Rapportage

Advies van ECP aan het Ministerie van Binnenlandse Zaken
over het gebruik van publieke middelen in het eID stelsel
op basis van een consultatie in een aantal private en semipublieke sectoren

In opdracht van DGBK, directie B&I, afdeling Identiteit.

Versie 1.0

Auteurs: Jelle Attema, Maartje Breeman

Januari 2015

Inleiding

Dit advies is geschreven op verzoek van het ministerie van Binnenlandse Zaken. Aanleiding is het Algemeen Overleg tussen de Tweede Kamer en de minister van Binnenlandse Zaken van 25 juni 2014, waarin de minister de Tweede Kamer heeft toegezegd een consultatie te organiseren onder bedrijfsleven, burgers en belangenorganisaties over de mogelijkheid en de wenselijkheid van een publiek eID middel.

Het advies is gebaseerd op een consultatie van een aantal private partijen ("het bedrijfsleven"), die (online) diensten aanbieden aan klanten of hun transacties digitaal willen afhandelen en daarvoor eID middelen en eID diensten nodig hebben. De vraag is of en op welke manier de overheid een publieke eID moet uitgeven. Het advies is geformuleerd vanuit het perspectief van deze dienstaanbieders: de "relying parties".

De resultaten van de consultatie zijn gedeeld met de leveranciers van eID middelen die, parallel aan deze consultatie, zich over dezelfde vraag hebben gebogen. Doel van dat gesprek was om de implicaties van de eisen en wensen van de dienstenleveranciers voor de beantwoording van onderzoeksvraag te verkennen en om een beeld te krijgen van de communicatievalkuilen waar dit rapport ook aandacht aan besteedt.

ECP roept de overheid op de ontwikkeling van het eID stelsel te faciliteren en de vraag naar, het vertrouwen in en het gebruik van eID te stimuleren. Dat kan de overheid doen door zelf hoog niveau authenticatie te eisen voor toegang tot online overheidsdiensten (die dat vereisen). Uit de interviews komt naar voren dat in tal van private sectoren wordt geïnvesteerd in hoog niveau eID middelen. Tegelijkertijd blijkt dat, door het ontbreken afspraken over interoperabiliteit van de verschillende soorten hoog niveau eID middelen en het feit dat veel Nederlanders niet over een gebruikersvriendelijk hoog niveau eID middel beschikken, de totale digitalisering van allerlei online dienstverlening moeilijk te realiseren is. Bedrijven spreken het vertrouwen uit dat er voldoende betaalbare, bruikbare, veilige en betrouwbare eID middelen zullen komen als de overheid deze markt niet overneemt of bedreigt, maar juist versterkt.

Belangrijk voor de interpretatie van dit advies is het volgende:

- Dit advies gaat over meer dan de mogelijkheid en wenselijkheid van een publiek eID middel. Het kijkt ook naar de rol van de overheid bij de ontwikkeling en het gebruik van het eID stelsel. Het eID middel en het eID stelsel blijken voor de geconsulteerden nauw verbonden. De reden is dat de partijen die werden geconsulteerd bij eID en de rol van de overheid breder kijken dan een publiek eID middel.

- Andere perspectieven, zoals veiligheid, techniek, of meer politieke en maatschappelijke argumenten (denk aan privacy of het consumentenperspectief) worden in dit advies niet meegenomen: het advies probeert het perspectief van de dienstaanbieders (relying parties) zo zuiver mogelijk te schetsen.

De geconsulteerde sectoren zijn een selectie van de sectoren waarvoor eID mogelijk relevant is. Maar vanwege de beperkte tijd hebben we ons beperkt tot de een klein aantal sectoren/bestuurders, die door hun massa en omvang van cruciaal belang zijn voor de acceptatie, het gebruik en het draagvlak voor eID (zie hoofdstuk 1, punt 4, voor een kwantitatieve indicatie).

Leeswijzer

De opdrachtomschrijving en verder achtergrondinformatie is te vinden in de Bijlagen. Bijlage 1 (**Bijlage I: Achtergrond en context consultatie eID en bedrijven**.) beschrijft de achtergrond van deze opdracht. Bijlage II (**Bijlage II: het eID stelsel**.) beschrijft het eID stelsel. Het eID stelsel zoals beschreven in Bijlage II is voor veel respondenten de referentie.

Wanneer de geconsulteerden spreken over Europese ontwikkelingen speelt de eIDAS regulation een centrale rol: deze Regulation heeft ten doel dat hoog niveau eID middelen ook grensoverschrijdend gebruikt kunnen worden. In Bijlage III (**Bijlage III: de eIDAS Regulation**) worden de hoofdlijnen van de Regulation beschreven, waarbij opgemerkt moet worden dat de implementatie en interpretatie (door Nederland en andere lidstaten) van de Regulation nog niet is afgerond en er nog veel ruimte is voor interpretatieverschillen.

Het advies wordt opgebouwd in de volgende stappen.

Hoofdstuk 1 gaat in op het **belang** van eID voor verschillende sectoren.

Hoofdstuk 2 benoemt **de eisen** van bestuurders aan een eID middel en eID stelsel, ongeacht de vraag of het publiek of privaat is.

Hoofdstuk 3 beschrijft de antwoorden van bestuurders op de vraag wat de **rol van de overheid** kan zijn bij de ontwikkeling, de uitrol en het beheer van een eID middel of stelsel en de argumenten.

Hoofdstuk 4 diept het onderwerp "**betrouwbaarheid**" uit en de implicaties daarvan voor een rol van de overheid en de rolverdeling overheid en bedrijven.

Hoofdstuk 5 bevat het eigenlijke **advies** over de verdeling publiek/privaat in de vorm van een scenario waarin de eisen, de keuzeopties en de andere overwegingen zo goed mogelijk zijn meegenomen.

Hoofdstuk 6 adresseert de communicatie en geeft advies over het voorkomen van misverstanden over eID. Het advies is gebaseerd op de ervaringen van de onderzoekers bij de consultatie.

Bijlage IV bevat een korte beschrijving van een aantal casussen die het belang van eID en de eisen die respondenten stellen aan eID illustreren. **Bijlage V** noemt de geconsulteerde personen en meelezers.

ECP Platform voor de InformatieSamenleving

Inhoud

Hoofdstuk 1: het belang van eID

Voor deze consultatie zijn experts en bestuurders geïnterviewd uit de volgende domeinen: accountancy, bouw, logistiek, verzekeringen, webwinkels, zorg en onderwijs. Daarnaast is de directeur van het CIO platform geïnterviewd. Voor de namen van de geconsulteerden, hun functie en een aantal casussen worden wordt verwezen naar de bijlagen IV en V.

De geïnterviewden staan allen een snelle introductie van een eID voor, waar de meeste Nederlanders op korte termijn over kunnen beschikken, waarmee met grote zekerheid de online identiteit van iemand kan worden vastgesteld en dat veel/breed gebruikt wordt.

De overwegingen zijn niet precies identiek voor de sectoren:

- Voor de **accountancy, bouw, logistiek, verzekeraars en de leden van het CIO platform** is de belangrijkste overweging: omdat in Nederland een breed gebruikt hoog niveau eID middel ontbreekt, moeten allerlei processen (die al grotendeels digitaal plaatsvinden) uiteindelijk toch nog op papier moeten worden afgehandeld.
  Voor de afronding van deze grotendeels digitale processen is uiteindelijk face-to-face contact nodig (voor legitimatie) of uitwisseling van documenten op papier (bijvoorbeeld ter ondertekening).
  Wettelijke verplichtingen vergen bovendien steeds vaker betrouwbare manieren van (online) identificatie: denk aan de wet ketenaansprakelijkheid in de bouw.

- Voor sectoren als de **webwinkels** en (online) gaming is veiligheid/privacy, laagdrempelige en betrouwbare leeftijdsverificatie en verstrekking van andere attributen (zoals kredietwaardigheid, adresgegevens, naam en geboortedatum) de belangrijkste drijfveer om een oproep te doen voor een breed gebruikt en betrouwbaar systeem voor online identificatie. eID moet de consument in staat stellen gemakkelijk (gevalideerde) gegevens te verstrekken zonder dat de consument de controle over de verspreiding van die gegevens verliest en de online dienstverlener (zoals de webwinkelier) wordt ontzorgd: het beheer van deze privacygevoelige data vormt meer en meer een afbreukrisico.

- In sectoren waar gebruik van ICT nog sterk in ontwikkeling is (zoals **zorg, onderwijs**) en waar authenticatie en autorisatie nu nog op allerlei verschillende manieren wordt georganiseerd, zal een betrouwbaar breed gebruikt eID middel als best practice kunnen gelden en daardoor bijdragen aan veiligheid, innovatie en marktontwikkeling. De afwezigheid van een breed gebruikt eID draagt bij aan vendor-lockin: de overstap naar een ander ICT-leverancier is nu kostbaar, o.a. omdat eID geheel opnieuw moet worden georganiseerd.
  Wat daar bovendien speelt is dat niet alle patiënten of kinderen die recht hebben op zorg of onderwijs, beschikken over een door de Nederlandse staat erkende identiteit. Toch moeten zij (of hun ouders) met een betrouwbaar middel online toegang kunnen krijgen tot diensten.

Het is belangrijk om te bedenken dat deze argumenten voor eID en het stelsel sterk zijn gekleurd door het perspectief van de geconsulteerden. Wat daarbij opvalt is:

1. Bij eID denken de respondenten zowel aan het eID middel waarmee iemand online de eigen identiteit kan bewijzen als aan het eID stelsel waarmee allerlei eID diensten mogelijk maakt: de eigenaar van de eID kan binnen dat stelsel bijvoorbeeld gevalideerde attributen verstrekken (bijvoorbeeld "ik ben ouder dan 18"), elektronische handtekeningen zetten of elektronische documenten versleutelen en aangetekend bezorgen. Het over en weer kunnen (h)erkennen van eID middelen met een hoog niveau van betrouwbaarheid en toepassingsmogelijkheden is daarbij van belang.

2. Privacy: het zakelijk gebruik van eID vereist vaak dat een eID herleid kan worden naar een natuurlijke persoon. Bijvoorbeeld wanneer een werkgever moet weten of een uitzendkracht in de bouw of in de zorg, die zich online heeft geïdentificeerd, werkelijk gerechtigd was om te werken, moet kunnen worden getraceerd welke natuurlijke persoon bij die online identiteit hoorde.
In het consumentendomein en op andere momenten is die traceerbaarheid misschien juist onwenselijk: een webwinkelier hoeft alleen betrouwbaar vast te stellen dát iemand ouder dan 18 is. En hoeft niet te weten wie de natuurlijke persoon is die schuil gaat achter een identiteit. Iemand mag zich kenbaar maken met allerlei fantasienamen als maar (zonder fraude) betaald wordt en, bij bepaalde producten, met hoog niveau van zekerheid is vastgesteld dát de persoon ouder is dan 18. Ook dan is het belangrijk dat, bij malversaties, duidelijk is wie heeft gefraudeerd.
Volledige anonimiteit en volledige traceerbaarheid lijken elkaar uit te sluiten. De verschillende technische oplossingen voor eID gaan op een verschillende manier om met anonimiteit en traceerbaarheid. PKI oplossingen werken met certificaten. Wanneer verschillende partijen hun bestanden koppelen kunnen, de gangen van een persoon worden nagegaan: het certificaat is altijd hetzelfde. Privacy wordt gewaarborgd omdat de wet verbiedt deze koppelingen te maken en er "Trusted Third Parties" zijn die aan zware eisen moeten voldoen bij het verstrekken en uitvoeren van controles op certificaten: privacy wordt uiteindelijk beschermd door wetgeving.
Andere technische oplossingen, zoals de IRMA kaart, maken volledig anonieme betrouwbare attribuutverstrekking mogelijk: maar op het moment dat in een zakelijke context iemand traceerbaar moet zijn (bijvoorbeeld bij tekenen van een arbeidscontract, of om toegang tot een informatiesysteem te krijgen) moet de eindgebruiker de eigen identiteit alsnog "onthullen" en bijvoorbeeld aantonen op dat moment nog steeds Nederlands staatsburger te zijn. Dan is adequate wetgeving nodig om te voorkomen dat partijen gegevens onterecht gaan koppelen.
ECP bepleit om de strijd niet uit te vechten welke technologie het beste privacy waarborgt, maar de eisen aan privacy en traceerbaarheid op te stellen en partijen zelf te laten beslissen op welke wijze ze aan die eisen willen voldoen. Effectief toezicht daarop is belangrijk.

3. Een belangrijk aandachtspunt dat de geinterviewden benadrukken is dat overheid en bedrijfsleven beide belang hebben bij een gezonde markt met gebruikersvriendelijke, betaalbare en betrouwbare eID middelen en diensten, die aantrekkelijk is om nieuwe en innovatieve eID diensten en eID producten voor te ontwikkelen. De overheid kan die snelle adoptie versnellen, maar ook verhinderen: in het bijzonder door onduidelijk te zijn over tijdpaden, commitment, eisen enz.

4. Deelvraag 3 (zie bijlage I) van dit onderzoek is de vraag wat in kwantitatieve zin het 'marktaandeel' is van de geconsulteerde sectoren, in termen van (potentieel) gebruik van publieke eID-middelen. Deze cijfers benadrukken de noodzaak dat bedrijfsleven en overheid samen eID oppakken.
De sectoren die aan de orde komen in dit advies bieden werk aan ongeveer 32% van de Nederlandse beroepsbevolking (in 2012) en dat komt overeen met 15% van de totale Nederlandse bevolking (in 2012). Om volledig digitale dienstverlening mogelijk te maken, is het niet voldoende is om de mensen die werken in deze sectoren, beschikking te geven over een hoog niveau eID. Ook de klanten van deze sectoren hebben een hoog niveau eID nodig om processen te kunnen digitaliseren: alle Nederlanders die dat willen en op enigerlei moment in hun leven diensten afnemen van deze sectoren.
Deze cijfers maken daarom duidelijk dat overheid en bedrijfsleven samen moeten optrekken om eID breed uitgerold te krijgen en er voor te zorgen dat deze eID's regelmatig worden gebruikt. Sectoren kunnen dat niet op eigen houtje of slechts tegen hoge kosten.

Sector	Aantal werkenden (x 1000)	Percentage beroepsbevolking
Aantal werkenden (2012) over alle sectoren	7387	100%
Bouwnijverheid	469	6%
Vervoer en opslag	362	5%
Financieel	233	3%
Gezondheidszorg	576	8%
Zorg en welzijn	714	10%
Totaal:	2354	32%
Bron: statline.cbs.nl		

5. De overwegingen in dit hoofdstuk geven ook een antwoord op deelvraag 4 (zie bijlage I) of er een verband is tussen de sector waarvan respondenten deel uitmaken en de voorkeur die zij hebben voor rolverdeling tussen de overheid en bedrijfsleven.
Gesteld kan worden dat de visie op samenwerking met de overheid rond eID identiek is voor de verschillende sectoren, maar dat de onderbouwing van die visie wordt gekleurd door sectorspecifieke verschillen. Doel van de samenwerking van overheid en bedrijfsleven is:
a. er voor te zorgen dat alle Nederlanders die dat willen over een hoog niveau eID beschikken zodat deze sectoren kunnen werken aan volledig digitale afhandeling van nu al grotendeels gedigitaliseerde processen (accountancy, bouw, logistiek, verzekeringen, leden CIO platform),
b. er breed gebruikte, betrouwbare, gebruikers- en privacy vriendelijke manieren van attribuutverstrekking (webwinkels) ontstaan, waar iedere Nederland, die dat wil, de beschikking over kan hebben en
c. bij te dragen aan het ontstaan van een breed gedragen en gebruikte best-practices rond eID (zorg, onderwijs). Dat heeft een positief effect op veiligheid en privacy, maar doorbreekt ook de dreiging van vendor-lockin (met name in zorg en onderwijs): het inrichten van een goed eID systeem is op dit moment zo kostbaar dat al snel te duur is om over te stappen naar een andere leverancier.

Hoofdstuk 2: Eisen aan een eID middel/stelsel.

Uit de gesprekken komt een aantal breed gedragen eisen naar voren aan het eID systeem (middelen + stelsel):

Eis 1 – snelheid uitrol. Het eID middel[1] of de eID middelen (en functionaliteit van het eID stelsel) moet snel uitgerold kunnen worden (1 á 2 jaar).

Eis 2 – breed gebruik. Het middel moet breed en vaak gebruikt worden (meeste Nederlanders moeten er over beschikken en het ook regelmatig gebruiken).

Eis 3 - betrouwbaarheid: het middel en het stelsel moeten betrouwbaar zijn (identiteiten moeten tot personen herleid kunnen worden).

Eis 4 – gebruik over sectoren. Het middel en het stelsel moeten bruikbaar zijn voor transacties in het overheids-, zakelijke- en burgerdomein.

Eis 5 – Europa. Het middel en het stelsel moeten in lijn zijn met Europese ontwikkelingen.

Eis 6 – eigen functionaliteit en innovatie. Het moet mogelijkheden bieden om zelf (bedrijfs- of sectorspecifieke) functionaliteit toe te voegen en de toepassing van innovaties op het gebied van eID moet worden gestimuleerd en zeker niet belemmerd worden.

Eis 7 – uitgifteproces: kosten en gemak. De kosten van aanschaf van het middel (acquisitie) en van de uitrol moeten laag zijn en het gemak (van het verstrekking proces) hoog.

[1] De respondenten bedoelen, wanneer ze spreken over een "eID middel" over online identificatie met een hoog betrouwbaarheidsniveau: of dat plaatsvindt met een publiek of een privaat eID middel en of er sprake is van een enkel of diverse eID middelen, wordt in het midden gelaten. Ook bedoelen respondenten vaak allerlei functionaliteit uit het eID stelsel wanneer zij spreken over een "eID middel": het kunnen zetten van een elektronische handtekening, werken met een beroepscertificaat, het kunnen versleutelen van berichten, of betrouwbare attribuutverstrekking zijn onverbrekelijk verbonden met "het middel". In de latere hoofdstukken wordt verder geanalyseerd wat de meest verstandige interpretatie is van het woord "middel".

Hoofdstuk 3: De rol van de overheid

Op de vraag of de overheid kan bijdragen aan het vervullen van de eisen uit hoofdstuk 2 zijn de volgende antwoorden geïnventariseerd:

Overheidsrol 1. De overheid kan bijdragen aan:

- de snelheid van de introductie **(eis 1)**,
- het gebruik **(eis 2)** en
- innovatie van eID middelen (zie voetnoot 1 op de vorige pagina voor interpretatie van het begrip "eID middel") en diensten versnellen **(eis 6)**

door

- hoog (niveau) private eID middelen, die voldoen aan eisen van het eID stelsel, verplicht te stellen voor online toegang tot een aantal veel gebruikte overheidsdiensten (die dat hoge niveau van zekerheid vereisen) en
- het mogelijk te maken dat deze middelen binnen het overheids-, zakelijke en consumentendomein gebruikt kunnen worden **(eis 4)** en
- samen met het bedrijfsleven een minimum set aan eisen te formuleren waar het eID middel aan moet voldoen. Daar bovenop kunnen sectoren of individuele eID leveranciers hun eigen functionaliteit bouwen: maar de middelen moeten, ondanks dat, in andere sectoren en bij transacties met de overheid bruikbaar zijn.

Respondenten hechten belang aan een breed gebruik van eID middelen, door zo veel mogelijk Nederlanders, omdat veel dienstverleners met veel van hun klanten slechts incidenteel contact hebben. Als dan een hoog niveau van identificatie nodig is loont het niet om die klant voor die incidentele keer van een eID te voorzien. Bijvoorbeeld:

- Business to Consumer: een pakketbezorger die een mobiele telefoon aflevert bij een klant kan met zijn logistiek-pas zichzelf identificeren en de ontvangende klant kan dat straks doen met het hoog niveau eID middel dat hij kan gebruiken om bijvoorbeeld Belastingaangifte te doen of om een verzekering helemaal digitaal af te sluiten.
- Business to Business: Een chauffeur krijgt toegang tot een bouwplaats op basis van zijn logistiek-pas of zijn persoonlijke eID-middel (op de telefoon) om daar vervolgens een vracht af te kunnen leveren.

Overheidsrol 2. De overheid kan:

- het vertrouwen **(eis 3)** en daarmee de bereidheid bij het bedrijfsleven om in private eID - middelen en het stelsel te investeren vergroten

door:

- een goed toezicht op het naleven van afspraken in te richten,
- samen met marktpartijen samen te werken om fraude en misstanden snel te signaleren en maatregelen te nemen dit aan te pakken.

- zelf de eID middelen te gebruiken: het systeem zal, volgens de respondenten, niet snel omvallen en het is stevig genoeg om voor eigen dienstverlening te gebruiken.

De overheid kan aansluiting op Europese ontwikkelingen **(eis 6)** borgen door eisen aan de eID middelen zoveel mogelijk techniek onafhankelijk te stellen.
De overheid moet de eID middelen met hoog niveau van betrouwbaarheid, die op de markt zijn en die voldoen aan alle eisen, de kans geven om zich te kwalificeren voor deelname aan het eID stelsel en op die middelen vertrouwen bij de eigen online dienstverlening. Dat betekent dat de overheid zich beperkt tot het stellen van generieke eisen aan het betrouwbaarheidsniveau (STORK 3 of STORK 4) of de betrouwbaarheidsniveaus "substantial" en "high" zoals de Regulation die formuleert. Het eID stelsel moet primair afspraken maken over koppelvlakken en niet over de technische invulling.

Overheidsrol 3. De overheid kan bijdragen aan het verlagen van de kosten van het eID middelen en het vergroten van het gemak van uitgifte **(eis 7)**,

door:

- a) het aantal transacties waarvoor eID wordt gebruikt te vergroten (door zelf een hoog niveau te eisen voor online overheidsdiensten die dat vereisen) en

- b) samen te werken met marktpartijen om de kosten van het verstrekkingsproces en uitgifteproces te verlagen en het gemak van uitgifte te vergroten

Ad a). Bijdrage van de overheid aan het verlagen van de kosten van het uitgifteproces en vergroten van het gemak van uitgifte.
Uitreiking van eID's, die hogere niveaus van betrouwbaarheid ondersteunen, is kostbaar: zowel de registratie als uitgifte van zulke eID middelen moet worden verricht door iemand die daartoe bevoegd is en de benodigde tools heeft. Die persoon moet immers de echtheidskenmerken van het paspoort (ook buitenlandse) kunnen controleren en de persoon aan wie de eID wordt verstrekt kunnen matchen met de pasfoto op het identiteitsbewijs. Dat vergt training.
De uitreiking van een hoog niveau identificatiemiddel is bovendien belastend voor degene die het eID middel ontvangt: bij aanvraag en uitreiking is er een baliemoment en persoonlijk contact nodig.

Omdat de uitreiking van hoog niveau eID's complex is, is dat een drempel voor toetreding tot de eID markt: een leverancier die een goede eID oplossing heeft, moet ook het uitgifteproces inrichten.

Ad b). Bijdrage van de overheid aan het verlagen van de kosten van het gebruik van eID voor de consument/burger.

Sommige respondenten die zijn geconsulteerd (zoals uit de bouw, logistiek en accountancy) stellen voor dat de relying parties, degenen die bij het verlenen van online diensten eID gebruiken, de kosten van het eID middel vergoeden. In branches als die van Bouwend Nederland en Transport en Logistiek Nederland worden al afspraken gemaakt met de door hen geselecteerde Identity Service Providers dat de relying parties het gebruik van eID middelen vergoeden. De middelen zijn dan gratis voor de (kleinere) eindgebruikers

Daarmee wordt concurrentie op de kwaliteit en bruikbaarheid van eID middelen bevorderd: het aantal consumenten dat hun eID middel aanschaft en het werkelijk gebruikt is bepalend voor de inkomsten van de leveranciers van eID middelen.

Hoofdstuk 4: Versterken van betrouwbaarheid.

De rol van de overheid zoals de respondenten die formuleren is een andere dan het introduceren van een publiek middel. Eigenlijk laten de respondenten in het midden of een publiek middel noodzakelijk is: ze vragen de overheid om samen te werken met het bedrijfsleven en te zorgen voor een snelle uitrol van eID middelen en het eID systeem, de betrouwbaarheid en de betaalbaarheid van het stelsel te vergroten en het gebruik te bevorderen.

De respondenten geven aan dat de overheid bij het maken van keuzes zich bewust moet zijn dat die keuzes een positieve of een negatieve invloed kunnen hebben op het ontstaan van een gezonde markt: met betaalbare, betrouwbare eID middelen die gebruik maken van de technologische ontwikkelingen.

Dit hoofdstuk gaat verder in op de vraag of binnen deze kaders een publiek middel een rol zou kunnen spelen.

Om die vraag te kunnen beantwoorden wordt in dit hoofdstuk nagegaan wat er nu precies onder een "publiek middel" moet worden verstaan: waarin verschilt een publiek middel van een privaat middel.

In de gesprekken over eID, de eID middelen en het stelsel komen eigenlijk twee verschillende vormen van eID middelen ter sprake:

> **Type 1**: **eID als digitaal identiteitsbewijs**.
> Identiteitsdocumenten als het paspoort, de identiteitskaart en rijbewijs (WID)worden door de overheid verstrekt. Met dat document kan iemand bewijzen dat de Nederlandse overheid hem of haar een identiteit heeft verleend: het zijn "identiteitsbewijzen".
> Dit WID vormt de basis voor veel diensten en transacties: het is nodig bij het openen van een bankrekening en het aanvragen van een bankpas, voor het afsluiten van een verzekering, of het tekenen van een arbeidscontract. Maar ook voor het afgeven van een STORK 3 of STORK 4 (een hoog niveau) eID.
> Op dit moment is er geen digitaal equivalent van het fysieke paspoort, de identiteitskaart of het rijbewijs: er is geen digitaal WID of eWID.
>
> De vraag naar een publiek middel kan worden opgevat als de vraag of er een nieuwe vorm van Wettelijk Identiteitsbewijs moet komen: een digitaal WID, een eWID.
>
> **Type 2**: **Afgeleid eID**.
> Naast de door overheid verstrekte identiteitsbewijzen (WID) zijn er tal van andere eID's: deze zijn persoonlijk afgegeven aan de eigenaar na controle van de gegevens op het identiteitsbewijs. De afgeleide eID's hebben vele verschijningsvormen: denk aan een bedrijfspas, een username/password combinatie met SMS authenticatie, of de bankpas met reader, de passen en readers uitgegeven onder PKI overheid, eHerkenning (STORK 3 en 4).

De andere verschillen tussen deze twee typen identiteitsbewijzen hebben betrekking op het proces van uitgifte (enrollment) en de controles op echtheid. Deze twee verschillen worden hier besproken.

Verschil tussen type 1 en 2: proces van Enrollment.

Type 1: Een cruciaal onderscheid tussen het digitaal identiteitsbewijs (type 1) en het afgeleide eID (type 2) is het **proces van enrollment**. Een burger gaat bij de aanvraag van een identiteitsbewijs (de enrollment) naar het loket van de overheid, met een pasfoto en een aantal gegevens. Die gegevens worden door een ambtenaar gecontroleerd in het BRP en de ambtenaar controleert of de foto overeenkomt met de persoon. Op basis van die controles geeft de ambtenaar opdracht tot het maken van het paspoort of de identiteitskaart.
Het moment dat wordt vastgesteld dat de foto, persoon en gegevens met elkaar overeenkomen en dat de opdracht wordt gegeven een wettelijk identiteitsbewijs te maken, is belangrijk. Immers: de overheid geeft daarmee aan dat deze specifieke persoon met deze kenmerken, een Nederlands Staatsburger is. Omdat de overheid het proces uitvoert mogen we er op vertrouwen dat, als er al fouten worden gemaakt, dit geen systematische fouten zijn. De overheid heeft bijvoorbeeld geen zakelijke belangen, maakt zelf de fouten, heeft bovendien allerlei mogelijkheden om te ontdekken dat die fouten zijn gemaakt en heeft zelf allerlei middelen en bevoegdheden om die fouten op te lossen. Een private partij heeft die mogelijkheden minder.

Type 2: De procedure rond de aanvraag en de uitgifte van **een type 2, hoog niveau afgeleid eID middel** steunt op het WID en veronderstelt dat dit proces van enrollment goed is verlopen.

Het proces van enrollment bij afgeleide eID's wordt vervuld door de leverancier van het afgeleide eID middel op basis van een controle van het WID: iemand die een eID aanvraagt bij een eID leverancier krijgt dat op vertoon van zijn WID. De leverancier van eID middelen is gecertificeerd om controles uit te voeren op de echtheid van het WID en om vast te stellen vast dat deze persoon bij dit WID hoort (iets wat behoorlijke training vergt). Dat vaststellen van de identiteit op basis van het WID is een complex en kostbaar proces: er is een hele organisatorische en technische infrastructuur voor nodig. En het is een drempel voor nieuwe toetreders en de adoptie van nieuwe technologieën. Bovendien is het een proces dat belastend voor de eindgebruiker: iedere keer is face-to-face controle nodig. En bovendien zal die controle iedere paar jaar moeten worden herhaald.

Het verschil tussen een eID en een WID: de drager.

Een ander relevant onderscheid bij het beantwoorden van de vraag of een publiek eID middel noodzakelijk is, is de vraag of de veiligheid en kwaliteit van een eID kan worden vergroot door, net zoals bij het fysieke WID, het eID op een besloten manier te ontwikkelen.
Bij het ontwikkelen van een betrouwbaar WID op papier of op een kaart ID heeft het zin dat de overheid hier de regie op voert: de overheid er voor zorgen dat het WID zodanige (geheime) kenmerken heeft dat het bijzonder moeilijk is de drager en de informatie daarop na te maken. Bij een identiteitsbewijs op papier of een kaart bepalen de kenmerken die zijn toegevoegd aan de drager (de kaart of het papier) of een bewijs geldig en echt is. Door die kenmerken is het moeilijk en kostbaar om het identiteitsbewijs na te maken, te veranderen of aan te passen. Het ligt voor de hand, met het oog op veiligheid en betrouwbaarheid, dat een WID in alle beslotenheid en in opdracht van de overheid wordt ontwikkeld, geproduceerd en verstrekt.
Bij een digitaal eID worden de echtheid en geldigheid gecontroleerd met allerlei (automatisch uitgevoerde) en breed bekende en op deugdelijkheid getoetste technische controles: die controles vinden gedurende de hele levensloop van het eID plaats en vaak iedere keer als het eID wordt gecontroleerd. Verschillende eID oplossingen hebben daar verschillende methoden voor: een PKI overheid systematiek werkt met andere controles dan een bankpas of een kaart gebaseerd op de

IRMA techniek. Alle drie leveren ze, op hun eigen manier, bewijs over geldigheid en echtheid[2]. En nieuwe eID's zullen waarschijnlijk weer nieuwe controles gebruiken, bijvoorbeeld met hulp van biometrie.

Conclusie: bij de ontwikkeling van een paspoort of identiteitskaart heeft het zin dat de overheid met en publiek middel komt. Beslotenheid en geheimhouding is een belangrijk element in de beveiliging. Bij de veiligheid van een eID heeft deze beslotenheid geen zin: de controle op echtheid gebeurt op basis van breed geteste en overal bekende algoritmes en mechanismen. Beslotenheid is eerder een risicofactor dan een bijdrage aan veiligheid.

De discussie over een publiek middel zou volgens ECP daarom teruggebracht worden naar de vraag:

> Kan de overheid een bijdrage leveren aan veiligheid, gebruikersvriendelijkheid, het brede gebruik, de betrouwbaarheid, het gemak of betaalbaarheid van eID (zowel het eID middel als het stelsel) door een rol te spelen in het enrollment proces bij de uitgifte van een hoog niveau eID?

Om deze vraag te beantwoorden is een blik op de toekomst nodig: immers zowel marktpartijen als de overheid kunnen een betrouwbare enrollment uitvoeren op basis van de bestaande identiteitspapieren. Onze verwachting (ECP) is echter dat het steeds gemakkelijker en goedkoper zal worden voor burgers, consumenten en organisaties om zich met een hoog niveau van betrouwbaarheid online te legitimeren. Naast een kaart met een reader zal de smartphone in toenemende mate worden gebruikt, of de tablet of laptop en allerlei nieuwe apparaten zoals smartwatches. Er zullen allerlei nieuwe vormen van authenticatie komen zoals biometrie (vingerafdruk, ader, hartslag, gezicht) al dan niet aangevuld met allerlei vormen van risicodetectie (IMEI, gedragsanalyse) die een hoog niveau van zekerheid kunnen bieden over de identiteit van een persoon. Als iedere nieuwe toetreder op de markt van hoog niveau eID middelen een compleet uitgifteproces moet inrichten, vormt dat een drempel voor die toetreder en daarmee voor innovatie.

Ons voorstel (ECP) is daarom een elektronische WID te introduceren, dat gebruikt kan worden om het complexe uitgifteproces van hoog niveau eID's te vereenvoudigen: deze eWID mag gebruikt worden door organisaties en consumenten om afgeleide hoog niveau eID's (online) te activeren. Zo'n digitaal WID is dan de moeder voor andere hoog niveau eID middelen: de kernidentiteit.

De overheid bepaalt wie er zo'n eWID krijgt (enrollment), maar de gebruiker/eigenaar kan zelf kiezen uit de daarvoor gekwalificeerde eID leveranciers, wie de eID levert. Omdat het eWID technisch gezien hetzelfde werkt als de afgeleide eID's (de controles op de geldigheid en echtheid zijn vooral automatisch/technisch en vinden continu plaats) is het niet nodig om te kiezen voor een specifieke technologie: de eisen kunnen techniekonafhankelijk zijn. Voor zowel de afgeleide eID's als deze eWID zijn er zware eisen op allerlei gebied: eisen aan functionaliteit, eisen aan de organisatie en meer juridische eisen zoals rond continuïteit, privacy, toezicht, transparantie.

Om te voorkomen dat dit digitale brondocument de markt gaat verstoren (en daarmee de ontwikkeling van betaalbare, gebruikersvriendelijke en innovatieve eID middelen op korte termijn hindert) bepleiten wij dat het digitaal eWID pas op termijn wordt geïntroduceerd en (in eerste instantie) alleen gebruikt mag worden voor het activeren van andere hoog niveau eID's.

---

2 De IRMA kaart bevindt zich in de pilotfase: het enrollmentproces van de huidige kaarten voldoet mogelijk nog niet aan de eisen van Stork 4. Maar dat is een organisatorisch en niet een technisch probleem.

Hoofdstuk 5: Advies ECP over een publiek/private rolverdeling

In deze paragraaf wordt een scenario geschetst dat tegemoet komt aan de eisen aan het eID middel en stelsel zoals geformuleerd in hoofdstuk 1 en 2[3]. Dat rekening houdt met de antwoorden op de vraag of een publiek eID middel moet worden ontwikkeld, weergegeven in hoofdstuk 3.

Het advies is daarnaast gebaseerd op een analyse van het begrip "publiek middel" dat in hoofdstuk 4 werden voorgesteld. Op basis van die analyse en een blik in de toekomst werd voorgesteld op termijn een digitaal equivalent van de bestaande identiteitsbewijzen te introduceren, een eWID, waarmee gebruikers online een hoog niveau eID middel kunnen activeren. Daarmee kan de overheid invulling aan de verantwoordelijkheid de wettelijke identiteit van iemand vast te stellen.

Het advies bestaat uit de volgende drie stappen.

Stap 1: Met marktpartijen ontwikkelt de overheid de functionele, techniekonafhankelijke eisen waar afgeleide (zie hoofdstuk 4) eID middelen aan moeten voldoen (inclusief koppelvlakken) en maakt de overheid afspraken hoe partijen kunnen aantonen dat ze aan deze eisen voldoen en hoe het toezicht er uit ziet. Ook over de systematiek voor het verstrekken van (betrouwbare) attributen worden afspraken gemaakt.
De overheid kondigt tevens aan dat overheidsdiensten die een hoog niveau van authenticatie vereisen alleen toegankelijk zijn met een middel dat aan die afgesproken eisen voldoet. En de overheid geeft de zekerheid dat de overheid gedurende een aantal jaren (bijvoorbeeld 5 jaar) deze weg zal bewandelen: dat biedt het bedrijfsleven dat eID middelen gebruikt (de relying parties, de respondenten in dit onderzoek) investeringszekerheid en degenen die eID middelen op de markt brengen de mogelijkheid een business case te berekenen.

Stap 2: de overheid richt toezicht in en werkt structureel met marktpartijen (zowel relying parties als leveranciers van eID middelen), aan het vergroten van de betrouwbaarheid van de middelen en het snel en adequaat signaleren en aanpakken van incidenten. Doel is het vertrouwen van de samenleving in eID te vergroten. Doel is het voorkomen en aanpakken van identiteitsfraude, en veiligheid, privacy en betrouwbaarheid te vergroten.

Stap 3: de overheid ontwikkelt een elektronisch equivalent van het paspoort, het eWID (zie hoofdstuk 4): een brondocument voor de digitale identiteit, waarbij de gebruiker zelf mag kiezen welke (gekwalificeerde) leverancier dat middel levert, maar de overheid de enrollment uitvoert (bepaalt of een persoon een digitaal identiteitsbewijs verstrekt krijgt). Met dat middel kunnen afgeleide hoog niveau eID middelen worden geactiveerd.

[3] Ook hier wordt gesproken over eID en eID middelen in een brede zin: zie pagina 7, voetnoot 1

Hoofdstuk 6: Advies ECP over de communicatie.

Deze paragraaf bespreekt misverstanden en discussiepunten die naar voren kwamen tijdens de interviews en gesprekken rond dit advies: met de partijen die eID willen gebruiken en degenen die eID oplossingen aanbieden.

Uit de consultatie blijkt dat de relying parties, degenen die geconsulteerd werden, grote behoefte hebben aan eID: in diverse sectoren zijn de business cases beschreven en berekend en die is zonder uitzondering positief. De rol van de overheid zoals de respondenten die formuleren is een andere dan het introduceren van een publiek middel. Eigenlijk laten de respondenten in het midden of een publiek middel noodzakelijk is: ze vragen de overheid om samen te werken met het bedrijfsleven en te zorgen voor een snelle uitrol van eID middelen en het eID systeem. De overheid kan meehelpen de betrouwbaarheid en de betaalbaarheid van het stelsel te vergroten en het gebruik te bevorderen.

Het advies geformuleerd in het vorige hoofdstuk wordt door de geconsulteerde partijen in grote lijnen ondersteunen.

Omstreden is ons advies echter bij meelezers uit de hoek van de overheid en de leveranciers van eID middelen. De argumenten die worden aangevoerd, zijn vaak niet inhoudelijk (technische haalbaarheid, efficiency) maar gaan vaak over vertrouwen: van de overheid in de leveranciers van eID middelen en omgekeerd. De leveranciers eID middelen vragen zich af of de overheid uiteindelijk toch niet een eigen weg kiest en alle inspanningen om tot samenwerking te komen voor niets zijn geweest. Meelezers van de kant van de overheid vragen zich af of de leveranciers van eID middelen niet vooral gedreven worden door winstbejag en de samenleving met kostbare, inferieure techniek en oplossingen opzadelen.

Het gebrek aan vertrouwen over en weer leidt tot een impasse. In het advies in hoofdstuk 5 is dat herstel van vertrouwen een belangrijk element: zonder vertrouwen zijn zowel stap 3 (voor meelezers uit de hoek van eID leveranciers) als stap 1 (voor sommige meelezers uit de hoek van de overheid) een brug te ver, terwijl voor de respondenten uit het bedrijfsleven (de relying parties) zo'n scenario het bespreken waard is.

De redenen voor het wantrouwen zijn begrijpelijk. Een drietal redenen komen steeds terug.

1. Overheden die eID moeten gaan gebruiken en de leveranciers van eID middelen vormen geen homogene groepen: een afspraak met "de overheid" of met "de markt" is daardoor niet mogelijk. Verschillende overheden hebben andere behoeften prioriteiten rond eID (denk aan BZK, MinFin, V&J en EZ) en een gesprek met het ene ministerie betekent niet automatisch dat een ander ministerie op dezelfde manier denkt. Ook de eID leveranciers vormen geen homogene groep: zij hebben sterk verschillende opvattingen over de kwaliteit van de producten van hun concurrenten en de eID leveranciers proberen de eigen technische keuzes deel uit te laten maken van het stelsel. De debatten worden daardoor steeds technischer (welke oplossingen beter zijn) en omdat die debatten zelden op iets uitlopen wordt het spel steeds politieker gespeeld (het debat gaat plotseling over "privacy" en "marktwerking").

2. De leveranciers zijn daarbij beducht dat de overheid uiteindelijk een groot deel van de markt van eID middelen gaat bepalen (een techniek kiest of een leverancier) waardoor de businesscase voor hen ingrijpend verandert of de overheid uiteindelijk afspraken over samenwerking niet nakomt. Bijvoorbeeld door één op één afspraken met banken of de RDW.
De overheid daarentegen heeft bedenkingen of leveranciers wel voldoende hoog niveau middelen kunnen leveren (hun organisatie bijvoorbeeld op orde hebben) en zich op die markt willen begeven. Ook vergroten de kritische opmerkingen van leveranciers over de kwaliteit van elkaars oplossingen niet het vertrouwen bij de overheid in publiek-private samenwerking.

3. Tenslotte hebben de leveranciers van eID middelen weinig oog voor de (legitieme) behoefte van de overheid om controle te houden wie in Nederland een identiteitsbewijs heeft: achtergrond daarvoor is de angst dat de overheid (de facto) het alleenrecht krijgt op verstrekking van brondocumenten voor identiteit en de attribuutverstrekking bepaalt.

Een observator met een wat machiavellistische kijk zou kunnen zeggen dat gebrek aan vertrouwen geen reden hoeft te zijn voor een impasse: één van de partijen kan zijn opvatting toch "doordrukken". Maar omdat alle partijen hindermacht hebben is dat ook geen optie: eID leveranciers kunnen via politiek, het maatschappelijk middenveld of de rechter initiatieven van de overheid blokkeren. De overheid kan succesvol samenwerking met eID leveranciers traineren en er voor zorgen dat er geen eID stelsel komt of zoveel onzekerheden boven de markt laten hangen, dat het vertrouwen in de komst van een eID weg is en het bedrijfsleven wacht met investeringen.

De situatie kan naar de mening van ECP worden doorbroken door het eID stelsel veel meer op hoofdlijnen en techniekonafhankelijk te formuleren (zoals de Europese eIDAS regulation dat voorstelt). De overheid moet de hoog niveau private eID middelen, die op de markt zijn en die voldoen aan die afspraken, vertrouwen bij toegang tot online overheidsdiensten. En tenslotte, door een helder signaal af te geven dat dat de overheid het elektronische WID pas op termijn zal introduceren, en de gebruiksmogelijkheden daarvan zal beperken tot activatie van hoog niveau eID middelen.

In een toekomst waarin consumenten gewend zullen raken om op allerlei manieren met een hoog niveau eID middel hun online identiteit te bewijzen, kan de uitgifte van zo'n eWID om andere eID's te activeren de kosten van de uitgifte en uitrol van deze hoog niveau eID's beperken. Het zal de drempel voor nieuwe toetreders op de markt van eID middelen enorm verlagen. En het geeft de overheid de mogelijkheid, om enerzijds de uitrol en het gebruik van hoog niveau eID's te versnellen en anderzijds invulling te geven aan de verantwoordelijkheid te bepalen welke personen in Nederland een identiteit hebben.

Bijlage I: Achtergrond en context consultatie eID en bedrijven.

Achtergrond

Dit advies heeft als aanleiding het Algemeen Overleg tussen de Tweede Kamer en de minister van Binnenlandse Zaken van 25 juni 2014, waarin de minister de Tweede Kamer heeft toegezegd een consultatie te organiseren onder bedrijfsleven, burgers en belangenorganisaties over de mogelijkheid en de wenselijkheid van een publiek eID-middel

De minister licht deze consultatie als volgt toe: "We zien af van het maken van een DigiD-kaart, maar ik wil niet op voorhand het gesprek met de markt aangaan met als doel dat we helemaal afzien van een publiek middel"

De toezegging die de minister aan de Tweede Kamer heeft gedaan wordt langs drie hoofdsporen uitgewerkt:

- Een internationale vergelijking; welke EU-lidstaten hebben welke (publieke- en private) middelen en diensten en welke argumentatie ligt aan hun keuze ten grondslag. Welk gebruik wordt gemaakt van eID-middelen;
- Consultatie van marktpartijen. In samenwerking met het ECP (Platform voor de Informatiesamenleving) en Nederland ICT vindt deze afstemming plaats. VNO/NCW en MKB zijn betrokken.
- Dialoog met burgers en burgerbelangenorganisaties.

Hiernaast vindt een juridische toetsing plaats en wordt de kosten-batenanalyse eNIK (2011) herijkt.

Dit advies werkt spoor II uit.

Doel van de consultatie (spoor II)

Het doel van de consultatie is als volgt:

De consultatie moet inzicht bieden in de argumenten van private partijen voor of tegen het ontwikkelen, produceren en uitgeven van publieke eID-middelen en de achtergronden en overwegingen daarbij. Het onderzoek verzamelt de informatie die hiervoor nodig is en haalt deze op bij individuele DIENSTENAANBIEDERS (degenen die diensten aanbieden en daarbij behoefte hebben aan een betrouwbaar proces van authenticatie en autorisatie, de relying parties) en brancheorganisaties, zowel in de private sector als in de semipublieke sector.

Een consultatie van DIENSTENLEVERANCIERS (degenen die middelen leveren in het eID Stelsel) wordt uitgevoerd in samenwerking met Nederland ICT. De onderzoekers zullen daarbij overleggen met Nederland ICT over (tussen)resultaten zodat de onderzoeksresultaten vergelijkbaar zijn.

De uitkomsten van het onderzoek worden, met de uitkomsten van de andere hoofdsporen, ter onderbouwing van een voorstel voor het al dan niet uitgeven van een publiek eID-middel aangeboden aan –in eerste instantie- de minister van BZK –in tweede instantie- de ministerraad;

Het voorstel aan de minister moet antwoord geven op de vraag of het mogelijk en wenselijk is dat de overheid een publiek eID-middel realiseert op één of meer bestaande dragers;

Over het voorstel wordt advies uitgebracht door de Interdepartementale Regiegroep Publieke eID-middelen en de Stuurgroep eID.

Het rapport wordt openbaar gemaakt en het wordt hoogstwaarschijnlijk meegezonden aan de Tweede Kamer, wanneer deze wordt geïnformeerd over het kabinetsbesluit over het publieke eID-middel.

De hoofdvraag voor de consultatie is: welke mogelijke rolverdeling bij het uitgeven van eID-middelen, tussen overheid en private partijen, de betrokken organisaties en bedrijven – de DIENSTENAANBIEDERS (degenen die diensten aanbieden en daarbij behoefte hebben aan een betrouwbaar proces van authenticatie en autorisatie) zien.

Deelvragen die uit de hoofdvragen voortvloeien zijn:

- Aan welke type rolverdeling wordt door de DIENSTENAANBIEDERS de voorkeur gegeven;
- Wat zijn daarvoor de argumenten;
- Wat is –in kwantitatieve zin- het 'marktaandeel' van de ondervraagde sectoren, in termen van (potentieel) gebruik van publieke eID-middelen[4];
- Is er een verband tussen de sector waarvan respondenten deel uitmaken en de voorkeur die zij hebben voor een type rolverdeling tussen de overheid en het bedrijfsleven.

Framing

De observatie van ECP is dat in de huidige discussie over de verhouding publiek/privaat de keuze van de terminologie een van de redenen is waarom er veel misverstanden zijn ("framing"). Wij stellen voor om het onderzoek zo op te zetten dat expliciet en herkenbaar blijft welk perspectief en welke begrippen onze gesprekspartners kiezen om hun voorkeuren te beschrijven en in het advies een paragraaf op te nemen of keuze van terminologie kan helpen de discussies en samenwerking vruchtbaarder te maken.

4

Bijlage II: het eID stelsel.

Deze bijlage gaat in op de vraag hoe het advies zich verhoudt tot het werk dat overheid en marktpartijen al hebben gedaan rond de verhouding publiek/privaat.

Het eID stelsel, waar de Minister over spreekt, is een initiatief van diverse ministeries en marktpartijen.

Doelstellingen van het eID Stelsel zijn:

- 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.

Het eID Stelsel moet het volgende mogelijk maken:

- authenticatie met een hoog betrouwbaarheidsniveau,
- verificatie van aanvullende gegevens (attributen),
- de ondersteuning van (wettelijke) vertegenwoordiging (machtiging) en
- een gemakkelijk te gebruiken elektronische handtekening.

Een belangrijke stap in de samenwerking tussen markt en overheid is het benoemen van de belangen van verschillende stakeholders die participeren in het eID Stelsel. Belangrijke belangen van het bedrijfsleven zijn:

- Het eID Stelsel draagt bij aan de betere beveiliging, de continuïteit van digitale dienstverlening, toekomstvastheid van oplossingen voor online authenticatie en autorisatie, maakt een hoger betrouwbaarheidsniveau mogelijk en zorgt voor betere omgang met privacygevoelige informatie.
- Het eID Stelsel zal voor de consument en burger het gemak en de gebruikersvriendelijkheid van procedures voor online authenticatie en autorisatie vergroten.
- Het stelsel zal kosten beperken van digitale authenticatie en verificatie.

Op 4 april 2014 hebben DIENSTENAANBIEDERS (degenen die gebruik willen maken van het stelsel), DIENSTENLEVERANCIERS (degenen die het stelsel mogelijk maken) en overheid een intentieverklaring getekend waarin zij verklaren samen te willen werken aan de ontwikkeling van een nationaal eID Stelsel:

> *Partijen streven naar een verdere digitalisering van dienstverlening aan burgers en bedrijven. Dit zowel met het oog op het verbeteren van de veiligheid en betrouwbaarheid van hun digitale dienstverlening als met het oog op verbetering van de efficiëntie en kostenbeheersing. Daarbij zal tevens worden aangesloten op Europese ontwikkelingen.*

Partijen onderschrijven de noodzaak tot innovatie van processen, middelen en voorzieningen waarmee veilig, betrouwbaar en op toekomstbestendige wijze toegang tot digitale dienstverlening wordt verkregen.

Partijen onderschrijven de wenselijkheid en noodzaak van een multimiddelen-strategie, die inhoudt dat burgers en bedrijven, waar mogelijk, keuzevrijheid hebben ten aanzien van de eID- middelen die zij bij het verrichten van digitale transacties in het publieke en private domein gebruiken.

De rol van de overheid staat in die intentieverklaring als volgt omschreven:

"De overheid acht het haar verantwoordelijkheid om over de ontwikkeling van een eID Stelsel de regie te voeren. Zij heeft daarvoor een programma eID ingericht. Zij wenst bij de ontwikkeling en realisatie van het eID Stelsel nadrukkelijk samen te werken met private partijen. Die samenwerking is essentieel voor breed draagvlak voor digitale dienstverlening en een succesvolle brede uitrol en acceptatie van eID-diensten en –middelen binnen een eID Stelsel."

Dit advies richt zich op een deelperspectief, namelijk dat van de DIENSTENAANBIEDERS die belang hebben bij een nationaal eID Stelsel, al dan niet direct betrokken zijn bij de ontwikkeling van het eID Stelsel en stelt hen de vraag of zij zich willen uitspreken over:

Het belang dat zij hechten aan het stelsel en of zij specifieke eisen stellen aan het stelsel.

Welke visie zij hebben op de rolverdeling overheid/bedrijfsleven bij de ontwikkeling, uitrol en in de gebruiksfase van het stelsel.

In alle gesprekken is het uitgangspunt dat de overheid alleen dat op zich neemt wat "moet" en het bedrijfsleven wat "kan".

Bijlage III: de eIDAS Regulation

Het is belangrijk dat de overheid bij de ontwikkeling van eID en het stelsel aansluit op de Europese ontwikkelingen, zo stellen de respondenten. Deze paragraaf geeft een beknopt, en selectief overzicht van een aantal, volgens de onderzoekers, relevante opmerkingen uit de Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (eIDAS).

eIDAS beschrijft de generieke en techniekonafhankelijke eisen aan eID schema's, met als doel dat online (overheids)diensten (en bedrijven) grensoverschrijdend op elkaars eID middelen kunnen vertrouwen. Die eisen betreffen o.a. zaken als de registratie van het eID middel, inrichten van toezicht en waarborgen op continuïteit, omgang met intrekking van eID's, omgang met privacy enz.

eIDAS heeft ten doel :

> "to enhance trust in electronic transactions in the internal market by providing a common foundation for secure electronic interaction between citizens, businesses and public authorities, thereby increasing the effectiveness of public and private online services, electronic business and electronic commerce in the Union" (inleiding, lid 2).

en:

> "to contribute to the digital single market by creating appropriate conditions for the mutual recognition of key enablers across borders, such as electronic identification, electronic documents, electronic signatures and electronic delivery services, and for interoperable e-government services across the European Union." (inleiding, lid 3)

T.a.v. de vraag van deze consultatie, over de rol van een publiek middel laat de eIDAS Regulation grote ruimte voor eigen invulling van de lidstaten (lid 13). Maar de eIDAS Regulation geeft ook aan (in lid 17, inleiding) dat Europese lidstaten het gebruik van eID middelen en schema's in het MKB en onder consumenten moeten stimuleren, evenals innovatie (lid 26 en 28, 55) en gebruiksgemak van eID middelen en de schema's.

De Regulation bepleit daarom het **hergebruik van eID middelen** in verschillende contexten (bedrijf, overheid, consument) en door de eisen technologieneutraal te formuleren (lid 27) met als doel dat niet alleen tussen lidstaten maar ook binnen lidstaten eID middelen en stelsels die voldoen aan de eisen elkaars middelen en diensten moeten vertrouwen.

De eIDAS Regulation stelt voor dat de overheid het gebruik van kwalitatief goede diensten stimuleert door "**Qualified Trustservices**" te introduceren (lid 28): "eID schema's en middelen met die kwalificatie kunnen door burgers en bedrijfsleven gebruikt worden".

De eIDAS Regulation harmoniseert de **betrouwbaarheidseisen** die online diensten stellen aan identificatie en de eisen waar eID diensten aan moeten voldoen om aan die betrouwbaarheidseisen te voldoen (zie Inleiding, lid 15 en 16). Die eisen worden nu nog gedefinieerd in termen van de vertrouwensniveau's van STORK 1 t/m 4. in 2015 zal de STORK indeling worden vervangen door vertrouwensniveau laag, hoog en substantieel. Hoe Stork 3 en 4 zullen mappen op de hoog en substantieel wordt bekend gemaakt in 2015.

De Regulation maakt een onderscheid tussen

"**electronic identification scheme**": een stelsel voor elektronische identificatie waarbinnen elektronische identificatiemiddelen worden uitgegeven aan natuurlijke personen, rechtspersonen of natuurlijke personen, die rechtspersonen vertegenwoordigen

en

"**trust services**" ("vertrouwensdiensten"): een elektronische dienst die gewoonlijk tegen betaling wordt verricht en het onderstaande inhoudt: elektronische handtekeningen, zegels, tijdstempels, aangetekende bezorging en de certificaten die daarbij horen, alles wat nodig is voor authenticatie van websites of de opslag van handtekeningen, zegels en certificaten).

Doel van de eIDAS Regulation (zie de eerste paragrafen van dit hoofdstuk) is dat twee eID middelen of trustservices of deze schema's, uitgegeven onder verschillende schema's of in verschillende landen, maar die voldoen aan de STORK 3 of 4 eisen, elkaar kunnen vertrouwen als ze aan de eisen voldoen van de Regulation.

Een belangrijke eis die de eIDAS regulation aan de schema's stelt is **Privacy by Design** (artikel 12, lid 3, c), maar ook dat een overheid de natuurlijke of de rechtspersoon kan traceren op het moment dat dat nodig is (inleiding, lid 33).

Het onderscheid dat in dit advies wordt bepleit tussen een brondocument voor de digitale identiteit, dat wordt tussen uitgifte van hoog niveau eID middelen op basis van fysieke controle en een afgeleide eID, dat wordt verstrekt of geactiveerd op basis een eerder verstrekt hoog niveau eID middel is niet strijdig met de Regulation. Immers: de Regulation stelt dat wanneer een certificaat wordt uitgegeven ten behoeve van een trust service, de uitgever de identiteit moet verifiëren van degene aan wie het certificaat wordt uitgegeven. Dat kan op vier verschillende manieren: direct "physical presence" (de methode die we nu gebruiken bij het uitreiken van STORK 3 en 4 certificaten) of "remotely" (waarbij een gekwalificeerd certificaat wordt gebruikt, dat eerder is verstrekt op basis van de fysieke controle).

In de interviews komt de eis terug dat de natuurlijke persoon moet kunnen worden getraceerd, wanneer iemand zich kenbaar heeft gemaakt met een eID. De eIDAS regulation (artikel 7, lid 1, punt d, Eligibility for notification of electronic identification schemes) stelt dat de overheid die een eID stelsel aanmeldt met de betrouwbaarheidsniveau substantieel en hoog waarborgt dat de persoonsidentificatiegegevens op het moment van uitgifte kunnen worden gekoppeld aan de natuurlijke persoon ("the notifying Member State ensures that the person identification data uniquely representing the person in question is attributed, in accordance with the technical specifications, standards and procedures for the relevant assurance level set out in the implementing act referred to in Article 8(3), to the natural or legal person referred to in point 1 of Article 3 at the time the electronic identification means under that scheme is issued;)

De manier waarop de overheid die koppeling tussen een natuurlijke person en de identificerende gegevens waarborgt ligt open.

Bijlage IV: Casusbeschrijvingen

Casus 1. Bouw: Bouwend Nederland.

Bouwend Nederland
de vereniging van bouw- en infrabedrijven

Bouwend Nederland is de vereniging van bouw- en infrabedrijven en met ongeveer 4300 aangesloten bouwbedrijven de grootste ondernemersorganisatie in de bouw.

In de bouw is een grote behoefte aan eID rond vier verschillende domeinen:

1. **procesautomatisering**: er zijn bij een bouwproject tientallen aannemers en onderaannemers betrokken. Tal van toeleveranciers leveren producten. De partijen maken in het ideale geval gebruik van dezelfde digital bouwdocumenten, maar in de praktijk is dat nog niet het geval. De faalkosten van deze processen bedragen zo'n 5% van de bouwsom. Deze faalkosten zijn eigenlijk onacceptabel in tijden van economische crisis en Bouwend Nederland heeft met het factuurportaal een overkoepelende infrastructuur geschapen om digitale en automatische gegevensuitwisseling tussen de vele betrokken partijen te faciliteren. Bij iedere transactie moeten de personen aan beide kanten van de digitale lijn eenduidig worden geïdentificeerd en het moet duidelijk zijn wat de bevoegdheden zijn van die persoon. Bouwend Nederland heeft gekozen voor eHerkenning als oplossing om identificatie mogelijk te maken: met een middel kunnen medewerkers zich kenbaar maken bij het bouwportaal, of worden de eID middelen waarmee ze zich kenbaar maken binnen hun eigen bedrijfssystemen gebruikt. Het voordeel van eHerkenning is dat maar ook bij veel gemeenteloketten en vergunningenloketten. De verwachting is dat deze middelen ook gebruikt kunnen worden voor andere overheidsdiensten.

2. **Verzekeringen**: bouwmaterialen moeten op de bouwplaats worden afgeleverd en moeten, voordat voor ontvangst wordt getekend, worden geïnspecteerd. In de praktijk gaat hier veel in mis: het is niet meer duidelijk wie een vracht heeft afgeleverd, wie deze heeft geïnspecteerd en geaccepteerd. Voor de vervoerder levert dit ook problemen op: onvoorspelbare kosten, mogelijk extra transport en vertragingen. En dat leidt tot hogere verzekeringspremies. Omdat zoveel verschillende mensen (incidenteel) bij dit proces zijn betrokken is het complex en duur om hen eenmalig van een betrouwbaar eID middel te voorzien en dit proces helemaal digitaal af te handelen.

3. **Vergunningen** en communicatie met de overheid: de werknemers op de bouwplaats moeten regelmatig in contact treden met overheden voor vergunningen of om informatie op te vragen (bijvoorbeeld over de ondergrond). Een centrale systematiek om vanuit een bouwproject mensen te machtigen en de informatie die uit die opvragingen komt goed op te slaan is belangrijk voor bouwprojecten. Met het bouwportaal en eHerkenning lost de bouw dit probleem op.

4. **Wet ketenaansprakelijkheid** stelt de opdrachtgever aansprakelijk wanneer er iets niet in orde is met werkvergunningen. Deze aansprakelijkheid vergt grote investeringen van bouwbedrijven: het optuigen van een systeem voor het identificeren en controleren van mensen is kostbaar. Ook uitzendbureaus moeten instaan voor betrouwbare identificatie en de toegang tot de bouwplaats moet toezicht op worden ingericht.

De eisen (genoemd in hoofdstuk 2) aan een eID systeem vloeien vooral voort uit deze vier behoeften.

Iedere Nederlander die betrokken is of raakt bij een bouwproject en daarbij digitaal gegevens uitwisselt, beschikt idealiteit over een eigen hoog niveau eID dat meteen gebruikt kan worden op het moment dat dat nodig is. Daarom is het belangrijk dat het eID middel snel wordt uitgerold en iedere Nederlander waar de bouw zaken mee doet beschikt over zo'n hoog niveau eID: liever vandaag dan morgen. Ook eID systemen uit andere sectoren moeten worden gebruikt: denk aan een hoog niveau eID uit de chemische industrie, logistiek of van een overheidsinstelling.

De eis dat verschillende eID's moeten kunnen worden herleid tot een enkele natuurlijke persoon is belangrijk in deze sector: om de juridische aspecten te kunnen afdekken.

Een belangrijk aandachtspunt voor de bouw zijn de kosten van het uitgifteproces: wanneer bouwbedrijven of uitzendbureaus zelf een (duur) uitgifteproces moeten inhuren of inrichten of wanneer medewerkers pas na enkele dagen aan het werk kunnen (omdat een betrouwbare eID moet worden uitgereikt) is dat een belangrijke beperking.

Casus 2. Logistiek: Transport en Logistiek Nederland.

TLN is de grootste werkgeversorganisatie van transporterend Nederland. Met circa 5.600 kleine, middelgrote en grote transportondernemers en logistieke dienstverleners.

In de transport is de vrachtbrief een cruciaal document, dat wordt gebruikt tijdens de vracht en bij de financiële afhandeling. Deze documenten worden nog op papier afgehandeld: bij iedere vracht is een begeleidend document nodig en de verwerking van deze documenten is een grote kostenpost: het overtikken in systemen leidt tot (kostbare) fouten en veel handmatig werk. Handtekeningen en namen zijn niet herleidbaar tot natuurlijke personen, waardoor, als er iets fout gaat, moeilijk te traceren is wie betrokken was.

De grote vrachtbedrijven besteden veel vrachten uit aan kleine bedrijven: het geven van opdrachten (via de vrachtbrieven) en de afhandeling is nog vaak op papier.

TLN en de grote transporteurs hebben daarom het initiatief genomen om een logistiek portaal te ontwikkelen waarin kleine transporteurs hun brieven digitaal kunnen ontvangen en kunnen invullen. De kosten van de verwerking van een vrachtbrief zijn ruim €20. Die kosten kunnen tot enkele Euro's worden teruggebracht (waarbij natuurlijk in het klein MKB waar mensen niet full time op het verwerken van vrachtbrieven zitten en functies combineren niet altijd direct merkbaar zal zijn).

Daarnaast heeft iedere chauffeur een vergunning nodig. Die wordt verstrekt door de Stichting NIWO (Nationale en Internationale Wegvervoer Organisatie). De toezichthouder zou eigenlijk bij het verlenen van de vergunningen al een eID moeten verstrekken, waarmee de chauffeur ook digitaal zijn vrachtbrieven kan afhandelen.

De tweede toezichthouder, de Inspectie voor Leefomgeving en Transport houdt zich op rijtijden en de uitvoering (bijvoorbeeld gevaarlijke stoffen). Het toezicht rond de rijtijden is al grotendeels digitaal.

TLN heeft daarnaast behoefte aan een hoog niveau eID waar de meeste Nederlanders over kunnen beschikken, omdat in toenemende mate vrachten ook worden bezorgd bij particulieren. Het bezorgen van grotere en duurdere pakketten zou daarmee gemakkelijk en veiliger zou kunnen worden. Nu is dat een kostbaar proces: het herkennen van identiteitsdocumenten en het ontbreken van gevalideerde adresgegevens maakt dat misbruik moeilijk kan worden opgespoord en is een afbreukrisico voor de transporteur.

Casus 3. Accountancy: SRA.

De SRA is een koepelorganisatie voor accountants, met enkele honderden leden, die voor de eigen leden diensten verzorgt om de kwaliteit van de eigen leden te vergroten. Bijvoorbeeld door scholing te verzorgen en leden te adviseren over bedrijfsvoering en het gebruik van ICT.

In de accountancy speelt volgens de SRA eID een centrale rol bij dienstverlening. Vaak werken accountantskantoren en administratiekantoren nauw digitaal samen met hun klant en het moet duidelijk zijn wie met welke bevoegdheden welke wijzigingen in een administratie heeft aangebracht.

eID speelt een rol bij de Belastingaangiftes, die door de klant zelf ondertekend moeten worden voordat ze worden verstuurd naar de Belastingdienst. Het versturen en ontvangen van digitale documenten van de Belastingdienst, zoals de kopie aangifte is nu nauwelijks met veiligheidswaarborgen omgeven: dat is in toenemende mate een probleem. Ook het waarmerken van informatie is van toenemend belang: is een kopie aangifte (in SBR) ongewijzigd als hij wordt gebruikt voor een kredietaanvraag (ook in SBR).

De Beroepsvereniging van accountants (NBA) heeft inmiddels een beroepscertificaat ontwikkeld, waarmee accountants een verklaring mede kunnen ondertekenen en waarmee gecontroleerd kan worden of de accountant bevoegd is en of het document later nog is veranderd.

Een belangrijk aspect in dit traject is ook machtigen: is een medewerker van een bedrijf gemachtigd om een transactie uit te voeren en wie heeft hem dan gemachtigd ? Zijn er grenzen aan die machtiging ?

Veel accountantskantoren en boekhoudsystemen maken al gebruik van eID en bekostigen dat zelf. Het is een randvoorwaarde voor dienstverlening.

Het belang van een breed gebruik eID is voor de accountancy groot: nu moet iedere nieuwe klant of medewerker van een klant worden uitgerust met een eID en de machtigingen moeten worden aangepast.

De EDI-circle.

Al meer dan twintig jaar wisselen kredietverleners, de grote toeleveranciers van veebedrijven (diervoeding, meststoffen), Belastingdienst en accountants digitale informatie uit over de transacties en afhandeling daarvan. Daarvoor is een EDI-keten opgezet, een framework voor digitale gegevensuitwisseling, dat dateert uit de eerste decennia van de ICT en nog steeds breed wordt gebruikt: een EDI keten was de eerste jaren helemaal gesloten (met inbellen en dedicated lijnen), en had een eigen netwerk. Maar steeds meer is de keten ook via internet toegankelijk. Daarmee wordt betrouwbare authenticatie een groter issue.

Machtigingen

Een belangrijk punt daarin is het machtigingsregister: moet dat een publieke voorziening worden, een combinatie van publiek en privaat of een private voorziening waar ook andere partijen gebruik van kunnen maken. Kosten spelen hierin een rol, maar ook privacy: wie heeft toegang tot dat register en welke informatie kan daaruit worden gehaald. De SRA stelt zich op het standpunt dat het machtigingsregister rond aangiften door de overheid moet worden ingericht.

Casus 4. Webwinkels.

Voor webwinkels is een betrouwbaar en hoog niveau eID, dat door Nederlanders die dat willen, gebruikt kan worden belangrijk om vier redenen:

1. Het **registreren van digitale klantgegevens** is noodzakelijk om er voor te zorgen dat een klant, als hij terug komt, weer terug kan naar zijn eigen gegevens en eerdere bestellingen of voorkeuren kan bekijken of aanpassen. Iedere webwinkel organiseert zelf de registratie en opslag van gegevens. Dat is niet hun core-business. De aanvallen op dit soort persoonsgegevens worden frequenter en geavanceerder en daarmee is het online toegankelijk houden van deze gegevens steeds meer een afbreukrisico: een gehackte database met persoonsgegevens kan een webwinkelier enorme schade berokkenen.

2. Het moeten opgeven van allerlei gegevens is bovendien een **conversieremmer**: het invullen van gegevens is een bron van fouten en vaak loopt de bestelling daar al mis.

3. Voor ongeveer 3% van de bestellingen is **leeftijdsverificatie** nodig: bijvoorbeeld voor drank en rookwaar, films, games.

4. **Innovatie van online dienstverlening**. Het volledig online afhandelen van diensten die handtekeningen vragen zijn nog niet goed mogelijk

eID biedt allerlei nieuw mogelijkheden dat klanten (gevalideerde en betrouwbare) gegevens verstrekken zonder dat ze hun identiteit prijsgeven. Bijvoorbeeld: de klant kan bijvoorbeeld helemaal anoniem blijven en toch overtuigend bewijs leveren dat hij of zij ouder is dan 18 jaar. Bij

een leeftijdsverificatie kan de klant een door de overheid, telecomprovider of bank (of andere partij die de persoonsgegevens en het identiteitsbewijs van die persoon heeft gecontroleerd) gevalideerde vlag tonen, dat hij of zij ouder is dan achttien en met een pincode bewijzen dat die gevalideerde vlag ook echt bij hem of haar hoort, zonder dat de webwinkelier ook maar iets weet van de naam, adres of andere gegevens. Als er verdenking is dat er identiteitsfraude is gepleegd (iemand heeft de gevalideerde leeftijdsverklaring van iemand anders getoond) kan justitie dat controleren door bij de identiteitsproviders controles uit te voeren. Zo kan ook een adres worden gevalideerd. Stel dat PostNL een pakket heeft bezorgd op adres/naam xyz en bij een andere webwinkel wil die persoon een grote bestelling doen en die afleveren op hetzelfde adres. PostNL kan bevestigen dat er op die naam en met dat adres eerder een bestelling is afgeleverd en dat daar geen klachten of malversaties aan de hand waren.

Het eID stelsel zou het mogelijk maken voor klanten om hun persoonlijke gegevens zelf te beheren en te verstrekken via het stelsel. Om die gegevens goed te beheren heeft de klant zelf een goed en betrouwbaar eID nodig.

Casus 5. Zorg: Vita Valley

VitaValley is een kennisnetwerk voor vernieuwing in de zorg. Met partners ontwikkelen en realiseren zij zorginnovaties. VitaValley faciliteert innovatie door kennis en ervaring te delen en een aanjagende rol te spelen door partijen te verbinden en te ondersteunen. Partijen zijn zorgaanbieders, ziekenhuizen, universiteiten, kennisinstituten, technologiebedrijven etc.

Het veilig en goed uitwisselen van digitale gegevens speelt een centrale rol in de zorg. Eigenlijk staat in alle projecten betrouwbare identificatie centraal: en dan meteen op het hoogste betrouwbaarheidsniveau. Het is kostbaar om dat voor ieder nieuw project goed te regelen en betrokken van de juiste eID middelen te voorzien. De zorgvrager moet immers de eigen gegevens in kunnen zien en kunnen controleren wie gegevens in ziet. Zorgverleners moeten gecontroleerd toegang kunnen krijgen tot de gegevens van zorgvragers waar ze een relatie mee hebben en ook kunnen constateren wanneer er onregelmatigheden plaatsvinden.

Iedere zorginstelling en ieder zorgproject worstelt met het inrichten van authenticatie en autorisatie. Dat belemmert vernieuwing en concurrentie: wanneer authenticatie en autorisatie eenmaal is ingeregeld met een aantal partijen, is het kostbaar om een overstap te maken naar een andere leverancier van zorg.

Het eID stelsel kan dienen als best practice voor het inrichten van eID waardoor het mogelijk wordt om gemakkelijker over te stappen naar andere technologieën en andere dienstverleners.

Bijlage V: respondenten

Het rapport is niet onomstreden: er zijn een aantal paragrafen waar diverse meelezers zich niet in konden vinden. In hoofdstuk 5 hebben we proberen aan te geven waar die verschillen in inzicht uit voortkomen en hoe ECP tot het advies is gekomen. De verschillen van inzicht hebben vooral te maken met het (wan)vertrouwen van markt en overheid. Ondanks die meningsverschillen hebben de onderstaande personen toegestemd hun naam en bijdrage te vermelden.

Bestuurders van de sectoren, die zich achter het advies stellen (bijlage IV beschrijft de casussen voor elk van deze sectoren):

Bouw: Bouwend Nederland	Maxime Verhagen (voorzitter)
Cross-sectoraal: CIO-Platform	Ronald Verbeek (directeur)
Zorg: Vita Valley	Dik Hermans (Raad van Bestuur Vita Valley, boegbeeld doorbraakproject zorg en ICT, voormalig voorzitter College van Zorgverzekeringen.
Logistiek: Transport en Logistiek Nederland	Peter Sierat (directeur)
Accountancy: SRA	Cees Meijer (directeur SRA)
Accountancy: Alpha accountants, SRA	Fu Khan Tsang (directeur Alpha accountants, voorzitter vakgroep vaktechniek SRA, mede initiator van EDI-circle agrarische sector)

Beleidsmedewerkers, Experts en Belanghebbenden

Naam	**Organisatie**	**Functie**
Beleidsmedewerkers die zich achter het advies stellen		
Joppe Duindam	Bouwend Nederland	Adviseur
Wout van den Heuvel	Transport en Logistiek Nederland	Adviseur
Tony van Oorschot	SRA (Samenwerkende Register Accountants)	Adviseur
Arie van Bellen	ECP	Directeur
Experts die hebben bijgedragen aan de		

feitelijke correctheid en casussen:		
Rene van den Assem	Expertise: eID, onderwijs, zorg, PKI	Voorzitter College Belanghebbenden TTP.nl en adviseur eID in de onderwijssector
Jaap Kuipers	Expertise: eID (o.a. zorg, verzekeringen) en maatschappelijke aspecten eID	Initiatiefnemer en onafhankelijk adviseur, PIMN – Platform Identity Management Nederland
Experts met rol van belanhebbende:		
Bart Pegge	Nederland ICT	Adviseur, onderzoeker spoor III (consultatie eID leveranciers)
David de Nood	VNO-NCW	Adviseur: zowel vanuit de relying parties (bedrijfsleven) als de eID leveranciers.
Poppe Wijnsma	PKI partners	Adviseur PKI overheid

Waardevolle bijdrage aan de gedachtenvorming waren de gesprekken met:

Webwinkels: Bol.com	Daniel Ropers (directeur/oprichter), boegbeeld doorbraakproject Massaal Digitaal, lid van Thuiswinkel Waarborg.
Onderwijs: Groep Educatieve Uitgeverijen	Rene Montenarie (directeur)
Overheid/zorg: Stichting Rinis	Rob Verweij (directeur)
eID leveranciers: UL-TS	Arjan Geluk (adviseur)

Overheid

Over de (diverse) manier waarop binnen de Rijksoverheid wordt gedacht over eID kreeg ECP input van ambtenaren van BZK, het Ministerie van Economische Zaken en het Ministerie van Financiën.

ECP wil alle respondenten en meelezers graag bedanken dat zij ondanks de verschillen in inzicht toch zijn blijven meedenken en meepraten.