

Vergaderjaar 2004–2005

26 581

Nationaal TTP-project

Nr. 3

BRIEF VAN DE MINISTER VAN ECONOMISCHE ZAKEN

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 24 juni 2005

Inleiding

Middels deze brief wil ik u informeren over de evaluatie van het TTP-beleid. TTP's («Trusted Third Parties») zijn tussenpersonen die een rol spelen bij beveiligde elektronische communicatie. In dit verband wordt hiermee vooral bedoeld: authenticatie (dus het garanderen dat de afzender van een bericht degene is die hij zegt te zijn). TTP's kunnen o.a. de echtheid van een elektronische handtekening garanderen. Bij de aanbieding van de nota Nationaal TTP beleid, op 3 juni 1999, is de toezegging gedaan dat het beleid binnen twee jaar na de daadwerkelijke start geëvalueerd zou worden.

Het TTP-beleid had tot doel, randvoorwaarden te creëren ten behoeve van elektronische handel. Er werd geconstateerd dat de belangrijkste bottleneck voor elektronische handel *gebrek aan vertrouwen* was (dit is ook nu nog een belangrijke factor). Een betrouwbaar systeem van elektronische handtekeningen zou kunnen helpen om vertrouwen in de identiteit van de handelspartner te creëren. Een goed-ontwikkelde openbare Nederlandse TTP-infrastructuur werd als voorwaarde gezien voor een wijd-verbreed gebruik van elektronische handtekeningen.

Het beleid richtte zich dus op:

- 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 openbare Nederlandse TTP-infrastructuur.

In het voorliggende evaluatierapport¹, afkomstig van de Universiteit van Tilburg, is vastgesteld of het doel (randvoorwaarden voor elektronisch handel) is bereikt en in welke mate dat aan het beleid kan worden gerelateerd.

¹ Ter inzage gelegd bij het Centraal Informatiepunt Tweede Kamer.

Het TTP-beleid

Om elektronische handel (en elektronische overheidsdienstverlening) te bevorderen is in de tweede helft van de jaren negentig het TTP beleid ingezet door de overheid. Het ontbreken van een betrouwbare infrastructuur voor elektronische communicatie werd toen gezien als een belemmering voor de elektronische handel (en later ook voor het elektronisch bestuur). Het beleid beoogde de totstandkoming van een markt voor openbare TTP diensten te stimuleren. Deze diensten kunnen betrekking hebben op het waarborgen van de authenticiteit, integriteit en vertrouwelijkheid van berichten; het beleid legde daarbij de nadruk op de authenticiteitsdiensten (elektronische handtekeningen).

Het beleid bestond aanvankelijk uit het creëren van een vrijwillig *toetsingskader* (het TTP-NL schema) voor de kwaliteit van openbare TTP dienstverlening. Dit toetsingskader, dat volledig aansluit bij de op Europees niveau ontwikkelde specificaties (ETSI criteria), is tot stand gekomen in een nationaal project waaraan overheid en bedrijfsleven deelnamen. In het project werden eisen geformuleerd waaraan TTP-diensten zouden moeten voldoen, en een systeem van «certificerende instellingen» gecreëerd (geen overheidsinstellingen, maar private partijen) die aan TTP-diensten die aan de eisen voldoen, erkenning kunnen geven.

Onder invloed van de uitgebrachte Europese Richtlijn 1999/93/EG van het Europese Parlement en de Raad van 13 december 1999 is het eerder genoemde voorstel van 3 juni 1999 herzien. De Richtlijn beoogde het gebruik van elektronische handtekeningen te stimuleren en stelde dat aan een elektronische handtekening, mits tot stand gekomen volgens een methode die «in de omstandigheden voldoende betrouwbaar is», rechtsgeldigheid niet kan worden ontzegd. Dit kan dus nog voor vele verschillende systemen van elektronische handtekeningen gelden. Daarnaast introduceert de Richtlijn de zgn. «gekwalficeerde» elektronische handtekening, waarbij (in principe) in *alle* omstandigheden een vermoeden van «voldoende betrouwbaarheid» bestaat. Deze «gekwalficeerde» handtekeningen moeten aan een aantal criteria voldoen, die in de Richtlijn omschreven zijn.

De unanieme verwachting van marktpartijen was dat er in de praktijk de meeste vraag zou ontstaan naar de handtekening-systemen van het hoogste, «gekwalficeerde» niveau. De verdere uitwerking van het toetsingskader heeft zich vervolgens uitsluitend op dit hoogste niveau gericht. Dit toetsingskader, gereed gekomen in 2002, kan als de werkelijke start van het TTP-beleid worden beschouwd.

Daarnaast heeft als gevolg van de Richtlijn de overheid zelf (in dit geval de OPTA) een toezichthoudende rol gekregen. Deze rol is vastgelegd in de wet Elektronische Handtekeningen, die op 21 mei 2003 in werking is getreden.

De evaluatie

Het rapport schetst een helder beeld van de fluide achtergrond waartegen het TTP beleid tot stand gekomen is. Het constateert dat de doelstelling van het beleid («betrouwbare communicatie ten behoeve van elektronische handel) *twee maal* versmald is:

- Rond 1999 zag vrijwel iedereen «het gebrek aan vertrouwen in het Internet» als dé grote bottleneck voor de ontwikkeling van elektronische handel. Bijna ongemerkt werd toen aangenomen dat dit vertrouwen zou kunnen worden geschapen door technische

beveiligingsmiddelen. Het probleem van het «vertrouwen» werd versmald tot een *technisch* probleem.

- Na de komst van de Richtlijn werd het beleid nogmaals versmald tot *technische beveiliging van het allerhoogste niveau*.

Het beleid is tot stand gekomen in een periode dat over elektronische handel veel werd geschreven en nagedacht, maar nog niet veel ervaring was opgedaan. Er kwam beleid tot stand waarover het rapport in het algemeen positief oordeelt: het beleid laat de TTP dienstverleners veel ruimte om de randvoorwaarden op een eigen manier in te vullen en hun «maatschappelijke rol» zelf op de door hen verstandig geachte manier vorm te geven. Ook is in flankerend beleid voorzien. Er zijn enkele extra (tijdelijke) stimuleringsmaatregelen door de overheid aangebracht met een «licht» karakter. Zo is er een tweejarige subsidie verstrekt om de toezichtkosten van de OPTA op de TTP's te verlagen, en is er een zgn. restitutieregeling van kracht geweest.

Inmiddels zijn enkele jaren verstreken en kunnen we constateren dat:

- de rol van TTP dienstverleners zich niet zo ontwikkeld heeft als vijf jaar geleden verwacht werd;
- «E-business» als nooit tevoren bloeit (de consument heeft blijkbaar «vertrouwen» gekregen), maar in de praktijk «lagere» vormen van authenticatie¹ gebruikt.

De «gekwalficeerde» elektronische handtekening (conform het «toetsingskader») wordt niet meer gezien als vertrekpunt maar als «plafond». Daardoor heeft de markt voor TTP-diensten op hoog niveau zich ook nog nauwelijks ontwikkeld. Er zijn nog maar enkele aanbieders die gecertificeerd zijn volgens het «toetsingskader». De markt groeit wel, maar in een langzaam tempo en niet «stormachtig» zoals oorspronkelijk verwacht was. Voor de nabije toekomst wordt groei voorzien wegens het gebruik van gekwalficeerde handtekeningen in de zorg, voor het ondertekenen van elektronische recepten en diagnoses.

Actuele ontwikkelingen

In het beleid rond de Elektronische Overheid staan vier actielijnen centraal²:

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

In het kader van de eerste actielijn worden er voorzieningen getroffen voor een veilig elektronisch verkeer tussen overheid en burgers of bedrijven. Belangrijk is dat zekerheid bestaat over de identiteit van degene aan wie elektronische diensten worden verleend. Om dat mogelijk te maken zal nog in 2004 een authenticatievoorziening worden ingericht, die overheidsbreed ter beschikking zal komen. Het gaat hierbij om realisatie van een centrale authenticatievoorziening voor de overheid (DigID), die waar mogelijk zal worden gecombineerd met de Overheidstransactiepoort (OTP). DigID is een eerste aanzet tot een volwaardige infrastructuur voor elektronische beveiliging en identificatie op verschillende niveaus («hoog», «middel», en «laag»). Ook is er het streven om in deze kabinetsperiode een elektronische identiteitskaart te introduceren.

¹ In de overheidssfeer is er het voorbeeld van de Belastingdienst, die al jaren een vijfcijferige pincode gebruikt als «handtekening» onder het aangiftebiljet Inkomstenbelasting.

² Kamerstukken II, 2003–2004, 29 362, nr. 1.

Hier liggen kansen om de elektronische handtekening op een relatief eenvoudige wijze voor een breed publiek beschikbaar te krijgen. De toepassingen en de daarvoor benodigde infrastructuur zullen dan volgen.

Hoe verder?

Het TTP-beleid is geslaagd, in de zin dat een toetsingskader (gebaseerd op internationale standaarden) met een daarop gebaseerd certificatiemechanisme, en een toezichtmechanisme, inderdaad tot stand gekomen is. De Nederlandse uitwerking van het toetsingskader voor TTP's heeft ook in andere Europese landen aandacht gekregen. Recent is bekend geworden dat de in Nederland ontwikkelde aanvullingen en interpretaties («guidance» documenten) nu worden geïncorporeerd in de volgende versie van de Europese criteria, die eind 2004 beschikbaar zal komen.

Aan de andere kant wordt er van het toetsingskader nog weinig gebruik gemaakt (twee certificerende instellingen, en nog maar enkele gecertificeerde TTP's). Het rapport noemt drie mogelijkheden voor het toekomstige TTP-beleid: «stoppen», «voortzetten», en «verbreden». Hieronder beargumenteer ik dat op dit moment de beste keuze is: voortzetten, de daadwerkelijke ontwikkeling van de markt goed volgen, en een optie openhouden voor verbreding. Ik licht dit nader toe.

Voortzetting van het huidige beleid betekent in de praktijk: pas op de plaats, omdat de rol van de overheid, nu het institutioneel kader gereed is, zeer gering is. Hier is nauwelijks geld of inspanning mee gemoeid. Het is de moeite waard het kader in stand te houden; weliswaar wordt er op dit moment weinig gebruik van gemaakt, maar dit kan in de toekomst veranderen, als de behoefte aan «zwaardere» vormen van elektronische handtekening groeit. Dit laatste is wel te verwachten (beveiligingseisen nemen in het algemeen toe) maar wanneer dit zal gebeuren is nog onduidelijk.

Op twee manieren is een *verbreding* mogelijk: verbreding van de TTP-diensten die onder het beleid vallen (naast elektronische handtekening ook andere diensten met betrekking tot authenticiteit, integriteit en vertrouwelijkheid van het berichtenverkeer) en/of verbreding van het betrouwbaarheidsniveau (dus ook standaardisatie van lagere niveaus). In beide gevallen betekent dit voor het beleid dat het huidige certificatieschema wordt uitgebreid, of dat gewerkt wordt aan een of meer nieuwe schema's voor certificering. Of we hiertoe moeten overgaan is nu nog niet duidelijk. Wel heeft de stichting ECP-NL inmiddels, in samenwerking met gebruikers en aanbieders van authenticatie-systemen, een classificatie gemaakt (het «e-OK» raamwerk) waarin de betrouwbaarheidsniveaus «laag», «middel», en «hoog» precies omschreven worden; deze actie heb ik gesteund.

Stoppen met het TTP-beleid (de derde mogelijkheid die in het evaluatierapport wordt genoemd) is geen optie omdat er invulling gegeven moet worden aan de eerder genoemde Europese Richtlijn uit 1999.

De evaluatie leert ons (nogmaals) dat het erg moeilijk is om (markt-)ontwikkelingen in de informatiemaatschappij tevoren te voorspellen. Het blijft van groot belang om de daadwerkelijke ontwikkelingen (aan aanbod- en vraagzijde) op de voet te volgen en beleid waar nodig aan te passen.

Ik heb derhalve besloten door te gaan met het huidige TTP beleid, en met het stimuleren van het gebruik van de elektronische handtekening. Het beleid ten aanzien van de «elektronische overheid», en de inrichting van een centrale toegangsvoorziening die ook met «lagere» vormen van authenticatie zal kunnen werken, zal daarnaast worden voortgezet. Ik zal onderzoeken of een verbreding van beleid (o.a. certificatie van «lagere» vormen van elektronische handtekening) ook daadwerkelijk voorziet in

een behoefte van de markt. Zodra ik nadere plannen heb uitgewerkt zal ik u hiervan op de hoogte stellen.

Financiële aspecten

Voor het jaar 2005 heb ik besloten de tarieven die OPTA aan TTP's berekent voor het financieren van het toezicht te verlagen, omdat hantering van het beginsel van «kostendekkende tarieven» in de praktijk tot erg hoge tarieven leidt bij de huidige geringe omvang van de markt. Ook het evaluatierapport constateert dat dit tot instapbarrières kan leiden. Ik verwacht dus dat verlaging van het tarief de groei van de TTP-markt zal stimuleren. Een eventuele extra financieringsbehoefte voor OPTA (in de orde van grootte van € 100 000) zal bekostigd kunnen worden uit de reguliere begroting.

De Minister van Economische Zaken,
L. J. Brinkhorst

OP WEG NAAR DE ELEKTRONISCHE OVERHEID

Basisvoorzieningen

Hoofdstuk 1: Inleiding

Zoals is aangegeven in het Programma Andere Overheid en in de rijksbrede ICT-beleidsagenda wil het Kabinet van de mogelijkheden die door de toepassing van ICT geboden worden gebruik maken om de dienstverlening aan burgers en bedrijven te verbeteren. Daarbij zijn onder andere de volgende speerpunten geformuleerd:

- burgers en bedrijven hoeven bepaalde gegevens nog maar één keer aan te leveren bij de overheid
- er komt een elektronisch systeem waarmee burgers en bedrijven zich éénduidig bekend kunnen maken bij de overheid
- voor haar communicatie, zowel intern als met de buitenwereld, gaat de overheid open standaarden gebruiken, waardoor de leveranciersafhankelijkheid wordt vergroot
- het streven dat in 2007 65% van de publieke dienstverlening van rijk, provincies en gemeenten plaats kan vinden via het internet.

Goed gebruik van nieuwe technologieën¹ biedt evenzeer kansen voor verbetering van handhaving van de regelgeving als voor een (aanmerkelijk) efficiëntere overheid. Het versterkt de concurrentiepositie van ons land en geeft mede invulling aan de ambitieuze doelen die het kabinet zich heeft gesteld in het kader van de Lissabon-agenda van de EU. Internet en daarmee verbonden technologie bieden ook nieuwe mogelijkheden om individuele en georganiseerde burgers, bedrijven en andere maatschappelijke instellingen in staat te stellen hun eigen verantwoordelijkheid te nemen. Het opent nieuwe wegen voor openbaarheid, transparantie, responsiviteit en het afleggen van verantwoording door de overheid.

Een ander zwaarwegend issue is de vermindering van administratieve lasten voor burgers en bedrijven. Inzet van ICT biedt een uitgelezen kans om de informatieverplichtingen te vereenvoudigen. Daaruit kunnen interessante voordelen voortvloeien.

Het gebruik van informatie- en communicatietechnologie voor deze doeleinden wordt veelal aangeduid met de term e-Government of "De elektronische overheid".

Het tij is gunstig voor de elektronische overheid. Er zijn sterke politieke impulsen met het programma Andere Overheid, de Administratieve Lastenoperaties voor burgers en bedrijven en de ICT-beleidsagenda. Er is een sterke bereidheid en noodzaak tot samenwerking bij de in

¹ Zowel tussen overheidsorganisaties onderling zowel als tussen overheid en burgers en bedrijven.

dit verband belangrijkste uitvoerende diensten. En er zijn op deelterreinen al veel nuttige programma's in voorbereiding of in uitvoering.

Voor de realisatie van de elektronische overheid is een goed geregisseerd gebruik van ICT noodzakelijk; technisch zijn daarvoor geen belemmeringen.

De regie/sturing kent twee kanten:

- A Het aanbod van ICT-basisvoorzieningen als basisregistraties, identificerende nummers, authenticatievoorzieningen, standaarden voor gegevenstransport en dergelijke.
- B Het ontwikkelen van het gebruik van de basisvoorzieningen voor nieuwe/ betere manieren van dienstverlening, handhaving en maatschappelijke participatie.

Ad A

De basisvoorzieningen kunnen centraal worden ontwikkeld en het gebruik daarvan kan en moet na de initiatieffase snel (en in sommige gevallen dwingend) worden bevorderd. Wat het gebruik betreft zal daartoe het uitgangspunt worden gehanteerd van 'ja, tenzij' (omgekeerde bewijslast).

Om de basisvoorzieningen te realiseren moet samenhang worden aangebracht tussen reeds lopende activiteiten, en moet gemeenschappelijke beheer worden georganiseerd. Daarbij is het nodig om tot afspraken te komen voor verantwoordelijkheden over opdrachtgeverschap, beheer en exploitatie en over houderschap van administraties.

Een samenhangend programma, is nodig om de volgende redenen:

- Zolang afzonderlijke overheidsonderdelen bij de inzet van ICT in relatief isolement hun eigen weg gaan, blijven ontwikkelingen die voor burgers en bedrijven én voor de overheid zelf echt zoden aan de dijk zetten buiten bereik. De initiatieven die er al zijn, bij met name de uitvoerende diensten van de rijksoverheid en bij de gemeenten, gaan wel dezelfde richting uit, maar kiezen niet allemaal voor precies dezelfde oplossing. Dat is niet handig en ook niet nodig. Geen enkel project is echter al zodanig ontwikkeld dat bundeling van krachten uitgesloten is.
- De Tweede Kamer heeft te kennen gegeven dat gestreefd moet worden naar algemeen verbindende afspraken met betrekking tot onder meer de basisregistraties, het burgerservicenummer en de elektronische identificatie².
- Gezamenlijke ontwikkeling heeft onmiskenbaar kostenvoordelen en imagovoordelen (één overheid), en zij maakt een betere dienstverlening en handhaving mogelijk. De Tweede Kamer heeft invoering van het principe van éénmalige gegevensverstrekking gevraagd³ voor de realisatie waarvan de invoering van gezamenlijke voorzieningen noodzakelijk is.
- Verder kan door de inzet van ICT een aanzienlijke bijdrage geleverd worden aan de vermindering van administratieve lasten voor burgers en bedrijven. Om deze

² motie van der Ham en Szabo, Kamerstukken II, 29 362, nr.4.

³ motie Szabo c.s., Kamerstukken II, 29 362, nr. 8.

vermindering te realiseren is het wel noodzakelijk dat gebruik wordt gemaakt van de gezamenlijk ontwikkelde voorzieningen. Om dit te bewerkstelligen, zal de vermindering van administratieve lasten bij de uitwerking in de afzonderlijke projecten zo concreet mogelijk worden aangegeven en zal deze uitwerking zo nodig worden bespoedigd teneinde tijdig zicht te krijgen op de bijdrage aan de realisering van de kabinetsdoelstelling van een kwart reductie aan administratieve lasten.

Ad B

De ontwikkeling van de diensten e.d. vergt een heel ander sturingsaanpak. Uiteindelijk zijn het de vele honderden overheidsorganisaties, met ieder hun eigen verbindingen met burgers en bedrijven, die dat zelf moeten verzorgen. Een 'slimme' sturing daarvan dwingt niet maar verleidt, zorgt voor convergentie in de activiteiten, en biedt best practices en innoverende oplossingen aan.

Een dergelijke wijze van sturing is nodig door de grote verschillen in organisaties waar het hier om gaat: van de kleinste gemeente tot het grootste departement, ieder met hun eigen tempo van ontwikkeling en hun eigen mogelijkheden. Maar het is ook nodig vanwege de grote variatie aan activiteiten. Ook hier kan door invulling van de doelstelling van reductie van de administratieve lasten het nodige worden bereikt; de in Europees verband gemaakte opsomming van 20 openbare diensten (12 voor burgers en 8 voor bedrijven), waar overheden het leven een stuk makkelijker kunnen maken door het gebruik van nieuwe technologie, maakt dat snel duidelijk (zie bijlage 1).

Hoofdstuk 2: Een samenhangend programma

De inspanningen om de ICT-voorzieningen ten behoeve van de elektronische overheid te realiseren, worden verricht in zeven domeinen, die bij elkaar het model vormen van de openbare elektronische 'informatie-infrastructuur':

- A. elektronische toegang tot de overheid
- B. elektronische authenticatie
- C. éénduidige nummers voor personen en voor bedrijven
- D. basisregisters
- E. elektronische identificeringsmiddelen (chipcards)
- F. elektronische informatie-uitwisseling
- G. snelle verbindingen tussen overheidsorganisaties

Per domein worden voorzieningen ontwikkeld, vaak in meerjarige trajecten, soms ook in een domeinoverstijgende programmatische samenhang (het ICTAL programma bijvoorbeeld is gericht op voorzieningen in de keten bedrijfsleven-overheid, en combineert activiteiten uit alle onderscheiden domeinen). In dit hoofdstuk worden per domein de activiteiten beschreven, wordt waar nodig de samenhang geschetst, en worden verantwoordelijkheden aangegeven waar nodig.

2.1 Domein A: elektronische toegang tot de overheid

De elektronische overheid begint bij het elektronisch beschikbaar stellen van informatie over documenten, diensten en producten van de overheid. Daartoe is al veel gedaan en gerealiseerd: via talloze websites is informatie toegankelijk gemaakt, van onze Tweede Kamer tot onze kleinste gemeente. In het kader van het 12-punten plan van de Secretarissen-Generaal, dat is opgenomen in het Programma Ander Overheid, worden daartoe verdergaande activiteiten ontwikkeld bij de Rijksoverheid. Voorts zijn op basis van de Kabinetsreactie op het rapport 'In dienst van de democratie' van de tijdelijke commissie Toekomst Overheidscommunicatie⁴ (commissie Wallage) diverse activiteiten in gang gezet.

Iedere overheidsorganisatie of onderdeel daarvan, is zelf verantwoordelijk voor haar eigen elektronische loket. Wil de gemiddelde Nederlander of een bedrijf door de bomen het bos kunnen blijven zien, dan is verdere ontsluiting noodzakelijk: iemand moet in enkele 'muis-kliks' bij de gevraagde informatie kunnen komen. Het perspectief is een overheid die actief en gericht informatie kan verstrekken aan burgers en bedrijven, en de mogelijkheden kan benutten van interactieve beleidsvorming. Dat vraagt de systematische ontsluiting van de overheidsinformatie en van door de overheid geboden diensten. Door het 'elektronisch koppelen' van het informatie- en dienstenaanbod, kan het ene virtuele overheidsloket worden

gerealiseerd, zonder dat daar direct een reorganisatie van de achterliggende administraties bij aan de orde is.

In dit domein lopen er reeds diverse (samenwerkings-)trajecten. In bijlage 2 wordt een aantal van deze trajecten met naam genoemd.

2.2 Domein B: Elektronische authenticatie

Een van de doelen bij de elektronische overheid is dat transacties elektronisch kunnen worden afgehandeld, in plaats van met papier en aan het fysieke loket. Dit gebeurt al in de bankwereld (voorbeelden: elektronisch bankieren, de betaalautomaat) en in vele vormen van commerciële dienstverlening (voorbeelden te over: amazon.com, wehkamp.nl, bol.com, ebay, etcetera). Bij elektronische afhandeling:

- moeten burgers en bedrijven de zekerheid hebben dat hun gegevens uitsluitend daar terecht komen waar ze horen, alsmede dat de een niet de identiteit kan aannemen van een ander,
- verlangen burgers en bedrijven logischerwijze dat zij *op een en dezelfde manier* toegang kunnen krijgen tot welke overheidsorganisatie dan ook (en dus niet voor elke overheidsdienst een aparte (pin)code moeten onthouden),
- verlangen burgers en bedrijven van een moderne overheid dat die de informatie die zij al heeft, hergebruikt (éénmalige gegevensverstrekking),
- verlangt de overheid uit een oogpunt van handhaving dat de gegevens over de burger of het bedrijf éénduidig zijn.

Bovenstaande punten komen in de volgende domeinen aan de orde. Eerst wordt nu ingegaan op de authenticatie.

Elektronische authenticatie is het elektronisch vaststellen dat een bepaalde identiteit terecht geclaimd wordt. Dit kan bijvoorbeeld door gebruik te maken van een pincode of van een digitale handtekening. In Nederland zijn al vormen van authenticatie bij banken (digitaal bankieren), politie (digitaal aangifte doen), Belastingdienst (digitaal belastingaangifte doen), Kamers van Koophandel, een aantal gemeenten en een aantal ZBO's. Ieder voor zich heeft een eigen voorziening en een eigen beheerorganisatie.

De OTV (Overheidstoegangsvoorziening) is een programma dat het mogelijk maakt dat overheden die hun diensten *online* aanbieden, zich niet hoeven te bekreunen om het beheer van een authenticatievoorziening.

Met de OTV, waarvan een eerste versie in 2004 operationeel zal zijn, wordt beoogd de aanbieders van authenticatiediensten, de afnemers van overheidsdiensten (burgers/bedrijven) en de overheidsdiensten zelf bij elkaar te brengen. Zoals nu voorzien, accepteert de OTV dat er verschillende authenticatiemiddelen en -leveranciers zijn, zoals bijvoorbeeld de middelen van de banken voor digitaal bankieren, een simpele code

⁴ Tweede Kamer, vergaderjaar 2001-2002, 26 387, nr 12

(vergelijkbaar met de pincode van de Belastingdienst) als middel voor transacties met een laag risico, en het middel software certificaat van bijvoorbeeld de Kamers van Koophandel. Via de OTV zullen burgers en bedrijven niet alleen transacties kunnen verrichten met de overheid, maar wordt ook een belangrijke voorwaarde vervuld voor het door de burger of het bedrijf geautoriseerd hergebruik van gegevens die de overheid al over hun heeft. Daarnaast zullen burgers en bedrijven ook kunnen "zien" wat overheidsinstanties aan gegevens over hen hebben. Aldus wordt handen en voeten gegeven aan hun inzage- en correctierecht.

De Tweede Kamer heeft recent aangegeven naar één authenticatievoorziening te willen voor overheidsdiensten. Dat lijkt ook de goede weg te zijn, willen we de burgers/bedrijven niet opzadelen met een forse digitale sleutelbos: door middel van één voorziening kan immers (breed) hergebruik van (ook reeds bestaande) sleutels plaatsvinden. Bovendien hebben de overheidsorganisaties ieder voor zich te weinig transacties om de investering in een eigen transactievoorziening te rechtvaardigen. Deze lijn betekent dat het aantal sleutels dat één persoon dient te bezitten aanmerkelijk wordt teruggebracht, en dat een aantal overheidsorganisaties afscheid moet nemen van de "eigen" voorziening en dus transitiekosten moet maken.

In de authenticatievoorziening zullen niet meer dan drie veiligheidsniveau's worden onderscheiden:

- hoog veiligheidsniveau: daaraan voldoet de PKI-standaard⁵ (hetgeen de elektronische handtekening op het niveau van de Wet Elektronisch Bestuurlijk Verkeer mogelijk maakt)
- midden veiligheidsniveau: daaraan voldoen op dit moment de huidige middelen voor internetbankieren en mogelijk softwarecertificaten (zoals die welke de Kamers van Koophandel willen introduceren);
- basis veiligheidsniveau: identificatienummer/wachtwoord zoals bij de Belastingdienst wordt gebruikt.

De mate van veiligheid van een authenticatiemiddel hangt in het algemeen niet alleen af van het middel zelf, maar ook van de wijze waarop het wordt uitgegeven (bijvoorbeeld per post toegestuurd dan wel bij een loket afgehaald) en beheerd. Grotere zorgvuldigheid bij het uitgifteproces kan een authenticatiemiddel naar een hoger niveau brengen (bijvoorbeeld de internet-bankiermiddelen naar 'hoog', of nummer/wachtwoord naar 'midden') – ten koste, wellicht, van grotere complexiteit⁶

Het is niet opportuun in één keer snel de drie veiligheidsniveau's) binnen die éne authenticatievoorziening in te vullen.

⁵ PKI = Public Key Infrastructure

⁶ In het door EZ gestimuleerde 'e-OK' project overleggen vertegenwoordigers van overheid en bedrijfsleven over een classificatieschema dat de veiligheidsniveaus van diverse authenticatiemiddelen beschrijft en in kaart brengt.

Wij willen nu een lijn aangeven voor de laatste twee niveaus. Voor het basisveiligheidsniveau wordt voor iedere overheidsorganisatie de *username/password*-combinatie de standaard. Voor het midden niveau bezien we of de softwarecertificaten als standaard bruikbaar zijn. De praktische modaliteiten worden nu snel uitgezocht. Voor dit beveiligingsniveau zouden wellicht ook de middelen voor internetbankieren gebruikt kunnen worden onder de voorwaarde dat alle banken kunnen meedoen⁷.

De OTV is er voor alle overheidsorganisaties. Het ligt daarom voor de hand deze voorziening onder gemeenschappelijke aansturing te ontwikkelen, beheren en exploiteren, onder politieke eindverantwoordelijkheid van de ministers voor BVK en van EZ. De voorziening zelf kan daarbij door de markt worden geleverd: kennis van de ondersteunende processen voor elektronische berichtendiensten wordt sneller in de markt opgebouwd dan binnen de overheid. Daarbij gaat het met name om technologische ontwikkelingen.

2.3 Domein C: éénduidige nummers voor personen en bedrijven

Éénduidige opslag van gegevens vereist het toekennen van een uniek nummer. Een identificatienummer heeft in beginsel uitsluitend een administratieve functie ten behoeve van het voeren van massale administraties. Ook is het nummer noodzakelijk voor geautomatiseerde gegevensuitwisseling. Een identificatienummer op zichzelf heeft geen enkele andere waarde. Het heeft wel waarde in digitale authenticatievoorzieningen: samen met wachtwoorden, certificaten e.d. wordt het risico beperkt dat de een zich voor de ander uitgeeft.

- We willen de 'nummerproblematiek' nu definitief ordelijk te regelen. Uit een oogpunt van privacy is één transparant, goed geprotocolleerd en beheersbaar stelsel van nummers te prefereren boven een stelsel van al dan niet georganiseerde wanorde.
- Nu er een helder rapport ligt over een Burger Service Nummer⁸, er de verplichting is van de EU met betrekking tot facturen/nummers, is dat ook gemakkelijk mogelijk. In feite zou het daarbij om twee typen nummers gaan: het Burger Service Nummer en het Bedrijfservice Nummer.

Het Burger Service Nummer (BSN)

Het Burger Service Nummer wordt uitgegeven door gemeenten. Basis voor het BSN is het sofi-nummer, dat hebben alle Nederlandse burgers immers al.

Een BSN wordt verstrekt aan een persoon, als die persoon:

- goed te identificeren is
- een relatie heeft met de Nederlandse overheid.

Het BSN is op zich betekenisloos; het krijgt pas betekenis als het in een sector wordt

⁷ In feite zijn de banken met hun voorziening nu de belangrijkste aanbieder van dit niveau. Het is goed ons te realiseren dat de banken al zo'n 4,5 miljoen e-bankierders kennen en een aantal overheidsafnemers als universiteiten, hogescholen, bibliotheken en een te starten pilot bij LNV.

⁸ Inmiddels is een brief aan de Tweede Kamer gestuurd over BSN (nummer TK, 29 362, nr. 15).

gebruikt, *volgens de regels die de betreffende sector voor het gebruik er van stelt (normaal gesproken door wetgeving)*. Zo is het BSN in de sociale en fiscale sector te gebruiken als SoFi-nummer, in de zorgsector als Zorg Identificatie Nummer (ZIN), in de onderwijssector als Onderwijsnummer (ON) en in de vreemdelingensector als Vreemdelingsnummer. De genoemde nummers kunnen simpelweg gerekend worden tot een juridisch goed gedefinieerde en beheerste verschijningsvorm van het Burger Service Nummer. Daarbij ligt de verantwoordelijkheid voor *het gebruik* van de nummers in de verschillende publieke domeinen (sofi, veiligheid, zorg, rechtspraak, onderwijs e.d.) bij de verantwoordelijke ministers.

Introductie van het Burger Service Nummer impliceert dat de *uitgifte* van nummers verhuist van de Belastingdienst naar de gemeenten. De politieke verantwoordelijkheid voor de uitgifte van het BSN komt te liggen bij de minister voor BVK (voor het gebruik van het nummer zijn de diverse ministers verantwoordelijk). Een speciale verantwoordelijkheid is weggelegd voor de minister van V&I voor de uitgifte van het BSN aan bepaalde categorieën niet-ingezetenen. Bij het beheer van het nummer door de minister voor BVK zullen de gebruikers en de gemeenten goed moeten worden betrokken.

Het Bedrijfsservice Nummer (BN)

In het informatieverkeer tussen overheid en bedrijfsleven kan het Bedrijfsservice nummer een overeenkomstige functie vervullen als het BSN in het burgerdomein. Voor het BN kan mogelijk aansluiting worden gezocht bij het KvK-nummer of het BTW-nummer. Bedrijven hebben, indien zij belaste producten/diensten leveren, een omzetbelastingnummer nodig (EU-richtlijn factuurverplichting). Het merendeel van de bedrijven/ondernemers is overigens BTW-plichtig. Bij éénmanszaken is het BTW-nummer gekoppeld aan het SoFi-nummer. Voor bedrijven die vrijgesteld zijn van de BTW, kan een fictief nummer worden afgegeven. Zo zou het BTW-nummer gebruikt kunnen worden als Bedrijfsservice nummer. Er zijn ook andere opties.

De politieke verantwoordelijkheid voor het beheer van het BN ligt bij de minister van EZ. Indien het beheer van de basisadministratie bedrijven/ondernemers en het Bedrijvenloket bij de Kamers van Koophandel wordt belegd, ligt het voor de hand daar ook het beheer van een BN te plaatsen. De uitgifte van een BN verloopt via het Bedrijvenloket. Dat op deze wijze alles in een hand komt, heeft ook voordelen voor die publieke domeinen die een nummer voor bedrijven/ondernemers nodig achten. Weer als voorbeeld: het zorgnummer voor zorginstellingen zou dan het Bedrijfsservice Nummer kunnen zijn. Ook hier geldt dan dat de betrokken ministers verantwoordelijk zijn voor het gebruik van dat nummer. De aanpak van een BN wordt in een nieuw programma onderzocht onder verantwoordelijkheid van de minister van EZ

2.4 Domein D: basisregisters

Eenduidige opslag en beheer van gegevens vindt plaats in de zogenoemde basisregisters. Basisregisters zijn de spil in de gegevensuitwisseling over burgers en bedrijven. Bij de basisregisters zit de sleutel tot het bereiken van gegevenshergebruik en eenmalige uitvraag van gegevens. Een basisregistratie bevat per definitie gegevens die ook voor de werkzaamheden van andere overheidsorganisaties noodzakelijk zijn. Een basisregistratie dient aan onder andere de volgende vereisten te voldoen:

- zij fungeert overheidsbreed als unieke bron van bepaalde gegevens
- de gegevens zijn éénduidig gedefinieerd
- de registratie heeft één beheerder (lokaal of landelijk)
- de privacy-aspecten van de registratie zijn adequaat geregeld
- bepaalde (overheids-)gebruikers van de gegevens uit de basisregistratie hebben een terugmeldplicht (het doorgeven van mogelijke wijzigingen van gegevens aan de beheerder van de basisregistratie); op deze wijze wordt in de loop van een periode een kwalitatief hoogstaande gegevensverzameling gerealiseerd.

Het gebruik maken van basisregistraties betekent in het algemeen een voordeel voor die organisaties die hun eigen administratie niet meer hoeven te handhaven, maar de gegevens (uiteraard geautomatiseerd) krijgen aangeleverd vanuit de basisregistratie. Daartegenover staat dat de beheerder van de basisregistratie soms aanvullende investeringen moet doen om zijn basisregistratie te laten voldoen aan de vereisten. Ten aanzien van de *basisregisters* staat het *verplicht* gebruik van de gegevens door alle overheidsorganisaties voorop. Bij de invoeringstermijn zal rekening worden gehouden met het normale investeringsritme van vernieuwing van de geautomatiseerde systemen, zodat geen onnodige kosten ontstaan.

In bijlage 3 is een opsomming gegeven van diverse basisregisters, met vermelding van de verantwoordelijke minister, en de stand van zaken van realisatie. Sommige basisregisters vereisen een wettelijke grondslag (de zgn. authentieke basisregisters, waarvan er 6 zijn aangewezen), met name in geval er sprake is van een taakverdeling tussen verschillende overheidslagen.

Voor het stelsel van basisregisters is de minister voor BVK verantwoordelijk. Voor de noodzakelijke activiteiten rond de basisregisters zet het ministerie van BZK het programma Stroomlijning Basisgegevens voort. Daarbij zal onder andere, op verzoek van de Tweede Kamer, worden gezien welke regelgeving noodzakelijk is ter ondersteuning van de invoering en werking van de basisregisters. Ook zal de inhoudelijke afstemming tussen de diverse basisregisters punt van aandacht zijn, zowel als de wijze van financiering, het verplicht gebruik, de uitwisselingsinfrastructuur en de visie op welke registraties onderdeel uitmaken van het stelsel en welke niet.

Voor de gegevenshuishouding van de overheid is tevens van belang dat de meta-informatie (informatie over de informatie) goed is gestructureerd. Daarom wordt, aanvullend op en in

relatie met de basisregisters, gewerkt aan het opzetten van een gegevenswoordenboek, aan gegevens- en begrippenharmonisatie en aan het opzetten van elektronische verwijzindexen.

2.5 Domein E: elektronische identificeringsmiddelen (chipcards)

Het doel van het gebruik van deze middelen is eenduidige identificatie van burgers⁹. Dit instrumentarium omvat op dit moment een paspoort of identiteitskaart (NIK) voor alle ingeschrevenen in de GBA, een SoFi-kaart voor EU/EER-ingezetenen en een vreemdelingenkaart voor niet-ingezetenen. Deze kaarten zijn voorzien van een uniek nummer. Naast deze kaarten bestaan op dit moment andere documenten die als identiteitsdocument worden geaccepteerd (bijvoorbeeld het rijbewijs).

Invoering van een chipcard (of het toevoegen van een chip aan de bestaande identiteitsbewijzen) creëert de mogelijkheid elektronisch leesbare informatie op de kaart op te nemen. Gedacht kan dan worden aan het aangekondigde nieuwe Burger Service Nummer en, op termijn, van biometrische kenmerken van de kaarthouder. Met een dergelijke chipcard kan een scala van elektronisch af te handelen publieke diensten worden ontsloten, waarvoor unieke authenticatie met een elektronisch identiteitsmiddel met een hoog betrouwbaarheidsniveau is vereist. Bovendien kan een veel effectievere fraudebestrijding worden bereikt.

Invoering van een chipcard betekent overigens niet dat zo'n elektronische kaart ook direct massaal kan worden gebruikt. Daarvoor moet een infrastructuur worden ontwikkeld: de chip moet kunnen worden gelezen, en de systemen achter de leesapparatuur moeten de op de chip opgeslagen informatie kunnen verwerken. Dit vraagt aanzienlijke aanpassingen in de werkprocessen en de systemen van organisaties.

Waar de banken al ruim gebruik maken van een dergelijke infrastructuur (denk aan de betaalautomaat, die van een magneetstrip gebruik maakt), waarbij de te gebruiken technieken ook internationaal zijn gestandaardiseerd, ligt het voor de hand te bezien of niet moet worden aangesloten bij de technische standaards die ook door de banken worden gehanteerd (wellicht op termijn de EMV-chip¹⁰ in plaats van de huidige chip of magneetstrip).

Invoering vraagt om een stevige regie en een goed scenario. Het zou geldverspilling zijn om verschillende elektronische identiteitsbewijzen te ontwikkelen. Gegeven de noodzakelijke standaardisatie in de investeringen zou met één chipcard per burger moeten worden

⁹ Eénduidige identificatie is altijd een middel. In het navolgende wordt alleen ingegaan op de mogelijkheden van het gebruik van chipcards voor identificatie, en niet op het doel daarvan (het beleid ten aanzien van identificatie).

¹⁰ EMV is een acroniem voor Europay, MasterCard en Visa en betreft de standaard die deze organisaties zijn overeengekomen voor interactie tussen chipcard en terminal. Deze standaard is inmiddels wereldwijd geaccepteerd.

volstaan, zoals in februari 2004 door een meerderheid van de Tweede Kamer bij motie per uiterlijk 1 januari 2007 ook is gevraagd¹¹.

Daarbij is van belang ook hier voor de invoering niet alles tegelijk te willen. Gestart zou kunnen worden met een chip op de al bestaande Nederlandse Identiteitskaart (eNIK, de elektronische Nederlandse identiteitskaart), met op de chip de informatie die nu op de MRZ (machine readable zone) van de reisdocumenten staat vermeld (waaronder het SoFi-nummer, straks BSN).

De huidige Nederlandse identiteitskaart is tevens te gebruiken als reisdocument. Het ligt ook voor de hand deze relatie te behouden, en de eNIK te laten ontwikkelen, invoeren en beheren door de minister voor BVK.

2.6 Domein F: elektronische informatie-uitwisseling

Bij de uitwisseling van gegevens spelen verschillende vraagstukken.

Zo moet worden voorzien in het gebruik van open standaarden voor elektronische gegevensuitwisseling tussen overheid en burgers en bedrijven, alsook tussen overheidsinstellingen onderling. Gezien het belang van open standaarden neemt de Nederlandse overheid een actieve rol in bij het toepassen daarvan. Daarnaast volgt de Nederlandse overheid nauwgezet de ontwikkelingen rondom open standaarden in Europees verband.

Verder is gegevensharmonisatie nodig: daartoe worden in het vervolg op het programma Stroomlijning Basisgegevens activiteiten ontplooid.

Ook het gegevensverkeer moet worden geregeld. Het gaat hier in eerste instantie vooral over het berichtenverkeer van bedrijven naar de overheid. Het model dat daarvoor is gekozen is de Overheids Transactie Poort (OTP), dat in het kader van het EZ-programma ICT & Administratieve Lasten is ontwikkeld. De ontwikkeling van de OTP – een initiatief van EZ, SZW, LNV en Financiën – is inmiddels zover, dat besluiten voor de deur staan over het beheer. De verschillende opties daarvoor worden op dit moment onderzocht, als onderdeel van de voorbereiding van een gemeenschappelijke beheersoplossing (zie paragraaf 3.1).

Het wordt ook mogelijk berichten te transporteren die gegenereerd zijn door de software die ondernemers/intermediairs gebruiken (voor het overgrote deel samen te vatten onder de noemer 'boekhoudpakketten van de markt'). Het voordeel van dit type berichtenverkeer is dat bedrijven tijdens hun eigen administratieve processen de gegevens genereren ten behoeve van het eindbericht aan de betrokken overheidsdienst. Het eindbericht - aanvraag, aangifte, statistiekbericht e.d. - wordt dan geautomatiseerd aangemaakt. Deze wijze om berichten samen te stellen levert onmiskenbaar een flinke reductie van de administratieve lasten op.

¹¹ Motie Szabo c.s., Kamerstukken II, 29 362, nr. 9.

Bovendien heeft dit tot voordeel dat de frequentie van de gegevensuitvraag niet relevant is en dat 'hetzelfde' gegeven al in de eigen administratie wordt gebruikt ten behoeve van de verschillende gegevensuitvragers.

Hoewel deze vorm van berichtenverkeer uitermate interessant is voor administratieve lastenverlichting, komt dat niet vanzelf van de grond. Pas nu de belastingaangiften voor bedrijven *verplicht* digitaal moeten, is de markt geïnteresseerd. Het is interessant te overwegen voor alle overheidsdiensten deze weg op te gaan, althans een discussie te voeren over verdere verplichtingen/inbouw softwarepakketten.

Een vergelijkbare discussie is nodig over het verplicht gebruik van de basisvoorzieningen door de overheidsinstellingen.

2.7 Domein G: Snelle verbindingen tussen overheidsorganisaties

Voor wat betreft bedrijfsvoering en beheer speelt ook de bundeling van de ICT-netwerkinfrastructuur. De rijksoverheid streeft ernaar om een gezamenlijke breedbandige ICT-infrastructuur te realiseren. Een dergelijke infrastructuur betekent niet alleen een veiligere communicatie, maar biedt ook een goede basis voor gezamenlijke diensten (shared services). Bovendien zijn er mogelijkheden om in de toekomst diensten als telefonie via dit netwerk plaats te laten vinden. Het is daarom zaak de ICT-infrastructuur dusdanig in te richten dat zij opschaalbaar is.

De eerste stap op weg naar een gezamenlijke ICT-infrastructuur is het realiseren van een breedbandig netwerk voor de rijksoverheid in Den Haag. Hiermee zijn wel aanvangskosten gemoeid, maar die worden daarna terugverdiend. De bedoeling is dat vervolgens aansluiting wordt gezocht met andere overheidsorganisaties. Daarbij kan zowel gedacht worden aan instellingen van de rijksoverheid buiten de regio Den Haag, als aan samenwerking met de gemeenten en provincies.

Hoofdstuk 3: Gezamenlijk beheer, samenwerking en sturing, juridische en financiële aspecten

3.1: Gezamenlijk beheer

Ten aanzien van de elektronische overheid is de minister voor BVK verantwoordelijk voor e-government in het algemeen en het burgerdomein, en de minister van Economische Zaken voor het nationale ICT-beleid en het bedrijvendomein. De iCT-ontwikkelingen zijn van belang voor alle overheidsorganisaties. De uitdaging is bestuurlijke arrangementen te treffen die het mogelijk maken de kansen die ICT biedt à tempo maximaal te benutten.

In het voorgaande zijn in de diverse domeinen de verantwoordelijkheden geschetst.

Voor basisvoorzieningen die moeten gaan worden gebruikt door alle of vele overheidsorganisaties (zoals de OTP en de OTV), worden voorbereidingen getroffen om te komen tot een gemeenschappelijk beheer. Voor de vormgeving van een dergelijke gemeenschappelijke beheerorganisatie, waarbij de gebruikende overheidsorganisaties moeten worden betrokken, ligt enigerlei vorm van zelfstandige positionering in het publieke domein voor de hand.

Het is denkbaar dat diverse functionaliteiten met een gemeenschappelijk karakter bij eenzelfde gemeenschappelijke beheerorganisatie worden ondergebracht.

Op het punt van de realisatie van het hier geschetste beleid is een belangrijke rol voorzien voor private leveranciers van ICT-producten en -diensten. De algemene lijn is, dat optimaal gebruik wordt gemaakt van de specifieke kennis en vaardigheden van het bedrijfsleven op dit terrein. De overheid beperkt zich tot professioneel opdrachtgeverschap richting private partijen en het bevorderen van marktwerking. Behoud van leveranciersafhankelijkheid is voor de overheid daarbij een essentiële randvoorwaarde.

3.2 Samenwerking en sturing

Er bestaan reeds diverse programmatische kaders en bijbehorende sturingsafspraken. De meest betrokken partijen voeren reeds in verschillende verbanden overleg. De programma's zijn georganiseerd binnen de onderscheiden domeinen en ook wel óver de domeinen heen, in ketens (bijvoorbeeld ICTAL). De invoering van de uniforme openbare informatie-infrastructuur als in het voorgaande geschetst vereist echter aanvullende maatregelen op het punt van samenwerking en sturing. De aanvullingen betekenen geen ingreep in de bestaande structuren, wel het sturen op samenwerking.

Daartoe wordt interdepartementaal (Coördinatiegroep Elektronische Dienstverlening - CEDI) en interbestuurlijk (Regiegroep ICT en Overheid, VNG, stuurgroep e-Provincies, IPO en Manifestpartijen¹²) afgestemd..

De diverse trajecten kennen, alle op zich, een eigen dynamiek van besluitvorming en realisatie, gegeven de vele betrokken partijen. Voorkomen moet worden dit alles in één alomvattende projectaanpak te gaan persen: dat leidt alleen maar tot stagnatie. Wel kan en moet gestuurd worden op onderlinge afhankelijkheden en op synergie, en dient de voortgang te worden gestimuleerd.

Wanneer de diverse trajecten beter uitgekristalliseerd zijn, kunnen zij steeds beter in een gemeenschappelijk tijdsperspectief worden geplaatst. Voorlopig gaat het er om dat, in deze notitie, een eerste stap is gezet om de programma's inhoudelijk en functioneel met elkaar in verband te brengen.

De samenhang tussen de programma's in de onderscheiden domeinen zal worden versterkt. Dit zal gebeuren door een gemeenschappelijk ontwikkelingsperspectief te hanteren dat bij de realisatie van de programma's als richtpunt kan dienen. Het bestaat uit een overzicht van de gemeenschappelijke voorzieningen, dat de voorzieningen inhoudelijk en functioneel met elkaar in verband brengt. Waar programma's op onderdelen van elkaar afhankelijk zijn, geeft dit overzicht houvast bij het vaststellen van plannings- en uitvoeringsmodaliteiten. In bijlage 4¹³ zijn de belangrijkste elementen van dit overzicht weergegeven.

Het overzicht heeft een voortschrijdend karakter: de plannings- en uitvoeringsmodaliteiten die er in zijn opgenomen kunnen wijzigen onder invloed van ontwikkelingen die zich tijdens de realisatie voordoen. Het overzicht is een instrument waarmee, vanuit een gemeenschappelijk ontwikkelingsperspectief, kan worden gestuurd op samenhang en afstemming.

3.3. De juridische verankering van de elektronische overheid

Veel wet- en regelgeving op dit vlak is maar tot op zekere hoogte een zaak van de Nederlandse wetgever. EU-ontwikkelingen zijn een steeds dominantere factor bij de formulering van het nationale beleid. Niet alleen de juridische basis voor de elektronische handtekening is daarvan een voorbeeld. Het geldt onder meer tevens voor de in 2005 te effectueren EU-richtlijn inzake toegankelijkheid en exploitatie van overheidsinformatie¹⁴. En het geldt zeker ook voor een ontwikkeling als het, in het kader van de Lissabon-agenda van de EU dit voorjaar gepubliceerde, voorstel voor een richtlijn waarin voor de hele Europese Unie de invoering van één loket (*"a single point of contact"*) wordt bepaald waar dienstverleners *langs elektronische weg* hen regarderende administratieve formaliteiten

¹² In de Manifestgroep hebben een aantal uitvoeringsinstellingen zich verenigd met het oogmerk om in samenwerking beter gebruik te maken van de mogelijkheden van ICT. Het betreft de UWV, de CWI, de SVB, de Belastingdienst, de IB-Groep en het CvZ.

¹³ Het gaat hier uitdrukkelijk om een eerste versie, met een eerste globaal en tentatief beeld. In de loop van de komende tijd zal het beeld kunnen worden aangescherpt, waarvoor overleg nodig is met de relevante partijen.

¹⁴ Deze richtlijn schrijft voor dat overheden documenten en databases die volgens de nationale wetgeving openbaar zijn ook beschikbaar worden gemaakt voor commercieel gebruik. Tevens wordt harmonisatie beoogd van de gebruikscondities en wordt een plafond vastgesteld in de prijsstelling.

moeten kunnen afhandelen. De huidige planning is, dat een en ander uiterlijk eind 2007 in nationaal recht is omgezet en uiterlijk eind 2008 is geëffectueerd.¹⁵

In de afgelopen jaren is al veel werk verzet om wet- en regelgeving gelijke tred te laten houden met de technologische ontwikkelingen op ICT-terrein. De komende jaren zullen deze inspanningen versterkt moeten worden voortgezet.

3.4 De financiering van de elektronische overheid

Er zijn op dit moment geen aparte middelen voor de realisatie van de elektronische overheid uitgetrokken, zij het dat voor de diverse lopende programma's uiteraard in de financiering is voorzien. Op centraal niveau zijn zeer beperkt middelen aanwezig. Deze middelen zijn bedoeld om ontwikkelingen op gang te brengen en om het opstellen van business-cases te faciliteren voor de investeringen die noodzakelijk zijn. Of de noodzakelijke investeringen worden gedaan, zal worden afgewogen op basis van kosten-baten analyses (business-cases). Daarbij wordt wel de kanttekening gemaakt dat het knap lastig kan blijken te zijn om heel exact dergelijke analyses op te stellen:

- in verband met de interactie tussen tal van elementen
- ten gevolge van de soms aanwezige ongewisheid door allerlei zij-effecten
- omdat veel van de investeringen die nodig kunnen zijn, anders vermoedelijk nodig zouden zijn geweest voor reguliere afschrijvingen respectievelijk herinvesteringen. Oftewel: in hoeverre er echt extra uitgaven nodig zijn, is in hoge mate afhankelijk van het tempo waarin nieuwe voornemens tot implementatie komen
- omdat het karakter van enerzijds de kosten en anderzijds de baten sterk uiteen kan lopen. Zo zal een flink deel van de baten de vorm aannemen van toenemende fraudepreventie; deze baten laten zich per definitie moeilijk ex-ante (of ex-post) meten, maar zijn wel degelijk relevant.

Een en ander laat onverlet dat concrete investeringsbeslissingen plaats zullen moeten vinden op basis van deugdelijke business-cases. Daarbij zullen partijen die de vruchten plukken van de investeringen een bijdrage moeten leveren. Per basisvoorziening wordt bepaald wat het meest deugdelijke financieel ontwerp is¹⁶.

Wat betreft kosten voor exploitatie en beheer zal het uitgangspunt worden gehanteerd van een - zo eenvoudig mogelijke - systematiek van verrekening op basis van het profijtbeginsel. Ook ingeval van algemeen gebruikte publieke voorzieningen móet er een prikkel zijn en blijven voor doelmatig gebruik.

¹⁵ Voorstel voor een richtlijn van het Europese Parlement en de Raad betreffende diensten op de interne markt, d.d. 9 februari 2004 [SEC (2004 21)].

¹⁶ Inmiddels is op deze wijze voorzien in de financiering van de introductie van het Burger Service Nummer (BSN), het Basis Gebouwen Register (BGR) en het Basisregister Adressen (BRA)

BIJLAGE 1

EU-LIJST VAN OPENBARE DIENSTEN

De in Europees verband gemaakte opsomming van 20 openbare diensten (12 voor burgers en 8 voor bedrijven) waar overheden het leven een stuk makkelijker kunnen maken door het gebruik van nieuwe technologie:

Basisdiensten voor burgers

Aangifte en aanslag inkomstenbelasting

Diensten op het gebied van toeleiding naar werk

Aanvragen sociale verzekeringen, uitkeringen, kinderbijslag, studietoelagen, ziekenfonds e.d.

Aanvragen paspoort en rijbewijzen

Registratie en overschrijving van kentekens/ voertuigen

Aanvragen bouwvergunningen

Aangifte bij de politie

Zoeken in en reserveren bij bibliotheken

Aanvragen geboortebewijzen, uittreksels

Inschrijving bij onderwijsinstellingen

Doorgeven adreswijzigingen

Adviezen over beschikbaarheid van diensten in ziekenhuizen, afspraken e.d.

Basisdiensten voor bedrijven:

Loonheffing en premies werknemersverzekeringen

Winst aangifte en aanslag vennootschapsbelasting en inkomstenbelasting

BTW- aangiften en aanslagen

Registratie van een nieuwe onderneming

Verstrekking van statistische gegevens aan CBS

Douane- aangiften

Milieu- vergunningen

Elektronische verwerving goederen en diensten

BIJLAGE 2

VOORBEELDEN VAN (SAMENWERKINGS-)TRAJECTEN OP HET GEBIED VAN ELEKTRONISCHE TOEGANKELIJKHEID

Trajecten met betrekking tot het aanbieden van informatie

- standaardisatie van officiële overheidspublicaties
- organisatieonafhankelijk doorzoeken overheidsinformatie (burgerzoekmachine)
- *abonnementenservice voor overheidsinformatie, bijvoorbeeld over uitgifte van vergunningen, besluiten van bestuursorganen*
- actieve publicatie van overheidsinformatie op internet (12-puntenplan SG's)
- (decentrale) wettenbanken

Trajecten met betrekking tot het aanbieden van diensten

- productencatalogi van rijksoverheid, provincies, gemeenten en waterschappen
- elektronische formulieren en transactiegeneratoren
- portals (bijvoorbeeld overheid.nl, [bedrijvenloket](http://bedrijvenloket.nl), regering.nl; dergelijke portals zijn gericht op specifieke doelgroepen, maar onderling gekoppeld, om dubbel werk te voorkomen)

BIJLAGE 3

BASISADMINISTRATIES

De authentieke basisregisters:

- *basisadministratie natuurlijke personen (GBA en BRV)*

inhoud: Minister voor BVK (GBA)
Minister voor V en I (BRV)

beheer: gemeenten

- *basisadministratie bedrijven/ondernemers*

inhoud: Minister van EZ. Overige betrokkenen: Minister van FIN, Minister van LNV,
Minister van JUS, Minister voor VWS, Minister van SZW, Minister van
OC&W, Minister voor BVK

beheer: Kamers van Koophandel

- *basisadministratie gebouwen en adressen*

inhoud: Minister van VROM

- beheer: gemeenten

- *basisadministratie Vastgoed*

inhoud: Minister van VROM

beheer: Kadaster

- *basisadministratie geografische basiskaarten*

inhoud: Minister van VROM. Overige betrokkenen: Minister van DEF, Minister
van LNV, Minister van V&W, Minister van FIN.

beheer: Kadaster

Zoekrichting overige basisregisters (voorlopig)

- *basisadministratie werknemers/uitkeringsgerechtigden (polisadministratie)*

inhoud: Minister van SZW

beheer: UWV

- *basisadministratie inkomens*

inhoud: Minister van FIN. Overige betrokkenen: Minister van SZW, Minister
van VROM, VWS, Minister van OC&W.

beheer: Belastingdienst

- *basisadministratie goederen (afhankelijk van ontwikkeling in EU)*

inhoud: Minister van FIN. Overige betrokkenen: alle departementen behalve AZ

beheer: douane

- *basisadministratie voertuigen*

inhoud: Minister van V&W

beheer: RDW

– *basisadministratie Nederlandse ondergrond*

inhoud: Minister van VROM, Overige betrokkenen: Minister vanEZ, minister van OC&W, minister van LNV, minister van V&W.

beheer: TNO/NITG

BIJLAGE 4 Overzicht van activiteiten, eerste werkversie (zie ook par. 3.2 van hoofdstekst)

	2004	2005	2006	2007
Elektronische toegang tot de overheid				
Openbaarmaking		-ELU-richtlijn hergebruik overheidsinformatie van kracht	-wetenbank volledig gevuld	-wettelijk verplichte openbaarmaking elektronisch
Vindbaarheid		-abonnementservice	-overheidszoekmachine operationeel	
Elektronische authenticatie				
Overheidstoegangsvoorziening	- pilot OTV	-OTV operationeel, stapsgewijze uitrol bij diensten en uitbreiding authenticatiemiddelen	- OTV operationeel, verdere uitbreiding diensten en middelen	- OTV operationeel
Beheer	- tijdelijk beheer OTV en OTP	- besluitvorming samenwerking met banken op authenticatie gebied	- beheer OTV door Gemeenschappelijke beheerorg.	
	- eerste opzet gemeenschappelijk beheer + kwartemaker	- voorbereiding Gemeenschappelijke Beheerorganisatie	- besluitvorming en regelgeving gemeenschappelijk beheer	- uitbesteding operationeel beheer
			- oprichting Gemeenschappelijke Beheer Organisatie	
Éénduidige nummers voor personen en bedrijven	- onderzoek bedrijvennummer	- besluitvorming invoering BN	-invoering BSN	- invoering BN
	- besluitvorming BSN en ZIN			
Basisregistraties	- LRD operationeel (GBA)		- GBA in TK	
	- BBR versie 1 operationeel	- BBR wet in TK	- BBR wet in werking	- BGR in TK
	BGR		- vrijwillige invoering BGR (Basis Gebouwen Register) en BRA (Basis Register Adressen)	- BRA in TK
	BRA			
	Percelen			
	Topografisch kernbestand			
	Overige	- beleidsnotitie basisregisters	-basisregister niet-ingezetenen operationeel	- Topografisch kernbestand in TK
	- ontwikkeling WFSV (polisadm.)			

	2004	2005	2006	2007
Elektronische identificeringsmiddelen (chipcards)		-besluitvorming over biometrie	-besluitvorming over samenwerking met banken op chipcard gebied -invoering BSN-kaart voor EU/EER Ingezetelen	- Introductie chipcard
Elektronische informatie uitwisseling	- eerste versie OTP	-verplichte elektronische aangifte ondernemers -doorgroei OTP	- invoering gebruik XBRL in jaarrekeningen	-beheer OTP door gemeenschappelijke beheerorg