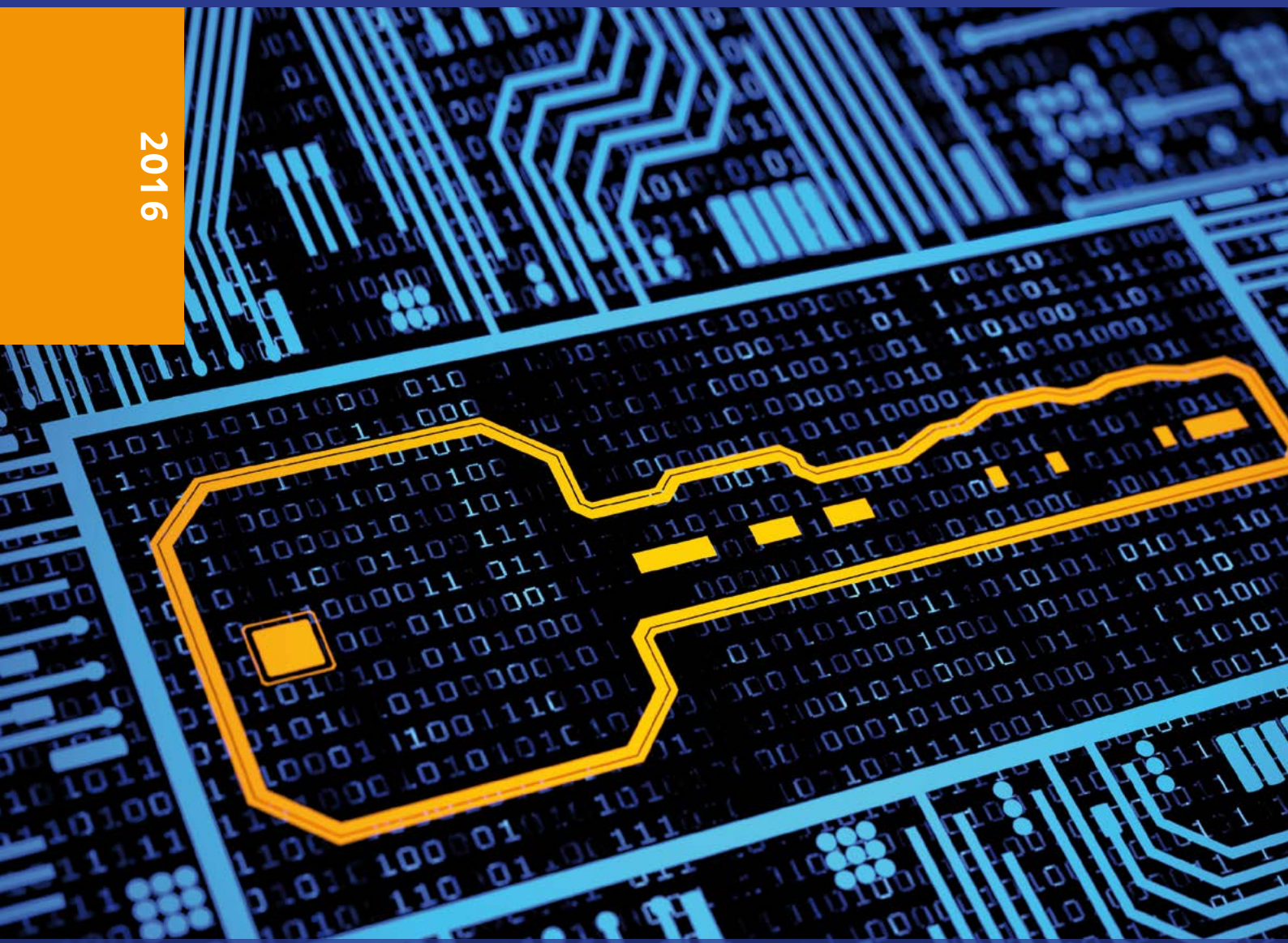
Algemene Rekenkamer

Vernieuwing stelsel voor digitale identificatie en authenticatie (eID-stelsel)

2016



Vernieuwing stelsel voor digitale identificatie en authenticatie (eID-stelsel)

De tekst in dit document is vastgesteld op 31 augustus 2016. Dit rapport is op 8 september 2016 aangeboden aan de Tweede Kamer.

Inhoud

Samenvatting

Het kabinet treft op dit moment voorbereidingen om te komen tot een nieuw stelsel voor digitale identificatie en authenticatie. Dit stelsel is nodig om burgers en bedrijven in staat te stellen (overheids)diensten digitaal af te nemen of hun zaken met de overheid digitaal te regelen. Burgers en bedrijven moeten daartoe hun identiteit kunnen aantonen door gebruik te maken van een zogeheten authenticatiemiddel, zoals DigiD. Burgers maken in totaal al ongeveer 200 miljoen keer per jaar gebruik van DigiD, maar door de voortschrijdende digitalisering wordt verwacht dat dit aantal nog aanzienlijk zal stijgen.
Gelet op het belang van digitale transacties, moeten hoge eisen worden gesteld aan de betrouwbaarheid en beschikbaarheid van authenticatiemiddelen. De bestaande authenticatiemiddelen kunnen hieraan niet voldoen. Bij DigiD speelt ook een rol dat de afhankelijkheid van één authenticatiemiddel als een risico wordt gezien ('single point of failure'). Mede daarom is gestart met de ontwikkeling van nieuwe authenticatiemiddelen en -diensten met bijbehorende regelgeving en afsprakenstelsels. In het kader van ons onderzoek duiden wij dit geheel aan als het eID[1]-stelsel (het stelsel voor elektronische identificatie en authenticatie).

Achtergrond

Het onderwerp van de digitale authenticatie heeft de laatste tijd veel aandacht in de Tweede Kamer, onder andere met het oog op het realiseren van de digitaliseringsdoelstellingen van de overheid in 2017.[2] Volgens het regeerakkoord van het kabinet Rutte II is de ambitie om het uiterlijk in 2017 voor burgers en bedrijven mogelijk te maken hun zaken met de overheid digitaal af te handelen. De tijdsdruk om besluiten te nemen over het eID-stelsel is hoog, omdat de minister van BZK streeft naar de introductie van een publiek (authenticatie)middel in 2017, waarvoor ook nog tijdig een wettelijke basis tot stand moet komen.[3]
In de eerste helft van 2016 zijn pilots uitgevoerd met verschillende authenticatiemiddelen en daarover heeft de commissie-Kuipers (2016) een evaluatierapport uitgebracht. Daarnaast is in mei 2016 een advies uitgebracht door het Bureau ICT-toetsing (BIT, 2016). De minister van BZK (2016) heeft het advies van BIT, voorzien van zijn standpunt, op 17 juni 2016 aan de Tweede Kamer gestuurd.

Conclusies

Ons onderzoek is erop gericht om de Tweede Kamer tijdig, en dus vooraf tijdens de ontwikkeling, te informeren of aan een aantal wezenlijke randvoorwaarden op het terrein van de aansturing (governance), de zakelijke rechtvaardiging (business case) en het

toezicht is voldaan. Daarom bieden wij deze rapportage al in deze fase van het besluitvormingstraject aan de Tweede Kamer aan.

Samenvattend is ons beeld dat tot nu toe (stand van zaken tot en met het voorjaar van 2016) nog niet is voldaan aan een aantal door ons onderzochte randvoorwaarden:

- De verantwoordelijkheden voor het eID-stelsel zijn niet eenduidig belegd en de governancestructuur is ingewikkeld.
- Op wezenlijke onderdelen van het eID-stelsel moeten nog besluiten worden genomen of uitgewerkt.
- Een actuele integrale business case en alternatievenafweging ontbreken vooralsnog.
- Een integrale visie op de inrichting van het toezicht voor het eID-stelsel ontbreekt.

Om de Tweede Kamer in staat te stellen gefundeerde keuzes te maken over de definitieve inrichting van het eID-stelsel, is het van belang dat het kabinet duidelijkheid schept over deze randvoorwaarden.

Reactie minister van BZK en ons nawoord

In zijn reactie van eind augustus 2016 plaatst de minister het eID-stelsel, naar onze mening terecht, binnen het bredere kader van de digitale overheid. Wij kunnen ons vinden in het streven van de minister om de governance rond de digitale overheid in één hand te leggen, maar stellen vast dat er op dit moment voor het eID-stelsel nog geen sprake is van een eenduidige verantwoordelijkheid voor alle domeinen van het stelsel.
Verder stellen we vast dat, ondanks de verwijzing van de minister van BZK (2016a) naar zijn brief van 25 augustus 2016 over de Impuls eID, meer helderheid nodig is over onder andere de inhoud van de toelatingseisen voor het BSN-domein, de multi-middelenbenadering, het toezicht en de privacybescherming.
Tot slot geeft de minister in zijn reactie aan het niet opportuun te achten om alsnog een integrale business case op te stellen. Wij vinden een business case en alternatievenafweging echter onontbeerlijk voor een onderbouwde besluitvorming over de definitieve vorm van het eID-stelsel.

Leeswijzer

In ons rapport geven we eerst een korte uitleg over wat het eID-stelsel behelst (zie hoofdstuk 1). We geven daarna in de hoofdstukken 2, 3 en 4 een schets van de stand van zaken per thema van ons onderzoek (governance, business case en toezicht) en formuleren daarbij conclusies of aan de door ons onderzochte randvoorwaarden is voldaan. Deze

conclusies kunnen bij de verdere besluitvorming over, en vormgeving van, het eID-stelsel in de overwegingen worden betrokken. Tot slot komt in hoofdstuk 5 de reactie van de minister van BZK en ons nawoord aan de orde.

1 Wat behelst het eID-stelsel?

Om burgers en bedrijven in staat te stellen veilig online (overheids)diensten af te nemen of hun zaken met de overheid digitaal te regelen, moeten zij hun identiteit kunnen aantonen door gebruik te maken van een zogeheten authenticatiemiddel, zoals DigiD of eHerkenning.

Om de beperkingen van bestaande authenticatiemiddelen te ondervangen, zijn de afgelopen jaren, min of meer onafhankelijk van elkaar, verschillende (ontwikkel) trajecten gestart, waarbij verschillende ministeries betrokken zijn:

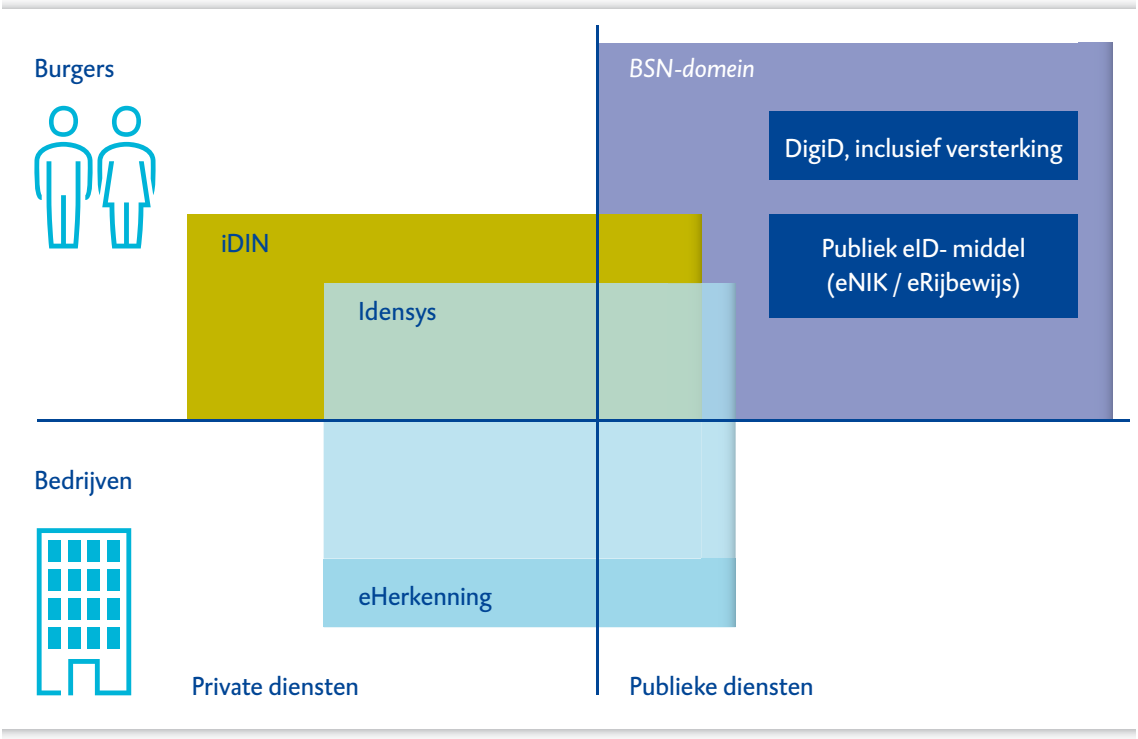
- *Publieke eID-middelen*
  De overheid ontwikkelt zelf enkele authenticatiemiddelen, die worden aangeduid als publieke eID-middelen. Het gaat daarbij om nieuwe versies van zogenoemde WID-documenten,[4] die voorzien zijn van een geschikte chip. Dit omvat onder andere de authenticatiemiddelen eNIK en eRijbewijs.[5] De minister van BZK is hiervoor verantwoordelijk.
- *Afsprakenstelsel elektronische toegangsdiensten (ETD-stelsel)*
  Dit betreft authenticatiemiddelen onder de merknamen eHerkenning en Idensys, welke zijn gebaseerd op een publiek/privaat samenwerkingsverband. Het gaat hier om een afsprakenstelsel waarin verschillende (private) aanbieders van authenticatiemiddelen en –diensten participeren. Volgens het Instellingsbesluit besturing elektronische toegangsdiensten is de minister van EZ (2015) verantwoordelijk voor dit afsprakenstelsel.
- *Inzet van bankmiddelen in het publieke domein*
  Dit omvat de toepassing van authenticatiemiddelen van banken (merknaam: iDIN) ten behoeve van de Belastingdienst. Daardoor is het mogelijk om, in plaats van DigiD, inlogmiddelen van banken te gebruiken om elektronisch belastingaangifte te doen. De werking hiervan is vergelijkbaar met het gebruik van iDEAL voor betalingen. De staatssecretaris van Financiën is hiervoor verantwoordelijk.

Ondertussen werken BZK (Logius) en de Rijksdienst voor het Wegverkeer (RDW) in een pilot samen aan de *versterking van DigiD*. Met de inzet van een chip op het rijbewijs en toepassing van RDA (*Remote Document Authentication*) wordt gewerkt aan een hoger betrouwbaarheidsniveau dan DigiD in de huidige opzet.

Al deze trajecten en middelen maken onderdeel uit van het eID-stelsel in brede zin, zoals wij het in dit onderzoek afbakenen.[6]

In figuur 1 geven we een beeld van de verschillende domeinen en van de (bestaande en nieuwe) authenticatiemiddelen voor:

- burgers en/of bedrijven;
- private online-diensten (bijvoorbeeld elektronisch bestellen bij webshops) en/of publieke online diensten (zoals bijvoorbeeld het aanvragen van toeslagen).



Figuur 1 Domeinen en authenticatiemiddelen

In het 'kwadrant' van de publieke dienstverlening aan burgers, inclusief zzp'ers en eenmanszaken, wordt het Burgerservicenummer (BSN) als identificerend gegeven gebruikt en daarom wordt dit kwadrant ook wel aangeduid als BSN-domein. Dit omvat niet alleen digitale dienstverlening door overheden, maar ook door private organisaties en rechtspersonen, zoals zorgverzekeraars, onderwijsinstellingen en pensioenfondsen, die voor bepaalde publieke diensten het BSN mogen gebruiken.

Zoals in figuur 1 tot uitdrukking gebracht, is het uitgangspunt dat de publieke middelen uitsluitend in het BSN-domein en niet voor private diensten gebruikt zullen worden. De gedachte is dat private authenticatiemiddelen wel gebruikt kunnen worden in het BSN-domein, mits toegelaten door de minister van BZK. Dat kan bijvoorbeeld de mogelijkheid bieden om de authenticatiemiddelen van banken (iDIN) in te zetten voor publieke diensten. Ook voor de middelen die verschillende marktpartijen onder de merknaam Idensys aanbieden, geldt dat die zowel in het private als het publieke domein ingezet kunnen worden.

Digitale identificatie en authenticatie is mogelijk met verschillende betrouwbaarheidsniveaus.[7] Het is de bedoeling dat authenticatiemiddelen beschikbaar komen op het hoogste niveau van betrouwbaarheid, bijvoorbeeld voor toepassingen in de zorgsector. De aanbieders van digitale overheidsdiensten (zoals de Belastingdienst of gemeenten) bepalen overigens in beginsel zelf op welk niveau van betrouwbaarheid de online-dienstverlening plaatsvindt.

Omdat digitale identificatie en authenticatie onmisbaar is voor digitale dienstverlening, moeten hoge eisen worden gesteld aan de continue beschikbaarheid van het eID-stelsel. Ook is het van belang het risico van afhankelijkheid van één authenticatiemiddel te beperken om een ‘single point of failure’ te vermijden. In zijn brief van december 2015 licht de minister van BZK (2015) daarom toe dat hij voor het BSN-domein een multi-middelenstrategie hanteert, waarbij meerdere middelen (publiek en privaat) toegelaten kunnen worden.

2 Governance

2.1 Verantwoordelijkheden niet eenduidig belegd

In het kader van ons onderzoek hebben we getoetst of voldaan is aan de voorwaarde dat de bestuurlijke eindverantwoordelijkheid voor het eID-stelsel eenduidig is belegd en in de besluitvormingsstructuur voor het stelsel herkenbaar is.

We stellen vast dat de verantwoordelijkheden voor het eID-stelsel en de daarin toe te passen authenticatiemiddelen niet eenduidig zijn belegd. Zoals we in hoofdstuk 1 hebben aangegeven, zijn vanuit het verleden, min of meer onafhankelijk van elkaar, verschillende (ontwikkel)trajecten gestart met eigen governance- en overlegstructuren.
Eind 2015 is, mede op aandringen van de Tweede Kamer, de verantwoordelijkheid voor de digitale burgerauthenticatie in het publieke domein (ook wel aangeduid als BSN-domein) nadrukkelijk(er) bij de minister van BZK (2015) gelegd. Dit omvat onder andere de ontwikkeling en wettelijke verankering van uniforme toelatingseisen voor het BSN-domein. Voor het private domein behoudt de minister van EZ (2015) het voortouw en is er een publiek-private samenwerking, waarvan de besturing is geregeld in het Instellingsbesluit besturing elektronische toegangsdiensten.
Het Ministerie van BZK kampt nu met de uitdaging om in een korte periode de afzonderlijke trajecten te verbinden om een eenduidig authenticatiestelsel voor het BSN-domein te realiseren. Tegelijkertijd moet het ministerie de aansluiting met de ontwikkelingen buiten het BSN-domein in het oog houden, om een samenhangend stelsel voor digitale identificatie en authenticatie te kunnen bereiken voor zowel het publieke als private domein.

We constateren dat de governancestructuur om tot een eID-stelsel te komen ingewikkeld is en veranderlijk. Verschillende ministeries, agentschappen, zelfstandige bestuursorganen en private partijen spelen een rol en de verantwoordelijkheden en belangen lopen uiteen. De onderscheiden (ontwikkel)trajecten voor de publieke eID-middelen, het Afsprakenstelsel elektronische toegangsdiensten en de inzet van bankmiddelen, hebben elk een eigen governancestructuur. Verder zijn er interdepartementale structuren tot stand gebracht voor de verbinding tussen de verschillende trajecten. Het eID-stelsel behoort daarnaast ook tot de Generieke Digitale Infrastructuur (GDI), waarvoor de minister van BZK (2014) de Nationaal Commissaris Digitale Overheid (NCDO) heeft aangesteld. Deze Digicommissaris voert regie ten aanzien van deze GDI en heeft, mede met het oog op het eID-stelsel, een Regieraad Identificatie en Authenticatie (I&A) ingesteld, die een eigen governance- en overlegstructuur toevoegt aan de bestaande structuren.

De structuur van stuurgroepen, werkgroepen, programma's, projecten en overleggen is niet alleen ingewikkeld, maar verandert ook regelmatig. Zo is de aansturing van de realisatie van authenticatiemiddelen in het BSN-domein recent ingrijpend gewijzigd. Een bestaande interdepartementale stuurgroep is in april 2016 vervangen door een nieuwe stuurgroep met een geheel andere samenstelling op het niveau van directeuren-generaal. Daarmee beoogt het Ministerie van BZK focus aan te brengen op het BSN-domein, de aansturing te versterken en de complexiteit van de governance te reduceren.
Ook het BIT (2016) concludeert in zijn advies dat de governance ingewikkeld is en dat verdere beperking van complexiteit nodig is. Met de focus op het BSN-domein heeft het Ministerie van BZK volgens het BIT een belangrijke stap gezet om de complexiteit te reduceren, maar is het gevaar van een te grote complexiteit nog niet geweken.

Conclusie
De verantwoordelijkheden voor het eID-stelsel zijn niet eenduidig belegd en de governancestructuur is ingewikkeld.

2.2 Eisen aan eID-stelsel niet uitgekristalliseerd

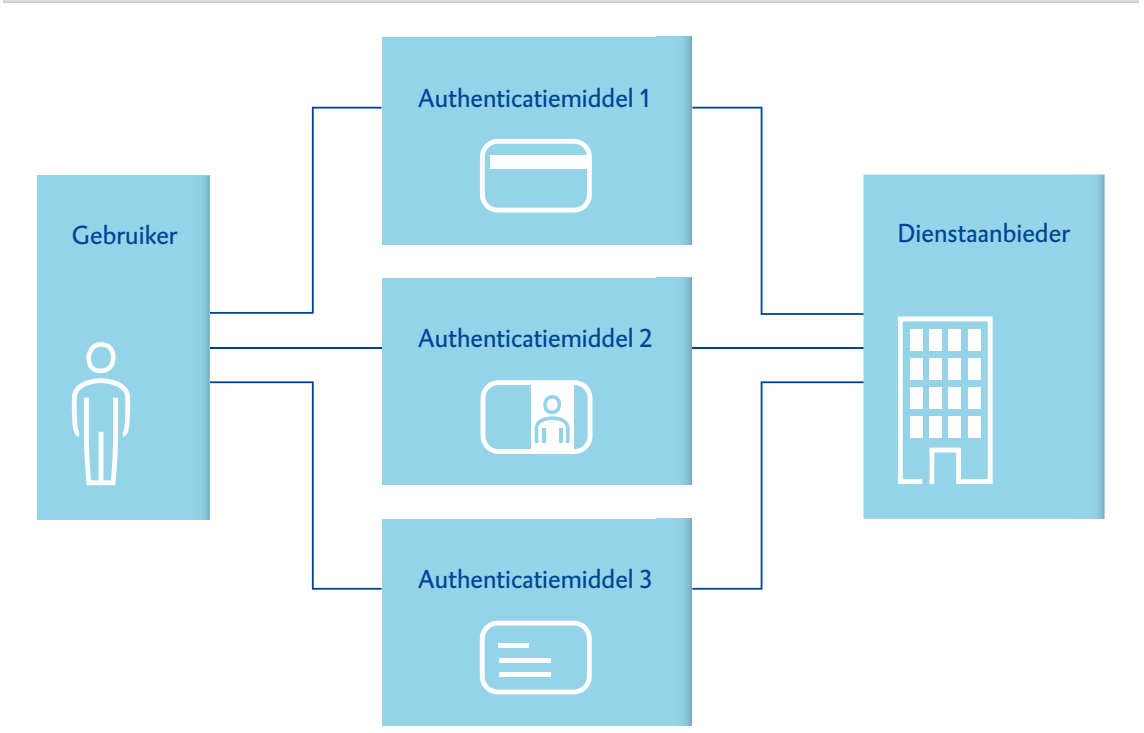
Om een functionerend stelsel voor digitale identificatie en authenticatie tot stand te kunnen brengen, zullen de aan dit stelsel te stellen eisen helder moeten zijn. Doelstellingen, principes en uitgangspunten moeten vooraf zijn uitgewerkt, voorzien zijn van een logische onderbouwing en onderling consistent zijn.

Wij hebben geconstateerd dat ten tijde van de afronding van ons onderzoek in het voorjaar van 2016 op wezenlijke punten nog besluiten moesten worden genomen, zoals over de in de wet te verankeren toelatingseisen voor authenticatiemiddelen in het BSN-domein.

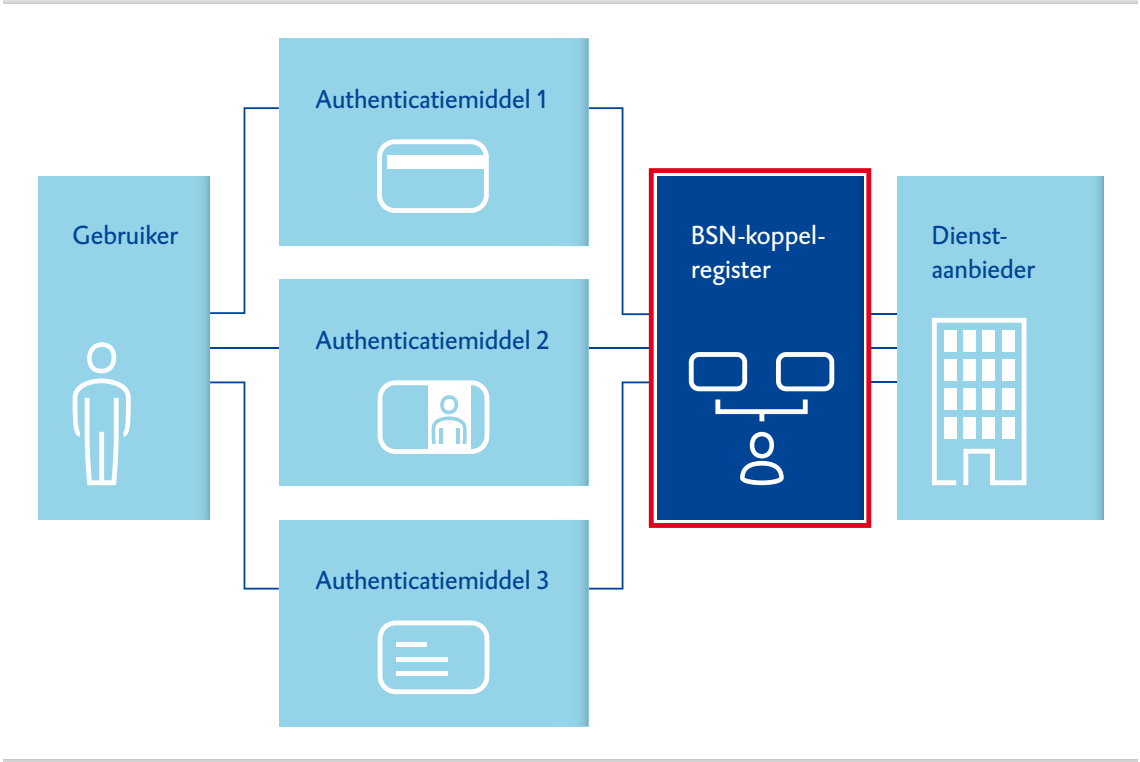
Een belangrijk uitgangspunt voor het eID-stelsel is de 'multi-middelenstrategie'. Een multi-middelenstrategie houdt in dat een vervangend authenticatiemiddel beschikbaar is, mocht een bepaald authenticatiemiddel uitvallen of worden gecompromitteerd. Deze strategie is mede bedoeld om kwetsbaarheden als gevolg van de afhankelijkheid van een enkel middel ('single point of failure') te reduceren. Een dergelijke kwetsbaarheid bestaat nu met DigiD. Over de uitwerking van dit belangrijke uitgangspunt bestaat er echter nog veel onduidelijkheid. Zo is niet helder of hieruit als eis voortvloeit dat elke burger over meerdere geactiveerde authenticatiemiddelen op een hoog betrouwbaarheidsniveau zou moeten beschikken.

Overigens is het hebben van meerdere authenticatiemiddelen op zichzelf niet voldoende om een 'single point of failure' geheel te voorkomen. Die kan zich namelijk ook elders in het eID-stelsel voordoen, bijvoorbeeld bij het BSN-koppelregister.[8] Het is echter nog onduidelijk welke eisen aan andere componenten van het eID-stelsel, zoals het BSN-koppelregister, worden gesteld om een 'single point of failure' te vermijden. Voor het welslagen van de multi-middelenstrategie is het van belang dat voor alle componenten van de keten bij uitval een alternatief voor handen is.

In figuur 2.1 is schematisch een multi-middelen eID-stelsel in beeld gebracht zonder een 'single point of failure' en vervolgens in figuur 2.2 een multi-middelen eID-stelsel, waarin het BSN-koppelregister een 'single point of failure' vormt.



Figuur 2.1 Multi-middelen eID-stelsel zonder 'single point of failure'



Figuur 2.2 Multi-middelen eID-stelsel met BSN-koppelregister als 'single point of failure'

Omdat een wettelijke basis nodig is en de totstandkoming van wetgeving de nodige tijd vergt, is de tijdsdruk om besluiten te nemen hoog geworden. Dit mede met het oog op de beoogde introductie van een publiek authenticatiemiddel in 2017. Het risico bestaat dat daardoor de zorgvuldigheid van de besluitvorming in gevaar komt.
Daarbij komt dat de commissie-Kuipers (2016) in haar rapport nog een aantal 'kernpunten' heeft geschetst, die om meer fundamentele overwegingen en keuzes vragen. Dit betreft onder andere de vereiste niveaus van betrouwbaarheid en de gevolgen daarvan voor de authenticatiemiddelen en ook de beperking van het gebruik van publieke middelen tot het BSN-domein.

Conclusie

Op wezenlijke onderdelen van het eID-stelsel moeten nog besluiten worden genomen of uitgewerkt, onder andere over de invulling van de multi-middelenstrategie.

3 Business cases en alternatievenafweging

3.1 Actuele integrale business case ontbreekt

Grootschalige (ICT-)projecten behoeven een zakelijke onderbouwing in de vorm van een zogeheten business case.[9] Een business case moet over de gehele levenscyclus van een project een beeld geven van de op te leveren producten/resultaten en van de daarmee samenhangende (verwachte) kosten en baten. Tijdens de verschillende fasen moet de business case waar nodig worden geactualiseerd om als stuurmiddel te kunnen blijven fungeren.

We hebben vastgesteld dat de afgelopen jaren op verschillende momenten en voor verschillende componenten van het eID-stelsel kosten-/batenanalyses of business cases zijn opgesteld. Een actuele *integrale* business case ontbreekt op dit moment echter. Daarin zouden de voorgestelde oplossingen, de toe te passen authenticatiemiddelen en eventuele scenario's moeten zijn doorgerekend en geanalyseerd, zowel inhoudelijk als wat betreft kosten, baten en planning. De integraliteit van de analyse is van belang, omdat er onderlinge afhankelijkheden bestaan bij de inzet van verscheidene authenticatiemiddelen. We constateren dat er nog verschillende beslissingen moeten worden genomen, bijvoorbeeld over de functionele eisen en de gewenste uitroltermijn, die een wezenlijke invloed kunnen hebben op de kosten en op de business case. Ook daarnaast bestaan er nog veel onzekerheden die doorwerken naar de business case. Zo is er nog weinig zicht op de omvang van de dienstverlening in de toekomst (aantallen raadplegingen of transacties), verdeeld over de verschillende betrouwbaarheidsniveaus. Dit kan een grote invloed hebben op de inrichting en de kosten van het authenticatiestelsel.

Ten tijde van ons onderzoek was niet bekend wat de (verwachte) totale kosten zijn van de ontwikkeling, implementatie en uitrol van het eID-stelsel. In maart 2016 heeft het kabinet besloten voor de periode 2016 en 2017 een bedrag van € 23 miljoen vrij te maken voor de ontwikkeling in het BSN-domein. Wat de kosten, ook voor de andere domeinen van het eID-stelsel, op de langere termijn zijn en welke eigen bijdrage de burger daaraan eventueel moet leveren, is nog niet helder. Ook de commissie-Kuipers (2016) en het BIT (2016) wijzen er in hun rapportages op dat er nog beslissingen genomen moeten worden over de financiering.

Conclusie

Een actuele integrale business case, op basis waarvan keuzes gemaakt kunnen worden voor de uiteindelijke oplossing, ontbreekt vooralsnog.

3.2 Geen systematische alternatievenafweging

Een zakelijke rechtvaardiging van grote (ICT-)projecten omvat eveneens een alternatievenanalyse, inclusief een nul-alternatief, waarin wordt aangegeven welke alternatieven (naast de voorkeursoptie) zijn onderzocht en waarom deze alternatieven eventueel zijn afgevallen.[10]

Een gestructureerde alternatievenafweging kent in hoofdlijnen de volgende stappen:

- een brede inventarisatie van mogelijke oplossingen, bijvoorbeeld via een marktverkenning of -consultatie;
- het formuleren van expliciete beoordelings- of afwegingscriteria;
- een systematische analyse en weging van de alternatieven in relatie tot de geformuleerde beoordelingscriteria;
- het bepalen van de voorkeursoptie op basis van een totaalbeeld van de (beoordeling van de) alternatieven.

We stellen vast dat een gestructureerde afweging van alternatieven voor het stelsel van digitale identificatie en authenticatie nog niet heeft plaatsgevonden. De huidige situatie, waarin pilots met verschillende authenticatiemiddelen plaatsvinden, is niet gebaseerd op een systematische inventarisatie en integrale afweging van (combinaties van) alternatieven. Daardoor is er geen zekerheid dat de nu gekozen oplossingsrichtingen optimaal zijn, bijvoorbeeld ten aanzien van kosten, functionaliteit, betrouwbaarheid, beveiliging en privacybescherming.

Zoals we in § 3.1 al hebben vermeld, zijn voor sommige componenten afzonderlijke business cases opgesteld, maar niet of slechts in beperkte mate in onderlinge samenhang. Voor andere alternatieven, zoals IRMA[11] en de authenticatiemiddelen van de banken (iDIN), ontbreekt een dergelijke analyse.

De Tijdelijke commissie ICT van de Tweede Kamer (2014a) heeft al in december 2014, naar aanleiding van vragen vanuit de Kamer, kritische kanttekeningen geplaatst bij de wijze van totstandkoming van het eID-stelsel. Volgens de commissie moet een politieke afweging over het eID-stelsel worden bezien in het licht van een gedegen en goed onderbouwde zakelijke rechtvaardiging, waarin de maatschappelijke kosten opwegen tegen de maatschappelijke baten. Hoewel de commissie geen onderzoek heeft gedaan naar het

eID-stelsel, constateert zij dat in de verkennende fase al enkele belangrijke richtinggevende keuzes zijn gemaakt, die zakelijk gerechtvaardigd hadden moeten worden.

Conclusie

Een systematische alternatievenafweging voor de besluitvorming over het eID-stelsel, heeft (nog) niet plaatsgevonden.

4 Toezicht

4.1 Toezichtobjecten en -normen staan nog niet vast

Gelet op de aard van het eID-stelsel, is het van belang dat voorzien is in toezicht op de betrouwbaarheid, beveiliging en privacybescherming.

Zoals in hoofdstuk 2 toegelicht, is voor het eID-stelsel nog niet helder welke middelen en voorzieningen definitief ingezet zullen gaan worden. Daardoor staat nog niet vast op welk(e) object(en) toezicht gehouden moet worden. Daarnaast is nog onduidelijk welke (uniforme) normen en criteria zullen gelden, bijvoorbeeld op het terrein van betrouwbaarheid, beveiliging en privacy, voor de middelen die in het BSN-domein worden toegelaten. In het Afsprakenstelsel voor elektronische toegangsdiensten[12] zijn op hoofdlijnen normen en criteria vastgelegd, maar nog niet duidelijk is hoe die zich verhouden tot de eisen die straks voor het BSN-domein zullen gelden.

De normen voor de privacybescherming spelen, gelet op de aard van het eID-stelsel, een belangrijke rol. De versleuteling of encryptie van gegevens(transport) is een belangrijke maatregel ter bescherming van de privacy. In de pilotfase van het eID-stelsel is er nog geen sprake van 'end-to-end encryptie', dat wil zeggen: versleuteling van gegevens vanaf het begin (de gebruiker) tot aan het eind (de dienstverlener). Om de privacy optimaal te beschermen is end-to-end encryptie gewenst, maar nog onduidelijk is of dit voor het uiteindelijke stelsel een norm wordt.

Voor wat betreft het aspect privacy is verder van belang dat cumulaties van gevoelige persoonsgegevens, zogenaamde 'hotspots', worden voorkomen. In een door Mazars (2015) uitgevoerde Privacy Impact Assessment (PIA) is dit aan de orde gekomen, maar nog onduidelijk is of en in welke mate er eisen worden gesteld om dergelijke 'hotspots' te vermijden.

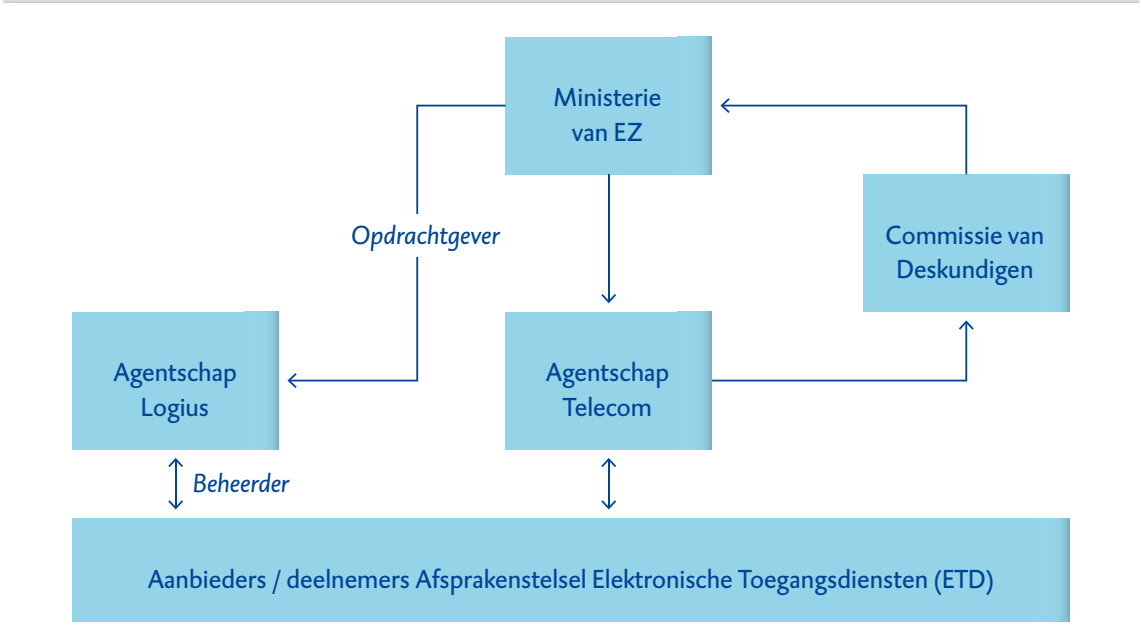
Conclusie

Er is nog geen helderheid over het object of de objecten van het toezicht en de daarbij te hanteren criteria en principes. Het is van belang bij de inrichting van het eID-stelsel rekening te houden met de vereisten die later van belang zijn bij de vormgeving van het toezicht op betrouwbaarheid, beveiliging en privacybescherming.

4.2 Inrichting toezicht niet helder

Omdat er nog onduidelijkheid bestaat over de eisen ten aanzien van het stelsel, is ook nog onduidelijk hoe het toezicht op de betrouwbaarheid, beveiliging en privacybescherming ingericht zal worden.

Vanaf 1 januari 2016 heeft het Ministerie van EZ de toezichttaak voor het Afsprakenstelsel elektronische toegangsdiensten (ETD-stelsel: eHerkenning en Idensys) van de beheerorganisatie Logius overgenomen. Om deze taak te kunnen vervullen heeft de minister van EZ (2016) een Commissie van Deskundigen (CvD) voor het toezicht op het ETD-stelsel ingesteld. Het Agentschap Telecom (AT) voert sinds maart 2016 het secretariaat voor deze commissie. Schematisch ziet deze toezichtstructuur er als volgt uit (zie figuur 3).



Figuur 3 Toezichtstructuur ETD-stelsel

Dit is overigens een tijdelijke constructie; uiteindelijk zou het toezicht een publiekrechtelijke grondslag kunnen krijgen in de wet GDI. Het AT houdt zich voor de Commissie van Deskundigen en de minister van EZ in dit stadium vooral bezig met de toetsing of partijen aan de toetredingscriteria voor het ETD-stelsel voldoen.
Het Agentschap Telecom (AT) is de beoogd toezichthouder voor de publieke authenticatiemiddelen. De Rijksdienst voor Identiteitsgegevens (RvIG) houdt toezicht op de aan

vraag, productie en distributie van identiteitsbewijzen en moet op een of andere manier ook in de toezichtstructuur worden ingepast. Daarover bestaat nog geen duidelijkheid.

De banken, die nu een pilot uitvoeren in samenwerking met de Belastingdienst, hebben DNB als toezichthouder. De Betaalvereniging Nederland (BVN) speelt een coördinerende en toezichthoudende rol bij de identificatie- en authenticatiediensten, die banken en andere betaaldienstverleners aanbieden. Zo toetst de BVN of partijen die toe willen treden tot iDIN voldoen aan de licentievoorwaarden.
De banken ervaren het tegelijk moeten voldoen aan meerdere toezichtkaders als zeer complicerend of zelfs ondoenlijk. Het is nog onduidelijk hoe het toezicht op de banken zal worden ingericht voor wat betreft het verlenen van identificatie- en authenticatiediensten, die geen verband houden met het betalingsverkeer.

Omdat privacyaspecten een belangrijke rol spelen, is er ook een toezichthoudende taak voor de Autoriteit Persoonsgegevens (AP) te onderkennen. De AP heeft hierin een eigenstandige verantwoordelijkheid, maar een goede onderlinge afstemming met overige toezichthouders lijkt wenselijk.

Conclusie
Een integrale visie op de inrichting van het toezicht voor het eID-stelsel ontbreekt vooralsnog.

5 Bestuurlijke reactie en nawoord

Van de minister van BZK ontvingen we eind augustus 2016 een reactie op ons conceptrapport. In dit hoofdstuk geven we een weergave van de reactie van de minister (zie § 5.1) en ons nawoord daarbij (zie § 5.2). De integrale brief van de minister van BZK is te vinden op onze website (www.rekenkamer.nl).

5.1 Reactie minister van BZK

De minister van BZK legt in zijn bestuurlijke reactie op ons conceptrapport eerst een verbinding met het grotere governancevraagstuk op het terrein van de digitale overheid. Vervolgens besteedt hij aandacht aan onze specifieke conclusies ten aanzien van het eID-stelsel.

Governance van de digitale overheid

In zijn reactie merkt de minister op dat steeds duidelijker wordt dat de inrichting van onze samenleving in hoog tempo bepaald wordt door digitale ontwikkeling en dat de overheid met haar dienstverlening hier midden in zit. Het kabinet werkt daarom aan het realiseren van een solide en toekomstbestendige digitale overheid. Volgens de minister zijn er sinds de start van de Digicommissaris twee jaar geleden essentiële stappen gezet op onder meer de (door)ontwikkeling van de generieke digitale infrastructuur (GDI) en de inrichting van de governance rond de digitale overheid. Volgens de minister is de doelstelling om deze thema's overheidsbreed eenduidig op te pakken, waarbij in de governance de verantwoordelijkheid nadrukkelijk belegd wordt in één hand; dit in lijn met de koers die de Digicommissaris heeft ingezet, gezien de samenhang van de onderwerpen. Nu worden digitaliseringtrajecten nog te vaak individueel door overheidsorganisaties opgepakt en is er sprake van een sterk verbrokkelde financiering, terwijl digitalisering juist de mogelijkheid biedt om meer de verbinding op te zoeken, aldus de minister. Digitalisering van overheidsdienstverlening vraagt dan ook, daar waar nu nog sprake is van gedeelde en overlappende verantwoordelijkheid, onder meer tussen de ministers van EZ en BZK, om een meer centraal ingerichte governance om effectief stappen te kunnen zetten. De minister deelt mee dat de Studiegroep Informatiesamenleving, onder voorzitterschap van de secretaris-generaal van BZK, werkt aan het concretiseren van de visie op de rol van de overheid in de informatiesamenleving, om voort te kunnen bouwen op het werk van de Digicommissaris. De studiegroep is samengesteld uit deskundigen uit de publieke en private sectoren en levert volgens de minister begin 2017 haar rapport op. De aanbevelingen van de studie

groep zijn bedoeld om in opmaat naar de nieuwe kabinetsperiode te adviseren over de benodigde vervolgstappen in de doorontwikkeling van de digitale overheid.

Governance en complexiteit

De minister onderschrijft onze conclusie dat de verantwoordelijkheden voor het eID-stelsel niet eenduidig zijn belegd en dat de governancestructuur ingewikkeld is. De complexiteit van het programma vraagt volgens hem om een governance die een strakke sturing op tijd, geld en kwaliteit mogelijk maakt. Verantwoordelijkheden moeten duidelijk en eenduidig belegd zijn, zeker gelet op de vele actoren en (commerciële) belangen. De minister licht toe dat het kabinet om deze reden in 2015 de verantwoordelijkheidsverdeling ten aanzien van dit onderwerp duidelijker heeft belegd bij de minister van BZK en de minister EZ. Om de complexiteit verder te reduceren zijn in de afgelopen maanden de verantwoordelijkheden in de aansturing van het programma verduidelijkt, bijvoorbeeld door de instelling van een hoogambtelijke stuurgroep onder leiding van de directeur-generaal Overheidsorganisatie, die tevens de opdrachtgever is van het programma Impuls eID. Verder merkt de minister op dat de Digicommissaris wordt geconsulteerd over de besluitvorming, evenals de Regieraad Identificatie en Authenticatie (I&A). De minister zegt toe om zich in de toekomst, daar waar mogelijk, te blijven inzetten om de complexiteit van het programma verder te reduceren. Dit neemt volgens hem overigens niet weg dat het volledig uitbannen van risico's bij innovaties als deze per definitie niet kan.

Eisen aan het eID-stelsel

Volgens de minister concluderen wij terecht dat ten tijde van ons onderzoek op wezenlijke onderdelen van het eID-stelsel nog besluiten moesten worden genomen of uitgewerkt, onder andere over de invulling van de multi-middelenstrategie. Volgens de minister heeft het kabinet in de afgelopen maanden belangrijke besluiten genomen ten aanzien van de eisen aan het eID-stelsel. De minister van BZK (2016a) verwijst naar een brief van 25 augustus 2016, waarmee hij de Tweede Kamer over deze besluiten heeft geïnformeerd. Na overleg met de Kamer over deze brief, beoogt het kabinet op korte termijn het programma Impuls eID te starten. De minister geeft aan dat hij de Tweede Kamer eens per half jaar zal informeren over de voortgang van dit programma, te beginnen via het Dashboard ICT (bij de Jaarrapportage Bedrijfsvoering Rijk) op de derde woensdag in mei 2017.

Business case

De minister geeft in zijn reactie aan dat het kabinet het, gelet op maatschappelijke en technische ontwikkelingen, noodzakelijk acht om over te gaan tot hoger beveiligde

authenticatie, ook als hier geen (positieve) business case aan ten grondslag ligt. Volgens de minister is de ontwikkeling van de kosten van dit stelsel in de tijd van vele variabelen afhankelijk. Dat geldt volgens hem vooral voor de kosten die samenhangen met het gebruik, aangezien de mate van gebruik van alle publieke middelen (ook in verhouding tot elkaar) nog onvoorspelbaar is. Het gebruik als zodanig, evenals exogene technologische ontwikkelingen, zullen periodiek nieuwe en aanvullende eisen stellen aan het stelsel. Daarom zullen de kosten van beheer, exploitatie en doorontwikkeling volgens de minister pas gedurende de rit volledig duidelijk worden. De minister merkt daarnaast op dat het stelsel een aantal maatschappelijk te duiden kwalitatieve baten kent, die niet te kwantificeren zijn in termen van financiële middelen. De minister acht het daarom, hoewel hij onze constatering onderkent, niet opportuun om alsnog een integrale business case op te stellen. Dit laat volgens hem onverlet dat hij scherp zal sturen op de uitvoering van het programma en de kosten die daarin gemaakt worden.

Systematische alternatievenafweging

Wat betreft de alternatievenafweging, verwijst de minister van BZK naar de 'Strategische verkenning en voorstel voor vervolg', waarin de ministers van BZK en EZ (2013) de contouren van een toekomstig eID-stelsel hebben geschetst. Volgens de minister heeft het kabinet op basis hiervan, en na intensief overleg met meerdere departementen en de Tweede Kamer, keuzes gemaakt over de inrichting van het stelsel, die mede worden onderschreven door de Digicommissaris. Ook de resultaten van de reeds uitgevoerde pilots hebben aan deze besluitvorming bijgedragen. De minister stelt dat tijdens dit besluitvormingsproces vele alternatieven tegen elkaar zijn afgewogen. Daarnaast merkt de minister op dat hij in de loop van het programma stuurt op de uitvoering van gateway reviews en CIO-oordelen bij iedere projectovergang. Op deze manier beoogt de minister grip te houden op onder andere de kosten, de functionaliteiten, de betrouwbaarheid, de beveiliging en de privacyaspecten van het stelsel.

Toezicht

Ten aanzien van het toezicht op het stelsel merkt de minister op dat het kabinet ook op dit punt in de afgelopen maanden belangrijke besluiten heeft genomen, waarover de Tweede Kamer in de brief van 25 augustus is geïnformeerd.

Tot slot

Afrondend merkt de minister nog op dat een veilige en continue toegang tot de overheidsdienstverlening cruciaal is. Hij wil daarom dat het programma eID, na overleg met de Tweede Kamer, voortvarend van start gaat en ziet ons rapport daarbij als steun in de rug.

5.2 Nawoord Algemene Rekenkamer

In zijn reactie plaatst de minister het eID-stelsel, naar onze mening terecht, binnen het bredere kader van de digitale overheid. Hij kondigt in dit kader aan dat de Studiegroep Informatiesamenleving, onder leiding van de SG van BZK, begin 2017 zal komen met aanbevelingen voor de doorontwikkeling van de digitale overheid. Mede met het oog op de governance voor het eID-stelsel, zien we met belangstelling uit naar deze aanbevelingen.

De reactie van de minister op de specifieke onderdelen van ons onderzoek, geeft ons verder nog aanleiding tot de volgende opmerkingen.

Governance, besluitvorming en toezicht

De minister wijst op het bredere vraagstuk van de inrichting van de governance rond de digitale overheid en op de doelstelling om in deze governance de verantwoordelijkheid nadrukkelijk te beleggen in één hand. Wij kunnen ons vinden in dit streven, maar stellen eveneens vast dat er op dit moment voor het eID-stelsel nog geen sprake is van een eenduidige verantwoordelijkheid voor alle domeinen van het stelsel.

In zijn reactie verwijst de minister naar zijn brief van 25 augustus 2016 aan de Tweede Kamer over de Impuls eID en naar de besluiten die daarin zijn genoemd over het vervolgtraject van het eID-stelsel. Deze besluiten nemen echter slechts ten dele de onduidelijkheden weg die wij signaleren ten aanzien van bijvoorbeeld de inhoud van de toelatingseisen voor het BSN-domein, de multi-middelenbenadering, het toezicht en de privacybescherming. We vinden het van belang dat op deze punten meer helderheid ontstaat, ter onderbouwing van de besluitvorming en de verantwoording aan het parlement.

Business case en alternatievenafweging

De minister stelt in zijn reactie dat het eID-stelsel een aantal kwalitatieve baten heeft, die niet in financiële termen uit te drukken zouden zijn. Wij merken echter op dat een business case ook niet-financiële doelstellingen kan bevatten. Wij zijn van oordeel dat de (directe en indirecte) baten van een hogere mate van betrouwbaarheid en continuïteit voor digitale

authenticatiemiddelen te kwantificeren zijn. Dit hebben eerdere, inmiddels gedateerde, business cases ook laten zien.[13]
Onze conclusie dat een actuele integrale business case ontbreekt, heeft niet alleen betrekking op de baten, maar ook op de kosten voor de gehele looptijd van het vernieuwde eID-stelsel. In zijn reactie stelt de minister dat de kosten pas 'gedurende de rit' volledig duidelijk zullen worden en geeft hij aan dat hij het alsnog opstellen van een integrale business case niet opportuun acht. Wij zijn van oordeel dat een business case altijd onzekerheden bevat, en ondanks deze bepaalde mate van onzekerheid, inzicht in de kosten van de voorgestelde oplossing(en) onontbeerlijk is, om onderbouwde besluiten te kunnen nemen over de definitieve vorm van het eID-stelsel. Naarmate in de loop der tijd nauwkeuriger indicaties van de kosten te geven zijn, zal de business case geactualiseerd moeten worden. We verwijzen in dit verband naar het eindrapport van de Tijdelijke commissie ICT van de Tweede Kamer (2014).

Wat betreft de afweging van alternatieven verwijst de minister in zijn reactie naar een eerdere verkenning over het eID-stelsel en afwegingen die daarbij een rol hebben gespeeld. Wij bedoelen met het ontbreken van een alternatievenafweging echter dat er geen systematische afweging is aangetroffen van verschillende oplossingen voor de inrichting van het eID-stelsel, onder andere ten aanzien van kosten, functionaliteit, betrouwbaarheid, beveiliging en privacybescherming.

Resumerend is ons beeld dat in de ontwikkeling van het eID-stelsel, ondanks de voortgang die inmiddels is geboekt, nog belangrijke stappen te zetten zijn. Dat maakt het temeer van belang dat er vooraf duidelijkheid bestaat over de door ons getoetste randvoorwaarden, om de Tweede Kamer in staat te stellen gefundeerde keuzes te maken over de definitieve inrichting van het eID-stelsel. Inzicht in de business case en afweging van alternatieven, waaronder de kosten van ontwikkeling, implementatie en uitrol, is daarbij naar onze mening onontbeerlijk. Tijdens de rit en achteraf kan dan worden geëvalueerd en geleerd van opgedane ervaring.

Bijlagen

Bijlage 1
Afkortingen

AP	Autoriteit Persoonsgegevens
AT	Agentschap Telecom
BIT	Bureau ICT-toetsing
BSN	Burgerservicenummer
BVN	Betaalvereniging Nederland
BZK	(Ministerie van) Binnenlandse Zaken en Koninkrijksrelaties
CvD	Commissie van Deskundigen
DigiD	Digitale Identiteit
eID	Elektronische Identiteit
eIDAS	*Electronic Identity and Assurance Services*
ETD	Elektronische Toegangsdiensten
EZ	(Ministerie van) Economische Zaken
GDI	Generieke Digitale Infrastructuur
I&A	Identificatie en Authenticatie
ICT	Informatie- en Communicatietechnologie
IRMA	*I Reveal My Attributes*
NCDO	Nationaal Commissaris Digitale Overheid
NIK	Nederlandse Identiteitskaart
RDW	Rijksdienst voor het Wegverkeer
RvIG	Rijksdienst voor Identiteitsgegevens
STORK	*Secure idenTities acrOss boRders linKed*
VWS	(Ministerie van) Volksgezondheid, Welzijn en Sport
WID	Wet op de identificatieplicht

Bijlage 2
Toelichting eID-stelsel

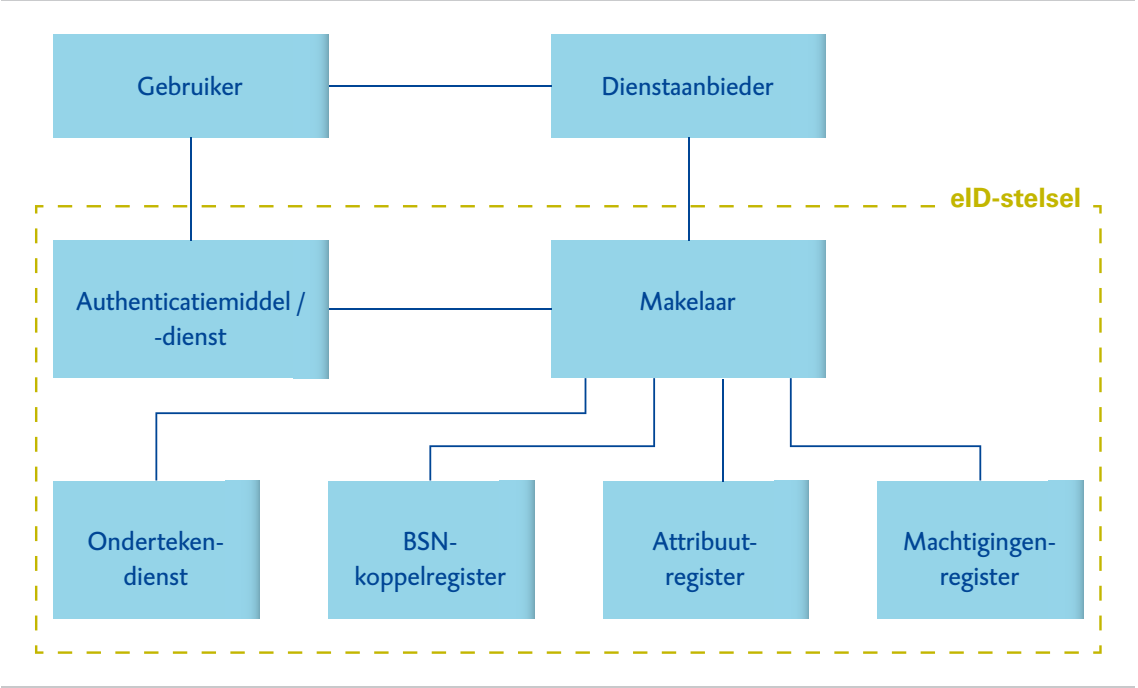
Het nieuwe stelsel voor digitale identificatie en authenticatie (eID-stelsel) is erop gericht dat burgers en bedrijven diensten digitaal af kunnen nemen of hun zaken digitaal kunnen regelen. Daarvoor is het nodig dat burgers en bedrijven hun identiteit kunnen aantonen door een zogeheten authenticatiemiddel te gebruiken.

Bij de zorgvuldige totstandkoming van een transactie moeten de volgende stappen worden doorlopen:

- Identificatie: aangeven wie je bent.
- Authenticatie: aantonen dat je bent wie je zegt te zijn.
- Autorisatie: vaststellen dat je de transactie mag doen.
- Ondertekenen: bekrachtigen van de transactie (onbetwistbaarheid).

Het eID-stelsel moet eraan gaan bijdragen dat een gebruiker van digitale diensten deze stappen op een veilige en betrouwbare wijze kan zetten.
In die zin vervult het eID-stelsel dus essentiële functies om digitale dienstverlening mogelijk te maken. Dit geldt overigens niet alleen voor digitale dienstverlening in het publieke domein, maar ook in de private sector.

In de volgende figuur zijn enkele belangrijke componenten van het eID-stelsel schematisch in beeld gebracht.



Figuur 4 Componenten eID-stelsel

In deze opzet start een gebruiker een inlogprocedure bij een (publieke of private) aanbieder van digitale diensten. De dienstaanbieder wil zich ervan overtuigen dat de identiteit van de gebruiker klopt en eventueel ook nagaan of de gebruiker gerechtigd is om een dienst af te nemen. Daartoe sluit de dienstaanbieder een contract af met een makelaar, die als intermediair fungeert om de benodigde informatie te verzamelen. De makelaar maakt daarvoor contact met de authenticatiedienst. Nadat de gebruiker zich op het juiste betrouwbaarheidsniveau heeft geauthentiseerd met zijn middel, stuurt de authenticatiedienst een reactie terug naar de makelaar.

Afhankelijk van de behoefte van de dienstaanbieder kan de makelaar nog aanvullende informatie verzamelen over attributen, machtigingen, het BSN of de ondertekening (het plaatsen van een digitale handtekening).

Binnen het eID-stelsel (dat met de rode stippellijn is afgebakend) bestaan onder andere de volgende voorzieningen:

- Authenticatiemiddel/-dienst (de 'sleutel')
- Het middel is de sleutel waarmee de gebruiker inlogt bij een aanbieder van een digitale dienst. Het authenticatiemiddel kan voor natuurlijke personen zowel publiek als privaat

worden aangeboden, voor alle betrouwbaarheidsniveaus. De authenticatie van (medewerkers van) rechtspersonen wordt uitsluitend privaat aangeboden.

- Makelaar (ontzorgt een dienstaanbieder)
  Via de makelaar is het mogelijk in te loggen bij een publieke of private organisatie (het 'slot'). Een makelaar verzamelt alle informatie (wie de persoon is, wat de persoon mag en dergelijke) voor een dienstaanbieder om een persoon toegang te kunnen verlenen.
- Machtigingenregister
  Hierin wordt geregistreerd dat een persoon een andere persoon heeft gemachtigd namens hem/haar diensten af te nemen bij een dienstverlener. Het machtigingenregister voor natuurlijke personen kan zowel publiek als privaat worden aangeboden. Het machtigingenregister voor rechtspersonen wordt, mits aan bepaalde voorwaarden wordt voldaan, uitsluitend privaat aangeboden.
- BSN-koppelregister
  Een eID-middel in het kader van het stelsel bevat een uniek identificerend pseudoniem. Bij gebruik van een eID-middel in het private domein wordt geen BSN uitgewisseld, maar een pseudoniem dat per dienstaanbieder uniek is. Bij gebruik van een privaat eID-middel (bijvoorbeeld een bankpas) in het publieke domein wordt het pseudoniem vertaald in een BSN. Dit wordt in een door de overheid (Logius) beheerd BSN-koppelregister bijgehouden, zoals nu ook in het huidige DigiD. Vanwege de verwerking van het BSN is het in stand houden van deze voorziening een exclusieve publieke taak.
- Attribuutregister
  Het attribuutregister is bedoeld om bepaalde attributen (bijvoorbeeld het lidmaatschap van een bepaalde beroepsgroep) te kunnen koppelen aan een specifieke identiteit.
- Ondertekendienst
  De ondertekendienst is bedoeld om binnen het stelsel het kunnen plaatsen van digitale handtekeningen te ondersteunen.

Uitgangspunten eID-stelsel

In een brief van de ministers van BZK en EZ (2013) van 19 december 2013 zijn de hoofddoelen en hoofdlijnen van het stelsel voor digitale identificatie en authenticatie geschetst. In deze brief constateren de ministers dat publieke en private organisaties tot dan toe aan eigen oplossingen werkten, die onderling niet of beperkt uitwisselbaar zijn en in een aantal gevallen niet meer toereikend. Daarom streven de ministers naar een stelsel met publieke en private partijen om kosten te spreiden en om afhankelijkheden van een enkele oplossing te voorkomen. De Ministeries van BZK (2012) en EZ, enkele grote

uitvoeringsorganisaties en medeoverheden hebben daarom in 2012 een strategische verkenning uitgevoerd naar de mogelijkheden voor een publiek-privaat stelsel voor elektronische identificatie en authenticatie (het eID-stelsel). Dit is een stelsel, waarbinnen burgers, consumenten en ondernemers zowel publieke als private authenticatiemiddelen gebruiken, waarmee ze veilig online zaken kunnen doen met de overheid en het bedrijfsleven. De bedoeling is dat binnen het eID-stelsel diverse publieke en private middelen met verschillende betrouwbaarheidsniveaus worden ondergebracht. Dit wordt een multi-middelenstrategie genoemd. In deze opzet heeft het eID-stelsel de brede reikwijdte, zoals wij in hoofdstuk 1 van dit rapport hebben beschreven.

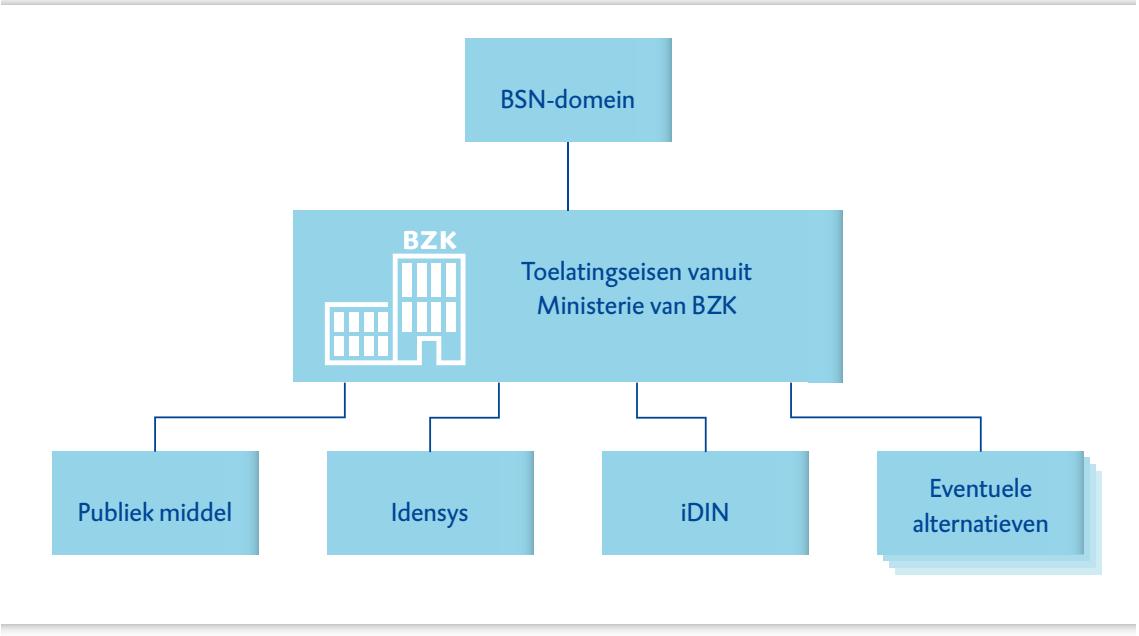
Om uitwisselbaarheid te borgen moeten binnen het eID-stelsel standaarden, eisen en normen worden gedefinieerd, onder andere voor de beveiligingsniveaus. Daarnaast moeten voorwaarden worden vastgelegd waaronder partijen mogen deelnemen.
Dit moet het volgende mogelijk maken:

1 Er komt één eID-stelsel voor authenticatie- en bevoegdheidsdiensten, te gebruiken bij elektronische transacties door natuurlijke en niet-natuurlijke personen waardoor:
   - dezelfde standaarden gelden voor het burger- en bedrijvendomein;
   - verschillende typen gebruikers bediend worden, ook de minder en niet digitaal vaardigen;
   - de privacy van mensen en organisaties gewaarborgd blijft;
   - waar mogelijk gebruik gemaakt wordt van bestaande en bewezen oplossingen en open standaarden;
   - een toekomstvaste en robuuste open publiek-private infrastructuur voor authenticatie- en bevoegdheidsdiensten ontstaat, waarbij binnenlandse en buitenlandse organisaties vrijwillig kunnen toetreden;
   - private en publieke organisaties niet individueel toegangsvoorzieningen in stand hoeven te houden, maar gebruik kunnen maken van gestandaardiseerde oplossingen binnen het stelsel.

2. Het eID-stelsel omvat de volgende elektronische vertrouwensdiensten:
   - authenticatie;
   - machtiging en wettelijke vertegenwoordiging (het vaststellen van bevoegdheden om voor een ander te handelen);
   - attributenlevering (bijvoorbeeld een beroepsbevoegdheid of het voldoen aan een leeftijdsgrens);
   - ondertekenen (digitale handtekening).

3 Binnen het stelsel wordt gewerkt met een beperkt aantal betrouwbaarheidsniveaus,[14] waaraan elektronische identificatie voor een bepaalde dienst moet voldoen.
   - De organisatie die digitaal toegang wil verlenen tot haar dienstverlening classificeert de dienst op een bepaald betrouwbaarheidsniveau.
4 De gebruiker van de dienst kan vervolgens de keuze maken met welk eID middel hij zijn identiteit op het gevraagde betrouwbaarheidsniveau aantoont. Hiertoe kan hij de beschikking hebben over een publiek of een privaat authenticatiemiddel dat in het stelsel is ondergebracht. Voor bedrijfsgebonden authenticatiemiddelen van rechtspersonen zijn er alleen private middelen beschikbaar.
5 De middelen onder het stelsel zijn bruikbaar voor de toegang tot zowel publieke als private elektronische diensten.
6 In de toekomst kunnen de in het stelsel ondergebrachte middelen ook in het buitenland gebruikt worden.

Naar aanleiding van een algemeen overleg in de Tweede Kamer en een daaropvolgende brief van de minister van BZK (2015) van december 2015, is ten opzichte van de hiervoor genoemde uitgangspunten een koerswijziging opgetreden. De minister van BZK heeft de oorspronkelijke aanpak verlaten om via één programma van BZK en EZ zoveel als mogelijk te komen tot één infrastructuur voor inlogmiddelen voor alle publieke en private digitale dienstverlening. De minister van BZK wil zich concentreren op het BSN-domein en de daarvoor wettelijk te verankeren uniforme toelatingseisen voor inlogmiddelen. Binnen dit kader van toelatingseisen is er in beginsel ruimte voor verschillende middelen en afsprakenstelsels, zoals in het volgende schema is geïllustreerd.



Figuur 5 Toelating authenticatiemiddelen in het BSN-domein

Deze multi-middelen strategie krijgt vorm langs drie parallelle sporen:

1 het scheppen van voorwaarden voor het gebruik van hoogwaardige private middelen in het BSN-domein:
- de ontwikkeling en wettelijke verankering van uniforme toelatingseisen en van toezicht door de minister van BZK;
- technische voorzieningen, in het bijzonder de doorontwikkeling van het zogeheten BSN-koppelregister (dan wel een opvolger daarvan) voor massaal gebruik.

2 de ontwikkeling van publieke middelen op het hoogste beveiligingsniveau: de elektronische identiteitskaart (eNIK) en het elektronisch rijbewijs.

3 de voortgaande versterking van DigiD door middel van verdergaande beveiligingsmaatregelen en mogelijk een technologisch nieuwe versie.

Eigenaar van de voor het BSN-domein in te richten systematiek is de minister van BZK. Binnen die verantwoordelijkheid is Logius de tactisch beheerder van de toelatingseisen en het BSN-koppelregister. Het agentschap Telecom is de beoogd toezichthouder.

Met de focus op het BSN-domein, laat de minister van BZK de zorg voor de overige domeinen van het eID-stelsel over aan de minister van EZ.

Dit vereenvoudigt mogelijk de realisatie van oplossingen voor het BSN-domein, maar levert eveneens de uitdaging op om alsnog een samenhangend stelsel te bereiken voor digitale identificatie en authenticatie in zowel het publieke als private domein.

Bijlage 3
Onderzoeksopzet/-normen

Probleemstelling / onderzoeksvragen
Met ons onderzoek hebben we de vraag willen beantwoorden of ter onderbouwing van de besluitvorming over het eID-stelsel is voldaan aan randvoorwaarden op het terrein van governance (waaronder verantwoordelijkheden, doelstellingen en uitgangspunten), business case (zakelijke rechtvaardiging en alternatievenafweging) en toezicht.

Normen
Voor het onderdeel governance hebben we als normen gehanteerd dat de bestuurlijke eindverantwoordelijkheid voor het eID-stelsel eenduidig moet zijn en de doelstellingen, principes en uitgangspunten vooraf zijn uitgewerkt.
Voor het onderdeel business case hanteren we als norm dat voor het ontwikkelen en realiseren van het eID-stelsel een analyse is opgesteld die over de gehele levenscyclus een beeld geeft van de op te leveren producten / resultaten en van de (verwachte) kosten en baten. Tevens moet er een afweging van alternatieven zijn, waarbij een integraal beeld wordt gegeven van de kosten en baten van deze alternatieven.
Voor het onderdeel toezicht hanteren we als norm dat in de verschillende fasen van het eID-stelsel voorzien moet zijn in toezicht op de betrouwbaarheid, beveiliging en privacybescherming.

Onderzoeksactiviteiten
Ter beantwoording van de onderzoeksvragen hebben we relevante (beleids)documenten bestudeerd en interviews gehouden met onder andere ambtenaren van het Ministerie van BZK (directeur Informatiesamenleving en Overheid, gedelegeerd opdrachtgever eID, projectleider ontwikkeling publiek middel, directeur Financieel Economische Zaken, wetgevingsjurist Constitutionele Zaken en Wetgeving), het Ministerie van EZ (programma Idensys), het Ministerie van VWS, de Belastingdienst, RDW, Logius en RvIG. Daarnaast hebben we gesproken met deskundigen van de AP, AT, NCDO, BVN en de Radboud Universiteit.

Bijlage 4
Literatuur

BIT (2016). *BIT-advies programma eID; 12 mei 2016*. Bijlage bij Tweede Kamer, vergaderjaar 2015-2016, 26 643, nr. 414. Den Haag: Sdu.

BZK (2012). eID Stelsel NL, *Strategische verkenning en voorstel voor vervolg, oktober 2012*. Den Haag: Ministerie van BZK.

BZK (2013). *Informatie- en communicatietechnologie (ICT). Brief van de minister van BZK: visiebrief digitale overheid 2017*. Tweede Kamer, vergaderjaar 2012-2013, 26 643, nr. 280. Den Haag: Sdu.

BZK (2014). *Instelling Nationaal Commissaris Digitale Overheid*. Tweede Kamer, vergaderjaar 2013–2014, 26 643, nr. 314. Den Haag: Sdu.

BZK (2015). *Brief aan de Tweede Kamer van 14 december 2015*. Tweede Kamer, vergaderjaar 2015-2016, 26 643, nr. 379. Den Haag: Sdu.

BZK (2016). B*rief aan de Tweede Kamer van 17 juni 2016; reactie op BIT-advies programma eID*. Tweede Kamer, vergaderjaar 2015-2016, 26 643, nr. 414. Den Haag: Sdu.

BZK (2016a). Brief aan de Tweede Kamer van 25 augustus 2016 over Impuls eID. DGOO/DIO/DT&I, kenmerk: 2016-0000492258. Den Haag: BZK.

BZK en EZ (2013). *Brief aan de Tweede Kamer van 19 december 2013 over EID Stelsel*. Tweede Kamer, vergaderjaar 2013-2014, 26 643, nr. 299. Den Haag: Sdu.

BZK en EZ (2015). *Brief aan de Tweede Kamer van 9 februari 2015 over voortgang EID Stelsel*. Tweede Kamer, vergaderjaar 2014-2015, 26 643, nr. 349. Den Haag: Sdu.

EZ (2015). *Instellingsbesluit besturing elektronische toegangsdiensten. Besluit van de minister van EZ van 15 april 2015, nr. WJZ/15023462*. Stcrt. 2015 nr. 10829.

EZ (2016). *Instelling Commissie van Deskundigen voor het toezicht op het ETD-stelsel. Besluit van de minister van EZ van 14 april 2016 (met terugwerkende kracht tot 1 maart 2016), nr. WJZ/16008896*, Staatscourant 2016 nr. 20595.

Kuipers (2016). *Advies van de commissie evaluatie pilots publieke en private authenticatie-middelen (commissie-Kuipers)*. 31 mei 2016.

Mazars (2015). *Privacy Impact Assessment Introductieplateau eID Stelsel NL; 31 juli 2015.*

Tijdelijke Commissie ICT van de Tweede Kamer (2014). *Parlementair onderzoek ICT-projecten bij de overheid. Eindrapport*. Tweede Kamer, vergaderjaar 2014-2015, 33 326, nr. 5. Den Haag: Sdu.

Tijdelijke Commissie ICT van de Tweede Kamer (2014a). *Parlementair onderzoek ICT-projecten bij de overheid. Lijst van vragen en antwoorden (vraag 80)*. Tweede Kamer, vergaderjaar 2014-2015, 33 326, nr. 7. Den Haag: Sdu.

Bijlage 5
Noten

1 eID staat voor elektronische identificatie.
2 Visiebrief digitale overheid 2017 (BZK 2013).
3 Neer te leggen in de Wet Generieke Digitale Infrastructuur (GDI).
4 WID-documenten zijn documenten die op basis van de Wet op de identificatieplicht dienen ter vaststelling van de identiteit van personen.
5 eNIK en eRijbewijs zijn Nederlandse Identiteitskaarten (NIK) en rijbewijzen met een chip voorzien van eID-functionaliteit.
6 Bijlage 2 bevat een nadere toelichting op de componenten en de uitgangspunten van het eID-stelsel. Het begrip eID-stelsel wordt door anderen soms in een meer beperkte betekenis gebruikt. Zie bijvoorbeeld de brief van de minister van BZK van 20 juni 2014, waarin hij met het eID-stelsel het Afsprakenstelsel elektronische toegangsdiensten bedoelt (Tweede Kamer, vergaderjaar 2013–2014, 26 643, nr. 315). Tenzij anders aangeven, bedoelen wij steeds het eID-stelsel in brede zin.
7 Het Europese STORK (Secure idenTities acrOss boRders linKed) -kader voor grensoverschrijdend gebruik van digitale diensten, onderscheidt vier niveaus: (1) minimaal, (2) beperkt, (3) redelijk en (4) hoog. Met de introductie van de Europese verordening (nr. 910/2014) voor elektronische identificatie en vertrouwensdiensten (de eIDAS-verordening) wordt een onderscheid gemaakt tussen drie betrouwbaarheidsniveaus: laag, substantieel en hoog.
8 Het BSN-koppelregister legt ten behoeve de digitale dienstverlening in het BSN-domein de relatie tussen het authenticatiemiddel en het toepasselijke BSN.
9 Zie onder andere het Handboek Portfoliomanagement Rijk (3.02) en het toetsingskader van het Bureau ICT Toetsing (BIT).
10 Zie onder andere het Handboek Portfoliomanagement Rijk (3.02).
11 IRMA staat voor 'I Reveal My Attributes' en betreft een authenticatiesysteem in een decentrale vorm, waaraan een onderzoeksgroep van de Radboud Universiteit heeft gewerkt, onder leiding van professor Bart Jacobs.
12 Versie 1.10 van maart 2016.
13 Bijvoorbeeld de business case die als bijlage is meegestuurd met de voortgangsbrief van de ministers van BZK en EZ (2015) van 9 februari 2015 (Tweede Kamer, vergaderjaar 2014–2015, 26 643, nr. 349).
14 Het Europese STORK (Secure idenTities acrOss boRders linKed) -kader voor grensoverschrijdend gebruik van digitale diensten, onderscheidt vier niveaus: (1) minimaal, (2) beperkt, (3) redelijk en (4) hoog. Met de introductie van de Europese verordening (nr. 910/2014) voor elektronische identificatie en vertrouwensdiensten (de eIDAS-verordening) wordt een onderscheid gemaakt tussen drie betrouwbaarheidsniveaus: laag, substantieel en hoog.

Onderzoeksteam

Dhr. drs. J.G.L. (Hans) Benner RE RA (projectleider)
Dhr. ing. A. (Ab) Colon RE
Mw. mr. M. (Marion) Janson
Mw. T. (Tanja) Koeckhoven BSc
Dhr. H.J. (DirkJan) Klip MSc MPIM

Voorlichting

Afdeling Communicatie
Postbus 20015
2500 EA Den Haag
telefoon (070) 342 44 00
voorlichting@rekenkamer.nl
www.rekenkamer.nl

Omslag

Ontwerp: Corps Ontwerpers
Foto: Getty Images / Danil Melekhin

Infographics

Joris Fiselier Infographics

Den Haag, september 2016