Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

eID stelsel Nederland

Strategische verkenning en voorstel voor vervolg

Voorwoord

De Nederlandse overheid biedt haar diensten steeds vaker op digitale wijze aan. Naast slimme ICT, goed georganiseerde processen en bescherming van persoonsgegevens is het op betrouwbare wijze verkrijgen van toegang door burgers en bedrijven tot elektronische dienstverlening van primair belang om het vertrouwen in die dienstverlening te waarborgen. Dat vergt de beschikbaarheid van oplossingen om de identiteit met een voldoende mate van zekerheid digitaal vast te kunnen stellen: een elektronische identiteit (eID).

Voor u ligt het resultaat van een strategische verkenning van een aantal Nederlandse overheidsorganisaties naar de mogelijkheden voor een gecoördineerd, nationaal stelsel van elektronische identiteiten. Deze verkenning is in de zomer van 2012 uitgevoerd op verzoek van bestuurders van organisaties van de Rijksoverheid, uitvoeringsorganisaties en gemeenten en in gezamenlijkheid tot stand gekomen.

De Nederlandse overheid heeft op dit moment via verschillende sporen invulling gegeven aan haar beleid op het gebied van elektronische identiteiten: voor burgers is er DigiD, bedrijven kunnen gebruik maken van eHerkenning en voor machine-machineverkeer met en tussen overheidsorganisaties bestaat PKI-Overheid. Daarnaast bestaan er nog tal van organisatiespecifieke oplossingen.

De elektronische identiteiten van burgers en bedrijven zijn momenteel dus strikt gescheiden. Voor bijvoorbeeld ZZP'ers en intermediairs is deze situatie ongewenst. De oplossing is om deze sporen met elkaar te integreren.

Ook heeft een reeks incidenten bij de overheid (DigiNotar, Lektober) en in de private sector (hacks bij KPN, LinkedIn etc.) geleid tot negatieve beeldvorming over de veiligheid van digitaal zaken doen. Daardoor is het vertrouwen in elektronische dienstverlening in de publieke én private sector onder druk komen te staan. Er is een breed gedeeld gevoel van urgentie: dit moet veiliger, elektronische identiteit voor burgers in Nederland moet naar een hoger plan getild worden.

Onderstaande bestuurders en hun overheidsorganisaties onderschrijven allemaal nut en noodzaak van een generiek eID stelsel voor burgers en bedrijven in Nederland. Er kan slim gebruik gemaakt worden van wat er al is, zowel binnen de publieke als private sector. Deze groep ziet een meerwaarde van samenwerking op het gebied van elektronische identiteit. Samenwerking binnen Rijk, gemeenten en uitvoeringsorganisaties, maar ook samenwerking tussen de publieke en de private sector.

Deze verkenning is een eerste stap naar meer en betere samenwerking binnen de overheid op dit thema. De tweede stap is verbinding zoeken met de private sector. Op termijn is de visie één nationaal stelsel eID, waarin overheid en bedrijfsleven samenwerken om burgers, consumenten en bedrijven zo goed, snel en veilig mogelijk elektronisch kunnen bedienen.

Hans Blokpoel	Algemeen Directeur Landelijk Kantoor Belastingregio's Belastingdienst
Elly Bogerman	Directeur Stichting ICT Uitvoeringsorganisatie (ICTU)
Gert-Jan Buitendijk	Directeur-generaal Bestuur en Koninkrijksrelaties Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Staf Depla	Wethouder van Financiën, Dienstverlening & Organisatie Gemeente Eindhoven
Johanan van Diermen	Programmamanager ICT in de Zorg Ministerie van Volksgezondheid, Welzijn en Sport
Arco Groothedde	Tot september 2012 lid Raad van Bestuur Kadaster
Johan Hakkenberg	Algemeen Directeur Rijksdienst voor het Wegverkeer (RDW)
Maarten Hillenaar	Directeur Informatie Rijk (CIO Rijk) Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Gerdine Keijzer-Baldé	Directeur Agentschap Basisadministratie Persoonsgegevens & Reisdocumenten (BPR)
Rob Kerstens	Directeur-generaal Dienst Uitvoering Onderwijs (DUO)

Nicole Kroon	Directeur Regeldruk en ICT-beleid Ministerie van Economische Zaken, Landbouw en Innovatie
José Lazeroms	Lid Raad van Bestuur Uitvoeringsinstituut Werknemers Verzekeringen (UWV)
Steven Luitjens	Directeur Dienst digitale overheid Logius
Hans Nijman	Chief Information Officer Gemeente Rotterdam
Simon Rijsdijk	Vicevoorzitter Nederlandse Vereniging voor Burgerzaken (NVVB)
Ron Roozendaal	Chief Information Officer Ministerie van Volksgezondheid, Welzijn en Sport
Bertine Steenbergen	Directeur Burgerschap en Informatiebeleid Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Inhoudsopgave

Managementsamenvatting

Aanleiding

De Nederlandse maatschappij wordt in hoog tempo gedigitaliseerd. Elektronische dienstverlening is zowel gebruiksvriendelijk als (kosten)efficiënt.
Voor de private en publieke sector is het vertrouwen van mensen en organisaties in elektronische dienstverlening essentieel. Dat vertrouwen komt steeds meer onder druk te staan, ondermeer omdat het betrouwbaarheidsniveau van bestaande elektronische identificatiemiddelen (gebruikersnaam/wachtwoord) voor burgers niet toereikend is. Het is wenselijk dat op grote schaal eID-voorzieningen op hogere veiligheidsniveaus voor burgers beschikbaar komen, zodat het vertrouwen in de digitale dienstverlening geborgd blijft. Voor bedrijven bestaan er binnen eHerkenning al voorzieningen op het hoogste veiligheidsniveau.

Voor burgers en bedrijven is het van belang dat het gebruik van betrouwbare authenticatiemiddelen en elektronische diensten in de toekomst veilig is (met betrouwbare technologie), gemakkelijk is (tijd en plaatsonafhankelijk), over de grenzen gaat van het onderscheid tussen burgers/bedrijven. Voor een grote groep (circa 1,1 miljoen) natuurlijke personen die een onderneming hebben, bijvoorbeeld in de rechtsvorm van een eenmanszaak (zoals ZZP'ers), is het onderscheid tussen voorzieningen voor burgers en bedrijven onwenselijk. Tot slot is het uitgangspunt dat eID middelen op termijn binnen de Europese Unie uitwisselbaar zijn en dat de privacy voldoende geborgd is.

Om de afhankelijkheid van één specifiek elektronisch identificatiemiddel (eID-middel) te beperken is het van belang een strategie te hebben waarin meerdere middelen beschikbaar zijn om dienstverlening te ontsluiten, een zogenoemde multi-middelen strategie. Daarmee wordt een fallback bij calamiteiten gecreëerd. Verder moeten afzonderlijke (overheids-) dienstverleners moeten 'ontzorgd' worden, zodat zij geen directe migratie- en koppelafhankelijkheid hebben van de diverse eID-dienstverleners (identiteit leveranciers) en niet zelf hun eigen voorzieningen hoeven te ontwikkelen en beheren. Gelijkwaardige bruikbaarheid van publieke en private eID-middelen heeft een enorm potentieel economisch rendement van gemaakte investeringen en opent innovatiemogelijkheden, zowel nationaal als internationaal. Nederlandse burgers en bedrijven moeten dan ook zonder enige blokkade kunnen deelnemen aan het vrije (digitale) handelsverkeer binnen de Europese grenzen.

Opdracht

Voer een verkenning uit naar de mogelijkheden voor een overheidsbreed eID stelsel, o.a. gericht op een bredere beschikbaarheid van

elektronische identificatiemiddelen op hoog niveau.

De verkenning is uitgevoerd door de beleidsverantwoordelijke ministeries (Binnenlandse Zaken en Koninkrijksrelaties, Economische Zaken, Landbouw en Innovatie) samen met drie grote uitvoeringsorganisaties, te weten de Belastingdienst, de Rijksdienst voor het Wegverkeer (RDW) en het Uitvoeringsinstituut Werknemers Verzekeringen (UWV).[1] Daarnaast zijn diverse andere overheidsuitvoeringsorganisaties geconsulteerd.

De verkenning heeft geresulteerd in deze strategische verkenning, inclusief een voorstel voor vervolg (periode oktober 2012 en verder, zie hoofdstuk 5) en een eerste overzicht van de benodigde stelselafspraken en -specificaties (bijlage 2).

Behoefte overheidsdienstenaanbieders

Uit een consultatieronde met overheidsdienstverleners komen de volgende hoofdconclusies naar voren:

1. De meerwaarde van een nationaal eID-stelsel wordt onderschreven. De meerwaarde bevindt zich zowel op het niveau van beleid/bestuur als gemeenschappelijke uitvoeringskaders en (op onderdelen) gemeenschappelijke infrastructuur.
2. Het eID stelsel is een randvoorwaarde voor het realiseren van de compacte overheid.
3. Er is een grote behoefte aan een generiek eID stelsel in o.a. zorg, onderwijs en sociaal-financieel domein. Daar is nog veel winst (in termen van administratieve lastenverlichting) te halen door verdere digitalisering van de processen en veilige uitwisseling van informatie.
4. Het eID stelsel is essentieel om de diversiteit in de bestaande en toekomstige e-dienstverlening en de daarbij behorende betrouwbaarheidsniveaus te faciliteren en te stroomlijnen.
5. Overheidsdienstverleners geven aan dat zij met een authenticatiemiddel voor burgers en bedrijven op hoog niveau een aantal voordelen kunnen behalen, die zij op dit moment nog niet kunnen realiseren:
   1. Optimalisering van bestaande e-dienstverlening
   2. Verdere digitalisering van dienstverleningsprocessen
   3. Een hogere effectiviteit en efficiency, resulterende in kostenbesparingen
   4. Hogere veiligheid/betrouwbaarheid
6. De ene overheidsdienstverlener heeft meer behoefte aan een snelle uitrol van een authenticatiemiddel op hoog niveau dan de andere. De behoefte aan snelle uitrol bevindt zich vooral in het burgerdomein. In het bedrijvendomein is een hoog niveau al beschikbaar. Daar gaat

[1] Het ministerie van VWS is agendalid van de zomerwerkgroep.

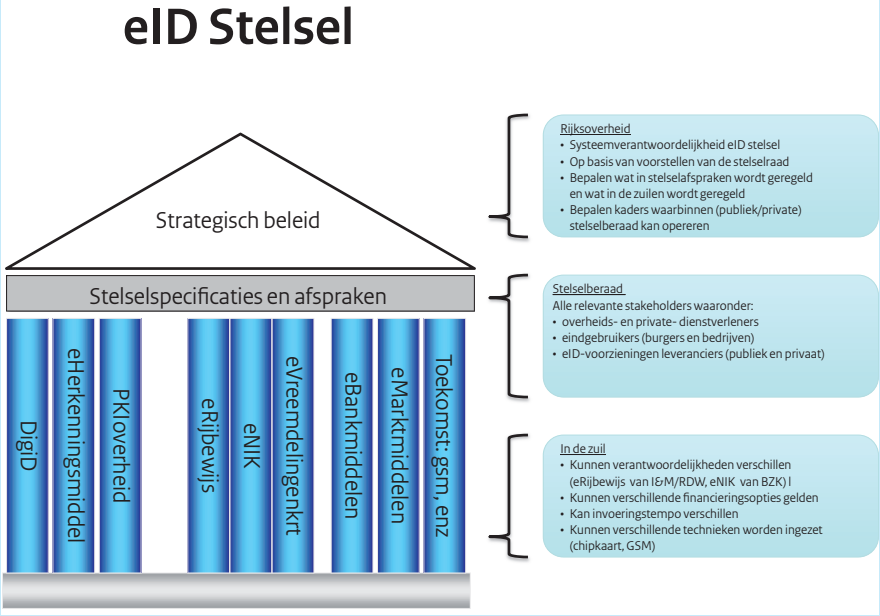
het vooral om functionele toevoegingen, zoals voor machine-machineverkeer en om implementatie.
7. De wens om binnen het stelsel rekening te houden met verschillende implementatiesnelheden.
8. Financiële laagdrempeligheid voor eindgebruikers is in beide domeinen (burger en bedrijf) een belangrijke wens.

Voorgestelde oplossingsrichting voor het stelsel eID Nederland

In de uitwerking van het eID-stelsel zijn drie niveaus te onderscheiden:

1. Het strategisch beleid van de overheid op het gebied van authenticatie en autorisatie. Het consolideren van het strategisch beleid is primair de taak van de beleidsdepartementen. Dit eID-beleid is een gezamenlijke verantwoordelijkheid van de ministeries van BZK en van ELenI. Om een gedragen strategisch beleid tot stand te brengen is afstemming met alle betrokken partijen essentieel.
2. Stelselafspraken en –specificaties, gebaseerd op het strategisch beleid. De specificaties en afspraken worden opgesteld en beheerd door betrokken uitvoerende organisaties (zowel publiek als privaat) en gezamenlijk met alle stakeholders opgesteld, in een daarvoor ingerichte governancestructuur.
3. Specifieke eID-voorzieningen: diensten voor authenticatie (chip-)cards, certificaten, tokens e.d.) autorisatie (machtigingsregisters) en elektronische handtekeningen, gebaseerd op de stelselspecificaties en –afspraken. Voor de ontwikkeling en het beheer zijn de respectieve uitvoerende publieke en private partijen verantwoordelijk: zij bepalen hun eigen uitrolstrategie en kunnen binnen het strategisch beleid en kaders hun eigen keuzes maken met betrekking tot inrichting en techniek.

Schematisch ziet het stelsel eID Nederland er als volgt uit:



Doordat met behulp van gezamenlijk vastgestelde afspraken en specificaties de eisen aan voorzieningen worden gestandaardiseerd, kunnen zowel private als publieke voorzieningen worden toegevoegd aan het stelsel. Voorwaarde is dat deze voldoen aan de afspraken en dat partijen zich onderwerpen aan het bijbehorende toezicht. Het toezicht zal op een adequate en passende wijze moeten worden ingericht, hierbij zal de optie wettelijk toezicht ook onderzocht worden. Hierdoor kunnen nieuwe technologieën en middelen worden opgenomen in het stelsel en verouderde technologieën en middelen worden uitgefaseerd. Het stelsel wordt daarmee toekomstbestendig.

Door standaardisatie komt een ontkoppeling tot stand tussen de primaire diensteninfrastructuur van de overheidsdienstverlener en het elektronisch identificatie proces. Dienstverleners worden op deze manier ontzorgd en hoeven niet separaat steeds grotere investeringen in kennis en techniek op te brengen om aan steeds hogere veiligheidseisen te voldoen.

Door de voorgestelde multimiddelenstrategie zijn er binnen het stelsel meerdere middelen beschikbaar. Voordelen hiervan zijn dat de gehele populatie van mogelijke klanten sneller afgedekt wordt en dat men indien nodig direct terug kan vallen op een ander middel. De middelen zijn daarnaast breed inzetbaar; bedrijven en consumenten kunnen dezelfde middelen zowel voor de diensten van de overheid als van bedrijven gebruiken. Bedrijven hoeven daardoor niet in het uitgeven van eigen middelen te investeren om diensten te kunnen aanbieden aan burgers. Zo geeft de brede beschikbaarheid en herbruikbaarheid van betrouwbare eID-voorzieningen met een hoog veiligheidsniveau voor burgers een impuls aan de digitale economie en maakt verdere ontwikkeling van e-dienstverlening mogelijk. Wel zal het nodig zijn om blijvend te investeren in betrouwbaarheid, vanwege de toegenomen risico's op misbruik. Huidige dienstverlening kan zo veilig blijven.
De strikte scheiding in middelen tussen burgers en bedrijven verdwijnt, immers er zijn vele natuurlijke personen die een onderneming hebben. Voor hen is het onderscheid tussen burger en bedrijf onnodig en ongewenst. Burgers en bedrijven krijgen binnen het afsprakenstelsel keuzevrijheid in relatie tot het (publieke of private) middel dat zij willen gebruiken.

De definitieve tekst van de Europese verordening elektronische identiteit, die onlangs is gepubliceerd door de Europese Commissie, is op dit moment nog niet bekend. Vast staat dat op termijn Nederlandse overheidsdienstverleners ook buitenlandse eID's met het hoogste betrouwbaarheidsniveau zullen moeten kunnen accepteren, maar mogelijk ook dat NL burgers worden uitgesloten voor bepaalde elektronische dienstverlening in andere EU-lidstaten, die dit hogere betrouwbaarheidsniveau vereisen, waarover zij (nog) niet beschikken.
Ook wordt het belangrijk dat Nederlandse eID middelen op termijn binnen de gehele EU bruikbaar zijn, zodat Nederlandse burgers en bedrijven hiermee toegang krijgen tot de Europese digitale interne markt en overheidsdiensten in andere lidstaten. Voor grensoverschrijdend gebruik van eID middelen zal hierdoor een uitvoeringsvraag gaan ontstaan. In de toekomst zal dit ook binnen de scope van het afsprakenstelsel worden gebracht.

Voor het realiseren van het bovenstaande, wordt het volgende tweesporen beleid voorgesteld:
Het ontwikkelen van het eID Stelsel NL
Zorg dragen voor het breed beschikbaar krijgen van een hoog niveau eID-middel voor burgers/consumenten.

Beide sporen worden in deze managementsamenvatting kort weergegeven. Een uitgebreide beschrijving is te vinden in hoofdstuk 4.

1. Eén eID stelsel Nederland

Ten aanzien van de ontwikkeling van het eID stelsel adviseert de werkgroep dat:

1. Er één eID-afsprakenstelsel komt, voor het burger én bedrijvendomein, waardoor
   a. dezelfde standaarden gelden voor het burger- en bedrijvendomein;
   b. er een ontkoppeling plaatsvindt tussen diensteninfrastructuur en eID-middelen infrastructuur (ontzorgen dienstverleners);
   c. en waarbinnen een ontkoppeling van technologie plaatsvindt (toekomstvaste adaptiviteit i.p.v. technologieafhankelijkheid).
2. Zowel publieke als private online authenticatiemiddelen in het eID-stelsel zullen worden ondergebracht.
3. De middelen onder het stelsel zowel bruikbaar zullen zijn voor publieke als voor private (elektronische) dienstverleners.
4. In de toekomst de hierin ondergebrachte middelen ook in het buitenland gebruikt kunnen worden.
5. De Rijksoverheid systeemverantwoordelijk is voor het afsprakenstelsel. En daarmee dat de overheid:
   a. Gecoördineerd beleid ontwikkelt m.b.t. digitale identiteiten en machtigingen
   b. Het afsprakenstelsel actief onderhoudt en beheert
   c. Toezicht uitoefent op (delen van) het afsprakenstelsel en de deelnemers
6. Het aansluiten op het eID stelsel voor overheidsdienstverleners op de "pas-toe-of-leg-uit"-lijst van het standaardisatiecollege wordt gezet.

2. Hoog niveau eID middel voor burgers

Ten aanzien van het breed beschikbaar krijgen van een hoog niveau eID middel voor burgers adviseert de werkgroep dat:

1. De overheid ervoor zorgt dat middelen op relatief korte termijn op het hoogste niveau beschikbaar komen voor burgers.
2. Het mix-scenario de voorkeur heeft: daarin worden publieke middelen èn private middelen uitgegeven en gebruikt.
3. De overheid gaat publieke middelen op het hoogste niveau uitgeven.
4. Ten behoeve hiervan dient het mixscenario nader te worden uitgewerkt. Daarbij komt naar voren:
   a. Welke (combinatie van) dragers wenselijk is, mede gelet op het afdekken van de gehele klantpopulatie (vertrekpunt zijn de huidige 9 miljoen DigiD gebruikers).
   b. Welke massale uitrol scenario's mogelijk zijn (bijvoorbeeld niet wachten op regulier vervanging bij NIK/Rijbewijs maar stimuleringsmaatregelen om eerder om te wisselen; en het versneld inschakelen van reeds uitgerolde marktmiddelen zoals bankmiddelen).
   c. Welke kosten brengt het met zich mee, en welke financieringsopties zijn er (kostendekking aanschaf, kostendekking gebruik, wat kost het de burger, wat kost het een dienstaanbieder, welke kosten worden centraal

gedragen). In de vorm van een businessmodel vertaald naar maatschappelijke baten en bedreigingen (ontwrichting van de infrastructuur).

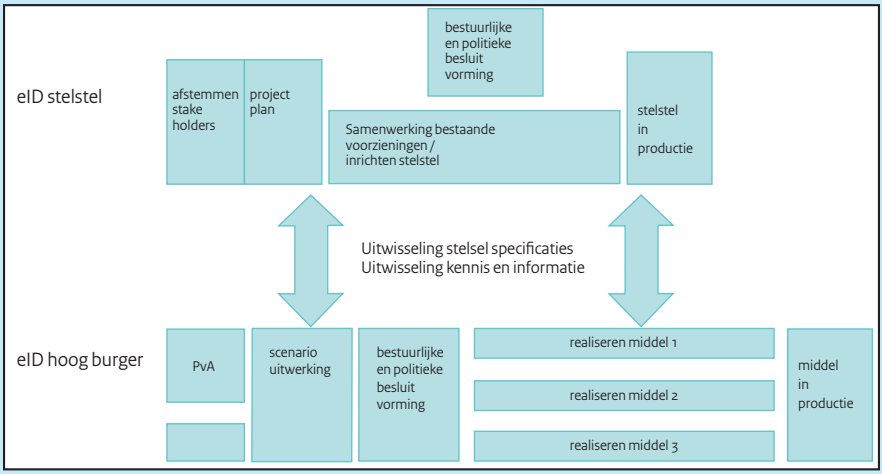
5. Deze middelen niet noodzakelijkerwijs gratis zijn (vergelijkbaar met identiteitsbewijzen in de fysieke wereld).
6. De overheid een 'omnummervoorziening' realiseert, die het gebruik van private eID-middelen bij overheidsdiensten mogelijk maakt (overheidsdienstverleners herkennen hun klant immers aan het BSN).
7. Nader wordt onderzocht - hoe privaat gebruik van deze middelen (op termijn) conform paragraaf 4.2.3. - op een privacyvriendelijke manier kan plaatsvinden.

Voorstel voor vervolg

Deze strategische verkenning wordt na afstemming met de Berlijngroep en de Manifestgroep voorgelegd aan een stuurgroep eID op 4 oktober 2012. Op dit punt bereikt het document de status van een binnen de overheid vervaardigde en ambtelijk overeengekomen conceptversie. Hoofdstuk 5 beschrijft een aantal aspecten die specifiek aan de politiek dienen te worden voorgelegd. Ter voorbereiding op deze politieke besluitvorming worden de komende maanden gebruikt voor afstemming met stakeholders en het daadwerkelijk voorbereiden op implementatie van de adviezen via twee sporen.

1. Spoor 1: Inrichten van het eID-stelsel Nederland
2. Spoor 2: Uitwerken van verschillende scenario's voor een eID-middel op hoog niveau voor burgers

Beide sporen zijn aparte projecten met een eigen karakter en temp. Hierdoor kan meer slagkracht worden gemaakt. Schematisch ziet dit er als volgt uit:



Spoor 1: Stelsel eID NL

Stap 1: Betrekken overige publieke en private belanghebbenden (oktober/november). De externe stakeholders zijn in ieder geval, maar niet perse beperkt tot, banken, leveranciers van trust diensten (bv marktpartijen eHerkenning), medeoverheden), VNO/NCW, ECP-EPN, vertegenwoordiging softwareleveranciers, vertegenwoordiging fiscale en andere dienstverleners en vertegenwoordiging consumenten/burgers.

Resultaat: Gedragen strategische visie die voorgelegd kan worden aan de politiek (NB: Snelheid/route is afhankelijk van de kabinetsformatie)

Stap 2: Uitwerken programmaplan

Resultaat: Door de opdrachtgever(s) goedgekeurd programmaplan in november 2012

In het programmaplan komen de volgende deelresultaten terug:

I. Verdeling verantwoordelijkheden & toezicht
II. Inhoudelijk: stelselafspraken en specificaties
III. Implementatie

Spoor 2: eID-middel hoog voor burgers

Het doel van het tweede spoor is het beschikbaar komen van een eID-middel hoog (STORK niveau 3 en 4) voor burgers. Het heeft betrekking op zowel publieke als private eID middelen voor burgers. De trajecten voor het ontwikkelen en het inzetten van publieke en private middelen verlopen parallel aan elkaar. Voor de realisatie van eID hoog voor burgers voorziet de werkgroep drie stappen, namelijk:

- Stap I: voorbereidingen en uitwerking voorkeurscenario
- Stap II: bestuurlijke en politieke besluitvorming
- Stap III: de middellange termijn: realisatie en implementatie

De volgende (deel)resultaten worden in de verschillende fases opgeleverd:

Stap I		**Deadline**
Deelresultaten	Plan van aanpak voorbereiding en scenario's	September 2012
	Uitgewerkte scenario's en financieringsarrangementen (kosten en financiële dekking) voor publieke en private middelen	November 2012
	PvA wetgevingstraject(en)	November 2012
	Herijkte analyse, haalbaarheidsstudie, inclusief keten-afhankelijkheidstudie	December 2012
Eindresultaat	Besluitvormingsmemorandum in stuurgroep eID stelsel NL (voorkeursscenario)	December 2012

Stap II		**Deadline**
Deelresultaten	Detail plan van aanpak fase Kabinetsbesluit	PM, afhankdelijk van vastege-stelde aanpak in stap I
	Planning van de bestuurlijke route (onderraden, adviescommissies, etc)	PM, idem
	Besluitvormingsmemorandum in stuurgroep	PM
Eindresultaat	Besluitvormingsmemorandum in Kabinet	PM

De start van deze stap is afhankelijk van consensus en besluitvorming in de stuurgroep eID stelsel NL en voortgang kabinetsformatie na de verkiezingen.

Stap III		Deadline
Deelresultaten	Detailplan van aanpak fase ontwikkeling en realisatie	PM
	Aanbesteding en gunning eID-middel hoog	PM
	Ontwikkeling en realisatie eID middel(en)	PM
	Wetswijzigingen wetgeving (indien van toepassing)	PM
	Implementatiestrategie	PM
	Mediacampagne naar burgers	PM
Eindresultaat	eID-middel hoog	PM

Conclusie

Met een nationaal eID stelsel Nederland kan een belangrijke stap gezet worden naar een toekomstbestendige en betrouwbare ICT-infrastructuur, die essentieel is voor een blijvend vertrouwen van burgers en bedrijven in elektronische overheidsdienstverlening en de digitale economie, en dus voor de digitale samenleving als geheel.

1. Inleiding

1.1 Aanleiding

Nationaal

De Nederlandse samenleving raakt in hoog tempo gedigitaliseerd, zowel in de private als in de publieke sector. De overheid biedt haar diensten steeds vaker ook op digitale wijze aan, sommige diensten zijn zelfs alleen nog maar digitaal af te nemen. Naast slimme ICT, goed georganiseerde processen en bescherming van persoonsgegevens is het op betrouwbare wijze verkrijgen van toegang tot deze elektronische dienstverlening van primair belang om het vertrouwen er in te waarborgen. Dat vergt de beschikbaarheid van oplossingen om de identiteit van organisaties en burgers met een voldoende hoge mate van zekerheid vast te kunnen stellen: een eID.

De overheid heeft via verschillende sporen invulling gegeven aan beleid voor elektronische identiteiten: voor portaaldiensten aan burgers is er DigiD, voor bedrijven is er eHerkenning, en voor machine-machineverkeer met en tussen overheidsorganisaties is er PKI-Overheid. Daarnaast bestaan er nog tal van organisatiespecifieke oplossingen. Op dit moment zijn de oplossingen voor burgers en bedrijven strikt gescheiden. Voor een grote groep (circa 1,1 miljoen) natuurlijke personen die een onderneming hebben, bijvoorbeeld in de rechtsvorm van een eenmanszaak (zoals zzp'ers) is het onderscheid tussen voorzieningen voor burgers en bedrijven onwenselijk.

Goede elektronische dienstverlening is een aan twee kanten snijdend mes: enerzijds gebruiksvriendelijk, veilig en betrouwbaar zijn, anderzijds kostenefficiënt.

Voor een veelvuldig gebruik in zowel de private sector als met de overheid is blijvend vertrouwen van mensen en organisaties in de betrouwbaarheid van deze diensten essentieel. Dat vertrouwen komt steeds meer onder druk te staan (zie bijlage 3). Een reeks incidenten bij de overheid (DigiNotar, Lektober) en in de private sector (hacks bij KPN, LinkedIn, Twitter-accounts etc.) heeft geleid tot negatieve beeldvorming over de veiligheid van digitaal zaken doen en de informatiebeveiliging bij de overheid. Daardoor komt bestaand gebruik van authenticatiemiddelen onder druk te staan en daarmee ook bestaande verworvenheden, zoals behaalde kostenbesparingen. Tevens kan dit leiden tot een rem op concurrentiekracht en innovatie (zoals *cloud computing*).

Er is inmiddels een breed gedeeld gevoel van urgentie in de maatschappij en bij de overheid ontstaan.
Op de eerste plaats is een laag veiligheidsniveau (gebruikersnaam plus wachtwoord) voor sommige vormen van (overheids) dienstverlening niet langer acceptabel. Dit lage niveau is niet sterk genoeg om de betrouwbaarheid van complexe diensten te borgen noch voldoende om in de toekomst cybercrime te weerstaan. Als maatregel is gewenst dat er op grote schaal voorzieningen op hogere betrouw-

baarheidsniveaus beschikbaar komen, zodat het vertrouwen in de digitale dienstverlening overeind blijft.

Op de tweede plaats is ook de afhankelijkheid van één specifiek elektronisch identificatiemiddel (eID middel) waarmee alle dienstverlening wordt ontsloten, een risico. Daarom is het voor de samenleving van belang een strategie te hebben waarin meerdere middelen beschikbaar zijn om dienstverlening te ontsluiten, een zogenoemde *multimiddelen* strategie. Daarmee wordt een fallback bij calamiteiten gecreëerd.

Met de benodigde hogere veiligheid gaan ook steeds grotere investeringen gepaard die voor individuele organisaties en bedrijven niet meer rendabel zijn. De afzonderlijke (overheids-)dienstverleners moeten 'ontzorgd' worden. Het is gewenst dat zij hun eigen voorzieningen, waar deze nu nog in gebruik zijn, kunnen gaan afstoten. Daarnaast is het gewenst dat zij geen afzonderlijke aansluitingen hoeven te realiseren naar de diverse eID-dienstverleners (leveranciers van authenticatiediensten). Zij moeten gebruikers van diverse authenticatiemiddelen op efficiënte wijze toegang kunnen bieden tot hun diensten. Dat vraagt om standaardisatie van koppelvlakken.
De vraagstukken bij deze voorzieningen zijn voor het burger- en bedrijven domein in hoge mate vergelijkbaar. Een geïntegreerde aanpak is daarom gewenst.

Een goed functionerende digitale economie draagt bij aan economische groei. Zo kan bij voldoende vertrouwen in de digitale markt de digitale dienstverlening met circa € 1,2 mrd groeien[2]. Kernvoorwaarden hierbij zijn veilige en betrouwbare ICT voorzieningen, die de bescherming van persoonsgegevens borgen, eenvoudige toegang tot en beschikbaarheid van de digitale snelweg garanderen, landsoverschrijdende dienstverlening mogelijk maken, vertrouwde internetdiensten garanderen en de controleerbaarheid van datastromen en dataopslagen door burgers en bedrijven versterken. Betrouwbare eID-voorzieningen vormen daarvoor een noodzakelijke voorwaarde. Gelijkwaardige bruikbaarheid van publieke en private eID-middelen heeft een enorm potentieel economisch rendement van gemaakte investeringen en opent innovatiemogelijkheden zowel nationaal als internationaal.

Internationaal

De *Routekaart voor stabiliteit en groei*[3] van de Europese Commissie benadrukt dat het toekomstige gemeenschappelijke wetgevingskader voor wederzijdse erkenning en aanvaarding van grensoverschrijdende elektronische identificatie en

[2] Onderzoek Ernst & Young, Groeien door veiligheid – Onderzoek naar de waarde van een veilige en betrouwbare IST infrastructuur voor de Nederlandse economie.

[3] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0669:FIN:EN:PDF

authenticatie een cruciale rol speelt in de ontwikkeling van de digitale economie. De Europese Commissie heeft in het voorjaar van 2012 een conceptverordening gepubliceerd die als doel heeft het vertrouwen in elektronisch verkeer tussen burgers, bedrijven en overheden binnen Europa te vergroten door dit onbelemmerd en veilig te laten plaatsvinden. Burgers en bedrijven moeten zonder enige blokkade kunnen deelnemen aan het vrije (digitale) handelsverkeer binnen de Europese grenzen. Concreet komt het erop neer dat alle Nederlandse overheidsdienstverleners door de Europese Unie goedgekeurde eID's van een hoog veiligheidsniveau moeten kunnen accepteren. Een groot deel van de EU lidstaten beschikt nu[4] of in de nabije toekomst over een hoogwaardige eID voor burgers. In Nederland is momenteel een hoogwaardige eID beschikbaar voor bedrijven (binnen het stelsel eHerkenning en PKIoverheid), dit is nog niet het geval voor burgers. Nederland loopt op dat gebied dus flink achter.
In de conceptverordening worden er verder vergaande eisen gesteld aan authenticatiemiddelen en andere vertrouwensdiensten zoals een digitale handtekening die Europees geaccepteerd kunnen worden. Om aan deze verordening te kunnen voldoen is gemeenschappelijk vastgesteld beleid en vergaande samenwerking op het vlak van authenticatie en autorisatie noodzakelijk. De inschatting is dat de druk vanuit Europa op lidstaten om een eID met het hoogste niveau van betrouwbaarheid aan haar burgers uit te reiken, verder zal toenemen (zoals is aangegeven in de Digitale Agenda van eurocommissaris Neelie Kroes5). Als Nederland niet kan voldoen aan de eisen die gesteld worden aan grensoverschrijdend gebruik van eID's, dan betekent dit dat Nederlandse burgers en bedrijven op termijn uitgesloten worden van de interne digitale markt. Dat beperkt de potentiële groei van de Nederlandse digitale economie.

1.2 Opdracht

De hierboven geschetste ontwikkelingen vergen een vergaande samenwerking en verdere beleidsontwikkeling op het gebied van elektronische identiteiten in Nederland. Daarom is, namens de Berlijngroep6, de volgende opdracht bepaald.

Voer een verkenning uit naar de mogelijkheden voor een overheidsbreed eID stelsel, o.a. gericht op een bredere beschikbaarheid van elektronische identificatiemiddelen op hoog niveau.

[4] Oostenrijk, België, Estland, Frankrijk, Duitsland, Luxemburg, Portugal, Slovenië, Spanje, Zweden. In verschillende landen wordt daarbij samengewerkt met de private sector, c.q. het bankwezen (o.a. Denemarken, Finland en Estland).

[5] COM (2010) 295, Brussel 26-8-2010

[6] In de Berlijngroep zijn de volgende organisaties vertegenwoordigd: EL&I, BZK, Agentschap BPR, CIO Rijk, Doorbraakgemeenten, DUO, ICTU, Kadaster, NVVB, V&J, RDW, VWS, VNG, UWV.

In de verkenning worden de thema's internationaal, privacy, gebruiksgemak, toekomstvastheid, veiligheid, risicospreiding, wetgeving en publiekprivate samenwerking verwerkt. Daarin zullen verschillende scenario's worden onderscheiden.

Het gaat dan om de benodigde voorzieningen (middelen, registers en diensten) ten behoeve van authenticatie-, autorisatie- en elektronische handtekening processen van burgers en bedrijven met de overheid, tussen overheden onderling, tussen bedrijven onderling en tussen bedrijven en consumenten (burgers) en burgers onderling. Daarbij worden de mogelijkheden voor een strategie verkend, waarbij burgers en bedrijven de beschikking krijgen over meerdere middelen die ze breed kunnen inzetten (keuzevrijheid).

Deliverables

De volgende resultaten worden naar aanleiding van de verkenning opgeleverd:
Strategische verkenning (dit document)
Voorstel voor vervolg (periode oktober 2012 en verder) (hoofdstuk 5 van dit document)
Overzicht van benodigde stelselafspraken en –specificaties (volgt later)

1.3 Uitwerking

De verkenning is uitgevoerd door de beleidsverantwoordelijke ministeries (BZK, EL&I) samen met drie grote uitvoeringsorganisaties, de Belastingdienst, de RDW (Rijksdienst Wegverkeer) en het UWV (Uitvoeringsinstituut Werknemers Verzekeringen).[7] Daarnaast zijn diverse andere overheidsuitvoeringsorganisaties geconsulteerd. Indien in principe op basis van deze beleidsnota de beleidswens wordt vastgesteld om een Nederlands eID-stelsel in te richten, worden ook de stakeholders uit bedrijfsleven en consumentenorganisaties geconsulteerd en betrokken om in samenwerking uitgangspunten vast te stellen en tot inrichting te komen, met behoud van ieders eigen verantwoordelijkheid, alsook de politieke verantwoordelijkheid van de betrokken ministers. Voor het inventariseren van de behoeften en wensen op het terrein van authenticatie en autorisatie is in deze verkenning eerst de behoefte binnen de overheid geïnventariseerd.

In dit document zijn drie niveaus onderscheiden, die in paragraaf 4.2.1. worden uitgewerkt:

1. Het hoogste niveau betreft het strategisch beleid van de overheid op het gebied van authenticatie en autorisatie.
2. Het tweede niveau betreft stelselafspraken en -specificaties, gebaseerd op het strategisch beleid.
3. Het derde niveau betreft de specifieke eID-voorzieningen: diensten voor authenticatie (tokens, certificaten etc.) en autorisatie (machtigingsregisters), gebaseerd
   op de stelselspecificaties en –afspraken.

[7] Het ministerie van VWS is agendalid van de zomerwerkgroep.

1.4 Leeswijzer

In dit document worden in hoofdstuk 2 eerst toekomstbeelden geschetst voor 2014, 2016 en 2020 als een "wenkend perspectief". In hoofdstuk 3 gaat in op de belangrijkste stakeholders die betrokken zijn bij een eID stelsel en wordt inzicht gegeven in de wensen van een grote groep overheidsdienstverleners. De input uit deze hoofdstukken worden in hoofdstuk 4 vertaald in een voorstel voor de inrichting van het eID stelsel.
In hoofdstuk 5 wordt ten slotte nog een voorstel gedaan voor de vervolgstappen na deze nota.

1.5 Begrippen

Dit document behandelt een onderwerp waarbinnen er veel verwarring bestaat over de gehanteerde begrippen. We geven daarom onze interpretatie van een aantal belangrijke begrippen die vaak terugkomen.

eID voorzieningen

Met de term eID voorzieningen bedoelen we in dit stuk zowel de eID-middelen (zoals wachtwoorden, pinpassen) als de voorzieningen die nodig zijn voor de afhandeling van het digitale authenticatie proces. Daarnaast vallen hier ook eID-diensten als (de afhandeling) van autorisatie/machtiging, en de elektronische handtekening onder. Deze voorzieningen kunnen door publieke of private partijen worden aangeboden. Zie verder paragraaf 3.2

Autorisatie/machtigingsdiensten

De eID-voorzieningen met betrekking tot autorisatie/machtiging maken het mogelijk dat dienstverleners kunnen verifiëren wat een bepaalde persoon mag namens een organisatie (of namens een ander persoon). Een speciale variant daarvan zijn eID-voorzieningen omtrent leeftijdverificatie (wanneer elektronische dienstverleners verplicht zijn de leeftijd van hun klant vast te stellen).

eID stelselafspraken en specificaties

Met stelselafspraken en specificaties wordt in dit stuk bedoelt de afspraken die gemaakt moeten worden om authenticatie en autorisatie binnen een stelsel met meerdere middelenleveranciers en dienstverleners, zoals eID en eHerkenning, goed te laten functioneren. Het gaat dan om uniforme technische standaarden en interoperabiliteit, koppelvlakken, beveiligingsniveaus, juridische voorwaarden en dergelijke.

Voor een verdere toelichting over identificatie, authenticatie en autorisatie wordt verwezen naar bijlage 1.

2. De toekomstige betrouwbare toegang tot de dienstverlening

Het wenkend perspectief van het eID stelsel NL voor burgers en bedrijven is dat het gebruik van betrouwbare authenticatiemiddelen en elektronische diensten:

- veilig en gemakkelijk is (tijd en plaatsonafhankelijk);
- over de grenzen gaat van het onderscheid tussen burgers/bedrijven;
- binnen de Europese Unie uitwisselbaar is;
- met betrouwbare en up to date technologie gebeurt;
- kosten bespaart;
- en borging van de privacy geeft.

Het wenkend perspectief voor markt- en overheidspartijen is:

- kostenbesparingen door het her- en gemeenschappelijk gebruik van bestaande markt- en overheidsmiddelen en diensten (die al beschikbaar zijn, en zo mogelijk breed uitgerold).
- bundelen van expertise, delen van kennis, vaststellen van gemeenschappelijke strategieën en specificaties/ standaarden resulteert in efficiency en kostenbesparing.

Het eID stelsel NL biedt de randvoorwaarden voor flexibele en betrouwbare oplossingen voor identificatie, authenticatie en autorisatie bij elektronische dienstverlening, zowel voor communicatie tussen overheid en bedrijven en burgers, als tussen burgers en bedrijven onderling. De volgende scenario's schetsen een beeld van de gebruiker van de toekomst.

	Burgers	Bedrijven
2014/15	**“Nieuw: Gebruik bankpas voor belasting-aangifte”** Kees van Dijk doet aangifte inkomstenbelasting. Daarvoor logt hij in op Mijnbelastingdienst.nl. De Belastingdienst ondersteunt nu verschillende publieke en private eID’s. Kees kiest voor zijn bankpas. Hij heeft die vorige week geactiveerd voor gebruik bij de overheid, omdat hij dat een veilig idee vindt: Een eID middel dat goed genoeg is voor geldzaken, vindt hij ook betrouwbaar voor zaken met de overheid. **“Mantelzorg makkelijker en veiliger”** Kees verzorgt ook de belastingaangifte van zijn moeder. Dat gaat gemakkelijk met de machtiging die zij vanuit huis online voor hem heeft geregistreerd in het publieke machtigingsregister van DigiD Machtigen. Met die machtiging en zijn eigen bankpas kan hij de vooringevulde gegevens van zijn moeder ophalen en de belastingaangifte insturen.	**“Multi inzetbaarheid van eID middel bij bedrijven”** Chantal van Breemen werkt bij VanderVen Retail BV, een middelgroot bedrijf in Eburg. VanderVen doet zoveel mogelijk digitaal en maakt daarbij gebruik van een eID-middel in combinatie met een privaat machtigingsregister in beheer van SecurID BV. Chantal logt met het token dat door SecurID BV aan VanderVen is verstrekt in op het digitaal bedrijvenloket van de gemeente Eburg om de contactgegevens van het bedrijf bij te werken. Daarna logt zij met het token in om bij de groothandel spullen te bestellen. VanderVen heeft via de autorisatiedienst van SecurID BV precies vastgelegd voor welke handelingen en tot welke bedragen Chantal bevoegd is. **“Machtiging voor aanvragen zorgtoeslag veilig geregeld”** Daarnaast is Chantal onlangs een eigen onderneming gestart, een eenmanszaak. Ze gaat de administratie van met name ouderen verzorgen. Ze heeft zelf ook gekozen voor de online diensten van SecurID BV om zaken te kunnen doen met de overheid. Omdat ze een eID-middel met het hoogste betrouwbaarheidsniveau heeft aangeschaft, kon ze zich hiermee online inschrijven bij de Kamer van Koophandel. Voor enkele bedlegerige klanten, die haar gemachtigd hebben via het publieke machtigingsregister van DigiD Machtigen, kan ze daarmee bijvoorbeeld zorgtoeslag voor hen aanvragen.

	Burgers	Bedrijven
2016	**“Met overheidsmiddel op marktplaats”** Kees van Dijk wil bezwaar maken tegen de WOZ-beschikking die hij van de gemeente Eburg ontving. Om zijn bezwaar in te dienen logt hij met zijn eRijbewijs in bij www.gemeente-eburg.nl. Kees heeft zijn eRijbewijs gisteren ook gebruikt om een advertentie voor zijn auto op Marktplaats te zetten. Hij vraagt er een flink bedrag voor, dus is het wel fijn als mensen erop kunnen vertrouwen dat hij ook daadwerkelijk de persoon is die hij claimt te zijn. Als hij zijn auto verkoopt kan hij deze ook online overschrijven.	**“Kwaliteitsverbetering administratie-kantoren”** De administratie van VanderVen wordt gedaan door Boekbeheer BV. VanderVen heeft Boekbeheer BV hiervoor gemachtigd. Daardoor mag Boekhoud BV alle informatie over VanderVen direct bij de Belastingdienst inzien en muteren. Zo kan Boekhoud BV snellere en betere dienstverlening bieden. **“Nieuw: Online je bedrijf starten en inschrijven bij de Kamer van Koophandel ”** Chantals echtgenoot Ruud wil graag een eigen bedrijf beginnen. Met zijn persoonlijke eID middel gaat hij zich online inschrijven bij de Kamer van Koophandel. Daarvoor hoeft hij nu niet meer naar een KvK-kantoor, dat kan hij veilig vanuit huis doen. Daarna kan hij met datzelfde middel ook alle zaken van zijn bedrijf met de overheid en andere bedrijven elektronisch afhandelen.
2020	**“Met je telefoon geld terugvragen van de Spaanse belastingdienst”** Jurjen van Dijk, de zoon van Kees, gaat studeren en vraagt daarvoor met zijn smartphone studiefinanciering aan Omdat Jurjen net een nieuwe smartphone heeft, kiest hij voor dat middel (geen extra gedoe of kosten). In zijn smartphone is een eID chip opgenomen in de SIMkaart, waardoor de telefoon persoonsgebonden is. Afgelopen zomer heeft Jurjen aan de Spaanse kust gewerkt. Daar is belasting op ingehouden. Hij kan dat nu mooi via zijn smartphone om belastingteruggave bij de Spaanse belastingdienst vragen. Eerder deze week vroeg hij met de smartphone ook digitaal een nieuw rijbewijs aan. Hij hoeft nu alleen nog voor het afhalen even naar de gemeentebalie.	**“Verdere groei Europese online zaken-doen gerealiseerd”** VanderVen Retail verkoopt ook op maat gemaakte meubelen. Sinds kort zijn zij begonnen met digitale verkoop, omdat ze nu met zekerheid kan vaststellen van klanten binnen de Europese Unie wie de bestelling plaatst en dat deze persoon akkoord is met de voorwaarden en de prijs. Bij de uitvoering van de werkzaamheden laat VanderVen veel activiteiten uitvoeren door andere bedrijven. Die zijn gemachtigd om namens VanderVen te handelen. Hierdoor heeft VanderVen zijn werkprocessen kunnen vereenvoudigen en, doorlooptijden verkort. De organisatie is hiermee flexibeler gemaakt en de winstmarge is daardoor verhoogd.

3. Wensen stakeholders

3.1 Inleiding

Dit hoofdstuk gaat in op de belanghebbenden bij eID-voorzieningen (paragraaf 3.1) en de klantvraag van een groep stakeholders: de overheidsdienstverleners (paragraaf 3.2).

3.2 Stakeholders

De belangrijkste belanghebbenden van een eID stelsel zijn de eindgebruikers, elektronische dienstverleners (zowel publiek als privaat), eID-voorzieningenaanbieders (publiek en privaat), politiek verantwoordelijken en toezichthouders.

Eindgebruikers

Burgers en bedrijven hebben als eindgebruikers van eID's een groot belang, immers hun (geclaimde) identiteit kan hiermee online worden vastgesteld vervolgens kunnen zij publieke en private diensten afnemen. Het is belangrijk dat burgers en bedrijven vertrouwen hebben in de middelen die het eID stelsel biedt. Daarnaast dienen de middelen betaalbaar te zijn, en gemakkelijk in gebruik.
Wat bedrijven betreft zullen de beschikbare middelen zoveel mogelijk aansluiten op de juridische vorm waarin bedrijven ondernemen (als natuurlijk- of als rechtspersoon).

Elektronische dienstverleners

Elektronische dienstverleners maken gebruik van het eID stelsel voor hun digitale dienstverleningsprocessen. Zij identificeren hun gebruikers elektronisch, zodat zij met een hoge mate van zekerheid weten met wie ze te maken hebben. Geld, producten en persoonsgegevens vallen zo niet in verkeerde handen. Er zijn zowel publieke (uitvoeringsorganisaties, gemeenten etc) als private elektronische dienstverleners (o.a. webwinkels). De inzetbaarheid van publieke en private eID middelen in de verschillende publieke en private domeinen brengt - per domein verschillende - vraagstukken met zich mee (o.a. persoonsnummergebruik, financiering, aansprakelijkheid).

De behoefte van elektronische overheidsdienstverleners aan een eID-stelsel komt mede voort uit de (politieke) wens tot optimaliseren van de digitale dienstverlening, efficiëntere bedrijfsvoering en een compactere overheid en het gelijktijdig terugdringen van risico's op identiteitsfraude en het waarborgen van de privacy. Meer specifiek geeft de Belastingdienst aan een sterker middel voor identificatie nodig te hebben. Daarnaast vraagt de Tweede Kamer te bewerkstelligen dat burgers met ingang van 2013 elektronische inzage in het eigen medisch dossier krijgen. Tevens heeft de Tweede Kamer al in 2004 verzocht om over te gaan tot introductie van één uniforme identiteitskaart voor alle overheidsdiensten waarvoor authenticatie vereist is[8] en in 2012 de regering verzocht om een digitaal paspoort te ontwikkelen

[8] Motie Szabo kamerstukken II 2003 - 2004,29 362,nr. 9

opdat het contact op internet tussen burger en overheid optimaal beveiligd is.[9] Verder zijn bepaalde organisaties wettelijk verplicht de identiteit of leeftijd van hun klanten vast te stellen. Voor al deze en meer zaken zijn hoogwaardige oplossingen nodig.

De behoefte van private dienstverleners aan een eID stelsel komt eveneens voort uit de wens op een hoger betrouwbaarheidsniveau elektronisch zaken te kunnen doen met burgers/consumenten, zodat fraude en het lekken van persoonsgegevens kan worden voorkomen. Ook voor elektronisch commercieel zaken doen op het internet is het vertrouwen van burgers/consumenten en bedrijven essentieel[10].

eID voorzieningenaanbieder

eID-voorzieningen zijn zowel de eID-middelen (zoals wachtwoorden, pinpassen) als de voorzieningen die nodig zijn voor de afhandeling van het digitale authenticatie proces en autorisatie/machtiging. Een eID voorzieningenaanbieder is de organisatie die deze voorzieningen levert. Dan kunnen zowel publieke organisaties zijn (DigiD bij BZK), als private organisaties (eHerkenningsleverancier).
De afgelopen jaren heeft ELenI samen met het bedrijfsleven geïnvesteerd in ontwikkeling van het afsprakenstelsel eHerkenning, dat voorziet in private authenticatie- en autorisatiediensten voor bedrijven. Daarnaast is het stelsel PKIoverheid ontwikkeld, gericht op beschikbaarheid van hoogwaardige certificaten voor machine-machineverkeer met en tussen overheidsorganisaties.[11] Ook de overheid zelf biedt voorzieningen aan voor elektronische authenticatie en autorisatie. Om private en publieke diensten naast elkaar te kunnen laten voortbestaan in een eID-stelsel moet rekening worden gehouden met mededingingsrechtelijke aspecten (level playing field) en investeringen die het bedrijfsleven al heeft gedaan in het kader van eHerkenning en PKIoverheid.

Politieke verantwoordelijkheid en toezichthouder

Tot slot dient in de publieke sector ook de politieke verantwoordelijkheid te worden belegd. Dat geldt voor het eID-stelsel, en voor de middelen in dat stelsel. Er is overigens niet één politiek verantwoordelijke minister voor alle onderdelen van het stelsel, omdat verschillende departementen verantwoordelijk zijn voor onderdelen van het nationale eID-stelsel. Zo blijft het ministerie van Infrastructuur en Milieu bijvoorbeeld verantwoordelijk voor het Rijbewijs, BZK voor de nationale identiteitskaart en is EL&I politiek verantwoordelijk voor het elektronisch zakendoen en

[9] Motie Recourt Gesthuizen 26 643 nr. 236

[10] Zie bijlage 3 voor een aantal voorbeelden hiervan.

[11] Momenteel wordt naar aanleiding van DigiNotar het Programma van Eisen van PKI Overheid aangepast. Hierover vindt afstemming plaats met onder andere de Manifestgroep en medeoverheden.

het migreren van het afsprakenstelsel eHerkenning naar het nationale eID Stelsel. Om ervoor te zorgen dat alle onderdelen logisch samenwerken en in samenhang kunnen worden gebruikt, dient echter een verantwoordelijkheid voor het eID stelsel te worden belegd bij de Rijksoverheid (zie verder paragraaf 4.2.5), aangevuld met een mogelijkheid om toezicht te houden op de naleving van de afspraken, zodat een werkend en betrouwbaar samenhangend stelsel kan worden gewaarborgd.

3.3 Wensen van overheidsdienstverleners

De zomerwerkgroep heeft de klantvraag van een aantal betrokken overheidsdienstverleners in kaart gebracht: waar hebben zij op het gebied van authenticatie en autorisatie (dringend) behoefte aan? [12].

- Het eID stelsel is essentieel om de diversiteit in de bestaande en toekomstige e-dienstverlening en de daarbij behorende betrouwbaarheidsniveaus te faciliteren en te stroomlijnen.

Voorlopige conclusies

Meerwaarde stelsel

- Overheidsdienstverleners zien de meerwaarde van een gecoördineerd nationaal eID-stelsel. Deze meerwaarde zit in gezamenlijke afspraken en duidelijkheid over zaken als: te gebruiken koppelvlakken, standaarden, identiteitsverklaringen en fallback scenario's.
- Daarnaast heeft het ontwikkelen van gemeenschappelijke voorzieningen, zoals een omnummerfaciliteit voor het BSN eveneens voordelen. Het ontzorgen van overheidsdienstverleners is daarbij een belangrijk uitgangspunt. Velen zijn er voorstander van om complexiteit in gemeenschappelijke voorzieningen op te pakken en de uitwerking/koppeling die de dienstverleners zelf dienen uit te voeren, daarmee te versimpelen.
- Het eID stelsel wordt gezien als een randvoorwaarde voor het realiseren van de compacte overheid.
- De meerwaarde bevindt zich dus op verschillende niveaus: zowel op het niveau van beleid/bestuur als gemeenschappelijke uitvoeringskaders als gemeenschappelijke infrastructuur (op onderdelen).

Behoefte aan hoog niveau eID middelen

- De organisaties die digitaal diensten aanbieden zien een dringende noodzaak om binnen niet al te lange termijn over te gaan op een hoger beveiligingsniveau.
- Zij vinden het hierbij relevant dat het hierbij gaat – vanuit het klantperspectief gezien – om betaalbare oplossingen.
- Vooral bij organisaties die werken met persoonsgegevens is de behoefte dringend: hoe hoger de gevoeligheid/risicoklasse, hoe hoger de behoefte.

[12] Het betreft: Agentschap BPR, CIO Rijk, Doorbraakgemeenten, DUO, ICTU, Kadaster, NVVB, V&J, RDW, VWS, KvK, VNG, UWV.

- Voor organisaties die louter openbare registers beheren is de noodzaak voor een sterker elektronisch identificatiemiddel minder dringend. Daar speelt geen privacyvraagstuk, maar is het wel belangrijk dat voor de diensten wordt betaald (en daarvoor is koppeling met een natuurlijk persoon soms weer wel van belang).
- Overheidsdienstverleners geven aan dat zij met een authenticatiemiddel voor burgers en bedrijven op hoog niveau een aantal voordelen kunnen behalen, die zij op dit moment nog niet kunnen realiseren:
  1. Optimalisering van bestaande e-dienstverlening
  2. Verdere digitalisering van dienstverleningsprocessen
  3. Een hogere effectiviteit en efficiency, resulterende in kostenbesparingen
  4. Hogere veiligheid/betrouwbaarheid dienstverlening
- Het merendeel van de overheidsdienstverleners geeft aan zelf te willen bepalen wat het betrouwbaarheidsniveau van zijn processen is. Een enkele overheidsdienstverlener geeft aan uit te willen gaan van één betrouwbaarheidsniveau voor alle processen bij alle dienstverleners.
- Sommige overheidsdienstverleners willen uit betrouwbaarheidsoverwegingen (anti-fraude, bescherming persoonsgegevens, financiële risico's) hun klantgroep verplichten om een middel op een hoog niveau te gebruiken.
- Andere overheidsdienstverleners geven aan dat de behoefte van de eindgebruiker wat hen betreft voorop staat en dat zij meer zien in een natuurlijke ontwikkeling dan in het afdwingen van het gebruik van bepaalde middelen door hun eindgebruikers.
- Zij geven daarbij wel aan dat van verplicht gebruik bij de Belastingdienst een precedentwerking uit kan gaan voor andere uitvoerders: hun eindgebruikers hebben dan immers voor online verkeer met de Belastingdienst al een hoogwaardig middel, dat ook gebruikt kan worden voor het afnemen van diensten bij andere uitvoeringsorganisaties.

Concrete verbeteringen e-dienstverlening met eID hoog

Er is een steeds groter wordende behoefte aan eID middelen op hoog niveau in verschillende sectoren. Er is nog veel winst in termen van financiele en administratieve lastenverlichting te behalen door verdere digitalisering van de processen en veilige uitwisseling van informatie.
Een aantal concrete voorbeelden zijn:

Belastingdienst:
De Belastingdienst is van plan om de digitale dienstverlening aan ondernemers verder uit te breiden. In het portaal voor ondernemers zal veel meer informatie beschikbaar worden gesteld en het aantal digitale diensten zal ook gaan toenemen. Het beveiligingsniveau dat de huidige eigen voorziening van de Belastingdienst biedt wordt voor deze ontwikkelingen niet toereikend geacht. Om de verdere ontwikkeling van de digitale dienstverlening aan ondernemingen en ook aan burgers mogelijk te maken moet het beveiligingsniveau omhoog. Dat kan alleen als daarvoor de juiste eID middelen beschikbaar zijn.

Ministerie Volksgezondheid, Welzijn en Sport (VWS)
Zowel voor zorgprofessionals als zorgconsumenten is er behoefte aan een eID middel op hoog niveau. Op dit moment is wetgeving in voorbereiding waarin wordt bepaald dat patiënten recht hebben op elektronische inzage in de medische gegevens die over hem/haar zijn vastgelegd. Digitale toegang tot dit soort gegevens dient zorgvuldig en alleen met een goed beveiligd eID middel plaats te vinden. Voor zorgprofessionals wordt door VWS vooralsnog kosteloos een authenticatiemiddel beschikbaar gesteld. De kosten worden gedragen door VWS, maar dit is kostbaar. Indien een ander eID middel op hoog niveau beschikbaar komt, dan zal VWS bezien of het mogelijk is dit middel te gaan gebruiken.

Uitvoeringsinstituut Werknemers Verzekeringen (UWV):
De dienstverlening van UWV wordt gemoderniseerd. Sinds 1 juli van dit jaar is de wijziging op de Wet structuur uitvoeringsorganisatie werk en inkomen (SUWI) van kracht, waarbij geldt dat de communicatie tussen UWV en klanten van UWV in principe verplicht elektronisch verloopt, waar het gaat om inschrijving voor arbeidsmarktdienstverlening en aanvragen van uitkeringen. Deze ontwikkeling is erop gericht een efficiënte werking van de arbeidsmarkt te bevorderen met de nadruk op de eigen verantwoordelijk van burgers en bedrijven. Tevens leidt dit tot kosten-

besparing in de uitvoering. Gelet op de toekomstige toename van het digitaal verkeer tussen UWV en haar klanten, hebben de klanten van de UWV een steeds groter belang bij veilige, beschikbare en betrouwbare (eID) authenticatiemiddelen waardoor betere en efficiëntere dienstverlening mogelijk wordt (administratieve lastenverlichting). Hoog niveau authenticatie maakt het ook mogelijk verantwoord en efficiënt gegevens uit te wisselen met andere partijen die een rol spelen op het domein van werk en re-integratie: uitzendbureaus en andere dienstverleners op het gebied van re-integratie, arbeidsomstandigheden of zorg. Vooral waar het gaat om arbeidsongeschiktheid en daaraan gerelateerde medische informatie is hoog niveau authenticatie een harde voorwaarde.

Kamer van Koophandel:
De gegevens die de KvK gebruikt zijn persoonsgegevens en potentieel fraudegevoelig. Daarom is het op dit moment zo dat bij inschrijving in het Handelsregister een face-to-face identiteitscontrole aan de KvK balie wordt gedaan door hiervoor opgeleid personeel. Een eID middel op hoog niveau kan de online identificatie van personen mogelijk maken. Het inschrijfproces voor het Handelsregister wordt daarmee voor de ondernemen plaats- en tijdonafhankelijk. De KvK kan zo haar e-dienstverlening verder optimaliseren. Dit levert efficiencywinsten en besparingen op.

Dienst Uitvoering Onderwijs (DUO):
Behalve een toegevoegde waarde van een eID middel op hoog niveau voor klanten van DUO is er ook winst mogelijk voor DUO zelf. Als op termijn meer digitaal en via online self service mogelijk is, worden andere (kostbaardere) kanalen, zoals telefoon en balie, minder belast. DUO heeft een doelstelling om 80% van de dienstverlening digitaal af te willen handelen. Doorontwikkeling van e-dienstverlening door middel van een eID middel op hoog niveau kan hieraan bijdragen. Naast de groep klanten bestaande uit scholieren en studenten nemen ook onderwijsinstellingen diensten af van DUO. Denk daarbij aan digitale bestandsuitwisseling.
DUO heeft een jonge populatie klanten, die gewend zijn met nieuwe technologie om te gaan. Op termijn ziet DUO daarom de behoefte aan mobiele eID toepassingen groeien.

Tijdpad en fasering

- De ene overheidsdienstverlener heeft meer behoefte aan een snelle uitrol van een authenticatiemiddel op hoog niveau dan de andere. De behoefte aan snelle uitrol bevindt zich vooral in het burgerdomein. In het bedrijvendomein is een hoog niveau al beschikbaar, maar is de behoefte minder groot. Financiële laagdrempeligheid voor eindgebruikers is voor beide domeinen een belangrijke wens.
- Organisaties horen graag op tijd wat zij wanneer en waarvoor moeten regelen. Zij pleiten voor fasering in de uitrol en voor het kunnen voeren van regie over wat zij zelf binnen hun eigen organisatie moeten regelen. De ene organisatie is verder dan de andere. Een grote uitrol van het gehele wenkend perspectief in één keer lijkt niet haalbaar. Zij pleiten ervoor dit geen stelselverantwoordelijkheid te maken, zodat zij een tempo kunnen bepalen dat zoveel mogelijk aansluit op hun investeringscyclus.

4. Voorgestelde oplossingsrichting

4.1 Inleiding

In dit hoofdstuk wordt een oplossingsrichting beschreven, waarmee kan worden voldaan aan de behoefte zoals deze in hoofdstuk drie is verwoord.
Voor het realiseren van de beoogde doelstellingen, adviseert de werkgroep eID stelsel het volgende twee sporen beleid:

1. Het ontwikkelen van het eID Stelsel NL
2. Zorg dragen voor het breed beschikbaar krijgen van een hoog niveau eID-middel voor burgers/consumenten.

In de volgende paragrafen worden onderbouwde adviezen per spoor voorgelegd.

4.2 eID stelsel Nederland

Ten aanzien van de ontwikkeling van het eID stelsel adviseert de werkgroep dat:

1. Er één eID-afsprakenstelsel komt, voor het burger én bedrijvendomein, waardoor
   a. dezelfde standaarden gelden voor het burger- en bedrijvendomein;
   b. er een ontkoppeling plaatsvindt tussen diensteninfrastructuur en eID-middelen infrastructuur (ontzorgen dienstverleners);
   c. en waarbinnen een ontkoppeling van technologie plaatsvindt (toekomstvaste adaptiviteit i.p.v. technologieafhankelijkheid).
2. Zowel publieke als private online authenticatiemiddelen in het eID-stelsel zullen worden ondergebracht.
3. De middelen onder het stelsel zowel bruikbaar zullen zijn voor publieke als voor private (elektronische) dienstverleners.
4. In de toekomst de hierin ondergebrachte middelen ook in het buitenland gebruikt kunnen worden.
5. De Rijksoverheid systeemverantwoordelijk is voor het afsprakenstelsel. En daarmee dat de overheid:
   a. Gecoördineerd beleid ontwikkelt m.b.t. digitale identiteiten en machtigingen
   b. Het afsprakenstelsel actief onderhoudt en beheert
   c. Toezicht uitoefent op (delen van) het afsprakenstelsel en de deelnemers
6. De standaarden en specificaties van het eID stelsel voor overheidsdienstverleners op termijn op de “pas-toe-of-leg-uit”-lijst van het College Standaardisatie komen.

Hieronder worden alle adviezen inhoudelijk toegelicht.

4.2.1 *Ontwikkeling één eID stelsel NL*

In de uitwerking van het eID-stelsel zijn drie niveaus te onderscheiden:

1. Het hoogste niveau betreft het strategisch beleid van de overheid op het gebied van authenticatie en autorisatie. Het consolideren van het strategisch beleid is primair de taak van de beleidsdepartementen. Dit eID-beleid is een gezamenlijke verantwoordelijkheid van

de ministeries van Binnenlandse Zaken en van Economische Zaken, Landbouw en Innovatie. Van belang is dat er één gedragen strategisch beleidsdocument tot stand komt, in samenwerking met alle betrokken partijen, en met gebruikmaking van hun expertise. Daarmee zijn de kaders voor alle betrokkenen in het vervolgproces duidelijk.

In het strategisch beleid worden in elk geval belangrijke uitgangspunten voor de verdeling van rollen en verantwoordelijkheden tussen publieke en private partijen expliciet gemaakt. Dat geeft de overheid bijvoorbeeld de ruimte om in een van de zuilen eID-basisvoorzieningen te ontwikkelen wanneer de borging van publieke belangen dat vergt. Daarbij kunnen specifieke financierings- en governancearrangementen van toepassing zijn, maar altijd zal in principe dienen te worden aangesloten op de (technische) standaarden uit het stelsel die interoperabiliteit met andere diensten verzekeren.
Op deze basis zal bijvoorbeeld ook een hoogwaardig eID-middel voor burgers worden ontwikkeld. In paragraaf 4.3.5 wordt dit nader uitgewerkt.

De publieke verantwoordelijkheid voor adequate voorzieningen voor authenticatie en autorisatie betekent ook dat in het stelsel voorzien wordt in publiek toezicht. Daarbij wordt rekening gehouden met de aard van de organisaties en bestaande toezichtmechanismen die daarvoor gelden of beschikbaar zijn. Zo zullen voor gemeenten, die in het stelsel een rol zouden krijgen als uitgevers van een publiek hoogwaardig eID (eNIK, eRijbewijs) generieke wettelijke toezichtmechanismen worden toegepast.
Bij private partijen zal dit toezicht kunnen worden vormgegeven door bestaande toezichthouders (Opta op basis van de Telecommunicatiewet, Logius als PA in het kader van PKIoverheid en als beheerorganisatie van eHerkenning), mogelijk ondersteund door private certificerings- en auditsystemen. Het stelsel dient deze verschillende modaliteiten te ondersteunen.

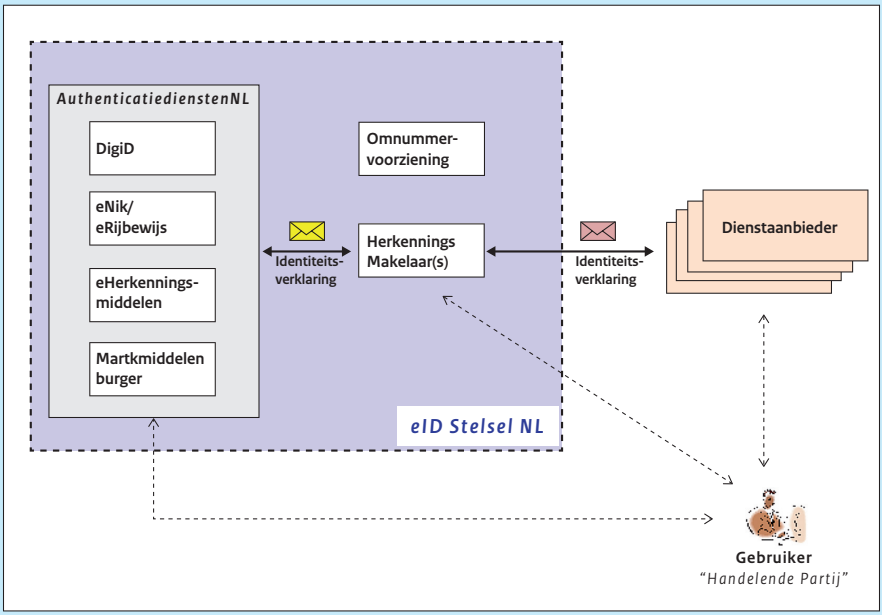
Andere belangrijke uitgangspunten van het stelsel zijn:

a. *Dezelfde standaarden bedrijven en burgerdomein*
   Door te komen tot één afsprakenstelsel (eID stelsel NL) voor zowel burgers en bedrijven, worden dienstverleners niet meer geconfronteerd met een overlappende aanpak vanuit de verschillende eID-voorzieningen voor burgers en bedrijven, en treden er in de ontwikkeling van beleid en standaarden synergie op, doordat dit voor alle voorzieningen gezamenlijk wordt opgepakt. De afzonderlijke voorzieningen zoals DigiD, eHerkening en PKIoverheid hoeven dus niet meer los van elkaar aangesloten te worden. Verder ontstaat er een uniforme en

herkenbare werkwijze voor burgers en bedrijven.

b. *Ontkoppeling dienstverlener en middelen*
Er vindt in het stelsel zoveel mogelijk ontkoppeling plaats tussen dienstverleners en eID-middelen, waardoor deze dienstverleners 'ontzorgd' worden. Dienstverleners sluiten op een gestandaardiseerde manier aan op het stelsel via een standaardaansluiting. Dit is vergelijkbaar met een webwinkel die aansluit op iDeal voor het afhandelen van het betalingsverkeer.
Voor dienstverleners betekent dit dat zij geen eigen eID voorzieningen meer hoeven te ontwikkelen en beheren. Dit levert kostenbesparingen op.

c. *Toekomstvast: ontkoppeling van de technologie*
Binnen het stelsel wordt er gekozen voor een ontkoppeling van technologie. Een essentieel kenmerk van het eID Stelsel NL is dat het *technologie-onafhankelijk* en daarmee toekomstvast wordt ingericht. Hierdoor kunnen nieuwe technieken en veiligheidseisen makkelijk in het systeem worden opgenomen en oude technieken worden uitgefaseerd.
Daarmee hebben deze ontwikkelingen geen direct effect op de aansluiting van de dienstverleners. Dit is wederom vergelijkbaar met een webwinkel die onafhankelijk is van de gebruikte techniek van de bankmiddelen binnen iDeal. In figuur 1 is aangegeven hoe de ontkoppeling van de dienstverlening van eID voorzieningen eruit ziet.



Figuur 1: Ontkoppeling van dienstverlener en eID-voorzieningen

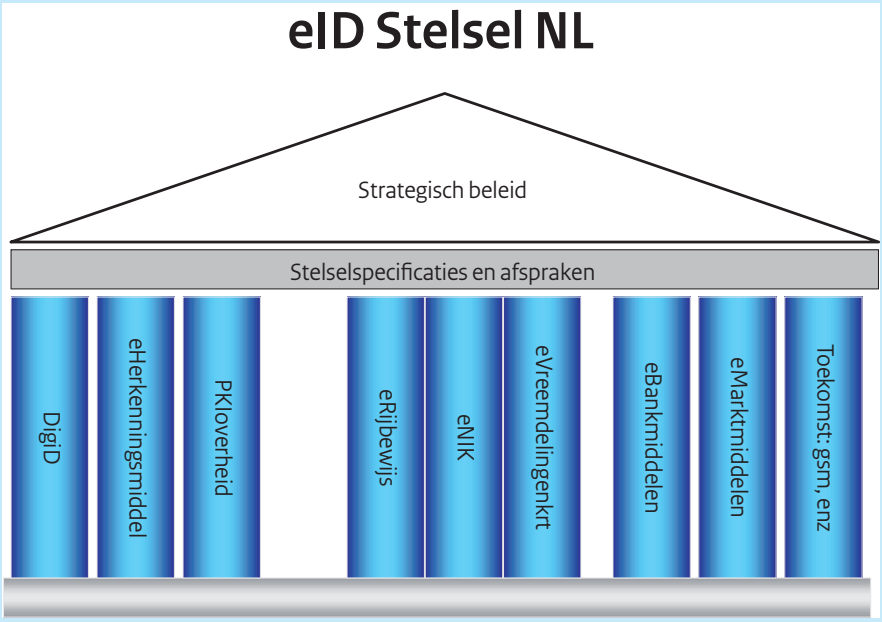
d. Conformiteit met wet- en regelgeving
Het stelsel moet in lijn zijn met geldende nationale en internationale wetgeving, zoals mededingingsregels, regels omtrent bescherming persoonsgegevens. Op dit laatste wordt in 4.3.6 nader ingegaan, in het licht van de EU-Verordening bescherming persoonsgegevens. Verder wordt in paragraaf 4.2.4 ingegaan op de Europese verordening ten aanzien van eID en vertrouwde diensten.

2. Het tweede niveau betreft stelselafspraken en -specificaties, gebaseerd op het strategisch beleid. De specificaties en afspraken worden opgesteld en beheerd door betrokken uitvoerende organisaties (zowel publiek als privaat) en gezamenlijk met alle stakeholders vastgesteld, in een daarvoor ingericht governance-structuur. Voor de opzet van de stelselafspraken en –specificaties kan o.a. gebruik gemaakt worden van het afsprakenstelsel eHerkenning en van de specificaties die er al zijn voor DigiD en het Programma van Eisen van PKIoverheid. Nieuwe middelen zoals de eNIK, eRijbewijs, bankpassen en eVreemdelingendocument zullen in lijn met de stelselafspraken en specificaties worden ontwikkeld.

Een eerste aanzet voor de stelselafspraken en -specificaties is opgenomen in bijlage 2.

3. Het derde niveau betreft de specifieke eID-voorzieningen: diensten voor authenticatie (tokens, certificaten etc.) en autorisatie (machtigingsregisters), gebaseerd op de stelselspecificaties en –afspraken. Voor de ontwikkeling en het beheer zijn de respectieve uitvoerende private en publieke partijen verantwoordelijk. Zij bepalen zelf hun uitrolstrategie en kunnen binnen strategisch beleid en kaders eigen keuzes maken met betrekking tot inrichting en techniek. De daadwerkelijke ontwikkeling van voorzieningen wordt in deze verkenning niet uitgewerkt, met uitzondering van een hoogwaardig eID-middel voor burgers (zie paragraaf 4.3).

Onderstaande figuur geeft de opbouw van het stelsel weer.



Figuur 2: Opbouw van het eID stelsel

Bestaande stelsels/voorzieningen

Bestaande stelsels (Stelsel eHerkenning) en eID voorzieningen, zoals DigiD, PKIoverheid en authenticatiemiddelen van eHerkenningspartijen worden zoveel mogelijk hergebruikt (geen desinvesteringen) en in een geleidelijk migratieproces in het Stelsel ingebracht

(interoperabiliteit door conformiteit afsprakenstelsel). Nieuwe eID voorzieningen (zoals eRijbewijs, eNIK, marktmiddelen/eBankmiddelen) sluiten op het eID Stelsel aan.

4.2.2 Publieke én private middelen worden ondergebracht in het stelsel

De overheid draagt zorg dat voor burgers en bedrijven eID-voorzieningen beschikbaar zijn. Dit houdt niet in dat zij die noodzakelijkerwijs zelf uitgeeft of beheert, zij kan er ook voor kiezen om dit binnen de kaders van het eID-stelsel over te laten aan de markt. Onder het stelsel vallen daarmee zowel publieke als private eID-voorzieningen. Reeds bestaande middelen worden ingebracht zoals DigiD, DigiD-machtigen, PKIoverheid en eHerkenning. In de toekomst kan het uitgebreid worden met nieuwe middelen zoals bankmiddelen, mobile devices, etc en kunnen 'verouderde' middelen uit gefaseerd worden.
In andere EU-lidstaten wordt het mix-model ook gehanteerd, zoals in Zweden en binnen het Finse eID stelsel. In het Finse en Zweedse stelsel is er eveneens bewust voor gekozen om bankmiddelen en overheidsmiddelen naast elkaar aan te bieden. Er is op dit moment niet te voorspellen of en zo ja welke middelen in het stelsel domineren[13]. Daarom wordt het eID Stelsel techniek onafhankelijk en wordt voor het totale aanbod van publieke en private eID-middelen periodiek geëvalueerd te worden of zij bestaansrecht hebben.

De voordelen van zo'n multi-middelen strategie zijn:

- Burgers en bedrijven hebben keuzevrijheid ten aanzien van de middelen zie zij willen gebruiken. Men kan kiezen voor één publiek of privaat middel, men kan er ook voor kiezen om meerdere middelen naast elkaar te gebruiken.
- Een multi-middelen strategie voorziet in *fallback* mogelijkheden. Als om de een of andere reden een middel niet te gebruiken is/onveilig is, kunnen burgers en bedrijven meteen gebruik maken van een ander middel voor diezelfde dienst.

Er zijn evenwel ook een aantal aandachtspunten. Een multi-middelen strategie brengt complexiteit met zich mee. Zowel op technisch vlak (o.a. verschillende eID middelen, die op eenzelfde manier moeten communiceren), als op het vlak van verantwoordelijkheid (gedeelde verantwoordelijkheid van markt en overheid). Daarnaast brengt de strategie - door standaardisatie - minder vrijheidsgraden voor organisatiespecifiek maatwerk met zich mee.

Publieke eID-voorzieningen voor burgers

Momenteel verstrekt de overheid digitale eID-middelen aan haar burgers via DigiD (basaal betrouwbaarheidsniveau). De overheid verstrekt op dit moment geen eID-middelen van het hoogste betrouw-

[13] Overleg met Finse collega's is opgestart, er zijn op dit moment echter nog geen gegevens beschikbaar. In september komen deze beschikbaar.

baarheidsniveau (uitgegeven na face-to-face controle aan de balie). Op termijn zullen de huidige DigiD-wachtwoord en DigiD-sms niveau's onvoldoende zijn. Er moeten dus eID-middelen op hoog niveau voor de burger beschikbaar worden gemaakt. Dat kan door de overheid zelf en/of door de markt. Een mix-scenario heeft de voorkeur. Zie verder paragraaf 4.3

Private eID-voorzieningen voor bedrijven, beroepsgroepen, etc.

Het daadwerkelijk uitgeven en beheren van middelen en voorzieningen voor bedrijven wordt overgelaten aan de markt, voor zover de markt voldoende in staat is dit op te pakken. Dit is conform het huidige beleid voor zowel de analoge als digitale wereld. Het wordt niet als overheidstaak gezien om bedrijven en hun medewerkers van identificatiemiddelen te voorzien.
De overheid draagt zorg voor het opnemen van eisen in het eID Stelsel ten aanzien van minimum beschikbaarheid en *fallback*opties. Deze eisen dragen bij aan de continuïteit en robuustheid van het stelsel in het geval een private aanbieder (tijdelijk) uit het stelsel wegvalt. In het geval dat het maatschappelijk belang in het geding komt, kunnen de verantwoordelijke ministers altijd ingrijpen in het stelsel. Deze fallbackoptie door de beschikbaarheid van meerdere aanbieders is een meerwaarde van de Nederlandse oplossing binnen Europa. De DigiNotar-crisis heeft aangetoond dat *fallback* van groot belang is, zeker als kritische ICT-processen betreft. Door dit soort afspraken uit te breiden naar het burgerdomein kan ook daar de continuïteit van dienstverlening beter gewaarborgd worden.

Degene die als natuurlijk persoon een onderneming drijft kan kiezen tussen een marktmiddel of zijn persoonlijke (burger-) overheidsmiddel. Hierdoor hoeven kleinere bedrijven (zzp-ers, bedrijven met de rechtsvorm eenmanszaak) geen tweede middel aan te schaffen.[14]
Voor de betrouwbaarheid van middelen is het wel noodzakelijk dat bij het uitgeven van middelen aan de hand van basisregisters het recht op de elektronische vertegenwoordiging wordt getoetst; toetsing aan het Handelsregister bij niet-natuurlijke personen en het GBA bij natuurlijke personen.

Waar overheidsdienstverleners nu eigen eID-middelen uitgeven aan bedrijven, die een wettelijke taak uitvoeren (bijvoorbeeld in het geval van de APK-garages) en ten behoeve van die taak authenticatie en autorisatiemiddelen nodig zijn, faseren zij deze middelen op termijn uit of brengen deze onder in het eID-stelsel.

[14] Eindadvies Adviescommissie Authenticatie en Autorisatie voor Bedrijven 2011. http://www.rijksoverheid.nl/documenten-en-publicaties/rapporten/2011/11/17/adviescommissie-authenticatie-en-autorisatie-bedrijven.html

Interoperabliteit

Het eID stelsel brengt interoperabiliteit op meerdere fronten:

- Zowel private als publieke eID-middelen kunnen worden gebruikt.
- eID middelen kunnen door zowel publieke als private elektronische dienstaanbieders worden gebruikt.
- Middelen voor burgers en bedrijven zijn (deels) uitwisselbaar .
- eID middelen zijn binnen de gehele EU bruikbaar.

4.2.3 Middelen zowel privaat als publiek te gebruiken

In het stelsel functioneren publieke en private eID-middelen op gelijke wijze naast elkaar. De burger en het bedrijf zijn vrij in de keuze van het middel dat zij inzetten ten behoeve van hun digitale identificatie. Belangrijk aandachtspunt hierbij is het waarborgen van het consumentenvertrouwen in de digitale economie (zie bijlage 3). In principe kan men met de onder het eID-stelsel vallende middelen, mits het middel van het gevraagde beveiligingsniveau is, alle digitale publieke dienstverlening ontsluiten. Publieke dienstverleners stellen geen andere of aanvullende eisen aan het gebruik.
Men kan met publieke middelen private dienstverlening ontsluiten en andersom: met private middelen kan publieke dienstverlening ontsloten worden. Dat betekent dat de eID-middelen in het eID stelsel zowel communicatie van burgers en bedrijven richting de overheid, als richting bedrijven (of andere burgers) ondersteunen. Het gaat hierbij wel om een groeiproces; bekeken zal nog moeten worden of bestaande middelen daarvoor geschikt zijn en/of eventueel geschikt gemaakt moeten worden.

Om dit mogelijk te maken is het noodzakelijk dat de nationale interoperabiliteit (herbruikbaarheid) op de verschillende betrouwbaarheidsniveaus wordt geborgd. Voor de dienstverleners betekent dit dat zij zelf bepalen welk betrouwbaarheidsniveau hun dienst nodig heeft met als leidraad de “Handreiking betrouwbaarheidsniveaus voor authenticatie bij elektronische overheidsdiensten” [15] van het Forum Standaardisatie.
Voor het betrouwbaarheidsniveau haken we aan bij het Europese STORK-vertrouwens-model dat als objectief kader dient. Er wordt een Europese interpretatie van betrouwbaarheidsniveaus gehanteerd zodat de verschillende middelen van gelijke niveaus uitwisselbaar zijn.

Belangrijk aandachtspunt hierbij is het waarborgen van privacy. Om bredere inzetbaarheid van publieke eID-middelen in het private domein mogelijk te maken, zullen technische oplossingen gezocht moeten worden om gebruik zonder uitwisseling van BSN mogelijk te maken. De wijze waarop dit wordt gerealiseerd komt in paragraaf 4.3.7 terug.

[15] Zie http://www.forumstandaardisatie.nl/fileadmin/os/publicaties/HR_Betrouwbaarheidsniveaus_WEB.pdf

4.2.4 Internationale interoperabiliteit

In juni 2012 publiceerde de Europese Commissie een voorstel voor een Verordening die wederzijdse erkenning van elektronische identiteiten en vertrouwensdiensten tussen de lidstaten regelt. Een van de verwachtte consequenties van de Verordening is dat Nederlandse burgers en bedrijven moeten in het buitenland elektronisch zaken kunnen doen en dat buitenlandse elektronische identificatiemiddelen ook in Nederland dienen geaccepteerd te kunnen worden.
Ook al is de exacte inhoud van de verordening nog niet bekend, vast staat dat overheidsdienstverleners op termijn buitenlandse middelen zal moeten kunnen accepteren. Ingeschat wordt dat dit nog ca. 2 jaar zal duren. Ook hiervoor is een ontkoppeling tussen diensteninfrastructuur en eID-middelen infrastructuur nodig.

In onderstaand kader wordt toelichting gegeven op de Verordening.

Europese Verordening eID

- Op 4 juni jl. publiceerde de Europese Commissie een voorstel voor een verordening die wederzijdse erkenning van elektronische identiteiten en vertrouwensdiensten tussen de lidstaten regelt.
- De conceptverordening heeft tot doel het vertrouwen in het elektronische verkeer tussen burgers, bedrijven en overheden binnen Europa te vergroten door dit onbelemmerd en veilig te laten plaatsvinden.

Voor Nederland betekent dit:
Als de verordening (waarschijnlijk begin 2014) van kracht wordt kan Nederland haar eigen eID's notificeren, waarmee Nederlandse burgers en ondernemingen toegang kunnen krijgen tot de Europese digitale interne markt. Op termijn wordt het dan mogelijk voor Nederlandse burgers om met hun Nederlandse eID's bij buitenlandse overheidsdienstverleners een dienst af te nemen.

Om dit technisch, juridisch en organisatorisch mogelijk te maken heeft Nederland een voorziening nodig, gebaseerd op de bouwstenen uit het STORK project, die het mogelijk maakt om:

1) Nederlandse eID's te laten 'praten' met buitenlandse dienstverleners
2) Buitenlandse eID's te laten 'praten' met Nederlandse overheidsdienstverleners

Wat betreft het eerste punt heeft Nederland zelf keuzevrijheid. Nederland is niet verplicht om eID's te notificeren. Met betrekking tot het tweede punt heeft Nederland geen keuzevrijheid, dit wordt op termijn en onder bepaalde voorwaarden afgedwongen door de verordening.

De verordening is een randvoorwaardelijk kader voor het stelsel eID NL

- Een verordening is het zwaarste instrument dat de Commissie kan inzetten. Een verordening heeft voorrang boven nationale wetten en wordt niet omgezet in nationale wetgeving. Nederland heeft dus geen implementatievrijheid ten aanzien van de verordening.
- Het moeten kunnen accepteren van buitenlandse elektronische identiteiten voor Nederlandse overheidsdienstverleners is voor Nederland geen beleidskeuze, maar wordt een door de verordening afgedwongen situatie.

- Focus ligt nu op het onderhandelen over de uiteindelijke tekst van de verordening. Nadat de tekst is vastgesteld en de verordening geïmplementeerd, moet Nederland binnen een nog nader te bepalen termijn buitenlandse eID's kunnen accepteren die bij de Europese Commissie genotificeerd zijn.
- De onderhandelingen zullen naar schatting een jaar duren (tot eind 2013).

Nederlandse eID's kunnen op termijn toegang krijgen tot de Europese digitale interne markt

- Nederland kan bij de Europese Commissie een stelsel voor elektronische identificatie aanmelden.
- Onder stelsel voor elektronische identificatie wordt verstaan: een systeem voor elektronische identificatie waarbinnen elektronische identificatiemiddelen worden uitgegeven en ondubbelzinnige wijze middels persoonsidentificerende gegevens in elektronische vorm zijn gekoppeld aan een natuurlijke of rechtspersoon.
- Na acceptatie kunnen Nederlandse burgers en ondernemingen in het buitenland terecht met hun Nederlandse elektronisch identificatiemiddel en daarmee onbelemmerd deelnemen aan de Europese digitale interne markt. .

Nederlandse overheidsdienstverleners moeten op termijn buitenlandse eID's accepteren

- Een lidstaat moet een eID uit een andere lidstaat accepteren, indien het stelsel waaronder deze is uitgegeven bij de Europese Commissie volgens de geldende procedure is aangemeld.
- De verplichte acceptatie geldt wanneer elektronische identificatie met gebruikmaking van een elektronisch identificatiemiddel vereist is op grond van wetgeving of gangbare bestuursrechtelijke praktijk om toegang te krijgen tot een overheidsdienst.
- Het verplicht moeten accepteren van elektronische identiteit uit een andere lidstaat voor Nederlandse overheidsdiensten betekent dat Nederlandse overheidsdienstverleners in staat moeten zijn om die buitenlandse elektronische identiteit te kunnen ontvangen, accepteren en verwerken, zoals zij dat ook met Nederlandse elektronische identiteiten doen. Hier zal Nederland in technisch, organisatorisch en juridisch opzicht zaken voor moeten regelen.
- Ontkoppeling van authenticatie en autorisatie van de primaire e-overheidsdienstverlening is voor de lange termijn oplossing een voorwaarde om een optimale voorziening voor Nederland te kunnen inrichten.

Toezicht

- Vanwege het incident met DigiNotar is stevig toezicht voor Nederland een belangrijk punt. De Verordening regelt geen toezicht voor elektronische identiteiten. Er zal bepaald moeten worden in welke vorm Nederlandse elektronische identiteiten onder toezicht zullen worden gesteld.

Nederlandse inzet in Brussel:

- De onderhandelingen over de definitieve tekst van de Verordening zijn inmiddels van start gegaan. Het uitreiken van eID's is en blijft een nationale aangelegenheid, de Verordening ziet voor wat betreft elektronische identiteiten enkel toe op de grensoverschrijdende aspecten. Inzet van Nederland in Brussel zal zijn dat geborgd moet zijn dat Nederlandse eID voorzieningen op termijn grensoverschrijdend gebruikt kunnen worden. Ook moet afdoende gewaarborgd zijn dat Nederland alleen die eID's van andere lidstaten hoeft te accepteren die voldoende betrouwbaar zijn voor de dienstverlening die Nederland aanbiedt. De Europese Commissie lijkt vooral in te zetten op eID's van een hoog betrouwbaarheidsniveau, maar uit de Verordening blijkt vooralsnog onvoldoende duidelijk welke eisen en criteria gelden die dit waarborgen.
- Lidstaten worden aansprakelijk geacht ten aanzien van de kwaliteit van identificatie en validatie van door hen genotificeerde eID's, maar het is maar de vraag in hoeverre dit tot het gewenste resultaat leidt. Daarnaast is Nederland geen voorstander van het overnemen van verantwoordelijkheden van het bedrijfsleven door de overheid en zal ook voor dit punt aandacht vragen in Brussel.

4.2.5 Rijksoverheid systeemverantwoordelijkheid eID stelsel NL

Deze systeemverantwoordelijkheid omvat het volgende:

- Het ontwikkelen, vaststellen en uitdragen van een visie op beleidslijnen met betrekking tot digitale identiteiten en machtigingen in Nederland,
- Het (laten) vaststellen en onderhouden van stelselspecificaties en –afspraken. Op basis van de specificaties en afspraken kunnen zowel publieke als private partijen authenticatie- en autorisatiediensten inrichten. Iedere aanbieder van eID-voorzieningen, die aan deze eisen voldoet en zich onderwerpt aan toezicht, kan toetreden tot het stelsel op basis van deze afspraken.
- Het (laten) uitvoeren van het beheer van het stelsel. Het eID domein is een dynamische en innovatieve omgeving. De snelheid van technologische ontwikkelingen ligt hoog. Dit betreft zowel devaluatie van middelen als het

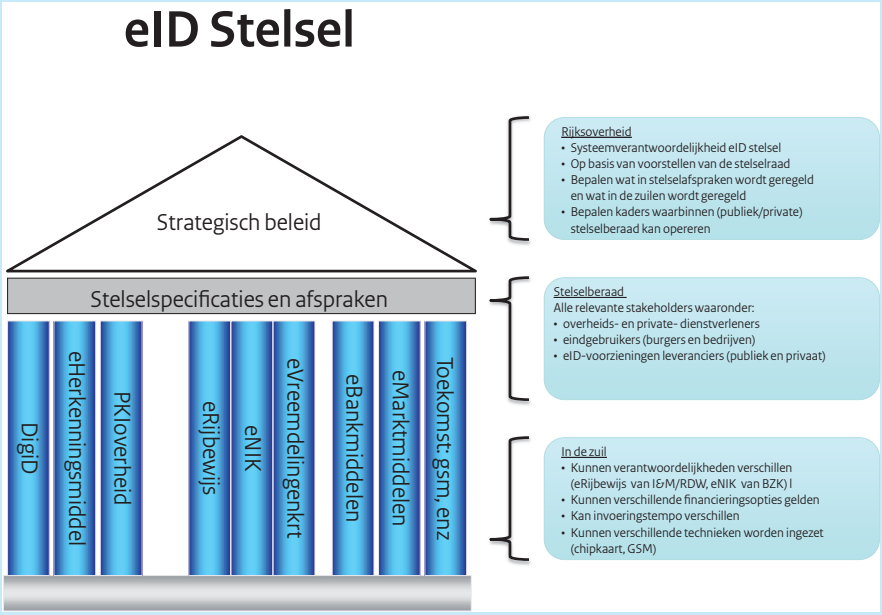
opnemen van nieuwe ontwikkelingen en vergt dus een actief beheer van de middelenlijst en de bijbehorende specificaties in het stelsel.
Het beheer van het afsprakenstelsel wordt bij één uitvoeringsorganisatie belegd . De kosten worden in eerste instantie gedragen door de beleidsdepartementen BZK en EL&I. Er zijn binnen de bestaande stelsels (zoals PKIoverheid, DigiD, eHerkenning) al veel zaken (qua afspraken, standaarden en overleginfrastructuur) beschikbaar die (her)gebruikt zullen worden.

- Het uitvoeren van het daarbij behorende toezicht. De publieke verantwoordelijkheid voor adequate voorzieningen voor authenticatie en autorisatie betekent ook dat in het stelsel voorzien wordt in publiek toezicht. Hiertoe behoren het opzetten en borgen van adequate mechanismen voor controles op deugdelijke authenticatie en autorisatie in de eigen processen van dienstverleners in het stelsel en een goed toegeruste organisatie voor toezicht op aanbieders van middelen en diensten met passende handhavingsmogelijkheden (sancties). Daarbij wordt rekening gehouden met de aard van de organisaties en bestaande toezichtmechanismen die daarvoor gelden of beschikbaar zijn. Bij de inrichting van het toezicht wordt bezien welke elementen uit de toezichtsarrangementen uit eHerkenning en PKIoverheid hergebruikt kunnen worden. Daarnaast wordt de noodzaak bezien om (voor onderdelen) een wettelijk toezichthouder aan te wijzen;dit in relatie tot de benodigde betrouwbaarheid van het stelsel. Dit wettelijk toezicht kan ook bestaande mechanismen betreffen, zoals in het kader van de Telecomwet, Gemeentewet en dergelijke. Indien het huidige toezicht moet worden verzwaard, mede op basis van de Europese Verordening, dan moet bekeken worden hoe dit financieel gedekt wordt.

Geadviseerd wordt dat de rijksoverheid deze systeemverantwoordelijkheid op zich neemt omdat de overheid verantwoordelijk is voor het beschikbaar komen van ondubbelzinnig uitgeven digitale identiteiten, Ook wordt het stelsel voor de dienstverlening van de overheid, en daarnaast - door het brede gebruik - een onmisbare infrastructuur voor de Nederlandse samenleving. Verder sluit het aan bij de verantwoordelijkheid van de Nederlandse overheid op grond van de Europese eID verordening.

De beleidsverantwoordelijke ministeries zijn systeemverantwoordelijk voor het afsprakenstelsel. Zij zijn verantwoordelijk voor een deugdelijk proces van totstandkoming van de governance (beheer en toezicht). Het daadwerkelijk invullen van de inhoud is een gezamenlijke verantwoordelijkheid van de dienstverleners, publieke en private eID leveranciers en de eindgebruikers (burgers en bedrijven). De inhoud van het stelsel wordt dus gezamenlijk

vormgegeven. Hierbij is er een belangrijke rol voor een stelselraad waarin vertegenwoordigers van alle stakeholders zitten.



Figuur 3: Rollen per niveau in het stelsel.

De systeemverantwoordelijkheid is te vergelijken met de systeemverantwoordelijkheid die de minister van EL&I heeft t.a.v. de telecombranche. De daadwerkelijke uitvoering binnen de pijlers valt dus niet onder de systeemverantwoordelijkheid. De verantwoordelijkheid voor de afzonderlijke middelen, zoals een eNIK en eRijbewijs, liggen bij de organisatie die de middelen uitgeven (zoals BZK voor eNIK en I&M/RDW voor eRijbewijs).

4.2.6 *Aansluiting overheidsdienstverleners*

Het is belangrijk dat het eID-stelsel zo snel mogelijk, zo breed mogelijk wordt geaccepteerd en daarmee ook daadwerkelijk wordt gebruikt. Brede acceptatie van middelen uit het stelsel zal ervoor zorgen dat de bestaande overige elektronische identificatiemiddelen onder het stelsel worden gebracht of uitgefaseerd.
Daarom wordt de standaarden en specificaties van het eID-stelsel te zijner tijd aangemeld voor de 'pas-toe-of-leg-uit-lijst' van het College Standaardisatie. Dit geeft overheidsdienstverleners de mogelijkheid om afhankelijk van de complexiteit van de huidige integratie met de primaire processen en afhankelijk van investeringsregimes de eID infrastructuur te ontkoppelen en eID-middelen breed te gaan accepteren.
De winst van één afsprakenstelsel is namelijk vooral te realiseren als alle partijen eraan deelnemen. Indien de overheid investeert in een generiek stelsel, is het onwenselijk dat een overheidsdienstverlener zelf een eigen systemen gaat/blijft ontwikkelen.

4.3 Hoog niveau eID middel voor burgers

Ten aanzien van het breed beschikbaar krijgen van een hoog niveau eID middel voor burgers adviseert de werkgroep dat:

1. De overheid ervoor zorgt dat middelen op relatief korte termijn op het hoogste niveau beschikbaar komen voor burgers (en voor natuurlijke personen die een onderneming drijven).
2. Het mix-scenario de voorkeur heeft: daarin worden publieke middelen èn private middelen uitgegeven en gebruikt.
3. De overheid gaat publieke middelen op het hoogste niveau uitgeven.
4. Ten behoeve hiervan dient het mixscenario nader te worden uitgewerkt. Daarbij komt naar voren:
   a. Welke (combinatie van) dragers wenselijk is, mede gelet op het afdekken van de gehele klantpopulatie (vertrekpunt zijn de huidige 9 miljoen DigiD gebruikers).
   b. Welke massale uitrol scenario's mogelijk zijn (bijvoorbeeld niet wachten op regulier vervanging bij NIK/Rijbewijs maar stimuleringsmaatregelen om eerder om te wisselen; en het versneld inschakelen van reeds uitgerolde marktmiddelen zoals bankmiddelen).
   c. Welke kosten brengt het met zich mee, en welke financieringsopties zijn er (kostendekking aanschaf, kostendekking gebruik, wat kost het de burger, wat kost het een dienstaanbieder, welke kosten worden centraal gedragen).
5. Deze middelen niet noodzakelijkerwijs gratis zijn (vergelijkbaar met identiteitsbewijzen in de fysieke wereld).
6. De overheid een 'omnummervoorziening' realiseert, die het gebruik van private eID-middelen bij overheidsdien-

sten mogelijk maakt (overheidsdienstverleners herkennen hun klant immers aan het BSN).
7. Nader wordt onderzocht - hoe privaat gebruik van deze middelen (op termijn) conform paragraaf 4.2.3. - op een privacyvriendelijke manier kan plaatsvinden.

4.3.1 Overheid zorgt voor beschikbaar komen hoog niveau eID-middelen burgers

In toenemende mate stellen overheidsdiensten steeds hogere betrouwbaarheidseisen aan de toegang tot digitale overheidsportalen en –dossiers. Enerzijds door uitbreiding van de online raadpleegbare informatie, maar ook doordat burgers digitaal correctieverzoeken kunnen doorgeven in deze portalen, zoals MijnOverheid.nl. Hierdoor worden deze verzamelingen van persoonsgegevens steeds meer geclassificeerd op het niveau van risicoklasse III Beveiliging van persoonsgegevens binnen de Wet Bescherming Persoonsgevens, waarvoor strenge beveiligingseisen gelden en waarvoor dito zwaardere maatregelen moeten worden getroffen. Zonder een eIDmiddel op het hoogste veiligheidsniveau is deze uitbreiding van digitale dienstverlening kwetsbaar. Hier speelt ook de toenemende mate van identiteitsfraude en cybercrime activiteiten op het internet een rol. Zie in lijn hiermee de behoefte van de bevraagde (overheids)dienstverleners in hoofdstuk 3.

Momenteel verstrekt de overheid - analoog aan haar taakopvatting in de 'papieren wereld' - digitale authenticatiemiddelen (wachtwoord, wachtwoord+sms) aan haar burgers met DigiD. Het huidige uitgifteproces (dat kosten en vriendelijk qua administratieve lasten is) vindt plaats via de post, en heeft daardoor een basaal betrouwbaarheidsniveau. De overheid verstrekt op dit moment geen digitale authenticatiemiddelen van het hoogste betrouwbaarheidsniveau conform de niveaus van STORK[16] (uitgegeven na face-to-face controle aan de balie). Op termijn zal DigiD basis en midden onvoldoende zijn om de privacy en beveiliging van persoonsgegevens en financiële transacties te borgen.
Er moeten dus eID-middelen op hoog niveau voor de burger beschikbaar worden gemaakt.

4.3.2 Mix-scenario van publieke middelen èn private middelen heeft de voorkeur

Het beschikbaar krijgen van eID middelen op hoog niveau kan op verschillende manieren: a. door de overheid zelf (publieke eID-middelen), of b. met gebruikmaking van marktmiddelen (private eID middelen), c. of een combinatie daarvan (mix-scenario).

De uitgifte van een geheel nieuw eID middel dat face-to-face aan een balie is uitgegeven, is kostbaar. Met het oog op

[16] www.eid-stork.eu

kostenbesparing heeft het daarom voorkeur om aan te haken bij reeds bestaande middelen/dragers en uitgifteprocessen. Dat geldt zowel voor publieke als private middelen.

a. Overheidsmiddelen

In het overheidsdomein zijn het Rijbewijs (11 miljoen houders), de Nederlandse IdentiteitsKaart (7,5 miljoen houders) breed uitgerolde, en face-to-face uitgegeven identiteitsdocumenten. Aan deze dragers (op creditcardformaat) kan een eID (chip) worden toegevoegd. Doordat de bestaande kaarten en het uitgifteproces al zijn gefinancierd, worden de uitrolkosten van het middel in dat geval beperkt tot de meerkosten voor het toevoegen van een eID(chip) plus kaartlezer. Aandachtspunt daarbij is wel de tienjarige geldigheidsduur (ten aanzien van het uitroltempo en extra kosten bij versnelde invoering).

b. Marktmiddelen

In het private domein is een aantal potentiële eID middelen (hoger niveau dan de huidige publieke middelen) breed uitgerold: mobiele telefoons en internetbankiermiddelen. De techniek van elektronische identificatie met de mobiele telefoon is op dit moment nog niet voldoende uitgekristalliseerd, gestandaardiseerd en breed uitgerold, maar wel interessant voor de toekomst. Internetbankiermiddelen zijn interessant omdat ze face-to-face zijn uitgegeven en momenteel breed (en dagelijks) worden gebruikt voor elektronische transacties. Mensen zijn gewend deze middelen te gebruiken, en vertrouwen ze voldoende voor financiële transacties (veiligheid). Het is waarschijnlijk dat zij het vertrouwen in die middelen ook hebben op het moment dat deze voor elektronische identificatie (eID) kunnen worden gebruikt.

c. Mix-scenario heeft voorkeur

Een eID stelsel met een mix van publieke en private middelen heeft de voorkeur:

- Het maakt tempo mogelijk, want mensen hebben één van de middelen vaak al in bezit;
- Het maakt een geleidelijk uitrolscenario van het overheidsmiddel mogelijk (de overheidsmiddelen hoeven niet per direct de gehele doelgroep 'af te dekken'), met bijbehorende kostenbesparingen;
- Mensen kunnen zelf kiezen aan welk middel zij de voorkeur geven (o.a. WRR[17] studie geeft aan dat een deel van de mensen een strikte scheiding wil in het gebruik van publieke en private middelen);
- Er is een fall-back mogelijkheid, wanneer 1 van de middelen onverhoopt uitvalt (risicospreiding).

[17] Rapport 'iOverheid', http://www.wrr.nl/fileadmin/nl/publicaties/PDF-Rapporten/I_Overheid.pdf van de Wetenschappelijke Raad voor Regeringsbeleid (WRR)

4.3.3 Overheid gaat zorgen voor publieke middelen op het hoogste niveau

Zowel in het mix-scenario als in een scenario met louter overheidsmiddelen, geeft de overheid zelf publieke middelen uit. Het is daarom een no-regret optie om op korte termijn te beginnen met de herijking van de reeds uitgevoerde onderzoeken m.b.t. het plaatsen van een eID op NIK en/of Rijbewijs, met het oog op de introductie van een publiek eID middel. Daarbij dient ondermeer de vraag aan de orde te komen welk deel van de huidige klantpopulatie van DigiD (9 mln), in het bezit is van (een van) beide dragers.

4.3.4 Nadere uitwerking mix scenario

Voorgesteld wordt om het mix scenario nader uit te laten werken, inclusief (een) haalbaarheidsonderzoek(en). Naast het eerder genoemde aspect van de afdekking van de doelgroep, komen daarbij aan de orde:

a. De dragers NIK(BZK), Rijbewijs(RDW), en de marktmiddelen/bankmiddelen (FIN), en evt. overige middelen.
b. Welke versnellingsscenario's zijn mogelijk
c. Wat zijn de kosten (evt. aan de hand van een RFI/marktconsultatie)
d. Welke financieringsinvulling kan worden gekozen (waaronder kostendekking aanschaf, kostendekking gebruik, wat kost het de burger, wat kost het een dienstaanbieder, welke kosten worden centraal gedragen). In de vorm van een businessmodel vertaald naar maatschappelijke baten en bedreigingen (ontwrichting van de infrastructuur).

4.3.5 Middelen en diensten zijn niet noodzakelijkerwijs gratis

Het gebruik van publieke eID middelen is niet noodzakelijkerwijs gratis. Met het oog op de eigen verantwoordelijkheid van de burger, en – mede met het oog op een level playing field[18] in het Stelsel – kan een tarief in rekening worden gebracht (vergelijk met de leges voor een conventionele ID-kaart).

4.3.6 Omnummervoorziening ten behoeve van gebruik private middelen door overheid

Private eID middelen mogen niet het BSN bevatten. Dat komt omdat het BSN alleen door overheidsorganisaties mag worden gebruikt (of private organisaties die daarvoor een specifieke wettelijke grondslag hebben[19]; dat is niet het geval bij private eID middelen).
Omdat overheidsdienstverleners hun klanten herkennen aan het BSN, moet er - aan overheidszijde - een vertaalslag plaatsvinden naar het BSN. Daartoe moet een omnummervoorziening worden ingericht. Deze omnummervoorziening

[18] Onderzocht wordt in hoeverre de wet markt en overheid van invloed is op de doorberekening van kosten aan de burger.

[19] Voorbeeld van dergelijke private organisaties zijn private organisaties in de zorg (wet BSN in de zorg). Een ander voorbeeld zijn werkgevers die loongegevens aan de fiscus moeten doorgeven, zij mogen het BSN echter alleen gebruiken voor dat doel.

bevat een koppeltabel[20] van (privaat) klantnummer naar het BSN.

Achtergrond

De bescherming van de privacy van burgers en bedrijven vastgelegd in het Europees Verdrag van de Rechten van de Mens – EVRM, en nader uitgewerkt in de EU Privacy Richtlijn m.b.t. de verwerking van persoonsgegevens. Deze Richtlijn is voor Nederland vertaald in de Wet Bescherming Persoonsgegevens (WBP). Hierin is ondermeer het gebruik van persoonsidentificerende persoonsnummers geregeld[21]. De overheid heeft m.b.t. haar taken, het gebruik van een persoonsnummer, in casu het burgerservicenummer (BSN), in aanvullende wetgeving geregeld (Wet algemene bepalingen burgerservicenummer), en m.b.t. de zorg in de wet BSN in de zorg.

Bij ontwikkeling van het eID-stelsel wordt ervan uitgegaan dat dit beperkte gebruik (voorlopig) in stand blijft, dat wil zeggen dat het gebruik van het BSN beperkt blijft tot overheden, of door private organisaties die daarvoor een wettelijke grondslag hebben. Aanpassing en/of uitbreiding van de wetgeving voor het bredere gebruik van het BSN door private partijen stuit waarschijnlijk op politieke bezwaren.

4.3.7 Waarborgen privacy bij privaat gebruik

Om bredere inzetbaarheid van publieke eID-middelen in het private domein mogelijk te maken, zullen technische oplossingen gezocht moeten worden om:

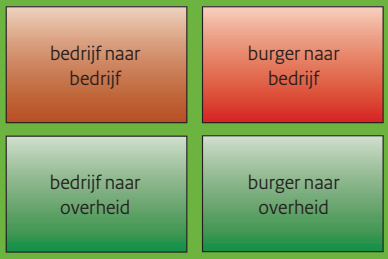
a. gebruik in die sector zonder uitwisseling van BSN of een ander standaard persoonsnummer mogelijk te maken (denk aan pseudonomisering, omnummering en minimal disclosure).
b. daarbij zoveel mogelijk het risico van hotspots te voorkomen (een hotspot is één plek, waarin ook het totale - dus ook het private - gebruik van een eID middel in kaart zou kunnen worden gebracht). Zie verder kader.

[20] Om toekomstige kraakbaarheid te voorkomen, betreft het een tabel met nummers die geen wiskundig/algoritmisch verband houden. De tabel zelf (met alle private eID klantummers en BSN's) dient vanzelfsprekend hoogwaardig te worden beveiligd (vergelijkbaar met de huidige DigiD wachtwoord tabel).

[21] (WBP, art. 8, 11 en 24, eerste lid)

Privacy eisen leiden tot een hybride vorm van het eID stelsel

Mede vanwege zaken als de kwetsbaarheden van de OV-chipkaart, de DigiNotar affaire, Lektober', incidenten en hacks bij KPN, is privacy, of ten minste de beeldvorming rond beveiliging en privacy, een kritische succesfactor van een nieuw te definiëren eID-stelsel.



Er zijn vier domeinen waar een eID-stelsel een goede rol kan spelen voor Nederland: zie figuur.

De lading die privacy heeft is verschillend binnen deze domeinen. Dit geldt ook voor de beeldvorming.

Als wordt uitgegaan van maximaal hergebruik en minimale impact voor bestaande gebruikers van DigiD en eHerkenning, dan ligt een centrale component in de infrastructuur voor de hand. Ervan uitgaande dat het eID stelsel moet voldoen aan internationaal aanvaarde privacy-eisen blijkt dat bij de domeinen *'burger/bedrijf naar bedrijf'* een centrale component in de infrastructuur het risico met zich meebrengt dat er in die component een 'hot spot' ontstaat, waarin privacy gevoelige informatie beschikbaar komt (namelijk de informatie over de digitale private 'handel en wandel' van een individu). Het risico is dat daardoor beeldvorming negatief wordt, en dat ondanks de beste bedoelingen de burger het niet vertrouwt, en daardoor het eID-stelsel niet gebruikt wordt in de domeinen *'bedrijf/burger naar bedrijf'*. Omdat het domein *'bedrijf naar bedrijf'* zakelijke transacties betreft met beperkte persoonlijke gegevens, is het privacy issue overzienbaar.

Voor het domein 'burger naar bedrijf' zal gezocht worden naar oplossingen om het risico van hotspots zoveel mogelijk te voorkomen (een van die oplossingen is een model waarin een burger zich rechtstreeks bij een bedrijf authenticeert zonder tussenkomst van een centrale (overheids)component).

5. Vervolgstappen

5.1 Inleiding

Het concept van dit strategisch document wordt na afstemming met de Berlijngroep en de Manifestgroep voorgelegd aan de stuurgroep eID op 4 oktober 2012. Op dit punt bereikt het document de status van een binnen de overheid vervaardigde en ambtelijk overeengekomen conceptversie. Het document kan pas definitief vastgesteld worden indien alle groepen belanghebbenden zijn geconsulteerd. Het is van belang dat de strategische visie door een meerderheid van de belanghebbenden gedragen wordt.

Het document bevat een aantal aspecten, die specifiek aan de politiek dienen te worden voorgelegd (zie kader). In oktober zullen, afhankelijk van verkiezingsuitslag en te verwachten formatieperiode, de verantwoordelijk ministers worden geïnformeerd. Politieke besluitvorming vindt bij voorkeur door een nieuw kabinet plaats, en kan pas plaatsvinden na consultatie van alle stakeholders.

Politieke besluitvorming

Beleggen politieke verantwoordelijkheid eID-stelsel:
Hoewel er weinig politieke weerstand wordt verwacht ten aanzien van het inrichten van het stelsel, dient de politieke verantwoordelijkheid genomen en belegd te worden.

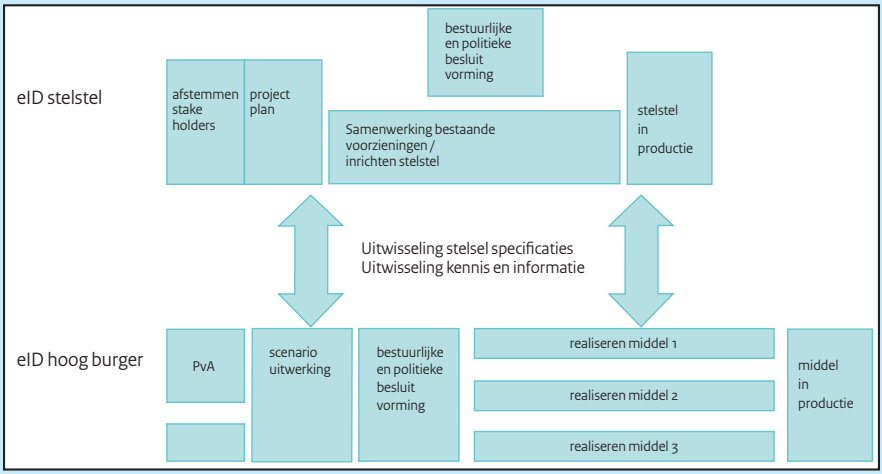
Vooruitlopend daarop wordt gestart met de voorbereiding en samenwerking van de verschillende bestaande oplossingen. Samenwerking is een no-regret-option.
Vaststellen onderstaande strategische uitgangspunten in het stelsel
* **Multi middelen/mix scenario:** inzetbaarheid van zowel publieke eID-middelen als private eID-middelen voor burgers (zoals bijvoorbeeld internetbankiermiddelen) bij overheidsdienstverlening (voetnoot: voor bedrijven/rechtspersonen is al besloten dat zij private middelen gebruiken).
* **Multi gebruik:** met eID middelen (publiek of privaat) kun je zowel bij overheidsdienstverleners als private dienstverleners terecht, voor zover dit nu nog niet van toepassing is.

De overheid gaat publieke middelen op het hoogste niveau uitgeven
Zowel in het voorkeurscenario, als in een (fallback)scenario waarin alleen overheids eID-middelen worden uitgegeven, dienen overheids eID middelen te worden uitgegeven.
Middelen wel of niet gratis: Moeten burgers betalen voor een eID middel, of verstrekt de overheid deze (deels) 'gratis'[22]

[22] eID middelen voor bedrijven/rechtspersonen worden door henzelf betaald.

Ter voorbereiding op de politieke besluitvorming worden de komende maanden gebruikt voor afstemming met stakeholders en het voorbereiden van daadwerkelijke implementatie van de adviezen via 2 sporen, te weten spoor 1: Het inrichten van eID stelsel NL en spoor 2: Het uitwerken van de verschillende scenario's voor een eID-middel op hoog niveau voor burgers.

De beide sporen zijn twee aparte projecten, met ieder een eigen karakter en tempo; hierdoor kan er met meer slagkracht tempo gemaakt worden. Zodat stapsgewijs de verbeterslagen gemaakt kunnen worden die nodig zijn, onafhankelijk van elkaar. Dit wilt niet zeggen dat er geen afstemming is tussen beide projecten. Hier wordt in de aansturing van de projecten rekening mee gehouden. Zie figuur 4 voor een overzicht van de voorziene stappen binnen de beide sporen.



Figuur 4: Stappen binnen de vervolgsporen

5.2 Spoor 1 eID stelsel NL

Het eID-stelsel zal stapsgewijs worden ontwikkeld. De stappen die gezet moeten worden, zijn:

- Stap 1: betrekken overige belanghebbenden
- Stap 2: opstellen programmaplan

Stap 1: betrekken overige belanghebbenden
De eerste stap die in oktober/november genomen wordt is het consulteren van alle belanghebbenden. Dit gebeurt aan de hand van het door de stuurgroep eID vastgestelde kader. Dit heeft als doelstelling hen de gelegenheid te geven bij te dragen aan het concept en zo consensus te bereiken over het strategisch beleidsdocument. Tevens wordt hun betrokkenheid/inzet bij de vervolgstappen besproken om zo draagvlak, toekomstig gebruik en het aanbod van eID middelen te borgen.
De externe stakeholders zijn in ieder geval, maar niet perse beperkt tot, banken, leveranciers van trust diensten (bv marktpartijen PKIoverheid en eHerkenning), medeoverheden (gemeenten) VNO/NCW, ECP-EPN, vertegenwoordiging softwareleveranciers, vertegenwoordiging fiscale en andere dienstverleners, medeoverheden, vertegenwoordiging consumenten/burgers.

Resultaat: Gedragen strategische visie die voorgelegd kan worden aan de politiek, afhankelijk van de kabinetsformatie zal dit in december/januari plaatsvinden.

Stap 2: opstellen programmaplan
De tweede stap betreft het opstellen van een programmaplan, inclusief de aansturing en de besluitvormingsprocedures voor het inrichten afsprakenstelsel eID.
Een nog aan te stellen programmamanager en programmateam stelt in overleg met belanghebbenden dit plan op. Dit plan omvat op te leveren deelresultaten (zie hieronder) en de inrichting van aansturing van het programma. Bij dit laatste wordt aandacht besteed aan de vertegenwoordiging van en afstemming met de stakeholders en besluitvormingsprocedures. Initieel wordt het programmateam gevormd door de organisaties uit de huidige zomerwerkgroep. Het programmateam zal na overleg stakeholders worden aangevuld/vervangen met deze stakeholders.

Resultaat: Door opdrachtgever(s) goedgekeurd programmaplan in november

Programma eID stelsel NL
In de huidige situatie bestaan er diverse oplossingen voor digitale identiteiten, zo is er een afsprakenstelsel eHerkenning, publieke middelen als DIGID, etc. Er is dus het nodige basismateriaal dat hergebruikt kan worden. Dit heeft betrekking op zowel de inhoud (standaarden) en de governance als op het toezicht. Binnen het programma eID stelsel NL wordt bezien op welke wijze deze elementen hergebruikt worden voor het eID-afsprakenstelsel, welke aanpassingen er nodig zijn en welke nieuwe elementen er moeten worden ingevuld.
De uitdaging is om bestaande afspraken over de verschillende voorzieningen in een gezamenlijk afsprakenstelsel onder te brengen op een dusdanige wijze dat het een door alle belanghebbenden gedragen stelsel vormt. Dat zal een groeiproces zijn.

De scope van het stelsel wordt stapsgewijs uitgebreid. Er wordt gestart met de middelen en machtigingen. In de loop van

de tijd uitgebreid wordt de scope uitgebreid met vertrouwensdiensten zoals de gekwalificeerde digitale handtekening.

Europese verordening
Ook al is de definitieve tekst van de Verordening eID van de Europese Commissie op dit moment nog niet bekend, vast staat dat op termijn Nederlandse overheidsdienstverleners buitenlandse eID onder bepaalde voorwaarden zullen moeten kunnen accepteren. Hiervoor is onder andere ontkoppeling tussen de diensteninfrastructuur en eID-middelen infrastructuur wenselijk. Ook wordt het belangrijk gevonden dat Nederlandse eID middelen op termijn binnen de gehele EU bruikbaar zijn, zodat Nederlandse burgers en bedrijven hiermee toegang krijgen tot de Europese digitale interne markt.
Voor grensoverschrijdend gebruik van eID middelen zal hierdoor een uitvoeringsvraag gaan ontstaan. In de toekomst zal dit ook binnen de scope van het afsprakenstelsel worden gebracht.

Capaciteit
Voor het slagen van de opdracht, zal er voldoende capaciteit moeten zijn met name om een breed draagvlak voor de plannen te realiseren. Een te vormen programmateam bestaat uit een programmamanager en secretaris, aangevuld met deskundigen uit de huidige bestaande voorzieningen, en eindgebruikers (overheidsdienstverleners). Voor de opstartfase is er de komende maanden circa 4 FTE nodig. Er is deskundigheid nodig op onder meer juridisch gebied, informatietechnologie en veiligheid, privacy en (beleidsmatige) wensen van overheidsdienstverleners.

Deelresultaten
In het programma eID-stelsel worden onder andere de volgende deelresultaten opgeleverd:
Verantwoordelijkheden en toezicht
- Een voorstel voor de structurele inrichting van de governance (wie beslist er over het eID afsprakenstelsel?)
- Een voorstel voor de inrichting van het toezicht en de handhaving
- Een voorstel voor afbakening stelsel (in het dak van het eID afsprakenstelsel); wat wordt er geregeld op stelselniveau en wat in de zuilen.

Inhoudelijk: stelselafspraken en specificaties
- Een uitgewerkte overzicht van een eID afsprakenstelsel op basis van beschikbare informatie (wat is er al?); zie ook bijlage 2 voor de inhoudsopgave van het afsprakenstelsel. Hier wordt ondertussen al aan gewerkt.
- Set van stelsel- specificaties en afspraken, zodat de ontkoppeling van diensten en eID-voorzieningen mogelijk wordt.
- Financiering en communicatie

Implementatie
- Een impactanalyse van het eID afsprakenstelsel op de bestaande voorzieningen
- Een gedegen risico analyse en een overzicht van de kritische succesfactoren
- Een plan van aanpak voor de implementatie van het eID afsprakenstelsel

eID-stelsel
Korte termijn – stap 1 (2012)

Stuurgroep:
De stuurgroep eID-stelsel bestaat uit EL&I (vz), BZK, RDW, FIN/ Belastingdienst, UWV en is in ieder geval verantwoordelijk voor het opleveren van een programmaplan.

Kerngroep:
- Huidige zomerwerkgroep (BZK, EL&I, Belastingdienst, RDW, UWV)

Projectteam (minimaal 4 FTE)
- Programmamanager eID afsprakenstelsel
- Secretaris eID-afsprakenstelsel
- Vertegenwoordiging van stakeholders
- per fase inzetbare expertise (juristen, architecten, business consultants, technische adviseurs, communicatie-adviseurs) vanuit binnen en buiten de verschillende organisaties

Na afronding van het programmaplan moet bepaald worden wat de optimale personele bezetting is.

Samenhang project Hoog niveau eID-middel burger
De samenhang wordt gewaarborgd doordat dezelfde personen in de kern groep van zowel spoor 1 als spoor 2 deelnemen, daarnaast zal in de uitwerking van het programma hier nader aandacht aan besteed worden, en is de huidige stuurgroep eID vooralsnog voor beide trajecten verantwoordelijk.

5.3 Spoor 2 Hoog niveau eID-middel voor de burger

Reikwijdte

Het doel van het tweede spoor is het beschikbaar komen van een eID-middel hoog (STORK niveau 3 en 4) voor burgers, voor bedrijven is dit al beschikbaar. Het heeft betrekking op zowel de publieke als de private middelen:

- Voor publieke middelen (niveau 4) betreft dat het plaatsen van een eID op een overheidsdocument die valt onder de Wet op de Identificatieplicht, te weten de Nederlandse identiteitskaart, het rijbewijs en de vreemdelingenkaart (inclusief de specifieke wet- en regelgeving per document).
- Voor private middelen betreft dit het geschikt maken van breed uitgerolde private middelen (m.n. bankmiddelen) voor overheidsdiensten, als mede de inrichting van een omnummervoorziening.
- Parallel aan dit traject worden innovaties van andere eID-middelen gevolgd, zoals die van de mobiele devices (telefoon, tablets). Op basis van voortschrijdend inzicht kunnen deze dragers worden ingezet.

Stappen

De trajecten voor het ontwikkelen en het inzetten van publieke en private eID-mid-

delen verlopen parallel aan elkaar. De realisatie van eID hoog burger wordt in algemene zin in drie stappen gerealiseerd, namelijk:

- Stap I: voorbereidingen en uitwerking van het voorkeurscenario (mix-scenario)
- Stap II: bestuurlijke en politieke besluitvorming
- Stap III: de middellange termijn: realisatie en implementatie

Stap I: voorbereidingen en uitwerking voorkeurscenario

Binnen stap I wordt de besluitvorming voorbereid om tot een weloverwogen besluit door het kabinet te komen. Hiertoe wordt het mix-scenario nader uitgewerkt, waarin private en publieke middelen voor de verschillende diensten worden gebruikt. Ontwikkeling m.b.t. de verkiezingen en de kabinetsformatie worden hierin ook meegenomen.

Stap II: bestuurlijke en politieke besluitvorming

Stap II omvat de feitelijke besluitvorming per eID-middel (publiek/privaat) door het kabinet en de voorbereidingen in de voorportalen/onderraden.

Stap III: de middellange termijn: realisatie en implementatie

Stap III betreft de feitelijke realisatie en implementatie van het eID-middel hoog voor de burger. Dit varieert van het starten van de aanbesteding (specificaties t/m definitieve gunning), het wetgevingstraject, realisatie van de middelen en voorzieningen, de communicatie/ voorlichting aan burgers, het aansluiten van dienstverleners, tot de implementatiestrategie.

De volgende (deel)resultaten worden in de verschillende fases opgeleverd:

Stap I		**Deadline**
Deelresultaten	Plan van aanpak voorbereiding en scenario's	September 2012
	Uitgewerkte scenario's en financieringsarrangementen (kosten en financiële dekking) voor publieke en private middelen	November 2012
	PvA wetgevingstraject(en)	November 2012
	Herijkte analyse, haalbaarheidsstudie, inclusief ketenafhankelijkheidstudie	December 2012
Eindresultaat	Besluitvormingsmemorandum in stuurgroep eID middel hoog (voorkeursscenario)	December 2012

Stap II		Deadline
Deelresultaten	Detailplan van aanpak fase Kabinetsbesluit	PM, afhankelijk van de gekozen aanpak in stap 1
	Planning van de bestuurlijke route (onderraden, adviescommissies, etc)	PM, idem
	Besluitvormingsmemorandum in stuurgroep	PM, idem
Eindresultaat	Besluitvormingsmemorandum in Kabinet	PM, idem

De start van deze stap is afhankelijk van consensus en besluitvorming in de stuurgroep eID stelsel NL en voortgang kabinetsformatie na de verkiezingen.

Stap III		Deadline
Deelresultaten	Detailplan van aanpak fase ontwikkeling en realisatie	PM, idem
	Aanbesteding en gunning eID-middel hoog	PM
	Ontwikkeling en realisatie eID middel(en)	PM
	Wetswijzigingen wetgeving (indien van toepassing)	PM
	Implementatiestrategie	PM
	Mediacampagne naar burgers	PM
Eindresultaat	eID-middel hoog	PM

De start van deze stappen is geheel afhankelijk van de installatie van het nieuwe kabinet, tenzij verdere uitstel van de besluitvorming dit niet toestaat. De doorlooptijd van deze stap wordt geschat op tenminste 2 jaar. Dit wordt in belangrijke mate bepaald door het wetgevingstraject en het aanbestedings- en realisatietraject.

De organisatie wordt als volgt weergegeven:

eID-middel hoog burger Korte termijn - Stap I (2012)

Stuurgroep tot start programma's :
De huidige stuurgroep is de eerste maanden nog verantwoordelijk voor het opstellen van de programma's. Daarna kan er specifiek voor het 'eID-middel hoog burger 'traject een aparte stuurgroep ingericht worden. De stuurgroep eID-middel hoog voor burgers bestaat uit BZK , RDW, FIN/ Belastingdienst, VWS, UWV en is verantwoordelijk voor de invoering van het eID-middel hoog.

Kerngroep:
Huidige zomerwerkgroep

Programmamanager eID hoog burger
- 1 persoon fulltime

Programmateam:
- Projectsecretaris,
- Deelnemers vanuit organisaties (BZK, RDW, FIN/Belastingdienst, UWV, VWS)
- per fase inzetbare expertise (juristen, architecten, business consultants, technische adviseurs, communicatieadviseurs) vanuit binnen en buiten de verschillende organisaties.

Samenhang met eID Stelsel NL
Het eID middel– hoog wordt gerealiseerd binnen de door het eID-stelsel vastgestelde kaders, specificaties en afspraken.
De samenhang wordt gewaarborgd doordat dezelfde personen in de kern groep van zowel spoor 1 als spoor 2 deelnemen, daarnaast zal in de uitwerking van het programma hier nader aandacht aan besteed worden, en is de huidige stuurgroep eID vooralsnog voor beide trajecten verantwoordelijk.

Bijlage 1: toelichting begrippen

Dienstverleners (overheden en bedrijven) bieden burgers (consumenten) en bedrijven in toenemende mate de mogelijkheid om hun diensten digitaal af te nemen en steeds meer burgers en bedrijven maken hiervan gebruik. Om transacties te kunnen verrichten in het kader van een digitale dienst zal een dienstaanbieder twee basisvragen stellen:
a. Wie ben je?
b. Wat mag je?

Ad a. Wie ben je?

Bij het beantwoorden van deze vraag spelen twee begrippen een rol: identificatie en authenticatie. Bij identificatie gaat het erom dat voor de dienstaanbieder bekend wordt welke partij (natuurlijke of niet-natuurlijke persoon) gebruik wil maken van de digitale dienst. Identificatie is het koppelen van een set specifieke gegevens aan een persoon, waarmee deze kan worden onderscheiden van andere personen. De set specifieke gegevens die nodig is om een persoon uniek te identificeren hangt af van de context. Wanneer MijnOverheid.nl bijvoorbeeld een burger uniek wil onderscheiden wordt in Nederland het BSN gebruikt. Voor een bedrijf geldt dat het RSIN wordt gebruikt (of het KvK-nummer, of soms nummers voor specifieke beroepsgroepen, zoals bij Advocatenregister, BIG, UZI).

Voorbeeld:

In het administratieve verkeer met de Belastingdienst wordt voor het uniek herkennen van een partij twee identificerende nummers gehanteerd, het BSN voor natuurlijke personen en het RSIN voor niet-natuurlijke personen[23].

Om in het digitale verkeer de identiteit te kunnen bevestigen zijn hulpmiddelen nodig. Deze hulpmiddelen worden aangeduid met de term authenticatiemiddelen. Een voorbeeld van een authenticatiemiddel is de gebruikersnaam-wachtwoordcombinatie van DigiD. Het proces waarin een authenticatiemiddel als hulpmiddel voor identificatie wordt gebruikt, wordt aangeduid met de term authenticatie. Authenticatie is het verifiëren van een geclaimde elektronische identiteit. Het proces van authenticeren wordt ondersteund door een authenticatiedienst (bijvoorbeeld de dienst DigiD in beheer bij Logius). De door de authenticatiedienst vastgestelde (administratieve) identiteit, is vastgesteld met een bepaalde mate van zekerheid. Deze zekerheid is mede afhankelijk van het gebruikte authenticatiemiddel. Zo heeft DigiD met

[23] Sinds 2010 wordt door het Handelsregister het fiscaalnummer aangeduid met de term RSIN (rechtspersonen en samenwerkingsverbanden informatienummer). De Belastingdienst identificeert overigens ook nog rechtspersonen met een fi-nummer n plaats van met een RSIN, omdat ze bv. niet bij (de Nederlandse) KvK ingeschreven zijn.

gebruikmaking van een aanvullende SMS-code een hogere zekerheid, dan alleen de gebruikersnaam en wachtwoord combinatie.

In Europees verband is een standaard ontwikkeld om vergelijkbare zekerheidsniveaus eenduidig te beschrijven, genaamd STORK. Het moge duidelijk zijn dat de betrouwbaarheid van de authenticatiedienst zelf onomstotelijk vast moet staan, omdat een dienstaanbieder er 'blind' op moet kunnen vertrouwen dat identiteit door de authenticatiedienst met de bijbehorende mate van zekerheid is vastgesteld. Dit vertrouwen wordt getoetst op basis van regelgeving en toezicht daarop.

Ad b. Wat mag je?

Deze vraag wordt gesteld indien een persoon niet voor zichzelf, maar voor een andere partij (belanghebbende) de digitale dienst wil afnemen. Dan zal de dienstaanbieder willen weten of deze persoon wel bevoegd is om namens de belanghebbende partij te mogen handelen. De bevoegdheid of autorisatie kan gebaseerd zijn op een wettelijke vertegenwoordiging (bijvoorbeeld bewindvoerder of curator) of op een door de belanghebbende verstrekte volmacht. Om in het digitale verkeer geautomatiseerd de bevoegdheid te kunnen vaststellen, is het nodig dat:

- wettelijke vertegenwoordiging geautomatiseerd raadpleegbaar is.
- volmachten in een digitale vorm in een machtigingsregister worden vastgelegd.

Op dit moment zijn nog lang niet alle vormen van wettelijke vertegenwoordiging raadpleegbaar, behoudens de bestuurdersrollen van ingeschreven niet-natuurlijke personen in het Handelsregister. Voor de betrouwbaarheid van middelen is het noodzakelijk dat bij het uitgeven van middelen toetsing aan het Handelsregister (bij niet-natuurlijke personen) en het GBA (bij natuurlijke personen) plaatsvindt.

Voor de registratie van de volmachten worden machtigingenregisters ontwikkeld, bijvoorbeeld de voorziening DigiD Machtigen. De houder van zo'n register kan dan een verklaring afgeven, waarin is opgenomen dat een gemachtigde partij bevoegd is om te handelen namens een belanghebbende voor een bepaalde dienst. Op basis van deze verklaring kan dan de dienstaanbieder vaststellen of de handelende partij bevoegd is. Net als een authenticatiedienst moet ook het gestelde vertrouwen in de houder van een machtigingsregister hoog zijn. Ook hiervoor is regelgeving en toezicht vereist.

Bijlage 2: Inhoud afsprakenstelsel

Werking van het stelsel

- Opzet stelsel (definities, begrippen, werking)
- Architectuur (er moet een standaard worden vastgesteld waaraan middelen en voorzieningen moeten kunnen voldoen, en waarop architecten van organisaties zich kunnen baseren voor de e-dienstenontwikkeling, die de ontkoppeling mogelijk maakt (standaard voor ontkoppeling tussen de authenticatiemiddelen infrastructuur en de diensten infrastructuur). Op basis van de standaard kunnen bestaande oplossingen aan het stelsel worden getoetst en wel of niet daarin worden opgenomen.
- Het vastleggen en ontwikkelen van een handreiking voor het vaststellen van benodigde niveaus van dienstverlening en een toetsingskader om de middelen te classificeren.
- Bericht- en (ont)koppelvlak specificaties (DV-HM, HM-AD, HM-MR, buitenland, associatiebewijzen)
- Technische voorzieningen om privacy te borgen (omnummeringsvoorzieningen en vastleggen minimal disclosure principe)
- Authenticatie (betrouwbaarheidsniveaus)
- Bevoegdheid (machtigingen)
- Wilsuiting (digitale handtekening, ondertekendienst)
-

Vertrouwen generiek

- Toetreden
- Privacy
- Informatie beveiliging
- Toezicht en sanctiebeleid
- Schadebeperking en herstel
- Uittreden

Vertrouwen per rol

Per rol beschrijven:

	normen	toezicht
toetreden		
operationele beheersing		
uittreden		
servicelevel		
aansprakelijkheid		
gebruikersvoorwaarden		

Governance/ beheer en toezicht

- Besturingsmodel
- Changes en ontwikkeling
- Relatie met bestaande governance structuren

Businessmodel/financiering

- Bekostiging beheerorganisatie
- Evt. verrekening binnen stelsel

Aanvullend op het Afsprakenstelsel worden toelichtende documenten opgesteld, zoals:

- Use cases (praktijk voorbeelden)
- Operationeel handboek

Bij de uitwerking van deze onderdelen zal er gekeken naar relevante (juridische) kaders (zoals de wet Markt en Overheid, de

Europese verordening.) en bestuurlijke afspraken en regelgeving (zoals Paspoortwet en Wet of de Identificatieplicht, Wet op de rijvaardig- en rijbevoegdheid).

Aanvullend wordt ingegaan op de generieke uitgangspunten:

- Privacy
- Interoperabiliteit
- Toekomstvastheid
- Gebruiksgemak
- Interoperabiliteit

Bijlage 3: Overzicht incidenten

Hieronder een greep uit de nieuwsberichten van het afgelopen half jaar m.b.t. problemen met veiligheid van digitale informatie, datalekken/ wachtwoorden in de semi-publieke en private sector.

http://www.omroepbrabant.nl/?news/173054732/Diagnostiek+voor+U+wijst+vooral+naar+anderen+na+lekke+website.aspx
Lek Cyberlab: Cyberlab is een beveiligde internetapplicatie, waarin laboratoriumuitslagen en uitslagen van functieonderzoeken worden ingevoerd. Met Cyberlab kunnen aanvragers, die tevens geregistreerd gebruiker zijn, nog sneller beschikken over de resultaten van de eigen patiënten. Het is ook mogelijk om online toegang te krijgen tot patiënten behorende tot de eigen huisartsenpraktijk (dus van de collega huisartsen).

http://www.nu.nl/internet/2880357/dertien-universiteiten-getroffen-beveiligingslek.html
Dertien universiteiten blijken kwetsbaar geweest te zijn voor een datalek in de website. In sommige gevallen waren persoonsgegevens toegankelijk.

http://www.nu.nl/internet/2740606/200000-e-mailadressen-gestolen-database-philips.html
Een hacker stelt meer dan 200.000 e-mailadressen en telefoonnummers te hebben verkregen via een Philips-server waarop marketingsites werden gehost.

http://www.nu.nl/internet/2889724/lek-in-website-knvb.html
De site voetbal.nl van de KNVB heeft enige tijd een lek vertoond, waardoor onbevoegden bij gegevens van KNVB-leden konden komen.

http://www.nu.nl/internet/2885020/hacker-kan-meekijken-met-webcam-kinderdagverblijf.html
Een 16-jarige jongen is erin geslaagd het systeem van een kinderdagverblijf te hacken en zo via een webcam live mee te kijken naar spelende en slapende kinderen. Reitsma laat aan NU.nl weten dat hij via een SQL-injectie toegang kreeg tot een tabel met inlognamen en wachtwoorden die niet versleuteld waren opgeslagen.

http://www.nu.nl/internet/2847807/vodafone-slaat-wachtwoorden-onversleuteld.html
Vodafone slaat wachtwoorden van klanten onversleuteld op. De database is wel beveiligd, maar wachtwoorden worden in 'plain text' opgeslagen.

http://www.nu.nl/internet/2830058/mogelijk-wachtwoorden-gestolen-bij-lastfm.html
Muziekdienst Last.fm meldt op zijn website dat de site het lek van gebruikerswachtwoorden onderzoekt.

http://www.nu.nl/internet/2737997/wachtwoorden-kpn-klanten-gepubliceerd.html
Er is vrijdagmiddag een bestand online gezet met de gegevens van ruim 500 KPN-klanten. In het document staan ook e-mailadressen en wachtwoorden. KPN lijkt de mailservers offline te hebben gehaald.

http://www.nu.nl/internet/2641559/wachtwoorden-raad-van-state-gelekt.html
Wachtwoorden om in te kunnen loggen in het systeem van de Raad van State, het belangrijkste adviesorgaan van de regering, zijn gemakkelijk via Google te vinden.

http://www.nu.nl/internet/2677824/sites-npo-en-radiostations-lekken-gegevens-23-miljoen-mensen.html
Door een lek in het beheersysteem van publieke omroepen en radiostations zijn de gegevens van 2,3 miljoen mensen toegankelijk.

http://www.nu.nl/internet/2317685/wachtwoordbeleid-bij-grote-websites-zwak.html
85 procent van de door de Consumentenbond onderzochte grote websites dwingt sterke wachtwoorden niet af. De bond noemt het wachtwoordbeleid zwak.

http://www.nu.nl/internet/2851128/scholen-niet-opgewassen-hackende-leerlingen.html
Nederlandse middelbare scholen erkennen dat systemen regelmatig gehackt worden door leerlingen. Dit is vooral mogelijk door onkunde van leraren en scholen.

http://www.nu.nl/internet/2743211/klantgegevens-apothekers-slecht-beveiligd.html
Het College bescherming persoonsgegevens (CBP) heeft ingegrepen bij 15 instellingen, omdat die de beveiliging van persoonsgegevens niet op orde hadden. Het ging onder andere om websites van apothekers en een gemeente, zo meldde een woordvoerster vrijdag.

http://www.nu.nl/internet/2828977/linkedin-reset-accounts-lekken-wachtwoorden.html
LinkedIn heeft de accounts waarvan het wachtwoord gelekt is tijdelijk afgesloten. Getroffen gebruikers krijgen een e-mail van het sociale netwerk. Dat heeft het bedrijf laten weten in een blogpost <http://blog.linkedin.com/2012/06/06/linkedin-member-passwords-compromised/> naar aanleiding van een hack. 6,5 miljoen wachtwoorden van LinkedIn-accounts zouden zijn buitgemaakt, maar dat nummer wordt door het sociale netwerk zelf niet bevestigd. Wel erkent LinkedIn dat er 'een aantal wachtwoorden' is buitgemaakt. De getroffen accounts zijn tijdelijk afgesloten. Gebruikers die proberen in te

loggen krijgen de melding dat hun wachtwoord niet geldig is.

http://www.nu.nl/games/2521919/hack-playstation-network-kost-sony-120-miljoen-euro.html
Sony denkt meer dan 120 miljoen euro verloren te hebben met de hack waardoor het Playstation Network grofweg een maand offline is geweest. Dat laat het bedrijf maandag aan investeerders weten.

http://www.thuiswinkel.org/mededelingen/alle-mededelingen/fraude-op-marktplaats-en-speurders
Op zondag 22 april heeft op marktplaats <http://www.marktplaats.nl/> een advertentie gestaan waarvan het leek of deze van Expert <http://www.expertwinkels.nl/> afkomstig was.

http://marktplaatsoplichting.nl/phishing/voorkom-phishing-laat-u-niet-beetnemen/ <http://marktplaatsoplichting.nl/phishing/voorkom-phishing-laat-u-niet-beetnemen/>
ICS cardservices de uitgever van creditcards zoals Mastercard Bijenkorf card) , Visa heeft een waarschuwing op de website geplaatst.

http://www.nu.nl/internet/2829739/tweede-kamer-eist-uitleg-minister-hack-linkedin.html
De Tweede Kamer wil voor het einde van volgende week uitleg over de hack bij LinkedIn van minister Liesbeth Spies (Binnenlandse Zaken).

http://www.nu.nl/internet/2854835/nederlanders-passen-wachtwoorden-relatief-vaak.html
Nederlanders maken zich meer zorgen over cybercriminaliteit dan gemiddeld in Europa. In Nederland worden wachtwoorden dan ook vaker aangepast. Dat blijkt uit een onderzoek <http://europa.eu/rapid/pressReleasesAction.do?reference=IP/12/751&format=HTML&aged=0&language=EN&guiLanguage=en> van de Europese Unie.

http://www.nu.nl/internet/2346352/helft-gaat-slordig-met-wachtwoorden.html
Zeker de helft van de Nederlanders gaat slordig om met wachtwoorden. Een op de tien mensen gebruikt zelfs overal hetzelfde wachtwoord.

http://www.nu.nl/internet/2858570/boete-bedrijven-bij-verlies-data.html
Bedrijven die veel persoonsgegevens beheren kunnen in de toekomst een boete tegemoet zien als door nalatigheid gegevens op straat komen te liggen. Dat staat in een wetsvoorstel van staatssecretaris Fred Teeven van Veiligheid en Justitie dat vrijdag door de ministerraad is goedgekeurd.

Dit is een uitgave van:
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Postbus 20011 | 2500 EA Den Haag
www.rijksoverheid.nl

Oktober 2012