Advies van de commissie evaluatie pilots publieke en private authenticatiemiddelen (commissie-Kuipers)

Commissie bestaande uit:

drs. R.IJ.M. Kuipers

prof. dr. E.A. van Zoonen

mr. C.J. van der Horst

dr. A. Zuurmond

31 mei 2016

1. Samenvatting

De commissie-Kuipers (verder vaak 'de commissie') onderschrijft het grote belang en tevens de urgentie van een versterking van het instrumentarium van elektronische authenticatie. Zowel de maatschappelijke en de technologische ontwikkelingen als ook de eigen overheidsambities op het vlak van de digitale dienstverlening (Digitale Agenda 2017), nopen tot een slagvaardige aanpak, ook op het vlak van een hoogwaardige authenticatievoorziening. In de afgelopen jaren is op dat laatste vlak weinig voortgang geboekt. De nu door het kabinet voorgenomen multimiddelenaanpak, toegespitst op toegang tot het BSN-domein, biedt, naar het oordeel van de commissie, ten principale een goed perspectief. Via de evaluatie van een aantal pilots hebben we ons een beeld gevormd hoe kansrijk die aanpak daadwerkelijk is.

Op basis van de onderzoeksrapportages van Panteia en TNO, alsmede op basis van haar eigen waarnemingen bij de pilots, komt de commissie tot de conclusie dat uit de gehouden pilots met diverse (nieuwe) authenticatiemiddelen geen onoverkomelijke obstakels zijn gebleken voor de totstandkoming van de beoogde multimiddelenaanpak. Zowel op het vlak van het gebruiksgemak als ook op aspecten als technische degelijkheid, pricacybescherming en ervaringen van de aanbieders van middelen, diensaanbieders en gemeenten, geven de pilots acceptabele tot zelfs gunstige uitkomsten te zien. De onderzoeksuitkomsten indiceren dat de multimiddelenaanpak blijkt te (kunnen) werken. Wel hebben de pilots en de onderzoeken die daarnaar zijn verricht, behartenswaardige inzichten opgeleverd die om een oplossing vragen (bijvoorbeeld de gebleken problemen bij het installeren en hanteren van de kaartlezer bij met name de eNIK, alsmede een aantal issues rond de privacy), en aanbevelingen die daarbij benut kunnen worden.

Op basis hiervan komt de commissie tot de conclusie dat er, op basis van de uitgevoerde pilots, goede grond is om, met inachtneming van de bevindingen uit de pilots, te komen tot zo concreet mogelijke en implementatiegerichte vervolgstappen in de multimiddelenaanpak.

Bij deze conclusie past de kanttekening dat de pilots slechts een beperkte strekking hadden; dat was overigens van tevoren bekend. Zo richtten de verschillende pilots zich vooral op het toetsen van afzonderlijke authenticatiemiddelen en slechts in beperkte mate op het naast elkaar hanteren van verschillende nieuwe authenticatiemiddelen. Daarnaast zijn de pilots (nog) niet specifiek gericht geweest op kwetsbare groepen, zoals laagopgeleiden, 'digibeten', ouderen en jongeren. De commissie adviseert in het vervolgtraject ook hier nadere pilots aan te wijden. Meer in het algemeen adviseert de commissie tot een aanpak waarin concrete en behapbare stappen pas gezet worden wanneer in pilots is gebleken dat ze kunnen gaan werken.

Aan de commissie is ook gevraagd om advies uit te brengen over de na de evaluatie te ondernemen vervolgstappen.
In dat kader merkt de commissie op dat, naast datgene wat in de pilots is verkend, er nog tal van andere zaken zijn die geregeld moeten worden, wil de multimiddelenaanpak als geheel kunnen gaan 'vliegen'. Dat geldt voor de totstandkoming van het beoogde publieke middel; denk onder andere aan de bekostigingsvraag. Maar ook het gaan functioneren van de private authenticatiemiddelen (iDIN respectievelijk Idensys) in het BSN-domein zal, zowel van overheidszijde als van de kant van de desbetreffende private aanbieders, nog de nodige keuzes en inspanningen vergen. Voor de private

partijen moet er ook voldoende perspectief ontstaan om in de aanpak rond het BSN-domein te gaan participeren. Voor de overheid zitten daar ook budgettaire consequenties aan vast die nog in kaart moeten worden gebracht.
Daarenboven vergt de multimiddelenaanpak als geheel, dus in overkoepelende zin, nog de nodige besluitvorming. Hoe blijft de overheid (samen met de betrokken private partijen) waarborgen dat de burger 'ontzorgd' wordt, zowel qua gebruiksgemak als qua privacy? De commissie adviseert om het burgerperspectief hoog in het vaandel te houden. Denk in dit verband aan bijvoorbeeld de zogeheten 'stop-ID-faciliteit'; we komen daar nog op terug. Bij de keuzes voor en de ontwikkeling van middelen moet daarnaast ingespeeld worden op de maatschappelijke realiteit van een steeds sneller toenemend gebruik van mobiele devices, ook in het elektronische verkeer tussen burgers en aanbieders van publieke diensten.
Ook moet nog nader uitkristalliseren hoe de overheid (opnieuw samen met de betrokken private partijen) ervoor zorgt dat de aanbieders van publieke diensten zonder al te grote problemen aan alle voorwaarden van de nieuwe authenticatiemiddelen kunnen voldoen.

De commissie heeft inmiddels tevens kennis genomen van het zogeheten BIT-advies (de dato 12 mei 2016) rond het eID-programma. In dit BIT-advies is niet gekeken naar de pilots en de evaluatie daarvan, maar naar andere aspecten van het eID-programma. Als spiegelbeeld geldt dat aan de commissie-Kuipers niet is gevraagd de programmatische aanpak van het eID-programma onder de loep te nemen. De commissie beschouwt het werk van haarzelf respectievelijk van het BIT, dan ook als nagenoeg geheel complementair.
Hoewel de commissie-Kuipers zich (dus) niet met grote diepgang heeft begeven op de terreinen waarop het BIT-advies ingaat, heeft de commissie zich, tijdens haar werkzaamheden, wel een redelijk beeld kunnen vormen van de aspecten waarop het BIT-advies ingaat. Vanuit dat beeld merkt de commissie op dat zij het BIT-advies in hoge mate herkent (met de aantekening dat de commissie, op basis van de rapportage van Panteia, tot een minder ongunstig oordeel komt over het gebruiksgemak van het publieke middel) en waardevol acht. Voor een succesvolle implementatie van de multimiddelenaanpak achten wij daarom - op hoofdlijnen - navolging van de aanbevelingen van het BIT-advies van belang.
Op enkele onderdelen van ons oordeel en onze adviezen, raken we aan elementen van het BIT-advies. Dat is dan bedoeld als een aantal aanvullende noties.

Alles overziende concludeert de commissie dat er voldoende aanleiding is om te komen tot zo concreet mogelijke vervolgstappen in de multimiddelenaanpak. Daarbij zal langs een tweetal lijnen nog veel werk verzet moeten worden.

De eerste lijn betreft het *overkoepelend niveau*: het niveau van de drie sporen (publiek middel, iDIN-middelen en Idensysmiddelen) gezamenlijk.
Zoals gezegd: boven alles moet goed nagedacht worden over de vraag in hoeverre het eindresultaat van alles waartoe nog besloten moet worden, mede ten dienste staat van de uiteindelijke gebruikers van de authenticatiemiddelen, in casu de burgers en de dienstaanbieders in het BSN-domein. Dit vereist zowel goed doordachte keuzes als een uitgekiende communicatiestrategie.
Daarnaast vergen diverse keuzes nog nadere doordenking en explicitering. Denk aan de vraag hoe de businessmodellen in de diverse sporen vorm zullen gaan krijgen en hoe de overheid de daartoe benodigde besluitvormingsmechanismen vorm gaat geven en hoe een en ander budgettair gedekt gaat worden. Denk ook aan de vraag welke betrouwbaarheidsniveaus qua authenticatie gehanteerd

zullen gaan worden in het BSN-domein en in hoeverre eventuele uiteenlopende niveaus gaan interfereren met de techniek van de middelen. Ook kan gedacht worden aan de vraag waar de afbakening van het BSN-domein nu ligt en in de toekomst kan komen te liggen.
Daarnaast doet zich op overkoepelend niveau de vraag voor welke centrale voorzieningen cruciaal zijn voor het functioneren van de multimiddelenaanpak, alsmede de vraag in hoeverre er behoefte kan zijn aan - tijdelijke - ondersteuning van partijen met het oog op aansluiting op de diverse authenticatiemiddelen.

De tweede lijn is dat er voor *elk van de drie te onderscheiden sporen* heel eigen, ongelijksoortige opgaven zijn die om een oplossing vragen.
Voor het spoor van het publieke middel moet besloten worden hoe zich dit verhoudt tot het huidige DigiD en hoe de ontwikkelingen binnen het publieke spoor budgettair ingepast kunnen worden. Daarnaast doet zich de vraag voor in welk tempo en in welke fasering respectievelijk volgens welk stappenplan het nieuwe publieke middel valt uit te rollen; de RDA-oplossing waarmee (parallel aan de andere uitgevoerde pilots) een aparte pilot heeft plaatsgevonden bij RDW, kan daarbij een nuttige tussenstap zijn. Ook lijkt het cruciaal een oplossing te vinden voor de problemen die in de eNIK-pilot gebleken zijn met het installeren en hanteren van de kaartlezer; wellicht kan op korte termijn winst geboekt worden door hierbij ook het gebruik van mobiele devices mogelijk te maken.
Voor de iDIN-middelen geldt dat die middelen reeds breed in Nederland beschikbaar zijn: het gaat immers om de bestaande (en toekomstige) bankenmiddelen. Daarvoor bestaat al een grote - private - markt. De vraag die zich voordoet, is hoe deze middelen ook in het BSN-domein grootschalig bruikbaar kunnen worden gemaakt. Daarbij lijkt met name de reeds genoemde vraag naar de businessmodellen (in casu de ‘pricing’) een cruciale te zijn.
Voor de Idensysmiddelen geldt, anders dan voor de iDIN-middelen, dat er nog geen grootschalige markt tot ontwikkeling heeft kunnen komen in Nederland. In andere landen ligt dat soms anders, maar is de context vaak ook een andere. Hier doet zich dus met name de vraag voor of en hoe de desbetreffende markt een kans kan krijgen tot ontplooiing te komen. Dat kan te maken hebben met de eerder bedoelde vraag rond businessmodellen en pricing, maar ook met zaken als acceptatie door burgers en de haalbaarheid voor dienstaanbieders. Hiertoe zou mede gekeken moeten worden naar de aansluitondersteuning.

De commissie bepleit over de hele linie van het vervolgtraject een aanpak met enerzijds een redelijk uitgekristalliseerde, maar niet in beton gegoten stip op de horizon en met anderzijds een implementatietraject van relatief bescheiden, behapbare maar tegelijkertijd betekenisvolle stappen voorwaarts, liefst per stap onderbouwd met gerichte nadere pilots. De commissie adviseert daarbij tevens om met enige regelmaat, liefst door mensen die juist niet middenin de programmatische aanpak zitten, de ‘peilstok’ erin te (laten) steken: is de voortgang adequaat, is de richting nog steeds goed, wordt de samenhang der dingen voldoende bewaakt, is realisatie van de voornemens binnen de gewenste tijdlijnen nog realistisch en dergelijke vragen.

2. Inleiding

In deze rapportage brengt de commissie-Kuipers (in het vervolg ook vaak aangeduid als 'de commissie') u advies uit naar aanleiding van haar bevindingen rond de evaluaties van de pilots met publieke en private authenticatiemiddelen.

a. De opdracht

De commissie is ingesteld via het instellingsbesluit d.d. 29 december 2015. Het instellingsbesluit is toegevoegd als bijlage 1. Kort na aanvang van de werkzaamheden heeft de aanvankelijke voorzitter van de commissie (drs. P.W.A. Veld) zijn betrokkenheid moeten beëindigen, en is drs. R.IJ.M. Kuipers hem als voorzitter opgevolgd.

De opdracht voor de commissie was om toe te zien op de evaluatieonderzoeken van een aantal pilots in het domein van de digitale authenticatiemiddelen en om de minister van BZK (en in afschrift de minister van EZ) te adviseren over de daaruit te trekken bevindingen, alsmede over de na de evaluatie te nemen vervolgstappen.

Doel van de pilots en van de evaluatie daarvan is om inzicht te verkrijgen in het gebruik van zowel publieke als private authenticatiemiddelen waarmee publieke diensten worden afgenomen. Daartoe zijn evaluatiecriteria opgesteld die door de beide onderzoeksbureaus voor elk van de drie pilots zijn toegepast; de gehanteerde evaluatiecriteria zijn vastgelegd in een document dat als bijlage 2 is bijgevoegd.

b. De uitvoering van de opdracht

De commissie heeft vanaf het moment van haar instelling mede sturing gegeven aan de evaluatieonderzoeken van de toen reeds voorziene en deels zelfs al gestarte pilots. Voor de goede orde: de pilots als zodanig vielen en vallen niet onder het bereik van waar de commissie over adviseert of heeft geadviseerd: ons werk beperkte zich tot *de evaluatie van die pilots*.

Zoals vastgelegd in het instellingsbesluit van de commissie, is de uitvoering van de evaluatieonderzoeken opgedragen aan onafhankelijke onderzoeksbureaus: Panteia en TNO. De aanbesteding daarvan en de gunning van de opdrachten daartoe, lagen bij BZK. De commissie is vervolgens wel betrokken geweest bij de wijze waarop beide geselecteerde bureaus hun onderzoeken hebben aangepakt, zonder te treden in de professionele verantwoordelijkheden van beide bureaus. Vervolgens heeft de commissie de uitkomsten van deze evaluatieonderzoeken kunnen benutten.

De commissie heeft zich ook anderszins laten informeren. We hebben een aantal werkbezoeken afgelegd en een veelheid aan documenten kunnen raadplegen. Daarnaast hebben de leden van de commissie zelf ook actief deelgenomen in de pilots. We hebben dus ook in de praktijk ervaren hoe diverse middelen werken.

Daarnaast heeft een aantal zogeheten reflectiebijeenkomsten plaatsgevonden waarbij de onderzoeksbureaus inzicht hebben verschaft in hun aanpak en in de voortgang van hun werkzaamheden; daarbij waren niet alleen leden van de commissie en ambtenaren vanuit BZK, EZ en diverse ministeries aanwezig, maar ook diverse vertegenwoordigers van betrokken marktpartijen. Deze bijeenkomsten hebben ons inziens bijgedragen aan de kwaliteit van de evaluatieonderzoeken.

De werkzaamheden van de commissie zijn gefaciliteerd door met name ambtelijk BZK.

In een late fase van haar werkzaamheden heeft de commissie er kennis van kunnen nemen dat BZK, in overleg met andere departementen en medeoverheden, een zogeheten 'Masterplan' in voorbereiding heeft. De commissie is niet in staat geweest daar nog kennis van te nemen, maar gaat ervan uit dat haar adviezen betrokken zullen worden bij de verdere totstandkoming van genoemd 'Masterplan'.

We danken al diegenen die hebben bijgedragen aan de werkzaamheden en de gedachtevorming van de commissie.

c. De kern van de vraagstelling en de precisering van een aantal begrippen

De kern van de vraagstelling is (in overleg met de opdrachtgever) door de commissie opgevat als de vraag in hoeverre BZK en het kabinet als geheel (en ook het parlement) er vertrouwen in kunnen hebben dat de voorgestane multimiddelenaanpak in het BSN-domein een houdbare en verstandige aanpak behelst. De intentie was en is dat deze multimiddelenaanpak beoordeeld kan worden op basis van de eerder vastgestelde evaluatiecriteria, waarna - bij een positief oordeel - concrete vervolgstappen genomen kunnen gaan worden richting implementatie van deze aanpak.

Ter toelichting daarop het volgende.

Op dit moment vindt authenticatie voor elektronische interactie tussen burgers en dienstenaanbieders in het (goeddeels) publieke domein (ook wel het BSN-domein genaamd) plaats via DigiD. Alle partijen zijn ervan overtuigd dat de levensduur van de huidige DigiD-oplossing op afzienbare termijn ten einde loopt en dat gemigreerd moet worden naar een oplossing op een hoogwaardiger betrouwbaarheidsniveau.
In de zoektocht naar dat hoogwaardiger alternatief, is geconstateerd dat het verstandig is om daarbij te zoeken naar een stelsel waarin diverse middelen bruikbaar zijn; dat verkleint de afhankelijkheid van slechts één oplossing en daarmee ook de kwetsbaarheid van het systeem als geheel. Daarmee was de gedachte geboren van de zogeheten multimiddelenaanpak.

De hoofdgedachte is dat burgers de keuze krijgen uit verschillende middelen: er komt een (nieuw) publiek middel dat op termijn voor iedere burger beschikbaar zal zijn, en daarnaast kan iedereen desgewenst gebruik maken van inlogmiddelen die thans al bij de banken toegepast worden (dit wordt aangeduid als iDIN-middelen) en iedereen kan desgewenst gebruik gaan maken van (veelal nieuwe) private middelen die in het (reeds ontwikkelde) Idensysstelsel passen. Elke burger kan zelf kiezen welk(e) middel(en) hij/zij wil benutten bij welke contacten met publieke organisaties. En elk van die organisaties in het publieke (BSN-)domein moet dus zorgen voor een aansluiting op elk van

die beschikbare middelen; daartoe wordt binnen het BSN-domein gedacht aan de inrichting van een speciale rol van (overheids)makelaar (bij Idensys en iDIN is al voorzien in die makelaarsrol).

In lijn met deze multimiddelenaanpak zijn in de afgelopen maanden pilots ingericht om deze aanpak in de praktijk te toetsen. Daartoe zijn drie soorten pilots ingericht: pilots rond het nieuwe publieke middel, een pilot rond de iDIN-middelen en pilots rond de Idensysmiddelen.

Zoals gezegd richt de kernvraag zich erop of deze multimiddelenaanpak een houdbare en verstandige is. Dit impliceert dus dat het geenszins de bedoeling is om de drie soorten middelen te gaan vergelijken als zou er uiteindelijk een keuze uit deze drie soorten van authenticatiemiddelen moeten worden gemaakt. In tegendeel: ze zijn, in de multimiddelenaanpak, juist elkaars complement en er is zelfs sprake van een soort symbiose; we gaan daar in paragraaf 8 nog uitgebreid op in. De vraag die zich dus voordoet, is enerzijds of de drie soorten middelen elk voor zich kunnen gaan functioneren zoals beoogd en tevens of er aanwijzingen zijn dat ze naast elkaar kunnen gaan functioneren.

De commissie merkt graag nog het volgende op.
Ons is gebleken dat er een fors risico is op begripsverwarring op het abstracte niveau van wat wel aangeduid wordt als 'het stelsel'. We doen graag een voorzet hoe hiermee om te gaan.
We stellen voor om de aanpak die de minister van BZK vorm aan het geven is in het BSN-domein, voortaan aan te duiden als de 'multimiddelenaanpak': meer dan de term 'multimiddelenstrategie' brengt de term multimiddelenaanpak tot uitdrukking dat het om méér gaat dan een strategie: de aanvankelijke strategie kan nu immers omgezet gaan worden in concrete besluitvorming en concrete implementatietrajecten. De term 'aanpak' dekt die lading goed.
Daarnaast zien we dat de term 'stelsel' op uiteenlopende wijzen wordt gehanteerd. Soms wordt het overkoepelende niveau van de multimiddelenaanpak gezien als het 'stelselniveau'. Maar de term 'stelsel' wordt evenzeer, en niet ten onrechte, benut op het niveau van het iDIN-stelsel en het Idensysstelsel. De commissie stelt voor om de term 'stelsel' te reserveren voor het niveau van het iDIN-stelsel en het Idensysstelsel. Dat doet ook recht aan het feit dat die twee private stelsels ook - in ieder geval op onderdelen - een eigen regime kunnen hanteren, met name ook daar waar het gaat om toepassing *buiten* het BSN-domein. De commissie stelt voor om aangelegenheden die zich voordoen op het overkoepelende niveau van de drie soorten middelen in het BSN-domein, simpelweg als zodanig aan te duiden: *het overkoepelend niveau van de multimiddelenaanpak in het BSN-domein*. Op dat overkoepelende niveau moeten bijvoorbeeld afspraken worden gemaakt over interoperabiliteit tussen de verschillende middelen en stelsels, alsmede over de privacy-randvoorwaarden die voor elk van de middelen en stelsels gelden bij gebruik van de middelen in het BSN-domein.

d. Relatie met BIT-advies

De commissie heeft tijdens haar werkzaamheden kennis genomen van een inmiddels uitgebracht advies van het BIT (Bureau ICT Toetsing) over de aanpak van het eID-programma.

Naar het oordeel van de commissie zijn de opdracht en de benadering van het BIT en de opdracht en de benadering van de commissie-Kuipers complementair aan elkaar. Het BIT heeft gekeken naar de programmatische aanpak van het eID-programma. Voor het BIT waren de pilots en de evaluatie

daarvan geen relevante input, laat staan onderwerp van advisering. Omgekeerd geldt dat de commissie heeft gekeken naar de pilots en de evaluatie daarvan, en juist niet naar de programmatische aanpak van het eID-programma. In beginsel zit er dus geen overlap tussen de invalshoek van het BIT en die van de commissie. Desondanks is de commissie zaken tegengekomen die ook aan de orde zijn in het BIT-advies. Dat heeft als achtergrond dat de commissie, tijdens haar werkzaamheden en in de gesprekken met vele stakeholders, ook met een bredere vraagstelling werd geconfronteerd dan louter de evaluatie van de pilots.

Inhoudelijk acht de commissie het BIT-advies in hoge mate herkenbaar en waardevol.

Kort weergegeven onderkent de commissie in het BIT-advies een zestal elementen die zij goed herkent:
- de noodzaak van reductie van complexiteit
- de noodzaak een aantal fundamentele keuzes expliciet te maken
- de noodzaak van helderheid over de financiële en budgettaire consequenties
- kritisch nagaan in welke tijdslijn welke stappen haalbaar zijn
- de noodzaak van het inrichten van een strakke governance (aansturing)
- de noodzaak van het inrichten van een stevige programmatische aanpak

Wel tekent de commissie aan dat het oordeel van het BIT over de gebruiksvriendelijkheid van het nieuwe publieke middel negatiever en stelliger is dan wat gebleken is in de evaluatie van de pilots.

Voor zover onze bevindingen en adviezen aan dezelfde punten raken als het BIT-advies, moeten onze opmerkingen als aanvullend worden beschouwd.

e. Voorgenomen brief Algemene Rekenkamer

De commissie heeft ook kennis genomen van het voornemen van de Algemene Rekenkamer (ARK) om over de onderhavige materie eind 2016 een rapportage uit te brengen. Daarbij heeft de ARK aangegeven dat ze overweegt om in juni of juli, maar pas nadat de minister van BZK zijn nadere voornemens rond het eID-programma kenbaar heeft gemaakt aan de Tweede Kamer, een interim-brief aan deze materie te wijden. De commissie heeft derhalve bij het schrijven van haar advies geen kennis kunnen nemen van de inhoud van die interim-brief van de ARK.

3. Opbouw van het vervolg van deze rapportage

In het navolgende geven we eerst in paragraaf 4 weer wat de bevindingen respectievelijk aanbevelingen van de beide onafhankelijke onderzoeksbureaus zijn.

Vervolgens geven we in paragraaf 5 weer welke bevindingen de commissie hieraan verbindt en tot welke aanbevelingen onzerzijds dat leidt. Dit zijn de bevindingen en aanbevelingen van de commissie die direct gebaseerd zijn op de evaluatie van de pilots; dus op het eerste deel van de opdracht aan de commissie.

Vervolgens gaan we in de daarop volgende paragrafen 6, 7 en 8 in op een aantal aanbevelingen en noties die niet in de meest directe zin voortvloeien uit (de evaluatie van) de pilots, maar die de commissie, in het licht van het tweede deel van haar opdracht, graag wil meegeven voor de na de evaluatie te nemen vervolgstappen. Het gaat om punten die de commissie heeft opgedaan via de eerder vermelde bronnen: gesprekken, werkbezoeken, documentatie en eigen ervaringen als deelnemer in de pilots.

4. De bevindingen en aanbevelingen van de onafhankelijke onderzoeksbureaus

a. Algemeen

Zoals reeds aangegeven, hebben de geselecteerde onderzoeksbureaus hun evaluatieonderzoeken in alle professionele onafhankelijkheid kunnen verrichten. Daarbij was sprake van een taakverdeling, waarbij Panteia met name heeft gekeken naar de ervaringen van de eindgebruikers (in casu de burgers) en TNO met name heeft gekeken naar de aspecten techniek, privacy en ervaringen van de leveranciers van middelen, van dienstaanbieders en van gemeenten. Mede met inbreng vanuit de commissie, maar ook van tal van stakeholders, hebben beide bureaus hun werkzaamheden op goede wijze op elkaar afgestemd.

Hoewel de pilots en de evaluatieonderzoeken in een krap tijdschema hebben moeten plaatsvinden, zijn zowel de bureaus zelf als de commissie ervan overtuigd dat de bevindingen voldoende valide zijn voor de nu te trekken conclusies. De steekproefomvang was, zeker wanneer de uitkomsten van de afzonderlijke pilots samengevoegd worden op het niveau waarop conclusies worden getrokken, in het algemeen voldoende groot en de uitkomsten waren in het algemeen voldoende significant. En waar dat niet het geval was, is dat expliciet aangegeven.

De commissie hecht eraan om, alvorens we de inhoud ingaan, een aantal noties mee te geven die cruciaal zijn bij het lezen en goed interpreteren van het vervolg.

In de eerste plaats: we gaven al aan dat de evaluatie gaat over drie soorten van pilots die passen in een multimiddelenaanpak. Dat betekent dus dat we de pilots *niet* moeten bezien vanuit een perspectief als zou er uiteindelijk een voorkeurskeuze gemaakt moeten worden uit de drie middelen (publiek middel, iDIN-middelen en Idensysmiddelen). Het gaat dus niet om een ‘beauty contest’, maar de kern is juist dat het voor het functioneren van het beoogde geheel cruciaal is dat ze naast elkaar (kunnen gaan) functioneren.

In de tweede plaats is het van belang om te (blijven) bedenken dat het hier gaat om pilots. Pilots hebben de bedoeling om te kijken of (vaak nieuwe) oplossingen kunnen (gaan) werken. Maar dat betekent ook dat er in pilots dingen fout kunnen gaan. Pilots hebben de bedoeling dat je, via een proces van vallen en opstaan, leert van wat er aanvankelijk niet goed is gegaan, met als oogmerk om aan het einde van de pilot beter te weten hoe je bij de uiteindelijke bredere uitrol een grote(re) kans op succes kunt hebben. Onvolkomenheden wijzen dus niet per se op een contra-indicatie.

In de derde plaats is het logisch dat in deze fase van pilots, er soms is gekozen voor (af en toe provisorische) technische inrichtingen waarvan op voorhand helder is dat die bij een bredere uitrol niet (meer) bruikbaar zullen zijn. Dat betekent aan de ene kant dat heel helder moet zijn dat de meer structurele oplossing nog gerealiseerd moet worden. Maar het betekent aan de andere kant tevens dat het soms provisorische karakter van de in de pilot gekozen oplossing niet als zwaarwegende contra-indicatie mag worden opgevat.

In de vierde plaats: in de nu uitgevoerde pilots is er (nog) niet voor gekozen om juist ook aparte aandacht te geven aan specifieke - soms ook kwetsbare - groepen als laagopgeleiden, digibeten, ouderen maar bijvoorbeeld ook jongeren. Dit betekent dat de pilots weliswaar vrij breed toepasbare bevindingen hebben opgeleverd, maar dat in een latere fase nog wel specifieke aandacht geboden is voor dergelijke specifieke groepen.

b. Bevindingen en aanbevelingen van Panteia

Panteia heeft evaluatieonderzoek verricht naar de ervaringen van de eindgebruikers, in casu de burgers die hebben deelgenomen aan de pilots. Als bijlage 3 treft u de volledige rapportage van Panteia aan, inclusief de samenvatting van Panteia zelf. Hieronder geven we in kort bestek de belangrijkste inhoudelijke bevindingen weer en daarna gaan we in op de aanbevelingen die Panteia meegeeft.

i. Bevindingen van Panteia

Panteia schetst een boeiend beeld van de ervaringen die gebruikers hebben opgedaan met de diverse authenticatiemiddelen in de verschillende pilots.

Bij dat beeld wijst de commissie op een bijzondere factor die voor een zinvolle interpretatie van de resultaten op voorhand moet worden vermeld. Het gaat om één van de pilots met het publieke middel (het publieke middel is namelijk in twee pilots getest: één pilot met de eNIK en één met het eRijbewijs). Bij de pilot met de eNIK hebben veel pilotdeelnemers problemen ervaren met zowel de installatie als het feitelijk gebruik van dat middel. Bij maar liefst 15% van de deelnemers is het uiteindelijk niet gelukt het middel geïnstalleerd te krijgen, en maar liefst 36% geeft aan de installatie ‘lastig’ te hebben gevonden. De oorzaak daarvan was bovenal dat het voor velen niet mogelijk bleek om de bij dit middel benodigde kaartlezer geïnstalleerd te krijgen op de eigen computer. Dat kan hebben gelegen aan die computer, aan het operating system en/of aan de browser. Hoe dan ook, dit heeft in veel gevallen tot problemen geleid. Duidelijk is dat hier uitdrukkelijk werk aan de winkel is. Tegelijkertijd blijkt uit de pilot met het eRijbewijs dat daar dergelijke problemen in veel mindere mate voorkwamen. Dit wijst erop dat de problemen die zich bij de eNIK-pilot hebben voorgedaan, technisch oplosbaar moeten zijn en niet inherent zijn aan elk publiek middel.

Een andere factor die op voorhand het vermelden waard is, is de omstandigheid dat in sommige pilots de gebruikers geconfronteerd zijn met voor hen een geheel nieuwe manier van het aanvragen en hanteren van een authenticatiemiddel (bijvoorbeeld bij de Idensysmiddelen), terwijl bijvoorbeeld het activeren en het hanteren van de iDIN-middelen (lees de middelen die men al gewend is in het domein van de banken)als veel ‘normaler’ worden ervaren.

Met deze context als achtergrond, tekent zich het volgende beeld af.

Rond de uitgifte en de installatie van de diverse middelen zien we dat veruit de meeste problemen zich hebben voorgedaan bij de pilot met de eNIK (hierboven al toegelicht). Bij de pilot met het eRijbewijs vond een deel van de pilotdeelnemers (17%) de installatie en activering wel lastig, maar

uiteindelijk lukte het vrijwel iedereen. Bij de iDIN-pilot verliep de activering over het algemeen goed. Bij de Idensyspilots was de meerderheid van de deelnemers tevreden over het aanvraagproces, maar vond nog wel een aanzienlijk deel (30%) het een vrij ingewikkeld en langdurend proces.

De Panteia-rapportage geeft aan dat de 'administratieve last' voor het verkrijgen van een publiek middel, veel hoger is dan voor een iDIN-middel en voor een Idensysmiddel. De achtergrond daarvan is vooral dat bij de publieke middelen uitgifte aan een balie vereist is. De commissie wijst erop dat dit verschil inherent is aan het bijzondere karakter van een publiek middel en dat die uitgifte aan een balie ook voordelen heeft. In paragraaf 8 gaan we hier nader op in.

Bij het 'gemak' van feitelijke gebruik van de diverse middelen zien we dat het gebruik van de eNIK het minst gunstig wordt beoordeeld (66% geeft aan gemakkelijk in te kunnen loggen met de eNIK); dit heeft vrijwel zeker de achtergrond waarop hierboven al is ingegaan. Het gebruiksgemak van het eRijbewijs, de iDIN-middelen en de Idensysmiddelen ontloopt elkaar maar marginaal: die scoren alle goed, met een 'tevredenheidspercentage' van tussen de 80% en 85%.

Ook is gekeken naar de mate waarin de deelnemers een goed gevoel hadden bij de veiligheid, de betrouwbaarheid en de privacy van de diverse middelen. Hier zien we een matige score voor de eNIK (vermoedelijk opnieuw bepaald door de reeds vermelde technische perikelen), een acceptabele score voor het eRijbewijs, een goede score voor de iDIN-middelen en een opvallend goede score voor de Idensysmiddelen. Deze hoge score voor de Idensysmiddelen heeft, zo veronderstelt Panteia, vermoedelijk te maken met het weliswaar pittige en tijdrovende aanvraagproces daarvan: dat geeft blijkbaar ook een gevoel van zorgvuldigheid.

Ten slotte is aan de pilotdeelnemers gevraagd in hoeverre ze denken het desbetreffende middel ook in de toekomst te zullen gebruiken. De eNIK en het eRijbewijs scoren daar vrij hoog op (69% respectievelijk 68%), de iDIN-middelen hoog (81%) en de Idensysmiddelen zelfs zeer hoog: 91%.

ii. Aanbevelingen van Panteia

Panteia formuleert, op basis van de zojuist weergegeven bevindingen, een aantal aanbevelingen. Deze aanbevelingen zijn bondig weergegeven in de samenvatting van de Panteia-rapportage.

De commissie is van oordeel dat deze aanbevelingen voor BZK een belangrijke input kunnen vormen bij de verdere vormgeving van het implementatietraject van de multimiddelenaanpak.

c. Bevindingen en aanbevelingen van TNO

TNO heeft de pilots onderzocht naar drie aspecten: techniek, privacy en ervaringen middelenleveranciers, dienstaanbieders en gemeenten. Als bijlage 4 treft u de volledige rapportage van TNO aan, inclusief de samenvatting van TNO zelf. Hieronder geven we in kort bestek de belangrijkste inhoudelijke bevindingen weer en daarna gaan we in op de aanbevelingen die TNO

meegeeft.

i. Bevindingen van TNO

TNO wijdt een aantal opmerkingen aan de uiteenlopende aspecten rond techniek, privacy en ervaringen van de aanbieders van authenticatiemiddelen.

Wat betreft de technische kant blijkt dat de verschillende middelen succesvol zijn toe te passen om in te loggen bij partijen in het BSN-domein en dat de vereiste technische infrastructuur elke dag beschikbaar bleek te zijn.

Wat betreft het aspect privacy schetst TNO een aantal beperkingen waaraan zijn bevindingen onderhevig zijn (onder andere dat TNO niet heeft kunnen kijken naar de technische implementatie van de borging van de privacy). Daarnaast merkt TNO specifiek op dat er enkele nadere mitigerende maatregelen geboden zijn die geïmplementeerd dienen te worden bij een brede uitrol na de pilotfase. Ook wijst TNO uitdrukkelijk op het belang van een zorgvuldige communicatie over gegevensverwerkingen, richting burger en tussen betrokken partijen onderling.

Wat betreft de ervaringen van de organisaties die authenticatiemiddelen aanbieden, van dienstaanbieders en van gemeenten, komt een aantal signalen aan de orde in de TNO-rapportage. Zo gaven verschillende middelenleveranciers bij de Idensyspilot aan dat zij het als lastig hebben ervaren om aan te sluiten bij de desbetreffende pilot. Een zelfde signaal gaven verschillende dienstaanbieders af bij de iDIN-pilot.

TNO vraagt aandacht voor de wenselijkheid om te komen tot een uniform toetsingskader dat binnen de verschillende contexten van de stelsels toegepast kan worden.

Resumerend over de drie aspecten (techniek, privacy en ervaringen van middelenaanbieders, dienstaanbieders en gemeenten) te samen komt TNO tot de conclusie dat gedurende het onderzoek duidelijk is geworden dat de afzonderlijke middelen van de multimiddelenaanpak in de praktijk technisch werken. De verschillende middelen konden worden gebruikt om bij dienstaanbieders in te loggen, ook via de verschillende stelsels (publiek middel, iDIN en Idensys). Deze stelsels bleken naast elkaar te werken en bieden burgers, aldus TNO, dus de keus om een type middel te kiezen dat zij prefereren.

ii. Aanbevelingen van TNO

TNO formuleert een aantal aanbevelingen/aandachtspunten. Deze aanbevelingen/aandachtspunten zijn bondig weergegeven in de samenvatting van de TNO-rapportage.

De commissie is van oordeel dat deze aanbevelingen/aandachtspunten voor BZK een belangrijke input kunnen vormen bij de verdere vormgeving van het implementatietraject van de multimiddelenaanpak.

5. Bevindingen en aanbevelingen Commissie-Kuipers die direct voortvloeien uit de evaluatie van de pilots

a. Bevindingen van de commissie die direct voortvloeien uit de evaluatie van de pilots

De commissie is van oordeel dat de pilots ordentelijk zijn verlopen. Weliswaar stond bij sommige pilots het tijdschema stevig onder druk, maar dat heeft, voor zover wij hebben kunnen waarnemen, geen onoverkomelijke afbreuk gedaan aan de kwaliteit van de pilots. De enige aantekening is dat in een aantal pilots niet alle beoogde dienstverleners bleken te kunnen deelnemen, waardoor de bevindingen uit de pilots een wat minder breed draagvlak hebben. Maar dat laat de bevindingen die wel konden worden getrokken, onverlet.

De commissie is van oordeel dat de beide onderzoeksbureaus bij de evaluatieonderzoeken van de pilots adequaat werk hebben geleverd. Ook voor de onderzoeksbureaus gold dat hun werkzaamheden stevig onder tijdsdruk hebben gestaan. De commissie spreekt haar waardering uit voor zowel het 'improvisatievermogen' van beide bureaus om daarmee om te gaan, als ook voor de degelijkheid waarmee dat gepaard is gegaan. De bureaus zijn er ook in geslaagd om tijdens het evaluatieonderzoek goed te blijven communiceren met de relevante stakeholders. De zogeheten reflectiebijeenkomsten hebben daarbij goede diensten bewezen.

Uit de rapportages van TNO en Panteia kan, naar het oordeel van de commissie, de conclusie worden getrokken dat uit de pilots geen aanwijzingen zijn verkregen die als min of meer prohibitief zijn aan te merken voor vervolgstappen op het vlak van de multimiddelenaanpak. Elk van de drie soorten middelen lijkt te kunnen gaan werken, en er zijn ook geen aanwijzingen gevonden die erop zouden wijzen dat ze niet naast elkaar zouden kunnen gaan functioneren. En de scores die de burgers die deelnamen aan de pilots hebben afgegeven, liggen binnen de grenzen van (voor pilots als deze) acceptabel tot zelfs zeer gunstig. Er ligt wel een duidelijke opgave om tal van grotere en kleinere issues die in de pilots als 'pijnpunten' en aandachtspunten naar boven zijn gekomen, aan te pakken en op te lossen.
Daarnaast hebben de evaluatieonderzoeken van Panteia en TNO waardevolle aanbevelingen opgeleverd.

b. Aanbevelingen van de commissie die direct voortvloeien uit de evaluatie van de pilots

De bevindingen zoals zojuist weergegeven, impliceren dat er vanuit (de evaluatie van) de pilots geen contra-indicaties zijn voor het zetten van concrete vervolgstappen in het eID-programma en voor het perspectief van implementatie van de multimiddelenaanpak. Bij die vervolgstappen hoort ook het oplossen van de diverse issues die in de pilots en in de evaluatieonderzoeken van Panteia en TNO boven water zijn gekomen.

Er is, naar het oordeel van de commissie, alle reden om nu zo snel als verantwoord is, over te gaan tot een implementatiegerichte aanpak. Er is, vanuit de uitvoeringspraktijk, immers behoefte aan een snelle voortgang, omdat anders de risico's (met name op het vlak van de betrouwbaarheid/veiligheid en op het vlak van de continuïteit) die besloten liggen in de huidige praktijk, te groot gaan worden.

Een slagvaardige implementatiegerichte aanpak wordt, naar het oordeel van de commissie, in hoge mate bevorderd wanneer de onderlinge afhankelijkheden van de in de diverse sporen te ondernemen activiteiten, beperkt kunnen blijven tot datgene wat strikt noodzakelijk is. Daarbij tekent de commissie aan dat er wel degelijk enkele uitdagingen resteren op het overkoepelende niveau; daar blijft dus sprake van een vorm van onderlinge afhankelijkheid van de sporen. Die uitdagingen komen niet of nauwelijks tot uiting in de evaluatieresultaten van de pilots in enge zin, maar in de navolgende paragrafen 6, 7 en 8 geeft de commissie wel een opsomming van een aantal belangrijke issues die op dit overkoepelende niveau nog nader geregeld zullen moeten worden.

Gegeven die uitdagingen op het overkoepelende niveau, kan nu niet geconcludeerd worden tot een volstrekte loskoppeling van de drie sporen. Maar wel geldt dat, naar de mate waarin het in ontwikkeling zijnde 'Masterplan' van BZK de uitdagingen op het overkoepelende niveau scherper benoemt en van een geloofwaardige aanpak voorziet, er des te meer reden en ruimte is voor het zetten van concrete stappen voorwaarts op de drie afzonderlijke sporen. Binnen deze redenering adviseert de commissie om groen licht te geven voor een slagvaardige aanpak voor elk van de drie afzonderlijke sporen (publiek middel, iDIN-middelen en Idensysmiddelen), met daarbij de uitdrukkelijke aantekening dat het de taak van BZK, in samenwerking met EZ en met de betrokken private partijen, is om te blijven bewaken dat op het overkoepelende niveau de maatregelen worden genomen en de afspraken worden gemaakt die nodig zijn om te borgen dat ook de multimiddelenaanpak als geheel zich ontwikkelt in de beoogde richting.

In concreto kunnen dan stappen gezet worden op het spoor dat ertoe leidt om uiteindelijk een hoogwaardig *publiek middel* tot stand te brengen waarover iedere ingezetene kan beschikken.

Daarnaast kan dan een implementatieplan gemaakt worden waarlangs de *iDIN-middelen* in de volle breedte kunnen worden toegepast in het publieke (BSN-)domein.

En ook het derde spoor, het *Idensysstelsel*, kan dan door worden ontwikkeld naar een brede toepassing, ook in het publieke (BSN-)domein.

De commissie tekent hierbij aan dat deze - positieve - bevindingen niet betekenen dat de vervolgtrajecten een sine cure gaan worden. Bij elk van de vervolgtrajecten zullen zich nader vraagstukken/problemen kunnen voordoen. Ten dele gaan we daarop in de paragrafen in.

6. Keuzes maken

a. Op weg naar een aanpak waarvan de uitkomst ook breed begrepen en gehanteerd kan worden

Kernpunt:

De commissie beveelt aan om alle keuzes die nog gemaakt moeten worden, continu primair te beoordelen vanuit de vraag in hoeverre het aannemelijk is dat de uiteindelijke gebruikers van de authenticatiemiddelen de uitkomst van die keuzes nog kunnen begrijpen en hanteren en – sterker nog – in hoeverre die keuzes en uitkomsten de belangen van met name burgers en publieke dienstverleners dienen. Ondervang dus de risico's van een focus op louter 'systeemdenken'.

Toelichting:

Het is de commissie gebleken dat het beoogde stelsel in eerste aanleg voor slechts weinigen meteen begrijpelijk is. Anders geformuleerd: voor wie niet geneigd of genoodzaakt is om 'op systeemniveau' te denken en te redeneren, is de beoogde multimiddelenaanpak een complex geheel. Dat is geen reden om tegen de beoogde aanpak te zijn, maar het vergt wel veel aandacht om bij de verdere grootschalige implementatie ongelukken te voorkomen. Deze invalshoek is in de pilots niet indringend aan de orde gekomen, omdat de meeste pilots *per middel* zijn uitgevoerd (en dus niet op middeloverstijgend niveau).

We belichten dit graag vanuit twee perspectieven: het perspectief van de individuele burger en het perspectief van de dienstverleners in het BSN-domein. De vragen die we opperen, zijn niet bedoeld als vragen van de commissie (wij kunnen de antwoorden wel verzinnen), maar als vragen die ons inziens kunnen leven bij burgers respectievelijk publieke dienstverleners.

Bezien vanuit een individuele burger kan zich de vraag voordoen of en waarom hij/zij een keuze moet maken tussen verschillende middelen, waar er nu maar één middel is (DigiD) om toegang te krijgen tot het BSN-domein. Daarnaast doet zich voor de individuele burger waarschijnlijk de vraag voor of men kan volstaan met het beschikken over slechts één middel, of dat het verstandig of zelfs noodzakelijk is om ook zelf over meer dan één middel te beschikken. In dat verband zal ook de vraag aan de orde kunnen komen of de burger dan zelf moet beslissen over de vraag op welk 'betrouwbaarheidsniveau' dat middel moet zijn geborgd, dan wel dat de betrouwbaarheidseisen gedicteerd worden door de dienstverlener met wie de burger in contact wil treden, of anderszins van overheidswege worden bepaald. In dat laatste geval zou de individuele burger zich kunnen afvragen of het wel zinvol is om te beschikken over een authenticatiemiddel dat niet op het hoogste niveau beveiligd is, in de wetenschap dat hij/zij in bepaalde situaties toch gedwongen zal zijn een authenticatiemiddel van het hoogste betrouwbaarheidsniveau te hanteren.

Kortom: redenerend vanuit de beoogde eindgebruiker, kunnen zich tal van vragen voordoen die niet alleen om een inhoudelijk antwoord vragen, maar die, naar zich laat aanzien, ook tot inspanningen nopen op het vlak van de begrijpelijke communicatie over de beoogde aanpak, en over datgene wat die aanpak vergt van de individuele burgers.

Daarnaast moet de beoogde aanpak ook vanuit alle dienstverleners in het BSN-domein begrijpelijk en hanteerbaar zijn. In de pilots heeft een aantal dienstverleners geparticipeerd, maar uiteraard bij lange na niet alle. En in de pilots bleek al dat aansluiting van de dienstverleners op bepaalde authenticatiemiddelen niet altijd zo vlot verliep als gedacht.
Dienstverleners zullen ervoor in moeten staan dat iedere burger met een door die burger gekozen authenticatiemiddel dat voldoet aan de eisen van het de multimiddelenaanpak, zaken kan doen met die dienstverlener. Het is aan de overheid, in casu aan de desbetreffende dienstverlener dan wel op een hoger coördinerend niveau, om eisen te stellen aan het minimale niveau van betrouwbaarheid van dat middel. Voor dienstverleners is vervolgens de opgave om te zorgen dat voor elk van de toegestane middelen, de toegang ook daadwerkelijk functioneert. Zoals in de pilots is gebleken, is dat geen sine cure. Daarbij moet bedacht worden dat het gaat om vele honderden dienstverleners in het BSN-domein, waaronder ook vele kleine dienstverleners.
Kortom: redenerend vanuit de dienstverleners in het BSN-domein, moet er nog het nodige geregeld worden om iedere dienstverlener gereed te krijgen om volwaardig te functioneren in de beoogde nieuwe setting. Dit vergt inspanningen, vermoedelijk zowel op het niveau van de aanpak als geheel (hiertoe wordt in de beoogde stelsels gekozen voor de zogeheten makelaarsrol tussen dienstverleners in het BSN-domein en aanbieders van authenticatiemiddelen) als ook per dienstverlener in het BSN-domein.

In dit verband bepleit de commissie dat voor de uiteindelijke gebruikers van de authenticatiemiddelen (in casu aan de ene kant alle burgers en aan de andere kant alle dienstverleners in het BSN-domein) er uiteindelijk een situatie resulteert die echt als één logisch en begrijpelijk geheel gezien kan worden.
Voorkomen moet worden dat burgers keuzes moeten gaan maken die ze niet kunnen overzien, bijvoorbeeld doordat het gaat om voor hen wellicht ‘nietszeggende’ begrippen en systeemkeuzes. De risico’s van een te grote focus op ‘systeemdenken’ moeten dus vermeden worden.
En voor dienstverleners moet er ook geen enkele onnodige complicatie voortvloeien uit het naast elkaar bestaan van uiteenlopende middelen.

b. Hoe gaan de businessmodellen van de authenticatiemiddelen vorm krijgen?

Kernpunt:

Voor het daadwerkelijk tot stand komen van private authenticatiemiddelen is het essentieel dat duidelijkheid gaat ontstaan rond de businessmodellen voor die middelen, en in het bijzonder welke doorbelasting naar de overheid zal gaan

plaatsvinden.
Die duidelijkheid is ook snel vereist, omdat de private partijen pas gaan investeren in de beschikbaarheid van hun middelen voor het BSN-domein nadat die duidelijkheid is ontstaan.
De overheid moet snel bepalen langs welke lijnen zij die gewenste duidelijkheid kan gaan geven en in hoeverre daarbij sprake kan zijn van een onderlinge afstemming van partijen binnen het BSN-domein.

Toelichting:

De vraag rond het 'businessmodel' is voor het publieke middel een andere dan voor de private middelen. Voor het publieke middel gaat het om een inschatting van de kosten die daarmee gemoeid zijn en om de budgettaire inpassing van die kosten. Het behoorde niet tot de opdracht van de commissie om zich over die kosten en over de budgettaire inpasbaarheid van het publieke middel een oordeel te vormen. Evenmin behoorde het tot onze opdracht ons een oordeel te vormen over de maatschappelijke kosten en baten van het eID-stelsel als geheel.

Maar voor de overheid is niet alleen het publieke middel bepalend voor het totale (budgettaire) kostenplaatje. Geredeneerd vanuit het overheid, is de multimiddelenaanpak gekozen om de kwetsbaarheid van één enkele publiek authenticatiemiddel voor toegang tot het BSN-domein te ondervangen. Vanuit die optiek bezien is het logisch dat de kosten die voortvloeien uit die multimiddelenaanpak, voor de overheid niet beperkt blijven tot de kosten van het publieke middel. Linksom of rechtsom zal ook vanuit de private authenticatiemiddelen een doorbelasting naar het publieke domein moeten plaatsvinden. Dat verloopt via de businessmodellen rond de private middelen. Daarover zijn nog geen afspraken gemaakt tussen overheid en die private partijen.

Wat betreft de iDIN-middelen geldt dat die middelen reeds bestaan en reeds een grote verspreidingsgraad hebben. Er hoeft dus geen middel meer compleet nieuw 'in de markt te worden gezet'. Wel zal geïnvesteerd moeten worden in de benodigde infrastructuur om, bij gebruik van de iDIN-middelen in het BSN-domein, het toenemende gebruik op te vangen, en in het aansluiten van gebruikers. Daarnaast geldt dat banken blijvend zullen moeten investeren in het op voldoende veiligheidsniveau houden van hun systemen, met inbegrip van de toegangsmiddelen.
Naar we aannemen, zullen de iDIN-middelen ook in het niet-BSN-domein gebruikt (mogen) gaan worden.
Dit alles leidt uiteraard tot een bepaald kostenplaatje. Voor zover de commissie kan overzien, heeft dat nog niet een concrete vertaling gekregen in een businessmodel respectievelijk in afspraken over vergoeding bij het gebruik van het iDIN-middel in het BSN-domein. In de uitgevoerde pilots was een dergelijke vergoeding ook niet aan de orde.
Het is evident dat de werking van het model van de iDIN-middellen alleen van de grond kan komen wanneer er daadwerkelijk afspraken gemaakt blijken te kunnen worden over de vergoeding bij het gebruik van de iDIN-middelen.

Wat betreft de Idensysmiddelen geldt dat daar wel degelijk (deels nieuwe) middelen nagenoeg compleet nieuw 'in de markt gezet moeten gaan worden'. Dat vergt een fundamenteel nadenken over het businessmodel oftewel het verdienmodel. In de pilots is daar nog geen sprake van geweest. Hierbij geldt overigens dat de verdienmodellen voor de Idensysmiddelen (net als de iDIN-middelen) niet alleen beperkt zijn tot het BSN-domein: Idensysmiddelen richten zich ook op gebruik in het niet-BSN-domein.
Overigens geldt dat iedere aanbieder van een Idensysmiddel zijn eigen verdienmodel kan hebben. Het gaat om private aanbieders en om een markt, zij het een markt die nog tot ontwikkeling moet komen.
De commissie kan niet overzien welke marktpotentie er op termijn zal zijn voor Idensysmiddelen. Daarmee is tevens niet te overzien hoe die markt zich zal gaan ontwikkelen: hoeveel aanbieders zullen er komen, welke omvang heeft hun markt en dergelijke. Evident is wel dat de multimiddelenaanpak gediend is met het tot ontwikkeling komen van een volwassen markt voor (ook) de Idensysmiddelen. En dat vergt snelle duidelijkheid over de grondslagen voor hun businessmodellen.

Bij dit alles doet zich tevens de vraag voor hoe de overheid zichzelf positioneert in dit soort vraagstukken respectievelijk in de onderhandelingen die dat gaat vergen tussen de spelers in het BSN-domein en de (private) aanbieders van authenticatiemiddelen. Zo moet er nog een antwoord komen op de vraag langs welke weg de overheid (of juist de verschillende overheden) zich gaat/gaan organiseren: gaat iedere publieke dienstverlener zelfstandig dit soort afspraken maken met aanbieders van authenticatiemiddelen, of wordt dat gebundeld? En kan die bundeling ook zo ver gaan dat Rijk en medeoverheden samen optrekken?
De commissie kan die vraag niet beantwoorden, maar tekent wel aan dat enigerlei vorm van bundeling wel dienstbaar zal zijn aan het doen ontstaan van een enigszins overzienbaar speelveld. En dat lijkt ons randvoorwaardelijk voor een ordelijk tot stand komen van een redelijk functionerende markt.

c. Over de vereiste niveaus van betrouwbaarheid

Kernpunt:

De commissie beveelt aan dat BZK en EZ snel de taak op zich nemen om te komen tot een breed gedragen interpretatie van het nieuwe eIDAS-normenkader, en tot consequente toepassing daarvan, in ieder geval in het BSN-domein.
Daarnaast moet BZK snel het punt ter hand nemen rond de vereiste betrouwbaarheidsniveaus die in het BSN-domein gehanteerd moeten gaan worden en de vraag op welk bestuurlijk niveau daarover besloten gaat worden.

Daarbij moet ook helder worden welke consequenties dit kan hebben voor de authenticatiemiddelen.

Toelichting:

Een van de belangrijkste drijfveren rond het hele traject is dat breed wordt onderkend dat de huidige DigiD-oplossing op korte termijn versterking behoeft. Gelet op de voortgeschreden eisen op het vlak van de betrouwbaarheid van authenticatiemiddelen, is een forse stap voorwaarts nodig. Die kan bereikt worden via de voorziene middelen in de multimiddelenaanpak.

Rond dit betrouwbaarheidsniveau is wel sprake van een aantal vraagstukken waar de commissie ruimschoots mee is geconfronteerd in haar werkzaamheden en waar de commissie dus ook graag aandacht voor vraagt.

Nieuw normenkader: eIDAS

Op dit moment voltrekt zich een wijziging in het (internationale) normenkader rond de betrouwbaarheid van authenticatiemiddelen. Tot nu toe werd geredeneerd in termen van 4 betrouwbaarheidsklassen: van Stork 1 t/m Stork 4, waarbij Stork 1 een laag betrouwbaarheidsniveau weergeeft en Stork 4 het hoogste betrouwbaarheidsniveau representeert. Inmiddels echter is de Stork-indeling niet meer de te hanteren methodiek, en vindt een omschakeling plaats naar een nieuwe indeling: de vanuit EU-verband voorgeschreven zogeheten eIDAS-systematiek. In deze nieuwe systematiek bestaan niet meer vier betrouwbaarheidsklassen, maar slechts drie: laag, substantieel en hoog.

Deze omschakeling vergt heroriëntatie.

Enerzijds moeten alle dienstverlenende organisaties opnieuw bepalen op welk(e) betrouwbaarheidsniveau(s) ze willen werken en welke eisen dit dus ook stelt aan de te hanteren authenticatiemiddelen. De commissie onderkent dat het moeilijk is het (recente) verleden los te laten: vele organisaties blijven redeneren in de oude vierdeling van Stork 1 t/m 4. Dit is verwarrend. Snelle omschakeling over de hele linie is gewenst.

Anderzijds worstelen experts en dienstverleners nog met de interpretatie van het nieuwe normenkader: het eIDAS-kader blijkt nog niet volledig te zijn uitgekristalliseerd. Weliswaar lijkt de verordening erop te wijzen dat de drie nieuwe niveaus corresponderen met de drie hoogste Stork-niveaus, maar bij de implementatie ervan doen zich nog discussies voor over hoe de internationale standaarden en eisen daarop gelezen moeten worden. Dat maakt een herleiding van de oude Stork-niveaus naar de nieuwe eIDAS-indeling een lastige, met als automatisch gevolg dat de overstap naar het nieuwe normenkader daardoor alleen maar geremd wordt en dat men er dus aan hecht om nog maar even in de oude Stork-niveaus te blijven redeneren.

Onze aanbeveling hieromtrent is dat BZK en EZ snel invulling geven aan hun taak om te komen tot een breed gedragen interpretatie van het nieuwe eIDAS-normenkader, en tot consequente

toepassing daarvan, in ieder geval in het BSN-domein; wij hebben begrepen dat EZ hier reeds het voortouw in heeft genomen.

Welk betrouwbaarheidsniveau hanteren?

De vraag doet zich voor welk(e) betrouwbaarheidsniveau(s) in het BSN-domein gehanteerd moet(en) gaan worden. De commissie wijst graag op de volgende afwegingsfactoren.

Uit internationale vergelijking komen indicaties naar voren dat er een zekere trade-off kan zijn tussen aan de ene kant de mate van betrouwbaarheid van authenticatiemiddelen en aan de andere kant de gebruiksvriendelijkheid daarvan. Dit heeft als gevolg dat, bij het gaan hanteren van een hoger betrouwbaarheidsniveau, er oog moet zijn voor dat risico. Voorkomen moet worden dat het kind met het badwater wordt weggespoeld. Dit is overigens geen argument tegen een hoog betrouwbaarheidsniveau, maar wel een uitdrukkelijk aandachtspunt bij de wijze waarop en het tempo waarin een veranderstrategie wordt ingezet.
Overigens kan zich ook een andere - onverwachte - trade-off voordoen, zo is gebleken uit de pilots met de Idensysmiddelen: naar de mate waarin burgers het aanvraagproces van een bepaald middel als 'intensiever' ervaren, geeft dat hen ook het prettige gevoel dat het uitgifteproces zorgvuldig en hoogwaardig is.
Het is dus van belang om, gegeven deze uiteenlopende trade-offs, een goede balans te vinden in de veranderstrategie en het communicatietraject daaromheen.

In de tweede plaats zullen alle dienstverleners in het BSN-domein (en de partijen die verantwoordelijk zijn voor subdomeinen daarbinnen) zich uitdrukkelijk moeten bezinnen op de nieuwe eIDAS-systematiek waar we hierboven al op ingingen. Men moet keuzes maken rond het te hanteren niveau van betrouwbaarheid van de authenticatiemiddelen. Afhankelijk van de te verrichten dienst, kan dat variëren van 'laag' tot 'hoog'. De commissie kan niet overzien of het niveau 'laag' vaak gehanteerd zal gaan worden (maar sluit dit niet uit, bijvoorbeeld als het om relatief risicoloze diensten gaat, zoals het maken van een afspraak om op het gemeentehuis een baliebezoek af te komen leggen). Indringend echter zal zeker de discussie zijn over de keuze tussen de betrouwbaarheidsniveaus 'substantieel' en 'hoog'.

Daarbij doet zich de vraag voor op welk (bestuurlijk) niveau uiteindelijk besluitvorming plaatsvindt over het vereiste betrouwbaarheidsniveau. In de voorgaande alinea is nog verondersteld dat elke overheidsorganisatie daar een eigen afweging over maakt. Maar de vraag is of een dergelijke aanpak nog wel past in de hedendaagse verhoudingen. Het is niet aan de commissie om daarop een antwoord te geven, maar denkbaar is dat op overkoepelend niveau afwegingen worden gemaakt die maatgevend zijn voor afzonderlijke organisaties. Het gaat immers vaak om soortgelijke gegevens en soortgelijke gevoeligheden, en het valt moeilijk te betogen - en moeilijk uit te leggen aan burgers - indien afzonderlijke publieke organisaties daarover uiteenlopende afwegingen zouden kunnen maken.

In het verlengde hiervan moet nagedacht worden over de vraag in hoeverre, wanneer in ook maar één van de BSN-domeinen zou worden geconcludeerd dat het niveau 'substantieel' niet hoog genoeg is en dus het niveau 'hoog' vereist is, dat noodzakelijkerwijs implicaties zou kunnen hebben voor de vereiste betrouwbaarheidsniveaus in andere BSN-domeinen.
Naar het oordeel van de commissie hoeft dat niet het geval te zijn. Voorwaarde is wel dat de

authenticatiemiddelen zodanig zijn vormgegeven dat elk middel het mogelijk maakt om op betrouwbaarheidsniveau 'hoog' in te loggen, maar tevens de optie kent om, met minder moeite, op betrouwbaarheidsniveau 'substantieel' en eventueel zelfs op niveau 'laag' in te loggen waar dat niveau zou volstaan. Dit pleit voor een zogeheten 'multifactor authenticatie'. Voor zover de commissie heeft kunnen nagaan, is dit ook de bedoeling en is respectievelijk wordt deze aanpak ook al feitelijk geïmplementeerd bij diverse authenticatiemiddelen. Om een simpel voorbeeld te noemen: het publieke middel zou dan bruikbaar kunnen zijn zonder pincode op niveau 'substantieel', terwijl voor transacties die niveau 'hoog' vereisen, daarenboven bijvoorbeeld een pincode moet worden ingebracht. Soortgelijke (technisch bezien uiteenlopende) multifactor-oplossingen bestaan ook in het iDIN-stelsel en het Idensysstelsel.

d. Afbakening van gebruik publieke middel tot BSN-domein

Kernpunt:

De commissie is van mening dat het van groot belang is om een aantal vraagstukken rond de hanteerbaarheid van de huidige afbakening van het BSN-domein nog eens heel goed te doordenken. Dat doordenken is niet alleen nodig om er zeker van te zijn dat de gemaakte keuzes consistent en ook op langere termijn hanteerbaar zijn, maar ook om na te gaan of het geheel goed valt uit te leggen aan burgers en dienstaanbieders in en buiten het BSN-domein.

Toelichting:

Algemeen

De commissie heeft er kennis van genomen dat de multimiddelenaanpak inhoudt dat één van de drie beoogde middelen, te weten het publiek middel, beperkt zal worden qua gebruik: anders dan de iDIN-middelen en de Idensysmiddelen, zal het publieke middel louter in het BSN-domein gehanteerd mogen worden. De commissie onderkent dat deze keuze (mede) voortkomt vanuit de gedachte dat aldus wordt voorkomen dat er anders wellicht geen reële markt zou resteren voor de private middelen. Maar tegelijkertijd signaleert de commissie wel dat deze keuze een aantal vragen kan oproepen.

Begrijpelijkheid

De eerste vraag betreft - opnieuw - de begrijpelijkheid van het geheel. Voor burgers zal begrijpelijk moeten zijn wat er wel kan en wat er niet kan met een bepaald middel. In dit verband kan het behulpzaam zijn om de beoogde werking van het model te beschrijven langs de lijnen van enerzijds 'toegang tot' en anderzijds 'toegang met'. We doen een poging.

De beoogde multimiddelenaanpak regelt in beginsel alleen de *toegang tot* het BSN-domein: hoe kunnen burgers inloggen bij organisaties met een publiek karakter? Het stelsel regelt niet hoe de toegang tot het niet-BSN-domein is of wordt geregeld; dat is ook niet de opgave van wat nu voorligt. Het kabinet heeft er welbewust voor gekozen om de toegang tot het BSN-domein tot een apart beleidstraject te maken (onder de hoede van BZK), vanwege de noodzaak om snel alternatieven te realiseren voor de huidige DigiD-oplossing.
De beoogde multimiddelenaanpak regelt daarbij dat die toegang tot het BSN-domein gerealiseerd kan worden via een *toegang met* een drietal soorten middelen, waarvan het publieke middel er één is. En dat publieke middel ontleent zijn bestaansrecht, anders dan de twee andere - private - middelen, alleen aan het feit dat de overheid vindt dat iedere burger *juist in het BSN-domein*, het recht moet hebben om daarbij een publiek middel te hanteren.

Afbakening nog valide?

De tweede vraag die gesteld moet worden, is of het huidige begrip 'BSN-domein' nog wel valide is afgebakend. Thans vallen onder het BSN-domein niet alleen de evidente overheidsorganisaties (Rijksoverheid, gemeenten, provincies, waterschappen, ZBO's), maar tevens - evident als privaat aan te merken - partijen als de zorgverzekeraars, zorginstellingen en de pensioenfondsen.
Dat doet de vraag rijzen waarom andere (min of meer vergelijkbare) private organisaties (zoals andere soorten verzekeraars, de banken en het Bureau Kredietregistraties (BKR)) niet tot het BSN-domein worden gerekend, terwijl ze evenzeer als zorgverzekeraars en pensioenfondsen persoonsgegevens verwerken. Sterker nog, om een heel concreet voorbeeld te noemen: banken zijn van overheidswege verplicht het BSN van hun klanten in hun administraties op te slaan en te benutten voor enkele expliciet omschreven vormen van informatieverschaffing van de banken aan de overheid (in casu het doorgeven van bankgegevens aan de Belastingdienst en het doorgeven van gegevens die relevant zijn voor het depositogarantiestelsel). Desondanks worden banken en de andere genoemde organisaties niet tot het BSN-domein gerekend. Zoals gezegd, kan de vraag rijzen waarom dat zo is.
Omgekeerd kan de vraag rijzen of het tot het BSN-domein rekenen van de (private) zorgverzekeraars en de pensioenfondsen nog wel van deze tijd is. Dit punt kan nog scherper komen te liggen in het perspectief van hoe de businessmodellen voor de private authenticatiemiddelen vorm moeten gaan krijgen.
In ieder geval lijkt een herbezinning op de afbakening van het BSN-domein opportuun, nu zo duidelijk de beleidslijn geldt dat het benutten van één van de authenticatiemiddelen (te weten het publieke middel) beperkt blijft tot het BSN-domein.

Terughoudende of ruimhartige benutting van het BSN?

In het verlengde hiervan kan de vraag gesteld worden in hoeverre een terughoudende dan wel juist ruimhartige toelating tot het gebruik van het BSN door private organisaties in de rede ligt. Historisch bezien is gekozen voor een terughoudend gebruik van het BSN, althans voor niet-publieke organisaties. Die terughoudendheid was (en is) te verklaren vanuit de vrees dat via het BSN (te) gemakkelijk allerlei gegevens gekoppeld zouden kunnen worden, wat een bedreiging kan zijn voor ieders privacy.
Met respect voor die vrees rond aantasting van de privacy, merkt de commissie op dat de tijden wel veranderd zijn. Koppeling van gegevens is inmiddels niet meer iets wat alleen maar mogelijk is via

een voorziening als een BSN. In de wereld van de sociale media en in een wereld waarin tal van partijen gebruik maken van big data analytics, zou het gebruik van het BSN niet meer bij uitstek 'de (enige) spil' in het privacydebat moeten zijn. Daar komt bij dat er ook al een nieuwe en bredere normatiek aan het ontstaan is rond de borging van de privacy in deze 'nieuwe wereld', los van alleen het risico van koppeling via bijvoorbeeld een BSN; zie onder andere het recente rapport van de WRR ter zake ("Big Data in een vrije en veilige samenleving').
De commissie adviseert om deze discussie over de borging van de privacy en de mate waarin dat noopt tot een blijvende terughoudendheid in het gebruik van het BSN door private organisaties dan wel dat er ruimte is voor een ruimhartiger gebruik ervan, nadrukkelijk te voeren en te betrekken bij de vraag over het toegestane bereik van het publieke middel. We realiseren ons dat deze discussie in zekere zin complicerend kan werken (en dus tegengesteld kan zijn aan het pleidooi van het BIT om de complexiteit te verminderen), maar aan de andere kant moet voorkomen worden dat nu wegen worden ingeslagen die later problematisch begaanbaar blijken te zijn. Hoe dan ook is een welbewuste keuze nodig.

Mag er straks minder dan voorheen?

Een volgende vraag maken we graag duidelijk aan de hand van een concreet voorbeeld: in hoeverre klopt de redenering dat een burger zich nu bij een hotelbalie wel kenbaar mag maken met behulp van een paspoort (een publiek middel), en in hoeverre en waarom zou diezelfde burger zichzelf in de toekomst bij Booking.com niet digitaal mogen authenticeren met een publiek authenticatiemiddel? Generaliserend doet dat de vraag rijzen of het inderdaad zo is dat de multimiddelenaanpak ertoe leidt dat burgers in de toekomst bij het benutten van het publieke middel minder vrij zijn in hun handelen dan voorheen, en waarom dat zo is.
Het is niet aan de commissie om dit soort vragen te beantwoorden, maar het lijkt ons onontkoombaar dat dit soort vragen alleen maar met argumenten 'op overkoepelend niveau' beantwoord kunnen worden. Bijvoorbeeld met het argument dat we nu geen privaat alternatief hebben voor het paspoort, en straks wel een privaat alternatief hebben voor het elektronisch publieke middel (waarbij dat private alternatief dan wel weer 'leunt op' het elektronisch te gebruiken publieke middel dat fungeert als 'moederkaart'; we gaan daar nog op in), in combinatie met het argument dat de werking van de multimiddelenaanpak vereist dat het publieke middel geen verdringende werking mag hebben ten opzichte van de private middelen in het niet-BSN-domein. Daarbij kan tevens worden bedacht dat het toestaan van het gebruik van het publieke middel buiten het BSN-domein, ook vragen oproept rond de daarbij toe te passen tarifering.
Bij deze discussie moet in het oog worden gehouden hoe de uitkomsten ook echt uitgelegd kunnen worden aan de uiteindelijke gebruiker in casu aan de burger.

Dreigt zelfs niet een zekere mate van inconsistentie?

Dit alles wordt nog gecompliceerder wanneer we bedenken dat het bovenbedoelde (en verderop nog uitgewerkte) idee van het publieke middel als 'moederkaart', eigenlijk een zekere mate van inconsistentie oplevert met de gedachte dat het publieke middel alleen beschikbaar is voor toegang tot het BSN-domein. Immers, het idee van het publieke middel als 'moederkaart' impliceert dat je dat publieke middel juist wèl mag benutten in het niet-BSN-domein, bijvoorbeeld door je met dat (digitale) publieke middel te identificeren bij de uitgifte van een privaat authenticatiemiddel.
De commissie beoogt met deze redenering geen spaak in het wiel te steken van deze gedachte rond

de ‘moederkaart’, maar wel een aanzet te geven om te komen tot een weldoordachte set van afspraken, die ook op langere termijn houdbaar zal blijken.

7. Een zorgvuldige en verantwoorde aanpak

a. Over de stip op de horizon en de stappen op weg daarheen

Kernpunt:

De commissie adviseert om te kiezen voor een benadering waarbij enerzijds een redelijk helder beeld wordt gekozen in de zin van de stip op de horizon, waar je uiteindelijk heen wilt, en om anderzijds in de implementatieplannen vooral vorm te geven aan concrete en behapbare stappen op weg daarheen. Geen blauwdrukken, geen big bangs, geen te grote stappen ook, maar wel betekenisvolle stappen.
Voor het publieke middel betekent dit dat de commissie uitdrukkelijk adviseert om te bezien of varianten als de consequente toepassing van de sms-verificatie en/of de door de RDW aangedragen RDA-oplossing wellicht een nuttige tussenstap zijn op weg naar – uiteindelijk – een nieuw publiek middel op het hoogste veiligheidsniveau. De commissie adviseert om daarbij het 'label' DigiD te behouden.
Ook voor de private middelen geldt dat soms via kleine stappen al verregaande winst denkbaar is. Zo wijzen de uitkomsten van de iDIN-pilot erop dat deze reeds grootschalig beschikbare oplossing snel ook voor het BSN-domein toepasbaar is. Verwacht mag worden dat ook binnen het Idensysstelsel dergelijke stappen mogelijk zijn.

Toelichting:

Algemeen

Zoals bij elk groot programma, geldt ook hier dat het verstandig is om enerzijds een redelijk helder beeld te willen hebben van de stip op de horizon, waar je uiteindelijk heen wilt, en om anderzijds in de implementatieplannen vooral vorm te geven aan concrete en behapbare stappen op weg daarheen. Geen blauwdrukken, geen big bangs, geen te grote stappen ook, maar wel betekenisvolle stappen.

Heel concreet wijst de commissie op het volgende.

We leven nu met een situatie waarin we bij alle transacties tussen burger en overheden genoegen nemen met DigiD. We weten ook dat DigiD zich op betrouwbaarheidsniveau ‘laag’ bevindt. Desondanks functioneert DigiD nog alleszins naar behoren, zij het dat alle partijen hechten aan een snelle opwaardering van de betrouwbaarheid (in termen van de eIDAS-verordening) van DigiD als zodanig en naar een opwaardering van het eID-stelsel als geheel: de multimiddelenaanpak.

Als stip op de horizon zien we een situatie waarin de burger kan kiezen uit een publiek middel en een aantal private middelen (iDIN-middelen en Idensysmiddelen), die ten minste op betrouwbaarheidsniveau ‘substantieel’ en op termijn ook op betrouwbaarheidsniveau ‘hoog’ zijn vormgegeven. En, gegeven de stormachtige ontwikkelingen op dat front, zien we die stip op de horizon ook nog eens een vorm aannemen die zo veel als mogelijk gebruik maakt van smartphones oftewel mobiele devices.

Maar wanneer we nu over de hele linie met niets minder genoegen zouden gaan nemen dan met de ‘ultieme’ oplossing die zich zou bevinden op betrouwbaarheidsniveau ‘hoog’ en die al dwingend gebruik maakt van de mobiele devices, dan weten we één ding vrijwel zeker: dan gaat de eerste stap op weg naar de stip op de horizon niet alleen veel langer duren dan gewenst, maar ook veel duurder uitpakken dan we aan geld beschikbaar hebben. Met als consequentie dat er voorlopig waarschijnlijk niets gaat veranderen. Dat is dus ‘een garantie voor mislukking’.

De logische consequentie is dat we er verstandig aan doen genoegen te nemen met relatief bescheiden - en daardoor behapbare - , maar toch betekenisvolle stappen voorwaarts, en dat we aldus al werkende weg steeds dichter bij het gewenste eindbeeld komen. Dit ook in het besef dat over een aantal jaren de inzichten in wat er uiteindelijk mogelijk (en nodig) is, waarschijnlijk weer anders zijn dan nu. De stip op de horizon moet continu herijkt kunnen worden.

De commissie bepleit dus zeer uitdrukkelijk deze aanpak van enerzijds een redelijk uitgekristalliseerde, maar niet in beton gegoten stip op de horizon, en anderzijds een implementatietraject van relatief bescheiden, behapbare maar tegelijkertijd betekenisvolle stappen voorwaarts.

In concreto: de RDA-oplossing als aanvulling op DigiD

Om dit concreet te maken, vermelden we een stap die inmiddels, parallel aan de onder de hoede van de commissie geëvalueerde pilots, in een afzonderlijke pilot is verkend. Aangezien deze pilot meer gezien werd als versterking van het huidige DigiD dan als onderdeel van het nieuwe eID-stelsel, maakte deze pilot geen onderdeel uit van de pilots die geëvalueerd zijn onder de hoede van de commissie-Kuipers. De commissie tekent hierbij aan dat zij dit (niet door haarzelf gemaakte) onderscheid irrelevant vindt.

De RDW heeft, op verzoek van BZK en in afstemming met de Manifestgroep, een pilot verricht op de zogeheten RDA-techniek (RDA staat voor Remote Document Authentication). Dit is een techniek die gebruik maakt van de huidige chip zoals die reeds beschikbaar is op rijbewijzen, paspoorten en identiteitskaarten die in de afgelopen jaren zijn uitgegeven.
Daarbij is een uiterst relevant gegeven dat langs deze weg de overgrote meerderheid van de Nederlanders reeds beschikt over een document (lees publiek middel) met deze chip: alle in omloop zijnde paspoorten en alle in omloop zijnde identiteitsbewijzen; en daarnaast ook de rijbewijzen die

vanaf 2014 zijn uitgegeven. In totaal gaat het om grofweg 20 miljoen uitgegeven documenten die van de desbetreffende chip zijn voorzien. Dit betekent een dekking van bijna 100% voor de groep van Nederlanders ouder dan 16 jaar.
In combinatie met de huidige DigiD-voorziening levert deze RDA-techniek een significante verbetering op ten opzichte van DigiD: waar DigiD niet meer kan leveren dan - in eIDAS-termen - een betrouwbaarheidsniveau 'laag', levert de nieuwe RDA-aanpak, in combinatie met DigiD en onder een aantal voorwaarden die vervulbaar lijken, een betrouwbaarheidsniveau 'substantieel' op.
De genoemde RDA-pilot is langs dezelfde lijnen geëvalueerd als de (andere) eID-pilots. De uitkomst van deze evaluatie is dat de RDA-pilot succesvol is verlopen, met daarbij de aantekening dat de pilot wel een aantal belangrijke aanbevelingen heeft opgeleverd, met name rond het thema privacy. De RDW is doende invulling te geven aan die aanbevelingen. De commissie heeft zich zelf vergewist van de aanpak en heeft ook de beschikking gekregen over de evaluatie van de pilotresultaten. Die evaluatie is als bijlage 5 toegevoegd.

Gelet op de - op hoofdlijnen - succesvolle resultaten van deze RDA-pilot, gelet op de mogelijkheden om deze RDA-aanpak binnen een overzienbaar tijdsbestek breed uit te rollen (omdat de reeds op grote schaal aan burgers uitgegeven documenten reeds beschikken over de vereiste chip) en gelet op de relatief geringe kosten die een brede uitrol van de RDA-aanpak met zich brengt (iedere burger hoeft slechts te beschikken over zijn bestaande paspoort of identiteitsbewijs of (vanaf 2014 uitgegeven) rijbewijs, alsmede over hetzij een daartoe geschikte smartphone hetzij een specifiek daarvoor te verstrekken usb-kaartlezer), geeft de commissie in overweging deze variant zeer uitdrukkelijk te overwegen in het stappenplan voor het publieke middel. Niet als de ultieme oplossing, maar als eerstvolgende stap. Een stap die - ingebed in de voorwaarden die door onderzoekers van het PWC daarover zijn geformuleerd - een betekenisvolle verbetering biedt ten opzichte van de status quo. En ook een stap die de ruimte biedt om een volgende, meer definitieve, oplossing van het publieke middel zorgvuldig vorm te geven en ook via de weg van de geleidelijkheid budgettair goed inpasbaar te maken.

De commissie maakt in dit verband van de gelegenheid gebruik om aan te geven dat deze stapsgewijze aanpak ook een goede reden kan zijn om geen afscheid te nemen van succesvolle 'labels', zoals in dit geval het label DigiD. De RDA-techniek is de facto een slimme doorontwikkeling op DigiD, die het betrouwbaarheidsniveau van DigiD in een overzienbaar tijdsbestek en tegen relatief geringe kosten betekenisvol opwaarderen van 'laag' naar 'substantieel'. En het is ook een stap die bijdraagt aan de verdere ontwikkeling van een publiek middel naar betrouwbaarheidsniveau 'hoog' .
De commissie geeft in overweging om in deze stapsgewijze aanpak een label als DigiD te behouden. Vermoedelijk doet het blijven hanteren van het label DigiD ook recht aan het begrip bij burgers van datgene wat geboden wordt.

Generaliserend

Toegespitst op het publieke middel lijkt de RDA-oplossing een kansrijke, behapbare en toch betekenisvolle stap op weg naar de stip op de horizon. Een ander denkbaar alternatief zou zijn om te bezien of verplichtstelling van de reeds beschikbare optie van de zogeheten sms-verificatie binnen het huidige DigiD een toegevoegde waarde kan hebben; ook deze variant zal niet gratis zijn, maar ook hiervan zijn de budgettaire implicaties overzienbaar.
Voor de private sporen van de iDIN-middelen en de Idensysmiddelen geldt dat het primair aan de

marktpartijen in kwestie is om, al dan niet stapsgewijs, voortgang te boeken. Verwacht mag worden dat juist vanuit het private domein ook innovatieve impulsen zullen ontstaan en dat bijvoorbeeld de integratie richting mobiele devices/ smartphones juist ook vanuit de private sporen een impuls zal krijgen.

Kanttekening

De commissie kan niet geheel overzien of haar voorstel om qua implementatietraject te streven naar bescheiden, behapbare maar betekenisvolle stappen, een specifiek domein in de problemen kan brengen. We doelen dan specifiek op het zorgdomein. De minister van VWS heeft een aantal concrete toezeggingen gedaan rond het op afzienbare termijn beschikbaar zijn van een middel met een hoog betrouwbaarheidsniveau voor een vrij grote groep van chronisch zieken. De commissie adviseert om desnoods een specifiek op deze groep toegespitste oplossing te overwegen, liever dan dat overhaast stappen worden gezet van algemene strekking waar we later alleen maar spijt kunnen krijgen.

b. Wat is er nodig aan structurele voorzieningen en welke impact heeft dat op de vereiste governance?

Kernpunt:

Om de multimiddelenaanpak te laten functioneren, is een aantal structurele voorzieningen essentieel. Voor de totstandkoming maar ook voor het duurzaam functioneren daarvan, is een stevige interdepartementale governance noodzakelijk, waarbij naast BZK ook EZ , medeoverheden en uitvoeringsorganisaties betrokken zijn en blijven. Tevens zal afstemming met de leveranciers van de private middelen moeten blijven plaatsvinden.

Toelichting:

De commissie heeft er kennis van kunnen nemen dat de werking van de beoogde multimiddelenaanpak mede afhankelijk is van een aantal (structurele) voorzieningen; we hanteren het begrip ‘voorziening’ hier breed. De commissie vermeldt graag enkele voorbeelden expliciet. We sluiten af met een generaliserende aanbeveling.

Voorbeeld BSN-koppelregister

In het kader van de pilots een voorlopige versie gebouwd van het zogeheten ‘BSN-koppelregister’. Daardoor kunnen de aanbieders van private authenticatiemiddelen, ook als ze daartoe geen gebruik mogen maken van het BSN van de betrokkene, gebruik maken van een pseudo-identiteit (een soort schaduw-BSN).

De huidige versie van het koppelregister is niet de versie die uiteindelijk nodig is. Het is duidelijk dat het op de weg van BZK ligt om de uiteindelijk benodigde versie van het BSN-koppelregister te (laten) bouwen en op hoogwaardig niveau te (laten) blijven exploiteren.

Voorbeeld Stop-ID

Onder andere in het kader van de RDA-pilot bij RDW is (door PWC) geadviseerd om zorg te dragen voor een zogeheten Stop-ID-faciliteit. Die faciliteit dient ertoe dat burgers op elk moment per direct het gebruik van hun authenticatiemiddel kunnen stopzetten wanneer daar aanleiding toe is (bijvoorbeeld bij zoekgeraakte of gestolen documenten). Zo'n faciliteit maakt, zo adviseerde PWC, onderdeel uit van de voorwaarden om een middel als de RDA-oplossing tot het beoogde betrouwbaarheidsniveau (in dit geval 'substantieel') te brengen. De commissie benadrukt dat een dergelijke faciliteit, juist ook vanuit burgerperspectief, van groot belang is.

Voorbeeld toezichtsarrangementen

In het kader van (de evaluatie van) de pilots is geen specifieke aandacht besteed aan verschillen in de toezichtsarrangementen op de organisaties die de authenticatiemiddelen uitgeven. Daarbij is met name interessant in hoeverre het toezicht op de private middelen verschillend belegd gaat worden. Zoals nu is voorzien, is het Agentschap Telecom de instantie die toezicht gaat uitoefenen op de uitgevers van Idensysmiddelen, terwijl het toezicht op de banken, in casu de uitgevers van de iDIN-middelen, belegd is bij DNB, als onderdeel van het integrale toezicht dat DNB uitoefent op de banken.
De commissie is van mening dat het geen verstoring van de verhoudingen hoeft te betekenen wanneer het toezicht op de aanbieders van Idensysmiddelen elders is belegd dan dat op de uitgevers van iDIN-middelen, maar dat vergt dan wel een zo gelijk mogelijk toezichtsarrangement in beide stelsels. Voor zover de commissie heeft kunnen nagaan, moeten daar nog afspraken over worden gemaakt.

Voorbeeld makelaarsrol

In de beoogde multimiddelenaanpak zullen alle dienstaanbieders in het BSN-domein een aansluiting moeten regelen voor alle authenticatiemiddelen die voldoen aan de eisen die op overkoepelend niveau worden gehanteerd. Daartoe is in zowel het iDIN-stelsel als in het Idensysstelsel reeds voorzien in de rol van makelaars tussen de dienstaanbieders en de middelenleveranciers.
Wat nog moet uitkristalliseren is hoe invulling gegeven gaat worden aan de makelaarsrol ten opzichte van de beoogde publieke authenticatiemiddelen. Moet daartoe ook een publieke makelaar ingesteld worden? Blijft het bereik van die publieke makelaar beperkt tot het publieke middel? In dat laatste geval: moeten dienstverleners dan dus twee makelaars inhuren? Of kunnen dienstverleners er ook voor kiezen om te volstaan met één private makelaar?

Generaliserend

Dit zijn niet meer dan enkele voorbeelden van voorzieningen (respectievelijk systeemkeuzes) die nodig zijn om de multimiddelenaanpak te laten werken. En het zijn soms ook voorbeelden die illustreren dat de aanpak die nu, onder regie van BZK, plaatsvindt voor het BSN-domein, zorgvuldige afstemming zal blijven vergen met de aanpak die, onder regie van EZ, plaats zal blijven vinden in het

niet-BSN-domein. De commissie is van oordeel dat de 'knip' die nu is aangebracht tussen het BSN-domein en het niet-BSN-domein, alleen verantwoord blijft wanneer BZK en EZ zorgvuldig blijven afstemmen. Dit vergt dus ook op overkoepelend niveau een hoogwaardige governance. In die governance moeten overigens niet allen genoemde twee departementen, maar ook medeoverheden en uitvoeringsorganisaties een belangrijke rol (blijven) spelen. Uiteraard zal ook afstemming moeten blijven plaatsvinden met de leveranciers van private authenticatiemiddelen.

c. Transitievoorzieningen nodig?

Kernpunt:

Naar analogie van de ervaring bij andere grote trajecten, geeft de commissie in overweging om na te gaan of enigerlei vorm van aansluitondersteuning opportuun is: hoe borgen we dat alle dienstverleners daadwerkelijk is staat zijn om, op tijd, aan te sluiten op alle toegestane authenticatiemiddelen?

Toelichting:

In het kader van onze oriënterende gesprekken met stakeholders kwam regelmatig de vraag op in hoeverre alle dienstverleners in het BSN-domein op eigen kracht in staat zullen zijn om de transitieslag naar het beoogde stelsel te maken. Veel zal afhangen van de mate waarin en de wijze waarop de beoogde makelaarsrol daarin voorziet. Maar los van de makelaarsrol lijkt het de commissie ook dat één van de basisvoorwaarden voor een succesvolle transitie zal zijn dat de softwareleveranciers van die dienstverleners in staat en bereid zijn die transitie de facto vorm te geven in de onderliggende software van de dienstverleners.

De commissie adviseert om indringend na te gaan in hoeverre het opportuun is om enigerlei vorm van - tijdelijke - aansluitondersteuning te realiseren. Daarbij zijn, ook vanuit 'het veld', voorbeelden genoemd als de aansluitingsondersteuning die gegeven is in de aanvangsfase van het implementatietraject rond Standard Business Reporting (SBR). Toentertijd is die aansluitondersteuning georganiseerd door de overheid, aangezien het ging om de eerste stromen richting een overheidsorganisatie (in casu de Belastingdienst).

8. Enkele nadere noties om rekening mee te houden

a. Noties vanuit internationaal perspectief

Kernpunt:

Uit een internationale vergelijking kunnen geen aanwijzingen worden ontleend met een generieke strekking. Wel kunnen we leren dat bij de wijze waarop in Nederland toegewerkt gaat worden naar een hoger betrouwbaarheidsniveau van de authenticatiemiddelen, gewaakt moet worden voor het risico dat de gebruiksvriendelijkheid te zeer onder druk komt te staan: dit vereist dus een zorgvuldige veranderstrategie en een hoogwaardig communicatietraject. Daarnaast staan alle EU-landen voor de opgave om het aanstaande eIDAS-regime te gaan toepassen. Dat vraagt om een strakke regie vanuit EZ en BZK, maar roept ook technische complicaties op (zie ook BIT-advies).

Toelichting:

De commissie heeft zich laten informeren over hoe in andere landen met de onderhavige materie wordt omgegaan, alsmede met de vraag welke eisen vanuit internationaal perspectief (in het bijzonder ook EU-perspectief) op ons af komen.

Hoe doen andere landen het?

Uit vergelijking van hoe andere landen omgaan met de onderhavige materie, komt een zeer uiteenlopend beeld naar voren. Ook in landen waarmee Nederland in veel opzichten sterk vergelijkbaar is, zien we zeer uiteenlopende aanpakken. Dat geldt voor het al dan niet hanteren van centrale databases als onze Basisregistratie Personen. Het geldt ook voor het al dan niet hanteren van een voorziening als ons BSN. Ook op privacyvraagstukken zien we opvallende verschillen: er zijn landen waar niet alleen ieders BSN een openbaar gegeven is, maar ook de inkomens en de betaalde belasting per belastingplichtige. En daartegenover zijn er landen waar dit soort gegevens juist strikt tot de privacy van ieder individu worden gerekend.
Ook de mate waarin authenticatiemiddelen privaat dan wel publiek van karakter zijn, loopt sterk uiteen: soms gaat het om middelen die publiek van karakter zijn en ook door een publieke organisatie worden geproduceerd, soms zijn ze publiek van karakter maar door een privaat bedrijf geproduceerd; maar het komt ook voor dat de voor het overheidsdomein bedoelde authenticatiemiddelen juist *niet* publiek van karakter zijn; in die gevallen worden de middelen door een privaat bedrijf geproduceerd.
Ook doen zich grote verschillen voor in de mate van betrouwbaarheid die in de middelen respectievelijk in de systemen is verankerd. Er zijn duidelijke indicaties dat landen die kiezen voor het

hanteren van een hoog betrouwbaarheidsniveau, vaak moeite hebben met het behalen van een grote verspreidingsgraad en een hoog niveau van het daadwerkelijk hanteren van de desbetreffende authenticatiemiddelen. Dat heeft vermoedelijk veel te maken met het gebruiksgemak dat eindgebruikers (in casu burgers) ervaren: hoe meer middelen beveiligd zijn, des te minder gebruiksvriendelijk ze zijn en des te groter is de drempel om ze ook te gaan gebruiken. Landen die beginnen met een relatief bescheiden betrouwbaarheidsniveau, bereiken vaak sneller een hoog verspreidings- en benuttingsniveau. Nederland valt in de categorie waar - met DigiD - een hoog niveau van verspreiding en benutting is behaald, met daarbij de aantekening dat DigiD, naar de huidige maatstaven, een relatief laag betrouwbaarheidsniveau kent. Desondanks heeft DigiD op zich nog steeds stand gehouden, op een enkel incident na.

De commissie trekt hieruit de volgende conclusies.
In de eerste plaats: er is geen best practice waaraan we ons zonder meer kunnen spiegelen. Elk land kent zijn eigen tradities, zijn eigen voorkeuren en in zekere zin ook zijn eigen taboes. Er is, vanuit deze notie, geen contra-indicatie af te leiden ten opzichte van de in Nederland voorgestane multimiddelenaanpak.
In de tweede plaats: een evident opletpunt in de beoogde nieuwe aanpak is dat we aan de ene kant wel moeten toewerken naar een hoger betrouwbaarheidsniveau dan wat thans mogelijk is met DigiD, maar dat we aan de andere kant het kind niet met het badwater moeten wegspoelen: de overgang naar een hoger betrouwbaarheidsniveau moet, als het even kan, niet gepaard gaan met significant hogere drempels voor een 'burgervriendelijk' gebruik. Uit de evaluatie van de pilots is niet gebleken dat dit nu het geval dreigt te zijn, maar het blijft wel een opletpunt.

Wat komt er vanuit EU-perspectief op ons af rond grensoverschrijdend gebruik?

Via (in de maak zijnde) EU-regelgeving, moeten nationaal te ontwikkelen authenticatiemiddelen ook grensoverschrijdend gehanteerd kunnen worden. Hiervoor geldt het eerder genoemde zogeheten eIDAS-kader. Dit kader (waarop we ook in het voorgaande reeds zijn ingegaan) stelt indringende eisen aan de binnen ons beoogde stelsel te hanteren regels. Dit geldt beide kanten op: onze eigen Nederlandse authenticatiemiddelen moeten eraan voldoen, maar onze publieke organisaties in het BSN-domein zullen ook in staat moeten zijn om te gaan met (Nederlandse en buitenlandse) burgers die met authenticatiemiddelen willen inloggen die elders (in andere EU-landen) zijn uitgegeven.

Dit alles levert complicaties op, zowel op het overkoepelende niveau als op het niveau van de techniek van de afzonderlijke middelen en op het niveau van de individuele publieke organisaties. De commissie heeft hier slechts oppervlakkig kennis van kunnen nemen. Onze indruk is dat de bedoelde complicaties hanteerbaar zijn en ook onderkend worden door de partijen die daarvoor aan de lat staan. Maar dat laat onverlet dat hier nog een forse opgave op tafel ligt. Nagegaan moet worden hoe aan die complicaties het hoofd kan worden geboden, zonder de risico's te lopen waar het BIT-advies op duidt (in zijn pleidooi voor vermindering van complexiteit).

b. Interactie tussen publieke en private middelen

Kernpunt:

Als de multimiddelenaanpak goed wordt ingevoerd, zijn er kansen op een soort symbiose. Het nieuwe publieke middel kan op termijn waarschijnlijk profiteren van het innovatieve vermogen van marktpartijen. En een hoogwaardig, via baliecontact uitgegeven maar ook elektronisch te gebruiken publiek middel bevordert niet alleen de kwaliteit van de private middelen, maar ook de kansen van marktpartijen om, tegen een redelijk tarief, hoogwaardige private middelen aan de man te brengen.

Toelichting:

Al eerder wezen we erop dat de multimiddelenaanpak impliceert dat het beoogde publieke middel en de beoogde private middelen *naast elkaar* bestaan. Waar we nog extra aandacht voor willen vragen is het punt dat versterking van het publieke middel ook als meerwaarde kan hebben dat daardoor de private middelen versterkt kunnen worden. En mogelijkerwijs geldt dat ook andersom. De redenering daarbij is als volgt.

Het publieke middel is te beschouwen als een soort 'moederkaart'. Iedereen in Nederland hoort - nu al - te beschikken over een door de overheid uitgegeven publiek middel waarmee hij/zij zich kan authenticeren (paspoort, identiteitskaart, rijbewijs). Als we ervan uitgaan dat het beoogde publieke middel voor elektronische authenticatie voorshands gebonden zal blijven aan die documenten, dan ontleent dat document zijn unieke waarde mede aan het feit dat zo'n document alleen wordt afgegeven door de overheid en altijd via een fysieke uitgifte aan een balie, waarmee ook een duidelijke controle kan plaatsvinden of het document wordt uitgegeven aan degene op wiens naam het document is gesteld. Dit is een belangrijk element waardoor een publiek middel uiteindelijk, met inbegrip van hoogwaardige techniek in de chip van zo'n document, betrouwbaarheidsniveau 'hoog' zal kunnen bereiken.
Het is van belang te weten dat juist dit uitgifteproces zo'n publiek document duur maakt (niet duurder overigens dan wanneer dat document niet zou worden voorzien van een hoogwaardige chip): het balieproces kost tijd en geld.

Private middelen kunnen gebruik maken van dit hoogwaardige proces van uitgifte van het fysieke (maar tevens juist elektronisch te gebruiken) publieke middel. Zo zijn er uitgifteprocessen van private middelen in de maak en zelfs al werkzaam waarbij in het geheel geen baliecontact met betrokkene nodig is, omdat de uitgever van het private middel zich kan vergewissen van de identiteit van de betrokkene door on line gebruik te maken van de mogelijkheden die het fysieke publieke middel, na uitgifte bij een overheidsbalie, elektronisch biedt. Mits hoogwaardig vormgegeven kunnen aldus ook private middelen het betrouwbaarheidsniveau 'hoog' bereiken *zonder de hoge kosten van een eigen baliecontact*. Dit kan zeer bevorderlijke effecten hebben voor de uitgifteprocessen van authenticatiemiddelen door private partijen, en via die lijn dus ook voor het tot ontwikkeling komen van de markt voor private authenticatiemiddelen.

Andersom kan ook sprake zijn van een impuls. Het is niet onaannemelijk dat marktpartijen innovatiever zullen zijn dan de overheid zelf, waar het gaat om ontwikkelingen die een

authenticatiemiddel gebruiksvriendelijker en/of betrouwbaarder maken. Denkbaar is dat het publieke middel daarvan ook kan profiteren, door innovaties die bij de private middelen zijn ontwikkeld, over te nemen.

Wat we dus zien, is een vorm van symbiose: het (elektronisch te gebruiken) publieke middel kan op termijn waarschijnlijk gebruik maken van het innovatief vermogen van marktpartijen, en een hoogwaardig (via de balie uit te geven maar ook elektronisch te gebruiken) publiek middel bevordert niet alleen de kwaliteit van de private middelen, maar ook de kansen van marktpartijen om, tegen een redelijk tarief, hoogwaardige private middelen aan de man te brengen.
Overigens zien we hier een bijzondere vorm waarin het gebruik van het publieke middel in het niet-BSN-domein als zinnig en zelfs essentieel is aan te merken voor het functioneren van de multimiddelenaanpak als geheel.