Bijlage I: Het kabinetsbeleid inzake (digitaal) inloggen nader toegelicht

Huidige situatie

Ruim 10 jaar geleden heeft het kabinet voor de digitale toegang tot de dienstverlening in het BSN-domein voor natuurlijke personen DigiD geïntroduceerd en voor rechtspersonen korte tijd later DigiD voor bedrijven. De essentie van het beleid was door standaardisatie op één infrastructuur met één inlogmiddel voor de dienstverlening in het BSN-domein de digitalisering van deze dienstverlening vleugels te geven. Dit beleid is zeer succesvol geweest.

Doorslaggevend voor de adoptie van DigiD was het besluit van de Belastingdienst dat digitaal doen van de aangifte inkomstenbelasting vanaf 1 januari 2007 alleen nog met DigiD mogelijk was. Vanaf dat moment zijn de ontwikkelingen, ook in internationale vergelijking, pijlsnel gegaan en dat heeft Nederland op dit terrein een koppositie in de wereld bezorgd. Bij grote uitvoeringsinstanties als de Belastingdienst, het UWV of DUO verloopt de bulk van de klantcontacten inmiddels voor ruim meer dan 95% digitaal. Maar in veel bredere zin wordt steeds meer dienstverlening in het BSN-domein inmiddels plaats- en tijdonafhankelijk digitaal afgedaan, met alle gemak en kostenbesparing van dien voor zowel klant als dienstverlenende instantie. Dit heeft geleid tot een exponentiële volumegroei van inloggen, die in alle prognoses de komende jaren onverminderd doorgaat. DigiD wordt inmiddels door ruim 12 miljoen mensen al meer dan 200 miljoen keer per jaar gebruikt voor een nog steeds groeiende variëteit van diensten van honderden zowel overheidsorganisaties als andere organisaties met een publieke taak in het BSN-domein. DigiD voor bedrijven is nooit echt van de grond gekomen. Op initiatief van de minister van EZ is daarom een aantal jaar geleden voor inloggen door rechtspersonen een alternatieve aanpak ontwikkeld. Onder de naam eHerkenning is een publiek-privaat afsprakenstelsel gemaakt, waarbinnen inmiddels diverse onder dit merk erkende private oplossingen operationeel zijn voor een gestaag groter aantal situaties waarin bedrijven digitaal zaken doen met de overheid, met hun consumenten en met elkaar.

De enorme vlucht die digitale dienstverlening in het BSN-domein in ons land heeft genomen en blijft nemen, verplicht tot onophoudelijk en met voorrang verder investeren in de infrastructuur voor (digitaal) inloggen. Dit investeren beziet het kabinet in het licht van de samenloop van de onstuimig in ontwikkeling blijvende technologie en de steeds nieuwe toepassingen die voor deze technologie ontstaan enerzijds en het voortdurend grimmiger dreigingsbeeld waar het gaat om de borging van continuïteit en veiligheid van de digitalisering anderzijds. Toegespitst op het Nederlandse publieke domein impliceren deze trends, dat er met name waar het gaat om inloggen door natuurlijke personen met DigiD twee hoofdpunten zijn die noodzaken tot een koerswijziging van het tot nu gevoerde doorontwikkel beleid. In de eerste plaats betekent de groeiende afhankelijkheid van digitalisering dat steeds zwaardere eisen worden gesteld aan de permanente beschikbaarheid van de DigiD infrastructuur, die inmiddels alom wordt gezien als onderdeel van de vitale infrastructuur van ons land. In de tweede plaats worden ook steeds zwaardere eisen gesteld aan de veiligheid van het middel DigiD. Kwaadwilligen blijven voortdurend nieuwe mogelijkheden zoeken om digitale identiteiten te stelen of te vervalsen of om anderszins infrastructuren daarvoor te ondermijnen. Daar weerbaar tegen zijn en blijven klemt te meer, omdat onder invloed van zowel de technologische ontwikkelingen als de wens tot betere dienstverlening en verdere kostenbesparingen er tegelijk steeds nieuwe digitale transacties in zwang komen, waarbij de gevolgen van corrumpering

van digitale identiteiten steeds ernstiger kunnen zijn vanuit bijvoorbeeld het oogpunt van privacybescherming. Middelen met een hogere beveiliging zijn noodzakelijk.

Een voorbeeld van wat met dit laatste concreet wordt bedoeld, vormt het recente onderzoek naar het betrouwbaarheidsniveau voor patiëntauthenticatie bij elektronische gegevensuitwisseling in de zorg[1]. Dit onderzoek onderschrijft het belang van betrouwbaarder inlogmiddelen en stelt dat minimaal niveau substantieel eIDAS nodig is. Als het gaat om gegevens waarop het medisch beroepsgeheim van de zorgverlener rust is het hoogste betrouwbaarheidsniveau (hoog eIDAS) vereist.

Multimiddelenaanpak

De multimiddelenaanpak waartoe het kabinet thans definitief heeft besloten richt zich op die situaties waarvoor tot nu toe alleen DigiD mag worden gebruikt. Dat wil zeggen dat de strategie ziet op inloggen door iedereen die DigiD gebruikt op de digitale dienstverlening van overheidsorganisaties en andere organisaties die gerechtigd zijn het burgerservicenummer te gebruiken. Deze mensen krijgen (i) de vrijheid om zelf uit meerdere door de overheid erkende inlogmiddelen te kiezen en (ii) daarbij de beschikking over ook hoger beveiligde middelen dan tot nu toe voor toekomstige informatie-uitwisselingen waarvoor dat is vereist. Voor authenticatie van niet-natuurlijke personen zijn en blijven er daarnaast de ook thans al beschikbare eHerkenning inlogmiddelen.

De multimiddelenaanpak heeft als doelstelling: het tot aanvaardbare proporties terugbrengen van de afhankelijkheid van DigiD door het grootschalig introduceren van meerdere inlogmiddelen naast DigiD die tezamen wat betreft borging van continuïteit en beveiliging kunnen blijven meegroeien met de generatie(s) toepassingen die we tegemoet gaan. Het kabinet stapt daarmee af van het erkennen van alleen DigiD als enig inlogmiddel voor alles. Het kabinet wil dat er in de toekomst voor iedereen meerdere inlogmiddelen/-methoden van meerdere leveranciers naast elkaar beschikbaar zijn, waarmee ze bij alle dienstverleners in het BSN-domein terecht kunnen. Zo wordt voorkomen dat de hele dienstverlening stokt met alle maatschappelijke ontwrichting van dien wanneer er sprake is van een - nooit helemaal uit te sluiten - serieuze storing of een - eveneens nooit helemaal uit te sluiten - hack. Meerdere inlogmiddelen van meerdere leveranciers hebben bovendien als voordeel dat meerdere technologieën naast elkaar worden gebruikt. Dat betekent ook vanuit dat gezichtspunt een reductie van kwetsbaarheid. Het heeft tegelijk als voordeel dat er meer ruimte ontstaat voor snelle introductie van nieuwe technologische innovaties.

Het kabinet heeft met genoegen kennis genomen van de conclusie uit de recente evaluatie van de pilots, dat deze zogeheten multimiddelenstrategie van meerdere inlogmiddelen naast elkaar - mits zorgvuldig stap voor stap doorgevoerd - in de praktijk goed blijkt te kunnen werken voor de doelgroep waarvoor hij is bedoeld. In de pilots is met een steekproef van deelnemers geëxperimenteerd met diverse zowel publieke als private middelen, waarmee mensen kunnen inloggen op websites van dienstverleners in het zogeheten BSN-domein[2]. Bij private inlogmiddelen moet worden gedacht aan middelen die mensen ook gebruiken voor bijvoorbeeld kopen bij webwinkels of internet bankieren. Bij publieke middelen komen er, conform ook de wens van uw

[1] Onderzoek betrouwbaarheidsniveau patiëntauthenticatie bij elektronische gegevensuitwisseling in de zorg.
[2] BSN-domein of publiek domein: dienstverlening door overheden en andere instanties die gerechtigd zijn het BSN te gebruiken.

kamer[3], naast de huidige varianten van DigiD ook op niveau hoog beveiligde varianten. In de pilots is in dat kader succesvol geëxperimenteerd met van een geavanceerde chip voorziene versies van de Nederlandse Identiteitskaart en het Rijbewijs. Ook is er een succesvolle proef met RDA (Remote Document Authentication) methode uitgevoerd door de RDW, die de basis gaat vormen van een hoger betrouwbaar DigiD middel (onder de werktitel DigiD Substantieel). Het kabinet kiest er voor de naam DigiD te handhaven als merknaam voor het totale toekomstige aanbod van de overheid wat betreft inlogmiddelen/-methoden conform in de EU-classificatie onderscheiden niveaus van beveiliging. Uit meerdere onderzoeken blijkt dat de naamsbekendheid van DigiD zeer groot is en bovendien dat dit merk groot vertrouwen geniet: 95% kent het en 77% vertrouwt het.

Mensen kiezen aldus in de toekomst zelf hun inlogmiddel dat voor hen vertrouwd is en past bij de eigen gebruiksvoorkeur. Aldus krijgt men bij inloggen op publieke diensten een vergelijkbaar keuzemenu te zien als bij digitaal betalen in ons land is gebeurd. In beginsel kan iemand met één inlogmiddel volstaan.

Toelating en toezicht onder één wettelijk regime

Zoals eerder met u besproken, betekent de multimiddelenaanpak uitdrukkelijk niet dat in de toekomst ieder inlogmiddel in de dienstverlening in het BSN-domein wordt toegestaan. Er is een nadrukkelijk onderscheid met inlogmethoden zoals burgers deze kennen voor bijvoorbeeld sociale media toepassingen. Rechtovereind blijft het uitgangspunt van het kabinet, dat geautoriseerde digitale toegang tot de dienstverlening in het BSN-domein en het kunnen vaststellen van de identiteit of andere kenmerken zoals leeftijd van degene met wie digitaal zaken wordt gedaan, aan strenge eisen is gebonden. Kabinet en Kamer hebben eerder uitgesproken, dat juist het stellen van deze eisen en het toezicht op de nakoming daarvan bij uitstek een overheidstaak zijn en dat de politieke verantwoordelijkheid daarvoor bij de minister van BZK berust.

Zoals in mijn al genoemde brief van 14 december 2015 aangekondigd, geef ik die verantwoordelijkheid invulling door de toelating van alle publieke en private inlogmiddelen voor het BSN-domein onder één publiekrechtelijk regime te brengen: er worden wettelijke eisen gesteld waaraan inlogmiddelen voor gebruik in het BSN-domein moeten voldoen, alsook waaraan hierbij betrokken partijen moeten voldoen. Deze eisen worden gesteld op basis van de wet Generieke Digitale Infrastructuur (Wet GDI), die eerder is aangekondigd[4]. Een en ander wordt hierbij bezien in het bredere verband van de EU-verordening elektronische identiteiten en vertrouwensdiensten (eIDAS-verordening)[5]. Bij de voorbereiding van het wettelijke regime zijn relevante stakeholders, waaronder private aanbieders van authenticatiemiddelen, onder meer banken, en beoogd toezichthouders betrokken. Gebleken is dat er constructief wordt meegedacht over inhoud en vorm van de eisen, toelating en toezicht, en dat er bereidheid bestaat om – met inachtneming van ieders verantwoordelijkheid – binnen een geharmoniseerd publiek regime te opereren.

[3] Motie De Caluwé, Kamerstuk 26643, nr. 376.
[4] Laatstelijk in mijn brief Uitgangspunten Wetgeving Generieke Digitale Infrastructuur d.d. 4 december 2015; Kamerstuk 26 643 nr. 373.
[5] De eIDAS (electronic Identities And Trust Services, nr 910/2014) verordening ziet op grensoverschrijdend gebruik van digitale identiteiten en vertrouwensdiensten tussen de lidstaten van de Europese Unie. De verordening regelt onder meer dat Nederlandse burgers en bedrijven hun Nederlandse digitale inlogmiddelen in de toekomst kunnen gaan gebruiken om in te loggen op websites van openbare instanties in andere lidstaten. Andersom wordt het voor burgers en bedrijven uit andere lidstaten mogelijk om in te loggen op websites van Nederlandse openbare instanties. Een en ander voor zover de betreffende inlogmiddelen bij de Europese Commissie zijn aangemeld.

Gedurende de pilots de afgelopen maanden en mede op basis van de daarbij verder opgedane kennis en ervaring, is een voorstel voor de inrichting van dit regime - conform ook uw verzoek[6] - op hoofdlijnen door het kabinet vastgesteld. Het eIDAS normenkader is daarbij leidend[7].

De voorgenomen Wet GDI legt een wettelijke basis onder digitale dienstverlening in het BSN-domein aan burgers en bedrijven via de generieke digitale infrastructuur. De beoogde wet zal tevens bepalingen over identificatie en authenticatie bevatten, waarin de belangrijkste onderwerpen zijn:

- de verantwoordelijkheid van de Minister van BZK voor de uitgifte van een (of meerdere) publieke middel(en) alsmede voor de voorziening BSN-koppelregister;
- de basis voor de verwerking van persoonsgegevens door bij authenticatie betrokken partijen;
- de basis voor het stellen van eisen terzake van publieke en private authenticatiemiddelen op verschillende betrouwbaarheidsniveaus. Deze eisen kunnen betrekking hebben op alle partijen die betrokken zijn bij authenticatie in het publieke domein;
- regels omtrent de toelating van authenticatiediensten die authenticatiemiddelen leveren voor gebruik in het publieke domein;
- toezicht op de naleving van de aan partijen in de keten gestelde eisen.

De Wet GDI wordt zoveel mogelijk technologie-onafhankelijk geformuleerd, waardoor een zekere mate van flexibiliteit en toekomstbestendigheid wordt gerealiseerd. In de memorie van toelichting bij het wetsvoorstel zal worden ingegaan op de nadere uitwerking in lagere regelgeving en op de afstemming met andere toezichtsarrangementen die betrekking hebben op partijen (waaronder banken) die authenticatiemiddelen uitgeven ten behoeve van het gebruik van deze middelen in het publieke domein. Planning is het wetsontwerp nog in 2016 in consultatie te brengen.

Doel en belang van de Impuls eID

Mede gezien de rapportage en het advies van de Commissie Kuipers over de dit jaar uitgevoerde pilots met het aldus gewijzigde beleid voor digitaal inloggen in het BSN-domein, heeft het kabinet geconcludeerd dat er geen beletsels meer zijn om thans - na overleg met uw Kamer - zo snel als mogelijk stapsgewijs tot daadwerkelijke realisatie over te gaan van dat beleid.

Het kabinet heeft er voor gekozen om de kwaliteitssprong voor te stellen als een per 1 oktober a.s. te starten, centraal gestuurde Impuls gedurende twee jaar. Het algemene doel van deze Impuls eID is, de in de afgelopen 10 jaar gegroeide infrastructuur voor inloggen op de dienstverlening in het BSN-domein binnen de in deze brief vastgelegde kaders op uiterlijk 1 oktober 2018 zodanig te hebben doorontwikkeld, dat hij klaar is voor een weer meer reguliere verdere doorgroei in de daarop volgende jaren. Meer concreet dient de Impuls er in te hebben geresulteerd dat per oktober 2018 in beginsel alle dienstverleners in het BSN-domein in staat zijn om grootschalig alle door de minister van BZK toegelaten inlogmiddelen in hun digitale dienstverlening te accepteren. Het kabinet kiest bij het uitwerken van de planning voor het gaandeweg realiseren van dit resultaat in de diverse geledingen van de dienstverlening, met de Zorg en de Belastingdienst als eerste prioriteiten (‘voorlopers’).

[6] Motie De Caluwé, Kamerstuk 26 643, nr. 374.
[7] Zie bijlage III voor een uitgebreide toelichting.

Ter illustratie een duiding van de voorloper ‘Belastingdienst’.

Dit werkt voor de belastingdienst als volgt uit: In 2016 heeft de Belastingdienst pilots uitgevoerd met een eerste invulling van de multimiddelenaanpak. Naast DigiD was het ook mogelijk om met private inlogmiddelen van de banken (iDIN) en inlogmiddelen uit het stelsel Idensys de aangifte inkomstenbelasting in te dienen. In 2017 is het de wens van de Belastingdienst om deze aanpak stapsgewijs te verbreden naar alle portalen van de Belastingdienst, waarbij het de voorkeur geniet om ook een versterkte invulling van DigiD beschikbaar te hebben. Burgers kunnen dan geleidelijk kennismaken met andere inlogmiddelen dan het huidige DigiD om in te loggen bij MijnBelastingdienst en MijnToeslagen. Voor ondernemers stelt de Belastingdienst nog een Belastingdienst-eigen gebruikersnaam/wachtwoord ter beschikking. Ook die invulling zal worden vervangen door een multimiddelen aanpak: de ZZPers (de eenmanszaken) kunnen inloggen met dezelfde inlogmiddelen die beschikbaar komen voor het BSN-domein. Voor de rechtspersonen wordt overgestapt op het al langer beschikbare eHerkenning (nivo eH3).

Dit impliceert bij een start van de Impuls per 1 oktober a.s. zoals nu voorzien:

a) Vanaf het eerste kwartaal 2017 wordt gestart met de uitrol van DigiD Substantieel.
b) Als onderdeel van de structurele aandacht voor privacybescherming[8] zijn voor het vierde kwartaal 2017 de aanbevelingen voortgekomen uit de diverse Privacy Impact Assessments voor stelselmatig gemaximeerde privacybescherming binnen de totale multimiddeleninfrastructuur doorgevoerd.
c) Het erkennings- en toelatingsproces voor publieke en private inlogmiddelen, alsmede het toezicht, zijn voor het einde van 2017 voor grootschalig gebruik operationeel.
d) Vanaf begin 2018 is DigiD Hoog op het Rijbewijs gereed voor grootschalige uitgifte en grootschalig gebruik.
e) Vanaf het vierde kwartaal 2018 is de DigiD Hoog op de Nederlandse Identiteitskaart (NIK) gereed voor grootschalige uitgifte en grootschalig gebruik.
f) In het derde kwartaal van 2018 is een over langere periode lopende algemene publiekscampagne afgerond en geëvalueerd, die mensen succesvol heeft duidelijk gemaakt (i) op welke manieren digitaal inloggen op de publieke dienstverlening kan, (ii) welke voordelen dat hen biedt, (iii) hoe daarbij hun privacy door, respectievelijk onder toezicht van, de overheid wordt beschermd, (iv) wat zij zelf kunnen doen om hun privacy in de digitale wereld te beschermen en (v) wat zij zelf kunnen doen om te zorgen dat ze overal en altijd kunnen inloggen op publieke (en overigens ook niet-publieke) websites.
g) De technische en organisatorische voorzieningen om met meerdere inlogmiddelen tegelijk te werken zijn per 1 oktober 2018 zodanig uitontwikkeld, dat (i) de voor dat moment geprognosticeerde gebruiksvolumes met een bandbreedte van plus 25% probleemloos kunnen worden geaccommodeerd en (ii) verdere groei van gebruiksvolumes vanaf dat moment op een gecontroleerde manier kan gaan worden opgevangen.
h) Het beleid is formeel juridisch verankerd, dat wil zeggen dat benodigde wet- en regelgeving in werking is getreden.

[8] Onderdeel van de beleidsrealisatie is dat voor elke substantiële ontwerpwijziging (of beperktere wijziging waarbij impact op privacybescherming niet kan worden uitgesloten) een Privacy Impact Assessment (PIA) wordt uitgevoerd.

Realisatie- en invoeringsplan

De uitvoering van de Impuls eID geschiedt op basis van een operationeel Realisatie- en invoeringsplan dat voor eind augustus dit jaar gereed zal zijn. Bij het opstellen van dit plan wordt inmiddels dankbaar gebruik gemaakt van de ervaringen uit de pilots en de recent uitgebrachte adviezen van het BIT en van de Commissie Kuipers.
Kern van het advies van de Commissie Kuipers is, de verkende multimiddelenstrategie te continueren. Zowel op het vlak van gebruiksgemak als op aspecten als technische degelijkheid, privacybescherming en ervaringen van de aanbieders van inlogmiddelen en landelijke en lokale dienstenaanbieders, geven de pilots acceptabele tot ronduit gunstige uitkomsten te zien. De Commissie adviseert om tot zo concreet mogelijke en implementatiegerichte vervolgstappen te komen in de multimiddelenaanpak en raadt daarbij aan om het overkoepelende niveau van de drie sporen in die aanpak (publieke middelen, iDIN middelen en Idensys middelen) in samenhang te bezien.

Kern van het BIT-advies is dat door de focus van het programma eID op het BSN-domein en het instellen van de interdepartementale stuurgroep op het niveau directeuren-generaal belangrijke stappen zijn gezet om de complexiteit op inhoud en op sturing te reduceren, die kenmerkend was voor de beleidsvoornemens tot eind 2015. Het gevaar van te grote complexiteit is daarmee echter niet definitief geweken aldus het BIT. Expliciet waarschuwt het BIT voor een te optimistische tijdsplanning en voor een mogelijk te bescheiden ingeschat eenmalig ontwikkel budget.

In globale termen impliceert de koers die het kabinet met inachtneming van beide adviezen voorstaat, dat in de Impuls eID identiteit op hoofdlijnen in elk geval het volgende moet gebeuren:

- Het ontwerp voor de wet GDI moet worden afgemaakt en aan uw Kamer voorgelegd, met daarin de basis voor de aan de inlogmiddelen te stellen eisen, het beheer van deze eisen, het toelatingsproces en het toezicht, alsook de verantwoordelijkheidsverdeling en de financiering;
- De gemeenschappelijke technische voorzieningen die voor de pilot zijn gemaakt om de praktische werking van de multimiddelenaanpak te kunnen beproeven moeten op basis van de ervaringen op onderdelen worden aangepast en moeten worden opgeschaald voor massaal gebruik;
- DigiD Substantieel moet gereed worden gemaakt voor grootschalige uitgifte en grootschalig gebruik en zal vervolgens moeten worden ingevoerd;
- Er moet een aanbesteding worden gedaan voor de realisatie van DigiD Hoog op de NIK (en mogelijk ook voor het Rijbewijs). Het beheer moet worden ingericht en met gemeenten moeten afspraken worden gemaakt over de uitgifte;
- De voor de pilot ingerichte processen voor toelating en toezicht moeten op basis van de evaluatie van de pilots worden klaargemaakt en ingeregeld voor de definitieve fase;
- Zowel de processen voor toelating en toezicht als de alsnog doorgevoerde maatregelen uit de Privacy Impact Analyses zullen wat betreft hun werking in de praktijk een eerste keer moeten worden geëvalueerd en de verbeterpunten daaruit zullen moeten worden gerealiseerd;
- De voor de pilotfase nog niet doorgevoerde aanbevelingen uit de uitgevoerde Privacy Impact Analyses zullen moeten worden doorgevoerd;
- De systemen van de dienstenaanbieders zullen moeten worden aangepast op basis van de koppelvlak specificaties van de multimiddelenaanpak;

- De financiële verrekenprocessen zullen moeten worden ingeregeld;
- De governance voor de fase na afronding van de Impuls zal moeten worden ingericht en ingeregeld;
- De eerder genoemde publiekscampagne moet worden voorbereid en uitgevoerd.

De Impuls eID wordt onder de politieke verantwoordelijkheid van de minister van BZK uitgevoerd, waarbij het opdrachtgeverschap is belegd bij een topambtelijke stuurgroep. Deze stuurgroep is samengesteld uit dezelfde directeuren-generaal van de rijksoverheid, die dit voorjaar voor het kabinet de in deze brief toegelichte beleidswijziging hebben voorbereid, aangevuld met een directielid van de Vereniging Nederlandse Gemeenten.

Uitrol strategie

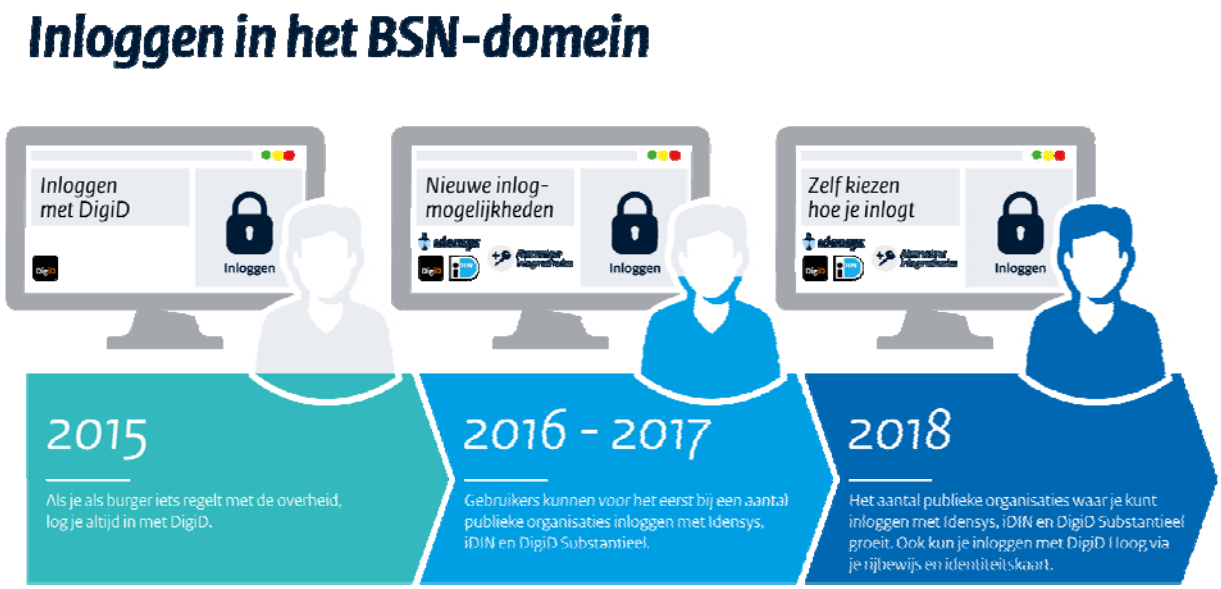
Op dit moment is DigiD Basis feitelijk de beveiligingsnorm van 90% van de transacties. Het kabinet vindt de tijd gekomen om DigiD Substantieel tot de facto beveiligingsnorm te verheffen. Nagegaan wordt hoe dat handen en voeten te geven. Dat mede in het licht van de nog te maken keuze over de verschijningsvorm van DigiD niveau Substantieel op basis van de recente pilots en andere experimenten. Ook de (meerjarige) afbouw van het huidige DigiD Basis is een van de bouwstenen van het realisatie- en invoeringsplan.

Met de afronding van de *verkenningsfase* kan worden overgegaan tot de uitrolfase per 1 oktober 2016: het toewerken naar enkele *voorlopers*. Graag ga ik hierover voor die tijd met uw Kamer in gesprek; tot dan zullen geen onomkeerbare stappen worden gezet. Wanneer de randvoorwaarden daartoe gereed zijn, is vervolgens per Q3 2017 een gecontroleerde grootschaliger uitrol bij deze dienstverleners voorzien. Het kabinet sluit met deze aanpak specifiek aan bij de gevoelde urgentie en de getoonde betrokkenheid in de zorgsector en de samenhang met de verdere modernisering van de aangifte inkomstenbelasting. Deze fase is vervolgens de opmaat naar een bredere uitrol in uiteindelijk de *beheers- en exploitatiefase* van nieuwe inlogmiddelen binnen de multimiddelenaanpak.
Met het genomen besluit ligt de voortgang niet stil en is tevens uw Kamer in de gelegenheid om, alvorens de uitrol onder *voorlopers* plaatsvindt, over de verdere uitrol met het kabinet van gedachten te wisselen. Het kabinet benut op deze wijze de positieve energie die de pilots bij de betrokken partijen hebben gegenereerd. De eerdere opzet van werken met pilots zal ten bate van een goede voorbereiding op de realisatiefase, indachtig de recente adviezen, in de komende maanden worden doorgezet.

Voor de goede orde, er is met deze strategie - mede in het licht van het advies van de commissie Kuipers - gekozen voor een geleidelijke overgang tussen beleidsvoorbereiding en beleidsrealisatie met ruimte voor overleg met uw Kamer. Het betreft een gecontroleerde uitrol, waarbij in de opzet rekening wordt gehouden met de adviezen van BIT en de commissie Kuipers. Zo zal in het realisatie- en invoeringsplan wat betreft DigiD ondermeer worden ingegaan op het benutten van RDA technologie als relatief sneller te realiseren tussenstap, op weg naar de beschikbaarheid van het middel ‘hoog’ zoals eerder in deze brief benoemd onder ‘doel en belang’ van deze impuls. Het realisatie- en invoeringsplan toont tevens specifiek op welke wijze de introductie van in ieder geval één zwaarder beveiligd publiek middel in 2017 is beoogd (DigiD Substantieel).

Onderdeel van de Impuls eID is het realiseren van een eNIK en eRijbewijs met beveiliging op het hoogste niveau. De uitrol hiervan is naar zijn aard gebonden aan de vervangingscyclus welke geldt voor deze officiële identiteitsdocumenten. Omdat het reguliere tempo 10 jaar in beslag zal nemen, is ernstig overwogen of een versnelling noodzakelijk zou zijn. Het kabinet kiest hier vooralsnog niet voor. Enerzijds vergt een versnelde vervanging (waarbij burgers niet onevenredig financieel getroffen worden) een zeer substantiële kostenpost, van enkele honderden miljoenen. Anderzijds realiseert de gekozen uitrolstrategie de spoedige beschikbaarheid van alternatieve middelen (publiek en privaat) op het niveau Substantieel en mogelijk zelfs Hoog. Dit tezamen creëert een context van steeds meer en hoger beveiligde middelen die voor burgers beschikbaar komen, die past bij de ambitie van het kabinet om digitaal inloggen een impuls te geven. In de aankomende periode zal het reeds bestaande contact met de VNG over mogelijke uitvoeringsimplicaties van de gekozen aanpak worden gecontinueerd.

Figuur: Planning burgerperspectief



Financiering

Gedegen ontwikkeling, beheer en exploitatie van de multimiddelenaanpak vergt extra middelen bovenop de bestaande budgetten voor (digitaal) inloggen. Een toekomstbestendige financieringsstrategie ziet bovendien op de financiering van veelvuldig gebruik - ook als dat gebruik intensiever is dan verwacht - evenals op de periodiek noodzakelijke doorontwikkeling van het stelsel en zijn instrumenten.
Uitgangspunten voor de financiering van het beleid zijn dan ook:

- De overheid draagt de kosten voor de (door)ontwikkeling en instandhouding van het publiekrechtelijk verankerde regime voor toelating van en toezicht op publieke en private inlogmiddelen voor het BSN-domein, alsook de kosten van de technische voorzieningen (zoals

met name het BSN-koppelregister) om de multimiddelenaanpak 7x24 uur te laten werken. Dit hangt samen met de verantwoordelijkheid voor het systeem. Hiertoe dragen overheidspartijen naar rato van gebruik bij, evenals (private) organisaties met een publieke taak die digitale diensten leveren in het BSN-domein. Voor de eenmalige kosten van de ontwikkeling van de publieke inlogmiddelen op het hoogste beveiligingsniveau en van het publiekrechtelijk verankerde regime voor toelating en toezicht is reeds een budget van 23 mln. bijeen gebracht[9].

- Een eerste grove indicatie van de kosten samenhangend met de infrastructuur voor authenticatie en identificatie (BSN-koppelregister en authenticatiedienst) , inclusief toelating en toezicht duiden op minimaal structureel € 36 mln. Daarbovenop komen de gebruiksafhankelijke kosten.
- Burgers, beroepsbeoefenaren en zzp-ers betalen middels leges de eenmalige aanschafkosten voor ieder publiek middel dat zij aanschaffen, langs dezelfde lijn als geldt voor de WID-middelen in de analoge wereld.
- Burgers, beroepsbeoefenaren en zzp-ers betalen de eenmalige kosten voor door hen gekozen private middelen; de prijs per middel wordt bepaald door de betreffende middelenleverancier.
- De dienstenaanbieders betalen de eigen kosten voor aansluiten op de middelenaanpak en voor zowel de publieke als de private middelen betalen de dienstaanbieders voor de kosten van het daadwerkelijke inloggen. Hierbij is het uitgangspunt dat dienstaanbieders baten genereren met een generieke, betrouwbare infrastructuur voor digitaal inloggen. De precieze doorbelastingssystematiek zal worden gekozen met oog voor het zoveel mogelijk beperken van de administratieve last.

De ontwikkeling van de kosten van de multimiddelenaanpak is van vele kostendrijvers afhankelijk. Uiteraard worden de kosten per middel mede bepaald door het betrouwbaarheidsniveau waaraan een dergelijk middel moet voldoen. Ook speelt de inrichting van de processen van digitaal inloggen - zoals het aantal keren inloggen als onderdeel van een proces - een rol. Een cruciale factor is de mate van gebruik van elk van de middelen in het stelsel. Een intensief gebruik zal leiden tot hoge totaalkosten maar naar verwachting (zoals de ervaring met DigiD de afgelopen jaren ondubbelzinnig heeft laten zien) geringere marginale kosten. Ook zal een gebruik dat hoger is dan waarvan aanvankelijk werd uitgegaan, vanaf een bepaalde drempel, hogere eisen stellen aan het stelsel als zodanig. Het stelsel zal immers voor intensiever gebruik moeten worden toegerust.

Verondersteld wordt voorts dat zonder versnelling van uitrol van publieke middelen Hoog in eerste instantie het aandeel van private middelen op niveau Hoog relatief groot zal zijn, maar dat tegelijkertijd geldt dat op termijn het aandeel van publieke middelen vanzelf toch groter wordt vanwege de andere (fysieke) functies van de eNIK en het eRijbewijs die voor burgers van belang zijn. Overigens geldt ondertussen wel, dat het op deze manier kijken naar het aandeel van de beschikbare middelen iets anders is dan kijken naar het aandeel van het feitelijk gebruik van de middelen. Daar speelt de ongewisse factor dat het in de multimiddelenaanpak uiteindelijk de gebruiker is die bepaalt welke inlogmiddelen hij prefereert. Kosten zijn daarbij naar ieders verwachting, zeker bij overzichtelijke prijsverschillen, slechts één overweging.

[9] Dit bedrag is aanvullend aan reeds beschikbare budgetten.

Risicobeheersing

De 'Impuls eID' is zeer omvangrijk: het raakt nagenoeg alle burgers van Nederland (en voor een deel ook andere Europese burgers), alle dienstverleners in het BSN-domein, alsmede de (private en publieke) middelenleveranciers. De Impuls behoeft derhalve een navenante risicobeheersing. In het Realisatie- en invoeringsplan wordt dit nader uitgewerkt. Gedurende het verloop van de Impuls wordt door middel van risicomanagement continu een focus op de risico's, consequenties, tegenmaatregelen en besluitvorming gelegd.

De Impuls wordt zodanig ingericht dat het qua aansturing beheersbaar wordt gehouden. Zo is er, mede gelet op het BIT-advies en het advies van de Commissie Kuipers, qua structuur gekozen voor een gecontroleerde uitrol van de impuls en niet voor een 'big bang'; er is dus geen sprake van enkel één 'go/no go' moment. Waar nodig zullen pilots worden gestart om op onderdelen te testen of technieken en procedures werken, dan wel of de beoogde deelnemers kunnen werken met het middel. De centraal vereiste infrastructuur zal geleidelijk worden opgeschaald en beschikbaar gemaakt voor meer deelnemers. Ook zal het aantal beschikbare inlogmiddelen geleidelijk groeien. Daarnaast wordt gekozen voor een heldere communicatiestrategie teneinde het gebruik te bevorderen en de gebruiksvriendelijkheid van de middelen te bewaken.

In de realisatiefase is ondermeer specifiek aandacht voor:

- de opbouw van de uitrol multimiddelenaanpak in stappen, met een steeds versterkte beveiliging als uitgangspunt. De gekozen governance en periodiek overleg met uw kamer sluit hierbij aan.
- de randvoorwaarden zoals tevens in deze brief benoemd en de opbouw daarin (waaronder wettelijke basis).
- de impact van ontwikkelingen in het cyberbeeld en andere (nieuwe) technologische dreigingen op de realisatie en invoering zoals gekozen.
- adequaat begrip van het publiek van de (aanstaande) veranderingen middels de publiekscampagne.
- mogelijke aanvullende Europese ontwikkelingen rond eIDAS.
- de impact van onder meer aanbestedingen en nieuwe technologische ontwikkelingen op de kosten.

Mochten deze en andere risico's nopen tot bijstelling van de plannen, volgt overleg met uw Kamer over deze aanpassingen. Daarnaast maakt de Impuls onderdeel uit van de reguliere planning- en controlcyclus van het ministerie van BZK. Ook is de Impuls onderhevig aan de reguliere toetsmomenten die gelden voor grote ICT-projecten, zoals CIO-oordelen en gateways en audits bij faseovergangen.