Business Case Inloggen in het BSN-domein

De kosten en baten van het eID-stelsel

Definitief eindrapport

Opdrachtgever: Ministerie van Binnenlandse Zaken & Koninkrijksrelaties

Rotterdam, 9 november 2016

Business Case Inloggen in het BSN-domein

De kosten en baten

Opdrachtgever: Ministerie van Binnenlandse Zaken & Koninkrijksrelaties

Ecorys BV Nederland
Van Zutphen Economisch Advies

Rotterdam, 9 november 2016

Over Ecorys

Met ons werk willen we een zinvolle bijdrage leveren aan maatschappelijke thema's. Wij bieden wereldwijd onderzoek, advies en projectmanagement en zijn gespecialiseerd in economische, maatschappelijke en ruimtelijke ontwikkeling. We richten ons met name op complexe markt-, beleids- en managementvraagstukken en bieden opdrachtgevers in de publieke, private en not-for-profitsectoren een uniek perspectief en hoogwaardige oplossingen. We zijn trots op onze 85-jarige bedrijfsgeschiedenis. Onze belangrijkste werkgebieden zijn: economie en concurrentiekracht; regio's, steden en vastgoed; energie en water; transport en mobiliteit; sociaal beleid, bestuur, onderwijs, en gezondheidszorg. Wij hechten grote waarde aan onze onafhankelijkheid, integriteit en samenwerkingspartners. Ecorys-medewerkers zijn betrokken experts met ruime ervaring in de academische wereld en adviespraktijk, die hun kennis en best practices binnen het bedrijf en met internationale samenwerkingspartners delen.

Ecorys Nederland voert een actief MVO-beleid en heeft een ISO14001-certificaat, de internationale standaard voor milieumanagementsystemen. Onze doelen op het gebied van duurzame bedrijfsvoering zijn vertaald in ons bedrijfsbeleid en in praktische maatregelen gericht op mensen, milieu en opbrengst. Zo gebruiken we 100% groene stroom, kopen we onze CO_2-uitstoot af, stimuleren we het ov-gebruik onder onze medewerkers, en printen we onze documenten op FSC- of PEFC-gecertificeerd papier. Door deze acties is onze CO_2-voetafdruk sinds 2007 met ca. 80% afgenomen.

ECORYS Nederland B.V.
Watermanweg 44
3067 GG Rotterdam

Postbus 4175
3006 AD 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

Inhoudsopgave

Managementsamenvatting

Aanleiding en opdracht

In het Algemeen Overleg in de Tweede Kamer d.d. 29 september 2016 over eID heeft de minister van BZK toegezegd dat er over circa een maand een actuele business case naar de Tweede Kamer gestuurd zou worden. De business case heeft betrekking op de maatregelen die de minister van BZK neemt om inloggen in het BSN-domein met betrouwbare authenticatiemiddelen te faciliteren.

In 2014 heeft Ecorys de Business case publieke eID-middelen opgesteld en in maart 2016 is deze business case herijkt op basis van voortschrijdende inzichten. Gezien de ontwikkelingen van de afgelopen maanden en de discussie in de kamer, is Ecorys gevraagd een business case op te stellen met een bredere scope. De investering behelst centrale voorzieningen die nodig zijn om de multi-middelenaanpak te faciliteren (USvE, BSNk, kosten voor toelating en toezicht) en versterking van DigiD door nieuwe middelen op eIDAS betrouwbaarheidsniveaus substantieel en hoog te introduceren. De centrale vraag in deze business case is of de kwalitatieve en kwantitatieve baten de investering rechtvaardigen.

Uitgangspunten

Enkele belangrijke uitgangspunten relevant voor een goede duiding van de resultaten zijn:

- Er is een analyse gemaakt van de integrale kosten en baten van het eID-stelsel met publieke en private middelen op betrouwbaarheidsniveau substantieel en hoog.
- Voor de kosten en baten hebben wij de periode van 2015 tot en met 2027 (10 jaar na inwerkingtreding) beschouwd.
- Alle digitale diensten van overheidsdienstverleners zijn toegankelijk via het eID-stelsel.
- Het is de verwachting dat DigiD (eIDAS betrouwbaarheidsniveau laag) op termijn zal worden uit gefaseerd en dat voor deze transacties tenminste betrouwbaarheidsniveau substantieel zal worden vereist. Het is niet duidelijk wanneer dit zal gebeuren. Voor onze analyse en berekeningen hebben wij het jaar 2020 als moment van deze uitfasering gebruikt.
- Vanaf 2018 worden eID-middelen op het niveau DigiD Hoog (eNIK en eRijbewijs) uitgereikt en kunnen deze worden geactiveerd en gebruikt. Voor het uitgiftetempo van DigiD Hoog is aangesloten bij het bestaande vervangingspatroon van identiteitsbewijzen.
- Private middelen, zoals bv. de bankpas, krijgen toegang tot het eID-stelsel.
- Burgers kunnen de beschikking hebben over meerdere eID-middelen. Bij de berekening van de kosten en de baten is hiermee rekening gehouden.

Waarom een eID-stelsel voor het BSN-domein?

Er zijn drie belangrijke redenen waarom er een behoefte is aan een eID-stelsel met middelen op betrouwbaarheidsniveau substantieel en hoog.

- Op dit moment gebruiken burgers DigiD om in te loggen en digitaal transacties af te handelen met overheidsdienstaanbieders in het BSN-domein (in 2016 263 miljoen keer), 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. Zo is de Autoriteit Persoonsgegevens van oordeel dat “het huidige lage beveiligingsniveau van DigiD, gelet op de stand van de techniek en de gevoelige en/of bijzondere persoonsgegevens (waaronder het BSN) die in het kader van DigiD worden verwerkt, onvoldoende is.”

- Daarnaast bieden veel overheidsdienstaanbieders digitale diensten aan achter DigiD, waar eigenlijk een middel met een hoger betrouwbaarheidsniveau vereist zou zijn vanuit privacy en veiligheidsoverwegingen. Als er een middel is met een hoger betrouwbaarheidsniveau kunnen overheden beter voldoen aan Europese en nationale regelgeving op het gebied van privacy en veiligheid.
- Als laatste is er de wens om nieuwe diensten te digitaliseren, maar dat is slechts mogelijk wanneer er een stelsel en middelen zijn op betrouwbaarheidsniveau hoog. Het kan dan bv. gaan om uitwisseling van privacygevoelige informatie (gezondheid, strafrecht) in het zorgdomein en het sociale domein. Als deze diensten kunnen worden gedigitaliseerd kan dat leiden tot een betere dienstverlening aan burgers in de vorm van een tijdsbesparing (transacties kunnen dan digitaal worden aangeboden i.p.v. op papier).

Wat is daar voor nodig?

Om veilig inloggen in het BSN-domein met een adequaat en toekomstbestendig betrouwbaarheidsniveau mogelijk te maken moeten investeringen worden gedaan in stelselvoorzieningen. Het gaat hier om eenmalige investeringen in de periode van 2015 tot en met 2018 met een totale waarde van € 53,2 miljoen. Dit betreft zowel kosten voor de verkenningsfase als de realisatiefase. Daarnaast moeten dienstaanbieders ook kosten maken om aan te sluiten op het eID-stelsel, deze kosten zijn nog niet bekend.

Daarnaast moeten er jaarlijks kosten gemaakt worden voor het beheer & onderhoud van de stelselvoorzieningen (beheer- en exploitatiefase). Het betreft hier kosten van de authenticatiedienst, toezicht en beheer en BSNk. De kosten hiervoor bedragen € 36,8 miljoen per jaar.[1] Deze jaarlijkse kosten staan min of meer vast voor deze periode, in de zin dat deze niet afhankelijk zijn van het gebruik van het stelsel.

Ook is het van belang dat burgers de beschikking hebben op middelen op betrouwbaarheidsniveau substantieel en hoog (DigiD Substantieel, DigiD Hoog met kaartlezer en/of private middelen). Voor de publieke middelen zijn deze kosten gelijk aan gemiddeld € 15 miljoen per jaar. Daar komen eventuele kosten voor private middelen nog bij, de hoogte van deze kosten is nog niet bekend.

Daarbij is een deel van de jaarlijkse kosten van inloggen in het BSN-domein afhankelijk van het aantal authenticaties per jaar. De kosten zijn ongeveer € 10 miljoen per jaar en lopen vanaf 2021 terug tot € 6 miljoen per jaar (wanneer DigiD met sms-verificatie niet meer nodig zal zijn). Gemiddeld zijn deze kosten gelijk aan € 7,5 miljoen per jaar.

Ook zijn er kosten voor de verdere doorontwikkeling en beleidsvorming van de publieke eID-middelen. De kosten hiervan zijn gelijk aan € 1,4 miljoen per jaar.

Om de volledige potentie van het inloggen in het BSN-domein te kunnen benutten is het vanzelfsprekend ook relevant dat overheidsdienstaanbieders nieuwe diensten voor burgers digitaliseren (in het bijzonder in het zorg- en sociale domein wat mogelijk wordt door de beschikbaarheid van middelen met betrouwbaarheidsniveau hoog). Hiervoor moeten overheidsdienstaanbieders enerzijds kosten maken (procesaanpassingen en investeringen in ondersteunende ICT-systemen) en dit levert overheidsdienstaanbieders ook voordelen op (efficiencyvoordelen, betere kwaliteit dienstverlening, etc.). Het palet aan potentiële diensten dat mogelijk wordt door een eID-stelsel is echter dusdanig veelzijdig net zoals de daarbij behorende

[1] Dit is inclusief de eenmalige kosten van groot onderhoud van € 10 miljoen.

kosten en baten voor overheidsdienstverleners dat het niet mogelijk en zinvol is om deze kosten en baten te kwantificeren.

In de volgende tabel is het totaalbeeld opgenomen van de kosten. Hierbij zijn investeringskosten in de periode 2015 tot 2018 naast de jaarlijkse kosten voor de periode 2018 t/m 2027 gezet. Dat resulteert in een totaaloverzicht in de te maken kosten over een periode van 13 jaar. Voor de gehele periode zijn de kosten gelijk aan € 658,8 miljoen. Naast eenmalige investeringskosten van € 53,2 miljoen moet er ieder jaar gemiddeld - als we alle kosten voor de overheid en burgers bij elkaar optellen - voor € 60,5 miljoen worden uitgegeven om inloggen met middelen op betrouwbaarheidsniveau substantieel en hoog mogelijk te maken in het BSN-domein.

Tabel S1.1: Kosten totaal (bedragen in € mln.)

Kostenpost	Investeringskosten (2015-2018)	Gemiddelde kosten per jaar in beheerfase (2018-2027)	Kosten totaal [a)]
Investeringskosten stelselvoorzieningen	53,2		53,2
Vaste kosten beheer en onderhoud stelselvoorzieningen		36,8	368,0
Investeringskosten middelen op betrouwbaarheidsniveau substantieel en hoog		14,8	148,3
Variabele kosten gebruik		7,6	75,7
Vaste kosten doorontwikkeling en beleidsvorming middelen		1,4	13,5
Totaal	**53,2**	**60,5**	**658,8**

a) Het gaat hier om de kosten over de periode van 2015 t/m 2027.

Wat leveren deze investeringen op?

Door de investeringen in het nieuwe eID-stelsel hoeft een aantal toekomstige kosten die samenhangen met het huidige stelsel niet meer te worden gemaakt. Dit zijn baten die aan het eID-stelsel mogen worden toegerekend. Deels zijn deze baten goed te kwantificeren. Te denken valt dan aan kosten voor de huidige DigiD oplossing die kunnen komen te vervallen en bv. kosten voor het in de lucht houden van alternatieve authenticatiesystemen. Per saldo valt een bedrag oplopend naar € 31,7 miljoen per jaar weg door het nieuwe eID-stelsel.

De belangrijkste baten van het eID-stelsel in het BSN-domein zijn gelegen in 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. Juist deze baten zijn lastig te becijferen. Er is onzekerheid over het groeipad van middelen en aantallen authenticaties, er is onzekerheid over de mate waarin bv. de identiteitsfraude teruggedrongen kan worden en er is onzekerheid over de mate waarin dienstaanbieders ook daadwerkelijk digitale oplossingen voor burgers zullen gaan ontwikkelen. Om toch een beter gevoel te krijgen bij de mate waarin de business case positief uit zal vallen hebben wij voor een alternatieve aanpak gekozen. Wij hebben gekeken hoeveel minder fraude er per jaar moet zijn en hoeveel transacties er op betrouwbaarheidsniveau hoog bij moeten komen waarbij de maatschappelijke business case in evenwicht is.

Het resultaat hiervan is dat de maatschappelijke business case in evenwicht is als:

- Er jaarlijks 1.400 gevallen van identiteitsfraude kunnen worden vermeden; of
- Er jaarlijks 30 miljoen digitale transacties op betrouwbaarheidsniveau hoog mogelijk worden dankzij het veilig kunnen inloggen in het BSN-domein.

Een aantal van 30 miljoen transacties per jaar lijkt daarbij op het eerste gezicht niet onrealistisch hoog te zijn. Alles overziend is de conclusie gerechtvaardigd dat het verstandig is om te investeren in het eID-stelsel in het BSN-domein met middelen op betrouwbaarheidsniveau substantieel en hoog.

1 Inleiding

1.1 Aanleiding

In het regeerakkoord ‘Bruggen slaan’ is de doelstelling opgenomen dat de dienstverlening door de overheid beter moet en dat bedrijven en burgers uiterlijk in 2017 zaken met de overheid digitaal moeten kunnen afhandelen. In de ‘Visiebrief digitale overheid 2017’ is deze ambitie verder uitgewerkt. Eén van de belangrijke elementen om dit mogelijk te maken is dat er een systeem is en dat er middelen zijn voor elektronische identificatie en authenticatie.

In het Algemeen Overleg in de Tweede Kamer d.d. 29 september 2016 over eID heeft de minister van BZK toegezegd dat er over circa een maand een actuele business case naar de Tweede Kamer gestuurd zou worden. De business case heeft betrekking op de maatregelen die de minister van BZK neemt om inloggen in het BSN domein met betrouwbare authenticatiemiddelen te faciliteren.

In 2014 heeft Ecorys de *Business case publieke eID-middelen*[2] opgesteld en in maart 2016 is deze business case herijkt op basis van voortschrijdende inzichten[3]. Gezien de ontwikkelingen van de afgelopen maanden en de discussie in de Tweede Kamer is Ecorys gevraagd een business case op te stellen met een bredere scope.

1.2 Onderzoeksvragen

De reikwijdte van deze geactualiseerde business case is breder dan de aanvankelijke ‘Business case herijking publiek eID-middel’ van maart 2016. In de business case van maart 2016 is gekeken naar de *meerkosten* die nodig zouden zijn om *publieke eID-middelen op eIDAS betrouwbaarheidsniveau hoog*[4] te kunnen gebruiken binnen de bestaande centrale voorzieningen voor DigiD (zoals bv. de huidige DigiD authenticatiedienst). In deze business case is gekeken naar *integrale kosten en baten* van de centrale voorzieningen die nodig zijn om de multi-middelenaanpak te faciliteren in combinatie met het introduceren van nieuwe *eID-middelen op eIDAS betrouwbaarheidsniveau substantieel en hoog*. Met andere woorden: alle investeringen die nodig zijn om inloggen in het BSN-domein op betrouwbaarheidsniveau substantieel en hoog mogelijk te maken. Merk daarbij op: het huidige DigiD heeft eIDAS betrouwbaarheidsniveau laag.

Meer concreet gaat het dan om de volgende zaken:

- De kosten voor de centrale voorzieningen, die een multi-middelenstrategie mogelijk maken, zoals onder meer de authenticatiedienst, het BSN koppelregister en inzagefunctie;
- De kosten (productie, uitgifte en gebruik) voor publieke middelen op eIDAS niveau substantieel (DigiD app) en eIDAS betrouwbaarheidsniveau hoog (eNIK en eRijbewijs)[5] [6];
- De kosten voor private middelen, zoals bv. bankmiddelen;

---

2 Ecorys (2014), *Business Case publieke eID-middelen.*

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

4 In die business case is naar de volgende eID-middelen gekeken: eNIK, eRijbewijs, eVreemdelingendocument en eID-bewijs voor geprivilegieerden.

5 Het paspoort is in dit onderzoek niet meegenomen als mogelijke drager van de eID-functionaliteit. Reden daarvoor is dat het op dit moment nog niet duidelijk is of het juridisch mogelijk is om een eID-functionaliteit toe te voegen aan het paspoort. Dit wordt nu onderzocht, de resultaten hiervan komen naar verwachting later beschikbaar.

6 Het eVreemdelingendocument en het eID-bewijs voor geprivilegieerden zijn ook niet meegenomen in deze business case. In eerdere business cases is overigens naar voren dat het algemene beeld en de conclusies niet heel erg veranderen als deze middelen wel worden meegenomen.

- De kosten voor overheidsdienstaanbieders om aan te sluiten op het eID-stelsel;
- De kosten voor toelating en toezicht, ondersteuning (helpdesk) en exploitatie van het eID-stelsel.
- De baten van het inloggen in het BSN-domein voor alle betrokken partijen.

Kosten en baten zijn waar mogelijk en zinvol gekwantificeerd, in andere gevallen zijn deze in kwalitatieve zin beschreven en toegelicht. Het gebruik van middelen in het private domein (bv. het inloggen bij Bol.com) is in deze analyse buiten beschouwing gelaten, er is alleen gekeken naar het gebruik van middelen in het BSN-domein.

Het financieringsvraagstuk (wie betaalt wat?) is in deze business case eveneens buiten beschouwing gelaten.

1.3 Onderzoeksaanpak

Het onderzoek borduurt voort op de opgestelde business case van maart 2016. Met een zeer beperkte doorlooptijd van vier weken is gekozen voor een aanpak waarbij de meest in het oog springende veranderingen ten opzichte van de business case uit maart mee zijn genomen.

Er zijn gesprekken gevoerd met het Ministerie van BZK, het Ministerie van VWS/CIBG, RDW, Logius, RvIG en NVVB om zowel de kosten als de baten goed in beeld te krijgen. Er is een aantal pilots (eNIK in Den Haag, eRijbewijs in Eindhoven) afgerond en geëvalueerd (Commissie Kuipers). Daarnaast is gebruik gemaakt van de verschillende rapporten die de afgelopen maanden zijn verschenen (denk aan gebruikerservaringen, betrouwbaarheid & veiligheid). Relevante bevindingen voor de business case hebben we meegenomen, in de bijlage zijn alle gebruikte bronnen opgenomen.

Het opstellen van de analyse van de kosten en baten is gedaan conform de voorschriften uit de *OEI-leidraad*[7], de recentere *Algemene leidraad voor maatschappelijke kosten-batenanalyses*[8] 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-projecten*[9] die in opdracht van het Ministerie van Economische Zaken is opgesteld. Baten voor burgers zijn becijferd aan de hand van de daarvoor geldende voorschriften uit de *Werkmap en StandaardKostenModel administratieve lasten burgers*[10], de handleiding van het ministerie van BZK voor het definiëren en meten van administratieve lasten als gevolg van beleid en regelgeving.

1.4 Leeswijzer

In een business case of kosten-batenanalyse wordt een vergelijking gemaakt tussen het zogenaamde nulalternatief en het projectalternatief. Na dit inleidende hoofdstuk beschrijft hoofdstuk 2 het projectalternatief (eID-stelsel met beschikbaarheid over middelen met op eIDAS betrouwbaarheidsniveau substantieel en hoog) en het nulalternatief (situatie dat er niet wordt geïnvesteerd in een eID-stelsel met middelen op eIDAS betrouwbaarheidsniveau substantieel en hoog)

---

7 CPB & NEI (2000), *Evaluatie van grote infrastructuurprojecten. Leidraad voor kosten-batenanalyse. Onderzoeksprogramma Economische Effecten Infrastructuur*

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

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

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

Hoofdstuk 3 presenteert de potentiële kosten en baten op hoofdlijnen. In hoofdstuk 4 werken wij de kosten nader uit en in hoofdstuk 5 de baten. Toelichtende overzichten en achtergrondinformatie zijn in de bijlagen opgenomen.

2 Het eID-stelsel voor inloggen in het BSN-domein

In dit hoofdstuk lichten wij toe wat er voor nodig is om naar een eID-stelsel te komen met middelen op betrouwbaarheidsniveau substantieel en hoog, zodat inloggen in het BSN-domein mogelijk wordt. Wij starten met een korte beschrijving van de huidige situatie (nulalternatief). Vervolgens geven wij een korte beschrijving van het project. Daarna geven wij een korte introductie van de kosten en tot slot van de baten.

2.1 Huidige situatie

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 263 miljoen authenticaties met DigiD door burgers in 2016.

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.

Wensen en behoeften

Er zijn drie belangrijke redenen waarom er een behoefte is aan een eID-stelsel met middelen op betrouwbaarheidsniveau substantieel en hoog.

- Op dit moment gebruiken burgers DigiD om in te loggen en digitaal transacties af te handelen met overheidsdienstaanbieders in het BSN-domein (voor heel 2016 263 miljoen keer), maar de ***betrouwbaarheid en veiligheid van DigiD is niet in alle gevallen voldoende*** – zeker in het huidige tijdsgewricht. Hierdoor is er een risico op identiteitsfraude. Zo is de Autoriteit Persoonsgegevens van oordeel dat “het huidige lage beveiligingsniveau van DigiD, gelet op de stand van de techniek en de gevoelige en/of bijzondere persoonsgegevens (waaronder het BSN) die in het kader van DigiD worden verwerkt, onvoldoende is”.[11]
- Daarnaast bieden veel overheidsdienstaanbieders digitale diensten aan achter DigiD, waar eigenlijk een middel met een hoger betrouwbaarheidsniveau vereist zou zijn vanuit privacy en veiligheidsoverwegingen. Als er een middel is met een hoger betrouwbaarheidsniveau kunnen ***overheden beter voldoen aan Europese en nationale regelgeving op het gebied van privacy en veiligheid***.
- Als laatste is er de wens om nieuwe diensten te digitaliseren, maar dat slechts is mogelijk wanneer er een stelsel en middelen zijn op betrouwbaarheidsniveau hoog. Het kan dan bv. gaan om uitwisseling van medische informatie. Als deze diensten kunnen worden

[11] Autoriteit Persoonsgegevens (2016), *eID. Brief aan de Minister van Binnenlandse Zaken & Koninkrijksrelaties, d.d. 14 september 2016.*

gedigitaliseerd kan dat leiden tot een ***betere dienstverlening aan burgers*** in de vorm van een tijdsbesparing (transacties kunnen dan digitaal worden aangeboden i.p.v. op papier).

2.2 Projectbeschrijving

In deze businesscase is gekeken naar het eID-stelsel zoals dat momenteel onder de verantwoordelijkheid van de minister van BZK ontwikkeld wordt. Het doel van het eID stelsel is de modernisering van inloggen en overgaan op een hogere betrouwbaarheid voor officiële online identificatie.

Nederlanders kunnen in de toekomst kiezen uit meerdere manieren om in te loggen en zich te identificeren in het BSN-domein. Om het eID-stelsel tot stand te brengen stelt de minister een Uniforme Set van Eisen (USvE) op, ontwikkelt hij een toetsingskader, regelt hij toelating, toezicht en beheer, realiseert hij centrale voorzieningen zoals het BSNk en een inzagefunctie en introduceert hij publieke eID-middelen op de eIDAS betrouwbaarheidsniveaus substantieel en hoog. Om het stelsel te laten functioneren dienen dienstaanbieders in de publieke sector daarop aan te sluiten, ook de aansluitkosten van deze dienstaanbieders zijn in deze businesscase meegenomen.

2.2.1 Stelselvoorzieningen

In het navolgende zijn de stelselvoorzieningen verder uitgewerkt.

Authenticatiedienst

De authenticatiedienst bepaalt op basis van het gebruikte inlogmiddel of een gebruiker daadwerkelijk is wie hij beweert te zijn. Op dit moment is er een authenticatiedienst voor DigiD en de bestaande authenticatiedienst van DigiD wordt daarom omgebouwd tot de authenticatiedienst voor de publieke middelen.[12]

Uniforme Set van Eisen (USvE)

De uniforme eisen is gebaseerd op de Europese eIDAS verordening. Het behelst 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 BZK een Nederlands kader kan worden vastgesteld.

Toelating, toezicht en beheer

Er worden eisen geformuleerd die aan de inrichting van toelating, toezicht en beheer gesteld zullen worden. Er wordt besloten waar de toelating, het toezicht en het beheer organisatorisch belegd zullen worden. De processen om toelating, toezicht en beheer uit te voeren zullen bij de betreffende organisatie(s) daadwerkelijk worden ingericht.

BSN-koppelregister (BSNk)

Authenticatiemiddelen die voor gebruik in het BSN-domein worden toegestaan, moeten gaan voldoen aan de Uniforme Set van Eisen. Het ontwerp dat aan deze stelseleisen ten grondslag ligt, is gebaseerd op gebruik van de privacybeschermende techniek van pseudonimisering. Aan ieder authenticatiemiddel (zowel privaat als publiek) wordt een polymorf pseudoniem (PP) gekoppeld dat gebaseerd is op het BSN. Het BSNk wordt de bouwsteen die dergelijke polymorfe pseudoniemen uitgeeft aan geautoriseerde publieke en private partijen (‘identiteitsverstrekkers’).

[12] Informatie Ministerie van Binnenlandse Zaken en Koninkrijksrelaties.

Inzagefunctie

Door de multi-middelenaanpak kan de burger dadelijk met meerdere middelen inloggen bij dienstverleners in het BSN-domein. Echter, dit betekent ook dat de burger inzage moet hebben in zijn of haar middelen die hij gebruikt voor dit doel. De inzagefunctie verschaft de burger op een hoog beveiligd niveau inzage op de registratie en het gebruik van al zijn middelen. Daarnaast biedt de Inzagefunctie de mogelijkheid tot gerichte misbruik- en fraudebestrijding.

Aansluiten dienstaanbieders

Het is de verantwoordelijkheid van de dienstaanbieders zelf om op het eID stelsel aan te sluiten en daarvoor de benodigde maatregelen te nemen.

2.2.2 DigiD Hoog

Het publieke middel DigiD Hoog[13], 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. Concreet betekent dit het toevoegen van een e-functionaliteit aan de NIK en het rijbewijs. Hiermee worden burgers voorzien van een middel waarmee ze eenvoudig op hoog betrouwbaarheidsniveau bij publieke dienstverleners kunnen inloggen. Deze publieke eID-middelen worden opgenomen in het eID-stelsel. De uitrol van het publieke eID-middel verloopt via het natuurlijke vervangingspatroon van de betreffende WID-documenten.[14] Als een burger vanaf 2018 een nieuw WID-document aanvraagt, 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[15]). De burger heeft dan zelf de keuze om de eID-functionaliteit te activeren en te gebruiken.[16] De burger activeert de eID-functionaliteit zelf met pincode, die hij in een PIN/PUK-brief heeft ontvangen van de middelenuitgever. In bijlage 1 zijn de stappen uitgebreider beschreven.

Het publieke eID-middel kan alleen worden gebruikt in het publieke domein (BSN-domein[17]).[18] Eventueel gebruik van publieke eID-middelen in het private domein is in deze business case buiten beschouwing gelaten.

Om in te kunnen loggen met zijn publieke eID-middel moet de burger de beschikking hebben over een smartphone met NFC of een kaartlezer. Bij het inloggen moet de burger een pincode invoeren om toegang te krijgen (vergelijk: bij DigiD is dat een wachtwoord). Als een burger zijn pincode en pukcode is vergeten, dan heeft hij de mogelijkheid om zijn pincode opnieuw te laten activeren.

2.2.3 DigiD Substantieel

Daarnaast komt er ook een publiek middel met betrouwbaarheidsniveau substantieel. Beoogd is een middel (DigiD app) te introduceren en uit te rollen met betrouwbaarheidsniveau eIDAS substantieel (DigiD Substantieel) voor de doelgroep personen met een NFC compatible

---

13 Er zijn drie verschillende eIDAS betrouwbaarheidsniveaus: laag, substantieel en hoog. Naast deze betrouwbaarheidsniveau zijn er ook vier verschillende DigiD middelen: DigiD Basis is het huidige DigiD, DigiD Midden is DigiD met sms-verificatie. DigiD Basis en DigiD Midden hebben eIDAS betrouwbaarheidsniveau laag. DigiD Substantieel (DigiD app) heeft eIDAS betrouwbaarheidsniveau substantieel en DigiD Hoog (eNIK, eRijbewijs) heeft eIDAS betrouwbaarheidsniveau hoog. Als in het vervolg van het rapport wordt gesproken over betrouwbaarheidsniveaus, dan worden daarmee de eIDAS betrouwbaarheidsniveaus bedoeld. Als in het vervolg van het rapport wordt gesproken over DigiD dan wordt daarmee gedoeld op DigiD Basis of DigiD Midden.

14 Informatie Ministerie van Binnenlandse Zaken en Koninkrijksrelaties.

15 Informatie Ministerie van Binnenlandse Zaken en Koninkrijksrelaties.

16 Informatie Ministerie van Binnenlandse Zaken en Koninkrijksrelaties.

17 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.

18 Informatie Ministerie van Binnenlandse Zaken en Koninkrijksrelaties.

smartphone, waarmee de chip in WID-documenten uitgelezen kan worden. Er wordt nog gekeken naar oplossingen voor burgers die niet in het bezit zijn van zo'n telefoon.

DigiD Substantieel draagt bij aan een versnelling van de toegang tot digitale diensten van overheidsdienstaanbieders op een substantieel betrouwbaarheidsniveau, doordat het huidige DigiD eenvoudig kan worden opgewaardeerd met bestaande WID-documenten naar betrouwbaarheidsniveau substantieel.

Om in te kunnen loggen op substantieel betrouwbaarheidsniveau moet de DigiD app eenmalig worden gekoppeld aan het WID-document. 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.

De meerwaarde van de DigiD app is dat alle burgers al in het bezit zijn van een NIK, rijbewijs en/of paspoort (hoge dekkingsgraad) en dat burgers daardoor op relatief korte termijn de beschikking hebben over een publiek eID-middel op substantieel betrouwbaarheidsniveau.

2.3 Wel type kosten moeten worden gemaakt?

Om naar een eID-stelsel met publieke en private middelen op eIDAS betrouwbaarheidsniveau substantieel en hoog te komen, zodat burgers kunnen inloggen in het BSN-domein, moeten de volgende kosten worden gemaakt.

Wij hebben de volgende kostensoorten onderscheiden:

- **Investeringskosten stelselvoorzieningen**. Het gaat hier onder meer om investeringskosten in de authenticatiedienst, toezicht en beheer, het BSNk en aansluitkosten voor overheidsdienstaanbieders.
- **Vaste kosten beheer en onderhoud stelselvoorzieningen**. Jaarlijks moeten er kosten worden gemaakt voor beheer, onderhoud en verdere doorontwikkeling van de authenticatiedienst, toezicht en beheer en het BSNk.
- **Investeringskosten middelen op betrouwbaarheidsniveau substantieel en hoog**. Burgers moeten de beschikking hebben over middelen op betrouwbaarheidsniveau substantieel en hoog. Er moeten extra kosten worden gemaakt voor deze middelen zelf en voor de uitgifte van deze middelen.
- **Variabele kosten gebruik**. Bepaalde kosten zijn afhankelijk van het aantal authenticaties en het gebruik van de middelen (helpdesk en ondersteuning).
- **Vaste kosten doorontwikkeling en beleidsvorming middelen**. Er moeten jaarlijks ook kosten worden gemaakt voor de doorontwikkeling en beleidsvorming van de publieke eID-middelen.

Deze kosten werken wij in hoofdstuk 4 verder uit.

2.4 Welk type baten levert de investering op?

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.***[19] 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.

[19] Zie ook: Ecorys & Van Zutphen Economisch Advies (2014), *Business Case eNIK.*

- Wat is de waarde van het fundament van een gemiddeld rijtjeshuis?
- En wat is de waarde van hetzelfde fundament met een twee keer zo grote woning?
- En wat is de waarde van dat fundament als het een luxe villa is?

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.

Hetzelfde geldt ook voor veel e-overheidsprojecten (bv. basisregistraties) en ook voor bv. 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***'. Enerzijds 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 eruit ziet).

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 *Realisatie & Invoeringsplan Impuls eID* van het Ministerie van BZK[20] wordt reeds treffend verwoord wat het belang van het eID-stelsel is als fundament voor de verdergaande digitalisering van de maatschappij en de noodzaak hierop te acteren:

> De daadwerkelijke start van de uitrol van meerdere manieren van inloggen en officiële online identificatie is een cruciaal onderdeel van de doelstelling uit het Regeerakkoord dat Nederlanders per eind 2017 hun zaken met de overheid en private organisaties in het BSN-domein digitaal kunnen doen. Het is ook urgent omdat de huidige infrastructuur tien jaar geleden is ingevoerd en mogelijkheden voor kwaadwillenden toenemen in deze (technologisch) snel veranderende wereld. Permanente aandacht voor verbeterde beveiliging is essentieel. Het huidige eID beleid is daarnaast verbonden met verschillende beleidsvoornemens op andere terreinen; zaken zoals de zorg (eHealth) en de modernisering van de interactie bij belasting- en toeslagzaken zijn hiervan afhankelijk. Kortom, het onophoudelijk en met voorrang verder investeren in de infrastructuur voor digitaal inloggen is noodzakelijk vanwege **(i) kwaliteitsverbetering** van de publieke dienstverlening, **(ii)** het steeds grimmiger dreigingsbeeld in het digitale domein, bijvoorbeeld ten aanzien van mogelijkheden voor **identiteitsfraude** en **(iii)** het **binnen de financiële kaders** blijven bij de uitvoering van deze dienstverlening.

Hieronder presenteren we een aantal baten van de Impuls eID en noemen we voorbeelden van use cases die een indicatie geven van de potentiële impact / reikwijdte van de baten.

Verbetering van de kwaliteit van de dienstverlening & vermindering van de inspanningen voor burgers om een dienst af te kunnen nemen

DigiD Substantieel en DigiD Hoog komen algemeen beschikbaar voor een omvangrijke populatie van burgers en is laagdrempelig toe te passen. Voor DigiD Hoog betekent dit dat in essentie een burger alleen bij de aanvraag van een nieuw WID-document naar het loket moet. Alle andere diensten waar in het verleden een bezoek aan het loket nodig was kunnen op termijn digitaal afgenomen worden. Gebruikers ervaren de publieke eID-middelen in het elektronisch gebruik als één geheel (zelfde 'look and feel' voor de burger), waarbij digitaal toegang wordt verkregen tot

[20] Versie 0.99, 25 september 2016. Pagina 6

meerdere dienstverleners. Hiermee kan gesteld worden dat de inzet van eID-publieke middelen bijdraagt aan een hogere **gebruiksvriendelijkheid** en **lagere kosten** / minder inspanningen voor de burger.

De komst van DigiD Substantieel en DigiD Hoog draagt bij aan de **keuzevrijheid** van burgers door naast private middelen ook een publiek middel beschikbaar te stellen.[21]

DigiD Hoog maakt gebruik van het bestaande hoogwaardige aanvraag- en uitgifteproces van WID-documenten, waardoor tegen **relatief lage meerkosten voor burger en maatschappij** een middel op betrouwbaarheidsniveau hoog kan worden uitgereikt aan burgers.

DigiD Hoog is zo ingericht dat het **privacybescherming** het beste waarborgt, in die zin dat de burger kan inloggen bij een dienstverlener, zonder dat dit feit bij de DigiD authenticatiedienst of andere partijen in de keten bekend is.

DigiD Substantieel kent niet het betrouwbaarheidsniveau van DigiD Hoog, maar kent wel een **hoger beveiligingsniveau dan het huidige DigiD** dat werkt met een wachtwoord (en sms).

Efficiencyvoordelen bij overheidsdienstaanbieders

Er zijn tientallen use-cases / voorbeelden, zoals het vanuit huis voor het inzien van het medisch dossiers, die **efficiencyvoordelen** kunnen opleveren, mits DigiD Hoog er is en in welk tempo dit wordt uitgerold. Bovendien zijn er use-cases, zoals arbeidsongeschiktheid en bijzondere persoonsgegevens, waarbij het hoogste betrouwbaarheidsniveau een vereiste is.

Milieubaten door digitalisering

Het aantal brieven vanuit dienstverleners kan nog verder gereduceerd bij intreding van DigiD Substantieel.

2.5 Groeipad van het gebruik van middelen en het aantal authenticaties

Een belangrijke determinant voor de kosten en de baten is het gebruik van eID-middelen in het eID-stelsel (of het aantal authenticaties) en meer in detail de groei van het gebruik. In deze paragraaf lichten wij kort toe welke uitgangspunten wij hebben gebruikt om een indicatie te kunnen geven van het groeipad van het gebruik.

De laatste jaren is het gebruik van DigiD sterk gegroeid. Van 117 miljoen authenticaties in 2013 naar 158 miljoen authenticaties in 2014, naar 206 miljoen authenticaties in 2015 tot aan 263 miljoen authenticaties in 2016.[22] En het is de verwachting dat deze groei nog verder door zal zetten in de komende jaren. In een eerdere business case is ervan uitgegaan dat het aantal authenticaties in het BSN-domein door kan groeien tot 500 miljoen authenticaties per jaar.[23] Het is daarbij de verwachting dat dit niveau van 500 miljoen authenticaties geleidelijk bereikt zal worden, waarbij de relatieve groei af zal nemen. In de analyse is het uitgangspunt gehanteerd dat de groeivoet in ieder jaar gelijk is aan de 80% van de groeivoet van het jaar daarvoor.[24] Immers, de grote uitvoeringsorganisaties waar veel burgers mee te maken hebben (Belastingdienst, UWV, SVB en DUO) hebben een groot deel van hun diensten al gedigitaliseerd.

---

21 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.

22 Zie Ministerie van BZK (2016), *Monitor Generieke Digitale Infrastructuur 2016*. De aantallen authenticaties uit 2016 komen van Logius,

23 Zie Ecorys (2015), *Business Case publieke eID-middelen.*

24 Dit komt ook terug in de feitelijke cijfers over de periode 2013 – 2016.

Uitgangspunt voor onze analyse is daarbij geweest dat betrouwbaarheidsniveau laag (DigiD) vanaf 2020 volledig is uitgefaseerd en dat burgers[25] vanaf 2020 minimaal gebruik moeten maken van een middel op betrouwbaarheidsniveau substantieel. De burger kan dan bijvoorbeeld gebruik maken van DigiD app, van bankmiddelen (iDIN) of van andere private middelen (o.a. Idensys). Voor de middelen op niveau substantieel is geen apart uitgifteproces nodig (behoudens mogelijk het activeren van het middel) en dat betekent dat hier geen knelpunt hoeft te ontstaan ten aanzien van de beschikbaarheid van middelen.

Daarbij is het nadrukkelijk ook niet de verwachting dat 100% van de burgers gebruik zal gaan maken van de digitale dienstverlening. In een studie van Dialogic[26] is geschat dat 5% van de burgers zogenaamd “digitaal niet-redzaam” is en dat er daarnaast een groep is van 10% tot 15% van de burgers die alleen redzaam is met ondersteuning. Ook in andere analyses komen percentages van 10% tot 15% terug over het deel van de burgers voor wie digitaal contact niet goed of helemaal niet mogelijk is.[27] Wij zijn er in onze analyse vanuit gegaan dat de niet-digitale kanalen voor burgers om transacties te doen met de overheid gewoon open blijven voor minder digivaardige burgers. Bij de kosten is wel rekening gehouden met kosten voor de reguliere helpdesk en ondersteuning.

Een groot deel van het volume van authenticaties in het eID-stelsel kan op betrouwbaarheidsniveau substantieel worden afgehandeld. In aanvulling daarop zijn er ook authenticaties waarvoor betrouwbaarheidsniveau hoog gewenst is. Het gaat dan in het bijzonder om elektronische gegevensuitwisseling met gegevens die gevoelig zijn in de zin van de Wet Bescherming Persoonsgegevens: strafrechtelijke gegevens, gezondheid, seksuele geaardheid e.d.. Gegevensuitwisselingen met gezondheidsgegevens komen bijvoorbeeld voor bij zorgaanbieders, bij zorgverzekeraars, bij het UWV en bij gemeenten (WMO-loket), dus in het zorgdomein en het sociale domein. Op beperktere schaal zijn ze ook aan de orde in de financiële sector. Strafrechtelijke gegevens spelen een grote rol in het justitiële domein.

In de eerdere Business Case Publieke eID-middelen is alleen kwalitatief gekeken naar de mogelijkheden in het zorgdomein en/of sociale domein, in de voorliggende analyse hebben wij ook gekeken wat de orde van grootte van baten zou kunnen zijn. Recent is een inventarisatie gemaakt voor welke type diensten in de zorg een authenticatie op betrouwbaarheidsniveau hoog gewenst is.[28] Daaruit komt naar voren dat voor een groot deel van de transacties betrouwbaarheidsniveau hoog benodigd is. In bijlage 2 zijn ter illustratie enkele voorbeelden opgenomen met bijbehorende betrouwbaarheidsniveaus.

Er is op dit moment geen helder beeld van het aantal transacties of authenticaties per jaar in het zorgdomein en het sociale domein. Het is ons advies dat hier nader onderzoek naar wordt gedaan om een beter beeld te krijgen van de potentie van het eID-stelsel voor het zorgdomein en het sociale domein.

Belangrijk is daarbij wel dat er middelen zijn op betrouwbaarheidsniveau hoog. Hiervoor komen publieke middelen in de vorm van een eNIK en een eRijbewijs beschikbaar en daarnaast kan de burger mogelijk ook gebruik gaan maken van private middelen met betrouwbaarheidsniveau hoog.[29] Voor de groei van de publieke middelen op betrouwbaarheidsniveau hoog zijn wij

---

25 Nederlandse burgers in het buitenland zijn hierbij buiten beschouwing gelaten.

26 Dialogic (2013), *De digitale (zelf)redzaamheid van de burger: ondersteuning bij de Digitale Overheid 2017*

27 I&O Research (2015), *De kwaliteit van overheidsdienstverlening 2014*

28 PBLQ (2016), *Onderzoek betrouwbaarheidsniveau patiëntauthenticatie bij elektronische gegevensuitwisseling in de zorg.*

29 Voor onze analyse zijn wij er overigens vanuit gegaan dat bankmiddelen betrouwbaarheidsniveau substantieel krijgen.

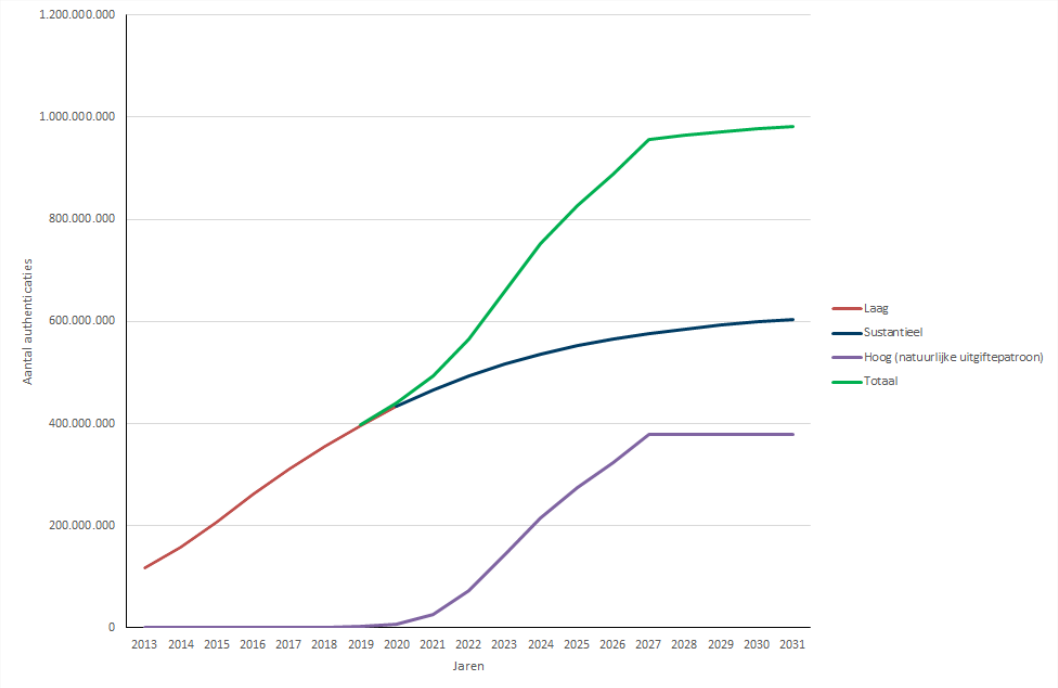
uitgegaan van het natuurlijke vervangingspatroon van de NIK en het Rijbewijs. In de volgende tabel is het te verwachten uitgiftetempo opgenomen voor de periode 2018 - 2027.

Tabel 2.1 Uitgiftetempo publieke eID-middelen (in miljoenen)

Jaar	NIK	Rijbewijs
2018	1,1	1,8
2019	0,7	1,8
2020	0,6	1,8
2021	0,9	1,5
2022	0,4	1,1
2023	0,3	1,1
2024	1,2	1,1
2025	1,5	1,1
2026	1,8	1,3
2027	1,3	1,9

Voor de verwachte groei van het aantal transacties op betrouwbaarheidsniveau hoog hebben wij aangesloten bij het vervangingspatroon van de eNIK en het eRijbewijs.[30] In de volgende figuur hebben wij de bovenstaande uitgangspunten vertaald om een indicatie te kunnen geven van een mogelijk groeipad. Daarbij hebben wij 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 (en dat voor 80% van de authenticaties in het zorgdomein betrouwbaarheidsniveau hoog vereist is).

Figuur 2.1 Illustratief groeipad als # authenticaties BSN-domein = # authenticaties zorg- en sociale domein



In de bovenstaande figuur is een illustratief groeipad gepresenteerd als ervan wordt uitgegaan dat het aantal authenticaties in het BSN-domein even groot is als het aantal authenticaties in het zorgdomein en sociale domein. Te zien is de groeicurve van betrouwbaarheidsniveau laag (huidige DigiD) en hoe dit overgaat in substantieel. Deze curve vlakt af in de tijd. Daarnaast is het groeipad

[30] In onze analyse zijn eventuele versnellingsstrategieën om ervoor te zorgen dat burgers eerder beschikken over een publiek middel met betrouwbaarheidsniveau hoog buiten beschouwing gelaten.

te zien van hoog, dat het natuurlijke uitgiftepatroon van de eNIK en het eRijbewijs volgt. De groene curve tot slot presenteert het totaal aantal authenticaties over de periode van 2013 tot en met 2031.

3 Resultaten op hoofdlijnen

In dit hoofdstuk presenteren wij de resultaten van de business case op hoofdlijnen. Detailinformatie over de kosten en de baten is te vinden in de hoofdstukken 4 (kosten) en 5 (baten). Wij starten dit hoofdstuk met de belangrijkste uitgangspunten van de analyse. Vervolgens presenteren wij de kosten en de baten. Wij sluiten af met een beschouwing van de uitkomsten.

3.1 Uitgangspunten

Enkele belangrijke uitgangspunten relevant voor een goede duiding van de resultaten zijn:

- Er is een analyse gemaakt van de integrale kosten en baten van het eID-stelsel met publieke en private middelen op betrouwbaarheidsniveau substantieel en hoog.
- Voor de kosten en baten hebben wij de periode van 2015 tot en met 2027 (10 jaar na inwerkingtreding) beschouwd.
- Alle digitale diensten van overheidsdienstverleners zijn toegankelijk via het eID-stelsel.
- Het is de verwachting dat DigiD (eIDAS betrouwbaarheidsniveau laag) op termijn zal worden uit gefaseerd en dat voor deze transacties tenminste betrouwbaarheidsniveau substantieel zal worden vereist. Het is niet duidelijk wanneer dit zal gebeuren. Voor onze analyse en berekeningen hebben wij het jaar 2020 als moment van deze uitfasering gebruikt.
- Vanaf 2018 worden eID-middelen op het niveau DigiD Hoog (eNIK en eRijbewijs) uitgereikt en kunnen deze worden geactiveerd en gebruikt. Voor het uitgiftetempo van DigiD Hoog is aangesloten bij het bestaande vervanging van identiteitsbewijzen.
- Private middelen, zoals bv. de bankpas, krijgen toegang tot het eID-stelsel.
- Burgers kunnen de beschikking hebben over meerdere eID-middelen. Bij de berekening van de kosten en de baten is hiermee rekening gehouden.

3.2 Waarom een eID-stelsel voor het BSN-domein?

Er zijn drie belangrijke redenen waarom er een behoefte is aan een eID-stelsel met middelen op betrouwbaarheidsniveau substantieel en hoog.

- Op dit moment gebruiken burgers DigiD om in te loggen en digitaal transacties af te handelen met overheidsdienstaanbieders in het BSN-domein (voor heel 2016 263 miljoen keer), maar de ***betrouwbaarheid en veiligheid van DigiD is niet in alle gevallen voldoende*** – zeker in het huidige tijdsgewricht. Hierdoor is er een risico op identiteitsfraude. Zo is de Autoriteit Persoonsgegevens van oordeel dat “het huidige lage beveiligingsniveau van DigiD, gelet op de stand van de techniek en de gevoelige en/of bijzondere persoonsgegevens (waaronder het BSN) die in het kader van DigiD worden verwerkt, onvoldoende is”.[31]
- Daarnaast bieden veel overheidsdienstaanbieders digitale diensten aan achter DigiD, waar eigenlijk een middel met een hoger betrouwbaarheidsniveau vereist zou zijn vanuit privacy en veiligheidsoverwegingen. Als er een middel is met een hoger betrouwbaarheidsniveau kunnen ***overheden beter voldoen aan Europese en nationale regelgeving op het gebied van privacy en veiligheid***.
- Als laatste is er de wens om nieuwe diensten te digitaliseren, maar dat is slechts mogelijk wanneer er een stelsel en middelen zijn op betrouwbaarheidsniveau hoog. Het kan dan bv.

[31] Autoriteit Persoonsgegevens (2016), *eID. Brief aan de Minister van Binnenlandse Zaken & Koninkrijksrelaties, d.d. 14 september 2016.*

gaan om uitwisseling van medische informatie. Als deze diensten kunnen worden gedigitaliseerd kan dat leiden tot een ***betere dienstverlening aan burgers*** in de vorm van een tijdsbesparing (transacties kunnen dan digitaal worden aangeboden i.p.v. op papier).

3.3 Wat is daar voor nodig?

Om veilig inloggen in het BSN-domein met een adequaat en toekomstbestendig betrouwbaarheidsniveau mogelijk te maken moeten investeringen worden gedaan in stelselvoorzieningen. Het gaat hier om eenmalige investeringen in de periode van 2015 tot en met 2018 met een totale waarde van € 53,2 miljoen. Dit betreft zowel kosten voor de verkenningsfase als de realisatiefase. Daarnaast moeten dienstaanbieders ook kosten maken om aan te sluiten op het eID-stelsel, deze kosten zijn nog niet bekend.

Daarnaast moeten er jaarlijks kosten gemaakt worden voor het beheer & onderhoud van de stelselvoorzieningen (beheer- en exploitatiefase). Het betreft hier kosten van de authenticatiedienst, toezicht en beheer en BSNk. De kosten hiervoor bedragen € 36,8 miljoen per jaar.[32] Deze jaarlijkse kosten staan min of meer vast voor deze periode, in de zin dat deze niet afhankelijk zijn van het gebruik van het stelsel.

Ook is het van belang dat burgers de beschikking hebben op middelen op betrouwbaarheidsniveau substantieel en hoog (DigiD Substantieel, DigiD Hoog met kaartlezer en/of private middelen). Voor de publieke middelen zijn deze kosten gelijk aan gemiddeld € 15 miljoen per jaar. Daar komen eventuele kosten voor private middelen nog bij, de hoogte van deze kosten is nog niet bekend.

Daarbij is een deel van de jaarlijkse kosten van inloggen in het BSN-domein afhankelijk van het aantal authenticaties per jaar. De kosten zijn ongeveer € 10 miljoen per jaar en lopen vanaf 2021 terug tot € 6 miljoen per jaar (wanneer DigiD met sms-verificatie niet meer nodig zal zijn). Gemiddeld zijn deze kosten gelijk aan € 7,5 miljoen per jaar.

Tot slot zijn er ook kosten voor de verdere doorontwikkeling en beleidsvorming van de publieke eID-middelen. De kosten hiervan zijn gelijk aan € 1,4 miljoen per jaar.

Om de volledige potentie van het inloggen in het BSN-domein te kunnen benutten is het vanzelfsprekend ook relevant dat overheidsdienstaanbieders nieuwe diensten voor burgers digitaliseren (in het bijzonder in het zorg- en sociale domein wat mogelijk wordt door de beschikbaarheid van middelen met betrouwbaarheidsniveau hoog). Hiervoor moeten overheidsdienstaanbieders enerzijds kosten maken (procesaanpassingen en investeringen in ondersteunende ICT-systemen) en dit levert overheidsdienstaanbieders ook voordelen op (efficiencyvoordelen, betere kwaliteit dienstverlening, etc.). Het palet aan potentiële diensten dat mogelijk wordt door een eID-stelsel is echter dusdanig veelzijdig net zoals de daarbij behorende kosten en baten voor overheidsdienstverleners dat het niet mogelijk en zinvol is om deze kosten en baten te kwantificeren.

In de volgende tabel is het totaalbeeld opgenomen van de kosten. Hierbij zijn investeringskosten in de periode 2015 tot 2018 naast de jaarlijkse kosten voor de periode 2018 t/m 2027 gezet. Dat resulteert in een totaaloverzicht van de te maken kosten over een periode van 13 jaar. Voor de gehele periode zijn de kosten gelijk aan € 658,8 miljoen. Naast eenmalige investeringskosten van € 53,2 miljoen moet er ieder jaar gemiddeld - als we alle kosten voor de overheid en burgers bij

[32] Dit is inclusief de eenmalige kosten van groot onderhoud van € 10 miljoen.

elkaar optellen - voor € 60,5 miljoen worden uitgegeven om inloggen met middelen op betrouwbaarheidsniveau substantieel en hoog mogelijk te maken in het BSN-domein.

Tabel 3.1: Kosten totaal (bedragen in € mln.)

Kostenpost	Investeringskosten (2015-2018)	Gemiddelde kosten per jaar in beheerfase (2018-2027)	Kosten totaal [a]
Investeringskosten stelselvoorzieningen	53,2		53,2
Vaste kosten beheer en onderhoud stelselvoorzieningen		36,8	368,0
Investeringskosten middelen op betrouwbaarheidsniveau substantieel en hoog		14,8	148,3
Variabele kosten gebruik		7,6	75,7
Vaste kosten doorontwikkeling en beleidsvorming		1,4	13,5
Totaal	**53,2**	**60,5**	**658,8**

a) Het gaat hier om de kosten over de periode van 2015 t/m 2027.

3.4 Wat leveren deze investeringen op?

Door de investeringen in het nieuwe eID-stelsel hoeft een aantal toekomstige kosten die samenhangen met het huidige stelsel niet meer te worden gemaakt. Dit zijn baten die aan het eID-stelsel mogen worden toegerekend. Deels zijn deze baten goed te kwantificeren. Te denken valt dan aan kosten voor de huidige DigiD oplossing die kunnen komen te vervallen en bv. kosten voor het in de lucht houden van alternatieve authenticatiesystemen. Per saldo valt een bedrag oplopend naar € 31,7 miljoen per jaar weg door het nieuwe eID-stelsel.

Tabel 3.2: Te kwantificeren baten (bedragen in € mln.)

Baten	Baten per jaar (vanaf 2022) [a]	Baten totaal [b]
Vermeden kosten authenticatiedienst DigiD	24,0	240,0
Vermeden kosten alternatieve authenticatiesystemen	7,7	48,3
Totaal	**31,7**	**288,3**

a) Voor het gekozen rekenvoorbeeld voor de vermeden kosten van alternatieve authenticatiesystemen zijn er pas baten te verwachten vanaf 2022 (zie paragraaf 5.2.)

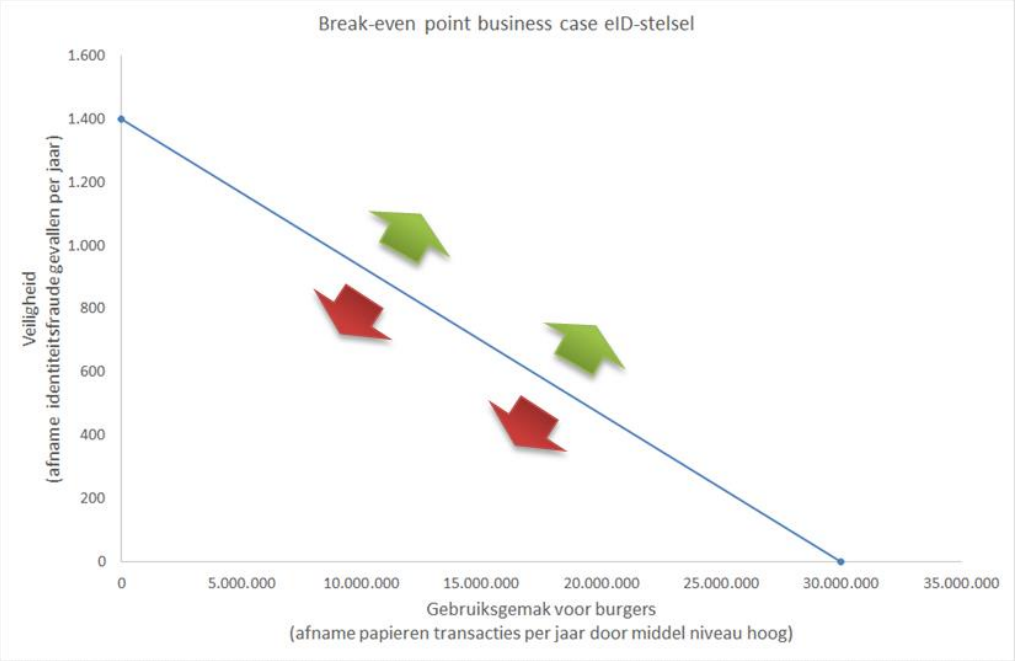
b) Het gaat hier om de som van de baten over de periode van 2018 t/m 2027. In de periode voor 2018 zijn er geen baten.

De belangrijkste baten van het eID-stelsel in het BSN-domein zijn gelegen in 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. Juist deze baten zijn lastig te becijferen. Er is onzekerheid over het groeipad van middelen en aantallen authenticaties, er is onzekerheid over de mate waarin bv. de identiteitsfraude teruggedrongen kan worden en er is onzekerheid over de mate waarin dienstaanbieders ook daadwerkelijk digitale oplossingen voor burgers zullen gaan ontwikkelen. Om toch een beter gevoel te krijgen bij de mate waarin de business case positief uit zal vallen hebben wij voor een alternatieve aanpak gekozen. Wij hebben gekeken hoeveel minder fraude er per jaar moet zijn en hoeveel transacties er op

betrouwbaarheidsniveau hoog bij moeten komen (bv. in het zorgdomein of sociale domein) waarbij de maatschappelijke business case in evenwicht is.

In de volgende figuur is het resultaat hiervan te zien. Het blijkt dat als het aantal gevallen van identiteitsfraude afneemt met ongeveer 1.400 per jaar, dan is het resultaat van de business case gelijk aan 0. Ook is te zien dat de business case op 0 uitkomt, wanneer er 30 miljoen transacties per jaar[33] dankzij een middel met betrouwbaarheidsniveau hoog digitaal kunnen worden afgehandeld in plaats van op papier. De business case komt eveneens op 0 uit bij alle andere punten op de curve in de figuur (dus bv. ook bij 700 gevallen minder identiteitsfraude en bij 15 miljoen minder papieren transacties).

Figuur 3.1 Break-even point business case eID-stelsel



De business case is dus positief boven de blauwe lijn en negatief eronder. Een middel op betrouwbaarheidsniveau hoog is grosso modo nodig bij gegevensuitwisseling waarbij gevoelige gegevens in de zin van de Wet Bescherming Persoonsgegevens opgenomen zijn. Deze gegevensuitwisseling kan er zowel zijn bij zorgaanbieders, bij zorgverzekeraars, bij het UWV en bij gemeenten (WMO-loket). Transacties zijn dan bv. het maken van afspraken, het inzien van privacygevoelige en/of medische gegevens, het bestellen medische producten, zorg op afstand, etc. Ook in de financiële sector en de sector justitie komen gegevensuitwisselingen met gevoelige gegevens voor. Een aantal van 30 miljoen transacties per jaar lijkt daarbij op het eerste gezicht niet onrealistisch hoog te zijn.

Het is wat lastiger om het cijfer van de identiteitsfraude goed te kunnen duiden. Wel is er bekend dat er in 2015 maatregelen genomen zijn bij 14.750 DigiD's in verband met mogelijke fraude en misbruik.[34] En dat is uiteraard het zichtbare of ontdekte deel van de fraude.

Alles overziend is de conclusie gerechtvaardigd dat het verstandig is om te investeren in het eID-stelsel in het BSN-domein met middelen op betrouwbaarheidsniveau substantieel en hoog.

---

33 Het gaat hier om 30 miljoen transacties in het eindbeeld. Hierbij is er ook rekening gehouden met het groeipad van middelen.

34 Zie Ministerie van BZK (2016), *Rijksjaarverslag 2015. VII Binnenlandse Zaken & Koninkrijksrelaties.*

3.5 Gevoeligheidsanalyse

In deze paragraaf presenteren wij de resultaten van de gevoeligheidsanalyse. In de gevoeligheidsanalyse hebben wij gekeken in hoeverre het project bij andere uitgangspunten nog steeds een interessant project blijft. Hierbij is in het bijzonder gekeken naar die uitgangspunten, waarover relatief meer onzekerheid bestaat.

Aangezien er vooral onzekerheid is over de baten die samenhangen met het toekomstige aantal authenticaties, hebben wij gekeken hoe het beeld in figuur 3.1 verandert bij gewijzigde uitgangspunten. Zo hebben we gekeken wat de gevolgen zijn als alle kosten 25% hoger uitvallen dan geraamd en wat de gevolgen zijn als er geen baten zijn van de wegvallen van alternatieve authenticatiepassen. Te zien is, dat de aantallen transacties om op break even uit te komen dan weliswaar iets hoger uitvallen, maar dat de orde van grootte vergelijkbaar is. De resultaten zijn opgenomen in de onderstaande tabel. Dit betekent dat de uitkomsten van de business case wel onzeker zijn, maar tegelijkertijd ook robuust zijn, in de zin dat de business case niet volledig verandert bij gewijzigde uitgangspunten. .

Tabel 3.3: Gevoeligheidsanalyse (aantallen fraude en aantal authenticaties)

Baten	Veiligheid [a)]	Gebruiksgemak [b)]
Kosten 25% hoger	1.925	41.000.000
Exclusief baten alternatieve authenticatiesystemen	1.525	31.500.000
Basisvariant	**1.400**	**30.000.000**

a) Business case is break-even bij x minder casus van identiteitsfraude

b) Business case is break-even bij x extra digitale transacties met middel op betrouwbaarheidsniveau hoog i.p.v. papieren transacties.

4 De kosten van het eID-stelsel

In dit hoofdstuk is een nadere uitwerking gemaakt van de te maken kosten voor het realiseren van het eID-stelsel waarin authenticatie op het eIDAS betrouwbaarheidsniveau substantieel en hoog mogelijk is. Hierbij hebben wij een onderscheid gemaakt naar:

- Investeringskosten stelselvoorzieningen;
- Vaste kosten beheer en onderhoud stelselvoorzieningen;
- Investeringskosten middelen op betrouwbaarheidsniveau substantieel en hoog;
- Variabele kosten gebruik;
- Vaste kosten doorontwikkeling en beleidsvorming middelen.

De gepresenteerde kosten zijn de kosten zoals die zijn aangeleverd door het Ministerie van Binnenlandse Zaken en Koninkrijkrelaties, Logius, VWS/CIBG, RvIG en RDW. Daar waar kosten niet veranderd zijn of er geen nieuwe inzichten zijn over de kosten is aangesloten bij de opgenomen kosten uit vorige business cases. Er is door Ecorys geen check uitgevoerd op de plausibiliteit van de gepresenteerde cijfers. Cijfers uit het Realisatie & Invoeringsplan zijn vastgesteld en de cijfers uit het Bestedingsplannen 2017 e.v. worden naar verwachting eind 2016 vastgesteld. Beheer en onderhoudskosten zijn minder hard en betreffen vooral indicaties zoals afgegeven door Logius.

4.1 Investeringskosten stelselvoorzieningen

In de navolgende tabel staan de investeringskosten weergegeven om te komen tot het eID-stelsel, waar burgers kunnen inloggen met middelen op betrouwbaarheidsniveau substantieel en hoog. De volgende kosten zijn kosten zijn onderscheiden kosten publiek middel, programmakosten eID, de Uniforme Set van Eisen, toezicht en beheer, kosten aanpassingen aan het BSNk, Inzagefunctie en investeringskosten voor uitrol DigiD Substantieel en DigiD Hoog.

Voor de jaren 2015 t/m 2018 samen zijn deze kosten gelijk aan € 53,2 miljoen. In vergelijking met de kostenraming uit de vorige business case (2014) zijn meerdere kostenposten beter in zicht en zijn niet alleen de kosten voor het publieke middel meegenomen, maar ook de kosten voor het eID-stelsel om het gebruik van publieke en private middelen mogelijk te maken. De verschillende kostenposten worden na de tabel verder toegelicht.

Tabel 4.1 Investeringskosten stelselvoorzieningen (bedragen in € 1.000)

Kosten	2015	2016	2017	2018	Totaal
Gerealiseerde kosten publiek middel	4.300	3.925	0	0	8.225
Programmakosten eID	9.340	1.900	400	600	12.240
USvE	0	1.400	1.450	0	2.850
Toezicht en beheer	0	0	750	0	750
BSNk	0	2.250	3.800	0	6.050
Inzagefunctie	0	0	2.490	510	3.000
DigiD Substantieel	0	300	1.200	0	1.500
DigiD Hoog	0	0	13.000	4.300	17.300
Invoeringskosten	0	0	1.310	0	0
Aansluitkosten dienstaanbieders	-	-	PM	PM	PM

Kosten	2015	2016	2017	2018	Totaal
Totaal	13.640	9.775	24.400	5.410	53.225

Hieronder volgt een korte toelichting op de verschillende kostenposten. Een belangrijke bron hiervoor is het Realisatie & Invoeringsplan Impuls eID[35] en diverse bestedingsplannen. Andere gebruikte bronnen zijn verschillende uitvoeringstoetsen, Dashboard ICT en ramingen van de kosten in 2016 door Logius en het ministerie van BZK.

Kosten publiek middel

De kosten publiek middel omvatten de reeds gemaakte kosten in 2015 voor de verkenningsfase en de geraamde kosten in 2016 (zie tabel 4.1).

Programmakosten eID

Onder programmakosten eID vallen reeds gemaakte kosten in 2015 voor voorbereiding en invoering en de geraamde programmakosten vanaf 2016 voor onder andere privacy & misbruikbestrijding, communicatie en kwaliteitsborging (zie tabel 4.1).

Uniforme set van eisen (USvE)

De uniforme set van eisen (USvE) vormt de normatieve set van eisen die gebruikt worden voor toelating en toezicht zoals gebaseerd op de eIDAS verordening (EU910/2014) met onderliggende uitvoeringsregelingen, die eisen stelt aan wederzijdse erkenning van publieke en private middelen. Dit kader, aangevuld met nationaal beleid, geeft antwoord op vragen als: welke inhoudelijke, procesmatige en technische eisen wenselijk zijn, aan wie deze eisen moeten worden opgelegd (normadressaten/actoren in de keten) en op basis van welke belangen/doelen dit dient te gebeuren. Privacyaspecten spelen hierin een belangrijke rol.

De kosten voor het ontwikkelen van een uniforme set van eisen voor toelating tot het BSN-domein van elektronische middelen voor het inloggen (identificatie en authenticatie) op digitale publieke dienstverlening zijn in tabel 4.1 weergegeven. De USvE heeft zowel betrekking op publieke als private middelen. De betreffende middelen moeten blijvend voldoen aan deze eisen.

Inrichting toelating, toezicht & beheer

De investeringskosten voor het inrichten van toelaten, toezicht en beheer voor partijen die diensten en producten leveren voor het inloggen (identificatie en authenticatie) in het BSN-domein zijn in tabel 4.1 weergegeven. De weergegeven kosten kennen nog een aantal afhankelijkheden waaronder de wijze waarop vanuit de Wet GDI aangesloten wordt bij het generieke toezicht en hoe specifiek toezicht op authenticatie ingericht gaat worden (hierover vindt in Q1/Q2 van 2017 nog overleg plaats tussen de beoogde toezichthouders. De te maken keuzes hebben ook effect op de beheer en exploitatiekosten in de komende jaren.

BSN-koppelregister

Het BSNk is een voorziening in het kader van de Generieke Digitale Infrastructuur (GDI) die het mogelijk maakt om publieke en private authenticatiemiddelen te gebruiken in het publiek domein. Het BSNk stelt een Authenticatiedienst in staat om een dienstverlener op een veilige, betrouwbare en vertrouwelijke manier een BSN of persistent pseudoniem te leveren van een gebruiker. Daarnaast stelt het BSNk de gebruiker in staat om met behulp van een inzage functie bij MijnOverheid controle te houden over zijn authenticatiemiddelen.

[35] Ministerie van BZK Versie 0.99, 25 september 2016

Ten behoeve van zijn functie implementeert BSNk een aantal hoofdfuncties: authenticatie, misbruikbestrijding, inzage, sleutelbeheer, metadatabeheer en overige operationeel beheer.

Tot slot hebben alle dienstverleners in het BSN-domein een eigen cryptografische sleutel nodig om het BSN van de gebruiker te lezen uit het versleutelde pseudoniem dat ze na een succesvolle authenticatie ontvangen. Het BSNk zorgt voor de veilige verstrekking van deze sleutels, nadat getoetst is dat de dienstverlener inderdaad gerechtigd is het BSN te verwerken.

Bij de registratie van een nieuw authenticatiemiddel door de gebruiker wordt er altijd gebruik gemaakt van het BSNk. Als de authenticatiedienst de Hardware Security Module (HSM) inbouwt, wordt er bij het reguliere inloggen geen gebruik meer gemaakt van het BSNk. Het BSNk is dan in gebruik geen Single Point of Failure meer.

De weergegeven kosten in tabel 4.1 zijn opgebouwd uit de geraamde kosten in 2016 en nog te maken kosten in 2017. Denk voor nog te maken kosten aan:[36]

- Productiewaardige BSNk aangepast voor gebruik HSM, dat voldoet aan niet-functionele specificaties en 24/7 kan worden beheerd;
- Aanbesteedde en ingerichte HSMs;
- Ingericht sleutelbeheer met bijbehorend uitgifte proces;
- In beheer name BSNk op basis van PP;
- Geschikt BSNk voor DigiD Hoog.

Inzagefunctie

Het geschikt maken van het BSNk voor registratie van nieuwe authenticatiemiddelen is randvoorwaardelijk voor de start van een grootschalige uitrol en gebruik van private en publieke middelen. Hiermee wordt de mogelijkheid geboden dat de burger daadwerkelijk met meerdere middelen kan inloggen bij dienstverleners in het BSN-domein (multi-middelenaanpak). Dit betekent ook dat de burger inzage moet hebben in zijn of haar middelen die hij gebruikt voor dit doel. Hiertoe is een Inzagefunctie nodig, die door Identiteitsverstrekkers wordt bijgewerkt wanneer een authenticatiemiddel wordt uitgegeven. Deze Inzagefunctie is, naast het geschikt maken van het BSNk, een tweede bouwsteen in het kader van de multi-middelenaanpak.

De Inzagefunctie verschaft de burger op een hoog beveiligd niveau inzage op de registratie en het gebruik van al zijn middelen. Daarnaast biedt de Inzagefunctie de mogelijkheid tot gerichte misbruik- en fraudebestrijding. De toepassing van de functionaliteiten moeten nog vanuit de werkgroep misbruik en fraudebestrijding nader worden vastgesteld.

Bij de ontwikkeling van deze Inzagefunctie zal de gebruiksvriendelijkheid voor burgers een centraal element zijn. De Inzagefunctie wordt gecreëerd om burgers transparantie, controle en dus comfort te bieden. De minister van BZK hanteert verder flankerend beleid voor minder digivaardigen om hen te betrekken bij technologische ontwikkelingen en mogelijkheden in de dienstverlenging.

De kosten voor ontwikkeling van de Inzagefunctie zijn in tabel 4.1 gepresenteerd.

DigiD Substantieel

Het doel is om voor DigiD een middel te introduceren en uit te rollen met eIDAS betrouwbaarheidsniveau substantieel (DigiD Substantieel) voor de personen met een NFC compatible smartphone. Vervolg is het onderzoeken en vervolgens implementeren van oplossingen voor burgers die niet in het bezit zijn van zo'n telefoon.

[36] Realisatie & Invoeringsplan, versie 0.99

De meerwaarde van DigiD Substantieel is dat alle burgers al in bezit zijn van een NIK, rijbewijs en/of paspoort (hoge dekkingsgraad) en dat burgers daardoor op relatief korte termijn de beschikking hebben over een publiek eID-middel op substantieel betrouwbaarheidsniveau.[37]

De investeringskosten qua stelselvoorzieningen voor DigiD Substantieel zijn in tabel 4.1 weergegeven en opgebouwd uit kosten voor:

- Aanpassingen aan de DigiD Kern (incl. koppeling met beide registers voor controle op actief document en ophalen sleutelgegevens);
- Aanpassingen aan de DigiD app (incl. ondersteuning beperkt aantal smart devices);
- BRP & Rijbewijsregister. Hier zijn vermoedelijk geen aanpassingen nodig, daarom zijn hier geen kosten voor opgenomen.

DigiD Hoog

De publieke middelen gaan gebruik maken van één authenticatiedienst. De bestaande authenticatiedienst van DigiD moet daarvoor worden uitgebouwd tot de authenticatiedienst voor de publieke middelen (Substantieel en Hoog). Als uitgangspunt hierbij is gehanteerd dat de functionaliteit van het publieke middel kan worden uitgeschakeld en/of aangepast zonder verstoring van de dienst DigiD. De authenticatiedienst voor DigiD kan vanaf 2018 niet alleen authenticaties van DigiD's afhandelen, maar ook authenticaties van publieke middelen (tegelijk).

In plaats van nieuwbouw/aanpassen van de bestaande DigiD-kern is ervoor gekozen om een Card Interface Server te bouwen om ervoor te zorgen dat de bestaande DigiD-authenticaties blijven draaien. De Card Interface Server is een component die als intermediair fungeert tussen de bestaande DigiD kern en het publieke middel. Daarnaast is een Card Test Server voorzien, een test voorziening voor burgers om de werking van het eID-middel te kunnen controleren en of hun PC geschikt is voor gebruik van het publieke eID-middel. De huidige oplossing met een CIS en CTS was nog niet in beeld bij het opstellen van de vorige business case.

Op dit moment is de DigiD authenticatiedienst geschikt voor het afhandelen van authenticaties voor de pilot. Er moet echter nog wel geïnvesteerd worden in het productierijp maken van de CIS en de CTS (om grote aantallen requests af te kunnen handelen). Daarnaast moet er nog een nieuwe release komen van de CIS en moet er nog hardening van de CIS komen. Hierdoor worden de mogelijkheden om het systeem te compromitteren verlaagd en ontstaat een maximale veiligheid.

Tot slot is er nog een extra functionaliteit in 'Mijn DigiD' voorzien zodat de gebruikers de gegevens van zijn middel kan bekijken en waarin hij zelf het middel (tijdelijk of definitief) kan deactiveren en een tijdelijke deactivering ongedaan kan maken. Ook deze voorziening was nog niet voorzien in de business case uit 2014.

[37] Het verdient nog wel de aanbeveling om het huidige uitgifteproces van WID-documenten 'eID-proof' te maken. Mogelijk moet het proces van de uitgifte en identiteitsvaststelling aan de voorkant versterkt worden. omdat er meer en nieuwe gebruiksmogelijkheden bijkomen van WID-documenten in het digitale domein.

In het Realisatie & Invoeringsplan zijn 4 projectdoelen geformuleerd voor DigiD Hoog, te weten:

- Oplevering van DigiD Hoog met het rijbewijs dat voldoet aan eIDAS Hoog op 1-1-2018, waarna uitgifte door gemeenten gaat plaatsvinden primair volgens het natuurlijke vervangingspatroon bij vervanging of aanschaf van een nieuw document door de burger;
- Oplevering van DigiD Hoog met de NIK die voldoet aan eIDAS Hoog in Q4 2018, waarna uitgifte door gemeenten gaat plaatsvinden primair volgens het natuurlijke vervangingspatroon bij vervanging of aanschaf van een nieuw document door de burger;
- Oplevering van een authenticatiedienst die alle bruikbare functies heeft;
- Ondersteuning van gemeenten bij de invoering van de van eID voorziene identiteitsdocumenten.

Impactanalyse Uitgifteproces publiek eID middel

Voor de laatste bullet geldt dat NVVB en KING in de *Impactanalyse Uitgifteproces publiek eID middel*[38] hebben aangegeven dat de uitgifte van het publiek eID-middel door gemeenten implementeerbaar en uitvoerbaar is. Wel wordt er expliciet aandacht gevraagd om samen met de betrokken partijen (Ministerie van BZK, NVVB, VNG, KING, gemeenten) het proces van aanvraag en uitgifte van een publiek eID-middel en de initiële ID-vaststelling te versterken. Waar in de autonome situatie na uitgifte nog met enig regelmaat face-to-face controle plaatsvindt omdat diensten dat vereisten, is dit niet noodzakelijk meer het geval na uitrol eID. In theorie hoeft iemand, na het verkrijgen van een eID, zich tien jaar lang niet 'opnieuw' te identificeren. Uitgaande van een goed proces is de kans op fraude klein, maar mocht er sprake zijn van identiteitsfraude dan kan de impact groot zijn.

Er is een aantal activiteiten en deliverables gedefinieerd, die dan wel solitair dan wel in gezamenlijkheid worden uitgevoerd respectievelijk opgeleverd. Zo vindt er een gezamenlijke ontwikkeling (ontwerp, aanbesteding, realisatie, voorbereiding van de invoering) plaats van de middelen en de authenticatiedienst door BZK, RvIG, RDW en Logius. Tevens wordt een aanbesteding voorzien van de applet en de middleware (in elk geval voor de NIK, voor rijbewijs afhankelijk van de uitkomsten van de marktconsultatie) in de periode juli 2016 tot en met mei 2017.

In tabel 4.1 zijn de investeringskosten voor DigiD Hoog weergegeven.[39] In navolging van eerder uitgevoerde pilots bij gemeenten vindt een nauwe samenwerking met beleid en gemeenten - en haar vertegenwoordigers NVVB en VNG - plaats ter voorbereiding op en uitvoering van de uitrol.

Invoeringskosten

In 2016 zijn er in het BSN-domein verschillende pilots van start gegaan met publieke en private middelen op hogere betrouwbaarheidsniveaus. Met de organisaties die meedoen aan de pilots is afgesproken dat zij bij positieve evaluatie en na besluitvorming in de Tweede Kamer deze dienstverlening kunnen continueren. In een tweede stap kunnen onder meer pilotdeelnemers en 'voorlopers' als eerste in het BSN-domein gebruik maken van de nieuwe inlogmethodes onder een eerste versie van de uniforme toelatingseisen.

Aansluitkosten dienstaanbieders

Alle overheidsdienstaanbieders moeten investeren om aan te sluiten op het eID-stelsel, zodat hun diensten toegankelijk worden voor publieke en private middelen op alle betrouwbaarheidsniveaus. In het verleden zijn er kosten gemaakt, zodat burgers DigiD kunnen gebruiken bij overheidsdienstaanbieders, maar deze koppelvlakken moeten worden aangepast zodat er ook met andere middelen toegang kan worden verkregen tot de digitale diensten van

---

38 NVVB & KING (2016). *Impactanalyse Uitgifteproces publiek eID-middel*.

39 Omdat het gesprek over de precieze taken en activiteiten van de gemeenten bij de uitgifte van een publiek eID middel nog niet is afgerond is het opgenomen bedrag de beste schatting die op dit moment beschikbaar is. Het kan op een later moment nog aan wijziging onderhevig zijn.

overheidsdienstaanbieders. Wij hebben voor de aansluitkosten bij dienstaanbieders daarom een Pro Memorie (PM-post) opgenomen.

4.2 Vaste kosten beheer en onderhoud stelselvoorzieningen

Naast de eenmalige investeringskosten moeten ieder jaar kosten worden gemaakt voor het beheer en onderhoud van de stelselvoorzieningen. Ten opzichte van de business case uit 2014 is de raming van de vaste beheer en onderhoudskosten verder uitgewerkt door Logius en BZK, maar het betreft nog steeds een indicatie.

Op basis van de input vanuit het Ministerie van BZK en Logius is een kostenindicatie afgegeven voor de vaste beheer- en onderhoudskosten (structurele kosten) van circa 36 miljoen euro per jaar. Deze kosten zijn opgebouwd uit kosten voor de authenticatiedienst (infra, doorontwikkeling en onderhoud etc.), kosten voor toelating, toezicht en beheer (en beheer USvE) en kosten voor BSNk + Inzageregister (beheer en exploitatie, doorontwikkeling en onderhoud). Verondersteld is dat de kosten voor communicatie onderdeel uitmaken van de vaste kosten ten behoeve van de authenticatiedienst. De kosten die samenhangen met het gebruik (bv. helpdesk) zijn in de volgende paragraaf beschreven. In de volgende tabel zijn deze kosten naast elkaar gezet.

Tabel 4.2 Vaste kosten beheer en onderhoud stelselvoorzieningen (bedragen in € mln.) [a)]

	Kosten per jaar [b)]
Authenticatiedienst	20
Toelating, toezicht en beheer	6
BSNk	10
Totaal	**36**

a) Informatie Logius, Deze raming is eerder ook opgenomen in *Bijlage I: Het kabinetsbeleid inzake (digitaal) inloggen nader toegelicht* bij de kamerbrief Impuls eID d.d. 25 augustus 2016 van de minister van BZK aan de Tweede Kamer.
b) In het jaar 2018 zijn de kosten voor BSNk niet gelijk aan € 10 mln. maar gelijk aan € 8 mln.

In aanvulling op deze jaarlijkse kosten moet er vijf jaar na de start (in 2023) eenmalig groot onderhoud worden gedaan voor de authenticatiedienst. Hiervoor is een bedrag van € 10 miljoen meegenomen in de berekeningen.

4.3 Investeringskosten middelen op betrouwbaarheidsniveau substantieel en hoog

Naast investeringen in het eID-stelsel moeten er ook middelen komen op eIDAS betrouwbaarheidsniveau substantieel en hoog. Daarvoor zijn er drie verschillende alternatieven:

- DigiD app. Hiermee krijgt de burger de beschikking over een publiek middel op eIDAS betrouwbaarheidsniveau substantieel.
- DigiD Hoog (eNIK of eRijbewijs). Hiermee krijgt de burger de beschikking over een publiek middel op eIDAS betrouwbaarheidsniveau hoog.
  - In aanvulling op het middel moet een deel van de burgers dan ook een kaartlezer aanschaffen.
- Private middelen zoals een bankpas en Idensys-middelen.

Wij lopen de investeringskosten voor de verschillende middelen hierna kort langs.

Investeringskosten DigiD app

Naast de investeringen in de stelselvoorzieningen (zoals bv. het bouwen van de DigiD app) zijn er geen aanvullende investeringen nodig om te kunnen beschikken over de DigiD app. Burgers

beschikken reeds over een DigiD, een NIK / rijbewijs / paspoort en de app is straks gratis te downloaden. Hiervoor hoeven dus nauwelijks aanvullend investeringskosten te worden gemaakt.

Investeringskosten eNIK / eRijbewijs

Voor het eNIK en het eRijbewijs is dit iets anders. Het eID wordt standaard op alle exemplaren van de NIK en het rijbewijs aangebracht.[40] Dit leidt tot extra productiekosten voor de chip. Daarnaast moeten er ook extra kosten gemaakt worden bij de uitgifte van de eNIK en het eRijbewijs.

Kosten eID-functionaliteit

In de volgende tabel zijn de extra kosten voor het toevoegen van de eID-functionaliteit opgenomen. De extra kosten voor de eID-functionaliteit (chip + applet + PIN/PUK brief) per WID-document bedragen € 2,04 voor het eRijbewijs en € 2,82 voor de eNIK. De cijfers en uitgangspunten zijn niet gewijzigd ten opzichte van de vorige business case.

Een mogelijk risico met gevolgen voor de kosten is de volgende. In deze business case is het startjaar 2018 i.p.v. 2017 zoals in de vorige business case. De aantallen uit te geven NIK's kende daarbij een piek in de jaren 2017 en 2018. Doordat 2017 (met relatief hoge aantallen) is weggevallen is het de vraag of het bovengenoemde bedrag voor de NIK nog steeds reëel is in combinatie met de minder goede mogelijkheden om de investeringen terug te verdienen via de uit te geven NIK's. Uit het gesprek met RDW is bijvoorbeeld gebleken dat de kosten per chip mogelijk iets hoger liggen. Er is nog onzekerheid over hoe de nieuwe chip er uit gaat, voor nu is uitgegaan van de kosten zoals bekend uit de oorspronkelijke business cases van de individuele middelen.

Daarbij is op dit moment niet duidelijk of en in hoeverre burgers tussentijds certificaten moeten vernieuwen op hun publieke eID-middel en zo ja, hoe dat moet worden georganiseerd. Dit moet nog nader uitgewerkt worden evenals de financiële consequenties hiervan.

Kosten uitgifte eID-middelen

Voor deze business case zijn wij uitgegaan van het beleidsuitgangspunt van het ministerie van BZK om zoveel mogelijk aan te sluiten bij het huidige aanvraag- en uitgifteproces van de middelen. Wij hebben dit (aansluiten bij huidige aanvraag- en uitgifteproces van de middelen) als een gegeven beschouwd voor de beoogde eindsituatie.

De baliemedewerker zal naar verwachting meer tijd kwijt zijn aan de uitgifte van het eID-middel dan aan de uitgifte van een regulier WID-document. Denk aan de uitleg van de baliemedewerker aan de burger dat hij nu ook een eID-functionaliteit heeft, waarom dit relevant is en hoe alles werkt (reader, eID-middel, installatiehandleiding, informatie over het gebruik van het middel). Er zijn nog geen uitgangspunten vastgelegd of er een dergelijke instructie komt en hoe deze instructie eruit komt te zien, maar het is denkbaar dat dit contactmoment met de burger wordt gebruikt om een nadere toelichting te geven. Dit moet ook in samenhang met de andere communicatie-uitingen worden vastgesteld.

In de pilots voor de publieke eID-middelen is ook gekeken naar de ervaringen bij het uitreiken van het eID-middel. Daarnaast is medio 2016 een impactanalyse voor publieke eID-middelen uitgevoerd.[41] Daarin is dit onderwerp ook meegenomen, maar is geen raming gemaakt van de extra tijdsbesteding. Uit het Adviesrapport van de Commissie Kuipers[42] is gebleken dat de pilots een sterk wisselend beeld laten zien in hoeverre de burger het installeren en activeren als lastig

---

40 Informatie Ministerie van Binnenlandse Zaken en Koninkrijksrelaties.

41 NVVB & KING (2016), *Impactanalyse Uitgifteproces publiek eID middel.*

42 Advies van de commissie evaluatie pilots publieke en private authenticatiemiddelen (commissie-Kuipers), 31 mei 2016

heeft ervaren en daarmee in hoeverre er extra toelichting gewenst is bij de uitgifte van het eID-middel.

Voor deze business case hebben wij daarom aangesloten bij de eerdere *Business case publieke eID-middelen*, waar is uitgegaan van een extra tijdsbesteding van 2 minuten en daarmee een extra kostenpost van € 2 per uitgegeven eNIK of eRijbewijs.[43] Het is overigens aan te raden[44] om dit nader uit te zoeken in de vorm van een impactanalyse en/of praktijkbeproeving bij gemeenten om scherp te krijgen hoeveel extra tijd er nodig is voor de instructie en uitleg over het publieke eID-middel en om te kijken of het uitgifteproces en de identiteitsvaststelling versterkt moet worden.

De kosten voor de uitgifte van de eID-middelen per jaar is daarbij afhankelijk van het natuurlijke vervangingspatroon van NIK's en rijbewijzen. Daarom is hier niet direct een jaarlijks cijfer te noemen. Ter illustratie hebben wij de cijfers voor verschillende jaren opgenomen evenals een totaalcijfer voor de gehele periode 2018 tot en met 2027. De extra kosten per jaar lopen uiteen van € 6,4 tot € 12,4 miljoen per jaar. Over de gehele periode van 2018 tot en met 2027 zijn de kosten gelijk aan circa € 106 miljoen, ofwel gemiddeld € 10,6 miljoen per jaar.

Tabel 4.3 Investeringskosten eNIK en eRijbewijs (bedragen in € mln.)

Kosten	2018	2020	2022	2024	Totaal [a)]
Kosten eID-functionaliteit	6,7	5,3	3,4	5,7	57,2
Kosten uitgifte eID-middelen	5,7	4,7	3,0	4,6	48,5
Totaal	**12,4**	**10,0**	**6,4**	**10,3**	**105,7**

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.

Investeringskosten kaartlezer

De chip op het publieke eID-middel kan op verschillende manieren worden uitgelezen. Dit kan door middel van een kaartlezer of door middel van NFC in combinatie met software op mobiele devices (laptop, tablet, smartphone).

In de vorige business case is ervan uitgegaan dat 50% van de gebruikers een kaartlezer nodig zal hebben en dat 50% gebruik zal maken van een NFC oplossing. Daarnaast is ervan uitgegaan dat een kaartlezer door gemiddeld 1,5 personen wordt gebruikt en dat de kosten voor een kaartlezer gelijk zijn aan € 10 per stuk.

Er zijn verschillende wijzigingen ten opzichte van de vorige business case. Zo beschikken steeds meer Nederlanders over een smartphone (81% van de Nederlanders van 18 tot 80 jaar) of een tablet (61% van de huishoudens).[45] Dat zijn er meer dan waarvan is uitgegaan bij het opstellen van de vorige business case. Het blijft enigszins lastig om hier een goede nieuwe schatting voor te maken, mede in verband met het onvoldoende bekend zijn van de percentages van die smartphones en tablets met een bruikbare NFC implementatie in de toekomst. Voor onze business case hebben wij daarom de berekeningen gelijk gelaten, waarbij wij wel de constatering maken dat deze kosten naar verwachting lager uit zullen vallen.

In de pilots voor de publieke eID-middelen zijn bedragen betaald van € 30 incl. btw voor een kaartlezer (na korting bij een afname van 1.500 stuks, de oorspronkelijk prijs was gelijk aan € 60 incl. btw). Het ging hier echter om een kaartlezer met veel extra functionaliteiten ten opzichte van

[43] Uitgaande van een baliemedewerker in functieschaal 8 zijn de kosten gelijk aan € 2 per uitgereikt document (uurtarief schaal 8 = € 61, *Handleiding Overheidstarieven 2016)*.

[44] Dit is ook een aanbeveling van de NVVB/

[45] Marketingfacts (2015), *Marketingfacts Jaarboek 2015-2016.*

de kaartlezer die nodig is voor het gebruik van een publiek eID-middel. Daarom hebben wij de prijs per kaartlezer niet naar boven bijgesteld en gerekend met een bedrag van € 10 per kaartlezer.

Per saldo variëren de kosten voor kaartlezers tussen de € 3 en € 6 miljoen per jaar in de periode van 2018 tot en met 2027. Gemiddeld zijn de kosten gelijk aan € 4,3 miljoen per jaar.

Investeringskosten private middelen

Burgers kunnen ook private middelen gebruiken om in te loggen in het BSN-domein. Hiervoor kan gedacht worden aan bankmiddelen (iDIN) of andere private middelen (o.a. Idensys). Het is op dit moment nog niet duidelijk welke private middelen er op de markt zullen komen en hoe hoog de kosten van deze middelen zijn voor de burger. Daarom zijn deze kosten als een PM-post opgenomen.[46]

Resumerend

In de volgende tabel hebben wij de investeringskosten in alle publieke middelen naast elkaar gezet. Over een periode van 10 jaar (2018 t/m 2027) zijn de kosten gelijk aan circa € 148 miljoen of € 14,8 miljoen per jaar. Daarbovenop komen de kosten voor de private middelen, die wij nog niet hebben kunnen ramen.

Tabel 4.4 Investeringskosten middelen (bedragen in € mln.)

Kosten	2018	2020	2022	2024	Totaal [a)]
DigiD Substantieel (DigiD app)	.	.	.	.	.
DigiD Hoog (eNIK / eRijbewijs)	12,4	10,0	6,4	10,3	105,7
Kaartlezer	5,4	4,7	2,9	3,7	42,6
Private middelen	PM	PM	PM	PM	PM
Totaal	**17,8**	**14,7**	**9,3**	**14,0**	**148,3**

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.

4.4 Variabele kosten gebruik

Naast de vaste beheer- en onderhoudskosten zijn er ook beheer- en onderhoudskosten die sterk samenhangen met het aantal gebruikers van eID-middelen en het aantal authenticaties. Het gaat hierbij onder meer om kosten die gemaakt moeten worden voor de helpdeskondersteuning en kosten, die gemaakt moeten worden als burgers hun pincode zijn vergeten en hun PIN/PUK brief zijn kwijtgeraakt.

[46] In het verlengde daarvan gaan private partijen kosten en baten maken voor het aanbieden van private middelen. Er is echter geen inzicht in de business cases van private partijen. Wel is het uitgangspunt logisch dat private partijen pas middelen gaan aanbieden op het moment dat zij hier een positieve business case aan over houden (immers, als de kosten voor private partijen hoger zijn dan de baten, dan is het verstandiger om geen middelen aan te gaan bieden). Als de kosten en baten van private partijen dan meegenomen zouden worden, dan zou de business case er alleen nog maar positiever uit komen te zien. Door deze niet apart te becijferen zitten wij met de maatschappelijke business case aan de conservatieve kant.

Tabel 4.5 Variabele kosten gebruik (in € mln.)

	2018	2019	2020	2021 en verder	Totaal
Brieven (heractivatie)	2,1	2,1	2,1	2,1	21,0
Externe helpdesk	3,0	3,0	3,0	3,0	30,0
SMS	2,75	3,0	3,3	0	9,1
BRP	2,4	2,4	2,4	1,2	15,6
Totaal	**10,25**	**10,5**	**10,8**	**6,3**	**75,7**

De variabele beheer- en onderhoudskosten zijn afhankelijk van het eerder gepresenteerde uitgiftetempo van eID-middelen en als gevolg daarvan het groeipad van gebruikers van een (publiek) eID-middel. Logius heeft hiervoor een globale inschatting gemaakt, waarbij de verwachting is dat de kosten voor sms na 2020 wegvallen, omdat als uitgangspunt is gehanteerd dat vanaf 2021 ten minste betrouwbaarheidsniveau substantieel moet worden gebruikt. Kosten voor raadpleging van het BRP zijn vanaf 2021 constant verondersteld.

De kosten voor de helpdesk zijn constant. Hoewel het gebruik en daarmee de bevragingen een grilliger verloop laten zien is de veronderstelling dat er tegelijkertijd een leereffect optreedt bij de gebruikers waardoor per saldo over een periode van tien jaar het aantal bevragingen voor ondersteuning gelijk blijven. De eerste jaren zijn de kosten gelijk aan ongeveer € 10 miljoen per jaar, vanaf 2021 zijn de kosten gelijk aan € 6,3 miljoen per jaar. Voor de gehele periode zijn de kosten gelijk aan € 7,5 miljoen per jaar.

4.5 Vaste kosten doorontwikkeling en beleidsvorming middelen

In deze business case hebben wij een raming gemaakt van de personele bezetting voor een organisatie die zich bezig gaan houden met deze doorontwikkeling en beleidsvorming aangevuld met informatie vanuit de RDW en RvIG. De hiervoor gepresenteerde kosten van doorontwikkeling zitten vooral bij Logius. De hieronder gepresenteerde organisatie betreft een indicatie van de kosten voor doorontwikkeling en beleidsvorming vanuit BZK, RDW en RvIG. In de volgende tabel is een overzicht opgenomen van de relevante functies bij de verdere doorontwikkeling en beleidsvorming van het publieke eID-middel.

Tabel 4.6 Functies en FTE organisatie voor doorontwikkeling en beleidsvorming publieke eID-middel

	Aantal FTE
Directeur	0,25
Ondersteuning	0,5
Business development (nieuwe toepassingen)	2
Vertegenwoordiger (externe commissies)	1
Legal / juridische zaken	1
Liaison Europese Unie	0.5
Totaal	**5,25**

Per saldo komen wij uit op een organisatie van ongeveer 5,25 FTE voor het ministerie van BZK. Als uit wordt gegaan van een gemiddeld niveau van schaal 11 / 12, dan zijn de kosten hiervoor ongeveer gelijk aan € 600 duizend per jaar. Het is daarbij de verwachting dat er ook 1 FTE nodig is vanuit het ministerie van I&M (voor het rijbewijs) voor ongeveer € 100 duizend per jaar. Daarnaast bedragen de kosten voor RvIG ongeveer € 500 duizend per jaar[47] en de kosten voor de RDW

[47] Informatie RvIG.

ongeveer € 150 duizend per jaar[48]. Per saldo komen de totale kosten voor doorontwikkeling en beleidsvorming van het publieke eID-middel dan uit op een bedrag van ongeveer € 1,35 miljoen per jaar.

4.6 Totale kosten

In de volgende tabel is het totaalbeeld opgenomen van de kosten. Hierbij zijn investeringskosten in de periode 2015 tot 2018 naast de jaarlijkse kosten voor de periode 2018 t/m 2027 gezet. Dat resulteert in een totaaloverzicht van de te maken kosten over een periode van 13 jaar. Voor de gehele periode zijn de kosten gelijk aan € 658,8 miljoen.[49] Naast eenmalige investeringskosten van € 53,2 miljoen moet er ieder jaar gemiddeld - als we alle kosten voor de overheid en burgers bij elkaar optellen - voor € 60,5 miljoen worden uitgegeven om inloggen met middelen op betrouwbaarheidsniveau substantieel en hoog mogelijk te maken in het BSN-domein.

Tabel 4.7: Kosten totaal (bedragen in € mln.)

Kostenpost	Investeringskosten (2015-2018)	Gemiddelde kosten per jaar in beheerfase (2018-2027)	Kosten totaal [a)]
Investeringskosten stelselvoorzieningen	53,2		53,2
Vaste kosten beheer en onderhoud stelselvoorzieningen		36,8	368,0
Investeringskosten middelen op betrouwbaarheidsniveau substantieel en hoog		14,8	148,3
Variabele kosten gebruik		7,6	75,7
Vaste kosten doorontwikkeling en beleidsvorming middelen		1,4	13,5
Totaal	**53,2**	**60,5**	**658,8**

a) Het gaat hier om de kosten over de periode van 2015 t/m 2027.

48 Informatie RDW, Business case eRijbewijzen,

49 Aangezien gerekend wordt met een risicovrije discontovoet van 0% voor de kosten is de reële waarde van de kosten gelijk aan de contante waarde van de kosten. Voor de baten is overigens gerekend met een risico-opslag van 3% boven op de risico-vrije discontovoet van 0%. Wij hebben hier de standaard richtlijnen gevolgd, die te vinden zijn op https://staticresources.rijkswaterstaat.nl/binaries/Vragen%20en%20antwoorden%20rondom%20de%20nieuwe%20regels%20voor%20disconteren_tcm21-82362.pdf.

5 De baten van het eID-stelsel

In dit hoofdstuk zijn de baten van het eID-stelsel nader uitgewerkt. Wij starten het hoofdstuk met een inventarisatie van de baten van het eID-stelsel. In de tweede paragraaf hebben wij de te kwantificeren baten verder uitgewerkt en in de derde paragraaf hebben wij becijferd wat de orde van grootte van de minder goed te kwantificeren baten zou moeten zijn om ervoor te zorgen dat de business case in evenwicht is.

5.1 Inventarisatie van de baten

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 werken wij deze verder uit.

Digitale dienstverlening en authenticatie met DigiD

In 2016 wordt er 263 miljoen keer ingelogd met DigiD (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.[50]
- Het Forum Standaardisatie heeft een handreiking[51] 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 hoofdstuk 4 hebben wij 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 er uit komt te zien, er moeten kosten voor digitale authenticaties worden gemaakt. In kosten-batenanalyses

[50] 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.

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

spreekt men hier van kosten van het nulalternatief of vermeden kosten van het projectalternatief.[52] 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 tijdsonafhankelijk en plaatsonafhankelijk 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 private middelen ook een publiek middel beschikbaar te stellen.[53]

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

---

[52] 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.

[53] 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.

5.2 Te kwantificeren baten

In de vorige paragraaf zijn de verschillende baten naast elkaar gezet. Slechts een deel van deze baten zijn goed te kwantificeren en de baten die te kwantificeren zijn hebben wij in dit hoofdstuk beschreven. De te kwantificeren baten hebben het karakter van zogenaamde vermeden kosten. Het gaat dan om vermeden kosten van de authenticatiedienst DigiD en te vermijden kosten van alternatieve passen. Hierna worden de verschillende baten naast elkaar gezet.

Vermeden kosten authenticatiedienst DigiD

Ook als er geen eID-stelsel is met middelen met betrouwbaarheidsniveau substantieel en hoog, moeten er kosten worden gemaakt om de authenticatiedienst voor DigiD in de lucht te houden. Voor het jaar 2017 zijn de kosten van de authenticatiedienst geraamd op € 24,0 miljoen per jaar.[54] Wij zijn er in onze analyse vanuit gegaan, dat deze kosten in de jaren daarna gelijk blijven.[55] Over de gehele periode van 2018 tot en met 2027 zijn deze kosten gelijk aan € 240 miljoen (met een contante waarde van € 187,4 miljoen.[56]

Voor een goede vergelijking in de onderstaande tabel zijn de jaarlijkse kosten van de authenticatiedienst voor DigiD naast de jaarlijkse kosten van de authenticatiedienst voor alle eID-middelen gezet. De huidige kosten bedragen € 24,0 miljoen per jaar. De kosten voor een authenticatiedienst voor alle middelen zijn gelijk aan € 26,3 miljoen per jaar. Enerzijds is er een stijging van de kosten per jaar door de extra functies van de authenticatiedienst (multi-middelen), anderzijds is er een daling van de kosten per jaar in de variabele kosten van het gebruik (afname van het aantal te versturen sms-berichten[57] en afname van de BRP-bevragingen). Per saldo zijn de kosten voor de authenticatiedienst voor eID-middelen vanaf 2021 € 2,3 miljoen per jaar duurder dan de huidige authenticatiedienst.

Tabel 5.1 Jaarlijkse kosten authenticatiedienst DigiD & authenticatie eID vanaf 2021 (in € mln.)

Kosten	Authenticatiedienst DigiD	Authenticatiedienst eID (substantieel + hoog)	Extra kosten projectalternatief
Authenticatiedienst	14,0	20,0	6,0
Variabele kosten gebruik	10,0	6,3	-3,7
Totaal	**24,0**	**26,3**	**2,3**

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.

Vermeden kosten alternatieve authenticatiesystemen

Naast DigiD zijn er nog andere oplossingen voor elektronische identificatie en toegang tot digitale diensten, zoals verschillende bestaande passen voor authenticatie. Deze alternatieve authenticatieoplossingen worden overbodig wanneer de publiek eID-middel beschikbaar komt. In de wereld zonder publiek eID-middel (het nulalternatief) moeten proceseigenaren hun eigen

---

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

55 Naarmate de kosten van de huidige authenticatiedienst voor DigiD in de toekomst verder gaan stijgen, wordt het alternatief (investeren in een eID-stelsel met middelen op betrouwbaarheidsniveau substantieel en hoog) alleen maar aantrekkelijker. Het hanteren van gelijkblijvende kosten in het nulalternatief is daarmee dus een conservatief uitgangspunt.

56 Voor de baten is conform de daarvoor geldende richtlijnen gerekend met een risico-opslag van 3% boven op de risico-vrije discontovoet van 0%. De standaard richtlijnen gevolgd zijn te vinden op https://staticresources.rijkswaterstaat.nl/binaries/Vragen%20en%20antwoorden%20rondom%20de%20nieuwe%20regels%20voor%20disconteren_tcm21-82362.pdf.

57 Deze afname van de kosten is er overigens pas vanaf 2021 (zie ook tabel 4.5) als DigiD Midden is uit gefaseerd en er alleen nog maar authenticaties op betrouwbaarheidsniveau substantieel zijn.

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 hebben wij de te besparen baten van de UZI-pas voor de gebruiker doorgerekend als deze vervangen worden door een publiek of privaat middel met betrouwbaarheidsniveau hoog. De kosten voor een UZI-pas zijn gelijk aan € 255 voor een periode van 3 jaar.[58] Er zijn op dit moment circa 90.000 UZI-passen in omloop. Voor de berekening van de baten zijn wij uitgegaan van een stabiel aantal UZI-passen van 90.000 die iedere 3 jaar vervangen moeten worden. Deze kosten hebben wij naast de kosten gezet waarbij alle 90.000 zorgprofessionals met een UZI-pas in 2021[59] een privaat middel of een eNIK aanschaffen voor € 57,77 (zijnde € 52,95 voor de NIK en € 4,82 voor de extra e-functionaliteit) met een geldigheid van 10 jaar. Dit leidt tot een kostenbesparing van € 7,7 miljoen per jaar vanaf 2022.

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 advocatenpas[60] en diverse stadspassen. In beginsel kunnen allerlei andere passen worden uitgefaseerd en vervangen door eID-middelen. Wij hebben in deze paragraaf ter illustratie een voorbeeld gepresenteerd en 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.

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 € 288,3 miljoen, de contante waarde van deze baten is gelijk aan € 223,0 miljoen.

---

58 http://www.uziregister.nl/uzipas/kosten/. 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.

59 Er is op dit moment een aanbesteding voor nieuwe UZI-passen voor de komende drie jaar. De UZI-pas kan daarom pas vanaf 2021 worden vervangen door middelen met betrouwbaarheidsniveau hoog.

60 Zie bijvoorbeeld: https://www.advocatenorde.nl/3837/advocaten/update-advocatenpas.

Tabel 5.2: 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	187,4
Vermeden kosten alternatieve authenticatiesystemen	48,3	35,6
Totaal	**288,3**	**223,0**

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).

5.3 Bepaling van het break-even point

In de eerste paragraaf is aangegeven dat de belangrijkste redenen van het eID-stelsel met middelen op betrouwbaarheidsniveau substantieel en hoog liggen in de ***betere veiligheid*** (minder fraude), ***betere compliance van overheden*** en ***betere dienstverlening aan burgers***. Vanwege diverse redenen is het echter lastig om deze baten goed te becijferen. Om toch een beter gevoel te krijgen bij de mate waarin de business case positief uit zal vallen hebben wij voor een alternatieve aanpak gekozen.

Wij hebben gekeken hoeveel fraude er zou moeten worden voorkomen om ervoor te zorgen dat de business case in evenwicht is. Tevens hebben wij gekeken hoeveel digitale authenticaties er op betrouwbaarheidsniveau hoog zouden moeten zijn, waarbij de voordelen van deze authenticaties voor de burgers zo groot zijn dat de business case eveneens in evenwicht is. En dan is het ook mogelijk om combinaties te maken van beiden (minder fraude in combinatie met meer digitale authenticaties op betrouwbaarheidsniveau hoog).

Er zijn namelijk kengetallen beschikbaar van de maatschappelijke schade per fraudegeval en ook van de tijd die burgers kunnen besparen wanneer overheidsdiensten digitaal kunnen worden afgehandeld in plaats van op papier of fysiek (bezoek aan de overheidsdienstverlener). Zo blijkt dat de maatschappelijke schade van een fraudegeval ongeveer gelijk is aan € 40.000 per fraudegeval.[61]

Uit eerdere studies komt een gemiddelde tijdsbesteding van een burger bij een papieren transactie van 25 minuten naar voren, terwijl een digitale transactie de burger slechts 10 minuten kost.[62] Het doen van een digitale transactie in plaats van een papieren transactie levert voor burgers een tijdwinst van gemiddeld 15 minuten op. Uitgaande van het uurtarief voor burgers van € 15 zijn de baten per transactie gelijk aan € 3,75.[63]

Hiermee is te bepalen hoe groot de afname van de identiteitsfraude (als proxy voor de toegenomen veiligheid) en de afname van het aantal papieren contacten dat mogelijk wordt door een middel op betrouwbaarheidsniveau hoog (als proxy voor het gebruiksgemak voor burgers) moeten zijn om een break-even business case te krijgen.

---

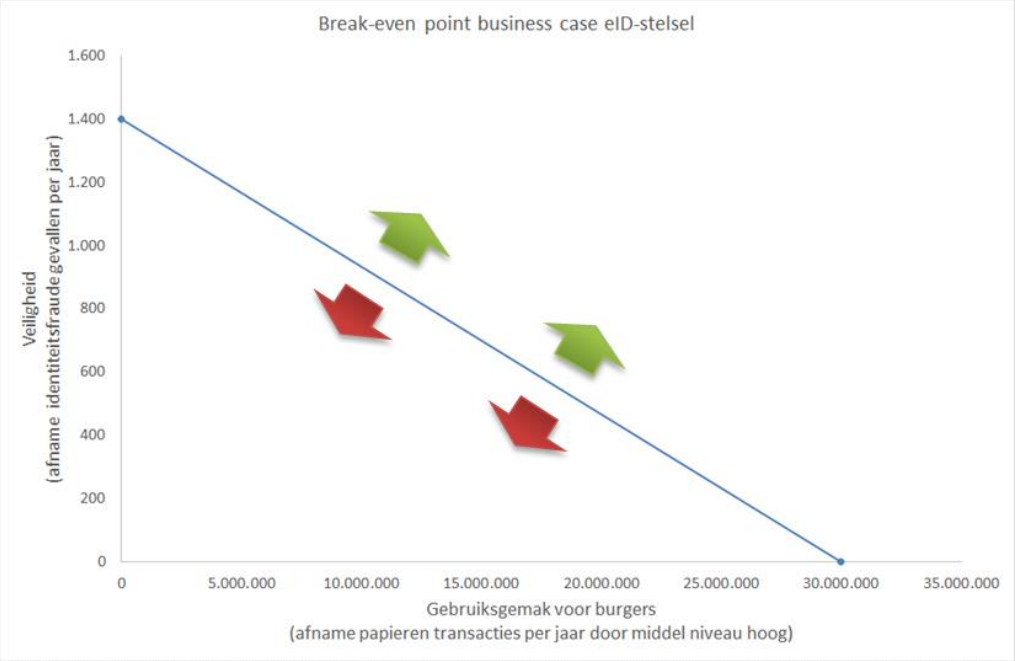
61 In de kamerbrief (Tweede Kamer der Staten-Generaal (2001-2002), *17 050 nr. 234 Misbruik en oneigenlijk gebruik op het gebied van belastingen, sociale zekerheid en subsidies*) is een bedrag van € 36.300 genoemd als potentieel benadelingsbedrag per vals of vervalst document. Dit cijfer is gebaseerd op ervaringscijfers van de Centrale Recherche Informatiedienst (CRI). Het ligt in de lijn der verwachting dat het benadelingsbedrag van een vals of vervalst document vergelijkbaar is met het benadelingsbedrag van een vals eID. Rekening houdend met inflatie resulteert dan een bedrag van € 40.000 per fraudegeval,

62 Zie bijvoorbeeld Ecorys & Van Zutphen Economisch Advies (2011), *MKBA eHerkenning*.

63 Deze besparing wordt zelfs nog groter wanneer de vergelijking tussen een digitale transactie en een fysieke transacties (bv. bezoek aan een balie of een arts). Wij hebben echter conservatief gerekend en zijn daarom uitgegaan van een potentiele besparing van 15 minuten.

In de volgende figuur is het resultaat hiervan[64] te zien, als het aantal gevallen van identiteitsfraude afneemt met ongeveer 1.400 per jaar, dan is het resultaat van de business case gelijk aan 0. Ook is te zien dat de business case op 0 uitkomt, wanneer er 30 miljoen transacties per jaar[65] dankzij een middel met betrouwbaarheidsniveau hoog digitaal kunnen worden afgehandeld in plaats van op papier. De business case komt eveneens op 0 uit bij alle andere punten op de curve in de figuur (dus bv. ook bij 700 gevallen minder identiteitsfraude en bij 15 miljoen minder papieren transacties). De business case is dus positief boven de blauwe lijn en negatief eronder.

Figuur 5.1 Break-even point business case eID-stelsel



In hoofdstuk 3 hebben wij een nadere duiding van deze cijfers gemaakt.

64 Hiervoor hebben wij de contante waarde van de kosten naast de contante waarde van de baten gezet.

65 Het gaat hier om 30 miljoen transacties in het eindbeeld. Hierbij is er ook rekening gehouden met het groeipad van middelen.

Bijlage 1: DigiD Hoog proces en gebruik

Onderstaande stappen geven het proces van aanvraag, productie tot uitgifte van DigiD Hoog Middel (eNIK of eRijbewijs), zoals beschreven in de PSA DigiD Hoog.

1. Als eerste stap dient de burger een aanvraag in voor NIK of rijbewijs. Hiertoe gaat de burger fysiek naar het aanvraagloket, in de meeste gevallen bij de gemeente. Bij de gemeente wordt onder meer de identiteit gecontroleerd en of alle gegevens voor een aanvraag aanwezig zijn.
2. Als alles goed is, wordt er vanuit de gemeente een aanvraag voor het produceren van een NIK of rijbewijs naar de Middelenverantwoordelijke verzonden. De Middelenverantwoordelijke voor de NIK is de Rijksdienst voor IdentiteitsGegevens (RvIG) en voor het rijbewijs de Rijksdienst voor het Wegverkeer (RDW). De Middelenverantwoordelijke zal het fysieke document produceren en voorzien van de persoonlijke gegevens van de aanvrager (personaliseren). Nieuw is dat de Middelenverantwoordelijke in de chip een DH middel zal plaatsen en dat DH middel ook zal personaliseren.
3. Hiervoor haalt de Middelenverantwoordelijke een (polymorf) pseudoniem op bij BSN koppelregister (BSNk). Het BSNk is een nieuwe component die een BSN van een burger koppelt aan een (polymorf) pseudoniem. Het (polymorf) pseudoniem wordt vervolgens in het DH middel geplaatst.
4. Het document met daarop het DH middel zal vervolgens naar het uitgifteloket worden verstuurd.
5. Als de burger het document ophaalt, zal er ook een toelichting worden meegegeven over het activeren en het gebruik van het DH middel.
6. Op het moment dat de gemeente de uitreiking van het document vastlegt, gaat er een signaal naar de Middelenverantwoordelijke.
1. Dit signaal is voor de Middelenverantwoordelijke het teken dat er een brief (PIN-mailer) naar de burger moet worden gezonden waarin de persoonlijke PIN staat waarmee de burger het DH middel kan activeren.
7. De activering vindt plaats bij DigiD via het zelfserviceportaal Mijn DigiD. Hierbij dient de burger een eigen PIN in te stellen. De burger kan na de activering het middel gaan gebruiken om toegang te verkrijgen tot diensten van overheidsinstanties, zorgverzekeraars, zorgaanbieders, pensioenfondsen en onderwijsinstellingen of andere private partijen met een publieke taak.

(Bron: *Projectstartarchitectuur DigiD Hoog, Identificeren en authenticeren met je identiteitskaart of rijbewijs.* Versie 1.0, 29 september 2016)

Onderstaande stappen geven het gebruik van het DH middel weer. De burger wil inloggen op een website van een Dienstverlener (DV) waarbij de burger aangeeft gebruik te willen maken van een DH middel op NIK of rijbewijs:

1. De dienstverlener stuurt de burger via DigiD naar de DigiD Hoog Authenticatiedienst (DH Authenticatiedienst) om zich te authenticeren.
2. De burger gebruikt daarvoor de smartphone met de DigiD app als kaartlezer en wordt gevraagd de PIN in te voeren.
3. Als de PIN invoer juist is, zal het DH middel het (polymorf) pseudoniem aan de DH Authenticatiedienst afgeven. Aan de hand hiervan controleert de DH Authenticatiedienst bij de DigiD Hoog Status Controller (DH SC) of het DH middel actief is en niet geblokkeerd of ingetrokken.
4. Als het middel actief is en alle controles positief waren, zal de DH Authenticatiedienst een (pseudonieme) identiteitsverklaring aan de DV afgeven. De DH Authenticatiedienst kan hieruit zelf niet opmaken wat de identiteit van de burger is. Die identiteit (BSN) kan alleen door de

ontvangende DV worden bepaald aan de hand van de (pseudonieme) identiteitsverklaring. Vervolgens zal de DH Authenticatiedienst de transactie in naar de DH Transactielog (DH TL) wegschrijven.

5. Ten slotte zal de burger worden teruggeleid naar de DV en kan de burger de gevraagde dienst afnemen.

(Bron: Projectstartarchitectuur DigiD Hoog, Identificeren en authenticeren met je identiteitskaart of rijbewijs. Versie 1.0, 29 september 2016)

Bijlage 2: Onderzoek betrouwbaarheidsniveau patiëntenauthenticatie bij elektronische gegevensuitwisseling

Voorbeelden van authenticaties op het eIDAS betrouwbaarheidsniveau substantieel en hoog:

A. Een patiënt controleert zijn inschrijvingsgegevens bij een zorgaanbieder (NAW gegevens die geen betrekking hebben op zijn gezondheid).

We onderscheiden twee scenario's vanwege de vraagstelling:

- Inschrijfgegevens die – ook in combinatie met de gegevens van de zorgaanbieder - niets zeggen over de gezondheidssituatie van de patiënt en waarbij ook geen inzage is in het BSN.
- Inschrijfgegevens inclusief het BSN en inzicht in het specialisme van de zorgaanbieder. De gegevens vallen in alle gevallen wel onder het medisch beroepsgeheim van de zorgverlener.

Conclusie: In scenario 1 wordt minimaal betrouwbaarheidsniveau substantieel (en STORK 3) en in scenario 2 niveau hoog (en STORK 4) passend geacht.

B. Een patiënt wijzigt zijn inschrijvingsgegevens bij een zorgaanbieder (NAW gegevens die geen betrekking hebben op zijn gezondheid).

Ook in deze use case bepaalt het verschil in de soort te wijzigen gegevens, zoals deze bij use case A zijn onderscheiden in scenario 1 en 2, alsmede de koppeling daarvan aan het zorgdossier, het verlangde betrouwbaarheidsniveau. Wij verwachten daarvoor hetzelfde niveau als bij use case A.
Conclusie: In scenario 1 wordt minimaal niveau substantieel (en STORK 3) en in scenario 2 niveau hoog (en STORK 4) passend geacht.

C. Een patiënt maakt/wijzigt een afspraak met de zorgverlener (bijvoorbeeld voor het spreekuur of een onderzoek).

In aansluiting op use case A1 zou het enkele feit van een afspraak met een algemene zorgaanbieder, zoals een huisarts of tandarts geen gezondheidsgegevens hoeven te bevatten. De afspraakgegevens vallen wel onder het beroepsgeheim van de arts.
Conclusie: In een situatie vergelijkbaar met het scenario onder A.1 is niveau substantieel (en STORK 3) passend en in een situatie vergelijkbaar met scenario A.2 is betrouwbaarheidsniveau hoog (en STORK 4) passend, afhankelijk van de soort te wijzigen gegevens.

D. Een patiënt raadpleegt zijn medisch dossier bij de hulpverlener (bijvoorbeeld zijn huisartsdossier, laboratoriumuitslagen, beeldverslagen of medicatie).

In deze casus is het (gehele) medisch dossier zichtbaar en is er dus geen twijfel over de vraag of er sprake is van gezondheidsgegevens, inzage in het BSN en toepasselijkheid van het medisch beroepsgeheim.
Conclusie: betrouwbaarheidsniveau hoog (eIDAS), dan wel STORK 4 wordt passend geacht.

E. Een patiënt maakt aanvullingen op zijn medisch dossier (bijvoorbeeld door het toevoegen van resultaten van zelfmetingen van parameters zoals bloedsuikerspiegel, bloeddruk, gewicht).

Het muteren van het medisch dossier brengt meer risico's met zich mee dan alleen inzage.
Conclusie: Betrouwbaarheidsniveau hoog eIDAS / STORK 4 wordt passend geacht.

F. Een patiënt vraagt een herhaalrecept aan

De manier waarop de mogelijkheid wordt geboden maakt verschil in of de verwerking bij de zorgaanbieder begint of bij de patiënt. Het gaat om een het verwerken van een beperkte

hoeveelheid gezondheidsgegevens. Er is geen twijfel over de vraag of er sprake is van het verwerken van gezondheidsgegevens, verwerken/inzien van het BSN en toepasselijkheid van het medisch beroepsgeheim op de gegevens die verwerkt worden.
Conclusie: Betrouwbaarheidsniveau hoog eIDAS / STORK 4 wordt passend geacht.

Bijlage 3: Geraadpleegde bronnen

Hieronder zijn de geraadpleegde bronnen weergegeven, naast de gevoerde interviews en mailwisselingen.

Bronnen
Rijks ICT Dashboard 2015
Realisatie en Invoeringsplan / Agendapunt 5 20160925 R&I Plan versie 099 dd
Berekeningen Ecorys i.h.k. van Input Wet GDI
Business case Ecorys maart 2016 en 2014
Verkenning RDA (Ecorys)
Forum Standaardisatie (2014), Betrouwbaarheidsniveaus voor authenticatie bij elektronische overheidsdiensten (versie 3). Een handreiking voor overheidsorganisaties.
Ecorys & Van Zutphen Economisch Advies (2014), Business Case eNIK
http://www.uziregister.nl/uzipas/kosten/
https://www.advocatenorde.nl/3837/advocaten/update-advocatenpas
Ecorys & Van Zutphen Economisch Advies (2011), MKBA eHerkenning
Ecorys & Conict (2007), Handreiking voor kosten-batenanalyse voor ICT projecten
NVVB & KING (2016). Impactanalyse Uitgifteproces publiek eID-middel.
Projectstartarchitectuur DigiD Hoog, Identificeren en authenticeren met je identiteitskaart of rijbewijs. Versie 1.0, 29 september 2016
Onderzoek betrouwbaarheidsniveau patientenauthenticate bij elektronische gegevensuitwisseling zorg-versie 0 14 finaalcon.

Overzicht geïnterviewde personen

Naam	Instantie
Mariëlle Slooff	NVVB
Carlo Luijten	Min. Binnenlandse Zaken en Koninkrijkrelaties
Corien Pelsrijcken	Min. Binnenlandse Zaken en Koninkrijkrelaties
Dirk Schravendeel	PBLQ
Evelina de Valk	Min. Binnenlandse Zaken en Koninkrijkrelaties
Eveline O'Brien	Logius
Jaap Verhagen	Logius
Noortje Verheij	Logius
Matthijs Claessen	Logius
Cynthia Henskens-Mathijssen	RvIG
Jetske ten Brug	RDW
Auke van der Meulen	RDW
Jacob Moehn	Ministerie van Volksgezondheid, Welzijn en Sport
Marco van der Steeg	Ministerie van Volksgezondheid, Welzijn en Sport
Margreet Lont van Gelder	Ministerie van Volksgezondheid, Welzijn en Sport

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

W www.ecorys.nl

Sound analysis, inspiring ideas