Programma eID
Afsprakenstelsel

Stakeholders, belangen en ontwerpeisen programma eID

Versie: 1.0

Datum: 21 januari 2014

Status: Definitief

Colofon

Programma eID
Deelproject Afsprakenstelsel

Bezoekadres:
Herman Gorterstraat 5
Utrecht

Versie	1.0
Opdrachtgever	Stuurgroep eID
Bijlage(n)	
Aantal pagina's	18
Exemplaarnummer	

Inhoud

Inleiding

In dit document zijn de overkoepelende doelstellingen van het eID Stelsel beschreven. Daarna is beschreven welke stakeholders er zijn voor het eID Stelsel en wat hun belang is.

In Hoofdstuk 3 is vervolgens beschreven welke ontwerpeisen er zijn voor het stelsel. Deze eisen zijn gerelateerd aan het belang van de verschillende stakeholders.

In Hoofdstuk 4 zijn de ontwerpeisen verder uitgewerkt.

1 Doelstelling eID Stelsel

Bij de totstandkoming van een publiek-privaat stelsel voor elektronische identificatie, authenticatie en autorisatie (eID Stelsel) werkt een aantal partijen nauw samen. Iedere organisatie brengt daarbij haar eigen visie en zienswijze in op de wijze waarop elektronische identificatie toekomstvast en veilig geregeld kan worden. Om de verschillende invalshoeken inzichtelijk te maken worden in de volgende paragraaf de stakeholders en hun belangen beschreven.

Doelstellingen eID Stelsel

- Een toekomstbestendige en betrouwbare elektronische identiteitsinfrastructuur creëren die gebruikt kan worden door zowel publieke als private DIENSTAANBIEDERS en die publiek-privaat beheerd en doorontwikkeld wordt.
- Mogelijk maken dat publieke DIENSTAANBIEDERS de toegang en afhandeling van online dienstverlening vanaf 2015 via het eID Stelsel kunnen inrichten waardoor zij de doelstelling 'Digitaal 2017' uit het regeerakkoord kunnen realiseren: *Bedrijven en burgers kunnen in 2017 zaken met de overheid digitaal afhandelen.*

2 Belangrijke stakeholders en hun belang

De implementatie van het eID Stelsel in Nederland raakt vele onderdelen van de overheid en de private sector. Voor een flink aantal overheidsorganisaties geldt dat zij nieuwe diensten digitaal kunnen ontsluiten omdat het eID Stelsel identificatie en gegevensuitwisseling op een hoger betrouwbaarheidsniveau mogelijk maakt. Voor private organisaties is dit ook zeer interessant.

Zowel publieke als private partijen spelen in de huidige situatie een rol in het proces van realisatie en implementatie van EID-MIDDELEN. Bij de komst van het eID Stelsel maken zij ieder de balans op of en op welke manier zij deze voorzieningen willen continueren.

Deze paragraaf bevat een overzicht van belangrijke stakeholders en wat hun belang is bij het eID Stelsel en wat eventuele bedenkingen zijn. Hierbij is een onderscheid gemaakt in stakeholders die beleidsmatig een belang hebben, stakeholders die binnen het eID Stelsel diensten willen aanbieden (EID-DEELNEMERS), en stakeholders die gebruik willen maken van het eID Stelsel (DIENSTAANBIEDERS).

2.1 Beleidsverantwoordelijke ministeries

Er zijn twee ministeries beleidsverantwoordelijk voor het eID Stelsel.

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (MinBZK)
Dit ministerie vervult de rol van hoofdopdrachtgever (DG Bestuur en Koninkrijksrelaties) van het eID-programma en is verantwoordelijk voor de realisatie van 'Digitaal 2017'.

Ministerie van Economische Zaken (MinEZ DG UITVOERING)
Dit ministerie is als tweede verantwoordelijk voor het eID-programma. EZ is in het bijzonder betrokken als schakel richting de markt om de verhouding markt/overheid te borgen. EZ heeft belang bij een eID Stelsel vanwege de kansen die het eID Stelsel biedt voor private organisaties. EZ is deelnemer en kennisleverancier in de ontwikkeling van het eID Stelsel, ook vanuit de rol als verantwoordelijk ministerie voor de authenticatievoorziening eHerkenning. Onder de verantwoordelijkheid van het ministerie valt een aantal organisaties die in de rol van DIENSTAANBIEDER gebruik zal maken van de voorzieningen in het eID Stelsel.

2.2 Belanghebbende organisaties

Er zijn verschillende overige organisaties die belang hebben bij het eID Stelsel.

Belangenorganisaties

Alle ontwikkelingen op het gebied van (elektronische) identiteit, authenticatie en machtigen van burgers hebben mogelijke impact op de privacy. Bij toegang tot persoonsgegevens (zoals burgerservicenummer (BSN), adres en leeftijd), al dan niet via diensten, dient grote zorgvuldigheid in acht genomen te worden. Het programma betrekt daarom belangen- en maatschappelijke organisaties, zoals het College Bescherming Persoonsgegevens (CBP), de Consumentenbond, Bits of Freedom, de Autoriteit Consument en Markt (ACM) en toonaangevende media. Ideeën en denkbeelden, maar ook voorgestelde (deel)oplossingen, worden zo in een vroegtijdig stadium vanuit verschillende gezichtspunten gedeeld en besproken. Verder worden deze organisaties betrokken bij Privacy Impact Analyses en geconsulteerd in het kader van het wetgevingstraject.

Wetenschappers en experts

Het is belangrijk om bij de ontwikkeling van het eID Stelsel partijen te betrekken die beschikken over specialistische kennis. Het stelsel gebruikt namelijk nieuwe innovatieve technologie, waarbij niet alle onderdelen daarvan grootschalig in de praktijk zijn bewezen.

Bij de invoering van de OV-chipkaart toonde onderzoek van de Radboud Universiteit Nijmegen aan dat er diverse issues waren op het gebied van beveiliging. De wetenschap kan daarom een toetsende rol vervullen bij de ontwikkeling van het eID Stelsel en tevens adviseren bij het maken van keuzes bij complexe technologisch vraagstukken. Hetzelfde geldt voor organisaties (publiek en privaat) die ervaring hebben met onder andere chiptechnologie, identificatiemiddelen en informatiebeveiliging. Het Nationaal Bureau voor Verbindingsveiligheid (NBV) adviseert de Rijksoverheid bij beveiliging van bijzondere informatie. Bij de Basisadministratie Persoonsgegevens en Reisdocumenten (BPR) is expertise aanwezig op het gebied van identiteitsdocumenten.

Manifestgroep

De Manifestgroep is een samenwerking tussen verschillende overheidsorganisaties met een uitvoerende taak.

De leden hebben zich ten doel gesteld om gezamenlijk op te trekken om de dienstverlening aan burgers en bedrijven te verbeteren. Deze dienstverlening is digitaal waar dat kan en persoonlijk waar nodig.

Het is belangrijk dat er bij de verschillende overheidspartijen een groot draagvlak ontstaat voor de implementatie van het eID Stelsel. De manifestgroep kan een belangrijke bijdrage aan de bekendheid van en het draagvlak voor het eID Stelsel.

2.3 Publieke eID-deelnemers

Logius

Logius is de beheerder van diverse toegangsvoorzieningen die publiek en privaat gebruikt worden, zoals DigiD, eHerkenning, PKIoverheid en het portaal MijnOverheid.

Logius heeft op verzoek van BZK/B&I de consultatiefase begeleid, waarin de uitgangpunten van de Strategische Verkenning getoetst zijn en mogelijke interesse bij (publieke en private) partijen in deelname aan het eID Stelsel geïnventariseerd is. Verder treft Logius voorbereidingen voor de inrichting van de (tijdelijke) beheerorganisatie voor het eID Stelsel en werkt het de stelselafspraken en de inrichting van de governance uit. De ervaring die Logius heeft in het beheer van het vergelijkbare stelsel eHerkenning komt daarbij goed van pas. Tot slot richt Logius de communicatiefunctie binnen het eID-programma in.

Gemeenten

De gemeenten pleiten voor een realistisch tijdpad voor de invoering van één van de mogelijke eID-middelen: de DigiD-kaart. Een ‘dubbele kaart’ (DigiD-kaart en WID) vindt de meerderheid niet wenselijk, onder andere vanwege de kosten voor de burger en het gebruikersongemak.

Als de huidige wettelijke toegestane identiteitsdocumenten niet gebruikt kunnen gaan worden voor digitale transacties, dan zien de gemeenten mogelijkheden om de nieuwe DigiD-kaart geschikt te maken om de WID-functie te vervullen in de fysieke wereld (bijvoorbeeld door het plaatsen van een pasfoto op het document). Ook kan bijvoorbeeld een attribuut als rijbevoegdheid op de kaart opgenomen worden.

De uitvoerbaarheid voor gemeenten is verder afhankelijk van de kostendekkendheid en de kostprijs. Gemeenten kunnen hierop realistische input geven.

2.4 Private eID-deelnemers

Diverse private partijen hebben interesse getoond in deelname aan het eID Stelsel en een aantal daarvan is inmiddels betrokken geweest bij de marktconsultaties die hebben plaatsgevonden. Private partijen hebben een eigen afweging bij eventuele deelname aan het eID Stelsel. De overheid streeft ernaar om nadrukkelijk de samenwerking op te zoeken met private partijen en de ontwikkeling van nieuwe diensten en middelen zoveel mogelijk aan de markt over te laten.

Leveranciers eHerkenning

eHerkenning is een voorziening waarmee ondernemers zaken kunnen doen met de overheid. eHerkenning is georganiseerd als publiek-privaat stelsel waarin leveranciers (eHerkenningspartijen) transactiediensten leveren aan ondernemers.

De eHerkenningspartijen zijn bekend met het perspectief dat er één eID Stelsel komt. Ze onderschrijven de noodzaak om kwalitatieve normen op te stellen voor de registratie van machtigingen voor publieke dienstverlening en digitale handtekeningen.

Waar de eHerkenningspartijen zich zorgen over maken, is wat de komst van het stelsel betekent voor de huidige diensten die zij op dit moment aanbieden. De leveranciers benadrukken dat het uitgangspunt 'privaat wat kan, publiek wat moet' pleit voor overheidsregulatie, maar niet per definitie voor overheidsuitvoering. Het is belangrijk dat er een helder afwegingskader komt op basis van juridische en beleidsmatige criteria.

Er bestaat ook de vrees dat als de overheid in het eID Stelsel vergelijkbare diensten gaat aanbieden als de eHerkenningspartijen, het principe *level playing field* zou kunnen verdwijnen. Dit hangt onder meer af van de (toekomstige) kostprijsberekening van de voorzieningen die de overheid zou kunnen aanbieden. Als in de berekeningswijze alle voorinvesteringen worden meegenomen, maken de eHerkenningspartijen zich al minder zorgen over oneerlijke concurrentie, omdat zij voorspellen tegen lagere tarieven dan de overheid diensten aan te kunnen bieden.

De eHerkenningspartijen hebben behoefte aan een vergelijking van het eID Stelsel met eHerkenning. Ze verwachten dat een aantal vraagstukken die in dit verband spelen, al opgelost zijn in de recente release (1.7) van eHerkenning.

(ICT) Leveranciers

Volgens potentiële leveranciers van eID-diensten is het stelsel geslaagd als binnen twee jaar een aantal grote publieke en private partijen is aangesloten en op grote schaal interessante diensten aanbiedt voor gebruikers. Een tweede belangrijke succesfactor van het stelsel zou kunnen zijn dat hiermee identiteitsfraude daalt.

Voor wat betreft de businessmodellen die commerciële eID-deelnemers zich bij de toekomstige eID-middelen kunnen voorstellen is de wijze van attribuutverstrekking interessant en ook de rol die zij kunnen spelen in het totstandkomings-, uitgifte- en beheerproces van een fysieke kaart.

Als je de gegevens set op de eID-middelen beperkt, kan er digitaal een veel rijkere attributenset ontsloten worden die dat ook mogen doen volgens de stelselnormen. Dit kan interessante nieuwe businessmodellen opleveren.

De leveranciers adviseren om uit te gaan van de technologie die nu al beschikbaar is ('the latest proven state of the art').

Verschillende leveranciers hebben innovatieve deeloplossingen gerealiseerd op basis van bijvoorbeeld PKI-certificaten. Zij onderstrepen dat deelname aan het eID Stelsel voor hen als vliegwiel kan werken om bekendheid te geven aan deze oplossingen.

De leveranciers hebben behoefte aan een scherpe(re) definitie van het begrip eID. Zij onderstrepen dat er in de digitale wereld veel vormen van elektronische identiteiten mogelijk zijn zoals B2B, B2C, etc.

De leveranciers vragen om bij de uitwerking van de rollen in het eID Stelsel rekening te houden met de IT-dienstverlener. Deze zorgt er bijvoorbeeld voor dat gemeenten kunnen aansluiten op een eID-makelaar. Standaardisatie op koppelvlakken is hierbij van belang. Overheid en markt kunnen de mogelijkheid benutten om te kijken of certificering voor IT-dienstverleners ingevoerd kan worden.

De leveranciers zijn benieuwd hoe de wet Markt en Overheid toegepast wordt om *level playing field* te garanderen. De kwestie van aansprakelijkheid ('wat gebeurt er als het fout gaat in het stelsel?') moet worden opgelost.

Tot slot moet er een aantal belangrijke knopen worden doorgehakt over privacy. Een aantal leveranciers geeft aan dat bij de uitgifte van EID-MIDDELEN het uitgangspunt van dataminimalisatie zou moeten gelden. Dit houdt in dat je zo min mogelijk gegevens standaard op het middel meegeeft en dat dit in ieder geval bij een fysieke verschijningsvorm geen persoonskenmerken zijn zoals een pasfoto of naam. Een neutraal EID-MIDDEL kan op die manier bij verlies of diefstal niet aan iemands fysieke identiteit gekoppeld worden.

2.5 Publieke DIENSTAANBIEDERS

Er zijn verschillende ministeries, publieke uitvoeringsorganisaties en andere publieke instanties die belangen hebben binnen het eID Stelsel.

Ministerie van Veiligheid en Justitie (MinV&J)

Het eID Stelsel biedt mogelijkheden voor verbetering en innovatie in de digitale dienstverlening binnen diverse justitiële ketens. De rechtspleging en juridische beroepen hebben grote behoefte aan standaarden met betrekking tot de borging van de authenticiteit en integriteit van elektronische bewijsstukken die bij elektronische transacties tot stand komen of worden uitgewisseld.

Een belangrijk speerpunt voor het Ministerie van Veiligheid en Justitie is een betrouwbare, praktisch handzame en bruikbare elektronische handtekening binnen het bereik van burgers en professionals te brengen, die aansluit bij de hedendaagse elektronische dienstverlening via webportalen en webservices.

Het Ministerie van Veiligheid en Justitie levert een bijdrage aan de voorbereiding van de conceptwetsvoorstellen die nodig zijn voor de inrichting van het eID Stelsel (wijziging Telecomwet, Wet op de identificatieplicht, etc.).

Ministerie van Volksgezondheid, Welzijn en Sport (MinVWS)

VWS heeft belang bij een AUTHENTICATIEMIDDEL met een hoog betrouwbaarheidsniveau als het gaat om uitwisseling van elektronische informatie in de zorg, bijvoorbeeld bij elektronische inzage in medische gegevens voor consumenten en zorgprofessionals.

Een ander belang van VWS is dat leeftijdsverificatie wordt uitgevoerd bij de aankoop van tabak of alcohol (leeftijdsgebonden middelen), waarbij het bedrijfsleven een wettelijk verplichte handeling uitvoert. Daarnaast geeft het CIBG (uitvoeringsorganisatie binnen VWS) de Unieke Zorgverlener Identificatiepas (UZI-pas) uit. Mogelijk kan informatie over beroepsgroep worden ontsloten via de DigiD-kaart, waardoor een aparte UZI-pas (met bijbehorende afgifte- en beheerprocessen) kan vervallen.

Vereniging van Nederlandse Gemeenten (VNG) en Nederlandse Vereniging Voor Burgerzaken (NVVB)

Gemeenten, vertegenwoordigd door de VNG en meer specifiek de NVVB, zijn in twee rollen bij de DigiD-kaart betrokken: enerzijds als mogelijke uitgever van de DigiD-kaart en anderzijds als DIENSTAANBIEDER (bijvoorbeeld bij de registratie van de verhuizing van een burger).

Voor gemeenten is het eID Stelsel geslaagd als het meerwaarde oplevert voor burgers en het onterecht gebruik van overheidsvoorzieningen voorkomt. Als huidige voorzieningen zoals DigiD en eHerkenning opgenomen worden in het stelsel, dan is het logisch dat gemeenten er ook gebruik van gaan maken. In diverse kringen (zoals de NVVB en VNG) zal verkend worden welke nieuwe vormen van gemeentelijke dienstverlening mogelijk worden door de invoering van het stelsel. Zo kunnen lokale passen als de stadspas en de milieupas overbodig worden. Via eHerkenning kan een vroedvrouw aangifte doen van een geboorte en een begrafenisondernemer van een overlijden. Aanverwante nieuwe mogelijkheden kunnen in het eID Stelsel worden uitgedacht.

Belastingdienst

De Belastingdienst heeft als DIENSTAANBIEDER een groot belang bij een eID Stelsel en een voldoende hoog niveau EID-MIDDEL. De Belastingdienst heeft het initiatief genomen om de ontwikkelingen in het burger- en bedrijvendomein bij elkaar te brengen onder de paraplu van één stelsel. Betrouwbare toegang is van belang bij de steeds verder toenemende digitale dienstverlening van de Belastingdienst. Het eID Stelsel maakt betere fraudepreventie mogelijk en biedt een *fallback* doordat mensen en organisaties zelf kunnen kiezen met welk EID-MIDDEL ze op een bepaald betrouwbaarheidsniveau online zaken willen doen. Mocht een middel onverhoopt niet gebruikt kunnen worden, dan logt iemand in met een ander middel. Zo is er een betere garantie voor de continuïteit van digitale dienstverlening.

Binnen het eID Stelsel wordt het ook mogelijk om de registratie van machtigingen en wettelijke vertegenwoordiging te ontsluiten, zodat (alleen) bevoegde derden toegang hebben tot gegevens van burgers en bedrijven en voor hen handelingen kunnen verrichten.

Rijksdienst voor het wegverkeer (RDW)

RDW heeft behoefte aan authenticatie, autorisatie en rechtsgeldige digitale ondertekening met een hoger betrouwbaarheidsniveau om verdere digitalisering van de dienstverlening op het gebied van overschrijven en schorsen van voertuigen mogelijk te maken.

Uitvoeringsinstituut Werknemersverzekeringen (UWV)

Het UWV heeft in de eerste plaats belang bij een robuuste infrastructuur voor authenticatie omdat UWV grootgebruiker is van DigiD en gebruik van de e-dienstverlening voor UWV-klanten in het WW-proces verplicht is. Het niet beschikbaar zijn van een authenticatievoorziening is zeer verstorend.

Daarnaast heeft UWV belang bij een authenticatie op een hoger betrouwbaarheidsniveau. Concrete nieuwe diensten die UWV voor ogen heeft zijn het bieden van toegang tot het digitaal dossier voor haar klanten waar het gaat om meer gevoelige gegevens zoals in het sociaal medisch proces in verband met arbeidsongeschiktheid. In dat geval is het hoogste betrouwbaarheidsniveau vereist. Ook de werkgever en behandelende medici kunnen betrokken zijn in dit proces. Het is daarom voor UWV bij uitstek van belang dat er een algemeen beschikbare infrastructuur voor authenticatie is van hoog niveau. Verder wil UWV bezwaar- en beroepsprocessen zowel in de communicatie met klanten als met justitie digitaliseren. Ook daarvoor is authenticatie met een hoog betrouwbaarheidsniveau vereist.

Sociale Verzekeringsbank (SVB)

De SVB voert in opdracht van de overheid de volksverzekeringen in Nederland uit: kinderbijslag, AOW-pensioen en nabestaandenuitkering ANW. In het kader van de elektronische dienstverlening richting de volksverzekerden is het voor SVB van belang dat de (elektronische) identiteit betrouwbaar vastgesteld kan worden. Verder biedt het eID Stelsel de mogelijkheid om nieuwe elektronische diensten te ontwikkelen waarvoor een hoog betrouwbaarheidsniveau noodzakelijk is.

2.6 Private DIENSTAANBIEDERS

Een groot aantal private partijen heeft als aanbieder van digitale diensten belang bij het eID Stelsel. Zij hebben er belang bij dat er EID-MIDDELEN in de markt komen die breed door burgers/consumenten worden gebruikt en die ook gebruikt kunnen worden om digitale diensten van private partijen af te nemen. Zij zullen steeds een afweging maken tussen veiligheid (risico's), gebruikersgemak en de kosten die ze moeten maken.

Financiële DIENSTAANBIEDERS

Voor verschillende DIENSTAANBIEDERS in de financiële sector betekent de ontwikkeling van het eID Stelsel en hoogwaardige authenticatiemiddelen een interessante mogelijkheid om de eigen dienstverlening te optimaliseren. Zo wil Bureau Kredietregistratie (BKR) klanten digitaal inzicht kunnen geven in de vastgelegde klantgegevens. Het Standaardisatie Instituut voor Verzekeringen in de Intermediairsbranche (SIVI) en de Bond van Verzekeraars willen het authenticatie- en autorisatieproces in de verzekeringsbranche standaardiseren en zo één branchebreed inlogmechanisme creëren. Ook vanuit de bancaire wereld zijn er aanknopingspunten. ABN Amro heeft interesse om de door hen geregistreerde financiële identiteit ook breder in te zetten voor andere DIENSTAANBIEDERS. ING ziet met name kansen om het onboarding-proces (inschrijven nieuwe klant) digitaal te laten verlopen met een EID-MIDDEL op hoger betrouwbaarheidsniveau (met een WID-status).

Banken en financiële DIENSTAANBIEDERS moeten voldoen aan een wettelijke zorgplicht zoals vastgelegd in de Wet Financieel Toezicht (WFT en WWFT). Deelname aan het eID Stelsel kan voor deze sector interessant zijn als zij op het gebied van authenticatie, autorisatie en verificatie op attribuutniveau (leeftijd, kredietwaardigheid etc.) ontzorgd worden en op het gebied van klantidentificatie aan hun wettelijke eisen kunnen voldoen. Het eID Stelsel is volgens de financiële DIENSTAANBIEDERS geslaagd als er massaal gebruik van gemaakt wordt. Een belangrijke randvoorwaarde is de gegarandeerde en veilige beschikbaarheid van voorzieningen. Financiële DIENSTAANBIEDERS geven aan dat zij wel willen samenwerken in een soort van 'nationaal platform'.

Webwinkels

De webwinkels zijn geïnteresseerd in de mogelijkheden van het eID Stelsel en de DigiD-kaart. Of ze er ook gebruik van zullen maken hangt af van de gebruiksvriendelijkheid, snelheid, veiligheid en kosten per transactie (geen fee per transactie). Het eID Stelsel is voor hen geslaagd als de digitale processen net zo gemakkelijk en goedkoop verlopen als in de fysieke wereld, als klanten er massaal gebruik van maken, en als de dienstverlening zo goed als gratis is voor de DIENSTAANBIEDERS. De winkels zullen altijd de afweging maken tussen veiligheidsrisico's en gebruiksgemak voor de klant. De webwinkels adviseren om goed na te denken hoe je aansluiting voor hen interessant maakt. Verificatie (leeftijd) kan interessant zijn; de verkleining van de digitale sleutelbos is dat veel minder.

2.7 Overzicht belangen stakeholders

Het eID Stelsel moet de volgende diensten mogelijk maken:

- Authenticatie met hoog betrouwbaarheidsniveau;
- Verificatie van aanvullende gegevens (attributen) zoals leeftijd;
- Ondersteuning (wettelijke) vertegenwoordiging;
- Een betrouwbare, praktisch handzame en bruikbare elektronische handtekening.

Belangen van de stakeholders die direct gevolgen hebben voor het ontwerp zijn:

- Verhogen beveiliging en betrouwbaarheidsniveau;
- Verhogen vertrouwelijkheid en zorgvuldige omgang met privacygevoelige informatie;
- Gebruikersgemak en toegankelijkheid;
- Participatie private partijen (*level playing field* in stand houden). Invulling: privaat wat kan, publiek (alleen) wat moet;
- Verbetering continuïteit digitale dienstverlening;
- Toekomstvastheid (uitbreidbaar);
- Beperken kosten.

3 Belangen

In de vorige paragraaf zijn de belangen van de verschillende stakeholders in kaart gebracht. Ieder

belang stelt eisen aan het ontwerp van het eID Stelsel.

In deze paragraaf zijn de belangen verder uitgewerkt en is in kaart gebracht welke eisen deze belangen aan het ontwerp van het eID Stelsel stellen.

Nr.	Belang	Bron
B1	**Verhogen beveiliging, betrouwbaarheid.** De toegang tot digitale diensten moet geregeld worden op een adequaat beveiligingsniveau (zoals vastgelegd in de handreiking authenticatieniveau). De ontwerpeisen die hieraan een bijdrage leveren: • E07. Ondersteunen van verschillende betrouwbaarheidsniveaus. • E22. BELANGHEBBENDE kan zelf machtigingen achteraf controleren. • E23. GEBRUIKERS hebben controle over machtigingen en gegevens. • E32. Niet meer gegevens leveren dan strikt noodzakelijk. • E33. DIENSTAANBIEDERS kunnen verantwoording afleggen. • E51. Misbruik kan eenvoudig ontdekt en opgespoord worden.	Stakeholders
B2	**Verhogen vertrouwelijkheid.** De GEBRUIKERS van het eID Stelsel moeten er op kunnen vertrouwen dat het stelsel veilig is. Alleen dan zal het stelsel breed worden toegepast. De ontwerpeisen die hieraan een bijdrage leveren: • E21. Laagdrempelig voor betrokkenen. • E22. BELANGHEBBENDE kan zelf machtigingen achteraf controleren. • E23. GEBRUIKERS hebben controle over machtigingen en gegevens. • E31. Bescherming privacy betrokkenen onderling. • E32. Niet meer gegevens leveren dan strikt noodzakelijk.	Stakeholders
B3	**Gebruiksgemak en toegankelijkheid** Deelnemers (met name burgers) begrijpen het toegangs- en vertegenwoordigingsproces en willen/durven het te gebruiken. De ontwerpeisen die hieraan een bijdrage leveren: • E02. Bruikbaar voor digitaal minder vaardigen. • E03. Derden moeten namens een DIENSTAANBIEDER digitale diensten kunnen aanbieden. • E04. Opheffen domeinscheiding burger/bedrijf. • E05. Sectoren met eigen nummers moeten ondersteund kunnen worden. • E06. Voorbereiden op aansluiten EU-middelen. • E21. Laagdrempelig voor betrokkenen. • E22. BELANGHEBBENDE kan zelf machtigingen achteraf controleren. • E23. GEBRUIKERS hebben controle over machtigingen en gegevens. • E24. Keuzevrijheid in aanschaf en gebruik.	Stakeholders
B4	**Participatie private partijen / marktwerking** In het eID Stelsel mogen zowel publieke partijen als ook private partijen participeren. • Private partijen mogen eID-diensten aanbieden aan publieke en private DIENSTAANBIEDERS. • Private DIENSTAANBIEDERS mogen gebruik maken van de eID-diensten van publieke EID-DEELNEMERS. • GEBRUIKERS kunnen zowel bij private als publieke partijen AUTHENTICATIEMIDDELEN aanschaffen. • Publiek wat moet, privaat waar het kan De ontwerpeisen die hieraan een bijdrage leveren: • E03. Derden moeten namens een DIENSTAANBIEDER digitale diensten kunnen aanbieden. • E05. Sectoren met eigen nummers moeten ondersteund kunnen worden. • E06. Voorbereiden op aansluiten EU-middelen.	Stakeholders

Nr.	Belang	Bron
	• E11. Multimiddelenstrategie. • E12. Hergebruik bestaande voorzieningen. • E13. Zorg ervoor dat alle partijen gelijke kansen hebben. • E14. Businessmodel t.b.v. investeren private partijen. • E24. Keuzevrijheid in aanschaf en gebruik. • E41. Zorg voor robuustheid, flexibiliteit en veerkracht in het ontwerp. • E42. Ontkoppelen van techniek. • E43. Aansluiten op (Europese) standaarden.	
B5	**Verbeteren continuïteit digitale dienstverlening van de DIENSTAANBIEDERS** Niet meer afhankelijk zijn van één AUTHENTICATIEDIENST en/of MACHTIGINGSDIENST. Nadat een EID-DEELNEMER gehackt is of in geval van cyberaanvallen moet het stelsel blijven werken. Het eID Stelsel moet (zoveel mogelijk) kunnen meebewegen indien de bedrijfsvoering van een DIENSTAANBIEDER wijzigt. De ontwerpeisen die hieraan een bijdrage leveren: • E11. Multimiddelenstrategie. • E32. Niet meer gegevens leveren dan strikt noodzakelijk. • E41. Zorg voor robuustheid, flexibiliteit en veerkracht in het ontwerp. • E51. Misbruik kan eenvoudig ontdekt en opgespoord worden.	Stakeholders
B6	**Toekomstvastheid (uitbreidbaarheid)** Het eID Stelsel moet een bijdrage leveren om de digitale dienstverlening op korte en lange termijn te ondersteunen. Het aantal partijen dat eID diensten gaat leveren zal sterk wisselen. Ook de techniek zal in de komende periode sterk veranderen. Het eID Stelsel moet onafhankelijk van deze veranderingen een stabiele rol kunnen blijven spelen. De ontwerpeisen die hieraan een bijdrage leveren: • E01. Ontzorgen van de DIENSTAANBIEDER. • E06. Voorbereiden op aansluiten EU-middelen. • E11. Multimiddelenstrategie. • E41. Zorg voor robuustheid, flexibiliteit en veerkracht in het ontwerp. • E42. Ontkoppelen van techniek. • E43. Aansluiten op (Europese) standaarden.	Stakeholders
B7	**Beperken van de kosten** DIENSTAANBIEDERS in zowel de private als de publieke sector moeten hoge kosten maken om AUTHENTICATIEDIENSTEN te exploiteren. Deze kosten gaan stijgen als AUTHENTICATIEMIDDELEN met een hoger betrouwbaarheidsniveau vereist zijn. Door AUTHENTICATIEMIDDELEN beschikbaar te stellen die gebruikt kunnen worden om toegang te krijgen tot een groot aantal diensten van een groot aantal DIENSTAANBIEDERS, kunnen de kosten over meerdere partijen worden verdeeld. De ontwerpeisen die hieraan een bijdrage leveren: • E01. Ontzorgen van de DIENSTAANBIEDER. • E04. Opheffen domeinscheiding burgers/bedrijf. • E11. Multimiddelenstrategie. • E12. Hergebruik bestaande voorzieningen. • E14. Businessmodel t.b.v. investeren private partijen.	Strategische verkenning

4 Ontwerpeisen voor het eID Stelsel

In deze paragraaf zijn de ontwerpeisen verder uitgewerkt. De ontwerpeisen zijn ondergebracht in de volgende clusters:

- Ontkoppelen van DIENSTAANBIEDERS
- Marktwerking stimuleren
- Gebruikersgemak bevorderen
- Privacy garanderen
- Zorgen voor een toekomstvast ontwerp
- Inrichten van toezicht en opsporing

In de sectie *Werking van het stelsel* is beschreven op welke wijze de ontwerpeisen zijn verwerkt in het ontwerp van het eID Stelsel.

4.1 Ontkoppelen van DIENSTAANBIEDERS

Nr.	Ontwerpeis	Bron
E01	**Ontzorgen van DIENSTAANBIEDERS** Ontkoppeling tussen diensteninfrastructuur van publieke- en private DIENSTAANBIEDERS en de infrastructuur van EID-MIDDELEN. DIENSTAANBIEDERS 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. De leveranciers van EID-MIDDELEN worden ook ontzorgd omdat deze niet op iedere DIENSTAANBIEDER afzonderlijk hoeven aan te sluiten.	Strategische verkenning
E02	**Bruikbaar voor digitaal minder vaardigen** Digitaal minder vaardigen moeten ook de gelegenheid hebben om gebruik te maken van de diensten die de overheid aanbiedt.	Strategische verkenning
E03	**Derden moeten namens een DIENSTAANBIEDER digitale diensten kunnen aanbieden.** Een publieke DIENSTAANBIEDER is niet altijd in staat om goed aan te sluiten op de processen van de GEBRUIKER. Om er toch voor te zorgen dat deze aansluiting wordt gerealiseerd wil de GEBRUIKER (of DIENSTAANBIEDER) vaak gebruik maken van een derde partij. Deze is vaak veel beter in staat om kwaliteit aan de digitale diensten toe te voegen en hiermee het gebruikersgemak te vergroten.	Strategische verkenning
E04	**Opheffen domeinscheiding burgers / bedrijven** In Nederland kennen we inmiddels ruim 850.000 eenmanszaken. Bij eenmanszaken komen de rollen van burger en bedrijf samen in één persoon met één burgerservicenummer (BSN). Het moet mogelijk worden dat een persoon zich voor burgerzaken en voor bedrijfszaken kan authentiseren met hetzelfde middel.	Strategische verkenning

Nr.	Ontwerpeis	Bron
E05	**Sectoren met eigen nummers moeten ondersteund kunnen worden** Vanuit het belang van privacybescherming worden binnen het eID Stelsel PSEUDOID's gebruikt. De DIENSTAANBIEDER wil echter een identiteit die binnen de eigen sector te herleiden is.	Strategische verkenning
E06	**Voorbereiden op aansluiten EU middelen** AUTHENTICATIEMIDDELEN en MACHTIGINGEN die in het Buitenland (EU) zijn afgegeven moeten gebruikt kunnen worden binnen het eID Stelsel (volgens EU-verordeningen). AUTHENTICATIEMIDDELEN en MACHTIGINGEN die binnen het eID Stelsel zijn afgegeven moeten ook gebruikt kunnen worden om diensten van buitenlandse DIENSTAANBIEDERS af te kunnen nemen.	Europese verordening
E07	**Verschillende betrouwbaarheidsniveaus ondersteunen** De toegang tot digitale diensten moet geregeld worden op een adequaat beveiligingsniveau (zoals vastgelegd in de Handreiking Betrouwbaarheidsniveaus).	Strategische verkenning

4.2 Marktwerking stimuleren

Nr.	Ontwerpeis	Bron
E11	**Multimiddelenstrategie** Door de multimiddelenstrategie zijn er binnen het eID Stelsel meerdere EID-MIDDELEN beschikbaar. Voordelen hiervan zijn dat de gehele populatie van mogelijke GEBRUIKERS 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 voor de diensten van zowel de overheid als van bedrijven gebruiken. Bedrijven hoeven daardoor niet te investeren in het uitgeven van eigen middelen om diensten te kunnen aanbieden aan burgers. Een multimiddelenstrategie voorziet in *fallback*-mogelijkheden. Als om de een of andere reden een middel niet te gebruiken is of onveilig is, dan kunnen burgers en bedrijven meteen gebruik maken van een ander middel voor diezelfde dienst.	Strategische verkenning
E12	**Hergebruik bestaande voorzieningen** Zowel aan de kant van de overheid als van marktpartijen zijn er verschillende ICT-voorzieningen die, na migratie, opgenomen worden in het eID Stelsel. Denk hierbij aan: DigiD, DigiD Machtigen, eHerkenning en PKIoverheid.	Opdracht eID Stelsel NL
E13	**Zorg ervoor dat alle partijen gelijke kansen hebben.** De keuze van de overheid om ook of zelfs uitsluitend een of meer publieke AUTHENTICATIEDIENSTEN of MACHTIGINGSDIENSTEN aan te bieden in het eID Stelsel mag niet leiden tot oneerlijke concurrentie tussen publieke en private partijen die in het eID Stelsel diensten aanbieden of middelen uitgeven. Dat betekent dat de overheid goed moet kunnen definiëren en onderbouwen waar het belang van realisatie van publieke diensten in het eID Stelsel ligt. Daarnaast moet er ruimte zijn voor alle partijen om innovatie door te voeren binnen de geldende afspraken van het eID Stelsel.	Afwegings-kader publiek privaat eID Stelsel.
E14	**Businessmodel t.b.v. investeren private partijen** Dit model zou het voor deelnemers aantrekkelijk moeten maken zelfstandig, proactief te investeren. Het businessmodel moet hiertoe de juiste prikkels geven.	Strategische verkenning

4.3 Gebruikersgemak bevorderen

Nr.	Ontwerpeis	Bron
E21	**Wees laagdrempelig, gebruikersvriendelijk en consistent voor betrokkenen** Beveiliging is mede afhankelijk van de mate waarin de GEBRUIKERS het toegangs- en machtigingsproces begrijpen. GEBRUIKERS (met name burgers) moeten het toegangs- en vertegenwoordigingsproces willen en durven gebruiken. Gebruiksacceptatie is één van de belangrijkste voorwaarden voor het slagen van het eID Stelsel.	Strategische verkenning
E22	**BELANGHEBBENDE kan zelf machtigingen en activiteiten achteraf controleren** Een hogere betrouwbaarheid: de BELANGHEBBENDE (of zijn daartoe bevoegde vertegenwoordiger) kan beoordelen of een machtiging correct is of dat een activiteit door een bevoegde is uitgevoerd. De mogelijkheid van zelfcontrole zorgt voor betrouwbaardere machtigingen en snellere ontdekking van misbruik.	Strategische verkenning
E23	**GEBRUIKERS houden de controle over machtigingen en gegevens** GEBRUIKERS blijven baas over eigen gegevens.	Strategische verkenning
E24	**Keuzevrijheid in aanschaf en gebruik** Burgers en bedrijven hebben keuzevrijheid ten aanzien van de EID-MIDDELEN die zij willen gebruiken. Men kan kiezen voor één publiek of privaat EID-MIDDEL. Men kan er ook voor kiezen om meerdere EID-MIDDELEN naast elkaar te gebruiken. Met andere woorden, de GEBRUIKER heeft de mogelijkheid om zelf te bepalen wat de samenstelling wordt van zijn digitale sleutelbos. Een GEBRUIKER moet overstapvrijheid hebben om van de ene aanbieder van EID-MIDDELEN naar een andere aanbieder van EID-MIDDELEN over te kunnen stappen. Dit is goed vergelijkbaar met het nummerbehoud in de telecomsector. Als de GEBRUIKER *kiest* voor nummerbehoud, dan verandert zijn mobiele nummer niet bij verandering van telecomaanbieder. Voor het eID Stelsel betekent dit: als de GEBRUIKER overstapt naar een andere aanbieder en kiest voor nummerbehoud, dan moet de GEBRUIKER het nieuwe eID-middel zonder conversie kunnen gebruiken bij al bestaande 'klant accounts' bij de DIENSTAANBIEDERS.	Strategische verkenning

4.4 Privacy garanderen

Nr.	Ontwerpeis	Bron
E31	**Bescherming privacy betrokkenen** Verbeterde vertrouwelijkheid, privacy en de privacywet- en regelgeving (o.a. WBP) zijn gerespecteerd. GEBRUIKERS mogen volledig vertrouwen op de borging van hun privacy en het zorgvuldig handelen van de deelnemende partijen. Organisaties mogen volledig vertrouwen op het bewaken van gevoelige informatie.	Strategische verkenning
E32	**Een EID-DEELNEMER krijgt niet meer gegevens dan strikt noodzakelijk is voor het uitvoeren van zijn taak.** Deze ontwerpeis is van belang voor E31, maar ook voor verbeterde continuïteit. Indien een EID-DEELNEMER is gehackt, dan is slechts een beperkt aantal gegevens gecompromitteerd. Het is dan eenvoudiger om de deelnemer uit het eID Stelsel te verwijderen zonder dat dit grote gevolgen heeft voor het eID Stelsel.	Strategische verkenning
E33	**DIENSTAANBIEDERS (en andere deelnemende partijen) kunnen verantwoording afleggen.** De verschillende partijen binnen het eID Stelsel moeten verantwoording kunnen afleggen over hun elektronische activiteiten. Een DIENSTAANBIEDER moet kunnen aantonen dat hij vertrouwelijke informatie terecht heeft afgeven. Ook andere partijen (bijvoorbeeld AUTHENTICATIEDIENSTEN en MACHTIGINGSDIENSTEN) moeten achteraf kunnen aantonen dat ze terecht informatie hebben afgegeven.	Strategische verkenning

4.5 Zorgen voor een toekomstvast ontwerp

Nr.	Ontwerpeis	Bron
E41	**Zorg voor robuustheid, flexibiliteit en veerkracht in het ontwerp** Door het ontwerp zo technologieonafhankelijk mogelijk op basis van rollen en relaties daartussen te formuleren, is er veerkracht en flexibiliteit mogelijk. Het ontwerp geeft duidelijkheid welke rollen er onderkend worden en wat een deelnemer moet doen om een rol in te vullen. Periodieke releases maken innovatie en uitbreiding van functionaliteit mogelijk.	Opdracht eID Stelsel Strategische verkenning

Nr.	Ontwerpeis	Bron
E42	**Zoveel mogelijk ontkoppelen van techniek** Zoveel mogelijk ontkoppeling tussen de gebruikte technologieën van DE EID-MIDDELEN en het verkrijgen van toegang bij de DIENSTAANBIEDER. Alleen daar waar strikt noodzakelijk schrijft het eID Stelsel de technische invulling van de verschillende rollen voor. Hierdoor kunnen in het stelsel nieuwe technologieën en middelen worden opgenomen en verouderde technologieën en middelen worden uitgefaseerd. Het eID Stelsel wordt daarmee toekomstbestendig (toekomstvaste adaptiviteit i.p.v. technologieafhankelijkheid). De koppelvlakken tussen de deelnemers zijn gestandaardiseerd en daar zullen dan ook technische specificaties vanuit het stelsel voor worden opgelegd.	Strategische verkenning
E43	**Aansluiten op (Europese) standaarden** In overeenstemming met het rijksbeleid inzake ICT wordt gewerkt met open standaarden. Hiervan kan alleen met goede redenen en uitdrukkelijke toestemming van de Stuurgroep eID worden afgeweken.	Strategische verkenning

4.6 Inrichten van toezicht en opsporing

Nr.	Ontwerpeis	Bron
E51	**Misbruik kan eenvoudig ontdekt en opgespoord worden** Het is van groot belang dat er vertrouwen is in het eID Stelsel. Om die reden moet misbruik eenvoudig ontdekt en opgespoord kunnen worden.	Strategische verkenning