

Herijking business case inloggen BSN domein

Impact recente beleidswijzigingen en inzichten

Opdrachtgever: Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Rotterdam, 1 maart 2018



Herijking business case inloggen BSN domein

Impact recente beleidswijzigingen en inzichten

Opdrachtgever: Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Rotterdam, 1 maart 2018

Inhoudsopgave

Samenvatting	3
1 Inleiding	7
1.1 Aanleiding	7
1.2 Onderzoeksopdracht en afbakening	8
1.3 Gebruikte methodiek en aanpak	9
1.4 Leeswijzer	11
2 Project- en nulalternatief	12
2.1 Probleemanalyse	12
2.2 Nulalternatief	14
2.3 Projectalternatief	15
2.3.1 Groeipad	19
3 Resultaten op hoofdlijnen	24
3.1 Gevolgen koerswijziging, nieuwe inzichten en bredere scope	24
3.2 Overzicht kosten en baten: break even point	27
3.3 Impactanalyse bij gemeenten	28
3.4 Resultaten van de use cases in de zorg en bij gemeenten	28
4 Kosten en baten nader uitgewerkt	31
4.1 Kosten	31
4.1.1 Kostenramingen	31
4.1.2 Kosten nulmeting	38
4.1.3 Conclusies	39
4.2 Baten	40
4.2.1 Inventarisatie van de baten	40
4.2.2 Te kwantificeren baten	42
Bijlage 1 Uitwerking impactanalyse	44
Bijlage 2 Uitwerking use cases	54
Bijlage 3 Gesprekspartners	65

Samenvatting

Beschouwing en advies

Het 'nieuwe' eID-stelsel is een essentieel onderdeel van de 'digitale snelweg', dat moet worden gerealiseerd en beheerd. De kosten zijn fors, maar maatschappelijk te verantwoorden vanuit de potentiële baten. De herijking laat zien dat de koerswijziging leidt tot lagere kosten, maar dat de kosten per saldo toch stijgen ten opzichte van de raming uit 2016, zeker als de kosten van eIDAS toe worden toegerekend aan eID. Wij achten het raadzaam om een aantal kostenposten aan een nadere review te onderwerpen. Wellicht zijn er efficiëntere oplossingen mogelijk die hetzelfde effect op veiligheid en betrouwbaarheid realiseren. Tevens raden wij aan om te zoeken naar een goedkoper alternatief voor de relatief dure oplossing met de kaartlezers, en - na de aanbesteding van de private middelen - besparingen van de kosten voor de publieke middelen in beeld te brengen.

Een eID-stelsel als essentiële voorwaarde voor betrouwbare dienstverlening aan burgers

Er is een nadrukkelijke behoefte aan een eID-stelsel met middelen op een hoger betrouwbaarheidsniveau. Op dit moment gebruiken burgers DigiD om in te loggen en digitaal transacties af te handelen met overheidsdienstaanbieders in het BSN-domein, maar de betrouwbaarheid en veiligheid van DigiD is in niet alle gevallen voldoende – zeker in het huidige tijdsgewricht. Hierdoor is er een risico op identiteitsfraude.

Daarnaast bestaat de wens om nieuwe diensten te digitaliseren, maar dat is slechts mogelijk wanneer er een stelsel is en er middelen zijn op betrouwbaarheidsniveau hoog. Het kan dan bijvoorbeeld gaan om uitwisseling van privacygevoelige informatie (gezondheid, strafrecht, financiën). Als deze diensten kunnen worden gedigitaliseerd kan dat leiden tot een betere dienstverlening aan burgers in de vorm van tijd- en kostenbesparing. Bovendien worden, door het waarborgen van de continuïteit van de digitale dienstverlening, burgers minder afhankelijk van DigiD als publieke authenticatiedienst en de publieke middelen als enige optie om mee in te loggen.

Nieuwe business case noodzakelijk

De vorige business case uit 2016 gaf al een goed inzicht in de kostenraming en potentiële baten van de invoering van middelen met een hogere betrouwbaarheid. Essentiële koerswijzigingen in het beleid, nieuwe inzichten door meer specifieke ontwerpen en een bredere scope door implementatie van EU-wetgeving zijn aanleiding om die business case te herijken. Alle drie de aspecten worden in deze business case meegenomen. Tevens is in deze business case illustratief in beeld gebracht wat de gevolgen van het eID-programma zijn bij dienstverleners in de zorg en bij gemeenten.

Samenvattend leidt de herijking tot een totaalbeeld van de kosten van € 995 miljoen, ten opzichte van € 659 miljoen uit de vorige business case van 2016(zie tabel S1). Een aantal kostenposten was en is nu nog niet in beeld te brengen (PM).

Tabel S1 Verschillenoverzicht kosten business case 2016 en huidige business case (bedragen in € mln.)

Kosten	Business Case november 2016	Business Case 2018
Kosten die samenhangen met de beleidswijziging		
Aansluitkosten dienstaanbieders (oplossing: routeringsdienst) ^{a)}	PM (schatting nu: 35 - 58 mln.)	0
Beheer eID-stelsel & routeringsdienst	158	143
Private middelen	PM	PM
Herijkte kosten die ook in de vorige businesscase waren opgenomen		
Authenticatiedienst DigiD	286	438
Investeringskosten eID-programma	52	69
Kosten DigiD Hoog middelen (productie en uitgifte)	106	120
Kaartlezer	43	145
Doorontwikkeling beleid	14	14
Onderwerpen buiten scope in de vorige businesscase		
Aansluitkosten dienstaanbieders door eIDAS	n.v.t.	13
Investeringskosten eIDAS-voorzieningen	n.v.t.	12
Beheerkosten eIDAS	n.v.t.	42
Totaal	659 + PM	995 + PM

a) Aangezien deze kostenpost in de vorige business case niet inzichtelijk was gemaakt (PM-post), nemen we deze post nu separaat als kostenbesparing op door de kosten in de huidige business case op 0 te zetten.

Hieronder gaan we in op de belangrijkste wijzigingen en resultaten.

Koerswijziging: minder uitgaven bij dienstaanbieders en lagere beheerkosten van het eID-stelsel

Naar aanleiding van de Kamerbrief van 23 juni 2017 en het Algemeen Overleg Impuls eID d.d. 5 juli 2017, heeft de Kamer verzocht de bestaande business case uit 2016 te actualiseren op basis van de herziene koers van het programma eID. De herziene koers is om 'bij de verdere uitwerking het stelsel op enkele onderdelen te vereenvoudigen om de uitvoerbaarheid te waarborgen'.

De **ontzorging van de dienstaanbieders** leidt tot een vermindering van de beoogde uitgaven. Over de gehele looptijd van 10 jaar, betekent dit een verlaging van de kosten van circa € 35 tot € 58 miljoen. De kosten voor het **beheer van het eID-stelsel** (incl. kosten routeringsdienst) bedragen € 143 miljoen, waar deze in 2016 nog op € 158 miljoen waren geraamd. Per saldo is hier een besparing van € 15 miljoen ten opzichte van de vorige business case door enerzijds lagere kosten voor het beheer door het loslaten van de Uniforme Set van Eisen en de vereenvoudiging van de multi-middelenstrategie (€ 42 miljoen) en anderzijds extra kosten voor de routeringsdienst.

Nieuwe inzichten en bredere scope leiden tot hogere kostenraming

In 2016 was de raming dat de totale kosten over de gehele periode uitkwamen op circa € 659 miljoen, exclusief een aantal kostenposten die nog niet inzichtelijk waren te maken (PM). De verbeterde kostenraming leidt ertoe dat de kosten na herijking stijgen. Meest belangrijk is dat er, op basis van de recente bestedingsplannen, € 438 miljoen benodigd is voor de **authenticatiedienst substantieel en hoog**; een stijging van ruim € 150 miljoen. Overigens vallen er ook kosten weg omdat deze ook hadden moeten worden gemaakt als er niet in het eID-stelsel wordt geïnvesteerd (zie hiervoor de baten in de vorm van 'vermeden kosten' in tabel S3). Omdat de kosten van een **kaartlezer** nu hoger wordt geschat (€ 30 i.p.v. € 10), nemen de (mogelijke) kosten voor de burger toe met € 102 miljoen. Het blijkt dat het plaatsen van **eIDAS** binnen de scope leidt tot extra kosten van € 66 miljoen.

Investeringskosten en beheerkosten per jaar

Een uitsplitsing van de kosten laat zien dat het merendeel van de kosten moet worden gemaakt in de beheerfase vanaf 2018. De totale investeringskosten bedragen €94 miljoen voor de periode 2015 tot en met 2020. Vanaf 2018 worden er kosten gemaakt voor het beheer van de publieke authenticatiedienst en worden er kosten gemaakt voor de productie en uitgifte van publieke middelen (DigiD Hoog), de aanschaf van kaartlezers en het beheer van eIDAS. Jaarlijks gaat het om een bedrag van €89 miljoen (zie tabel S2).

Tabel S2 Investeringskosten versus beheerkosten (bedragen in € mln.)

Kostenpost	Investeringskosten (2015-2020)	Gemiddelde kosten per jaar beheerfase (2018-2027)	Kosten totaal
Ontwikkelkosten eID	69		69
Ontwikkelkosten eIDAS	12		12
Aansluitkosten dienstverleners eIDAS	13		13
Kosten DigiD Hoog middelen		12	120
Kosten kaartlezers		15	145
Kosten private middelen		PM	PM
Beheer eID-stelsel		14	143
Authenticatiedienst DigiD - vaste kosten		28	282
Authenticatiedienst DigiD - variabele kosten		16	156
Authenticatiedienst (privaat)		PM	PM
Beheer eIDAS		4	42
Doorontwikkeling beleid		1	14
Totaal ^{a)}	94	89 + PM	995 + PM

a) Door afrondingsverschillen lijken bedragen niet altijd bij elkaar op te tellen.

Het eID-programma bespaart ook aanzienlijke kosten

In de volgende tabel is het totaaloverzicht opgenomen van de baten, voor zover het mogelijk was om deze te kwantificeren. Het gaat om vermeden kosten van in totaal €275 miljoen. Een belangrijke post is de authenticatiedienst van het huidige DigiD. Deze kosten van in totaal €240 miljoen over 10 jaar, moeten ook worden gemaakt als er niet in het eID-stelsel wordt geïnvesteerd (om DigiD te blijven beheren). Tevens kunnen verschillende bestaande authenticatiepassen worden uitgefaseerd en vervangen door eID-middelen. Dit levert een indicatieve besparing op van circa €35 miljoen.

Tabel S3 Te kwantificeren baten (bedragen in € mln.)

Kosten	Businesscase november 2016	Onderhavige Businesscase
Vermeden kosten authenticatiedienst DigiD	240	240
Vermeden kosten alternatieve authenticatiesystemen	48	35
Totaal	288 + PM	275 + PM

In de vorige business case was de waarde van de baten gelijk aan €288 miljoen. Deze daling wordt veroorzaakt doordat het aantal alternatieve authenticatiepassen in omloop iets lager blijkt te zijn en doordat de vervanging later mogelijk wordt (in 2022 in plaats van in 2021).

Kosten kunnen worden terugverdiend door minder fraude en gebruiksgemak voor de burger

Zonder betrouwbare middelen is er onvoldoende zekerheid over de identiteit van de burger en zijn er diverse risico's dat er iets mis gaat (fraude, misbruik, veiligheid en privacy). Uit berekeningen,

blijkt dat, als er circa 2.070 fraudegevallen kunnen worden vermeden door gebruik te maken van meer betrouwbare middelen, de kosten kunnen worden terugverdiend. Gelet op het feit dat er de laatste jaren circa 9.000 tot 15.000 maal per jaar een DigiD account is ingetrokken vanwege mogelijke fraude, lijkt het aantal van 2.070 vermeden fraudegevallen bereikbaar. Tevens wordt duidelijk dat er jaarlijks circa 43 miljoen digitale transacties op betrouwbaarheidsniveau hoog moeten worden uitgevoerd om de kosten terug te verdienen door het gebruiksgemak bij burgers. Binnen de zorg werd er in 2017 al circa 49 miljoen maal met DigiD ingelogd, terwijl een groot deel van de zorgaanbieders nog niet is aangesloten op DigiD en dat straks wel moeten gaan doen. Door meer processen te digitaliseren en meer partijen (in de zorgsector) aan te sluiten, lijkt ook het aantal van 43 miljoen authenticaties per jaar in de toekomst haalbaar.

Het zorg domein heeft baat bij hoge betrouwbaarheid van middelen

Een belangrijke uitkomst is dat door het beschikbaar komen van eID middelen op substantieel en hoog betrouwbaarheidsniveau het palet aan diensten dat in de zorg en het gemeente domein gedigitaliseerd kan worden toeneemt. Met name in de zorg is de meerwaarde van een middel met betrouwbaarheidsniveau hoog significant. Het zorg domein is al geruime tijd proactief bezig met het digitaliseren van diensten en gebruikt hiervoor ook private middelen. Zorgpartijen hechten dan ook grote waarde aan een middel op niveau hoog met een zo groot mogelijk gebruiksgemak. Dienstverleners zien baten voor zichzelf en voor hun patiënten. Vooral als een digitaal proces een terugkerend fysiek bezoek aan de arts of instelling vervangt. Denk hierbij bijvoorbeeld aan het digitaal doorgeven van meetgegevens. Ook het identificeren van de zorgprofessional zelf binnen het eigen systeem en tussen organisaties zou baat kunnen hebben bij een middel op niveau hoog.

Gemeenten zien ook baten, maar zijn nog afwachtend

Bij gemeenten is er een breed gedragen wens is om de digitale dienstverlening voor de burger verder uit te breiden. Ideeën over de nieuwe diensten op basis van eID-middelen op substantieel en hoog betrouwbaarheidsniveau bevinden zich echter nog in een erg vroeg stadium. De baten concentreren zich op verminderd baliebezoek, tijdswinst en gebruikersgemak voor de burger, zoals blijkt uit een aantal recente pilots (aanvragen rijbewijs, aanvragen geboorteaangifte). Wel moet in ogenschouw worden genomen dat het in sommige gevallen wenselijk is om het persoonlijk contact met de gemeente in stand te houden. De gemeenten geven daarnaast aan dat potentiële baten alleen gerealiseerd kunnen worden bij voldoende opname van het nieuwe middel onder de bevolking. Op dit moment bestaat hier nog onzekerheid over bij de gemeenten, wat vaak leidt tot een afwachtende houding.

1 Inleiding

1.1 Aanleiding

In 2014 heeft Ecorys de Business case publieke eID-middelen¹ opgesteld en in maart 2016 is deze business case herijkt op basis van voortschrijdende inzichten². In navolging van ontwikkelingen en discussie in de Tweede Kamer heeft Ecorys na de herijking een nieuwe business case opgesteld met een bredere scope³. Hierin is, naast de meerkosten die nodig zouden zijn om *publieke eID-middelen op eIDAS betrouwbaarheidsniveau hoog* te kunnen gebruiken binnen de bestaande centrale voorzieningen voor DigiD (zoals de huidige DigiD authenticatiedienst), ook gekeken naar de *integrale kosten en baten van de centrale voorzieningen* om de multi-middelenaanpak te faciliteren in combinatie met het introduceren van nieuwe *eID-middelen op eIDAS betrouwbaarheidsniveaus substantieel en hoog*. Deze business case is door de minister van BZK op 9 november 2016 naar de Tweede Kamer gestuurd.

Naar aanleiding van de Kamerbrief⁴ van 23 juni 2017 en het Algemeen Overleg Impuls eID⁵ d.d. 5 juli 2017, heeft de Tweede Kamer in de motie Bruins-Slot c.s.⁶ verzocht de business case te actualiseren op basis van de herziene koers van het programma eID. In het Algemeen Overleg Impuls eID lichtte de minister de plannen als volgt toe:

‘We voeren nu snel het gewenste hogere niveau «substantieel» in, met tweewegidentificatie. Binnenkort starten we met het uitgeven van een middel op het rijbewijs en de nationale identiteitskaart waardoor mensen ook op het allerhoogste beveiligingsniveau kunnen inloggen. Daarnaast doen we een marktconsultatie over de vraag of private partijen geïnteresseerd en in staat zijn om te voldoen aan het ook produceren van een product vanuit de markt. ... of dit betekent dat we nu meer zeggen dat we als overheid het voortouw nemen. Het antwoord daarop is bevestigend. De verschillende afnemers van het product identificatie zeggen echt niet verder te kunnen als er geen hogere beveiligingsniveaus en additionele middelen komen. De markt kan kennelijk niet altijd zijn werk zo snel volledig doen, want de markt is met andere dingen bezig. We gaan daar nu mee verder. Dat is inderdaad wat ik hier voorstel.’

De herziene koers omvat met name aanpassingen van de uitwerking van het stelsel omwille van een eenvoudiger uitvoerbaarheid.

¹ Ecorys (2014), *Business Case publieke eID-middelen*. (TK 26 643 nr. 349).

² Ecorys & Van Zutphen Economisch Advies (2016), *Herijking business case publiek eID-middel*.

³ Ecorys & Van Zutphen Economisch Advies (2016), *Business case Inloggen in het BSN-domein. De kosten en baten van het eID-stelsel* (TK 26 643 nr. 425).

⁴ TK 26 643 nr. 476.

⁵ TK 27 859 nr. 111.

⁶ TK 27 859 nr. 108.

1.2 Onderzoeksopdracht en afbakening

De vorige business case uit 2016 gaf al een goed inzicht in de kostenraming en potentiële baten van de invoering van middelen met een hogere betrouwbaarheid. Het is echter noodzakelijk om business cases regelmatig te herijken. Essentiële koerswijzigingen in het beleid, nieuwe inzichten door specifieke ontwerpen en een bredere scope door implementatie van EU-wetgeving waren nu de directe aanleiding voor deze herijking. Alle drie de aspecten worden in deze business case meegenomen. Tevens moet deze business case illustratief in beeld brengen wat de gevolgen van het eID-programma zijn bij dienstverleners in de zorg en bij gemeenten.

Het bovenstaande heeft geleid tot een **onderzoeksopdracht** in drie onderdelen:

Onderdeel 1: De effecten van de koerswijziging in de kamerbrief van juni 2017

Concreet gaat het om:

- Een vereenvoudiging van de set van eisen, omwille van uitvoerbaarheid en verlaging van de kosten;
- Het ontzorgen van dienstverleners door middel van een routeringsdienst, omwille van de uitvoerbaarheid en lagere kosten;
- Het aanwijzen van een of meer eID-middelen geleverd door private partijen, in plaats van het toelaten van alle middelen die aan de eisen voldoen, omwille van vereenvoudiging van het stelsel en lagere kosten.

Onderdeel 2: De actualisatie van de business case uit 2016 en de gevolgen van een bredere scope

- De actualisering van de originele business case, gebruikmakend van de nieuwste bronnen, data en cijfers;
- Bredere scope: hierbij gaat het om de gevolgen van de bekrachtiging van de eIDAS verordening per 29 september 2018.

Onderdeel 3: Een illustratief beeld van de gevolgen van het eID-programma bij dienstverleners in de zorg en bij gemeenten

- Een impactanalyse bij gemeenten, waarbij in beeld wordt gebracht:
 - De impact op de afdelingen Burgerzaken doordat gemeenten de publieke middelen op niveau DigiD Hoog uitgeven.
 - De impact die het aansluiten op eID op de gemeentelijke organisatie heeft.
- Beschrijving van een aantal use cases in het zorg domein en bij gemeenten, met nadruk op:
 - De (maatschappelijke) baten in de domeinen zorg en gemeenten toe te wijzen aan het stelsel en de middelen;
 - De maatschappelijke baten voor de burger door het aanbieden van (nieuwe vormen van) dienstverlening door het beschikbaar komen van middelen met een hogere betrouwbaarheid in de domeinen zorg en gemeenten.

Voor de use cases is door het ministerie van BZK bewust gekozen voor de focus op de grote (semi)publieke sectoren binnen het BSN-domein, waar mogelijkheden zijn om met middelen met een hogere betrouwbaarheid de digitale dienstverlening te verbeteren, zoals 'zorg' en 'gemeenten'⁷. Voor andere sectoren zijn er ook kosten en baten als gevolg van het eID-programma, maar worden deze niet specifiek in deze business case in beeld gebracht.

⁷ Ministerie BZK (2017) Opdrachtformulering Herijking Business Case "Inloggen in het BSN-domein".

De drie onderdelen zijn uitgevoerd met behulp van een kwantitatieve herijking, een (kwantitatieve en kwalitatieve) impactanalyse bij gemeenten en de kwalitatieve beschrijving van een aantal relevante use cases. Hierbij is de volgende afbakening in tijd gevolgd:

- De eenmalige ontwikkelkosten gerekend met ingang van 2015;
- De meerjarige investerings-, beheers en exploitatiekosten kennen een tijdshorizon van 10 jaar;
- De meerjarige baten kennen een tijdshorizon van 10 jaar, gerekend vanaf de inwerkingtreding van de Wet digitale overheid;
- Het exploitatiekostenoverzicht heeft een tijdshorizon van 10 jaar, vanwege de 10-jarige levensduur van het publieke inlogmiddel op betrouwbaarheidsniveau 'hoog'.

1.3 Gebruikte methodiek en aanpak

Deze herijking is methodologisch in lijn met de vorige business cases. Hieronder gaan we in op de volgende onderdelen:

- Gebruikte methodiek bij de business case;
- Het onderscheid tussen 'het fundament en het huis';
- Gebruikte methodiek bij de impactanalyse;
- Gehanteerde aanpak.

Gebruikte methodiek bij de business case

De analyse van de kosten en baten is uitgevoerd conform de voorschriften uit de Algemene leidraad voor maatschappelijke kosten-batenanalyses⁸ van het CPB en PBL, die rijksbreed wordt gebruikt voor het opstellen van kosten-batenanalyses voor grote projectinvesteringen, en de Handreiking van kosten-batenanalyse voor ICT-projecten⁹ die in opdracht van het ministerie van Economische Zaken is opgesteld. Tevens is gebruik gemaakt van de meest recente inzichten als gevolg van de lopende opdracht om een nieuwe werkwijzer voor maatschappelijke kosten-batenanalyses voor projecten binnen de digitale overheid op te stellen¹⁰.

Baten voor burgers zijn becijferd aan de hand van de daarvoor geldende voorschriften uit de Werkmap en Standaard Kosten Model (SKM) administratieve lasten burgers¹¹; de handleiding van het Ministerie van BZK voor het definiëren en meten van administratieve lasten als gevolg van beleid en regelgeving.

Het onderscheid tussen 'het fundament en het huis'

Voor de baten is het relevant om voor dit type e-overheidsbouwstenen een onderscheid te maken in de zogenaamde waarde van het fundament en de waarde van het huis. Een fundament kan direct al waarde hebben, maar de waarde van het fundament wordt voor een groot deel ook bepaald door de waarde van het huis dat er bovenop staat. Meer details van het huis geven ook meer inzicht in de waarde van het fundament. En zonder huis heeft een fundament (los van de waarde van een eventuele optie om een huis te bouwen) nauwelijks tot geen waarde en omgekeerd is het bouwen van een huis zonder een goed fundament niet mogelijk.

Hetzelfde geldt ook voor veel e-overheidsprojecten (bv. basisregistraties) en ook voor publieke eID-middelen. Het publieke eID-middel kan worden gezien als 'het fundament' en de digitale overheidsdiensten waarvoor een publiek eID-middel nodig is als 'het huis'. Het publieke eID-middel is randvoorwaardelijk voor het digitaal aan kunnen bieden van (nieuwe) overheidsdiensten.

⁸ CPB & PBL (2013), *Algemene leidraad voor maatschappelijke kosten-batenanalyses Den Haag*.

⁹ Ecorys & Conict (2007), *Handreiking voor kosten-batenanalyse voor ICT-projecten*. Rotterdam

¹⁰ Momenteel (begin 2018) uitgevoerd door de combinatie SEO/Ecorys/Van Economisch Zutphen Advies.

¹¹ Deze handleiding is te vinden op: https://www.kcwj.nl/sites/default/files/Standaardkostenmodel_Admlasten_burgers.pdf.

Eenzijds zijn er baten die samenhangen met het fundament, maar anderzijds hangen baten samen met het huis. De meerwaarde van een publiek eID-middel wordt pas gerealiseerd als er veel transacties met een publiek eID-middel worden afgehandeld. Het is daarbij ook van belang om inzicht te hebben in welke processen en overheidsdiensten kunnen gaan veranderen en hoe deze kunnen gaan veranderen (of hoe het huis eruitziet?). Daarbij zijn de baten van het fundament zekerder dan de baten van het huis (ook omdat voor de 'bouw van het huis' nog andere beleidsbeslissingen moeten worden genomen). De baten van het huis hebben meer het karakter van opties of mogelijkheden.

Om de efficiencyvoordelen van digitale diensten te kunnen realiseren, is alleen een publiek eID-middel niet voldoende, maar is het ook van belang dat de betreffende overheidsdiensten worden gedigitaliseerd. In het hoofdstuk met de use cases noemen we voorbeelden die een indicatie geven van de potentiële baten van het huis.

Gebruikte methodiek bij de impactanalyse

Bij het opstellen van de businesscase is extra aandacht geweest voor de impact die de invoering van eID op de gemeenten zal hebben. Er is gedetailleerd onderzoek gedaan en ook in beeld gebracht wat de gevolgen voor gemeenten van een aantal maatregelen zullen zijn waar nog niet definitief toe is besloten. Door zo volledig mogelijk alle mogelijke kosten in beeld te brengen in deze impact analyse wordt voorkomen dat kostenposten ten onrechte buiten beeld zouden kunnen blijven. Bij het bepalen van de impact, sluiten we aan bij de methodiek voor het maken van impact analyses van VNG Realisatie (voormalig KING). Dit houdt in dat we de impact voor gemeenten in beeld hebben gebracht met behulp van de SCOPAFIJTH-elementen (security, communicatie, organisatie, personeel, administratieve organisatie, financiën, informatie, juridisch, technologie, huisvesting). Financiering laten we hierbij buiten beschouwing, omdat dit geen onderdeel is van de business case.

In overleg met de Vereniging Directeuren Publieksdiensten (VDP), Nederlandse Vereniging voor burgerzaken (NVVB) en de Vereniging Nederlandse Gemeenten (VNG), is een vijftal gemeenten uit het Kennisnetwerk eID van de VNG geselecteerd, waarmee gesproken is over de impact op de afdelingen Burgerzaken doordat gemeenten de publieke middelen op niveau DigiD Hoog uitgeven, en de impact die aansluiten op eID op de gemeentelijke organisatie heeft.

Dezelfde gemeenten zijn geïnterviewd over mogelijke extra kosten en baten voor gemeenten die het gevolg zijn van de realisatie van het eID programma.

Gehanteerde aanpak

Uitgangspunt voor de herijking zijn de meest actuele formele documenten. Sinds het opstellen van de vorige business case, zijn er verschillende Project Startarchitecturen (PSA's) uitgewerkt. Tevens zijn de meest recente wetgeving en bijbehorende memories van toelichting geraadpleegd.

De PSA's en wetteksten vormen een belangrijke bron voor de bepaling van het nul- en project-alternatief. Voor het bepalen van de kosten in de herijking is uitgegaan van de aan ons beschikbaar gestelde bestedingsplannen en opdrachtbrieven. Aan de batenkant is gebruik gemaakt van beschikbare kengetallen, in combinatie met een prognose van het groeipad van het gebruik van de verschillende eID-middelen. Bij het bepalen van het groeipad zijn de gehanteerde uitgangspunten zoveel mogelijk gelijk gehouden aan de vorige business case, tenzij er een goede aanleiding was om uitgangspunten te wijzigen. In de beschrijvingen van het nul- en projectalternatief en de verschillende kosten- en batenposten, wordt middels voetnoten gerefereerd aan de gebruikte bronnen.

Aanvullend op de analyse van de genoemde documenten, zijn gesprekken gevoerd met het ministerie van Binnenlandse Zaken en Koninkrijksrelaties, het ministerie van Volksgezondheid, Welzijn en Sport (VWS), Dienst Wegverkeer (RDW), Logius, Rijksdienst voor Identiteitsgegevens (RvIG), Vereniging Directeuren Publieksdiensten (VDP), Nederlandse Vereniging voor burgerzaken (NVVB) en de Vereniging Nederlandse Gemeenten (VNG) om zowel de kosten als de baten goed in beeld te krijgen. Voor de impactanalyse en de use cases zijn specifieke interviews uitgevoerd met een aantal gemeenten en organisaties in de zorg. Voor dit onderdeel zijn ook gesprekken gevoerd met twee grote ICT-leveranciers in de sector gemeenten (zie bijlage 3).

Daarnaast is gebruik gemaakt van relevante rapporten. Ook naar deze bronnen wordt met voetnoten specifiek verwezen in de betreffende paragrafen.

1.4 Leeswijzer

Op basis van de onderzoeksopdracht, is gekozen voor een rapportage met (na deze inleiding) een drietal hoofdstukken, waarin alle aspecten binnen de reikwijdte van het onderzoek terugkomen. In **hoofdstuk 2** behandelen we het project- en nulalternatief en het groeipad van de middelen en het aantal authenticaties. **Hoofdstuk 3** bevat de resultaten op hoofdlijnen, waarbij we eerst ingaan op de gevolgen van de koerswijziging, nieuwe inzichten en de bredere scope. Daarna gaan we in de analyse wanneer de kosten en baten in evenwicht zijn, de belangrijkste resultaten van de impactanalyse bij de gemeenten en de resultaten van de use cases. In het afsluitende **hoofdstuk 4** beschrijven we uitgebreid de verschillende kosten- en de batenposten. In de **bijlagen** is (1) de uitwerking van de impactanalyse, (2) een beschrijving van de use cases, en (3) een lijst met interviewpartners opgenomen.

2 Project- en nulalternatief

In dit hoofdstuk is de herijking van de business case uitgewerkt. In de eerste paragraaf is een uitwerking gemaakt de probleemanalyse. In de tweede en derde paragraaf zijn het nulalternatief en het projectalternatief beschreven.

Er is bij de herijking van de business case naar gestreefd om uitgangspunten voor de business case zoveel mogelijk gelijk te houden aan de vorige business case¹², tenzij er een goede aanleiding was om uitgangspunten aan te passen. Er zijn drie redenen waarom onderdelen zijn gewijzigd: nieuwe en betere informatie (door bijvoorbeeld een nadere uitwerking van de plannen in Project Startarchitecturen, PSA's), wijzigingen van het beleid (zie bijvoorbeeld de brief van 23 juni 2017 van de minister van Binnenlandse Zaken en Koninkrijksrelaties¹³) en wijzigingen van de scope van de business case (eIDAS is bijvoorbeeld ook meegenomen in deze business case). Indien relevant is een uitgebreide toelichting gegeven op de wijzigingen ten opzichte van de vorige business case.

In een business case wordt altijd een vergelijking gemaakt tussen de ontwikkelingen met het gewenste beleid (projectalternatief) en de ontwikkelingen zonder dit beleid (nulalternatief). Op die manier wordt duidelijk wat de maatschappelijke kosten en baten van het beleid zijn. In deze paragraaf is eerst de probleemanalyse (de aanleiding voor het beleid) geschetst en daarna is ingegaan op het nulalternatief en het projectalternatief.

2.1 Probleemanalyse

De maatschappij digitaliseert. Ook de overheid zet grootschalig in op digitalisering, steeds meer diensten aan burgers worden langs het digitale kanaal afgehandeld. En in de toekomst zal het aantal transacties dat langs het digitale kanaal kan worden afgehandeld nog verder toenemen. Daarvoor is het wel essentieel dat dienstaanbieders - vanwege rechtmatigheid - zeker weten dat ze hun diensten aan de juiste persoon leveren. Bij dienstverlening aan de balie is het 'relatief eenvoudig' om vast te stellen of de dienst aan de juiste persoon wordt geleverd (door bv. om een WID-document te vragen en deze te vergelijken met de persoon voor de balie), bij digitale dienstverlening is dit minder goed mogelijk. Daarom zijn eID-middelen met een hoge betrouwbaarheid nodig, zodat dienstaanbieders zekerheid hebben over de (digitale) identiteit van de persoon die een transactie doet.

Vanaf 29 september 2018 is de Europese eIDAS-verordening van kracht en daarin zijn onder meer de criteria voor het vaststellen van betrouwbaarheidsniveaus van authenticatiemiddelen vastgelegd.¹⁴ De volgende betrouwbaarheidsniveau zijn te onderscheiden: minimale betrouwbaarheid, beperkte betrouwbaarheid (eIDAS laag), redelijke betrouwbaarheid (eIDAS substantieel) en hoge betrouwbaarheid (eIDAS hoog). Het Forum Standaardisatie heeft een handreiking¹⁵ geschreven voor dienstaanbieders waarmee dienstaanbieders zelf kunnen bepalen welke betrouwbaarheidsniveau vereist moet worden bij hun dienst.

¹² Ecorys & Van Zutphen Economisch Advies (2016), *Business case Inloggen in het BSN-domein. De kosten en baten van het eID-stelsel*.

¹³ Brief van de minister van Binnenlandse Zaken en Koninkrijksrelaties aan de Tweede Kamer der Staten-Generaal d.d. 23 juni 2017 betreffende 'Voortgangsrapportage programma eID' (TK 26 643, nr. 476).

¹⁴ Meer informatie hierover is te vinden op <https://www.digitaleoverheid.nl/dossiers/eidas/>.

¹⁵ Forum Standaardisatie (2016), *Handreiking betrouwbaarheidsniveaus voor digitale dienstverlening. Een handreiking voor overheidsinstanties*.

In deze handreiking zijn onder meer de volgende voorbeelden van diensten en betrouwbaarheidsniveaus opgenomen naar niveau van de authenticatie:

- **Geen eisen:** Anoniem bezoeken overheidswebsites, gemeentelijke lokale diensten (zoals meldingen over de openbare ruimte of aanvragen afvalcontainers) en inzien WOZ-waardering.
- **Laag:** Registreren gepersonaliseerde portalen, kapvergunning, evenementvergunning, omgevingsvergunning particulieren en aangifte lichte delicten (zoals een gestolen fiets).
- **Substantieel:** Melding voorgenomen huwelijk of geregistreerd partnerschap (door partners), aangifte geboorte (door ouder), vooringevulde aangifte Belastingdienst, aanvraag subsidie, aanvraag financiële toeslagen en aangifte ernstige delicten (zoals mishandeling of huiselijk geweld)
- **Hoog:** Raadplegen medisch dossier, raadplegen beslissingen bestuursorgaan met (medische) gegevens, raadplegen strafrechtelijke gegevens en aanvraag screening voor een derde.

Te zien is dat voor een groot aantal digitale diensten betrouwbaarheidsniveau substantieel of hoog-nodig is. Voordat het eID-programma was gestart, waren er nog geen eID-middelen op betrouwbaarheidsniveau substantieel en hoog. Het ontbreken van eID-middelen die voldoende betrouwbaar zijn betekent dat bepaalde digitale diensten helemaal niet tot stand komen of dat digitale diensten weliswaar worden aangeboden, maar dat er een lager betrouwbaarheidsniveau wordt gevraagd dan er eigenlijk nodig is (dit speelt bijvoorbeeld bij de genoemde voorbeelden onder substantieel). Dit betekent dat er eigenlijk onvoldoende zekerheid is over de identiteit van de burger en dat er diverse risico's zijn dat er iets mis gaat (fraude, misbruik, veiligheid en privacy).

Er is ook een scenario denkbaar, waarbij er zeer strikt wordt gehandhaafd op de voorschriften uit de Handreiking Betrouwbaarheidsniveaus. In dat geval zou een belangrijk deel van de huidige digitale dienstverlening achter DigiD Basis en DigiD Midden niet meer langs het digitale kanaal kunnen worden aangeboden (omdat substantieel hiervoor het adequate niveau is). Dat zou betekenen dat een groot aantal diensten weer op papier of aan alternatieve manier zouden moeten worden afgehandeld (denk bijvoorbeeld aan de vooringevulde aangifte van de Belastingdienst). Dat scenario zou tot zeer substantiële kosten voor organisaties en voor de maatschappij kunnen leiden.

Onderdeel van het eID-programma is de Wet digitale overheid. De Wet digitale overheid heeft onder meer als doel het regelen van het veilig en betrouwbaar kunnen inloggen voor burgers en bedrijven bij de (semi-)overheid.¹⁶ Met veilig en betrouwbaar inloggen wordt bedoeld dat burgers elektronische identificatiemiddelen (eID-middelen) krijgen met een hogere mate van betrouwbaarheid dan het huidige DigiD. Deze identificatiemiddelen geven publieke dienstverleners meer zekerheid over iemands identiteit. De wet stelt daarnaast open standaarden verplicht. Hiermee implementeert Nederland de EU-richtlijn over toegankelijkheid van overheidswebsites en apps. De Wet digitale overheid biedt een kader voor oplossingen voor de eerder in deze paragraaf geschetste problemen.

Met betrekking tot de scope van de analyse is het volgende nog van belang. Er is alleen gekeken naar het burgerdomein en niet naar het bedrijvendomein.¹⁷ En er is ook alleen gekeken naar het gebruik van eID-middelen voor de toegang tot het BSN-domein.^{18, 19} DigiD Machtigen is eveneens buiten de scope van de business case gelaten. Er is in de analyse ook alleen gekeken naar de

¹⁶ <https://www.digitaleoverheid.nl/voorzieningen/identificatie-en-authenticatie/eid/wet-gdi/>

¹⁷ Bedrijven kunnen gebruik maken van eHerkenningmiddelen.

¹⁸ BSN staat voor Burgerservicenummer. Het BSN is een uniek persoonsnummer voor iedereen die ingeschreven staat in de Basisregistratie Personen (BRP). Met het BSN-domein wordt bedoeld het domein waarbinnen het gebruik van het BSN wettelijk is voorgeschreven, zijnde publieke taken uitgevoerd door overheidsinstanties, zorgverzekeraars, zorgaanbieders, pensioenfondsen en onderwijsinstellingen.

¹⁹ Publieke eID-middelen mogen ook alleen in het BSN-domein worden gebruikt, zie artikel 8 'Gebruik in publieke domein' van de Wet Digitale Overheid (conceptversie 8 december 2017).

doelgroep van de huidige gebruikers van DigiD Basis en DigiD Midden en naar Europese burgers die inloggen met een aangemeld middel (volgend uit de eIDAS-verordening). Eventuele extra maatregelen om minder digivaardige burgers, die nu nog geen DigiD gebruiken, te ondersteunen zijn ook buiten de scope van de analyse gelaten.

2.2 Nulalternatief

Voor een goede vergelijkbaarheid van deze business case met de vorige business case zijn de uitgangspunten in het nulalternatief zoveel mogelijk gelijk gehouden. Het nulalternatief beschrijft de 'theoretische' ontwikkeling met betrekking tot inloggen in het BSN-domein voor de periode 2015-2027 ervan uitgaande dat er in 2015 niet was gestart met het eID-programma. In de tekstbox hieronder is het nulalternatief opgenomen.²⁰

Op dit moment hebben burgers verschillende manieren om zich digitaal te kunnen identificeren en authenticeren. In het BSN-domein is DigiD het meest gebruikt (soms in combinatie met sms) door burgers om in te loggen in de digitale omgeving van overheidsdienstaanbieders om hier informatie in te zien en transacties af te kunnen handelen.

Het aantal transacties is in de laatste jaren sterk gegroeid van 117 miljoen authenticaties in 2013 naar 280 miljoen²¹ authenticaties met DigiD door burgers in 2017.

Naast DigiD bestaan er nog alternatieve manieren om in te loggen in de digitale omgeving van overheidsdienstaanbieders. Zo wordt er bv. nog gebruik gemaakt van eigen gebruikersnaam-wachtwoord combinaties of van alternatieve authenticatiesystemen.

Een deel van de digitale diensten van overheidsdienstaanbieders is echter nog niet ontsloten, omdat de betrouwbaarheid van DigiD onvoldoende is, hiervoor zijn middelen met een hogere betrouwbaarheid vereist.

Aanvulling: eIDAS-verordening binnen scope

Er is ten opzichte van de vorige business case wel een wijziging in de scope van de analyse. In verband met de behoefte aan een integrale afweging van kosten en baten van het gehele eID-domein voor burgers is ook de eIDAS-verordening meegenomen in de analyse. De eIDAS-verordening stelt dat Europese burgers en bedrijven vanaf 29 september 2018 bij alle Nederlandse organisaties in de publieke sector moeten kunnen inloggen met een door Europa erkend nationaal inlogmiddel. Het doel van deze verordening is dat het gemakkelijker en veiliger wordt om binnen Europa online zaken te regelen.

Ook in het nulalternatief is de eIDAS-verordening van toepassing. In het nulalternatief wordt ervan uitgegaan dat er alleen middelen zijn op betrouwbaarheidsniveau laag. De eIDAS-verordening geeft aan dat een organisatie alleen Europese burgers en bedrijven met een Europees erkend inlogmiddel toegang dient te verlenen als de organisatie ook Nederlandse burgers en bedrijven op betrouwbaarheidsniveau substantieel of hoog accepteert.²² Aangezien er in het nulalternatief geen middelen op betrouwbaarheidsniveau substantieel of hoog zijn, 'accepteren' Nederlandse organisaties deze middelen ook niet. En in dat geval hoeven buitenlandse middelen ook niet

²⁰ Deze beschrijving van het nulalternatief is integraal overgenomen uit Ecorys & Van Zutphen Economisch Advies (2016), *Business case Inloggen in het BSN-domein. De kosten en baten van het eID-stelsel*.

²¹ In de vorige business case stond hier aantal van 263 miljoen opgenomen (dat was een voorlopig cijfer over 2016). Het hier genoemde aantal van 280 miljoen is het definitieve cijfer over 2017 en is ontvangen van Logius.

²² Zie <https://www.eherkenning.nl/vraag-antwoord/eidas/>.

geaccepteerd te worden. Met andere woorden: de verordening is er dan nog steeds, maar dit heeft geen consequenties voor Nederlandse dienstverleners (geen kosten en geen baten).

2.3 Projectalternatief

Bij de beschrijving van het projectalternatief is ervan uitgegaan dat er een eID-stelsel komt voor de modernisering van het inloggen en overgaan op een hogere betrouwbaarheid voor officiële online authenticatie. Ook het projectalternatief is in deze analyse zo veel mogelijk gelijk gehouden aan de vorige business case.²³ Ten opzichte van de vorige business case zijn er in de tussentijd verschillende Project Startarchitecturen (PSA's) uitgewerkt en dat heeft ook gevolgen gehad voor de gekozen oplossingen.²⁴

Bij de beschrijving van het projectalternatief is een onderscheid gemaakt naar de eID-stelselvoorzieningen, de authenticatiediensten, de eIDAS-voorzieningen, het aansluiten van dienstverleners en de eID-middelen.

eID-stelselvoorzieningen

Het projectalternatief gaat ervan uit dat er een eID-stelsel komt voor de modernisering van het inloggen en het overgaan op een hogere betrouwbaarheid voor officiële online authenticatie. Daarvoor moeten verschillende stelselvoorzieningen worden gerealiseerd: een set van eisen & toezicht en beheer, een BSN-koppelregister en een routeringsvoorziening voor de aansluiting van dienstverleners (ontzorging).

Set van eisen & toezicht en beheer

In de vorige business case is uitgegaan van de Uniforme Set van Eisen (USvE).²⁵ Deze USvE is na de consultatie van het wetsontwerp en de USvE²⁶ vervangen door een set van eisen zoals opgenomen in de Beleidsregels eID. Belangrijkste wijzigingen betreffen het abstractieniveau van de regels (meer gericht op het wat, niet op het hoe van de oplossing) en nieuwe eisen met betrekking tot de routeringsvoorziening, meervoudige aansluitingen, het afleiden van middelen en misbruikbestrijding.

Naast het vaststellen van de set van eisen moeten hier ook kosten worden gemaakt voor het beheer (communicatie, beheer van de privacy impactassessment en risicoanalyse op de set van eisen, secretariaat en changes). Tevens moeten kosten gemaakt worden voor de aanbesteding van private middelen, toezicht en beheer op de partijen die diensten en producten leveren voor het inloggen in het BSN-domein.

BSN-koppelregister

Het BSN-koppelregister (BSNk) is een voorziening die een relatie legt tussen een uniek identificerend kenmerk op een privaat authenticatiemiddel of Europees middel en het BSN van de houder. Een private authenticatiedienst authentificeert de gebruiker, maar het BSNk levert

²³ Ecorys & Van Zutphen Economisch Advies (2016), *Business case Inloggen in het BSN-domein. De kosten en baten van het eID-stelsel*.

²⁴ Hierbij moet worden opgemerkt dat de wijzigingen in de brief van de minister van Binnenlandse Zaken en Koninkrijksrelaties aan de Tweede Kamer der Staten-Generaal d.d. 23 juni 2017 betreffende 'Voortgangsrapportage programma eID' (TK 26 643, nr. 476) nog niet zijn verwerkt in de diverse PSA's. Waar relevant is aangegeven of wijzigingen uit de brief mogelijk consequenties hebben voor de kosten en baten.

²⁵ De USvE is een normatieve set van eisen die gebruikt wordt voor toelating en toezicht van hetgeen met die verordening wordt beoogd, zodat op basis daarvan door de minister van Binnenlandse Zaken en Koninkrijksrelaties een Nederlands kader kan worden vastgesteld.

²⁶ Zie <https://www.internetconsultatie.nl/wetqdi/details>.

uiteindelijk het BSN aan de dienstverlener op basis van het pseudoniem van de authenticatiedienst.²⁷ Het BSNk heeft daarmee een soort van vertaalfunctie. Het BSNk is een GDI-bouwsteen en heeft verschillende functies: activatie, transformatie, sleutelbeheer, stelselbeheer, inzageregister en misbruikdetectie-register. In het inzageregister wordt per gebruiker bijgehouden welke middelen op zijn naam staan en wat de status is van deze middelen.²⁸

Routeringsvoorziening

Voor de aansluiting op het eID-stelsel kunnen dienstaanbieders gebruik maken van een routeringsvoorziening. De routeringsvoorziening zorgt ervoor dat diverse 'landschappen' (publieke eID-middelen, private eID-middelen, Europese eID-middelen (eIDAS) en eHerkenningmiddelen) kunnen worden ontsloten via één koppelvlak.²⁹ Het is de verwachting dat de routeringsvoorziening vanaf het eerste kwartaal van 2019 beschikbaar is. De versie van de routeringsvoorziening, die vanaf begin 2019 beschikbaar komt, kan overigens nog niet omgaan met polymorphe pseudoniemen. Dit gaat op een later tijdstip nog leiden tot een wijziging in de koppelvlakspecificaties van de routeringsvoorziening.

Authenticatiediensten

De authenticatiedienst bepaalt op basis van het gebruikte inlogmiddel of een gebruiker daadwerkelijk is wie hij beweert te zijn (dat een bepaalde identiteit terecht wordt geclaimd). Op dit moment is er reeds een authenticatiedienst voor DigiD Basis en DigiD Midden. Deze bestaande authenticatiedienst moet in het projectalternatief worden aangepast naar een authenticatiedienst voor alle publieke eID-middelen.

Indien private middelen worden toegelaten voor gebruik in het BSN-domein, dan moet er ook één (of meerdere) authenticatiedienst(en) komen voor het afhandelen van de authenticaties van private middelen. Deze kosten maken onderdeel uit van de business case van de private partijen, die voorafgaand aan de aanbesteding vanzelfsprekend nog niet bekend is. Deze kosten zijn niet apart inzichtelijk gemaakt.

eIDAS-voorzieningen

De eIDAS-verordening stelt dat Europese burgers en bedrijven vanaf 29 september 2018 bij alle Nederlandse organisaties in de publieke sector moeten kunnen inloggen met een door Europa erkend nationaal inlogmiddel als zij voor hun diensten betrouwbaarheidsniveau substantieel of hoog accepteren. Op centraal niveau zijn er verschillende voorzieningen nodig voor de implementatie van eIDAS in Nederland. De volgende componenten maken onderdeel uit van de eIDAS functionaliteit:³⁰

- eIDAS koppelpunt. Het eIDAS koppelpunt faciliteert de interoperabiliteit tussen het Nederlandse eTD-stelsel en buitenlandse eIDAS koppelpunten. Het eIDAS koppelpunt bestaat uit een eIDAS connector (functionaliteit voor koppeling aan buitenlandse authenticatiestelsels), een eIDAS proxyservice (functionaliteit voor koppeling van nationale authenticatiestelsel op buitenlandse dienstverleners) en een eIDAS berichtenservice (brugfunctie tussen Europese eIDAS componenten en het nationale eTD-stelsel).
- BRP koppelpunt. Met behulp van het BRP koppelpunt kan worden vastgesteld of een persoon die met een buitenlands eID-middel inlogt al in de Basisregistratie Personen (BRP) bekend is en derhalve in het bezit is van een BSN.
- Stelsel Elektronische Toegangsdiensten (eTD-stelsel). Het (reeds bestaande) eTD-stelsel bestaat uit de infrastructuur en het afsprakenstelsel voor federatieve toegangsdiensten (Idensys

²⁷ Logius (2016), *BSNk voor de Uniforme Set van Eisen 1.0. Projectstartarchitectuur – Architectuurkaders*.

²⁸ De PSA van het BSNk is weliswaar gebaseerd op de USvE, maar de kostenramingen die zijn gebruikt voor het BSNk zijn wel gebaseerd op de set van eisen (*Bestedingsplan 2018 eID-voorziening opgesteld door het ministerie van BZK*).

²⁹ Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (2017), *Onderzoek ontzorging*.

³⁰ Logius (2017), *Startarchitectuur. Nationale implementatie van eIDAS met het stelsel Elektronische Toegangsdiensten*.

voor burgers en eHerkenning voor bedrijven). Er is voor gekozen om de eIDAS infrastructuur onder te brengen binnen het eTD-stelsel.

- BSNk. Het BSNk zorgt voor de koppeling van een authenticatiemiddel aan het BSN (zie ook de eerdere paragraaf over het BSNk).

In de vorige business case viel de eIDAS-verordening buiten de scope van de analyse, vandaar dat deze voorzieningen in de vorige business case niet zijn meegenomen.

Aansluiten dienstverleners

Dienstverleners beschikken reeds over een DigiD aansluiting. Zij moeten straks aansluiten op het eID-stelsel. Voor de aansluiting op het eID-stelsel kunnen dienstverleners gebruik maken van een routeringsvoorziening. In de vorige business case was het aansluiten van de dienstverleners nog niet uitgewerkt. In de vorige business case is daarom het uitgangspunt gehanteerd dat de dienstverleners gebruik konden blijven maken van het huidige DigiD koppelvak om ook aan te sluiten op het eID-stelsel (en daarmee zonder noemenswaardige aanvullende investeringen).

Dienstverleners moeten niet alleen aansluiten op het eID-stelsel, maar moeten vanaf 29 september 2018 ook voldoen aan de eisen van de eIDAS-verordening. De eIDAS-verordening geeft aan dat een organisatie Europese burgers en bedrijven met een Europees erkend inlogmiddel toegang dient te verlenen als de organisatie ook Nederlandse burgers en bedrijven op betrouwbaarheidsniveau substantieel of hoog accepteert.³¹ Dienstverleners die diensten met DigiD Basis of DigiD Midden aanbieden, accepteren ook automatisch DigiD Substantieel. Dat betekent dat alle Nederlandse dienstverleners die DigiD gebruiken vanaf 29 september 2018 ook genotificeerde Europese eID-middelen moeten accepteren. De enige manier om in Nederland vanaf 29 september 2018 te voldoen aan de eIDAS verordening is door Europese burgers en bedrijven toegang te verlenen via het eTD-koppelvak versie 1.11 van eHerkenning of Idensys via een eHerkenning- of Idensys-makelaar.³² Vanaf het eerste kwartaal van 2019 (ongeveer 3 maanden later) kunnen dienstverleners ook gebruik maken van de routeringsvoorziening om te voldoen aan de eIDAS-verordening.³³

Het is de vraag in hoeverre dienstverleners voor een periode van drie maanden eerst over zullen gaan naar het eTD-koppelvak en drie maanden later naar het koppelvak van de routeringsvoorziening. In het algemeen is het aansluiten op een nieuw of substantieel gewijzigd koppelvak namelijk een impactvolle exercitie (niet alleen financieel, maar ook technisch).

Voor deze business case is het uitgangspunt gehanteerd dat de dienstverleners acteren compliant met geldende wet- en regelgeving. Dat betekent dat de kosten voor de migratie naar het eTD-koppelvak en de kosten voor de migratie naar de routeringsvoorziening drie maanden later hebben meegenomen in de business case.³⁴ Of deze kosten ook daadwerkelijk tot uitgaven gaan leiden is daarbij op dit moment ongewis.

eID-middelen

Naast een eID-stelsel is het ook van belang dat burgers beschikken over middelen om mee in te kunnen loggen. In deze paragraaf worden de verschillende eID-middelen besproken: DigiD Basis, DigiD Midden, DigiD Substantieel, DigiD Hoog en private middelen.

³¹ Zie <https://www.eherkenning.nl/vraag-antwoord/eidas/>.

³² Zie ook bijvoorbeeld <https://www.digitaleoverheid.nl/nieuws/staatssecretaris-knops-voortgang-eid/>.

³³ Er zal dan overigens nog wel enige tijd overheen gaan voordat alle dienstverleners zijn aangesloten op de routeringsvoorziening.

³⁴ Vanzelfsprekend zijn ook de baten daarvan meegenomen.

DigiD Basis en DigiD Midden

De huidige middelen DigiD Basis en DigiD Midden zijn middelen op eIDAS-betrouwbaarheidsniveau laag. DigiD Basis bestaat uit een gebruikersnaam en wachtwoord. Bij DigiD Midden logt de burger in via de DigiD app of logt de burger in met zijn DigiD Basis gebruikersnaam en wachtwoord aangevuld met een code die via sms wordt ontvangen. De minister van Binnenlandse Zaken en Koninkrijksrelaties heeft aangegeven dat de eID-middelen op betrouwbaarheidsniveau laag in overleg met de belangrijkste (semi-) publieke dienstverleners zullen worden uitgefaseerd.³⁵ Een verplichting voor dienstaanbieders om eID-middelen op eIDAS-betrouwbaarheidsniveau substantieel of hoog te gaan gebruiken is voorzien nadat DigiD Substantieel - in combinatie met een eventueel toegelaten privaat eID-middel - een zeer hoge dekkinggraad heeft binnen de doelgroep van de huidige DigiD gebruikers.³⁶

DigiD Substantieel

Om DigiD Substantieel te krijgen moeten burgers met hun DigiD app een eenmalige controle uitvoeren op een van de volgende WID-documenten (paspoort, rijbewijs of identiteitskaart (NIK)). Hiervoor is het nodig dat de burger een smartphone met te gebruiken Near Field Communication (NFC)³⁷ heeft om de chip uit het WID-document uit te kunnen lezen. Ongeveer 40% van de burgers heeft een bruikbare NFC chip op zijn smartphone.³⁸ Een bruikbare NFC chip zit op de nieuwere Android smartphones en tablets. iPhones hebben ook een NFC-functionaliteit, maar deze functionaliteit is (op dit moment) niet opengesteld voor breder gebruik, zoals bv. het uitlezen van WID-documenten. Er wordt momenteel nagedacht over oplossingen voor burgers die geen smartphone met bruikbare NFC-chip hebben.

Vanaf dat moment kan de burger dan eenvoudig met zijn DigiD app inloggen op substantieel betrouwbaarheidsniveau zonder opnieuw iedere keer het identiteitsbewijs uit te hoeven lezen.

DigiD Hoog

Het publieke middel DigiD Hoog verwijst naar een chipkaart toepassing die op de chip van een document als genoemd in de Wet op de Identificatieplicht (WID-document) wordt geplaatst om de houders van het document in staat te stellen zich bij dienstverleners te identificeren en authenticeren. Hiervoor wordt een e-functionaliteit aan de NIK en het rijbewijs toegevoegd. Voor de uitrol van DigiD Hoog wordt aangesloten bij het natuurlijke vervangingspatroon van de betreffende WID-documenten.³⁹

Als een burger vanaf mei 2018 een nieuw eRijbewijs aanvraagt of vanaf januari 2019 een nieuwe eNIK, dan krijgt de burger hier ook automatisch het publieke eID-middel op bijgeplaatst (het eID wordt standaard op alle exemplaren van het publieke middel aangebracht). De burger heeft dan zelf de keuze om de eID-functionaliteit expliciet te activeren en te gebruiken. De burger activeert de eID-functionaliteit zelf met pincode, die hij in een PIN/PUK-brief heeft ontvangen van de middelenuitgever.⁴⁰

³⁵ Zie de brief van de minister van Binnenlandse Zaken en Koninkrijksrelaties aan de Tweede Kamer der Staten-Generaal d.d. 23 juni 2017 betreffende 'Voortgangsrapportage programma eID' (TK 26 643, nr. 476).

³⁶ Zie *Algemene regels inzake het elektronisch verkeer in het publieke domein en inzake de generieke digitale infrastructuur (Wet digitale overheid)*. Memorie van Toelichting, concept 8 december 2017.

³⁷ Near Field Communication of NFC is een techniek om draadloos kleine hoeveelheden data uit te wisselen met een bereik van ongeveer 10 centimeter.

³⁸ Zie Verdonck, Klooster & Associates (2017), *Expert opinion publieke authenticatie. Advies over implementatiestrategie DigiD substantieel en hoog en alternatieven*.

³⁹ Zie ook paragraaf 2.1.4 over het groeipad.

⁴⁰ De uitgangspunten in deze en de volgende alinea zijn niet veranderd ten opzichte van de vorige business case en zijn nu ook opgenomen in de PSA voor DigiD hoog (Architectuurgroep Publiek Middel hoog (2017), *Projectstartarchitectuur DigiD hoog. Identificeren en authenticeren met je identiteitskaart of rijbewijs*).

Een gebruiker die in wil loggen met DigiD Hoog kan daarvoor zijn DigiD app gebruiken in combinatie met een smartphone met NFC⁴¹ om de chip in de eNIK of het eRijbewijs uit te lezen (dat moet worden gedaan bij iedere inlog). Daarna wordt de gebruiker gevraagd om zijn pincode in te voeren en krijgt de gebruiker toegang tot diensten op betrouwbaarheidsniveau hoog. Het is ook mogelijk om de eNIK of het eRijbewijs op een contactloze NFC-reader te plaatsen en met een pincode in te loggen.

Er moet bij het gebruik van een eNIK altijd kunnen worden vastgesteld of een NIK nog geldig is en wat de status is van het document. Voor de eNIK moet daarvoor het bestaande negatief register (waarin alle documenten staan opgenomen die niet in omloop mogen zijn) worden omgebouwd naar een positief register (met de statussen van alle WID-documenten).⁴² Dit is voorzien met het basisregister reisdocumenten. Het ministerie van BZK heeft aangegeven dat dit basisregister reisdocumenten er sowieso zal komen (of er nu wel of geen eNIK komt). Daarmee is het basisregister reisdocumenten niet onderscheidend voor het projectalternatief en het nulalternatief en heeft het geen impact op deze business case.

Private middelen

De minister van Binnenlandse Zaken en Koninkrijksrelaties heeft in de kamerbrief d.d. 23 juni 2017 aangegeven voorrang te geven aan de realisatie van publieke middelen (DigiD Substantieel en DigiD Hoog). Tevens is in die brief aangegeven dat het gewenst is dat er naast de publieke eID-middelen een of meerdere alternatieven voor betrouwbaarheidsniveau substantieel breed beschikbaar komen. Daarvoor is in 2017 een (markt)verkenning geïnitieerd op basis waarvan een besluit zal worden genomen over de vervolgstappen. Dat is gewijzigd ten opzichte van de vorige business case, waarin het uitgangspunt was dat alle private middelen op betrouwbaarheidsniveau substantieel en hoog toegelaten konden worden op voorwaarde dat zij zouden voldoen aan de Uniforme Set van Eisen.

De staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties geeft in de brief d.d. 31 januari 2018 aan dat er een marktconsultatie is geweest en dat de hoofdconclusie is dat marktpartijen naar verwachting kunnen voldoen aan de doelstellingen en eisen van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties.⁴³ De komende maanden wordt de aanbesteding voorbereid om één of meerdere private eID-middelen te kunnen toelaten voor het gebruik op (ten minste) een substantieel betrouwbaarheidsniveau. De staatssecretaris schrijft eveneens in zijn brief dat uit de aanbestedingsprocedure definitief zal blijken of en zo ja welke marktpartijen kunnen worden toegelaten en tegen welke prijs.

Vanwege bovenstaande ontwikkelingen zijn de kosten en baten van de mogelijk toe te laten private middelen als PM-post opgenomen in de business case. Het is aan te raden om de business case weer te herijken als er meer informatie is uit de aanbestedingsprocedure.

2.3.1 Groeipad

Het groeipad van het gebruik van de verschillende eID-middelen is een belangrijke factor voor de hoogte van de kosten en baten van de business case van inloggen in het BSN-domein. Bij het bepalen van het groeipad zijn de gehanteerde uitgangspunten zoveel mogelijk gelijk gehouden aan de vorige business case, tenzij er een goede aanleiding was om uitgangspunten te wijzigen.

⁴¹ Ongeveer 40% van de burgers heeft een smartphone met een bruikbare NFC-chip.

⁴² Voor rijbewijzen is er reeds een positief register.

⁴³ Brief van de staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties aan de Tweede Kamer der Staten-Generaal d.d. 31 januari 2018 betreffende 'Voortgangsbrief programma eID juli – december 2017' (TK 26 643 nr. 514).

De volgende uitgangspunten zijn gewijzigd ten opzichte van de vorige business case:

- Uitgangspunt in de vorige business case was dat betrouwbaarheidsniveau laag (DigiD Basis en DigiD Midden) vanaf 2020 volledig zou zijn uitgefaseerd en dat burgers vanaf 2020 minimaal gebruik zouden gaan maken van een middel op betrouwbaarheidsniveau substantieel. Dat zal nu niet eerder zijn dan 2023 rekening houdend met de overgangstermijnen zoals genoemd in de Wet Digitale Overheid. Er blijkt⁴⁴ daarnaast dat ongeveer 40% van de burgers een smartphone met bruikbare NFC heeft, die nodig is om de chip uit het WID-document uit te kunnen lezen om de DigiD app naar betrouwbaarheidsniveau substantieel op te waarderen. Er is onderzoek⁴⁵ gedaan naar alternatieven om ervoor te zorgen dat ook de overige 60% kan beschikken over DigiD Substantieel. Op dit moment is er echter nog geen besluit genomen over een geschikte oplossing om ervoor te zorgen dat deze groep de beschikking krijgt over een eID-middel op niveau substantieel. Private middelen kunnen mogelijk ook bijdragen aan een oplossing om ervoor te zorgen dat alle burgers een eID-middel op (ten minste) betrouwbaarheidsniveau substantieel krijgen, maar pas nadat uit de aanbestedingsprocedure zal blijken of marktpartijen kunnen worden toegelaten en tegen welke prijs. Voor deze business case zijn daarom twee verschillende groeipaden geschetst: een groeipad (zonder aanvullend beleid) en een potentieel groeipad inclusief activiteiten voor verbreding van de doelgroep én inclusief private middelen.
- In de herijking is het startjaar voor het gebruik van DigiD Hoog 2019, in de vorige business case was 2017 het startjaar voor het gebruik van DigiD Hoog. Uitgangspunt is dat de eerste eRijbewijzen worden uitgegeven vanaf mei 2018 (was januari 2018 in de vorige business case) en de eerste eNIK's worden uitgegeven vanaf januari 2019 (was januari 2018 in de vorige business case).
- Er komen vooralsnog geen private eID-middelen op betrouwbaarheidsniveau hoog, de nog te starten aanbestedingsprocedure gaat alleen over eID-middelen op betrouwbaarheidsniveau substantieel. Dat betekent dat de eNIK en het eRijbewijs de enige middelen worden op betrouwbaarheidsniveau hoog. In de vorige business case was het uitgangspunt dat de burger mogelijk ook gebruik kon maken van private middelen met betrouwbaarheidsniveau hoog.

Naast bovengenoemde verschillen zijn de overige uitgangspunten voor zover mogelijk gelijk gehouden. Voor het groeipad van DigiD Hoog is aangesloten bij het natuurlijke vervangingspatroon van de eNIK en het eRijbewijs. Het uitgiftetempo is opgenomen in de volgende tabel:

⁴⁴ Zie Verdonck, Klooster & Associates (2017), *Expert opinion publieke authenticatie. Advies over implementatiestrategie DigiD substantieel en hoog en alternatieven.*

⁴⁵ Logius (2017), *Verbreden doelgroep DigiD substantieel. Concept eindversie 0.91.*

Tabel 2.1 Uitgiftetempo publieke eID-middelen (in miljoenen)

Jaar	NIK	Rijbewijs	DigiD Hoog (nieuw) ^{b)}	DigiD Hoog (cumulatief)
2018 ^{a)}	0	1,2	0,9	0,9
2019	0,7	1,8	1,5	2,4
2020	0,6	1,8	1,4	3,8
2021	0,9	1,5	1,2	5,0
2022	0,4	1,1	0,9	5,9
2023	0,3	1,1	0,9	6,8
2024	1,2	1,1	1,1	7,9
2025	1,5	1,1	1,2	9,0
2026	1,8	1,3	1,3	10,3
2027	1,3	1,9	1,8	12,1

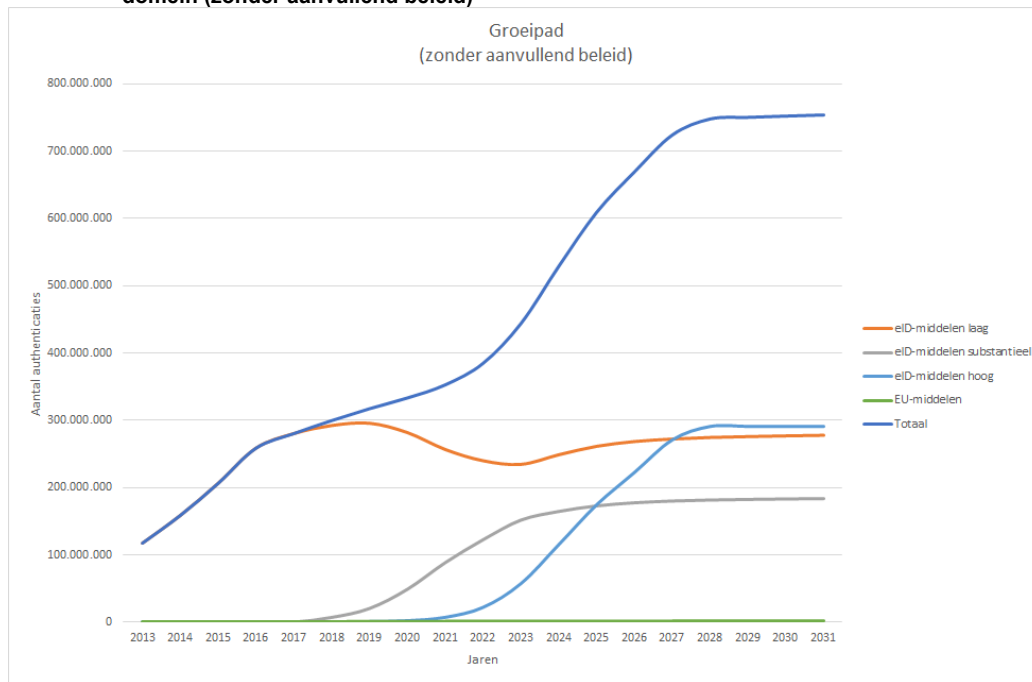
- a) In deze business case is het uitgangspunt gehanteerd dat de eerste eRijbewijzen vanaf mei 2018 en de eerste eNIK's vanaf januari 2019 worden uitgegeven. In de vorige business case werd ervan uitgegaan dat er in 2018 1,1 miljoen NIK's en 1,8 miljoen rijbewijzen werden uitgegeven.
- b) In de kolommen DigiD Hoog (nieuw) en DigiD Hoog (cumulatief) is het aantal burgers (in miljoenen) opgenomen met DigiD Hoog. Hierbij is rekening gehouden dat burgers meerdere middelen kunnen hebben (NIK en rijbewijs of meerdere rijbewijzen).

Net als in de vorige business case is ook nu weer gekeken hoe het beeld eruit ziet als het aantal authenticaties in het BSN-domein even groot is als het aantal authenticaties in het zorg- en sociale domein.⁴⁶ Tevens is het uitgangspunt gehanteerd dat voor 80% van de authenticaties in het zorg- en sociale domein betrouwbaarheidsniveau hoog vereist is.

In de onderstaande twee figuren is een schets gemaakt van twee mogelijke groeipaden. In de eerste figuur is de ontwikkeling getoond als slechts 40% van de burgers de beschikking krijgt over DigiD Substantieel (er komen geen aanvullende activiteiten om de doelgroep te verbreden én er komen geen private eID-middelen) en dat deze groep binnen een periode van 4 jaar ook DigiD Substantieel gaat gebruiken. In dat geval blijven eID-middelen op betrouwbaarheidsniveau laag (DigiD Basis en DigiD Midden) nodig voor meer dan een derde van de transacties. Te zien is dat de groei van substantieel gelimiteerd is. Mede daardoor vlakt het gebruik op betrouwbaarheidsniveau laag eerst iets af (gebruikers die van laag naar substantieel gaan, 40% van de gebruikers) en daarna weer opnieuw gaat groeien (door de autonome groei van het aantal authenticaties).

⁴⁶ Op dit moment zijn er nog beperkt digitale diensten voor burgers in het zorg- en sociale domein, omdat er (nog) geen eID-middelen zijn met een voldoende hoog betrouwbaarheidsniveau.

Figuur 2.1 Illustratief groeipad als # authenticaties BSN-domein = # authenticaties zorg- en sociale domein (zonder aanvullend beleid)

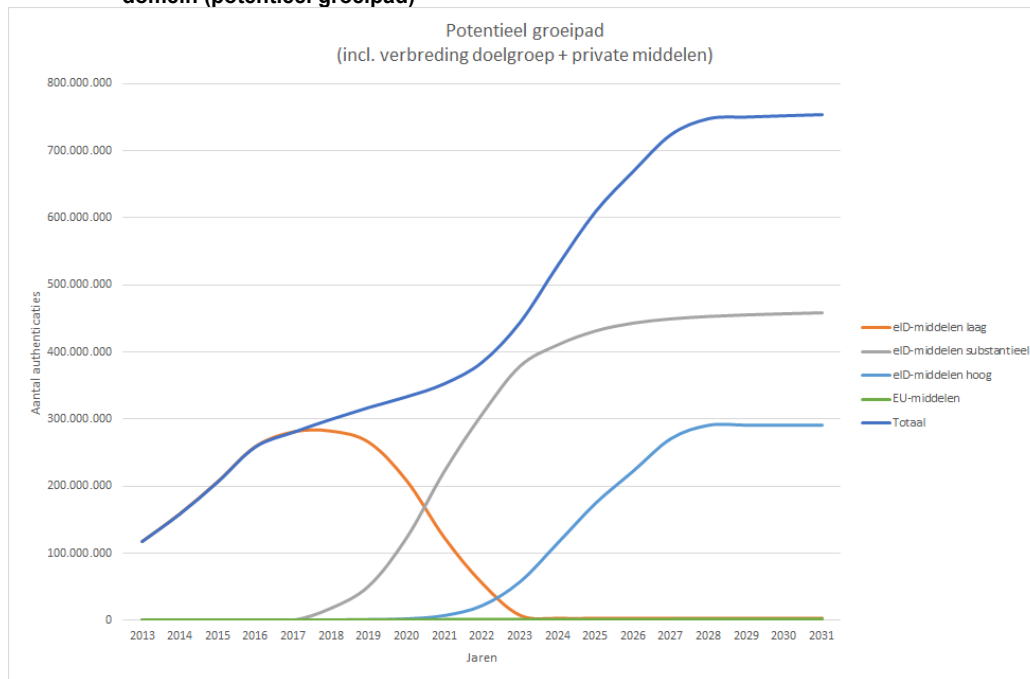


In beide figuren zijn ook de ontwikkelingen van eID-middelen op betrouwbaarheidsniveau hoog en de ontwikkelingen van EU-middelen (volgend op de eIDAS-verordening⁴⁷) meegenomen. De groeipaden voor betrouwbaarheidsniveau hoog zijn gelijk in figuur 2.1 en figuur 2.2.

In de tweede figuur is het potentiële groeipad gepresenteerd als alle huidige DigiD gebruikers wel de beschikking krijgen over een eID-middel op betrouwbaarheidsniveau substantieel (DigiD Substantieel of een privaat middel) en deze ook gaan gebruiken. In dat geval kunnen DigiD Basis en DigiD Midden vanaf 2023 worden uitgefaseerd.

⁴⁷ De aantallen transacties door EU-burgers zijn gebaseerd op een kwantitatieve analyse van PBLQ over de belasting van het eIDAS koppelvlak. In vergelijking met het totaal gaat het hier om beperkte aantallen (maximaal 1,5 miljoen transacties per jaar).

Figuur 2.2 Illustratief groeipad als # authenticaties BSN-domein = # authenticaties zorg- en sociale domein (potentieel groeipad)



Als alle burgers de beschikking hebben over middelen op betrouwbaarheidsniveau substantieel dan kan betrouwbaarheidsniveau laag worden uitgefaseerd. In de Memorie van Toelichting bij de Wet Digitale Overheid is een overgangperiode opgenomen van maximaal vier jaar dat het mogelijk is betrouwbaarheidsniveau laag te accepteren waarvoor substantieel vereist is (en maximaal zeven jaar om betrouwbaarheidsniveau substantieel te accepteren waarvoor hoog vereist is).⁴⁸ In de figuur zijn middelen op betrouwbaarheidsniveau laag vanuit 2023 uitgefaseerd.

⁴⁸ In de Memorie van Toelichting is opgenomen, dat dit pas relevant wordt als er een zeer hoge dekking is van middelen op het betreffende betrouwbaarheidsniveau, zie de volgende zinsnede: "Met het oog op massale processen zoals het doen van belastingaangifte ligt het voor de hand de verplichting voor bestuursorganen en aangewezen organisaties om identificatiemiddelen van betrouwbaarheidsniveau substantieel of hoog te gebruiken niet eerder in werking te laten treden, dan nadat DigiD substantieel - in combinatie met een eventueel toegelaten privaat identificatiemiddel - een zeer hoge dekking heeft binnen de doelgroep van de 13,6 miljoen DigiD-gebruikers."

3 Resultaten op hoofdlijnen

3.1 Gevolgen koerswijziging, nieuwe inzichten en bredere scope

Nieuwe business case noodzakelijk

De vorige business case uit 2016 gaf al een goed inzicht in de kostenraming en potentiële baten van de invoering van middelen met een hogere betrouwbaarheid. Essentiële koerswijzigingen in het beleid, nieuwe inzichten door specifieke ontwerpen en een bredere scope door implementatie van EU-wetgeving zijn aanleiding om die business case te herijken. Alle drie de aspecten worden in deze business case meegenomen. Tevens moet deze business case illustratief in beeld brengen wat de gevolgen van het eID-programma zijn bij dienstaanbieders in de zorg en bij gemeenten.

Samenvattend leidt de herijking tot het volgende totaalbeeld van de kosten van €995 miljoen (zie tabel 3.1). Een aantal kostenposten is nu nog niet in beeld te brengen (PM).

Tabel 3.1 Verschillenoverzicht kosten business case 2016 en huidige business case
(bedragen in € mln.)

Kosten	Business Case november 2016	Business Case 2018
<i>Kosten die samenhangen met de beleidswijziging</i>		
Aansluitkosten dienstaanbieders (oplossing: routeringsdienst) ^{a)}	PM (schatting nu: 35 - 58 mln.)	0
Beheer eID-stelsel & routeringsdienst	158	143
Private middelen	PM	PM
<i>Herijkte kosten die ook in de vorige businesscase waren opgenomen</i>		
Authenticatiedienst DigiD	286	438
Investeringskosten eID-programma	52	69
Kosten DigiD Hoog middelen (productie en uitgifte)	106	120
Kaartlezer	43	145
Doorontwikkeling beleid	14	14
<i>Onderwerpen buiten scope in de vorige businesscase</i>		
Aansluitkosten dienstaanbieders door eIDAS	n.v.t.	13
Investeringskosten eIDAS-voorzieningen	n.v.t.	12
Beheerkosten eIDAS	n.v.t.	42
Totaal	659 + PM	995 + PM

a) Aangezien deze kostenpost in de vorige business case niet inzichtelijk was gemaakt (PM-post), nemen we deze post nu separaat als kostenbesparing op door de kosten in de huidige business case op 0 te zetten.

Hieronder gaan we successievelijk in op al deze aspecten, beginnend bij de koerswijziging van juni 2017.

Koerswijziging programma eID leidt tot minder uitgaven bij dienstaanbieders

Naar aanleiding van de Kamerbrief van 23 juni 2017 en het Algemeen Overleg Impuls eID d.d. 5 juli 2017, heeft de Kamer verzocht de bestaande business case uit 2016 te actualiseren op basis van de herziene koers van het programma eID. De herziene koers is om 'bij de verdere uitwerking het stelsel op enkele onderdelen te vereenvoudigen om de uitvoerbaarheid te waarborgen'. Concreet gaat het om:

1. Vereenvoudiging van de set van eisen, omwille van uitvoerbaarheid en verlaging van de kosten;
2. Ontzorgen van dienstaanbieders door middel van een routeringsdienst, omwille van de uitvoerbaarheid en lagere kosten van het beheer van het eID-stelsel.
3. Het aanwijzen van een of meer eID-middelen geleverd door private partijen, in plaats van het toelaten van alle middelen die aan de eisen voldoen, omwille van vereenvoudiging van het stelsel en lagere kosten.

De **ontzorging van de dienstaanbieders** leidt tot een vermindering van de beoogde uitgaven. Over de gehele looptijd van 10 jaar, betekent dit een verlaging van de kosten van circa € 35 tot € 58 miljoen. Aangezien deze kostenpost in de vorige business case niet inzichtelijk was gemaakt (PM-post), nemen we deze post nu separaat als kostenbesparing op door de kosten in de huidige business case op 0 te zetten (zie tabel 3.1).

De kosten voor het **beheer van het eID-stelsel** (incl. kosten routeringsdienst) bedragen in totaal € 143 miljoen, waar deze in 2016 nog op € 158 miljoen waren geraamd. Per saldo is hier een besparing van € 15 miljoen ten opzichte van de vorige business case. De specifieke besparing van de **vereenvoudiging van de set van eisen** binnen deze kostenpost bedraagt € 42 miljoen (jaarlijks € 4,2 miljoen). Hier staan echter kosten voor de routeringsdienst (zowel investering als beheer) tegenover, vandaar het lagere saldo.

De **kosten van private middelen** zijn thans (eind februari 2018) nog niet in beeld te brengen. De marktconsultatie geeft wel aan dat er voldoende animo vanuit de markt is om middelen met een hoger betrouwbaarheidsniveau te gaan ontwikkelen. De kosten hiervan komen pas in beeld na de aanbesteding, welke later in 2018 wordt uitgevoerd.

Nieuwe inzichten leiden tot hogere kostenraming

Tegelijkertijd heeft in deze nieuwe business case een herijking plaatsgevonden van de oude cijfers van de business case uit 2016. Hierbij gaat het om het actualiseren van de cijfers o.b.v. hardere uitgangspunten, concretere ontwerpen en betere inzichten in een aantal kostenposten. In 2016 was de raming dat de totale kosten over de gehele periode uitkwamen op circa € 659 miljoen, exclusief een aantal kostenposten die nog niet inzichtelijk waren te maken (PM). De verbeterde kostenraming leidt ertoe dat de kosten na herijking stijgen.

Op basis van de recente bestedingsplannen, is € 438 miljoen benodigd voor de **authenticatiedienst substantieel en hoog**, een stijging van ruim € 150 miljoen. Overigens zijn dit maar voor een deel additionele kosten, omdat een deel van deze kosten ook hadden moeten worden gemaakt als er niet in het eID-programma was geïnvesteerd (zie hiervoor de baten in de vorm van 'vermeden kosten' in tabel 3.3). De **investeringskosten van het eID-programma** bedragen nu € 69 miljoen, waar dit in de vorige business case nog op € 52 miljoen was geraamd. Nieuw inzichten (duurdere chip op de NIK en rijbewijs), leiden tot een stijging van de raming van de **kosten voor DigiD hoog** (reguliere productie en uitgifte middelen) met € 9 tot € 14 miljoen, zodat deze in totaal uitkomen op € 115 tot € 120 miljoen. Indien voor het gebruik van middelen met betrouwbaarheidsniveau hoog **een kaartlezer** moet worden gebruikt, zal dit voor een deel van de burgers leiden tot uitgaven van € 145 miljoen. Omdat de kosten van een kaartlezer nu hoger wordt geschat (€ 30 i.p.v. € 10), nemen de kosten voor de burger toe met € 102 miljoen.

Bredere scope geeft inzicht in de totale kosten

Aanvullend is in deze business case een aantal beleidszaken, die in de business case van 2016, nog buiten scope waren geplaatst, inzichtelijk gemaakt. Hierbij gaat het om de gevolgen van de bekrachtiging van de eIDAS verordening per 29 september 2018. Het plaatsen van eIDAS binnen de scope leidt tot extra kosten van € 66 miljoen. Hierbij gaat het om € 42 miljoen aan beheerkosten

en € 12 miljoen aan investeringskosten. Aanvullend moeten dienstverleners gezamenlijk bijna € 4 tot € 13 miljoen uitgeven voor het aansluiten op een eTD-makelaar om te kunnen voldoen aan de eIDAS-verordening.

Investeringskosten en beheerkosten per jaar

Een uitsplitsing van de kosten laat zien dat het merendeel van de kosten moet worden gemaakt in de beheerfase vanaf 2018. De totale investeringskosten bedragen €94 miljoen voor de periode 2015 tot en met 2020. Vanaf 2018 worden er kosten gemaakt voor het beheer van het eID-stelsel en de publieke authenticatiedienst en worden er kosten gemaakt voor de publieke middelen (DigiD Hoog), de aanschaf van kaartlezers en het beheer van eIDAS. Jaarlijks gaat het om een bedrag van € 89 miljoen (zie tabel 3.2)

Tabel 3.2 Investeringskosten versus beheerkosten (bedragen in € mln.)

Kostenpost	Investeringskosten (2015-2020)	Gemiddelde kosten per jaar beheerfase (2018-2027)	Kosten totaal
Ontwikkelkosten eID	69		69
Ontwikkelkosten eIDAS	12		12
Aansluitkosten dienstverleners eIDAS	13		13
Kosten DigiD Hoog middelen		12	120
Kosten kaartlezers		15	145
Kosten private middelen		PM	PM
Beheer eID-stelsel		14	143
Authenticatiedienst DigiD - vaste kosten		28	282
Authenticatiedienst DigiD - variabele kosten		16	156
Authenticatiedienst (privaat)		PM	PM
Beheer eIDAS		4	42
Doorontwikkeling beleid		1	14
Totaal ^{a)}	94	89 + PM	995 + PM

a) Door afrondingsverschillen lijken bedragen niet altijd bij elkaar op te tellen.

Het eID-programma bespaart ook aanzienlijke kosten

In de volgende tabel is het totaaloverzicht opgenomen van de baten, voor zover het mogelijk was om deze te kwantificeren. Het gaat om vermeden kosten van in totaal € 275 miljoen. Een belangrijke post is de authenticatiedienst van het huidige DigiD. Deze kosten van in totaal € 240 miljoen over 10 jaar, moeten ook worden gemaakt als er niet in het eID-stelsel wordt geïnvesteerd. Tevens kunnen allerlei bestaande authenticatiepassen worden uitgefaseerd en vervangen door eID-middelen. Dit levert een indicatieve besparing op van circa € 35 miljoen.

Tabel 3.3 Te kwantificeren baten (bedragen in € mln.)

Kosten	Businesscase november 2016	Onderhavige businesscase
Vermeden kosten authenticatiedienst DigiD	240	240
Vermeden kosten alternatieve authenticatiesystemen	48	35
Totaal	288 + PM	275 + PM

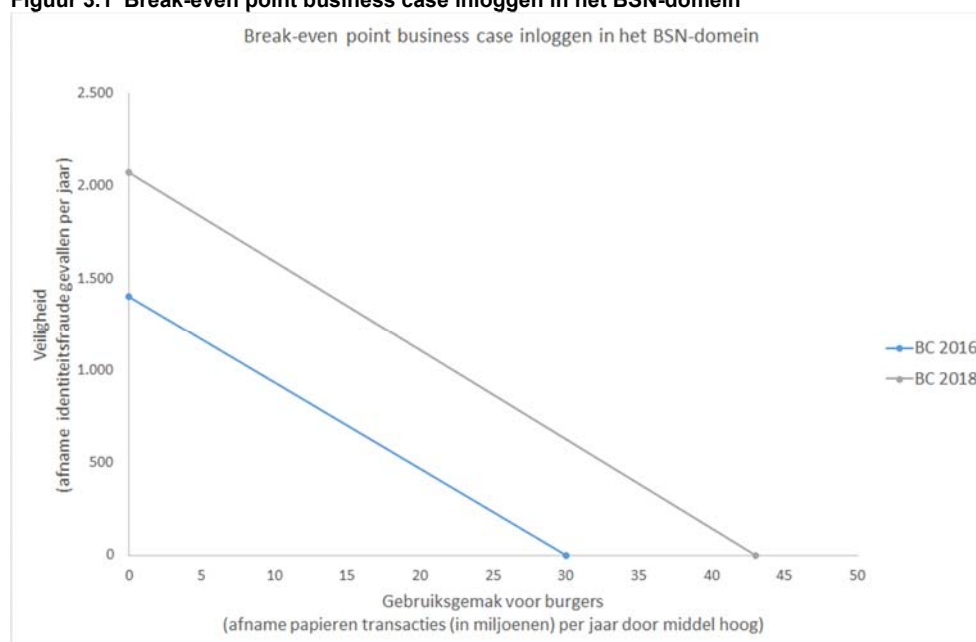
In de vorige business case was de waarde van de baten gelijk aan € 288 miljoen. Deze daling wordt veroorzaakt doordat het aantal alternatieve authenticatiepassen in omloop iets lager blijkt te zijn en doordat de vervanging later mogelijk wordt (in 2022 in plaats van in 2021).

3.2 Overzicht kosten en baten: break even point

De belangrijkste baten van het nieuwe eID-stelsel zijn een betere betrouwbaarheid en veiligheid, het beter voldoen aan Europese en nationale regelgeving op het gebied van privacy en veiligheid en betere dienstverlening aan burgers. Zoals ook opgemerkt in de vorige business case zijn dit type baten lastig te becijferen. Net als in de vorige business case is er daarom gekeken hoeveel minder fraude er moeten zijn en hoeveel transacties er op betrouwbaarheidsniveau hoog bij moeten komen (in het zorgdomein of het sociale domein), waarbij de maatschappelijke business case precies in evenwicht is.

In de volgende figuur is het break-even point te zien voor zowel deze business case (de oranje lijn) en de vorige business case (de blauwe lijn). De business case is positief boven de lijnen en negatief onder de lijnen. Te zien is dat het break-even point na de herijking minder snel bereikt wordt, hetgeen in het bijzonder te maken heeft met de toename van de kosten in de business case. Als het aantal gevallen van identiteitsfraude afneemt met 2.070 per jaar, dan is de business case in evenwicht.⁴⁹ Wanneer er op termijn op jaarbasis 43 miljoen transacties⁵⁰ op betrouwbaarheidsniveau hoog kunnen worden afgehandeld, dan is de business case ook in evenwicht. De business case is eveneens in evenwicht bij alle andere combinaties op de grijze lijn.

Figuur 3.1 Break-even point business case inloggen in het BSN-domein



Gelet op het feit dat er de laatste jaren circa 9.000 tot 15.000 maal per jaar een DigiD account is ingetrokken vanwege mogelijke fraude, lijkt het aantal van 2.070 vermeden fraudegevallen bereikbaar. Binnen de zorg werd er in 2017 al circa 49 miljoen maal met DigiD ingelogd, terwijl een groot deel van de zorgaanbieders nog niet is aangesloten op DigiD en dat straks wel moeten gaan doen. Door meer processen te digitaliseren en meer partijen (in de zorgsector) aan te sluiten, lijkt ook het aantal van 43 miljoen authenticaties per jaar in de toekomst haalbaar.

⁴⁹ Dit is ervan uitgaande dat de maatschappelijke schade van een fraudegeval gelijk is aan €40.000 per fraudegeval. Deze uitgangspunten zijn ook gebruikt in de vorige business case.

⁵⁰ Dit is ervan uitgaande dat de maatschappelijke baten van een digitale transactie in plaats van een papieren transactie gelijk is aan 15 minuten en equivalent aan een maatschappelijke waarde van €3,75. Deze uitgangspunten zijn ook gebruikt in de vorige business case. Het gaat hier overigens om 43 miljoen transacties in het eindbeeld. Hierbij is er ook rekening gehouden met het groeipad van middelen.

3.3 Impactanalyse bij gemeenten

Naast het opstellen van de businesscase is extra aandacht geweest voor de impact die de invoering van eID op de gemeenten zal hebben. Er is gedetailleerd onderzoek gedaan en ook in beeld gebracht wat de kosten voor gemeenten zijn van een aantal maatregelen zullen zijn waar nog niet definitief toe is besloten. Naast de kosten die uit het voorstel voortkomen is er ter illustratie ook gekeken naar de baten, gerealiseerd in de 'huizen' (zie uitleg in hoofdstuk 1). Deze paragraaf vat de belangrijkste resultaten kort samen. In bijlage 1 is de impactanalyse nader uitgewerkt.

In overleg met VNG, NVVB en VDP, is een vijftal gemeenten uit het Kennisnetwerk eID van de VNG geselecteerd, waarmee gesproken is over twee onderwerpen:

- De impact op de afdelingen Burgerzaken doordat gemeenten de publieke middelen op niveau DigiD Hoog uitgeven. Het betreft de Nederlandse Identiteitskaart (NIK) en het rijbewijs. De verwachte consequenties van aanvraag, uitgifte en gebruik zijn in beeld gebracht. Hier is de gemeente in de *rol van uitgever van publieke authenticatiemiddelen*.
- De impact die het aansluiten op eID op de gemeentelijke organisatie heeft. Hier betreft het de *rol als dienstaanbieder die op het eID-stelsel moet aansluiten*. Als uitgangspunt is aangenomen dat er een routeringsvoorziening zal komen die de gemeenten ontzorgt. Voor dit onderdeel zijn ook gesprekken gevoerd met ICT-leveranciers in de sector gemeenten.

Aansluiting bij het VNG Realisatie framework

Bij het bepalen van de impact, sluiten we aan bij de methodiek voor het maken van impact analyses van VNG Realisatie (voormalig KING). We benadrukken dat deze impactanalyse specifiek is opgesteld voor onderhavige business case, en niet voldoet aan de eisen van een impactanalyse van VNG Realisatie, welke meer gericht is op de uitvoeringsmogelijkheden. Dit houdt in dat we de impact voor gemeenten in beeld hebben gebracht met behulp van de SCOPAFIJTH-elementen (security, communicatie, organisatie, personeel, administratieve organisatie, financiën, informatie, juridisch, technologie, huisvesting). Deze elementen geven weer waar de (maatschappelijke) kosten en baten binnen de organisatie naar verwachting gaan vallen.

Betrouwbare middelen maken bij gemeenten een geleidelijk proces van digitalisering mogelijk

Door de routeringsvoorziening zullen de processen bij de gemeenten nauwelijks veranderen. Kwalitatief is de routeringsvoorziening wel degelijk van belang: die heeft de potentie om duidelijkheid, voorspelbaarheid, eenvoud en zekerheid te bieden. Initiële aansluiting is een technisch eenvoudige operatie waarvan de kosten verwaarloosbaar zijn. Het is zeker dat het koppelvlak met de routeringsdienst gemoderniseerd zal worden, maar over de kosten daarvan kunnen pas uitspraken gedaan worden wanneer er meer bekend is over de specificaties.

Authenticatiemiddelen op substantieel en hoog niveau bieden gemeenten nieuwe mogelijkheden om processen die hogere betrouwbaarheidsniveaus nodig hebben te digitaliseren. Dat zal een geleidelijk proces zijn waarbij gemeenten per geval een kosten – baten afweging zullen maken. De kosten van een aansluiting op eID zijn in dat geheel een relatief kleine factor, waarbij de kosten van de auditvoorschriften worden ervaren als (soms nodeloos) hoog.

3.4 Resultaten van de use cases in de zorg en bij gemeenten

Potentie digitalisatie van dienstverlening hoger betrouwbaarheidsniveau bij zorg en gemeenten

Het eID-stelsel kan gezien worden als 'het fundament'; een stuk infrastructuur nodig voor het realiseren van digitale dienstverlening (zie uitleg in hoofdstuk 1). De baten van de te realiseren

digitale dienstverlening maken bewust géén onderdeel uit van de businesscase. Immers, om deze baten te realiseren zullen partijen zelf moeten investeren in het digitaliseren van processen aangesloten op het eID-stelsel. Het eID-stelsel is een randvoorwaarde om diensten met een hoger betrouwbaarheidsniveau digitaal aan te kunnen gaan bieden.

Er is echter wel behoefte aan meer duidelijkheid rond de (maatschappelijke-) baten die kunnen worden gerealiseerd door digitale dienstverlening. Om hieraan tegemoet te komen is er gekozen om de baten te illustreren aan de hand van 'use cases'. De 'use cases' zijn de 'huizen' die gebouwd kunnen worden op het 'fundament'.

In bijlage 2 wordt een aantal 'use cases' beschreven in de grote (semi)publieke sectoren binnen het BSN-domein met significante potentie voor verdere digitalisatie van dienstverlening op hoger betrouwbaarheidsniveau; zorg en gemeenten. Deze paragraaf schetst de belangrijkste resultaten.

In de use cases kijken we naar (individuele) 'huizen' op het 'fundament'. Hierbij moet worden opgemerkt dat (i) dit geen totaalbeeld geeft van de maatschappelijke baten van het eID-stelsel (we kijken naar een paar huizen) én (ii) dat de baten niet direct kunnen worden toegeschreven aan het eID-stelsel. Dienstaanbieders of derden investeren om de huizen te bouwen en zonder eID-stelsel zouden de huizen wellicht ook (deels) met een alternatieve infrastructuur gerealiseerd kunnen worden.

Zowel kosten als baten voor dienstaanbieders en burger in beeld

Wat de use cases wél illustreren is het belang van het faciliteren van digitale dienstverlening en de brede scope aan toepassingen (huizen) die in de toekomst op het fundament kunnen worden gebouwd. Bij de use cases is gekeken naar:

- De kosten voor het digitaliseren van de betreffende processen voor de dienstaanbieder
- De baten voor de dienstaanbieder
- De maatschappelijke baten voor de burger

Om een selectie te maken van de use cases is geïnformeerd bij verschillende partijen (VNG, VNG Realisatie, NVVB, VDB en VWS) naar aansprekende voorbeelden van toepassingen:

- Waar draagvlak in het veld voor bestaat
- Die actueel en concreet zijn
- Die bij voorkeur zonder aanpassingen van de wet mogelijk zijn
- Die mogelijk worden gemaakt door eID op minimaal substantieel niveau

Het zorgdomein heeft baat bij hoge betrouwbaarheid van middelen

Door het beschikbaar komen eID middelen op substantieel en hoog betrouwbaarheidsniveau neemt het palet aan diensten die in de zorg en het gemeente domein gedigitaliseerd kunnen worden toe. Met name in de zorg is de meerwaarde van een middel met betrouwbaarheidsniveau hoog significant en noodzakelijk gezien het type gegevens. Gemeenten noemen vooral veel potentiële use cases die ook met een middel met betrouwbaarheidsniveau substantieel kunnen worden gerealiseerd.

Het zorg domein is al geruime tijd proactief bezig met het digitaliseren van diensten en gebruikt hiervoor ook private middelen. Generaliserend kan opgemerkt worden dat gemeenten meer reactief wachten op brede beschikbaarheid van een publiek middel op substantieel en hoog betrouwbaarheidsniveau alvorens over te gaan tot digitaliseren van diensten. Dit verschil kan deels verklaard worden door de 'hoge waarde achter het slot' voor een aantal doelgroepen in het zorgdomein.

Zorgpartijen hechten dan ook grote waarde aan een middel op niveau hoog met een zo groot mogelijk gebruiksgemak. Dienstverleners zien baten voor zichzelf en voor hun patiënten. Zo zou het digitaliseren van logistieke processen in bijvoorbeeld een ziekenhuis kunnen zorgen voor een snellere doorlooptijd per ziekenhuisbezoek en minder 'wacht' momenten. Naast het versimpelen wordt, wanneer men zeker weet met wie je te maken hebt, de kans op fouten kleiner en kunnen de administratieve handelingen (leesuren) omlaag. De patiënt is ook gebaat met een sneller, makkelijker proces en minder fouten. Mensen die regelmatig zorg nodig hebben (chronisch zieken) of zorg voor een ander ondersteunen (ouders en/of (mantel)zorgers) zullen naar verwachting het eerste gebruik gaan maken van digitale dienstverlening. Vooral als een digitaal proces een terugkerend fysiek bezoek aan de arts of instelling vervangt. Denk hierbij bijvoorbeeld aan het digitaal doorgeven van meetgegevens.

Ook het identificeren van de zorgprofessional zelf binnen het eigen systeem en tussen organisaties zou baat kunnen hebben bij een middel op niveau hoog. Naast het gebruik van portalen om informatie op te halen en uit te wisselen is het gebruik van applicaties in de zorg sterk in opkomst.

Gemeenten zien ook baten, maar zijn nog afwachtend

Bij gemeenten is er een breed gedragen wens is om de digitale dienstverlening voor de burger verder uit te breiden. Ideeën over de nieuwe diensten op basis van eID middelen op substantieel en hoog betrouwbaarheidsniveau bevinden zich echter nog in een erg vroeg stadium. De baten concentreren zich op verminderd baliebezoek, tijdswinst en gebruikersgemak voor de burger, zoals blijkt uit een aantal recente pilots (aanvragen rijbewijs, doen van geboorteaangifte). Wel moet in ogenschouw worden genomen dat het in sommige gevallen wenselijk is om het persoonlijk contact met de gemeente in stand te houden. De gemeenten geven daarnaast aan dat potentiële baten alleen gerealiseerd kunnen worden bij voldoende opname van het nieuwe middel onder de bevolking. Op dit moment bestaat hier nog onzekerheid over bij de gemeenten, wat vaak leidt tot een afwachtende houding.

De kosten en baten voor de burger die het gevolg zijn van digitalisering van diensten - mogelijk gemaakt door een eID-middel op betrouwbaarheidsniveau hoog - alsmede de kosten en baten van de 'huizen op het fundament' zijn nog niet met voldoende zekerheid te kwantificeren. Gemeenten noemen verschillende mogelijk toepassingen en in het zorgdomein zijn pilots en businesscases gemotiveerd die de waarde van de huizen onderstrepen. Baten voor burgers manifesteren zich met name in de vorm van tijdswinst door de afname van papieren processen en baliebezoeken en verlaging van reistijd en reiskosten. Hoe groot deze baten zijn zal in sterke mate afhangen van het aantal burgers dat gebruik gaat maken van de eID middelen en het gebruiksgemak van diensten die beschikbaar komen.

4 Kosten en baten nader uitgewerkt

In dit hoofdstuk is een nadere uitwerking gemaakt van de kosten en baten van inloggen in het BSN-domein. In de eerste paragraaf zijn de kosten uitgewerkt en in de tweede paragraaf de baten.

4.1 Kosten

In deze paragraaf zijn de kosten van het projectalternatief verder uitgewerkt. De kostenramingen zijn gebaseerd op informatie vanuit het ministerie van Binnenlandse Zaken en Koninkrijksrelaties, Logius, RDW, RvIG en RVO. Voor zover mogelijk is aangesloten bij openbare bronnen (realisatiecijfers, bestedingsplannen). Er is binnen deze opdracht geen check uitgevoerd door Ecorys op de plausibiliteit van de gepresenteerde cijfers.

De cijfers zijn gepresenteerd op hoofdlijnen en voor een nadere onderbouwing en toelichting op de bedragen wordt verwezen naar de achterliggende documentatie en bronnen. Wanneer bedragen zijn gewijzigd ten opzichte van de vorige business case is – voor zover bekend – een toelichting gegeven op de redenen waarom bedragen zijn gewijzigd.

In deze business case is alleen gekeken naar welke kosten er gemaakt moeten worden en wie deze kosten maakt. Wie de kosten betaalt of financiert, ligt buiten de scope van deze business case en daarvoor worden in deze business case geen voorstellen of suggesties gedaan.

4.1.1 Kostenramingen

In deze business case is een onderscheid gemaakt naar de volgende kostensoorten:

- Ontwikkelkosten;
- Aansluitkosten dienstverleners;
- Kosten DigiD Hoog middelen;
- Beheer- en onderhoudskosten;
- Vaste kosten doorontwikkeling en beleidsvorming middelen.

Ontwikkelkosten

In de volgende tabel zijn de ontwikkelkosten opgenomen. Het betreft hier de kosten in de periode van 2015 tot en met 2020. In totaal zijn deze ontwikkelkosten gelijk aan €80,8 miljoen over de periode van 2015 tot en met 2020.

Tabel 4.1 Ontwikkelkosten (bedragen in € mln.)

Kosten	2015 ^{a)}	2016 ^{b)}	2017 ^{c)}	2018 ^{d)}	2019	2020	Totaal
Ontwikkelkosten eID-stelsel	9,3	5,1	10,2	8,4	2,0	-	35,0
Ontwikkelkosten publieke authenticatiedienst en publiek middel	4,3	5,4	14,2	10,2	0	-	34,0
Ontwikkelkosten eIDAS-voorzieningen ^{e)}	0	0,9	5,4	4,0	1,2	0,4	11,8
Totaal ^{f)}	13,6	11,3	29,8	22,5	3,2	0,4	80,8

- a) De cijfers over 2015 zijn niet gewijzigd ten opzichte van de vorige business case.
- b) De cijfers over 2016 zijn wel iets gewijzigd ten opzichte van de vorige business case, omdat in deze business case is uitgegaan van realisatiecijfers met betrekking tot de uitgaven en niet van budgetten. In de vorige business case stond voor 2016 een totaalbedrag van €9,8 mln. opgenomen voor de ontwikkelkosten eID-stelsel en ontwikkelkosten publieke authenticatiedienst en publiek middel. Deze kosten met iets meer dan €0,5 mln. gestegen tot €10,4 mln. (€5,1 mln. + €5,4 mln. = €10,4 mln. (met afronding).
- c) De cijfers over 2017 zijn niet veranderd ten opzichte van de vorige business case, realisatiecijfers over 2017 waren op het moment van schrijven van de business case nog niet beschikbaar. Daarom is nog steeds uitgegaan van de cijfers uit het bestedingsplan van 2017.
- d) De cijfers over 2018 zijn eveneens veranderd, in de vorige business case was een totaalbedrag van €5,4 miljoen over 2018 opgenomen, in deze business case een totaalbedrag van €18,6 miljoen (excl. eIDAS). Dat heeft onder meer te maken met de doorontwikkelambities (extra investeringen van €7,7 mln. in 2018 en €2 mln. in 2019) met beoogde investeringen in ontzorging/routeringsvoorziening (nieuw beleid in vergelijking met de vorige business case), een inzagefunctie voor MijnOverheid, voorlichting en onderzoek Wet Digitale Overheid en activiteiten om de dekkingsgraad van DigiD te vergroten.
- e) In de vorige business case vielen de eIDAS voorzieningen buiten scope van de analyse, vandaar dat deze kosten niet in de vorige BC waren meegenomen.
- f) Door afrondingsverschillen lijken bedragen soms niet bij elkaar op te tellen.

Bronnen: BZK, *Rijks ICT Dashboard* (cijfers 2015), BZK, *Realisatiecijfers 2016* (cijfers 2016), De Digicommissaris, *Bestedingsplan 2017 e.v. 2.2 eID en publiek middel* (cijfers 2017), De Digicommissaris, *Doorontwikkelambities DigiD* (ontwikkelkosten AD en middel 2018), De Digicommissaris, *Bestedingsplan 2018 e.v. Naam voorziening 2.1 eID* (ontwikkelkosten eID-stelsel 2018 en verder), *informatie RvO* (cijfers eIDAS voorzieningen 2016 en 2017), De Digicommissaris, *Bestedingsplan 2018 e.v. Naam voorziening 2.3 eIDAS* (cijfers eIDAS voorzieningen 2018 en verder),

Aansluitkosten dienstverleners

In de bijlage impactanalyse voor gemeenten is een beeld geschetst van wat gemeenten moeten doen om aan te sluiten op het eID-stelsel en om te voldoen aan de eIDAS-verplichting vanaf 29 september 2018. In deze sectie is op basis van die informatie een schets gemaakt van de te verwachten kosten. Alle dienstverleners moeten voor 29 september 2018 aansluiten op een eTD-makelaar. In 2016 waren er 570 overheidsorganisaties aangesloten op DigiD met 771 webdiensten en in hetzelfde jaar waren 257 overheidsorganisaties aangesloten op eHerkenning (of eTD).⁵¹ Per saldo zijn er dus 570 -/ 257 of 313 overheidsorganisaties die voor 29 september 2018 nog een aansluiting moeten regelen met naar verwachting 423 webdiensten.

De éénmalige aansluitkosten die eTD-makelaars een gemeente in rekening brengen variëren tussen €500 en €5.000 (zie paragraaf 3.3). Daarnaast moeten gemeenten jaarlijkse kosten maken, die afhangen van het aantal transacties. Het is de verwachting dat het aantal transacties de eerste jaren zeer beperkt zal zijn.⁵² In dat geval bedragen de jaarlijkse kosten ongeveer €1.500 per jaar. Als we de hierboven genoemde kengetallen hanteren voor alle webdiensten dan leidt dit tot een extra rekening van de eTD-makelaars tussen de €0,8 en €2,8 miljoen.

Om aan te sluiten moet de dienstverlener een eigen koppelvlak inrichten en aanpassingen doen in haar eigen applicatielandschap, voor zover er digitale dienstverlening in het burgerdomein mee wordt verricht. Voor de analyse is ervan uitgegaan dat het tussen de €5.000 en €15.000 kost om

⁵¹ Ministerie van BZK (2017), *Monitor Generieke Digitale Infrastructuur*.

⁵² Uit de kwantitatieve analyse van PBLQ over de belasting van het eIDAS koppelvlak komt naar voren dat het de verwachting is dat er per jaar voor heel Nederland ongeveer 20.000 transacties zijn voor de ongeveer 500 overheidsorganisaties (niet zijnde de Belastingdienst, UWV, SVB, DUO, CJIB, zorg, Kadaster en RDW). Als we ervan uitgaan dat alle transacties evenredig zijn verdeeld over deze 500 overheidsorganisaties, dan komt dit neer op 40 transacties per jaar per overheidsorganisatie.

de aansluiting werkend te krijgen. Voor alle 423 webdiensten leidt dat tot een kostenpost van tussen de € 2,1 en € 6,4 miljoen.

De rekening van de softwareleveranciers voor de dienstaanbieders loopt daarmee op tot een bedrag tussen de € 2,9 en € 9,2 miljoen. In aanvulling daarop is het reëel om ook interne uren mee te nemen voor de medewerkers van de eigen organisatie. Dit zal leiden tot éénmalige additionele kosten tussen de € 0,8 en € 3,7 miljoen.⁵³ In de onderstaande tabel is het overzicht opgenomen van de kosten voor het aansluiten op een eTD-makelaar voor de overheidsdienstaanbieders die nog geen aansluiting hebben op een eTD-makelaar.

Tabel 4.2 Kosten aansluiten op eTD-makelaar t.b.v. eIDAS-verplichtingen (bedragen in € mln.)

Kosten	Minimum	Maximum
Aansluiting eTD-koppelvlak	0,8	2,8
Aanpassingen applicatielandschap	2,1	6,4
Interne uren gemeenten	0,8	3,7
Totaal	3,7	12,8

Per saldo komen de kosten voor de dienstaanbieders zonder aansluiting op een eTD-koppelvlak neer op een bedrag tussen de € 3,7 en € 12,8 miljoen. De kosten per organisatie (uitgaande van 570 -/ 257 = 313 organisaties) komen dan uit op een bedrag tussen de € 12.000 en € 41.000. Als we deze cijfers leggen naast het aantal te verwachten transacties per organisatie (40 transacties per jaar⁵⁴), dan komen de kosten per transactie uit op bedragen tussen de € 300 en € 1.000 per transactie voor dienstaanbieders die nog niet zijn aangesloten op het eTD-koppelvlak. Dergelijk hoge kosten per transactie zijn zakelijk moeilijk te rechtvaardigen. Zeker aangezien er begin 2019 een routeringsvoorziening beschikbaar komt, waarbij de kosten voor aansluiting redelijk beperkt kunnen blijven (omdat deze aansluit op het huidige DigiD koppelvlak). Wij raden het ministerie van Binnenlandse Zaken en Koninkrijksrelaties aan om de huidige inefficiënte oplossing te heroverwegen.

Overheidsorganisaties die reeds een aansluiting hebben op een eTD-koppelvlak moeten over van eTD-koppelvlak versie 1.9 naar versie 1.11 van eHerkenning of Idensys via een eHerkenning- of Idensys-makelaar. Aan de ene kant is uit diverse gesprekken naar voren gekomen, dat de impact van de migratie van versie 1.9 naar versie 1.11 voor overheidsorganisaties relatief beperkt zou zijn. Aan de andere kant is ook aangegeven dat deze dienstaanbieders vanaf 29 september 2018 een polymorph pseudoniem ontvangen (bij versie 1.11). eTD-makelaars hebben aangegeven dat het nog niet mogelijk is om hiervan de kosten te ramen, omdat de specificaties van het koppelvlak met polymorphe pseudoniemen nog niet bekend zijn. Voor nu zijn de kosten hiervoor op PM gezet.

Dienstaanbieders kunnen vanaf begin 2019 aansluiten op de routeringsvoorziening. De routeringsvoorziening is bedoeld om de dienstaanbieders te ontzorgen met één aanspreekpunt, één koppelvlak en één factuur in plaats van de situatie dat dienstaanbieders meerdere koppelvlakken moeten onderhouden (DigiD, eIDAS, private partijen) om aan te sluiten op het eID-stelsel. In de vorige business case zijn deze kosten als een PM-post opgenomen, daarom leidt dit niet direct tot besparing ten opzichte van de vorige business case. Ter illustratie hebben wij in de volgende tekstbox een indicatieve berekening opgenomen hoe hoog deze PM-post eruit had

⁵³ Hierbij is ervan uitgegaan dat een interne medewerker 1 tot 1,5 keer zoveel uren kwijt is aan de implementatie dan de softwareleverancier. Qua uurtarieven is uitgegaan van € 150 voor een softwareleverancier en € 41 voor een interne medewerker (schaal 8).

⁵⁴ Er worden maximaal 1,5 miljoen transacties per jaar verwacht (kwantitatieve analyse van PBLQ over de belasting van het eIDAS koppelvlak). Het overgrote merendeel van de transacties hangt samen met dienstverlening van de Belastingdienst, UWV, SVB, DUO, CJIB. Per saldo worden er ongeveer 20.000 transacties per jaar bij de 500 overige dienstverleners verwacht, ofwel $20.000/500 = 40$ transacties per overige dienstverlener.

kunnen zien als er op drie koppelvlakken aangesloten had moeten worden om toegang tot het eID-stelsel te kunnen realiseren.

Zonder een routeringsvoorziening moet iedere dienst aanbieder verschillende koppelvlakken onderhouden om burgers toegang te kunnen verlenen tot het eID-stelsel (DigiD, eIDAS en private middelen). Dankzij de routeringsvoorziening kan worden volstaan met één koppelvlak. De routeringsvoorziening leidt ertoe dat dienst aanbieder niet hoeven te investeren in een koppelvlak voor private middelen en dat er slechts eenmaal beheerkosten zijn in plaats van driemaal beheerkosten (DigiD, eIDAS en private middelen). Uitgaande van het huidige aantal van 771 webdiensten en een éénmalige investering van € 15.000 tot € 25.000 per koppelvlak kan dan een bedrag van € 12 tot € 19 miljoen bespaard worden aan investeringskosten in 2018. Daarnaast kunnen jaarlijks beheerkosten bespaard worden. Uitgaande van 771 webdiensten en 2 maal een besparing op de beheerkosten van 10 tot 15% van de eenmalige investeringskosten van € 15.000 tot € 25.000 leidt dat tot een mogelijke besparing van tussen de € 2 en € 4 miljoen per jaar. Per saldo leidt een routeringsvoorziening daarmee tot een besparing van tussen de € 35 en € 58 miljoen over de periode tot en met 2027.

De eerste versie van de routeringsvoorziening levert de dienst aanbieder een bericht met BSN. In een latere versie van de routeringsdienst zullen polymorphe pseudoniemen worden geleverd aan de dienst aanbieder. Deze dienst aanbieder moet het polymorphe pseudoniem zelf ontsleutelen en daarvoor moeten zij ook nog kosten maken. Er is op het moment van schrijven nog geen beeld van de hoogte van deze kosten (ook omdat de koppelvlakken nog niet zijn vastgesteld) en deze kosten zijn daarom op als PM-post meegenomen.

In de volgende tabel zijn de verschillende kosten voor dienst aanbieder om aan te sluiten naast elkaar gezet.

Tabel 4.3 Kosten aansluiten dienst aanbieder (bedragen in € mln.)

Kosten	Minimum	Maximum
Migratie eTD-koppelvlak 1.9 naar 1.11	PM	PM
Aansluiting eTD-koppelvlak 1.11	3,7	12,8
Aansluiting routeringsvoorziening	.	.
Migratie routeringsvoorziening (incl. PP) ^{a)}	PM	PM
Totaal	3,7 + PM	12,8 + PM

. Staat voor beperkte kosten

a) PP staat voor polymorphe pseudoniem.

Kosten eID-middelen

Naast investeringen in de stelselvoorzieningen moeten er ook eID-middelen komen op het betrouwbaarheidsniveau substantieel en hoog. De volgende eID-middelen zijn te onderscheiden: DigiD Substantieel, DigiD Hoog en private middelen op betrouwbaarheidsniveau substantieel.

DigiD Substantieel

Alle burgers kunnen zonder extra kosten beschikken over de DigiD app en 40% van de burgers kan deze DigiD app opwaarderen naar betrouwbaarheidsniveau substantieel. Daarvoor hoeft de burger geen extra kosten te maken.

DigiD Hoog

Burgers die willen beschikken over DigiD Hoog moeten kunnen beschikken over een eRijbewijs of een eNIK. Hiervoor wordt op ieder rijbewijs (vanaf mei 2018) en op iedere NIK (vanaf januari 2019) een chip met e-functionaliteit geplaatst. De extra kosten voor de eID-functionaliteit liggen tussen minimaal € 3,15 en maximaal € 3,50 voor het rijbewijs⁵⁵ en minimaal € 3,00 voor een NIK.⁵⁶ In de vorige business case was nog uitgegaan van een bedrag van € 2,04 voor het rijbewijs en een bedrag van € 2,82 voor een NIK. In een eerdere raming van de kosten van het eRijbewijs waren veel zaken nog niet duidelijk (er waren destijds bv. nog geen PSA's uitgewerkt) en bij de nieuwe raming zijn veel meer zaken wel uitgedacht. Zo blijkt bijvoorbeeld dat de productie van de chip op het rijbewijs langer duurt, zo is er in het uitgifteproces uitgegaan van een hogere beveiliging en is gebleken dat er verschillende systeemaanpassingen en procesaanpassingen nodig waren.

Naast de extra kosten voor de chip is er in de vorige business case ook vanuit gegaan dat een baliemedewerker bij de uitgifte van het eID-middel een korte toelichting geeft aan de burger dat het rijbewijs of de NIK een eID-functionaliteit heeft, waarom dit relevant is en hoe deze werkt (reader, eID-middel, installatiehandleiding en informatie over het gebruik van het eID-middel).⁵⁷ In de vorige business case is uitgegaan van een tijdsbesteding van 2 minuten en daarmee een extra kostenpost van € 2 per NIK of rijbewijs. Conclusie uit de impactanalyse (zie bijlage) was ook om deze tijdsbesteding te handhaven.

Per saldo betekent dit dat de extra kosten voor een eRijbewijs minimaal € 5,15 en maximaal € 5,50 bedragen en de extra kosten voor een eNIK € 5,00.⁵⁸ De kosten voor de gehele maatschappij zijn daarbij ook afhankelijk van het natuurlijke vervangingspatroon van NIK's en rijbewijzen. In de vorige business case werd uitgegaan van een start van de uitgifte per januari 2018, in deze business case is het uitgangspunt dat de eerste eRijbewijzen worden uitgegeven vanaf mei 2018 en de eerste eNIK's worden uitgegeven vanaf januari 2019. Daardoor vallen de kosten in 2018 iets lager uit. Er is niet echt een jaarlijks cijfer te presenteren voor de hoogte van de kosten (omdat het aantal te verstrekken WID-documenten per jaar verschilt (zie ook tabel 2.1). Ter illustratie zijn de cijfers voor enkele jaren opgenomen evenals het totaalbedrag over de periode van 2018 tot en met 2027.

Tabel 4.4 Investeringskosten eNIK en eRijbewijs (bedragen in € mln.)

Kosten	2018	2020	2022	2024	Totaal ^{a)}
Minimumvariant	6,2	12,1	7,7	11,8	115,1
Maximumvariant	6,6	12,7	8,1	12,2	120,0

a) Het gaat hier om de totale kosten te maken over een periode van 10 jaar (van 2018 tot en met 2027). Let op: deze kolom geeft niet de som weer van de cijfers uit de eerdere vier kolommen, daar zijn niet de kosten van alle jaren gepresenteerd.

⁵⁵ Informatie van de RDW. Deze kostenraming van de RDW is gebaseerd op de aannames dat de koppelvlakken worden bevroren en niet veranderen (koppelvlak tussen rijbewijskaart en authenticatiedienst), de afspraak dat Logius de helpdesk realiseert en er geen vragen bij RDW-helpdeks komen, er tijdig een pin-reset functie wordt gerealiseerd voor de heraanvraag van PUK-brieven, de uitgifte van de eRijbewijzen start per mei 2018 en er wordt uitgegaan van de financiële basis tariefstelling van 1 oktober 2018. Voor de business case is met een minimumbedrag van € 3,15 en een maximumbedrag van € 3,50 per rijbewijs gerekend.

⁵⁶ Informatie RvIG. Er zijn nog wel onzekerheden in de realisatie, onder meer vanwege de huidige versie van de beleidsregels, waardoor de kosten nog hoger uit kunnen vallen.

⁵⁷ Zo is het ook opgenomen in de PSA voor DigiD hoog (Architectuurgroep Publiek Middel hoog (2017), *Projectstartarchitectuur DigiD hoog. Identificeren en authenticeren met je identiteitskaart of rijbewijs*).

⁵⁸ Merk op: Of dat ook tot een stijging van de leges met deze bedragen voor een NIK of rijbewijs leidt is afhankelijk van het resultaat van de financieringsdiscussie (wie deze kosten gaat betalen).

Te zien is dat de kosten over de gehele periode (van 2018 tot en met 2027) optellen tot een bedrag van tussen de € 115,1 en € 120,0 miljoen. Ter vergelijking: in de vorige business case werden deze kosten geraamd op een bedrag van € 105,7 miljoen. Enerzijds leidt de duurdere e-functionaliteit tot hogere kosten, anderzijds vallen de kosten lager uit omdat de eerste eID-middelen pas op een later tijdstip worden uitgereikt.

Kaartlezers

Ongeveer 40% van de burgers heeft een bruikbare NFC functionaliteit op zijn smartphone om daarmee de chip op de eNIK of het eRijbewijs uit te lezen.⁵⁹ Burgers die niet in het bezit zijn van een smartphone met bruikbare NFC functionaliteit (de andere 60%) zullen een kaartlezer aan moeten schaffen om DigiD Hoog te kunnen gebruiken. Er is in deze business case (net als in de vorige business case) vanuit gegaan dat een kaartlezer door gemiddeld 1,5 personen wordt gebruikt. Uit een nadere analyse⁶⁰ van de functionaliteiten en kosten van de kaartlezers is naar voren gekomen dat een kaartlezer met de gewenste functionaliteiten gemiddeld ongeveer € 30 per kaartlezer zal kosten. In de vorige business case was er nog vanuit gegaan dat de meest eenvoudige kaartlezer van € 10 ook geschikt zou zijn om de chip uit de eNIK of het eRijbewijs uit te lezen.

In dat geval variëren de kosten voor kaartlezers tussen de € 10,5 en € 21,1 miljoen per jaar afhankelijk van het aantal uitgegeven NIK's en rijbewijzen met een gemiddelde van € 14,5 miljoen per jaar. In de vorige business case kwam het gemiddelde uit op een bedrag van € 4,3 miljoen per jaar.

De aanschaf van de kaartlezers is een zeer substantiële kostenpost op het totaal. Het is daarom aan te raden om nader te onderzoeken wat de mogelijkheden zijn voor goedkopere alternatieven om zo de kosten te kunnen beperken.

Private middelen

Zoals eerder aangegeven zijn de kosten en baten van de mogelijk toe te laten private middelen als PM-post opgenomen in de business case.

Beheer- en onderhoudskosten

In de onderstaande tabel zijn de jaarlijkse beheer- en onderhoudskosten opgenomen. De beheerkosten zijn voor enkele zichtjaren (2018, 2020 en 2022) getoond, vanzelfsprekend moeten er in de tussenliggende jaren en de jaren 2023 tot en met 2027 ook beheerkosten worden gemaakt.⁶¹

⁵⁹ In de vorige business case was het uitgangspunt dat 50% van de gebruikers een kaartlezer nodig zal hebben en dat 50% gebruik zal maken van een NFC-oplossing.

⁶⁰ Onderzoek van PBLQ (2016), *Kaartlezers voor DigiD hoog*. PowerPoint presentatie d.d. 30 november 2016.

⁶¹ Voor de kosten voor beheer en onderhoud tot en met 2022 is aangesloten bij de bestedingsplannen. De beheerkosten na 2022 zijn (rekening houdend met incidentele kosten voor groot onderhoud in de jaren 2021, 2022 en 2023) gelijk verondersteld aan de kosten in 2022 na consultatie van het ministerie van BZK en Logius. In de vorige business case is ook uitgegaan van constante beheerkosten. Tegelijk is het ook reëel om van een beperkte jaarlijkse kostenstijging uit te gaan, omdat de praktijk leert dat de kosten voor ICT jaarlijks stijgen. Als wordt gerekend met een kostenstijging van 2,5% per jaar vanaf 2023, leidt dat tot een stijging van de totale kosten met € 24 miljoen over de gehele periode tot en met 2027.

Tabel 4.5 Kosten beheer en onderhoud (bedragen in € mln.) ^{a)}

	2018	2020	2022
eID-stelsel			
BSNk en inzage ^{b)}	10,5	10,5	10,5
Set van eisen & toezicht en beheer ^{c)}	1,3	1,3	1,3
Routeringsdienst ^{d)}	2,0	2,0	2,0
Subtotaal eID-stelsel	11,3	13,8	13,8
Authenticatiedienst DigiD Sub. + Hoog'			
Vaste kosten beheer & onderhoud ^{e)}	23,3	27,0	32,0
Variabele kosten beheer & onderhoud ^{f)}	10,7	16,5	16,3
Subtotaal authenticatiedienst DigiD	34,0	43,5	48,3
eIDAS-voorzieningen ^{e)}			
Beheer en exploitatie	1,3	4,5	4,5
Subtotaal eIDAS-voorzieningen	1,3	4,5	4,5
Totaal	46,6	61,8	66,6

- a) In de vorige business case zijn de vaste kosten en de variabele kosten voor beheer en onderhoud in aparte tabellen gepresenteerd. Er is nu voor gekozen om de kosten voor beheer en onderhoud integraal te presenteren, ook om een betere aansluiting van de cijfers te krijgen met de bestaande bestedingsplannen.
- b) De kosten voor BSNk en inzage zijn vanaf 2019 niet gewijzigd ten opzichte van de vorige business case (in beide gevallen een bedrag van € 10,5 mln. per jaar). Er zijn ook al kosten voor het beheer van het BSNk en inzage te zijn gemaakt in 2016 (€ 3,5 mln.) en in 2017 (€ 3,8 mln.).
- c) In de gebruikte bestedingsplannen staat voor de set van eisen & toezicht en beheer een bedrag van € 5,5 mln. per jaar opgenomen. Door de beleidswijzigingen (van USvE naar set van eisen én van multi-middelenstrategie naar één of enkele toegelaten middel) zullen deze kosten echter lager uit gaan vallen. Uit de opdrachtovereenkomst 2018 voor het programma eID komt naar voren dat Logius de activiteiten voor de set van eisen & toezicht en beheer in 2018 voor een bedrag van € 1,3 mln. uit gaat voeren. In de Programboard d.d. 22 februari 2018 is gesproken over de te maken kosten voor uitvoering van de activiteiten die samenhangen met de set van eisen & toezicht en beheer voor de jaren na 2018. Daaruit is naar voren gekomen, dat het bedrag van € 1,3 mln. per jaar adequaat is voor de set van eisen & toezicht en beheer. Logius (als beoogd uitvoerder van deze werkzaamheden) is ook deelnemer van deze program board en heeft daar ook mee ingestemd. Daarom is in deze business case het bedrag van € 1,3 miljoen per jaar ook gebruikt in de kostenramingen na 2018.
- d) De kosten voor de routeringsvoorziening zijn het resultaat van nieuw beleid en waren daarom in de vorige business case nog niet meegenomen. De hier gepresenteerde bedragen komen uit de bestedingsplannen, Logius heeft met betrekking tot deze kostenpost aangegeven dat deze raming niet (meer) accuraat is, op het moment van schrijven is er nog geen nieuwe en betere raming voorhanden. Mogelijk wijzigen deze bedragen dus nog.
- e) In de vorige business case was voor de vaste kosten een vast bedrag opgenomen van € 20 mln. per jaar. In de huidige business case lopen deze kosten op van € 23,3 mln. in 2018 naar € 28,0 mln. in 2022 en de jaren daarna (exclusief groot onderhoud). Er is ook groot onderhoud voorzien in 2021 (€ 2,0 mln.), 2022 (€ 4,0 mln.) en 2023 (€ 4,0 mln.), die overigens voor hetzelfde bedrag ook was opgenomen in de vorige business case. De vaste beheerkosten stijgen aanzienlijk ten opzichte van de vorige business case.
- f) De volgende kostenposten zijn als variabele kosten voor beheer & onderhoud aangemerkt: gebruik gerelateerde kosten DigiD Substantieel en DigiD Hoog, helpdeskkosten, sms-kosten, brieven (normale porto + beveiligde bezorging) en BRP-bevragingen. Ook voor de variabele kosten zijn er relatief grote verschillen ten opzichte van de vorige business case. In de vorige business case waren de variabele kosten in de eerste jaren geraamd op ongeveer € 10 mln. per jaar en zouden deze kosten dalen tot ongeveer € 6 mln. per jaar vanaf 2021. In de huidige business case stijgen deze kosten van € 10,7 mln. per jaar tot € 16,3 mln. in 2022 en ook de jaren daarna blijven deze kosten doorgaan. De kostenposten gebruik gerelateerde kosten DigiD Substantieel en DigiD Hoog waren in de vorige business case niet apart gespecificeerd. Daarbij moet wel rekening worden gehouden dat er in de huidige kostenraming van Logius van is uitgegaan dat alle burgers met DigiD Substantieel en DigiD Hoog gaan werken. Een groter marktaandeel van private middelen kan mogelijk wel leiden tot een daling van de kosten. Ook moet opgemerkt worden dat in de huidige raming van de kosten is uitgegaan van een start vanaf 2018 en niet van een start in 2019. In totaal bedroegen de kosten voor de authenticatiedienst in de vorige business case gemiddeld € 27,6 mln. per jaar. In de huidige business case is te zien dat de kosten voor de authenticatiedienst gemiddeld € 43,8 mln. per jaar bedragen. Dat is een aanzienlijke stijging ten opzichte van de vorige business case. De overige kosten zijn als vaste kosten voor beheer & onderhoud aangemerkt.
- g) In de vorige business case zijn geen kosten voor eIDAS-voorzieningen meegenomen, omdat de eIDAS-verordening in de vorige business case buiten de scope van de analyse lag. Het gaat hier dus om extra kosten ten opzichte van de vorige business case.

Bronnen: De Digicommissaris, *Bestedingsplan 2018 e.v. Naam voorziening 2.1 eID* (cijfers eID-stelsel), *De Digicommissaris, Bestedingsplan 2018 e.v. Naam voorziening: DigiD* (cijfers authenticatiedienst DigiD Sub + hoog), *De Digicommissaris, Bestedingsplan 2018 e.v. Naam voorziening 2.3 eIDAS* (cijfers eIDAS voorzieningen), Ministerie van BZK, *Opdrachtovereenkomst 2018 Programma eID* (cijfers BSNk en inzage + set van eisen & toezicht en beheer in 2018), *Programboard 22 februari 2018* (cijfers BSNk en inzage + set van eisen & toezicht en beheer na 2018).

In totaal bedragen de jaarlijkse beheer- en onderhoudskosten gemiddeld €61,5 miljoen per jaar. In de vorige business case was er nog vanuit gegaan dat de gemiddelde beheer- en onderhoudskosten gelijk waren aan €44,4 miljoen per jaar. Dat is een aanzienlijke stijging van de kosten, die overigens deels (voor ongeveer €4,5 miljoen) wordt verklaard doordat de kosten voor de eIDAS voorzieningen niet waren meegenomen in de vorige business case.

Vaste kosten doorontwikkeling en beleidsvorming middelen

In de vorige business case is ervan uit gegaan dat er een organisatie moet komen die zich bezig gaat houden met de verdere doorontwikkeling en beleidsvorming. Deze organisatie bestaat uit ongeveer 5,25 fte bij het ministerie van BZK en 1 fte bij het ministerie van IenM (voor het rijbewijs). In aanvulling is een bedrag van €500 duizend per jaar voor de RvIG en €150 duizend per jaar voor de RDW geschat. Per saldo kwamen de jaarlijkse kosten in de vorige business case uit op een bedrag van €1,35 miljoen per jaar. Deze kostenpost is gelijk gelaten in deze business case.

4.1.2 Kosten nulmeting

Eén van de onderzoeksvragen in dit rapport is wat de kosten en baten zijn als het eID-programma zou stoppen (bv. op 1 maart 2018). Als het eID-programma op 1 maart 2018 zou stoppen zijn er vanzelfsprekend geen baten meer ten opzichte van het nulalternatief waarbij het eID-programma überhaupt niet gestart zou zijn (burgers moeten dan gebruik blijven maken van DigiD Basis en DigiD Midden om in te loggen bij dienstverleners).

Allereerst zijn de gemaakte kosten in de periode van 2015 tot en met 2017 (in totaal een bedrag van €62 miljoen) dan voor een belangrijk deel voor niets geweest. Echter, deze kosten behoren geen rol te spelen bij het besluit om al dan niet te stoppen met het eID-programma. Dit zijn namelijk zogenaamde verzonken kosten en deze kosten zijn niet meer ongedaan te maken.

Mogelijk zijn er desinvesteringen en afbouwkosten als er gestopt zou worden met het eID-programma. Navraag heeft geleerd dat de afbouwkosten van het programma relatief beperkt zullen zijn. Waar in het fysieke domein mogelijk kosten moeten worden gemaakt voor het ontmantelen van een fabriek, is dit in het ICT-domein veel minder relevant.

Recent is de Operatie BRP beëindigd en daarbij is een 'bewindvoerder' aangesteld die is gevraagd om contracten, overeenkomsten, convenanten en dergelijke te inventariseren en te beëindigen en om de ontwikkelde programmatuur te inventariseren (ten behoeve van toekomstig hergebruik).⁶² Bij het nu beëindigen van het eID-programma zou er mogelijk een vergelijkbare 'bewindvoerder' moeten komen, de kosten daarvoor zijn naar verwachting ook beperkt.

Belangrijker is echter dat zowel Logius (onder meer authenticatiedienst), RvIG (eNIK) als RDW (eRijbewijs) lopende contracten hebben voor de komende jaren en dat het niet zonder meer mogelijk is om zonder extra kosten van deze contracten af te komen. Er is een grondige juridische analyse nodig om een serieuze inschatting te kunnen maken van de te maken kosten als contracten nu worden opgezegd. Daarnaast zijn de dan nog te maken kosten ook sterk afhankelijk van het onderhandelingsresultaat tussen enerzijds Logius, RvIG en RDW en anderzijds hun leveranciers. Die grondige juridische analyse valt buiten de scope van deze opdracht.

Mocht er serieus overwogen worden om de stoppen met het eID-programma dan is het sterk aan te raden om een grondige juridische analyse te maken van de bestaande contracten om de impact van stoppen goed in te kunnen schatten.

⁶² Brief van de minister van Binnenlandse Zaken en Koninkrijksrelaties aan de Tweede Kamer der Staten-Generaal d.d. 26 september 2017 betreffende 'Basisregistratie Personen'.

4.1.3 Conclusies

In de volgende tabel zijn alle kosten naast elkaar gezet. Daarbij zijn de reële waarde van de kosten (de som van alle kosten gedurende de gehele periode) en de contante waarde⁶³ van de kosten gepresenteerd. Voor het bepalen van de contante waarde van de kosten is een discontovoet van 3% gebruikt.⁶⁴ In de volgende tabel is het totaaloverzicht opgenomen van de kosten.

Tabel 4.6 Kosten totaal (in € mln.)^{a)}

Kosten	Reële waarde ^{a)}	Contante waarde
Ontwikkelkosten eID	69,0	64,5
Ontwikkelkosten eIDAS	11,8	10,8
Aansluitkosten dienstverleners eIDAS	12,8	11,6
Kosten DigiD Hoog	120,0	93,7
Kosten kaartlezers	144,9	114,4
Kosten private middelen	PM	PM
Beheer eID-stelsel	142,8	113,9
Authenticatiedienst DigiD Sub. + Hoog - vaste kosten	282,2	222,9
Authenticatiedienst DigiD Sub. + Hoog - variabele kosten	156,0	122,8
Authenticatiedienst (privaat)	PM	PM
Beheer eIDAS	41,8	32,8
Doorontwikkeling beleid	13,5	10,7
Totaal	994,7 + PM	797,9 + PM

a) Bij twee kostenposten is in deze business case gerekend met een bandbreedte, in deze tabel hebben wij voor deze kostenposten alleen de maximumwaarde gepresenteerd, omdat de verschillen tussen de minimumwaarde en de maximumwaarde relatief beperkt zijn in vergelijking met het totaalbedrag van de kosten. Het bedrag voor de kostenpost Kosten DigiD Hoog is € 115,1 mln. in de minimumvariant en € 120,0 mln. in de maximumvariant. Het bedrag voor de kostenpost Aansluitkosten dienstverleners eIDAS is € 3,8 mln. in de minimumvariant en € 12,8 mln. in de maximumvariant. In alle relevante tabellen in hoofdstuk 3 en de managementsamenvatting is alleen de maximumwaarde van deze beide kostenposten gepresenteerd.

b) Het gaat hier om de totale kosten over de gehele periode (van 2015 tot en met 2027).

Als alle kosten voor de periode 2015 tot en met 2027 naast elkaar worden gezet dan komen deze uit op een bedrag van € 994,7 miljoen (met een contante waarde van € 797,9 miljoen). Dit is een aanzienlijke stijging ten opzichte van de vorige business case, waar de gesommeerde kosten voor de periode 2015 tot en met 2027 gelijk waren aan een bedrag van € 658,8 miljoen. Dit is een stijging van de kosten met 51% ten opzichte van de vorige business case. Ook als de extra elementen uit de business case worden gehaald (eIDAS-verplichting), dan is nog een stijging van de kosten met ongeveer 41% te zien ten opzichte van de vorige business case.

Er is binnen deze opdracht geen uitgebreide analyse uitgevoerd door Ecorys op de plausibiliteit van de gepresenteerde cijfers. Het is daarom ook aan te raden om een review te laten uitvoeren op de hoogte van te maken de kosten.

⁶³ Kosten en baten vallen op verschillende momenten in de tijd. De contante waarde is een maat voor de huidige waarde van geld. Door kosten en baten uit te drukken in een contante waarde kunnen kosten en baten die op verschillende momenten in de tijd vallen met elkaar vergeleken worden. Als de netto contante waarde (contante waarde van de baten minus de contante waarde van de kosten) groter is dan 0, dan is het interessant om te investeren in het project.

⁶⁴ Deze discontovoet bestaat uit een risicovrije discontovoet van 0% en een risico-opslag van 3%. In de vorige business case is een discontovoet van 0% gehanteerd. Uit het lopende onderzoek voor het opstellen van een werkwijzer voor MKBA's voor digitale overheidsprojecten is de conclusie getrokken dat het een discontovoet van 3% voor digitale overheidsprojecten wordt geadviseerd. Daarom is hier ook een discontovoet van 3% voor de kosten en baten gebruikt.

4.2 Baten

In deze paragraaf zijn de baten van inloggen in het BSN-domein met eID-middelen op betrouwbaarheidsniveau substantieel en hoog verder uitgewerkt. In het eerste deel van deze paragraaf is een inventarisatie gemaakt van de baten en in het tweede deel van de paragraaf zijn de te kwantificeren baten verder uitgewerkt. In het derde deel van de paragraaf is bepaald wat de orde van grootte moet zijn van de minder goed te kwantificeren baten om ervoor te zorgen dat de business case net in evenwicht is.

4.2.1 Inventarisatie van de baten

De inventarisatie van de baten is niet veranderd ten opzichte van de vorige business case. Vandaar dat in deze paragraaf de tekst uit de vorige business case integraal is overgenomen.

De baten van het eID-stelsel in samenhang met het gebruik van publieke en private middelen zijn sterk afhankelijk van de wijze waarop toekomstige digitale diensten voor burgers *op dit moment* worden aangeboden. Uit een inventarisatie is naar voren gekomen, dat hier de volgende driedeling te maken is:

- Digitale dienstverlening en authenticatie met DigiD;
- Digitaal dienstverlening en authenticatie met een alternatief middel;
- Geen digitale dienstverlening.

In het navolgende zijn deze verder uitgewerkt.

Digitale dienstverlening en authenticatie met DigiD

In 2017 wordt er 280 miljoen keer ingelogd met DigiD Basis en DigiD Midden (betrouwbaarheidsniveau laag) en het is de verwachting dat dit aantal nog verder zal groeien. De meerwaarde van een eID-stelsel met middelen op betrouwbaarheidsniveau substantieel en hoog i.p.v. het bestaande stelsel met een middel op betrouwbaarheidsniveau laag zijn:

- Een stelsel met middelen op betrouwbaarheidsniveau substantieel en hoog heeft een hogere betrouwbaarheid dan DigiD basis en DigiD midden. Hierdoor neemt de zekerheid toe dat de overheidsdienstverlener met de juiste burger te maken heeft. Dit leidt tot voordelen op het gebied van **veiligheid, rechtmatigheid en minder mogelijkheden voor identiteitsfraude**. In het verlengde daarvan leiden minder mogelijkheden tot identiteitsfraude mogelijk ook tot besparingen voor toezicht en handhaving van fraude.⁶⁵
- Het Forum Standaardisatie heeft een handreiking⁶⁶ geschreven voor betrouwbaarheidsniveaus voor authenticatie bij elektronische overheidsdiensten. Nu zijn er nog veel overheden, waar digitale diensten worden aangeboden met DigiD (betrouwbaarheidsniveau laag), waar eigenlijk een middel met betrouwbaarheidsniveau substantieel of hoog vereist zou zijn. Het eID-stelsel met middelen op betrouwbaarheidsniveaus substantieel en hoog draagt bij een **betere compliance van overheden aan Europese en nationale wet- en regelgeving op het gebied van privacy en beveiliging**.
- Digitale dienstverlening en authenticatie met DigiD Basis en DigiD Midden (de huidige situatie) kost ook geld. In dit hoofdstuk zijn de integrale kosten meegenomen van de authenticatiedienst voor middelen van betrouwbaarheidsniveau substantieel en hoog. Deze kosten komen **in plaats van** de kosten die nu gemaakt moeten worden voor de authenticatiedienst voor DigiD Basis en DigiD Midden. Ongeacht hoe het vervolg eruit komt te zien, er moeten kosten voor digitale authenticaties worden gemaakt. In kosten-batenanalyses spreekt men hier van kosten

⁶⁵ De praktijk leert dat dit soort besparingen niet altijd tot een efficiencyvoordeel leiden, maar dat de hier uitgespaarde middelen kunnen worden gebruikt voor de toezicht en handhaving van andere vormen van fraude.

⁶⁶ Forum Standaardisatie (2014), *Betrouwbaarheidsniveaus voor authenticatie bij elektronische overheidsdiensten (versie 3). Een handreiking voor overheidsorganisaties*.

van het nulalternatief of vermeden kosten van het projectalternatief.⁶⁷ Voor een zuivere vergelijking moeten deze **vermeden kosten van huidige authenticatiedienst DigiD** kosten ook worden meegenomen.

Digitaal dienstverlening en authenticatie met een alternatief middel

Voor diensten die op dit moment al digitaal worden afgehandeld met bestaande passen voor authenticatie heeft het eID-stelsel met middelen op betrouwbaarheidsniveau substantieel en hoog de volgende toegevoegde waarde:

- Door het eID-stelsel met betrouwbaarheidsniveaus substantieel en hoog is het denkbaar dat bestaande passen voor authenticatie niet meer nodig zijn. Dit kan leiden tot aanzienlijke **kostenbesparingen voor bestaande passen voor authenticatie**. Het gaat dan om kosten voor de uitgifte van de authenticatiemiddelen (voor zowel de burger als de overheidsdienstverlener) en systeemkosten.

Geen digitale dienstverlening

Voor digitale diensten die op dit moment nog niet digitaal worden afgehandeld (omdat een middel met voldoende betrouwbaarheid ontbreekt) heeft een publiek eID-middel langs verschillende lijnen toegevoegde waarde ten opzichte van de huidige situatie. Deze zijn:

- Dienstverlening verloopt digitaal in plaats van op papier of aan de balie, doordat er een middel is met voldoende betrouwbaarheid. Papieren processen en het baliebezoek van burgers kunnen hierdoor afnemen. Dit leidt tot de volgende effecten:
 - **Kosten procesaanpassingen bij overheidsdienstverleners**. Overheidsdienstverleners moeten allereerst hun diensten aanpassen om de stap van papier of baliediensten naar digitale diensten te maken. Dit vereist procesaanpassingen en investeringen in ondersteunende ICT-systemen.
 - **Efficiencyverbetering dienstverlening**. Doordat diensten digitaal kunnen worden afgehandeld, kunnen processen efficiënter en met minder fouten worden uitgevoerd. Dit kan leiden tot aanzienlijke kwaliteitsslagen en efficiencybesparingen bij overheidsdienstverleners.
 - **Tijdsbesparing dienstverlening voor burgers**. Ook burgers ondervinden voordelen van digitale dienstverlening. Diensten kunnen sneller worden afgehandeld en bijvoorbeeld reistijden vervallen bij digitale dienstverlening. Daarbij kan de burger 24/7 tijdsafhankelijk en plaats onafhankelijk diensten afnemen op het moment dat het de burger uitkomt.

Aanvullend kan nog als baat benoemd worden dat gebruikers de publieke eID-middelen in het elektronisch gebruik ervaren als één geheel (zelfde 'look and feel' voor de burger), waarbij digitaal toegang wordt verkregen tot meerdere dienstverleners. Hiermee kan gesteld worden dat de inzet van eID-publieke middelen bijdraagt aan een hogere **gebruiksvriendelijkheid**. Verder draagt de komst van DigiD Substantieel en DigiD Hoog bij aan de **keuzevrijheid** van burgers door naast het publieke middel ook private middelen (op betrouwbaarheidsniveau substantieel) beschikbaar te stellen.⁶⁸

Merk op: Bij deze effecten gaat het om effecten van 'het huis'. Om de efficiencyvoordelen van digitale diensten te kunnen realiseren is alleen een eID-stelsel met middelen op

⁶⁷ Anders gesteld: Er is vanuit gegaan dat de authenticatiedienst van DigiD wordt omgebouwd tot een authenticatiedienst voor DigiD + de andere publieke middelen. Omdat we bij de raming van de kosten voor de authenticatiedienst zijn uitgegaan van de integrale kosten (en niet van de meerkosten om de authenticatiedienst aan te passen naar eID-middelen) moeten tegenover deze integrale kosten in het projectalternatief ook de integrale kosten in het nulalternatief worden meegenomen. Deze te maken kosten in het nulalternatief (authenticatiedienst voor DigiD) vormen daarmee ook baten voor het projectalternatief.

⁶⁸ Het burgeronderzoek wijst uit dat een meerderheid van de burgers er een voorkeur voor heeft om zich bij de overheid met een publiek middel te authenticeren.

betrouwbaarheidsniveau substantieel en hoog niet voldoende, maar is het ook van belang dat de betreffende overheidsdiensten worden gedigitaliseerd.

4.2.2 Te kwantificeren baten

In de vorige business case zijn de volgende baten gekwantificeerd: vermeden kosten van de authenticatiedienst DigiD en te vermijden kosten van alternatieve passen. Bij het berekenen van deze baten zijn de achterliggende uitgangspunten zoveel mogelijk gelijk gehouden als in de vorige business case, tenzij er nieuwe informatie was over de hoogte van de baten.

Vermeden kosten authenticatiedienst DigiD

In de vorige business case is een raming gemaakt van de kosten die gemaakt moeten worden om de authenticatiedienst voor DigiD Basis en DigiD Midden in de lucht te houden. Deze kosten zijn gelijk gehouden in de herijking van de business case, immers het nulalternatief is ook niet gewijzigd. Er is in de vorige business case geraamd dat de kosten voor een authenticatiedienst voor DigiD gelijk zijn aan €24,0 miljoen per jaar.⁶⁹

Tabel 4.7 Kosten authenticatiedienst DigiD Basis + Midden (in € mln.)

Kosten	Kosten per jaar	Reële waarde ^{a)}	Contante waarde
Vaste kosten beheer & onderhoud	14,0	140,0	110,9
Variabele kosten beheer & onderhoud	10,0	100,0	79,2
Totaal	24,0	240,0	190,1

a) Het gaat hier om de totale baten over de gehele periode (van 2015 tot en met 2027).

Vermeden kosten alternatieve authenticatiepassen

In de vorige business case zijn ook baten opgenomen in de vorm van vermeden kosten van alternatieve authenticatiepassen. Deze baat is nog steeds actueel en voor de volledigheid is de paragraaf uit de vorige business case hier integraal overgenomen, waarbij waar relevant gepresenteerde cijfers wel zijn geactualiseerd.

Naast DigiD zijn er nog andere oplossingen voor elektronische identificatie en toegang tot digitale diensten, zoals verschillende bestaande passen voor authenticatie. Deze alternatieve authenticatieoplossingen kunnen overbodig worden wanneer er een publiek eID-middel beschikbaar komt. In de wereld zonder publiek eID-middel (het nulalternatief) moeten proceseigenaren hun eigen systemen voor passen voor authenticatie in de lucht houden. Het gaat hier dan om het technische beheer van het eigen authenticatiesysteem (IT-component) en om het organisatorische beheer (het verzorgen van inschrijvingen, kwaliteitsbeheer en dergelijke). Ook moeten proceseigenaren een helpdesk voor haar klanten bemannen, waar (technische) vragen over de pas kunnen worden ondervangen.

Ter illustratie zijn ook in deze business case de te besparen baten van de UZI-pas voor de gebruiker doorgerekend als deze vervangen worden door een publiek middel met betrouwbaarheidsniveau hoog. De kosten voor een UZI-pas zijn gelijk aan €170 voor een periode van 2 jaar.⁷⁰ Er waren 77.818 UZI-passen in omloop op 1 november 2017.⁷¹ Voor de berekening van de baten is uitgegaan van een stabiel aantal UZI-passen van 77.818 die iedere 2 jaar vervangen moeten worden. Deze kosten zijn naast de kosten gezet waarbij alle 77.818 zorgprofessionals met een

⁶⁹ Ministerie van BZK (2016), *Bestedingsplan 2017 e.v., 2.2 DigiD (inclusief buitenland & Machtigen)*

⁷⁰ <https://www.uziregister.nl/uzi-pas/kosten-pas>. Het gaat hier om de aanschafprijs, het is niet duidelijk of dit ook de kostendekkende prijs is. In een interview met het CIBG is aangegeven dat de kostprijs per kaart gelijk is aan €400 per kaart. In de vorige business case is gerekend met een bedrag van €255 voor een periode van 3 jaar (het bedrag per jaar is in beide gevallen €85).

⁷¹ Nieuwe informatie ministerie van VWS. In de vorige business case is gerekend met 90.000 UZI-passen.

UZI-pas in 2022⁷² een eNIK aanschaffen voor €56,08 (zijnde €51,08 voor de NIK⁷³ en €5,00 voor de extra e-functionaliteit) met een geldigheid van 10 jaar. Dit leidt tot een kostenbesparing van €6,6 miljoen per jaar vanaf 2023. Per saldo valt deze kostenbesparing lager uit dan in de vorige business case, hetgeen in het bijzonder samenhangt met het lagere aantal passen dat op dit moment in omloop is.

In de praktijk zullen deze baten wel iets lager uitvallen. Om deze baten te kunnen realiseren moeten er namelijk nog aanpassingen in de huidige systemen worden gemaakt om gebruik van het eID-middel mogelijk te maken. Attributen kunnen dan via de stelseloplossing worden uitgelezen via het UZI-register. Deze kosten zijn niet in kaart gebracht en als PM-post opgenomen. Omdat de tarieven voor de UZI-middelen kostendekkend zijn, zullen deze kosten wel aan de gebruiker worden doorberekend.

De UZI-pas is een concreet voorbeeld van een pas voor de elektronische identificatie, maar er zijn ook andere authenticatieoplossingen in gebruik. Meest voorkomende zijn eigen databases met gebruikersnaam – wachtwoord combinaties, die overigens veel goedkoper zijn dan de bovengenoemde oplossing. Naar verwachting kan een volledige uitrol van het eID-stelsel met middelen op betrouwbaarheidsniveau substantieel en hoog hier ook nog tot aanvullende baten bij proceseigenaren leiden.

Andere voorbeelden van passen zijn bijvoorbeeld de Rijkspas, de Defensiepas, de advocatenpas⁷⁴ en diverse stadspassen. In beginsel kunnen allerlei andere passen worden uitgefaseerd en vervangen door eID-middelen. In deze paragraaf is ter illustratie een voorbeeld gepresenteerd en is berekend welke baten hier te realiseren zijn, voor andere passen kunnen vergelijkbare berekeningen worden gemaakt. Dit geeft in het bijzonder zicht in de orde van grootte van besparingen die hier mogelijk zijn.

Te kwantificeren baten totaal

In de volgende tabel is het totaaloverzicht opgenomen van de baten voor zover het mogelijk was om deze te kwantificeren. Te zien is dat de som van alle baten over de jaren van 2018 tot en met 2027 (de zogenaamde reële waarde) gelijk is aan €275,2 miljoen, de contante waarde van deze baten is gelijk aan €216,2 miljoen. In de vorige business case was de reële waarde van de baten gelijk aan €288,3 miljoen. Deze daling wordt veroorzaakt doordat het aantal UZI-passen in omloop iets lager blijkt te zijn en doordat de vervanging pas mogelijk wordt in 2022 in plaats van in 2021.

Tabel 4.8 Te kwantificeren baten (bedragen in € mln.)

Baten	Reële waarde van de baten ^{a)}	Contante waarde van de baten ^{b)}
Vermeden kosten authenticatiedienst DigID	240,0	190,1
Vermeden kosten basisregister reisdocumenten	PM	PM
Vermeden kosten alternatieve authenticatiesystemen	35,3	26,1
Totaal	275,3 + PM	216,2 + PM

a) Het gaat hier om de totale baten te realiseren over een periode van 10 jaar (van 2018 tot en met 2027).

b) De contante waarde is berekend voor 2015 (vergelijkbaar met de kosten).

⁷² Er is op dit moment een aanbesteding gaande voor nieuwe UZI-passen voor de komende drie jaar. Dit contract start vanaf oktober 2019 en heeft een looptijd van 3 jaar. Dat betekent dat de UZI-pas vanaf 2022 (dit was 2021 in de vorige BC) kan worden vervangen door een publiek eID-middel op betrouwbaarheidsniveau hoog.

⁷³ In de vorige business case is gerekend met een kostprijs voor een NIK van €52,95.

⁷⁴ Zie bijvoorbeeld: <https://www.advocatenorde.nl/advocatenpas>.

Bijlage 1 Uitwerking impactanalyse

Naast het opstellen van de businesscase is extra aandacht geweest voor de impact die de invoering van eID op de gemeenten zal hebben. Er is gedetailleerd onderzoek gedaan en ook in beeld gebracht wat de kosten voor gemeenten zijn van een aantal maatregelen zullen zijn waar nog niet definitief toe is besloten. Naast de kosten die uit het voorstel voortkomen is er ter illustratie ook gekeken naar de baten, gerealiseerd in de 'huizen'.

Het onderzoek is als volgt uitgevoerd. In overleg met VNG, NVVB en VDP, is een vijftal gemeenten uit het Kennisnetwerk eID van de VNG geselecteerd, waarmee gesproken is over twee onderwerpen:

- De impact op de afdelingen Burgerzaken doordat gemeenten de publieke middelen op niveau DigiD Hoog uitgeven. Het betreft de Nederlandse Identiteitskaart (NIK) en het rijbewijs. De verwachte consequenties van aanvraag, uitgifte en gebruik zijn in beeld gebracht. Hier is de gemeente in de *rol van uitgever van publieke authenticatiemiddelen*.
- De impact die het aansluiten op eID op de gemeentelijke organisatie heeft. Hier betreft het de *rol als dienst aanbieder die op het eID-stelsel moet aansluiten*. Als uitgangspunt is aangenomen dat er een routeringsvoorziening zal komen die de gemeenten ontzorgt. Voor dit onderdeel zijn ook gesprekken gevoerd met ICT-leveranciers in de sector gemeenten.

Introductie en samenvatting aan de hand van VNG Realisatie framework

Bij het bepalen van de impact, sluiten we aan bij de methodiek voor het maken van impact analyses van VNG Realisatie (voormalig KING). We benadrukken dat deze impactanalyse specifiek bedoeld is voor onderhavige business case, en niet voldoet aan de eisen van een impactanalyse van VNG Realisatie, welke meer gericht is op de uitvoeringsmogelijkheden. Dit houdt in dat we de impact voor gemeenten in beeld hebben gebracht met behulp van de SCOPAFIJTH-elementen (security, communicatie, organisatie, personeel, administratieve organisatie, financiën, informatie, juridisch, technologie, huisvesting). Deze elementen geven weer waar de (maatschappelijke) kosten en baten binnen de organisatie naar verwachting gaan vallen. In de volgende paragrafen lichten we de achtergrond van de elementen zoals opgenomen in de tabel verder toe.

	Impact→	Security	Communicatie	Organisatie	Personeel	Administratie	Financiën	Informatie	Juridisch	Technologie	Huisvesting
Gemeente rol	Oorzaak ↓										
Uitgever middel	Algemene voorlichting aan de balie										
	Doorverwijzing naar landelijke voorziening bij 'hij doet het niet' vragen										
	Hulp bij oplossen problemen										
	BRP adres-check aan de balie										
	Aanpassingen innameprocessen										
	Verhogen kwaliteit identiteitsvaststelling										
Dienstverlener	Aansluiten op de routeringsvoorziening										
	Gebruik van de routeringsvoorziening										
	Audit verplichtingen										

Uitgeven publiek middel

In de bestaande businesscase uit 2016 is één post opgenomen vanwege extra taken die de gemeente als uitgever van rijbewijs en NIK gaat uitvoeren. Die extra taken zijn beperkt van omvang omdat in het procesontwerp (de Project Start Architectuur of PSA) zoveel mogelijk is aangesloten op bestaande processen. In de business case is als enige taakverzwaring meegenomen dat gemeenten bij de uitreiking van NIK en Rijbewijs beperkte voorlichting geven over de authenticatie functionaliteit op de documenten. Geschat is dat daarvoor gemiddeld twee minuten extra tijd nodig is voor een uitreiking.

In een door KING in 2016 uitgevoerde impact analyse⁷⁵, is aangegeven dat er mogelijk meer verandering bij gemeenten plaatsvinden die tot extra kosten kunnen leiden. Die kunnen ontstaan door de identiteitsvaststelling kwalitatief op een hoger niveau te brengen en door extra werk voor gemeenten bij bijzondere situaties (de zogenaamde 'unhappy flows'). Naar aanleiding van het rapport van VNG Realisatie, zijn aanpassingen in de PSA doorgevoerd en beperken de veranderingen voor gemeenten zich tot de volgende onderwerpen:

- *Voorlichting bij uitreiking van documenten aan burgers* over de authenticatie functionaliteit bij de uitreiking van het document
- *Mogelijke rol gemeenten bij het oplossen van problemen* die zich voordoen met de werking van de authenticatiefunctie
- *Standaard check op de juistheid van het BRP-adres* tijdens de aanvraag van een nieuw document
- *Mogelijke aanpassing van inname- en ontwaardingsprocessen* zodat na inname onderzoek aan de chip en daarop geplaatste functies mogelijk wordt.
- *Verhoging kwaliteit van de identiteitsvaststelling* bij aanvraag en uitgifte van de documenten.

Dit wordt hieronder verder uitgewerkt.

Voorlichting bij uitreiking van documenten aan burgers

Gemeenten verstrekken bij het uitreiken van een nieuw document uitsluitend enige algemene informatie. De precieze inhoud van de te verstrekken informatie moet nog worden bepaald. Gesproken wordt over uitreiken van een folder, uitleg over de pinbrief die toegezonden zal worden, uitleg over het gebruik van het middel. Bij alle andere vragen en verzoeken van burgers beperkt de gemeente zich tot het doorverwijzen naar de website en de helpdesk van de landelijke beheerorganisatie.

Impact op de business case: Deze stand van zaken komt sterk overeen met de situatie bij het opstellen van de vorige businesscase. De inschatting van 2 minuten extra behandelings tijd voor de uitreiking van een document blijft daarom gehandhaafd. Zie hiervoor paragraaf 2.2.

Mogelijke rol gemeenten bij het oplossen van problemen

De PSA heeft als uitgangspunt dat algemene voorlichting, communicatie met burgers over het activeren, blokkeren en deblokkeren van het middel, het beantwoorden van vragen, het toezenden van brieven en ondersteuning bij het **oplossen van problemen wordt belegd bij de landelijke beheerorganisatie**. Gemeenten vinden alleen doorverwijzen slecht passen bij hun dienstverlenende rol als overheid die dicht bij de burgers staat en voorzien dat burgers minder tevreden zullen zijn over de dienstverlening. Alle bevroegde gemeenten verwachtten dat burgers zich, ondanks andere instructies, met vragen en problemen zullen wenden tot de gemeente. Ondersteuning die zich alleen beperkt tot het digitale kanaal zal, zoals de ervaring leert, niet alle problemen kunnen oplossen. Dit heeft als risico dat een groep burgers geen gebruik zal kunnen maken van de

⁷⁵ KING (2016) Impactanalyse Uitgifteproces publiek eID middel.

authenticatiefunctie op het publieke middel en hetgeen kan leiden tot reputatieschade van het middel.

Tegelijk wordt onderkend dat verdergaande voorlichting aan burgers en ondersteuning van het oplossen van problemen hoge eisen stelt aan de inhoudelijke en technische kennis van de betrokken medewerkers. Ook wordt de vraag gesteld of een servicepunt bij gemeenten alleen voor het publieke middel de beste oplossing is. Gesuggereerd wordt om aan te sluiten bij initiatieven die bredere ondersteuning verlenen, zoals bijvoorbeeld via bibliotheken gebeurt.

Impact op de business case: In de herziene businesscase wordt de PSA gevolgd met als uitgangspunt dat alleen via het digitale kanaal ondersteuning zal worden verleend. Wanneer alsnog besloten wordt tot het verlenen van ondersteuning op locatie zijn daar substantiële bedragen mee gemoeid.

Standaard check op de juistheid van het BRP-adres

In de uitgifte- en gebruiksprocessen die in de PSA worden beschreven, komen stappen voor waarbij een brief wordt verzonden naar het BRP-adres. Een voorbeeld is de Pin – Puk brief die binnen een week na uitreiking van een NIK of rijbewijs wordt toegestuurd. Het is van veel belang dat het adres in de BRP juist en actueel is. In de PSA wordt als uitgangspunt gehanteerd dat tijdens de aanvraag, waarvoor een burger fysiek bij de gemeente moet verschijnen, een check plaatsvindt op de juistheid van het BRP-adres. Gemeenten geven aan dat ze dit vanzelfsprekend vinden, bij de meerderheid is het onderdeel van de bestaande praktijk.

Impact op de business case: Het actueel houden van het BRP-adres is onderdeel van het beheer van de basisregistratie. Er is geen aanleiding om de kosten van een check bij de aanvraag van een NIK of rijbewijs aan de invoering van eID toe te rekenen.

Mogelijke aanpassing van inname- en ontwaardingsprocessen

Wanneer de authenticatiefunctie van het publieke middel na de uitreiking niet werkt, is een van de denkbare oorzaken een defecte chip. Gezien de intensieve controle die plaatsvindt bij de productie, is de kans hierop zeer klein. Wanneer een burger een publiek middel met een werkende authenticatie functie wil hebben, en daarom het document door de gemeente laat innemen, is het wenselijk om onderzoek aan de chip te kunnen uitvoeren. Dit vraagt een aanpassing van de bestaande inname en ontwaardingsprocessen, om te voorkomen dat de chip daarbij beschadigd wordt. Ook dient het document voor onderzoek naar de RDW of RvIG gezonden te worden. Gemeenten geven aan dat de processen rond het innemen en ontwaarden van identiteitsdocumenten sterk zijn gestandaardiseerd, gereguleerd en dat de voorschriften mede worden afgedwongen door de gebruikte ICT-systemen. Om in zo'n proces een uitzondering te kunnen maken, dienen verhoudingsgewijs zeer hoge kosten gemaakt te worden voor het oplossen van een weinig voorkomend probleem.

Impact op de business case: In de businesscase wordt met deze kosten geen rekening gehouden, er wordt vanuit gegaan dat een alternatieve oplossing gekozen zal worden. Daarbij kan gedacht worden aan niet oplossen van het probleem of het vervangen van het document zonder de burger kosten in rekening te brengen voor het vervangende document. Er zijn dan dus wel kosten aan verbonden, maar de waarschijnlijkheid dat het zich voordoet is zeer gering.

Verhogen kwaliteit identiteitsvaststelling.

Gemeenten (VNG en NVVB) zijn van mening dat de invoering van eID noodzaakt tot het verhogen van de kwaliteit van de initiële identiteitsvaststelling bij de aanvraag en de uitgifte van publieke eID middelen. Het eID programma beschouwt het betrouwbaar vaststellen van de identiteit als een

regulier onderdeel van de gemeentelijke taak. Mogelijke extra kosten voor vaststelling van identiteit worden daarom niet meegenomen in de businesscase. Wel geven we een indicatie van de maatregelen die gemeenten nodig achten voor identiteitsvaststelling

Om sterker te identificeren moeten medewerkers worden opgeleid

Een indicatie van de kosten voor het grondiger vaststellen van de identiteit bij uitgifte van het middel baseren we op de aannamen dat baliepersoneel zal moeten worden bijgeschoold.

Het bijscholen van baliepersoneel is op dit moment mogelijk door bijvoorbeeld het volgen van modules aan de publieksacademie. De modules gericht op het opleiden van baliepersoneel om de identiteit van personen en de geldigheid van brondocumenten te waarborgen kosten nu respectievelijk € 825 en € 550. Wanneer dit op grote schaal plaats gaat vinden kunnen de kosten wellicht nog iets lager uitvallen. Hierop baseren we onze aanname voor bijscholingskosten voor baliepersoneel: **€ 1.000 per medewerker**. Baliepersoneel dat in aanmerking komt voor deze bijscholing moet een opleidingsniveau mbo-4 hebben. Normaal is een opleidingsniveau mbo-2. Voor kleine gemeenten kan dit zorgen voor additionele kosten als er een gebrek is aan medewerkers geschikt voor bijscholing.

Afhankelijk van het aantal fte dat nodig is voor het afhandelen van de uitgifte van de eID middelen aan de gemeente balie, verschilt het aantal medewerkers dat moet worden opgeleid. We gaan ervanuit dat er minimaal **2 medewerkers per gemeente** moeten worden opgeleid zodat er altijd één gekwalificeerde medewerker aanwezig kan zijn. Bij grotere gemeenten is dit naar verwachting niet toereikend. Niet alleen zal het aantal aanvragen hoger liggen, dit zullen ook vaker complexe aanvragen zijn. Uitgaande van **380 gemeenten**, ligt de ondergrens voor **bijscholingskosten rond één miljoen euro**.

Gemeenten sluiten als dienstverlener aan op eID via de routeringsvoorziening.

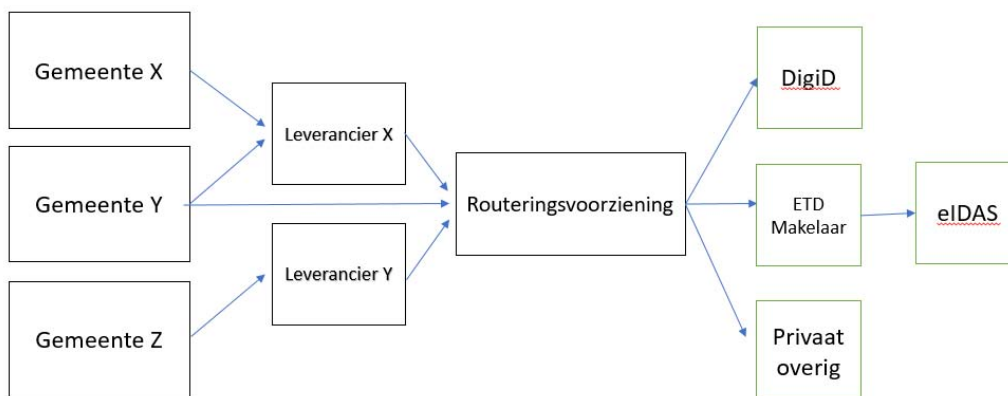
Of gemeenten aansluiten, óf ze de aansluiting gebruiken en h e ze de eID en de daarbij horende authenticatiemiddelen waarden afhangt van verschillende zaken af. In dit hoofdstuk beschrijven we de:

1. Algemene toelichting Routeringsvoorziening
2. Meerwaarde van de routeringsvoorziening voor gemeenten
3. Aansluiten op de routeringsvoorziening en bijkomende kosten
4. Gebruik van de aansluiting

De routeringsvoorziening

Een nieuw element in de architectuur van eID is de routeringsvoorziening. De routeringsvoorziening is bedoeld om de dienstaanbieders die moeten aansluiten op eID te ontzorgen door  en aanspreekpunt,  en factuur en  en koppelvak te bieden. Tot nu toe was er sprake van dat dienstaanbieders (waaronder gemeenten) op alle ontsluitende diensten binnen eID zouden moeten aansluiten. Daarbij moet gedacht worden aan DigiD, ETD-makelaars als koppeling met eIDAS en private aanbieders zoals iDIN, Idensys en mogelijk nog andere private aanbieders.

Met gemeenten is gesproken over het voorstel dat momenteel binnen ontwikkeld wordt om dienstaanbieders via de routeringsvoorziening  en koppelvak te bieden. Schematisch kan dit als volgt in beeld gebracht worden:



Het plan is om de huidige DigiD aansluitingen van gemeenten op de routeringsvoorziening over te zetten. Gemeenten kunnen op meerdere manieren aangesloten zijn op DigiD: door zelf een of meer aansluitingen te nemen of door gebruik te maken van de aansluiting van een of meer ICT-dienstverleners. Veel gemeenten nemen in de huidige situatie een leverancier in de hand om de aansluitingen te verzorgen. Leveranciers ontzorgen gemeenten, door het aanbieden van servicediensten. De DigiD aansluiting is vaak een onderdeel van een groter dienstenpakket. Wanneer de routeringsvoorziening wordt opgezet, zullen de huidige DigiD aansluitingen worden overgezet op de routeringsvoorziening. Waar leveranciers de aansluiting voor gemeenten verzorgen, zullen zij dit naar verwachting blijven doen in de nieuwe situatie. De routeringsvoorziening verzorgt de koppeling met verschillende identificatiemiddelen en ontzorgt zo de gemeente direct, dan wel indirect via de leverancier (zie figuur).

Groepsaansluitingen of meervoudige DigiD aansluitingen

Bij een groepsaansluiting hanteert de ICT-leverancier één DigiD aansluiting met daarachter meerdere BSN-gerechtigde dienstverleners (bijvoorbeeld een gemeente of zorgpartij). Sinds 2014 worden geen nieuwe groepsaansluitingen meer toegestaan omdat ze niet aan de vereisten 'Herkenbaar, Betrouwbaar, Controleerbaar en Transparant' voldoen. Als alternatief wordt een meervoudige aansluiting voorgesteld. Hierbij heeft iedere BSN-gerechtigde dienstverlener zijn eigen DigiD aansluiting, technisch gefaciliteerd door de ICT-dienstverlener. Kosten voor het omzetten van de groepsaansluiting naar individuele DigiD aansluitingen vallen in eerste instantie bij de ICT-dienstverlener en kunnen, bij grote partijen oplopen tot **eenmalig € 20.000**. Naast het eenmalig omzetten moeten de aangesloten dienstverleners een PKlo certificaat bezitten. Indicatie van de kosten is **€ 500 per 3 jaar** exclusief een verwachte kostenreductie bij bulkinkoop door de ICT-leverancier. Ook moet de dienstverlener een URL hebben voor de website/portal; kosten ongeveer **€ 10 per jaar**. Tot slot moeten de DigiD aansluitingen jaarlijks ge-audit worden. Bij meervoudige aansluiting wordt de inrichting, werking en bestaan van de koppeling met DigiD met de diestaanbieders getoetst bij de ICT-leverancier. Deze organiseert het toezicht op de koppeling en laat de publieke dienstverlener een verklaring tekenen voor het beheer.

Wanneer de DigiD aansluiting wordt omgezet naar een aansluiting op de routeringsvoorziening, blijft die inhoudelijk bij de start gelijk aan de bestaande DigiD aansluiting: de dienaarbieder ontvangt een bericht met een BSN. Op termijn zal dit koppelvlak worden gemoderniseerd. Dit is nodig om nieuwe functionaliteiten die binnen eID beschikbaar komen te kunnen faciliteren. Het betreft bijvoorbeeld het toevoegen van machtigingsfunctionaliteit of het leveren van polymorfe pseudoniemen aan de dienaarbieders. Ook bestaat de wens om de bestaande protocollen (CGI, SAML) te vervangen door een moderner protocol.

Meerwaarde van de routeringsvoorziening voor gemeenten.

De meerwaarde van de routeringsvoorziening wordt door gemeenten en hun leveranciers meer in kwalitatieve dan in kwantitatieve termen geschetst. Gemeenten beschikken nu al over aansluitingen op meerdere voorzieningen die in de toekomst achter de routeringsvoorziening verdwijnen: DigiD (alle gemeenten hebben in principe minimaal één DigiD aansluiting), e-Herkenning en daarmee hetzelfde koppelvlak dat nodig is voor aansluiting op ETD (ongeveer de helft van de gemeenten) en Idensys omdat een aantal van de geïnterviewde gemeenten hebben meegewerkt aan pilots waarin Idensys middelen zijn beproefd. Het hebben en onderhouden van een koppelvlak is in relatie tot het geheel van de ICT kosten een relatief bescheiden post. Door de routeringsvoorziening zullen de processen bij de gemeenten nauwelijks veranderen. Kwalitatief is de routeringsvoorziening wel degelijk van belang: die heeft de potentie om duidelijkheid, voorspelbaarheid, eenvoud en zekerheid te bieden.

Het is erg belangrijk voor gemeenten dat hun authenticatievoorziening aan zeer hoge eisen qua beschikbaarheid en betrouwbaarheid voldoet. Een steeds groter deel van de dienstverlening wordt geheel of gedeeltelijk digitaal uitgevoerd. Wanneer er problemen zijn met de authenticatievoorziening, heeft dat meteen impact op de dienstverlening, waar zowel de medewerkers als de burger de nadelen van ondervinden. Een ongestoorde werking, ondersteund door een goed geregeld beheerproces inclusief releaseplanning en besluitvormingsprocedures zijn nodig om dat te bereiken.

Duidelijkheid, eenvoud en voorspelbaarheid kunnen in principe makkelijker eenvoudiger bereikt worden met één routeringsvoorziening dan met meerdere verschillende aanbieders van authenticatievoorzieningen. Voor het slagen van eID is het van veel belang dat de routeringsvoorziening als regie organisatie een dergelijk goed georganiseerd beheerproces biedt.

Aansluiten op de routeringsvoorziening en moderniseren van het koppelvlak.

De initiële aansluiting op de routeringsvoorziening is voor gemeenten erg eenvoudig. Het betekent dat de bestaande DigiD aansluitingen omgezet moeten worden naar aansluitingen op de routeringsvoorziening. Dat is technisch een eenvoudige operatie waarvan de kosten verwaarloosbaar zijn. Over de kosten van modernisering van het koppelvlak kunnen pas uitspraken gedaan worden wanneer duidelijk is wat de wijzigingen precies inhouden en wanneer de eisen van de releaseplanning en implementatie bekend zijn. Geen van de gesprekspartners waagt zich aan een uitspraak over de orde van grootte. Daarbij geeft men aan dat veel belangrijker is welk gebruik van de aansluiting een gemeente dan al maakt en voor de toekomst voorziet. De aansluitkosten betreffen een relatief gering bedrag dat in de afweging om een aansluiting te nemen minder zwaar weegt. Ook het technisch in stand houden van de aansluiting is geen grote kostenpost. Sommige gemeenten doen dit zelf, de meeste gemeenten besteden dit uit aan een van de grote leveranciers.

Gemeenten hebben vaak voor verschillende domeinen verschillende aansluitingen, denk bijvoorbeeld aan burgerzaken, belastingen en het sociaal domein. Het gemiddelde aantal actieve aansluitingen op DigiD ligt iets lager met 1,6 aansluitingen per gemeente⁷⁶. Sommige van deze aansluitingen zijn bij de gemeente zelf in beheer, andere zijn in beheer van een softwareleverancier. Er is een klein aantal grote leveranciers die voor veel gemeenten in aansluitingen voorzien. Omdat gemeenten regelmatig via dezelfde leverancier werken zal er, mochten zij massaal en ongeveer tegelijkertijd over willen gaan op de routeringsvoorziening, enige doorlooptijd worden gerekend. Of deze doorlooptijd beperkt kan blijven tot een aantal maanden is nog niet te zeggen omdat dit te sterk afhankelijk is van de omstandigheden en de leverancier.

⁷⁶ In totaal zijn er 1.013 gemeentelijke aansluitingen waarvan 589 actief. Landelijke diensten en gemeente-overstijgende samenwerkingsverbanden zijn hier niet in meegerekend

De jaarlijkse technische kosten voor de aansluiting zijn moeilijk vast te stellen omdat er pakketdiensten worden aangeboden door leveranciers (meerdere producten en diensten worden tegelijk afgenomen voor een all-in prijs). De auditkosten zijn de meest aanzienlijke jaarlijkse kosten (zie toelichting hieronder), het technisch mogelijk maken van de aansluiting kost jaarlijks een paar honderd tot een paar duizend euro per aansluiting (verschilt sterk per type aansluiting).

Voldoen aan audit verplichtingen

Elke overheidsorganisatie die DigiD gebruikt moet voldoen aan een beveiligingsnorm (zie brief minister Spies aan TK d.d. 2 februari 2012). Jaarlijks wordt getoetst of de organisatie de ICT-beveiliging op orde heeft middels een ICT-beveiligingsassessment. Hiervoor moeten zij een toetsing (kort gezegd een IT-audit) uitvoeren, in 2017 voor het eerst als onderdeel van de ENSIA normatiek⁷⁷. De kosten van de uitvoering van deze verplichte jaarlijkse audit verschillen. Wanneer een gemeente meerdere aansluitingen heeft, moeten er meerdere IT-audits worden uitgevoerd. In het geval van een groepsaansluiting zijn de auditkosten hoger, maar doordat deze kunnen worden verdeeld over de aangesloten gemeenten zijn de kosten per gemeente uiteindelijk juist lager. Er kan namelijk één audit over de gehele groepsaansluiting worden uitgevoerd. De audit wordt door gemeenten en leveranciers als een groot obstakel beschouwd omdat de kosten aanzienlijk zijn. Logius wil op dit moment de zekerheid hebben dat de websites aan de beveiligingsnormen voldoen, vastgesteld door een onafhankelijke deskundige. De kosten voor de huidige audit zijn dus al aanzienlijk, de verwachting is niet dat deze lasten verder zullen stijgen onder het huidige voorstel. Geïnterviewde gemeenten en leveranciers zouden echter graag zien dat de processen anders worden ingericht zodat de auditlasten omlaag kunnen.

DigiD had de afgelopen tijd een zeer stabiel koppelvlak waardoor de kosten overzichtelijk bleven. Het is voor de leveranciers nog onduidelijk of de routeringsvoorziening daarom direct te vergelijken valt met de huidige situatie. Wanneer een wijziging in het koppelvlak moet worden doorgevoerd, zal de leverancier dit doorvoeren richting de gemeente, die dat intern vormgeeft. Een grotere gemeente gaf bijvoorbeeld aan dat een kleine versiewijziging van eHerkenning die drie dagen tijd in beslag nam, wel een maand of drie doorlooptijd opleverde, waardoor de kosten opliepen tot zo'n € 25.000. Een grote organisatie moet de wijzigingen in veel verschillende gremia bespreken en overall doorvoeren, en dat neemt in de praktijk veel tijd in beslag, dat automatisch extra kosten meebrengt. Voor een kleine gemeente zullen de kosten van deze zelfde wijziging uiteindelijk een stuk lager uitkomen. Er zal per wijziging een aparte business case nodig zijn om iets te kunnen zeggen over de kosten van de wijziging. De verschillen tussen koppelvlakwijzigingen zijn dus erg groot qua impact op de organisatie. Uit de interviews blijkt echter dat de kosten voor de wijzigingen van het koppelvlak niet als een groot obstakel door gemeenten en leveranciers worden gezien. Wanneer het koppelvlak stabiel blijft, met een beperkt aantal wijzigingen, zullen de beheerlasten vergelijkbaar zijn met de huidige beheerlasten.

Gebruik van de aansluiting

Gemeenten hebben authenticatievoorzieningen nodig om digitale dienstverlening - waarvoor de identiteit van de betreffende burger bekend moet zijn - mogelijk te maken. Of een gemeente een dienstverlening digitaal maakt is in de eerste plaats een kosten-batenafweging bij de betreffende dienst, of een politieke afweging. Hoe groter het aantal diensten dat gebruik maakt van eID, hoe groter de impact die wijzigingen in de aansluiting op eID op een gemeente hebben. Die is dan altijd gekoppeld aan concrete dienstverlening met een positieve balans tussen kosten en baten en in zo'n kader zijn dergelijke kosten geen probleem. Een wettelijke verplichting om aan te sluiten op eID zal maar beperkt effect sorteren. Alleen wanneer de verplichting gehandhaafd wordt en gemeenten die niet aan hun verplichtingen voldoen een sanctie krijgen is een wettelijke verplichting effectief: een voorbeeld is de berichtendienst CORV waar gemeenten in het kader van de decentralisatie van de Jeugdzorg op moesten aansluiten. Door enkel nog CORV te accepteren

⁷⁷ ENSIA staat voor 'Eenduidige Normatiek Single Information Audit'.

werden gemeenten gedwongen om over te stappen. De gemeenten die geïnterviewd zijn maken deel uit van het Kennisnetwerk eID en een aantal noemden als voorbeeld de verplichting om tijdig aan te sluiten op een eTD-makelaar vanwege de, op grond van Europese regelgeving verplichte, ontsluiting van eIDAS. Men verwacht nauwelijks enig gebruik van de aansluiting en bereidt zich er (op één uitzondering na) niet op voor om aan de verplichting te gaan voldoen.

Aansluiten op eTD-makelaar.

Dienstaanbieders moeten niet alleen aansluiten op het eID-stelsel, maar moeten vanaf 29 september 2018 ook voldoen aan de eisen van de eIDAS-verordening. De eIDAS-verordening geeft aan dat een organisatie Europese burgers en bedrijven met een Europees erkend inlogmiddel toegang dient te verlenen als de organisatie ook Nederlandse burgers en bedrijven op betrouwbaarheidsniveau Substantieel of Hoog accepteert.⁷⁸ Dienstaanbieders die diensten met DigiD Basis of DigiD Midden aanbieden, accepteren ook automatisch DigiD Substantieel en DigiD Hoog. Dat betekent dat alle Nederlandse dienstverleners die DigiD gebruiken vanaf 29 september 2018 ook genotificeerde Europese eID-middelen moeten accepteren. Op 29 september is aansluiten op een eTD-makelaar de enige mogelijkheid om aan de verplichting te voldoen. Bij drie van de zes erkende leveranciers die als eTD-makelaar gaan optreden is nagegaan wat de aansluitkosten voor dienstverleners zullen zijn. Tevens is de ervaring meegenomen die in de zorg met het uitvoeren van pilots is opgedaan.

Kosten aansluiting

De kosten die hier gepresenteerd worden hebben betrekking op een 'kale' eTD aansluiting ten behoeve van het voldoen aan de eIDAS verplichting. Wanneer de aansluiting onderdeel is van een pakket waar meerdere diensten deel van uitmaken worden de kosten niet altijd geheel in rekening gebracht en zijn ze niet apart zichtbaar. Om aan te kunnen sluiten moeten de dienstverleners gemigreerd zijn naar e-Herkenning 1.11. De kosten daarvan zijn niet apart in beeld gebracht. Alle drie de leveranciers brengen eenmalig aansluitkosten in rekening, die variëren van €500,- tot €5000,-. De ondersteuning die geleverd wordt bij een aansluiting verschilt. De laagste prijs heeft betrekking op een 'kale' aansluiting met beperkte ondersteuning. Voor het gebruik wordt een bedrag in rekening gebracht dat afhankelijk is van het aantal transacties. De staffels die de leveranciers hanteren verschillen. Het laagste maandbedrag op basis van minder dan 1.000 transacties per maand bedraagt €125,-. Bij een maximum van 50.000 transacties per maand variëren de prijzen tussen €250,- en €1250,-, per maand. Bij grotere aantallen daalt de prijs per tik.

Kosten aanpassingen dienstverlener

Om aan te sluiten moet de dienstverlener een eigen koppelveld inrichten en aanpassingen doen in haar eigen applicatielandschap, voor zover er digitale dienstverlening in het burgerdomein mee wordt verricht. Het koppelveld van de eTD-makelaar is bekend voor dienstverleners die al gebruik maken van e-Herkenning of die deelgenomen hebben aan een Idensys pilot. De bedragen die nodig zijn variëren sterk met de omvang en samenstelling van dat applicatielandschap en met de kennis die in de organisatie aanwezig is. De ervaringen verschillen sterk.

- In de zorg is een pilot met Idensys uitgevoerd. In deze situatie, waarin een eTD-aansluiting en het uitrollen van authenticatiemiddelen aan de orde was, variëren de daadwerkelijk gemaakte kosten inclusief de kosten van de interne medewerkers tussen €35.000,- en €60.000,-⁷⁹.
- In grote organisaties met een ingewikkeld applicatie landschap en onvoldoende kennis van de gebruikte protocollen komen lange doorlooptijden (meer dan een half jaar) en zeer hoge bedragen voor externe ondersteuning (meer dan €100.000,-) voor.

⁷⁸ Zie <https://www.eherkenning.nl/vraag-antwoord/eidas/>.

⁷⁹ Zie "Het nieuwe eID-stelsel; een introductie voor de zorgsector". Nictiz 2017.

- Sommigen van de onderzochte leveranciers bieden ondersteuning in de vorm van consultancy of een adapter die ingezet kan worden (adapter kost minder dan €1000,-).
- Er zijn gespecialiseerde bedrijven die dienstverleners kunnen ondersteunen, diverse voorbeelden dat zij de aansluiting werkend krijgen voor een bedrag van € 5000,- tot € 15.000,-.

Strijdige uitgangspunten eTD en Routeringsdienst

Er lijkt strijdigheid te zijn tussen de uitgangspunten van de Routeringsdienst en het aansluiten op de eTD-makelaar. Dienstaanbieders ontvangen vanaf 29 september een bericht met daarin een polymorf pseudoniem. De dienstaanbieder moet het PP zelf ontsleutelen en omzetten in een BSN. Daarna wordt de eerste versie van de Routeringsdienst geïmplementeerd, die een bericht met een BSN oplevert. Strikt genomen horen de kosten voor het ontsleutelen van polymorfe pseudoniemen daarmee tot de aansluitkosten op een eTD-makelaar. De leveranciers die wij spraken kennen de exacte specificaties van het koppelvlak met PP nog niet en doen daarom geen uitspraken over de hoogte van de kosten. De kans dat dienstaanbieders op grote schaal gaan investeren in het ontsleutelen van berichten met PP is, gezien de fase waarin de voorbereiding zich bevindt en de korte beschikbare doorlooptijd, zeer klein.

Geen BSN bekend

Een PP kan alleen geleverd worden wanneer er van de Europese burger een BSN bekend is. Wanneer er geen BSN bekend is kan de dienstaanbieder een bericht laten tonen (via een 'landingspagina') dat de EU-ingezetene geen gebruik van de betreffende dienst kan maken, waarna de authenticatie stopt. De dienstaanbieder kan er ook voor kiezen een setje identificerende gegevens te ontvangen en de dienst wel te leveren. De kosten die daarvoor gemaakt moeten worden beschouwen we als kosten van het 'huis' die verder buiten beschouwing kunnen blijven.

Conclusies

Door de routeringsvoorziening zullen de processen bij de gemeenten nauwelijks veranderen. Kwalitatief is de routeringsvoorziening wel degelijk van belang: die heeft de potentie om duidelijkheid, voorspelbaarheid, eenvoud en zekerheid te bieden. Initiële aansluiting is een technisch eenvoudige operatie waarvan de kosten verwaarloosbaar zijn. Het is zeker dat het koppelvlak met de routeringsdienst gemoderniseerd zal worden, maar over de kosten daarvan kunnen pas uitspraken gedaan worden wanneer er meer bekend is over de specificaties.

Authenticatiemiddelen op substantieel en hoog niveau bieden gemeenten nieuwe mogelijkheden om processen die hogere betrouwbaarheidsniveaus nodig hebben te digitaliseren. Dat zal een geleidelijk proces zijn waarbij gemeenten per geval een kosten – baten afweging zullen maken. De kosten van een aansluiting op eID zijn in dat geheel een relatief kleine factor, waarbij de kosten van de auditvoorschriften worden ervaren als (soms nodeloos) hoog.

Bijlage 2 Uitwerking use cases

Het eID-stelsel kan gezien worden als 'het fundament'; een stuk infrastructuur nodig voor het realiseren van digitale dienstverlening (zie uitleg in paragraaf 1.3). De baten van de te realiseren digitale dienstverlening maken bewust géén onderdeel uit van de businesscase. Immers, om deze baten te realiseren zullen partijen zelf moeten investeren in het digitaliseren van processen aangesloten op het eID-stelsel. Het eID-stelsel is een randvoorwaarde om diensten met een hoger betrouwbaarheidsniveau digitaal aan te kunnen gaan bieden.

Er is echter wel behoefte aan meer duidelijkheid rond de (maatschappelijke-) baten die kunnen worden gerealiseerd door digitale dienstverlening. Om hieraan tegemoet te komen is er gekozen om de baten te illustreren aan de hand van 'use cases'. De 'use cases' zijn de 'huizen' die gebouwd kunnen worden op het 'fundament'.

In deze bijlage beschrijven we een aantal 'use cases' in de grote (semi)publieke sectoren binnen het BSN-domein met significante potentie voor verdere digitalisatie van dienstverlening op hoger betrouwbaarheidsniveau; zorg en gemeenten. Er wordt de volgende indeling gehanteerd:

1. Het gebruik van use cases ter illustratie van het belang van het eID-stelsel
2. Use cases in het gemeentedomein
3. Use cases in het zorgdomein

Use cases ter illustratie

In de use cases kijken we naar (individuele) 'huizen' op het 'fundament'. Hierbij moet worden opgemerkt dat (i) dit geen totaalbeeld geeft van de maatschappelijke baten van het eID-stelsel (we kijken naar een paar huizen) én (ii) dat de baten niet direct kunnen worden toegeschreven aan het eID-stelsel. Dienstaanbieders of derden investeren om de huizen te bouwen en zonder eID-stelsel zouden de huizen wellicht ook (deels) met een alternatieve infrastructuur gerealiseerd kunnen worden.

Wat de use cases wél illustreren is het belang van het faciliteren van digitale dienstverlening en de brede scope aan toepassingen (huizen) die in de toekomst op het fundament kunnen worden gebouwd.

Bij de use cases wordt gekeken naar:

- De kosten voor het digitaliseren van de betreffende processen voor de dienstaanbieder
- De baten voor de dienstaanbieder
- De maatschappelijke baten voor de burger

Om een selectie te maken van de use cases is geïnformeerd bij verschillende partijen (VNG, VNG Realisatie, NVVB, VDB en VWS) naar aansprekende voorbeelden van toepassingen:

- Waar draagvlak in het veld voor bestaat
- Die actueel en concreet zijn
- Die bij voorkeur zonder aanpassingen van de wet mogelijk zijn
- Die mogelijk worden gemaakt door eID op minimaal substantieel niveau

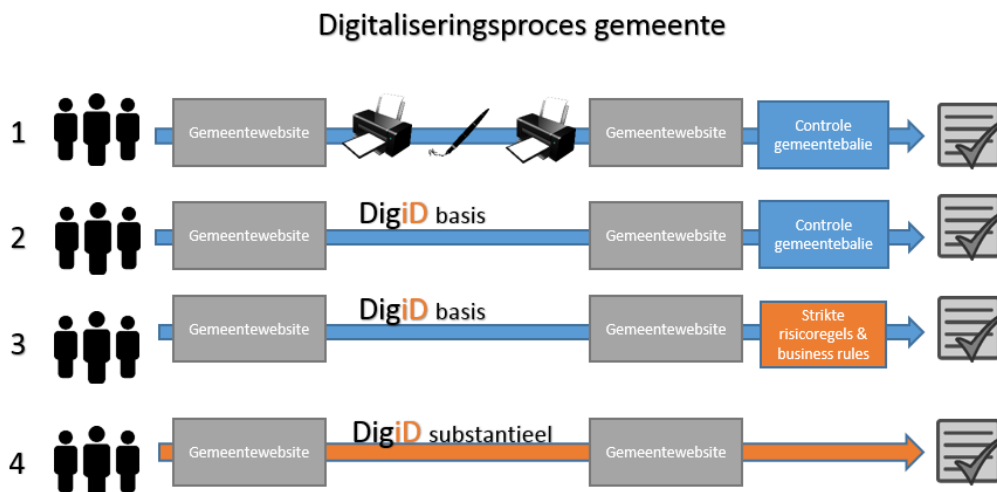
Use cases in het gemeentedomein

De verwachting binnen het gemeentedomein is dat de ontwikkeling van concrete toepassingen van digitaal geleverde diensten voor burgers op veiligheidsniveau substantieel en hoog, en dus ook de baten die de gemeenten hiervan zullen ondervinden, niet grootschalig of op korte termijn zullen worden ingezet. Wel worden proeven en pilots uitgevoerd en selectief diensten aangeboden op niveau substantieel. De omschreven use cases zijn dan ook op basis van een middel op niveau substantieel. We kunnen twee type diensten op niveau substantieel onderscheiden: Nieuwe diensten op het gebied van burgerzaken en bestaande digitale diensten waarvan het veiligheidsniveau moet worden opgekrikt. DigiD Hoog heeft nog geen concrete use cases op korte termijn in het gemeente domein, al wordt er op langere termijn wel gedacht aan toepassingen voor aanvragen in de sfeer van jeugdzorg en WMO.

Op basis van interviews met een vijftal gemeenten⁸⁰ lijkt DigiD Hoog in de toekomst met name geschikt te zijn voor processen waarbij gegevens direct worden aangepast in registratiesystemen, bij het digitaal aanvragen van identiteitsdocumenten, binnen het sociaal domein en WMO en in het stemproces. Hiermee wordt het gezien als iets wat zeer nuttig kan worden in de toekomst, maar waar op korte/midden lange termijn geen concrete toepassing voor in de wacht staat.⁸¹ Geen van de gesproken gemeente kon een indicatie geven van de doorlooptijd na het doorvoeren van de genoemde toekomstige mogelijkheden.

Digitalisering van dienstverlening

Het huidige proces van digitalisering van het dienstenaanbod van gemeenten ontwikkelt zich **gradueel**. Het niveau van digitalisering verschilt per dienst en per gemeente. Over het algemeen is er sprake van een trend onder gemeente om steeds meer papieren processen te digitaliseren. De kwartaalcijfers van de gemeente Montferland laten daarnaast bijvoorbeeld zien dat het gebruik onder burgers meegroeit met het aantal aangeboden diensten. Tussen 2013 en 2017 steeg het aantal digitale aanvragen van 613 naar meer dan 10.000⁸². Op basis van de gevoerde gesprekken met gemeenten onderscheiden wij drie stappen in het huidige digitaliseringsproces en een vierde stap op basis van DigiD Substantieel/Hoog.



⁸⁰ De geïnterviewde gemeenten zijn Den Haag, Eindhoven, Rotterdam, Montferland en Groningen.

⁸¹ Bevraging Logius bij gemeenten Montferland, Drechtsteden, Tilburg, Rotterdam en Den Haag

⁸² Gebaseerd op een voorlopige prognose in de 'Kwartaalmonitor dienstverlening derde kwartaal 2017' van Montferland.

1. Burgers kunnen digitaal documenten opleveren door deze te printen van de gemeentewebsite, te ondertekenen, in te scannen en op te sturen. Het balieproces blijft hierbij ongewijzigd.
2. Bepaalde diensten kunnen digitaal worden aangevraagd en ondertekend. Dit is alleen mogelijk voor die diensten die een laag veiligheidsniveau vereisen. Het balieproces blijft hierbij ongewijzigd.
3. Diensten kunnen digitaal worden geregeld, zonder dat gegevens gecontroleerd hoeven te worden aan de hand van het reguliere balieproces. **Zonder het gebruik van veiligheidsniveau substantieel/hoog** is het echter van belang dat er strikte risicoprofielen en business rules van kracht zijn om fraude tegen te gaan.
4. Met DigiD Substantieel en hoog kunnen diensten die een hoger veiligheidsniveau vereisen digitaal worden geregeld zonder controle aan de balie. Incidentele risicocontroles zijn hierbij nog steeds van belang, maar hoeven door de toegenomen controle aan de poort veel minder vaak uitgevoerd te worden.

Minder contact aan de balie en gebruikersgemak voor de burger zijn de belangrijkste meerwaarde van uitbreiding van de digitale dienstverlening. Gemeenten zijn het unaniem eens over het belang van het ontlasten van de gemeentebalies. Een gemeente geeft aan ongeveer € 100 per uur te besparen per balie die zij kan sluiten. Doordat nu 80 procent van de inzet van de gemeente nodig is voor 20% van de individuele gevallen, vragen de gemeenten zich wel af hoeveel balie-ontlasting verdere digitalisering precies kan bewerkstelligen. Naast het verlagen van de uitvoeringskosten van de gemeente, kan digitalisering in combinatie met een hoger veiligheidsniveau ook de burger ontlasten door minder bezoeken aan het gemeentehuis en een verminderde bewijslast. De mogelijkheid van digitale processen aanbieden op een hoger niveau zou hier op de lange termijn een positieve bijdrage aan kunnen leveren.

Het maximaal digitaliseren van dienstverlening wordt desondanks niet altijd als positief ervaren. De meerwaarde van persoonlijk contact wordt door gemeente erkend en gezien als een essentieel onderdeel van het serviceaanbod voor de burger. Digitalisering zal dus slechts gedeeltelijk de baliemedewerker vervangen. In dit kader wordt ook de politieke druk op het aanbieden van goede service aan de balie ervaren door de gemeenten. Een gemeente houdt er bijvoorbeeld rekening mee dat de verkiezingsuitslag van de komende gemeenteraadsverkiezingen grote invloed kan hebben op de visie over de bezetting van de balies. Het verminderen van het aantal contactmomenten van twee naar een bij bijvoorbeeld de uitgifte van een nieuw rijbewijs, zou desalniettemin al tot grote lastenverlichting leiden.

Use Case: Geboorteaangifte

De gemeente Groningen geeft via hun digitale I-burgerplatform de mogelijkheid om online aangifte van geboorte te doen. Bij grootschalig gebruik zou deze service de huidige mobiele gemeenteloketten in ziekenhuizen overbodig kunnen maken. De bereidheid onder burgers om van deze dienst gebruik te maken wordt onderschreven door een substantieel aantal aangiften op de eerste dag dat de service werd aangeboden, zelfs nog voordat de mogelijkheid om online aangifte toe doen door de gemeente op grote schaal was gecommuniceerd. Waar de gemeente Eindhoven digitale geboorteaangifte ook zou willen onderzoeken, ziet de gemeente Den Haag minder voordelen van de digitale geboorteaangifte in verband met het ceremoniële en incidentele karakter van geboorteaangifte. Momenteel is digitale geboorteaangifte buiten specifieke pilots om nog niet mogelijk. De 'Wet elektronische dienstverlening burgerlijke' stand sluit deze mogelijkheid echter niet uit.⁸³ Gebaseerd op de pilots digitale geboorteaangifte in 2017 zal hierover een definitieve beslissing worden genomen.

⁸³ Zie <https://zoek.officielebekendmakingen.nl/stb-2014-380.html>, wijziging artikel 19^e, 1^{ste} lid.

Gemeenten zien kansen in het aanbieden van digitale diensten op niveau substantieel, maar willen wachten tot het middel op grote schaal gebruik wordt. Veel van de voorgestelde diensten op niveau hoog en substantieel betreffen eenmalige administratieve handelingen, zoals het aanvragen van een verhuizing of geboorteaangifte. In tegenstelling tot de voorgestelde diensten voor chronisch zieken in de zorg (zie *trombosedienst in hoofdstuk 3.2*), zorgt het meestal incidentele karakter van contact met de gemeente voor een hogere barrière in de overgang naar het nieuwe middel. Dit creëert een 'kip-en-ei-probleem': Meer digitale diensten op hoog/substantieel niveau zijn nodig om mensen te overtuigen de overgang naar het nieuwe middel te maken, maar gemeenten willen deze diensten pas aan gaan bieden wanneer er genoeg gebruikers zijn, en de burgers er daadwerkelijk naar vragen. De gemeenten noemen het enthousiasmeren van de burger of wettelijke verplichting van het aanbieden van digitale diensten als oplossingen voor dit probleem. Hierbij moet in ogenschouw worden genomen dat de mogelijkheid om aan de balie of telefoon zaken af te handelen niet zal verdwijnen.

Wettelijke barrières verhinderen in sommige gevallen de mogelijkheid voor gemeenten om services digitaal aan te bieden. Verschillende gemeenten geven aan dat voor sommige diensten nog steeds een natte handtekening is vereist. De Wet Elektronische Handtekening (21 mei 2003) schrijft echter voor dat elektronische handtekeningen, mits gekwalificeerd, dezelfde rechtsgevolgen heeft als een handgeschreven handtekening.⁸⁴ Dit betekent echter niet automatisch dat alle diensten in al digitaal geleverd kunnen worden. Voorbeelden van diensten die op basis van huidige regelgeving (nog) niet digitaal geregeld kunnen worden: erkenning na geboorte, erkenning ongeboren vrucht, geregistreerd partnerschap omzetten in huwelijk, geslachtswijziging, inschrijving BRP, stemmen bij volmacht, aanvragen reisdocumenten en rijbewijzen. Hoewel ook digitaal stemmen door sommige gemeenten wordt geambieerd, wordt ook erkend dat hier nog veel veiligheidsproblemen, praktische moeilijkheden (controle dubbel stemmen, hoe om te gaan met groepen die fysiek willen blijven stemmen) en een gebrek aan draagkracht voor bestaan.

Gemeenten verwachten voorlopig nog geen groot aanbod van digitale diensten in de WMO en het sociaal domein. Sociale dienstverlening, sinds 1 januari 2015 ondergebracht bij de gemeente, maakt vaak gebruik van speciale persoonsgegevens en moet in die gevallen dus gebruik gaan maken van DigiD Hoog. Hoewel gemeenten wel degelijk de voordelen zien in termen van een verlaagde kans op fraude en verminderde uitvoeringskosten, geven de gesproken partijen aan hier nog niet mee bezig te zijn. Dit betekent dat zaken binnen het sociaal domein die momenteel en in de nabije toekomst digitaal geregeld worden eigenlijk gebruik maken van een te laag veiligheidsniveau. De Wet digitale overheid schrijft voor dat een dergelijke overgangsmaatregel maximaal vier jaar van kracht mag zijn. In het geval van DigiD Hoog zal het gedurende zeven jaar mogelijk blijven om met DigiD Substantieel in te loggen. De eerste stap is om deze relatief nieuwe gemeentelijke verantwoordelijkheid goed in het huidige serviceaanbod te integreren.

Gemeenten verwachten in de nabije toekomst geen sterk toenemende vraag naar digitale diensten vanuit het buitenland. De Europese verplichting om vanaf 29 september 2018 alle dienstverlening op niveau substantieel ook via de eIDAS voorziening aan andere Europese burgers te bieden heeft volgens hen nog weinig directe consequenties. Enkele gemeenten gaan pas serieus kijken naar de mogelijkheden wanneer meer landen hun middel bij de Europese Commissie hebben genotificeerd. Wel zien de gemeenten met een grote studenten- en/of expatpopulatie mogelijkheden om inschrijving en registratie van verhuizing in de toekomst digitaal te regelen. Op dit moment is dat ook al mogelijk, maar alleen wanneer de student of expat over een BSN beschikt. Daarnaast zouden bovengenoemde mogelijkheden alleen van toepassing zijn op Europese burgers.

⁸⁴ De definitie van de elektronische handtekening staat in art. 15a boek 3 BW. Onder elektronische handtekening wordt een handtekening verstaan die bestaat uit elektronische gegevens die zijn vastgehecht aan of logisch geassocieerd zijn met andere elektronische gegevens en die worden gebruikt als middel voor authenticatie.

Use Case: Internationale studenten en expats

De gemeenten Groningen, Rotterdam, Eindhoven en Den Haag kennen allen een grote studenten- en expat community. In Groningen is bijvoorbeeld ruim een vierde van de totale populatie (50.000) student. De studentenpopulatie wordt steeds internationaler. Tussen 2011 en 2016 groeide het aantal internationale studenten aan de Rijks Universiteit Groningen (RUG) van 2750 (2011) naar 4983 (2016) studenten. De concentratie van aanmeldingen aan het begin van het zomer- en wintersemester leidt tot grote administratieve druk bij de gemeenten. Groningen zet bijvoorbeeld speciale teams in gedurende deze twee drukke periodes. De mogelijkheid voor internationale studenten om zich digitaal te registreren en hun adres te wijzigen zou een derhalve tot grote lastenverlichting leiden.

De gemeente Rotterdam benadrukt dat alleen Duitsland eIDAS middelen heeft genotificeerd bij de Europese Commissie. De gemeente Den Haag wijst op de mogelijkheid voor elke Europese burger om in Estland een Europees breed geaccepteerde e-Residency aan te vragen, maar geeft tegelijkertijd aan dat het nog niet afgeronde notificatieproces via de EU en de noodzaak voor aanvraag bij een Estse ambassade deze optie vooralsnog minder realistisch maakt.

Overzicht use cases gemeenten

De volgende tabel geeft een overzicht van het dienstenaanbod waarvan (een deel van) de vijf gemeenten aangeven dat digitalisering in de toekomst een positief effect op kosten, veiligheid en/of gebruikersgemak zou kunnen hebben. De vroege fase waarin deze digitalisering zich bevindt maakt het niet mogelijk om meer precieze uitspraken te doen over de orde van grootte van het totale positieve effect. De tabel is samengesteld op basis van de gevoerde gesprekken en laat zien dat er grote verschillen bestaan tussen de visies van de gemeenten.

Use cases	Voorstel gemeente	Voordelen	Nadelen	Niveau
Opgeven vermiste documenten (ID-kaart, paspoort, rijbewijs)	Eindhoven	Verhoging veiligheidsniveau (naar substantieel)	Drempelverhogend, leidt tot meer baliebezoek (Den Haag)	Substantieel
			Kan bij de balie meteen gecombineerd worden met nieuwe aanvraag (burger moet dus toch gaan)	
Aanvragen rijbewijs	Eindhoven (Pilot)/ Den Haag	Ontlasting aan de balie (van 2 naar 1 contact moment)	Eens in de 10 jaar nodig dus geen aanleiding voor de burger	Substantieel
Geboorteaangifte	Rotterdam/ Eindhoven/ Montferland	Ontlasting aan de balie (gelimiteerd door symbolische waarde van 'fysieke aangifte')		Hoog
MijnAppEindhoven	Eindhoven	Koppelen van andere diensten, die voor de burger handig zijn zoals vuil afhalen. Deze extra services kunnen een positieve impuls aan de burger geven	Onderontwikkeld, valt nog niks over te zeggen in dit stadium	Substantieel
Expats (eIDAS)	Den Haag/ Rotterdam	Aansprekende use case voor expat gemeente.	Middelen zijn, met uitzondering van het Duitse middel, nog niet gecertificeerd op Europees niveau.	Substantieel

Use cases	Voorstel gemeente	Voordelen	Nadelen	Niveau
		Huidige systeem erg omslachtig, leidt tot niet registreren en kan pas bij aankomst in Nederland worden geregeld.	Expats van buiten de EU hebben niets aan eIDAS. Voor registratie verhuizing is nu nog een BSN-nummer nodig (Eindhoven).	
Machtigen	Den Haag	Digitaal meer opties, makkelijker aanbieden van bijvoorbeeld taak-specifiek machtigen		Substantieel/ hoog
WMO/jeugdzorg	Montferland	Liggen mogelijkheden in de toekomst, zeker op het gebied van keukentafelgesprekken.	Gemeente nog maar net aan het wennen met aanbieden van deze diensten. Verlies persoonlijk contact bij onder andere keukentafelgesprekken.	Hoog
Gehandicapten parkeerplek	Montferland	Hogere authenticatie is nodig in verband met specifieke rechten	Bepaalde doelgroep en gebruik.	Substantieel
Digitaal stemmen	Groningen	Grote ontlasting van de gemeente, voornamelijk door het wegnemen intensieve werkzaamheden in korte tijd.	Probleem bij gedeeltelijke penetratie van DigiD Hoog in de maatschappij. Veiligheidsrisico's.	Hoog
Direct muteren basisregistraties	Den Haag/ Montferland	Minder arbeidsintensief door het overbodig maken van het huidige 4-ogenprincipe Voordeel voor zowel de burger als de gemeente door directe doorwerking	Moeilijk meetbaar en implementatie vereist goede risicoprofielen en daarbij passende nieuwe processen.	Substantieel

Uit gesprekken met de gemeenten Den Haag, Eindhoven, Groningen, Montferland en Rotterdam blijkt dat er een breed gedragen wens is om de digitale dienstverlening voor de burger verder uit te breiden. Ideeën over de nieuwe diensten op basis van eID middelen op substantieel en hoog betrouwbaarheidsniveau bevinden zich echter nog in een erg vroeg stadium. De genoemde baten concentreren zich op verminderd baliebezoek, tijdswinst en gebruikersgemak voor de burger. Wel moet in ogenschouw worden genomen dat het in sommige gevallen wenselijk is om het persoonlijk contact met de gemeente in stand te houden. Met een aantal use cases zijn recent pilots uitgevoerd.⁸⁵ De gemeenten geven aan dat potentiële baten alleen gerealiseerd kunnen worden bij voldoende opname van het nieuwe middel onder de bevolking. Op dit moment bestaat hier nog onzekerheid over bij de gemeenten, wat vaak leidt tot een afwachtende houding.

⁸⁵ Dit is een voorbeeld uit het bedrijvendomein (niet het BSN-domein). Voor een indicatie van kosten en baten van het digitaal aanbieden van aangifte overlijden voor ondernemers, zie <https://www.da2020.nl/sites/default/files/2017-10/kosten-en%20batenoverzicht%20DAO.pdf>

Use cases in het zorgdomein

In het zorgdomein worden proactief concrete toepassingen ontwikkeld. Hierbij wordt gekeken naar de 'waarde achter de deur' voor patiënten en de 'zwaarte van het slot'. Hierbij is de aanname dat, pas als de waarde voor de gebruiker hoog genoeg is, deze gebruik zal gaan maken van een middel op niveau hoog.

In de volgende paragrafen gaan we nader in op:

1. De digitalisering van dienstverlening binnen het zorgdomein
2. Use case 'Medmij'
3. Use case 'zelfmanagement chronisch zieken'

Digitalisering van dienstverlening

In het zorgdomein worden uiteenlopende toepassingen ontwikkeld. Aanbieders en patiënten zijn met verschillende pilots digitale dienstverlening aan de gang. Denk hierbij ook aan programma's voor portaal diensten om digitaal afspraken te kunnen maken en digitaal vragenlijsten te kunnen invullen en applicaties voor specifieke patiëntgroepen. In de zorg moet rekening gehouden worden met remmende effecten die een belangrijke rol spelen in het wel of niet slagen van het digitaliseren van dienstverlening.

Persoonlijk contact is waardevol

Als dienstaanbieders een digitale dienst aanbieden, dan is dit vaak als een aanvulling op de bestaande dienstverlening en niet als vervanging van het bestaande proces. Persoonlijke dienstverlening en contact wordt gezien als een indicator van kwalitatief hoge zorgverlening. Hierdoor is er een natuurlijke barrière om (grootschalig) over te stappen naar digitale dienstverlening. Naar verwachting gebeurt dit pas wanneer de overgrote meerderheid van de patiënten de voorkeur geeft aan de digitale dienst. Dan zal het aantal persoonlijke contact momenten worden teruggebracht, al zal er altijd een zeker mate van persoonlijk contact gewenst blijven.

Digitale processen in de zorg moeten grote meerwaarde hebben voor de patiënt door noodzaak 'zwaar slot'

Naast de waarde van persoonlijk contact is een tweede overweging het identificatieproces zelf. Doordat diensten in de zorg veelal beveiligingsniveau hoog vereisen is er een groter risico dat het 'complexere' inloggen een barrière is dan wanneer er volstaan kan worden met inloggen op niveau laag of substantieel. Voor patiënten waarbij de digitale dienstverlening weinig meerwaarde heeft vergeleken met de huidige dienstverlening werkt zo'n 'zwaar slot' vertragend. Ook het activeren van het middel wordt als knelpunt ervaren in pilots. Dit wordt waargenomen in het eHealth domein; vaak wordt er maar weinig gebruik gemaakt van de aangeboden diensten.

Zorgpartijen hechten dan ook grote waarde aan een middel op niveau hoog met een zo groot mogelijk gebruiksgemak. Hierbij wordt gedacht aan bijvoorbeeld vingerafdrukken of gezichtsherkenning via de mobiele telefoon in plaats van het gebruik van NFC op telefoon of kaartlezer. Achterliggende gedachte is dat de patiënt dan 'slechts' zijn mobiele telefoon met de juiste applicatie nodig heeft om in te loggen in plaats van 'telefoon plus pas' in het geval van NFC op de telefoon, of zelfs 'telefoon plus pas plus kaartlezer' wanneer NFC niet via de telefoon plaats kan vinden.

Partijen die toepassingen ontwikkelen zien digitale dienstverlening als een verbetering in plaats van een verplichting voor organisatie en patiënt

Dienstverleners zien baten voor zichzelf en voor hun patiënten. Zo zou het digitaliseren van logistieke processen in bijvoorbeeld een ziekenhuis kunnen zorgen voor een snellere doorlooptijd

per ziekenhuisbezoek en minder 'wacht' momenten. Naast het versimpelen wordt, wanneer men zeker weet met wie je te maken hebt, de kans op fouten kleiner en kunnen de administratieve handelingen (leesuren) omlaag. De patiënt is ook gebaat met een sneller, makkelijker proces en minder fouten. Mensen die regelmatig zorg nodig hebben (chronisch zieken) of zorg voor een ander ondersteunen (ouders en/of (mantel-) zorgers) zullen naar verwachting het eerste op grote schaal gebruik gaan maken van digitale dienstverlening. Vooral als een digitaal proces een terugkerend fysiek bezoek aan de arts of instelling vervangt. Denk hierbij bijvoorbeeld aan het digitaal doorgeven van meetgegevens waar nu al dankbaar gebruik van wordt gemaakt door verschillende patiëntengroepen.

Doorontwikkeling zou ook andere toepassingen mogelijk kunnen maken

Ook het identificeren van de zorgprofessional zelf binnen het eigen systeem en tussen organisaties zou baat kunnen hebben bij een middel op niveau hoog. Hiervoor moet het mogelijk zijn om het attribuut zorgverlener op het middel mee te nemen en het moet toegestaan worden om voor dit type identificatie het BSN te gebruiken. Op het moment van schrijven wordt er gekeken naar deze mogelijkheid binnen de Wet digitale overheid.

Naast het gebruik van portalen om informatie op te halen en uit te wisselen is het gebruik van applicaties in de zorg sterk in opkomst. De huidige eID technologie is echter gericht op portalen en niet op applicaties. Voor toepassingen in de zorg ligt hier een kans.

Use case: Medmij

Het programma Medmij wil het mogelijk maken om persoonlijke gezondheidsgegevens te tonen op één plek. Nu worden gegevens op diverse locaties bewaard. De voorgesteld digitale 'persoonlijke gezondheidsomgeving' zou al deze gegevens bevatten en zo een waardevolle bron van informatie zijn voor de patiënt en (met toestemming van de patiënt) voor zorgaanbieders.

Om deze ontwikkeling mogelijk te maken wil het programma Medmij komen tot een afsprakenstelsel voor het veilig en betrouwbaar uitwisselen van gezondheidsgegevens tussen een persoonlijke gezondheidsomgeving en zorgaanbieders. Het programma gaat dus niet zelf een dergelijke toepassing ontwikkelen. Het programma is faciliterend in het wegnemen van barrières, met name met betrekking tot de gegevensuitwisseling met zorgaanbieders.

Diverse partijen in de zorg en ondersteuning werken samen aan de ontwikkeling van Medmij: brancheorganisaties, verenigingen van huisartsen, ziekenhuizen, apothekers, thuiszorgorganisaties, verpleeghuizen, zorgverzekeraars, patiënten(organisaties) en (lokale) overheden. In expertgroepen wordt samengewerkt met (ICT-) leveranciers en zorgaanbieders die nu al persoonlijke gezondheidsomgevingen maken waarmee mensen (delen van) hun gezondheidsinformatie kunnen inzien. Patiëntenfederatie Nederland coördineert het Medmij-programma en vormt samen met Nictiz en het ministerie van VWS het uitvoerende programmteam.⁸⁶

⁸⁶ Organisatie van het programma Medmij zoals omschreven op de website www.medmij.nl, februari 2018

Hieronder wordt het programma Medmij in meer detail omschreven

Vraagstelling/Doelstelling van Medmij

Iedereen die dat wil kan zijn gezondheidsgegevens uit allerlei bronnen verzamelen en gebruiken.

Context (waarom dit? waarom nu?)

Medmij is opgezet om belemmeringen voor opschaling van persoonlijke gezondheidsomgevingen weg te nemen. MedMij wil gebruik gaan maken van de middelen die onder het programma eID van BZK zullen worden aangeboden. Het beschikbaar zijn van een of meerdere authenticatie/identificatie middelen op voldoende hoog betrouwbaarheidsniveau is een voorwaarde voor het veilig uitwisselen van informatie tussen persoonlijke gezondheidsomgevingen en systemen van zorgaanbieders.

Er zijn twee authenticatie stappen die worden onderscheiden in het gebruik van persoonlijke gezondheidsomgevingen.

1. Zelf inloggen op de persoonlijke gezondheidsomgeving. Het is van belang te vermelden dat hiervoor het gebruik van BSN op het moment van schrijven niet is toegestaan. Het inloggen (inzien/bekijken van de omgeving) gebeurt dan met een andere methode (2-factor authenticatie).
2. Communiceren met zorgverleners. Wil je (nieuwe) gegevens ophalen en/of toevoegen dan is authenticatie en identificatie nodig voor (i) het ophalen van gegevens die onder beheer zijn van zorgaanbieders of (ii) het toevoegen van (meet-) gegevens (door de patiënt) aan het dossier van de zorgaanbieder. Het gaat hierbij in bijna alle gevallen om gezondheidsgegevens. Hiervoor is het gebruik van BSN als identificerend kenmerk verplicht en is betrouwbaarheidsniveau hoog het uitgangspunt. Zolang dit niet beschikbaar is adviseert MedMij voor het gebruik van DigiD Substantieel.

Scope (wat doet Medmij?)

Medmij realiseert samen met zorgpartijen die zitting nemen in het 'Informatieberaad Zorg' (brancheorganisaties, verenigingen van huisartsen, ziekenhuizen, apothekers, thuiszorgorganisaties, verpleeghuizen, zorgverzekeraars, patiënten en (lokale) overheden) een afsprakenstelsel. Hierin staan afspraken over standaarden, beveiliging en privacy zodat gezondheidsgegevens gemakkelijk en veilig kunnen worden ontsloten en uitgewisseld. Het afsprakenstelsel omschrijft een situatie waar de markt naartoe moet gaan groeien zodat marktpartijen persoonlijke gezondheidsomgevingen kunnen bouwen waar zorgpartijen en patiënten mee uit de voeten kunnen.

Beperkingen (wat doet Medmij (nog) niet?)

Er zijn (nog) geen afspraken wie voor welk deel van diensten en voorzieningen betaalt.

Een veel genoemde belemmering voor opschaling is het ontbreken van duurzame businessmodellen voor persoonlijke gezondheidsomgevingen. Maar ook over noodzakelijke ondersteunende diensten en voorzieningen, zoals infrastructuur, koppelvlakken en authenticatie, bestaat nog onduidelijkheid. Dit weerhoudt partijen ervan om te investeren.

Criteria voor succes (wanneer is Medmij geslaagd en wat is daarvoor nodig?)

Er is samenspel nodig van zorgverzekeraars, overheid, patiëntenorganisaties, leveranciers en zorgaanbieders en zeker ook de ICT-industrie.

Van leveranciers wordt verwacht dat zij zelf investeren en de ontwikkeling om de patiënt daadwerkelijk centraal te plaatsen, prioriteit geven. Van hen is nodig dat zij ervoor zorgen dat gezondheidsgegevens uitgewisseld kunnen worden conform het MedMij afsprakenstelsel, zodat op het 'platform' waarbinnen gezondheidsgegevens worden samengebracht ook waardevolle functionaliteiten (tools, apps, online-programma's) beschikbaar komen voor patiënten en consumenten. De onderzoekers geven aan dat opschaling en ruimte voor innovatie belangrijke baten zijn, wanneer men kan uitgaan van een gezamenlijk

afsprakenstelsel. Van verantwoordelijke partijen -met name zorgverzekeraars en overheid - mogen leveranciers verwachten dat er uitzicht is op een gezonde businesscase.⁸⁷

Kosten en baten voor betrokken partijen (wie is betrokken en wat betekent Medmij voor deze partijen?)

Medmij heeft het bureau Gupta Strategists gevraagd de kosten en baten van persoonlijke gezondheidsomgevingen te analyseren⁸⁸. De baten van een persoonlijke gezondheidsomgeving zijn ingeschat op basis van een achttal functionaliteiten; zelfmanagement programma's, delen van onderzoeksresultaten, overzicht en analyse medicatiegegevens, e-visit, remote monitoring, invullen van vragenlijsten, online maken van afspraken en delen van professionele samenvatting. Voor het afsprakenstelsel zelf, een voorwaarde voor het ontwikkelen van een persoonlijke gezondheidsomgeving, zijn de baten niet gekwantificeerd.

Het rapport onderschrijft een sterke maatschappelijke businesscase voor persoonlijke gezondheidsomgevingen. Afhankelijk van het gekozen scenario, is het break-even punt 3 tot 8 jaar (resp. basis of conservatief). Het is belangrijk om te noemen dat als randvoorwaarde een authenticatie middel op betrouwbaarheidsniveau hoog wordt voorzien. Dit kan een publiek of privaat middel, of een combinatie hiervan zijn. Ook wordt er in deze maatschappelijke businesscase gekeken naar toepassing van persoonlijke gezondheidsomgevingen op grote schaal en is er discussie mogelijk over een aantal onderliggende aannamen.

Use case zelfmanagement chronisch zieken

Nederland telde in 2014 ongeveer 8 miljoen chronisch zieke patiënten.⁸⁹ Voor verschillende patiëntgroepen die regelmatig zorg nodig hebben worden er pilot programma's aangeboden om zelf, met behulp van digitale zorgverlening, een actieve rol te spelen in het omgaan met hun aandoening.

Een illustratief voorbeeld is het trombose zorgportaal van ziekenhuisorganisatie Isala. Patiënten geven via het portaal hun INR-waarden (maat voor stollingstijd van het bloed) en eventuele ziekteverschijnselen door. Een doseerarts kijkt hiernaar en adviseert de patiënt op afstand over eventuele aanpassingen aan de medicatie. Voor dit type digitale dienstverlening is inloggen met een publiek of privaat middel met betrouwbaarheidsniveau hoog nodig.

In de kosten-baten analyse van Medmij uitgevoerd door Gupta Strategists⁹⁰ zijn de baten voor patiënten van dergelijke zelfmanagement programma's voor patiënten met Diabetes Mellitus type II, COPD, astma en cardiovasculaire ziekten (ongeveer 2 miljoen patiënten) ingeschat op een totaal van ongeveer € 125 miljoen per jaar.⁹¹

Conclusies use cases

Door het beschikbaar komen eID middelen op substantieel en hoog betrouwbaarheidsniveau neemt het palet aan diensten die in de zorg en het gemeente domein gedigitaliseerd kunnen worden toe. Met name in de zorg is de meerwaarde van een middel met betrouwbaarheidsniveau hoog

⁸⁷ Medmij. Reactie op de kosten-batenanalyse (Gupta rapport), 9 februari 2017

⁸⁸ Gupta Strategists. Kosten-batenanalyse persoonlijke gezondheidsomgeving, 8 februari 2017

⁸⁹ Op 1 januari 2014 hadden 8,2 miljoen mensen in Nederland een of meer chronische ziekten. Dit komt overeen met de helft van de Nederlandse bevolking. Een 'chronische ziekte' is hier gedefinieerd als een ziekte waarbij over het algemeen geen uitzicht is op volledig herstel. De schatting is gebaseerd op een selectie van 109 door de huisarts geregistreerde chronische ziekten. Bron: www.volksgezondheidszorg.info. Op basis van Nivel zorgregistraties eerste lijn.

⁹⁰ Gupta Strategists. Kosten-batenanalyse persoonlijke gezondheidsomgeving, 8 februari 2017

⁹¹ Op basis van 2 miljoen chronische patiënten met Diabetes Mellitus type II, COPD, astma en cardiovasculaire ziekten in Nederland waarvan 60% in aanmerking komt voor zelfmanagement en een tijdsbesparing van 7-8 uur per patiënt per jaar opgebouwd uit tijdsbesparingen door minder reistijd, minder reguliere consulten en integratie van diensten en een 'value of time' van € 14 per uur.

significant en noodzakelijk gezien het type gegevens. Gemeenten noemen vooral veel potentiële use cases die ook met een middel met betrouwbaarheidsniveau substantieel kunnen worden gerealiseerd.

Het zorg domein is al geruime tijd proactief bezig met het digitaliseren van diensten en gebruikt hiervoor ook private middelen. Generaliserend kan opgemerkt worden dat gemeenten meer reactief wachten op brede beschikbaarheid van een publiek middel op substantieel en hoog betrouwbaarheidsniveau alvorens over te gaan tot digitaliseren van diensten. Dit verschil kan deels verklaard worden door de 'hoge waarde achter het slot' voor een aantal doelgroepen in het zorgdomein.

De kosten en baten voor de burger die het gevolg zijn van digitalisering van diensten mogelijk gemaakt door een eID middel op betrouwbaarheidsniveau hoog; de kosten en baten van de 'huizen op het fundament' zijn nog niet met voldoende zekerheid te kwantificeren. Gemeenten noemen verschillende mogelijk toepassingen en in het zorgdomein zijn pilots en businesscases gemotiveerd die de waarde van de huizen onderstrepen. Baten voor burgers manifesteren zich met name in de vorm van tijdswinst door de afname van papieren processen en baliebezoeken. Hoe groot deze baten zijn zal in sterke mate afhangen van het aantal burgers dat gebruik gaat maken van de eID middelen en het gebruiksgemak van diensten die beschikbaar komen.

Bijlage 3 Gesprekspartners

Naam	Instantie en gebruikte afkorting
Michiel Dollenkamp	Logius
Frans de Kok	Logius
Eric Schneider	Logius
Cynthia Zonneveld	Logius
Nico van der Neut	Logius
Marc Gerrards	Logius
Bart Overbeek Bloem	Logius
Edward Hardam	Logius
Carlo Luijten	Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK)
Hans Meijering	Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK)
Richard van der Luit	Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK)
Wouter Diephuis	Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK)
Freek van Krevel	Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK)
Evelina de Valk	Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK)
Jurgen de Jong	Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK)
Rob Blommestijn	Dienst Wegverkeer (RDW)
Jetske ten Brug	Dienst Wegverkeer (RDW)
Auke van der Meulen	Dienst Wegverkeer (RDW)
Mandy van Tol	Rijksdienst voor Identiteitsgegevens (RvIG)
Merik Seven	Nictiz
Herbert Fetter	MedMij
Margreet Lont- van Gelder	Ministerie van Volksgezondheid, Welzijn en Sport (VWS)
Erwin Eisinger	Ministerie van Volksgezondheid, Welzijn en Sport (VWS)
Vincent van de Laar	Ministerie van Volksgezondheid, Welzijn en Sport (VWS)
Sanne Claessens	Ministerie van Volksgezondheid, Welzijn en Sport (VWS)
Willeke van Dijk	Nederlandse Vereniging voor burgerzaken (NVVB)
Marieke Colstee	Gemeente Groningen
Ton Koppen	Gemeente Eindhoven
Menno Stigter	Gemeente Den Haag
Marco Smit en Jaap den Otter	Gemeente Rotterdam
Marco Robins	Gemeente Montferland
Tjerk Venrooy en Jelmer van der Windt	PinkRocade
Lidwien Meijers en Alain Mahieu	Centric

Over Ecorys

Ecorys is een toonaangevend internationaal onderzoeks- en adviesbureau dat zich richt op de belangrijkste maatschappelijke uitdagingen. Door middel van uitmuntend, op onderzoek gebaseerd advies, helpen wij publieke en private klanten bij het maken en uitvoeren van gefundeerde beslissingen die leiden tot een betere samenleving. Wij helpen opdrachtgevers met grondige analyses, inspirerende ideeën en praktische oplossingen voor complexe markt-, beleids- en managementvraagstukken.

Onze bedrijfsgeschiedenis begon in 1929, toen een aantal Nederlandse zakenlieden van wat nu beter bekend is als de Erasmus Universiteit, het Nederlands Economisch Instituut (NEI) oprichtten. Het doel van dit gerenommeerde instituut was om een brug te slaan tussen het bedrijfsleven en de wereld van economisch onderzoek. Het NEI is in 2000 uitgegroeid tot Ecorys.

Door de jaren heen heeft Ecorys zich verspreid over de wereld met kantoren in Europa, Afrika, het Midden-Oosten en Azië. Wij werven personeel met verschillende culturele achtergronden en expertises, omdat wij ervan overtuigd zijn dat mensen met uiteenlopende eigenschappen een meerwaarde kunnen bieden voor ons bedrijf en onze klanten.

Ecorys excelleert in zeven werkgebieden:

- Economic growth;
- Social policy;
- Natural resources;
- Regions & Cities;
- Transport & Infrastructure;
- Public sector reform;
- Security & Justice.

Ecorys biedt een duidelijk aanbod aan producten en diensten:

- voorbereiding en formulering van beleid;
- programmamanagement;
- communicatie;
- capaciteitsopbouw (overheden);
- monitoring en evaluatie.

Wij hechten waarde aan onze onafhankelijkheid, onze integriteit en onze partners. Ecorys geeft om het milieu en heeft een actief maatschappelijk verantwoord ondernemingsbeleid, gericht op meerwaarde voor de samenleving en de markt. Ecorys is in het bezit van een ISO14001-certificaat dat wordt ondersteund door al onze medewerkers.



Postbus 4175
3006 AD Rotterdam
Nederland

Watermanweg 44
3067 GG Rotterdam
Nederland

T 010 453 88 00
F 010 453 07 68
E netherlands@ecorys.com
K.v.K. nr. 24316726

W www.ecorys.nl

Sound analysis, inspiring ideas