Adviescommissie Authenticatie en Autorisatie Bedrijven (A3 Bedrijven)

Eindadvies

11 november 2011

Voorwoord

Voor u ligt het eindrapport van de Adviescommissie Authenticatie en Autorisatie Bedrijven, ook wel A3 Bedrijven. Deze commissie is door de DG's van Binnenlandse Zaken (DGBK), Financiën (DG Bel) en Economische Zaken, Landbouw en Innovatie (DGETM, inmiddels DGBI) gevraagd te adviseren over:

- een aantal inhoudelijke en beleidsmatige vragen rond (de inrichting van) eHerkenning;

- het wegnemen van bestaande belemmeringen voor de brede implementatie van eHerkenning;

- mogelijkheden om de groei naar massaal gebruik van eHerkenning te faciliteren en te versnellen.

Bij de advisering over deze thema's heeft de commissie ervoor gekozen te redeneren vanuit de gewenste eindsituatie voor authenticatie en autorisatie van bedrijven. Daarvan uitgaand is de weg er naar toe bepaald. Die weg is ingevuld in de vorm van een aantal concrete adviezen. Door deze werkwijze vormen de adviezen in dit eindrapport een samenhangend geheel, wat het onwenselijk maakt om zogenoemd "selectief te winkelen" in de adviezen.

De leden van de commissie hebben met groot plezier aan dit advies gewerkt, mede vanuit hun overtuiging dat het voor de implementatie van elektronische dienstverlening voor bedrijven van cruciaal belang is dat eHerkenning van de grond komt. Zij hopen dat u evenveel plezier beleeft aan het lezen van het eindrapport en dat het u zal helpen bij het nemen van die maatregelen die nodig zijn om van eHerkenning een succes te maken.

De commissie A3 Bedrijven,

Cor Franke (voorzitter)
Arie van Bellen
Hans Blokpoel
Hans Nijman
Daisy Geurts (secretaris)

Inhoudsopgave

Voorwoord 2
Inhoudsopgave 3
1. Inleiding 4
2. Management samenvatting 5
3. Scope en afbakening 9
4. Opzet en werking van het stelsel eHerkenning 1.0 13
5. Deelopdracht 1: twee inhoudelijke obstakels die groei van het stelsel blokkeren 19
6. Deelopdracht 2: Kwaliteit en continuïteit 25
7. Deelopdracht 3: Implementatiestrategie 29
8. Randvoorwaarden 37
9. Doorkijk naar het burgerdomein 41
10. Roadmap 42
Bijlagen 44
Bijlage 1: Conceptueel kader GOA 45
Bijlage 2: Ecorys onderzoek naar financieel model 62

1. Inleiding

Begin juni 2011 is de Adviescommissie Authenticatie en Autorisatie Bedrijven (A3 Bedrijven) van start gegaan. Deze adviescommissie heeft van een drietal DG's vanuit EL&I, BZK en FIN de opdracht gekregen om te komen met een advies over een samenhangende authenticatie- en autorisatiesystematiek voor bedrijven, in relatie tot verschillende al bestaande voorzieningen (Digipoort, DigiD en DigiD Machtigen). De adviescommissie adviseert de DG's omtrent de wijze waarop de vereiste samenhang tussen de verschillende voorzieningen voor bedrijven op strategisch niveau tot stand kan worden gebracht en geborgd. Dit alles met het oog op een grootschalige implementatie van eHerkenning bij overheidsdienstaanbieders (zoals ook afgesproken in de overheidsbrede implementatieagenda voor dienstverlening en eOverheid, i-NUP).

De toenemende digitale communicatie en de toenemende afhankelijkheid van digitale voorzieningen maken een robuuste, veilige, betrouwbare en gebruikersvriendelijke voorziening voor authenticatie en autorisatie noodzakelijk. Ook in de digitale wereld moet je er immers op kunnen vertrouwen dat degene met wie je zaken doet, is wie hij zegt dat hij is en geautoriseerd is voor dat wat hij doet. Authenticatie en autorisatie (toegang, machtigingen, eenduidig vastleggen van wilsuitingen, traceerbaarheid van transacties tot op persoon) zijn daarbij van centraal belang. Het Diginotar incident, dat optrad toen de commissie al was begonnen, heeft het vertrouwen van burgers en bedrijven in digitale communicatie sterk aangetast. Binnen het stelsel van eHerkenning is een leverancier uitgevallen en dat heeft gevolgen gehad voor de primaire processen van de aangesloten overheidsdienstaanbieders. De commissie heeft gemeend er goed aan te doen om, in aanvulling op de opdracht, ook te adviseren over het herstel van het vertrouwen in digitale communicatie in het algemeen en met betrekking tot de kwaliteit en continuïteit van de authenticatie- en autorisatiesystematiek in het bijzonder.

Bij het ontbreken van een voorziening voor authenticatie en autorisatie, of 'trust framework', wordt digitaal zaken doen belemmerd en innovatie geremd. Het is voor de commissie een gegeven dat eHerkenning de basis vormt voor dat noodzakelijke 'trust framework'. Dat betekent dat de hoofdvraag voor de commissie is hoe eHerkenning zich kan ontwikkelen tot de voornoemde robuuste, betrouwbare, veilige en gebruikersvriendelijke voorziening die nodig is. Dat betekent ook dat dit advies geen voorstellen zal doen om de opzet van en de rolverdeling binnen het stelsel eHerkenning aan te passen. Het bestaande en reeds vastgestelde conceptueel kader, dat binnen eHerkenning is ontwikkeld, wordt verder als uitgangspunt gehanteerd en is opgenomen in Bijlage 1. Het een en ander laat onverlet dat de commissie wel voorstellen zal doen omtrent de wijze van gebruik van het stelsel. Verder zal de commissie expliciet aandacht geven aan hetgeen nodig is om te zorgen dat het stelsel volwassen wordt, in die zin dat ondernemers en overheidsdienstverleners op grote schaal gebruik gaan maken van hetgeen het stelsel biedt.

Dit advies is primair bedoeld ter ondersteuning van besluitvorming door de drie opdrachtgevende DG's. Om te komen tot een realistisch en implementeerbaar advies, heeft de commissie een breed scala aan belanghebbenden geconsulteerd en verschillende onderzoeken uitgezet. Daar waar relevant, wordt in de tekst naar de verschillende bronnen gerefereerd. In Bijlage 2 is een samenvatting opgenomen van het onderzoek dat is uitgevoerd naar het financieel model.

2. Management samenvatting

Inleiding
De Adviescommissie Authenticatie en Autorisatie Bedrijven, ook wel A3 Bedrijven, is door de DG's van Binnenlandse Zaken, Financiën en Economische Zaken, Landbouw en Innovatie DGBK, DGBel en DGETM, inmiddels DGBI) ingericht.

De achtergrond daarbij is de volgende. Maatschappelijke en economische ontwikkelingen maken het onontkoombaar dat steeds meer contacten tussen bedrijven en de overheid langs *elektronische* weg plaatsvinden. Op die manier is het mogelijk de overheid dienstbaar te laten zijn aan bedrijven terwijl tegelijkertijd de uitvoeringskosten van diezelfde overheid dalen. Deze ontwikkeling naar elektronisch zakendoen is expliciet benoemd in de Digitale Agenda.nl.

Voor een betrouwbare elektronische communicatie, is een betrouwbare inrichting van authenticatie en autorisatie randvoorwaardelijk. Sinds 2009 werkt het ministerie van EL&I in dit kader hard aan de ontwikkeling en implementatie van het stelsel eHerkenning. In dat traject is een aantal obstakels aan het licht gekomen, die de groei van het stelsel op korte termijn blokkeren. De commissie is in het leven geroepen om oplossingen en voorstellen te ontwikkelen om deze blokkades weg te nemen.

Drie lastige onderwerpen
Voor het advies als zodanig aan de orde komt wil de commissie een drietal zaken specifiek noemen.

Het eerste punt dat de commissie wil adresseren zijn de ingrijpende consequenties van het Diginotar-incident. Door dit incident heeft het vertrouwen van burgers en bedrijven in het elektronisch zakendoen (met de overheid) een fikse knauw gekregen. Het is de commissie glashelder dat een advies over de toekomst van het stelsel eHerkenning alleen serieus genomen kan worden als dat advies expliciet aangeeft welke maatregelen nodig zijn om de veiligheid, de betrouwbaarheid binnen en de continuïteit van het stelsel te borgen. Op dit punt heeft de commissie zijn opdracht daarom breder opgevat, leidend tot een aantal concrete aanbevelingen rond beveiliging en continuïteit van eHerkenning. De commissie meent dat glashelder moet zijn wie welke verantwoordelijkheden heeft bij het voorkomen en bestrijden van misbruik van elektronische dienstverlening door de overheid.

Ten tweede heeft de commissie bij de uitwerking van zijn opdracht vastgesteld dat het onderscheid tussen burgers en bedrijven steeds minder relevant is. In Nederland kennen we inmiddels ruim 850.000 eenmanszaken. Dat aantal is nog steeds groeiend. Bij eenmanszaken komen de rollen van burger en bedrijf samen, in één persoon met één Burgerservicenummer (BSN). In het licht van deze ontwikkeling constateert de commissie dat er stringente beperkingen bestaan rond het gebruik van het BSN. Die beperkingen leiden er concreet toe dat een persoon in de hoedanigheid van burger zaken met overheidsorganisaties kan doen en daarbij DigiD kan gebruiken om zich, met zijn BSN, te identificeren en te authenticeren, maar dat wanneer dezelfde persoon zich in de hoedanigheid van een bedrijf (eenmanszaak) meldt en gebruik maakt van eHerkenning, het gebruik van het BSN niet is toegestaan. Bovendien mag DigiD, dat werkt op basis van het BSN, niet gebruikt worden in het private domein, tenzij daar een expliciete wettelijke grondslag voor is gemaakt. De commissie heeft de bestaande regelgeving rondom BSN als een gegeven beschouwd.

Ten derde heeft de commissie geconstateerd dat het wettelijk kader rondom Markt en Overheid hier en daar op gespannen voet staat met beleidswensen met betrekking tot het realiseren van publieke voorzieningen voor bedrijven. Kern van de wet Markt en Overheid is dat marktpartijen bij hun activiteiten geen oneerlijke concurrentie van de overheid mogen ondervinden. De commissie beschouwt het wettelijk kader rondom Markt en Overheid als een gegeven.

Opzet van het advies
De commissie heeft ervoor gekozen te redeneren vanuit de gewenste eindsituatie: een eenvoudig en robuust stelsel van eHerkenning dat het vertrouwen heeft van burgers, bedrijven en overheid. Uitgaande daarvan is de weg daar naar toe bepaald. De weg naar de gewenste eindsituatie vergt op een tweetal terreinen (respectievelijk identificatie en authenticatie van eenmanszaken en de vastlegging van machtigingen ten behoeve van het zogenoemde machine-machine-verkeer met de Belastingdienst) transitievoorzieningen. Die voorzieningen maken het mogelijk om:

- de marktpartijen die rollen binnen het stelsel eHerkenning (willen) vervullen de kans te geven hun producten en diensten (verder) te ontwikkelen en deze aan overheidsdienstaanbieders en bedrijven te leveren;

- voor deze (verdere) ontwikkeling de tijd te nemen die daarvoor nodig is (hetgeen betekent dat de marktpartijen niet ineens te maken krijgen met een massale vraag naar producten en diensten die de nu beschikbare capaciteit verre zou overstijgen);

- op een termijn van twee á drie jaar aanvullende besluiten te nemen rond deze voorzieningen in het licht van de verdere inrichting en implementatie van het stelsel eHerkenning.

Daarnaast is het naar de mening van de commissie belangrijk dat de transitievoorzieningen het mogelijk maken dat de Belastingdienst, als grootste publieke uitvoerder, een voortrekkersrol neemt bij de implementatie van eHerkenning.

De commissie sluit tenslotte niet uit dat het, tijdens de verdere implementatie van eHerkenning, nodig kan zijn andere transitievoorzieningen te treffen. De randvoorwaarde daarbij moet zijn dat de transitievoorziening een bijdrage levert aan een beheerste ontwikkeling in de richting van de eindsituatie (en dus niet blokkerend werkt voor het bereiken daarvan).

Kernpunten in het advies
Het onderhavige rapport is uitgebreid en werkt op onderdelen gedetailleerd uit wat de visie van de commissie is. Dat is het gevolg van de wens van de commissie om zowel vanuit een eindbeeld te redeneren als pragmatisch om te gaan met de concrete problemen en obstakels die zich op dit moment rond eHerkenning voordoen.

Los daarvan kent het advies een aantal kernpunten. Die kernpunten zijn gebaseerd op het uitgangspunt dat eHerkenning de generieke voorziening moet zijn voor authenticatie en autorisatie van bedrijven, en dat de markt de ruimte krijgt om de rollen binnen het stelsel in te vullen. Bij de kernpunten gaat het concreet om voorstellen om:

- de marktpartijen door het gebruik van de voornoemde transitievoorzieningen voldoende tijd te bieden om in hun rol te groeien, zodat er over twee jaar een robuust stelsel staat, dat grootschalige digitale communicatie tussen overheid en bedrijven kan faciliteren;

- de markt te ondersteunen bij die groei, door krachtige actie aan zowel de aanbodkant (aanbod van diensten die met eHerkenning worden ontsloten) als de vraagkant (aanschaf van authenticatiemiddelen door bedrijven). Analyse wijst namelijk uit dat de markt voor eHerkenning een tweezijdige markt is, in die zin dat partijen aan beide zijden van de markt, dus bedrijven én overheidsdienstaanbieders, beiden in voldoende mate toe moeten treden om de markt volwassen te maken. Tot de markt volwassen is spreken we van een groeifase. Het dringende advies is deze groeifase zo kort mogelijk te maken, om zo de baten van de introductie van eHerkenning maximaal te maken en te voorkomen dat marktpartijen voortijdig uittreden.

De commissie ziet de volgende mogelijkheden om deze gewenste snelle groei te bevorderen:

1. ontwikkeling van applicaties die snelle groei bevorderen;
2. eHerkenning toevoegen als tweede sleutel bij bestaande elektronische overheidsdiensten voor bedrijven;
3. op termijn uitfaseren van bestaande (organisatie- of sectorgebonden) middelen voor identificatie en authenticatie van bedrijven op termijn;
4. inzichtelijk maken van de kosten voor het gebruik van eHerkenning en ondersteunen van bedrijven bij het kiezen van het juiste eHerkenningsmiddel;
5. op gang brengen van een tijdelijke geldstroom van overheidsdienstaanbieders om de aanschaf van voldoende hoogwaardige private authenticatiemiddelen te stimuleren;
6. mogelijk maken en bevorderen van hergebruik van eHerkenning (als "trust framework") in andere domeinen, zoals B2B (Business to Business), G2G (Government to Government) en B2C (Business to Consumer).

- op termijn de nu nog volledig gescheiden stelsels voor burgers (DigiD) en bedrijven (eHerkenning) op elkaar aan te laten sluiten, door het gebruik van dezelfde standaarden en koppelvlakken *en* door zo spoedig mogelijk, maar in ieder geval binnen 2 á 3 jaar, een "DigiD hoog" (eID) te ontwikkelen, dat zodanig wordt ontworpen dat het mogelijk wordt om deze voorziening ook in private omgevingen te (her)gebruiken. Als identificerend kenmerk wordt daarbij niet het BSN, maar een pseudoniem gebruikt, met de mogelijkheid dit pseudoniem om te zetten in een BSN (voor organisaties die het BSN mogen verwerken). Deze voorziening moet een betrouwbaarheidsniveau 4 (Stork) hebben;

- zolang dit "Digid hoog" er niet is, toe te staan dat de bedrijven waarbij de rol van burger en bedrijf samenvallen (de eenmanszaak) voor identificatie en authenticatie voor de korte termijn Digid gebruiken;

- om voor de Belastingdienst de transitie van de huidige inrichting van machtigingen naar een stelselinrichting mogelijk te maken, wordt in opdracht van de Belastingdienst een publiek beheerde machtigingsvoorziening ingericht. Deze voorziening maakt het voor bedrijven (niet zijnde eenmanszaken) mogelijk om enkelvoudige machtigingen te registreren. Met deze oplossing kunnen deze bedrijven hun financieel of fiscaal dienstverlener machtigen om (met behulp van machine-machine interactie) elektronische aangiften bij de Belastingdienst in te dienen en onder andere elektronische kopie-aanslagen te ontvangen. De commissie onderschrijft, vanuit een continuïteitsperspectief van de overheidsdienstverlening, de noodzaak van deze voorziening en stelt vast, dat deze niet blokkerend werkt voor de eindsituatie. Over 2 jaar wordt gekeken of het nodig is om deze voorziening te continueren.

De commissie doet verder, zoals eerder aangegeven, een aantal concrete aanbevelingen rond beveiliging en continuïteit van eHerkenning. In het verlengde daarvan vraagt de commissie nog aandacht voor het volgende. De reeds geuite politieke wens om de burger niet meer dan nodig lastig te vallen met vervanging van identiteitsdocumenten staat op gespannen voet met de door de commissie gevoelde noodzaak de dragers van deze documenten frequent te vervangen (en zo gebruik te maken van nieuwe technische (beveiligings)oplossingen.

Verder bevat het advies een zogenoemde "road map", een lijst met acties die nodig zijn om de adviezen van de commissie te implementeren.

Andere aandachtspunten
De commissie hecht er aan een drietal zaken expliciet onder de aandacht van de opdrachtgevende DG's te brengen, hoewel deze zaken feitelijk buiten de opdracht aan de commissie liggen. Het gaat om het volgende:

- de commissie stelt vast dat de kennis van eHerkenning geconcentreerd is bij een beperkt aantal "insiders", zowel binnen de overheid als daarbuiten. Gerichte aandacht voor verspreiding van het gedachtengoed rond eHerkenning zal de groei in het gebruik van eHerkenning verder versterken;

- de implementatie van eHerkenning in andere domeinen dan B2G (Business to Government), zoals voorgesteld in de groeistrategie vraagt om gerichte aandacht, op hoog niveau, zowel binnen de overheid als bij het bedrijfsleven, om zo te voorkomen dat de aanzienlijke baten die een nationaal “trust framework” kan bieden te laat of niet worden geïncasseerd;

- overheidsdienstaanbieders kiezen zelf welk betrouwbaarheidsniveau vereist is voor toegang tot hun diensten. Daartoe is een Handreiking opgesteld. Om redenen van eenduidige dienstverlening aan bedrijven verdient het aanbeveling dat gelijkwaardige diensten binnen de overheid met hetzelfde betrouwbaarheidsniveau toegankelijk zijn. Dit zou met neer nadruk bevorderd kunnen worden.

3. Scope en afbakening

3.1 Relevante ontwikkelingen

Een aantal ontwikkelingen heeft invloed op de wijze waarop overheidsdienstverleners elektronische diensten aanbieden en ondernemers die afnemen. De belangrijkste daarvan zijn:

Het belang van digitale dienstverlening neemt toe en daarmee de behoefte aan een 'trust framework'
Digitale communicatie neemt toe, in de maatschappij, tussen bedrijven onderling en tussen de overheid en bedrijven. De toenemende afhankelijkheid en de kwetsbaarheid van het digitale kanaal vraagt om robuuste voorzieningen voor authenticatie en autorisatie, waarmee digitaal veilig en betrouwbaar zaken kunnen worden gedaan. Daarvoor is het nodig dat dienstverleners op het gebied van authenticatie en autorisatie, bedrijven en overheidsdienstaanbieders afspraken maken over:

1. de voorwaarden waaronder men elkaars authenticatie- en autorisatiemiddelen vertrouwt;
2. de manier waarop het overheidstoezicht en het beheer worden geregeld, ook in relatie tot partijen die wel of juist niet meer aan de voorwaarden voldoen (nieuwe toetreders, beëindigen van deelname);
3. juridische aansprakelijkheid;
4. interoperabiliteit: de uitwisselbaarheid en herbruikbaarheid van de verschillende middelen en voorzieningen.

Een dergelijk afsprakenstelsel of 'trust framework', dat onderdeel is van de digitale infrastructuur van Nederland en onder toezicht staat van de overheid, is nodig om efficiënt en effectief in te kunnen spelen op bedreigingen zoals criminaliteit en spionage.

Het onderscheid tussen burger en bedrijf vervaagt
Het onderscheid tussen burgers en bedrijven is steeds minder relevant als het gaat om het ontwikkelen van elektronische diensten door de overheid. In Nederland kennen we inmiddels ruim 850.000 eenmanszaken. Dat aantal groeit nog steeds. Bij eenmanszaken[1] komen de rollen van burger en bedrijf samen, in één persoon met één BSN.

Voor de Belastingdienst is in geval van een eenmanszaak het onderscheid tussen de betrokken persoon als burger (die bijvoorbeeld IB-aangifte doet) en bedrijf (dat BTW-aangifte doet) eigenlijk niet meer relevant. Het gaat in beide gevallen om dezelfde persoon, met hetzelfde BSN. Voor een gemeentelijke organisatie geldt iets vergelijkbaars: veel ondernemers in de gemeente wonen er ook als burger. In deze rollen hebben ze te maken met dezelfde gemeente en de grote diversiteit aan diensten die de gemeente steeds meer digitaal wil aanbieden.

Het gevolg hiervan kan zijn dat authenticatievoorzieningen uit het burgerdomein soms ook in het bedrijvendomein gebruikt kunnen worden. Op termijn is het omgekeerde ook niet uit te sluiten.

Misbruik en oneigenlijk gebruik komen steeds meer voor en worden complexer en bedreigender
Een aantal jaren geleden werd het misbruik van creditcardgegevens als belangrijkste probleem gezien bij het gebruik van het internet, op de voet gevolgd door "phishing" en de zogenoemde "Nigeriaanse e-mails" (bedoeld om de ontvanger te verleiden een klein bedrag te betalen om zo de beschikking te krijgen over prijzen en erfenissen). Deze vormen van criminaliteit zijn gebaseerd op respectievelijk diefstal (van gegevens) en misleiding (door het aannemen van een fictieve identiteit).

[1] Het gaat hier om de *rechtsvorm* eenmanszaak (die geen rechtspersoonlijkheid heeft). Zie www.kvk.nl/ondernemen/rechtsvormen/overzicht-van-alle-rechtsvormen/

Inmiddels hebben we te maken met andere vormen van criminaliteit. Eén daarvan is gebaseerd op het onrechtmatig gebruiken van de "digitale identiteit" van een (rechts)persoon. Een voorbeeld daarvan is het via internet wijzigen van rekeningnummers waarop toeslagen worden betaald. Een andere vorm van criminaliteit maakt gebruik van de snelheid van handelen bij digitale dienstverlening. Een voorbeeld hiervan zijn de zogenoemde "BTW-carroussels". In het verlengde van het voorgaande heeft het Diginotar incident laten zien dat het vertrouwen in authenticatiemiddelen en daarmee in electronische diensten ernstig ontregeld kan worden door digitale criminaliteit (hacking). Door de toenemende verwevenheid van overheidsprocessen en systemen en de voortschrijdende digitalisering wordt de potentiële impact van dergelijke criminaliteit steeds groter.

Het is te verwachten dat digitale criminaliteit zich, net als andere vormen van criminaliteit, blijft ontwikkelen en daarmee steeds geavanceerder wordt. Daarom zal breed gebruik van eHerkenning om te beginnen eisen stellen aan de snelheid waarmee digitale identiteiten en autorisaties "buiten werking kunnen worden gesteld" in geval van misbruik. Verder vraagt breed gebruik van eHerkenning om indringend toezicht door de overheid op de aanbieders van authenticatie- en autorisatiediensten.

3.2 Uitgangspunten

Gezien bovenstaande ontwikkelingen is bij het ontwerp, de implementatie en het gebruik van een samenhangende authenticatie- en autorisatiesystematiek voor bedrijven een aantal uitgangspunten van groot belang. Dat zijn:

Een bedrijf moet de authenticatie- en autorisatievoorziening kunnen afstemmen op zijn behoefte
Met het toenemende belang van digitale dienstverlening, neemt ook de behoefte bij bedrijven aan een solide voorziening voor authenticatie en autorisatie toe. Bedrijven verschillen van elkaar in aard en frequentie van hun contacten met de overheid en in de manier waarop zij omgaan met digitalisering. Het komt de acceptatie van de voorziening ten goede, als een bedrijf keuzes kan maken in de vorm van de digitale voorziening, zodat de voorziening aansluit bij de werkwijze en voorkeuren van het bedrijf.

Een bedrijf moet namelijk, op grond van wet- en regelgeving, voldoen aan een aantal administratieve verplichtingen die de overheid hem oplegt. Waar het gaat om die verplichtingen zelf heeft hij geen keuzevrijheid, waar het gaat om de wijze van nakomen ervan wel. Zo kan een ondernemer ervoor kiezen om zijn administratie zelf te voeren en daarmee ook zelf aan de administratieve verplichtingen van de overheid te voldoen. Hij kan er ook voor kiezen om deze taken uit te besteden aan één (of meer) gespecialiseerde dienstverlener(s). Een veel voorkomend onderwerp van een dergelijke uitbesteding is de salarisadministratie, naast natuurlijk de boekhouding of de aanvraag van subsidies. In het geval dat een ondernemer er voor kiest om taken uit te besteden betekent dit dat de betrokken dienstverlener namens hem moet kunnen handelen. Dit vergt dat het bedrijf de dienstverlener machtigt.

Welke keuze het bedrijf ook maakt, om digitaal zaken te kunnen doen met de overheid heeft het bedrijf een authenticatiemiddel nodig. Dat ligt voor de hand als hij zelf zijn administratie voert en zijn administratieve verplichtingen verzorgt. In dat geval moet de overheid in staat zijn om het bedrijf te herkennen en vast te stellen of hij bevoegd is de gevraagde dienst af te nemen. Maar ook als het bedrijf (een deel van) zijn administratieve taken heeft uitbesteed, heeft hij zo'n authenticatiemiddel nodig om de door hem gekozen dienstverlener te machtigen.

Authenticatiemiddelen hebben uiteenlopende verschijningsvormen met verschillende betrouwbaarheidsniveaus. Het bedrijf kan kiezen wat het best aansluit bij de eigen manier van digitaal zaken doen met de overheid. De verschillende middelen onderscheiden zich in de inrichting van het uitgifteproces en de werking van de techniek. Samen bepalen deze zaken de sterkte/het betrouwbaarheidsniveau van het middel. In de regel is het zo dat de inspanningen die moeten worden verricht om het middel te verkrijgen en de kosten toenemen naarmate het betrouwbaarheidsniveau toeneemt. Het is lang niet altijd noodzakelijk om het hoogste

betrouwbaarheidsniveau te gebruiken. Doordat er verschillende betrouwbaarheidsniveaus bestaan, is een afweging tussen risico's, kosten en gebruikersgemak mogelijk.

Een overheidsdienstaanbieder maakt voor iedere elektronische dienst die hij ontwikkelt een afweging rond het betrouwbaarheidsniveau dat voor deze dienst wordt vereist. Daarbij kan de overheidsdienstaanbieder de handreiking[2] van het College Standaardisatie gebruiken als hulpmiddel. Het gebruik van deze handreiking bevordert dat dezelfde betrouwbaarheidsniveaus worden gekozen voor vergelijkbare diensten. Een bedrijf kiest voor een betrouwbaarheidsniveau dat hij wil gebruiken en voor een middel dat bij dat niveau past. De keuze voor een betrouwbaarheidsniveau impliceert dat het bedrijf geen diensten kan afnemen die een hoger niveau van betrouwbaarheid vergen dan zijn middel ondersteunt.

Transparantie voor overheidsdienstverleners
Overheidsdienstverleners bieden in toenemende mate elektronische diensten voor ondernemers aan. Daarbij hanteren zij vaak eigen oplossingen voor authenticatie en autorisatie. Deze oplossingen kennen als nadeel dat ze vaak maar bij één overheidsorganisatie kunnen worden gebruikt. Als gevolg hiervan ontstaat voor bedrijven die zaken doen met meerdere overheidsorganisaties een zogenoemde "digitale sleutelbos". Dat is niet handig. Daarnaast kost het opzetten en beheren van een eigen voorziening de overheidsdienstverlener geld, terwijl dat geen kerntaak is.

Het doel van eHerkenning is om ondernemers via één oplossing, en op eenduidige wijze, toegang te bieden tot elektronische overheidsdiensten. Door gebruik te maken van eHerkenning besteden de overheidsdienstverleners de activiteiten rond authenticatie en autorisatie feitelijk uit.

Zoals eerder aangegeven is zijn er authenticatiemiddelen in allerlei soorten en maten. Door gebruik te maken van eHerkenning voorkomen de overheidsdienstverleners dat zij het gebruik van al deze middelen moeten ondersteunen. Zij krijgen daarentegen te maken met een gestandaardiseerd koppelvlak. Dit koppelvlak beschrijft (functioneel gezien) de identiteit van het bedrijf dat een dienst wil afnemen, het betrouwbaarheidsniveau van het authenticatiemiddel dat wordt gebruikt en het pseudoniem van deze persoon. Hierdoor kan een overheidsdienstverlener verschillende soorten authenticatiemiddelen accepteren, al dan niet in combinatie met een machtiging. Een overheidsdienstaanbieder kan zich concentreren op de vraag welk betrouwbaarheidsniveau nodig is voor de digitale dienst die wordt aangeboden. Als het betrouwbaarheidsniveau is vastgesteld, staat niets afname van de dienst meer in de weg.

Wettelijke kaders
Relevante wettelijke kaders binnen de scope van de adviesvraag zijn de wet Markt en Overheid en het wettelijke kader rondom het Burger Service Nummer (BSN).

Kern van de onlangs aangenomen wet Markt en Overheid is dat marktpartijen bij hun activiteiten geen oneerlijke concurrentie van de overheid mogen ondervinden.

De commissie beschouwt het huidige wettelijk kader rondom BSN, als een gegeven. Overheidsorganisaties mogen voor de uitvoering van hun taak het BSN verwerken. De wetgeving biedt echter geen ruimte voor verwerking van het Burger Service Nummer (BSN) door private partijen, zonder dat daarvoor een expliciete wettelijke grondslag bestaat. DigiD werkt op basis van BSN en daarom is het niet mogelijk DigiD in het private domein te gebruiken, als voor het gebruik van het BSN geen expliciete wettelijke grondslag bestaat.

Het stelsel eHerkenning is BSN-loos opgezet. Dat betekent dat het afsprakenstelsel geen BSN hanteert waar het gaat om de identificatie van natuurlijke personen die handelen namens een bedrijf of hun eigen bedrijf. Bij eHerkenning wordt in eerste instantie het bedrijf herkend. Daarnaast is, om dienstverlening te kunnen personaliseren en misbruik of fraude te kunnen

---

[2] Handreiking Bepalen van betrouwbaarheidsniveaus voor authenticatie bij digitale overheidsdiensten, versie 1.0

herleiden naar een handelende persoon, informatie nodig over de identiteit van de handelende persoon. Daarvoor gebruikt het stelsel een zogenoemd persistent pseudoniem.

3.3 Concretisering van de vraag aan de commissie

De commissie richt zich op de hoofdvraag hoe eHerkenning zich kan ontwikkelen tot de robuuste voorziening voor authenticatie- en autorisatie, die nodig is om de toenemende digitale communicatie te ondersteunen, die rekening houdt met het vervagende onderscheid tussen burgers en bedrijven en die voldoet aan de drie uitgangspunten 'ondernemer moet voorziening kunnen aanpassen aan zijn behoefte', 'transparantie voor overheidsdienstaanbieders' en 'geen gebruik van het BSN'. Binnen deze scope heeft de commissie drie deelopdrachten opgepakt:

Ten eerste het wegnemen van een aantal concrete inhoudelijke onduidelijkheden. Er zijn twee inhoudelijke vraagstukken die grootschalige implementatie van eHerkenning in de weg staan: de behoefte aan één stelsel voor álle bedrijven in relatie tot de beperkingen m.b.t. het gebruik van het BSN (en daarmee de rol van DigiD ten opzichte van het stelsel) en de inrichting van machtigingen en de rol van een eventueel publiek machtigingenregister daarbij, met name in het machine-machine domein.

Ten tweede het adviseren over eventuele aanvullende maatregelen die nodig zijn om kwaliteits-, en continuïteitsrisico's van het stelsel voor eindgebruikers en overheidsdienstaanbieders acceptabel te maken zodat zij over zullen gaan tot implementatie en gebruik van eHerkenning. Deze deelopdracht wint aanmerkelijk aan belang sinds het Diginotar-incident.

Ten derde het formuleren van een implementatiestrategie, om een snelle groei van het stelsel te realiseren. Essentieel voor een levensvatbaar stelsel is een 'korte groeifase': zowel aan de kant van overheidsdienstaanbieders als aan de kant van gebruikers zal snel op grote schaal gebruik moeten worden gemaakt van eHerkenning, omdat anders het stelsel niet financieel zelfredzaam wordt.

3.4 Leeswijzer

In het volgende hoofdstuk 4 wordt eerst de werking van het stelsel eHerkenning beschreven, omdat dat de voorziening is waarop zal worden doorontwikkeld. Daarna volgt een drietal hoofdstukken met daarin de verschillende adviezen op de drie deelopdrachten. Deze adviezen worden op deelaspecten nader uitgewerkt in hoofdstuk 8 over randvoorwaarden die nodig zijn om verdere groei te faciliteren, zoals standaarden, toe- en uittreding, hergebruik van middelen en beheer- en toezichtsaspecten. Dit rapport sluit af met een doorkijkje naar het burgerdomein en tenslotte een roadmap, waarin is weergegeven wie wat wanneer moet doen om de robuuste voorziening voor authenticatie en autorisatie van bedrijven (die eHerkenning bedoeld is te zijn) te realiseren.

In de bijlage zijn achtergrondstukken opgenomen over een aantal randvoorwaardelijke aspecten van het stelsel: conceptueel kader, financieringsmodel, werking van het stelsel.

De lezer die op de hoogte is van de werking en de ontstaansgeschiedenis van eHerkenning en die graag snel kennis wil nemen van de hoofdlijnen van het advies van de commissie, adviseren wij om hoofdstuk 5, 6 en 7 te lezen en daarna door te gaan naar de roadmap.

Voor de lezer die zich een beeld wil vormen van de werking van het bestaande stelsel eHerkenning, biedt hoofdstuk 4 een toegankelijke samenvatting van de werking van het stelsel.

4. Opzet en werking van het stelsel eHerkenning 1.0

Het afsprakenstelsel eHerkenning 1.0 ondersteunt bedrijven bij het afnemen van elektronische diensten bij publieke organisaties. Het stelsel faciliteert de processen rond identificatie, authenticatie en autorisatie die voorafgaan aan het feitelijk gebruiken van de dienst.

De beschrijving van de werking van het stelsel valt uiteen in drie onderdelen:

- de werking gezien vanuit het perspectief van de eindgebruiker (bedrijven)[3];
- de werking gezien vanuit het perspectief van een overheidsdienstaanbieder.
- de werking van het stelsel vanuit het perspectief van de marktpartijen die rollen in het stelsel vervullen.

In Bijlage 1 is een uitleg opgenomen over de verschillende interactiepatronen bij het afnemen van overheidsdiensten door bedrijven, aan de hand van de situatie bij de Belastingdienst.

4.1 Werking vanuit het perspectief van de eindgebruiker

Eindgebruikers zijn de bedrijven die het stelsel benutten om zich aan de overheid bekend te maken en zich (dan wel hun medewerkers) te autoriseren ten behoeve van afname van elektronische diensten.

De eerste stap in het gebruik van het stelsel is de aanschaf van één of meer authenticatiemiddelen die bedoeld zijn om medewerkers van een bedrijf te identificeren. Deze middelen zijn alleen te gebruiken door het bedrijf dat ze aanschaft. De ondernemer maakt daarbij een keuze voor een leverancier en voor een betrouwbaarheidsniveau.

Daarna legt de bevoegd vertegenwoordiger van het bedrijf desgewenst voor ieder middel vast welke machtigingen daaraan zijn gekoppeld. Dat doet hij in een zogenoemd Machtigingenregister. Bij deze vastlegging toetst de beheerder van het Machtigingenregister in het register van de Kamer van Koophandel of degene die de machtigingen wil vastleggen daadwerkelijk de bevoegd vertegenwoordiger van het bedrijf is. Na deze stap heeft het bedrijf één of meer middelen beschikbaar, waarbij per middel duidelijk is wat de houder van het middel namens het bedrijf mag doen.

Op het moment dat het bedrijf een elektronische dienst bij een overheidsdienstaanbieder wil afnemen of toegang wil krijgen tot een online portaal zoekt een medewerker (die in het bezit is van een authenticatiemiddel zoals hierboven bedoeld) contact met de betrokken dienst. Hij doorloopt dan een aantal stappen, waarin hij zich respectievelijk identificeert, die identiteit bevestigt (authenticatie) en waarin het stelsel toetst (aan de hand van de registraties in het Machtigingenregister) of de medewerker daadwerkelijk bevoegd is deze dienst af te nemen. Als deze toetsen succesvol verlopen krijgt de medewerker namens het bedrijf toegang tot de dienst of tot het portaal.

Mogelijk kan het bij de uitvoering van de dienst nodig zijn een zogenoemde elektronische handtekening te zetten. Het stelsel ondersteunt in de toekomst ook deze activiteit, in die zin dat

---

[3] voor het leesgemak wordt overal in dit rapport de term 'bedrijven' gebruikt. Daaronder worden alle organisaties begrepen die eHerkenning als eindgebruiker kunnen gaan gebruiken: eenmanszaken, rechtspersonen en samenwerkingsverbanden, maar ook verenigingen en stichtingen.

ook hier de medewerker een aantal stappen doorloopt die leiden tot het zetten van de gevraagde handtekening.

Een aantal aanvullende opmerkingen:

- de bevoegd bestuurder kan een medewerker van het bedrijf machtigen om de machtigingen van het bedrijf, zoals opgenomen in het machtigingsregister, te onderhouden;

- het staat het bedrijf natuurlijk vrij om op ieder gewenst moment middelen aan te schaffen, in te trekken of machtigingen te wijzigen. De verantwoordelijkheid hiervoor berust bij het bedrijf.

4.2 Werking vanuit het perspectief van de overheidsdienstverlener

De overheidsdienstverlener heeft één of meer elektronische diensten online (in een webportaal) beschikbaar gesteld aan bedrijven. Op het moment dat een bedrijf een dergelijke dienst wil afnemen geeft de overheidsdienstverlener dit door aan een Herkenningsmakelaar. Deze zorgt dat de identificatie en de authenticatie plaatsvinden en toetst bij de beheerder van het Machtigingenregister of de houder van het middel bevoegd is deze dienst uit te voeren.

Na afronding van deze activiteiten zorgt de Herkenningsmakelaar dat de gegevens uit het stelsel transparant worden doorgegeven aan de overheidsdienstaanbieder. Het gaat hier in ieder geval om de volgende gegevens:
- het KvK-nummer van het bedrijf;
- het betrouwbaarheidsniveau waarop de identiteit van de betrokken medewerker is vastgesteld;
- de uitkomst van de toets op de bevoegdheid van deze medewerker om de dienst af te nemen;
- het pseudoniem van de betrokken medewerker.

Daarmee komt een medewerker van een bedrijf pas binnen bij de overheidsdienstaanbieder, als de identiteit van het bedrijf en het betrouwbaarheidsniveau zijn vastgesteld en de handelende persoon ook gemachtigd is om de transactie via het portaal in gang te zetten. Zo wordt de overheidsdienstaanbieder ontzorgd en blijft de ondernemer verantwoordelijk voor het gebruik van authenticatiemiddelen en machtigingen. De overheidsdienstaanbieder kan, met de beschikbare gegevens, zelf beslissen of hij de dienst ter beschikking wil stellen (dat zal met name afhangen van het gebruikte betrouwbaarheidsniveau en van de uitkomst van de toets op de bevoegdheid).

4.3 Werking van het stelsel vanuit het perspectief van de marktpartijen

Het afsprakenstelsel werkt met een viertal duidelijk omschreven rollen:

- Middelenuitgevers (MU);

- Authenticatiediensten (AD);

- Machtigingenregisters (MR);

- Herkenningsmakelaars (HM).

De middelenuitgevers zijn marktpartijen die de authenticatiemiddelen uitgeven. Bij middelen gaat het om naam/wachtwoord-combinaties, tokens, passen, elektronische certificaten, etc.

Authenticatiediensten controleren of de gebruiker van een middel daadwerkelijk is wie hij zegt dat hij is, door bijvoorbeeld de combinatie gebruikersnaam en wachtwoord te controleren of de PIN-code die de houder van het middel gebruikt bij activering van een certificaat te toetsen.

De rollen van Middelenuitgever en Authenticatiedienst zijn gescheiden om het zo mogelijk te maken dat middelen die uitgegeven zijn buiten het eHerkenningsstelsel (denk bijvoorbeeld aan bankmiddelen) kunnen worden hergebruikt binnen het stelsel. De authenticatiedienst is dan de

dienst die deze middelen "toegankelijk" maakt voor gebruik in het stelsel en waarlangs de daarbij geldende (juridische) voorwaarden verankerd worden.

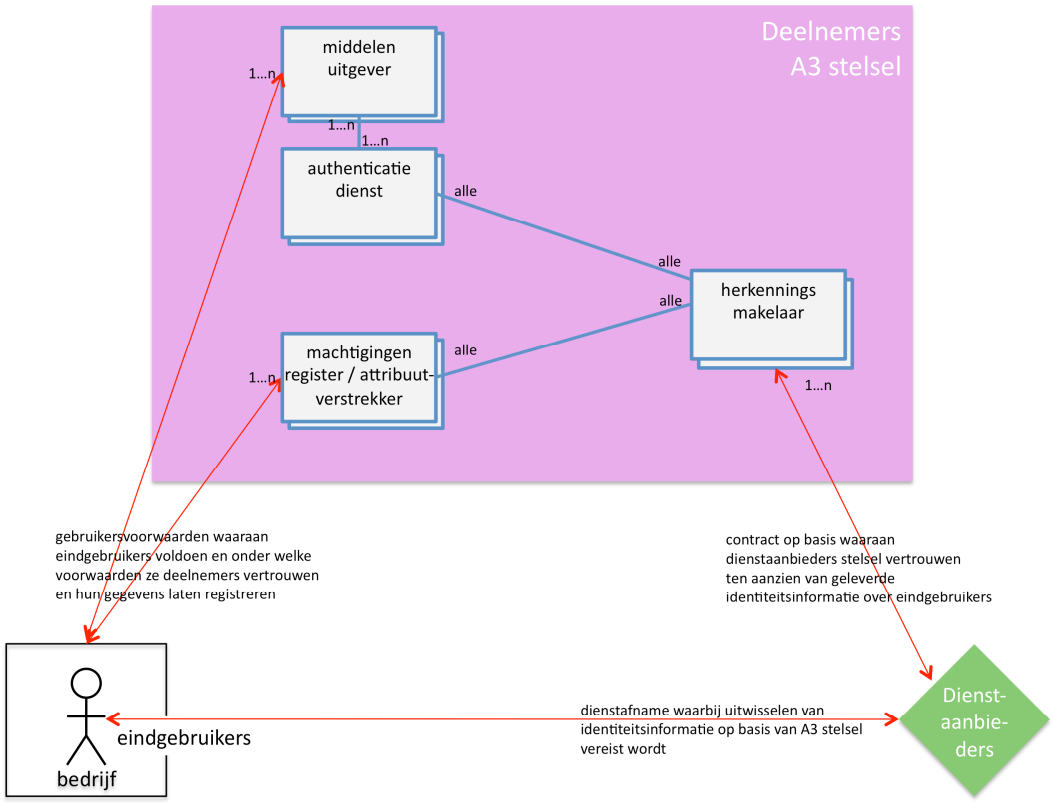
Machtigingenregisters leggen de bevoegdheden vast die verbonden zijn aan de uitgereikte authenticatiemiddelen. Het beheer van de machtigingen van een onderneming gebeurt in eerste instantie door de bevoegd vertegenwoordiger van die onderneming. Die kan anderen machtigen om dit beheer te voeren.

Machtigingen en autorisaties worden separaat van de Authenticatiemiddelen vastgelegd. Dat geldt ook voor andere gegevens (attributen) over de partijen die middelen aanschaffen.

Herkenningsmakelaars vormen een noodzakelijke (technische) rol in het stelsel die het mogelijk maken dat de overheidsdienstverleners één aanspreekpunt hebben, terwijl er toch meerdere middelenuitgevers, authenticatiediensten en machtigingenregisters naast elkaar kunnen bestaan. De herkenningsmakelaar is daarmee de partij die de communicatie tussen het stelsel en de overheidsdienstaanbieder verzorgt en de complexiteit van het stelsel reduceert.

Zowel eindgebruikers (bedrijven) als overheidsdienstaanbieders hebben dus één relatie met deelnemers in het stelsel. Deze relaties liggen contractueel vast, zodat formele helderheid bestaat over wederzijdse rechten en verplichtingen.

Het volgende schema toont de onderlinge samenhang tussen enerzijds de rollen in het stelsel en anderzijds de relatie die eindgebruikers en overheidsdienstverleners met het stelsel hebben.



4.4 Werking van het stelsel bij machine to machine (M2M) verkeer

In Bijlage 1 wordt toegelicht, aan de hand van de situatie bij de Belastingdienst, welke rol machine to machine (M2M) verkeer vervult. Ook bij M2M verkeer is sprake van authenticatie en autorisatie. Voorafgaand aan de instelling van de commissie hebben de ministeries van BZK, EL&I en FIN samen het GOA-traject uitgevoerd. Het doel van dit traject was een aantal zogenoemde POC's (POC staat voor "proof of concept") te realiseren om zo de gewenste inrichting van onder andere onderdelen van het stelsel eHerkenning verder uit te werken en te beproeven.

GOA had voorzien vier POC's uit te voeren. Drie daarvan zijn uitgevoerd en afgerond, leidend tot besluitvorming in de stuurgroep GOA en, waar aan de orde, nadere vraagstellingen aan de commissie. De vierde POC, gericht op M2M interactie is niet afgerond. Dat heeft de volgende reden.

De overheid voorziet dat het per 1 januari 2013 verplicht is om bij levering van (bepaalde) gegevens aan de Belastingdienst gebruik te maken van Standard Business Reporting (SBR), waarbij gebruik gemaakt wordt van de gegevensstandaard XBRL en de fysieke levering van de gegevens plaatsvindt via Digipoort. Later volgt ook (een deel van) de gegevensaanlevering aan het Centraal Bureau voor de Statistiek en de Kamer van Koophandel.

De Belastingdienst heeft als beleidslijn dat dergelijke massale implementaties voorafgegaan worden door een proefjaar, dat bedrijven en hun dienstverleners in staat stelt ervaring op te doen en kinderziekten op te lossen. Om dat mogelijk te maken moet per 1 januari 2012 een tijdelijke oplossing beschikbaar komen voor authenticatie en autorisatie bij Digipoort. Het was helder dat uitvoering van de POC ertoe zou leiden dat die oplossing te laat beschikbaar zou komen.

Inmiddels heeft de Belastingdienst de bedoelde tijdelijke oplossing gedefinieerd. Bij de presentatie daarvan heeft de Belastingdienst tevens aangegeven deze oplossing na het beschikbaar komen van de definitieve oplossing, uit te faseren.

Om tot de definitieve oplossing te komen is het volgende traject voorzien:

- de stuurgroep heeft de marktpartijen eHerkenning gevraagd om met een voorstel voor een definitieve oplossing te komen (in de vorm van een offerte);

- de marktpartijen hebben deze offerte inmiddels ingediend. Zij geven daarbij aan dat het mogelijk is voor 1 januari 2012 een werkende testopstelling te presenteren.

De oplossing die marktpartijen voorstellen maakt het mogelijk naast elkaar gebruik te maken van zowel een publiek Machtigingsregister als private Machtigingsregisters.

4.5 Kenmerken van het stelsel

De hiervoor beschreven opzet van het stelsel heeft een aantal belangrijke kenmerken. Dat zijn:

- het stelsel stelt *keuzevrijheid en verantwoordelijkheid van het bedrijf* centraal. Het bedrijf kiest zelf zijn authenticatiemiddel en het daaraan gerelateerde betrouwbaarheidsniveau. Daarmee maakt hij impliciet een keuze voor de diensten die hij wel en de diensten die hij niet kan afnemen (omdat het betrouwbaarheidsniveau van het door hem gekozen middel te laag is voor een bepaalde dienst);

- verder maakt het stelsel het mogelijk dat de *overheidsdienstverlener wordt ontzorgd*. Die hoeft geen eigen authenticatievoorzieningen te ontwikkelen, te onderhouden en te exploiteren, dat besteedt hij uit aan de partijen binnen het stelsel. De herkenningsmakelaar regelt voor de overheidsdienstaanbieder met één dienst de hele toegang voor bedrijven tot zijn digitale dienstverlening;

- het stelsel kent *verschillende betrouwbaarheidsniveaus*, die aansluiten bij Europese standaarden (STORK). Een betrouwbaarheidsniveau geeft een indicatie van de betrouwbaarheid waarmee de identificatie en authenticatie zijn uitgevoerd. Door het hanteren van verschillende betrouwbaarheidsniveaus is het voor overheidsdienstaanbieders mogelijk voor verschillende diensten verschillende niveaus van betrouwbaarheid te eisen, afhankelijk van de afweging tussen risico's, kosten en gebruikersvriendelijkheid die wordt gemaakt. Met het vaststellen van een beperkt aantal gestandaardiseerde niveaus wordt voorkomen dat er een groot aantal betrouwbaarheidsniveaus worden gehanteerd die op detailniveau van elkaar verschillen en daardoor niet inter-operabel zijn.

- eHerkenning is een *open stelsel* waarin iedere private partij die dat wenst en aan de eisen voldoet mag toetreden. Dit geldt ook voor buitenlandse partijen. De ratio achter een dergelijk open stelsel is dat duidelijke en expliciete eisen aan de te leveren diensten interoperabiliteit bewerkstelligen en dat duidelijke regels voor transparantie competitie tussen deelnemers mogelijk maken. Deze eisen en regels zijn vervat in het zogenaamde afsprakenstelsel eHerkenning. Zo ontstaat een stelsel waarin enerzijds wordt samengewerkt om interoperabiliteit en vertrouwen te bewerkstelligen, terwijl er anderzijds concurrentie is op producten en proposities. Het stelsel stelt ondernemers en overheidsdienstaanbieders in staat eigen keuzes te maken. Een ondernemer kan er ook voor kiezen om een bedrijfseigen authenticatie- of machtigingsvoorziening aan het stelsel te koppelen. Deze optie zal met name voor grote ondernemingen interessant zijn.

- *de veiligheid en interoperabiliteit van het stelsel* is gebaseerd op verschillende pijlers. In het afsprakenstelsel zijn eisen t.a.v. de veiligheid van processen en techniek vastgelegd en geborgd in juridische overeenkomsten. Regelmatig en op verschillende niveaus vindt controle plaats op de naleving van deze afspraken. Bij toetreding moeten partijen gecertificeerd zijn op basis van algemene (ISO 27001 en 27002) en voor eHerkenning specifieke normenkaders. Dit gebeurt op basis van technische tests die afgenomen wordt door specialisten. Tests zullen periodiek worden herhaald. Indien een deelnemer niet aan de normen voldoet zijn er sancties. De deelnemer kan aansprakelijk worden gesteld en uiteindelijk ook uit het netwerk verwijderd worden.

  Dienstaanbieders en bedrijven voor wie eHerkenning bedrijfskritisch is, kunnen hun afhankelijkheid van specifieke marktpartijen verminderen door middelen respectievelijk verbindingen met de herkenningsmakelaar dubbel uit te voeren en deze te verdelen over twee of meer partijen. De hoge mate van standaardisatie van de koppelvlakken maken de kosten van dergelijke risicospreiding relatief laag. Alle cruciale standaarden waarop het netwerk is gebaseerd, staan op de pas-toe-of-leg-uit-lijst van Forum Standaardisatie of zijn in het proces van beoordeling voor die lijst.

- de *privacy van de gebruiker*s en de bescherming van de bedrijfsgegevens die in het stelsel worden uitgewisseld is een uitgangspunt van het afsprakenstelsel en krijgt vorm doordat het stelsel van eHerkenning BSN-loos is opgezet en werkt volgens het principe van dataminimalisatie. De grondarchitectuur van het stelsel gaat uit van het uitwisselen van alleen die identiteitsinformatie die strikt noodzakelijk is (het minimum). De overheidsdienstaanbieder ontvangt standaard deze minimaal benodigde dataset. Voor die toepassingen waar aanvullende informatie noodzakelijk is (need-to-know) wordt deze op basis van de minimale basisinformatie opgehaald op het moment dat deze daadwerkelijk nodig is.

  In geval van een vermoeden van misbruik of oneigenlijk gebruik kan de overheidsdienst-aanbieder meer informatie krijgen. Dit maakt het mogelijk de uitwisseling van gevoelige gegevens te beperken tot die situaties waarin het strikt noodzakelijk is en bovendien dit te doen op een wijze die aan de eindgebruikers transparant gemaakt kan worden en in het stelsel eenduidig gelogd kan worden (voor verantwoording achteraf).

- vanuit het oogpunt van een kostenefficiënte dienstverlening (NUP, Visie op Dienstverlening) is verder afgesproken dat de voorzieningen *generiek* worden opgezet zodanig dat ze door (vrijwel) alle overheidsorganisaties benut kunnen worden. Dat maakt het mogelijk bestaande oplossingen

voor authenticatie, die gekoppeld zijn aan een specifieke dienst, te migreren naar de generieke voorziening eHerkenning.

- *standaardisatie en hergebruik*: de belangrijkste standaard in het stelsel is het koppelvlak tussen de herkenningsmakelaar en de overheidsdienstaanbieder. Die standaard maakt het mogelijk dat:

    - nieuwe private partijen tot het stelsel toetreden;
    - partijen nieuwe middelen introduceren;

  beiden zonder dat dat consequenties heeft voor de overheidsdienstaanbieders.

  Verder sluit het stelsel aan op de Europese (concept) STORK standaarden. Daarmee is een aantal betrouwbaarheidsniveau's gedefinieerd waaraan zowel de middelenuitgevers als de overheidsdienstaanbieders zich kunnen conformeren. Dit zorgt voor interoperabiliteit over de landsgrenzen heen: buitenlandse authenticatiediensten werken met dezelfde standaarden en ondersteunen zo een eenduidig betrouwbaarheidsniveaus voor buitenlandse bedrijven die bij de Nederlandse overheid elektronische diensten afnemen.

  Binnen het stelsel zijn verder standaarden gedefinieerd die de interactie(s) tussen de verschillende rollen definiëren. Deze standaarden zorgen voor interoperabiliteit (iedere rol kan waar nodig met de andere rollen samenwerken) en voor helderheid voor nieuwe toetreders (die vóór toetreding weten aan welke eisen ze moeten voldoen);

- authenticatiemiddelen en -processen worden geleverd door *marktpartijen*. Deze marktpartijen ontwikkelen, leveren en beheren de technische voorzieningen die samen het stelsel vormen. De overheid heeft daarbij een coördinerende en toezichthoudende rol. De coördinerende rol krijgt vorm door de initiële ontwikkeling van het afsprakenstelsel. De toezichthoudende rol waarborgt de betrouwbaarheid en de continuïteit van het stelsel.

5. Deelopdracht 1: twee inhoudelijke obstakels die groei van het stelsel blokkeren

In 2010 en 2011 is er onder auspiciën van de stuurgroep GOA (Gemeenschappelijk Ontwerp Authenticatie en Autorisatie) een globaal ontwerp gemaakt van de authenticatie- en autorisatievoorzieningen voor burgers en bedrijven. Ook is er een aantal zogenoemde POC's ingericht, waarbij POC staat voor "Proof Of Concept".

Het eindrapport van het GOA-programma is op 26 augustus 2011 in de stuurgroep GOA behandeld. De stuurgroep heeft zich bij de behandeling van het eindrapport met name geconcentreerd op de besluitvorming rond een aantal beleidsvragen. Daarbij heeft de stuurgroep een aantal richtinggevende besluiten genomen (die de commissie als uitgangspunt heeft gehanteerd). Daarnaast heeft de stuurgroep de volgende vragen aan de commissie voorgelegd:

- de commissie A3 Bedrijven zal worden gevraagd om een advies over het gebruik van private authenticatiemiddelen bij organisaties die het BSN willen hebben voor hun eigen proces (*het gebruik van private authenticatiemiddelen maakt omnummeren noodzakelijk vanwege beperkingen rond het gebruik van het BSN)*;

- de commissie A3 Bedrijven wordt gevraagd om suggesties/een voorstel te doen over een beperkt en gratis publiek basis-machtigingenregister.

De antwoorden op deze vragen komen in het navolgende aan de orde, in de vorm van twee adviezen.

Advies 1: de rol van DigiD en eID in het stelsel

Eenvoud en laagdrempeligheid van de authenticatie- en autorisatievoorziening is belangrijk voor eindgebruikers, omdat zij zo makkelijk mogelijk elektronisch hun zaken met de overheid moeten kunnen regelen. Omdat het onderscheid tussen burger en bedrijf steeds minder hanteerbaar wordt en het aantal eenmanszaken toeneemt, is de vraag actueel welke rol DigiD moet spelen in de authenticatie van bedrijven. Het gebruik van DigiD is immers –letterlijk- ingeburgerd, en voor eenmanszaken kan het kunnen gebruiken van DigiD voor zakelijke transacties met de overheid bijdragen aan compliance: op die manier wordt het voor kleine ondernemers zo makkelijk mogelijk gemaakt om zich aan de overheidsregels te houden.

De commissie is van mening dat eHerkenning, als stelsel voor authenticatie en autorisatie voor bedrijven, zo snel mogelijk en zo breed mogelijk moet worden geïmplementeerd en gebruikt. Het verplicht invoeren van eHerkenning als standaard voor alle bedrijven, zonder daarbij rekening te houden met het middel dat in het burgerdomein wordt gebruikt, stuit echter op grote weerstand bij overheidsdienstaanbieders, die complianceproblemen vrezen bij met name eenmanszaken.

Een breed gebruik van DigiD als middel voor authenticatie van bedrijven wordt geblokkeerd door het feit dat DigiD werkt met het BSN. Het gebruik van het BSN is wettelijk beperkt tot overheidsdienstaanbieders en enkele private partijen met een expliciete wettelijke grondslag (zorgverzekeraars, pensioenfondsen). Daarnaast kent DigiD ook zijn beperkingen voor wat betreft de betrouwbaarheid. Voor transacties waarvoor een hoger betrouwbaarheidsniveau vereist is dan DigiD momenteel biedt, is een andere oplossing nodig.

De commissie heeft daarom gezocht naar een manier om het streefbeeld van één eenvoudige, laagdrempelige voorziening voor authenticatie voor alle bedrijven te realiseren. Die voorziening moet bovendien veilig gebruikt kunnen worden door alle overheidsdienstaanbieders en eindgebruikers en er moet een levensvatbaar businessmodel aan ten grondslag liggen, om te zorgen dat het stelsel duurzaam kan worden gefinancierd. Uiteraard moet de vormgeving van deze voorziening passen binnen de bestaande juridische kaders.

De commissie adviseert daarom om:

1. zo spoedig mogelijk, maar in ieder geval binnen 2-3 jaar, een "DigiD hoog" (eID) te ontwikkelen, die zo wordt opgezet dat het mogelijk wordt om deze ook in private organisaties te gebruiken. Als identificerend kenmerk wordt niet het BSN, maar een pseudoniem gebruikt.[4] Deze voorziening moet een betrouwbaarheidsniveau 4 (Stork) hebben;
2. dit 'DigiD hoog' op te nemen als herkenningsmiddel in het eHerkenningsstelsel en de kosten hiervan bij de gebruikers in rekening te gaan brengen;
3. tot die tijd, DigiD tijdelijk als tweede sleutel –naast eHerkenning- mogelijk te maken op webportalen van overheidsdienstaanbieders die het BSN mogen verwerken, waarbij dit gebruik strikt beperkt blijft tot de groep eenmanszaken[5];
4. de groeivertraging van het stelsel eHerkenning, die optreedt als gevolg van het toestaan van DigiD voor eenmanszaken, te compenseren met een aantal maatregelen (zie implementatiestrategie). Ook zal sneller en vol moeten worden ingezet op B2B gebruik van eHerkenning om de groei van het stelsel als geheel te versnellen.

Als toelichting bij advies 2 nog het volgende: Indien 'DigiD hoog' binnen het stelsel van eHerkenning wordt gebracht is er sprake van concurrentie tussen 'DigiD hoog' en eHerkenning. DigiD is nu gratis, terwijl eHerkenning de gebruiker geld kost. De wet Markt en Overheid bepaalt dat de overheid in dergelijke gevallen een voorziening (zoals 'DigiD hoog') alleen maar op de 'markt' mag brengen indien de integrale kostprijs daarvan wordt doorberekend aan de gebruikers.

Met het oog op de robuustheid, veiligheid en betrouwbaarheid van het stelsel voor authenticatie en autorisatie als geheel, wijst de commissie nog op een aantal punten:

Ten eerste is het belangrijk dat overheidsdienstaanbieders ervan doordrongen zijn dat zij *zelf* verantwoordelijk zijn voor de keuze van het vereiste betrouwbaarheidsniveau van het middel waarmee bedrijven toegang krijgen tot hun digitale dienstverlening. Waar het betrouwbaarheidsniveau van DigiD onvoldoende wordt geacht en de overheidsdienstaanbieder toch aan eenmanszaken toestaat om met DigiD toegang te krijgen tot een dienst die mogelijk een hoger betrouwbaarheidsniveau vraagt, moeten de overheidsdienstverleners zelf, in het achterliggende proces, compenserende maatregelen nemen om het risico van misbruik en fraude te reduceren.

Daarnaast vindt de commissie het belangrijk dat dragers van eHerkenningsmiddelen (zoals in de toekomst dragers van DigiD hoog) een zeker vervangingsritme hebben om nieuwe technieken en innovaties te kunnen implementeren en zo voldoende weerstand te bieden tegen nieuwe vormen van cybercriminaliteit. De reeds geuite politieke wens om de burger niet meer dan nodig lastig te vallen met vervanging van identiteitsdocumenten staat op gespannen voet met de door de commissie gevoelde noodzaak de dragers van deze documenten frequent te vervangen (en zo gebruik te maken van nieuwe technische (beveiligings)oplossingen.

Waar het gaat om de technische inrichting van eID vindt de commissie het wenselijk om geen BSN op het eID op te nemen maar te volstaan met een (betekenisloos) pseudoniem. Het BSN zou, naar analogie met DigiD-laag en –midden, dan samen met dit pseudoniem opgenomen zijn in een separate registratie (koppeltabel). Na identificatie en authenticatie met behulp van eID zou de betrokken dienstaanbieder, als hij daartoe gerechtigd is, het BSN daar op kunnen halen. In andere gevallen maakt de dienstaanbieder gebruik van het voornoemde pseudoniem. De stuurgroep GOA heeft eerder besloten dat in het Dienstenregister wordt geregistreerd welke organisatie wettelijke toestemming heeft om het BSN te verwerken.

---

[4] Dat vergt de opname van een pseudoniem voor het BSN op het eID, gecombineerd met de optie om het bij het pseudoniem bijzoeken van het BSN te blokkeren (voor partijen die het BSN niet mogen verwerken)

[5] De afbakening tot eenmanszaken is belangrijk vanwege de wet Markt & Overheid. Indien eenmanszaken als burger worden beschouwd en DigiD het enige middel is dat met een BSN kan authenticeren, concurreert DigiD niet met private middelen.

Advies 2: eisen, inrichting en werking van machtigingen

Machtigingen - autorisaties- zijn een essentieel onderdeel van het zakelijk verkeer. Tegelijkertijd leven er nog onduidelijkheden over hoe met machtigingen in het stelsel van eHerkenning moet worden omgegaan. Naar de mening van de commissie moeten er twee verschillende soorten machtigingen worden onderscheiden:

1. verticale machtigingen: machtigingen binnen een bedrijf, waarmee bevoegdheden worden gekoppeld aan medewerkers binnen een bedrijf; en
2. horizontale machtigingen tussen bedrijven, waarmee het ene bedrijf het andere bedrijf machtigt om namens hem zaken te doen.

Machtigingen binnen een bedrijf (verticale machtigingen)
In een register kunnen bedrijven vastleggen welke bevoegdheden verschillende medewerkers in het bedrijf hebben. In het Handelsregister legt een onderneming vast wie de bestuurder(s) is/zijn, van daaruit kunnen de vertegenwoordigingsbevoegdheden/volmachten verder in een Machtigingsregister worden vastgelegd en beheerd.

Wanneer een medewerker van een bedrijf met een authenticatiemiddel een digitale transactie in gang zet, haalt de herkenningsmakelaar eerst gegevens op bij de authenticatiedienst om vast te stellen om welke medewerker, welk bedrijf en om welk betrouwbaarheidsniveau het gaat. Met die gegevens toetst de Herkenningsmakelaar bij een machtigingenregister of de handelende persoon de transactie daadwerkelijk namens het bedrijf mag verrichten. In het eHerkenningsstelsel wordt daartoe gewerkt met een pseudoniem. Uit dit pseudoniem kan de werkelijke identiteit niet door de overheidsdienstaanbieder zelf worden achterhaald (het is tenslotte een pseudoniem). In geval van misbruik en/of oneigenlijk gebruik is het wel mogelijk de identiteit van de (handelend natuurlijk) persoon vast te stellen. Immers, conform de regels voor het uitgifteproces voor middelen, heeft de Middelenuitgever de identiteit van de betreffende persoon geverifieerd/vastgesteld en aan de persoon een pseudoniem toegekend. Het pseudoniem kan ook gebruikt worden om de dienstverlening van de overheidsdienstaanbieder te personaliseren (bij herhaald bezoek aan het webportaal kan bijvoorbeeld een boodschap als 'Welkom, mevrouw de Vries' worden getoond).

Essentieel in het ontwerp van het stelsel eHerkenning is dat de digitale transactie pas start als bedrijf en betrouwbaarheidsniveau zijn vastgesteld en de handelende persoon ook gemachtigd is om de transactie in gang te zetten. Machtigingen *binnen* een bedrijf zijn feitelijk niet van belang voor een *overheidsdienstaanbieder.* Het stelsel eHerkenning zorgt er namelijk voor dat de identiteit van de medewerker van een bedrijf is vastgesteld op het gevraagde betrouwbaarheidsniveau en dat vastgesteld is dat de handelende persoon bevoegd is voor de transactie voordat de digitale transactie start. De overheidsdienstaanbieder hoeft geen formele gevolgen aan de beschikbare informatie over (de bevoegdheid van) de handelende persoon te verbinden, maar kan deze wel gebruiken voor betere dienstverlening. De commissie concludeert dat verticale machtigingenregisters met name een functie hebben in het bedrijvendomein en minder voor overheidsdienstaanbieders. Voor bedrijven is het wel belangrijk dat de machtigingen/ vertegenwoordigingsbevoegdheden binnen het bedrijf adequaat digitaal zijn vastgelegd. In geval van onregelmatigheden is het namelijk van belang om na te kunnen gaan welke medewerker welke transactie heeft gedaan ('audit trail'). Verder is het in B2B transacties bijna altijd relevant om de bevoegdheid van degene die de handeling verricht te kennen. Om te voorkomen dat er twee stelsels ontstaan of dat de ondernemer te maken krijgt met extra lasten voor het gebruik in verschillende domeinen, beveelt de commissie een eenduidige werking rond machtigingen binnen eHerkenning aan waarbij het aan de dienstverlenende organisatie is om te bepalen wat men met de verkregen informatie over machtigingen doet.

Er zijn al verschillende aanbieders in de markt die machtigingsregisters beschikbaar stellen. Het Handelsregister heeft de rol van 'moederregister', alleen de in het Handelsregister (HR) geregistreerde bestuurder(s) zijn bevoegd om namens het bedrijf nadere machtigingen in een Machtigingenregister vast te leggen. Bestuurders kunnen hun medewerkers ook weer machtigen om machtigingen vast te leggen in een register. Zo ontstaat een 'boom' die herleidbaar is naar de

bestuurder van een bedrijf. Daarom is het van belang dat er op korte termijn een functionaliteit voor machtigingenregisters beschikbaar komt (in de vorm van een webservice) waarmee online in het HR gecontroleerd kan worden of iemand geregistreerd staat als bestuurder.

Adviezen:

1. benadruk in alle communicatie dat de overheid vanuit het oogpunt van veilige digitale dienstverlening bedrijven aanraadt om machtigingen volledig en actueel te registreren in een Machtigingenregister;
2. laat Machtigingenregisterfunctionaliteit voor verticale machtigingen door marktpartijen of bedrijfseigen voorzieningen invullen (zoals ook nu al het geval is).

Machtigingen tussen bedrijven (horizontale machtigingen)
Deze situatie komt vooral voor wanneer een bedrijf gebruik maakt van een zakelijke dienstverlener om namens hem transacties met de overheid te verrichten. Een overheidsdienstaanbieder zal dan willen vaststellen of die zakelijke dienstverlener inderdaad bevoegd is om namens dat bedrijf te handelen. Om dit vast te kunnen stellen zullen registraties van deze bevoegdheden in een Machtigingsregister opgenomen moeten worden.

Omdat er vragen zijn over de inrichting van het Machtigingsregister voor horizontale machtigingen, heeft de stuurgroep GOA aan de commissie A3 Bedrijven gevraagd om met suggesties of een voorstel te komen ten aanzien van een functioneel beperkt en gratis publiek machtigingenregister. Deze vraag heeft betrekking op machtigingen *tussen* bedrijven.

De commissie redeneert als volgt:

- voor burgers is door de overheid het stelsel DigiD (en DigiD Machtigen) ontwikkeld, gebaseerd op BSN. Dat stelsel is een volledig publieke voorziening (want verwerking van het BSN kent nu eenmaal zijn wettelijke restricties);
- het is consistent om - aansluitend bij het hiervoor verwoorde advies over DigiD- ook voor het registreren van machtigingen het perspectief van het bedrijf centraal te stellen. Voor eenmanszaken is dan de publieke basisvoorziening DigiD Machtigen voorhanden, want eenmanszaken kunnen gebruik maken van hun BSN. Eenmanszaken kunnen er ook voor kiezen om een private oplossing van eHerkenning te gebruiken;
- voor rechtspersonen/samenwerkingsverbanden ligt dat anders, daar is de organisatie zelf het aanknopingspunt en deze wordt aangeduid met een RSIN. Omdat er, in tegenstelling tot het BSN, geen wettelijke restricties aan het gebruik van het RSIN zijn gesteld, is hiervoor geen publieke voorziening vereist.

Publiek beheerde machtigingsvoorziening M2M machtigingen Belastingdienst
De Belastingdienst (BD) gaat met de introductie van SBR bij binnenkomende aangiften vragen om een bevoegdheidsverklaring van de betrokken partij. Dat gebeurt op dit moment niet. Verder brengt de Belastingdienst wijzigingen aan in de bestaande werkwijze rond uitgaande informatiestromen, daar wijzigt men van “opt out” naar “opt in”. Tenslotte gebruikt de Belastingdienst een intern informatiesysteem voor het registreren van machtigingen in geval van uitgaand verkeer. De Belastingdienst faseert dit systeem uit.

Op dit moment komt 85% van de aangiften via fiscale dienstverleners bij de Belastingdienst elektronisch binnen (en waar het om bedrijven gaat is dit zelfs 100%, als gevolg van de verplichtstelling voor bedrijven om elektronische aangifte te doen).

De voornoemde veranderingen in de wijze waarop de Belastingdienst omgaat met machtigingen zijn op zichzelf al majeur en brengen risico’s met zich mee voor de continuïteit van deze gegevensstromen. De Belastingdienst wil dat risico niet vergroten door het gebruik van private machtigingenregisters. De Belastingdienst geeft daarbij het volgende aan:

- het gaat bij het voorgaande om ongeveer 900.000 bedrijven (niet-eenmanszaken). Ongeveer 95% van die bedrijven maakt gebruik van de diensten van fiscaal dienstverleners. Dat betekent dat (private) machtigingsregisters ongeveer 850.000 machtigingen moeten registreren (een machtiging geldt overigens per belastingmiddel, dus de feitelijke registratie is een veelvoud van 850.000);

- het aantal partijen dat de functionaliteit van een privaat machtigingsregister aanbiedt is beperkt. Verder is de omvang (in termen van personele bezetting) van ieder van deze partijen klein;
- bovendien hebben deze partijen nog maar zeer beperkt ervaring opgedaan met het registreren en gebruiken van machtigingen binnen het stelsel.

Om voor de Belastingdienst de transitie van de huidige inrichting van machtigingen naar een stelselinrichting mogelijk te maken (en dus het voornoemde continuïteitsrisico te voorkomen), wil de Belastingdienst een specifiek publiek beheerd machtigingenregister inrichten.

De commissie is van mening dat –gezien het grote belang van continuïteit en het aanvullende argument dat de private machtigingenregisters nog niet klaar zijn voor grootschalig registreren en gebruiken van machtigingen- een goed ontworpen voorziening kan passen in het groeipad van eHerkenning. De commissie geeft daarbij de volgende randvoorwaarden mee, die ervoor moeten zorgen dat blijvend wordt voldaan aan de uitgangspunten van de authenticatie- en autorisatiesystematiek zoals beschreven in dit advies:

1. heldere afbakening van de doelgroep: het gaat om bedrijven anders dan eenmanszaken, die gebruik maken van de diensten van een fiscaal dienstverlener waarbij die dienstverlener via M2M interactie met de Belastingdienst communiceert;
2. beperkte werkingssfeer: het register is alleen bedoeld voor het registreren van machtigingen van bedrijven aan hun fiscaal dienstverlener om namens hen elektronische belastingaangiftes bij de Belastingdienst in te dienen (M2M). Het is niet mogelijk machtigingen voor diensten van andere overheidsdienstverleners vast te leggen;
3. beperkte functionaliteit: in het register legt het bedrijf alleen horizontale enkelvoudige machtigingen vast, van een bedrijf naar een fiscaal dienstverlener (RSIN naar RSIN). In theorie kan een RSIN-bedrijf gebruik maken van een 'klein' administratiekantoor dat een eenmanszaak is. Dus ook RSIN naar BSN moet mogelijk zijn in het publieke register. Bij DigiD Machtigen is de belanghebbende altijd een BSN, bij het in dit kader besproken register is de belanghebbende altijd een RSIN. Het is verder niet mogelijk meervoudige machtigingen vast te leggen. Tenslotte hebben de machtigingen in het register een zogenoemd doorlopend karakter (zijn dus niet éénmalig);
4. in lijn met eerdere adviezen van de commissie: bij het beheer van de machtigingen door de belanghebbende in het publieke register gebruikt het bedrijf voor identificatie en authenticatie een eHerkenningsmiddel. Het gebruik van DigiD is uitgesloten;
5. het register conformeert zich aan het afsprakenstelsel eHerkenning (het communiceert met eHerkenningspartijen op dezelfde wijze als private machtigingsregisters dat doen en gebruikt dus dezelfde koppelvlakken op dezelfde wijze);
6. de Belastingdienst draagt zelf zorg voor de ontwikkeling en exploitatie van het publieke machtigingsregister;
7. toetsing: twee jaar na ingebruikname van het publieke machtigingsregister evalueren het ministerie van EL&I en de Belastingdienst of deze specifieke publieke voorziening in stand moet blijven. Hierbij wordt aan de markt-en-overheidsvoorschriften getoetst. Criteria als "gebruik van de publieke voorziening" en "beschikbaarheid van alternatieven in de markt" komen in deze evaluatie expliciet aan de orde. Als de toets uitwijst dat het nodig is het register in stand te houden vindt periodiek hertoetsing plaats. Indien de toets op dat punt negatief uitvalt, wordt het register afgebouwd en beëindigd.

De commissie sluit niet uit dat het, tijdens de verdere implementatie van eHerkenning, nodig kan zijn andere transitievoorzieningen te treffen. De voorwaarde daarbij moet zijn dat de transitievoorziening een bijdrage levert aan een beheerste ontwikkeling in de richting van de eindsituatie (en dus niet blokkerend werkt voor het bereiken daarvan). In relatie daarmee wijst de commissie nog op het volgende: publieke (transitie)voorzieningen zullen moeten worden getoetst aan de markt-en-overheidsvoorschriften, die stellen dat de overheid geen oneerlijke concurrentie mag plegen jegens marktpartijen. Indien de markt niet voorziet in een bepaalde faciliteit kan de overheid daarin voorzien. Ook dient de overheid haar dienstverlening op basis van kostprijs af te rekenen. De eigenaar van de (transitie)voorziening is er verantwoordelijk voor dat de voorziening past binnen de kaders van de wet.

Samengevat adviseert de commissie met betrekking tot horizontale machtigingen om:

1. aansluitend bij het hiervoor verwoorde advies over DigiD, ook voor het registreren van machtigingen het perspectief van het bedrijf centraal te stellen;
2. voor de eenmanszaak een publieke basisvoorziening met beperkte functionaliteit beschikbaar te stellen, als laagdrempelige voorziening;
3. daarvoor concreet de bestaande voorziening DigiD Machtigen te gebruiken;
4. alle andere bedrijven hun machtigingen te laten registreren in private machtigingsregisters binnen het stelsel eHerkenning of bedrijfseigen voorzieningen die aan het stelsel worden gekoppeld;
5. de Belastingdienst (maar eventueel ook andere partijen met relevante inhoudelijke argumenten) toe te staan om met een transitievoorziening in hun behoefte te voorzien, mits die transitievoorziening voldoet aan de randvoorwaarden zoals hierboven genoemd;
6. op termijn van 2 à 3 jaar te evalueren of de publieke voorziening nog noodzakelijk is. Criteria als 'gebruik van de publieke voorziening' en 'beschikbaarheid van alternatieven in de markt' dienen daarbij te worden gebruikt.

Op deze manier wordt op korte termijn een duidelijke verbinding gelegd tussen de twee bestaande stelsels, doordat de eenmanszaak zowel met DigiD/DigiD Machtigen als eHerkenning kan en mag werken. Op langere termijn ontstaat er één homogeen stelsel waarin één set van standaarden wordt gebruikt voor toepassing in zowel het publieke als het private domein.

Daarnaast roept de commissie de marktpartijen op om:

1. duidelijkheid te verschaffen over de daadwerkelijke kosten van het raadplegen van de machtigingsregisters en daarvoor waar mogelijk te werken met vaste, voorspelbare tarieven (niet per raadpleging, maar per periode).
2. machtigingsvoorzieningen te ontwikkelen met toegevoegde waarde voor ondernemers, die op (korte) termijn de publieke voorziening overbodig maken.

6. Deelopdracht 2: Kwaliteit en continuïteit

Op 3 september 2011 om 01.00 uur gaf de Minister van Binnenlandse Zaken een persconferentie waarin hij mededeelde dat het Rijk het vertrouwen in het bedrijf Diginotar opgezegd had. De reden voor die opzegging was een onderzoek naar de mogelijke compromittering van het uitgifteproces van certificaten op betrouwbaarheidsniveau 4, waaronder de PKI-Overheidscertificaten. Door die compromittering was het niet meer mogelijk op deze certificaten te vertrouwen bij communicatie met burgers (via webdiensten) en bij machine-machine-communicatie. Het opzeggen van het vertrouwen maakte het voor overheidsorganisaties noodzakelijk om alle certificaten van Diginotar die zij in hun applicaties gebruikten te vervangen door certificaten van andere leveranciers.

Eerder in dit rapport benoemde de commissie al een aantal ontwikkelingen, waaronder die rond cybercriminaliteit. In de eerdere beschrijving ging het met name om criminaliteit in individuele gevallen. In contrast daarmee is de Diginotar-problematiek een voorbeeld van de wijze waarop (een deel van) de infrastructuur voor elektronische dienstverlening uit kan vallen. Een dergelijke uitval kan twee soorten problemen veroorzaken:

- op de korte termijn is het niet meer mogelijk om veilig elektronische diensten van de overheid af te nemen, de elektronische overheid valt stil. Dat betekent dat burgers, bedrijven en overheidsdienstaanbieders over moeten stappen op het gebruik van formulieren en post;

- incidenten als de situatie rondom Diginotar ondermijnen het fundamentele vertrouwen van burgers en bedrijven in het elektronisch zakendoen met de overheid. Dat kan leiden tot de keuze om zaken met de overheid voortaan weer op papier af te handelen.

Naar aanleiding van deze recente incidenten heeft de commissie zich afgevraagd welke aanvullende maatregelen nodig zijn om de continuiteits- en kwaliteitsrisico's van het stelsel voor eindgebruikers en overheidsdienstaanbieders acceptabel te maken, zodat zij over kunnen en zullen gaan tot implementatie van eHerkenning. De commissie realiseert zich dat de onderzoeken, die zijn opgestart om de Diginotar-problematiek te evalueren in relatie tot de betrouwbaarheid en de veiligheid van digitale dienstverlening aan bedrijven, nog niet zijn afgerond.[6] Toch beschouwt de commissie het als deel van haar opdracht om aan te geven wat de Diginotar problematiek betekent voor digitaal zaken doen in het algemeen en voor eHerkenning in het bijzonder. Dit is een brede en wederkerige vraag: als een overheid of ondernemer die eHerkenning gebruikt, de beveiliging niet op orde heeft of onzorgvuldig omgaat met middelen, kunnen daar incidenten uit voorkomen die afstralen op het authenticatie– en autorisatiestelsel als geheel.

Ten aanzien van digitaal zaken doen in het algemeen vindt de commissie dat het besef moet groeien dat overheidsorganisaties en eindgebruikers moeten zorgen dat de veiligheid van hun systemen (infrastructuur en processen) in overeenstemming moet zijn met de eisen die hun primaire proces stelt. Overheidsdienstaanbieders moeten daarom allereerst het vereiste veiligheids- en betrouwbaarheidsniveau van hun (primaire) processen bepalen, aan de hand van een risicoanalyse (waarin aspecten als rechtsgevolgen, financiële gevolgen en gevoeligheid van de uit te wisselen gegevens een rol spelen). Voor het uitvoeren van een dergelijke risicoanalyse is inmiddels een Handreiking Betrouwbaarheidsniveau's beschikbaar.

Dat gezegd hebbende, realiseert de commissie zich dat daar waar authenticatie en autorisatie van bedrijven nodig is, het per definitie gaat om kritische processen bij overheidsdienstaanbieders. Dat leidt om te beginnen tot de eis dat eHerkenning veilig te gebruiken moet zijn voor overheidsdienstaanbieders en eindgebruikers. Concreet: er moeten maatregelen genomen worden om zowel de criminaliteit in individuele gevallen (gebruik maken van een werkend stelsel) als de uitval van delen van de infrastructuur voor de elektronische overheid maatregelen te voorkomen,

[6] Kamerbrief 26643-189

om zo de daling in het vertrouwen van burgers en bedrijven in de (elektronische) overheid tot staan te brengen dan wel te keren. Toegespitst op eHerkenning betekent dit het volgende:

1) fraude in individuele gevallen

Bij fraude in individuele gevallen gaat het om het aannemen van de identiteit van een ander bedrijf om hiermee namens die onderneming elektronisch zaken te doen, met de overheid en/of met andere bedrijven; of om het creëren van een nieuw bedrijf met een eigen identiteit, om die te gebruiken om geld en/of goederen te verkrijgen van de overheid en/of andere bedrijven en die daarna te verduisteren.

Het voorkomen van dergelijke fraudes stelt om te beginnen hoge eisen aan het uitgifteproces en de gebruikte techniek van middelen. eHerkenning kent, in navolging van de Europese concept STORK standaards, vier niveau's van betrouwbaarheid. Bij uitgifte van middelen wordt het uitgifteproces zwaarder als de betrouwbaarheid van het uit te geven middel toeneemt.

Overheidsdienstaanbieders moeten verder voor al hun diensten vaststellen welk niveau van betrouwbaarheid zij voor het gebruik van die diensten vereisen. Diensten die rechtsgevolgen en/of financiële consequenties hebben behoeven betrouwbaarheidsniveau 3 of 4 (zie Handreiking Betrouwbaarheidsniveau's, zoals opgesteld in samenwerking met het Forum Standaardisatie).

Deze voorzorgsmaatregelen beperken het risico van misbruik of oneigenlijk gebruik van middelen maar heffen dat risico niet helemaal op. Dat betekent dat overheidsdienstaanbieders te maken kunnen krijgen met pogingen authenticatiemiddelen te "misbruiken". Het lastige daarbij is dat e-diensten in principe 7 x 24 uur beschikbaar zijn. Dat maakt het voor kwaadwillenden mogelijk misbruik van middelen te maken op momenten dat de kantoren van de betrokken overheids-dienstaanbieder gesloten zijn. Dat maakt de kans op succesvol misbruik groter.

In eerste instantie is het aanpakken van dit misbruik een rol bij de overheidsdienstaanbieder ligt (net als in de huidige papieren situatie), die kan besluiten om iemand niet langer toegang te verschaffen tot een dienst. Gaat het niet om misbruik van de dienst, maar om misbruik van het stelsel, dan moet het mogelijk zijn verdergaande ingrepen 24 uur per dag en 7 dagen per week uit te laten voeren. Naar de mening van de commissie leidt 7 x 24 uur dienstverlening dan ook tot de noodzaak om het mogelijk te maken middelen 7 x 24 uur buiten werking te kunnen stellen.
Er moet dan dus één punt komen, waar je het hele stelsel aan kunt spreken. Eén van de concrete maatregelen zou kunnen zijn dat in het stelsel een helpdesk wordt ingericht die "à la minute" en "7 x 24" kan reageren op meldingen van misbruik en de daarbij gebruikte middelen direct ongeldig kan verklaren.

Een zorgvuldige authenticatie en autorisatie van bedrijven, inclusief de hierboven genoemde maatregelen leidt tot een stevige 'voordeur' bij de overheidsdienstaanbieder, maar ook 'de achterdeur en het kelderraam' moeten veilig zijn. DigiD kent daarom aansluitvoorwaarden voor overheidsdienstaanbieders, waarin de eisen aan de overheidsdienstaanbieder worden verwoord. Het ligt voor de hand dergelijke aansluitvoorwaarden ook bij eHerkenning te gebruiken.

2) uitval van delen van de infrastructuur

Uit het Diginotar-incident leren we dat schijnbaar geïsoleerde incidenten in de infrastructuur voor elektronische communicatie ingrijpende consequenties kunnen hebben voor de primaire processen van publieke organisaties. Concreet: het primaire proces kan stil komen te liggen als gevolg van het feit dat:

- browsers het webportaal van de dienstaanbieder niet meer vertrouwen (SSL-certificaten);

- elektronische communicatie tussen servers niet meer mogelijk is (PKI-certificaten) .

Een dergelijke situatie kan zich ook in eHerkenning voordoen als één van de marktpartijen (die één of meer van de verschillende rollen uitvoert) in ongerede raakt. Dat heeft niet alleen consequenties

voor overheidsdienstaanbieders. In zo'n situatie krijgen bedrijven namelijk te maken met het feit dat de door hen aangeschafte middelen en/of de door hen vastgelegde machtigingen "waardeloos zijn geworden". Dat betekent dat zij geen elektronische diensten van de overheid meer kunnen afnemen.

eHerkenning is een cruciaal onderdeel van de infrastructuur voor elektronische dienstverlening aan bedrijven. Naar de mening van de commissie is de kernvraag 'welke aanvullende maatregelen in en rond het stelsel moeten worden genomen om de continuïteits- en kwaliteitsrisico's van het stelsel voor eindgebruikers en overheidsdienstaanbieders beheersbaar te maken zodat zij over kunnen gaan tot implementatie en acceptatie van het stelsel'.

Concreet gaat het om de volgende maatregelen:

- overheidsdienstaanbieders moeten eenduidig en onderbouwd vaststellen wat het vereiste betrouwbaarheidsniveau van hun elektronische diensten is (zie ook onderdeel 1) hierboven. Daar is aangegeven dat de eisen aan het betrouwbaarheidsniveau in overeenstemming moeten zijn met de gevolgen die het primaire proces kan hebben (rechtsgevolg, financieel gevolg, aard van de verwerkte gegevens). Hier kan de eerder genoemde Handreiking Betrouwbaarheidsniveaus voor worden gebruikt;

- bij cruciale onderdelen van de infrastructuur, ook wel "single points of failure" (SSL- en PKI-certificaten, maar ook de Herkenningsmakelaar, die de verbinding is tussen het stelsel en de overheidsdienstaanbieder), moet de overheidsdienstaanbieder er voor zorgen dat minstens twee aanbieders zijn gecontracteerd, zodat bij uitval van één aanbieder de elektronische diensten "in de lucht blijven";

- overheidsdienstaanbieders moeten zich goed beraden op de "service levels" die zij in "Service Level Agreements (SLA's)" overeenkomen. Het gevaar is er in gelegen dat men bij het afsluiten van een SLA kiest voor de laagste prijs. Het risico van een dergelijke keuze is dat men in geval van calamiteiten zeer beperkte, dan wel geen ondersteuning van de leverancier krijgt. Dat is geen gewenste situatie gezien de afhankelijkheid van de primaire processen van de overheidsdienstaanbieders van het stelsel;

- uitgevers van middelen en de beheerders van machtigingenregisters spelen een cruciale rol in het stelsel. Op basis van hun registraties nemen overheidsdienstaanbieders beslissingen om bedrijven wel of geen gebruik te laten maken van hun diensten (dan wel, zij leveren vertrouwen). Het is daarom noodzakelijk dat de procedures die zij hanteren voor het beheer van middelen en registraties:
    - zeer gedetailleerd zijn voorgeschreven;
    - toetsbaar zijn aan de hand van een door de beheerorganisatie vastgesteld normenkader;
    - frequent getoetst worden op de aspecten opzet, bestaan en werking (dit toezicht is dus inhoudelijk gericht en moet leiden tot een zogenoemde Third Party Mededeling die voldoet aan de daarvoor geldende standaarden (zoals SAS70)), aan de hand waarvan de afnemers kunnen vaststellen dat de betrokken aanbieder nog aan de eisen rond veiligheid en continuïteit voldoet, waarbij deze toetsing
        - gecombineerd wordt met een (anonieme) meldplicht, waardoor inbreuken op de veiligheid direct helder worden en de nodige maatregelen in gang gezet kunnen worden;
        - over de toetsing rapportage plaatsvindt naar de beheerorganisatie van het stelsel.

- in het verlengde daarvan moet er worden gehandhaafd, dat wil zeggen dat
  a. in de contracten tussen beheerorganisatie en leveranciers het voorgaande rond toetsen, Third Party Mededeling en meldingsplicht wordt vastgelegd;
  b. de bevoegdheid om sancties (bijvoorbeeld schorsing of uitzetting uit het stelsel) op te leggen in geval van het niet nakomen van deze afspraken wordt neergelegd bij de beheerorganisatie;

c. de beheerorganisatie ook daadwerkelijk gevolgen verbindt aan de uitkomsten van de jaarlijkse toetsing dan wel een incidentele melding en sancties daadwerkelijk ten uitvoer legt.

De commissie realiseert zich dat een dergelijk intensief toezicht leidt tot hogere kosten van het stelsel en daarmee van hogere kosten voor overheidsdienstaanbieders en/of eindgebruikers. Het belang van veiligheid en betrouwbaarheid weegt echter zwaarder dan de extra kosten die dit toezicht met zich meebrengt.

Dan geeft de commissie nog drie meer algemene overwegingen. De eerste is de optie om het stelsel eHerkenning te benoemen tot onderdeel van de nationale kritische ICT-infrastructuur. In het licht hiervan verdient het ten tweede aanbeveling om het beheer van het afsprakenstelsel eHerkenning vast te leggen als een Dienst van Algemeen Economisch Belang. De derde is te overwegen aan te sluiten op de praktijk in de VS, waar bij aanbestedingen ook de nummer 2 aanbieder in de markt wordt gehouden, zodat er een alternatieve optie beschikbaar blijft.

7. Deelopdracht 3: Implementatiestrategie

Het advies van Ecorys over het financieringsmodel (zie Bijlage 2) benadrukt dat snelle groei van het gebruik een cruciale succesfactor voor eHerkenning is. Daarbij merkt Ecorys op dat de markt voor eHerkenning een tweezijdige markt is, in die zin dat partijen aan beide zijden van de markt, dus bedrijven én overheidsdienstaanbieders, beiden in voldoende mate toe moeten treden om de markt volwassen te maken. Tot de markt volwassen is spreekt Ecorys van een groeifase. Het dringende advies van Ecorys is deze groeifase zo kort mogelijk te maken, om zo de baten van de introductie van eHerkenning maximaal te maken.

Een kenmerk van tweezijdige markten is dat daar netwerkeffecten optreden. Ecorys illustreert dat met het voorbeeld van mobiele telefonie, waarbij het gebruiksnut van een mobiele telefoon meer dan evenredig toeneemt met een stijging van het aantal mobiele telefoons dat in omloop is.

Dat netwerkeffect treedt ook in de markt voor eHerkenning op. Als overheidsdienstaanbieders snel nieuwe elektronische diensten aanbieden leidt dit ertoe dat ondernemers middelen aanschaffen en machtigingen registreren, wat het voor andere overheidsdienstaanbieders aantrekkelijker maakt om ook elektronische diensten te ontwikkelen die met die middelen te ontsluiten zijn, wat weer leidt tot extra vraag naar middelen, enzovoorts.

De keerzijde van het netwerkeffect is dat elektronische dienstverlening uitblijft omdat de ondernemers niet beschikken over authenticatiemiddelen die nodig zijn voor de toegang tot deze diensten. De ondernemer zal op zijn beurt alleen bereid zijn om te betalen voor een authenticatiemiddel wanneer dit toegang geeft tot meerdere elektronische diensten. Dit 'kip –ei-probleem' kan alleen doorbroken worden door beide zijden van de markt tegelijkertijd tot ontwikkeling te brengen.

Gegeven deze analyse van Ecorys ziet de commissie een aantal mogelijkheden om deze snelle groei te bevorderen:

a) Creëer toepassingen die snelle groei bevorderen

De overheid biedt een veelheid aan diensten aan. Lang niet ieder bedrijf maakt van al die diensten gebruik, maar er is een beperkt aantal diensten die bedrijven nu al op grote schaal gebruiken. Als de overheid deze diensten elektronisch beschikbaar zou stellen en het daarnaast mogelijk maakt om eHerkenning te gebruiken om toegang tot deze diensten te krijgen wordt daarmee een sterke prikkel gecreëerd voor de snelle groei van de markt rond eHerkenning.

De commissie ziet drie diensten die een dergelijke rol kunnen spelen:

- *Aanvragen Verklaring Omtrent het Gedrag*
In een aantal sectoren is het verplicht (taxibranche) dan wel zeer gewenst (vrijwilligerswerk) om voor iemand aan de slag gaat voor deze persoon een Verklaring Omtrent het Gedrag (VOG)aan te vragen.

Inmiddels heeft de dienst Justis (ressorterend onder het Ministerie van Veiligheid en Justitie) vanaf juli 2010 een proef uitgevoerd met het via het internet aanvragen van een VOG. Door deze digitale dienst hoeven gemeenten geen gegevens meer in te voeren, voor aanvragende bedrijven is het goedkoper (in Euro's). De proef is succesvol afgesloten. Daarom is in de eerste helft van 2011 een wetsvoorstel over het elektronisch aanvragen naar de Tweede Kamer gestuurd. De Tweede Kamer en de Eerste Kamer hebben dit wetsvoorstel aangenomen en de verwachting is dat het elektronisch aanvragen van een VOG vanaf januari 2012 voor iedereen beschikbaar is.

Voor het elektronisch aanvragen van een VOG moet een aanvrager zich identificeren bij het portaal van dienst Justis. In de proef is dit gebeurd met eHerkenning. Als dienst Justis het vanaf

begin 2012 voor bedrijven en rechtspersonen mogelijk maakt de VOG elektronisch aan te vragen met eHerkenning ontstaat (ook hier) een prikkel voor de aanschaf van een eHerkenningsmiddel.

- *Muteren gegevens Kamer van Koophandel*
De Kamer van Koophandel beheert het Handelsregister, dat informatie bevat over alle bedrijven en rechtspersonen in Nederland. Bij de oprichting van een bedrijf vindt registratie van het bedrijf in het register plaats.

De Kamer van Koophandel heeft drie rollen ten opzichte van eHerkenning:
1) het RSIN (en voor sommige organisaties het KvK-nummer) vormt voor Nederlandse bedrijven hét herkenningsnummer en de basis voor eHerkenning.
2) het Handelsregister is het "moederregister" voor machtigingen en moet als zodanig geraadpleegd kunnen worden door machtigingenregisters;
3) als overheidsdienstaanbieder kan de KvK de eigen dienstverlening aan bedrijven ontsluiten met eHerkenning.

De tweede rol is uitgewerkt in hoofdstuk 5, advies 2. Met betrekking tot de derde rol vindt de commissie het belangrijk dat de KvK-diensten ontsloten worden met eHerkenning, omdat het diensten zijn waar veel bedrijven gebruik van maken.

Gedurende de levensloop van het bedrijf kunnen de gegevens van het bedrijf veranderen. Die verandering moet het bedrijf ook aan de Kamer van Koophandel opgeven, zodat die de wijziging in het Handelsregister kan verwerken.

De wijzigingen vallen uiteen in twee soorten:
- relatief eenvoudig, zoals wijziging van vestigingsadres of contactgegevens;
- complex, zoals wisseling van bestuurders of een overname.

De Kamer van Koophandel streeft ernaar om het mogelijk te maken deze wijzigingen door te geven via het internet. In dit kader zijn de ontwikkelingen rond het Ondernemingsplein relevant. Zie in dit kader de brief van de minister van EL&I gedateerd 13 oktober 2011 aan de Tweede Kamer, waarin hij het volgende aangeeft: "Essentieel is verregaande digitalisering van de dienstverlening." Het moge helder zijn dat het betrouwbaarheidsniveau voor de relatief eenvoudige mutaties (veel) lager kan zijn dan voor de meer ingrijpende wijzigingen. Dat betekent dat partijen die een identificatiemiddel gebruiken met een relatief lage betrouwbaarheid alleen eenvoudige mutaties kunnen doorgeven. Het gaat hier desondanks om grote aantallen wijzigingen.

Als de Kamer van Koophandel het mogelijk maakt dat bedrijven en rechtspersonen zich bij het doorgeven van wijzigingen identificeren met eHerkenning ontstaat (ook hier) een prikkel voor de aanschaf van een eHerkenningsmiddel.

De Kamer van Koophandel kan overigens nog een heel andere rol spelen in het bevorderen van de snelle groei van het stelsel. Bij de start van een nieuw bedrijf vindt inschrijving daarvan in het register van de Kamer van Koophandel plaats. Dit gebeurt veelal ten kantore van de Kamer. Het moment van inschrijven is heel geschikt om de ondernemer de mogelijkheid te bieden ter plekke een eHerkenningsmiddel aan te schaffen (de Kamer moet dan zowel informatiemateriaal als aanvraagformulieren van alle aanbieders beschikbaar hebben).

- *Indienen aangiftes bij de Belastingdienst*
De Belastingdienst geeft prioriteit aan het SBR-programma (met name omdat 85% van de aangiftes al digitaal bij de Belastingdienst binnenkomt) en zal via dat programma aansluiten op de ontwikkeling van het machine2machine kanaal van eHerkenning. Daarnaast heeft de Belastingdienst voor het online kanaal het programma MijnBelastingdienst in ontwikkeling genomen. Deze portaalvoorziening zal zowel burger- als bedrijf-gerelateerde diensten aanbieden, waarbij de eerste prioriteit wordt gegeven aan burgergerelateerde diensten. Voor dit programma is nog geen invoeringsjaar bepaald (2013 of later). In de ontwikkeling van het project wordt in de ontwerpfase aangesloten op de GOA-standaarden en het voorziene gebruik van het stelsel

eHerkenning. De publiek beheerde machtigingsvoorziening die door de Belastingdienst wordt ingericht (zie advies 2 in hoofdstuk 5), zal worden ontsloten met eHerkenning (voor het beheer van de machtigingen gebruikt het bedrijf eherkenning). Daarmee is deze voorziening ook een grootschalige toepassing van eHerkenning.

b) Maak bestaande diensten geschikt voor eHerkenning

Naast de voornoemde drie genoemde grootschalige diensten stellen overheidsorganisaties nog een aantal elektronische diensten voor ondernemers beschikbaar. Deze organisaties gebruiken daarbij eigen oplossingen voor identificatie en authenticatie (leidend tot een "digitale sleutelbos voor ondernemers").

Om het gebruik van eHerkenning te bevorderen adviseert de commissie om deze diensten niet alleen toegankelijk te maken met de voornoemde eigen oplossingen maar ook met eHerkenning (tweede sleutel). Zo snijdt het mes aan twee kanten:
- bedrijven die al gebruik maken van eHerkenning ervaren een groeiend gebruiksnut van de door hen aangeschafte middelen en vastgelegde machtigingen, wat een positieve impuls geeft aan het eerder beschreven netwerkeffect;
- de betrokken organisaties hoeven hun eigen oplossingen niet direct uit te faseren, welke uitfasering het risico met zich mee zou kunnen brengen dat klanten terugvallen op formulieren.

Deze werkwijze vergt overigens niet alleen een aanpassing in de dienst zelf maar noodzaakt de betrokken organisatie ook om een contract te sluiten met een Herkenningsmakelaar.

Voor toepassingen rond gemeentelijke dienstverlening moet onderzocht worden hoe de toekomstige eHerkenningsvoorziening gebruikt kan worden voor de diversiteit aan processen die een gemeente kent. De POC's die zijn uitgevoerd in het kader van GOA kennen namelijk een beperkte scope (focus op Rijk en op uitvoering/Belastingdienst). Daarmee is de opgedane ervaring te beperkt om ongeclausuleerd tot brede implementatie van eHerkenning in het gemeentelijk domein over te gaan.

De commissie ziet wel het grote potentieel aan diensten wanneer de gemeentelijke diensten met eHerkenning worden ontsloten. De commissie adviseert dan ook om in samenwerking met VNG en KING pilots uit te voeren met gemeenten om de bruikbaarheid van eHerkenning in de gemeentelijke praktijk te beproeven. Hierdoor wordt direct draagvlak gecreëerd bij lagere overheden hetgeen een positief effect heeft op breder gebruik. Voor wat betreft het migratietempo is diezelfde diversiteit aan diensten en processen van (grote) gemeentelijke organisaties een aandachtspunt, dat in migratiescenario's en handreikingen voor gemeenten nader uitgewerkt zal moeten worden. Dit is belegd bij KING (Kwaliteitsinstituut Nederlandse Gemeenten) in het kader van het implementatieprogramma i-NUP.

c) Faseer eigen middelen op termijn uit

Het creëren van nieuwe diensten die met eHerkenning worden ontsloten en het openstellen van bestaande diensten voor eHerkenning zullen zorgen voor een impuls voor het gebruik van eHerkenning. Die impuls zal met name komen van nieuwe gebruikers van elektronische diensten. De ervaring bij de "launching customers" is dat bedrijven die gebruik maken van bestaande middelen (die door de overheidsorganisatie zijn uitgegeven) niet geneigd zijn om bestaande 'gratis' middelen te vervangen door eHerkenning waarvoor moet worden betaald. Dat behoeft een extra stimulans.

Die impuls is te vinden in de aankondiging dat de bestaande organisatiegebonden middelen op termijn, denk aan twee tot drie jaar, zullen verdwijnen. Zo'n termijn is ten eerste nodig om een robuust, veilig en stabiel stelsel te borgen (zie hoofdstuk over continuïteit en kwaliteit) en de markt voor middelen en diensten op gang te brengen. Bovendien geeft een vroegtijdige aankondiging bedrijven de mogelijkheid om op een door hen gekozen moment een eHerkenningsmiddel aan te schaffen, het hoeft niet onmiddellijk. Een dergelijke werkwijze voorkomt het risico dat bedrijven er op korte termijn voor kiezen af te zien van het gebruik van elektronische diensten en dat zij de

stap terug naar formulieren maken. Aan de andere kant maakt het stellen van een termijn de aanschaf van een eHerkenningsmiddel onontkoombaar. De aanschaf van dat middel wordt met het verstrijken van de tijd ook aantrekkelijker omdat steeds meer elektronische diensten beschikbaar komen die met behulp ervan zijn te gebruiken.

Deze stimulans kan worden geconcretiseerd door aan te sluiten bij een 'recht op elektronisch zakendoen'. In de Digitale Agenda.nl is aangekondigd dat het Kabinet bedrijven het recht wil geven om alle zaken met de overheid langs elektronische weg af te handelen. Momenteel loopt daartoe een verkenning. Een dergelijk recht vergt naar de mening van de commissie dat wettelijk vast wordt gelegd dat overheidsdienstaanbieders uitsluitend generieke, gestandaardiseerde voorzieningen voor authenticatie en autorisatie gebruiken. Naast eHerkenning zijn dat dus ook de interoperabele buitenlandse elektronische handtekeningen en authenticatiemiddelen, zoals in EU-verband is en wordt afgesproken. Buitenlandse ondernemers moeten met gebruik van eigen middelen zaken kunnen doen met Nederlandse overheden.

Het spiegelbeeld van het recht op elektronisch zakendoen is de verplichting voor bedrijven om zaken elektronisch met de overheid af te handelen. Zo is het voor bedrijven verplicht elektronisch met de Belastingdienst te communiceren. De commissie adviseert om te bezien of op termijn andere overheidsdienstaanbieders dan de Belastingdienst ook een dergelijke verplichting in kunnen voeren.

d) Maak de kosten van middelen inzichtelijk en help bedrijven met kiezen

De markt voor eHerkenning is op dit moment klein. Bedrijven die geen gebruik maken van eHerkenning beschikken over weinig informatie over zowel de werking van het stelsel als zodanig als over de kosten die het stelsel voor hen meebrengt.

Om te beginnen leidt dit tot foutieve beelden over de kosten die gebruik van eHerkenning met zich meebrengt. Veel ondernemers identificeren eHerkenning met middelen op betrouwbaarheidsniveau 4, waarvan de kosten kunnen oplopen tot € 300,-- per jaar. Voor veel kleine bedrijven is dit een te groot bedrag, wat hen ervan zal weerhouden een middel aan te schaffen.

Verder blijkt uit de ervaringen van de eerste overheidsdienstaanbieders die eHerkenning gebruiken dat bedrijven moeite hebben door de bomen van eHerkenning het bos nog te onderscheiden. Concreet, men vindt het kiezen van het juiste middel heel lastig en is bang dat men een verkeerde keuze maakt, die grote financiële consequenties kan hebben (men baseert zich in dit kader op de ervaringen die men heeft opgedaan bij de introductie van mobiele telefonie, waar de eerste gebruikers veel te veel bleken te betalen, waar niet eenvoudig wat aan te doen was als gevolg van langjarige contracten en leveranciersgebondenheid ("SIM-locks")).

De commissie adviseert in het licht van het voorgaande om een langjarige communicatiecampagne rond eHerkenning te ontwikkelen. De nadruk daarbij moet liggen op de website eHerkenning.nl, die om te beginnen moet uitgroeien tot het portaal voor diegenen die vragen over eHerkenning hebben. Die vragen zullen in eerste instantie gericht zijn op wat het bedrijf precies moet kopen, en wat het betrouwbaarheidsniveau van het middel zou moeten zijn. In tweede instantie verschuift het vraagpatroon naar de middelen zelf, met vragen over kosten, dienstenniveau en looptijd van het contract. Het gericht beantwoorden van dergelijke vragen verlaagt de drempel voor ondernemers om daadwerkelijk tot eHerkenning toe te treden (vergelijk in dit verband de rol van eHerkenning.nl met het portaal dat het mogelijk maakte aanbiedingen van mobiele telefoonaanbieders te vergelijken).

e) Breng een tijdelijke geldstroom op gang van overheidsdienstaanbieders om de aanschaf van voldoende hoogwaardige private authenticatiemiddelen te stimuleren

Conclusies Ecorys
Op verzoek van het ministerie van EL&I heeft Ecorys onderzoek gedaan naar de financiering van eHerkenning. De samenvatting van het Ecorys rapport is opgenomen in bijlage 2 van dit rapport. Ecorys geeft aan dat de implementatie van eHerkenning gekenmerkt wordt door het bekende kip-ei

probleem: voor dienstaanbieders is het pas rendabel om diensten te ontsluiten met eHerkenning als er voldoende eindgebruikers zijn; voor eindgebruikers is het pas interessant om een middel aan te schaffen wanneer er voldoende digitale diensten zijn waarvoor het middel gebruikt kan worden. Dit kip-ei probleem bemoeilijkt de financiering en de implementatie van het stelsel. Ecorys stelt vast dat de financiering op middellange termijn (3 à 4 jaar, wanneer er sprake is van een volwassen stelsel) relatief eenvoudig is, omdat er dan genoeg gebruikers zijn die voor de middelen en diensten willen betalen, zeker als het B2B gebruik op gang is gekomen. De moeilijkheid zit in de fase daarvoor, wanneer het stelsel een snelle groei moet doormaken richting volwassenheid én er tegelijkertijd voor sommige partijen in het stelsel onvoldoende financiële prikkels zijn om in te stappen en zo die groei te realiseren.

Ecorys heeft becijferd dat de totale kosten voor het stelsel in de eerste jaren ongeveer 2 tot 4 miljoen Euro per jaar bedragen. Tegenover deze financieringsbehoefte staat de financieringsruimte. Deze is in beginsel voldoende groot, de baten voor overheidsdienstverleners groeien van 0 naar 8 miljoen Euro per jaar en de baten voor bedrijven groeien van 0 naar 5 miljoen Euro per jaar. De kosten gaan echter voor de baat uit. Zeker voor bedrijven (die werken met een korte investeringshorizon) is een investering in eHerkenningsmiddelen niet binnen de gewenste periode terugverdiend. Uit zichzelf zullen bedrijven dan ook niet snel eHerkenningsmiddelen aanschaffen. En dat betekent, aldus Ecorys, dan eHerkenning niet in een volwassen fase terecht komt.

Er moet dus iets gebeuren om eHerkenning van de grond te krijgen, waarbij het uitgangspunt moet zijn om zo snel mogelijk van de groeifase in de volwassenheidsfase te komen, waarbij het stelsel zichzelf kan bedruipen. Ecorys geeft aan dat –gezien het 'kip-ei karakter' van de markt- er twee dingen moeten gebeuren:
1) stimuleren van het aanbod van eHerkenningsdiensten door overheidsdienstverleners en
2) stimuleren van gebruik van eHerkenningsmiddelen door bedrijven.
De implementatiestrategie zoals in dit advies tot nu toe beschreven, richt zich op het eerste: een aantal digitale overheidsdiensten die door veel ondernemers worden gebruikt, ontsluiten met eHerkenning en het gebruik van eHerkenning als tweede sleutel. De vraag is hoe het gebruik door eindgebruikers op gang gebracht kan worden.

Wijze van stimuleren
Ecorys suggereert drie manieren om eindgebruikers te stimuleren om eHerkenningsmiddelen aan te schaffen en te gebruiken. Ten eerste dwang: door gebruik van eHerkenning te verplichten worden alle kosten voor eHerkenningsmiddelen in de groeifase gedragen door de eindgebruiker/het bedrijfsleven. Zij verdienen die investering op langere termijn wel weer terug. De commissie vindt deze optie niet haalbaar. Een tweede optie is volgens Ecorys het hergebruik van bankmiddelen: daardoor dalen de totale kosten van het stelsel en is daarmee de totale financieringsbehoefte lager. Bedrijven hebben over het algemeen een dergelijk bankmiddel al. Deze optie is echter afhankelijk van het toetreden van banken tot het stelsel, de commissie vindt dat het succes van het stelsel daarvan niet afhankelijk gemaakt kan worden. Blijft over de derde optie: het subsidiëren van de aanschaf van eHerkenningsmiddelen, direct (via de eindgebruiker) of indirect (via marktpartijen). Ecorys becijfert dat een totale subsidiebijdrage van tussen de 1 en de 2 miljoen Euro ervoor zou kunnen zorgen dat meer dan 100 duizend bedrijven op korte termijn overgaan op eHerkenning. De commissie is van mening dat het op gang brengen van deze geldstroom van overheidsdienstaanbieders noodzakelijk is en adviseert om te zoeken naar manieren om deze geldstroom op gang te brengen. Voorbeelden van dergelijke stimuleringsmaatregelen zijn:
- subsidie aanvraag via AgentschapNL door de eindgebruiker, die inlogt met het aangeschafte authenticatiemiddel (daarmee wordt bewezen dat een middel ook daadwerkelijk is aangeschaft);
- subsidiering van middelenuitgevers en machtingenregister-houders, die dan de middelen per saldo gratis aan bedrijven ter beschikking kunnen stellen.

In navolging van Ecorys raadt de commissie daarbij aan te kiezen voor financiering vanuit een soort Algemeen Fonds, dat gevuld wordt met bijdragen van verschillende betrokken overheidsdienstverleners. Hiermee wordt voorkomen dat er voor overheidsdienstverleners een soort 'first mover disadvantage' ontstaat (de eerste die instapt, financiert de middelen voor de eindgebruiker en voor de andere overheidsdienstaanbieders), waardoor het benodigde aanbod niet

op gang komt. Financiering van middelen door overheidsdienstverleners ligt voor de hand omdat deze in de opstartfase het grootste profijt hebben van elektronische dienstverlening.

Deze stimulerende maatregelen moeten betrekking hebben op de aanschaf van voldoende hoogwaardige private authenticatiemiddelen (stimuleren aanschaf van authenticatiemiddelen van met name STORK-niveau 3 en eventueel 4). Dit betekent dat het accent van financiering wordt verlegd van STORK-niveau 1 middelen naar de hogere niveaus. De maatregelen moeten aan een aantal voorwaarden voldoen:
- de maatregel mag geen administratieve rompslomp opleveren, de afhandeling door de overheid moet simpel vormgegeven kunnen worden (anders spannen we het paard achter de wagen);
- de ondernemer houdt keuzevrijheid;
- de bijdrage moet gebaseerd zijn op een doorsnee middel en doorsnee gebruik daarvan (zodat het bedrijf zelf kan kiezen of hij wel of niet een duurder dan het doorsnee middel wil aanschaffen);
- de bijdrage moet de snelle aanschaf van middelen stimuleren (om de groeifase van eHerkenning zo kort mogelijk te houden), bijvoorbeeld door een plafond aan het voor subsidie beschikbare bedrag te stellen, zodat een stimulans ontstaat om snel over te gaan tot aanschaf.

Financiering van de groeifase
Wanneer de markt volwassen is, geldt de volgende redeneerlijn:

Om te beginnen worden de kosten voor inrichting en gebruik van het BSN-gerelateerde stelsel gedragen door de overheid.

Voor private (online) authenticatiemiddelen geldt verder het volgende:
- Aanschaf: voor eenmanszaken is het de eigen keuze om een dergelijk middel aan te schaffen en zijn de kosten geheel voor die eenmanszaak. Voor RSIN-gerelateerde authenticatiemiddelen zijn de kosten geheel voor het bedrijf;
- Gebruik: de overheid vereist voor elke online gebruiker een bepaalde kwalitatieve invulling van de private authenticatiedienst. Het is te verdedigen dat de overheid dan transactiekosten (deels) vergoedt (vergelijkbaar met de vergoeding die banken elkaar verstrekken bij het gastgebruik van een geldautomaat), ook al om dat de overheid geen investeringen meer hoeft te plegen in een eigen authenticatiedienst. Probleem met vergoeden per transactie, is dat onzeker is wat dat per jaar gaat kosten. Als er steeds meer wordt ingelogd, dan gaan de kosten sterk stijgen. Dat roept de wens op om 'vaste jaar staffels' (of "bundels") met de private authenticatiediensten te bepalen.

Waar het gaat om M2M-authenticatiemiddelen voor de private applicatiebeheerders (in GOA-termen de ApV, 'associatieproces verantwoordelijke') geldt dat deze partijen PKI-servicescertificaten gebruiken. De aanschaf hiervan valt geheel aan die dienstverlener. Op dit moment zijn er geen kosten per transactie gebonden aan het gebruik van een dergelijk certificaat.

Private machtigingsregisters: het is de eigen keuze van een belanghebbende om gebruik te maken van een gemachtigde. En als die machtiging is geregistreerd in een privaat machtigingsregister (al dan niet verplicht of eigen keuze), dan is het ook de gezamenlijke verantwoordelijkheid van belanghebbende en gemachtigde om een 'bevoegdheidsverklaring' aan te leveren, inclusief de kosten die hiermee samenhangen. De overheid draagt hieromtrent in een volwassen markt dus geen kosten.

Kosten Herkenningsmakelaar: de overheid kiest ervoor om gebruik te maken van private Herkenningsmakelaars. Elke overheidsdienstaanbieder zal dus een private Herkenningsmakelaar moeten kiezen (minimaal twee, zie eerdere opmerkingen naar aanleiding van de Diginotar-problematiek). De kosten voor de diensten van de Herkenningsmakelaar komen (natuurlijk) voor rekening van de overheidsdienstaanbieder. Afhankelijk van de omvang van de kosten, zal de verwerving van diensten van Herkenningsmakelaars via aanbestedingen plaats vinden en is reële marktwerking te verwachten.

De commissie brengt geen advies uit over de prijszetting richting de eindgebruikers (bedrijven) en ook niet over de interne verrekentarieven tussen partijen in het stelsel. Beide komen in het stelsel door marktwerking tot stand.

f) Hergebruik van eHerkenning binnen B2B (Business to Business), G2G (Government to Government) en (uiteindelijk) C2G (Consumer to Business) toepassingen

eHerkenning is in eerste instantie bedoeld voor gebruik door bedrijven bij het afnemen van diensten van de overheid. De opzet van het stelsel is echter zodanig dat het mogelijk is de gekozen oplossingen ook te gebruiken in andere domeinen. Het gaat daarbij met name om B2B (Business to Business, door bedrijven onderling) en G2G (Government to Government) toepassingen.

Ook in het B2B domein wordt een veilige voorziening voor authenticatie en authorisatie steeds belangrijker. Het toenemend aantal digitale transacties tussen bedrijven, en de afhankelijkheid en kwetsbaarheid daarvan, doet het besef groeien dat een goed digitaal slot op de deur noodzakelijk is. De trend om dat niet zelf te ontwikkelen en beheren, maar de voorzieningen in te kopen bij partijen die daarin gespecialiseerd zijn, is zichtbaar. Sterker nog, een deel van de marktpartijen die eHerkenningsdiensten aanbieden, zijn in die rol gegroeid vanuit het leveren van diensten op het gebied van authenticatie en autorisatie aan bedrijven of samenwerkingsvormen.
eHerkenning wordt dan ook voor veel bedrijven de manier om een voorziening voor authenticatie en autorisatie in huis te halen.

Het Ministerie van EL&I geeft aan dat voor daadwerkelijk B2B gebruik nog een beleidsbeslissing nodig is t.a.v. het accepteren van een zekere aansprakelijkheid voor fouten op stelselniveau.

De commissie beveelt B2B-hergebruik van eHerkenning aan. Dat heeft twee redenen. De eerste is dat bedrijven op deze manier de beschikking krijgen over één oplossing voor identificatie en authenticatie, ongeacht het domein waar zij actief zijn. Dat voorkomt dat zij twee maal moeten investeren in vergelijkbare functionaliteiten, namelijk voor communicatie met de overheid en communicatie met andere bedrijven. De tweede reden is dat door het toepassen van eHerkenning in het B2B domein het gebruik van middelen en machtigingsregister sterk in omvang toeneemt. Dat verkort de groeifase van het stelsel, verlaagt de prijs per eHerkenningstransactie en vermindert de afhankelijkheid van de groei van overheidsdienstverlening aan bedrijven. B2B-gebruik levert naar verwachting een belangrijke bijdrage aan de overgang van een gesubsidieerde oplossing naar een infrastructuur die zichzelf financieel bedruipt. De commissie adviseert dan ook om nog resterende barrières voor B2B gebruik op korte termijn te slechten en de markt de ruimte te geven om in dit domein actief te worden.

Het is echter ook zo dat grootschalig gebruik van eHerkenning door overheidsaanbieders een noodzakelijke voorwaarde en een enorme aanjager is voor gebruik in het B2B domein.
De commissie raadt aan om samen met een groot Nederlands bedrijf een B2B pilot te starten, waarbij zowel de makelaarsfunctie, de middelenfunctie als de machtigingen verder worden getest.

De commissie adviseert om ook in de governance van het stelsel zichtbaar te maken dat het stelsel een brede voorziening voor Nederland is en daarom B2B gebruikers zeggenschap te geven in de governance van het stelsel.

Een andere mogelijke verbreding van het toepassingsgebied van eHerkenning is verder gelegen in het domein van G2G toepassingen. In dat licht is het interessant dat gemeenten in het kader van medebewind[7] (delen van) regelingen van de hogere overheid uitvoeren. Hierdoor is de gemeente een spil in veel overheids(keten)processen vanuit het perspectief van burger en bedrijf. Kabinetsbeleid is om de komende jaren steeds meer uitvoering bij gemeenten neer te leggen. Het koppelvlak gemeente-Rijk is dus groeiende en eHerkenning zal op de G2G koppelvlak veelvuldig

---

[7] Medebewind` is de plicht van lagere overheden om medewerking te geven aan de uitvoering van regelingen van de hogere overheid.

gebruikt kunnen gaan worden. De commissie adviseert om het G2G gebruik aan te moedigen.

Er zijn twee mogelijke concrete toepassingen in het G2G domein in beeld (DigiD OEP en de Rijkspas); de commissie adviseert om hier werk van te maken, omdat ook deze toepassingen bij kunnen dragen aan een korte groeifase van het stelsel.

8. Randvoorwaarden

8.1 (Internationale) standaarden

Het stelsel eHerkenning kent is gebaseerd op een groot aantal standaarden:
a. internationaal aanvaarde standaarden die de basis vormen voor de technische inrichting (denk aan SAML 2.0 en XCAML);
b. gestandaardiseerde koppelvlakken tussen de rollen binnen het stelsel (zoals die voor de communicatie tussen Authenticatiediensten en Herkenningsmakelaars);
c. specifiek ontwikkelde standaarden, met doorwerking buiten het stelsel. Het gaat hier om
- het koppelvlak tussen het stelsel eHerkenning en de diensten van overheidsdienstverleners;
- de Nederlandse implementatie van de Stork betrouwbaarheidsniveaus.
d. specifiek ontwikkelde standaarden, die met name binnen het stelsel werken:
- het normenkader voor de inhoudelijke toets op de inrichting van de diverse voorzieningen binnen het stelsel;
- standaard contracten en standaard SLA's.

De standaarden onder b. en c. behoeven naar de mening van de commissie expliciet bekrachtiging in het College Standaardisatie, op aangeven van het Forum Standaardisatie. Vaststellling van deze standaarden voorkomt "vendor lock in" voor bedrijven en faciliteert tevens de toetreding van nieuwe marktpartijen tot het stelsel. Dat betekent dat het Ministerie van EL&I samen met de beheerorganisatie actie moet ondernemen om deze standaards aan te melden bij het Bureau Forum Standaardisatie.

De Beheerorganisatie stelt de standaarden onder d. vast. De vaststelling ervan vindt plaats door het bestuur van de Beheerorganisatie, op aangeven van de beheerorganisatie, in samenwerking met marktpartijen en overheidsdienstaanbieders. Het bestuur laat zich hierbij adviseren door experts op deze terreinen.

Het is verder van groot belang om de eherkenningsstandaarden in te brengen in Europese standaardisatieprojecten, onder meer om buitenlandse markten toegankelijk te maken en te houden voor Nederlandse bedrijven. [8]

Tenslotte behoeven "zachte standaarden", zoals het gebruik van logo's en beeldmerken, aandacht van de beheerorganisatie.

8.2 Toetreding tot en uittreding uit het stelsel

eHerkenning is, zoals eerder aangegeven, een open stelsel, waarin iedere private partij die dat wenst en aan de eisen voldoet mag toetreden. Dit geldt ook voor buitenlandse partijen. Daarnaast staat eHerkenning open voor hergebruik van bedrijfseigen middelen en machtigingsregister. Het een en ander is hieronder verder uitgewerkt.

Toetreding van een externe partij tot het stelsel
Als een partij de wens heeft toe te treden tot het stelsel kiest hij expliciet voor één of meer rollen die hij wil vervullen.

De eisen waaraan een partij moet voldoen voor toetreding tot het stelsel zijn dan de volgende:

- de toetredende partij maakt zijn eigen afweging over de rol(len) die hij wil vervullen. Daarbij spelen in ieder geval zaken als verwachte omzet, financieringsmodel en aansprakelijkheidsrisico een rol;

---

[8] Zie ook position paper thuiswinkel.org

- de invulling van de gekozen rol(len) moet voldoen aan de eisen die het stelsel stelt. Eén van die eisen is dat de gegevensuitwisseling met andere partijen plaatsvindt volgens de standaarden die daaromtrent in het stelsel zijn afgesproken;

- als de toetredende partij de rol Middelenuitgever kiest dan moet hij zijn uitgifteproces laten toetsen door de beheerorganisatie eHerkenning. Het doel van deze inhoudelijke toets is vast te stellen of het uitgifteproces voldoet aan de eisen die horen bij het betrouwbaarheidsniveau van het uit te geven middel.

  Als de toetredende partij meer soorten middelen wenst uit te geven (mogelijk op verschillende betrouwbaarheidsniveau's) dan vindt een onafhankelijke toets plaats op het uitgifteproces voor ieder middel. Hierbij wordt gekeken naar registratieprocessen, interne processen bij de middelenuitgever, technische oplossingen en het uitgifteproces van het middel zelf;

- na toelating tot het netwerk toetst de middelenuitgever permanent zelf of het uitgifteproces nog steeds aan de eisen voldoet; daarnaast voert de beheerorganisatie periodiek een inhoudelijke toets uit op naleving;

- de nieuw toetredende partij sluit tenslotte een overeenkomst met de beheerorganisatie, waarin alle rechten en verplichtingen zijn vastgelegd die van toepassing zijn binnen het stelsel eHerkenning.

Het is de commissie helder dat potentiële toetreders tot het stelsel meer informatie behoeven dan hiervoor is gegeven. Het gaat met name om informatie die hen in staat stelt het omzetvolume in te schatten, informatie over het financieringsmodel en meer inzicht in de aansprakelijkheid die voor deelnemers aan het stelsel geldt. Daarom geeft de commissie hierbij de volgende aanvullende informatie.

Waar het gaat om de omvang van de markt heeft Ecorys een schatting gemaakt van het aantal transacties tussen overheidsorganisaties en bedrijven en komt daarbij op ruim 44 miljoen transacties per jaar.

Het voorgestelde financieringsmodel voor eHerkenning is beschreven in hoofdstuk 7 e).

EL&I heeft een (juridische) analyse van het aansprakelijkheidsrisico gemaakt. Die geeft het volgende beeld. Marktpartijen zijn aansprakelijk voor de producten en diensten van eHerkenning aan ondernemers en overheidsdienstverleners. Op dit moment kan een deelnemer o.g.v. de Deelnemersovereenkomst tegenover een derde zijn aansprakelijkheid beperken tot directe schade voor een bedrag van max. € 30.000,- per gebeurtenis. Er is geen limiet per jaar vastgelegd.
De aansprakelijkheid van een Deelnemer t.o.v. ICTU en v.v. is beperkt tot directe schade van max. € 30.000,- per jaar. O.g.v. de Gebruiksvoorwaarden is de aansprakelijkheid van de ene partij tegenover de andere (partij = deelnemer, bedrijf of dienstverlener) beperkt tot directe schade van max. € 30.000,- per gebeurtenis en tot max. € 300.000,- per jaar.

Verder hebben de potentiële toetreders natuurlijk behoefte aan informatie over de standaarden die gelden voor de communicatie tussen de verschillende rollen in het stelsel. In het afsprakenstelsels liggen deze standaarden (concreet: koppelvlakspecificaties) vast in formele documenten.

Uittreding van een partij uit het stelsel
Partijen kunnen niet alleen toetreden tot maar ook uittreden uit het stelsel. Het uittreden kan twee oorzaken hebben:

- een partij heeft bedrijfseconomische (of andere) redenen om zijn dienstverlening niet langer te continueren en besluit zelf om het stelsel te verlaten;

- een partij voldoet niet aan de eisen die het stelsel stelt, waarna de beheerorganisatie de partij dwingt om het stelsel te verlaten.

Het uittreden van een partij uit het stelsel (vrijwillig of gedwongen) heeft grote consequenties voor de bedrijven die gebruik maken van eHerkenning. Zij worden door de uittreding gedwongen nieuwe middelen aan te schaffen en/of hun machtigingen in een ander Machtigingenregister vast te leggen.

Overheidsdienstaanbieders ondervinden in principe geen consequenties van het uittreden van Middelenuitgevers, Authenticatiediensten en Machtigingenregisters. De Herkenningsmakelaar schermt hen namelijk af van de interne werking van het stelsel. Zij ondervinden wel de gevolgen van het uittreden van Herkenningsmakelaars. Verder krijgen overheidsdienstaanbieders te maken met klanten die (tijdelijk) geen elektronische diensten af (kunnen) nemen.

Om het uittreden van partijen in goede banen te leiden is naar de mening van de commissie een aantal maatregelen en voorzieningen nodig:

- overheidsdienstaanbieders gebruiken in principe minimaal twee Herkenningsmakelaars (of dekken dit risico op een andere wijze af), zodat zij eHerkenning kunnen blijven gebruiken als één van de Herkenningsmakelaars (al dan niet gedwongen) het stelsel verlaat;

- een hulpmiddel dat het voor bedrijven mogelijk maakt op snelle en soepele wijze een vervangend middel aan te schaffen. Denk hierbij aan de overstapservice zoals die geboden is bij de vervanging van DigiD Bedrijven door eHerkenning. Een ander voorbeeld is de keuzeservice die bedrijven helpt een hulpmiddel te kiezen (zie voor een nadere uitwerking hoofdstuk Implementatiestrategie, onderdeel d);

- een faciliteit die de uitwisseling van machtigingsgegevens tussen Machtigingsregisters ondersteunt. Een dergelijke service moet het mogelijk maken geregistreerde machtigingen van het een naar het andere register over te brengen, waarbij de betrokken onderneming natuurlijk zelf aangeeft in welk register zijn Machtigingen terecht moeten komen.

Verder vestigt de commissie er de aandacht op dat het noodzakelijk is bij vrijwillige uittreding een relatief lange opzegtermijn (van minimaal enkele maanden) te hanteren. Dat maakt het zowel voor bedrijven als voor overheidsdienstaanbieders mogelijk beheerst over te stappen naar andere partijen binnen het stelsel.

Bij gedwongen uittreding (zie Diginotar) is een dergelijke beheerste overstap niet mogelijk. In dergelijke gevallen moeten de voornoemde faciliteiten een snelle overstap ondersteunen.

8.3 Hergebruik van bedrijfseigen middelen in het stelsel

Zoals eerder aangegeven is eHerkenning een open stelsel. Dat betekent dat naast de toetreding van nieuwe partijen tot het stelsel ook hergebruik van reeds bestaande middelen en machtigings-registers aan de orde is.

Waar het gaat om het hergebruik van reeds bestaande middelen geldt naar de mening van de commissie hetgeen hiervoor aan de orde was. Dat betekent dat een partij die middelen uitgeeft de mogelijkheid heeft toe te treden tot het stelsel in de rol van Middelenuitgever en/of Authenticatiedienst (en de middelen dan ook moeten voldoen aan de eisen van het stelsel). Het moge helder zijn dat dit alleen een levensvatbare optie is voor partijen die significante aantallen middelen (hebben) uit(ge)geven. In andere gevallen verdient men de investering die gemoeid is met het toetreden tot het stelsel zeer waarschijnlijk niet terug.

Een bijzonder geval waar hergebruik mogelijk aan de orde kan komen is dat van de Rijkspas. Het is de bedoeling dat iedere ambtenaar op korte termijn over een dergelijke pas kan beschikken. In het geval de overheid eHerkenning zou willen gebruiken voor Government to Government transacties zou hergebruik van de Rijkspas binnen eHerkenning mogelijk een goede optie zijn. Ook hier geldt echter dat de beheerder van de Rijkspas dan als Middelenuitgever en/of Authenticatiedienst tot het stelsel moet toetreden.

Waar het gaat om hergebruik van eigen Machtigingsregisters onderscheidt de commissie twee situaties:

- een onderneming heeft een intern machtigingenregister (dan wel procuratielijst). Hierin legt het bedrijf vast welke functionarissen waartoe bevoegd zijn. In deze gevallen is het weliswaar technisch mogelijk het bedrijf als Machtigingsregister toe te laten treden tot het stelsel. Echter, de omvang van het onderhavige register zal zodanig zijn dat dit niet kosteneffectief zal zijn. Dat betekent dat de onderneming zijn machtigingen moet vastleggen in een Machtigingsregister. Het lijkt niet onaannemelijk dat bestaande Machtigingsregisters bedrijven faciliteiten bieden om de gegevens zo eenvoudig mogelijk te "importeren".

- financieel en fiscaal dienstverleners leggen ook machtigingen vast. Daarbij gaat het om de machtigingen die hun klanten (i.c. bedrijven) aan hen hebben verstrekt om namens hen diensten bij de overheid af te nemen. De werkwijze in deze gevallen is reeds in hoofdstuk 5 aan de orde geweest.

8.4 Voorzieningen

De in dit rapport beschreven adviezen brengen met zich mee dat een aantal technische voorzieningen ontwikkeld zal moeten worden. Zo moet er, om machtigingen vast te kunnen leggen in een machtigingenregister, een dienstenregister komen. Dit is een gestandaardiseerde catalogus van alle mogelijke overheidsdiensten. Bedrijven hebben een dergelijk register nodig om vast te kunnen leggen wie voor welke dienst is gemachtigd. De commissie adviseert om bij het ontwikkelen van het dienstenregister aan te sluiten bij wat er al is: zowel bij de overheidsbrede open standaard 'Samenwerkende Catalogi' als het reeds bij Dienst Regelingen ontwikkelde Dienstenregister (dat operationeel is bij DR en nVWA).

9. Doorkijk naar het burgerdomein

De adviesaanvraag aan de commissie A3 kende als beperking dat het advies gericht moest zijn op het bedrijvendomein. De commissie heeft in haar advies dan ook geen aandacht gegeven aan de problematiek rond authenticatie en autorisatie in het burgerdomein. De beleidsverantwoordelijkheid voor het burgerdomein ligt bij BZK.

Het is wel de verwachting van de commissie dat er op korte tot middellange termijn een discussie op gang zal komen over de inrichting van authenticatie en autorisatie in het burgerdomein. De commissie hecht er aan een aantal aandachtspunten te formuleren die in deze discussie aan de orde zouden moeten komen.

Die aandachtspunten zijn:

- het onderscheid tussen burgers en bedrijven vervaagt (snel). De koers die, onder andere aan de hand van dit advies, wordt gekozen voor het bedrijventerrein, heeft gevolgen voor het burgerdomein: het is niet meer mogelijk gescheiden van elkaar te opereren. Een voorbeeld daarvan is de discussie rond het in rekening brengen van kosten voor publieke middelen. Als private middelen ook worden gebruikt in het burgerdomein, kunnen publieke middelen niet meer gratis zijn;

- eHerkenning is een stelsel, waarin verschillende deelnemers samenwerken, die ieder een deel van het stelsel vormgeven. Een dergelijke inrichting zorgt om te beginnen voor continuïteit: als één van de deelnemers (al dan niet gedwongen) uittreedt blijft het stelsel functioneren;

- het stelsel kent verschillende herkenningsmiddelen, wat bedrijven keuzevrijheid biedt bij het aanschaffen van een herkenningsmiddel. Daarbij kiezen bedrijven zelf voor een zeker betrouwbaarheidsniveau (en daarmee voor de diensten die zij elektronisch kunnen afnemen). Ook burgers kunnen en willen in toenemende mate zelf kiezen;

- eHerkenning is in de eindsituatie een stelsel waar met name eenmanszaken zowel publieke als private middelen kunnen gebruiken. Die keuzevrijheid is belangrijk in het licht van het feit dat in het geval van eenmanszaken het onderscheid tussen burgers en bedrijven vervaagt;

- het uitgeven van middelen en het beheer van machtigingsregisters vormen de hoekstenen van het stelsel. Dat betekent dat (de uitvoerders van) deze processen zich diepgaand en frequent moeten verantwoorden over de mate waarin hun processen voldoen aan daaraan gestelde eisen.

- het stelsel eHerkenning is qua opzet niet alleen bruikbaar voor B2G (business-to-government), maar ook voor B2B (business-to-business), G2C (government-to-government), mogelijk B2C (business-to-consumer) en zou in beginsel - wanneer daartoe politiek wordt besloten - ook ingezet kunnen worden voor C2G (citizen-to-government)

10. Roadmap

Om het advies van de commissie te implementeren, moet er op korte en wat langere termijn een aantal zaken gebeuren. Deze worden in dit hoofdstuk opgesomd.

Allereerst is het noodzakelijk dat er besluitvorming plaatsvindt op de volgende punten, aan de hand van dit advies:

1. Keuzevrijheid voor eenmanszaken doordat de eenmanszaak zowel DigiD/DigiD Machtigen als eHerkenning mag gebruiken voor authenticatie en autorisatie;
2. Overige bedrijven maken gebruik van eHerkenning voor authenticatie en autorisatie;
3. Er komt een transitievoorziening voor machtigingen aan fiscaal dienstverleners t.b.v. het doen van belastingaangifte;
4. Het ontwikkelen van een BSN-loos e-ID. Dit behoeft expliciet politieke aandacht en besluitvorming;
5. Er wordt gestuurd op de voorgestelde maatregelen om snelle groei van het stelsel te bevorderen ((grootschalige) toepassingen, B2B domein ontwikkelen, financieel model in groeifase);
6. Er worden maatregelen genomen om de continuïteit en kwaliteit van het stelsel te borgen.

Daarna moeten de volgende zaken worden opgepakt:

Actie	**wie**
1. In gang zetten ontwikkeling DigiD hoog, zonder BSN	BZK
2. Check Markt en Overheid op publieke voorziening machtigingsregister	Belastingdienst
3. In gesprek met overheidsdienstverleners die BSN mogen verwerken om eHerkenning als tweede sleutel op te nemen	EL&I, BZK
4. Opnemen van eHerkenning als tweede sleutel bij portaal Belastingdienst	Belastingdienst
5. In gesprek met KvK over ontsluiten digitale diensten met eHerkenning (te starten met het doorgeven van wijzigingen in het HR)	EL&I
6. In gesprek met overheidsdienstaanbieders met een eigen voorziening, om eHerkenning als tweede sleutel op te nemen	EL&I, BZK
7. Ontwikkelen van een functionaliteit (in de vorm van een webservice) waarmee online in het NHR gecontroleerd kan worden of iemand geregistreerd staat als bestuurder.	EL&I (KvK)
8. Realisatie omnummervoorziening, die overheidsorganisaties die het BSN mogen verwerken, kan voorzien van het BSN-nummer dat bij de gebruiker van een eHerkenningsmiddel hoort	EL&I
9. In gesprek met Dienst Regelingen om te komen tot de realisatie van een Dienstenregister (met aandacht voor hergebruik van de standaard Samenwerkende Catalogi). De stuurgroep GOA heeft eerder besloten dat in het Dienstenregister wordt geregistreerd welke organisatie wettelijke toestemming heeft om het BSN te verwerken.	EL&I
10. Communicatie richting eindgebruikers, met daarbij aandacht voor: - vanuit het oogpunt van veilige digitale dienstverlening bedrijven raadt de overheid aan om machtigingen volledig en actueel te registreren in een Machtigingenregister;	EL&I
11. Zorg dat er pilots of POCs worden gestart om de bruikbaarheid van eHerkenning bij gemeenten te toetsen. Sluit aan bij wat KING op dit gebied al doet.	EL&I
12. Zorg dat er duidelijkheid komt over de daadwerkelijke kosten van het raadplegen van de machtigingsregisters en daarvoor waar mogelijk te werken met vaste, voorspelbare tarieven (niet per raadpleging, maar per	Marktpartijen

periode).	
13. Gesprekken aangaan met vertegenwoordigers van braches (bv zorg en onderwijs), over toepassing van het stelsel	EL&I
14. Besluit nemen over aanvaarding aansprakelijkheid bij fouten op stelselniveau	EL&I
15. Uitwerken gestandaardiseerde user interface voor tweede sleutel	
16. Helpdesk inrichten	EL&I
17. Handreiking opstellen voor overheidsdienstaanbieders m.b.t. een veilige voorziening (inclusief aandacht voor het vaststellen van service levels, dubbel routeren van voorzieningen)	EL&I
18. Onderzoeken of aansluitvoorwaarden voor overheidsdienstaanbieder wenselijk zijn	EL&I
19. Opstellen nieuwe modelcontracten tussen beheerder en marktpartijen	EL&I
20. Ga in gesprek met dienst Justis, over gezamenlijke communicatie rondom aanvragen VOG met eHerkenning	EL&I
21. Ontwikkel een langjarige communicatiecampagne rond eHerkenning. De nadruk daarbij moet liggen op de website eHerkenning.nl,	EL&I
22. Start een B2B pilot samen met een groot Nederlands bedrijf, waarbij zowel de makelaarsfunctie, de middelenfunctie als de machtigingen verder worden getest.	EL&I
23. Geef B2B gebruikers zeggenschap in de governance van het stelsel	EL&I
24. Ga het gesprek aan over G2G toepassingen van eHerkenning (DigiD OEP en Rijkspas)	EL&I, BZK
25. Ontwikkel een hulpmiddel dat het voor bedrijven mogelijk maakt op snelle en soepele wijze een vervangend middel aan te schaffen. Denk hierbij aan de overstapservice zoals die geboden is bij de vervanging van DigiD Bedrijven door eHerkenning. Een ander voorbeeld is de keuzeservice die bedrijven helpt een hulpmiddel te kiezen (zie voor een nadere uitwerking hoofdstuk Implementatiestrategie, onderdeel d);	EL&I
26. Ontwikkel een faciliteit die de uitwisseling van machtigingsgegevens tussen Machtigingsregisters ondersteunt. Een dergelijke service moet het mogelijk maken geregistreerde machtigingen van het een naar het andere register over te brengen, waarbij de betrokken onderneming natuurlijk zelf aangeeft waar zijn Machtigingen terecht moeten komen.	EL&I

Bijlagen

1. **Begrippenkader GOA**
2. **Samenvatting Ecorys**

Bijlage 1: Conceptueel kader GOA

Conceptueel Kader

Gemeenschappelijk Ontwerp
Authenticatie en autorisatie (GOA)

Werkgroep GOA

Versie 1.0

28 oktober 2011

1. Inleiding

In dit document is een conceptueel kader toegelicht voor identificatie, authenticatie en autorisatie bij elektronische diensten tussen burgers en bedrijven enerzijds en de overheid anderzijds. Centraal in dit kader staan de rollen en verantwoordelijkheden van betrokkenen in een keten van digitale transacties en de (digitaal te leveren) verklaringen die de betrokken overheidsorganisatie nodig heeft om deze rollen en verantwoordelijkheden te kunnen verifiëren.

Met het kader worden de volgende resultaten beoogd:

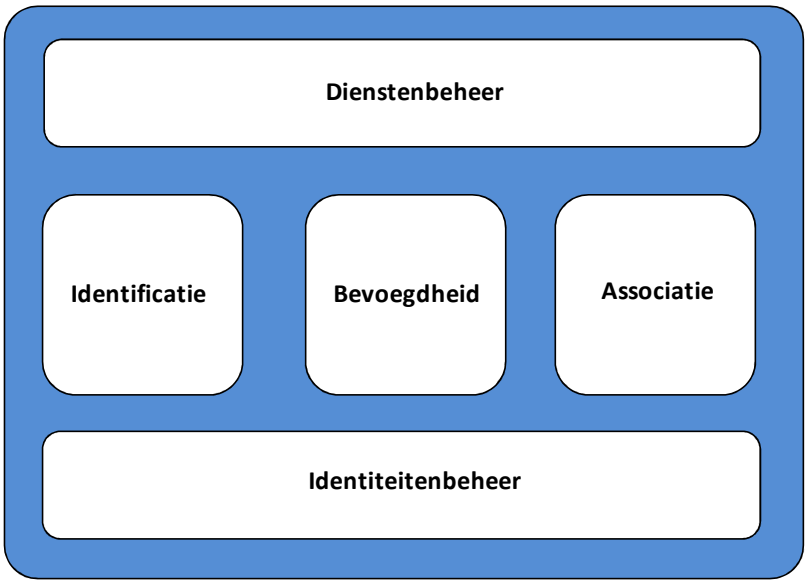
a. Zelfde gestandaardiseerde invulling voor alle internet kanalen: het online portaal kanaal en het machine-machine kanaal.
b. Zelfde gestandaardiseerde invulling voor het burger- en het bedrijven domein.
c. De invulling is onafhankelijk van de diverse technologieën die gebruikt worden bij de authenticatiemiddelen en machtigingsregisters.
d. Duidelijk en onderscheiden verantwoordelijkheden van de verschillende rollen van personen en partijen betrokken bij de totstandkoming van een transactie.
e. In de praktijk is sprake van veel verschillende situaties waarin een transactie wordt uitgevoerd, bijvoorbeeld wel of geen gemachtigde, het gebruik van een overheidsvoorziening of een private oplossing, etc. Het kader moet alle voorkomende situaties eenduidig ondersteunen.

In hoofdstuk 2 wordt het conceptueel kader beschreven. Het kader is implementatievrij beschreven. In hoofdstuk 3 wordt ter illustratie beschreven op welke wijze het kader bij de Belastingdienst wordt toegepast. Om het kader beter te kunnen begrijpen worden in hoofdstuk 4 een aantal scenario's beschreven. Deze zijn ontleend aan de praktijk van de Belastingdienst en SBR (Standard Business Reports). Deze scenario's laten zich echter abstraheren naar e-overheidsdiensten in het algemeen (subsidie-, vergunningaanvragen ed., al dan niet met tussenkomst van een zakelijke dienstverlener).

2. Conceptueel kader

Gemeenschappelijk Ontwerp Authenticatie en autorisatie (GOA) Grondplaat

Het kader dat in dit document wordt beschreven is gebaseerd op kennis opgedaan in het GOA-traject. Het GOA traject heeft in 2010 geleid tot een eerste aanzet van een gemeenschappelijk ontwerp. Als basis voor dit ontwerp is een hanteerbare indeling gemaakt van het gehele terrein van identificatie, authenticatie en autorisatie naar 5 functionele domeinen. In onderstaande figuur zijn deze domeinen weergegeven.



Elk domein heeft een eigen doel en levert essentiële functies in de uitvoering van elektronische transacties.

Dienstenbeheer: Dit domein richt zich op het beheren van de "catalogus" aan diensten die via internet bij de overheid zijn af te nemen. Voor elk van de diensten moet immers bekend zijn welk betrouwbaarheidsniveau van toepassing is en wat de vereiste betrouwbaarheid is van een eventueel benodigde ondertekening.

Identificatie: Dit domein richt zich op het met een bepaalde mate van betrouwbaarheid vaststellen van de Identiteit van de betrokken personen. Dit is nodig om een overheidsdienstaanbieder voldoende betrouwbaarheid te geven over de persoon waarmee hij zaken doet.

Bevoegdheden: Dit domein richt zich op het kennen van de bevoegdheid van een gemachtigde (mag hij namens een ander handelen) en het beheer van machtigingen in een register.

Associatie: Het domein 'Associatie' richt zich op het verkrijgen en beoordelen van een wilsuiting van een persoon. Kenmerkend hiervoor is dat deze onlosmakelijk verbonden wordt met de inhoud (de jaarcijfers, de aanvraag, de inschrijving), waardoor de integriteit van het gehele bericht wordt gewaarborgd.

Identiteitenbeheer: Dit domein omvat alle activiteiten gericht op het beheren van de Identiteiten van personen.

In deze versie van het conceptueel kader worden de drie primaire domeinen: identificatie, bevoegdheid en associatie nader uitgewerkt. De ondersteunende domeinen (identiteitenbeheer en dienstenbeheer) worden in een volgende versie nader uitgewerkt.

Uitwerking van de primaire domeinen

Voor het bereiken van de geschetste resultaten in de inleiding, is het conceptuele kader gebaseerd op twee pijlers:

I. Definiëring van de rollen en verantwoordelijkheden van betrokkenen in een keten van digitale transacties.
II. De inrichtingsonafhankelijke invulling van de 'bewijsstukken' die nodig zijn om vast te kunnen stellen "wie ben je?" en "wat mag je?". Deze bewijsstukken worden in de vorm van verklaringen in elke transactie aangeleverd.

Ad I. Definiëring van begrippen en rollen

Bij het elektronische verkeer tussen burgers en bedrijven enerzijds en de overheid anderzijds staan twee begrippen centraal, namelijk *dienst* en *keten van verklaringen*.

Een *dienst* is een samenstel van transacties, gericht op het tot stand komen van een specifieke publiekrechtelijke rechtshandeling (het nemen van een besluit) of het leveren van een product of het beantwoorden van een informatievraag. De dienst wordt aangeboden door een dienstaanbieder, die bepaalt welke eisen gesteld worden aan de keten van verklaringen, zoals niveau van betrouwbaarheid.

De *keten van verklaringen* representeert op een verifieerbare wijze de verklaringen over identiteit en bevoegdheden die bij de dienstaanbieder leiden tot de totstandkoming van een autorisatiebesluit voor een dienst. Alle schakels in een bevoegdheidsketen samen geven antwoord op de vraag "wie ben je?" en "wat mag je?".

Bij het tot stand komen van elektronische transacties worden de volgende *rollen* onderscheiden:

- *Dienstaanbieder*: een bestuursorgaan dat kenbaar heeft gemaakt dat het elektronisch bereikbaar is voor burgers en bedrijven. Dit betekent dat het elektronisch berichten kan ontvangen en verzenden, ofwel *elektronische transacties* ondersteunt ten behoeve van de totstandkoming van diensten.

- *Handelende partij:* de entiteit (organisatie of persoon) die handelingen verricht ten behoeve van het tot stand komen van een elektronische transactie met een dienstaanbieder, als onderdeel van totstandkoming van een dienst. De handelende partij kan twee rollen vervullen namelijk die van *belanghebbende* of die van *gemachtigde*.

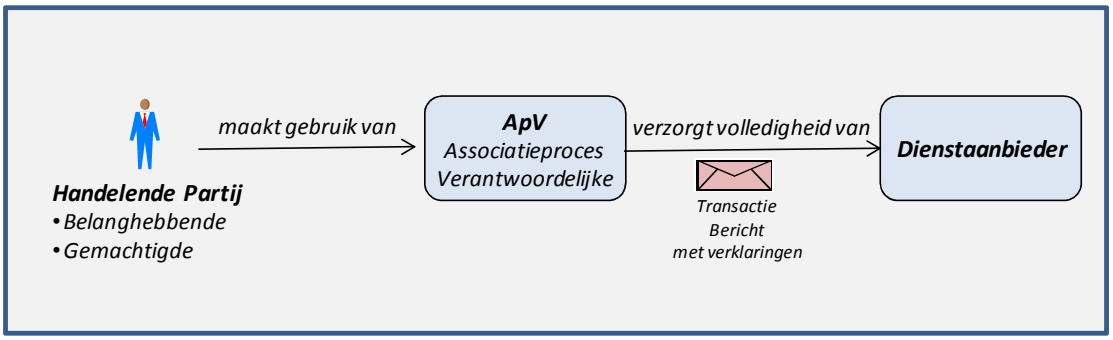
- *Belanghebbende*: degene wiens belang rechtstreeks bij een besluit is betrokken (artikel 1:2 Awb). In het algemeen zal dit degene zijn ten aanzien van wie – al dan niet op aanvraag – een besluit wordt genomen. Er kunnen echter ook diensten zijn die niet tot een besluit leiden, maar tot feitelijk handelen van de dienstaanbieder (zie definitie van dienst). In dit conceptuele kader wordt ook voor die gevallen het begrip belanghebbende gebruikt. Onder belanghebbenden vallen volgens Awb ook bijv. partijen als omwonenden bij een tracébesluit. In dit conceptueel kader worden deze partijen niet bedoeld en wordt het begrip verder beperkt zodat uitsluitend een zelf handelende of vertegenwoordigde belanghebbende wordt bedoeld.

- *Gemachtigde*: degene die op grond van een machtiging namens de belanghebbende transacties verricht. Meestal zal hierbij sprake zijn van een machtigingsrelatie als bedoeld in artikel 2:1 Awb. Dit artikel bepaalt dat eenieder zich in het verkeer met bestuursorganen kan laten bijstaan of door een gemachtigde kan laten vertegenwoordigen. Het bestuursorgaan kan daarbij een schriftelijke machtiging verlangen. De machtiging kan ook voortvloeien uit een privaatrechtelijke volmacht (artikel 3:60 BW). Tot slot worden ook wettelijke vertegenwoordigingsbevoegden, zoals bestuurders van rechtspersonen, eigenaren van eenmanszaken en curatoren tot gemachtigden gerekend.

- *Associatieproces Verantwoordelijke (ApV)*[9]: de partij die verantwoordelijk is voor het samenstellen en controleren van de keten van verklaringen en het verbinden van deze keten aan de inhoud van de transactie. De controle bestaat uit het authenticeren van de verschillende verklaarders en vaststellen van de bevoegdheid van de Handelende partij. De ApV geeft hierover de associatieverklaring af. De ApV draagt overigens anders dan de consistentie en integriteit geen inhoudelijke verantwoordelijkheid voor de geassocieerde verklaringen. Door middel van een ICT-voorziening wordt de transactie tussen de Handelende partij en de Dienstaanbieder afgehandeld.

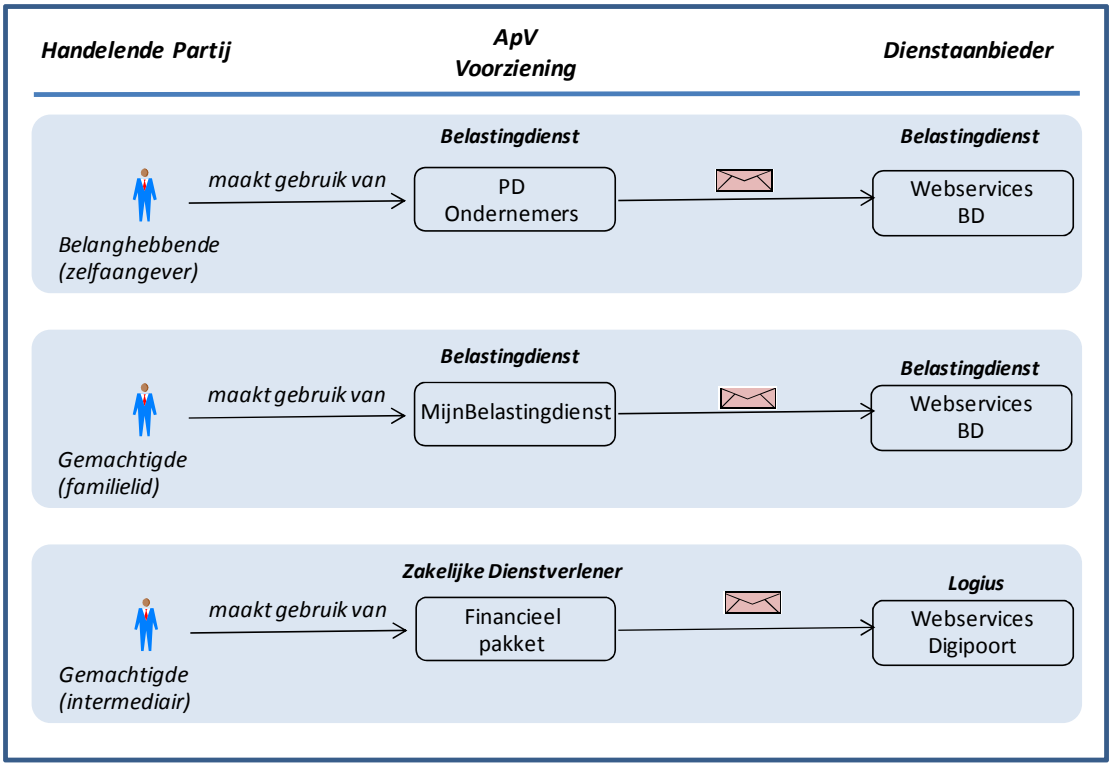
- *Verklaarder*: is verantwoordelijk voor de inhoud van een verklaring. Een verklaarder kan zijn een Belanghebbende zelf of een gecertificeerde vertrouwde partij.

De relaties tussen de betrokkenen in de uitvoering van een elektronische transactie is in onderstaand schema weergegeven.



Om het conceptuele schema toe te lichten, zijn in onderstaand schema drie Belastingdienst voorbeelden weergegeven.

[9] Het is lastig om een goede term voor deze persoonsrol aan te geven. Voorlopig wordt deze term gehanteerd.



In het schema wordt duidelijk gemaakt dat de rol van ApV zowel een overheidsrol kan zijn, maar ook een private rol. Voor de Dienstaanbieder is dat onderscheid niet relevant.

Ad II. Invulling van de 'bewijsstukken'

Om te kunnen verifiëren wie een handelende partij is en wat deze mag t.a.v. een bepaalde elektronische transactie, wordt de keten van verklaringen verzameld. Elke verklaring is afgegeven door een verklaarder, wiens identiteit blijkt uit de ondertekening van de verklaring. De volgende *verklaringen* worden onderscheiden:

- *Identiteitsverklaring*: geeft uitdrukking aan de identiteit van de handelende partij. *Wie ben je?*

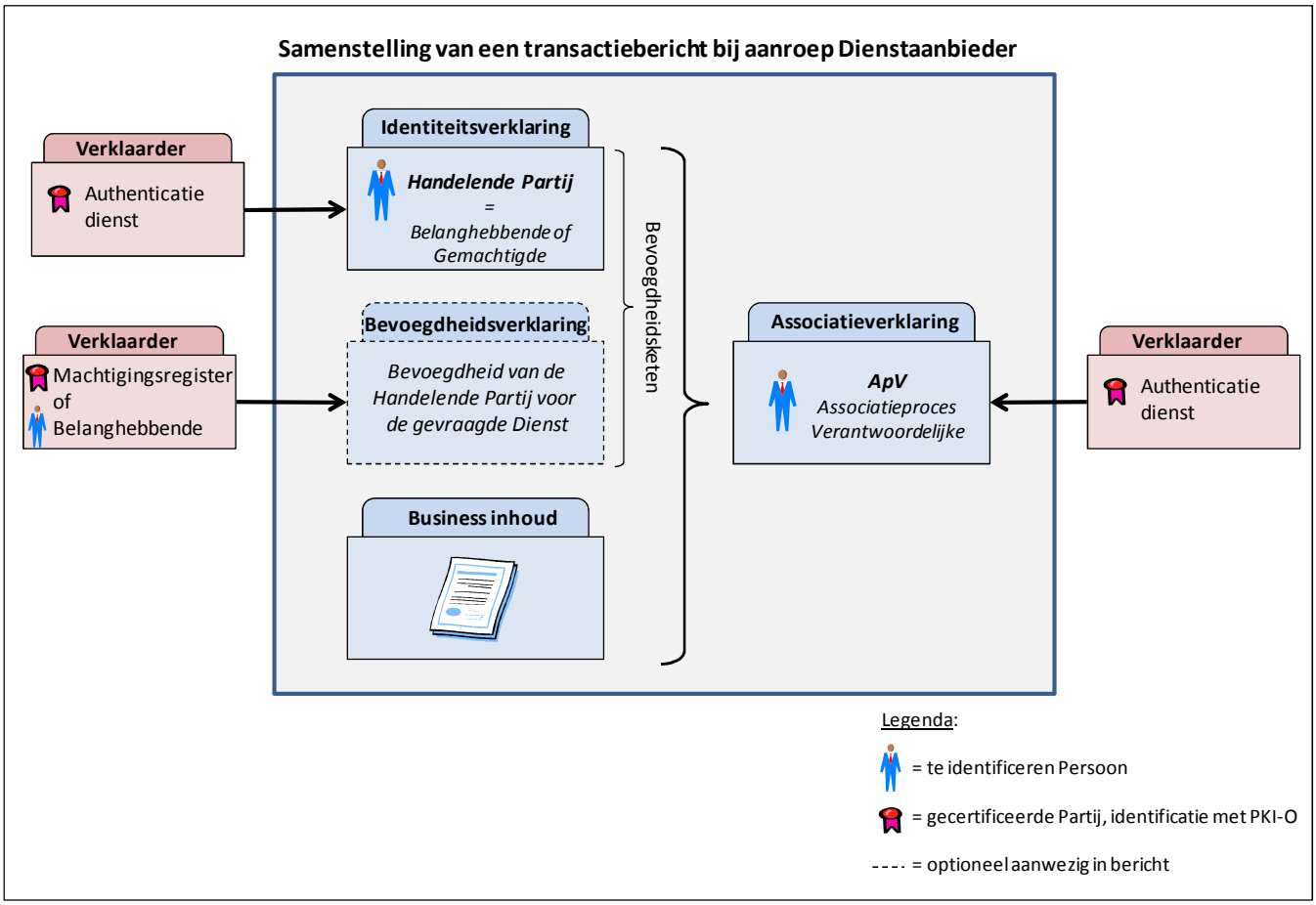
- *Bevoegdheidsverklaring*: geeft uitdrukking aan de bevoegdheid van de handelende partij. *Wat mag je?*
  Meer specifiek gaat het hier om de vraag of de handelende partij voor zichzelf handelt (en dus automatisch bevoegd is) of voor iemand anders. In beide gevallen wordt expliciet over de bevoegdheid verklaard.

- *Associatieverklaring*: geeft uitdrukking aan samenhang en consistentie van de keten van verklaringen, de inhoud van de transactie en de door de handelende persoon geuite wil t.a.v. deze inhoud.

Geen onderdeel van de bevoegdheidsketen, maar wel essentieel voor de geldigheid van de transactie is de bevestiging daarvan door de belanghebbende of zijn gemachtigde. Die bevestiging vindt plaats door middel van een wilsuiting. In wetgeving is deze vaak neergelegd in de vorm van een ondertekeningsvereiste. De wilsuiting kan – afhankelijk van de voor de transactie geldende (wettelijke) eisen – variëren van een eenvoudig 'vinkje' bij een 'voorgedrukte' verklaring tot een gekwalificeerde elektronische handtekening van de ondertekenaar. De wilsuiting is geen aparte verklaring, maar wordt onlosmakelijk verbonden aan de inhoud van de transactie en is daarmee onderdeel van de associatieverklaring. Hierin wordt vastgelegd met welke mate van

betrouwbaarheid het (onderteken)proces is uitgevoerd. Dit wordt vastgesteld door de Associatieproces Verantwoordelijke (ApV).

In het volgende schema worden de onderdelen in onderling verband geschetst.



Een voorbeeld van het toepassen van het werken met verklaringen is de architectuurkeuze voor online dienstverlening van de Belastingdienst op basis van een "Informatie Makelaar". Deze architectuur biedt een 'gelaagde' beveiliging, waarbij het verlenen van toegang op de frontoffice applicatie gescheiden is van het daadwerkelijk verstrekken van privacy gevoelige informatie door de Informatie Makelaar.

Een frontoffice applicatie zal een gebruiker bij de informatie-aanvraag helpen om de benodigde identiteits- en (in geval van vertegenwoordiging) een bevoegdheidsverklaring op te vragen bij DigiD en DigiD-machtigen (of eHerkenning). DigiD voorziet zo'n verklaring van een elektronische handtekening. Vervolgens stuurt de frontoffice applicatie de informatie-aanvraag met de verklaringen op naar de Informatie Makelaar. Ook al zou de frontoffice applicatie worden gehackt; de Informatie Makelaar controleert elke aanvraag alsnog aan de hand van de meegeleverde verklaring en beslist of de gebruiker toegang mag krijgen tot de betreffende vertrouwelijke informatie.

Omdat de Informatie Makelaar geen interactie met de gebruiker heeft en een strikte berichtspecificatie gebruikt, is hij relatief eenvoudig te beveiligen. Desondanks wordt er juist op deze 'toegangspoort tot vertrouwelijke informatie' een heel scala aan beveiligingsmaatregelen genomen bij bouw, test en beheer. De Informatie Makelaar zelf is dus goed beveiligd. Een hacker kan hem om de tuin leiden, maar zal dan eerst zowel DigiD als onze frontoffice applicatie moeten manipuleren. Het ongeautoriseerd naar buiten laten 'lekken' van vertrouwelijke gegevens wordt op deze manier vrijwel onmogelijk. Het belangrijkste voordeel is dat niet elke frontoffice applicatie alle denkbare maatregelen hoeft te bevatten om weerstand te bieden aan 'de boze buitenwereld', maar dat die weerstand geboden wordt door een stelsel van maatregelen in de keten.

3. Implementatie voorbeeld bij de Belastingdienst

Het conceptueel kader is bedoeld als algemeen geldend kader waarin de rollen en de verklaringen van het authenticatie- en autorisatie stelsel zijn onderkend en benoemd.
Dit kader is toepasbaar voor alle mogelijke scenario's, van eenvoudig (belanghebbende die zelf een aangifte indient) tot complex (een Belanghebbende machtigt een Fiscale dienstverlener om diensten voor hem uit te voeren, die ze vervolgens deels weer uitbesteed aan een ander bureau, waarvan de medewerker de aangifte uiteindelijk doet).

Om de implementatie vooralsnog niet te complex te maken, kiest de Belastingdienst ervoor om de bevoegdheidsketen te beperken tot *één niveau* (belanghebbende-gemachtigde). In werkelijkheid zal de keten van betrokkenen bij een transactie vaak langer zijn, maar de schakels in die keten zijn niet alle gebaseerd op een machtigingsrelatie.

Dit heeft de volgende consequenties:

- De gemachtigde kan zijn activiteiten uitbesteden, maar blijft verantwoordelijk voor de transactie en voor de daarbij verstrekte gegevens. Voorbeelden van uitbesteden zijn het inschakelen van een signingdienst, het gebruik maken van diensten van een saas-provider ed.

- Voldoende is (ook in juridisch opzicht, en in elk geval met het oog op de geldigheid van de transactie) dat betrouwbaarheid bestaat over de bevoegdheid van een *organisatie* als gemachtigde.[10] Indien binnen een organisatie autorisaties voor een transactie noodzakelijkerwijs beperkt zijn tot een bepaalde medewerker (bv. op grond van wettelijke eisen)[11], is het streven naar slechts één schakel niet mogelijk en kan een schakel aan de bevoegdheidsketen worden toegevoegd.

- Indien het uit oogpunt van dienstverlening gewenst is om informatie te krijgen ten behoeve van herkenning van personen bij herhaalde transacties (comfortinformatie: "Goedemorgen mw. Vrij") kan die gevraagd worden, doch deze maakt geen verplicht onderdeel uit van de bevoegdheidsketen, maar kan optioneel aan verklaringen worden toegevoegd.

---

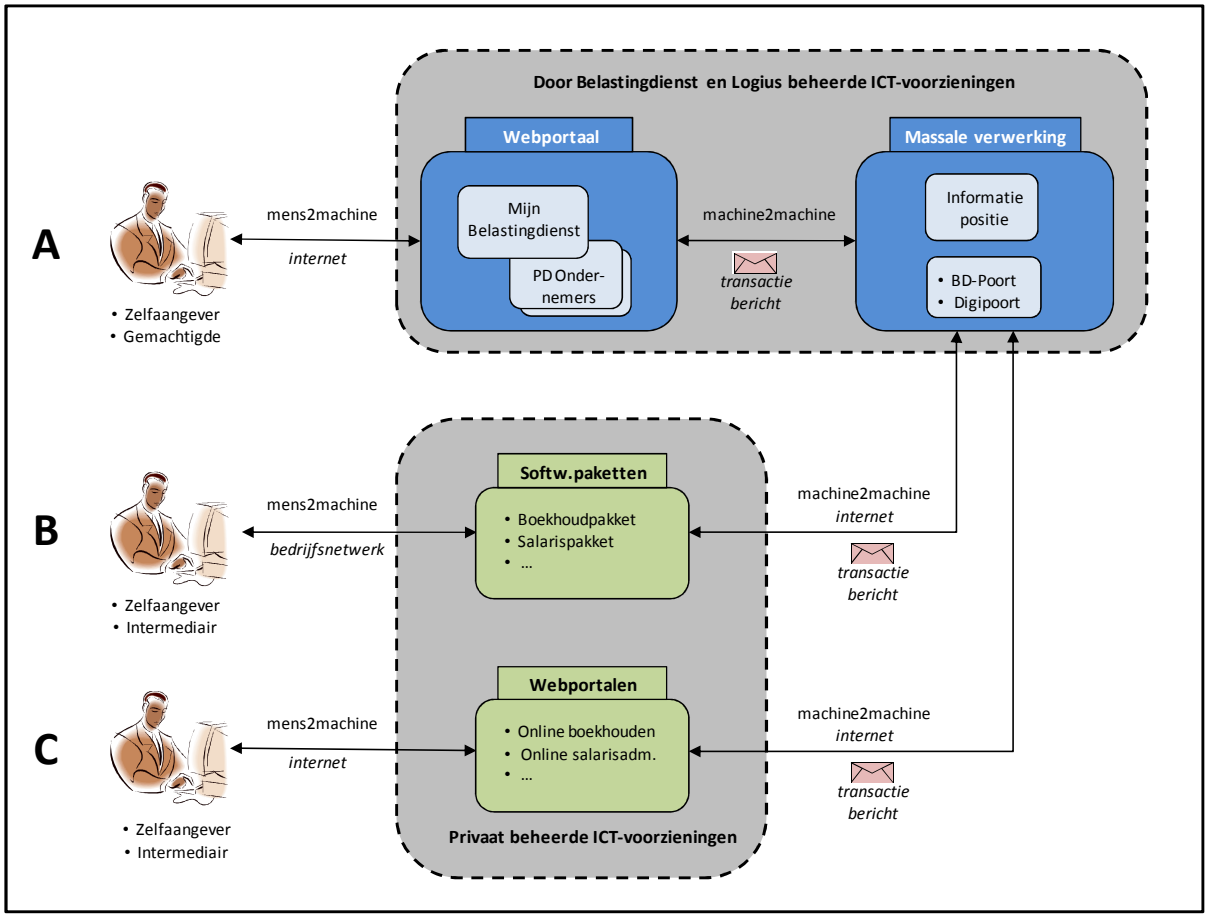
10 Deze benadering sluit aan op het uitgangspunt van federatieve authenticatie en autorisatie, zoals uitgewerkt voor informatie-uitwisseling in de strafrechtsketen (zie Verdiepingsstudie Authenticatie, autorisatie en logging (AAL), Ministerie van Justitie/Justitiële informatiedienst, januari 2010). Daarbij wordt uitgegaan van toegang op basis van rollen, niet op basis van gegevens van de medewerker. De koppeling van medewerkers aan rollen (binnen de eigen organisatie) is de verantwoordelijkheid van de 'vragende' partij (de afnemer van de dienst).

11 Een voorbeeld is bijvoorbeeld de APK-keurmeester die ook de afmelding doet bij RDW. Bij een keuringsstation is maar één persoon daartoe bevoegd.

4. Scenario's

In dit hoofdstuk wordt geïllustreerd hoe het conceptuele kader uitwerkt voor een aantal scenario's van de Belastingdienst en SBR.

In onderstaande figuur is weergegeven op welke wijze een transactiedienst van de Belastingdienst door een burger of bedrijf wordt afgenomen (interactiepatroon). Hierbij is onderscheid gemaakt in welke soort ICT-voorziening wordt gebruikt door die burger of bedrijf.



Interactiepatroon A

In deze situatie wordt gebruik gemaakt van een webportaal van de Belastingdienst. In de meeste gevallen is het dan de belastingplichtige of toeslagengerechtigde zelf, die dan gebruik maakt van deze voorziening (de zelfredzame burger of bedrijf). Met de introductie van DigiD Machtigen is het ook mogelijk dat een gemachtigde (bijvoorbeeld de partner of 'handige buurman') namens de betrokkene gebruik maakt van een Belastingdienst webportaal. Het gebruik door een gemachtigde is mogelijk bij het toekomstige MijnBelastingdienst en het nieuwe Toeslagen-portaal. In het PD-Ondernemers kan op dit moment niet met machtigingen worden gewerkt.

In de ICT-wereld wordt de wijze waarop gebruik wordt gemaakt van het Belastingdienst webportaal aangeduid als een mens naar machine communicatie invulling (mens2machine). Een webportaal van de Belastingdienst communiceert zelf ook weer met de achterliggende massale verwerkingssystemen van de Belastingdienst, bijvoorbeeld de voorzieningen van Ontvangen&Mededelen en de VIA-gegevensverzameling. In de ICT-wereld wordt deze vorm van communicatie aangeduid als machine naar machine communicatie (machine2machine).

Interactiepatroon B

Deze invulling wordt vooral in een bedrijfsmatige toepassing gebruikt. De grootste groep die van deze vorm gebruikt maakt, zijn de fiscale dienstverleners die met een eigen softwarepakket communiceren met de poort-voorzieningen van de Belastingdienst. Naast de fiscale dienstverleners zijn er ook bedrijven die met behulp van een softwarepakket voor zichzelf aangifte doen. Veelal zijn dat dan de wat grotere bedrijven. De communicatievorm vanuit de softwarepakketten met de Belastingdienst wordt aangeduid als een machine2machine invulling en staat ook wel bekend als het Bapi-kanaal. Met de introductie van het SBR-programma (XBRL-aangiften) is er een tweede kanaal ontwikkeld. In plaats van communicatie rechtstreeks met de Belastingdienst-poort, wordt alle communicatie geleid via Digipoort (de poort-voorzieningen in beheer bij Logius). De beleidslijn is dat het Bapi-kanaal op termijn geheel wordt vervangen door het Digipoort-kanaal.

Interactiepatroon C
Deze invulling is vergelijkbaar met interactiepatroon B. Het verschil echter is dat de gebruikte sofware niet op het bedrijfseigen netwerk is geïnstalleerd, maar de sofware is via internet toegankelijk als een 'cloud-voorziening'. In de ICT-wereld wordt dit ook wel aangeduid als "software as a service" (afgekort als saas). In dit geval is de beheerder van de software een andere partij dan het bedrijf die er gebruik van maakt. De verwachting is dat deze invulling een verdere groei gaat doormaken. Omdat er geen eigen softwarebeheer meer aan te pas komt en omdat de kosten laag zijn, is de drempel voor het gebruik van dit soort voorzieningen laag. Veel ZZP-ers en MKB bedrijven maken hier gebruik van.

De communicatie vanuit deze online voorzieningen met de Belastingdienst is verder identiek aan de invulling van patroon B: de Bapi- en Digipoort-kanalen.

Scenario's

De interactiepatronen uit de vorige paragraaf zijn nader uitgewerkt in scenario's die in de praktijk veel voorkomen. De scenario's 1 t/m 11 zijn opgesteld door de Belastingdienst in het kader van GOA. De overige scenario's zijn opgesteld door SBR.

Toelichting op de uitwerking van de scenario's

1. De rollen en verklaringen worden in meer detail uitgewerkt. De kenmerken van een verklaarder worden bijvoorbeeld specifieker gemaakt. Belangrijk onderdeel daarbij gaat over de identiteit van de verklaarder. Die identiteit zit besloten in de ondertekening van de verklaring. Bijvoorbeeld een identiteitsverklaring wordt geleverd door een authenticatiedienst als verklaarder. Die identiteitsverklaring wordt getekend door de authenticatiedienst. Om de identiteit van die authenticatiedienst betrouwbaar te kunnen vaststellen, dient er een identiteitsverklaring van de authenticatiedienst aanwezig te zijn. Die is niet apart gemodelleerd, maar die wordt geacht onderdeel te zijn van de ondertekening.
2. Het verkrijgen van een verklaring moet ook als een dienst beschouwd worden. Als een ApV een bevoegdheidsverklaring ophaalt bij een machtigingsregister, dan maakt die gebruik van de dienst "verkrijgen bevoegdheidsverklaring". Voor die dienst moet de aanvrager (de ApV) geautoriseerd worden, en ook dat gebeurt op basis van hetzelfde mechanisme van verklaringen. De ApV vraagt een bevoegdheidsverklaring, waarbij de ApV vaak een Belanghebbende is. Als bijv de ApV een Fiscaal Intermediair is, dan wordt de ApV beschouwd als belanghebbende, immers de Fiscaal Intermediair komt voor in de vastgelegde machtiging (tripel).

GOA scenario's

Scenario 1
Mw. de Haan doet IB-aangifte voor zichzelf met behulp van het online portaal van de Belastingdienst (BD).
Er zijn geen speciale vereisten m.b.t. de accordering.

Het aanbieden van de Business transactie samen met de benodigde verklaringen aan de Diensaanbieder gebeurt door het online portaal van de Belastingdienst[12].

Scenario 2
De dochter van mw. de Haan, Marieke, doet de IB-aangifte voor mw. de Haan met behulp van het online portaal van de Belastingdienst.
Er zijn geen speciale vereisten m.b.t. de accordering.

Scenario 3
Mw. Vrij, vrijwilligster (of medewerkster) bij FNV, doet de IB-aangifte voor mw. de Haan met behulp van het online portaal van de Belastingdienst.
Er zijn geen speciale vereisten m.b.t. de accordering.

Scenario 4
Dhr. Kordaat van intermediair Fisk BV (kantoor Utrecht) [13] maakt gebruik van een eigen pakket voor inzending van IB-aangifte van mw. de Haan.
Er zijn geen speciale vereisten m.b.t. de accordering. Er wordt geen gebruik gemaakt van de portaal van de Belastingdienst. Er wordt rechtstreeks met het backend van de Belastingdienst gecommuniceerd.

Scenario 5
Mw. Slob, medewerkster van Gigant NV, maakt de Vpb-aangifte van Gigant op in het eigen administratiepakket Gigaview en verzendt deze vanuit dit pakket naar de Belastingdienst.
Er zijn geen speciale vereisten m.b.t. de accordering.
Er wordt geen gebruik gemaakt van de portaal van de Belastingdienst. Er wordt rechtstreeks met het backend van de Belastingdienst gecommuniceerd.

Scenario 6
De hr. Kordaat van intermediair Fisk BV (kantoor Utrecht) maakt gebruik van een eigen administratiepakket voor het opstellen en inzenden van de Vpb-aangifte van Gigant NV aan de Belastingdienst.
Er zijn geen speciale vereisten m.b.t. de accordering.
Er wordt geen gebruik gemaakt van de portaal van de Belastingdienst. Er wordt rechtstreeks met het backend van de Belastingdienst gecommuniceerd
Scenario 6 is vergelijkbaar met scenario 4. In scenario 4 is de belanghebbende een burger in scenario 6 is dit een bedrijf.

---

12 In de uitwerking wordt er vanuit gegaan dat de Haan gebruik maakt van het online portaal van de BD ook wanneer er sprake is van een lokaal draaiend aangifteprogramma. In het laatste geval verzamelt dit programma slechts de business gegevens (business load van het bericht).

13 Dat de aangifte wordt verzorgd vanuit de kantoor Utrecht van Fisk BV is in feite niet relevant; dit kantoor is geen zelfstandige juridische entiteit.

Scenario 7
Dhr. Kordaat van Fisk BV (kantoor Utrecht) maakt gebruik van een SaaS-pakket van Zaas BV voor opmaken en inzenden van de Vpb-aangifte van Gigant NV.
Uitgangspunt bij dit scenario's is dat het Saas-pakket van Zaas BV gebruik maakt van het certificaat van Fisk BV en dan is dit scenario hetzelfde als scenario 6. Er wordt weliswaar gebruik gemaakt door Fisk van het SaaS pakket van Zaas BV, maar dat gedraagt zich alsof het een eigen pakket is van Fisk Bv. Het wordt anders wanneer het SaaS-pakket geen gebruik maakt van het certificaat van Fisk Bv. In dat geval is er ook een bevoegdheidsverklaring nodig van Fisk BV naar het SaaS pakket van Zaas BV.

Scenario 8
Dhr. Kordaat van Fisk BV (kantoor Utrecht) zet de Vpb-aangifte die hij heeft opgesteld voor Gigant NV klaar in het eigen portaal van Fisk BV. De heer Steur (bestuurder van Gigant NV) ondertekent de aangifte in het Fisk-portaal en verzendt deze vanuit het portaal naar de Belastingdienst.
Voor accordering wordt gebruik gemaakt van een eigen certificaat van Steur of door een ondertekendienst waar Steur gebruik van kan maken.
Voor de verzending vanuit het portaal naar de Belastingdienst wordt er gebruik gemaakt van S2S koppelvlakken.

Scenario 9a (geen keten van machtigingen)
Fisk BV heeft opdracht om de Vpb-aangifte van Gigant NV te verzorgen. Fisk besteedt deze uit aan Zaas BV. Mw. Sas van Zaas zendt de Vpb-aangifte in met behulp van het pakket Sala van Zaas.
In dit scenario wordt er vanuit gegaan dat het pakket van Zaas kan werken met het certificaat van Fisk BV. Het Zaas pakket gedraagt zich dan alsof het een pakket is van Fisk BV.
Dit scenario is identiek aan scenario 7.

Scenario 9b (met keten van machtigingen)
Fisk BV heeft opdracht om de Vpb-aangifte van Gigant NV te verzorgen. Fisk besteedt deze uit aan Zaas BV. Mw. Sas van Zaas zendt de Vpb-aangifte in met behulp van het pakket Sala van Zaas.
In dit scenario wordt er vanuit gegaan dat het pakket van Zaas BV niet kan werken met het certificaat van Fisk BV. Zaas BV maakt dus gebruik van haar eigen certificaat. Dit betekent dat Zaas BV de bevoegdheid moet hebben om de machtiging die Gigant NV aan Fisk BV heeft verstrekt om de Vpb-aangifte te doen te gebruiken. Fisk BV moet Zaas BV dus machtigen voor het indienen van de Vpb-aangifte van Gigant. Deze machtiging betekent overignes niet dat Zaas BV ook de Vpb aangifte van Fisk Bv mag doen.

Scenario 10
Dhr. Kordaat van Fisk BV (kantoor Utrecht) zet de Vpb-aangifte die hij heeft opgesteld voor Gigant NV klaar in het portaal van Zaas BV. Zaas verzorgt de ondertekening (signingdienst) en indiening van de aangifte bij de Belastingdienst. Voor de Belastingdienst is Zaas BV dus de handelende partij
In dit scenario wordt er vanuit gegaan dat Fisk BV geen gebruik maakt van een eigen certificaat om een verklaring te ondertekenen. Fisk BV levert de ruwe data aan die door Zaas BV verder verwerkt worden tot een Vpb-aangifte.
Tevens wordt er in dit scenario vanuit gegaan dat Gigant NV Fisk BV heeft gemachtigd haar Vpb-aangifte te doen. Aansluitend heeft Fisk BV Zaas BV gemachtigd om de Vpb-aangifte van Gigant NV in te dienen bij de Belastingdienst.

Overdenking:
Zaas BV zal voor al haar klanten een machtiging moeten hebben. De vraag is hoe Zaas BV betrouwbaar kan vaststellen wie iets klaar gezet heeft in het portaal. Indien zij dit niet goed regelt kan er eenvoudig misbruik worden gemaakt van de machtigingen die Zaas BV bezit. Om dit te voorkomen zou de handelende partij niet Zaas moeten zijn maar Fisk BV terwijl Zaas BV middels een machtiging aan moet tonen dat zij ApV mag zijn. Dit zou betekenen dat er nog een andere vorm van machtiging mogelijk moet zijn namelijk een ApV machtiging (zie ook verderop)

Scenario 11
Mw. Slob van Gigant NV dient de OB-aangifte van Gigant in via het online portaal van de Belastingdienst. Zij is alleen bevoegd voor de OB-aangiftes, haar collega verzorgt de Vpb-aangifte. Voor de Backend Belastingdienst maakt het niet uit wie de OB-aangifte van Gigant NV instuurt zolang maar duidelijk is dat het van Gigant NV komt als handelende partij. Het portaal van de Belastingdienst kan echter besluiten om een differentiatie in bevoegdheden te ondersteunen net zoals dat in een eigen applicatie van Gigant NV mogelijk zou zijn. Als we uitgaan van authenticatie (van Gigant NV) via eHerkenning dan kan het portaal eisen dat deze authenticatie alleen lukt wanneer de natuurlijk persoon die deze authenticatie uitvoert ook de bevoegdheid heeft om de OB-aangifte namens Gigant NV te doen. In het authenticatieverzoek aan eHerkenning wordt dan dus ook een bevoegdheidsvraag meegegeven. Het waarborgen dat mw. Slob alleen maar de OB-aangifte van Gigant NV in kan dienen ligt bij de Portaal van de Belastingdienst en niet bij het Backend van de Belastingdienst. Deze scheiding van verantwoordelijkheid komt overeen met de situatie wanneer er gebruik wordt gemaakt van een eigen pakket door Gigant NV. Dit pakket zal er dan voor moeten zorgen dat mw. Slob alleen de OB-aangifte in kan dienen en haar collega alleen de Vpb-aangifte. Ook in deze situatie is de backend van de Belastingdienst alleen geïnteresseerd of de aangifte van Gigant NV komt en niet welke natuurlijke persoon deze aangifte heeft verzorgd.

SBR scenario's
De volgende hoofdscenario's zijn onderkent voor SBR.
Deze scenario's zijn vergeleken met de GOA scenario's. Bij de scenario's is aangegeven of er een overeenkomstig GOA scenario is. Is dit het geval dan wordt alleen aangegeven wie welke rol speel. Is dit niet het geval dan is het scenario uitgewerkt.

1. Rapportage door de ondernemer met eigen certificaat.

Een bedrijf verzorgt de eigen boekhouding, met eigen software en een eigen certificaat
- Er is geen machtiging nodig, identiteit van het bedrijf komt uit certificaat.
- Het bedrijf is zelf verantwoordelijk voor het intern machtigen van medewerkers om gebruik te maken van het certificaat.
- Wanneer er iets mis lijkt te gaan, kan direct met het bedrijf contact worden opgenomen.

Dit scenario komt overeen met het GOA Scenario 5.

2. Rapportages door intermediair met eigen certificaat.

Een bedrijf laat zijn boekhouding verzorgen door een intermediair, die ook de rapportages naar de Belastingdienst, banken en KvK verzorgt. De intermediair heeft een eigen certificaat. Er is een interne mandatering, die bepaalde medewerkers machtigt om rapportages te verzorgen. De interne systemen zijn hierop ingeregeld.
- Degene op wiens naam het certificaat is afgegeven, blijft verantwoordelijk voor het correcte gebruik van dat certificaat.
- Wanneer er iets mis lijkt te gaan, is er altijd een contactpersoon aangewezen bij de intermediair om e.e.a. na te trekken.
- Omdat de intermediair verantwoordelijk is voor het correct aanleveren van de rapportage namens de ondernemer, is alles goed na te trekken.
- Het is de verantwoordelijkheid van de intermediair om te zorgen dat enkel daartoe bevoegde medewerkers rapportages kunnen versturen of gegevens kunnen opvragen.
- Het is de gezamenlijke verantwoordelijkheid van de intermediair en de ondernemer om te zorgen dat de machtiging correct is vastgelegd.

Dit scenario komt overeen met het GOA-scenario 6.

3. Rapportage door een ondernemer via een online boekhoudpakket

Een bedrijf A voert zelf de eigen boekhouding, en maakt daarbij gebruik van een online boekhoudpakket van aanbieder B. De aanbieder B heeft daarbij een eigen certificaat geïnstalleerd. De ondernemer A is zelf verantwoordelijk voor het machtigen van medewerkers die de boekhouding verzorgen.

- Wanneer de ondernemer A een rapportage aanlevert, ziet de ontvangende partij dat dit met een certificaat van aanbieder B wordt gedaan.
- Wanneer een machtiging vereist is als men niet met eigen certificaat aanlevert of opvraagt, zal die machtiging gegeven moeten zijn aan de online aanbieder B.
- Wanneer er iets mis lijkt te zijn, wordt contact opgenomen met aanbieder B, als houder van het certificaat en gemachtigde namens het bedrijf A. Aanbieder B zal moeten bevestigen voor welke ondernemer de rapportage is verzonden of gegevens zijn opgevraagd. Het feit dat aanbieder B daar zijn medewerking aan moet verlenen, zal vastgelegd moeten worden. De ondernemer A die volgens de machtigingen de rapportage aanlevert of opvraagt, is uiteraard ook aanspreekbaar.
- Een aandachtspunt is dat wanneer het een andere klant (C) van aanbieder B lukt om namens bedrijf A een rapportage in te dienen, dit enkel via de interne logging van aanbieder B te achterhalen is. Voor zowel A als C geldt immers dat aanbieder B gemachtigd is.
- Aanbieder B kan niet (zomaar) aansprakelijk gehouden worden voor incorrecte aanleveringen. Wel is hij eerste aanspreekpunt in geval van ongeregeldheden.
- Wanneer er (zeer) geregeld problemen zijn met een bepaalde aanbieder van een online boekhoudpakket, kunnen maatregelen worden getroffen tegen deze partij. De ultieme sanctie is uiteraard dat niet meer mag worden aangeleverd via de diensten van aanbieder B.

Een apart punt is dat bedrijf A zal moeten inloggen op het boekhoudpakket. Daar zijn diverse mogelijkheden voor, die ieder voor zich weer gebruik zou kunnen maken van eHerkenning.

Dit scenario heeft geen overeenkomstig GOA-scenario.

In dit scenario handelt Bedrijf B namens Bedrijf A en Bedrijf B moet dan ook gemachtigd zijn om namens bedrijf A te handelen. Dat de medewerkers van Bedrijf A de handelingen uitvoeren doet niet ter zake.

4. Rapportage door intermediair via een online boekhoudpakket.

Een bedrijf laat de boekhouding uitvoeren door een intermediair, die zelf weer gebruik maakt van een online boekhoudpakket van aanbieder B.

- Er is hier sprake van een cascade van machtigingen: de ondernemer machtigt de intermediair, die zelf weer de online dienstverlener machtigt.
- De ontvangende uitvragende partij ziet dat een rapportage met een certificaat van de online dienstverlener plaatsvindt. Bij de machtigingen blijkt dat die terug te voeren zijn op de ondernemer namens wie wordt gerapporteerd.
- Wanneer er iets mis lijkt te gaan, kan alles via online dienstverlener en intermediair nagetrokken worden.
- Aanbieder B kan niet (zomaar) aansprakelijk gehouden worden voor incorrecte aanleveringen. Wel is hij een aanspreekpunt in geval van ongeregeldheden. Ook het feit dat hij daar zijn medewerking aan moet verlenen, zal vastgelegd moeten worden. De intermediair die volgens de machtigingen de rapportage aanlevert of opvraagt, is uiteraard ook aanspreekbaar.
- Wanneer er (zeer) geregeld problemen zijn met een bepaalde aanbieder van een online boekhoudpakket, kunnen maatregelen worden getroffen tegen deze partij. De ultieme sanctie is uiteraard dat via de diensten van aanbieder B (eventueel tijdelijk) geen rapportages worden aanvaard. Het is aan de uitvragende partijen om daarover te beslissen. Zij zijn ook degene die ervoor moeten zorgen dat sancties tegen aanbieder B juridisch acceptabel zijn.

- Het is de gezamenlijke verantwoordelijkheid van de intermediair en de ondernemer om te zorgen dat de machtiging correct is vastgelegd.
- Het is de verantwoordelijkheid van de intermediair om te zorgen dat enkel daartoe bevoegde medewerkers rapportages kunnen versturen of gegevens kunnen opvragen.

Dit scenario komt overeen met het GOA-scenario 10.

5. Rapportage door ondernemer met certificaat van leverancier van softwarepakket

Wanneer een softwareleverancier één certificaat meelevert met alle installaties, wordt het voor de uitvragende partij niet mogelijk te zien wie nu daadwerkelijk aanlevert. Alle aanleveringen gebeuren immers met hetzelfde certificaat, dat de softwareleverancier als eigenaar aangeeft.

- Wanneer de ondernemer A een rapportage aanlevert, ziet de ontvangende partij dat dit met een certificaat van de softwareleverancier wordt gedaan.
- Wanneer er iets mis lijkt te gaan, wordt contact opgenomen met de softwareleverancier. Die kan echter niet (eenvoudig) zien voor wie de aanlevering bestemd was. Hij heeft immers geen controle over wie met het systeem werkt.
- Vastleggen van een machtiging op naam van de softwareleverancier zal in dit geval weinig helpen, want het blijft onmogelijk om na te gaan wie er dan aangeleverd heeft. Verwacht mag worden dat geen enkele softwareleverancier een log kan inzien waarin staat welke gebruiker van die software op welk moment aan welke uitvragende partij welk bericht aangeleverd heeft. Het is ook niet te verwachten dat de gebruikers van die software dat zouden accepteren.

Dit scenario heeft geen overeenkomstig GOA-scenario.

Bij de uitwerking van dit scenario is de aanname gemaakt dat de software de mogelijkheid heeft om betrouwbaar vast te stellen welke onderneming deze software gebruikt.
Deze informatie wordt gebruikt om de benodigde machtiging op te vragen bij een machtigingenregister.

Bijlage 2: Ecorys onderzoek naar financieel model

1

Achtergrond en leeswijzer

eHerkenning is de structurele voorziening voor het elektronisch kunnen herkennen van (medewerkers van) bedrijven en is daarmee de opvolger van DigiD Bedrijven. Deze herkenning is noodzakelijk om de identificatie en controle van de afnemer van elektronische overheidsdiensten uit te kunnen voeren. De implementatie van eHerkenning kenmerkt zich door het welbekende kip-ei probleem. De overgang naar eHerkenning wordt pas mogelijk wanneer overheidsdienstverleners voldoende digitale diensten via eHerkenning aanbieden. De diensten worden echter pas 'rendabel', wanneer voldoende eindgebruikers (bedrijven) beschikken over eHerkenningsmiddelen om deze diensten af te nemen. Maar het wordt pas interessant voor eindgebruikers om een eHerkenningsmiddel aan te schaffen, wanneer er voldoende digitale diensten met eHerkenning worden aangeboden. Dit bemoeilijkt de financiering op de korte termijn.

Op termijn is financiering van het systeem relatief eenvoudig, er zijn immers genoeg gebruikers die voor de middelen en diensten willen betalen, zeker als bedrijven onderling via eHerkenning elektronisch zaken gaan doen. De crux zit in het vinden van een adequaat financieringsmodel voor de groeifase. De kosten moeten uiteraard worden gedekt, maar de kosten voor het bedrijfsleven mogen niet te hoog zijn, anders gaan zij de middelen niet aanschaffen en komt eHerkenning niet van de grond. Volledige subsidiering door de overheid is ook geen reële optie, een gezonde marktwerking staat immers voorop.

Deze rapportage biedt inzicht in de mogelijkheden om in de groeifase voor het systeem van eHerkenning *tot een verdeelsleutel te komen die de implementatie en het gebruik van eHerkenning niet belemmert, maar juist bevordert*. Er wordt eerst inzicht geboden in *wie betaalt wat*? Vervolgens wordt er ook gekeken naar de wijze waarop de financiering kan worden opgezet en welke prijzen daar bij horen. Uitgangspunt hiervoor vormt de eerder opgestelde kosten-batenanalyse, welke medio 2011 is opgesteld voor het Ministerie van EL&I. Het voordeel van deze basis is dat er niet alleen inzicht is in wie de kosten maakt (niet betaalt!), maar tevens wat het de verschillende partijen oplevert.

Volwassen marktfase

Wanneer de markt volwassen is, dan is er voldoende aanbod van diensten (ook bedrijven onderling, B2B). Er is tevens voldoende vraag naar diensten door de bedrijven. De vaste kosten van het stelsel kunnen dan worden terugverdiend door middel van een groot aantal transacties, waarbij de kosten per transactie relatief laag zijn. eHerkenningsmiddelen vertegenwoordigen voldoende waarde voor bedrijven en kennen een relatief lage prijs. Het is dus interessant voor bedrijven om in het bezit te zijn van eHerkenningsmiddelen en om deze te gebruiken.

Financieringsbehoefte en -ruimte

De totale financieringsbehoefte is uiteraard nog wat lastig in te schatten, omdat nog niet bekend is hoe groot de markt op termijn zal gaan worden, maar er kan ten minste aan ongeveer 10 miljoen euro per jaar worden gedacht. Tegenover de financieringsbehoefte staat de financieringsruimte. Deze is voldoende groot, de jaarlijkse baten voor overheidsdienstverleners van eHerkenning bedragen ongeveer zes miljoen euro en de jaarlijkse baten voor bedrijven bedragen ruim 15 miljoen euro. Er is dan dus voldoende ruimte voor de financiering

Financieringsmodel

In een volwassen markt, is het aan te raden om te kiezen voor een iDeal achtige oplossing voor de financiering. Dit zou voor de financiering van eHerkenning het volgende betekenen:

- Overheidsdienstverleners betalen voor alle kosten die samenhangen met de transacties;
- Bedrijven betalen voor alle kosten die samenhangen met de eHerkenningsmiddelen.

Een belangrijk argument hiervoor is dat in de volwassen fase eindgebruikers (bedrijven) ook voordeel hebben van het eHerkenningsmiddel in haar B2B toepassingen. Door de mogelijkheid om

te betalen per transactie wordt het ook voor banken interessant om met hun bankmiddelen toe te treden tot de markt van eHerkenning. Overheidsdienstverleners staat het vrij in deze situatie om afspraken met authenticatie service providers te maken voor een betaling per transactie dan wel een betaling in de vorm van abonnementen.

Belangrijk is ook dat er een set van afspraken is tussen alle authenticatie service providers, waarin onder meer de onderlinge vergoedingen zijn vastgesteld. In deze fase is het belangrijk dat er een stabiele keten is. Alle verschillende rollen (middelenuitgever, machtigingenregister, authenticatiediensten en herkenningsmakelaar) binnen het stelsel van eHerkenning moeten een lange termijn duurzaam resultaat behalen. Het is overigens aan de authenticatie service providers onderling om hier afspraken over te maken.

Er bestaan verschillende succesvolle voorbeelden van vergoedingensystemen voor vergelijkbare markten als eHerkenning. Hier kan gedacht worden aan iDeal of aan point-of-sale transacties in winkels. Het is aan te raden om voor eHerkenning een vergelijkbare systematiek te ontwikkelen. Voor de hand ligt dat de authenticatie service providers in samenwerking met de banken een vergelijkbare systematiek ontwikkelen.

Groeifase
Wanneer de markt nog niet volwassen is, dan is er nog onvoldoende aanbod van diensten (B2B is er dan nog niet). Er is onvoldoende vraag naar diensten door bedrijven. De vaste kosten van het stelsel kunnen nog niet worden terugverdiend vanwege het beperkte aantal transacties, waarbij de kosten per transactie relatief hoog zijn. eHerkenningsmiddelen vertegenwoordigen nog onvoldoende waarde voor bedrijven en kennen een relatief hoge prijs. Het is dus nog niet interessant voor bedrijven om in het bezit te zijn van eHerkenningsmiddelen en om deze te gebruiken.

Financieringsbehoefte en -ruimte
Het is de verwachting dat de totale kosten voor het stelsel in de eerste jaren ongeveer 2 tot 4 miljoen euro per jaar bedragen. Tegenover de financieringsbehoefte staat de financieringsruimte. Deze is in beginsel voldoende groot, de baten voor overheidsdienstverleners groeien van nul naar acht miljoen euro per jaar en de baten voor bedrijven bedragen groeien van 0 naar 5 miljoen euro per jaar. Er zou in beginsel voldoende ruimte zijn voor de financiering, ware het niet dat de kosten voor de baat uitgaan.

Daar komt ook nog bij dat de investeringen in eHerkenning pas op de langere termijn worden terugverdiend. Zeker voor bedrijven (die werken met relatief korte investeringshorizonnen – bijvoorbeeld maximaal twee jaar) is een investering in eHerkenningsmiddelen niet binnen de gewenste periode terugverdiend. Uit zichzelf zullen bedrijven dan ook niet snel eHerkenningsmiddelen aanschaffen. En dat zou betekenen dat eHerkenning niet in een volwassen markt terecht zal komen.

Vanuit de marktstructuur van de tweezijdige markt is er al wel de incentive om eindgebruikers (bedrijven) lagere prijzen in rekening te brengen dan met normaal zou verwachten. Dit is positief omdat hiermee de marktwerking bijdraagt aan het stimuleren van het gebruik van eHerkenning. De eerste jaren zal er echter wel geld bij moeten om eHerkenning van de grond te krijgen (de kosten zijn hoger dan de baten). Pas op langere termijn worden de kosten terugverdiend. De groeifase zou daarom zo kort mogelijk moeten duren, een kortere groeifase betekent dat er eerder een volwassen markt ontstaat, waar geen geld meer bij hoeft. Een te lange groeifase zou er in theorie zelfs toe kunnen leiden, dat de markt nooit in de volwassen fase terecht komt, met het gevolg dat op een gegeven moment authenticatie service providers zich vanwege aanhoudende verliezen terug trekken uit de markt. Bij de inrichting van het financieringsmodel voor de groeifase, is het dan ook van het grootste belang dat de keuzes die worden gemaakt bijdragen aan het verkorten van deze groeifase.

Financieringsmodel
Voor het financieringsmodel, is het daarom ook van belang om de huidige situatie te doorbreken. Hiervoor is het volgende nodig:

- Stimuleren van het aanbod van eHerkenningsdiensten door overheidsdienstverleners. Er moet in het bijzonder worden ingezet op killer apps.
- Stimuleren van het gebruik van eHerkenningsmiddelen door bedrijven. Hiervoor bestaan – in theorie – drie verschillende alternatieven:
    1. Verplichten van gebruik. Vanuit de financieringskant beschouwd betekent dit dat in de groeifase alle kosten samenhangend met de eHerkenningsmiddelen door het bedrijfsleven worden gedragen.
    2. Subsidiëren van de aanschaf van eHerkenningsmiddelen. Dit kan direct via de eindgebruikers (bedrijven) of indirect via de authenticatie service providers.
    3. Hergebruik van bankmiddelen. Hierdoor dalen de totale kosten voor het stelsel en leidt daarmee tot een lagere financieringsbehoefte.

Wanneer wordt gekozen voor het subsidiëren van de aanschaf van eHerkenningsmiddelen dan is het uiteraard van belang om te kijken wat gesubsidieerd moet worden, hoeveel en hoe dit het beste geregeld kan worden.

Wanneer het uitgangspunt van de volwassen markt wordt gehanteerd (overheidsdienstverleners betalen voor transacties en bedrijven betalen voor eHerkenningsmiddelen) dan zou dit betekenen dat in de groeifase ongeveer 2/3 van de financiering (1 tot 2,5 miljoen euro per jaar) wordt betaald door overheidsdienstverleners en ongeveer 1/3 van de financiering door het bedrijfsleven (0,5 tot ruim 1 miljoen euro per jaar). Per overheidsdienstverlener gaat het dan om een gemiddeld bedrag van 25.000 tot 50.000 euro per dienst. De bedrijven betalen dan voor de aanschaf van een middel en voor het jaarlijkse gebruik. Deze verdeling hangt ook samen met het feit dat nog relatief weinig bedrijven in de groeifase een eHerkenningsmiddel bezitten. De kosten per bedrijf (tot 30 euro voor niveau II per jaar) voor de investering in eHerkenningsmiddelen liggen bij deze verdeelsleutel dan nog wel boven de huidige betalingsbereidheid van ongeveer 20 euro per jaar.

Een bijdrage voor de aanschaf van eHerkenningsmiddelen is daarom een interessant instrument om het gebruik van eHerkenning te stimuleren. Hierbij is het overigens niet noodzakelijk om de volledige aanschaf kosten te financieren, wanneer de kosten voor de aanschaf ongeveer 50 procent lager zijn dan wordt het voor bedrijven wel weer interessant om eHerkenningsmiddelen aan te schaffen (meer in lijn met de betalingsbereidheid van bedrijven en met een korte investeringshorizon). Een totale subsidiebijdrage van tussen de 1 en 2 miljoen euro zou ervoor kunnen zorgen dat meer dan 100 duizend bedrijven op korte termijn over gaan op eHerkenning.4 Tot slot zijn er verschillende manieren om de bijdrage van de overheid vorm te geven. Dit kan via de belastingen (middels afschrijvingen) of via een subsidieregeling. Mocht gekozen worden voor een vorm van subsidiëring in de groeifase, dan is het aan te raden om te kiezen voor een soort van Algemeen Fonds waaruit middelen worden gesubsidieerd. Dit fonds kan gevuld worden door bijdragen van de verschillende betrokken overheidsdienstverleners. Hiermee wordt voorkomen dat er voor overheidsdienstverleners een soort van ‘first mover disadvantage’ ontstaat, waardoor het benodigde aanbod toch niet wordt gerealiseerd.

Het verdient aanbeveling een plafond aan het totale subsidiebedrag te koppelen, zodat er een stimulans ontstaat om snel over te gaan tot aanschaf. Het subsidiebedrag zal ook in drie jaar trapsgewijs kunnen worden afgebouwd, als het bedrijfsleven nut en noodzaak van aanschaf meer gaat inzien en de gebruiksmogelijkheden toenemen.