopen. In al deze gevallen betreft het maatregelen met verstrekkende gevolgen, die bovendien, mede door de noodzakelijke internationale afstemming, niet eenvoudig zullen kunnen worden getroffen.

Samenvattend kan worden geconcludeerd dat de bewaring en/of herleidbaarheid van bepaald sleutelmateriaal voor vertrouwelijkheid door de TTP zowel uit het oogpunt van de gebruiker als uit het oogpunt van de andere betrokken partijen zekere voordelen biedt. Leveranciers van hardware en software waarmee TTP-diensten kunnen worden gerealiseerd, brengen in toenemende mate producten op de markt waarbij faciliteiten voor sleutelbewaring en herleidbaarheid zijn ingebouwd.

Aan het bewaren en/of herleiden van sleutelmateriaal zijn echter ook andere consequenties verbonden, die onder meer betrekking hebben op de vereiste integriteit en vertrouwelijkheid van het opgeslagen sleutelmateriaal en, daarmee samenhangend, de bescherming van de persoonlijke levenssfeer van de gebruikers van de TTP. Bovendien kunnen de hiermee samenhangende risico's slechts door een adequaat stelsel van randvoorwaarden worden ondervangen, waardoor sleutelbewaring en/of herleidbaarheid voor de aanbieder van een TTP-dienst kosten met zich mee zullen brengen.

Om bovengenoemde redenen en omdat er nog vragen zijn rondom de uitvoerbaarheid en de invloed op de ontwikkeling van elektronische handel, zijn de bewaring en de herleidbaarheid van sleutelmateriaal door TTP's nog steeds het onderwerp van internationale controverse. Bewaring en/of herleidbaarheid van sleutelmateriaal zijn daarom in deze beleidsnotitie niet als randvoorwaarden opgenomen.

Een andere reden om ons op dit moment niet vast te leggen op een bepaalde techniek of methodiek om versleutelde gegevens te kunnen ontcijferen is dat er op dit vlak volop ontwikkelingen gaande zijn.
Deze ontwikkelingen kunnen zowel de mogelijkheden om te versleutelen als ook de mogelijkheden om versleutelde gegevens te ontcijferen sterk beïnvloeden. Ook vanuit het belang van een adequate criminaliteitsbestrijding is het dus niet van belang om ons nu op een specifieke methodiek of technologie vast te leggen.
Daarentegen blijft het van belang om daar waar noodzakelijk voldoende instrumenten te hebben om afgetapte versleutelde gegevens te kunnen ontcijferen. Omdat het hier om een maatschappelijk belang gaat zal een brede groep betrokkenen aan de ontwikkeling van een dergelijk, voor alle partijen aanvaardbaar instrumentarium moeten bijdragen. Het relevante

bedrijfsleven heeft reeds aangegeven hieraan te willen meewerken, in een «partnership approach» met de overheid.

Verder zal worden bezien hoe gewaarborgd kan worden dat het relevante bedrijfsleven dit nog te ontwikkelen instrumentarium ook daadwerkelijk toepast. Daarbij zal in eerste instantie aansluiting worden gezocht bij het in hoofdstuk 5 beschreven zelfreguleringsmechanisme. Uitgangspunt hierbij zal zijn dat zelfregulering een wettelijke verankering krijgt. Onderzocht zal worden hoe hieraan vorm gegeven kan worden gelet op aspecten rondom bescherming van de belangen van het bedrijfsleven en het belang om de bevoegdheid tot rechtmatige toegang van Inlichtingen- en Veiligheidsdiensten alsmede Justitie te effectueren.

De evaluatieperiode van 2 jaar die is voorzien in deze beleidsnotitie (zie onder meer hoofdstuk 5), zal tevens worden gebruikt om de vorderingen op dit punt te bezien.
Indien het bedrijfsleven niet voldoende actief meewerkt aan de ontwikkeling van genoemd instrumentarium, zal de overheid nadrukkelijk overwegen om met nadere wetgeving de behoefte aan rechtmatige toegang in te vullen.

4.4 Exportcontrole

TTP's die vertrouwelijkheidsdiensten aanbieden dienen te voldoen aan de vigerende wet- en regelgeving inzake exportcontrole.

Cryptografische producten boven een bepaalde sterkte, met inbegrip van software, zijn met uitzondering van een aantal producten zoals voor banktoepassing, mobiele telefonie en Pay-TV, onder exportcontrole gebracht op grond van multilaterale afspraken in het (in december 1998 herziene) Wassenaar Arrangement. Deze afspraken komen voort uit internationale en nationale veiligheidspolitieke overwegingen.

Voor de ontwikkeling van een betrouwbare infrastructuur voor electronic commerce is het gebruik van cryptografische producten in toenemende mate van belang. Het exportcontrolebeleid is er dan ook op gericht om deze ontwikkeling zo min mogelijk te belemmeren. In het Wassenaar Arrangement komt derhalve geregeld exportcontrole van cryptografische hardware en software uitvoerig aan de orde met als inzet om een aantal van die producten van de exportcontrole lijst af te voeren en om de procedures voor exportcontrole te versoepelen. Het Ministerie van Economische Zaken (DGBEB) heeft bij deze onderhandelingen de coördinerende taak en is tevens verantwoordelijk voor de afgifte van exportvergunningen.

De exportcontrole op cryptografische producten en op producten die cryptografische producten bevatten, is gestoeld op de volgende wettelijke basis:
1. In en Uitvoerwet (Stb. 1988, 228);
2. Uitvoerbesluit strategische goederen 1963 (Stb. 1981, 118);
3. Verordening (EG) nr. 3381/94 van de Raad van de Europese Unie van 19 december 1994. De verordening introduceert een communautair systeem voor de uitvoer van goederen voor tweeërlei gebruik. In het daarmee verbonden Raadsbesluit nr. 94/942/GBVB is de lijst met de betrokken goederen opgenomen. Op basis van het herziene Wassenaar arrangement wordt deze lijst aangepast.

Bovengenoemde wet- en regelgeving is ook van toepassing op de export van cryptografische hardware en software voor TTP-diensten voor vertrouwelijkheid. Indien een TTP tot export van cryptografische

producten zou willen overgaan, zal op basis van bovenvermelde lijst van de EG-verordening moeten worden nagegaan of voor dit produkt een vergunning bij de Centrale Dienst voor In- en Uitvoer moet worden aangevraagd.

4.5 Interoperabiliteit

Voor TTP-diensten voor vertrouwelijkheid gelden in beginsel dezelfde randvoorwaarden inzake interoperabiliteit als voor TTP-diensten voor authenticiteit en integriteit (zie 3.5), uitgezonderd hetgeen is gesteld inzake de wederzijdse erkenning van digitale handtekeningen.

4.6 Overige randvoorwaarden

Voor TTP-diensten voor vertrouwelijkheid gelden in beginsel dezelfde overige randvoorwaarden als voor TTP-diensten voor authenticiteit en integriteit (zie 3.6).

5 INSTRUMENTEN VOOR HET WAARBORGEN VAN RANDVOORWAARDEN

5.1 Inleiding

Na de opsomming van randvoorwaarden in de secties 3 en 4 rijst de vraag hoe deze randvoorwaarden in de praktijk zouden kunnen worden gewaarborgd.

Overheid en bedrijfsleven beschikken hiertoe over een aantal instrumenten die variëren in de mate van regulering en overheidsinvloed. Ook in dit geval is sprake van een spectrum, met strikte regulering aan het ene uiterste, volledige deregulering aan het andere uiterste, en tal van mengvormen daar tussenin, zoals een verplicht vergunningenstelsel, aansluiting bij een bij wet ingestelde of wettelijk erkende organisatie met zelfregulering, aansluiting bij een door de marktpartijen zelf ingestelde organisatie met zelfregulering, certificatie met overheidstoezicht, en certificatie zonder overheidstoezicht.

Volledige zelfregulering stuit op bezwaren, die samenhangen met het belang van TTP-diensten voor een samenleving die zich meer en meer verlaat op inherent kwetsbare informatietechnologie. De overheid heeft in deze tot taak de burger tegen onaanvaardbare risico's te beschermen. Daarnaast zal de overheid moeten waarborgen dat de belangen van partijen met een wettelijke bevoegdheid tot het verkrijgen van elektronische gegevens voldoende worden bewaakt. In het MDW-rapport Normalisatie en Certificatie [15] is door de ministers van Economische Zaken en Justitie aangegeven onder welke omstandigheden voor certificatie kan worden gekozen, en onder welke omstandigheden een nauwere betrokkenheid van de overheid gerechtvaardigd is. Maatschappelijk belang is hierbij een essentieel criterium. Volledige zelfregulering lijkt om deze reden niet gerechtvaardigd. Aan het opstellen van nieuwe wet- en regelgeving zijn echter ook een aantal nadelen verbonden, zoals:

- wetgeving is relatief kostbaar, hetgeen vragen oproept omtrent proportionaliteit;
- vergaande wetgeving is weinig flexibel, terwijl flexibiliteit in de zich nog sterk ontwikkelende TTP-markt een noodzakelijke vereiste is;

Het kiezen van de instrumenten waarmee de gestelde randvoorwaarden kunnen worden gewaarborgd, komt derhalve neer op het vinden van een

balans tussen regulering en deregulering. De vraag is hoe deze balans kan worden gevonden.

Op basis van het uitgangspunt van deregulering en marktwerking wordt ervoor gekozen om het waarborgen van de in deze beleidsnotitie genoemde randvoorwaarden in beginsel via een zelfreguleringsmechanisme aan de markt over te laten. Het oprichten van een landelijke organisatie voor TTP's, onder begeleiding en stimulering van de overheid, is hierbij als veelbelovende mogelijkheid naar voren gekomen. Dit voorstel zal in hoofdstuk 5.2 nader worden toegelicht.

Terzake de in hoofdstuk 4.3 beschreven specifieke randvoorwaarde van rechtmatige toegang dient daarnaast via een partnership approach tussen de overheid en het relevante bedrijfsleven een voor alle partijen aanvaardbaar instrumentarium voor het faciliteren van de rechtmatige toegang te worden ontwikkeld. Om te waarborgen dat het relevante bedrijfsleven dit nog te ontwikkelen instrumentarium ook daadwerkelijk toepast zal ook hier aansluiting worden gezocht bij een zelfreguleringsmechanisme. Uitgangspunt hierbij zal zijn dat deze zelfregulering een wettelijke verankering krijgt.

5.2 TTP-kamer

Aanbieders en gebruikers van TTP-diensten dienen het initiatief te nemen tot de oprichting van een landelijke organisatie voor TTP's, onder begeleiding en stimulering van de overheid (zie figuur 4). Deze organisatie zal verder als «TTP-kamer» worden aangeduid.

Hierbij gelden ten minste de volgende overwegingen:
- de TTP-kamer dient een onafhankelijke organisatie te zijn;
- in de TTP-kamer hebben zowel de marktpartijen als de overheid zitting;
- aansluiting bij de TTP-kamer door marktpartijen dient op vrijwillige basis plaats te vinden. De criteria voor lidmaatschap dienen objectief te zijn;
- de TTP-kamer dient een openbare registratie van aangesloten TTP's te kennen;
- de TTP-kamer dient in overleg met de andere betrokken partijen een bindend algemeen reglement *(Policy Statement)* voor TTP-diensten op te stellen, waarin de rechten en plichten van de gebruikers en aanbieders van de TTP-dienst worden aangegeven en tenminste de in deze beleidsnotitie opgestelde randvoorwaarden inzake digitale handtekeningen, betrouwbaarheid, privacy, interoperabiliteit, enz. zijn opgenomen;
- elke bij de TTP-kamer aangesloten TTP zal handelen in overeenstemming met het aldus opgestelde reglement;
- het reglement dient periodiek of anders wanneer nodig te worden geëvalueerd en, indien nodig, te worden herzien;
- de TTP-kamer dient te onderzoeken of voor bepaalde TTP-diensten aanvullende randvoorwaarden moeten worden opgesteld, die door een TTP kunnen worden vastgelegd in een specifieke aanvulling op het reglement;
- elke bij de TTP-kamer aangesloten TTP dient zelf een specifiek reglement op te stellen, dat is toegesneden op de geleverde TTP-diensten. Dit specifieke reglement dient ten minste het algemeen reglement te omvatten;
- de TTP-kamer dient een klachtenregeling en een vorm van tuchtrecht te kennen;
- de TTP-kamer dient zorg te dragen voor aansluiting bij internationale ontwikkelingen;
- elke bij de TTP-kamer aangesloten TTP dient periodiek te worden

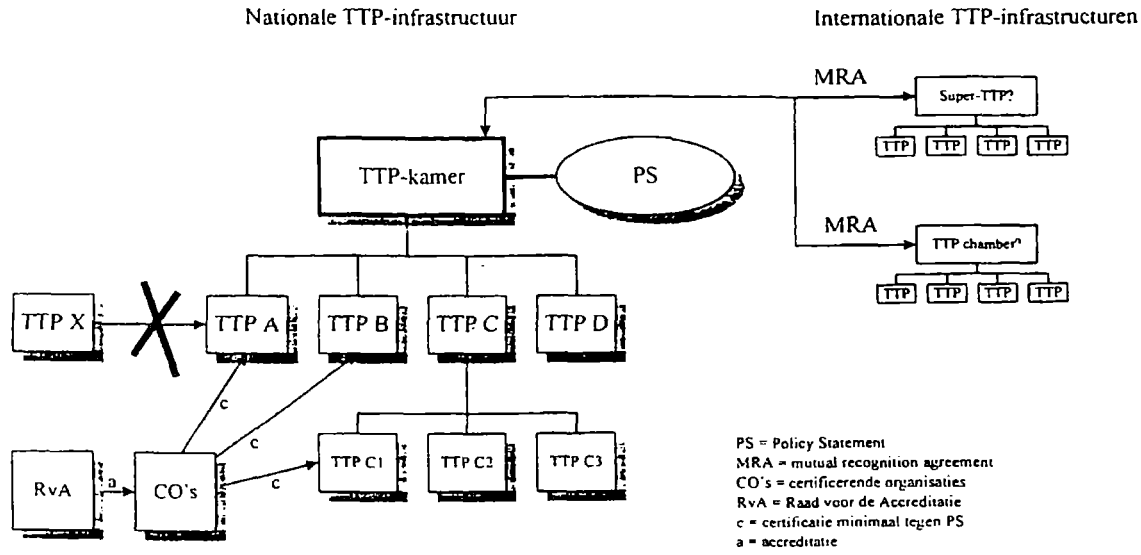
gecertificeerd door een door de Raad voor de Accreditatie geaccrediteerde organisatie. De in deze beleidsnotitie opgestelde randvoorwaarden dienen daarvoor te worden vertaald naar hanteerbare certificatiecriteria;
- bij de TTP-kamer aangesloten TTP's dienen uitsluitend elektronische certificaten te accepteren van TTP's die gecertificeerd zijn als boven beschreven of TTP's waarmee een nationale of internationale overeenkomst tot wederzijdse erkenning *(Mutual Recognition Agreement)* is gesloten.

Om de ontwikkeling van de TTP-kamer en de TTP-infrastuctuur te stimuleren dient een groeimodel te worden gevolgd. De belangrijkste rol van de overheid dient te bestaan uit het stimuleren van de ontwikkeling van de TTP-kamer en een TTP-infrastructuur die voldoet aan de in de beleidsnotitie gestelde randvoorwaarden, het internationaal uitdragen van het Nederlandse beleidsmodel in het kader van de wederzijdse erkenning van digitale handtekeningen en het wegnemen van de handelsbelemmeringen voor cryptografische goederen en producten op de interne Europese markt.

De overheid dient hiertoe een aantal concrete maatregelen te treffen, die hieronder worden opgenoemd:
- De overheid dient de totstandkoming van een certificatieschema te stimuleren, waarbij de in deze beleidsnotitie genoemde randvoorwaarden dienen te worden vertaald naar hanteerbare certificatiecriteria.
- De overheid dient TTP's die zich aansluiten bij de TTP-kamer actief te stimuleren, bijvoorbeeld door het beschikbaar stellen van subsidies of kredieten; aan deze stimulering dient zo spoedig mogelijk invulling te worden gegeven.
- De overheid dient een actieve rol te spelen op het gebied van voorlichting en onderwijs.
- De overheid dient aansluiting bij de TTP-kamer in principe als eis te stellen aan TTP's die diensten aan de overheid leveren.
- De overheid dient de ontwikkeling van specifieke apparatuur en programmatuur die voldoet aan de gestelde randvoorwaarden te stimuleren.
- De overheid dient het functioneren van een aldus op te richten TTP-kamer na een periode van twee jaar te evalueren.

De uiteindelijke taakstelling, positionering en samenstelling van de TTP-kamer zijn nog onderwerp van discussie. Overheid en marktpartijen dienen zo snel mogelijk een initiatief te nemen met de verdere uitwerking hiervan.

Figuur 4 – Schema voor TTP-infrastructuur



6 CONCLUSIES

Overheid en bedrijfsleven dienen concrete maatregelen te treffen om de snelle ontwikkeling van een betrouwbare TTP-infrastructuur te bevorderen. Daarbij zal aansluiting worden gezocht bij het zelfregulerings*mechanisme*.

Overheid, aanbieders en gebruikers van TTP-diensten dienen het initiatief te nemen tot het oprichten van een TTP-kamer, die waarborgt dat aan de gestelde randvoorwaarden wordt voldaan. In de TTP-kamer hebben, naast de overheid, zowel de aanbieders als de gebruikers van TTP-diensten op vrijwillige basis zitting.

De overheid dient de oprichting van genoemde TTP-kamer te begeleiden en te stimuleren. Aan deze stimulering dient zo spoedig mogelijk invulling te worden gegeven.

De overheid dient de totstandkoming van een certificatieschema te stimuleren, waarbij de in deze beleidsnotitie genoemde randvoorwaarden dienen te worden vertaald naar hanteerbare certificatiecriteria.

De overheid dient TTP's die zich bij de TTP-kamer aansluiten te stimuleren. Aan deze stimulering dient zo spoedig mogelijk invulling te worden gegeven.

In principe dient de overheid uitsluitend diensten af te nemen van TTP's die zich bij de TTP-kamer hebben aangesloten.

De overheid dient de ontwikkeling en het gebruik van apparatuur en programmatuur die bijdraagt aan een betrouwbare TTP-infrastructuur te stimuleren.

De overheid dient het Nederlandse schema in het kader van de wederzijdse erkenning van TTP's internationaal uit te dragen.

Terzake de in hoofdstuk 4.3 beschreven specifieke randvoorwaarde van rechtmatige toegang dient daarnaast via een partnership approach tussen de overheid en het relevante bedrijfsleven een voor alle partijen aanvaardbaar instrumentarium voor het faciliteren van de rechtmatige toegang te worden ontwikkeld. Om te waarborgen dat het relevante bedrijfsleven dit nog te ontwikkelen instrumentarium ook daadwerkelijk toepast zal ook hier aansluiting worden gezocht bij een zelfreguleringsmechanisme. Uitgangspunt hierbij zal zijn dat deze zelfregulering een wettelijke verankering krijgt.

De overheid dient na uiterlijk twee jaar de ontwikkelingen in Nederland te evalueren, waarbij wordt getoetst in hoeverre deze ontwikkelingen aan de gestelde randvoorwaarden voldoen en of de gestelde voorwaarden toereikend zijn.

Bijlage 1

Resultaten fase 3

1 Inleiding

Deze bijlage bevat een samenvatting van het rapport met de uitkomsten van de inventarisatie die is verricht met betrekking tot de implementatie van de mogelijke randvoorwaarden op basis van de versie d.d. 19-09-97 bij een viertal TTP-organisaties en -diensten. Deze inventarisatie is verricht door de EDP AUDIT POOL in samenwerking met de Technische Universiteit Delft in het kader van fase 3 van het «Projectplan NAP/TTP» d.d. 7 juli 1997.

2 Opdracht

De inventarisatie is in opdracht van het Ministerie van Verkeer en Waterstaat en het Ministerie van Economische Zaken uitgevoerd conform bovengenoemd projectplan.

3 Doelstelling inventarisatie

De doelstelling van de inventarisatie was om, ten behoeve van de rapportage in fase 4, met betrekking tot het stuk «NAP/TTP – Inventarisatie van mogelijke randvoorwaarden – Discussiestuk» versie d.d. 19 september 1997 (hierna te noemen: «Mogelijke randvoorwaarden»), na te gaan in hoeverre deze in fase 2 van het project geformuleerde mogelijke randvoorwaarden in de praktijk toepasbaar zijn voor een operationele TTP-dienst.

4 Objecten van onderzoek

De objecten van onderzoek zijn de «Mogelijke randvoorwaarden» en het daarop gebaseerde evaluatiekader zoals die zijn geformuleerd ten aanzien van de TTP-organisatie en de TTP-dienst in relatie tot de vier geselecteerde pilotprojecten.

5 Scope en reikwijdte werkzaamheden

De scope en reikwijdte van de door ons gedefinieerde werkzaamheden moeten worden bezien in de context van het gestelde in het hiervoor onder 1 genoemde projectplan en onder 3 vermelde discussiestuk d.d. 19-09-97.
Voor de goede orde wordt opgemerkt, dat:

- waar in het projectplan sprake is van het begrip «beoordelen» gelezen moet worden «inventariseren»;
- tijdens de onderzoeksperiode door de leden van de Consultatiegroep Aanbieders en Gebruikers commentaar is geleverd op de set «Mogelijke randvoorwaarden» d.d. 19-09-97 waarop de inventarisatie is gebaseerd. Met dit commentaar is alleen rekening gehouden voorzover het de vier pilotorganisaties betreft.

De opdracht omvatte niet het vormen van een oordeel of de «Mogelijke randvoorwaarden» noodzakelijk en voldoende zijn voor het realiseren van een betrouwbare TTP-organisatie en -dienst.

6 Aanpak en werkwijze

1. Volgens het projectplan is in fase 2 een raamwerk opgesteld dat is vastgesteld door de projectgroep. Daarin is een verzameling van basisvoorwaarden opgenomen die zijn gerelateerd aan de criteria betrouwbaarheid, aansprakelijkheid, privacy, interoperabiliteit,

rechtmatige toegang en onafhankelijkheid. De normen hebben betrekking op de TTP-organisatie en -dienst van de pilot-organisatie en zijn nader onderverdeeld in organisatorische en technische voorzieningen. Een aantal van deze voorwaarden is van toepassing op alle TTP-diensten, terwijl sommige voorwaarden slechts van toepassing zijn op specifieke klassen van TTP-organisaties en -diensten.

2. Uitgaande van dit raamwerk «Mogelijke randvoorwaarden» d.d. 19–09–97 hebben wij de belangrijkste aspecten van organisatorische en technische aard uitgewerkt in een evaluatiekader. De inhoud van dit kader is in de conceptfase afgestemd met de opdrachtgevers. Dit kader is verstrekt aan de pilot-organisaties en is gehanteerd als de basis voor de inventarisatie.

3. Het evaluatiekader is ingevuld door elk van de vier bij de inventarisatie betrokken TTP-organisaties en -diensten. Verder is schriftelijke informatie verkregen en zijn interviews gehouden. Bij de inventarisatie is door ons nagegaan in welke mate de in het evaluatiekader gedefinieerde aspecten van organisatorische en technische aard toepasbaar zijn bij de operationele TTP-organisatie en -dienst. Tevens is aan de hand van het evaluatiekader nagegaan of de «Mogelijke randvoorwaarden» d.d. 19-09-97 aanvulling of nadere uitwerking behoeven.

4. De besprekingsverslagen van de interviews zijn in de conceptfase met de pilotorganisaties afgestemd.

5. Met de betrokken TTP-organisaties is overeengekomen dat over de verkregen informatie alleen in geanonimiseerde vorm zal worden gerapporteerd. Daartoe is een geanonimiseerde samenvatting van de antwoorden met betrekking tot het evaluatiekader opgesteld.

6. In hoofdstuk 7 zijn de hoofdlijnen vermeld die bij de inventarisatie naar voren zijn gekomen. Deze hoofdlijnen dienen als invoer voor de beleidsnotitie die in het kader van fase 4 van het projectplan is voorzien.

7 Hoofdlijnen uitkomst inventarisatie

De hoofdlijnen van de uitkomsten van de inventarisatie en de daarbij naar voren gebrachte opmerkingen zijn hieronder weergegeven.

7.1 Volwassenheid TTP-dienst

De mate waarin de TTP-dienst ten tijde van de inventarisatie operationeel was, verschilde per pilot-organisatie.

De uitkomsten van de inventarisatie zijn door deze omstandigheid voor een deel gebaseerd op uitspraken en inzichten van de geïnterviewden, die niet konden worden getoetst aan de hand van een feitelijke implementatie van de TTP-dienst.

Bij de nog niet operationele TTP-diensten konden de randvoorwaarden door middel van interviews toch worden getoetst doordat belangrijke keuzes voor het realiseren van een volledig operationele TTP-dienst reeds waren gemaakt.

7.2 Mogelijke randvoorwaarden

De uitkomst van de inventarisatie naar de set van «Mogelijke randvoor-

waarden» versie d.d. 19-09-97, die is opgesteld in het kader van fase 2 van het projectplan, geeft aanleiding tot de volgende opmerkingen:

- de set anticipeert in onvoldoende mate op de (verwachte) praktijksituatie;
- de set is onduidelijk en/of multi-interpretabel;
- de set als geheel wordt door de pilotorganisaties te zwaar geacht;
- de set houdt onvoldoende rekening met:
  - TTP-diensten die een verschillend niveau van «trusted» bieden;
  - aanloopsituaties waarin nog niet aan alle randvoorwaarden kan worden voldaan;
  - degene voor wie de set bestemd is (voor de TTP-organisatie intern, het marktsegment, alle TTP-organisaties);
  - de wenselijkheid versus toepasbaarheid en haalbaarheid van randvoorwaarden;
  - de actoren/aspecten die de voorwaarden bepalen (TTP-organisaties intern, marktsegment, marktmechanisme, overheid).

7.3 Terminologie

De meningen van de pilotorganisaties lopen sterk uiteen ten aanzien van de inhoud en de strekking van het begrip «onafhankelijkheid» dat in de «Mogelijke randvoorwaarden» is omschreven als financiële en bestuurlijke onafhankelijkheid. Uit de interviews is gebleken, dat de pilotorganisaties het begrip «onafhankelijkheid» soms anders interpreteren. In de betekenis van «belangenverstrengeling» zien de pilotorganisaties onafhankelijkheid enerzijds als noodzakelijke randvoorwaarde voor het bewerkstelligen van het begrip «trusted». Anderzijds zien de pilot organisaties het juist als een voordeel voor het realiseren van een «trusted-niveau» indien de TTP-organisatie onderdeel van een gevestigde organisatie uitmaakt. In een dergelijke situatie wordt wel de noodzaak onderkend voor het realiseren van organisatorische functiescheidingen.

Daarnaast komen bij de pilotorganisaties verschillen naar voren ten aanzien van het begrip onafhankelijkheid in relatie tot het begrip «koppelverkoop». Dit betreft de scheiding tussen de TTP-organisatie als certificaten-uitgevende-instantie en de TTP-diensten waarbij deze certificaten worden toegepast. Een aantal van de pilotorganisaties ziet deze scheiding als een essentiële randvoorwaarde.

7.4 Scheiding CA/RA

Ten aanzien van de randvoorwaarde «functiescheiding» is de mening van de in de inventarisatie betrokken pilotorganisaties dat het in ieder geval vanuit de praktijk gezien wenselijk is scheiding aan te brengen tussen de functie van Registration Authority (RA) en die van Certification Authority (CA). Het is echter moeilijk deze scheiding bij kleine TTP-organisaties of TTP-organisaties in oprichting te realiseren.

7.5 Sleutelbeheer

Bij het merendeel van de TTP-organisaties wordt het creëren van de sleutelparen door de klanten verricht. De TTP-organisatie geeft alleen certificaten uit. In die situaties is key escrow (het bewaren van private sleutels door een TTP-organisatie) niet mogelijk, tenzij de klant zelf hiertoe mocht besluiten. De consequentie daarvan is, dat een groot deel van de randvoorwaarden niet, of slechts ten dele, van toepassing is. De belangrijkste voorbeelden hiervan zijn een onuitwisbare en volledige verslaglegging van transacties alsmede de herleidbaarheid van sleutelmateriaal. Doordat generatie van sleutelmateriaal niet bij de TTP-organisatie plaatsvindt heeft dit voor TTP-organisaties als voordeel het beperken van

de aansprakelijkheid tegen ongeautoriseerde kennisname van data en het niet kunnen vervullen van een rol bij key escrow. De verantwoordelijkheid (en daarmee de aansprakelijkheid) in de richting van de klanten wordt daarmee tevens beperkt.

7.6 Continuïteit

Bij de pilot-organisaties bestaat eenheid van opvatting ten aanzien van de noodzaak om de continuïteit te waarborgen, bijvoorbeeld door het stellen van eisen ten aanzien van de overdracht van de dienstverlening.

7.7 Gebruik van sleutelmateriaal

De TTP-organisatie kan niet voorkomen dat sleutelparen ten behoeve van digitale handtekeningen door de klant worden aangewend ten behoeve van encryptie, anders dan door gebruik te maken van specifieke algoritmen (Digital Signature Algorithm – DSA) of specifieke apparatuur.

7.8 Wederzijdse erkenning

De in de inventarisatie betrokken TTP-organisaties onderschrijven de noodzaak om te komen tot de een of andere vorm van wederzijdse (inter)nationale erkenning, zowel voor het eigen marktsegment als de facto voor alle TTP-diensten voor het creëren van voorwaarden voor interoperabiliteit. Implementatie van mechanismen voor wederzijdse erkenning is echter niet eenvoudig (zelfs niet binnen een marktsegment) en vergt een actieve en stimulerende rol van de overheid.

7.9 Abstractheid mogelijke randvoorwaarden

De formulering van de mogelijke randvoorwaarden is te abstract. Daardoor kunnen de randvoorwaarden in onvoldoende mate worden gecontroleerd, hetgeen problemen kan opleveren bij de certificering en erkenning van een TTP-organisatie.

7.10 Rol overheid

De onderzochte pilotorganisaties zijn verdeeld over de mate waarin de overheid een rol moet spelen bij het totstandkomen van een set van randvoorwaarden voor adequate TTP-diensten. (Bijna) operationele TTP's zijn geneigd hun eigen intern ontwikkelde normen als randvoorwaarden voor anderen te zien. TTP-organisaties in oprichting willen zo min mogelijk regulering door de overheid.

7.11 TTP-kamer

De pilotorganisaties zijn van mening, dat een oplossing moet worden gevonden tussen enerzijds regulering van randvoorwaarden door de overheid en anderzijds dit geheel over te laten aan de marktwerking. De meeste pilotorganisaties vinden dat ten minste moet worden gestreefd naar de instelling van een zogenaamde TTP-kamer. Deze kamer moet worden belast met ten minste:

- een niet verplichte certificering van TTP-organisaties op basis van door haar opgestelde minimum randvoorwaarden;
- het realiseren van internationale erkenningen.

Over de verhouding van een dergelijke kamer tot (de rol van) de overheid hebben de pilotorganisaties geen uitspraken gedaan.

7.12 Aanvullende randvoorwaarden

De inventarisatie heeft uitgewezen dat het aanbeveling verdient in de set met mogelijke randvoorwaarden rekening te houden met de volgende situaties: outsourcing van TTP-functies; sleutelgeneratie bij klanten dan wel de TTP-organisatie.

7.13 Vastlegging en bewaring van informatie

De TTP-organisaties zijn terughoudend in het aanvaarden van voorwaarden met betrekking tot vastlegging en bewaring van informatie, anders dan strikt noodzakelijk is voor de primaire doelstelling van de dienstverlening en het afleggen van externe (publieke) verantwoording.

Bijlage 2

Literatuur

Bij het opstellen van deze beleidsnotitie zijn de volgende bronnen geraadpleegd:

1. Opzet TTP-project in het kader van het Nationaal Actieprogramma Elektronische Snelwegen, 19 februari 1997
2. Projectplan NAP/TTP, KPMG Management Consulting / KPMG EDP Auditors, 4 juli 1997
3. Voorwaarden te stellen aan Trusted Third Parties t.b.v. TTP-project NAP, drs. R. van der Luit, Ministerie van Binnenlandse Zaken, 2 juni 1997, Stg. CONFIDENTIEEL
4. Overzicht randvoorwaarden, ing. J. van der Spek, Ministerie van Defensie, Centrale Organisatie/Bureau Beveiligingsautoriteit, 3 juni 1997
5. Randvoorwaarden voor het aanbieden en het gebruik van TTP-diensten, ir. S.B. Bootsma, Ministerie van Justitie, 3 juni 1997
6. TNO Fysisch en Elektronisch Laboratorium, Trusted Third Parties en Key Escrow, maart 1997
7. Gesetz zur digitalen Signatur (Signaturgesetz-SigG) – Referententwurf, Stand: 19. September 1996 – en verordnung zur digitalen Signatur (Signaturverordnung – SigV) – Referententwurf: Stand: 19. September 1996 – (Engelse versie beschikbaar als SOG-IS document 012/97,5 March 1997)
8. Ministry of Finance Finland, Electronic identification and Electronic Citizen Card, Helsinki, 29 October 1996
9. Ministry of Research and Information Technology Denmark, Draft Bill for Act on Digital Signature etc, IT-Policy Office, J nr 9601756, 14 November 1996
10. Information Society initiative, Licensing of Trusted Third Parties for the provision of encryption services, Public Consultation Paper on Detailed Proposals for Legislation, March 1997
11. ETSI, Technical Committee, Reference Technical Report, DEG/SEC-003000, Requirements for Trusted Third Party Services, Version 0.0.7, 26 March 1997
12. OECD, Cryptography Policy Guidelines, 27 March 1997
13. A European Initiative in Electronic Commerce, COM(97)157
14. Text of Administration March 12 Key Recovery Draft Legislation
15. MDW-rapport Normalisatie en Certificatie, MDW-werkgroep Certificering, februari 1996
16. Verslag van werkbijeenkomst Cryptografiebeleid, Canberra 9–11 juli 1997, mw. drs. H. de Brabander-Ypes
17. Commentaar op mogelijke randvoorwaarden ten behoeve van NAP/TTP-project, drs. R. van der Luit, Ministerie van Binnenlandse Zaken – vertrouwelijk
18. Japan paper, Working meeting on international cooperation on cryptography policy, Canberra, 9–11 juli 1997
19. ISO/IEC JTC1/SC27, PDTR 14516, Guidelines for the use and management of Trusted Third Parties, 9 juni 1997
20. APEC Task Group on Public Key Authentication, OECD, 20–21 October 1997
21. Ensuring Security and Trust in Electronic Communication, Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, COM (97) 503
22. Draft Uniform Rules on Electronic Signatures, United Nations Commission on International Trade Law (UNCITRAL), Working Group on Electronic Commerce, 32th session, Vienna, 19–30 January 1998.
23. MDW-rapport Elektronisch verrichten van rechtshandelingen, Ministerie van Justitie en Ministerie van Economische Zaken, maart 1998

24. Nota wetgeving voor de elektronische snelweg, Ministerie van Justitie, februari 1998
25. OECD Privacy guidelines: Guidelines for the protection of privacy and transborder flows of personal data, 23 september 1980.
26. EU Privacy-richtlijn: Richtlijn 95/46/EG van het Europees Parlement en de Raad van Europa van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens, COM(92) 422 def. -SYN 287
27. EU Telecom Privacy-richtlijn: Richtlijn van het Europese Parlement en de Raad betreffende de bescherming van persoonsgebonden gegevens en van de persoonlijke levenssfeer in het kader van digitale telecommunicatienetwerken, met name in het kader van het digitale netwerk voor geintegreerde diensten (ISDN) en van digitale mobiele netwerken, COM(94) 128 def. – SYN 288
28. EU Council Regulation (EC) No. 3381/94
29. EU Council Decision No. 94/942/PESC
30. Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies

Bijlage 3

Betrokken partijen

Leden van de projectgroep NAP/TTP

de heer H.W. de Vries	Ministerie van Verkeer en Waterstaat (voorzitter)
de heer R. de Bruin	Ministerie van Verkeer en Waterstaat (secretaris)
de heer E.R. de Lange	Ministerie van Verkeer en Waterstaat
de heer M. Buys	Ministerie van Economische Zaken (secretaris)
mevrouw H. de Brabander-Ypes	Ministerie van Economische Zaken
de heer P.H. Polman	Ministerie van Economische Zaken
de heer T. Regeer	Ministerie van Economische Zaken
de heer G.L. van den Hil	Ministerie van Algemene Zaken
de heer R.P. van der Luit	Ministerie van Binnenlandse Zaken
de heer J.G.M. Timmermans	Ministerie van Binnenlandse Zaken
de heer P.J. Rosenkrantz	Ministerie van Defensie
de heer S.B. Bootsma	Ministerie van Justitie
de heer H. de Zwart	EDP AUDIT POOL
de heer H.A. Kampert	EDP AUDIT POOL
de heer J.C.A. van der Lubbe	Technische Universiteit Delft
de heer E.E.O. Roos Lindgreen	KPMG EDP Auditors
mevrouw A.K.I. Tuinder	KPMG EDP Auditors

Leden van de Consultatiegroep Aanbieders en Gebruikers

de heer C.P. Louwerse	Academisch Ziekenhuis Leiden (Dienst CDIV)
mevrouw E. Aberson	Consumentenbond
de heer F. Schasfoort	Coopers & Lybrand
de heer R. Bloemer	Enschedé/Sdu B.V.
de heer A.A.J. Reuver	IBM Nederland B.V.
de heer R. van Wolferen	Interpay Nederland B.V.
de heer D. Rebel	KEMA Nederland B.V.
de heer G.J.C. Lekkerkerker	KNB
de heer J.J. Moelker	Ministerie van Binnenlandse Zaken (ACIB)
de heer M. Bullinga	Ministerie van Volkshuisvesting, Ruimtelijke Ordening en Milieubeheer
de heer R. van Esch	Nederlandse Vereniging van Banken
mevrouw A. Rotte	NInet B.V.
de heer E. Hardam	NLSign B.V.
de heer M.A.P.J. de Jager	Percomad B.V.
de heer H.A. Algra	Philips Crypto B.V.
de heer B. van Leent	Point Information Systems B.V.
de heer J. Döll	PTT Post B.V.
de heer G.J. Schuringa	Rabobank Nederland N.V.
de heer M. Huijbers	RCC
de heer F. van Doorn	Reginet B.V.
de heer J.J. Borking	Registratiekamer

de heer P. van Dijken	Shell Information Services B.V.
de heer A. van Bellen	Stichting Ediforum
de heer H. van Ginkel	VBN
de heer M.P. Crijns	Vereniging van KvK en Fabrieken
de heer S.H. Katus	VNO/NCW

Tweede Kamer der Staten-Generaal

2

Vergaderjaar 1999–2000

26 387 Actieprogramma Elektronische Overheid

Nr. 4

BRIEF VAN DE MINISTER VOOR GROTE STEDEN- EN INTEGRATIEBELEID

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 16 december 1999

Eind 1998 heb ik u het Actieprogramma Elektronische Overheid toegestuurd (Kamerstukken 26 387).
Graag doe ik u hierbij de eerste uitvoeringsrapportage, die het jaar 1999 betreft, van het Actieprogramma toekomen.

De Minister voor Grote Steden- en Integratiebeleid,
R. H. L. M. van Boxtel

KST43133
ISSN 0921 - 7371
Sdu Uitgevers
's-Gravenhage 2000

Uitvoeringsrapportage Actieprogramma Elektronische Overheid 1999

Inleiding

In het actieprogramma Elektronische Overheid (ELO)[1] dat u eind 1998 is toegezonden, werd aangegeven dat de Kamer jaarlijks geïnformeerd zal worden over de voortgang van het actieprogramma. Tijdens het algemeen overleg dat over de elektronische overheid op 5 oktober jl . werd gehouden, heb ik de Kamer toegezegd de eerste voortgangsrapportage nog in 1999 te zullen uitbrengen.
Zoals bekend is de algemene doelstelling van het actieprogramma om met inzet van informatie- en communicatietechnologie (ICT) de publieke sector efficiënter, effectiever en klantvriendelijker te laten functioneren. Het actieprogramma is langs vier lijnen opgezet, waarbij per actielijn een aantal concrete projecten wordt uitgevoerd:
- een goede elektronische toegankelijkheid van de overheid
- een betere publieke dienstverlening
- een verbeterde interne bedrijfsvoering bij de overheid
- flankerend beleid: doelgroepenbeleid en onderzoek ICT & overheid

Deze uitvoeringsrapportage volgt dezelfde volgorde, waarbij per actielijn wordt ingegaan op de voortgang van de projecten die inmiddels zijn gestart.

1. Een toegankelijke, digitale overheid

De eerste lijn is om zo veel mogelijk overheidsinformatie op Internet te krijgen, om zo de mogelijkheden te benutten die Internet biedt om de burger, bedrijven en instellingen vrijwel zonder kosten toegang te verlenen tot een grote hoeveelheid overheidsinformatie. Internet biedt bovendien mogelijkheden voor opzoeken, combineren en visualiseren van informatie die met traditionele media niet te evenaren zijn.

Communicatie Overheid Burger: www.overheid.nl

In 1999 is op dit vlak een forse slag gemaakt met de komst van www.overheid.nl, een algemene toegangspoort tot elektronische informatie van het openbaar bestuur. De site kent een simpel te hanteren zoekmachine, verwijst en biedt een verbinding naar de websites van alle overheidsorganisaties (ministeries, Hoge Colleges van Staat, adviesorganen, provincies, gemeenten, waterschappen, regionale openbare lichamen, zelfstandige bestuursorganen, e.d.). Met behulp van www.overheid.nl kan men nagaan of een overheidsorgaan verantwoordelijkheid neemt voor een bepaalde website. De databank van www.overheid.nl bevat nu rond duizend overheidssites. De ministeries en provincies beschikken allemaal over een officiële site, maar bij gemeenten en waterschappen is dit nog slechts bij één op de drie het geval. De portal site biedt verder toegang tot alle Kamerstukken en alle wet- en regelgeving uit Staatsblad, Staatscourant en Traktatenblad, zoals die vanaf 1995 verschenen zijn. (Van de jaren daarvoor zijn deze stukken veelal niet in elektronische vorm beschikbaar). Op basis van reacties van gebruikers is inmiddels een start gemaakt met het verfijnen van de mogelijkheden van de portal website. In de loop van 2000 zullen nieuwe ingangen opgenomen worden die meer uitgaan van de vraagkant van gebruikers, waarbij met name gedacht wordt aan thema- en doelgroeploketten. Momenteel bezoeken zo'n 5000 personen dagelijks de site. Zeker binnen de overheid en bij professionele gebruikers is de naamsbekendheid van de site al groot. Vanaf november 1999 is in televisiespotjes in samenwerking met het NBLC, het Nederlands Bibliotheek- en LectuurCentrum, geïntegreerd aandacht gevraagd voor de mogelijkheden van Internet in de bibliotheek en voor www.overheid.nl.

[1] Kamerstukken II, 1998/1999, 26 387, nr. 1.

Ook de Helpdesk Overheid.nl, die in september van start is gegaan, voorziet duidelijk in een behoefte. Overheden weten steeds beter de weg te vinden naar de Helpdesk voor advies over het bouwen van een website c.q. het kwalitatief verbeteren van hun overheidswebsite. Een onderzoek naar de kwaliteit van overheidssites is al afgerond, terwijl begin 2000 de resultaten beschikbaar komen van onderzoeken naar belemmeringen om te komen tot een overheidswebsite. De Helpdesk zal de resultaten hiervan zoveel mogelijk vertalen naar instrumenten voor het opheffen van deze belemmeringen. *Speciaal* voor overheden is al door de Helpdesk samen met OL2000 een handboek ontwikkeld en een speciale Internetsite www.overheid.nl/helpdesk in het leven geroepen. Via deze site en via andere communicatiekanalen kunnen overheden diensten afnemen van de Helpdesk, waarmee een bijdrage geleverd wordt de totstandkoming van (ver)nieuw(d)e overheidssites.

In het kader van het traject Communicatie Overheid Burger is al in 1998 f 15 mln aan het NBLC toegekend voor het project «Overheid een open boek». Het project beoogt in de eerste plaats om medio 2000 in 95% van de Nederlandse bibliotheken één of meerdere PC's met Internet te hebben geïnstalleerd. Inmiddels hebben de ruim 600 Nederlandse bibliotheek-organisaties voor ruim 1000 bibliotheekvestigingen (centrales en filialen) actieplannen ingediend om Internet aan het publiek aan te bieden. Naar verwachting zal het aantal Internet-werkplekken in bibliotheken eind 1999 het dubbele zijn van eind 1998. In de tweede plaats wordt bibliotheek-personeel bijgeschoold, daar medio 1998 slechts in de helft van de bibliotheekvestigingen een of meer op nieuwe media geschoolde medewerker beschikbaar was. Aan de cursussen over het verzorgen van Internet-trainingen aan het publiek hebben in periode medio 1998 tot medio 1999 360 bibliotheekmedewerkers deelgenomen. Het derde onderdeel van dit project richt zich op het geven van cursussen aan het publiek, waarmee in het najaar van 1999 in talrijke bibliotheekvestigingen is gestart. Doelgroep hierbij is allereerst het oudere publiek, dat nog geen of zeer weinig kennis heeft gemaakt met «de computer».
De ook in het leven geroepen site www.webwijzer.net geeft een handzaam overzicht van inspirerende en vernieuwende websites van Nederlandse overheden, musea en archiefdiensten. Als extra stimulans is de onafhankelijke WebWijzerjury ingesteld die in 1999 elke maand een prijs heeft uitgereikt voor de beste overheidssite. De feestelijke uitreiking van de WebWijzeraward 1999 vond begin december plaats op het congres «Wegen naar de virtuele overheid». De gemeente Amsterdam werd als winnaar onderscheiden. Gezien het succes van de WebWijzer zal ook in 2000 maandelijks een award worden toegekend.

Overheidsinformatie op Internet

Een goed voorbeeld van specifieke overheidsinformatie die dankzij het ELO-actieprogramma nu digitaal is ontsloten is het Elektronisch Loket Rechterlijke Organisatie, het ELRO-project. Vanaf begin december 1999 is de site *www.rechtspraak.nl* operationeel, die informatie geeft over de rechtspraak in het algemeen. Zo geeft het een toelichting op verschillende gerechtelijke procedures, adresgegevens van gerechten, tarieven voor griffierechten en verwijzingen naar aan rechtspraak georiënteerde sites (zowel in het binnen- als in het buitenland). Tevens biedt ELRO toegang tot eigen sites van zes gerechten die van een gezamenlijke lay-out en navigatiestructuur gebruik maken. Dit bevordert de herkenbaarheid van de rechterlijke organisatie alsmede door het gezamenlijke portal site de vindbaarheid van een gerecht. Via het elektronisch loket zullen ook belangwekkende arresten van de Hoge Raad kostenloos voor het publiek beschikbaar komen. Daarnaast worden in de databank bestuursrechtelijke

- uitspraken uit de interne Justex-databank geplaatst en zullen uitspraken opgenomen worden van zaken die veel publiciteit trekken.

Zoals bekend heeft de Staat in 1994 een overeenkomst met uitgever Kluwer gesloten over het tot stand brengen van de Algemene Databank Wet- en regelgeving (ADW). Onderdeel van deze overeenkomst is dat de Staat gedurende de looptijd van deze overeenkomst niet meewerkt aan een hiermee concurrerende wettenverzameling. Deze overeenkomst loop in september 2000 af. Vanaf dat moment staat het de Staat vrij om een wettenverzameling via Internet toegankelijk te maken. Daartoe zal in 2000 een Europese aanbesteding worden voorbereid.

In het voorjaar van 2000 zal het rijksdeel van de Staatsalmanak via www.overheid.nl voor een ieder gratis beschikbaar komen. Het zal twee keer per jaar geactualiseerd worden. Dit past binnen het lopende contract dat de Staat met de SDU heeft en dat eind 2001 afloopt. In 2001 zal een openbare aanbesteding plaatsvinden over het met ingang van 2002 op Internet plaatsen van een versie van de Staatsalmanak die dagelijks actueel gehouden zal worden.

Bij het digitaal beschikbaar stellen van overheidsinformatie op Internet is al het een en ander gebeurd ten aanzien van bestuurlijke informatie. Zo zijn van de Eerste en Tweede Kamer en ook van een redelijk aantal provinciale staten de vergaderstukken al op Internet beschikbaar. Maar met betrekking tot de besturen van gemeenten en waterschappen is dit nog nauwelijks het geval. Van alle gemeenten biedt slechts tien procent enige informatie over raadsstukken of verordeningen op Internet aan. Om hier verbetering in aan te brengen is in 1999 f 6 mln, waarvan f 4,5 mln uit het ELO-budget, toegezegd aan projectvoorstellen die beogen bestuurlijke informatie op Internet te krijgen. De subsidieregeling houdt in dat overheidsorganisaties die structureel bestuurlijke informatie integraal en kosteloos op Internet gaan publiceren een bijdrage in de eenmalige projectkosten kunnen krijgen van maximum f 250 000. Voor provincies, gemeenten en waterschappen geldt dat alleen collectieve projecten met minimaal vijf deelnemers worden gehonoreerd. De belangstelling voor de subsidieregeling was boven verwachting groot. Binnen drie maanden zijn 35 aanvragen ontvangen die voldoen aan de criteria van de regeling, waarvan ongeveer de helft van lagere overheden. Opmerkelijk is de grote belangstelling onder gemeenten voor het indienen van collectieve projecten. Rond 90 gemeenten en deelgemeenten zullen raadsinformaties op Internet gaan aanbieden. Dit waren er tot nu toe slechts 16. Daarnaast zullen rond zeventig gemeenten starten met een eigen website met een beperkte hoeveelheid bestuurlijke informatie. Ook onderzoeksinstituten als het SCP gaan met behulp van de subsidieregeling over tot het integraal publiceren van al hun rapporten op Internet. Daar het aantal aanvragen verre de verwachtingen overtrof, is het oorspronkelijke budget fors verhoogd. Met deze subsidieregeling wordt derhalve een flinke stap voorwaarts gezet bij het toegankelijk maken van overheidsinformatie.

Kader overheidsbestanden

De elektronische gegevensbestanden van het bestuur zijn in beginsel openbaar onder het regime van de Wet openbaarheid van bestuur. Bestuursorganen zijn, uiteraard voor zover dat binnen de kaders van de Wet openbaarheid van bestuur en de privacy-wetgeving is toegelaten, verplicht om die bestanden op verzoek aan burgers, bedrijven en overheden te verstrekken. Uit onderzoek is gebleken dat veel overheidsorganen zich het auteursrecht en het databankenrecht op deze bestanden voorbehouden. Dat heeft tot gevolg dat burgers en bedrijven de openbare bestanden vaak wel kunnen krijgen, maar deze verder niet mogen

gebruiken. Daarom is een helder beleidskader nodig. Bij het ontwikkelen van dit beleidskader is mijn inzet dat, in het verlengde van de tarieven van de Wet openbaarheid van bestuur, de elektronische gegevensbestanden van het bestuur algemeen beschikbaar komen tegen maximaal de marginale kosten van de verstrekking. Algemeen beschikbaar betekent dat burgers, overheden en bedrijven er niet alleen bij kunnen, maar dat zij die informatie ook vrij kunnen gebruiken. In ambtelijk overleg is gebleken dat er weliswaar brede steun is voor dit uitgangspunt van beleid, maar ook dat er enkele aanzienlijke obstakels zijn. Allereerst is er een aantal legitieme, gevestigde belangen van organisaties die opdracht dan wel toestemming hebben gekregen om (een deel van) de kosten van aanleg en beheer van hun bestanden aan afnemers in rekening te brengen. Daarnaast lijken er gevallen te bestaan waarin het vragen van een hogere vergoeding dan de marginale kosten van de verstrekking een hoger maatschappelijk rendement (positief welvaartseffect) genereert. Bestuurlijk overleg moet leiden tot meer inzicht in mogelijke uitzonderingen op het geformuleerde uitgangspunt en in wenselijke overgangsbepalingen. De Kamer zal op korte termijn op de hoogte gesteld worden van de resultaten van deze consultaties en de vervolgactiviteiten die in het licht van de commentaren nodig zijn om de voorgenomen beleidslijn te implementeren.

2. Elektronische dienstverlening door de overheid

Niet alleen voor het publiek relevante overheidsinformatie moet op het net beschikbaar komen, ook de transacties tussen overheid en burgers/bedrijven/instellingen moeten veel meer via de elektronische snelweg gaan plaatsvinden. Dat is de tweede lijn van het actieprogramma Elektronische Overheid.
In het Actieprogramma werd als doel geformuleerd dat in 2002 minimaal een kwart van de publieke dienstverlening langs elektronische weg afgehandeld moet kunnen worden. Deze doelstelling werd later in De Digitale Delta[1] herhaald

Overheidsloket 2000 (OL2000)

Om deze 25% te halen is in 1999 het programma OL2000 in 1999 fors geïntensiveerd. De deelnemende partijen, de ministeries van BZK, EZ, VROM en VWS, hebben inclusief ELO-bijdragen voor de periode 1999–2002 ruim f 25 mln beschikbaar gesteld voor OL2000, waarvan al f 10 mln in 1999 is vastgelegd. Van deze f 10 mln kwam f 6,2 mln uit de ELO-gelden
Het doel van het programma OL2000 is om komen tot een landelijk dekkend geheel van «fysieke» (balie, zuil, schriftelijk, telefonisch) en virtuele (internet)loketten op de beleidsdomeinen Bouwen & Wonen, Zorg & Welzijn en Bedrijven. Voor burgers en bedrijven moet hierlangs:
- alle informatie die van belang is voor de afname van publieke diensten op een voor hen logische plek integraal beschikbaar komen;
- minimaal de helft van de publieke dienstverlening op die terreinen op een voor hen logisch samenhangende wijze geleverd worden;
- minimaal een kwart van die dienstverlening elektronisch afgehandeld worden.

Het programma OL2000 bestaat uit vier projecten:
1) Het project «Bedrijvenloket», dat door het ministerie van EZ wordt aangestuurd, en dat er toe moet leiden dat eind 2001 op drie plaatsen fysieke en elektronische bedrijvenloketten functioneren en er een beproefde toolkit gereed is voor toepassing in geheel Nederland. In 1999 is het projectplan vastgesteld en is de eerste fase, de selectie, afgerond.

[1] Kamerstukken II, 1998/1999, 26 643, nr 1.

Besloten is dat de drie voorhoedeprojecten in de gemeente Groningen, de provincie Drenthe en de regio Alkmaar zullen plaatsvinden.
2) Het loket Zorg & Welzijn, waar het ministerie van VWS de eerst verantwoordelijke voor is. Resultaat van dit project moet zijn dat eind 2002 op vijf tot tien plaatsen loketten Zorg & Welzijn functioneren alsmede een beproefde toolkit beschikbaar is. In 1999 is het projectplan vastgesteld en is de eerste fase, de selectie van de voorhoedeprojecten, gestart.
3) Loket Bouwen & Wonen, dat getrokken wordt door het ministerie van VROM, met als beoogd resultaat eind 2002 op meerdere plaatsen functionerende fysieke en elektronische loketten gereed te hebben. Ook voor dit project geldt dat in 1999 het projectplan is vastgesteld en dat is begonnen met de eerste fase, de selectie van voorhoedeprojecten.
4) Ontwikkelen en toepassen van generieke instrumenten, plegen van onderzoek en missieactiviteiten (voortrekkersrol BZK). Dit moet erin resulteren dat eind 2002 ontwikkelde en beproefde generieke instrumenten beschikbaar zijn, waaronder overzichten van digitale vraagpatronen van overheidsklanten, alsmede een digitale catalogus van overheidsproducten, een elektronisch formulier en een model elektronisch loket. Uiteraard zal er daarbij voor gezorgd worden dat de betrokken publieke dienstverleners bereid zijn om deze instrumenten toe te passen. Begin 2000 komen de resultaten beschikbaar van een onderzoek naar de stand van zaken bij de geïntegreerde dienstverlening in Nederland. De gebruikte onderzoeksmethodiek wordt ook geschikt gemaakt als meetinstrument voor publieke dienstverleners om zelf hun voortgang op dit terrein te beoordelen. Verder komt op korte termijn een referentiemodel beschikbaar voor het elektronische loket dat kan dienen als een standaard voor dienstverleners en ICT-bedrijven.
Het oorspronkelijke voor 1999 geraamde ELO-budget van f 2,5 mln is met f 3,7 mln verhoogd tot f 6,2 mln. Voor de ontwikkeling van generieke instrumenten was namelijk f 1,9 mln extra nodig, opdat ook de publieke dienstverleners die niet worden betrokken in de voorhoedeprojecten al aan de slag kunnen met het integreren en digitaliseren van de eigen dienstverlening. Tevens is de ELO-bijdrage aan het Bedrijvenloket, die oorspronkelijk verspreid over de jaren 1999–2002 zou worden toegekend, in 1999 reeds in één keer is toegekend.

Virtueel loket Centra Werk en Inkomen (CWI)

Het beoogde eindproduct van het project «Virtueel CWI-loket» is een logisch en functioneel ontwerp voor de informatie- en adviesfunctie van de Centra voor Werk en Inkomen, waarbij optimale gebruik wordt gemaakt van elektronische hulpmiddelen. In de vervolgfase van het project zal de verdere uitwerking van het ontwerp plaatsvinden in onder andere een testopstelling, die op locatie door samenwerkende partijen in een regio wordt toegepast. Na de proefneming wordt het ontwerp geijkt en gefaseerd ingevoerd. Doel van het project is dat het virtuele CWI-loket door de samenwerkende partijen (met name Lisv, Arbeidsvoorziening Nederland, VNG en Stichting CVCS) gedragen wordt. Vanuit het ELO-actieprogramma is in 1999 een bijdrage van f 1,75 mln geleverd ter financiering van de aanloopfasen. Het blijkt dat de afstemming met lopende initiatieven tot enige vertraging en aanpassingen binnen oorspronkelijke planning leiden, maar naar verwachting kan het uitvoeringsprogramma zoals gepland halverwege 2000 beginnen.

Zorgpas

In 1999 is vanuit het ELO-actieprogramma een bijdrage van f 3 mln geleverd aan het project «Zorgpas». Het Zorgpas-project is gericht op het tot stand brengen van een open elektronisch netwerk in de Nederlandse gezondheidszorg, dat kan worden gebruikt door alle patiënten

(zorgconsumenten), zorgaanbieders en zorgverzekeraars. Centraal daarbij staat het standaardiseren van elektronische communicatie, waarbij een chipcard een hulpmiddel is. De bedoeling is dat iedere verzekerde gaat beschikken over een Zorgpas met in de chip persoonsgegevens ter identificatie alsmede gegevens over de verzekering, zoals geldigheid, administratieve gegevens en voorwaarden voor betalingsgarantie. De zorgaanbieder kan deze data benutten en doorwerken in zijn eigen administratie, de zorgverzekeraar houdt de gegevens actueel en de patiënt krijgt de mogelijkheid zelf de zorgpas elektronisch te laten actualiseren met behulp van informatiezuilen. In de periode april 2000 – april 2001 zal een experiment in de regio Eemland plaatsvinden met 370 000 chipcards. Er wordt een communicatienet van voldoende capaciteit ingericht dat door middel van smartcardlezers wordt voorzien van een aantal basisfunctionaliteiten. Hiermee krijgen 864 zorgaanbieders en 30 zorgverzekeraars de gelegenheid de communicatiemogelijkheden aan hun bedrijfsprocessen te toetsen. De plannen voor deze proef zijn opgesteld door zorgverzekeraars, zorgaanbieders en patiënten gezamenlijk. VWS is daar als waarnemer bij betrokken. De totale projectkosten belopen naar raming f 17,5 mln, waarvan de overheid de helft voor haar rekening neemt.

Elektronische Identiteitskaart

Zoals bekend zal begin 2001 een nieuwe generatie reisdocumenten het licht zien. Er komt een nieuw paspoort en de Europese Identiteitskaart zal worden vervangen, door een chipkaart. Deze chipkaart zal op een later moment voorzien worden van biometrie en een elektronische identiteitsfunctie. Zo zal de nieuwe identiteitskaart door toepassing van onder meer chiptechnologie geschikt worden gemaakt voor identiteitsvaststelling op afstand en om een digitale handtekening te zetten. Naar verwachting zal realisatie per 2003 plaats kunnen vinden. In 1999 zijn de eerste fasen («quick scans») van twee «best practise»-onderzoeken gestart. De betreffende eindrapporten over PKI en biometrie zijn door de externe deskundigen opgeleverd, terwijl het derde best practise-onderzoek naar chiptechnologie is gestart. Voor de beproeving van de toe te passen nieuwe technologieën zijn in 1999 pilots voorbereid. De pilot die samen met de partners uit de sociale zekerheid (SZW, LISV en ARBVO) wordt uitgevoerd, is zodanig vergevorderd dat deze half januari 2000 kan starten in de gemeente Delft. De taakverdeling tussen de partners is dat BZK zorgdraagt voor de kaart en de infrastructuur en de sociale zekerheidssector voor de (elektronische) diensten. Vanuit het ELO-budget is in 1999 een bijdrage van f 2 mln verstrekt aan de totale projectkosten van f 3,6 mln.

3. Achter de schermen van de overheid

Niet alleen in de front-office, in het verkeer tussen overheid en burger/bedrijven, is het zaak om zoveel mogelijk nuttig gebruik te maken van de voordelen die ICT biedt, ook in de back-office, achter de overheidschermen kan nog veel meer op een zinvolle wijze ICT worden ingezet, teneinde de overheid efficiënter, effectiever en klantvriendelijker te laten opereren.

Overheidscommunicatie

Een belangrijk project hierbij is het totstandbrengen van een overheidsintranet. In 1999 is een start gemaakt met dit intranet, waar om te beginnen in 2001 alle Rijksambtenaren en de werknemers bij de hoge Colleges van Staat op aangesloten zullen worden. Een uitgevoerd architectuuronderzoek heeft inmiddels geresulteerd in een bestek voor een Europese

aanbesteding en een contra-expertise. Naar verwachting zal in de tweede helft van 2000 een eerste versie van het rijksoverheidintranet, waar dan een aantal departementen op zullen zijn aangesloten, operationeel zijn. Een van de diensten van het rijksoverheidintranet zal een dynamische elektronische adresgids zijn, waarin alle rijksambtenaren met hun e-mailadres staan opgenomen. Deze adresgids moet in 2001 operationeel zijn. In 1999 is een consultatiedocument opgesteld om draagvlak van alle departementen te verwerven.
De departementen van AZ, BZ, EZ, Financiën, Justitie, LNV, OCW, SZW, V&W en VWS kennen inmiddels eigen intranetten, terwijl bij BZK en Defensie hiertoe pilots lopen. Ook de Eerste en Tweede Kamer en de Algemene Rekenkamer kennen eigen intranetten. Instellingen die al over een intranet beschikken kunnen straks makkelijker toegang krijgen tot het op te zetten overheidsintranet.

Elektronische handtekening en PKI

Het project «Public Key Infrastructure» (PKI) bouwt voort op twee studies die in 1999 zijn uitgevoerd: «Vertrouwen in Communiceren» en «Communiceren in vertrouwen». In de jaren 2000–2002 zullen meerdere projecten worden ondersteund teneinde in deze periode te komen tot een betrouwbare infrastructuur voor PKI-diensten, ook wel TTP (Trusted Third Parties)-diensten genoemd. Deze infrastructuur voorziet in een vastgesteld beveiligingsniveau voor de communicatie van de publieke sector, moet transparant zijn voor de gebruikers en biedt de mogelijkheid om de elektronische handtekening te gaan gebruiken. PKI-diensten ondersteunen ondermeer het beveiligen van elektronische post, Internetgebruik en de elektronische communicatie tussen overheden, burgers en bedrijfsleven. Een betrouwbare PKI is dan ook van importantie voor het grootschalig gebruik van de digitale handtekening. Om het vaak onderschatte belang van een goede PKI voor de publieke sector helder te maken, is in 1999 opdracht gegeven tot het opzetten en uitvoeren van een communicatieplan.

Stroomlijning Basisgegevens

Om de efficiëntie en effectiviteit van het overheidshandelen te verhogen dient de gegevensuitwisseling tussen organisaties, sectoren en bestuurslagen te worden gestroomlijnd. In 1999 is hiertoe een sterke impuls gegeven met de start van het programma Stroomlijning Basisgegevens. In 1999 lag het accent op het scheppen van de randvoorwaarden, het creëren van draagvlak, inventarisatie en analyse van de problematiek, de ontwikkeling van het inhoudelijke concept en de opstart van voorbeeldprojecten. Het programma kent zes programmalijnen.

- De lijn Programma-ondersteuning en Communicatie (voortrekkersrol BZK) heeft inmiddels geresulteerd in de aanstelling van een full-time programmamanager en de optuiging van een Programmabureau dat begin 2000 van start zal gaan.
- Binnen de lijn Informatiekaart Nederland (BZK) is een concept-informatiekaart gereed gekomen, bedoeld als analyse-instrument voor de opsporing van witte vlekken, overlap en strijdigheden op het zeer brede terrein van de basisgegevens. Mede aan de hand van deze kaart worden in de vorm van expert- en managementsessies de belangrijkste knelpunten op het terrein van de gegevensuitwisseling bepaald.
- Het tot stand brengen van een stelsel van authentieke registraties vormt de kern van het programma Stroomlijning Basisgegevens. In 1999 zijn binnen de lijn Authentieke Registraties (SZW) de uitgangspunten van het concept vastgesteld, op basis waarvan in 2000 in interactie met de andere programmalijnen de nadere uitwerking en vaststelling plaats zal vinden.

- De programmalijnen Kostenverrekening (Financiën) en Wetgeving (Justitie) zijn randvoorwaardelijk voor de programmalijn Authentieke Registraties. Beide programmalijnen zullen begin 2000 worden opgestart. Voor de programmalijn Kostenverrekening is al belangrijk voorwerk gereed gekomen in de vorm van het rapport van de Commissie Tops.
- Binnen de lijn Voorbeeldprojecten ten slotte zijn inmiddels vier voorbeeldprojecten gestart: Gebouwenregister (VROM, Ravi en VNG); Geografisch Kernbestand (VROM, Ravi); Basisbedrijvenregister (EZ, in samenwerking met Belastingdienst, CBS, Kamers van Koophandel en LISV) en Verzekerdenadministratie (SZW, LISV in samenwerking met de UVI's). Voor alle projecten zijn in 1999 plannen van aanpak vastgesteld en is met de uitvoering begonnen.

De activiteiten en planning voor 2000 zijn in hoge mate afhankelijk van de uitkomst van de lopende oriënterende activiteiten, die voor het grootste deel begin 2000 worden afgerond in de vorm van de lopende knelpunten- en haalbaarheidsanalyses, van een vastgesteld concept van authentieke registraties en van nader uitgewerkte projectplannen.

Overheidstelefonie 2000 (OT2000)

Het intensiveren van het ICT-gebruik in de back-office van de overheid brengt aanzienlijke kosten met zich mee, die veelal door de betrokken overheidspartijen zelf gedragen moeten worden. Op initiatief van BZK/GSI hebben verschillende overheidspartijen hun kracht gebundeld om via een Europese aanbesteding in de geliberaliseerde telecom-markt een substantiële besparing te bereiken op de kosten voor telefonie. In de aanbesteding die in 1999 plaatsvond, participeren rond 250 overheidsorganen, waaronder gemeenten, onderwijsinstellingen en waterschappen. De ministeries en provincies hebben daarvoor in het project OT 2000 het voortouw genomen. De aanbiedingen leveren over de percelen vaste, mobiele en internationale telefonie gemiddeld een (potentiële) korting op van 18% ten opzichte van de huidige markttarieven, waarbij het geboden dienstenpakket tevens volop mogelijkheden biedt tot toepassing van nieuwe communicatietechnologie binnen de overheid. Voor elk perceel zijn twee aanbieders geselecteerd, waardoor overheidsorganisaties voldoende keuzemogelijkheden krijgen te voorzien in hun telecommunicatiebehoeften. Besloten is de aanbesteding voorlopig te gunnen aan Dutchtone en KPN Telecom voor de vaste telefonie, aan Dutchtone en Libertel voor de mobiele telefonie en aan Dutchtone en Versatel voor telefonie naar bijzondere bestemmingen. Bij de formele gunning, die rond april 2000 wordt verwacht, zullen mantelovereenkomsten worden afgesloten met een looptijd van drie jaar met een totale waarde van circa f 400 miljoen.

Digitale Duurzaamheid

In het actieprogramma Elektronische Overheid is gewezen op het risico dat de overheid als gevolg van allerlei ICT-toepassingen haar institutionele geheugen kwijt zou kunnen raken. Om de «Digitale Duurzaamheid» van de overheid te verzekeren, is met een gelijknamig traject gestart. Allereerst zijn hiertoe in 1999 van een op te zetten Recordkeeping System (RKS) de functionele eisen geformuleerd, is een marktverkenning uitgevoerd en een laboratorium-opstelling ingericht. De resultaten van deze activiteiten zijn eind 1999 gepubliceerd in een brochure met CD-ROM «Het geheugen als actieve kracht». Ook n.a.v. een onderzoek naar e-mail is een brochure met de titel «Archivering van elektronische post» gepubliceerd. Daarnaast is de eerste fase van vooronderzoek naar een Digitaal Depot afgerond. In het rapport «Carrying Authentic, Understandable and Usable Digital Records Through Time» worden voorstellen gedaan voor een bewaar-

strategie en voor vervolgstappen. Het in het rapport geadviseerde testbed is in het najaar Europees aanbesteed. Tenslotte is het Archiefbesluit interdepartementaal becommentarieerd en voor advies aan de Raad voor Cultuur voorgelegd en heeft de KU Brabant onderzoek verricht naar de voor digitale duurzaamheid relevante wet- en regelgeving.

4. ICT-doelgroepenbeleid en onderzoek ICT & Overheid

Als flankerend beleid zijn in het kader van de Elektronische Overheid in 1999 op twee terreinen activiteiten gestart: specifiek ICT-doelgroepenbeleid en onderzoek «ICT & Overheid»

Specifiek doelgroepenbeleid: Digitale trapveldjes

Bedacht dient te worden dat aan de ene kant de ontwikkeling van een netwerksamenleving vele, vooral economische kansen biedt, maar dat aan de andere kant er het risico is dat bepaalde bevolkingsgroepen de aansluiting bij de netwerkmaatschappij missen, of slechts zeer eenzijdig in aanraking komen met (de gevolgen van) informatietechnologie. Het gaat hierbij om alle groepen inwoners, van jong tot oud, vrouwen en mannen, allochtonen en autochtonen. Daarom moet er met name in de aandachtswijken van de grote steden geïnvesteerd worden in ICT-educatie. Doel van het project Digitale Trapveldjes is om de inwoners van deze wijken mogelijkheden te bieden om Internet-vaardigheden op te doen en zich daarmee een betere positie op de arbeidsmarkt te verwerven. Op het «digitale trapveld» worden mensen met een zwakke arbeidsmarktpositie geschoold in ICT-gebruik, zodat ze hiermee meer kans krijgen op werk. Hiernaast kunnen potentiële «digibeten» (bijv. 50+ers en baanlozen) kennis maken met computers, e-mail en Internet. Het is de bedoeling om een koppeling tussen beide doelgroepen aan te brengen: degenen die geschoold worden in het ICT-gebruik gaan cursussen geven aan de «digibeten» uit hun wijk. Hiertoe wordt een ruimte ingericht als «digitaal trapveld» met alle bijbehorende faciliteiten. Deze ruimte kan onderdeel uitmaken van een buurthuis, school, bejaardenhuis of bibliotheek.
Het project digitaal trapveld start niet vanuit een nulsituatie; er loopt reeds een aantal soortgelijke lokale projecten in de G25, echter wel met verschillende accenten. Voorbeelden hiervan zijn de interculturele wijkmediacentra in Utrecht en Amsterdam en Rotterdam, het Telematicacentrum, verbonden aan de bibliotheek in de Haagse Schilderswijk en een project in Emmen. Dit zijn in feite digitale trapveldjes «avant la lettre». Op dit moment wordt geïnventariseerd welke plannen de 25 «Grote Steden», de G25, op de plank hebben liggen, maar waarvoor men lokaal onvoldoende budget voor de start beschikbaar heeft. Een aantal aansprekende lokale projecten zal reeds in de aanloopfase een startsubsidie ontvangen – d.w.z. vooruitlopend op het beschikbaar komen van eigen BZK-budget van f 20 mln.
Het project Digitale Trapveldjes start officieel begin 2000 met een conferentie met een informatiemarkt, best practices en demonstraties. Ook wordt voor een heldere en eenduidige informatievoorziening een website ontwikkeld. Tevens zal ook in 2000 de «cyberbus» worden ingezet. De cyberbus is een rijdend klaslokaal met 16 computers met internetaansluiting en is zeer geschikt als een soort «digitaal trapveld op wielen». De cyberbus heeft in ELO-opdacht in 1999 20 locaties bezocht, waardoor rond 750 personen (vaak voor de eerste keer) kennis hebben gemaakt met de virtuele wereld.

Onderzoek ICT & Overheid

In het Actieprogramma Elektronische Overheid werd het belang onderstreept van het verrichten van onderzoek naar de invloed van ICT op de

overheid. Met de in 1999 opgekomen discussie over de zogeheten «Nieuwe economie» is dit belang alleen nog maar groter geworden. Met het onderzoeksprogramma «ICT & Overheid» is in 1999 een start gemaakt door Nederland aan te melden als deelnemer aan het onderzoek «Governance in the digital economy». Dit onderzoeksprogramma wordt uitgevoerd door de «Alliance for converging technology» onder leiding van de bekende Amerikaanse publicist Don Tapscott. Het programma wil de praktische implicaties voor de overheid onderzoeken, die de nieuwe technologie en de nieuwe economie met zich meebrengen; «what kind of governments do citizens need for the 21st century?» Deelname aan dit internationale programma geeft via congressen, literatuurverwijzingen en e-mailcontacten direct toegang tot en inzicht in belangwekkende ontwikkelingen in toonaangevende landen op het gebied van ICT. In maart 2000 zal Tapscott voor de Nederlandse deelnemers een seminar houden.

Complementair aan de deelname aan het Tapscott-onderzoek is de deelname aan het Nederlandse programma Internet & Openbaar Bestuur. Bij dit onderzoeksprogramma zijn betrokken: de ministeries van VROM, BZK, V&W en Financiën, Katholieke Universiteit Brabant, Erasmus Universiteit Rotterdam, Ordina, Maatschappij voor Oude en Nieuwe Media, Tweede Kamer, TNO en Programmabureau OL2000. Centraal staat in dit programma de vraag: «Wat doet het Internet met het openbaar bestuur?». Op het Internet ontwikkelt zich immers een set van virtuele werkelijkheden die relatief autonoom is ten opzichte van de bestaande politiek-bestuurlijke werkelijkheid, die eigen vormen van politiek en bestuur laat zien en die talloze interferenties met de bestaande politiek-bestuurlijke werkelijkheid vertoont. Het is daarom van belang kennis van en inzicht te verwerven in de specifieke politiek-bestuurlijke aspecten van Internet, waarbij Internet een metafoor is voor politiek-bestuurlijke, sociaal-culturele en economische organisatiepatronen van de (nabije) toekomst. Er zijn drie onderzoeksvoorstellen geformuleerd. De eerste, Gekoppelde Verantwoordelijkheden, betreft de verdeling van verantwoordelijkheden bij Interbestuurlijke Gegevensuitwisseling. De tweede, ICT de baas?, gaat over informatietechnologie, stuurbaarheid en individuele autonomie, en de derde, De schaduwdemocratie, gaat in op het thema «ICT en maatschappelijke participatie».

Ook bij de ITAFIT tenslotte is vanuit het actieprogramma aansluiting gezocht. ITAFIT is een Nederlands netwerk dat case-studies verricht naar bijdragen van ICT aan de oplossing van bestuurlijke vraagstukken. Door daarbij een vaste opzet te hanteren ontstaan onderling vergelijkbare uitkomsten. Deelname aan dit netwerk biedt de mogelijkheid om bij de startfase van bepaalde overheidsprojecten gebruik te maken van ervaringen die elders al zijn opgedaan. In 1999 werden best-practices onderzocht ten behoeve van het Elektronisch Loket Rechtelijke Organisatie (in Australië) en de Elektronische Identiteitskaart (in Finland).

5. Financiën en organisatie van de Elektronische Overheid

Voor de uitvoering van het Nationaal Actieprogramma Elektronische Snelwegen (NAP) uit 1994, inmiddels opgevolgd door De Digitale Delta, is structureel f 70 mln per jaar beschikbaar. Overeengekomen is hiervan in principe jaarlijks f 20 mln à f 30 mln voor zowel de collectieve als de particuliere sector beschikbaar te stellen. In 1999 was f 31,6 mln beschikbaar voor de uitvoering van het Actieprogramma Elektronische Overheid. Van dit beschikbare budget is in 1999 f 25,5 vastgelegd en is f 4 mln (voor op het Internet plaatsen van wet- en regelgeving, A3) naar 2000 doorgeschoven.
Het beschikbare bedrag in 2000 komt daarmee op f 34 mln. Daar de uitgaven van sommige posten moeilijk exact van te voren te ramen zijn,

onder meer als gevolg van budgettair onzekere uitkomsten van bepaalde aanbestedingstrajecten, wordt het verantwoord geacht in de begrotingsopstelling voor het jaar 2000 uit te gaan van f 35,5 mln plus twee p.m.-posten en daarmee dus boven het beschikbare bedrag uit te komen. Uiteraard is de f 34 mln «het matje» waarbinnen het totaal van de ELO-uitgaven in 2000 moeten blijven.

Begroting Elektronische Overheid (verplichtingen in f mln)

	B 1999	Realis. 1999	B 2000
Toegankelijkheid van de overheid:			
A1: Communicatie Overheid Burger/ www.overheid.nl	0,7	0,7	–
A2: Kader overheidsbestanden	–	–	–
A3: Overheidsinformatie op Internet	*10,0*	*6,0*	*9,0*
■ wet- en regelgeving	4,0	–	4,0
■ overheidsaanbestedingen	1,0	–	1,0
■ gerechtelijke uitspraken	1,5	1,5	–
■ overheids-content/dienstverl.regeling	2,75	4,5	4,0
■ Staatsalmanak	0,75	0,0	–
Dienstverlening door de overheid:			
B1: OL2000	2,5	6,2	2,5
B2: Virtueel CWI-loket	2,0	1,75	4,0
B3: ICT zorgsector (o.a. Zorgpas)	3,0	3,0	4,0
B4: Elektronische Identiteitskaart	2,0	2,0	p.m.
B5: Elektronische Heerendiensten	–	–	p.m.
Achter de overheidsschermen:			
C1: Overheidsintranet en PKI	3,1	0,5	6,5
C2: Stroomlijning Basisgegevens	5,3	3,7	7,0
C3: ON21	–	–	–
C4: Digitale Duurzaamheid	2,0	0,1	2,0
Onderzoek en doelgroepenbeleid:			
D1: Onderzoek ICT & Overheid	0,5	0,3	0,5
D2: Voorlichting	0,5	–	–
D3: Digitale Trapveldjes	–	1,0	–
TOTAAL		25,25	35,5 + p.m.
Totaal beschikbaar	31,6		34,0

Voor de bewaking van de voortgang van het Actieprogramma als geheel is het zgn. interdepartementale ELO-directeurenoverleg ingesteld, dat in 1999 drie keer bijeen is geweest. Dit directeurenoverleg verricht als het ware het inhoudelijke voorwerk voor de NAP-Stuurgroep dat vervolgens dan ook nog slechts marginaal de voorgelegde ELO-plannen hoeft te toetsen. Deze werkwijze zal ook in 2000 gevolg worden.

6. ELO in 2000

De resultaten van 1999 overziend kan gesteld worden dat een goede start gemaakt is met de uitvoering van het actieprogramma Elektronische Overheid. Met name op de eerste twee actielijnen, elektronische toegankelijkheid tot en dienstverlening door de overheid, is onder meer bij de bibliotheken en bij het op Internet plaatsen van overheidsinformatie veel in gang gezet. Het voornemen om meer van Internet gebruik te gaan maken bij overheidsaanbestedingen heeft in 1999 evenwel nog niet tot concrete acties geleid. Die staan nu voor 2000 gepland. Hetzelfde kan gezegd worden over aangekondigde initiatieven voor «pro-actieve» dienstverlening, het door de overheid verrichten van service, zonder dat de burger daar eerst expliciet om gevraagd heeft. In het Actieprogramma werd verondersteld dat de activiteiten in de front-office, met name pijler A, vooral hun beslag zouden krijgen in 1999. Gebleken is evenwel dat ook

in de periode daarna nog financiële overheidstimulering nodig is. Vandaar dat ook voor 2000 hier middelen voor zijn vrijgemaakt.
De gestarte projecten «Elektronische identiteitskaart» en «PKI» zijn behalve voor hun primaire doelen ook van belang voor het realiseren van de elektronische handtekening: een thema dat onder meer aan de orde kwam in het algemeen overleg van oktober over het Actieprogramma. Mede op basis van de ervaringen uit deze twee projecten zal hier in 2000 verder aan worden gewerkt. Ook het project Stroomlijning basisgegevens zal in 2000 in een stroomversnelling komen. Dit mede n.a.v. het rapport van de commissie Slechte over het belang om de administratieve lasten te verminderen.
Onder de pijler «Onderzoek en doelgroepenbeleid» stond in het actieprogramma aangekondigd dat er een voorlichtingsprogramma voor overheidsmanagers zou worden opgezet. Zoals echter de sterke toename van het aantal e-mail- en Internetaansluitingen binnen de overheid laat zien, wordt het belang van ICT voor de dagelijkse interne bedrijfvoering steeds meer onderkend. Besloten is dan ook geen apart voorlichtingsprogramma voor overheidsmanagers te starten.

In het algemeen overleg van oktober kwam ook aan de orde dat naast de centrale vraag van het actieprogramma, wat doet de overheid met ICT?, minstens zo belangrijk is wat ICT met de overheid doet. Zoals toen aangekondigd ben ik voornemens om in het voorjaar van 2000 een nota uit te brengen die een visie formuleert op deze laatste vraag. In deze nota zal onder meer worden ingegaan op de invloed van ICT op de democratie, op de kwaliteitsnormen van een elektronische overheid en op de privacy. Een van de inspiratiebronnen voor het opstellen van deze nota is de discussie over de elektronische overheid die gedurende december gevoerd is op de site www.rogervanboxtel.nl. Eerder werd via deze site een maand lang aan de hand van stellingen gediscussieerd over de millenniumproblematiek resp. het minderhedenbeleid en nadien over het grote stedenbeleid. Aan het eind van elke maand vond een live-chat met mij plaats, waarbij direct werd gereageerd op de binnenkomende vragen en opmerkingen. Deze permanente elektronische spreekuren vinden vooral plaats om ervaring op te doen met het gebruik van ICT bij beleidsvorming en democratische participatie. Het experiment loopt door maart 2000, waarna het zal worden geëvalueerd. Aan de hand hiervan zal bekenen worden of zo'n elektronisch spreekuur van structurele aard zou moeten zijn.

Eind 2000 zal de Kamer opnieuw via een voortgangsrapportage op de hoogte gesteld worden van de voortgang van de projecten die voortkomen uit het Actieprogramma Elektronische Overheid.

De Minister voor het Grote Steden- en Integratiebeleid,
R. H. L. M. van Boxtel

Tweede Kamer der Staten-Generaal

2

Vergaderjaar 1999–2000

26 387 Actieprogramma Elektronische Overheid

Nr. 6

VERSLAG VAN EEN ALGEMEEN OVERLEG
Vastgesteld 15 maart 2000

De vaste commissie voor Binnenlandse Zaken en Koninkrijksrelaties[1] heeft op 22 februari 2000 overleg gevoerd met minister Van Boxtel voor Grote Steden- en Integratiebeleid over:

- **de brief van de minister voor Grote Steden- en Integratiebeleid d.d. 16 december 1999 bij de eerste voortgangsrapportage over het actieprogramma Elektronische overheid (26 387, nr. 4);**
- **de brief van de minister voor Grote Steden- en Integratiebeleid d.d. 23 december 1999 over de instelling van een PKI-taskforce (26 387, nr. 5);**
- **de brief van de minister voor Grote Steden- en Integratiebeleid d.d. 18 februari 2000 over elektronisch stemmen.**

Van dit overleg brengt de commissie bijgaand beknopt verslag uit.

Vragen en opmerkingen uit de commissie

Mevrouw **Augusteijn-Esser** (D66) was er verheugd over dat kort na het algemeen overleg van 5 oktober 1999 opnieuw een algemeen overleg over de elektronische overheid wordt gehouden. Zij vroeg de minister of de volgende voortgangsrapportage inderdaad nog voor het einde van 2000 kan worden besproken; de ontwikkelingen gaan immers zeer snel. Vervolgens vroeg mevrouw Augusteijn-Esser naar de uitkomsten van de verschillende onderzoeken die de minister in het vorige algemeen overleg had toegezegd. Deze zijn nodig voor een visie op de wederzijdse beïnvloeding van informatie- en communicatietechnologie (ICT) en de overheid. Zowel de tendens naar globalisering als die naar lokalisering zetten de positie van de nationale staat onder druk. Wanneer moet de overheid ingrijpen en wat moet zij faciliëren? In hoeverre kan zij met wet- en regelgeving haar rol blijven vervullen? Hoe wordt de versterking van digitale overheidsinformatie bevorderd in EU-verband en hoe worden de EU-richtlijnen op dit terrein geïmplementeerd?
Mevrouw Augusteijn-Esser sprak grote waardering uit voor het elektronische spreekuur van de minister. In mei verschijnt het eindrapport van de commissie-Franken over de digitale grondrechten. Hoe ziet de minister de invloed van ICT op de democratie?
In de brief van 16 december 1999 kondigt de minister onderzoek op drie

[1] Samenstelling:
Leden: Schutte (GPV), Te Veldhuis (VVD), ondervoorzitter, De Cloe (PvdA), voorzitter, Van de Camp (CDA), Van den Berg (SGP), Scheltema-de Nie (D66), Van der Hoeven (CDA), Van Heemst (PvdA), Oedayraj Singh Varma (GroenLinks), Rijpstra (VVD), Noorman-den Uyl (PvdA), Hoekema (D66), Dankers (CDA), Cornielje (VVD), O. P. G. Vos (VVD), Rehwinkel (PvdA), Wagenaar (PvdA), Luchtenveld (VVD), Verburg (CDA), Rietkerk (CDA), Halsema (GroenLinks), Kant (SP), Duijkers (PvdA), Balemans (VVD) en De Boer (PvdA).
Plv. leden: Rouvoet (RPF), Van Beek (VVD), Zijlstra (PvdA), Van Wijmen (CDA), Ravestein (D66), Augusteijn-Esser (D66), Balkenende (CDA), Barth (PvdA), Rabbae (GroenLinks), Cherribi (VVD), Gortzak (PvdA), Dittrich (D66), Wijn (CDA), Nicolaï (VVD), Van den Doel (VVD), Van Oven (PvdA), Apostolou (PvdA), Brood (VVD), Mosterd (CDA), Eurlings (CDA), Van Gent (GroenLinks), Poppe (SP), Belinfante (PvdA), Essers (VVD) en Kuijper (PvdA).

KST44517
ISSN 0921 - 7371
Sdu Uitgevers
's-Gravenhage 2000

terreinen aan. Mevrouw Augusteijn-Esser vroeg om een toelichting op de onderzoeksvoorstellen en om een tijdschema.
Het ministerie van Verkeer en Waterstaat heeft vorig jaar een notitie over trusted third parties (TTP's) aan de Tweede Kamer gezonden en doet samen met de ministeries van Justitie en van Binnenlandse Zaken en Koninkrijksrelaties (BZK) nader onderzoek voor de implementatie van de Europese richtlijn over elektronische handtekeningen. Mevrouw Augusteijn-Esser vroeg om nadere informatie hierover. Wie hebben er zitting in de taskforce? Hoe verloopt de samenwerking tussen de departementen?
De burger moet duidelijk inzicht hebben in datgene wat er met zijn gegevens wordt gedaan en bezwaar hiertegen kunnen aantekenen. Hoe is de bescherming van persoonsgegevens en datagegevens gewaarborgd? Zijn hiermee al problemen gebleken of kunnen er op dit punt problemen ontstaan?
Mevrouw Augusteijn-Esser complimenteerde de minister met de voortvarende start van het beleid, vooral voor de toegankelijkheid van de elektronische overheid en de elektronische dienstverlening. Verloopt het project Overheidsloket 2000 (OL2000) volgens plan? Hoe denkt de minister te bereiken dat de betrokken publieke dienstverleners de genoemde generieke instrumenten toepassen?
Zaken betreffende de backoffice konden volgens mevrouw Augusteijn-Esser sneller en efficiënter verlopen. Hoe wordt er draagvlak gecreëerd bij de andere departementen, de lagere overheden en andere betrokken instanties? Kan de minister een toelichting geven op het project stroomlijning basisgegevens?
Mevrouw Augusteijn-Esser noemde de digitale trapveldjes een goed initiatief en vroeg naar de plannen van de 25 grote steden. Ook vroeg zij naar het verloop van het project public key infrastructure (PKI), waarvan zij het doel ondersteunde.
De fractie van D66 heeft in het kader van de discussie over het begrotingsoverschot voorgesteld, 100 mln. extra te besteden aan de rol van de overheid als launching costumer. Wat is de reactie van de minister op dit initiatief? Welke mogelijkheden ziet hij voor de besteding van het geld? In ieder geval zou wet- en regelgeving zo snel mogelijk op internet moeten worden gezet.

De heer **Wijn** (CDA) complimenteerde de minister met de website www.overheid.nl, maar wees ook op fouten in de zoekmachine, die de kern van de site vormt. Hij achtte het voor iemand die de overheidsorganisatie niet goed kent moeilijk om zijn weg op de site te vinden en vroeg naar de resultaten van onderzoek onder gebruikers.
Een van de doelstellingen van de minister is dat goede voorbeelden onder sites die via www.overheid.nl bereikbaar zijn worden nagevolgd, maar de heer Wijn zag een dergelijk vliegwieleffect nauwelijks optreden. Een groot aantal gemeenten heeft nog geen site en slechts 10% geeft informatie over raadsstukken en verordeningen. Ook met dienstverlening door gemeenten via internet is sinds het verschijnen van het actieprogramma Elektronische overheid, een jaar geleden, nauwelijks vooruitgang geboekt. De rijksoverheid moet dit soort zaken niet van bovenaf opleggen, maar moet ook geen afwachtende houding nemen. Er wordt via de helpdesk goede informatie gegeven, maar de vraag is of gemeenten actief genoeg worden gestimuleerd. Zijn er streefdoelen, streeftermijnen, richtlijnen of voorschriften voor overheidsorganisaties vastgesteld in verband met het beschikbaar stellen van informatie via internet?
De heer Wijn haalde uit het actieprogramma aan dat voor een goed resultaat van ICT-projecten bij de overheid vooral commitment van de top in de organisatie noodzakelijk is. Hoe staat het met dit commitment bij gemeenten en andere overheden? Wil de minister de Tweede Kamer

regelmatig zowel kwalitatief als kwantitatief rapporteren over de stand van zaken bij medeoverheden en op andere ministeries?
Vervolgens haalde de heer Wijn uit het actieprogramma aan dat er onnodig hoge kosten worden gemaakt, veel ontwikkelingstrajecten te lang duren en desinvestering plaatsvindt door verouderde technologie of gebrek aan standaardisatie. Welke verbeteringen kan de minister inmiddels melden? Hoe vult hij zijn centrale rol voor standaardisatie ten behoeve van gemeenten en ministeries in?
Ter voorkoming van versnippering zou er in 1999 een ICT-uitvoeringsorganisatie worden opgericht, waarin bureaus zoals OL2000, ON21 en de helpdesk zouden worden samengevoegd. Wat is de stand van zaken? Zijn de schotten tussen de verschillende bureaus weggenomen?
Het actieprogramma bleek op sommige punten te ambitieus. De heer Wijn signaleerde achterstanden in het publiceren van wet- en regelgeving, aanbestedingen en de Staatsalmanak op internet. Wat zijn de oorzaken hiervan en welke conclusies trekt de minister hieruit? Ook de projecten overheidsintranet, stroomlijning van basisgegevens en digitaal archiveren lopen achter op de planning, terwijl juist de backoffice het mogelijk moet maken om in de frontoffice goede dienstverlening aan burgers te bieden. Wat zijn de oorzaken van deze achterstanden?
De heer Wijn zag in de activiteiten van SeniorWeb, dat zich richt op het gebruik van internet door ouderen een overeenkomst met de digitale trapveldjes. Hij vroeg de minister een subsidievoorstel voor uitbreiding van de activiteiten van deze organisatie te bekijken met een positieve instelling.
De heer Wijn concludeerde dat de vooruitgang in een jaar tijd mager is en drong bij de minister aan op een forse versnelling en een vernieuwd actieprogramma. Hij sloot zich aan bij het standpunt van mevrouw Augusteijn-Esser dat nog voor het einde van 2000 de volgende voortgangsrapportage moet worden besproken.

De heer **Cherribi** (VVD) wenste de minister geluk met het wegnemen van het millenniumprobleem en concludeerde dat de minister zich nu kan concentreren op het bereiken van een digitaal bestel. Hij herinnerde aan de grote ambities in het actieprogramma en constateerde een stagnatie in het vergroten van de toegankelijkheid van lagere overheden op internet, die van groot belang is voor de dienstverlening aan de burgers.
De VNG blijkt geen volledige lijst van gemeente- en plaatsnamen elektronisch beschikbaar te hebben waarmee zij bij de stichting Internet domeinregistratie Nederland het gebruik van die namen door anderen kan laten blokkeren. De heer Cherribi wees op de emotionele waarde van plaatsnamen voor de inwoners en vroeg de minister naar het aantal gemeenten en plaatsen dat niet de eigen naam als domeinnaam kan gebruiken. Verder vroeg hij de minister gemeenten en waterschappen te attenderen op dit probleem.
De heer Cherribi sprak er zijn teleurstelling over uit dat er voor de PKI alleen een taskforce binnen de overheid wordt ingesteld, terwijl de markt de beste encryptie levert. Hij vroeg de minister dan ook om een toelichting op de PKI-taskforce. Komt er aparte wetgeving voor de TTP's en is dit ook technisch mogelijk voor 2002?
De heer Cherribi complimenteerde de minister met de digitale trapveldjes en noemde diens website www.rogervanboxtel.nl een voorbeeld van interactiviteit. Hij vroeg om extra aandacht voor het betrekken van ouderen bij ICT-ontwikkelingen.
Ook vroeg de heer Cherribi om meer informatie over de methodologie en de bedoeling van het onderzoek van de heer Tapscott.
Ten slotte vroeg de heer Cherribi de minister in de volgende voortgangsrapportage niet alleen de vorderingen, maar ook de knelpunten te noemen. Aan de hand hiervan is immers de voortgang het beste te meten.

Mevrouw **Wagenaar** (PvdA) complimenteerde de minister met het tempo van zijn activiteiten, zeker wanneer het gaat om het tegengaan van een digitale tweedeling. De voortgangsrapportage is echter evenals het actieprogramma te veel top-down georiënteerd, terwijl internet juist gelijkwaardigere communicatie tussen overheid en burger mogelijk maakt.
Van de sites die via www.overheid.nl bereikbaar zijn, vond mevrouw Wagenaar die van het Koninklijk Huis het aardigste, vanwege de interactieve kinderspelletjes. Zij bepleitte meer kindersites van de overheid en vroeg om meer aandacht voor de professionaliteit, de toegankelijkheid en de interactiviteit van www.overheid.nl. Over de tekst «discussie gesloten» die zij op de meeste discussiesites tegenkwam, sprak zij haar verbazing uit. Volgens de monitor overheidssites biedt slechts 9% van de sites de mogelijkheid om over een onderwerp te discussiëren en worden vragen, zo die al per e-mail kunnen worden gesteld, vaak te laat of niet beantwoord. Op de website van Algemene Zaken (AZ) staat wel een postadres, maar geen e-mailadres. Verder wordt de actualiteit niet goed bijgehouden op www.overheid.nl. Het is onduidelijk waarom alleen het ministerie van Onderwijs, Cultuur en Wetenschappen apart wordt genoemd bij wetgeving.
In het algemeen overleg van 5 oktober 1999 heeft de minister toegezegd Postbus 51 en www.overheid.nl zo snel mogelijk in elkaar te zullen schuiven. Inmiddels wordt Postbus 51 op de overheidssite genoemd, maar op de website van Postbus 51 worden het nummer en de service van de Postbus-51-telefoon niet genoemd. Omdat dit onduidelijk is voor burgers die een vraag aan de overheid hebben, vroeg mevrouw Wagenaar de minister op korte termijn verbetering hierin te brengen.
Mevrouw Wagenaar vroeg de minister bij de webwijzeraward meer aandacht te geven aan digitale dienstverlening en interactiviteit of hiervoor een aparte prijs in te stellen. Wanneer worden de burgerinformatiesystemen actief, waarvoor de minister 6,3 mln. beschikbaar heeft gesteld?
Deelnemers aan SeniorWeb blijken wel met elkaar te kunnen e-mailen, maar niet met de gemeente, terwijl dit juist van groot belang is voor ouderen die slecht ter been zijn.
Mevrouw Wagenaar wees op het drempelverhogende effect van hoge uurtarieven voor internetgebruik in bibliotheken. Zij vroeg om een richtlijn voor internettarieven in bibliotheken en opperde de mogelijkheid van speciale tarieven van providers voor bibliotheken. Over de toegankelijkheid van overheidsinformatie, die vaak alleen gratis toegankelijk is op cd-rom, zouden nadere afspraken moeten worden gemaakt. Wat zijn overigens de kosten voor het gebruik van de digitale trapveldjes, die helemaal drempelloos zouden moeten zijn?
De minister heeft in het vorige algemeen overleg een proef met elektronisch stemmen bij de volgende gemeenteraadsverkiezingen toegezegd. Hoe staat het hiermee? In zijn brief van 18 februari 2000 kondigt de minister onderzoek aan naar aanpassing van het GBA en van het kiesrecht. Mevrouw Wagenaar drong erop aan dat de resultaten van deze onderzoeken zo tijdig worden toegestuurd dat de Tweede Kamer nog voor het komende zomerreces het debat erover kan afronden.
Verder vroeg zij de minister nader op de auteursrechtelijke aspecten in te gaan in het licht van de komende auteursrechtrichtlijn en het voorbehoud dat Nederland hierop heeft gemaakt en van de databankrichtlijn, waarin een uitzondering wordt gemaakt voor overheidsinformatie.
In het vorige algemeen overleg heeft de minister toegezegd samen met het ministerie van AZ een notitie te zullen opstellen over nieuwe uitgangspunten van beleid voor overheidscommunicatie in het digitale tijdperk. Mevrouw Wagenaar drong aan op enige spoed hiermee.

Het antwoord van de regering

De **minister** wees op de snelle ICT-ontwikkelingen, zowel in de markt als bij de overheid. In de nieuwe economie die aan het ontstaan is neemt de waarde van een netwerkproduct exponentieel toe met het aantal gebruikers ervan. De overheid moet meedoen met de ontwikkelingen, met ontsluiting van overheidsinformatie en interactieve informatie-uitwisseling. Een bijzondere verantwoordelijkheid heeft de overheid voor de toegankelijkheid door burgers toe te rusten om te kunnen deelnemen aan ICT-ontwikkelingen.
De minister herhaalde zijn toezegging dat in mei 2000 een nieuw beleidsplan over ICT verschijnt. Gezien de snelheid van de ontwikkelingen wilde hij hiermee niet tot het einde van de kabinetsperiode wachten. Het gaat hierbij om het ontwikkelen van strategieën en eerder om herontdekking van werkprocessen dan om automatisering. Omdat organisaties, ook die van de overheid, dit soort ontwikkelingen vaak als bedreigend ervaren, is er extern onderzoek nodig. Hierbij moet onderscheid worden gemaakt tussen service en dienstverlening en tussen het beleidsvormende en het beleidscontrolerende proces. Zeker in de uitvoering zal de overheid hierbij moeten samenwerken met bedrijven en instellingen. Als eerste stap voor een uitvoeringsorganisatie waarnaar de heer Wijn vroeg, zijn inmiddels de verschillende bureaus samengebracht. De minister wilde in het beginstadium invloed op de organisatie kunnen hebben en haar over enige tijd op afstand van de overheid plaatsen, zodat zij gemakkelijker relaties met het bedrijfsleven kan aangaan.
De minister ontkende dat het met OL2000 niet goed loopt. Door de contentregeling, voor het ontwikkelen van inhoudelijke websites groeit het aantal gemeenten met zo'n website van 3% naar 33 %. Het budget is dan ook verhoogd van 3 mln. naar bijna 7 mln. De minister benadrukte dat de websites interactief moeten worden. Van de generieke instrumenten die ontwikkeld worden, noemde hij de digitale catalogus van overheidsproducten, waarvan snelle invoering nu mogelijk is. OL2000 is begonnen met de ministeries van Volkshuisvesting, Ruimtelijke Ordening en Milieubeheer (VROM), van Volksgezondheid, Welzijn en Sport (VWS) en van Economische Zaken, die zich ook gecommitteerd hebben aan vervolgstappen. De minister hield vast aan de voortrekkersrol van deze drie ministeries, maar zei te proberen ook andere ministeries over te halen om mee te doen. Tegelijkertijd met de ontsluiting van de overheidsloketten komen er vragen van gemeenten om verbeteringen. Ook moeten modificaties op lokaal niveau afhankelijk van de behoefte mogelijk zijn. Uiteindelijk gaat het erom dat de burger weet hoe hij dienstverlening van de gemeente kan bereiken en overheidszaken via internet kan afdoen.
De minister benadrukte dat de overheid het belang van de privacy en de veiligheid moet bewaken. De overheid beveiligt zichzelf zeer goed, hoewel er geen volledige garantie is te geven. De website www.overheid.nl is beproefd door een bedreven hacker en bleek zeer goed beveiligd; de site is dan ook nooit gekraakt. Investeringen in de veiligheid van websites zijn ook van belang om het vertrouwen van de burger in de nieuwe economie te behouden.
De website www.rogervanboxtel.nl trekt veel belangstelling: er discussiëren maandelijks 250 mensen met elkaar en op de chatavonden willen er 500 meedoen. Hieruit blijkt een grote behoefte om direct contact met politici te leggen. Niet alleen wordt op deze manier de participatiegraad van burgers vergroot, maar het heeft ook gevolgen voor de ambtelijke organisatie, die intensief voorzien wordt van relevante informatie. De meerwaarde wordt op dit moment geëvalueerd, vooral om na te gaan of verdere bevordering van participatie in het democratische proces mogelijk is. Als minpunt beschouwde de minister het dat de discussie niet op een chatavond kan worden afgerond, maar de deelnemers zien hierin geen reden om ermee op te houden.

De komende Europese top in Lissabon is voor een belangrijk deel gewijd aan de invloed van ICT op het Europese beleid. De minister heeft weten te bereiken dat hierbij aandacht wordt besteed aan informatie van de overheid. De richtlijn over de digitale handtekening, die in Nederland wordt geïmplementeerd, komt overeen met de voornemens van de minister. Wel moet nog goed onderzocht worden voor welke overheidstransacties een digitale handtekening nodig is en voor welke niet. Deze is alleen nodig wanneer de identiteit en de authenticiteit van de burger in het geding zijn. De commissie-Franken zal in mei 2000 rapport uitbrengen aan de minister van Binnenlandse Zaken en Koninkrijksrelaties, onder wiens verantwoordelijkheid de Grondwet valt. De minister zag echter ook een grote betrokkenheid voor hemzelf in verband met de mogelijkheden om internet en multimedia in het democratische proces te gebruiken.
De minister kondigde aan in maart 2000 de officiële aftrap voor de digitale trapveldjes te geven, die overigens al in vele gemeenten worden opgezet. Elke gemeente kan zelf bepalen op welke plaats het digitale trapveldje komt en voor wie het bedoeld is; dit kunnen dus ook ouderen zijn. De gemeente krijgt van de minister een startbedrag, maar moet beheer en exploitatie zelf regelen, zo mogelijk met het bedrijfsleven. Zowel landelijk opererende als lokaal opererende bedrijven blijken hiervoor belangstelling te hebben. De kosten voor de gebruikers zullen zo laag mogelijk moeten zijn om een zo groot mogelijke toegankelijkheid te waarborgen.
SeniorWeb is intensief betrokken bij de ontwikkeling van het concept van het digitale trapveldje. De minister heeft zich ook ingezet voor het behoud van de subsidie van het ministerie van VWS voor SeniorWeb. Naar aanleiding van een vraag van mevrouw Van der Hoeven in het algemeen overleg van 5 oktober 1999 heeft hij de minister van Landbouw, Natuurbeheer en Visserij gevraagd de mogelijkheden voor dit soort centra op het platteland te bekijken. In verband met het huidige budget van 20 mln. wilde de minister de ondersteuning beperken tot de 30 grootste gemeenten.
De minister sprak de hoop uit voor het einde van 2000 de onderhandelingen met Kluwer over de openbaarmaking van wet- en regelgeving af te ronden. Hiervoor en ook voor elektronisch stemmen is nooit geld gereserveerd; dit zal dus nog moeten worden gevonden.
In reactie op een opmerking van de heer Wijn ontkende de minister dat het actieprogramma te ambiteus was, waardoor een deel van het budget voor 1999 niet is gebruikt. Wel leidt vertraging in enkele projecten tot uitgestelde uitgaven. Hij benadrukte dat de lopende projecten zijn voorzien van een planning van uitgaven en een tijdschema. De Staatsalmanak zal vanaf april 2000 op internet verschijnen.
De minister achtte de rapportage over de voortgang met de contentregeling voldoende en wilde op het gebied van rapportage over ICT bij medeoverheden niet zover gaan als de heer Wijn vroeg. Wel hield hij zich aanbevolen voor suggesties voor verbetering of verandering, zoals die in verband met de links tussen Postbus 51 en de website www.overheid.nl.
In 1999 heeft de minister elk ministerie om een vertegenwoordiger in de landelijke rijkscommissie stroomlijning basisgegevens gevraagd en het expertisecentrum gevraagd om begeleiding van het project. In de praktijk bleken de ministeries op grond van eigen overwegingen echter niet actief mee te denken. De minister hoopte zijn collega's te kunnen overtuigen met een rapport van het expertisecentrum dat binnenkort verschijnt en zegde toe in de volgende voortgangsrapportage hierop terug te komen.
De minister had de stichting Internet domeinregistratie Nederland gewezen op de problemen die gemeenten ondervinden bij registratie van de eigen naam. Een aantal namen is verdwenen door herindelingen; de VNG en het ministerie van BZK zijn hierop helaas niet alert geweest. Verder zijn er namen opgekocht door commerciële bedrijven. De minister zegde toe de aandacht van de VNG hiervoor te zullen vragen. Hij wilde zich niet over een definitieve oplossing uitspreken, zo deze al te vinden is.

Namen van overheden veranderen in Nederland voortdurend en hij achtte het de eerste verantwoordelijkheid voor die desbetreffende overheid om actie te ondernemen.
De minister zegde verder toe de voortgangsrapportage meer bottom-up te maken, vanuit het inlevingsvermogen van de burger.
Hij zei er trots op te zijn dat uit een vergelijking van websites van ministeries bleek dat die van het ministerie van BZK het publieksvriendelijkste is.
Hij constateerde dat de website www.rogervanboxtel.nl de enige discussiesite in het openbaar bestuur is en sprak de hoop uit dat dit goede voorbeeld wordt nagevolgd.
De minister herinnerde eraan dat hij in het algemeen overleg van 5 oktober 1999 niet heeft gezegd dat Postbus 51 en de website www.overheid.nl samengevoegd moeten worden, maar wel dat hij zich kon voorstellen dat zij naar elkaar toe zouden groeien. Postbus 51 verschaft informatie aan het publiek, terwijl www.overheid.nl toegang biedt tot een overheidsnetwerk. Na aanvankelijke problemen verlopen de contacten tussen de ministeries van AZ en van BZK hierover goed.
De minister sprak zijn verbazing uit over de hoge internettarieven in sommige bibliotheken en vroeg zich af hoe deze zich verhouden met de bijdrage van het rijk om internettoegang in bibliotheken mogelijk te maken. Deze blijkt overigens in een grote behoefte te voorzien. Hij zegde toe met de bibliotheken te zullen overleggen over meer uniformering van de tarieven.
De minister herhaalde de toezegging dat er bij de gemeenteraadsverkiezingen in 2003 een proef met elektronisch stemmen wordt gehouden. Inmiddels zijn er voorbereidingen in gang gezet om in 2001 een proef op een universiteit te houden. De ervaringen op dit gebied, ook in het buitenland, zijn overigens zeer klein.
De rapporten van de onderzoeken die in de brief van 18 februari 2000 worden genoemd, worden verwacht in juni. De minister wilde de kwaliteit ervan niet in gevaar brengen door te proberen ze eerder te laten verschijnen. Zodra de rapporten er zijn, zullen zij aan de Tweede Kamer worden gestuurd. Een debat erover zou dan uiterlijk direct na het zomerreces mogelijk moeten zijn.
Over de vraag over auteursrechten zegde de minister een schriftelijk antwoord toe.
In de ministerraad is een notitie over overheidsvoorlichting besproken. De minister zei de desbetreffende vraag te zullen doorspelen aan de minister van AZ, die de eerstverantwoordelijke hiervoor is.

Nadere gedachtewisseling

Mevrouw **Augusteijn-Esser** (D66) vond dat Nederland flinke voortgang moet maken met de digitalisering van de economie. Staatssecretaris Vermeend verklaarde in de Volkskrant van 22 februari 2000 dat Nederland op dit punt vooral volgt en niet voorloopt. Zij vroeg zich af of diens voorstel om software fiscaal aftrekbaar te maken de beste stimulans biedt. Wil de minister in de volgende voortgangsrapportage uiteenzetten hoe de problemen met de domeinnamen ontstaan zijn en hoe deze opgelost kunnen worden? Zij herhaalde haar standpunt dat een inhaalslag nodig is en dat hiervoor geld beschikbaar moet komen. Ten slotte vroeg zij de minister in de volgende voortgangsrapportage een duidelijk overzicht van de knelpunten te geven, zodat de Kamer de besluiten kan nemen die nodig zijn om zaken te bespoedigen.

De heer **Wijn** (CDA) bleef op het standpunt staan dat het actieprogramma te ambitieus was. Een aantal plannen is immers vertraagd en de dienstverlening via internet is nog zeer beperkt. Hij ging er echter van uit dat na de millenniumwisseling de aandacht meer hierop gericht zal worden en was blij met de aankondiging van een nieuw plan, waarmee de voortgang

verbeterd kan worden. De heer Wijn kon zich vinden in het antwoord van de minister op zijn vraag om een uitgebreide rapportage. Wel vroeg hij de minister de genoemde monitor de volgende keer aan de Tweede Kamer toe te zenden. Het antwoord van de minister over de standaardisatie stelde de heer Wijn op prijs. Hij zei de oplossing van de minister voor het probleem met de domeinnamen af te wachten.

De heer **Cherribi** (VVD) herhaalde zijn zorgen over de PKI-taskforce. Kan de overheid dit alleen? Wat zijn de kosten? Is het niet de markt die de beste encryptie kan leveren? Bestaat er het risico dat de overheid op dit punt achterblijft? Is er nieuwe wetgeving nodig voor de TTP's? Zo ja, is deze klaar voor 2002? Hij betreurde het verlies van domeinnamen van gemeenten, vooral vanwege de emotionele waarde ervan in verband met de lokale democratie. Voordat de domeinnamen in 2001 geliberaliseerd worden, moet er een lijst met alle gemeente- en plaatsnamen in Nederland komen en moeten deze namen geblokkeerd worden. Wil de minister de gemeenten nog eens hierop attenderen? De heer Cherribi herhaalde zijn vraag over het onderzoek van Tapscott en vroeg ten slotte of het wel mogelijk is diensten met een laag risico vast te stellen in verband met de kleine optie voor 2002.

Mevrouw **Wagenaar** (PvdA) drong bij de minister aan op verschijning van diens nieuwe nota in het voorjaar. Zij wees op de slechte toegankelijkheid en beschikbaarheid van Europese stukken en vroeg de minister op de top in Lissabon te proberen de andere landen op dezelfde lijn te krijgen als Nederland en de Scandinavische landen. Overheidsinformatie moet goed toegankelijk zijn voor het publiek. Op de website van Postbus 51 moet dan ook een telefoonnummer staan en elk ministerie moet per e-mail bereikbaar zijn. Mevrouw Wagenaar meldde dat ook het ministerie van VROM een discussiesite heeft en herhaalde dat de term «discussie gesloten» niet past op internet.
Zij was er verheugd over dat de minister zal proberen de internettarieven van de bibliotheken te uniformeren. Op de bibliotheken zou in ieder geval de overheidsinformatie zo goedkoop mogelijk toegankelijk moeten zijn. Als deze op een cd-rom staat, moet die wel altijd geactualiseerd zijn.

De **minister** nuanceerde de aangehaalde opmerking van staatssecretaris Vermeend. Dat Nederland een volger is in ICT, geldt misschien wel voor de markt, maar internationaal doet Nederland het op overheidsgebied goed. Hij verklaarde hard aan de voortgang van de ontwikkelingen te blijven werken.
De minister zegde toe een brief aan de gemeenten te zullen sturen over de registratie van domeinnamen. Hij wilde echter niet de verantwoordelijkheid van de gemeenten overnemen. Bij herindeling zullen gemeenten zelf actief moeten zijn in het claimen van een eventuele nieuwe domeinnaam. Het millenniumvraagstuk heeft inderdaad veel tijd en energie gekost, vooral in kleine gemeenten. Na de millenniumwisseling is er dus weer veel tijd en energie voor ICT-ontwikkelingen.
Bij de helpdesk wordt bijgehouden hoe het gaat met de gemeentelijke websites. De minister zegde toe deze informatie aan de volgende voortgangsrapportage te zullen toevoegen.
De PKI-taskforce, die in het actieprogramma is aangekondigd, is een initiatief van de overheid, waarin zij op onderdelen samen met het bedrijfsleven nagaat hoe zaken het beste kunnen worden aangepakt. De minister zegde toe rapportages van deze taskforce onmiddellijk aan de Kamer te zullen doorsturen.
De heer Tapscott onderzoekt op grond van uniforme uitgangspunten wat landen aan ICT doen en wat hun vorderingen zijn en betrekt hierbij beleidsinvloeden en demografische ontwikkelingen. De minister zou graag bij de overheid de omschakeling zien net zoals die onder invloed van ICT bij

sommige bedrijven plaatsvindt, maar wees op de complexiteit hiervan gezien de omvang en de verscheidenheid van organisaties van de overheid.
De minister meende dat de conceptrichtlijn over de openbaarmaking van Europese stukken ver achterblijft bij de Nederlandse praktijk. Vanuit Nederland wordt de Europese Commissie dan ook aangesproken op grotere openheid. Verder maakt de Nederlandse europarlementariër Lousewies van der Laan Europese stukken openbaar via haar eigen website.
De website www.overheid.nl wordt voortdurend geactualiseerd. De minister was verheugd over het grote aantal gemeenten dat gebruik maakt van de contentregeling.
Als de onderhandelingen over de openbaarmaking van wet- en regelgeving zijn afgerond, zal de informatie ook aan de bibliotheken ter beschikking worden gesteld. Over de resultaten zal de vaste commissie tijdens een apart overleg met de minister worden geïnformeerd.

De voorzitter van de commissie,
De Cloe

De griffier van de commissie,
Coenen