Anna van Buerenplein 1
2595 DA Den Haag
Postbus 96800
2509 JE Den Haag

www.tno.nl

T +31 88 866 90 00

TNO-rapport

TNO 2016 R10582 | Eindrapport v1.1

Uitkomsten van een onderzoek naar de betrouwbaarheid en veiligheid van de pilots publieke en private middelen in het BSN-domein

Datum	27 mei 2016
Auteur(s)	Hugo Gelevert Arnold Roosendaal Nicole de Koning Joke Kort Hiddo Hut
Exemplaarnummer	
Oplage	
Aantal pagina's	126 (incl. bijlagen)
Aantal bijlagen	5
Opdrachtgever	Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Projectnaam	Onderzoek naar de betrouwbaarheid en veiligheid van de pilots publieke en private middelen in het BSN-domein
Projectnummer	060.21706

Samenvatting

Het kabinet wil dat burgers en bedrijven in de toekomst al hun zaken met de overheid digitaal kunnen afhandelen. Overheid en bedrijfsleven werken daartoe samen aan de ontwikkeling van een stelsel voor betrouwbare elektronische toegangsdiensten.

Eén van de uitgangspunten hierbij is dat het stelsel zich niet beperkt tot alleen de overheid. Ook bedrijven moeten in verschillende rollen deel kunnen nemen aan het stelsel. Hierdoor ontstaat een publiek-private samenwerking waarin bedrijven gelijke kansen krijgen om producten en diensten te ontwikkelen die kunnen worden gebruikt voor identificatie en authenticatie. Een tweede uitgangspunt is, dat authenticatiemiddelen voor eindgebruikers worden ontkoppeld van dienstaanbieders. Er is sprake van een 'multimiddelenstrategie': eindgebruikers moeten kunnen kiezen welk(e) middel(en) zij willen gebruiken voor het inloggen, waarbij een gekozen middel moet kunnen worden gebruikt op de webpagina's van verschillende dienstaanbieders.

Voor het beproeven van de technologie en de processen rondom deze identificatie- en authenticatiemiddelen worden in de eerste helft van 2016 vier pilots uitgevoerd. In opdracht van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) heeft TNO de betrouwbaarheid, de beschikbaarheid, de veiligheid, de privacy en de technische werking van de in drie van de vier pilots beproefde middelen onderzocht, alsmede de ervaringen van de in die pilots deelnemende leveranciers, dienstaanbieders en gemeenten. Het betreft de pilot Idensys, de pilot iDIN en de pilot Publiek Middel, ofwel de pilots publieke en private middelen in het BSN-domein.[1] Dit rapport bevat de uitkomsten van dat onderzoek. Het rapport is bedoeld als bron voor de Commissie Kuipers, die de ministers van BZK en Economische Zaken (EZ) zal adviseren over de mogelijkheden en de wenselijkheid van de diverse identificatie- en authenticatiemiddelen die in de pilots worden getest.

Het onderzoek van TNO is opgebouwd rondom de onderzoeksvragen die zijn verwoord in de opdracht aan TNO. Deze vragen hebben betrekking op de techniek, de privacy en de ervaringen van gebruikers (middelenleveranciers, dienstaanbieders en gemeenten) tijdens de pilots. TNO heeft de vragen beantwoord op basis van interviews, meeloopdagen, pilotrapportages en documentatie die is aangeleverd. Ook zijn enkele middelen uitgeprobeerd op websites van dienstaanbieders. Het onderzoek is gestart op 4 februari 2016 en de door BZK vastgestelde deadline voor het opleveren van de onderzoeksresultaten lag op 27 mei 2016. De meetperiode besloeg daarmee effectief de maanden maart en april. Omdat verschillende pilots doorliepen tot na deze periode, heeft het onderzoek van TNO het karakter van een momentopname, beperkt tot de gegevens die tijdens de meetperiode konden worden verkregen en tot de ervaringen van de partijen die tijdens de meetperiode startten of al voor de meetperiode waren gestart.

[1] De vierde pilot die wordt uitgevoerd, en waarin door middel van Remote Document Authentication (RDA) een extra controle aan het huidige DigiD-stelsel wordt toegevoegd, maakt geen onderdeel uit van het onderzoek van TNO.

Ten aanzien van de vragen die betrekking hebben op de betrouwbaarheid, de beschikbaarheid, de veiligheid en de technische werking van het stelsel concludeert TNO het volgende:

- TNO heeft enkele middelen zelf uitgeprobeerd. Het betrof de middelen Digidentity, iDIN ING, iDIN Rabobank en eRijbewijs. Voor deze middelen is op basis van eigen onderzoek vastgesteld dat ze succesvol kunnen worden gebruikt om in te loggen bij websites van dienstaanbieders. Andere middelen zijn niet door TNO zelf geprobeerd maar waren wel onderdeel van dit onderzoek.

- Het inlogproces van de uitgeprobeerde middelen Digidentity, iDIN ING, iDIN Rabobank en eRijbewijs werkte in de test van TNO technisch goed en vlot.

- Bij het uitproberen van Digidentity en iDIN ING op de website van de Belastingdienst Aangifte Inkomstenbelasting komt een eindgebruiker met beide middelen op de correcte gebruikerspagina uit. Bij het uitproberen van eRijbewijs op de DigiD-website komt een eindgebruiker op dezelfde gebruikerspagina's uit als wanneer hij met zijn reguliere DigiD zou hebben ingelogd.

- Uit de ontvangen rapportages bleek dat er voor de verschillende pilots iedere dag eindgebruikers hebben ingelogd, met verschillende middelen. Hieruit concludeert TNO dat de benodigde technische infrastructuur van de betrokken partijen elke dag beschikbaar is geweest. Er zijn echter wel discrepanties tussen het aantal geslaagde authenticaties vanuit het perspectief van het BSNk en het aantal succesvolle logins op sites van dienstaanbieders.

Met betrekking tot de vragen over de privacy-aspecten van de pilots luidt de conclusie van TNO dat:

- Voor alle drie pilots PIA's zijn uitgevoerd: bij Idensys en Publiek Middel vanuit de overheid op stelselniveau, en bij iDIN hebben de individuele banken een PIA uit moeten voeren om toe te kunnen treden tot het iDIN-stelsel.

- Voor de private middelen van Idensys en iDIN een eindverantwoordelijke instantie (respectievelijk de minister van EZ en de Betaalvereniging Nederland (BVN)) heeft verklaard dat aan de privacy-vereisten van de respectievelijke stelsels is voldaan.

- Er nadere mitigerende maatregelen geïdentificeerd zijn door de ketenpartners, die geïmplementeerd dienen te worden voor een brede uitrol na de pilotfase.

- Communicatie over gegevensverwerkingen nog veel aandacht vereist, zowel richting burgers als tussen betrokken partijen onderling. Afspraken zijn wel vastgelegd in de normenkaders, maar vormen nog geen vanzelfsprekendheid voor alle betrokkenen.

De belangrijkste conclusies ten aanzien van de ervaringen van de in het onderzoek betrokken dienstaanbieders, gemeenten en middelenleveranciers, zijn dat:

- Er bij de partijen die bij de pilots zijn betrokken verschillen in perceptie bestaan ten aanzien van de pilots; het betreft bijvoorbeeld de doelstelling en reikwijdte ervan.

- Verschillende leveranciers (bij Idensys) en dienstaanbieders (bij iDIN: 'acceptanten') aangaven dat het lastig was om aan te sluiten ('live te gaan') bij een pilot. Genoemde punten waren de kosten en de doorlooptijd. Bij de pilot Publiek Middel speelde dit geen rol volgens de deelnemende partijen.

- Bij de pilot Publiek Middel de processen voor aanvraag en uitgifte van de documenten volgens de gemeenten over het algemeen goed verliepen. Wel werd aangegeven dat de communicatie richting burger op punten nog kan verbeteren. Ook werd gemeld dat burgers voornamelijk problemen ervoeren bij het installeren van de kaartlezer.

- Bij de pilot Idensys de communicatie vanuit de overheid volgens deelnemers beperkt en op punten onduidelijk was, bijvoorbeeld ten aanzien van het toekomstperspectief en het toekomstige financieringsmodel.[2] Een aantal betrokkenen gaf aan dat dit bij andere partijen in het veld en bij eindgebruikers tot onzekerheid leidt en daar een afwachtende houding opriep.

- De Belastingdienst en een bank aangaven dat hun aansluiting op de iDIN-pilot eenvoudig is verlopen. Met betrekking tot het aansluiten van nieuwe acceptanten (dienstaanbieders) is gezegd dat de doorlooptijd als lang en de kosten als hoog worden ervaren, hetgeen een belemmering kan zijn voor een verdere uitrol naar andere acceptanten.

Resumerend kan worden gesteld dat gedurende het onderzoek duidelijk is geworden dat de afzonderlijke middelen van de hiervoor aangehaalde multimiddelenstrategie in de praktijk technisch werken. Verschillende middelen konden worden gebruikt om bij dienstaanbieders in te loggen, ook via de verschillende stelsels (Publiek Middel, Idensys en iDIN). Deze stelsels bleken naast elkaar te werken en bieden burgers dus de keus om een type middel te kiezen dat zij prefereren.

Ook is gebleken dat er bij de pilots sprake is van middelen die onder verschillende stelsels vallen en dat er belangrijke verschillen zijn tussen de stelsels. Een verschil is bijvoorbeeld dat de stelsels hun eigen normenkaders hanteren ten aanzien van beveiliging (inclusief privacy) en betrouwbaarheid (LoA). Dat betekent dat de wijze van vaststellen van betrouwbaarheidsniveaus niet onderling uitwisselbaar is. Uit de aangeleverde documentatie valt niet op te maken of en zo ja welk toetsingskader is gebruikt om vast te stellen of een middel aan de normen voldoet, met andere woorden: op welke wijze en aan de hand van exact welke criteria toetsing plaatsvindt. Voor een verdere ontwikkeling en uitrol van de stelsels beveelt TNO aan een uniform normenkader te hanteren, met daarbij een uniform toetsingskader dat binnen de verschillende contexten van de stelsels toegepast kan worden.

Bij bovenstaande conclusies horen enkele kanttekeningen. Allereerst geldt dat TNO niet alles zelf heeft kunnen of mogen onderzoeken, maar zich bij de beantwoording

[2] Noot: het toekomstig financieringsmodel was geen onderdeel van de pilots.

van een aantal vragen heeft moeten beroepen op verklaringen van de daarvoor verantwoordelijke instanties. Het betrof dan vooral vragen die betrekking hebben op de vraag of aan de gestelde eisen voor toetreding van partijen tot de betreffende stelsels is voldaan. Daarnaast geldt met betrekking tot de borging van de privacy dat de eisen op papier helder zijn vastgelegd, maar dat TNO niet de mogelijkheid heeft gehad om de technische implementatie ervan te onderzoeken. Bovendien is alleen gekeken naar de pilots zoals deze gedurende de onderzoeksperiode zijn ingericht; TNO geeft geen uitsluitsel of deze inrichting ook daadwerkelijk de best mogelijke borging van privacy oplevert.

Een andere kanttekening is, dat TNO niet altijd de hele keten heeft kunnen doorlichten, maar zich in een aantal gevallen heeft moeten beperken tot puntmetingen. Ook wordt opgemerkt, dat niet altijd alle gewenste informatie kon worden aangeleverd door de bij de pilots betrokken partijen. In veel gevallen lag de oorzaak daarvan in het feit dat bepaalde data (nog) niet structureel werd bijgehouden tijdens de pilot. Aangezien TNO niet betrokken was bij de opzet en inrichting van de pilots, was dit een gegeven voor de onderzoekers. Het gevolg is dat de basis voor een aantal conclusies beperkt is. In voorkomende gevallen heeft TNO zich ingespannen om gegevens alsnog boven water te krijgen, danwel om via een alternatieve benadering tot beantwoording van de betreffende vragen te komen. De antwoorden in dit rapport zijn onderbouwd met bronvermelding zoals documenten, loggegevens, verklaringen of ontvangen e-mails.

TNO heeft een aantal aandachtspunten geïdentificeerd, die volgens TNO van belang zijn voor een verdere uitrol van de middelen en ontwikkeling van de stelsels:

1. Er is behoefte aan een uniform normenkader en stelsel van toezicht, om te waarborgen dat alle stelsels onder dezelfde vereisten en waarborgen vallen. Daarmee kunnen bijvoorbeeld de betrouwbaarheidsniveaus uit de stelsels vergelijkbaar worden gepresenteerd en is voor de eindgebruiker duidelijker bij wie een middel van een zeker niveau kan worden afgenomen.

2. Kijk naar verschillende mogelijkheden (ook buiten de huidige pilots) om privacy vorm te geven in de technische inrichting. Privacy moet bezien worden als een breder begrip dan alleen het voldoen aan de vereisten uit de Wbp, en omvat ook controle, transparantie en de mogelijkheid om activiteiten gescheiden te houden.

3. De verschillende middelen werken technisch naast elkaar. Voor burgers zou – ter voorkoming van fraude door derden – een middelen-overstijgend overzicht van de eigen actieve middelen en het gebruik daarvan beschikbaar moeten zijn.

4. De uitgangspunten voor de inrichting van de stelsels zijn, zowel technisch als organisatorisch, verschillend van aard. Houdt deze uitgangspunten voor ogen bij het beoordelen en nader vormgeven van de strategie voor elektronische toegangsdiensten. Tussen de verschillende stelsels bestaan (grote) verschillen in de historie en de ervaring met betrouwbare authenticaties, evenals met de wijze van inrichting van toezicht.

5. Onderzoek de mogelijkheden om de verwerking van het BSN tot een minimum te beperken. In bepaalde gevallen blijkt het BSN vaker over de lijn te gaan dan strikt noodzakelijk, vanwege de verplichte uitwisseling via het BSNk.

Tot slot, zoals genoemd had dit onderzoek het karakter van een momentopname. TNO beveelt dan ook aan om het onderzoek in het najaar van 2016 te herhalen, eventueel op onderdelen, om richting de toekomst ook lessen te trekken uit de ervaringen van partijen die tijdens de looptijd van dit onderzoek nog niet daadwerkelijk deelnamen aan de pilot, maar dat op korte termijn wel willen gaan doen. Ook de ervaringen van partijen die eventueel alsnog besluiten niet deel te nemen zijn daarbij interessant. Tevens kunnen aanpassingen die in de tussentijd worden getroffen op basis van de lessons learned en de bevindingen toe nu toe in een dergelijk vervolgonderzoek worden doorgelicht. Bovendien kunnen in een vervolg domeinen die nu nog buiten de scope van het onderzoek vielen worden meegenomen, inclusief hun mogelijke aandachtspunten. De onderzoekers hebben daartoe bewust een methodiek gehanteerd die herhaaldelijk kan worden toegepast, bijvoorbeeld nadat een nieuwe organisatie met een nieuw middel is toegetreden of nadat een al toegetreden organisatie een verandering heeft doorgevoerd aan de werking van een bestaand middel.

Inhoudsopgave

1 Inleiding

1.1 Achtergrond van het onderzoek

In 2012 stelde het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) het volgende:

'De Nederlandse maatschappij wordt in hoog tempo gedigitaliseerd. Voor de private en publieke sector is het vertrouwen van mensen en organisaties in elektronische dienstverlening essentieel. Dat vertrouwen komt steeds meer onder druk te staan, onder meer omdat het betrouwbaarheidsniveau van bestaande elektronische identificatiemiddelen (gebruikersnaam/wachtwoord) voor burgers niet toereikend is. Het is wenselijk dat op grote schaal eID-voorzieningen op hogere veiligheids-niveaus voor burgers beschikbaar komen, zodat het vertrouwen in de digitale dienstverlening geborgd blijft. Om de afhankelijkheid van één specifiek elektronisch identificatiemiddel (eID-middel) te beperken is het van belang een strategie te hebben waarin meerdere middelen beschikbaar zijn om dienstverlening te ontsluiten, een zogenoemde multimiddelenstrategie. Daarmee wordt een fallback bij calamiteiten gecreëerd' [1].

Overheid en bedrijfsleven werken daartoe samen aan de ontwikkeling van een stelsel voor betrouwbare elektronische toegangsdiensten. Eén van de uitgangspunten hierbij is dat dit stelsel zich niet beperkt tot alleen de overheid. Ook bedrijven moeten in verschillende rollen deel kunnen nemen aan het stelsel. Hierdoor ontstaat een publiek-private samenwerking waarin bedrijven gelijke kansen krijgen om producten en diensten te ontwikkelen die kunnen worden gebruikt voor identificatie en authenticatie [2].

Een tweede uitgangspunt van het stelsel is de multimiddelenstrategie. Hiermee moeten eindgebruikers kunnen kiezen welk(e) middel(en) zij willen gebruiken voor het inloggen en welke niet. Volgens de webpagina van de Rijksoverheid:

'*Dankzij Idensys (voorheen eID-Stelsel) kunnen mensen in de toekomst zelf kiezen hoe ze willen inloggen bij een organisatie. Bijvoorbeeld met een (hiervoor geschikt gemaakte) ID-kaart of bankpas. Zij zijn dan bij storingen niet afhankelijk van één digitaal inlogmiddel.*'[3]

Een belangrijke randvoorwaarde om online transacties betrouwbaar en veilig te kunnen uitvoeren, is dat er voldoende zekerheid bestaat over de identiteit van de bij een online transactie betrokken partijen. Het 'Masterplan eID' uit 2014 zegt hier het volgende over:

'De Nederlandse economie maakt dagelijks gebruik van de mogelijkheden die internet te bieden heeft en is er inmiddels sterk van afhankelijk. Denk aan het ophalen en uitwisselen van informatie, het delen van privacygevoelige gegevens en financiële transacties. Die afhankelijkheid zorgt voor een groot belang van vertrouwen in online identificatie en autorisatie. Het met grote zekerheid kunnen

[3] Zie https://www.rijksoverheid.nl/onderwerpen/digitale-overheid/inhoud/digitale-veiligheid-en-identiteit/naar-1-standaard-voor-elektronische-identiteit

vaststellen van iemands identiteit en bevoegdheid is cruciaal in een online samenleving' [3].

Voor het beproeven van de technologie en de processen rondom deze identificatie- en authenticatiemiddelen worden in 2016 een viertal pilots uitgevoerd in het publieke domein. De Minister van BZK heeft aan de Tweede Kamer toegezegd deze pilots te evalueren en heeft daartoe een evaluatiecommissie ingesteld: de Commissie Kuipers. Medio 2016 dient deze commissie advies uit te brengen aan de ministers van BZK en Economische Zaken (EZ). Op basis van dit advies is het kabinet voornemens om medio 2016 een standpunt voor te bereiden over de uitrol van de eID-middelen [4].

Om tot een advies te komen, zal de commissie zich mede baseren op twee extern uitgevoerde onderzoeken:

1. Een onderzoek naar de betrouwbaarheid, veiligheid, privacy, technische werking en de ervaringen van middelenleveranciers, dienstaanbieders en gemeenten die meedoen aan de pilots;
2. Een onderzoek naar de ervaringen van eindgebruikers (consumenten).

Dit rapport bevat de uitkomsten van het eerste onderzoek, zoals uitgevoerd door TNO. Het tweede onderzoek, naar de ervaringen van eindgebruikers, is gedaan door onderzoeksbureau Panteia dat daarover in een eigen rapport verslag uitbrengt.

1.2 Doelstelling van het onderzoek van TNO

Het door TNO uitgevoerde onderzoek heeft tot doel om de door BZK in de offerte-aanvraag gestelde onderzoeksvragen te beantwoorden. Deze onderzoeksvragen hebben betrekking op drie van de vier uitgevoerde pilots, namelijk de pilots publieke en private middelen in het BSN-domein: de pilot Idensys, de pilot iDIN en de pilot Publiek Middel.[4] Het achterliggende doel van de onderzoeksvragen is om inzicht te krijgen in de uitgevoerde pilots.[5]

In de offerte-aanvraag van BZK is dit als volgt verwoord:

1. Paragraaf 1.8, pagina 7 (pilots Idensys en iDIN):
   '*De scope van de pilots Idensys met hoogwaardige middelen in het Stelsel Idensys behelst de publieke diensten in het BSN-domein. Het doel van dit onderzoek is nagaan in hoeverre de middelen betrouwbaar, veilig, gebruiksvriendelijk en toegankelijk zijn en of de privacy is geborgd.*' [5]

2. Paragraaf 1.9, pagina 9 (pilot Publiek Middel):
   '*De scope van de pilots publieke eID-middelen is gericht op het aanvraagproces en op de transacties waarbij het publieke middel toegang geeft tot een publieke dienst in het BSN-domein. Het doel is om inzicht te bieden in de mate waarin voldaan is aan de gestelde criteria.*' [5]

[4] De vierde pilot die wordt uitgevoerd, en waarin door middel van Remote Document Authentication (RDA) een extra controle aan het huidige DigiD-stelsel wordt toegevoegd, vormt geen onderdeel van het onderzoek van TNO.

[5] De drie door TNO beschouwde pilots worden in hoofdstuk 3 beschreven. De door BZK aan TNO gestelde onderzoeksvragen zijn *verbatim* opgenomen in bijlage C.

Het onderzoek wordt vanuit de overheid begeleid door een begeleidingscommissie. De samenstelling van deze commissie en van de Commissie Kuipers is opgenomen in bijlage B.

1.3 Scope en afbakening

Het onderzoek van TNO is gebaseerd op de in de offerte-aanvraag opgegeven tijdslijnen en beperkt zich nadrukkelijk tot de drie in de voorgaande paragraaf genoemde pilots. Het onderzoek is gestart op 4 februari 2016 en de door BZK vastgestelde deadline voor het opleveren van de onderzoeksresultaten was 27 mei 2016. Opdat in mei de resultaten geanalyseerd en verwerkt konden worden, besloeg de meetperiode daarmee effectief de maanden maart en april.

De pilots liepen door tot na de meetperiode (verschillende zelfs tot na mei 2016). Het onderzoek van TNO is dan ook een momentopname, beperkt tot de gegevens die tijdens de meetperiode konden worden verkregen en tot de ervaringen van de partijen die tijdens de meetperiode zijn gestart. In overleg met de begeleidings-commissie is besloten deze partijen in drie groepen te verdelen, op grond van hun periode van actieve deelname aan de pilots tijdens de meetperiode:

1. De partijen die zijn gestart in de periode t/m 18 maart;
2. De partijen die zijn gestart in de periode van 19 maart t/m 15 april; en
3. Alle partijen die zijn gestart (of starten) op 16 april of later.

Met de deelnemers uit groep 1 zijn gesprekken, meeloopdagen, en workshops georganiseerd. Rapportages zijn opgevraagd over de maanden maart en april, en in de tweede helft van april heeft een belronde plaatsgevonden om de bevindingen te toetsen en laatste ervaringen op te halen. Voor groep 1 hebben de onderzoekers bovendien een aantal authenticatiemiddelen uitgeprobeerd, om de werking van het registratie- en gebruiksproces om in te loggen op een website van een dienstaanbieder zelf te ervaren.

De deelnemers uit groep 2 zijn slechts globaal meegenomen, aangezien zij pas laat tijdens de meetperiode zijn gestart c.q. nog over weinig voor het onderzoek relevante meetgegevens beschikten. Een deel van deze partijen is telefonisch geïnterviewd. Voor zover relevant en beschikbaar zijn bij deze groep rapportages over de maand april opgevraagd. TNO heeft in dit onderzoek niet geëxperimenteerd met middelen van leveranciers uit groep 2.

Alle partijen die op 16 april of later zijn gestart, dus de partijen in groep 3, vielen buiten scope en zijn niet actief betrokken in het onderzoek. Desondanks heeft TNO in overleg met de begeleidingscommissie een middelenleverancier in deze groep telefonisch gesproken, om waar mogelijk eerste indrukken en bevindingen op te halen. Bijlage D bevat een overzicht van de bij de pilots betrokken organisaties die TNO in de groepen 1, 2 en 3 heeft gesproken.

Dit onderzoek is grotendeels gebaseerd op informatie die is opgevraagd bij de bij de pilots aangesloten organisaties, bij de beheerder van het afsprakenstelsel, bij de beheerder van de technische IT-infrastructuur en bij de toezichthouder. Omdat de onderzoekers niet betrokken zijn geweest bij de opzet van de pilots, noch bij het evaluatieplan ervan, konden niet altijd alle benodigde inzichten worden verkregen

uit bijvoorbeeld de aangeleverde rapportages. Waar relevant is dat vermeld. Ook als informatie vertrouwelijk was, of om een andere reden niet ter beschikking kon worden gesteld, is dat aangegeven bij de beantwoording van de betreffende vraag.

TNO heeft voor deze studie geen toegang gehad tot de technische infrastructuur van de overheid of tot de technische infrastructuur van de betrokken middelen-leveranciers. Evenmin was er toegang tot ruwe logfiles uit de infrastructuur en tot de over het netwerk tussen de betrokken organisaties uitgewisselde technische berichten. Ook is in dit onderzoek geen software beschikbaar gesteld c.q. getest waaruit de eID-middelen en de server infrastructuur zijn opgebouwd. In het onderzoek is dan ook slechts beperkt ‘onder motorkap’ gekeken.

De onderzoekers hebben objectieve feiten en bevindingen verzameld en hebben daar geen waardeoordeel aan verbonden. De verantwoordelijkheid voor de uiteindelijke evaluatie van de pilots ligt bij de Commissie Kuipers en valt daarmee buiten scope van dit onderzoek.

1.4 Leeswijzer

De opbouw van dit rapport is als volgt:

- Hoofdstuk 2 beschrijft de opzet van het onderzoek, het gehanteerde analysekader en de gevolgde aanpak.
- Hoofdstuk 3 bevat een gedetailleerde beschrijving van de drie pilots die TNO heeft onderzocht. De lezer die bekend is met de pilots kan dit hoofdstuk eventueel overslaan.
- In hoofdstuk 4 zijn (per pilot) de onderzoeksvragen en de antwoorden opgenomen, inclusief onderbouwing en bronvermelding.
- De conclusies en aandachtspunten zijn opgenomen in hoofdstuk 5.

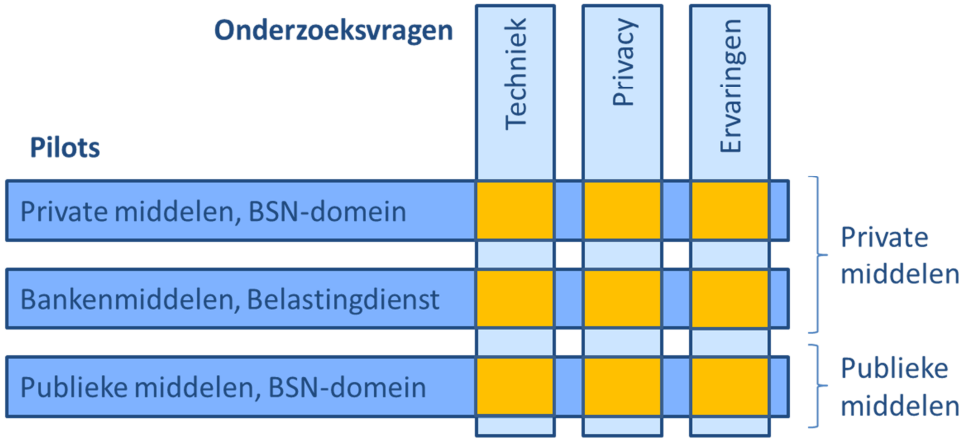
2 Analysekader en onderzoeksmethode

2.1 Opzet van het onderzoek

Het onderzoek van TNO richtte zich op drie pilots waarin private en publieke authenticatiemiddelen worden getest om in te loggen op verschillende online websites in het publieke domein. Alle drie de pilots werken op basis van een koppeling met het Burger Service Nummer (BSN) van eindgebruikers en vallen daarom in het gereguleerde domein.[6] In de pilot Idensys en de pilot Bankenmiddel wordt gebruik gemaakt van private inlogmiddelen en in de pilot Publiek Middel worden publieke inlogmiddelen gebruikt. Een publiek inlogmiddel is een inlogmiddel dat beschikbaar wordt gesteld door de overheid; een privaat inlogmiddel wordt beschikbaar gesteld door een (commerciële) private onderneming. De overheid schrijft het volgende over de drie pilots:

'*In het kader van de multimiddelenstrategie zijn er voor de pilots drie groepen van aanbieders van hoogwaardige authenticatiemiddelen, waarbij elke groep onder een eigen «merknaam» zichtbaar is voor de burger: via DigiD kan een pilotdeelnemer de (speciale) identiteitskaart of het (speciale) rijbewijs als een smartcard met een pincode gebruiken, onder de naam Idensys bieden private aanbieders diverse technologische oplossingen als authenticatiemiddel aan en onder de naam iDIN bieden banken het gebruik van de bestaande authenticatie-middelen voor internetbankieren aan.*' [6]

Figuur 1 schetst de opzet van het onderzoek. Horizontaal zijn de drie onderzochte pilots weergegeven en verticaal zijn de aan TNO gestelde onderzoeksvragen weergegeven, gegroepeerd naar de drie onderwerpen: techniek, privacy en ervaringen van betrokken partijen.



Figuur 1 Globale opzet van het onderzoek

De rijen: Het onderzoek richt zich op drie pilots. In twee daarvan wordt gebruik gemaakt van private middelen terwijl in de derde publieke middelen worden ingezet:

[6] Zie https://www.rijksoverheid.nl/onderwerpen/persoonsgegevens/vraag-en-antwoord/wat-is-het-burgerservicenummer-bsn

1. **Pilot met private middelen die toegang geven tot het BSN-domein**
   In deze pilot worden private authenticatiemiddelen in het BSN-domein getest. Met deze authenticatiemiddelen kunnen gebruikers inloggen bij verschillende dienstaanbieders, zoals bijvoorbeeld gemeenten of verzekeraars. Hiervoor wordt gebruik gemaakt van het BSNk. Voorbeelden van leveranciers van dergelijke middelen zijn Digidentity, KPN, Morpho en CreAim. Deze pilot wordt ook **'pilot Idensys'** genoemd.

2. **Pilot met bankenmiddelen die toegang geven tot de Belastingdienst**
   In deze pilot worden private authenticatiemiddelen van banken beproefd om in te loggen bij de Belastingdienst. Ook in deze pilot wordt daartoe gebruik gemaakt van het BSNk. Deze dienst van de banken, waarmee hun klanten zich bij andere organisaties online kunnen identificeren, heet iDIN[7]. Deze pilot wordt daarom ook **'pilot iDIN'** genoemd.

3. **Pilot met publieke middelen die toegang geven tot het BSN-domein**
   In deze pilot worden publieke authenticatiemiddelen in het BSN domein getest. Het betreft de volgende middelen: het eRijbewijs en de eNIK. Deze pilot richt zich in eerste instantie op de afname van overheidsdiensten op gemeentelijk niveau in Den Haag (eNIK), Eindhoven (eRijbewijs) en Groningen (eRijbewijs). Alle pilots in dit domein hebben 'DigiD onder de motorkap'. Deze pilot wordt daarom ook **'pilot Publiek Middel'** genoemd.

De kolommen: de in het onderzoek te beantwoorden onderzoeksvragen hebben betrekking op de techniek, de privacy en de ervaringen van gebruikers:

- **Techniek**
  In de offerte-aanvraag zijn onder het kopje 'Techniek' de vragen gegroepeerd die te maken hebben met onderwerpen als performance, beschikbaarheid en de technische werking van de pilot implementaties. Ook de werking van de technische keten (kaart, kaartlezer) valt onder het onderwerp 'Techniek'.

- **Privacy**
  Onder het kopje 'Privacy' zijn de onderzoeksvragen met betrekking tot privacy geclusterd. Een adequate bescherming van de privacy van burgers en consumenten is een belangrijke randvoorwaarde voor het Idensys-stelsel. Deze bescherming kan worden vormgegeven met behulp van technische en organisatorische maatregelen: technisch kunnen bijvoorbeeld processen dusdanig ingericht zijn dat privacy-inbreuken zoveel mogelijk worden voorkomen (bijvoorbeeld met behulp van encryptie), terwijl organisatorische maatregelen betrekking hebben op de rollen en bevoegdheden binnen een organisatie en de daarover vastgelegde afspraken. Het afsprakenstelsel van Idensys vormt dus een belangrijk kader, evenals de concrete implementatie van dat kader met betrekking tot ieder specifiek middel van de verschillende leveranciers. Een ander belangrijk onderdeel van privacybescherming betreft de heldere informatievoorziening richting burgers en consumenten.

- **Ervaringen**
  Dit cluster vragen heeft betrekking op de ervaringen van de middelenleveranciers, de dienstaanbieders en de gemeenten die deelnemen aan de pilots. Met

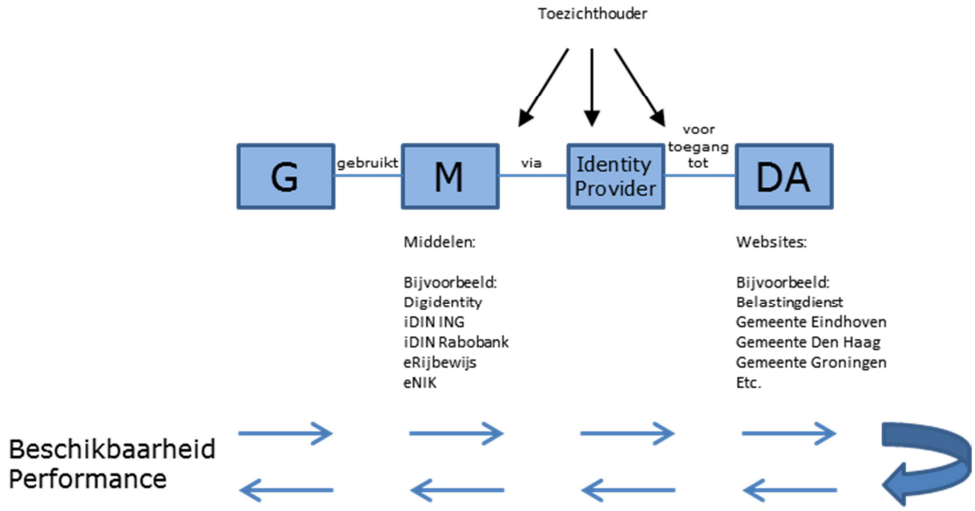
[7] Zie http://www.betaalvereniging.nl/giraal-en-online-betalen/idin/

'ervaringen' wordt in dit onderzoek gerefereerd aan de ervaringen van deze partijen ten aanzien van de (meer)waarde van de middelen in de eigen dienstverlening, de implementatie van de middelen, het gebruik ervan en de ondersteuning binnen de eigen organisatie en door andere organisaties, en tot slot ten aanzien van de transacties en communicatie tijdens de pilots.

2.2 Referentiemodel voor de pilots

De bij de pilots betrokken partijen en organisaties bekijken een pilot vaak vanuit hun eigen perspectief, vanuit de eigen plek in de authenticatie-dienstketen. De één zegt dan bijvoorbeeld: 'voor mij is de pilot het uitgifteproces aan de balie', terwijl de ander meent dat: 'de pilot draait voor mij om het koppelen van een BSN-nummer aan een gebruikersnaam'. Sommige onderzoeksvragen hebben echter betrekking op de gehele dienstketen: vanaf een eindgebruiker met een middel, via de tussenliggende infrastructuur van een vertrouwde derde partij, tot aan de online website van een dienstaanbieder.

Dergelijke vragen kunnen beter worden beantwoord als we een pilot beschouwen als een verzameling van identificatie- en authenticatie-dienstschakels, elk met hun eigen ervaringen, performance, beschikbaarheid enzovoort. Immers, een bepaald middel kan bijvoorbeeld heel vlot werken op website A maar heel langzaam op website B. Voor het beantwoorden van deze onderzoeksvragen heeft TNO in deze studie daarom het referentiemodel gebruikt dat is geschetst in Figuur 2.



Figuur 2 Het door TNO gehanteerde referentiemodel met enkele voorbeelden van partijen

In het referentiemodel gebruikt een gebruiker G een authenticatiemiddel M via een vertrouwde derde partij ('Identity Provider') op de website van een Dienstaanbieder DA. (Noot: de dienstaanbieder wordt in de standaarden ook wel 'Service Provider' genoemd.) Merk op dat de figuur een aantal voorbeelden van middelenleveranciers en dienstaanbieders bevat maar daarbij niet beoogt uitputtend of volledig te zijn.

2.3 Aanpak voor het beantwoorden van de onderzoeksvragen

2.3.1 Aanpak van het onderzoek

De onderzoekers hebben ernaar gestreefd de antwoorden op de onderzoeksvragen zoveel mogelijk onafhankelijk te laten zijn van het aantal eindgebruikers, het aantal

dienstaanbieders en het aantal authenticatiemiddelen. Zij hebben een methodiek gehanteerd die herhaaldelijk kan worden toegepast, bijvoorbeeld nadat een nieuwe organisatie met een nieuw middel is toegetreden of nadat een al toegetreden organisatie een verandering heeft doorgevoerd aan de werking van een bestaand middel. Alleen als de onderzoek- en meetmethodiek constant blijft kunnen immers verantwoorde meetresultaten voor een nulmeting en een latere effectmeting worden verkregen op basis van momentopnames door middel van steekproeven.

2.3.2 Onderzoeksvragen met betrekking tot techniek

Voor het onderzoeken van de **technische werking** van de verschillende pilot implementaties is onder andere gekeken naar hoe een middel moet worden aangevraagd (registratieproces), hoe het moet worden geïnstalleerd (installatieproces) en/of geactiveerd (activatieproces), en hoe het moet worden gebruikt (inlogproces) op de websites van de verschillende dienstaanbieders.

Voor het onderzoeken van de technische werking heeft TNO een aantal authenticatiemiddelen zelf uitgeprobeerd. Daarnaast is het onderzoek gebaseerd op rapportages uit technische systemen die door de betrokken organisaties in de hele keten zijn opgeleverd.

2.3.3 Onderzoeksvragen met betrekking tot privacy

In de bijlage bij de brief van Minister Plasterk aan de Tweede Kamer van 17 november 2015 is een overzicht gegeven van belangrijke criteria ten aanzien van **privacy** in Idensys en het bijbehorende stelsel [4]. Deze criteria dienden voor TNO als achtergrond bij het uitvoeren van het onderzoek naar de privacy-aspecten van de pilots. De genoemde criteria kwamen voort uit de PIA die eerder door Mazars is uitgevoerd. [7] Op basis van die PIA zijn al enkele maatregelen getroffen. In het privacy-onderzoek is dan ook gekeken of de getroffen maatregelen de geconstateerde tekortkomingen uit de PIA adequaat mitigeren. Op vergelijkbare wijze is gekeken naar de PIA activiteiten voor iDIN en de getroffen maatregelen.

Het onderzoek van het privacy-deel is gedaan aan de hand van deskresearch (opvragen en beoordelen van het privacy-beleid, in hoeverre er een PIA is uitgevoerd, faciliteren van recht op inzage van betrokkenen, en de invulling van informatieverplichtingen). Een deel van het onderzoek is gebaseerd op de beschikbaarheid van technische informatie, bijvoorbeeld voor het toetsen van eisen aan het gebruik van versleuteling. Tenslotte is aan de hand van interviews met de middelenleveranciers en de dienstenaanbieders nagegaan hoe privacy verder is geborgd binnen de stelsels, de pilots en de specifieke middelen die worden aangeboden en of de getroffen maatregelen van de geconstateerde tekortkomingen uit de PIA adequaat zijn gemitigeerd.

2.3.4 Onderzoeksvragen met betrekking tot de ervaringen van gebruikers

In het onderzoek wordt de ervaring van gebruikers (leveranciers, dienstaanbieders en gemeenten) op vier verschillende niveaus geadresseerd:

1. De waarde van inzet van middelen voor/binnen de eigen organisatie;
2. Het verloop van de pilot;
3. De integratie van middelen in het eigen proces (inclusief ondersteuning en communicatie);
4. Het proces gerelateerd aan derden (leveranciers en eindgebruikers).

De benodigde informatie is grotendeels verkregen uit meeloopdagen en interviews, waar nodig (en beschikbaar) ondersteund door deskresearch en loggegevens over dienstgebruik. Voor de interviews en meeloopdagen heeft TNO aan de hand van de gestelde onderzoeksvragen open/deels ongestructureerde interviewprotocollen opgesteld, voor een verdere verkenning en inventarisatie van de ervaringen van de stakeholders. TNO heeft de interviewprotocollen zo universeel mogelijk gehouden, zodat de resultaten achteraf goed met elkaar vergeleken konden worden.

2.4 Uitvoering van het onderzoek

De onderstaande tabel beschrijft de activiteiten die tijdens het onderzoek zijn uitgevoerd en wijze waarop informatie is verkregen.

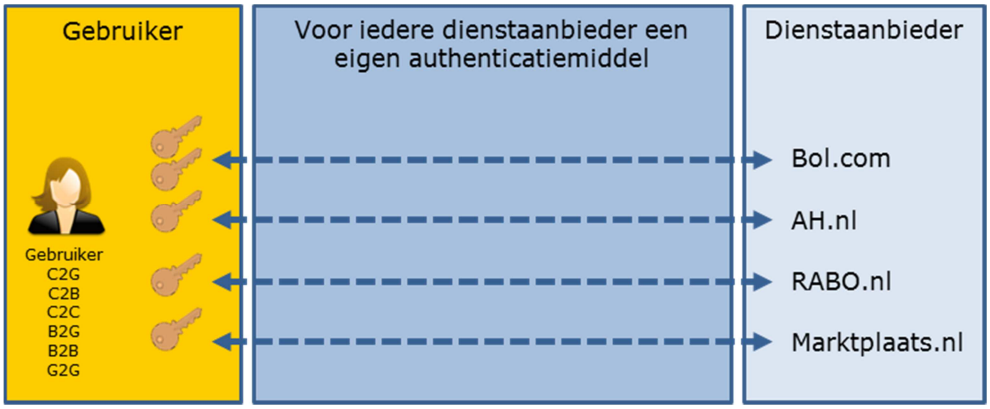
Activiteiten die tijdens het onderzoek zijn uitgevoerd

#	Activiteit	Omschrijving
1.	Interviews en meeloopdagen	Aan de hand van interviews en meeloopdagen bij de pilots betrokken organisaties is informatie verzameld over de beschikbare middelen, de gekozen gebruikersgroepen, de beschikbare websites en de ervaringen van deelnemende organisaties.
2.	Beschrijven van de pilots	De aldus verkregen informatie is verwerkt in de beschrijving van de drie pilots. Voor elke pilot is beschreven met welke authenticatiemiddelen de pilot werkt, hoe de leveringsketen in elkaar zit, hoe het registratieproces verloopt, hoe de middelen moeten worden geactiveerd en hoe de middelen kunnen worden gebruikt om in te loggen op een website van een dienstaanbieder (hoofdstuk 3).
3.	Experimenteren met middelen	Een aantal authenticatiemiddelen is uitgeprobeerd door de onderzoekers, om verdere details over de werking ervan te achterhalen. De resultaten zijn onderdeel gemaakt van de beschrijving van de pilots (hoofdstuk 3). Deze beschrijvingen zijn waar mogelijk gebruikt bij de beantwoording van een aantal onderzoeksvragen (hoofdstuk 4).
4.	Opvragen pilot rapportages	Op basis van de beschikbare pilot rapportages is een kwantitatieve data-analyse uitgevoerd ten aanzien van de middelen en diensten, om inzicht te krijgen in het daadwerkelijke gebruik en functioneren ervan tijdens de pilots (hoofdstuk 4).
5.	Beantwoording overgebleven onderzoeksvragen	De resultaten en inzichten van de bovenstaande vier activiteiten zijn gebruikt om de overgebleven onderzoeksvragen te beantwoorden. Voor die vragen waar nog extra gegevens (bijvoorbeeld meer details uit bepaalde technische systemen) nodig waren, zijn telefonisch of per e-mail extra details opgevraagd (hoofdstuk 4).
6.	Rapportage	Documenteren van de uitgevoerde activiteiten en de onderzoeksresultaten (dit rapport).

3 Beschrijving van de drie pilots

3.1 Wat is een authenticatiemiddel?

Om op een simpele manier uit te leggen wat centraal staat in de pilots, wordt verwezen naar Figuur 3. Aan de linkerkant staan eindgebruikers en aan de rechterkant staan websites van dienstaanbieders. Voordat een eindgebruiker op een website iets kan doen, moet deze eindgebruiker zichzelf meestal eerst identificeren. Identificatie van een gebruiker kan bijvoorbeeld aan de hand van een unieke gebruikersnaam. Tegelijkertijd met de gebruikersnaam moet vaak een wachtwoord worden opgegeven, waarna de combinatie van gebruikersnaam-wachtwoord naar de website wordt verstuurd. De website controleert of de identiteit van de eindgebruiker bekend is en of het opgegeven wachtwoord klopt met het geadministreerde wachtwoord. Dit proces van het controleren van een geclaimde identiteit wordt 'authenticatie' genoemd.[8]



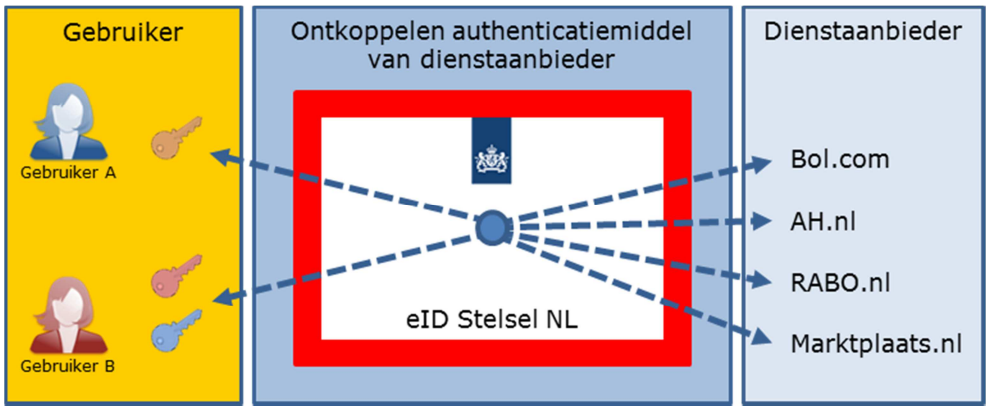
Figuur 3 Gebruiker met Middelen naar Dienstaanbieders (bron: [8])

In de fysieke wereld is een vaak gebruikt bewijsstuk van iemands identiteit het identiteitsbewijs, bijvoorbeeld een paspoort of identiteitskaart.[9] Bij een identiteitscontrole wordt gekeken naar (a) de echtheid van het bewijsstuk (aan de hand van bepaalde kenmerken) en naar (b) een vergelijking van de foto op het bewijsstuk met het gezicht van een persoon. Wanneer beide controles naar tevredenheid zijn uitgevoerd, is de identiteit van een persoon vastgesteld.

In de digitale wereld van het internet werkt dit niet, onder andere vanwege het niet fysiek kunnen 'zien' van een persoon. Daarom moet online iets anders worden gebruikt: een 'elektronische identiteit' (eID). Meestal hanteert een website online een eigen unieke identifier voor een gebruiker, bijvoorbeeld een Burger Service Nummer (BSN) bij de overheid, of een klantnummer bij een bank of verzekeraar. Vaak zijn de al eerder genoemde gebruikersnaam en wachtwoord attributen die bij een dergelijke unieke identifier worden opgeslagen. Een gebruikersnaam is een voorbeeld van een identificatiemiddel en een wachtwoord is het bijbehoren authenticatiemiddel. Een eindgebruiker (burger of consument) kan zichzelf er online mee identificeren en authentiseren bij een website.

[8] Zie https://nl.wikipedia.org/wiki/Authenticatie
[9] Zie https://www.rijksoverheid.nl/onderwerpen/paspoort-en-identiteitskaart

Een paspoort kan bij vele organisaties gebruikt worden om de houder van het paspoort te identificeren/authentiseren. Met andere woorden: een gebruiker kan met één middel terecht op meerdere plekken. Om deze eigenschap te benaderen in de digitale wereld, is een middel nodig dat herkend en erkend wordt door meerdere websites in plaats van een situatie dat elke website een eigen middel uitdeelt. Een voorbeeld van een dergelijk online identificatie/authenticatiemiddel is DigiD.[10] Bij DigiD is het middel ontkoppeld van een dienstaanbieder, en de bij DigiD aangesloten websites vertrouwen op een derde partij, namelijk de beheerder van DigiD, om de authenticatie van de gebruiker voor hen uit te voeren. Figuur 4 illustreert dit principe.



Figuur 4 Gebruiker met één middel naar verschillende dienstaanbieders (bron: [8])

Zoals hiervoor beschreven deelt een dienstaanbieder voor de bij DigiD aangesloten websites niet zelf een gebruikersnaam/wachtwoord uit, maar vertrouwt hij voor de registratie, uitgifte en het gebruik van het middel op een vertrouwde derde partij. Dit is een model waarbij een ‘Service Provider’ (website) vertrouwt op het registratie- en authenticatieproces van een ‘Identity Provider’ (DigiD) voor een gebruiker. In een dergelijk model spreekt men van een ‘federated identity’.[11]

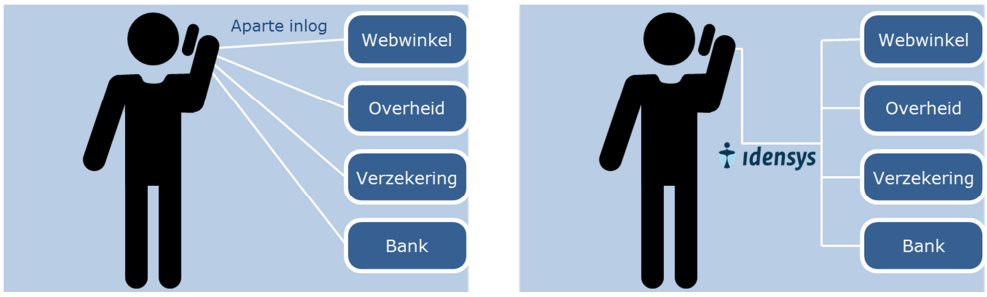
3.2 Wat is Idensys?

Idensys is een voorbeeld van een federated identity systeem (en datzelfde geldt ook voor bijvoorbeeld iDIN en DigiD). Idensys is een standaard in de vorm van een afsprakenstelsel waar verschillende organisaties, zoals aanbieders van authenticatiemiddelen, zich bij kunnen aansluiten. Figuur 5 bevat een illustratie. Een organisatie die wil toetreden tot Idensys moet voldoen aan bepaalde normen en eisen. Een eenmaal toegetreden partij die voldoet aan die normen en eisen, krijgt bepaalde rechten en plichten. Zo mag hij bijvoorbeeld het Idensys logo gebruiken. Binnen Idensys zijn verschillende rollen gedefinieerd, zoals die van middelenleverancier, authenticatiedienst en makelaar.

Bij Idensys kunnen middelenleveranciers toetreden met inlogmiddelen met verschillende zekerheidsniveaus (of ook wel betrouwbaarheidsniveaus genoemd). Hoe meer zekerheid een dienstaanbieder nodig heeft over wie de gebruiker is, hoe hoger het betrouwbaarheidsniveau van het inlogmiddel moet zijn dat hij gebruikt om

[10] Zie https://nl.wikipedia.org/wiki/DigiD
[11] Zie https://en.wikipedia.org/wiki/Federated_identity

in te kunnen loggen bij een bepaalde dienstaanbieder voor het uitvoeren van transacties bij die dienstaanbieder[12].



Figuur 5 Illustratie van Idensys: één inlogmiddel (Bron: RTL-Z)

Middelen die onder Idensys vallen, kunnen door verschillende middelenleveranciers worden aangeboden. De lijst van erkende leveranciers van Idensys bestaat ten tijde van dit onderzoek uit Digidentity, CreAim en KPN. Daarnaast bevindt Morpho zich in het toetredingsproces. Binnen het stelsel zijn middelen op verschillende niveaus beschikbaar, en de dienstverlener geeft aan met welk niveau de eindgebruiker moet inloggen. De eindgebruiker bepaalt op welk niveau en van welke leverancier hij/zij een middel wil gaan gebruiken, zolang hij met dit middel maar aan het betrouwbaarheidsniveau voldoet wat voor de afname van een dienst vereist is.

Een private middelenleverancier die is toegetreden tot het Idensys stelsel gebruikt een private identifier voor administratie van een eindgebruiker, bijvoorbeeld een unieke gebruikersnaam of een uniek klantnummer (hieronder pseudo-ID genoemd). Deze private identifier uit het private domein moet gebruikt, dat wil zeggen herkend en erkend, kunnen worden in het publieke domein. De koppeling tussen twee identiteiten uit twee verschillende domeinen wordt geïmplementeerd door het BSN koppelregister ('BSNk').

'*Nadat een burger met een privaat authenticatiemiddel heeft ingelogd bij een organisatie in het publieke domein, legt het Koppelregister een koppeling tussen het pseudo-ID van de gebruiker, waarmee de gebruiker is geregistreerd bij de private authenticatiedienst, en het eerder - eenmalig - door de authenticatiedienst aan het Koppelregister aangeleverde BSN van de gebruiker.*' [9]

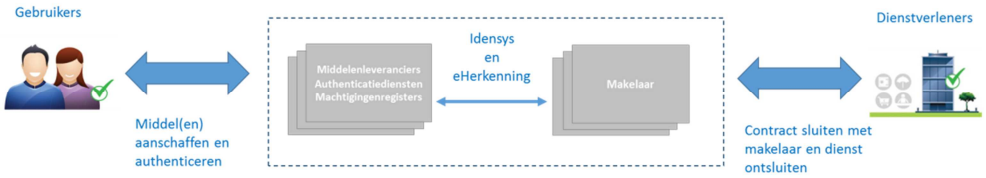
3.3 Pilot omschrijving Idensys

3.3.1 Pilot- en ketenpartners

De pilot/keten binnen de Idensys pilot is volop in beweging met nieuwe partijen die toetreden en nieuwe dienstaanbieders die burgers middels de middelen toegang geven tot hun websites. Zie Figuur 6 en Figuur 7 voor een overzicht van de structuur en werking van Idensys en de samenhang tussen de verschillende rollen.

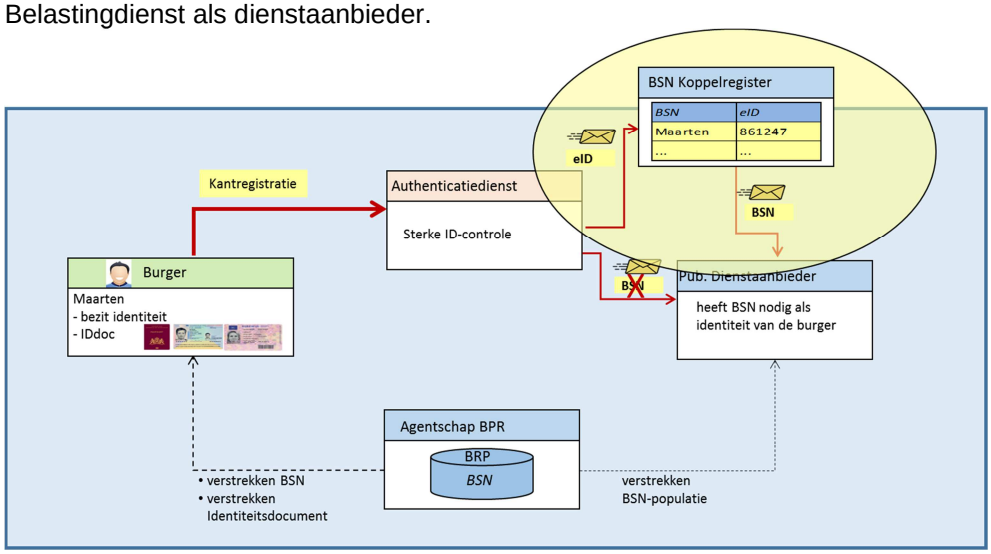
Op het moment van schrijven zijn de erkende leveranciers van Idensys-inlogmiddelen CreAim, Digidentity en KPN. CreAim, Digidentity en KPN zijn tevens authenticatiedienst en herkenningsmakelaar. Morpho treedt toe als zowel middelenuitgever als authenticatiedienst.

[12] Zie https://www.idensys.nl/inloggen-met-idensys/inlogmiddel-aanvragen/



Figuur 6 Rollen in het stelsel gedurende de pilots (Bron: Idensys)

Vanaf januari 2016 testen verschillende organisaties of Idensys goed werkt. Een compleet en actueel overzicht van deze dienstaanbieders kan worden gevonden op het internet.[13] Binnen de scope van dit onderzoek is alleen gekeken naar de Belastingdienst als dienstaanbieder.



Figuur 7 Inzet private authenticatiedienst in het BSN-domein (Bron: Idensys)

3.3.2 *Deelnemende partijen Idensys*

Voor een actueel overzicht van deelnemende partijen in Idensys verwijzen we naar de website van Idensys.[14]

3.3.3 *Pilot deelnemerswerving Idensys*

De Belastingdienst heeft de pilot opgedeeld in twee delen: een ‘friends and family’ fase (voorafgaand aan de pilot) en de publieksfase van de pilot. Omvang van de pilot in deze fase was maximaal drieduizend deelnemers. De Belastingdienst heeft voor deze fase zelf drieduizend middelen gekocht bij drie verschillende middelenleveranciers (duizend per leverancier) [10].

3.3.4 *Registratie en in gebruik name Idensys middelen*

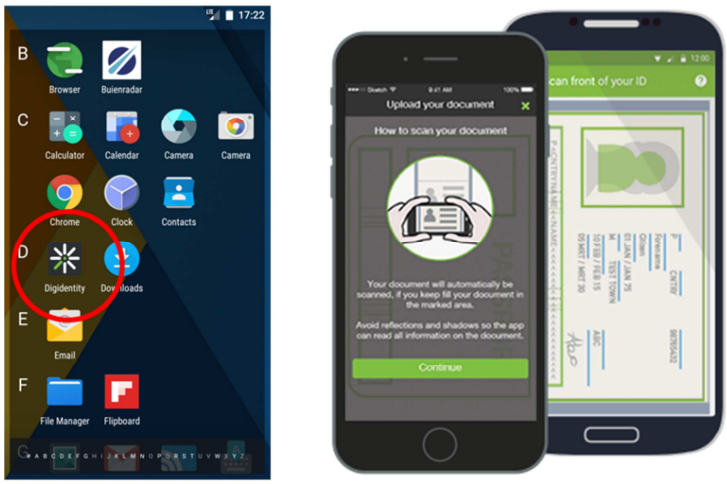
3.3.4.1 *Registratie Digidentity*

Het registratieproces voor het aanmelden van een nieuwe Digidentity gebruiker start met het registreren van een account op de website met een gebruikersnaam, wachtwoord en e-mailadres (zie Figuur 8).

[13] Zie: https://www.idensys.nl/inloggen-met-idensys/over-de-testen/
[14] Zie: https://www.idensys.nl/

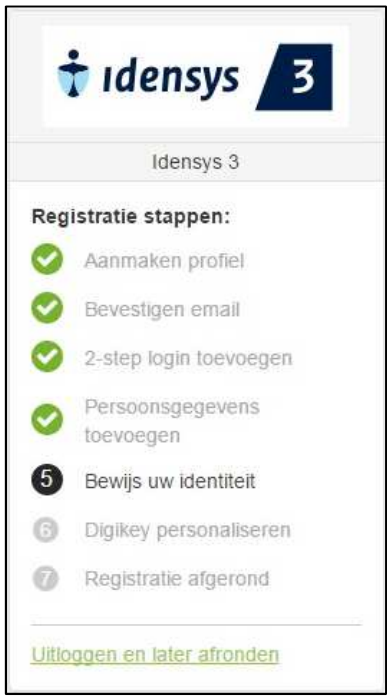
Figuur 8 Digidentity website start registratieproces

Naast de website is Digidentity voor de eindgebruiker vooral zichtbaar als een app op bijvoorbeeld een smartphone (zie Figuur 9). Het registratieproces is onder andere gebaseerd op het maken van een foto van de voor- en achterkant van een Wettelijk Identificatie Document (WID) zoals bijvoorbeeld een rijbewijs. Ook moeten twee selfies worden gemaakt van het gezicht van de houder van het rijbewijs naar aanleiding van een random opdracht van de app, bijvoorbeeld ‘knipoog-met-links’ en ‘glimlachen’.



Figuur 9 Digidentity app

Daarna worden de foto’s vanuit de app via een beveiligde verbinding naar Digidentity verstuurd waarna een persoon bij Digidentity de verificatie uitvoert. Digidentity laat de controle op echtheid van het WID uitvoeren door een externe daarin gespecialiseerde organisatie. De controle van de twee selfies met de foto op het WID wordt door een hiervoor opgeleide Digidentity medewerker zelf uitgevoerd (bron: interview Digidentity). Het hele Digidentity registratieproces bestaat uit zeven stappen en biedt uiteindelijk een betrouwbaarheid conform het Idensys Afsprakenstelsel op niveau 3 (zie Figuur 10).



Figuur 10 Digidentity registratieproces

3.3.4.2 Inloggen met Digidentity

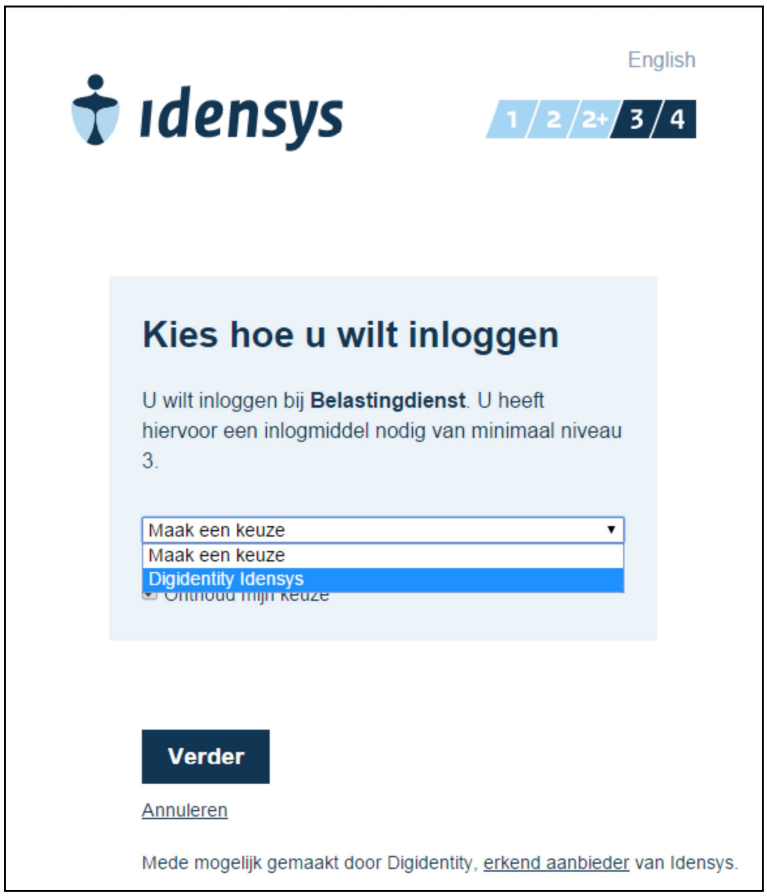
Gebruikers kunnen met Digidentity inloggen op bijvoorbeeld Mijn Belastingdienst om online hun belastingaangifte te doen. Het inlogproces op de website van de Belastingdienst ziet er als volgt uit: zie Figuur 11 tot en met Figuur 20.

Figuur 11 Digidentity Inlogproces Belastingdienst stap 1

Figuur 12 Digidentity Inlogproces Belastingdienst stap 2

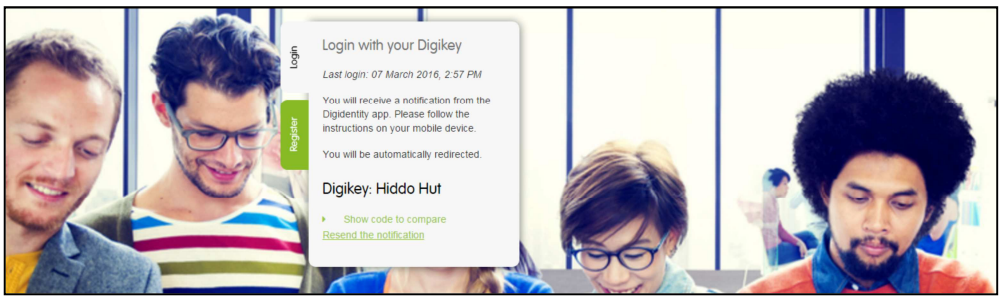
Figuur 13 Digidentity Inlogproces Belastingdienst stap 3

Figuur 14 Digidentity Inlogproces Belastingdienst stap 4

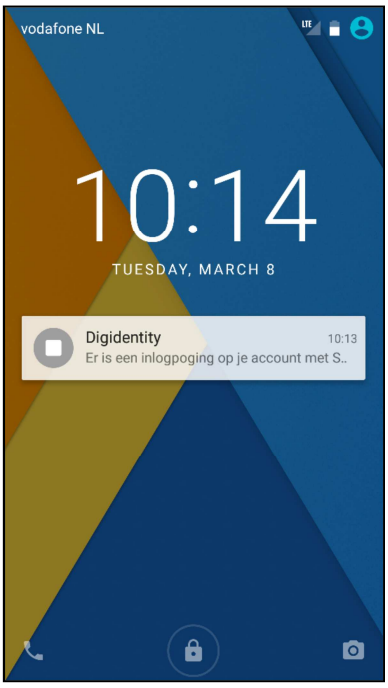


Figuur 15 Digidentity Inlogproces Belastingdienst stap 5

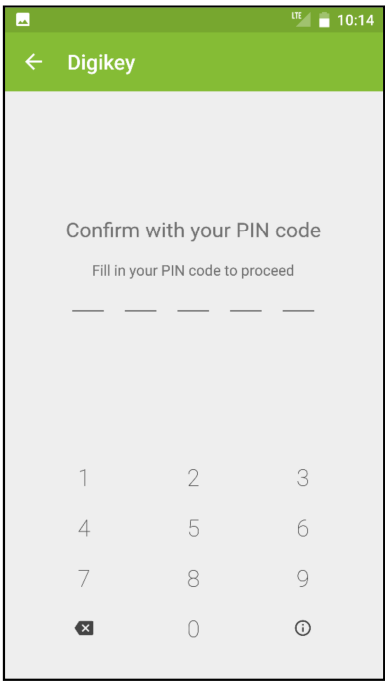
Figuur 16 Digidentity Inlogproces Belastingdienst stap 6



Figuur 17 Digidentity Inlogproces Belastingdienst stap 7



Figuur 18 Digidentity Inlogproces Belastingdienst stap 8



Figuur 19 Digidentity Inlogproces Belastingdienst stap 9

Figuur 20 Digidentity Inlogproces Belastingdienst stap 10

Merk op dat bovenstaande screenshots uit het inlogproces gemaakt zijn om het complete inlogproces inzichtelijk te maken bij een website, dus vanaf de homepage van de Belastingdienst[15]. Strikt genomen start het echte inloggen bij stap 5 wanneer de eindgebruiker zijn Idensys middel (Digidentity) selecteert en op de 'Verder' knop klikt.

3.4 Pilot omschrijving iDIN

3.4.1 Pilot- en ketenpartners en processen

iDIN is gericht op het breder inzetten van bestaande authenticatiemethodes en is een dienst van banken, waarmee hun klanten zich bij andere organisaties online kunnen identificeren. Mede hiervoor wordt een beperkt aantal persoonsgegevens verstrekt aan deze organisaties. Klanten die daarvoor kiezen, kunnen zich bekendmaken met behulp van de inlogmiddelen van hun eigen bank, bijvoorbeeld bij verzekeringsmaatschappijen, overheidsinstanties of in webwinkels. Binnen het iDIN-framework worden organisaties bij wie de klanten zich online met iDIN kunnen identificeren aangeduid als 'Acceptanten'. De bank van de klant wordt de 'Issuer' genoemd en de bank van de acceptant is de 'Acquirer'.

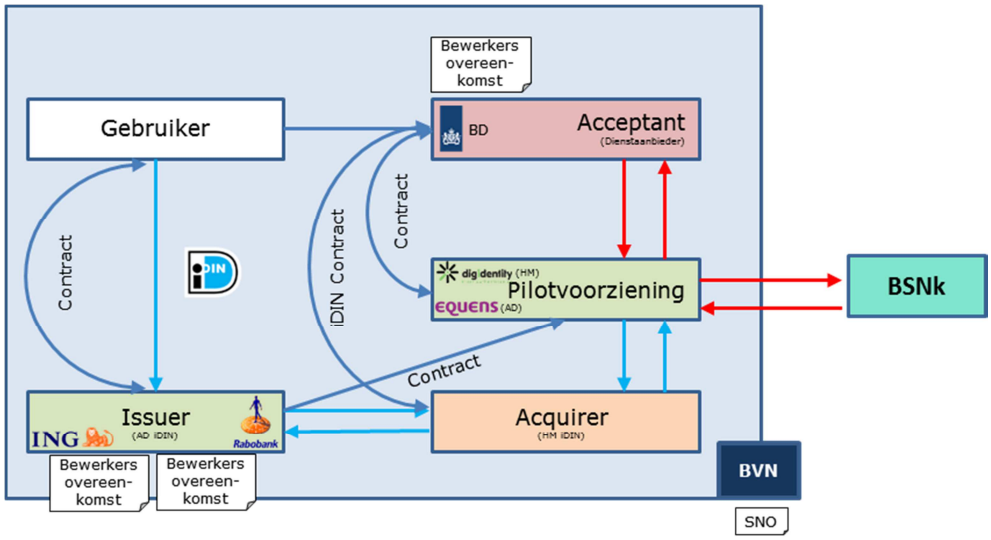
Zie Figuur 21 voor een illustratie van de werking van iDIN. Deze laat zich het best vergelijken met iDEAL: de klant selecteert zijn bank op de website van de Acceptant. De Acceptant heeft een iDIN-overeenkomst met een aanbieder van het product, de Acquirer. De Acquirers en de Issuers (consumentbanken) hebben een stelsel afgesproken waarbinnen iDIN operationeel, functioneel en juridisch geborgd is, waardoor het in de markt aangeboden kan worden. [11]

Figuur 20 geeft slechts één rol weer voor de pilotvoorziening, maar in werkelijkheid zijn er twee:

a. Pilotvoorziening 'Issuing' voor het initiëren van de associatie bij BSNk van BIN (pseudo-ID) en BSN;
b. Pilotvoorziening Acceptant voor opvragen BSN bij BSNk. De banken is toegestaan het BSN te leveren aan het BSNk. Het is de banken niet toegestaan het BSN te leveren aan acceptanten. Acceptanten kunnen daarom zelf een koppeling met BSNk realiseren voor het opvragen van het bij het pseudo-ID behorende BSN, danwel hiervoor een technische onderaannemer

[15] Zie http://www.belastingdienst.nl/wps/wcm/connect/nl/home/home

inhuren. Deze onderaannemer moet zich dan wel bij Logius kwalificeren om aan te mogen sluiten. Hiervoor heeft Logius aansluitvoorwaarden vastgesteld.



Figuur 21 De werking van iDIN binnen de keten (bron: [12])

Tijdens de pilot wordt de gebruikersondersteuning via de reguliere beheerprocessen uitgevoerd. Klantsignalen kunnen binnenkomen bij de dienstverleningskanalen van de Belastingdienst en van de banken. Alle meldingen worden op een centraal punt geregistreerd, waarna diagnose plaatsvindt. Afhankelijk van deze diagnose (functioneel, applicatief, netwerk, extern of communicatief) wordt het issue voor verdere afhandeling binnen de Belastingdienst uitgezet of wordt de melding doorgezet naar de herkenningsmakelaar. Er wordt een (virtuele) control room ingericht voor besluitvorming bij incidenten met een hoge prioriteit. Voor de BelastingTelefoon, webcare en op de website wordt een Q&A beschikbaar gesteld om klantvragen te beantwoorden. Deze wordt middels een leercirkel met de banken bijgesteld indien wenselijk. Er wordt vanuit gegaan dat klanten of hun bank of de Belastingdienst bellen met vragen. [13] Ook banken registeren binnengekomen vragen en communiceren dit waar nodig met andere partners binnen de pilot.

3.4.2 *Deelnemende partijen iDIN*

Op het moment van schrijven van dit rapport zijn er vijf banken bij de iDIN pilot aangesloten: ABN AMRO, ING, Rabobank, SNS, ASN Bank, RegioBank en Triodos Bank. [13] De deelnemerswerving verloopt via acceptant, in dit geval de Belastingdienst.

3.4.3 *Pilot deelnemerswerving iDIN*

Communicatie met de doelgroep tijdens de pilot verloopt via de website van de Belastingdienst. Iedereen die een iDIN middel heeft geregistreerd voor het BSN domein, kan in deze fase inloggen op mijnbelastingdienst.nl en zijn of haar aangifte doen. De Belastingdienst heeft hiervoor een applicatie laten maken waarmee klanten van de deelnemende banken hun iDIN middel kunnen registreren voor het BSN-domein. Op deze wijze wordt expliciet toestemming gegeven door de klant en wordt bovendien geborgd dat slechts eenmaal een uitgebreide dataset wordt uitgewisseld ten behoeve van de registratie. Voor het gebruik van iDIN voor het

afnemen van diensten wordt slechts pseudo ID van de banken gebruikt uitgewisseld. [13]

3.4.4 Ingebruikname iDIN door de gebruiker

3.4.4.1 Activatie iDIN ING

Het activeringsproces van ING voor het aanmelden van een nieuwe iDIN gebruiker kan worden gestart op de website van de Belastingdienst (zie Figuur 22 tot en met Figuur 25). Noot: de betrokken onderzoeker heeft al eerder bij ING een face-to-face identificatie doorlopen.

Figuur 22 iDIN ING Activatieproces stap 1

Figuur 23 iDIN ING Activatieproces stap 2

Figuur 24 iDIN ING Activatieproces stap 3

Figuur 25 iDIN ING Activatieproces stap 4

Het versturen van de gegevens aan de Belastingdienst in de laatste stap 4 van het activeringsproces voor iDIN ING moet worden bevestigd met een ING ‘Transactie Autorisatie Nummer’ (TAN-code), dat wordt verstuurd via SMS.

Omdat bij iDIN ING gebruik wordt gemaakt van bestaande middelen voor internetbankieren, namelijk gebruikersnaam en wachtwoord met bijbehorende TAN-codes, hebben de onderzoekers geen apart middel ontvangen.

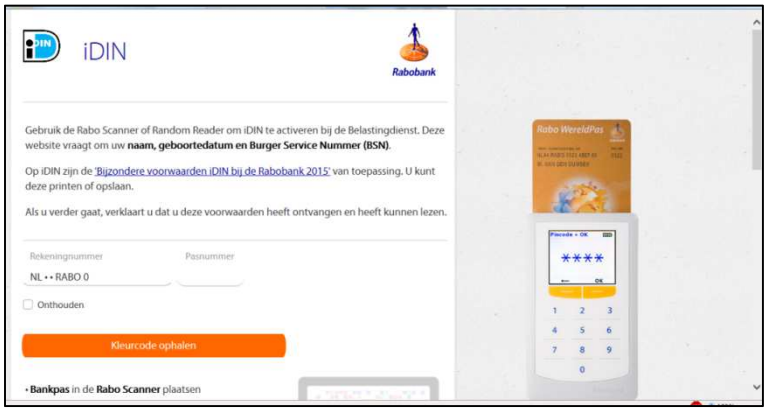
3.4.4.2 *Activatie iDIN Rabobank*

Bij de Rabobank verloopt het registratieproces voor iDIN op vergelijkbare wijze. Ook hier wordt begonnen op de site van de Belastingdienst, waar gekozen wordt

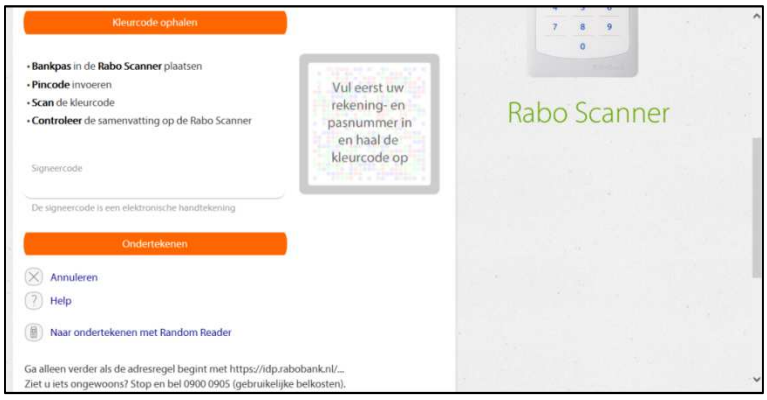
voor ‘inloggen met een ander middel’. Vervolgens kan iDIN geselecteerd worden en daarna, in het uitklapmenu: Rabobank.

Figuur 26 iDIN Rabobank Activatieproces stap 1

Daarna wordt de gebruiker doorgeleid naar de reguliere iDEAL-omgeving van de Rabobank.



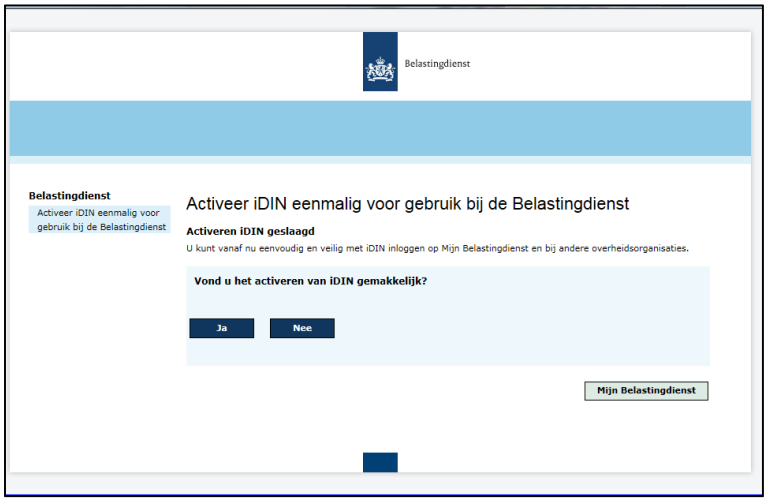
Figuur 27 iDIN Rabobank Activatieproces stap 2



Figuur 28 iDIN Rabobank Activatieproces stap 3

Na het inloggen bij de bank wordt aangegeven met welke gegevens iDIN bij de Belastingdienst geactiveerd kan worden. Indien akkoord verstuurt de Rabobank deze gegevens dus aan de Belastingdienst.

Na het akkoord wordt iDIN geactiveerd en wordt de gebruiker teruggeleid naar de site van de Belastingdienst.



Figuur 29 iDIN Rabobank Activatieproces stap 4

3.4.4.3 *Inloggen iDIN ING*

Gebruikers kunnen met iDIN inloggen op Mijn Belastingdienst, bijvoorbeeld om online hun belastingaangifte te doen. Het inlogproces van ING op de website van de Belastingdienst ziet er als volgt uit.

Figuur 30 iDIN ING Inlogproces Belastingdienst stap 1

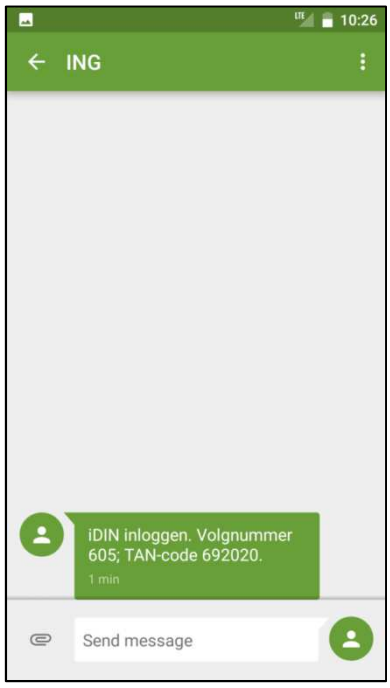
Figuur 31 iDIN ING Inlogproces Belastingdienst stap 2

Figuur 32 iDIN ING Inlogproces Belastingdienst stap 3

Figuur 33 iDIN ING Inlogproces Belastingdienst stap 4

Figuur 34 iDIN ING Inlogproces Belastingdienst stap 5

Figuur 35 iDIN ING Inlogproces Belastingdienst stap 6



Figuur 36 iDIN ING Inlogproces Belastingdienst stap 7

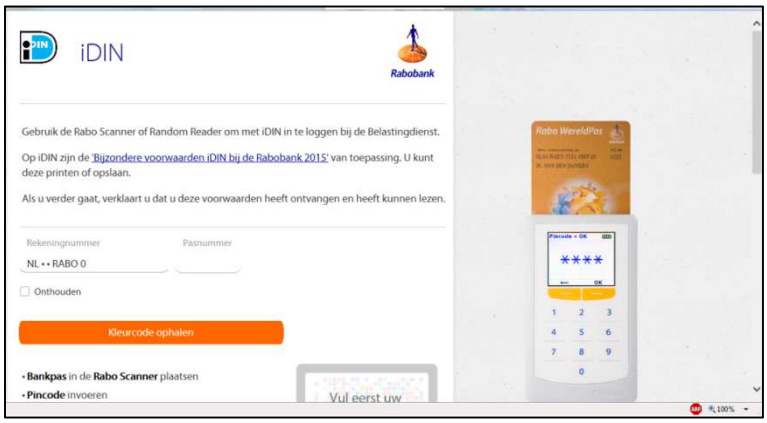
Figuur 37 iDIN ING Inlogproces Belastingdienst stap 8

Merk op dat bovenstaande screenshots uit het inlogproces gemaakt zijn om het complete inlogproces inzichtelijk te maken, dus vanaf de homepage van de Belastingdienst.[16] Strikt genomen start het echte inloggen bij stap 5 wanneer de eindgebruiker zijn bank selecteert en op de ‘Ga verder’ knop klikt.

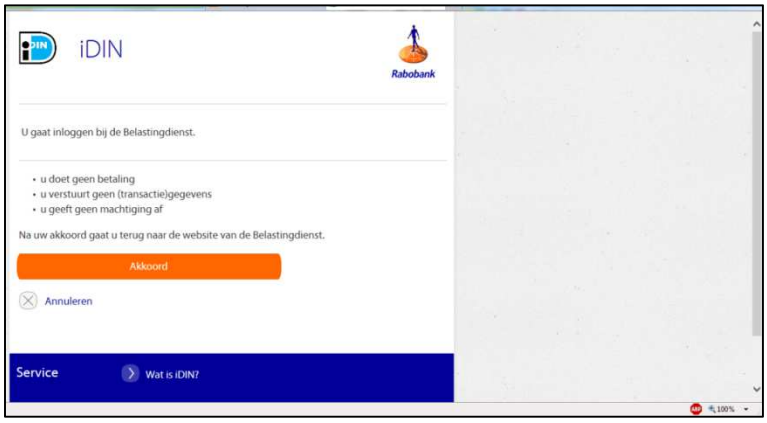
3.4.4.4 Inloggen iDIN Rabobank

Nadat het iDIN middel is geactiveerd kan het gebruikt worden om in te loggen bij de Belastingdienst. Daarbij wordt duidelijk aangegeven dat het om inloggen met iDIN gaat en niet om een reguliere banktransactie. Tevens wordt aangegeven dat er geen betaling plaatsvindt en dat er geen gegevens worden verstuurd. Dat mag alleen na expliciete toestemming van de gebruiker. Onderstaande screenshots tonen de processtappen.

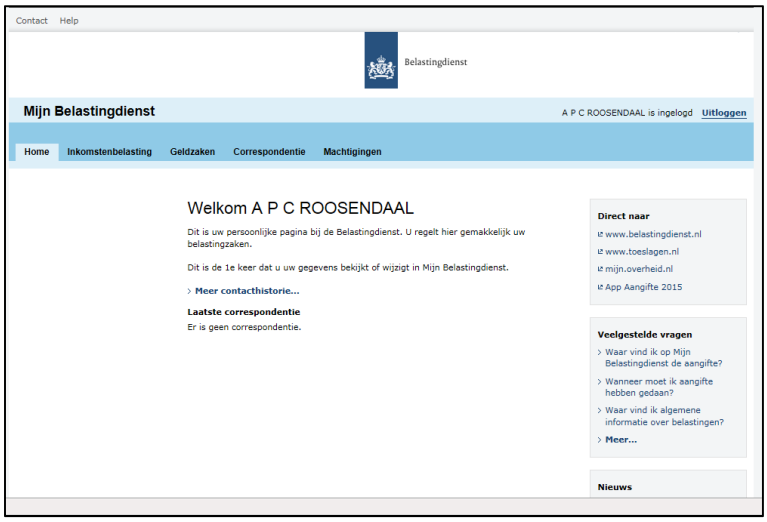
[16] Zie http://www.belastingdienst.nl/wps/wcm/connect/nl/home/home



Figuur 38 iDIN Rabobank Inlogproces Belastingdienst stap 1



Figuur 39 iDIN Rabobank Inlogproces Belastingdienst stap 2



Figuur 40 iDIN Rabobank Inlogproces Belastingdienst stap 3

3.5 Pilot omschrijving Publiek Middel

3.5.1 Pilot- en ketenpartners en processen

De aan de pilot Publiek Middel deelnemende partijen zijn: Logius, RvIG, RDW, ICTU, Morpho, Gemalto, Digidentity, de leverancier van Logius, en de gemeenten Eindhoven, Den Haag en Groningen.

De gemeenten Eindhoven en Groningen, die met het eRijbewijs aan de pilot deelnemen, leveren de databestanden met namen, voorletters, geboortedata, BSNs, rijbewijsnummers en mailadressen (en mogelijk telefoonnummers) van pilotdeelnemers aan bij het RDW voor het drukken van de eRijbewijs specimen. Deze databestanden worden middels een beveiligd bestand via mail verzonden door de gemeenten en het RDW controleert per pilot of de gegevens van de deelnemers kloppen. Voor de gemeente Den Haag, die aan de pilot deelneemt met het eNIK, geldt het reguliere NIK aanvraagproces. De uitgegeven kaarten worden geregistreerd en iedere dag wordt een hiervan update gestuurd aan Morpho, dat de kaarten vervolgens laat activeren bij Logius.

In de pilot Publiek Middel leveren Morpho en Gemalto de software/algoritmen en chips voor respectievelijk de eNIK en het eRijbewijs. Het RDW drukt vervolgens de eRijbewijzen met de Gemalto chips en software. Morpho levert de eNIKs direct aan de gemeente Den Haag in opdracht van RvIG. Levering vindt plaats volgens het gebruikelijke proces voor de uitgifte van identiteitskaarten en paspoorten. Het RDW verspreidt het middel (eRijbewijs) aan de gemeenten Eindhoven en Groningen. Zowel RDW als Morpho doet dit door middel van een fysieke overdracht aan de gemeenten.

Logius ontvangt een lijst van te activeren kaarten (de zogenaamde ‘white list’) van het RDW en Morpho. Het RDW heeft deze lijst ontvangen van de gemeenten Eindhoven en Groningen (iedere dag na het uitreiken van nieuwe eRijbewijzen), Morpho van de gemeente Den Haag (iedere dag na het uitreiken van nieuwe eNIKs). Logius verzorgt de BSN-koppeling tussen het publieke middel en de DigiD toegang op websites van dienstaanbieders.

Het RDW en Morpho communiceren eveneens met Logius welke kaarten geblokkeerd moeten worden (c.q. op de zogenaamde ‘blacklist’ geplaatst moeten worden) na verlies van de kaarten. Het eRijbewijs betreft een specimen rijbewijs, geen wettelijk document. Mocht een deelnemer de kaart kwijt raken dan wordt er geen nieuwe uitgereikt, maar het betreffende eRijbewijs wordt wel geblokkeerd (op de blacklist gezet). De eNIK is wel een wettelijk document; bij verlies wordt er een nieuwe NIK uitgereikt (geen vervangende eNIK) en wordt de desbetreffende eNIK op de blacklist geplaatst. Als een eRijbewijs of eNIK op de blacklist is geplaatst bij Logius kan de kaart niet langer gebruikt worden voor toegang tot DigiD dienstaanbieders. Per 15 mei 2016, de einddatum van de pilot, zullen alle eRijbewijzen ‘gedeactiveerd’ worden. Eind juni 2016, zullen alle eNIKs geblokkeerd worden.

Na blokkering worden de eRijbewijzen en de eNIKs door de pilotdeelnemers aan de gemeenten teruggegeven, in ruil waarvoor men als pilotdeelnemer bij een eRijbewijs een cadeaubon van vijftig euro ontvangt, mits men aan de pilot voorwaarden heeft voldaan. Op grond van de logdata kan op dit moment echter niet gecontroleerd worden of een deelnemer daadwerkelijk voldoet aan bijvoorbeeld het minimaal aantal keren inloggen bij dienstaanbieders.[17] Bij inlevering van een eNIK ontvangt men een nieuwe NIK, en terugbetaling van de kosten/betaling die men in eerste instantie voor de eNIK heeft gedaan.

[17] Logdata rapportages ICTU/Logius en RDW

Binnen de pilot Publiek Middel is een escalatieprocedure beschreven, aan de hand waarvan incidenten en calamiteiten opgepakt worden. [14] Ook staat in deze procedure beschreven hoe vragen van burgers/gebruikers en personeel afgehandeld moeten worden. Deelnemers konden met hun vragen terecht bij (eerste lijn):

- De Webhelp DigiD (of het bijbehorende telefoonnummer);
- In Groningen telefonisch bij het Klant Contact Centrum (KCC) of middels een voor de pilot ingericht mail adres;
- In Eindhoven bij een daarvoor ingericht mailadres;
- In Den Haag bij een daarvoor ingericht mailadres en telefoonnummer.

Technische vragen worden direct doorgezet naar het servicecenter van Logius. Logius verwijst eventueel door naar ICTU, Morpho, RDW, etc. mochten zaken bij Logius niet opgelost worden of tot hun verantwoordelijkheden of beheer in de pilot behoren (tweede lijn). Gemeenten konden met algemene of technische vragen direct terecht bij de andere partners (middelenleveranciers, de beheerorganisatie en ICTU).

3.5.2 Deelnemende partijen pilots Publieke Middelen

Aan de pilot Publiek Middel zouden in eerste instantie vijf gemeenten deelnemen met twee verschillende kaarten (eRijbewijs en eNIK). Uiteindelijk hebben de gemeenten Eindhoven en Groningen deelgenomen aan de pilot met het eRijbewijs, en de gemeente Den Haag met het eNIK. De onderstaande tabel geeft een overzicht van de startdata van de pilots voor verschillende gemeenten, gerekend vanaf het moment van uitgifte van het eRijbewijs en de eNIK. De werving van pilot deelnemers is al eerder gestart. De doorlooptijd van de werving van deelnemers verschilt per pilot. De pilot met de eNIK in Den Haag en met het eRijbewijs in Groningen eindigden eveneens op 15 mei, echter de uiterste inleverdatum is hierbij op eind juni 2016 gesteld.

Overzicht start- en einddata pilots in verschillende gemeenten

Publiek middel leverancier	**Middel**	**Startdatum**	**Einddatum**
Eindhoven	eRijbewijs	15 februari 2016 (start uitreiken)	15 mei 2016
Groningen	eRijbewijs	11 april 2016 (start uitreiken)	Eind juni 2016
Den Haag	eNIK	29 februari 2016 (start uitreiken)	Eind juni 2016

3.5.3 Pilot deelnemerswerving

De pilot Publiek Middel omvat het aanvraag- en het uitgifteproces van het eRijbewijs in de gemeenten Eindhoven en Groningen resp. het eNIK in de gemeente Den Haag. Het streven was om in totaal 1500 deelnemers te realiseren voor de pilot Publiek Middel. [15]

Zowel voor het eRijbewijs als voor de eNIK zijn specifieke doelgroepen benaderd en uitgenodigd om mee te doen aan de pilot.

In Eindhoven (eRijbewijs) zijn de volgende doelgroepen benaderd:

- Berichtenbox gebruikers;

- Collega's;
- Digipanel;
- Stembureauleden.

In Groningen (eRijbewijs) zijn de volgende doelgroepen benaderd:
- Stembureauleden;
- Afd. Burgerzaken;
- Onderzoek en Statistiek;
- KCC;
- Gemeenteambtenaren van Ten Boer;
- Tot slot kregen alle ambtenaren van de gemeente Groningen via een algemene oproep op intranet de kans om mee te doen totdat het maximum van honderd deelnemers was bereikt.

In Den Haag (eNIK) zijn de volgende doelgroepen benaderd:
- Studenten;
- Ambtenaren;
- WMO-cliënten.

In Den Haag waren 375 eNIK's beschikbaar. Binnen twee weken heeft het beoogde aantal deelnemers zich aangemeld. De gemeente Den Haag geeft hiervoor als mogelijk belangrijke reden het feit dat deelnemers aan de pilot de nieuwe NIK kosteloos krijgen. Op 4 januari is het aanmeldproces gestopt omdat er op dat moment er meer dan 500 aanmeldingen waren. Van de deelnemers die zich hebben opgegeven hebben er 320 daadwerkelijk een afspraak gemaakt om het eNIK aan te vragen. Daarom is er besloten om de wervingsperiode te verlengen. De mogelijkheid tot deelname aan de pilot is onder de aandacht gebracht bij medewerkers van de gemeente Den Haag, Logius en bij Rijksdienst Voor Identiteitsgegevens (RVIG) via de intranetten van deze organisaties. De laatste aanvraagmogelijkheid was op 4 maart. De laatste kaarten zijn door Morpho geproduceerd op 8 maart.

Onderstaande tabel toont de oorspronkelijk beoogde verdeling van deelnemers aan de pilot, de verdeling van aanmeldingen en de verdeling van de uiteindelijk uitgereikte eNIK's. Er heeft uiteindelijk een hoger aantal ambtenaren deelgenomen dan oorspronkelijk was gepland. Toen het duidelijk werd dat het gewenste aantal deelnemers niet zou worden behaald is er geworven binnen de gemeente Den Haag, het ministerie van BZK, ICTU en Logius.

Aantallen pilot eNIK Den Haag

	Beoogde aantal deelnemers	**Oorspronkelijk aanmelding van deelnemers**	**Gerealiseerde aantal deelnemers**
Studenten	150	228	131
Ambtenaren	150	150	178
WMO-cliënten	150	123	66
Algemeen belangstellenden (bijv. ambtenaren vanuit de gemeente Den Haag)	50		
Totaal	**500**	**501**	**375**

De onderstaande tabel geeft een overzicht van het aantal deelnemers dat zich aanvankelijk per gemeente en per doelgroep heeft aangemeld, het aantal personen dat is afgevallen en het totaal aantal personen dat het eRijbewijs of het eNIK heeft afgehaald (definitief geregistreerd als deelnemer). Uiteindelijk hebben 985 personen deelgenomen aan de pilot Publiek Middel door daadwerkelijk hun publieke middel af te halen.

Overzicht deelnemersaantallen per gemeente en doelgroep

Gemeente	**Doelgroep**	**Aanmeldingen**	**Afvallers**	**Deelnemers**	**Totaal**
Groningen	Ambtenaren	100	2	98	*98*[18]
Eindhoven	Berichtenbox-gebruikers	199	16	183	*464*
	Collega's	66	0	66	
	Digipanel	9	1	8	
	Stembureauleden	217	10	207	
Den Haag	Studenten	228	97	131	*375*[19]
	Ambtenaren	178	0	178	
	WMO-cliënten	123	57	66	
FUP users/extra uitgegeven kaarten RDW	6 naar ICTU en Logius, 5 naar evaluatie commissie, overige friends and family RDW	48	0	48	48
Totaal		**1168**	**183**	**985**	**985**

3.5.4 Het aanvraag- en uitgifte proces gedurende de pilot

3.5.4.1 Aanvraagproces eRijbewijs

Een aanvraag van het eRijbewijs verliep via de deelnemende gemeenten aan de hand van uitnodigingen aan potentiële pilotdeelnemers op voorwaarde dat men een geldig rijbewijs en DigiD heeft.[20] In de uitnodiging werd enige additionele informatie over de pilot en het eRijbewijs gegeven met contactinformatie en links naar aanvullende informatie. Men werd uitgenodigd om tot en met 15 mei een testrijbewijs en kaartlezer te gebruiken waarmee men toegang kreeg tot alle sites met DigiD-toegang.

Na aanmelding kregen deelnemers in Eindhoven later een bericht of ze geselecteerd waren voor de pilot of niet[21], in Groningen kon men zonder meer meedoen door naam en voorletters, geboortedatum, BSN, rijbewijsnummer, mailadres en telefoonnummer per mail door te geven aan een speciale postbus van de gemeente.[22] In Eindhoven verliep het aanmeldingen voor de pilot middels een website waar potentiële deelnemers zich in konden schrijven. Na daadwerkelijke

[18] Status pilot deelname tijdens interview gemeente Groningen 26 april, 2016.
[19] Status pilot deelname zoals doorgegeven door de gemeente Den Haag.
[20] Bron: meeloopdag gemeente Eindhoven en interview gemeente Groningen.
[21] Meeloopdag Eindhoven plus aanvullende documentatie ontvangen van ICTU.
[22] Bron: aanvullend interview met gemeente Groningen t.a.v. het verloop van de aanvraag procedure.

selectie ontving een pilotdeelnemer het verzoek om een afspraak te plannen via die website van de gemeente Eindhoven, met als aanvraag het afhalen van het product ‘pilot specimen rijbewijs’ op een door hem/haar zelf gekozen moment. In Groningen kon men het eRijbewijs afhalen tussen 12.00 en 17.00 (di t/m vr) of 13.00 en 17.00 (ma) zonder afspraak.

3.5.4.2 Aanvraagproces eNIK

Het aanvraagproces van de eNIK was op uitnodiging maar verliep verder exact zoals de gebruikelijk aanvraag van een NIK. Deelnemers moesten een afspraak maken en dienden alle in hun bezit zijnde reisdocumenten te tonen, plus pasfoto en betaalmiddel mee te nemen voor de aanvraag.

3.5.4.3 Uitgifteproces eRijbewijs

Tijdens het afhalen van het eRijbewijs dienden de pilotdeelnemers een wettelijk legitimatiebewijs (paspoort, identiteitskaart) en hun rijbewijs mee te brengen. De pilotdeelnemer ontving vervolgens (na een fysieke identificatie aan de hand van dit wettelijke document en het tonen van het rijbewijs) het eRijbewijs, de kaartlezer met instructies voor installatie en gebruik en korte uitleg over de pilot. Desgewenst kon men eveneens uitleg over het gebruik van het specimen rijbewijs en de kaartlezer krijgen van de baliemedewerker. Tijdens ontvangst moest de deelnemer een instemmingsverklaring tekenen om definitief mee te kunnen doen aan de pilot. Het afhalen van het eRijbewijs in Eindhoven gebeurde op de door de pilotdeelnemer ingevoerde datum en tijdstip. In Groningen konden deelnemers dagelijks op maandag van 13.00 tot 17.00 en dinsdag t/m vrijdag van 12.00 tot 17.00 uur hun eRijbewijs afhalen zonder afspraak.

Aan het einde van de dag stuurden de gemeenten een overzicht van alle uitgereikte eRijbewijs specimen aan het RDW. Dit ging middels een password beveiligd 7ZIP bestand via mail. Het password werd via SMS aan het RDW toegezonden. Het RDW verwerkte deze nieuw uitgereikte eRijbewijzen door ze op een white list te zetten voor activatie door Logius (BSN-koppeling actief maken) en aan de betreffende deelnemers een brief te sturen met informatie nodig om de kaart en de kaartlezer te activeren en in gebruik te nemen. Deze brief bevatte een persoonlijke pincode, puk-code en can-code en werd naar het huisadres van de deelnemers gestuurd.

3.5.4.4 Uitgifteproces eNIK

De uitgifte van de eNIK verliep hetzelfde als de uitgifte van de NIK. Burgers dienden wederom een afspraak te maken en een identiteitsbewijs mee te nemen. In de pilot Publiek Middel ontvingen deelnemers echter ook de kaartlezer, handleidingen voor installatie en gebruik van de kaartlezer en eNIK en uitleg over de eNIK. Daarnaast moesten ze de pilot voorwaarden/overeenkomst ondertekenen. Voor de uitgifte waren twee balies ingericht en bemand door speciaal opgeleid personeel. Deelnemers kregen na het in ontvangst nemen van de eNIK later per post de benodigde codes (pin, puk en can) toegestuurd om de kaartlezer te activeren en in gebruik te nemen.

3.5.5 Installatie en in gebruik name publieke middelen

3.5.5.1 Installatie kaartlezer en eRijbewijs

Als de gebruiker de kaartlezer op de computer met Microsoft Windows aansloot werd de benodigde driver voor de kaartlezer automatisch geïnstalleerd. Er was ook een card-driver voor Mac iOS beschikbaar.

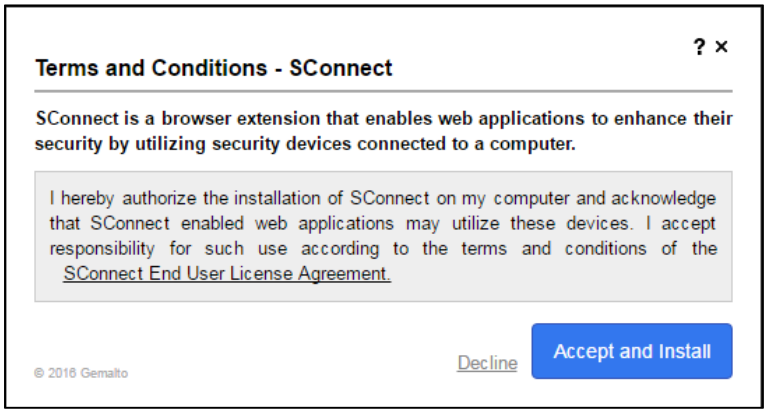
Voor het gebruik van de kaart in combinatie met de kaartlezer is er een speciale plug-in gemaakt. [16] Hoe de plug-in zich installeert is afhankelijk van de browser die de deelnemer gebruikt. Daarnaast kan de plug-in worden opgeslagen of worden uitgevoerd. De kaartlezer wordt eenmalig gekoppeld met de browser via deze browser plug-in en de door gebruiker ingevulde code van het RDW. Als dit eenmaal gebeurd is kan de gebruiker middels de card-reader, kaart en een pincode toegang krijgen tot alle sites die een DigiD toegang vragen.[23] Voor de installatie zijn er twee handleidingen beschikbaar voor deelnemers (een verkorte en een uitgebreide).

Gebruikers kunnen het eRijbewijs installeren via de website van DigiD.[24] Het installatieproces van eRijbewijs is weergegeven in onderstaande figuren.

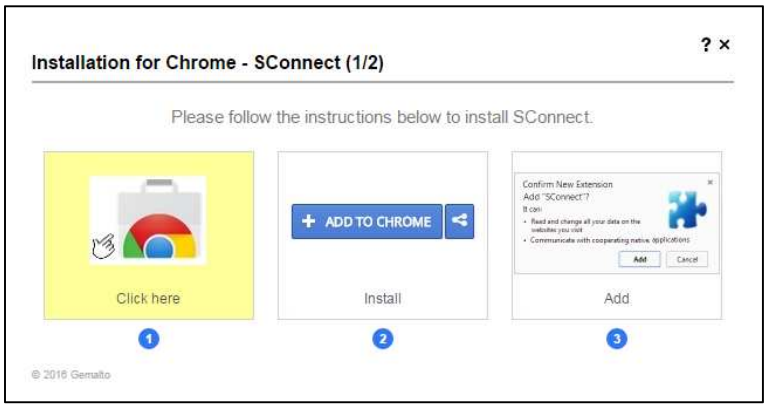
Figuur 41 eRijbewijs installatieproces stap 1

[23] Bron: meeloopdag Eindhoven, demonstratie en uitleg RDW.
[24] Zie https://www.digid.nl/over-digid/kaartlezer-pilot/

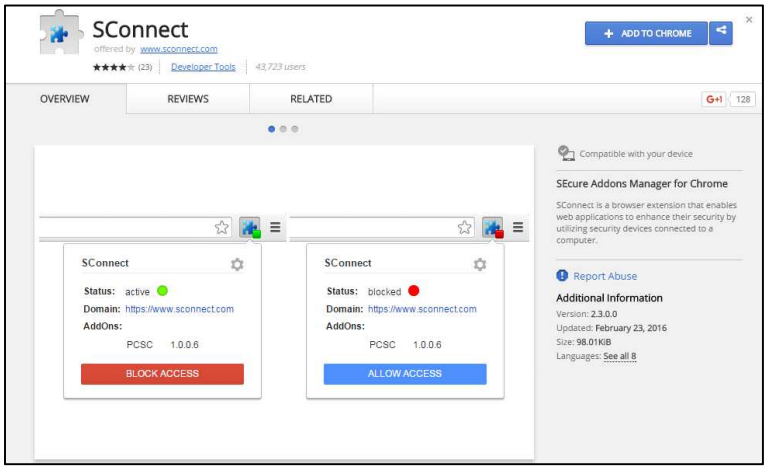
Figuur 42 eRijbewijs installatieproces stap 2



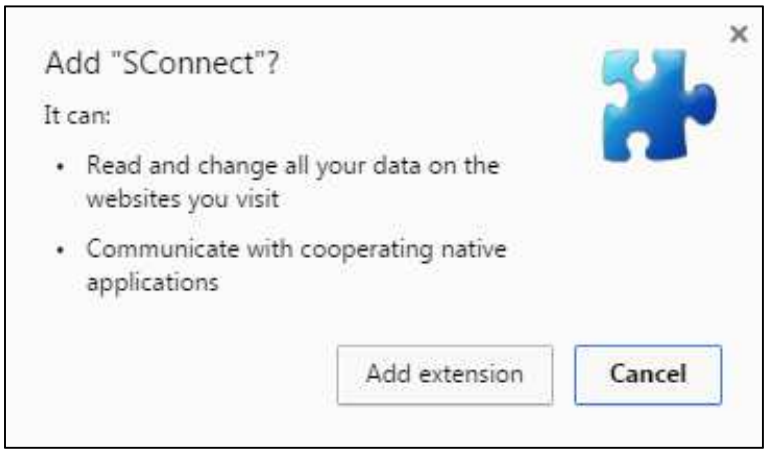
Figuur 43 eRijbewijs installatieproces stap 3



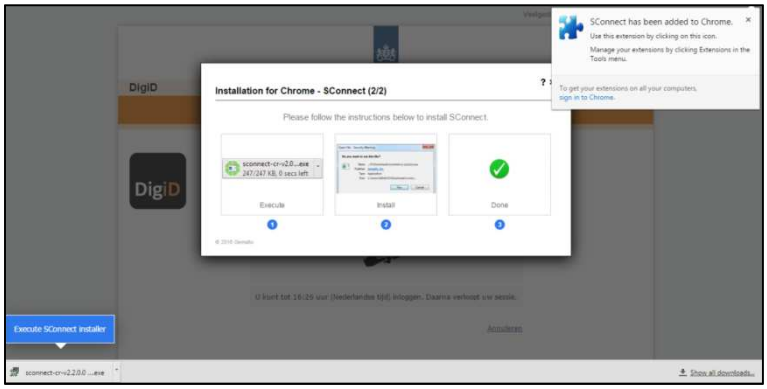
Figuur 44 eRijbewijs installatieproces stap 4



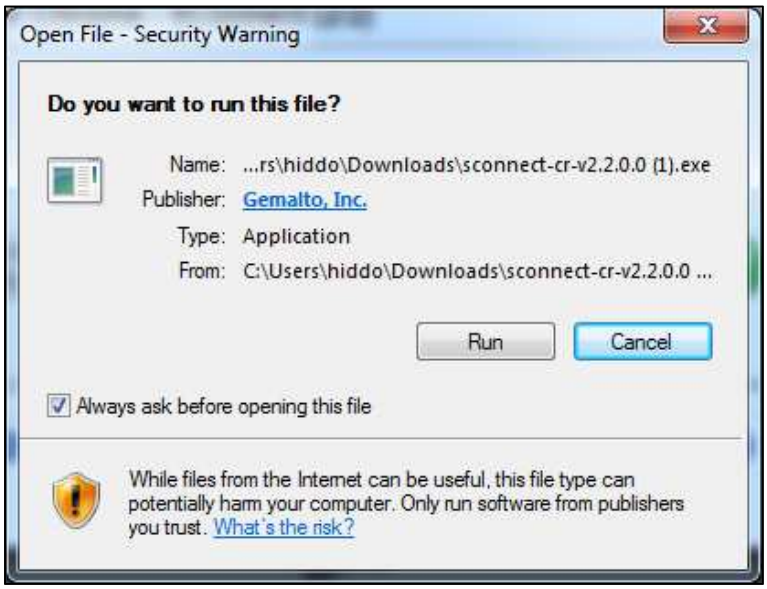
Figuur 45 eRijbewijs installatieproces stap 5



Figuur 46 eRijbewijs installatieproces stap 6



Figuur 47 eRijbewijs installatieproces stap 7



Figuur 48 eRijbewijs installatieproces stap 8

Figuur 49 eRijbewijs installatieproces stap 9

Figuur 50 eRijbewijs installatieproces stap 10

3.5.5.2 *Installatie kaartlezer en eNIK*

Experimenteren met dit middel was voor de onderzoekers van TNO niet mogelijk. Er was geen eNIK beschikbaar voor onderzoekers, aangezien geen van hen als inwoner ingeschreven stond in de gemeente Den Haag.

3.5.5.3 *Inloggen met eRijbewijs*

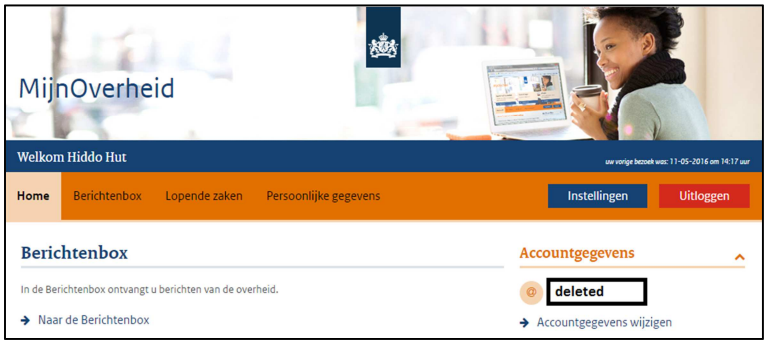
Gebruikers kunnen met een eRijbewijs inloggen op bij DigiD aangesloten websites zoals die van MijnOverheid. Het inlogproces van eRijbewijs op de website van MijnOverheid ziet er als volgt uit.

Figuur 51 eRijbewijs inlogproces MijnOverheid stap 1

Figuur 52 eRijbewijs inlogproces MijnOverheid stap 2

Figuur 53 eRijbewijs inlogproces MijnOverheid stap 3

Figuur 54 eRijbewijs inlogproces MijnOverheid stap 4



Figuur 55 eRijbewijs inlogproces MijnOverheid stap 5

Merk op dat bovenstaande screenshots uit het inlogproces gemaakt zijn om het complete inlogproces inzichtelijk te maken, dus vanaf de homepage van MijnOverheid.[25] Strikt genomen start het echte inloggen bij stap 2 wanneer de eindgebruiker zijn/haar publieke middel selecteert en op de 'Volgende' knop klikt.

3.5.5.4 *Inloggen met eNIK*

Experimenteren met dit middel was niet mogelijk, omdat de onderzoekers zoals vermeld niet beschikten over een eNIK.

[25] Zie https://mijn.overheid.nl/

4 Antwoorden op de gestelde onderzoeksvragen

Dit hoofdstuk beschrijft de gevonden antwoorden en bevindingen voor iedere specifieke onderzoeksvraag, met daarbij telkens de bronvermelding. De antwoorden op de onderzoekvragen zijn voor iedere pilot in een nieuwe paragraaf beschreven, waarbij in sub-paragrafen telkens onderscheid is gemaakt naar de drie onderzoeksgebieden techniek, privacy en ervaringen.

4.1 Beantwoording van de onderzoeksvragen voor de pilot Idensys

4.1.1 Onderzoeksvragen met betrekking tot techniek

Hoofdvraag 1: Is er voldaan aan de betrouwbaarheid zoals geformuleerd in het afsprakenstelsel?

Hierbij zijn de volgende deelvragen geformuleerd:
Deelvraag 1a: Zijn er incidenten die wijzen op een feitelijke lage betrouwbaarheid?
Deelvraag 1b: Hoe zijn deze incidenten afgehandeld?

Bevindingen hoofdvraag 1:
Op de bijeenkomst van de begeleidingscommissie dd. 15/02/16 is besloten dat deze vraag geïnterpreteerd dient te worden als ‘de betrouwbaarheid van iemands elektronische identiteit, ook wel ‘Level of Assurance’ (LoA)’ genoemd. Met andere woorden: het gaat hier specifiek om de betrouwbaarheidseisen. Dit komt overeen met de definitie van ‘Betrouwbaarheidsniveau’ in de begrippenlijst in het afsprakenstelsel (zie pagina 27 daarvan) [8]. Het afsprakenstelsel bevat een ‘Normenkader betrouwbaarheidsniveaus’ (vanaf pagina 420), dat weergeeft wat nodig is om een bepaald betrouwbaarheidsniveau te halen (pagina 422 - pagina 527).

In ‘Toezichtstaken toezichthouder’ staat dat de Toezichthouder de ‘conformiteit aan de toepasselijke normenkaders van partijen die wensen toe te treden tot het afsprakenstelsel’ toetst (pagina 49). Het toetsen of aan deze eis is voldaan is de bevoegdheid van de Minister van EZ. Hij laat zich bij zijn oordeel ondersteunen door externe accountantsrapporten, de beheerorganisatie van het afsprakenstelsel, het Agentschap Telecom en een Commissie van Deskundigen.[26]

De Minister van Economische Zaken heeft ten behoeve van dit onderzoek verklaard dat de partijen die binnen Idensys diensten aanbieden allemaal voldoen aan de gestelde eisen (zie bijlage E). Daaruit leidt TNO dan ook af dat de Minister van EZ, als verantwoordelijke, heeft geoordeeld dat aan de eisen is voldaan. Dit oordeel is gebaseerd op de uitkomsten van de toets van de auditor en het advies van de Commissie van Deskundigen. Daarbij bestaat overigens de mogelijkheid dat er nog aandachtspunten zijn die een partij moet oplossen, maar die de veiligheid of betrouwbaarheid van het stelsel niet in de weg staan. Of daarvan wel of geen sprake is of is geweest heeft TNO niet kunnen vaststellen.

[26] https://zoek.officielebekendmakingen.nl/stcrt-2016-20595.html

Noot: de onderzoekers van TNO hadden voor dit project niet het mandaat of de mogelijkheid om zelf het normenkader voor de betrouwbaarheidseisen te toetsen bij de toegetreden partijen. TNO kan deze vraag daarom niet op basis van eigen onderzoek beantwoorden. Als alternatief heeft TNO inzage gevraagd in de verklaring van Agentschap Telecom, dat toegetreden partijen voldoen aan de betrouwbaarheidseisen. Het betrof specifiek een verzoek om inzage in de assessmentrapportage van Agentschap Telecom aan de Commissie van Deskundigen en in het bijbehorende advies van die commissie aan de minister, betreffende de partijen die zijn toegetreden tot het stelsel. TNO heeft bij Agentschap Telecom echter geen inzage gekregen in het 'Controle Memorandum' betreffende toegetreden partijen. De reden hiervoor is dat deze rapportages vertrouwelijke gegevens bevatten; onder meer details over de beveiliging en de algehele werking van IT-systemen en -processen van toegetreden partijen. Het geven van inzage zou tevens in strijd zijn met het afsprakenstelsel.

Bevindingen deelvraag 1a:
Er zijn voor Idensys met betrekking tot deze betrouwbaarheidseisen tot nu toe geen incidenten gemeld bij het Agentschap Telecom en in bredere zin zijn bij het Agentschap Telecom ook geen incidenten bekend [Bron: Agentschap Telecom].

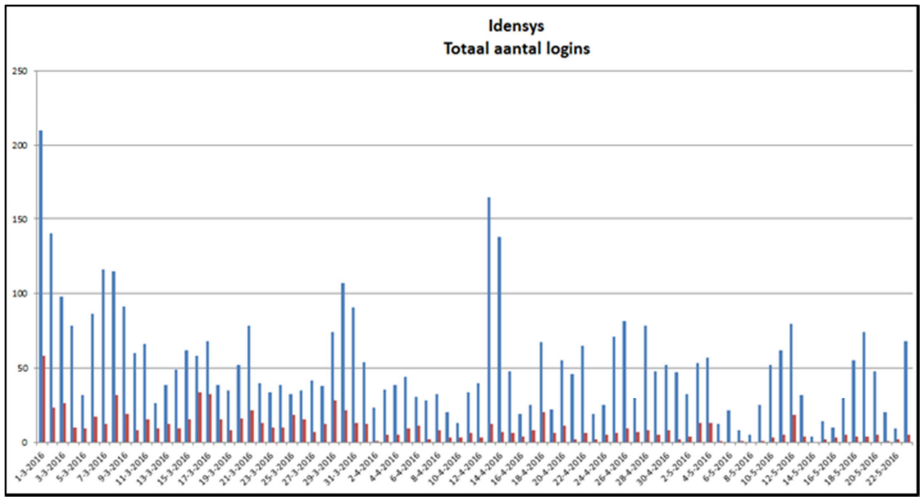
Bevindingen deelvraag 1b:
Niet van toepassing, zie vraag 1a.

Hoofdvraag 2: In welke mate is er voldaan aan de gestelde eisen omtrent beschikbaarheid?

Bevindingen hoofdvraag 2:
In de paragraaf 'Service Level' (pagina 133) in het Idensys afsprakenstelsel [17] staat genoemd 'Beschikbaarheid van diensten voor de productieomgeving' met als norm '24 uur x alle dagen van het jaar' en als minimaal te realiseren niveau 99,2%.

Uit de aangeleverde pilotrapportage kan niet worden afgeleid of de beschikbaarheid voor deze norm wordt gemeten, hoe deze wordt gemeten en welk niveau daadwerkelijk is gehaald. Als alternatief heeft TNO daarom inzicht gevraagd in de dag-statistieken van het BSNk (over alle middelen heen), om het aantal authenticaties per dag te kunnen zien. Op basis daarvan zou mogelijk kunnen worden afgeleid of de infrastructuur tijdens de meetperiode maart en april 2016 dagelijks is gebruikt en dus elke dag beschikbaar was. De betreffende data is echter niet aangeleverd door BSNk.

Uit de van de Belastingdienst ontvangen pilotrapportage [Bron: mail Belastingdienst dd. 24/05/2016] over de maanden maart en april 2016 (Figuur 56) blijkt echter wel dat met de Idensys-middelen elke dag eindgebruikers hebben ingelogd. Hierop baseert TNO het antwoord dat de hiervoor benodigde infrastructuur in de meetperiode elke dag beschikbaar is geweest.



Figuur 56 Pilotrapportage Belastingdienst m.b.t. Idensys

Hoofdvraag 3: In welke mate is voldaan aan de informatieveiligheidseisen?

Hierbij zijn de volgende deelvragen geformuleerd:
Deelvraag 3a: Zijn er incidenten die wijzen op het niet voldoen aan de informatieveiligheidseisen?
Deelvraag 3b: Hoe zijn deze incidenten afgehandeld?

Bevindingen deelvraag 3:
Aan beheerorganisatie van het Idensys-afsprakenstelsel (Logius), specifiek de security officer, is gevraagd of er veiligheidsincidenten zijn geweest in de meetperiode maart en april 2016.

Er is de meetperiode één incident gemeld, dat te maken had met een tijdelijke onbeschikbaarheid van een partij in het netwerk.[27] Dit incident was van dermate korte duur dat nog steeds is voldaan aan de beschikbaarheidseisen. Er zijn geen incidenten gemeld die te maken hebben met de vertrouwelijkheid of integriteit. Hiermee is voor 100% voldaan aan de informatieveiligheidseisen uit het Afsprakenstelsel [Bron: mail Logius dd. 18/05/2016].

Bevindingen deelvraag 3a:
Nee.

Bevindingen deelvraag 3b:
Incidenten worden afgehandeld volgens een vastgesteld proces.[28] Onderdeel van dat proces is het opstellen van een incidentrapport dat wordt gedeeld met stakeholders, zodat hier gezamenlijk lering uit kan worden getrokken.

Hoofdvraag 4: Hoe is het toezicht verlopen?

Bevindingen hoofdvraag 4:

[27] Merk op dat melden van incidenten verplicht is. Dit staat dan ook los van het permanent loggen van de beschikbaarheid van het stelsel, zoals behandeld bij hoofdvraag 2 hierboven.
[28] https://afsprakenstelsel.etoegang.nl/display/as/Proces+incidentmanagement

De Onderzoeksraad voor Veiligheid (OVV) heeft in een rapport met betrekking tot de DigiNotar-affaire aangegeven dat het toezicht en het beheer op soortgelijke diensten moeten worden gescheiden.[29] Voorheen vervulde Logius in relatie tot het ETD (elektronische toegangsdiensten)-stelsel beide rollen.

De minister van EZ is belast met het toezicht op het ETD-stelsel. Het gaat om atypisch toezicht aangezien er geen sprake is van publiekrechtelijk geregeld toezichthouderschap met de daarbij behorende bevoegdheden ten aanzien van informatievergaring en sanctionering (onder andere te vinden in de Algemene wet bestuursrecht (Awb). Er is alleen een privaatrechtelijk afsprakenstelsel. Om de minister te ondersteunen in de uitoefening van zijn atypische toezichttaak is een Commissie van Deskundigen ingesteld (Staatscourant 14 april 2016[30]) die bestaat uit drie externe experts afkomstig uit het veld en/of de wetenschap. Deze commissie verstrekt de minister advies omtrent te nemen beslissingen. Om te komen tot deze adviezen wordt de commissie ondersteund door een secretariaat. Naar aanleiding van het rapport van de OVV is de scheiding van beide rollen voor beheer en toezicht hiermee in werking gezet.

Het secretariaat van de commissie is onder andere belast met de uitvoering van de volgende activiteiten: het monitoren, het beoordelen van auditrapporten en proceswijzigingen, het toetsen van partijen die wensen toe te treden tot het ETD-stelsel, het doen van inspecties, afhandelen van klachten die de betrouwbaarheid van het stelsel schaden, optreden bij incidenten, opstellen van rapporten van bevindingen en het verrichten van werkzaamheden die dit mogelijk maken. Voor een volledig overzicht wordt verwezen naar de offerte die Agentschap Telecom heeft uitgebracht. [31] Agentschap Telecom is gevraagd om de secretariaatsfunctie gestalte te geven, vooruitlopend op de toezichttaak die vanaf 2017/2018 moet worden ingevuld op basis van het Wetsvoorstel Generieke Digitale Infrastructuur (GDI). Met het GDI-wetsvoorstel wordt naar verwachting Agentschap Telecom de externe toezichthouder waarmee formeel publiekrechtelijk toezicht mogelijk wordt op basis van een wettelijke grondslag.

In opdracht van EZ gaf Logius tot 1 januari 2016 uitvoering aan de toezichtactiviteiten van de formele toezichthouder: de Minister van EZ. Tussen 1 januari en 1 maart 2016 was het toezicht niet alleen formeel belegd bij EZ, het gaf op dat moment ook eigenstandig uitvoering aan de toezichtactiviteiten. Vanuit Logius en Agentschap Telecom zijn mensen hiervoor beschikbaar gesteld aan EZ.

Per 1 maart 2016 is de minister nog steeds formeel toezichthouder. Vanaf dat moment is ook de Commissie van Deskundigen actief die de minister adviseert. Het Agentschap Telecom vormt per 1 maart 2016 het secretariaat van de commissie, echter nog steeds op basis van een privaatrechtelijk afsprakenstelsel.

Tijdens het interview met TNO gaf Agentschap Telecom aan dat op dat moment drie partijen in de rol van middelenleverancier waren toegelaten tot het Idensys-stelsel:

---

[29] De Onderzoeksraad voor Veiligheid, Het Diginotar-incident – Waarom digitale veiligheid de bestuurstafel weinig bereikt, Den Haag, juni 2012.
[30] Zie http://wetten.overheid.nl/BWBR0037833/2016-04-20
[31] Zie “Offerte Secretariaatsfunctie voor de Commissie van Deskundigen ten behoeve van toezicht op het ETD-stelsel”, Agentschap Telecom, M.J. Schol, 10-12-2015

- Digidentity B.V. is op 29 december 2015 officieel tot het Introductieplateau Idensys toegetreden als herkenningsmakelaar, authenticatiedienst en middelenleverancier.[32]
- Op 13 april 2016: Met de toetreding van CreAim B.V. en KPN B.V. in de rollen van authenticatiedienst en middelenuitgever (beide partijen waren in eerdere tranches al toegetreden in de rol van herkenningsmakelaar voor het consumenten en BSN domein), zijn de mogelijkheden om via Idensys in te loggen bij dienstverleners uitgebreid.[33]

4.1.2 Onderzoeksvragen met betrekking tot privacy

Hoofdvraag 5: Wat zijn de resultaten van de PIA en hoe is omgegaan met de uitkomsten?

Hierbij zijn de volgende deelvragen geformuleerd:
Deelvraag 5a: Is er een PIA uitgevoerd?
Deelvraag 5b: Zijn er mitigerende maatregelen voorgesteld?
Deelvraag 5c: Zijn deze mitigerende maatregelen uitgevoerd?
Deelvraag 5d: Hebben zich desondanks nog privacy incidenten t.a.v. privacy voorgedaan?
Deelvraag 5e: Hoe zijn deze privacy incidenten opgelost?

Bevindingen hoofdvraag 5:
De PIA zoals die is uitgevoerd door Mazars [7] stelt dat in de omschrijvingen van het Introductieplateau eID en in het Afsprakenstelsel uitdrukkelijk aandacht is besteed aan technische en procedurele maatregelen waarmee de privacy van burgers is bevorderd. Er zijn echter ook een aantal risico's voor de privacybescherming onderkend, waarvan werd aangegeven dat het procedurele risico's betrof. Voorgestelde maatregelen waren dan ook louter van procedurele aard en er was geen sprake van nadere technische maatregelen. Bij een grootschaliger uitrol van het Introductieplateau zouden mogelijk wel meer technische maatregelen vereist zijn.

Bevindingen deelvraag 5a:
De PIA is uitgevoerd, waarmee vraag 5a positief beantwoord kan worden (zie ook Nota van Inlichtingen). [18]

Bevindingen deelvraag 5b:
In de PIA zijn enkele mitigerende maatregelen voorgesteld. De voorgestelde maatregelen zijn van verschillende aard. In totaal zijn twaalf belangrijke privacy-risico's benoemd en voorzien van een aanbeveling. Deze twaalf punten worden hier kort genoemd. Voor uitgebreide beschrijvingen wordt verwezen naar het PIA rapport van Mazars [7], in het bijzonder hoofdstuk 4.

De twaalf punten zijn:
a) Het gebruik van BSN binnen het private domein vereist aanpassing van wet- en regelgeving.

[32] Zie https://www.idensys.nl/actueel/item/artikel/eerste-toetreding-maakt-start-idensys-pilots-mogelijk-1/
[33] Zie https://www.idensys.nl/actueel/item/artikel/idensys-breidt-uit-inloggen-bij-belastingdienst-nu-ook-met-creaim-en-kpn/

b) Risico's van het verwerken van metadata (loggings, audittrails, etc.), inzet van third party services en inherente risico's die kleven aan het gebruik van internettechnologie, vereisen nadere aandacht zodat deze risico's ook vanuit privacy en security oogpunt worden beheerst.
c) Bij de Authenticatie Diensten ontstaan onvermijdelijk cumulaties van gevoelige verzamelingen van persoonsgegevens, zogenaamde 'hotspots'.
d) Er is een aantal specifieke privacy vraagstukken aangaande het bewaren van gegevens en het privacy principe van dataminimalisatie.
e) De bewaartermijn van 7 jaar dient waar mogelijk verkort te worden en er kan met gedifferentieerde bewaartermijnen gewerkt worden.
f) Het toetreden van dienstaanbieders dient te worden gereguleerd en voorzien van een eisenstelsel.
g) Er dient een vereiste te zijn voor technische scheiding van machtigings- en attributendiensten indien deze door één organisatie worden aangeboden.
h) Het Introductieplateau voorziet in de functionaliteit dat Authenticatiediensten vrij attributen kunnen toevoegen aan de verwerking van eID gerelateerde persoonsgegevens en deze attributen kunnen meeleveren aan Dienstverleners. De toepassing van vrije attributen vereist nadere regulering en toetsing, en met de middelenleveranciers moet worden afgesproken dat dit niet gebeurt.
i) Het BSNk legt van elke identificatie of inlogactie van een burger, ten minste het BSN, de Pseudo-identiteit én de Identiteit van de bezochte BSN-dienstverlenende organisatie vast. Het gevolg hiervan is dat centraal op één punt alle inlogacties van Burgers bij de websites van Dienstverleners in het BSN domein geregistreerd en dus zichtbaar zijn. Vanuit privacy-optiek is het BSNk een gevoelige verwerking van persoonsgegevens (hotspot).
j) Het risico van function creep vereist scherpe bewaking en toetsing bij betrokken overheidsdiensten én marktpartijen. Doorontwikkeling en optimalisatie van het eID Stelsel na het Introductieplateau eID is voorzien maar is ook essentieel om een breed en robuust eID Stelsel te kunnen realiseren en handhaven. Dit moet met de Toezichthouder worden besproken.
k) Maatregelen aangaande fraudedetectie, en interne controle maatregelen gericht op het verhogen van de datakwaliteit bij eID deelnemers en BSN-koppelregister zijn nog niet gedefinieerd.
l) Er zijn in het ontwerp geen voorzieningen getroffen voor opsporingsdoeleinden door Openbaar Ministerie en politie.

In aanvulling op deze twaalf punten is door het Strategisch Beraad nog een dertiende punt, dat ook in de PIA is aangekaart, als actiepunt benoemd, namelijk dat gebruikers tijdens het Introductieplateau eID (Idensys) op de hoogte moeten zijn van de risico's van het gebruik van het eID stelsel (Idensys). [19]

Bevindingen deelvraag 5c:
Onder referentie naar de lijst van punten in de beantwoording van voorgaande vraag wordt hier per punt telkens aangegeven wat er met de mitigerende maatregelen is gedaan op het gebied van implementatie.

a) De regelgeving (Wet GDI) is nog niet gereed en wordt ook niet voor 2017 verwacht. Bij gebrek aan deze publiekrechtelijke grondslag voor de verwerking van het BSN in het private domein is voor de pilotfase een oplossing gekozen om te werken met bewerkersovereenkomsten. Als mitigerende maatregel was voorgesteld om in de Wet Elektronisch Berichtenverkeer Belastingdienst (EBV)

op te nemen dat het BSNk er is en dat daarmee private partijen in staat worden gesteld het BSN te verwerken. Die wet is aangenomen en er wordt dus gewerkt met bewerkersovereenkomsten. De minister van BZK heeft, als verantwoordelijke voor de verwerking, deze overeenkomsten afgesloten met de Idensys middelenleveranciers (als bewerkers). In deze bewerkersovereenkomsten is vastgelegd op welke wijze en voor welke limitatieve doeleinden het BSN verwerkt mag worden middels het BSNk. Als tijdelijke oplossing voor de pilotfase is dat houdbaar, maar voor een uiteindelijke eventuele verdere uitrol is de wettelijke grondslag vereist.

b) Er is in het Afsprakenstelsel een verplichte pentest[34] opgenomen. Middelenleveranciers dienen jaarlijks zelf een onafhankelijke test te laten uitvoeren. Daarnaast wordt door Logius op reguliere basis een pentest uitgevoerd. Dit is een onderdeel van het reguliere auditproces, zoals dat ook vanuit het toezicht op het stelsel is vastgelegd.[35] Deze wijziging is de uitwerking van RFC1974. [20] Deze maatregel draagt bij aan een goede security van het stelsel. Primair is deze maatregel echter een wijziging in het kader van proces en beleid, en niet aangemerkt als voortvloeiend uit de PIA. [19] Een nadere uitwerking voor privacy staat gepland voor 2016.

c) Dit aspect is in het PIA rapport aangemerkt als onvermijdelijk. Wel is aanbevolen organisatorische waarborgen hiervoor uit te werken. Een eerste stap hiertoe is gezet middels RFC 2001, waarin de Attribuutverstrekking door Authenticatiediensten wordt beperkt tot attributen die zij zelf bij haar rol als authenticatiedienst reeds in beheer heeft. [20] Het aantal attributen dat hiermee door één Authenticatiedienst kan worden verwerkt wordt beperkt.

d) In het Afsprakenstelsel is een privacy-beleid opgenomen (RFC 1990). [20] Het privacy-beleid betreft vier specifieke onderdelen:
   1. Regulering, toezicht en handhaving ten aanzien van ‘hotspots bij Authenticatie Diensten;
   2. Transparantie ten aanzien van de verwerking van persoonsgegevens;
   3. Function creep (dus het voorkomen van gebruik van het stelsel voor andere doeleinden dan beoogd);
   4. ‘Privacy audits’ ten aanzien van de verwerking van persoonsgegevens.

   Tevens is voor de concrete implementatie van het privacy-beleid binnen de verschillende organisaties een methodiek aangereikt. Deze bestaat uit de volgende stappen:
   1. Inventarisatie van de verwerking en vastligging hiervan in Checklist Wet bescherming persoonsgegevens.
   2. Een jaarlijkse terugkerende Privacy Self-Assessment (PSA) waarin door de verantwoordelijken voor de verwerking van persoonsgegeven binnen het afsprakenstelsel elektronische toegangsdiensten wordt gecontroleerd:
      - Of de verwerking van persoonsgegevens nog actueel zijn en
      - De onderliggende processen die moeten worden ingericht ter naleving van de Wbp (zie Bijlage II) nog actueel zijn.

[34] Middels een pentest (penetratietest) wordt onderzocht of van buitenaf in de systemen van een partij kan worden ingebroken.
[35] https://afsprakenstelsel.etoegang.nl/display/as/Beleid+voor+penetratietesten

3. Privacy Impact Analyse (PIA) bij het voornemen een nieuwe functionaliteit in het afsprakenstelsel op te nemen.

e) Vooralsnog wordt de bewaartermijn van zeven jaar gehandhaafd. Wel is in de vorm van RFC 1991 een wijziging op het Afsprakenstelsel doorgevoerd die een onderbouwing voor de bewaartermijn toevoegt. [20] De zeven jaar is bepaald aan de hand van onder meer belastingwetgeving in het kader van fraudebestrijding. Later wordt nog bekeken of de bewaartermijn voor bepaalde gegevens bij bepaalde partijen verkort kan worden.

f) Er is een proces voor toetreding tot het stelsel vastgelegd. Gedurende dit proces wordt getoetst of een middelenleverancier voldoet aan de eisen uit het Afsprakenstelsel. De aspecten uit het normenkader moeten naar behoren zijn ingevuld. De minister van EZ besluit uiteindelijk op basis van de uitkomsten van de toets of een partij wordt toegelaten. Zie in dit kader ook het antwoord op vraag 4 hierboven over toezicht. Aanbeveling: normenkader ook uitwerken in toetsingskader.

g) Geen mitigerende maatregelen aangetroffen, deze staan geagendeerd voor 2016. [20]

h) RFC 2011 die in het Afsprakenstelsel versie 1.9c is geïmplementeerd bepaalt dat authenticatiediensten alleen attributen mogen verstrekken die reeds vanuit de uitoefening van haar rol in bezit zijn. [20] Verstrekken van verdere gegevens is niet toegestaan. Nadere afspraken over het beperken van attribuutverstrekking door middelenleveranciers zijn (nog) niet gemaakt. Integendeel, enkele middelenleveranciers geven aan in de toekomstige dienstverlening ook aanvullende attributen te willen verstrekken aan dienstaanbieders op basis van toestemming van de burger die het middel gebruikt.

i) Geen mitigerende maatregelen aangetroffen, deze staan geagendeerd voor 2016 (oplegnotitie Strategisch Beraad).

j) In RFC 1990 (privacy-beleid) is een onderdeel opgenomen dat zich hierop toespitst. Concreet is aandacht besteed aan de beperking van de te verwerken gegevens in relatie tot het doel van de verwerking en de rol van de dienstverlener die gegevens verwerkt. Ter ondersteuning zijn een aantal doelomschrijvingen uitgewerkt. [20]

k) Dit punt staat geagendeerd voor 2017.

l) Dit punt staat geagendeerd voor 2017.

Met betrekking tot het extra punt dat door het Strategisch Beraad is vastgesteld zijn al enkele maatregelen genomen. Deze maatregelen doelen hoofdzakelijk op het bieden van meer transparantie richting eindgebruikers. RFC 2008 stelt bijvoorbeeld vast dat Dienstverleners een privacy-beleid dienen vast te stellen en inzichtelijk te maken. Doelbinding is hierbij als centraal begrip gepositioneerd en de informatie dient dan ook primair te gaan over het gebruik en verstrekken van

persoonsgegevens. Per dienst en per attribuut dient de doelverantwoording opgenomen te worden in de dienstencatalogus. [20]

Bevindingen deelvraag 5d:
Agentschap Telecom heeft op 21 april 2016 verklaard dat er bij haar geen incidenten met betrekking tot de privacy of het anderszins aantasten van de betrouwbaarheid van het stelsel bekend zijn over de periode maart 2016.

Bevindingen deelvraag 5e:
Aangezien er geen incidenten bekend zijn bij Agentschap Telecom zijn er geen incidenten opgelost.

4.1.3 Onderzoeksvragen met betrekking tot ervaringen

De onderzoeksvragen ten aanzien van de ervaringen van de pilot Idensys hebben betrekking op twee groepen partners binnen deze pilot: Leveranciers (paragraaf 4.1.3.1) en dienstaanbieders (paragraaf 4.1.3.2).

De ervaringen van de leveranciers zijn geanonimiseerd en gebundeld aangezien er voor de beantwoording van de vragen en het trekken van conclusies geen noodzaak bestaat de ervaringen te kunnen herleiden naar specifieke organisaties of personen.

4.1.3.1 Onderzoeksvragen met betrekking tot ervaringen van leveranciers

Hoofdvraag 6: Hoe ervaren de leveranciers de deelname aan de pilot?

Hierbij zijn de volgende deelvragen geformuleerd:
Deelvraag 6a: Wat zijn redenen voor leveranciers om deel te nemen aan de pilot?
Deelvraag 6b: Hoe is de pilot voor de leveranciers verlopen?
Deelvraag 6c: In welke mate zien leveranciers het hoogwaardige middel als toegevoegde waarde?

Ter beantwoording van deze vragen zijn interviews gehouden met Digidentity, KPN en CreAim. Follow-ups ten aanzien van de interviews bestonden uit aanvullende telefonische gesprekken en mailuitwisseling ter bevestiging en vergaring van aanvullende data.

Bevindingen deelvraag 6a:
Deze deelvraag is opgedeeld in twee sub-vragen: ‘Waarom doen leveranciers mee aan Idensys?’ en ‘Waarom doen leveranciers mee aan de pilot?’

Samenvattend:
Aangedragen ***motivaties om mee te doen aan Idensys*** genoemd door leveranciers zijn de volgende:

- Visievorming t.a.v. het stelsel en middel: belang van veilige inlogmiddelen, bewustzijn dat er opvolgers/aanvullingen voor DigiD nodig zijn, belang van een publieke- private samenwerking.
- Gebruikers: overtuiging dat burgers zelf hun leverancier moeten kunnen kiezen.
- Markt: vanuit commerciële redenen, verbredingen van doelgroep, behoeften van klanten en hun wantrouwen ten opzichte van banken.

- Rol van de leverancier: jarenlange rol als dienstenleverancier op dit gebied, vanuit een maatschappelijke rol.
- Innovatie: waardevol om aan nieuwe initiatieven deel te nemen.

Aangedragen ***motivaties om mee te doen aan de pilot*** genoemd door leveranciers zijn de volgende:

- Vanwege het beroep aan leveranciers om te investeren;
- Leren van de pilots;
- Pilot als lakmoesproef;
- Pilots als test van het gehele stelsel.

Hieronder volgt de uitgebreide weergave van de antwoorden.

Aangedragen ***motivaties om mee te doen aan Idensys*** genoemd door leveranciers zijn de volgende:

<u>Visie vorming t.a.v. het stelsel en middel:</u>

- Belang van veilige inlogmiddelen die herbruikbaar zijn met optimale bescherming van privacy.
- Bewustzijn dat er opvolgers/aanvullingen voor DigiD nodig zijn: DigiD levert een beperkt betrouwbaarheidsniveau en een hoger betrouwbaarheidsniveau is wenselijk. Eén leverancier geeft aan te verwachten dat Idensys en/of iDIN de toekomst zijn. De verwachting is dat DigiD eindig zal zijn. DigiD zal wel een rol behouden aangezien er rekening moet worden gehouden met mensen die geen gebruik kunnen of willen maken van een privaat middel. Deze leverancier verwacht dat het publieke middel nagenoeg ongebruikt zal zijn aangezien het alleen voor overheidsdiensten gebruikt kan worden. De leverancier geeft aan dat Idensys en het bankenmiddel voor de meeste mensen makkelijker in het gebruik zijn; de meeste mensen beschikken al over een smartphone of een bankpas.
- Belang van een publieke- private samenwerking; met een middel op hoog betrouwbaarheidsniveau waarbij er innovaties plaatsvinden onder toezicht van de overheid en er transparantie is.

<u>Gebruikers:</u>

- De overtuiging dat burgers zelf hun leverancier moeten kunnen kiezen vanuit de volgende motivaties: privacy overwegingen van burgers, stimuleren van innovatie door leveranciers, ongeschiktheid van DigiD voor gebruik bij commerciële sites (commerciële sites mogen niet beschikken over een BSN terwijl deze met DigiD wel wordt uitgewisseld).

<u>Markt:</u>

- Vanuit commerciële redenen: één leverancier geeft aan middelen die succesvol lijken verder te willen ontwikkelen. Daarnaast vindt de leverancier het belangrijk om de verschillende middelen te kennen om naar klanten een eerlijke vergelijking te kunnen maken.
- Verbredingen van doelgroep: één leverancier wil ook burgers en consumenten kunnen bedienen naast de zakelijke markt.
- Behoeften van klanten en hun wantrouwen ten opzichte van banken: één leverancier geeft aan dat haar klanten het belangrijk vinden dat hun leverancier aan deze pilot deelneemt. Zij weten dat de privacy is gewaarborgd

bij de betreffende leverancier en wantrouwen banken; zij vrezen dat banken privacy gevoelige klantgegevens gaan misbruiken. Ook ervaren klanten het als een probleem dat banken een bankpas kunnen intrekken.

Rol van de leverancier:

- Jarenlange rol als dienstenleverancier op dit gebied: leveranciers noemen onder meer hun rol als 'trusted third party', dienstenleverancier van cryptografische systemen waarin overheid en bedrijfsleven met elkaar interacteren en als eHerkenning leverancier. Ook geven ze aan te hebben meegewerkt aan eerdere stelselontwikkelingen.
- Vanuit een maatschappelijke rol: één leverancier noemt dat zij vanuit eerdere digitale calamiteiten als les heeft opgedaan dat het identiteits- en toegangsmechanisme onderdeel wordt van de kritische infrastructuur. Het is belangrijk om dit niet lichtzinnig of uitsluitend vanuit het zakelijk perspectief te bezien; het leidt tot keten-effecten en catastrofes als mensen en systemen geen toegang hebben tot digitale systemen van overheidspartijen of andere private diensten in de samenleving.

Innovatie:

- Innovatie: het is waardevol om deel te kunnen nemen aan nieuwe initiatieven.

Aangedragen ***motivaties om mee te doen aan de pilot*** genoemd door leveranciers zijn de volgende:

- Vanwege het beroep aan leveranciers om te investeren: één leverancier geeft aan dat er een beroep op haar is gedaan om te investeren in Idensys. Een aantal andere partijen waren hier onvoldoende toe in staat.
- Leren van de pilots; met name over de beleving van gebruikers en dienstverleners: één leverancier geeft aan dat er in het verleden veel pilots zijn gedaan. Er was daarbij minder aandacht voor de beleving van dienstverleners en gebruikers. Er werd meer vanuit de overheid gekeken en vanuit de stappen die de overheid wil zetten. Deze leverancier wil in de pilot leren hoe burgers/consumenten reageren. Deze pilots zijn cruciaal om de gebruikersbeleving te optimaliseren; het gaat om gemak en eenvoud voor de gebruiker.
- Pilot als lakmoesproef: één leverancier ziet de pilot als lakmoesproef voor de ontwikkelingen die de afgelopen twee jaar hebben plaatsgevonden.
- Pilots als test van het gehele stelsel: bij de pilots gaat het om de vraag of het stelsel in de volle breedte werkt. Tijdens deze pilot wordt de consument in de volle breedte gezien; als klant én als burger in BSN domein. Het gaat om onderwerpen als marktsentiment, gebruikersbeleving, 'computer literacy', het normenkader, juridische raamwerk, security en continuity, privacy, etc. Voorbeelden van vragen die hierbij genoemd worden door één leverancier zijn:
  - Moeten burger betalen of de overheid voor de middelen?
  - Is een burger bereid te betalen voor een middel dat uitsluitend voor de overheid werkt?
  - Is een business case ook haalbaar voor de kleinere partijen? Als deze niet haalbaar is dan zullen slechts enkele grote partijen het middel leveren en dat is niet bevorderlijk voor de adoptie.
  - Hoe bied je gebruikers vertrouwen? Gebruikers moeten veel bekend maken over wie ze zijn. Welke partij vertrouwen mensen?

- Welke behoeften hebben mensen als het gaat om identificatie; gemak van identificatie aan de deur, aan een balie? Er zijn gebruikers in verschillende segmenten. De verwachting is dat elk segment ook specifieke ideeën heeft bij de betrouwbaarheid.

Bevindingen deelvraag 6b: Hoe is de pilot voor de leveranciers verlopen?
Samenvattend
Leveranciers noemen de volgende positieve ervaringen:
- Gebruik in BSN domein en commerciële domein;
- Concurrentie en innovatie;
- Veilig inlogmiddel leeft bij klanten;
- Tevreden gebruikers;
- Eenvoud en gebruikersbeleving;
- Steun van de Belastingdienst.

Leveranciers noemen relatief veel negatieve ervaringen:
- Opzet pilots en operationalisering:
  - De bredere adoptie door dienstverleners (naast de Belastingdienst) valt tegen;
  - Het heeft lang geduurd eer andere leveranciers meededen;
  - De kracht van privaat en publiek gebruik komt in evaluatie niet naar voren;
  - Versnelling van de pilots/korte pilotperiode
  - Vergelijking van ‘appels met peren’ in de pilots;
  - Domein-overstijgend gebruik is complex.
- Stelsels en middelen:
  - Complexiteit voor dienstverleners van meerdere systemen naast elkaar;
  - Veel oplossingen voor identificatie;
- Communicatie:
  - Communicatie vanuit de overheid over Idensys richting externen te beperkt;
  - Matige communicatie over privacy;
- Financiering: onduidelijkheid over financieringsmodel;
- Context: onduidelijkheid rond de financiering van het stelsel tussen de ministeries van BZK, Financiën (FIN) en EZ.

Hieronder volgt de uitgebreide weergave van de antwoorden.

Leveranciers noemen de volgende positieve ervaringen:
- Gebruik in BSN domein en commerciële domein: leveranciers geven aan dat de kracht van het Idensys middel is dat het door gebruikers zowel voor het BSN domein als voor commerciële sites kan worden gebruikt.
- Concurrentie en innovatie: het wordt als kracht gezien van de Idensys middelen dat er concurrentie en innovatie door partijen plaatsvindt.
- Veilig inlogmiddel leeft bij klanten: leveranciers geven aan dat klanten het belang inzien van een veilig inlogmiddel, met goede privacy bescherming en goed toezicht. De samenwerking tussen overheid en bedrijfsleven wordt toegejuicht. Daarbij geeft één leverancier aan dat vanuit de overheid/publiek middel geen innovaties zullen worden gedaan; zij kunnen niet ieder jaar vernieuwen. Deze leverancier geeft aan dat een publiek middel dat tien jaar hetzelfde blijft een risico vormt, zeker gezien de snelle ontwikkelingen op het vlak van security.

- Tevreden gebruikers: leveranciers geven aan dat gebruikers zeer tevreden zijn over de processen gerelateerd aan de middelen.
- Eenvoud en gebruikersbeleving: leveranciers geven aan dat ze veel aandacht hebben besteed aan het bieden van een zo eenvoudig mogelijk proces voor de gebruikers. Er worden daarbij bewuste keuzes – met de gebruiker als uitgangspunt - gemaakt over de wijze waarop identificatie plaatsvindt.
- Steun van de Belastingdienst: de leverancier is blij met de ondervonden steun van de Belastingdienst. De Belastingdienst heeft zeer veel gebruikers achter zich. De Belastingdienst heeft zich sterk ingezet om de pilot tot een succes te maken en heeft ook deels de kosten voor de pilot (aanschaf middelen) betaald. Het is echter onzeker hoe het investeringsmodel/business model er na de pilots uit zal zien (zie ook: negatieve ervaringen).

Leveranciers noemen verschillende negatieve ervaringen; deze zijn geclusterd in de onderstaande categorieën:

<u>Opzet pilots en operationalisering</u>

- De bredere adoptie door dienstverleners (naast de Belastingdienst) valt tegen: in eerste instantie waren er weinig overheidsdiensten die mee zouden doen en veel private partijen. In een later stadium hebben toch veel overheidspartijen zich aangesloten. Het duurt echter lang voordat alles op gang komt; veel partijen kijken naar elkaar en hebben in eerste instantie een afwachtende houding. Daarnaast duurt het ook lang eer partijen daadwerkelijk kunnen meedoen. Het duurt weken eer partijen op het BSNk worden aangesloten. Het ministerie van BZK heeft richting de leverancier aangegeven dat deelname aan de pilot met gesloten beurs diende te gebeuren. Deze leverancier geeft aan hiertoe bereid te zijn geweest maar verwachtte dan wel dat de pilot breed zou worden gesteund door veel dienstaanbieders. Deelname door dienstverleners blijft echter achter omdat de (resterende) doorlooptijd van de pilot kort is en de aanlooptijd (implementatie) lang is en veel geld kost. Dienstverleners geven aan dat de overheid heeft gezegd dat de pilots ‘gratis’ zijn. Daar komt bij dat er investeringen moeten worden gemaakt maar er geen garantie is voor de toekomst; het is niet duidelijk welk middel uiteindelijk de voorkeur krijgt.
- Het heeft lang geduurd eer andere leveranciers meededen: één leverancier geeft aan dat het lang heeft geduurd eer andere leveranciers meededen. Deze leverancier denkt dat dit te wijten is aan technische complicaties en de commissie van de Toezichthouder die weinig frequent bij elkaar komt waardoor het toetredingsproces lang duurt (zie ook het volgende punt).
- Het toetredingsproces duurt erg lang: twee leveranciers geven aan dat het toetredingsproces erg lang duurt. Er is nu een nieuwe toezichthouder met formele processen. Eén leverancier heeft te maken gehad met 6 weken vertraging door de administratieve toetredingsprocedure in Idensys. Het was gedurende één maand onbekend bij wie de betreffende leverancier moest zijn om toe te treden. Vervolgens was er afhankelijkheid van een commissie die slechts beperkt bij elkaar kwam om besluiten te nemen.
- Twee leveranciers hebben in maart 2016 bij het Tactisch Beraad aangedrongen op een versnelling van het proces waarbij de commissie bijvoorbeeld via video-conferencing zaken kan bespreken (nu moet er gewacht worden tot de commissie fysiek bij elkaar komt). Dit is niet gelukt.

- De kracht van privaat en publiek gebruik komt in evaluatie niet naar voren: Eén leverancier geeft aan dat de combinatie van privaat en publiek gebruik/de samenwerking tussen overheid en privaat fundamenteel is maar in de evaluatie niet naar voren komt. In het zakelijk domein moeten zaken vaak goed geregeld zijn en dan is er daarvoor ook betalingsbereidheid. Deze leverancier geeft aan dat het belangrijk is om daarom vanuit meerdere toegangsgebieden financiering mogelijk te maken; door de combinatie van publiek en privaat gebruik en door verschillende 'persona's' (burger, consument, zakelijke gebruiker). Burgers hebben relatief weinig contact met de overheid. Als het middel alleen voor overheidsgebruik zou zijn dan is het volgens de leverancier de vraag in hoeverre voldoende financiering voor betrouwbaarheid op het hoogste betrouwbaarheidsniveau is op te brengen.
- Versnelling van de pilots/korte pilotperiode: bij het gebruik van de middelen gaat het voor gebruikers niet om het inlogmoment maar om de waarde van de dienst. In de pilot komen het inloggen en het dienstgebruik samen. Het is dan belangrijk dat gebruikers toegang hebben tot waardevolle diensten. Eén leverancier geeft aan dat de pilots waar zij bij betrokken is doorlopen tot september/oktober. Pilotpartijen willen gebruikers iets zinvols kunnen aanbieden. Nog niet iedere partij is in staat om gebruiker iets aan te bieden. In eerste instantie is er door deze leverancier voor gekozen om de aanvraag van een middel niet publiek beschikbaar te maken. De leverancier wilde gebruikers het 'wat en waarom' helder kunnen maken. Daarnaast geven de dienstverleners de leverancier een basale vergoeding voor het middel. Een algemene openstelling heeft de signaalwerking dat Idensys gratis is. Nu wordt er vanuit de Commissie/Tweede Kamer een versnelling gevraagd. De leverancier heeft er daarom nu toch gekozen voor openstelling waarbij geldt dat burgers dan minder begeleid kunnen worden. De tijdslijnen van de evaluatie dwingen deze leverancier nu om deze openstelling te doen. Een andere leverancier geeft aan dat in de zorg veiligheid en privacy zeer belangrijk zijn. Er is daarom een hoog betrouwbaarheidsniveau (niveau 4) benodigd. De zorgpartijen willen daarom ook graag deelnemen aan de pilots. Deze leverancier geeft aan dat de planning voor deelname door de zorgpartijen altijd april is geweest. Deze leverancier geeft aan het jammer te vinden dat er veel druk staat op pilotperiode. De leverancier verwacht ook in deze korte periode te kunnen laten zien dat niveau 4 goed werkt.
- Vergelijking van 'appels met peren' in de pilots: één leverancier geeft aan dat er in de pilots zaken worden vergeleken die niet met elkaar zijn te vergelijken:
  - De pilot publiek middel en Idensys zijn niet met elkaar te vergelijken. Een leverancier geeft aan dat het ministerie van Binnenlandse Zaken tijdens de pilot het publieke middel test en hiermee een relatief klein deel test: functioneert de eNIK-chipkaart in de BZK context, bij de Belastingdienst. Er is dus een context gecreëerd voor dit specifieke middel en dat wordt benoemd als pilot. Leveranciers gaan echter tijdens de pilotperiode zeer veel dienstverleners aansluiten. Dit is een totaal andere dimensie; in de Idensys pilot hebben partijen te maken met techniek, innovatie en toezicht die bij elkaar komen. De leveranciers geeft aan tijdens de pilot te kijken vanuit een multi-perspectief; onder meer rol van dienstverleners, veldproeven en de betalingsbereidheid van gebruikers.
  - De pilot iDIN en Idensys zijn niet met elkaar te vergelijken. Bij iDIN gaat het om een oplossing die snel is te realiseren. Het middel is al uitgereikt door de banken. Dit is geen uniform middel voor de reeks van toepassingen die

vereist zijn in een stelsel. Het iDIN stelsel is niet te vergelijken met het Idensys stelsel, de context van iDIN is niet te vergelijken met de context van Idensys, de iDIN infrastructuur is niet te vergelijken met de Idensys infrastructuur, etc. Een onderwerp als betalingsbereidheid speelt bijvoorbeeld niet bij de iDIN pilot waar mensen al over het middel beschikken.

- Domein-overstijgend gebruik is complex: In de pilots wordt er alleen naar het burger domein gekeken terwijl mensen vaak domein overstijgend werken (gebruik in zowel het BSN domein als het commerciële domein). Afhankelijk van de rol van iemand (burger of klant) moet een passende dienstencatalogus worden aangeboden. Een leerpunt is dat hiervoor vereenvoudiging moet worden aangebracht in het stelsel.

<u>Stelsels en middelen</u>

- Complexiteit voor dienstverleners van meerdere systemen naast elkaar: Het feit dat er zoveel middelen uit verschillende stelsels zijn maakt het complex voor gebruikers/betrokkenen. Leveranciers geven aan dat keuze goed is maar dat gebruikers en dienstverleners de verschillen niet weten (bijvoorbeeld tussen iDIN, Idensys en eHerkenning) Het is niet mogelijk om mensen met een paar eenvoudige woorden mee te nemen door het speelveld (zie ook ‘Communicatie’).
- Veel oplossingen voor identificatie: De diverse leveranciers doen identificatie elk op hun eigen manier. Dit geeft verwarring maar kan tegelijkertijd ook inzichten bieden over wat het beste proces is. Het is daarom zowel een negatieve als een positieve ervaring van de pilot.

<u>Communicatie</u>

- Communicatie vanuit de overheid over Idensys richting externen te beperkt: de leveranciers benoemen dit als leerpunt voor de overheid. Gevolg van deze beperkte communicatie vanuit de overheid is dat er veel onzekerheid bestaat bij partijen en eindgebruikers en deze een afwachtende houding aannemen. De volgende ervaringen worden benoemd:
  - Complex onderwerp: een aantal leveranciers geeft aan dat Idensys een moeilijk onderwerp is dat daarom uitleg behoeft. Zo is er grote onduidelijkheid voor de gebruikers wat de functionaliteit is van elk middel, welke middelen gratis zijn, voor welke men moet betalen en op welke aspecten de middelen concurreren. Leveranciers hebben – vanwege het ontbreken van communicatie door de overheid – nu zelf de communicatie richting hun klanten (dienstverleners en eindgebruikers van het middel) verzorgd.
  - Verschillende domeinen: Het ministerie van BZK heeft te maken met communicatie in het BSN domein. De pilotpartijen van Idensys hebben te maken met mensen die de ene keer in het BSN domein acteren en de volgende keer in het commerciële domein. Dit maakt dat leveranciers hier veel uitleg over moet geven aan dienstverleners.
  - Onduidelijkheid over toekomst: eHerkenning is zwaar gepromoot. De partijen die eHerkenning wilden gebruiken hebben door onduidelijkheid over een eventueel samengaan van eHerkenning en Idensys een afwachtende houding. Er zou daarom snel duidelijkheid moeten worden geboden of het twee aparte oplossingen blijven of dat ze samengevoegd worden.

- Terughoudendheid in communicatie over DigiD: één leverancier heeft de perceptie dat de overheid nu erg huiverig is om te melden dat DigiD gaat verdwijnen. Deze leverancier benoemt dit nu wel expliciet in hun communicatie richting klanten. Zij geven aan dat DigiD is niet veilig is en niet voldoet aan (Europese) regelgeving en dat er daarom nu nieuwe middelen komen; een publiek middel en een middel vanuit publiek-private samenwerking.

- Matige communicatie over privacy: de thema's privacy en anonimiteit zijn zeer belangrijk voor consumenten. Tegelijkertijd is ook het thema 'big brother is watching you' belangrijk. Door de matige communicatie kunnen er onterechte beelden bij mensen ontstaan, zeker omdat tegenstanders van stelsels als Idensys wel veel communiceren. Sommige auteurs hebben volgens de leveranciers achterliggende belangen om negatieve berichten over Idensys te verkondigen. Er wordt volgens de leveranciers in de media veel gesuggereerd wat niet klopt. Zo denken sommigen dat leveranciers de data over wat gebruikers doen zullen verkopen. Ook wordt er weinig aandacht besteed aan Idensys 2.0 (na de pilots in Q42016). Zodra deze er is, zijn allerlei discussies minder relevant (Idensys 2.0 biedt onder meer polymorfe encryptie). Eén leverancier geeft aan dat Logius de aangewezen partij is om over privacy in algemene zin te communiceren. Eén leverancier benoemt dat het een sterk punt is dat bij Idensys deze discussies in de openbaarheid worden gevoerd. Dit is cruciaal voor het vertrouwen in het stelsel. Bij andere stelsels en initiatieven wordt de PIA niet publiek gemaakt.

<u>Financiering</u>

- Onduidelijkheid over financieringsmodel: de leveranciers geven aan dat de overheid (nog steeds) geen helderheid geeft over wie gaat betalen. Leveranciers geven aan dat deze onduidelijkheid bij dienstverleners en gebruikers leidt tot terughoudendheid aangezien ze niet weten waar ze instappen. Ze hebben behoefte aan meer zekerheid.

<u>Context</u>

- Eén leverancier geeft aan blij te zijn met de steun van het ministerie van EZ. Deze leverancier ervaart echter wel onduidelijkheid tussen de ministeries van BZK, FIN en EZ die volgends de leverancier ieder controle en invloed uit willen oefenen, waarbij het soms onduidelijk is wie wat doet.

Bevindingen deelvraag 6c:

Alle leveranciers zien een hoge toegevoegde waarde. Zij noemen de volgende elementen:

- Grote toegevoegde waarde voor de digitale transitie vraagstukken. Er komen steeds meer transacties waarbij het onvoldoende is dat een gebruiker inlogt met gebruikersnaam en wachtwoord (zoals bij de vooraf ingevulde belastingaangifte). De mate van zekerheid over de identiteit van de gebruiker is niet hoog genoeg voor sommige diensten. Eén leverancier geeft aan de ontwikkeling van het stelsel Idensys te gebruiken als springplank voor innovaties. Er wordt zorgvuldig in geïnvesteerd in de digitalisering van zijn klanten. In de zorg is men al jaren op zoek naar een goede manier om burgers/consumenten/patiënten toegang te geven tot het patiëntendossier. Het is volgens deze leverancier nog niet goed geregeld dat burgers geen toegang

hebben tot hun eigen dossier. Ook interacteren, zelf afspraken maken, werkt nog onvoldoende. Idensys is de mogelijk vereenvoudiging en de sleutel.
- Het middel biedt veel voordeel voor mensen die soms als burger, soms als consument en soms zakelijke gebruiker willen inloggen bij de overheid en dienstverleners. Het middel is zowel te gebruiken binnen het BSN domein als voor commerciële sites (B2B en B2C).
- Door de publiek private samenwerking vindt er innovatie plaats.
- De privacy en bijbehorende transparantie zijn een kracht.
- Het middel moet ook voldoen aan Europese regelgeving. eIDAS is in 2014 aangenomen. In 2018 moet het werken. Idensys is zich hier al volledig voor aan het klaarmaken (o.a. polymorfe pseudo ID's). Dit maakt Idensys het middel voor de toekomst.

Hoofdvraag 7: Hoe is het aanvraag- en uitgifteproces verlopen?
De volgende bronnen zijn gebruikt bij de beantwoording van deze vraag:
- Interview met CreAim;
- Interview met Digidentity;
- Interview met KPN;
- Excel 'Idensys Maart-April' (Digidentity, 6 mei 2016);
- Email van Digidentity, 11 mei 2016;
- Email van CreAim, 11 mei 2016;
- Email van KPN, 13 mei 2016.

De onderstaande tabel toont het aantal uitgegeven middelen per leverancier. Let op: de meetperiodes verschillen.

Aantal middelen per leverancier

Leverancier	**Middel (LOA: 3)**	**Middel (LOA: 4)**	**Totaal**
CreAim (periode: 25 april* t/m 11 mei 2016) * Maandag 25 april heeft CreAim de eerste Idensys-middelen uitgegeven. Op 30 april is de eerste Dienstverlener (World of Health) aangesloten.	74	13	87
Digidentity (periode: maart – april)	122	-	122
KPN (25 april – t/m 11 mei 2016)	184	15	199

De onderstaande tabel toont het aantal logins per leverancier in het BSN domein. Let op: De meetperiodes verschillen.

Aantal logins per leverancier in het BSN domein

Leverancier: CreAim	**Dienstaanbieder**	**LOA: 3**	**LOA: 4**	**Totaal**
CreAim (periode: 25 april* t/m 11 mei 2016) * Maandag 25 april heeft CreAim de eerste Idensys-middelen uitgegeven. Op 30 april is de	World of Health (Mijnzorgtoegang)	181	34	229
	Pharmeon	11	3	

Leverancier: CreAim	**Dienstaanbieder**	**LOA: 3**	**LOA: 4**	**Totaal**
eerste Dienstverlener (World of Health) aangesloten.				
Digidentity (periode: maart – april)	*Niet gespecificeerd*	485	-	485
KPN (periode: 25 april - 11 mei 2016)				*Geen gegevens beschikbaar*

De leveranciers geven aan dat het aanvraagproces voorspoedig, soepel en snel verloopt. Ook geven zij aan positieve signalen vanuit hun klanten te ontvangen over het proces.

Onderstaande tabel geeft een overzicht van de onderwerpen waarover gebruikers vragen stellen.

Onderwerpen waar gebruikers vragen over stellen per leverancier (van meest naar minst voorkomend)

Leverancier	**Onderwerp**
CreAim (periode: 25 april t/m 11 mei 2016)	Wachtwoord vergeten
	Wat kost Idensys na de pilot
	Wat is het verschil tussen Idensys niveau 3 en niveau 4
	Hoe werkt de fysieke identificatie
Digidentity (periode: maart - april)	Kan geen foto maken van ID document - probleem met scannen/reject *Toelichting: Digidentity heeft in maart een issue met de app gehad.*
	Hoe kan ik mijn Digikey personaliseren?
	Waarom kan ik niet verder met registratie? (afgekeurd/profile match/BSN)
	QR code is niet geaccepteerd via app
	Geen push notification Digikey bij inloggen
	Waarom werkt mijn Digikey pincode niet
	Succesvol afgerond, profiel geef melding "pending"
	Welke andere documenten/informatie nodig?
	Waar kan ik inloggen?
	Hoe kan ik mijn account reactiveren?
	Waarom kan ik niet inloggen?
	Hoe kan ik mijn inlog gegevens herstellen?
	User accessed Idensys instead of GOV UK
	Hoe kan ik mijn account verwijderen?
	iDEAL betaling mislukt door tweede naam niet zichtbaar profile match
	Hoe wij via uw makelaar hierop kunnen aansluiten?
	Account geblokkeerd door verkeerd inloggen
	Hoe kan ik mijn email bevestigen?

Leverancier	Onderwerp
	Mijn document blijft "pending"
KPN (25 april – t/m 11 mei 2016)	Wachtwoord vergeten/verloren
	Wat is het verschil tussen Idensys niveau 3 en 4?
	Hoe werkt het identificatieproces?
	Hoe kan ik mijn ID bewijs uploaden?

Eén leverancier licht toe dat hij tijdens de pilot zelf het gebruikers support verzorgt omdat dit het meeste inzicht geeft in waar gebruikers tegenaan lopen. Op basis van de binnengekomen input wordt bepaald hoe het product verbeterd kan worden. Deze leverancier vindt het belangrijk om het eindgebruikers support zelf te blijven doen omdat dit veel inzicht geeft in mogelijke verbeterpunten van het product.

Hoofdvraag 8: Zien authenticatiediensten/middelenleveranciers toekomst in het middel dat zij nu uitgeven?

De volgende bronnen zijn gebruikt bij de beantwoording van deze vraag:

- Interview met CreAim;
- Interview met Digidentity;
- Interview met KPN.

Eén leverancier geeft aan dit niet de juiste vraag te vinden. Deze leverancier vindt dat de middelenkeuze een keuze is van haar klanten. In de gezondheidszorg zijn tientallen actoren (bijvoorbeeld artsen en administratief medewerkers, patiënten), elk met eigen behoeften en manieren van werken. Deze leverancier heeft al 5 à 6 ‘middelen’ beschikbaar . Nu moet de volgende stap vanuit gebruikersperspectief worden gezet. Er is geen ‘one size fits all-middel’. Deze leverancier merkt op dat er in de discussie nu veel gesproken wordt over wat het beste middel is uit het pallet. Deze leverancier heeft hierop een andere visie: er zijn verschillende middelen nodig voor verschillende situaties, tenzij er een moment komt waarop alle innovaties samenkomen.

Eén leverancier geeft aan zeker toekomst te zien in het middel dat zij uitgeeft. Daarbij geeft zij aan dat zij geen enkele toekomst ziet in het publieke middel; vanuit de overheid is er geen mogelijkheid om te innoveren. Ook in het bankenmiddel ziet zij geen toekomst; banken worden niet vertrouwd op het vlak van privacy.

Eén leverancier hoopt dat er snel stappen worden na gezet na de pilot. De vrees is echter dat er een soort impasse zal ontstaan in verband met het business model; wie gaat er betalen. De leverancier verwacht dat het verkrijgen van helderheid hierover lang gaat duren. Hij geeft aan dat de ministeries (met nadruk op meervoud ‘ministeries’) een duidelijke lijn moeten kiezen; qua merken, stelsels, etc. De leverancier geeft aan dat Nederland op Europees niveau steeds meer in de problemen komt aangezien DigiD niet voldoet. In 2010 liep Nederland voorop maar nu wordt Nederland aan alle kanten vooruitgestreefd. Een voorbeeld daarvan is het feit dat Nederland nu een kaart gaat uitdelen terwijl in andere landen duidelijk is geworden dat dit niet of nauwelijks werkt.

Aansluiting met het buitenland is volgens deze leverancier essentieel aangezien het middel daar eveneens gebruikt moet kunnen worden. Partijen als de Belastingdienst, SVB, etc. zullen volgens de leverancier ook een belangrijke rol

spelen in het snel zetten van stappen na de pilot. Deze leverancier benoemt nog een aantal vraagstukken:

- Het idee achter Idensys is dat er een spreiding van leveranciers en dus middelen is. Wanneer iedereen één middel krijgt dan is van die spreiding geen sprake.
- eIDAS schrijft voor dat de publieke dienstaanbieders internationale middelen moeten accepteren. Zo ontstaat een soort marktwerking op Europees niveau.
- Transparantie over het gebruik van de data richting de gebruikers: er moet worden gecommuniceerd waarom een aanbieder de data wil hebben, wat er met de data wordt gedaan, waarom en waar de data voor wordt gebruikt en hoe lang deze wordt het bewaard. Deze zaken zijn gedurende de looptijd van de pilots op te lossen maar dienen ook op orde te zijn als het middel daadwerkelijk wordt ingevoerd. Hierbij dient er uiteraard aan wettelijke voorschriften (zoals de Wet persoonsregistratie) te worden voldaan.
- Multimiddelenstrategie: het is geen overzichtelijke oplossing voor gebruikers als ze overal met alle middelen in kunnen loggen met verschillende niveaus. Middelen kan hier worden gelezen als ‘stelsels’. Middelen binnen een stelsel kunnen allemaal verschillend zijn maar dat is geen probleem. Het probleem zit in het feit dat een gebruiker geen idee heeft wat het verschil is tussen stelsels. Gebruiksgemak, veiligheid en de prijs zijn het belangrijkst voor de gebruiker is gebleken uit onderzoek door deze leverancier.
- De ‘general data protection regulation’ (de nieuwe Europese wetgeving m.b.t. data beveiliging) zal van grote invloed zijn op hoe om te gaan met verschillende stelsels en middelen.

4.1.3.2 Onderzoeksvragen met betrekking tot ervaringen van dienstaanbieders

Hoofdvraag 9: Hoe ervaren de dienstaanbieders de deelname aan de pilot?

De volgende deelvragen zijn onder deze hoofdvraag geformuleerd:
Deelvraag 9a: Wat zijn de redenen voor dienstaanbieders om deel te nemen aan de pilot?
Deelvraag 9b: Hoe is de pilot voor de dienstaanbieders verlopen?
Deelvraag 9c: In welke mate zien dienstaanbieders het hoogwaardige middel als toegevoegde waarde?
Deelvraag 9d: Is de communicatie verlopen volgens het communicatieplan pilots?

Bevindingen deelvraag 9a:
De Belastingdienst noemt de volgende redenen om deel te nemen aan de pilot:

1. De digitale dienstverlening van de Belastingdienst is nu afhankelijk van DigiD. Er is behoefte aan nog een middel zodat er altijd een ‘fallback’ beschikbaar is mocht DigiD niet werken (de multimiddelenstrategie). Het voordeel van het bankenmiddel is dat dit al breed is uitgerold en daarom al op korte termijn als fallback kan dienen. De verwachting bij de Belastingdienst is dat het breed beschikbaar komen van het publiek middel lang zal duren. Vanuit het Idensys middel wordt innovatie verwacht.
2. De betrouwbaarheid van DigiD is te laag. Het College Bescherming Persoonsgegevens heeft aangegeven dat het betrouwbaarheidsniveau 2 (code 20) te laag is. Voor het type diensten dat de Belastingdienst aanbiedt, is het noodzakelijk dat er sprake is van betrouwbaarheidsniveau 3 (code 30). Ook

vindt er fraude plaats waarbij enveloppen met DigiD-codes uit brievenbussen worden gehengeld.

Bevindingen deelvraag 9b:
De Belastingdienst is tevreden over het verloop van de pilot. De Belastingdienst noemt de volgende positieve ervaringen:

- De doelstellingen zijn gehaald: er is een proces geïmplementeerd dat goed heeft gewerkt. Er zijn voldoende gebruikerservaringen opgehaald om lessen uit te kunnen leren. Deze lessen moeten nog nader worden bepaald. Een aantal eerste lessen betreffen het verbeteren van de customer journey (door vermindering van het aantal schermen) en het verbeteren van de communicatie (helder aan klanten uitleggen wat het verschil is tussen de middelen).
- De verschillende partijen in de keten hebben elkaar gevonden in de samenwerking en gezamenlijk een mooie keten gerealiseerd. Iedere partij verzorgt een klein stuk software van de keten. Zo is een 'lean & mean' oplossing gerealiseerd die weinig kosten met zich mee brengt.
- Tijdens de pilot hebben er geen incidenten plaatsgevonden. De Belastingdienst geeft aan dat alles technisch goed heeft gewerkt.
- De samenwerking met de partners in de keten is goed verlopen.
- De bereidwilligheid van deelnemers om mee te doen is lager dan gehoopt. De aantallen die ooit in de media zijn genoemd zijn niet bereikt (iDIN; max. 65.000 deelnemers, Idensys: max. 30.000 deelnemers)[36]. Dit lagere aantal deelnemers lag echter wel binnen de verwachting. Het doen van aangifte is voor burgers erg belangrijk. Zij willen dit doen zonder extra gedoe. Het feit dat de gebruikersaantallen lager zijn, heeft geen negatieve consequenties voor de Belastingdienst; het doel is bereikt (zie bovengenoemde ervaring).

De Belastingdienst noemt het volgende aandachtspunt:

- Het Idensys proces was nieuw voor gebruikers waardoor gebruikers bekend moesten raken met het gebruiken van het nieuwe middel.

Bevindingen deelvraag 9c:
De Belastingdienst ziet zeker toegevoegde waarde. Voor de Belastingdienst draait het om de multimiddelenstrategie; het hebben van meer dan één middel met het beveiliging-/betrouwbaarheidsniveau dat past bij de diensten. Belangrijk daarbij is de gebruiksvriendelijkheid voor gebruikers. De verwachting van de Belastingdienst is dat er straks concurrentie zal ontstaan die partijen ertoe aanzet om een zo goed mogelijk middel in markt te zetten. Voor de Belastingdienst is het hoogwaardig middel een voorwaarde om door te kunnen gaan met het aanbieden en het ontwikkelen van diensten die steeds meer online zullen worden aangeboden.

Bevindingen deelvraag 9d:
De communicatie is uitgevoerd zoals gepland. Er is geen communicatieplan op schrift. Wel is er met de Idensys partijen doorgesproken hoe de communicatie zou verlopen. Er is onder meer het volgende afgesproken:

- Interne communicatie via het intranet van de Belastingdienst om op kleine schaal medewerkers op te roepen om deel te nemen aan de pilot. Vervolgens

[36] Zie bijvoorbeeld: https://belastingdienst-in-beeld.nl/extra-mogelijkheid-om-in-te-loggen-op-mijnbelastingdienst-nl/

wordt er gefaseerd een bredere groep mensen opgeroepen om deel te nemen aan de pilot.
- Teksten worden door de partijen met elkaar afgestemd.
- Er wordt gebruik gemaakt van neutrale berichtgeving.
- De media wordt niet opgezocht. (Ook niet om hogere aantallen deelnemers te werven).
- Er worden geen persberichten verstuurd.
- Er vindt geen positionering plaats van het eigen merk van partijen.

De Belastingdienst geeft aan dat alle partijen zich aan de afspraken m.b.t. communicatie hebben gehouden.

Hoofdvraag 10: Hoe is het proces van aansluiting verlopen?
De volgende bron is gebruikt voor beantwoording van de vragen:
- Interviews met de Belastingdienst.

Het proces van aansluiting was een complex proces waarbij veel partijen zijn betrokken. Voor de betrokken partijen was het ook een leerproces om gezamenlijk uit te denken hoe zaken het beste kunnen worden ingericht. De Belastingdienst heeft het aansluitproces strak gestuurd. Het was zeer belangrijk om alles voor 1 maart 2016 (start van de aangifteperiode) te realiseren. Dit is ook gelukt.

Hoofdvraag 11: In welke mate wordt er van de diensten gebruik gemaakt door deelnemers aan de proef en hoe verloopt dit gebruik voor de dienstaanbieders?

Deze hoofdvraag bestaat uit de volgende deelvragen:
Deelvraag 11a: Hoeveel deelnemers maken gebruik van de diensten en hoe frequent is het gebruik van de diensten via het hoogwaardige middel?
Deelvraag 11b: Hebben zich nog problemen voorgedaan tijdens de pilot en hoe zijn deze opgelost?

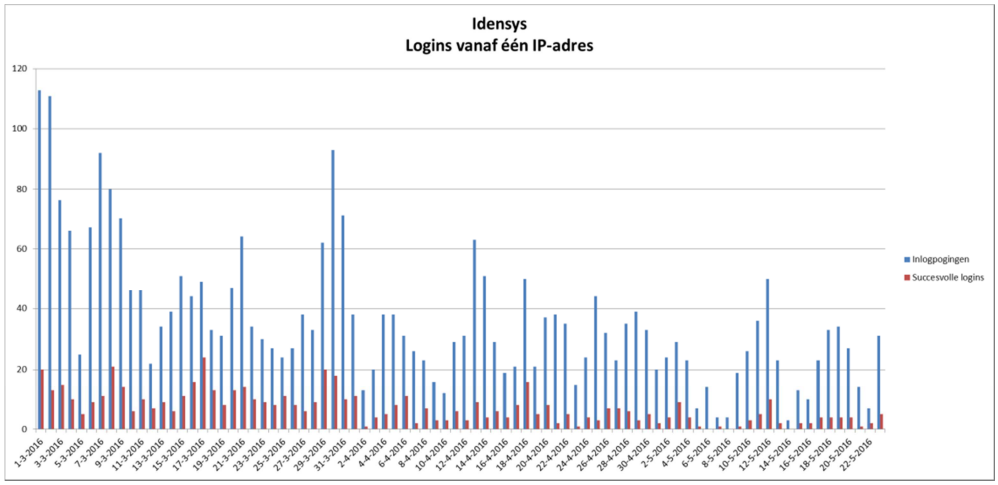
Bevindingen deelvraag 11a:
De volgende bronnen zijn gebruikt voor beantwoording van de vragen:
- Interviews met de Belastingdienst
- Email over gebruiksgegevens (Ambtelijk projectleider, 18 mei 2016)
- Logdata opgeleverd door de Belastingdienst op 24 mei, 2016

Overzicht gebruiksgegevens

Gegevens	**Idensys**
Inlogpogingen (totaal aantal keer dat op de knop voor inloggen is gedrukt) *Periode: 1 maart – 22 mei, bron: Belastingdienst*	4397
Succesvolle logins (Totaal aantal keer dat daadwerkelijk succesvol is ingelogd) *Periode: 1 maart – 22 mei, bron: Belastingdienst*	844
Inlogpogingen vanaf één IP-adres (Totaal aantal keer dat op de knop voor inloggen is gedrukt vanaf één IP-adres) *Periode: 1 maart – 22 mei, bron: Belastingdienst*	3043
Succesvolle logins vanaf één IP-adres (Totaal aantal keer dat daadwerkelijk succesvol is ingelogd vanaf één IP-adres)	601

Periode: 1 maart – 22 mei, bron: Belastingdienst	
Aantal geactiveerde inlogmiddelen *Periode: 1 maart – 13 mei, bron: Belastingdienst/BSNk*	484

TNO heeft geen verklaring voor het aantal niet-succesvolle inlogpogingen. Gezien de datum waarop de data is aangeleverd is TNO niet in staat geweest hier verder onderzoek naar te verrichten.



Figuur 57 Idensys - logins vanaf één IP-adres

Figuur 57 geeft een overzicht van het aantal keer per dag dat vanaf één IP-adres een inlogpoging is gedaan. Pogingen van meerdere personen vanaf één IP-adres (locatie) tellen als één mee. Figuur 56 (paragraaf 4.1.1) bevat een overzicht van het aantal keer per dag dat een inlogpoging is gedaan. Pogingen van meerdere personen vanaf één IP-adres (locatie) tellen allemaal mee.

Bevindingen deelvraag 11b:
De volgende bronnen zijn gebruikt voor beantwoording van de vragen:

- Memo Inrichting pilot Idensys bij de Belastingdienst; [10]
- Interviews met de Belastingdienst;
- Email over gebruiksgegevens (Ambtelijk projectleider, 18 mei 2016).

De gebruikersondersteuning voor de pilot Idensys is als volgt ingericht:
In de publieksfase wordt de gebruikersondersteuning via de reguliere beheerprocessen uitgevoerd. Klantsignalen kunnen binnenkomen bij de dienstverleningskanalen zoals BelastingTelefoon en webcare, maar er kunnen ook signalen (van meer technische aard) via de herkenningsmakelaar binnenkomen. Alle meldingen worden op een centraal punt geregistreerd waarna diagnose plaatsvindt. Afhankelijk van deze diagnose (functioneel, applicatief, netwerk, extern of communicatief) wordt het issue voor verdere afhandeling binnen de Belastingdienst uitgezet of wordt de melding doorgezet naar de herkenningsmakelaar. Er wordt een (virtuele) control room ingericht voor besluitvorming bij incidenten met een hoge prioriteit. Voor de BelastingTelefoon, webcare en op de website wordt een Q&A beschikbaar gesteld om klantvragen te beantwoorden.

Het registratieproces van het Idensys-middel verloopt via de middelenleverancier. Gebruikersondersteuning voor dit proces verloopt via de middelenleverancier.

Er is geen inzicht verschaft in het aantal en de inhoud van de binnengekomen vragen bij de Belastingtelefoon.

Vanuit medewerkers binnen de Belastingdienst zijn enkele vragen binnengekomen over het registratieproces van Digidentity. Ook hebben twee medewerkers vragen gesteld n.a.v. zorgen of borging van de privacy bij gebruik van het KPN middel.

4.2 Beantwoording van de onderzoeksvragen voor de pilot iDIN

4.2.1 Geconstateerde afwijking van verondersteld Stelsel

In de offerteaanvraag vanuit opdrachtgever zijn voor de pilot Idensys en de pilot iDIN dezelfde vragen gesteld. [5] Het uitgangspunt daarbij was het stelsel Idensys, voortbouwend op het Afsprakenstelsel van eHerkenning (zie paragraaf 1.8 offerteaanvraag). Ook specifiek met betrekking tot de PIA werden de pilots gelijkelijk behandeld, zoals blijkt uit paragraaf 1.8.1.1 van de offerteaanvraag, waarin gesteld wordt dat een PIA heeft plaatsgevonden ter voorbereiding op de pilots. In deze PIA werd nog gesproken van eID. In de Nota van Inlichtingen werd dit bevestigd bij vraag 10. [18]

Gedurende het onderzoek is echter gebleken dat voor iDIN niet gewerkt wordt met het Afsprakenstelsel zoals dat voor Idensys wordt gehanteerd. iDIN werkt met een eigen stelsel. Dat heeft onder meer tot gevolg dat er verschillende inrichtingen zijn van de LoA's, privacy-beleid, toezicht, technische inrichting en schakelen met het BSNk, en de processen voor toetreding. De vragen die vanuit opdrachtgever zijn opgesteld zijn ingegeven tegen de achtergrond van het Idensys Afsprakenstelsel. In dit hoofdstuk worden de vragen beantwoord binnen de context van iDIN. Er is dus gekeken naar het doel van de vragen en deze zijn beantwoord aan de hand van het iDIN Framework en de bijbehorende documentatie. De volgende documenten dienden als uitgangspunt: [21], [22], [23], [24] en [25]

4.2.2 Onderzoeksvragen met betrekking tot techniek

Hoofdvraag 1: Is er voldaan aan de betrouwbaarheid zoals geformuleerd in het afsprakenstelsel?

Deze hoofdvraag bestaat uit de volgende deelvragen:
Deelvraag 1a: Zijn er incidenten die wijzen op een feitelijke lage betrouwbaarheid?
Deelvraag 1b: Hoe zijn deze incidenten afgehandeld? (De afhandeling betreft het informeren van de toezichthouder en of er bij de afhandeling is voldaan aan de eisen omtrent afhandeling van incidenten in het afsprakenstelsel.)

Bevindingen hoofdvraag 1.
De eisen aan iDIN zijn geformuleerd in het control framework BankID [22], dat tot een half jaar geleden de werknaam was van iDIN. De Acquirers (partijen die iDIN aan zakelijke partijen mogen aanbieden, voor de pilot ING, ABN AMRO en Rabobank) hebben middels een door de BVN gevalideerd assessment aangegeven hoe zij hieraan voldoen. Hierin zijn door de Betaalvereniging geen onvolkomenheden geconstateerd die deelname binnen iDIN in de pilot zouden blokkeren. Voor de Issuers (partijen binnen iDIN die het product aan

consumentklanten mogen aanbieden, voor de pilot: ABN AMRO, ASN Bank, Rabobank, ING, SNS Bank, RegioBank en Triodos Bank) is een zelfde procedure doorlopen, tegen het voor Issuers relevante deel van het control framework, met hetzelfde resultaat.

Vanuit het BVN perspectief vormt de aansluiting op het BSNk om private identifiers te koppelen aan BSN identifiers de enige relatie naar Logius. Deze aansluiting is gebaseerd op een aparte juridische bewerkingsovereenkomst per issuing bank en niet op toetreding tot het Idensys afsprakenstelsel. Deze route werd als enige mogelijkheid geaccepteerd door de overheid voor het toepassen van iDIN binnen het BSN domein. Het zelf direct leveren van het BSN door de banken is technisch wel mogelijk, maar word niet geaccepteerd[37], omdat op basis van de Wet elektronisch berichtenverkeer (WEB) en bijbehorende AMvB alleen levering aan het BSNk is toegestaan. ([11] p. 10) Wel geldt dat de acceptanten in het BSN-domein die het BSN willen ontvangen zelf ook een relatie met Logius hebben, om het bij het BIN (pseudoID) behorende BSN op te halen. Dit vindt plaats buiten het iDIN-scheme, op verantwoordelijkheid van de acceptant, de banken mogen het BSN immers niet leveren.

Uit slide 15 van de presentatie blijkt dat voor de betrouwbaarheid van iemands elektronische identiteit, in dit geval voor iDIN, wel dezelfde begrippen worden gehanteerd, namelijk ‘Level of Assurance’ (LoA). Dit blijkt uit het volgende citaat: ‘Login met een vastgesteld minimaal Level of Assurance’ (slide 15). Dit komt overeen met de definitie van ‘Betrouwbaarheidsniveau’ in de Begrippenlijst in het Idensys afsprakenstelsel (zie pagina 27).Binnen iDIN worden de LoA’s conform STORK toegepast. Gedurende het activeren van het iDIN middel wordt echter niet getoond aan de gebruiker welk LoA wordt geboden. In de praktijk is dit op basis van de eisen een LoA 3.

In het iDIN Framework wordt de betrouwbaarheid primair afgeleid van de vereisten uit de Wet ter voorkoming van witwassen en financieren van terrorisme (Wwft). Op grond van de Wwft zijn er vier mogelijkheden voor identificatie van een gebruiker: in-person identification, introduction, outsourced identification en derived identification.[38] Voor de pilotfase vallen alleen in-person identification en derived identification binnen scope (pagina 9 en 10 Bank ID Framework). Naar aanleiding van de Wwft wordt bij het klant worden identificatie in persoon uitgevoerd. De gebruiker moet dus fysiek langskomen bij de bank en een wettelijk identificatiedocument overleggen. De identificatie wordt geregistreerd. iDIN maakt gebruik van bestaande middelen, waardoor het nu geen vereiste is om nogmaals fysiek langs te komen bij de bank. Een eerdere face-to-face identificatie wordt beschouwd als geldend voor het activeren van het iDIN middel.

Uiteindelijk vindt de identificatie dus in persoon plaats, of op basis van een eerdere fysieke identificatie en een match op de overlegde gegevens en een WID. Middels een transactie met behulp van een scanner, identifier of TAN code (afhankelijk van de bank) vindt twee factor authenticatie plaats.

---

[37] BVN merkt hierbij op dat zij dit een tekortkoming vinden, omdat het BSN zo vaker over de lijn gaat dan noodzakelijk.
[38] Bank ID Framework v 1.2, p. 8.

iDIN maakt gebruik van de LoAs zoals afkomstig uit STORK. De volgende aspecten zijn van toepassing voor de verschillende levels:

The following differences apply for the respective levels of assurance:
- LoA2: Provides single-factor remote network authentication. A wide range of available authentication technologies can be employed at level 2.
- LoA3: Provides multi-factor remote network authentication. At least two authentication factors are required. Level 3 authentication is based on proof of possession of the allowed types of tokens through a cryptographic protocol.
- LoA4: Level 4 is intended to provide the highest practical remote network authentication assurance. Level 4 authentication is logically based on proof of possession of a key through a cryptographic protocol. Additionally, the identification token requires the user to confirm the authentication request through a different "trusted" channel ("wilsuiting").

Figuur 58 De door iDIN gehanteerde betrouwbaarheidsniveaus (bron: [22])

Let op: LoA4 is geen onderdeel van iDIN.

Bevindingen deelvraag 1a:
Er zijn in de periode maart-april geen incidenten geweest die wijzen op een feitelijk lagere betrouwbaarheid. Dit is op 29 april 2016 per mail door BVN aangegeven.

Bevindingen deelvraag 1a:
N.v.t.

Hoofdvraag 2: In welke mate is er voldaan aan de gestelde eisen omtrent beschikbaarheid?

Bevindingen hoofdvraag 2:
iDIN hanteert de volgende beschikbaarheidseisen:

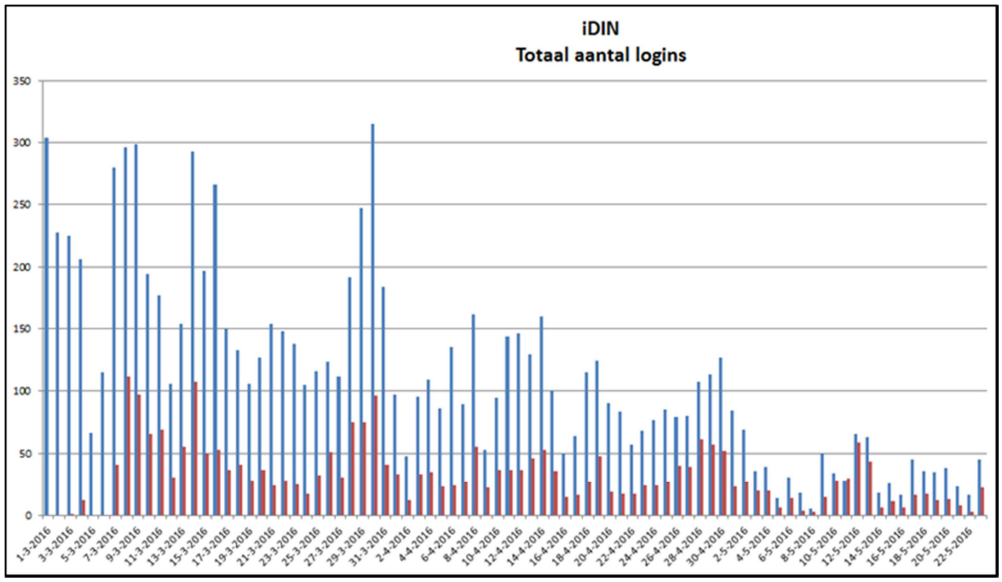
General norms		Level	Risks addressed
12.1	Primetime (7am till 1am): availability of 99.5%	All	Not having the possibility to block a BankID. BankID is temporarily unavailable. Unable to guarantee financial/operational continuity of long term availability of services.
12.2	Non-Primetime (1am till 7am): availability of 93.5%		
12.3	The issuer is able to show/prove that BankID performance demands are met as mentioned in the Implementations Guidelines.		
12.4	A 24/7 (security) monitoring is implemented for the BankID servic provided.		

Figuur 59 Beschikbaarheidseisen iDIN (bron: [22])

Uit de aangeleverde pilotrapportage kan niet worden afgeleid of de beschikbaarheid voor deze norm wordt gemeten, hoe deze wordt gemeten en welk niveau daadwerkelijk is gehaald.

Op 29 april heeft BVN het volgende aangegeven: ‘Eén van de 7 banken heeft in deze periode te maken gehad met tijdelijke onbeschikbaarheid van iDIN als gevolg van een algehele storing van internetbankieren, maar dat leidde niet tot een onbeschikbaarheid onder de norm. Alle andere 6 banken zijn continu beschikbaar geweest vanaf het moment dat de dienst geboden kon worden.’ De beschikbaarheid voor iDIN als geheel komt daarmee voor april op 99,9% Primetime en 99,4% Non-Primetime.

Uit de van de Belastingdienst ontvangen pilotrapportage [Bron: mail Belastingdienst dd. 24/05/2016] over de maanden maart en april 2016 (Figuur 60) blijkt echter wel dat met de iDIN-middelen elke dag eindgebruikers hebben ingelogd. Hierop baseert TNO het antwoord dat de hiervoor benodigde infrastructuur in de meetperiode elke dag beschikbaar is geweest. Merk op dat de pilot iDIN met de Belastingdienst Aangifte Inkomstenbelasting op 8 maart 2016 is gestart [Bron: BVN[39]].



Figuur 60 Pilotrapportage Belastingdienst m.b.t. iDIN (Bron: Belastingdienst)

Hoofdvraag 3: In welke mate is voldaan aan de informatieveiligheidseisen?

Deze hoofdvraag bestaat uit de volgende deelvragen:
Deelvraag 3a: Zijn er incidenten die wijzen op het niet voldoen aan de informatieveiligheidseisen?
Deelvraag 3b: Hoe zijn deze incidenten afgehandeld?

Bevindingen deelvraag 3a:
Er zijn geen incidenten die wijzen op het niet voldoen aan de informatieveiligheidseisen van iDIN geweest in de periode maart-april 2016. Dit is verklaard per mail door Allard Keuter van BVN op 29 april 2016.

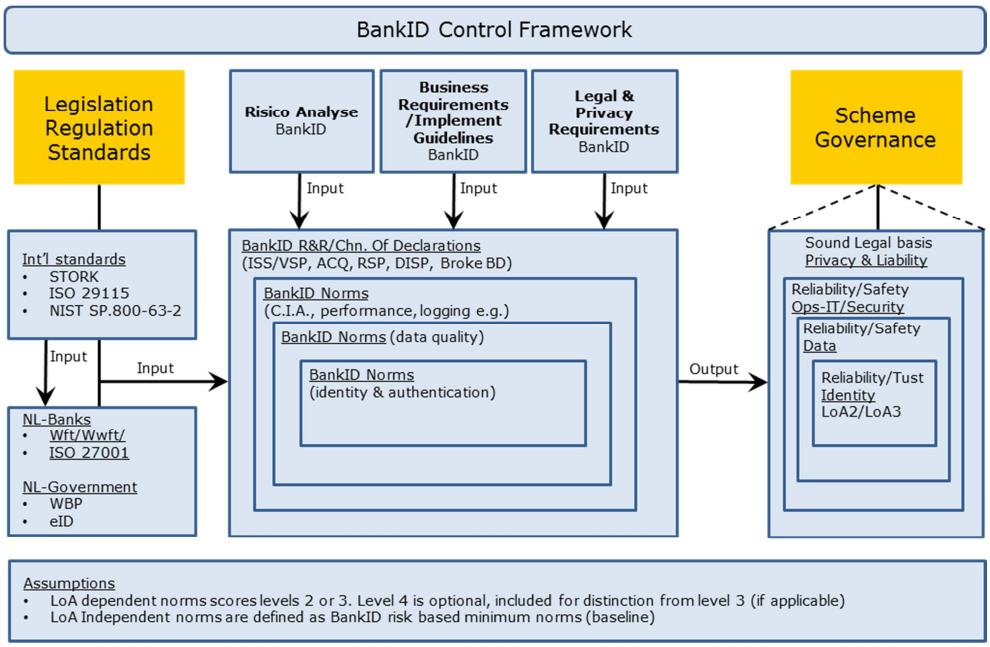
In het control framework (BankID framework Word 23102015 V 1 2) (eis 1.1) staat dat een Issuer een banklicentie moet hebben. Daarmee wordt bepaald dat de partij

[39] Zie “Banken starten pilot met online identificatiedienst iDIN”, http://www.betaalvereniging.nl/nieuws/pilot-idin/

onder toezicht staat en in dat toezichtkader worden ook de eisen rondom informatiebeveiliging gevat. Deze eisen gelden immers bank-breed en niet alleen voor iDIN. In eis 2.6 staat dat er een security framework geïmplementeerd moet zijn dat gebaseerd is op industry standards en 'aligned' met corporate policy. Voor iDIN zijn er geen *aanvullende* eisen bovenop waar banken al aan moeten voldoen.

Banken baseren hun informatiebeveiligingsbeleid op een veelheid van informatiebeveiliging standaarden zoals COBIT, ISO27001, Standard of Good Practise (SoGP) e.d. Op basis van deze breed geaccepteerde standaarden wordt er vaak een op maat gemaakte instelling-specifieke informatiebeveiliging standaard samengesteld die als leidraad fungeert voor de kwaliteitsborging en beveiliging van de interne of uitbestede infrastructuur waarin kritische informatie wordt verwerkt. De bewaking van dergelijke standaarden vindt plaats bij de deelnemende instellingen via het three-lines-of-defence principe waarbij in volgorde het Lijnmanagement, Risk & Compliance en tenslotte Audit, verificaties uitvoeren en toezien op naleving van (onderdelen van) de standaard. Binnen dit intern bewakingsmodel wordt regelmatig derde deskundige externe partijen ingezet voor het doen hele speciale veiligheidsonderzoeken (zoals penetratie en hackerstesten).

Naast dit interne bewakingsmodel voert ook de toezichthouder DNB periodiek toetsen uit ter vaststelling of de instelling voldoende weerbaar is tegen bijvoorbeeld cyberdreigingen.[40]



Figuur 61 iDIN Control Framework (bron: [22])

Uit Figuur 1 blijkt dat een 'control framework' wordt gehanteerd om de kwaliteit van de services rondom het BankID te kunnen waarborgen. In de begeleidende tekst (pagina 6) staat het volgende: 'In the initial phase of BankID, the scope of the control framework has been limited to the issuing domain. Therefore, it is limited to the criteria that are applicable to the issuer.' Intussen zijn ook de eisen verstrekt die gelden voor Acquirers en Routing Service Providers. [24], [25]

[40] zie bijvoorbeeld http://www.toezicht.dnb.nl/3/50-203304.jsp)." (Beheersing iDIN v2, p. 3-4)

Wel blijkt uit publieke bronnen[41] en uit aangeven door BVN dat oplichters nu al met valse 'phishing' e-mails proberen informatie van iDIN gebruikers te ontfutselen. 'Momenteel circuleert er een valse e-mail over iDIN. In de phishing mail die afkomstig lijkt van een bank willen oplichters u verleiden om de dienst te activeren in uw internetbankieromgeving.' Dit is een phishing poging die niet geslaagd lijkt. Hierdoor is geen informatieveiligheidsprobleem opgetreden.

Bevindingen deelvraag 3b:
N.v.t.

Hoofdvraag 4: Hoe is het toezicht verlopen?

Bevindingen vraag 4:
In het iDIN Framework wordt gewerkt met een stelsel van gelaagd toezicht. DNB houdt toezicht op de financiële instellingen in het algemeen. In 2014 heeft DNB ook iDEAL getoetst. Currence is (beoogd[42]) merkeigenaar en houdt toezicht op de instellingen die een iDIN licentie hebben verkregen. Currence staat op haar beurt weer onder 'oversight' van DNB. Het meest directe toezicht wordt dus uitgeoefend door Currence en in de praktijk door BVN.

De deelnemende instellingen dienen te worden toegelaten tot iDIN na toetsing door Currence op het voldoen aan alle vereisten. We hebben vastgesteld dat inmiddels alle deelnemende banken zijn toegetreden. Er is echter geen verklaring van een auditor beschikbaar gemaakt voor de onderzoekers waarmee kan worden onderbouwd dat wel of niet aan specifieke eisen is voldaan.

DNB houdt toezicht op de instellingen die iDIN aanbieden. Daarbinnen worden alle onderdelen waaruit iDIN bestaat (zoals identificatie klant) door DNB getoetst. De Betaalvereniging heeft de 5 pilotbanken voor de pilot gecertificeerd op basis van de self assessment die de banken hebben uitgevoerd. Dit certificeringsproces waarmee instelling bekend zijn in betalingsverkeer, zoals bijvoorbeeld betaalautomaten, iDEAL of Acceptgiro drukkerijen, is hier ook van toepassing. Belangrijk hierbij is dat de directie onafhankelijk kan besluiten over toetreding.

4.2.3 Onderzoeksvragen met betrekking tot privacy

Hoofdvraag 5: Wat zijn de resultaten van de PIA en hoe is omgegaan met de uitkomsten?

Deze hoofdvraag is opgedeeld in de volgende deelvragen:
Deelvraag 5a: Is er een PIA uitgevoerd?
Deelvraag 5b: Zijn er mitigerende maatregelen voorgesteld?
Deelvraag 5c: Zijn deze mitigerende maatregelen uitgevoerd?
Deelvraag 5d: Hebben zich desondanks nog privacy incidenten t.a.v. privacy voorgedaan?
Deelvraag 5e: Hoe zijn deze privacy incidenten opgelost?

Bevindingen deelvraag 5a:

[41] Zie "Oplichters haken met valse e-mail in op online identificeren met iDIN", 30 maart 2016, https://www.veiligbankieren.nl/nieuws/valse-mail-idin/
[42] iDIN is nu nog belegd binnen de projectorganisatie.

Er is voor iDIN geen algemene PIA uitgevoerd. Tijdens de ontwerpfase is er een privacy werkgroep actief geweest die steeds vanuit die discipline getoetst heeft of de voorgestelde ontwerpkeuzes voldeden aan privacy beginselen en pasten binnen het juridisch kader. Dit heeft interactief geleid tot een oplossing waarbinnen voorgestelde 'maatregelen' in het ontwerp al zijn meegenomen. Op basis hiervan hebben banken individueel hun PIA uitgevoerd. In het Bank ID Framework, v1.2, is vastgelegd dat het verplicht is dat banken een PIA uitvoeren of bijwerken voor iedere grote wijziging op de Bank ID dienst.([21], onder 11.2) Deze vereiste geldt dus voor de introductie van iDIN en het toetreden daartoe door iedere individuele bank. De onderzoekers hebben geen inzage gekregen in de uitgevoerde individuele PIA's en ook niet kunnen toetsen op welke wijze deze zijn uitgevoerd en wat de bevindingen daarin waren.

Op generiek niveau is een document opgesteld met interbancaire uitgangspunten bij de essentiële privacy-beginselen.[43] In dit document wordt op de verschillende beginselen uit de Wet bescherming persoonsgegevens kort ingegaan in relatie tot het iDIN Framework. Kern is dat de beginselen in het iDIN Framework gerespecteerd dienen te worden, zowel door de banken als door de Acceptanten (de dienstaanbieders waar een burger met iDIN kan inloggen). Specifieke uitwerkingen op het niveau van de individuele banken hebben we niet kunnen inzien, omdat deze als vertrouwelijk beschouwd worden. Aangaande beveiliging en fraudebestrijding wordt verwezen naar de ervaring met iDeal en betalingsverkeer in het algemeen waar iDIN op gebaseerd is.

De belangrijkste inrichtingskeuzes die in dit proces gemaakt zijn en dus van toepassing op iDIN als geheel zijn:

- de klant verleent voor elke gegevensverstrekking expliciet opdracht/toestemming.
- de Acceptant is in staat om gedifferentieerd gegevens uit te vragen zodat ook de Acceptant kan voldoen aan de Wbp eisen van doelbinding.
- niet voldoen aan de Wbp is een ontbindende voorwaarde in overeenkomsten met Acceptanten en (toekomstige) licentiehouders.

Vanuit Triodos is specifiek aangegeven dat in hun PIA de volgende maatregelen waren voorgesteld:

- Expliciete toestemming vragen aan klant in de iDIN schermen voor het versturen van de getoonde gegevens aan de acceptant.
- Voor het verwerken van BSN dient er een bewerkersovereenkomst te zijn met Equens (voor bouw pilotvoorziening) en Min van BZK.
- Doeleinde van de verwerking van de persoonsgegevens dienen in privacy statement te worden vastgelegd.

De eerste twee van deze punten zijn al uitgevoerd. Het derde punt dient te zijn uitgevoerd voordat de publieke fase van iDIN ingaat. (Bron: mail van Gerard Cillessen, 17 mei).

Met betrekking tot het verwerken van het BSN als bijzonder persoonsgegeven wordt aangegeven dat de verwerking en verstrekking aan het BSNk wettelijk is geregeld in de Wet elektronisch berichtenverkeer (WEB) en bijbehorende AMvB.

[43] Betaalvereniging Nederland, Achtergrond informatie over iDIN en privacy; Interbancaire uitgangspunten. 26 april 2016, versie 1.0 definitief.

Omdat de individuele banken in dit geval als bewerker optreden is door hen een bewerkersovereenkomst vastgesteld met de Minister van BZK als verantwoordelijke.

Bevindingen deelvraag 5b:
Het document met de privacy-beginselen [12] dateert van 28 april, dus tegen het einde van de looptijd van het onderzoek. Tussentijdse wijzigingen zijn daarvoor al verwerkt. Zie voor enkele voorbeelden het antwoord onder 5a. Op detailniveau of individueel bankniveau hebben de onderzoekers geen inzagemogelijkheid gekregen. Deze informatie is vertrouwelijk met het oog op de veiligheid van iDIN en het betalingsverkeer.

Bevindingen deelvraag 5c:
De beginselen uit de Wet bescherming persoonsgegevens (Wbp) zijn als uitgangspunt genomen in de ontwikkeling van iDIN. De privacy werkgroep heeft regelmatig de voorgestelde ontwerpkeuzes van iDIN gevalideerd en aanbevelingen gedaan over de te nemen maatregelen. Deze zijn verwerkt zodat ook het eindresultaat de gewenste inrichting heeft als het gaat om privacy. Op basis hiervan hebben de banken individueel hun PIA uitgevoerd en het product goedgekeurd.

Bevindingen deelvraag 5d:
Privacy incidenten betreffende iDIN dienen gemeld te worden bij Betaalvereniging Nederland (BVN). Over de periode maart en april 2016 zijn er geen incidenten gemeld bij BVN.

Bevindingen deelvraag 5e:
N.v.t.

4.2.4 Onderzoeksvragen met betrekking tot ervaringen

Hoofdvraag 6: Hoe ervaren de leveranciers de deelname aan de pilot?
De bronnen gebruikt bij het beantwoorden van deze vragen zijn:
- Interview met de Betaalvereniging Nederland;
- Mailwisseling met de ING;
- Mailwisseling met Triodos bank;
- Memo's van SVB en BVN. [26], [27]

Banken vullen met iDIN een maatschappelijke functie in op basis van bestaande dienstverlening, zij zoeken altijd mogelijkheden deze dienstverlening waar relevant uit te breiden. Daarnaast is volgens de Betaalvereniging Nederland een tweede reden voor banken om deel te nemen aan de pilot het feit dat de wetgeving zich zo ontwikkelt dat de markt van banken steeds meer opengebroken wordt. Andere partijen/spelers kunnen bijvoorbeeld betalingen initiëren uit naam van iemand waardoor een bank het risico loopt een soort van backoffice te worden. iDIN geeft banken de mogelijkheid om deze rol zelf te behouden in de toekomst.

Deze hoofdvraag is opgedeeld in de volgende deelvragen:
Deelvraag 6a: Wat zijn redenen voor leveranciers om deel te nemen aan de pilot?
Deelvraag 6b: Hoe is de pilot voor de leveranciers verlopen?

Deelvraag 6c: In welke mate zien leveranciers het hoogwaardige middel als toegevoegde waarde?

Bevindingen deelvraag 6a:
Met iDIN vervult ING haar maatschappelijke rol door online zaken doen makkelijk en veilig mogelijk te maken, zowel voor consumenten als acceptanten.
Voor Triodos is de reden voor deelname aan de pilot het opdoen van ervaring met het product met betrekking tot kwaliteit, betrouwbaarheid, gemak.

Bevindingen deelvraag 6b:
De ING is van mening dat de pilot vanuit issuing-perspectief uitstekend is verlopen. ING klanten hebben hierin geen problemen ondervonden.

Vanuit het acquiring-perspectief is de pilot voor de Belastingdienst als acceptant eveneens uitstekend verlopen. Bij het aansluiten van Zilveren Kruis en SVB (beide onderdeel van het BSN-domein) zijn er echter een aantal issues aan het licht gekomen. Beide partijen willen bij het inloggen een BSN ontvangen wat mogelijk is via het BSNk. Banken kunnen daarmee klanten in staat stellen hun iDIN te activeren voor gebruik in het BSN-domein (als issuing partij). Bij de Belastingdienst werkt dit succesvol. Voor acceptanten als Zilveren Kruis en SVB is het om dit te realiseren nodig het via iDIN verkregen BIN (het iDIN-pseudo-ID) te laten vertalen in een BSN door het BSNk. Daarvoor moeten deze partijen op het BSNk van Logius aansluiten. Zilveren Kruis heeft echter geen toestemming gekregen om op het BSNk aan te sluiten (overigens wel binnen de Idensys pilot). SVB en Zilveren Kruis hebben circa zeven weken gewacht op toestemming van BZK om op het BSNk aan te sluiten en SVB werd daarna geconfronteerd met onbekende impact in termen van tijd en kosten bij BZK/Logius als wel bij de technische partij die de koppeling voor SVB met het BSNk zou realiseren. [26] De BVN onderkent deze issues eveneens. [27] De kosten die gemaakt moeten worden om aan te sluiten op het BSNk zijn hoog en de doorlooptijden ten aanzien van het krijgen van goedkeuring en voor het maken van de daadwerkelijke aansluiting zijn lang. SVB heeft derhalve vooralsnog afgezien van deelname aan de iDIN pilot.

Voor Triodos is de pilot voorspoedig verlopen. De functionaliteit die door Triodos Bank is ontwikkeld werkt naar behoren.

Bevindingen deelvraag 6c:
Een hoogwaardige middel is voor ING van grote toegevoegde waarde. Met een dergelijk middel kan de ING Mijn ING (internetbankieren) veilig toegankelijk maken voor klanten en tegelijk fraude voorkomen. In verband met haar maatschappelijke rol willen ze dit middel via iDIN graag aanbieden aan de markt om online zaken doen te faciliteren met een gemakkelijk en veilig product.

Voor Triodos Bank bestaat de toegevoegde waarde uit het bieden van een alternatief identificatiemiddel voor DigiD. Iedere Nederlander heeft een bankrekening waardoor de banken een kwalitatief hoogwaardig alternatief met een hoog dekkingspercentage kunnen aanbieden indien DigiD eruit ligt. Daarnaast ziet Triodos Bank het middel als oplossing voor de komst van externe toetreders tot het betalingsverkeer (Google, Apple etc.). Door iDIN aan te bieden als een product zorgt Triodos Bank ervoor dat ze relevant blijft.

Hoofdvraag 7: Hoe is het aanvraag- en uitgifteproces verlopen?
Onderstaande vragen zijn beantwoord op basis van:

- Interview met de Betaalvereniging Nederland
- Mailwisseling met de ING
- Mailwisseling met Triodos bank.

iDIN is gebaseerd op bestaande middelen en bestaande klantrelaties. Voor ING geldt dat iDIN als functionaliteit is toegevoegd aan Mijn ING, zoals 10 jaar geleden ook iDEAL is toegevoegd. Daarmee is iDIN in de pilot ge-issued aan vrijwel alle meerderjarige particuliere klanten van ING die beschikken over Mijn ING (internetbankieren). Dat betekent dat deze klanten hun middelen reeds in bezit en in gebruik hadden voor de start van de pilot, waarmee iDIN een groot bereik onder burgers heeft. Om iDIN ook te kunnen gebruiken in het BSN-domein (bv. de Belastingdienst) hebben klanten iDIN eenmalig geactiveerd in het BSNk, via de site van de Belastingdienst. Het activatieproces is een gevolg van de keuze van BZK voor de wijze waarop in het BSN-domein gebruik kan worden gemaakt van inlogmiddelen en het BSN. Voor Triodos Bank doorloopt de klant hetzelfde proces, alleen wordt hiervoor het Triodos Bank bankmiddel gebruikt voor inloggen middels iDIN.

Hoofdvraag 8: Zien authenticatiediensten/middelenleveranciers toekomst in het middel dat zij nu uitgeven?
Deze vraag is beantwoord op basis van:

- Mailwisseling met de ING;
- Mailwisseling met Triodos bank.

ING ziet zeker toekomst in het middel dat ze nu uitgeven. De middelen zijn al jarenlang in de praktijk beproefd als toegangsmiddel voor Mijn ING. De middelen kennen een hoge mate van betrouwbaarheid, ING klanten hebben vertrouwen in de middelen en de klanten zijn bovendien vertrouwd met het gebruik van de middelen. In de markt bestaat een duidelijk behoefte aan gemakkelijke en veilige inlogmiddelen. Met iDIN wordt hieraan een invulling gegeven.

Triodos Bank geeft aan dat het huidige middel (identifier) de betrouwbaarheid en kwaliteit biedt die ze als bank eisen. Triodos Bank is volgens eigen zeggen uiteraard altijd op zoek naar nieuwe mogelijkheden om toegang nog veiliger en gemakkelijker te maken.

Hoofdvraag 9: Hoe ervaren de dienstaanbieders de deelname aan de pilot?

Deze hoofdvraag is opgedeeld in de volgende deelvragen:

Deelvraag 9a: Wat zijn de redenen voor dienstaanbieders om deel te nemen aan de pilot?
Deelvraag 9b: Hoe is de pilot voor de dienstaanbieders verlopen?
Deelvraag 9c: In welke mate zien dienstaanbieders het hoogwaardige middel als toegevoegde waarde?
Deelvraag 9d: Is de communicatie verlopen volgens het communicatieplan pilots?

Bevindingen deelvraag 9a:

De volgende bron is gebruikt voor beantwoording van de vragen:
- Interviews met de Belastingdienst.

De Belastingdienst noemt de volgende redenen om deel te nemen aan de pilot:
- De digitale dienstverlening van de Belastingdienst is nu afhankelijk van DigiD. Er is behoefte aan nog een middel zodat er altijd een 'fallback' beschikbaar is mocht DigiD niet werken (de multimiddelenstrategie). Het voordeel van het bankenmiddel is dat dit al breed is uitgerold en daarom al op korte termijn als 'fallback' kan dienen. De verwachting bij de Belastingdienst is dat het breed beschikbaar komen van het publiek middel lang zal duren. Vanuit het Idensys middel wordt innovatie verwacht.
- De betrouwbaarheid van DigiD is te laag. Het College Bescherming Persoonsgegevens heeft aangegeven dat het betrouwbaarheidsniveau 2 (code 20) te laag is. Voor het type diensten dat de Belastingdienst aanbiedt, is het noodzakelijk dat er sprake is van betrouwbaarheidsniveau 3 (code 30). Ook vindt er fraude plaats waarbij enveloppen met DigiD-codes uit brievenbussen worden gehengeld.

Bevindingen deelvraag 9b:
De volgende bron is gebruikt voor beantwoording van de vragen:
- Interviews met de Belastingdienst.

De Belastingdienst is tevreden over het verloop van de pilot. De Belastingdienst noemt de volgende positieve ervaringen:
- De doelstellingen zijn gehaald: er is een proces geïmplementeerd dat goed heeft gewerkt. Er zijn voldoende gebruikerservaringen opgehaald om lessen uit te kunnen leren. Deze lessen moeten nog nader worden bepaald. Een aantal eerste lessen betreffen het verbeteren van de customer journey (door vermindering van het aantal schermen) en het verbeteren van de communicatie (helder aan klanten uitleggen wat het verschil is tussen de middelen).
- De verschillende partijen in de keten hebben elkaar gevonden in de samenwerking en gezamenlijk een mooie keten gerealiseerd. Iedere partij verzorgt een klein stuk software van de keten. Zo is een 'lean & mean' oplossing gerealiseerd die weinig kosten met zich mee brengt.
- Tijdens de pilot hebben er geen incidenten plaatsgevonden. De Belastingdienst geeft aan dat alles technisch goed heeft gewerkt.
- De samenwerking met de partners in de keten is goed verlopen.
- De bereidwilligheid van deelnemers om mee te doen is lager dan gehoopt. De aantallen die ooit in de media zijn genoemd zijn niet bereikt (iDIN; max. 65.000 deelnemers, Idensys: max. 30.000 deelnemers)[44]. Dit lagere aantal deelnemers lag echter wel binnen de verwachting. Het doen van aangifte is voor burgers erg belangrijk. Zij willen dit doen zonder extra gedoe. Het feit dat de gebruikersaantallen lager zijn, heeft geen negatieve consequenties voor de Belastingdienst; het doel is bereikt (zie bovengenoemde ervaring).
- Ten aanzien van de iDIN pilot heeft de Belastingdienst de indruk dat deelnemers het een logisch proces vonden en het goed begrepen. Het registratieproces lijkt op het proces waarmee gebruikers al bekend zijn vanuit

[44] Zie bijvoorbeeld: https://belastingdienst-in-beeld.nl/extra-mogelijkheid-om-in-te-loggen-op-mijnbelastingdienst-nl/

hun bank. De Belastingdienst heeft ook enthousiasme gehoord bij de deelnemers om mee te doen aan de pilot.

Bevindingen deelvraag 9c:
De volgende bron is gebruikt voor beantwoording van de vragen:
- Interviews met de Belastingdienst.

De Belastingdienst ziet zeker toegevoegde waarde. Voor de Belastingdienst draait het om de multimiddelenstrategie; het hebben van meer dan één middel met het beveiliging-/betrouwbaarheidsniveau dat past bij de diensten. Belangrijk daarbij is de gebruiksvriendelijkheid voor gebruikers. De verwachting van de Belastingdienst is dat er straks concurrentie zal ontstaan die partijen ertoe aanzet om een zo goed mogelijk middel in markt te zetten.

Voor de Belastingdienst is het hoogwaardig middel een voorwaarde om door te kunnen gaan met het aanbieden en het ontwikkelen van diensten die steeds meer online zullen worden aangeboden.

Bevindingen deelvraag 9d:
De volgende bron is gebruikt voor beantwoording van de vragen:
- Interviews met de Belastingdienst.

De communicatie is uitgevoerd zoals gepland. Er is geen communicatieplan op schrift. Wel is er met de banken doorgesproken hoe de communicatie zou verlopen. Er is onder meer het volgende afgesproken:
- Interne communicatie via het intranet van de Belastingdienst om op kleine schaal medewerkers op te roepen om deel te nemen aan de pilot. Vervolgens wordt er gefaseerd een bredere groep mensen opgeroepen om deel te nemen aan de pilot.
- Teksten worden door de partijen met elkaar afgestemd.
- Er wordt gebruik gemaakt van neutrale berichtgeving.
- De media wordt niet opgezocht. (Ook niet om hogere aantallen deelnemers te werven).
- Er worden geen persberichten verstuurd.
- Er vindt geen positionering plaats van het eigen merk van partijen.

De Belastingdienst geeft aan dat alle partijen zich aan de afspraken m.b.t. communicatie hebben gehouden.

Hoofdvraag 10: Hoe is het proces van aansluiting verlopen?
De volgende bron is gebruikt voor beantwoording van de vragen:
- Interviews met de Belastingdienst

Het proces van aansluiting was een complex proces waarbij veel partijen zijn betrokken. Voor de betrokken partijen was het ook een leerproces om gezamenlijk uit te denken hoe zaken het beste kunnen worden ingericht. De Belastingdienst heeft het aansluitproces strak gestuurd. Het was zeer belangrijk om alles voor 1 maart 2016 (start van de aangifteperiode) te realiseren. Dit is ook gelukt.

Hoofdvraag 11: In welke mate wordt er van de diensten gebruik gemaakt door deelnemers aan de proef en hoe verloopt dit gebruik voor de dienstaanbieders?

Deze hoofdvraag is opgedeeld in de volgende deelvragen:
Deelvraag 11a: Hoeveel deelnemers maken gebruik van de diensten en hoe frequent is het gebruik van de diensten via het hoogwaardige middel?
Deelvraag 11b: Hebben zich nog problemen voorgedaan tijdens de pilot en hoe zijn deze opgelost?

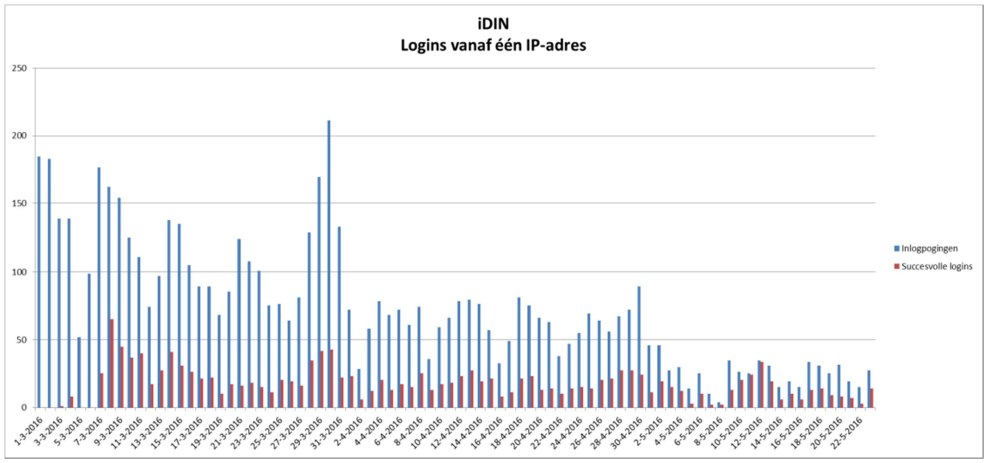
Bevindingen deelvraag 11a:
De volgende bronnen zijn gebruikt voor beantwoording van de vragen:
- Interviews met de Belastingdienst;
- Email over gebruiksgegevens (Ambtelijk projectleider, 18 mei 2016);
- Logdata aangeleverd t.a.v. iDIN pilot door de Belastingdienst op 24 mei, 2016.

Overzicht gebruiksgegevens

Gegevens	**iDIN**
Inlogpogingen (totaal aantal keer dat op de knop voor inloggen is gedrukt) *Periode: 1 maart – 22 mei, bron: Belastingdienst*	9566
Succesvolle logins (Totaal aantal keer dat daadwerkelijk succesvol is ingelogd) *Periode: 1 maart – 22 mei, bron: Belastingdienst*	2731
Inlogpogingen vanaf één IP-adres (Totaal aantal keer dat op de knop voor inloggen is gedrukt vanaf één IP-adres) *Periode: 1 maart – 22 mei, bron: Belastingdienst*	6150
Succesvolle logins vanaf één IP-adres (Totaal aantal keer dat daadwerkelijk succesvol is ingelogd vanaf één IP-adres) *Periode: 1 maart – 22 mei, bron: Belastingdienst*	1495
Aantal geactiveerde inlogmiddelen *Periode: 1 maart – 13 mei, bron: Belastingdienst/BSNk*	1407

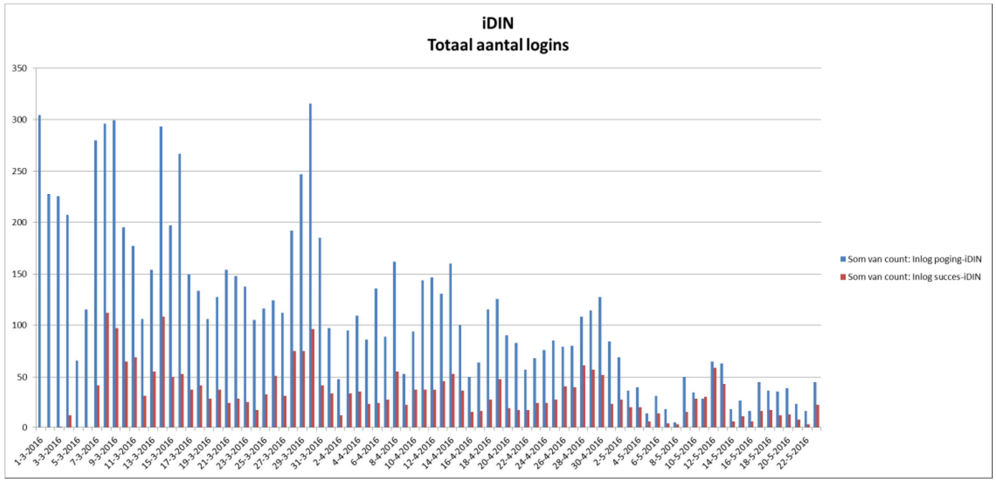
TNO heeft geen verklaring voor het aantal niet succesvolle inlogpogingen. Gezien de datum waarop de data is aangeleverd is TNO niet in staat geweest hier verder onderzoek naar te verrichten.

Figuur 62 geeft een overzicht van het aantal keer per dag dat vanaf één IP-adres een inlogpoging is gedaan. Pogingen van meerdere personen vanaf één IP-adres (locatie) tellen als één mee.



Figuur 62 iDIN - logins vanaf één IP-adres

Figuur 63 geeft een overzicht van het aantal keer per dag dat een inlogpoging is gedaan. Pogingen van meerdere personen vanaf één IP-adres (locatie) tellen allemaal mee.



Figuur 63 iDIN - totaal aantal logins

Bevindingen deelvraag 11b:
De volgende bronnen zijn gebruikt voor beantwoording van de vragen:

- Memo Inrichting pilot iDIN (BankID) bij de Belastingdienst [13];
- Interviews met de Belastingdienst;
- Email over gebruiksgegevens (Ambtelijk projectleider, 18 mei 2016).

De gebruikersondersteuning voor de pilot iDIN is als volgt ingericht:
In de publieksfase wordt de gebruikersondersteuning via de reguliere beheerprocessen uitgevoerd. Klantsignalen kunnen binnenkomen bij de dienstverleningskanalen van de Belastingdienst en de banken. Alle meldingen worden op een centraal punt geregistreerd waarna diagnose plaatsvindt. Afhankelijk van deze diagnose (functioneel, applicatief, netwerk, extern of communicatief) wordt het issue voor verdere afhandeling binnen de Belastingdienst uitgezet of wordt de melding doorgezet naar de herkenningsmakelaar. Er wordt een (virtuele) control room ingericht voor besluitvorming bij incidenten met een hoge prioriteit. Voor de BelastingTelefoon, webcare en op de website wordt een Q&A

beschikbaar gesteld om klantvragen te beantwoorden. Deze wordt middels een leercirkel met de banken bijgesteld indien wenselijk. De Belastingdienst gaat ervanuit uit dat klanten of hun bank of de Belastingdienst bellen met vragen.

TNO heeft geen inzicht gekregen in het aantal en de inhoud van de binnengekomen vragen bij de Belastingdienst. Bij de banken is volgens BVN één geregistreerde vraag over iDIN. Dit betrof een algemene vraag over de werking van iDIN.

4.3 Beantwoording van de onderzoeksvragen voor de pilot Publiek Middel

In de pilot Publiek Middel wordt voor de technische inrichting sterk uitgegaan van een pilot. Dat betekent dat erkend wordt dat bepaalde aspecten ten aanzien van techniek, privacy en het proces nog niet definitief zijn vastgesteld en dat dit ook bewust is gedaan. Aan de andere kant is echter ook sprake van een productieomgeving, omdat burgers daadwerkelijk rechtsgeldige transacties kunnen verrichten. De beantwoording van de vragen zal hier plaatsvinden aan de hand van de inrichting van het publieke middel zoals geïmplementeerd voor de pilotfase. De gekozen implementatie voor de pilot heeft echter ook consequenties ten aanzien van de informatie die wordt vastgelegd om onderzoeksvragen binnen deze pilot te beantwoorden.

De bronnen bestaan uit logbestanden uit verschillende systemen (kwantitatieve informatie) en van verschillende helpdesks. Daarnaast dient in acht genomen te worden dat voor de gemeente Groningen en Den Haag andere doelgroepen geworven zijn dan oorspronkelijk bedoeld en men derhalve niet zonder meer aan mag nemen dat de kwalitatieve of kwantitatieve data representatief zal zijn voor de Nederlandse burger in het algemeen.

4.3.1 Onderzoeksvragen met betrekking tot techniek

Hoofdvraag 1: Wordt voldaan aan de afgesproken eisen die verwoord staan in de gebruiksvoorwaarden van DigiD?

Op de website van Logius is het bestand gevonden met als titel ‘Voorwaarden DigiD’. [28] Echter de ‘Regeling voorzieningen GDI’ is sinds 1 november 2015 de opvolger van de Gebruiksvoorwaarden DigiD [Bron: mail ICTU dd. 15 maart 2016]. Daarmee zijn de eisen die verwoord staan in de gebruiksvoorwaarden van DigiD blijkbaar niet van toepassing op de Pilot Publiek Middel.

ICTU laat weten dat daar de Regeling voorzieningen GDI de Gebruiksvoorwaarden DigiD heeft opgevolgd laatstgenoemde niet meer relevant is. Onderzoeksvraag zou derhalve moeten zijn of de Pilot Publiek Middel aan de Regeling voorzieningen GDI voldoet.

Hoofdvraag 2: Voldoet de technische voorziening van Logius, RvIG en RDW aan de BIR?

De Baseline Informatiebeveiliging Rijksdienst (BIR) [29] is een normenkader, waarvoor de onderzoekers van TNO niet het mandaat noch de benodigde tijd

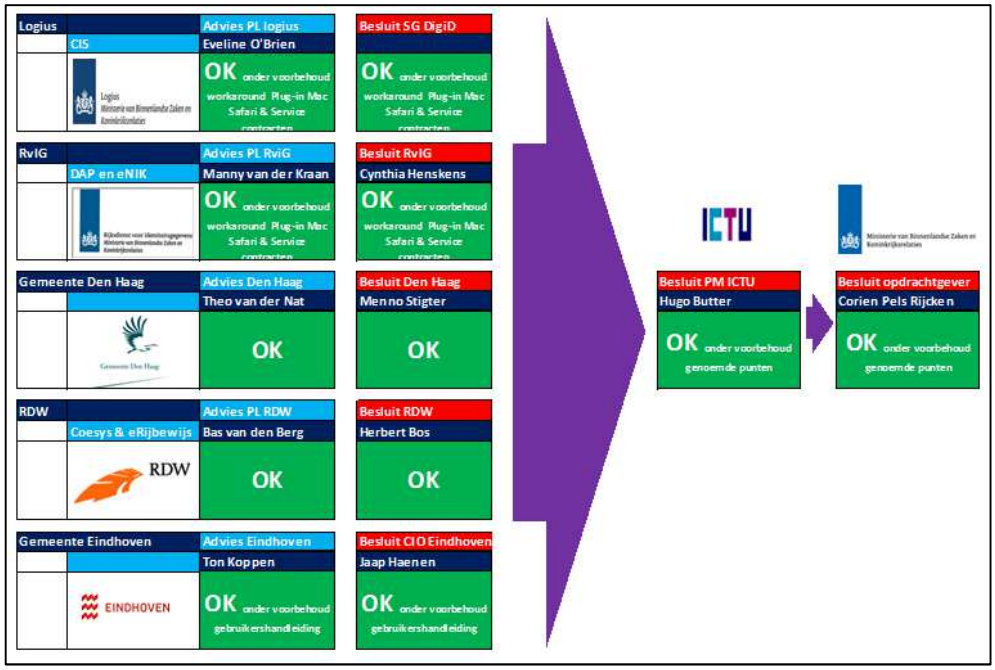
hebben om deze zelf te onderzoeken voor de technische voorziening van de organisaties Logius, RvIG en RDW voor de Pilot Publiek Middel.

Als alternatieve optie, zoals aangegeven in de onderzoeksvraag, wilden de onderzoekers deze vraag beantwoorden met: 'De Audit Dienst Rijk (ADR) verklaart dat de technische voorziening voldoet aan de BIR'. Met andere woorden refereren naar reguliere audits en de audit assessmentrapportage van de ADR en de bijbehorende In Control Verklaringen (ICV). Deze verklaringen zijn opgevraagd bij Logius maar niet gedeeld met de onderzoekers [Bron: mail Logius dd. 18-05-2016]. De ADR rapporten worden niet gedeeld i.v.m. vertrouwelijkheid van deze informatie [Bron: mail ICTU dd. 24/05/2016].

ICTU laat weten dat zowel Logius/DigiD als het RvIG er jaarlijks ICV's (in control verklaringen) in het kader van de BIR worden afgegeven alsook dat RDW voor haar dienstverlening over een ISO27001 certificering beschikt [Bron: mail Logius dd. 18-05-2016].

Hoofdvraag 3: Voldoen de ICT-componenten aan de gestelde technische veiligheidseisen en privacy-eisen

Van ICTU is een vrijgaveadvies ontvangen waarin een voorlopig positief 'vrijgavebesluit' is opgenomen (op pagina 16). [15] Zie ook Figuur 64.



Figuur 64 Positief vrijgavebesluit ICTU (Bron: [15])

In genoemd vrijgaveadvies staat op pagina 11: 'De technische vrijgave is gedaan op basis van de bevindingen uit de diverse (acceptatietesten) op diverse testomgevingen. Het betreft de volgende testen:

- Keten Integratie Test (Test) uitgevoerd door ICTU op de Publieke eID-middelen in combinatie met CTS.
- Keten Integratie Test (Test) uitgevoerd door ICTU op de Publieke eID-middelen in combinatie met CIS.'

In de ‘onder voorbehoud’ genoemde punten worden drie onderwerpen genoemd (zie pagina 16) waar Keten Integratie Test (KIT) niet bij staat. Hierop baseren wij dat volgens ICTU aan de technische veiligheidseisen van de Keten Integratie Test is voldaan.

Hierbij moet worden vermeld dat het daadwerkelijke Keten Integratie Test (KIT) document waarin de door BZK gerefereerde veiligheidseisen staan beschreven, niet is gedeeld met de TNO onderzoekers. Ook moet worden gemeld dat TNO niet op basis van eigen onderzoek tot deze bevinding is gekomen.

Daarnaast merken we nog het volgende op:
- Het gerefereerde document is een concept en niet definitief.
- Het gerefereerde document is een positief vrijgavebesluit ‘… voor de start van de Pilots op 15 februari 2016…’ maar dat is nog geen vrijgaveadvies voor grootschalige productie. Toelichting door ICTU: ‘Het vrijgaveadvies betreft nadrukkelijk en uitsluitend de pilot. Van grootschalige productie is in de huidige pilot geen sprake (maar onderwerp in het project inzake de structurele oplossing Publiek Middel) en is derhalve onderzocht noch beoogd want niet opportuun.’ [Bron: mail ICTU d.d. 23-05-2016]

(Noot voor de lezer: de hoofdvragen 3 (het privacy-deel) en de hoofdvragen 4 en 5 hebben betrekking op privacy en zijn opgenomen in paragraaf 4.3.2.)

Hoofdvraag 6: Hoe werkt de technische keten (kaart, kaartlezer, aanvraag/uitgifte en DigiD) tijdens de pilot?

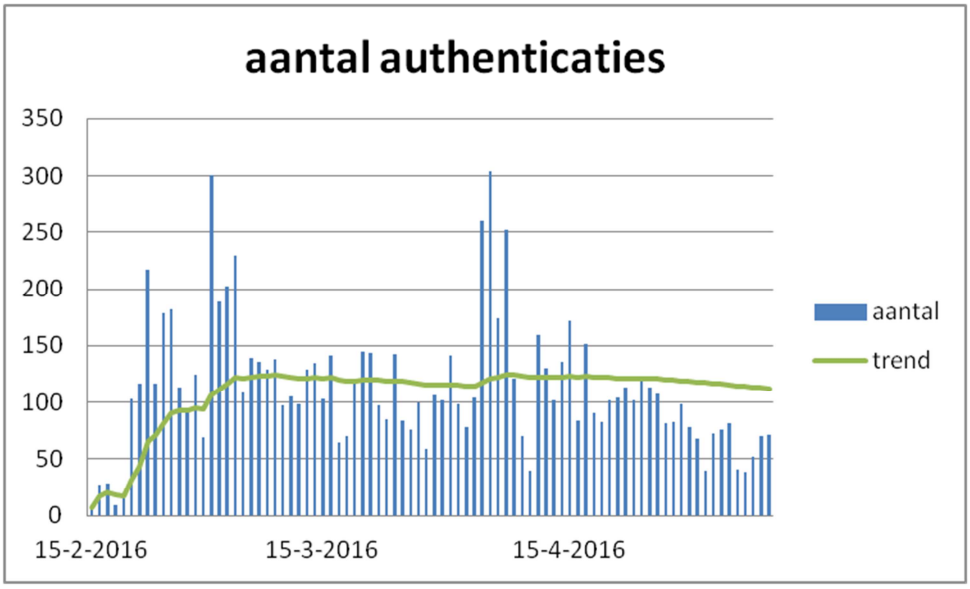
Deze hoofdvraag is opgedeeld in de volgende deelvragen:
Deelvraag 6a: Hoe verloopt het activeren door de deelnemers?
Deelvraag 6b: Hoe verloopt het inloggen bij de deelnemers?
Deelvraag 6c: In welke mate zijn er aanpassingen gedaan aan de techniek tijdens de pilot om problemen te verhelpen?

De installatie, activatie en login procedures zijn beschreven in hoofdstuk 3, in paragraaf 3.5.5. De hierna volgende onderzoekvragen zijn beantwoord op basis van:
- De meeloopdag in Eindhoven en de interviews tijdens die dag met het RDW, Logius, gemeente Eindhoven, gemeente Groningen.
- Logdata geleverd door en aanvullende gesprekken met het RDW.
- Logdata geleverd door ICTU met als bron Logius.
- Een overzicht van binnengekomen vragen van de helpdesk van de gemeente Eindhoven.
- Een overzicht van binnengekomen vragen van de helpdesk van de gemeente Den Haag.
- Een aanvullend gesprek met ICTU en Logius t.a.v. de logdata en vragen binnengekomen bij verschillende pilot organisaties.

Bevindingen deelvraag 6a:
In Eindhoven zijn 464 en in Groningen 98 eRijbewijzen uitgereikt en gecommuniceerd naar Logius voor activatie (whitelist), naast de 48 eRijbewijzen die zijn uitgereikt in een Friends and Family test van het RDW in samenwerking met andere pilot organisaties (e.g. ICTU). Hoeveel van deze kaarten daadwerkelijke in

gebruik zijn genomen door deelnemers is uit de aangeleverde (log)data van het RDW en Logius niet te achterhalen.

In Den Haag zijn 375 eNIKs uitgereikt. Hiervoor geldt eveneens dat op dit moment onbekend is hoeveel hiervan daadwerkelijke door deelnemers in gebruik zijn genomen op basis van de beschikbare logdata van Logius. Wel kan uit de logdata gehaald worden hoeveel logins of authenticaties er per pilot dag plaats hebben gevonden, zie Figuur 65. In die figuur kan het overigens zijn dat één persoon meerdere keren per dag ingelogd heeft.



Figuur 65 Overzicht aantal authenticaties per dag gedurende de pilot[45]

Voor vragen van deelnemers over het in gebruik nemen en gebruiken van het eRijbewijs heeft de gemeente Eindhoven een mailadres beschikbaar gesteld. De gemeente Groningen heeft een mailadres en telefoonnummer (shared service centrum) beschikbaar gesteld waar deelnemers terecht kunnen met vragen. Bij de gemeente Eindhoven is middels mail de laatste vraag op 4 april (2016) binnen gekomen. Daarmee zijn er in Eindhoven 87 vragen gesteld via mail door pilotdeelnemers[46] (464) waarvan:

- 12 vragen gerelateerd waren aan techniek (mogelijk dus ook de activatie van het middel);
- 19 vragen gerelateerd waren aan de codes voor activatie en gebruik (PIN, PUK en CAN codes niet ontvangen of beschadigd bij het openen van de post);
- 4 vragen gerelateerd waren aan de kaartlezer (defecte kaartlezer).

De twaalf technisch gerelateerde vragen zijn volgens de escalatieprocedure [14] doorgestuurd en afgehandeld door Logius. De overige vragen gesteld aan de gemeente Eindhoven betroffen andere categorieën niet relevant voor de activatie van het middel. Bij de gemeente Groningen zijn geen vragen binnen gekomen via het telefoonnummer of via email. Wel is de projectleider 3 keer direct een vraag gesteld waarbij 1 deelnemer te kennen gaf het middel niet te kunnen installeren in

[45] Bron: Logoverzichten ICTU gecreëerd door Logius, peildatum 9 mei 2016.
[46] Overzicht binnengekomen vragen via mail opgeleverd door de gemeente Eindhoven op 13 mei, 2016.

verband met zijn/haar virusscanner. 2 Deelnemers hadden een vraag maar niet technisch gerelateerd.

Op basis van de beschikbare bronnen en bovenstaande beschrijving is het niet mogelijk een eenduidig antwoord te geven op de vraag hoe de activatie van het middel eRijbewijs voor deelnemers is verlopen. Wel is duidelijk dat in Eindhoven 464 personen het eRijbewijs hebben afgehaald en in Groningen 98 personen het eRijbewijs hebben afgehaald met de intentie deze in gebruik te nemen. Er zijn daarbij 35 vragen aan de gemeente Eindhoven gesteld gerelateerd aan de activatie van het eRijbewijs. In Groningen geen vragen ten aanzien van het activeren van het eRijbewijs. Dit komt neer op 7,5 procent van alle deelnemers die bij het activeren tegen een probleem of vraag is aangelopen en dit kenbaar heeft gemaakt bij de desbetreffende gemeente.

Ten aanzien van vragen betreffende het in gebruik nemen en gebruiken van de eNIK heeft de gemeente Den Haag een e-mail adres en telefoonnummer (het Haags Contact Centrum) voor vragen van deelnemers beschikbaar gesteld. Vragen die telefonisch niet beantwoord konden worden zijn doorgestuurd naar het mail adres. Telefonische vragen zijn verder niet geregistreerd en inhoudelijk bijgehouden. Via de mailbox zijn er zo'n 157 vragen binnengekomen tot en met 11 mei 2016[47]. Van dit aantal geven 36 deelnemers te kennen dat het inloggen met het middel helemaal niet lukt. 6 Deelnemers gaven te kennen dat ze geen inlogcodes ontvangen hebben (data tot 1 april). Na 1 april zijn er nog 20 vragen binnengekomen in aanvulling op de vragen tot 1 april welke niet verder gespecificeerd zijn, de inhoud van deze vragen is voor de onderzoekers onbekend. Alle binnengekomen vragen zijn uiteindelijk opgelost; over het algemeen naar tevredenheid van de deelnemers. In sommige gevallen was echter de device/PC niet geschikt of de kaartlezer kapot (slechts een gering aantal, echter het exacte aantal is onbekend). In één geval werkte de eNIK niet[48].

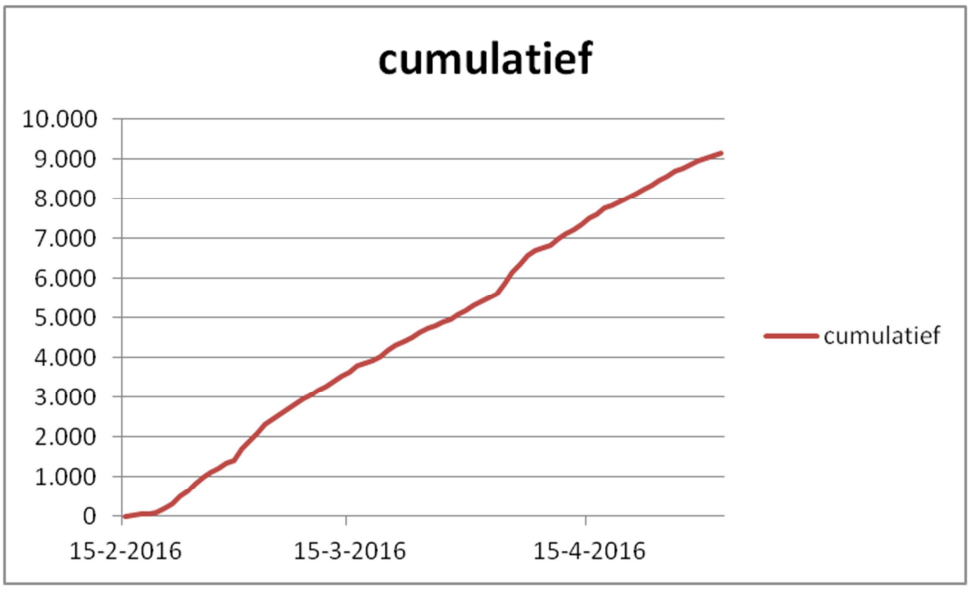
Op basis van bovenstaande informatie kan geconcludeerd worden dat rond de 11% van de deelnemers aanvankelijk problemen heeft gehad en deze heeft gecommuniceerd aan de gemeente Den Haag ten aanzien van het in gebruik nemen van het middel eNIK. Een groot deel hiervan is volgens de gemeente opgelost naar tevredenheid van de deelnemers.

Er is te kennen gegeven dat de installaties van de plug-in, als onderdeel van het activeren van het publieke middel, zorgen blijft baren en niet voor alle OS/Browser combinaties even soepel en/of voorspelbaar verloopt. Daarnaast is aangegeven dat ontwikkelingen in browser plug-ins uitwijzen dat de plug-ins benodigd voor het activeren van de kaartlezers zoals tijdens de pilot gebruikt, in de toekomst wellicht niet langer door alle browser leveranciers ondersteund zullen worden[49]. Het leveren van ondersteuning vanuit de pilot organisatie ten aanzien van specifieke operating systemen en browser combinaties is niet mogelijk[50]. Alternatieven dienen op dit gebied in de toekomst overwogen te worden.

[47] Mail communicatie met gemeente Den Haag waarin dit overzicht is opgevraagd.
[48] Mail communicatie met gemeente Den Haag.
[49] Telefonisch gesprek/interview 6 mei, 2016 met ICTU, Logius ten aanzien van de pilot publieke middelen.
[50] Meeloopdag Eindhoven

Samenvattend: Ten aanzien van het exact aantal uitgevoerde en geslaagde activatie van het publieke middel kunnen op dit moment nog geen eenduidige uitspraken worden gedaan op basis van de logdata. Wel blijkt op basis van de binnengekomen e-mails op de verschillende gemeentelijke mail adressen 7,5% van de deelnemers technisch gerelateerde problemen/vragen hadden die grotendeels samenhangen met de activatie van het eRijbewijs en 11% die samenhangen met de activatie van het eNIK.

Bevindingen deelvraag 6b:
Uit de door Logius gegenereerde logdata[51] blijkt dat in de periode van 15 februari 2016 tot en met 2 mei 2016 voor zowel het eRijbewijs als het eNIK 9136 authenticaties (logins) zijn uitgevoerd. Door Logius wordt verder aangegeven dat alle authenticatie pogingen gemaakt door deelnemers ook tot daadwerkelijke geslaagde authenticaties hebben geleid gedurende deze periode (zie Figuur 66).



Figuur 66 Overzicht authenticaties voor eRijbewijs en eNIK van 15 Februari 2016 tot en met 2 mei 2016 (Bron: Logius)

Uit de logdata van het RDW over dezelfde periode (gebaseerd op de Gemalto server data) blijkt dat 6.614 authenticaties gemaakt zijn met het eRijbewijs gedurende deze periode. De uitreiking van het eNIK is later gestart (29 februari 2016), gevolgd door Groningen met wederom het eRijbewijs op 11 april 2016. Als het aantal authenticaties gemaakt met eRijbewijs over deze periode afgetrokken wordt van het totaal aantal authenticaties uit de logdata van Logius over deze periode wordt duidelijk dat er met het eNIK over deze periode 2.522 authenticaties zijn gemaakt.

In de logdata wordt geen onderscheid gemaakt tussen door de gemeenten uitgegeven documenten en documenten uitgereikt in de friends and family test gedaan door het RDW in samenwerking met de andere (bij de) pilot (betrokken) partners zoals Logius en ICTU. Ervan uitgaande dat alle deelnemers hun middel daadwerkelijk in gebruik hebben genomen (inclusief de in de friends and family test

[51] ICTU logdata overzichten gegenereerd door Logius.

uitgereikte documenten) komt het gemiddeld aantal keren inloggen met het eRijbewijs op 12,9 keer per deelnemer gedurende de pilot periode. Voor het eNIK op 6,7 keer gemiddeld per pilot deelnemer over de pilot periode (die iets korter is dan die van het eRijbewijs) . Zoals aangegeven in paragraaf 3.5.3 is het de vraag of deze gegevens representatief zijn voor de Nederlandse burger (in Groningen en Den Haag zijn de selectiecriteria gaandeweg de pilot aangepast en een deel van de uitgereikte documenten zijn gebruikt door verschillende in de pilot deelnemende organisaties voor testdoeleinden). De gegevens geven echter aan dat het inloggen of de authenticatie, zoals gedefinieerd door Logius, geen problemen geeft en deze conclusie mag getrokken worden op basis van het aantal keren dat er een authenticatie is uitgevoerd.

Op basis van de logdata ten aanzien van authenticatie kan niet vastgesteld worden of de gebruikers ook daadwerkelijk toegang hebben gekregen tot de website van een dienstaanbieder. Dit is het gevolg van het feit dat sommige bij DigiD aangesloten dienstaanbieders het hogere beveiligingsniveau, afgegeven door het Publieke Middel, niet correct kunnen afhandelen. In de ogen van de pilot deelnemer zal een inlogpoging bij een dergelijke dienstaanbieder dan alsnog als mislukt gezien worden. Dit blijkt uit het feit dat bij de verschillende helpdesks er eveneens vragen binnen zijn gekomen ten aanzien van het inloggen bij verschillende dienstaanbieders (Eindhoven 25 vragen over instanties niet bereiken; Den Haag 17 vragen over instanties niet bereiken; Groningen geen vragen binnen gekomen ten aanzien van dit onderwerp; de website van de gemeente Groningen zelf was niet bereikbaar met het publieke inlog middel).

Uit het overzicht van Logius ten aanzien van de top 10 opgevraagd sites van dienstaanbieders met authenticatie met een publiek middel blijkt dat 22% van de opgevraagde sites in de top tien niet bereikbaar zijn middels het publieke middel (som van de belastingdienst, VGZ en UWV werkbedrijf), hoewel de authenticatie met het publieke middel goed verloopt. Zie onderstaande tabel voor een overzicht van de top 10 authenticaties voor dienstaanbieders.

Overzicht van geslaagde authenticaties top 10 dienstaanbieders (Bron: Logius)

Dienst	Actueel	% Totaal
Belastingdienst**	1482	16%
MijnOverheid	1412	15%
Mijn DigiD	993	11%
Gemeente Eindhoven2	589	6%
Gemeente Den Haag_	375	4%
Belastingdienst/Toeslagen	322	4%
MijnABP	291	3%
Mijn VGZ**	282	3%
UWV Werkbedrijf**	246	3%
SVB	228	2%
Totaal Top 10	**6220**	**68%**

Een aandachtspunt ten aanzien van het inloggen is derhalve te zorgen dat meer dienstaanbieders met het verhoogde beveiligingsniveau om kunnen gaan of het beveiligingsniveau te verlagen waar een lager niveau gevraagd/geaccepteerd wordt door een dienstaanbieder.

Samenvattend: Het aantal geslaagde authenticaties (logins) via Publieke Middelen is 100%. Tijdens de pilot periode zijn er enkele storingen bij DigiD geweest welke gezorgd hebben dat pilot deelnemers uiteindelijk toch niet op de site van een dienstaanbieder in konden loggen (aantal onbekend) en uit de reeds beschreven cijfers blijkt 22% van de opgevraagde websites van dienstaanbieders in de top 10 het hogere beveiligingsniveau niet aan te kunnen, hetgeen voor een pilotdeelnemer eveneens resulteert in het niet uitkomen bij de opgevraagde website. Het publieke middel zelf werkt echter uitstekend als authenticatiemiddel.

Bevindingen deelvraag 6c:
Tijdens de doorlooptijd van de pilot is er geen enkele technische aanpassing gedaan aan de technische systemen gebruikt binnen de pilot.

Ter voorbereiding op de pilot zijn er bij de verschillende gemeenten minimale aanpassingen gedaan of aanvullingen geformuleerd en geïmplementeerd op bestaande systemen bestaande uit:

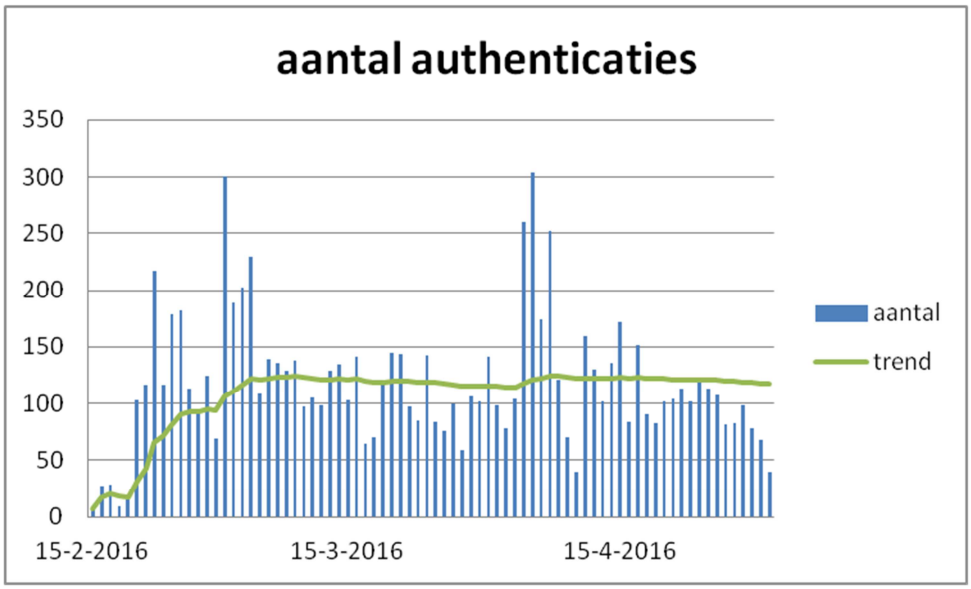
- Een koppeling met de back-office/CRM systemen voor het afhalen van het eRijbewijs op afspraak (Eindhoven, in Groningen geen afspraak nodig, in Den Haag is gebruik gemaakt van het reguliere systeem voor aanvraag en uitgifte van NIKs);
- Een Excel toepassing welke een check list bevat van stappen te doorlopen door baliemedewerkers, toegang gaf tot benodigde documenten en de registratie vormde van uitgegeven Publieke Middelen voor latere communicatie naar Logius voor activatie (Eindhoven, Den Haag en Groningen).

Hoofdvraag 7: Wat is de performance van de techniek?
De ‘snelheid’ interpreteren we voor deze vraag als de tijd die het kost om in te loggen. Om dit zinvol te kunnen meten, is een keten-overstijgende meting nodig vanuit het perspectief van de eindgebruiker. Dit lijkt op de definitie van ‘Round Trip Time’ (RTT)[52] en kan worden gezien als de tijdsduur tussen het moment dat de eindgebruiker op een Login knop drukt tot aan het moment dat de eindgebruiker op het scherm ‘U bent ingelogd’ ziet staan. In sommige gevallen zit hier nog een handmatige handeling tussen zoals bijvoorbeeld het invoeren van een PIN code (Digidentity).

Er is geen pilotrapportage verkregen waarin zichtbaar is of dit wordt gemeten, hoe dit wordt gemeten en welke performance daadwerkelijk (gemiddeld) is gehaald. Bovendien is de pilot omgeving een aparte omgeving in de zin dat maar een beperkt aantal eindgebruikers gebruik maakt van de authenticatie dienstketen. Ook de lokale omgeving van de eindgebruiker (computer, lokaal netwerk, internetverbinding) is van invloed op deze indicator. Uit de beperkte steekproef met het eRijbewijs blijkt dat het inloggen op de website van MijnOverheid vanaf een TNO laptop via een bedrade netwerkverbinding en de internetverbinding van TNO (Surfnet) ongeveer 1 á 2 seconden duurt.

Voor wat betreft beschikbaarheid is er geen pilotrapportage verkregen waarin zichtbaar is of dit wordt gemeten, hoe dit wordt gemeten en welke performance daadwerkelijk is gehaald.

[52] Zie http://www.globaldots.com/googles-web-performance-best-practices-2-minimize-round-trip-times/



Figuur 67 Dagstatistieken pilotrapportage (Bron: Logius)

Wel is uit de login-statistieken ontvangen van Logius (zie Figuur 67) op te maken dat tijdens de meetperiode elke dag eindgebruikers hebben ingelogd met een maximum van 300 eindgebruikers per dag. Hierop baseren we dat de techniek elke dag tijdens de meetperiode beschikbaar is geweest.

Hoofdvraag 8: Welke aandachtspunten zijn er bij de techniek?

Er worden door ICTU drie punten aangedragen die mogelijk een rol gaan spelen bij landelijke uitrol:

- De kaartlezer met USB aansluiting is een zorg voor landelijke uitrol. Er zijn veel devices in Nederland zonder een USB aansluiting (bv. Apple iPad).
- De installatie van webbrowser plug-ins (extensions) is lastig. Voor een landelijke uitrol zou dit simpeler moeten worden (minder handelingen met een lagere kans op fouten).
- De technische infrastructuur voor de pilot is gedimensioneerd naar 1500 gebruikers. Meer server capaciteit is nodig voor een landelijke uitrol maar hier worden geen problemen verwacht aan de DigiD-zijde.

De onderzoekers hebben gevraagd of het mogelijk is statistieken te krijgen van de monitoring oplossing van de server capaciteit van bijvoorbeeld de gebruikte web-, database- en overige servers maar deze zijn niet aangeleverd. Ze zijn echter voor het gedetailleerder beantwoorden van deze onderzoeksvraag niet noodzakelijk (nice-to-have).

Door gemeente Groningen is genoemd dat bij opschaling er wel veel kaartlezers op voorraad moeten zijn gezien de wekelijkse uitgifte van rijbewijzen en de fysieke afmetingen van kaartlezer en verpakking eisen een grote ruimte. Logistieke zaken spelen een rol.

4.3.2 Onderzoeksvragen met betrekking tot privacy

In januari 2016 is door Net2Legal Consultants een PIA uitgevoerd op de pilot Publieke eID middelen. [30] Dit was een vervolg op de eerdere PIA uit juni en

aanvullende notitie uit augustus 2015. In het PIA rapport worden een aantal zaken opgemerkt. De opmerkingen die relevant zijn voor de hier te beantwoorden vragen zullen worden behandeld, in samenhang met de eigen bevindingen van TNO.

Hoofdvraag 3: Voldoen de ICT-componenten aan de gestelde technische veiligheidseisen en privacy-eisen?

Deze vraag dient in samenhang gezien te worden met dezelfde vraag bij het technische onderdeel hierboven. Voor de gestelde privacy-eisen is gekeken naar de Regeling voorzieningen GDI. Daarin zijn echter geen specifieke privacy-vereisten opgenomen. Een specifiek kader met privacy-eisen is dan ook niet vastgesteld voor deze pilot. Wel wordt verwezen naar een aantal technische standaarden die van toepassing zijn volgens het 'pas toe of leg uit' principe. Enkele van deze standaarden dragen ook bij aan de privacybescherming door het technisch beveiligen van persoonsgegevens. Voor het privacy onderdeel kent deze vraag dus geen specifieke vereisten.

In algemene zin wordt wel aangegeven dat voldaan moet zijn aan de vereisten uit de Wet bescherming persoonsgegevens (Wbp). In de toelichting bij de Regeling wordt overigens ook indirect hiernaar verwezen via het Afsprakenstelsel dat van toepassing is indien gebruik gemaakt wordt van het BSNk.[53]

Vanuit de vereisten uit de Wbp die gelden ten aanzien van ICT-componenten geldt dat passende technische maatregelen getroffen dienen te worden om de gegevens adequaat te beschermen. In de PIA zijn drie privacy risico's benoemd, waarvan er in dit licht twee relevant zijn: risico's rond centrale gegevensverwerking en risico's rond de apparatuur van de pilotdeelnemer (burger).[54] Het eerste risico, centrale gegevensverwerking, wordt in de PIA aan de hand van verschillende punten toegelicht. Allereerst wordt ingegaan op aspecten omtrent aansprakelijkheid of sanctionering van burgers indien een transactie met een pilotmiddel achteraf niet gelukt blijkt te zijn. Dit is een organisatorisch aspect dat onder Hoofdvraag 5 hieronder behandeld wordt.

Vervolgens wordt aangeduid dat de vastlegging van gegevens bij gemeenten en dienstaanbieders mogelijk een nieuw risico vormt, omdat deze niet onder de bestaande gegevensverwerking van DigiD valt. Hier wordt opgemerkt dat pilot partijen alert dienen te zijn of onnodige verspreiding van gegevens plaatsvindt, dat dienstaanbieders geen gebruik mogen maken van de kennis dat een burger deelneemt aan de pilot, en dat een loket voor vragen of problemen ingericht dient te worden en dat het oplossen bij het loket/ de projectorganisatie dient te liggen en niet bij de pilotdeelnemer zelf. Ook dit zijn aspecten die met organisatorische afspraken afgedekt worden. De ICT-componenten zijn ook hier minder relevant.

Een aandachtspunt dat wel gaat over privacy in relatie tot de ICT-componenten en de verwerking van gegevens bij verschillende partijen betreft het beveiligen en het loggen van gegevens. De technische beveiliging is beschreven in het Technisch Ontwerp. [16] Er zijn standaarden voorgeschreven voor de technische inrichting en mechanismen voor versleuteling en uitwisseling van gegevens. Logging is ook

[53] Staatscourant 2015 nr. 37158, 29 oktober 2015, p.8.
[54] Het derde punt betrof de belegging van verantwoordelijkheid en is daarmee een organisatorische maatregel.

toegestaan op de servers van de leveranciers (Gemalto en Morpho). Het betreft dan technische logging, hoewel de scope daarvan niet expliciet bepaald is. Dat verdient wel de aanbeveling. Wel is vastgesteld dat deze logging na afloop van de pilots aantoonbaar verwijderd dient te worden van de servers.

De genoemde servers staan in respectievelijk Frankrijk en Finland, dus buiten Nederland, maar binnen de EU. Ook dat is toegestaan op basis van het Technisch Ontwerp. [16] De onderzoekers hebben echter niet nader kunnen toetsen welke gegevens daadwerkelijk tussen welke partijen of schakels worden uitgewisseld en in welke vorm. In het algemeen, maar zeker ook met het oog op grensoverschrijdende verwerkingen, verdient het aanbeveling dit te laten testen door de ADR. Dit kan plaatsvinden met inachtneming van het ICTU lessons learned rapport. Zorg voor goedgekeurde specificaties met meer detailniveau, op te leveren voor de start van het vervolgproject, o.a. gevoed door ervaringen uit het pilotproject en de pilotuitvoering. Besteed meer aandacht aan acceptatiecriteria (harde eisen) en evaluatieprocedures.

Bij de pilot met het eNIK is in de FAQ wel aangegeven dat privacy beschermd wordt. Specifiek wordt hier gewerkt met het principe van dataminimalisatie. Op de identiteitskaart staan alleen dezelfde gegevens als op de standaard identiteitskaart (naam, geboortedatum, BSN) en geen aanvullende gegevens.

Hoofdvraag 4: In welke mate zijn dienstaanbieders en andere betrokkenen duidelijk geïnformeerd over het doel van de pilot, de gegevens en het gebruik tijdens de pilot?

De dienstaanbieders en betrokkenen zijn niet of nauwelijks geïnformeerd over de verwerking van persoonsgegevens binnen de pilot en hoe daarmee omgegaan dient te worden. In het PIA rapport wordt opgemerkt dat er van uitgegaan wordt dat de verzamelingen van persoonsgegevens die tijdens de pilot ontstaan ten behoeve van de aanvraag, het aanmaken en de uitreiking van de publieke middelen na de pilot worden vernietigd. De deelnemers moeten aan het einde van de pilot wel de middelen terug inleveren bij de gemeente die de middelen heeft uitgegeven. De genoemde gegevens kunnen dan inderdaad vernietigd worden, behoudens eventuele wettelijke vereisten omtrent registratie van de uitgifte van een WID. Er wordt echter in de informatievoorziening richting deelnemers en dienstverleners (de gemeenten) niet gesproken over de te verwerken gegevens en de bewaartermijnen daarbij.[55] Ook in het Plan van Aanpak Pilots publieke eID-middelen zijn hier geen richtlijnen of vereisten over opgenomen. In de Instemmingsverklaring voor deelname aan de pilot met het eRijbewijs wordt wel aangegeven dat de verwerking van gegevens binnen de pilot plaatsvindt in overeenstemming met de Wbp.

Er zijn aan de dienstaanbieders brieven met instructies verspreid omtrent de pilots. In deze brieven wordt beschreven op welke wijze de uitgifte van de middelen plaatsvindt en welke zaken een pilot-deelnemer meekrijgt, zoals het WID of specimen, de kaartlezer en een informatiepakketje. Er is echter geen informatie opgenomen over het verwerken van gegevens gedurende de pilot. Ook is geen informatie opgenomen over wat er na de pilots met de gegevens gebeurt. Deze

[55] Zie bijvoorbeeld de informatiebrieven “Deelname aan pilot ‘Inloggen met een rijbewijs’ “ (Eindhoven) en “Deelname aan pilot ‘Inloggen met Nederlandse identiteitskaart’ “ en de Leaflet (Den Haag) en de verdere informatiebrieven en uitnodigingsbrieven zoals aan burgers verstuurd.

zullen echter (tenminste) deels bewaard blijven, aangezien het wel de uitgifte van een WID betreft (bij eNIK).

De dienstaanbieders naast de gemeenten zijn automatisch de partijen die hun website ontsluiten door middel van DigiD. Deze partijen zijn niet allen tot in detail geïnformeerd t.a.v. de het doel van de pilot. De middelen leveranciers (gemeenten) die deelnemen aan de pilot zijn ook niet voldoende geïnformeerd over het feit dat een code 30 wordt afgegeven door Logius en hun website dit aan moet kunnen ondanks dat Logius in de afgelopen anderhalf jaar regelmatig DidiD dienstaanbieders gewezen heeft op het feit dat code 30 als beveiligingsniveau mogelijk moet zijn[56]. Hierdoor zijn een aantal websites van dienstaanbieders niet toegankelijk. Het is onduidelijk welke logging daardoor ontstaat. Een site die niet bereikt wordt omdat het betrouwbaarheidsniveau code 30 niet verwerkt kan worden leidt immers niet tot een transactie.

Hoofdvraag 5: Zijn er issues opgetreden op het gebied van aansprakelijkheid bij de burger?

In de voorwaarden deelname pilot eRijbewijs zijn wel bepalingen opgenomen die vastleggen dat de deelnemer over een aansprakelijkheidsverzekering moet beschikken. Hoewel het niet verder is gespecificeerd lijkt hier gedoeld te worden op een aansprakelijkheidsverzekering voor (verkeers)ongevallen. De vraag uit de PIA lijkt meer te doelen op aansprakelijkheid voor fouten of onjuiste transacties waarbij het WID is gebruikt. Dergelijke issues zijn gedurende de onderzoeksperiode niet bekend geworden. Mocht een dergelijk issue zich voordoen, dan is de kans overigens ook groot dat zoiets zich niet op korte termijn manifesteert. Een onjuistheid moet leiden tot een probleem of conflict en vervolgens moet daarvoor ook de burger aansprakelijk gesteld worden. Dergelijke stappen vinden vaak niet binnen een korte tijd plaats.

Wel is vastgesteld dat in de Regeling voorzieningen GDI[57] geen bepalingen aangaande aansprakelijkheid zijn opgenomen. Deze Regeling is in de plaats gekomen van de gebruiksvoorwaarden DigiD. Voor de pilot met de eNIK zoals die in Den Haag plaatsvindt is in de Instemmingsverklaring[58] wel een bepaling over aansprakelijkheid opgenomen. In artikel 10 van de Instemmingsverklaring is bepaald dat met betrekking tot aansprakelijkheid en geschillenbeslechting in verband met de pilot en deze pilotvoorwaarden Nederlands recht van toepassing is. Dat betekent dat in de praktijk zal blijken of zich issues met betrekking tot deze aansprakelijkheid voordoen en hoe daarmee om wordt gegaan. Er is niet op voorhand een duidelijke stellingname over bij wie aansprakelijkheid zal liggen.

Voor de pilot eRijbewijs, zoals deze in Eindhoven loopt, is gekeken naar de brief die deelnemers aan de pilot ontvangen met de instructies en tevens naar de uitleg van de pilot op de DigiD website.[59] Ook bij deze pilot wordt gebruik gemaakt van een Instemmingsverklaring, de Instemmingsverklaring deelname aan de pilot elektronische specimen rijbewijzen. Deze Instemmingsverklaring bevat in artikel 8

[56] Gemeld tijdens de meeloopdag in Eindhoven.
[57] Staatscourant 2015-37158, Regeling voorzieningen GDI, 29 oktober 2015.
[58] Staatscourant 2016 nr. 2683, 20 januari 2016, Bijlage bij de Regeling Pilot Elektronische Nederlandse Identiteitskaart.
[59] https://www.digid.nl/over-digid/kaartlezer-pilot/

eenzelfde bepaling aangaande aansprakelijkheid en geschillen als de Instemmingsverklaring voor de pilot eNIK.

In de PIA werd aanbevolen de deelnemers geen sancties op te leggen indien achteraf een transactie met het pilotmiddel niet geslaagd blijkt. Over dergelijke afspraken hebben de onderzoekers geen documentatie gevonden waarin dit is vastgelegd.

4.3.3 Onderzoeksvragen met betrekking tot ervaringen

Voor leveranciers zal dit leiden tot een nadere specificatie en detaillering van de volgende hoofd- en deelvragen:

Aanvullende vraag: Reden voor deelname aan de pilot

Voor de formulering van het antwoord is er gebruik gemaakt van de volgende bronnen:

- Interview met RvIG
- Meeloopdag gemeente Eindhoven/interview met RDW

RvIG staat volledig achter de pilot. RvIG wil laten zien dat het kan en werkt in de pilot. RvIG geeft aan dat het niet is uit te leggen aan burgers dat ze nog steeds naar een loket moeten om diensten af te nemen. Soms moeten burgers ook nog eens naar verschillende loketten. Ook kunnen e-diensten veel besparingen opleveren.

Voor RDW geldt dat de pilot een betaalde opdracht is van BZK en dat het drukken van rijbewijzen en de bijbehorende administratie voeren behoren tot de kerntaken van het RDW. Voor het RDW is het voorzien in eRijbewijzen ook een ontwikkeling en stap in de toekomst en het deelnemen aan de pilot geeft de mogelijkheid ervaring op te doen met deze toekomstige dienstverlening en hier lering uit te trekken.

Hoofdvraag 9: Hoe ervaren de authenticatiediensten en leveranciers van het publieke middel de levering?

Voor de formulering van het antwoord is er gebruik gemaakt van de volgende bronnen:

- Interview met RvIG
- Meeloopdag gemeente Eindhoven/interview met RDW

Positieve ervaringen:

RvIG geeft aan dat de pilot in Den Haag erg positief is verlopen. Er zijn geen problemen ervaren. RvIG heeft alles zoveel mogelijk voor het echt gedaan; het totaalproces verloopt zoals dit altijd verloopt. De enige nieuwe zaken hierin zijn dat er een extra applet is aangebracht op het document en dat er gewerkt is met ‘extra runs’ (de data van de eNIKs is verzameld en de eNIKs worden tegelijkertijd geproduceerd). RvIG geeft aan dat de samenwerking tussen de partijen positief is verlopen. Er zijn in het project korte lijnen tussen RDW, RvIG en Logius.

RDW is zowel betrokken bij de pilot in Eindhoven als in Groningen. RDW geeft aan dat de pilot in Eindhoven is opgezet in nauwe samenwerking met RDW. Uitgangspunt is geweest om de gehanteerde processen van de pilot in Eindhoven

zoveel mogelijk één op één te kopiëren naar de gemeente Groningen. Ook het RDW is positief over de samenwerking met andere partijen in de pilot. De eRijbewijzen worden voor pilotdoeleinden per keer (pilot) gedrukt omdat het 'met de hand ingesteld moet worden' op dit moment. Bij een definitieve leverstraat zal dit uiteraard niet langer het geval zijn en verloopt het volledig geautomatiseerd. Deze afwijking van het gangbare proces geldt dus alleen tijdens de pilot en wordt bij definitieve invoering van het eRijbewijs verholpen met een aangepaste leverstraat.

Verbeter- en aandachtspunten
RvIG benoemt drie verbeter- en aandachtspunten:

- Ontbreken van user stories: het moet helder zijn wat er is ontworpen. Het is belangrijk om functioneel op te schrijven wat er gebeurt in het proces en op welk moment. User stories dienen bijvoorbeeld aan te geven: hoe de privacy van de burger wordt gegarandeerd en waar, wanneer welke info uit welke registers wordt gehaald. Op die manier kan het ontwerp worden getoetst; wordt er voldaan aan de voorwaarden die zijn gesteld? Er was echter slechts een beperkt aantal user stories beschikbaar. Wel waren er veel technische documenten, opgesteld door architecten.
- Ook bij de kaders van Idensys gaat het veel over techniek en ontbreken de user stories. De drie partijen – RDW, RvIG en Logius – hebben nu zelf interpretaties gemaakt. Dit was deels verfrissend omdat de partijen niet vastzaten aan een ontwerp. Het betekende wel dat er nog allerlei keuzes gemaakt moesten worden. Bij een structurele invoer moeten user stories worden opgesteld.
- Mix tussen beleid en uitvoering is soms lastig: zo wordt er bijvoorbeeld aangegeven dat er geen onomkeerbare beslissingen kunnen worden genomen. In de perceptie van RvIG worden die ook niet genomen; in de pilot worden zaken beproefd. In de perceptie van sommigen is dan echter het beleid al gezet.
- De politieke besluitvorming en doorlooptijd: voor de zomer zou het besluit moeten vallen. De planning is om voor 2017 te gaan uitrollen. Er is een aanbestedingstraject nodig en dat kost tijd.

Het RDW heeft geen verbeterpunten genoemd in verband met de pilot.

Hoofdvraag 10: Hoe ervaren de leveranciers het contact met de beheerorganisatie?

Voor de formulering van het antwoord is er gebruik gemaakt van de volgende bronnen:

- Interview met RvIG;
- Meeloopdag gemeente Eindhoven/interview met RDW.

RvIG, RDW en Logius zijn allen beheerorganisaties; alleen op een ander vlak. RvIG geeft aan dat er een goede samenwerking is geweest tussen RvIG, RDW en Logius. Tijdens de pilot is wel het inzicht gekomen dat er een 'system integrator' rol nodig is. Er is toen een projectleider aangesteld die over de keten heen beslissingen nam. De drie projectleiders van de afzonderlijke organisaties konden zich zo richten op hun eigen deel.

In de ervaring van RvIG poppen er altijd nieuwe vragen op tijdens de uitvoering. Een ontwerp kan niet in beton zijn gegoten. Zo is het soms nodig om het ontwerp te veranderen n.a.v. de uitwerking. De korte lijnen hebben erg geholpen om snel zaken te realiseren.

Het RDW heeft geen bijzonderheden in de samenwerking met de beheerorganisatie (Logius) genoemd die speciale aandacht behoeven. Deze samenwerking en het contact gedurende de pilot verloopt goed en de communicatie is veelal beperkt tot het uitwisselen van de white- en blacklist updates.

Hoofdvraag 11: Hoe ervaren gemeenten het aanvraag- en uitgifte proces van het publieke middel?

Deze hoofdvraag is opgedeeld in de volgende deelvragen:
Deelvraag 11a: Hoe ervaren gemeenten het aanvraagproces van het publieke middel?
Deelvraag 11b: Hoe ervaren gemeenten het uitgifteproces van het publieke middel?
Deelvraag 11c: In hoeverre verschilt het aanvraag- en uitgifteproces van het publieke middel met de huidige situatie?
Deelvraag 11d: Hoe worden eventuele verschillen ervaren door de gemeente en/of betrokken ambtenaren?
Deelvraag 11e: Hoe verloopt de communicatie over het publieke middel bij de gemeente?

Het aanvraag- en uitgifteproces van zowel het eRijbewijs als het eNIK zijn beschreven in hoofdstuk 3. Het aanvraag- en uitgifte proces gedurende de pilot. De bronnen gebruikt bij het beantwoorden van de onderstaande vragen zijn:

- Meeloopdag in Eindhoven tijdens welke de gemeente Eindhoven, Groningen, RDW, Logius en ICTU zijn geïnterviewd en baliemedewerker is geobserveerd en geïnterviewd tijdens het uitgeven van eRijbewijzen;
- Follow-up interview gemeente Groningen;
- Meeloopdag gemeente Den Haag.

Bevindingen deelvraag 11a: Hoe ervaren gemeenten het aanvraagproces van het publieke middel?

Gemeente Eindhoven:
Het aanvraag proces was geen onderdeel van de meeloopdag in Eindhoven (aangezien de aanvraag reeds plaats had gevonden). Tijdens de meeloopdag in Eindhoven is aangegeven dat het aanvraagproces niet wezenlijk verschilt van het normale proces, anders dan dat deelnemers specifiek uitgenodigd zijn deel te nemen aan de eRijbewijs pilot. Het aanvraagproces is verder verlopen zoals beschreven in paragraaf 3.6.5. Dit is goed verlopen, er waren geen problemen.

Gemeente Groningen:
In Groningen hebben de deelnemers deelgenomen aan de pilot op uitnodiging. Zie voor het verloop van dit proces paragraaf 3.6.5. In deze zin was er geen daadwerkelijk aanvraagproces zoals in Eindhoven maar hebben deelnemers via mail aangegeven een eRijbewijs te willen ontvangen en de benodigde gegevens

bijgesloten om deel te nemen aan de pilot. Ook dit aanvraagproces is zonder problemen verlopen.

Gemeente Den Haag:
De deelnemers dienen de volgende informatie mee te nemen naar de gemeente bij hun eerste afspraak:

- Alle in bezit zijnde reisdocumenten en een pasfoto;
- Euro 53,05 (deze kosten krijgen de deelnemers later terug);
- Instemmingsverklaring.

Medewerkers van de gemeente Den Haag geven aan dat het aanvraagproces zoals gebruikt in de pilot complexer is voor burgers dan het normale proces. Pilot deelnemers moeten vaker naar de gemeente komen in vergelijking tot het reguliere proces voor het aanvragen en ophalen van een NIK.

De eerste maandag van de proef waren er 35 van de 85 pilotdeelnemers die niet alle benodigde spullen (zoals pasfoto, geld en alle in bezit zijnde reisdocumenten) hadden meegenomen. Dit heeft geleid tot het opnieuw plannen van 115 afspraken volgens de projectleider. De gemeente Den Haag heeft toen een e-mail gestuurd met een toelichting over de materialen die deelnemers dienen mee te nemen naar de afspraak om een eNIK aan te vragen.

Er wordt ingeschat dat ongeveer 30% van de pilotdeelnemers niet alle benodigde documentatie meeneemt. Normaliter is dit ongeveer 10%. Veel deelnemers vergeten een ondertekende Instemmingsverklaring mee te nemen. Deze verklaring is de deelnemers per e-mail gestuurd. Als een deelnemer de verklaring heeft vergeten mee te nemen wordt de verklaring ter plekke door de medewerker geprint en kan de deelnemer deze alsnog ondertekenen.

De gemeente Den Haag wil graag een antwoord hebben op de vraag waarom deelnemers niet alle benodigde informatie meenemen en de wijze waarop dit middels de juiste communicatie kan worden opgelost. De gemeente Den Haag geeft aan dat burgers een bepaalde perceptie lijken te hebben die ervoor zorgt dat zij niet alle benodigde documentatie (bijvoorbeeld ‘Voor een e-kaart hoef ik toch geen foto mee te nemen’) en geld meenemen.

Een aantal voorbeelden van lessen die de gemeente heeft geleerd zijn:

- Het alleen op afspraak werken (voor aanvraag en uitgifte van eNIK) betekent een inperking van de flexibiliteit in het verstrekken van eNIKs gedurende de pilot periode. Meer vrijheid in het moment van aanvragen en afhalen (zonder afspraak) geeft de gemeente meer ruimte om drukte op te vangen tijden piekbelastingen (bijvoorbeeld in verband met het referendum dat werd gehouden tijdens de pilot waar eveneens medewerkers voor ingepland moeten worden).
- Een pilot vraagt om ruimte voor flexibiliteit. De periode waarin deelnemers zich kunnen opgeven voor deelname aan de pilot is verlengd om extra deelnemers te krijgen. Organisatorisch is dit lastig. Zo vraagt onder meer het referendum ook om capaciteit van medewerkers.

Gemeente Groningen en gemeente Eindhoven
Het bovenstaande proces wijkt op een aantal punten af van het reguliere proces voor het aanvragen en uitgeven van een rijbewijs en is voor de pilot niet geïntegreerd in de bestaande backoffice systemen van de gemeenten. In het reguliere proces:

- Kent men twee fysieke identificatiemomenten (tijdens aanvraag en uitgifte). In de eRijbewijs pilot in Groningen kent men slechts één identificatiemoment.
- Worden geen cardreaders en instructies/uitleg voor installatie en activatie bij het normale rijbewijs gegeven.
- Worden afgehaalde rijbewijzen niet gecommuniceerd naar het RDW om vervolgens door het RDW in communicatie met Logius op de white list geplaatst te worden.
- Worden eRijbewijzen niet door Logius op de white list geplaatst.
- Stuurt het RDW geen pin-, puk- en can-codes aan burgers.

Aan het einde van de pilot worden alle eRijbewijzen geblokkeerd en wordt de BSN-koppeling teniet gedaan. Hoe de eRijbewijzen weer ingeleverd worden is een proces dat nog niet concreet is vormgegeven anders dan dat een pilot deelnemer voor het terugbrengen van het eRijbewijs een vergoeding krijgt mits er is voldaan aan het minimum gebruik van het eRijbewijs als inlog middel voor DigiD.

Door zowel Groningen als Eindhoven wordt de aanvraag en de uitreiking van het eRijbewijs niet als heel erg belastend of afwijkend ervaren. Er zijn enkele additionele handelingen nodig boven op het bestaande proces. De doorlooptijd neemt toe als gevolg van de uitleg over het gebruik van de middelen en de uitreiking van de extra documentatie in Groningen. Eindhoven heeft aangegeven geen effect te bemerken op de doorlooptijd van afhandeling van aanvragen. Eindhoven merkt wel op dat er gewerkt wordt met specimen-documenten waarvoor bijvoorbeeld geen foto hoeft te worden gecontroleerd en geen registratie plaatsvindt in het reguliere systeem.

Gemeente Den Haag
De uitreiking van het eNIK verloopt wel volgens de reguliere procedure en is geïntegreerd in de backoffice processen voor het aanvragen van een NIK van de gemeente. Echter ook hier worden normaliter geen bestanden aan Morpho gestuurd ten aanzien van te activeren kaarten. In Den Haag is het aanvraag proces als meer belastend ervaren omdat hier veel afspraken opnieuw ingepland moesten worden en deze pieken moeilijker op te vangen waren. Hetzelfde geldt voor het uitgifte proces. Normaliter kan men een NIK zonder afspraak afhalen aan de balie op gezette tijden.

Bevindingen deelvraag 11b: Hoe ervaren gemeenten het uitgifteproces van het publieke middel?

Gemeente Eindhoven:
Pilot deelnemers vergeten vaak een paspoort of identiteitskaart mee te nemen naast het rijbewijs. In de instructies die vooraf gegeven zijn, wordt ook niet expliciet vermeld dat beide nodig zijn voor het afhalen van het eRijbewijs. Volgens de baliemedewerkers en ICTU is het aantal keren dat dit fout gaat echter gelijk aan het aantal keer dat dit in het reguliere proces gebeurt. Ook blijkt uit gesprekken met de balie medewerker(s) dat de doorlooptijd voor het uitgeven van een eRijbewijs

ongeveer hetzelfde is als bij een normale uitgave van het rijbewijs ondanks de extra informatie en uitleg die gegeven werd.

Gemeente Groningen:
Het uitgifteproces is beschreven in hoofdstuk 3. Ten aanzien van het uitgifteproces in Groningen zijn er geen problemen of moeilijkheden ervaren, dit is soepel verlopen. Deelnemers konden zonder afspraak het eRijbewijs afhalen tussen 12.00 en 17.00 (di t/m vr) of tussen 13.00 uur en 17.00 uur (ma). Het merendeel van de deelnemers heeft het eRijbewijs in de eerste week van de pilot in Groningen opgehaald.

Gemeente Den Haag:
Bij het uitgifteproces worden geen problemen ervaren. Deelnemers dienen de volgende zaken mee te nemen:
- In bezit zijnde reisdocumenten;
- Afhaalbewijs: dit is vergelijkbaar met de huidige situatie. Als een deelnemer dit niet heeft meegenomen dan wordt een kopie gemaakt van de eNIK en dient de deelnemer deze kopie te ondertekenen.

Bij alle gemeenten is er geen daadwerkelijke toename in de duur van afspraken tijdens afhalen/uitgifte. Wel worden meer zaken vergeten in Den Haag waardoor er veel afspraken opnieuw gepland moesten worden. Een aantal van de deelnemers is vervolgens niet meer naar de opnieuw geplande afspraak gekomen.

Bevindingen deelvraag 11c: In hoeverre verschilt het aanvraag- en uitgifteproces van het publieke middel met de huidige situatie?

Gemeente Eindhoven:
De aanvraag- en uitgifte van het eRijbewijs verschilt met de huidige situatie in de zin van dat het een pilot situatie betreft waarin een specimen uitgegeven werd. Het aanvraag proces is anders verlopen (zonder fysiek identificatiemoment), het uitgifte proces is volgens het normale proces verlopen, met een fysiek identificatie moment. Daarnaast dienen de uitgereikte kaarten gecommuniceerd te worden met het RDW, wat in het gewone proces niet nodig is.

Gemeente Groningen:
De aanvraag- en uitgifte van het eRijbewijs verschilt met de huidige situatie in de zin van dat het een pilot situatie betreft waarin een specimen uitgegeven werd. De aanvraag verschilt van de normale aanvraag in de zin van dat deelnemers uitgenodigd zijn. De deelnemers hebben hun akkoord om deel te nemen aan de pilot en de gegevens middels mail ingestuurd. Het uitgifte proces is verlopen zoals dit normaal gesproken ook verloopt, met een face 2 face controlemoment in dit proces. Daarnaast zijn uitgegeven kaarten gecommuniceerd met het RDW voor activatie.

Gemeente Den Haag:
De gemeente Den Haag geeft aan dat de aanvraag vrijwel hetzelfde is als het reguliere proces. Er wordt geschat dat slechts 5% afwijkend is van het reguliere proces.

Het aanvraag- en uitgifteproces is afwijkend t.o.v. de huidige situatie op de volgende punten:

- Er wordt onderscheid gemaakt tussen een normale aanvraag en een aanvraag voor eNIK. De kaartjes voor de aanvraag van een eNIK hebben een roze balkje. Op deze kaartjes wordt de pasfoto geplakt en deze worden gescand. Indien een medewerker per ongeluk het kaartje met het roze balkje gebruikt voor de aanvraag van een NIK/paspoort dan wordt dit niet gedetecteerd door het systeem.
- Het systeem voor het produceren van eNIKs is anders dan voor de overige identiteitsdocumenten. In het reguliere proces scant een medewerker de aanvragen en stuurt deze door. Tijdens de pilot worden de aanvragen voor eNIKs gescand en in aparte ‘batches’ naar Morpho verzonden. (Deze aanvragen gaan dus niet mee in het reguliere proces). Morpho heeft een reeks met de nummers 1 tot 500 afgegeven voor de pilot. Aan het eind van de dag wordt een overzichtslijstje in Excel gemaakt en naar Morpho gestuurd. Voorbeeld: ‘Kaarten 81 en 82 zijn gebruikt en nummer 83 is misgegaan en niet gebruikt’.
- Het ophalen van een eNIK is anders dan het ophalen van een NIK. Normaliter kunnen burgers zonder afspraak het document ophalen bij de informatiebalie. Nu wordt er een afspraak gemaakt met deelnemers om de eNIK op te halen. Deze afspraak wordt meteen gemaakt als de deelnemer zijn/haar eNIK komt aanvragen.

Bevindingen deelvraag 11d: Hoe worden eventuele verschillen ervaren door de gemeente en/of betrokken ambtenaren?

Gemeente Eindhoven:
Uit de feedback van baliemedewerkers blijkt dat nauwelijks verschillen worden ervaren. De baliemedewerkers hebben allen een training gehad (zoals bij iedere deelnemende gemeente). De balieplanning was van tevoren afgestemd en gecommuniceerd. Het uitreiken is goed en volgens plan verlopen. Er waren wat extra handelingen of net iets andere handelingen uit te voeren maar dit is goed en efficiënt aangepakt en opgevangen en heeft niet geleid tot problemen of tijdsverlies. De gemiddelde duur voor het uitreiken van een eRijbewijs werd door baliemedewerkers op ongeveer zeven minuten geschat.

Gemeente Groningen:
Op basis van de feedback van de projectleider kan geconcludeerd worden dat ook in Groningen tijdens het aanvraag- en uitgifte proces de medewerkers geen problemen hebben ervaren. De extra handelingen zijn op dezelfde manier ondersteund als in Eindhoven (training) en hebben eveneens tot een efficiënt proces geleid zonder effecten op bijvoorbeeld doorlooptijden. Ook hier zijn eventuele veranderingen in het proces als positief ervaren en hebben niet tot problemen geleid.

Gemeente Den Haag:
De baliemedewerkers die de aanvragen en uitgifte van de eNIK verzorgen hebben twee trainingsdagen gehad; zogeheten ‘simulatiedagen’ waarbij er ook rollenspellen zijn gedaan om te oefenen met vragen van burgers. De Gemeente Den Haag geeft aan dat deze dagen waardevol zijn geweest en dat baliemedewerkers het uitgifteproces nu goed kunnen uitvoeren.

Er zijn twee aparte balies (balies 7 en 8) speciaal gereserveerd voor de pilot. De openingstijden zijn conform de reguliere openingstijden waarbij op afspraak wordt gewerkt, n.l. maandag van 12.00 uur tot 20.00 uur en de overige dagen (di-vr) van 11.00 uur tot 17.00 uur. Dit brengt extra belasting mee voor de medewerkers. Collega's hebben het soms heel druk bij de andere balies (of juist rustig) maar er kan dan niet flexibel over en weer worden ingesprongen om burgers te helpen.

Voor de aanvraag van de eNIK is nu ook tien minuten gerekend. Normaliter is daar 5,5 minuut voor gerekend. Er is nu ongeveer tien minuten gerekend voor uitgifte van de eNIK tijdens de pilot vanwege het uitreiken van een additionele digitale identiteit plus bijbehorende middelen (kaartlezer, handleidingen) en het verstrekken van uitleg hierover. Normaal is dit uitgifte moment niet getimed (de uitgifte gebeurt normaliter via de informatiebalie zonder afspraak; zie de toelichting bij vraag 11c).

Er wordt verwacht dat er bij de definitieve situatie landelijk veel meer aandacht is voor de eNIK (bijvoorbeeld via grootschalige campagnes). De informatiestroom richting burgers ligt dan ook buiten de gemeente.

Bevindingen deelvraag 11e: Hoe verloopt de communicatie over het publieke middel bij de gemeente?

Gemeente Eindhoven en gemeente Groningen
Tijdens de aanvraag en uitgifte zijn er geen vragen geweest van pilotdeelnemers. De baliemedewerkers hebben hierin weinig verandering gezien. Het informatie pakket dat aan deelnemers werd overhandigd met een korte toelichting van de baliemedewerker sprak voor zich. Mochten baliemedewerkers vragen hebben dan konden zij direct terecht bij de projectleiding (ook met vragen van deelnemers waar ze niet direct een antwoord op hadden). In de aanvraag en uitgifte zijn op dit gebied geen bijzonderheden te melden.

Deelnemers die problemen ondervonden of vragen hadden tijdens het activeren van de kaartlezers/kaarten of het gebruik konden telefonisch of via e-mail (afhankelijk van de gemeente, zie escalatieprocedure in hoofdstuk 3) hulp vragen bij de gemeente. De meeste vragen zijn direct beantwoord, ofwel door baliemedewerkers ofwel door de projectleider. Technische vragen zijn doorgestuurd naar Logius en daar verder afgehandeld. De gemeenten geven aan dat dit is gebeurd naar tevredenheid van de pilotdeelnemers (in het overgrote deel van de vragen/problemen).

Medewerkers die vragen hadden ten aanzien van het proces of inhoudelijk ten aanzien van de kaartlezer/kaart konden terecht met hun vragen bij projectleider. Dit is echter nauwelijks aan de orde geweest.

De communicatie tussen de gemeente en RDW is uitstekend geweest en heeft met name bestaan uit het doorgeven van de activeren kaarten en een moment van fysieke uitwisseling/overdracht van de kaarten en kaartlezers aan de gemeente. Ook op dit gebied hebben zich geen problemen voorgedaan.

Gemeente Den Haag:
Er zijn door de gemeente Den Haag geen knelpunten genoemd in de communicatie over het publieke middel. Deelnemers hebben de volgende communicatie uitingen

ontvangen: brief met uitnodiging en toelichting, leaflet, info op de website, FAQ, mails met toelichting over de pilot en mogelijkheden vragen telefonisch (14070) en per mail te stellen. Wel is gebleken dat pilotdeelnemers niet altijd de benodigde documenten en geld meenamen naar de afspraak voor de aanvraag van de eNIK bij de gemeente (zie de toelichting bij vraag 11a).

Hoofdvraag 12: Hoe gaan gemeenten om met eventuele problemen van burgers en eigen vragen?

Deze hoofdvraag is opgedeeld in de volgende deelvragen:
Deelvraag 12a: In welke mate melden zich deelnemers met problemen bij gemeenten?
Deelvraag 12b: Hoe gaan gemeenten om met vragen, problemen en klachten?
Deelvraag 12c: Hoe gaan gemeenten om met vragen uit de eigen organisatie?

In de escalatieprocedure (hoofdstuk 3) is beschreven hoe gemeenten omgaan met vragen van burgers. Hierboven is kort beschreven dat het omgaan met vragen vanuit medewerkers goed is verlopen en nauwelijks aan de orde is geweest.

Vragen vanuit medewerkers bij de gemeente zijn opgelost door de projectleider zoals reeds aangegeven, is dit nauwelijks aan de orde geweest.

De onderstaande vragen zijn beantwoord op basis van:
- Meeloopdag Eindhoven
- Meeloopdag Den Haag
- Interview gemeente Groningen
- De escalatieprocedure
- Helpdesk informatie middels mail aangeleverd door de gemeenten Eindhoven en Den Haag.

Bevindingen deelvraag 12a: In welke mate melden zich deelnemers met problemen bij gemeenten?

De escalatieprocedure beschreven in hoofdstuk 3 voor de pilot Publiek Middel geeft aan hoe er met vragen van deelnemers omgegaan wordt en bij welke partijen men terecht kan met specifieke vragen.

Via mail binnengekomen vragen zijn geregistreerd en geanalyseerd. De telefonisch beantwoorde vragen zijn niet geregistreerd, derhalve heeft TNO daar geen inzicht in. Vragen gesteld door burgers in verband met het activeren en gebruiken van het middel zijn reeds behandeld in vraag 6. Overige vragen die bij de gemeenten binnen zijn gekomen via e-mail betreffen:
- Totaal: 49 deelnemers (42 eNIK, 7 eRijbewijs): Afspraak vergeten/nieuwe afspraak maken/verzetten.
- Totaal: 46 deelnemers (17 eNIK, 29 eRijbewijs): Inloggen bij bepaalde dienstaanbieders lukt niet (code 30) of waar kun je inloggen?
- Totaal: 28 deelnemers (25 eNIK, 3 eRijbewijs): Afmelden voor pilot/neem niet langer deel.
- Totaal: 6 deelnemers (eRijbewijs): waar blijft de evaluatie?
- Totaal: 5 deelnemers (4 eNIK, 1 eRijbewijs): Gegevens wijzigen vanwege verhuizen.

- Diversen: procedureel, vordering pilot, kaart kwijt (eRijbewijs); aanvraag op andere locatie, het was toch gratis, etc. (eNIK)

De gemeenten geven aan dat zij alle bovenstaande vragen naar behoren hebben opgelost volgens procedures vastgesteld binnen de pilot.

Naast de technisch gerelateerde vragen geadresseerd in hoofdvraag 6 valt op dat de meeste vragen van deelnemers afspraken omtrent het aanvragen of afhalen van een document betreffen. Deze categorie vragen wordt gevolgd door vragen over het niet kunnen bereiken van websites van bepaalde dienstaanbieders.

Bevindingen deelvraag 12b: Hoe gaan gemeenten om met vragen, problemen en klachten?

De escalatieprocedure beschreven in hoofdstuk 3 geeft aan hoe er met vragen, problemen en klachten wordt omgegaan. De inhoudelijke vragen en problemen - voor zover beschikbaar en geregistreerd tijdens de pilot - zijn hierboven beschreven. De projectleiders geven aan dat alle vragen/problemen naar behoren zijn beantwoord/opgelost. Sommige technische problemen ten aanzien van de installatie, het activeren en gebruik konden tijdens de pilot echter niet opgelost worden. In deze gevallen (een zeer beperkt aantal) is bijvoorbeeld de installatie uiteindelijk niet gerealiseerd.

Bevindingen deelvraag 12c: Hoe gaan gemeenten om met vragen uit de eigen organisatie?

Baliemedewerkers van iedere gemeente zijn opgeleid voor de aanvraag en uitgifte van de middelen tijdens de pilot. Daarnaast worden ze ondersteund door Excel dashboards waarin informatie over de pilot is opgenomen en de stappen die genomen moeten worden in het proces staan uitgelegd. Het dashboard bevat eveneens koppelingen naar benodigde documenten. Eén van deze documenten is de instemmingsverklaringen die deelnemers soms vergeten mee te nemen en die ter plaatse nog geprint en getekend kunnen worden. Het is een zeer overzichtelijk proces en de ervaringen van de projectleiders is dat medewerkers geen vragen hadden die niet direct beantwoord konden worden in het begin van de pilot. Later in het traject zijn er geen aanvullende vragen geweest.

Hoofdvraag 13: Welke aandachtspunten zijn er volgens de gemeente op basis van de ervaringen met de proef?

Deze hoofdvraag is opgedeeld in de volgende deelvragen:
Deelvraag 13a: Welke aandachtspunten zijn er volgens de gemeenten bij een eventuele verdere uitrol van de pilot naar andere gemeenten?
Deelvraag 13b: In hoeverre denkt de gemeente dat het publieke middel en de techniek toestaan om meer diensten te digitaliseren op termijn?

Deze vragen zijn beantwoord op basis van:
- Meeloopdag Eindhoven;
- Meeloopdag Den Haag;
- Interview gemeente Groningen.

Niet alle dienstaanbieder sites die DigiD ondersteunen of gebruiken[60] geven toegang middels het publieke middel. Dit komt dan doordat het publieke middel een hoger beveiligingsniveau afgeeft dan wat de dienstaanbieder op de site ondersteunt. Hieronder vallen ook gemeenten zoals de gemeente Groningen. De ervaring van de gemeente Groningen is dat het enigszins raar is een middel aan te bieden voor inloggen bij publieke instanties terwijl dit middel bij de eigen gemeente niet werkt. Dit is een probleem wat echter later opgelost gaat worden.

De gemeente Groningen geeft daarnaast aan dat - mocht het eRijbewijs als publiek middel beschikbaar worden gesteld - het aantal af te halen rijbewijzen per week dermate groot zal zijn dat er rekening moet worden gehouden met de opslag van middelen (kaartlezers).

Het door ontwikkelen van het middel op een manier waarbij een kaartlezer niet langer is vereist (bijv. via NFC van mobiele telefoons) kan een hele aantrekkelijke optie zijn en mogelijk tevens een oplossing voor de installatieproblemen van de benodigde plug-in.

Bevindingen deelvraag 13a: Welke aandachtspunten zijn er volgens de gemeenten bij een eventuele verdere uitrol van de pilot naar andere gemeenten?

De gemeenten Eindhoven en Groningen hebben geen specifieke aandachtspunten genoemd voor verdere uitrol bij andere gemeenten. Bij deze gemeenten is het proces voor aanvraag en uitgifte goed en zonder problemen verlopen. Het betreft uiteraard wel een pilot proces en de uitreiking van een specimen bij deze gemeenten. Bij het uitreiken van een officieel document (in plaats van een specimen) zal er rekening moeten worden gehouden met zaken zoals verlies en hoe dit op te lossen.

Gemeente Den Haag
De gemeente geeft aan dat een aantal processen nu niet zijn getest. Deze zouden bij een verdere uitrol naar andere gemeenten wel moeten worden getest:

- Revocatieproces: De koppeling tussen eNIK en DigiD kan worden aan- en uitgezet. Het certificaat kan echter niet worden ingetrokken; hier is geen proces voor. Als een deelnemer zijn/haar eNIK verliest of deze wordt gestolen dan maakt de deelnemer een afspraak met de gemeente Den Haag om een verklaring van vermissing in te vullen. De gemeente registreert de tijdelijke identiteitskaart dan als vermist. De deelnemer kan dan ook direct een nieuwe identiteitskaart aanvragen. De deelnemer krijgt een nieuwe identiteitskaart, maar geen tijdelijke identiteitskaart.
- Proces indien burgers geen DigiD hebben: een criterium voor deelname aan de pilot is dat de burger beschikt over een DigiD. Voor een structurele invoer van de eNIK moet het proces worden gedefinieerd voor als iemand nog geen DigiD heeft.

Bij een verdere uitrol van de pilot naar andere gemeentes blijft een aandachtspunt het vaststellen van de identiteit van een persoon. Indien de pilot grootschaliger wordt, betekent dit dat meer mensen door het registratieproces heen moeten en

[60] https://www.digid.nl/over-digid/wie-doen-mee/

wordt de kans groter dat er iemand tussen zit die probeert te frauderen. Er zijn nu 3000 mensen die een dubbele identiteit hebben. In sommige gemeenten zoals Scheveningen zijn relatief veel mensen met dezelfde naam. Ook komt het voor dat mensen bijvoorbeeld opgeven dat hun geboortedatum 01-01-1950 is omdat ze hun echte geboortedatum niet weten. Of dat mensen hun kinderen twee jaar jonger opgeven, zodat ze nog naar de basisschool kunnen. Deze problemen spelen echter altijd en zijn niet direct uniek voor de pilot.

Bevindingen deelvraag 13b: In hoeverre denkt de gemeente dat het publieke middel en de techniek toestaan om meer diensten te digitaliseren op termijn?

Alle gemeenten geven aan dat er een behoefte bestaat te digitaliseren wat gedigitaliseerd kan worden in de dienstverlening:

- Dit vergroot de flexibiliteit in dienstverlening (bijv. openingstijden en meer ruimte voor afspraken voor zaken die daadwerkelijk fysiek afgehandeld moeten worden).
- Dit werkt in het voordeel van gemeenten; vermindering van de effort die geleverd moet worden in de dienstverlening.

Een hoog betrouwbaarheidsniveau is voor bepaalde vormen van digitale dienstverlening een vereiste (hoger dan het niveau geleverd door DidiD) en het publieke middel maakt een uitbreiding van de digitale dienstverlening mogelijk in deze zin. De gemeenten zien mogelijkheden om dit te realiseren op termijn. Sommige zaken zullen echter niet gedigitaliseerd kunnen worden. Bijvoorbeeld het aanvragen van documenten waarbij een fysiek identificatie moment is vereist, de aangifte van de geboorte van een kind, etc. Hiervoor kan echter wel meer flexibiliteit en ruimte gecreëerd worden door andere diensten wel te digitaliseren.

5 Conclusies en aandachtspunten

Noot: de in dit hoofdstuk opgenomen conclusies en aandachtspunten zijn opgedeeld in vier groepen: ‘algemeen’, ‘techniek’, ‘privacy’ en ‘ervaringen’.

5.1 Conclusies

Op grond van het in dit rapport beschreven onderzoek en de antwoorden op de gestelde onderzoeksvragen, concluderen de onderzoekers het volgende.

5.1.1 Algemeen

In dit rapport zijn de door de opdrachtgever aan TNO voorgelegde vragen beantwoord. Bij enkele vragen, met name op het gebied van techniek en privacy, geldt dat de onderbouwing niet gebaseerd kon worden op een feitelijke toetsing van de techniek door TNO danwel op auditrapporten waaruit blijkt op basis waarvan middelen en implementaties zijn getoetst. Wanneer in die gevallen door betrokkenen of eindverantwoordelijken is verklaard dat aan de vereisten uit de stelsels is voldaan, dan heeft TNO dat met bronvermelding opgenomen in de beantwoording van de betreffende vraag.

Gedurende het onderzoek is duidelijk geworden dat de afzonderlijke middelen van de multimiddelenstrategie in de praktijk technisch werken. Verschillende middelen konden worden gebruikt om bij dienstaanbieders in te loggen, ook via de verschillende stelsels (Publiek Middel, Idensys en iDIN). Deze stelsels bleken naast elkaar te werken en bieden burgers dus de keus om een type middel te kiezen dat zij prefereren. De pilots worden echter in relatieve onafhankelijkheid van elkaar uitgevoerd. De kennisdeling en dus het leerproces tussen pilots blijft daardoor beperkt. Door de pilots in hun onderlinge samenhang te bekijken kan er bepaald worden welke (combinatie van) oplossingen het meest geschikt is om voortgang te boeken op het gebied van elektronische toegangsdiensten in het publieke (BSN-) domein en ten aanzien van de beoogde multimiddelenstrategie.

Bij de pilots in het BSN-domein zijn veel partijen betrokkenen. Er bleken bij partijen verschillende beelden te bestaan over wat een pilot precies inhoudt. Voorbeelden van verschillende percepties zijn: het ophalen van gebruikerservaringen, het beproeven van het hele stelsel, of het beproeven van processen van de aanvraag en uitgifte van middelen. De verschillende beelden kunnen ertoe leiden dat er ook verschillende beelden ontstaan over wat er gemeten dient te worden tijdens de pilot. Bovendien moeten pilots in ketens bezien worden, omdat het ‘live’ gaan van een middel weinig betekenis heeft indien er nog niet mee ingelogd kan worden bij een dienstaanbieder. Zaken als performance dienen ‘over een keten heen’ gemeten te worden, omdat een storing op één plaats tot gevolg heeft dat de keten onderbroken is waardoor een middel of dienst dus mogelijk niet werkt.

In het uitgevoerde onderzoek zijn 55 onderzoeksvragen behandeld. Om te kunnen bepalen in hoeverre de bevindingen bij deze vragen voldoen aan de verwachtingen en eisen zijn er vooraf opgestelde criteria nodig, met hun normering. Deze criteria ontbraken in de huidige onderzoeksopzet; ze zouden in een eventueel vervolg bij voorkeur op voorhand vastgesteld moeten worden.

5.1.2 Techniek

Met betrekking tot de technische aspecten van de pilots concludeert TNO het volgende:

- TNO heeft enkele middelen zelf uitgeprobeerd. Het betrof de middelen Digidentity, iDIN ING, iDIN Rabobank en eRijbewijs. Voor deze middelen is op basis van eigen onderzoek vastgesteld dat ze succesvol kunnen worden gebruikt om in te loggen bij websites van dienstaanbieders. Andere middelen zijn niet door TNO zelf geprobeerd maar waren wel onderdeel van dit onderzoek.

- Het inlogproces van de uitgeprobeerde middelen Digidentity, iDIN ING, iDIN Rabobank en eRijbewijs werkte in de test van TNO technisch goed en vlot.

- Bij het uitproberen van Digidentity en iDIN ING op de website van de Belastingdienst Aangifte Inkomstenbelasting komt een eindgebruiker met beide middelen op de correcte gebruikerspagina uit. Bij het uitproberen van eRijbewijs op de DigiD-website komt een eindgebruiker op dezelfde gebruikerspagina's uit als wanneer hij met zijn reguliere DigiD zou hebben ingelogd.

- Uit de ontvangen rapportages bleek dat er voor de verschillende pilots iedere dag eindgebruikers hebben ingelogd, met verschillende middelen. Hieruit concludeert TNO dat de benodigde technische infrastructuur van de betrokken partijen elke dag beschikbaar is geweest. Er zijn echter wel discrepanties tussen het aantal geslaagde authenticaties vanuit het perspectief van het BSNk en het aantal succesvolle logins op sites van dienstaanbieders.

Bovenstaande conclusies zijn gebaseerd op een (beperkte[61]) steekproef zoals door TNO uitgevoerd in de maanden maart en april 2016, en op de door de bij de pilots betrokken partijen aangeleverde rapportages.

5.1.3 Privacy

Met betrekking tot de borging van de privacy binnen de pilots concludeert TNO:

- Voor alle drie pilots zijn PIA's uitgevoerd: bij Idensys en Publiek Middel vanuit de overheid op stelselniveau, en bij iDIN hebben de individuele banken een PIA uit moeten voeren om toe te kunnen treden tot het iDIN-stelsel.

- Voor de private middelen van Idensys en iDIN heeft een eindverantwoordelijke instantie (respectievelijk de minister van EZ en de Betaalvereniging Nederland (BVN)) verklaard dat aan de privacy-vereisten van de respectievelijke stelsels is voldaan.

- Er zijn nadere mitigerende maatregelen geïdentificeerd door de ketenpartners, die geïmplementeerd dienen te worden voor een brede uitrol na de pilotfase.

[61] TNO heeft bijvoorbeeld niet zelf elke dag van de onderzoeksperiode zelf geprobeerd in te loggen met de verschillende middelen, maar dat op een aantal momenten geprobeerd en getest.

- Communicatie vereist over gegevensverwerkingen nog veel aandacht, zowel richting burgers als tussen betrokken partijen onderling. Afspraken zijn wel vastgelegd in de normenkaders, maar vormen nog geen vanzelfsprekendheid voor alle betrokkenen.

De in dit onderzoek voorgelegde vragen waren hoofdzakelijk toegespitst op privacy in de zin van gegevensbescherming. Het voldoen aan de regelgeving, in het bijzonder de Wet bescherming persoonsgegevens (Wbp), stond daarbij centraal. Ook de PIA Idensys en het privacy document met interbancaire uitgangspunten voor iDIN zijn vanuit dat gezichtspunt opgesteld. Het is gedurende het onderzoek duidelijk geworden dat privacy als een van de hoekstenen voor een goede en duurzame inrichting van de verschillende stelsels wordt gezien, alsook voor het bieden van elektronische toegangsdiensten in het algemeen. Algemeen wordt erkend dat een goede borging van de privacy, in samenhang met de veiligheid van de stelsels, essentieel is voor het vertrouwen van burgers in de geboden middelen. De kaders van de Wbp en de specifieke uitwerking daarvan voor de verschillende stelsels is daarom cruciaal.

Vanuit een breder privacy-perspectief is echter ook de borging van privacy van belang. In het kader van de stelsels en de noodzaak van vertrouwen in die stelsels leidt dat volgens TNO tot een betere benadering van het onderwerp. Op het gebied van borging, ondersteund door een heldere governance van de stelsels en gegevens, blijken echter nog gebreken te bestaan. Met name is gebleken dat er in de verschillende stelsels vaak geen goed beeld is van welke partij (dienstverlener, middelenleverancier, authenticatiedienst, BSNk) welke gegevens tot zijn beschikking heeft of kan hebben, en welke data gelogd worden door welke partijen. Op deze aspecten werd ook ingegaan in de PIA Idensys. Voor Elektronische Toegangsdiensten (ETD) is in het afsprakenstelsel vermeld welke cijfers maandelijks aangeleverd moeten worden en door wie (zie het Operationeel Handboek), dus dat is belegd. En in het hoofdstuk informatiebeveiligingsbeleid is vastgelegd welke partij wat moet *loggen*.)

De uitvraag van de onderzoekers naar *logging* heeft echter tot de conclusie geleid dat hier in de praktijk nog onduidelijkheid over bestaat. In bepaalde gevallen was onduidelijk welke partij gegevens kon leveren. Sommige partijen, zoals de beheersorganisatie, kunnen alleen op generiek pilotniveau loggegevens aanleveren, dus niet per middel. Ook bleek dat bij de pilot met het eRijbewijs *log*-gegevens werden bijgehouden door Gemalto, de leverancier van de kaartlezer. Hoewel dit volgens het Technisch Ontwerp [16] voor de pilot Publiek Middel is toegestaan, verdient het aanbeveling duidelijke afspraken te maken over welke *logging* van welke gegevens bij welke partij kan en mag plaatsvinden. Tevens dienen de *loggings* van bewaartermijnen te worden voorzien.

Een beperking binnen dit onderzoek was dat privacy-borging alleen beoordeeld kon worden op basis van documentatie en normenkaders. Een controle op technische implementatie van mitigerende maatregelen en de verdere technische inrichting ervan viel niet binnen de mogelijkheden van TNO. De conclusies aangaande privacy dienen dan ook met deze kanttekening gelezen te worden. Bovendien kon niet beoordeeld worden of de technische inregeling daadwerkelijk de beste privacy-borging oplevert. Het is mogelijk dat er betere oplossingen voorhanden zijn. Een concreet aandachtspunt is in ieder geval om te streven naar data-minimalisatie,

vooral ten aanzien van de verwerking van het BSN, het versturen van het BSN over de lijn, en het bieden van controlemogelijkheden voor eindgebruikers.

5.1.4 Ervaringen

Algemeen kan ten aanzien van de ervaringen van gebruikers in de pilots het volgende worden geconcludeerd:

- Er bij de partijen die bij de pilots zijn betrokken verschillen in perceptie bestaan ten aanzien van de pilots; het betreft bijvoorbeeld de doelstelling en reikwijdte ervan.

- Verschillende leveranciers (bij Idensys) en dienstaanbieders (bij iDIN: 'acceptanten') aangaven dat het lastig was om aan te sluiten ('live te gaan') bij een pilot. Genoemde punten waren de kosten en de doorlooptijd. Idensys middelenleveranciers vonden de doorlooptijd voor aansluiten lang, vanwege afhankelijkheid van het bijeenkomen van de Commissie van Deskundigen (eens in de een à twee maanden), voor iDIN gold een doorlooptijd van zeven weken tot een acceptant wist of hij mocht aansluiten op het BSNk. Voor implementatie van de koppeling moest bij iDIN rekening gehouden worden met een doorlooptijd van nog eens maximaal acht weken. Bij de pilot Publiek Middel speelde dit alles niet volgens de deelnemende partijen.

- Bij de pilot Publiek Middel de processen voor aanvraag en uitgifte van de documenten volgens de gemeenten over het algemeen goed verliepen. Wel werd aangegeven dat de communicatie richting burger op punten nog kan verbeteren. Ook werd gemeld dat burgers voornamelijk problemen ervoeren bij het installeren van de kaartlezer.

- Bij de pilot Idensys de communicatie vanuit de overheid volgens deelnemers beperkt en op punten onduidelijk was, bijvoorbeeld ten aanzien van het toekomstperspectief en het toekomstige financieringsmodel.[62] Een aantal betrokkenen gaf aan dat dit bij andere partijen in het veld en bij eindgebruikers tot onzekerheid leidt en daar een afwachtende houding opriep.

- De Belastingdienst en een bank aangaven dat hun aansluiting op de iDIN-pilot eenvoudig is verlopen. Met betrekking tot het aansluiten van nieuwe acceptanten (dienstaanbieders) is gezegd dat de doorlooptijd als lang en de kosten als hoog kunnen worden ervaren, hetgeen een belemmering kan zijn voor een verdere uitrol naar andere acceptanten.

Hieronder volgen enkele specifieke bevindingen per pilot.

Pilot Publiek Middel

De in de pilot Publiek Middel betrokken partijen hebben de samenwerking in de keten en de onderlinge communicatie als positief ervaren. Er hebben zich op dit gebied geen problemen voorgedaan. De onderzoekers hebben wel ervaren dat de ketenpartners – afgezien van hun eigen primaire proces – niet altijd het benodigde inzicht en de kennis hebben om informatie over de gehele keten heen te genereren. Voorbeelden hiervan zijn: inzicht in de verantwoordelijkheden, waar welke

[62] Noot: het toekomstig financieringsmodel was geen onderdeel van de pilots.

gegevens zijn opgeslagen, wie welke data aanlevert, hoe managementrapportages gegenereerd worden, en het monitoren van procesvoortgang, waaronder het aantal vragen dat eindgebruikers via verschillende kanalen stellen.

Een aandachtspunt is de vormgeving van de 'doosjes' (kaartlezers) en de installatie van het publieke middel (*plug-in*). De meeste problemen die de eindgebruikers volgens de ketenpartners rapporteerden hadden hier betrekking op. Ook bleek dat niet alle dienstaanbieders kunnen omgaan met het betrouwbaarheidsniveau dat wordt geleverd door het publieke middel ('code 30'), hetgeen vervolgens resulteert in een foutmelding bij het inlogproces. Tot slot gaven de betrokken partijen aan dat het voor eindgebruikers niet altijd duidelijk is dat het publiek middel alleen bedoeld is voor gebruik in het publieke domein.

Pilot Idensys

De leveranciers die deelnemen aan de pilot Idensys noemen naast positieve ervaringen ook relatief veel negatieve ervaringen. Daarvan zijn er verschillende die zijn gerelateerd aan de opzet en operationalisering van de pilots. Hierbij lijkt er sprake te zijn van verschillende percepties van betrokkenen over de doelstelling en de uitvoering van de pilots. Zo bestaan er bijvoorbeeld verschillende beelden over wat de onderzoeksvragen (zouden moeten) zijn en over de lengte van de pilot-periode. Daarnaast ervaren (sommige) leveranciers drempels om daadwerkelijk deel te kunnen nemen aan de pilots.

Leveranciers geven aan dat de communicatie vanuit de overheid richting externen (te) beperkt is, en dat ook de communicatie over privacy-aspecten matig is. Ook geven ze aan dat er onduidelijkheid is over het toekomstige financieringsmodel. De betreffende partijen noemen dat deze factoren een afwachtende en soms zelfs negatieve houding tot gevolg hebben bij partijen in het veld en bij eindgebruikers. Dit kan een drempel vormen bij de verdere uitvoering van de pilots en een structurele uitrol van middelen.

Pilot iDIN

Een voordeel van het bankenmiddel is dat er geen apart uitgifteproces voor middelen nodig is, de eindgebruiker reeds bekend is met het middel en kan bepalen welke data beschikbaar wordt gesteld aan de dienstaanbieder op wiens website wordt ingelogd. Dit is het middel waarbij de klant het 'meest aan de knoppen zit' en daadwerkelijk invloed heeft ten aanzien van wat uitgewisseld wordt.

iDIN partijen gaven aan dat de werking van iDIN is gebaseerd op en overeenkomt met die van een reeds bestaande dienst (iDEAL). De processen, communicatie, organisatie en technische implementatie komen in grote lijnen overeen met iDEAL. Het overstappen naar het nieuwe middel iDIN is daardoor voor de partijen relatief eenvoudig. Het aansluiten van een nieuwe acceptant bleek echter moeilijk te zijn vanwege de koppeling met het BSNk (lange doorlooptijd en hoge kosten).

5.2 Tot besluit

TNO heeft een aantal aandachtspunten geïdentificeerd, die volgens TNO van belang zijn voor een verdere uitrol van de middelen en ontwikkeling van de stelsels. Ze zijn opgenomen in deze paragraaf.

5.2.1 Algemeen

Met het oog op de verdere ontwikkeling en uitrol van eID-middelen wordt nog steeds ervaring opgedaan. De pilots lopen nog door en de kennis ontwikkelt zich. Mocht men in een later stadium een vervolgmeting willen uitvoeren ten aanzien van techniek, privacy en ervaringen dan is het van belang een strikte onderzoeksopzet te hanteren en op de belangrijkste aandachtspunten te focussen. Daartoe wil TNO het volgende meegeven.

1. **Methodiek**. Hanteer een S.M.A.R.T. geformuleerde meetmethodiek over alle betrokken organisaties heen, om inzicht te krijgen in welke mate het inloggen met een authenticatiemiddel 'end-to-end' (dus van eindgebruiker tot website) conform de wensen en eisen werkt:
   a. Maak een beperkte selectie van belangrijkste gewenste testindicatoren. Bijvoorbeeld uptime, performance[63] en aantal klachten.
   b. Ontwerp een geautomatiseerde toets die dergelijke indicatoren over de gehele dienstketen heen kan meten over een langere periode en met een bepaalde frequentie. Bijvoorbeeld eens per uur (24 keer per etmaal), over alle dagen van het jaar inclusief weekenden[64].
   c. Pas deze meetmethodiek vanaf dag één structureel toe.

   Op deze manier kan de impact van een geïmplementeerde wijziging bij een al toegetreden organisatie in de keten inzichtelijk worden gemaakt. Ook kan het middel van een nieuw toegetreden middelenleverancier op een objectieve en van tevoren vastgestelde manier worden vergeleken met andere middelen.

   Bekijk de pilots ook in hun onderlinge samenhang en geef een heldere definitie van wat onder een pilot wordt verstaan. Met andere woorden, hanteer een strikte omschrijving van hetgeen gemeten dient te worden.

5.2.2 Techniek

2. **Inzicht**. Een eindgebruiker zou middelen-overstijgend inzicht moeten (kunnen) hebben in welke middelen actief zijn en welke middelen waar bij welke dienstaanbieder gebruikt zijn om in te loggen. Als alleen op een website van een dienstaanbieder wordt getoond wanneer iemand voor het laatst ergens is ingelogd, dan ziet een eindgebruiker dit pas op het moment dat hij of zij daar zelf inlogt. Een mogelijkheid om dit vorm te geven is door een gebruiker per e-mail of SMS te informeren wanneer zijn identiteit wordt gebruikt.

3. **Fraude**. Als er fraude wordt gepleegd met iemands identiteit is de eindgebruiker slachtoffer en loopt hij of zij risico (financieel, aansprakelijkheid, privacy, enzovoort). Ook de betrokken organisaties kunnen schade ondervinden. Als het aantal middelen en het aantal dienstaanbieders groeit, kan binnen het stelsel op termijn de behoefte ontstaan voor een eindgebruiker om zijn of haar identiteit te beschermen door bepaalde diensten te blokkeren. Als een identiteit niet kan worden gebruikt voor bijvoorbeeld de Belastingdienst Aanvragen Toeslagen, kan een aanvaller daar ook geen misbruik maken van

[63] Bijvoorbeeld hoeveel tijd er is verstreken tussen het moment dat een eindgebruiker op de Login knop drukt en het moment dat de website op het scherm melding maakt van succesvol ingelogd zijn van de eindgebruiker.
[64] Beschikbaarheid en performance tijdens het weekend is erg belangrijk voor bijvoorbeeld de Belastingdienst in verband met Aangifte Inkomstenbelasting.

de betreffende identiteit. Of het blokkeren van een hele categorie van diensten of dienstaanbieders, bijvoorbeeld wel het gebruik voor publieke diensten ‘aanzetten’, maar niet het gebruik voor private diensten − of andersom.

5.2.3 Privacy

4. Voor het vervolg dient nagedacht te worden over de inrichting van de stelsels. Nu zijn er multimiddelen- en multistelsels (namelijk drie) die naast elkaar blijken te werken. De uitgangsposities voor de inrichting van die stelsels, zowel technisch als organisatorisch, zijn echter verschillend van aard. Dit is ingegeven door de context waarbinnen de stelsels ontwikkeld zijn. Dat heeft ook zijn weerslag op de inrichting van toezicht en verantwoordelijkheden. Een **uniform normenkader** voor alle stelsels met daarin privacy-eisen en een raamwerk voor toetsing is dan ook aan te bevelen. Het raamwerk dient uniform genoeg te zijn om binnen alle drie de stelsels te kunnen worden toegepast.

5. **Controle** bij de gebruiker (burger) is een ander aspect dat een bijdrage kan leveren aan vertrouwen en transparantie. Indien de burger zelf kan inzien bij welke dienstverleners hij heeft ingelogd en welke transacties zijn verricht met een middel biedt dat de mogelijkheid tot bestrijding van misbruik of fraude. Bovendien kan de burger dan zelf controleren welke organisaties gegevens van hem hebben ontvangen en kunnen verwerken.

6. Met betrekking tot het **verwerken van het BSN** verdient het aanbeveling om, in lijn met het principe van dataminimalisatie, te onderzoeken of de uitwisseling van dit bijzondere gegeven tot een minimum beperkt kan worden. Het BSNk levert hier een oplossing voor, maar er zijn gevallen waar de interactie met het BSNk vermeden kan worden, waardoor minder gegevens worden uitgewisseld tussen minder partijen. Het is ook niet geheel duidelijk wanneer het BSN zelf wordt gecommuniceerd en wanneer niet. In ieder geval dient de uitwisseling van het BSN (of andere gegevens) als gegeven zelf naar een dienstaanbieder altijd gebaseerd te zijn op geïnformeerde toestemming van de gebruiker.

7. Een toets op de **borging van privacy** dient voor het vervolg ook gericht te zijn op technische inbedding. Daarbij wordt aanbevolen specifiek te kijken naar alternatieve mogelijkheden voor de inrichting van middelen of stelsels die een betere borging van de privacy kunnen bewerkstelligen.

5.2.4 Ervaringen

8. In het huidige onderzoek is gesproken met leveranciers en dienstaanbieders die al deelnamen aan de pilot of die op het punt stonden om eraan deel te nemen. Het kan waardevolle inzichten opleveren om ook de ervaringen in kaart te brengen van leveranciers en dienstaanbieders die er voor hebben gekozen **om niet deel te nemen** aan de pilot, of die gaandeweg zijn afgehaakt. Welke drempels hebben zij ervaren en wat heeft hen ertoe doen besluiten om niet mee te doen? Kijk dan tevens naar partijen die nog niet hebben deelgenomen binnen deze onderzoeksperiode maar dat wel willen, zoals partijen in de zorg met mogelijk specifieke behoeften ten aanzien van bijvoorbeeld privacy en gegevensbeheer.

9. Als publieke middelen in de toekomst daadwerkelijk geleverd gaan worden door verschillende gemeenten, is het belangrijk om dan het verloop van de

processen goed te kunnen monitoren op basis van data, om zo de processen ook naar behoren aan te kunnen sturen. Overweeg een alternatief dat de logistiek eenvoudiger maakt (geen kaartlezers maar bijvoorbeeld NFC[65] via de mobiele telefoon) en de installatie vereenvoudigt (geen installatie van *plug-in*).

10. Breng in kaart waar een lager betrouwbaarheidsniveau kan worden aangeboden middels het publieke middel (daar waar acceptabel voor dienstaanbieders) en waar dienstaanbieders actie dienen te ondernemen om toegang tot diensten te realiseren met het vereiste **betrouwbaarheidsniveau** (code 30).

11. Zorg voor **heldere communicatie** over doelstellingen en aanpak bij alle betrokkenen in de verdere uitvoering van de pilots en een eventuele structurele uitrol van de middelen. Zorg voor een efficiënte uitvoering van de pilot-processen.

[65] Near Field Communication

A Referenties

[1] ‘eID stelsel Nederland; Strategische verkenning en voorstel voor vervolg’, Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, oktober 2012

[2] ‘Jaarplan 2015, Programma eID’, Versie 1.0, 24 maart 2015

[3] ‘Masterplan eID’, Versie 1.00, Bart Schmidt, 11 september 2014, Stuurgroep eID

[4] Kamerbrief ‘Pilotvoorwaarden en pilotcriteria Idensys en Publieke eID-middelen’, 17 november 2015

[5] Offerteaanvraag ‘Onderzoek naar betrouwbaarheid en veiligheid pilots publieke en private middelen in het BSN domein’, J.P. van Mierlo, Versie 1.0, 4 januari 2016

[6] Kamerstuk 26643 Nr. 403, ‘Uitrol publieke en private authenticatiemiddelen’, 8 april 2016, https://zoek.officielebekendmakingen.nl/dossier/26643

[7] Mazars, Privacy Impact Assessment, Introductieplateau eID Stelsel NL, (Versie 0.8), 31 juli 2015

[8] ‘Werking op hoofdlijnen van het eID Stelsel NL’, 28 oktober 2013

[9] Brief ‘Introductieplateau eID’ met kenmerk ‘z2015-00357’, 7 mei 2015, Autoriteit Persoonsgegevens

[10] Memo Inrichting Pilot Idensys bij de Belastingdienst (Lissy van Wissen, 18 januari 2016)

[11] Achtergrondinformatie over iDIN en privacy, Betaalvereniging Nederland. Marta Borrat i Frigola, Hanne-Esther Kruyt, Ilse Meyer, Annechien Sloots, Allard Keuter. 28 april 2016 versie 1.

[12] 16042016 Introductie Betaalvereniging en iDIN voor TNO.pdf.

[13] Memo Inrichting pilot iDIN (BankID) bij de Belastingdienst (Lissy van Wissen, 18 januari 2016)

[14] Escalatieprocedure bij Incidenten en calamiteiten, Logius v1.6

[15] Pilots publieke eID-middel Vrijgave & Lessons Learned – Technische en Functionele vrijgaveadviezen/-besluiten en Aanbevelingen ten behoeve van het vervolg, ICTU, Jeroen Rincker, versie 0.2, status concept, 04-03-2016.

[16] ‘Technisch ontwerp Pilot Publiek Middel’, Versie 1.0, 5 oktober 2015, Thijs van Beckhoven, Logius (DEPARTEMENTAAL VERTROUWELIJK)

[17] ‘Afsprakenstelsel Elektronische Toegangsdiensten’, Versie 1.9c, 08-01-2016, Logius

[18] Nota van Inlichtingen behorend bij Onderzoek naar betrouwbaarheid en veiligheid pilots publieke en private middelen in het BSN domein, Ministerie van BZK, 14 januari 2016.

[19] Strategisch Beraad, Oplegnotitie PIA, 10 september 2015.

[20] Overzicht RFCs, bijlage 5.1 bij [19].

[21] Guidance document for Bank ID Control Framework, v1.2 - Toelichting op de eisen aan een issuer

[22] Bank ID Framework, Word 23102015 V 1 2 – eisen aan een Issuer

[23] Beheersing iDIN v.2 – algemene toelichting / beschrijving van de beheersingsmaatregelen

[24] 151119 BankID framework Acquirers v1.0 – eisen aan een Acquirer

[25] 151119 BankID framework RSP v1.0 – eisen aan een Routing Service Provider

[26] '160524 iDIN pilot SVB.pdf', memo van SVB aan BVN, 24 mei, 2016

[27] 'Oplegnotitie iDIN pilot SVB.pdf', toelichting op memo SVB door BVN aan TNO, 25 mei, 2016

[28] 'Voorwaarden DigiD', 1 januari 2015, Versie 8.0, Logius, Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

[29] Baseline Informatiebeveiliging Rijksdienst Tactisch Normenkader (TNK), Versie 1.0 Definitief, 1 december 2012, Ministerie van BZK

[30] Privacy Impact Assessment (PIA), Pilot Publieke eID middelen, Net2Legal Consultants, versie 1.0, januari 2016.

Overige bronnen (waaraan in het tekst niet expliciet wordt gerefereerd):

[31] Guidance Document 23102015 v1 2 BD_V1.2. - Toelichting op de eisen aan een Issuer

[32] Training eID Publieke Middelen, ICTU, Thijs van Beckhoven, 1 februari 2016.

[33] 'Project Start Architectuur Pilot Publiek Middel', Versie 1.0, 6 november 2015, Wim Kegel, Logius

[34] 'Koppelvlakspecificatie DigiD SAML Authenticatie', Versie 3.2, 10 december 2015, Logius

[35] 'Pilotplan Publieke eID-middelen versie 1.0', 23 april 2015, Ministerie van BZK

[36] 'Rekenmodel eID-stelsel', SEO Economisch Onderzoek, Rob van der Noll e.a., augustus 2015

[37] 'Federated Identity Management Systems: A Privacy-Based Characterization', Eleanor Birrell en Fred B. Schneider, Cornell University, September 2013, IEEE Computer and Reliability Societies

[38] 'Werking van het eID Stelsel', Versie 1.0, 21 januari 2014

B Begeleidingscommissie en de Commissie Kuipers

Leden van de begeleidingscommissie:

Naam	**Functie**	**Organisatie**	**Opmerkingen**
Roelant van Zevenbergen	Voorzitter	MinBZK	Tot 1 april 2016
Hans Meijering	Voorzitter	MinBZK	Vanaf 1 april 2016
Hella van der Velde	Lid	MinBZK, BVO	Tot 1 april 2016
Corien Pels Rijcken[1]	Lid	MinBZK	
Bob van Os[2]	Lid	Logius	
Hans-Rob de Reus[3]	Lid	MinFIN	
Marije Stam	Lid	RDW	
Huub Janssen	Lid	MinEZ	

Noten:
[1] Ambtelijk projectleider Pilot Publiek Middel
[2] Ambtelijk projectleider Pilot Idensys
[3] Ambtelijk projectleider Pilot Bankenmiddel

Leden van de Commissie Kuipers:

Naam	**Functie**	**Organisatie**
Rob Kuipers	Voorzitter	MinBZK, ABD
Arre Zuurmond	Lid	Ombudsman Amsterdam
Liesbet van Zoonen	Lid	Erasmus Universiteit
Hans van der Horst	Lid	ING

C Lijst met de gestelde onderzoeksvragen

In deze bijlage zijn de door BZK aan TNO gestelde onderzoeksvragen overgenomen uit paragraaf 1.8 (pagina 7) en paragraaf 1.9 (pagina 9) van de offerte-aanvraag [5]. Het betreft 24 hoofdvragen met 31 deelvragen.

Merk op dat de onderzoeksvragen voor de drie pilots niet identiek zijn over de pilots heen. De vragen voor de twee pilots die betrekking hebben op private middelen in het publieke domein (pilot Idensys en pilot iDIN) zijn identiek aan elkaar: voor deze pilots wordt één vragenlijst gehanteerd. De vragenlijst voor de pilot met publieke middelen in het publieke domein (pilot Publiek Middel) is niet hetzelfde als de vragenlijst voor de private middelen.

Onderzoeksvragen Pilot Idensys en Pilot iDIN:

Hoofdvraag 1: Is er voldaan aan de betrouwbaarheid zoals geformuleerd in het afsprakenstelsel?

Deelvraag 1a: Zijn er incidenten die wijzen op een feitelijke lage betrouwbaarheid?
Deelvraag 1b: Hoe zijn deze incidenten afgehandeld?

Hoofdvraag 2: In welke mate is er voldaan aan de gestelde eisen omtrent beschikbaarheid?

Hoofdvraag 3: In welke mate is voldaan aan de informatieveiligheidseisen?

Deelvraag 3a: Zijn er incidenten die wijzen op het niet voldoen aan de informatieveiligheidseisen?
Deelvraag 3b: Hoe zijn deze incidenten afgehandeld?

Hoofdvraag 4: Hoe is het toezicht verlopen?

Hoofdvraag 5: Wat zijn de resultaten van de PIA en hoe is omgegaan met de uitkomsten?

Deelvraag 5a: Is er een PIA uitgevoerd?
Deelvraag 5b: Zijn er mitigerende maatregelen voorgesteld?
Deelvraag 5c: Zijn deze mitigerende maatregelen uitgevoerd?
Deelvraag 5d: Hebben zich desondanks nog privacy incidenten t.a.v. privacy voorgedaan?
Deelvraag 5e: Hoe zijn deze privacy incidenten opgelost?

Hoofdvraag 6: Hoe ervaren de leveranciers de deelname aan de pilot?

Deelvraag 6a: Wat zijn redenen voor leveranciers om deel te nemen aan de pilot?
Deelvraag 6b: Hoe is de pilot voor de leveranciers verlopen?

Deelvraag 6c: In welke mate zien leveranciers het hoogwaardige middel als toegevoegde waarde?

Hoofdvraag 7: Hoe is het aanvraag- en uitgifteproces verlopen?

Hoofdvraag 8: Zien authenticatiediensten/middelenleveranciers toekomst in het middel dat zij nu uitgeven?

Hoofdvraag 9: Hoe ervaren de dienstaanbieders de deelname aan de pilot?

Deelvraag 9a: Wat zijn de redenen voor dienstaanbieders om deel te nemen aan de pilot?
Deelvraag 9b: Hoe is de pilot voor de dienstaanbieders verlopen?
Deelvraag 9c: In welke mate zien dienstaanbieders het hoogwaardige middel als toegevoegde waarde?
Deelvraag 9d: Is de communicatie verlopen volgens het communicatieplan pilots?

Hoofdvraag 10: Hoe is het proces van aansluiting verlopen?

Hoofdvraag 11: In welke mate wordt er van de diensten gebruik gemaakt door deelnemers aan de proef en hoe verloopt dit gebruik voor de dienstaanbieders?

Deelvraag 11a: Hoeveel deelnemers maken gebruik van de diensten en hoe frequent is het gebruik van de diensten via het hoogwaardige middel?
Deelvraag 11b: Hebben zich nog problemen voorgedaan tijdens de pilot en hoe zijn deze opgelost?

Onderzoeksvragen Pilot Publiek Middel:

Hoofdvraag 1: Wordt voldaan aan de afgesproken eisen die verwoord staan in de gebruiksvoorwaarden van DigiD ?

Hoofdvraag 2: Voldoet de technische voorziening van Logius, RvIG en RDW aan de BIR?

Hoofdvraag 3: Voldoen de ICT-componenten aan de gestelde technische veiligheidseisen en privacy-eisen?

Hoofdvraag 4: In welke mate zijn dienstaanbieders en andere betrokkenen duidelijk geïnformeerd over het doel van de pilot, de gegevens en het gebruik tijdens de pilot?

Hoofdvraag 5: Zijn er issues opgetreden op het gebied van aansprakelijkheid bij de burger?

Hoofdvraag 6: Hoe werkt de technische keten (kaart, kaartlezer, aanvraag/uitgifte en DigiD) tijdens de pilot?

Deelvraag 6a: Hoe verloopt het activeren door de deelnemers?

Deelvraag 6b: Hoe verloopt het inloggen bij de deelnemers?
Deelvraag 6c: In welke mate zijn er aanpassingen gedaan aan de techniek tijdens de pilot om problemen te verhelpen?

Hoofdvraag 7: Wat is de performance van de techniek?

Hoofdvraag 8: Welke aandachtspunten zijn er bij de techniek?

Hoofdvraag 9: Hoe ervaren de authenticatiediensten en leveranciers van het publieke middel de levering?

Hoofdvraag 10: Hoe ervaren de leveranciers het contact met de beheerorganisatie?

Hoofdvraag 11: Hoe ervaren gemeenten het aanvraag- en uitgifte proces van het publieke middel?

Deelvraag 11a: Hoe ervaren gemeenten het aanvraagproces van het publieke middel?
Deelvraag 11b: Hoe ervaren gemeenten het uitgifteproces van het publieke middel?
Deelvraag 11c: In hoeverre verschilt het aanvraag- en uitgifteproces van het publieke middel met de huidige situatie?
Deelvraag 11d: Hoe worden eventuele verschillen ervaren door de gemeente en/of betrokken ambtenaren?
Deelvraag 11e: Hoe verloopt de communicatie over het publieke middel bij de gemeente?

Hoofdvraag 12: Hoe gaan gemeenten om met eventuele problemen van burgers en eigen vragen?

Deelvraag 12a: In welke mate melden zich deelnemers met problemen bij gemeenten?
Deelvraag 12b: Hoe gaan gemeenten om met vragen, problemen en klachten?
Deelvraag 12c: Hoe gaan gemeenten om met vragen uit de eigen organisatie?

Hoofdvraag 13: Welke aandachtspunten zijn er volgens de gemeente op basis van de ervaringen met de proef?

Deelvraag 13a: Welke aandachtspunten zijn er volgens de gemeenten bij een eventuele verdere uitrol van de pilot naar andere gemeenten?
Deelvraag 13b: In hoeverre denkt de gemeente dat het publieke middel en de techniek toestaat om meer diensten te digitaliseren op termijn?

D Lijst van interviewpartners en bijeenkomsten

Deze bijlage bevat een overzicht van de verschillende bijeenkomsten, partijen en personen die TNO ten behoeve dit onderzoek bijgewoond resp. gesproken heeft. In het overzicht is onderscheid gemaakt naar algemene contacten of bijeenkomsten, en naar de drie groepen van deelnemers zoals beschreven in paragraaf 1.3.

Algemene gesprekken en bijeenkomsten:

#	Datum	Organisatie	Omschrijving / onderwerp
1	04/02/16	Begeleidingscommissie en Commissie Kuipers	Startbijeenkomst, opzet onderzoek.
2	09/02/16	Diverse	Deelname aan Masterclass eID.
3	15/02/16	Begeleidingscommissie	Tweede bijeenkomst, afspraken opzet onderzoek.
4	16/02/16	Bob van Os	Interview pilot Idensys.
5	16/02/16	Logius	Beheerder afsprakenstelsel, gesproken met Nicole Damen en Maurice Pasman
6	19/02/16	Corien Pels Rijcken	Interview pilot Publiek Middel.
7	24/02/16	Logius	Interview met de beheerorganisatie van het Idensys afsprakenstelsel (Nicole Damen en Maurice Pasman).
8	07/03/16	Diverse stakeholders	Eerste reflectiebijeenkomst.
9	09/03/16	Hans-Rob de Reus	Interview pilot iDIN.
10	15/03/16	Bob van Os (organisatie van de bijeenkomst)	Bijeenkomst pilot Idensys bijgewoond, voor dienstverleners en leveranciers.
11	30/03/16	BZK, Commissie Kuipers	Deelname aan ronde tafel ‘internationaal’.
12	31/03/16	Commissie Kuipers	Voortgangsgesprek met Rob Kuipers.
13	21/04/16	Gesprek Agentschap Telecom	Toezichthouder Idensys. Gesproken met Bob Hulsebosch, Robert Adrian en Melle Schol.
14	21/04/16	Begeleidingscommissie	Derde bijeenkomst, voortgang.
15	28/04/16	ICTU	Rapportages Publiek Middel, gesproken met Hugo Butter en Bart Overbeek Bloem.
16	02/05/16	Begeleidingscommissie	Vierde bijeenkomst, voortgang.
17	09/05/16	Diverse stakeholders	Tweede reflectiebijeenkomst.
18	17/05/16	Begeleidingscommissie	Vijfde bijeenkomst, opzet en contouren eindrapport.
19	23/05/16	Begeleidingscommissie	Zesde bijeenkomst, concept eindrapport.

Partijen die zijn gestart in de periode t/m 18 maart (‘groep 1’):

#	Datum	Organisatie	Omschrijving / onderwerp
1	16/02/16	Gemeente Eindhoven	Pilot Publiek Middel, meeloopdag, gesproken met o.a. Ton Koppen.

2	16/02/16	RDW	Pilot Publiek Middel. Gesproken met Bas van Berkhout (contactpersoon).
3	16/02/16	ICTU	Pilot Publiek Middel. Gesproken met Jolanda Padmos, Hugo Butter, Bart Overbeek Bloem
4	16/02/16	Groningen	Pilot Publiek Middel. Andre Brands, Hendrik Woldring
5	01/03/16	Gemeente Den Haag	Pilot Publiek Middel, meeloopdag, gesproken met o.a. Theo van der Nat.
6	03/03/16	Belastingdienst	Meeloopdag pilot iDIN en pilot Idensys, met, functioneel architect en ICT architect en projectleider. Gesproken met Marco Eikenaar, Peter Kooi en Lissy van Wissen.
7	31/03/16	Belastingdienst en Hans-Rob de Reus	Interview Pilot iDIN.
8	14/04/16	BVN	Workshop pilot iDIN.
9	18/04/16	Digidentity	Interview ervaringen pilot Idensys, gesproken met Dick Dekkers.
10	10/05/16	RvIG	Pilot Publiek Middel. Gesproken met Cynthia Henskens

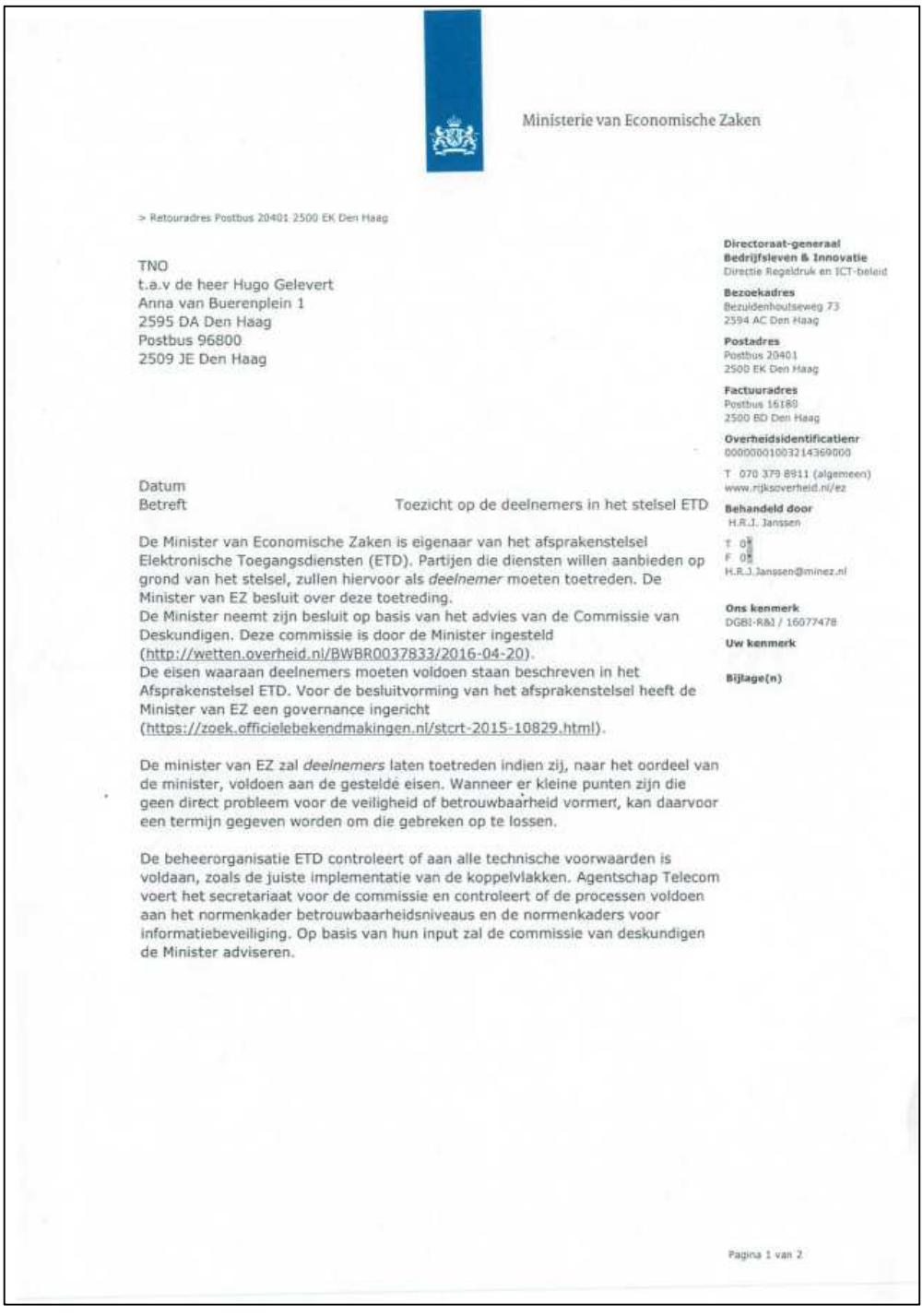
Partijen die zijn gestart in de periode van 19 maart t/m 15 april ('groep 2'):

#	Datum	Organisatie	Omschrijving / onderwerp
1	26/04/16	Gemeente Groningen	Interview pilot Publiek Middel, gesproken met André Brands en Hendrik Woldring.
2	28/04/16	CreAim	Interview pilot Idensys, gesproken met Frank Jonker, Mark Baas en Rogier Pafort
3	29/04/16	KPN	Interview pilot Idensys, gesproken met Haydar Cimen, Marco Scheerman en Sander Steenbergen
4	19/05/2016	Belastingdienst	Follow-up interview met Lissy van Wissen
5	19/05/16	ING	Vragenlijst per mail pilot iDIN, Vincent Prins
6	19/05/16	Triodos Bank	Vragenlijst per mail pilot iDIN, Gerard Cillessen
7	20/05/16	ING	Telefonisch interview Vincent Prins

Partijen die starten (of zijn gestart) op 16 april of later ('groep 3'):

#	Datum	Organisatie	Omschrijving / onderwerp
1	03/05/16	Morpho	Interview pilot Idensys, gesproken met Jouri de Vos en Freek van Gijn
2	18/05/16	Gemeente Rotterdam	Pilot Idensys, telefonisch contact met Marco Smit

E Verklaring Minister van Economische Zaken



Ministerie van Economische Zaken

> Retouradres Postbus 20401 2500 EK Den Haag

TNO
t.a.v de heer Hugo Gelevert
Anna van Buerenplein 1
2595 DA Den Haag
Postbus 96800
2509 JE Den Haag

Directoraat-generaal Bedrijfsleven & Innovatie
Directie Regeldruk en ICT-beleid

Bezoekadres
Bezuidenhoutseweg 73
2594 AC Den Haag

Postadres
Postbus 20401
2500 EK Den Haag

Factuuradres
Postbus 16180
2500 BD Den Haag

Overheidsidentificatienr
00000001003214369000

T 070 379 8911 (algemeen)
www.rijksoverheid.nl/ez

Behandeld door
H.R.J. Janssen

T 0[illegible]
F 0[illegible]
H.R.J.Janssen@minez.nl

Ons kenmerk
DGBI-R&I / 16077478

Uw kenmerk

Bijlage(n)

Datum
Betreft Toezicht op de deelnemers in het stelsel ETD

De Minister van Economische Zaken is eigenaar van het afsprakenstelsel Elektronische Toegangsdiensten (ETD). Partijen die diensten willen aanbieden op grond van het stelsel, zullen hiervoor als *deelnemer* moeten toetreden. De Minister van EZ besluit over deze toetreding.
De Minister neemt zijn besluit op basis van het advies van de Commissie van Deskundigen. Deze commissie is door de Minister ingesteld (http://wetten.overheid.nl/BWBR0037833/2016-04-20).
De eisen waaraan deelnemers moeten voldoen staan beschreven in het Afsprakenstelsel ETD. Voor de besluitvorming van het afsprakenstelsel heeft de Minister van EZ een governance ingericht (https://zoek.officielebekendmakingen.nl/stcrt-2015-10829.html).

De minister van EZ zal *deelnemers* laten toetreden indien zij, naar het oordeel van de minister, voldoen aan de gestelde eisen. Wanneer er kleine punten zijn die geen direct probleem voor de veiligheid of betrouwbaarheid vormen, kan daarvoor een termijn gegeven worden om die gebreken op te lossen.

De beheerorganisatie ETD controleert of aan alle technische voorwaarden is voldaan, zoals de juiste implementatie van de koppelvlakken. Agentschap Telecom voert het secretariaat voor de commissie en controleert of de processen voldoen aan het normenkader betrouwbaarheidsniveaus en de normenkaders voor informatiebeveiliging. Op basis van hun input zal de commissie van deskundigen de Minister adviseren.

Pagina 1 van 2

Directoraat-generaal
Bedrijfsleven & Innovatie
Directie Regeldruk en ICT-beleid

Ons kenmerk
DGBI-R&I / 16077478

De Minister van Economische Zaken heeft een positief besluit genomen op de toetredingsverzoeken voor de Idensys-pilots, voor alle beschreven rollen, aan:

- KPN
- CreAim
- Digidentity

Deze partijen voldoen volgens de Minister aan de gestelde eisen.

Hoogachtend,
De minister van Economische Zaken
Namens deze:

Drs.G.W.J.M. Linssen
Plv. directeur Regeldruk & ICT beleid

Pagina 2 van 2