Digitale identiteit vraagt veel van DigiD en eHerkenning

2023

Algemene Rekenkamer

Inhoud

1. Samenvatting en conclusies

Wij hebben onderzoek gedaan naar DigiD en eHerkenning. Dat zijn digitale authenticatiemiddelen die controleren of burgers en bedrijven zijn wie ze zeggen te zijn. De minister van Binnenlandse Zaken en Koninkrijksrelaties (BZK) is verantwoordelijk voor DigiD en het stelsel voor eHerkenning.
Wij concluderen dat DigiD en eHerkenning op dit moment toereikend functioneren. Wel maken wij ons zorgen om digitale authenticatie in de toekomst. Met ingang van 1 juli 2023 verandert namelijk het stelsel voor digitale authenticatie. Dan treedt de Wet digitale overheid (Wdo) in werking. De Europese Commissie heeft daarnaast een voorstel gedaan voor een verordening voor een Europese digitale identiteit.
Vanwege de veiligheid is het in de toekomst alleen mogelijk om via een app in te loggen met DigiD. Zo raken niet-digivaardige burgers verder achterop. Deze burgers, maar ook burgers met meer complexe vraagstukken, moeten vertegenwoordigd kunnen worden en hulp kunnen krijgen bij een loket. Dat kan beter.

Doelen grotendeels bereikt

De oorspronkelijke doelen voor digitale authenticatie zijn grotendeels bereikt. We lichten er 2 uit in deze samenvatting. Het doel voor ‘gebruik in Nederland’ is bereikt. Burgers en bedrijven gebruiken massaal DigiD en eHerkenning. Het doel ‘voorkomen van fraude’ is gedeeltelijk bereikt. De minister van BZK heeft geen goed kwalitatief en kwantitatief beeld van het voorkomen van fraude. Dat komt doordat de verantwoordelijkheid voor het voorkomen van fraude is verspreid over veel organisaties.

Baten wegen op tegen de kosten

De baten van DigiD en eHerkenning lijken op te wegen tegen de kosten. Een exacte berekening is niet te maken. De baten liggen vooral in tijdswinst voor de overheid en maatschappij. We hebben geen aanwijzingen voor ondoelmatigheid van DigiD of eHerkenning gevonden.

Kwaliteit voldoende beheerst

In algemene zin staat veiligheid van IT-dienstverlening en data voortdurend onder druk doordat nieuwe uitdagingen zich continu voor zullen doen. De minister van BZK treft voldoende maatregelen om ervoor te zorgen dat DigiD en eHerkenning beschikbaar en veilig zijn. Wel moet ze voor eHerkenning beter aantonen dat de maatregelen ook in de praktijk gevolgd worden. We concluderen verder dat er te weinig zicht is op de totaalarchitectuur. Hiermee bedoelen we de samenhang van alle componenten die nodig zijn om DigiD en eHerkenning te laten werken. Dit is belangrijk, zeker omdat het stelsel gaat veranderen. Een gedeeld inzicht en overzicht is nodig om het nieuwe stelsel goed in te richten en te laten werken.

Wet digitale overheid gaat in per 1 juli 2023

De Wet digitale overheid (Wdo) verandert het stelsel met ingang van 1 juli 2023. Er komen authenticatiemiddelen naast DigiD en eHerkenning. Daarvoor moet er een technisch aansluitpunt komen waar alle authenticatiemiddelen samenkomen. Dan hoeven uitvoerende organisaties zoals UWV, Belastingdienst en gemeenten slechts op één centraal punt aan te sluiten. Dit aansluitpunt is er niet.

Europese digitale identiteit en *wallet* op komst

Indien de Raad van de Europese Unie en het Europees Parlement daar mee instemmen, komt er ook een Europese digitale identiteit. Concreet is dit de *wallet*. Dit is een digitale portemonnee met (identiteits)gegevens, die een burger of bedrijf kan delen met publieke en private partijen. Met de *wallet* kunnen burgers en bedrijven ook inloggen, net als met DigiD en eHerkenning. Het zou in de toekomst kunnen dat veel authenticaties met de *wallet* worden gedaan en minder met DigiD of eHerkenning. Er is nog veel onduidelijkheid over hoe de *wallet* er uit komt te zien en hoe deze past in het stelsel voor digitale authenticatie. Belangrijk is dat de *wallet* kwalitatief dezelfde authenticatie biedt als DigiD en eHerkenning.

Hogere betrouwbaarheidsniveaus lastig voor niet-digivaardigen

Overheden en uitvoerende organisaties kiezen ten behoeve van betere beveiliging voor steeds hogere betrouwbaarheidsniveaus. Hierdoor wordt het voor niet-digivaardigen in de samenleving lastiger om DigiD te gebruiken. Sinds 1 oktober 2022 is het bijvoorbeeld bij Mijn Belastingdienst niet meer mogelijk om alleen met gebruikersnaam en wachtwoord in te loggen. Er vindt een extra sms-controle plaats. In de toekomst zal ook inloggen met sms uitgefaseerd worden. Dan is het alleen nog maar mogelijk om met de app in te loggen. Voor niet-digivaardigen is dit lastig, omdat juist zij veelal geen smartphone hebben of onvoldoende vaardig zijn om deze ten volle te kunnen gebruiken. De minister van BZK dient beveiliging en toegankelijkheid zorgvuldig af te wegen.

Ondersteuning niet-digivaardigen en burgers met complexe problematiek kan beter

Om de toegankelijkheid te borgen moet de minister van BZK ervoor zorgen dat digitale vertegenwoordiging op orde komt. Niet-digivaardigen moeten iemand kunnen machtigen om voor hen bij DigiD in te loggen en (overheids)zaken te regelen, zodat zij goed geholpen worden. Machtigen op eigen verzoek kan momenteel wel, maar wettelijke vertegenwoordigers kunnen niet namens een ander inloggen. We praten dan over bewindvoerders, curatoren en ouders.

Verder wil de overheid zorgen voor ondersteuning van niet-digivaardigen vanuit een overheidsloket. Daarvoor zijn nu Informatiepunten Digitale Overheid (IDO's) bij bibliotheken ingericht. Ook digivaardige burgers hebben een (fysiek) loket nodig. Bijvoorbeeld bij complexe zaken die niet via digitale formulieren zijn af te handelen. Te denken valt dan aan onterechte vermeldingen van burgers in frauderegisters, genderveranderingen, immigratie-/emigratieproblemen, et cetera. Naast IDO's kunnen ook gemeenteloketten hiervoor een goede plaats zijn. Wij constateren dat IDO-medewerkers maar tot op bepaalde hoogte kunnen helpen, omdat ze beperkte mogelijkheden en bevoegdheden hebben. We bevelen de minister van BZK aan te onderzoeken of meer bevoegdheden voor IDO-medewerkers rond het aanvragen van DigiD passen in de doorontwikkeling van de IDO's, zodat burgers beter ondersteund kunnen worden.

2. Over dit onderzoek

2.1 Waarom dit onderzoek?

De wereld digitaliseert. Het maatschappelijk handelen van burgers, bedrijven en overheid gebeurt steeds meer digitaal. Digitale authenticatie – *bent u wie u zegt dat u bent* – is voor veel van dit handelen inmiddels een randvoorwaarde. Denk bijvoorbeeld aan de CoronaCheck-app of de digitale belastingaangifte.

We hebben onderzoek gedaan naar 2 authenticatiemiddelen: DigiD en eHerkenning. Dit zijn momenteel de enige centrale authenticatiemiddelen die burgers en bedrijven kunnen gebruiken om in te loggen bij online overheidsdienstverlening in Nederland. We wilden weten:

- of DigiD en eHerkenning de juiste functionaliteiten bevatten – zoals machtigen – en of deze authenticatiemiddelen continu beschikbaar en veilig zijn;
- wat DigiD en eHerkenning de samenleving kosten en opleveren;
- of DigiD en eHerkenning klaar zijn voor de toekomst.

Een paar belangrijke begrippen

Digitale identiteit: een verzameling van betrouwbare gegevens die een persoon of organisatie representeert in het digitale domein.
Identificatie: het uniek duiden van een persoon of organisatie – wie of wat is het?
Authenticatie: het bevestigen van de identiteit – bent u wie u zegt dat u bent?
Autorisatie: het bepalen of iemand toegang mag krijgen tot een bepaalde dienst of informatie.
Momenteel zijn er nog geen middelen die voorzien in een digitale identiteit zoals hierboven gedefinieerd. Wel zijn er middelen voor digitale authenticatie: DigiD voor burgers en eHerkenning voor bedrijven. Overigens, DigiD en eHerkenning zijn eigenlijk 'diensten', maar voor de leesbaarheid gebruiken we steeds '**(authenticatie)middelen**'.

Vanaf juli 2023 verandert de wet- en regelgeving op het gebied van authenticatie. Dan gaat de Wet digitale overheid (Wdo) in. Deze wet regelt dat er private authenticatie-middelen kunnen komen naast het publieke DigiD. Ook regelt de Wdo dat er een publiek middel komt voor bedrijven, naast het private eHerkenning. Dit laatste gebeurt in het tweede deel van de wet, de zogeheten 'tweede tranche'.[1] Daarvan is de datum van invoering nog niet bekend.

Een tweede belangrijke verandering is het voorstel voor de Europese verordening *electronic identification and trust services* (eIDAS2). De ingangsdatum van deze verordening is nog niet bekend. De verordening schrijft voor dat elke lidstaat een 'gratis' *wallet* moet aanbieden. Dit is een digitale portemonnee met (identiteits)gegevens, die een burger of bedrijf kan delen met publieke en private partijen. Met de *wallet* kunnen burgers en bedrijven ook inloggen, zoals nu met DigiD en eHerkenning.

2.2 Wat hebben we onderzocht en hoe hebben we dat gedaan?

We gaan in deze paragraaf in op onze onderzoeksvragen en hoe we deze onderzochten. Dit doen we op hoofdlijnen. Voor een uitgebreidere methodologische verantwoording verwijzen we naar bijlage 1.

We stelden ons de volgende onderzoeksvragen:

1. In hoeverre zijn de doelen voor digitale identiteit en voor de nu beschikbare diensten DigiD en eHerkenning gerealiseerd?
We onderzochten in hoeverre de doelen bereikt zijn, die de minister van Binnenlandse Zaken en Koninkrijksrelaties (BZK) zich vanaf 2013 stelde. We onderzochten doelen voor gebruik/adoptie, functionaliteit en veiligheid. We verzamelden hiervoor documentatie en hielden interviews.

2. Hoe doelmatig zijn eHerkenning en DigiD vergeleken met elkaar en in vergelijking met een ander authenticatiemiddel of vergelijkbare dienst in binnen- of buitenland?
We brachten de kosten in beeld voor DigiD en eHerkenning. Dit deden we specifiek voor de jaren 2019 t/m 2021. Ook onderzochten we de mogelijke baten. We wilden de authenticatiemiddelen met een authenticatiemiddel in het buitenland kunnen vergelijken. Hiervoor hebben we een enquête uitgezet bij rekenkamers van Europese landen.

3. In hoeverre beheerst de overheid de kwaliteit van DigiD en eHerkenning?
Met kwaliteit bedoelen we de beschikbaarheid, integriteit en exclusiviteit van DigiD en eHerkenning. Respectievelijk betekenen deze begrippen dat de authenticatiemiddelen het moeten doen op de momenten dat gebruikers ze nodig hebben, dat de gegevens moeten kloppen en dat alleen de juiste personen bij systemen en gegevens kunnen komen.

We hebben hier een uitgebreid toetsingskader voor opgesteld, te vinden in § 4.4.1.
De toetsing hebben we gedaan aan de hand van documentatie en interviews.

We hebben DigiD en eHerkenning ook onderzocht in het licht van de Wdo en eIDAS2.
Dit is gedaan door wetsteksten en documentatie te analyseren en interviews te houden.

2.3 Leeswijzer

Dit rapport bestaat uit de volgende onderdelen. In hoofdstuk 3 beschrijven we de werking van DigiD en eHerkenning nu. In hoofdstuk 4 beantwoorden we onze onderzoeksvragen over doelen, doelmatigheid en kwaliteitsbeheersing. Hoofdstuk 5 bevat onze beschouwing op de Wdo en eIDAS2. Vervolgens gaan we in hoofdstuk 6 nader in op de afweging tussen betrouwbaarheidsniveaus en dienstverlening aan niet-digivaardigen.

3. DigiD en eHerkenning

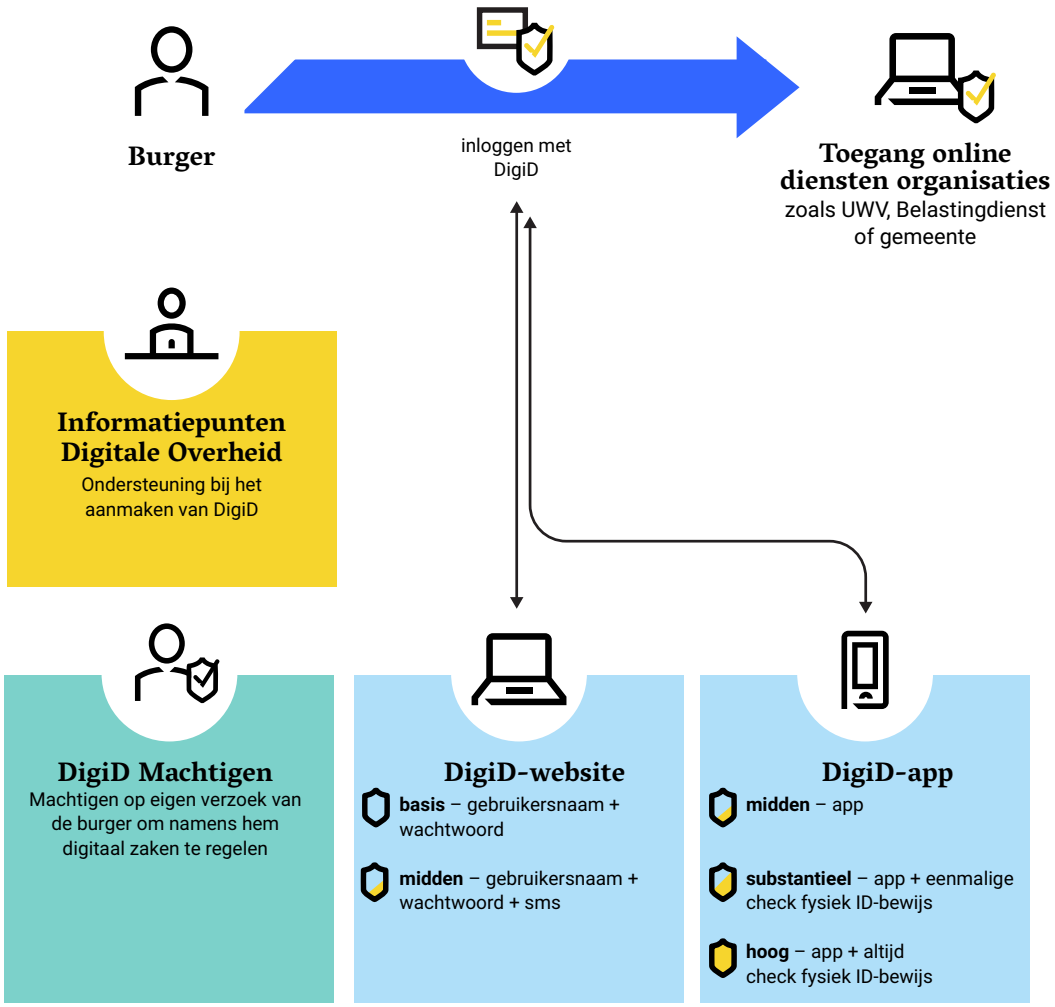
We lichten in dit hoofdstuk DigiD en eHerkenning toe. We gaan in op het ontstaan en hoe de authenticatiemiddelen momenteel functioneren.

3.1 DigiD

De naam DigiD is de afkorting van ‘Digitale Identiteit’. DigiD is in 2003 in het gemeentelijke domein van start gegaan als een middel om digitale loketdiensten te kunnen aanbieden. De Belastingdienst heeft DigiD vanaf januari 2005 in beheer genomen. Hierna volgde brede adoptie en gebruik. Het beheer ligt nu bij het agentschap Logius, onderdeel van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK).

DigiD heeft tegenwoordig in de basis nog dezelfde functie als in 2003: burgers kunnen via DigiD inloggen om toegang te verkrijgen tot online dienstverlening. Uitvoerende partijen zoals UWV, Belastingdienst en gemeenten weten zo wie de burger is die wil inloggen. Inloggen kan ondertussen met verschillende betrouwbaarheidsniveaus, waarbij bijvoorbeeld een app nodig is. Verder is er een machtigingsvoorziening voor machtigen op eigen verzoek en kunnen burgers onder andere terecht bij de Informatiepunten Digitale Overheid voor hulp. In figuur 1 is dit alles weergegeven.

Figuur 1 *Werking DigiD in de huidige situatie*



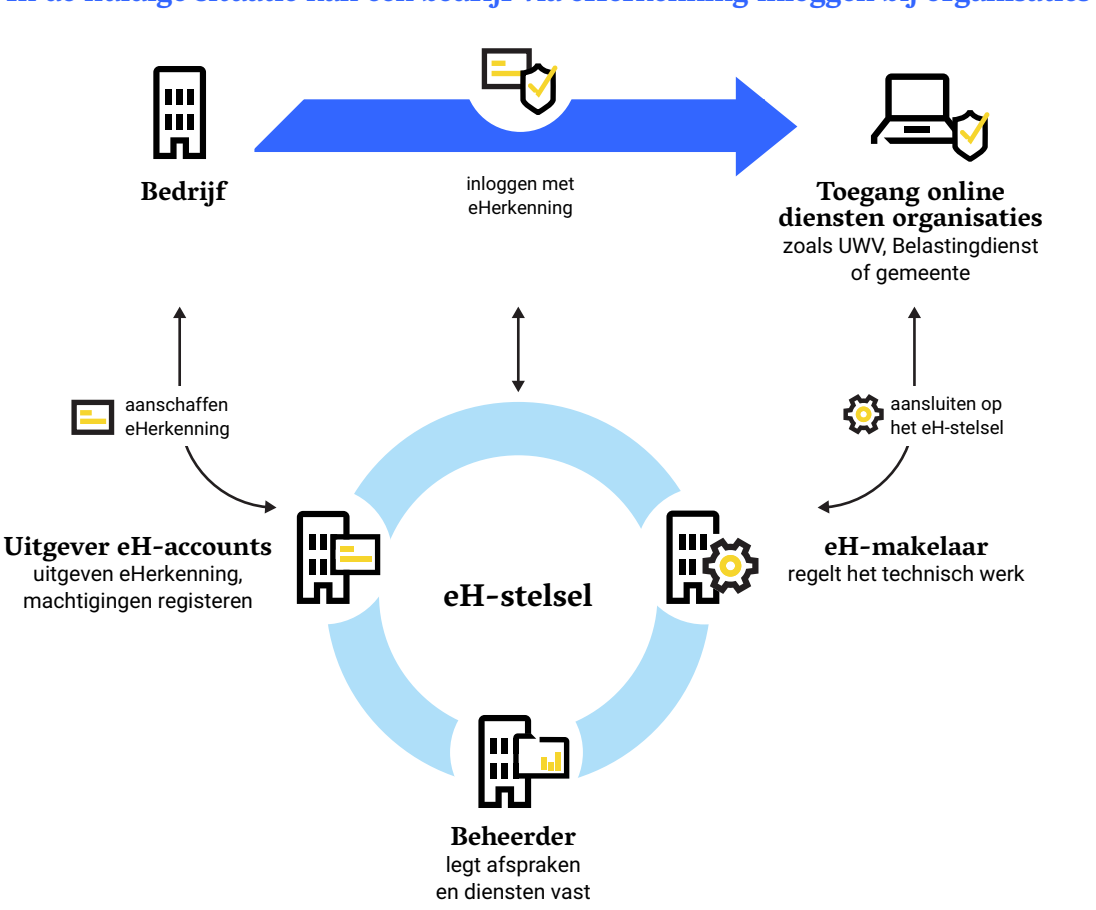
3.2 eHerkenning

In 2009 heeft het Ministerie van Economische Zaken (EZ) samen met commerciële partijen eHerkenning ontwikkeld. Het is de opvolger van 'DigiD voor bedrijven'. Tot dan toe ontbrak een inlogvoorziening voor bedrijven om betrouwbaar en veilig online zaken te doen met de overheid. In 2010 sloot het toenmalige Agentschap NL als eerste grote dienstverlener aan op eHerkenning. Agentschap NL ging in 2014 op in de Rijksdienst voor Ondernemend Nederland (RVO).

eHerkenning is een afsprakenstelsel met een netwerk van publieke en private partijen. Dit netwerk levert toegangsdiensten. Vandaar ook dat dit het Elektronische Toegangs-diensten-stelsel (ETD-stelsel) wordt genoemd. Het afsprakenstelsel is openbaar beschikbaar.[2]

In figuur 2 wordt dit stelsel weergegeven.[3] eHerkenning regelt in de basis de herkenning (authenticatie) en controleert de bevoegdheid (autorisatie) van personen die online een dienst willen afnemen. Ondernemers kunnen een account voor eHerkenning aanvragen bij private leveranciers die de rijksoverheid heeft erkend. In de figuur de uitgever van eH-accounts. Overheden kunnen aansluiten op eHerkenning met een zogenaamde eHerkenningsmakelaar, ook een private partij. Logius is de stelselbeheerder, de overheidspartij die de afspraken bijhoudt. Logius maakt bijvoorbeeld openbaar welke diensten worden aangeboden middels eHerkenning.

Figuur 2 *Werking eHerkenning in de huidige situatie*



4. Beoordeling van DigiD en eHerkenning

In dit hoofdstuk beoordelen we DigiD en eHerkenning en geven we antwoord op de onderzoeksvragen.

4.1 Conclusies

De digitale authenticatiemiddelen DigiD en eHerkenning functioneren momenteel toereikend. Dit oordeel baseren we op de volgende bevindingen.

- De minister van BZK stelde de afgelopen 10 jaar doelen voor digitale identiteit en authenticatie. Deze zijn grotendeels bereikt. We onderscheiden de categorieën gebruik, functionaliteit en veiligheid. We lichten de meest relevante doelen toe. Het doel voor 'gebruik in Nederland' is bereikt: burgers en bedrijven gebruiken massaal DigiD en eHerkenning. Voor de categorie 'functionaliteit' was een doel digitaal inloggen door 'wettelijke vertegenwoordiging'. We praten dan over bewindvoerders, curatoren en ouders. Dit doel is nog niet bereikt: wettelijke vertegenwoordigers kunnen nog niet namens bijvoorbeeld een niet-digivaardige inloggen. 'Machtigen op eigen verzoek' kan wel, dit doel is wel bereikt. Voor de categorie 'veiligheid' lichten we het doel 'voorkomen van fraude' toe. Dit doel is gedeeltelijk bereikt. Logius heeft een hiervoor wel een team fraude en misbruik, maar er is geen goed kwalitatief en kwantitatief beeld van het voorkomen van fraude. Dat komt doordat de verantwoordelijkheid voor het voorkomen van fraude is verspreid over veel organisaties.

- De baten van DigiD en eHerkenning lijken op te wegen tegen de kosten. De baten liggen vooral in tijdswinst voor de maatschappij en bij de overheid die diensten verleent. We hebben geen aanwijzingen voor ondoelmatigheid van DigiD of eHerkenning gevonden. Een exacte berekening of vergelijking tussen beide authenticatiemiddelen en een buitenlands authenticatiemiddel is niet te maken, omdat er te veel variabelen zijn en te veel gegevens ontbreken.
- De minister van BZK treft voldoende maatregelen om ervoor te zorgen dat DigiD en eHerkenning beschikbaar en veilig zijn. Wel moet ze voor eHerkenning beter aantonen dat de maatregelen ook in de praktijk gevolgd worden. Aanvullend vinden we dat er te weinig zicht is op de totaalarchitectuur. Hiermee bedoelen we de samenhang van alle componenten die nodig zijn om DigiD en eHerkenning goed te laten werken. Dit is belangrijk omdat het stelsel gaat veranderen. Een gedeeld inzicht en overzicht is nodig om het nieuwe stelsel goed in te richten en te laten werken.

4.2 Resultaten DigiD en eHerkenning

We stelden de volgende onderzoeksvraag: *in hoeverre zijn de doelen voor digitale identiteit en voor de nu beschikbare diensten DigiD en eHerkenning gerealiseerd?*
De afgelopen 10 jaar heeft de minister van BZK zichzelf doelen gesteld voor digitale identiteit en authenticatie. Wij toetsten of deze zijn bereikt. In de onderstaande tekst geven we per doel aan in hoeverre dit bereikt is. We rapporteren alleen over de in onze ogen meest relevante doelen. In bijlage 2 staat een uitgebreid toetsingskader, waarin we oordelen over alle door ons geïnventariseerde doelen. In deze bijlage worden de doelen beschreven en worden de bronnen benoemd waaruit deze doelen zijn overgenomen of afgeleid.

4.2.1 Doelen gebruik

Gebruik in Nederland
De minister van BZK had vanaf 2013 als doel middelen aan te bieden die interactie en digitale dienstverlening met de overheid en private partijen in de EU mogelijk maken. Wij constateren dat dit doel (groten)deels is bereikt. Dit gezien de hoeveelheid diensten die nu digitaal wordt aangeboden via DigiD of eHerkenning. Zowel publieke partijen (zoals UWV, Belastingdienst en gemeenten) als private partijen met een publieke taak (zoals pensioenfondsen en verzekeraars) bieden hun diensten aan via DigiD of eHerkenning. In 2021 boden 735 organisaties hun diensten aan via DigiD en waren er 16,5 miljoen actieve DigiD-accounts.[4] In 2021 boden 537 organisaties hun diensten aan via eHerkenning en waren er 767.700 eHerkenning-accounts.[5]

Sommige dienstverleners bieden meerdere diensten aan. De RVO is daar een voorbeeld van. RVO ontsluit onder andere diensten als perceelregistratie voor landbouwbedrijven, innovatiekredieten voor ondernemers en diverse subsidieregelingen met eHerkenning. De volgende tabellen bieden een overzicht van de jaren 2018 t/m 2021.

Tabel 1 *Kengetallen DigiD (ICTU, 2022)*

	2018	2019	2020	2021
Aangesloten organisaties	647	663	701	735
Aangesloten diensten	945	1.023	1.124	1.457
Actieve accounts	13.772.269	15.023.119	18.320.835	16.515.691[6]
Authenticaties	307.956.118	340.758.404	402.519.872	557.008.812

Tabel 2 *Kengetallen eHerkenning (ICTU, 2022)*

	2018	2019	2020	2021
Aangesloten dienstverleners	403	443	493	537
Aantal aangesloten diensten	1.383	1.686	1.927	2.083
Aantal organisaties met eHerkenning	226.504	276.953	526.643	692.041
Aantal uitgegeven eHerkennings-middelen/-accounts	285.969	383.994	609.387	767.700
Aantal authenticaties	5.499.618	9.160.456	15.499.531	16.973.001

Gebruik in de EU

De minister van BZK stelde zich ook doelen voor het inloggen in andere Europese landen. Hiervoor bestaat het zogenoemde eIDAS-netwerk. In § 5.3.1 gaan we hier nader op in. Met eIDAS is het mogelijk om in andere Europese landen met bijvoorbeeld DigiD in te loggen bij aangesloten dienstverleners, zoals gemeenten of de nationale belastingdienst. Andersom is dit ook mogelijk. Een Duitse burger kan met diens Duitse inlogmiddel bijvoorbeeld bij de Nederlandse Belastingdienst inloggen.

Voor deze EU-transacties liggen de aantallen lager:

- *Inkomend verkeer uit de EU:* in oktober 2022 zijn 275 Nederlandse overheidsdienstverleners of dienstverleners met een publieke taak aangesloten op het eIDAS-netwerk. Deze leveren in totaal 390 diensten. Het totaal aan authenticaties in de maand oktober bedraagt 10.242 (inkomend).

- *Uitgaand verkeer naar de EU:* Deze aantallen liggen nog lager: 4.263 transacties. Er is geen duidelijk beeld van hoeveel overheidsorganisaties en/of organisaties met een publieke taak nog moeten aansluiten op het eIDAS-netwerk. We hebben niet kunnen vaststellen in hoeverre burgers en bedrijven uit Nederland in het kader van eIDAS dezelfde zaken kunnen regelen als andere burgers en bedrijven in andere lidstaten. Hiervoor hebben we ook geen concrete doelstellingen aangetroffen. Het lage aantal transacties is een reden dat eIDAS is herzien en er nu sprake is van eIDAS2.

Gebruik via mobiel

Nog een doel voor 'gebruik' is dat de authenticatiemiddelen geschikt moeten zijn voor mobiele apparaten. Voor DigiD is dit doel bereikt. Kanttekening is wel dat de DigiD-app alleen werkt via het Google- en Apple-platform. Daarvoor moet de burger zich verplicht registreren bij Google of Apple. Als sms in de toekomst is uitgefaseerd en je alleen nog maar met de app kan inloggen, zal elke burger dit moeten doen. Zie § 6.2 voor meer details hierover. Voor eHerkenning is het doel gedeeltelijk bereikt: nog niet alle eHerkenningsleveranciers bieden apps aan.

Toegankelijkheid bij beperkingen

DigiD en eHerkenning moeten toegankelijk zijn. Burgers en ondernemers met bijvoorbeeld een visuele beperking moeten de authenticatiemiddelen ook kunnen gebruiken, met assistentie wanneer nodig. Niet alle onderdelen van DigiD zijn volledig toegankelijk. Voor eHerkenningsleveranciers geldt hetzelfde. Dit doel is dan ook gedeeltelijk bereikt.

Betrouwbaarheidsniveaus

Een doel dat voor zowel DigiD als eHerkenning bereikt is, is dat de authenticatiemiddelen verschillende betrouwbaarheidsniveaus moeten hebben. Dit heeft te maken met de classificatie van de gegevens en de aard van de diensten die ermee worden ontsloten. We gaan uitgebreid in op betrouwbaarheidsniveaus in § 6.2.

4.2.2 Doelen functionaliteit

De minister stelde zichzelf verschillende doelen over wat de middelen zouden moeten kunnen. Bijvoorbeeld: de identiteit vaststellen, bewijzen van bevoegdheden, je laten vertegenwoordigen en het mogelijk maken van een digitale wilsuiting/handtekening.

Identiteit vaststellen

Het doel 'identiteit vaststellen' is bereikt. Met de diensten DigiD en eHerkenning kunnen burgers en bedrijven zich authenticeren voor digitale diensten. Hierbij wordt de identiteit van betreffende burgers en/of bedrijven vastgesteld.

Machtigen en vertegenwoordigen
Het doel 'machtigen en vertegenwoordigen' is bij DigiD niet geheel bereikt, maar bij eHerkenning wel. Als burger maak je bij digitale dienstverlening van de overheid gebruik van DigiD. Dit kun je ook voor of namens anderen doen. De andere persoon moet je daarvoor machtigen. Bij DigiD is het zogenaamde DigiD Machtigen daarvoor beschikbaar. Hiermee kan iemand worden gemachtigd om 1 specifieke dienst voor/namens een andere persoon te doen. Het is niet mogelijk een persoon voor alles te machtigen.

In sommige gevallen ligt het voor de hand dat je *automatisch* de bevoegdheid hebt om namens iemand te handelen met je eigen DigiD, omdat je de wettelijke vertegenwoordiger bent. Bijvoorbeeld als het gaat om je kind of als je curator bent of als je de vertegenwoordiger van een handelingsonbekwaam familielid bent. Hiervoor lopen proeven. De realisatie zal pas over enkele jaren afgerond zijn. Dit doel is dus niet bereikt. Zie voor meer details § 6.3.2.

Bedrijven en organisaties gebruiken eHerkenning om in te loggen bij overheidsdienstverlening. Bedrijven moeten aangeven welke persoon binnen het bedrijf mag handelen. Dit is het zogenaamde 'verticale machtigen'. Als het nodig is dat een andere organisatie of bedrijf namens jou optreedt, kan dat met een zogenaamde 'ketenmachtiging'.

Bij eHerkenning kun je je dus wettelijk laten vertegenwoordigen, maar bij DigiD kan dat nog niet. In § 6.3 gaan we hier nader op in.

Wilsuiting en digitale handtekening
Dit doel is bereikt. Met DigiD en eHerkenning kunnen burgers en bedrijven een wilsuiting bevestigen of instemmen met de inhoud van een transactie. Een voorbeeld daarvan is de aangifte inkomstenbelasting, die wordt 'ondertekend' met DigiD. Een zogenaamde gekwalificeerde handtekening[7] zetten – volgens EU-wet- en regelgeving – kan niet met DigiD en eHerkenning, maar wel met andere middelen, die private marktpartijen aanbieden.

4.2.3 Doelen veiligheid
In de IT-audit – zie § 4.4 – hebben we onderzocht of DigiD en eHerkenning voldoende oog hebben voor informatiebeveiliging om gegevens van burgers en bedrijven te beschermen. Een specifiek doel van de minister bespreken we in deze paragraaf: dat de authenticatiemiddelen identiteitsfraude of oneigenlijk gebruik moeten voorkomen.

Logius heeft voor DigiD een intern team ‘Fraude en Misbruik’. Verder zijn er voor signalen over fraude met DigiD en eHerkenning de volgende kanalen:

- Nationale Ombudsman;
- Landelijke Fraude Helpdesk;
- Centraal Meldpunt Identiteitsfraude (CMI);
- Helpdesk/Klant Contact Centrum (KCC) Logius.

Voor eHerkenning bestaat geen overkoepelende organisatie die fraudegevallen oppakt en er is geen centraal fraudemeldpunt.[8] Het stelsel is nu zo ingericht dat het delen van opmerkelijke zaken in het algemeen tussen partijen van mogelijk misbruik op de identificatie wel centraal mogelijk is. Maar het melden van en reageren op specifieke signalen en meldingen ligt decentraal: bij de organisaties zelf, bij de leverancier en/of dienstverlener.

We constateren voor zowel DigiD als eHerkenning dat het voorkomen van en reageren op fraude verspreid is over verschillende partijen. Hierdoor ontbreekt er een goed kwalitatief en kwantitatief beeld. Dit heeft als risico dat zaken langs elkaar heen lopen en fraude minder effectief wordt voorkomen dan wanneer dit beeld er wel zou zijn. Het doel ‘voorkomen van identiteitsfraude’ is dan ook gedeeltelijk bereikt.

4.3 Kosten en baten van DigiD en eHerkenning

We stelden de volgende onderzoeksvraag: *hoe doelmatig zijn eHerkenning en DigiD vergeleken met elkaar en in vergelijking met een ander authenticatiemiddel of vergelijkbare dienst in binnen- of buitenland?*

We kunnen niet uitdrukken in welke mate de authenticatiemiddelen doelmatig zijn. We kunnen wel aangeven dat we geen aanwijzingen vonden voor ondoelmatigheid van DigiD of eHerkenning. Een exacte berekening of vergelijking tussen beide authenticatiemiddelen en een buitenlands authenticatiemiddel is niet te maken, omdat er te veel variabelen zijn en te veel gegevens ontbreken.
Het is echter wel aannemelijk dat de baten van DigiD en eHerkenning opwegen tegen de kosten.

4.3.1 Kosten

De totale maatschappelijke kosten van DigiD en eHerkenning zijn niet in kaart te brengen. Daarvoor zouden alle aansluitkosten bekend moeten zijn voor uitvoerende organisaties als UWV, Belastingdienst en gemeenten – en dat blijkt niet het geval. Ook is niet bekend hoeveel moeite het kost voor burgers en bedrijven om een account

aan te maken. Deze gegevens zijn beperkt of niet beschikbaar. We beperken ons daarom tot de kosten die wel bekend zijn en die direct betrekking hebben op de ontwikkeling, het beheer en de exploitatie van DigiD en eHerkenning.

Die directe kosten[9] van DigiD voor de rijksoverheid zijn als volgt:

Tabel 3 *Kosten voor de rijksoverheid voor DigiD voor ontwikkeling, beheer en exploitatie (BZK, 2019, 2020, 2021a en 2022a)*

	2018	2019	2020	2021
Ontwikkeling, beheer en exploitatie	€ 34.124.000	€ 28.567.000	€ 32.218.000	€ 46.240.000

Uit deze tabel blijkt dat de kosten in 2018, 2019 en 2020 een vergelijkbare grootte hebben, maar in 2021 flink hoger liggen. Deze hogere kosten zijn grotendeels een gevolg van de coronapandemie. DigiD werd gebruikt als inlogmiddel voor het plannen van coronatesten en het opvragen van testuitslagen (BZK, 2022a).
Het Ministerie van BZK financiert deze kosten. Daarnaast levert het Ministerie van BZK nog een jaarlijkse bijdrage aan het Ministerie van Buitenlandse Zaken (BZ) en gemeenten voor de uitgifte van DigiD in het buitenland en aan niet-ingezetenen. In 2021 bedroeg deze bijdrage € 435.000.

De directe kosten voor DigiD Machtigen voor de rijksoverheid zijn als volgt:[10]

Tabel 4 *Kosten voor de rijksoverheid voor DigiD Machtigen voor ontwikkeling, beheer en exploitatie (BZK, 2019, 2020, 2021a en 2022a)*

	2018	2019	2020	2021
Ontwikkeling, beheer, exploitatie	€ 11.053.000	€ 12.772.000	€ 14.215.000	€ 17.449.000

De directe kosten voor eHerkenning voor de rijksoverheid zijn als volgt:

Tabel 5 *Begrote kosten ontwikkeling, beheer en exploitatie van stelselvoorzieningen eHerkenning voor de rijksoverheid[11] (Logius.nl)*

	2018	2019	2020	2021
Ontwikkeling, beheer, exploitatie	€ 3.016.000	€ 3.600.000	€ 3.786.000	€ 3.961.000

Het Ministerie van BZK draagt daarnaast financieel bij aan toezicht op het stelsel voor eHerkenning. Deze kosten zijn jaarlijks ruim € 1,5 miljoen.

Een vergelijking tussen de kosten van DigiD en eHerkenning is niet zomaar te maken. Voor DigiD zitten de kosten voor het uitgeven van accounts al in bovenstaande kosten. Bij eHerkenning geven private partijen accounts uit. Hun boekhoudingen zijn voor ons niet inzichtelijk. Wat we wel konden doen, is het bedrag schatten: ongeveer € 20 miljoen in 2021.[12]

De kosten voor een vergelijkbaar middel als DigiD en eHerkenning in het buitenland zijn nog moeilijker te achterhalen. Dit komt doordat de middelen behoorlijk kunnen verschillen in functionaliteiten. Ook is er vaak geen goed inzicht in de betreffende kosten. Slechts 1 land (Letland) had gegevens over de afgelopen 4 jaar en een middel (eParaksts) dat enigszins vergelijkbaar is met DigiD. Dit middel kost jaarlijks circa € 2,5 miljoen.[13]

Afhankelijk van wat er in de berekening wordt meegenomen, zijn de kosten zoals in deze paragraaf beschreven voor DigiD, DigiD Machtigen en eHerkenning bij elkaar opgeteld grofweg jaarlijks zo'n krappe € 100 miljoen. Dit is belangrijk om in het achterhoofd te houden bij het lezen van de volgende paragraaf.

4.3.2 Baten

Het is aannemelijk dat de baten van het *hele stelsel* van digitale dienstverlening opwegen tegen de kosten. Ook voor de baten geldt dat deze lastig toe te schrijven zijn aan individuele middelen. Zonder DigiD en eHerkenning kan niet worden ingelogd. Deze authenticatiemiddelen zijn randvoorwaardelijk en dragen in grote mate bij aan de baten van digitale dienstverlening.

Digitale dienstverlening leidt met name tot tijdbesparing, voor zowel burgers en bedrijven als uitvoerende organisaties als UWV, Belastingdienst en gemeenten. We hebben geen zicht op de tijdsbesparing van bedrijven en organisaties. Voor burgers stellen we – mede op basis van vergelijkbare studies - dat een digitale transactie met de overheid de burger gemiddeld een kwartier tijdsbesparing oplevert (Ecorys, 2016 en 2018). Bij een gemiddeld uurloon van € 24 levert dit € 6 op. Het aantal transacties voor DigiD in 2021 is ruim 550 miljoen.[14] Het is te kort door de bocht om deze getallen te vermenigvuldigen, onder meer omdat de authenticatie slechts een onderdeel van de totale transactie is. Wel achten wij het hierdoor zeer aannemelijk dat de baten opwegen tegen de kosten. Daarnaast besparen digitale transacties aanzienlijk in papier- en transportkosten.

Als de 'centrale' authenticatiemiddelen DigiD en eHerkenning er niet zouden zijn, zouden diensten of sectoren andere manieren moeten inregelen om burgers en

bedrijven te authenticeren. Bijvoorbeeld door hun eigen authenticatiemiddel aan te bieden. De kosten zouden dan hoger zijn en er zouden meer beveiligingsrisico's zijn. Omdat dienstverleners met DigiD en eHerkenning met hogere zekerheid kunnen vaststellen dat de persoon is wie deze beweert te zijn, vermindert de kans op (identiteits) fraude en zijn er minder risico's bij digitale dienstverlening waarbij privacygevoelige gegevens worden uitgewisseld, bijvoorbeeld in de zorg (Ecorys, 2023).

Daarnaast maakt DigiD het digitaal machtigen op eigen verzoek mogelijk, waardoor er vaker machtigingsrelaties ontstaan en – als gevolg – subsidies en toeslagen vaker terechtkomen bij de juiste persoon. Dit komt het gebruik van toeslagen door rechthebbende burgers ten goede. Daarbovenop draagt een goede digitale machtigingsprocedure bij aan inclusie. Wanneer een burger daar zelf niet toe in staat is, kan deze digitale belangen laten behartigen door iemand anders (Ecorys, 2018).

4.4 Kwaliteit van DigiD en eHerkenning

We stelden ons de volgende onderzoeksvraag: *in hoeverre beheerst de overheid de kwaliteit van DigiD en eHerkenning?*

De overheid beheerst de kwaliteit van de authenticatiemiddelen voldoende. Dit is gebaseerd op een uitgebreide IT-audit die wij hebben uitgevoerd. In deze audit hebben wij daartoe op detailniveau beheersmaatregelen beoordeeld als effectief, niet effectief of deels effectief.

4.4.1 Uitkomsten toetsing

Zoals in § 2.2 beschreven, verstaan we onder kwaliteit dat de authenticatiemiddelen beschikbaar, integer en exclusief zijn:

- *Beschikbaarheid:* zijn DigiD en eHerkenning beschikbaar, 'doen' ze het op het moment dat je ze nodig hebt?
- *Integriteit:* kloppen de gegevens, zitten er geen fouten in?
- *Exclusiviteit:* kunnen alleen de juiste personen bij de systemen en gegevens?

Onderzochte componenten

We hebben de componenten in het IT-landschap onderzocht die belangrijk zijn voor de dienstverlening van DigiD en eHerkenning. Voor DigiD is dat 'DigiD Kern', de kernfunctionaliteit van DigiD. Deze functionaliteit bevat de technische authenticatie van een burger voor uitvoerende organisaties zoals UWV, Belastingdienst en gemeenten. Voor eHerkenning is dat het centraal beheerde deel van het afsprakenstelsel door Logius, de zogenaamde XML-aggregator. De afspraken en diensten in het stelsel

komen daar samen. De output daarvan is de zogenaamde ‘dienstencatalogus’. Dankzij deze catalogus weten de partijen in het eHerkenning-stelsel eenduidig welke afspraken en diensten er bestaan.

Zowel DigiD als eHerkenning zijn aangesloten op het BSN-koppelregister polymorfe pseudoniemen (BSNk PP). Polymorfe pseudoniemen zijn een technisch middel om niet het burgerservicenummer (BSN) te gebruiken maar een pseudoniem. Dit verhoogt de privacy/gegevensbescherming. BSNk PP wordt een belangrijk koppelpunt in het nieuwe authenticatiestelsel na invoering van de Wdo. Elke authenticatiemiddelenaanbieder moet hier in de toekomst op aansluiten. Vandaar dat we juist deze component van het stelsel hebben onderzocht.

Beheersmaatregelen

Een beheersmaatregel is een manier om risico’s te beheersen. Bijvoorbeeld het maken van back-ups en het hebben van een goed werkend proces voor beveiligingsincidenten. Verscheidene beheersmaatregelen dragen bij aan beschikbaarheid, integriteit en exclusiviteit. We duiden in tabel 6 met een ‘x’ aan welke maatregelen belangrijk zijn voor die begrippen. Voor de 3 genoemde componenten (DigiD Kern, eHerkenning, BSNk PP) zijn we met een uitgebreide set aan beheersmaatregelen nagegaan of deze maatregelen effectief, deels effectief of niet effectief zijn.

- Een beheersmaatregel is als ‘effectief’ beoordeeld als voldoende is aangetoond dat de beheersmaatregel volledig is geïmplementeerd. Dit wil zeggen dat de beheersmaatregel niet alleen op papier is uitgewerkt, maar dat de gecontroleerde partij ook aan ons kan bewijzen dat de beheersmaatregel in praktijk is toegepast.
- Een beheersmaatregel is als ‘deels effectief’ beoordeeld als:
  - Er alleen een beschrijving van de beheersmaatregel aanwezig is, maar dat er geen bewijs is dat dit in praktijk wordt nageleefd;
  - Of dat alleen praktische toepassing van een beheersmaatregel is aanwezig is, maar er geen (formeel goedgekeurde) beschrijving daarvan is.
- Een beheersmaatregel is als ‘niet effectief’ beoordeeld als er geen beschrijving is van de maatregel en geen bewijs dat de maatregel in de praktijk van toepassing is.

De uitkomsten van de audit zijn samengevat in tabel 6. Daarbij geven we per component en per beheersmaatregel aan of de kwaliteit in voldoende mate wordt beheerst.

Tabel 6 *Uitkomsten IT-audit*

				eHer-kenning	DigiD Kern	BSNk PP
	Beschikbaarheid	Integriteit	Exclusiviteit	Beheersmaatregelen	Beheersmaatregelen	Beheersmaatregelen
IT governance						
Duidelijke rollen en verantwoordelijkheden beschikbaarheid dienstverlening	x			Effectief	Effectief	Effectief
Duidelijke rollen en verantwoordelijkheden veiligheid en informatiebeveiliging		x	x	Effectief	Effectief	Effectief
Opdrachtgever/management kan door systemen/processen goed sturen	x	x	x	Effectief	Effectief	Effectief
De eigenaar is verantwoordelijk voor het juiste beheer gedurende de hele levenscyclus van bedrijfsmiddelen	x			Deels effectief	Deels effectief	Effectief
Organisatie en processen						
Informatie is geclassificeerd conform wettelijke eisen, waarde, belang en gevoeligheid en conform expliciete risicoafweging			x	Effectief	Effectief	Deels effectief
Er is een vastgesteld screeningsbeleid voor indiensttreding en functiewijziging			x	Effectief	Effectief	Effectief
Outsourcing						
Er is een vastgesteld en formeel goedgekeurd outsourcingsbeleid	x	x	x	Effectief	Effectief	Effectief
Outsourcing wordt gemonitored volgens overeenkomsten	x	x	x	Effectief	Effectief	Niet effectief
IT architecture						
Er is actueel inzicht in het IT-landschap waaronder in de belangrijkste componenten inclusief relaties en onderlinge afhankelijkheden	x	x	x	Deels effectief	Deels effectief	Deels effectief
Koppelingen worden via een vastgesteld proces onderhouden en geïmplementeerd	x			Deels effectief	Deels effectief	Effectief
Business continuity						
Continuïteitsplan: informatieverwerkende faciliteiten hebben voldoende redundantie	x			Effectief	Effectief	Effectief
Continuïteitsplan: voor het waarborgen van informatiebeveiliging tijdens een ongunstige situatie	x			Effectief	Effectief	Effectief
Back-up: van informatie, software en systeemafbeeldingen conform back-upbeleid	x			Effectief	Effectief	Effectief

				eHer-kenning	DigiD Kern	BSNk PP
IT operations						
Incidentmanagementproces aanwezig	x			Effectief	Effectief	Effectief
Wijzigingsbeheer: wijzigingen volgen een formeel proces van autoriseren en testen	x	x	x	Deels effectief	Effectief	Deels effectief
Patch management: patchbeleid wordt in praktijk gevolgd				Effectief	Effectief	Effectief
Systeemontwikkeling: geformaliseerde methodiek voor software-ontwikkeling en software-implementatie	x	x	x	Effectief	Effectief	Effectief
Wachtwoordbeheer generieke beheeraccounts	x	x		Deels effectief	Effectief	Effectief
Wachtwoordbeheer vertrouwde omgeving of twee-factor-authenticatie	x	x		Deels effectief	Effectief	Effectief
Gebruikersbeheer: alleen die rechten die noodzakelijk zijn		x	x	Deels effectief	Effectief	Effectief
Gebruikersbeheer: accounts met verhoogde rechten zijn zoveel mogelijk beperkt en verklaard		x	x	Deels effectief	Effectief	Effectief
Gebruikersbeheer: altijd persoonsgebonden		x	x	Deels effectief	Effectief	Effectief
Gebruikersbeheer: eindgebruikers hebben geen directe toegang tot bijvoorbeeld de database		x	x	Deels effectief	Effectief	Effectief
Gebruikersbeheer: toegangsrechten periodiek evalueren		x	x	Deels effectief	Effectief	Effectief
Beveiliging van componenten: actueel inzicht hoe de infrastructuur is beveiligd	x	x		Deels effectief	Deels effectief	Deels effectief
Capaciteitsmanagement: de IT-dienst kan de gewone beheerlast aan en dient tijdig herstelbaar te zijn	x			Deels effectief	Effectief	Effectief
Logging: van gebeurtenissen over bijvoorbeeld gebruikersactiviteiten, uitzonderingen en informatiebeveiliging		x		Deels effectief	Deels effectief	Effectief
Logging: beschermen van informatie tegen vervalsing en onbevoegde toegang		x	x	Deels effectief	Deels effectief	Effectief
Logging: van beheerders en operators, deze logbestanden beschermen en regelmatig beoordelen		x		Deels effectief	Deels effectief	Effectief
Information security						
Security by design als gangbaar principe bij ontwikkeling en de inrichting van systemen	x		x	Deels effectief	Deels effectief	Effectief
Detectie en respons van veiligheidsincidenten vindt plaats volgens een vaste procedure	x		x	Effectief	Effectief	Effectief
Kwetsbaarhedenmanagement: onafhankelijk periodiek toetsen van technische beveiligingsmaatregelen			x	Deels effectief	Effectief	Effectief
Kwetsbaarhedenmanagement: tijdig patchen van onderdelen van de IT-infrastructuur			x	Deels effectief	Effectief	Effectief

			eHer-kenning	DigiD Kern	BSNk PP
Standaarden: handhaven van de beveiliging van informatie die wordt uitgewisseld, intern en extern	x	x	Deels effectief	Deels effectief	Deels effectief
Encryptie: er is beleid voor het gebruik van cryptografische beheersmaatregelen	x	x	Deels effectief	Deels effectief	Effectief
Encryptie: beleid voor gebruik, bescherming en levensduur van cryptografische sleutels	x	x	Deels effectief	Deels effectief	Deels effectief
Persoonsgegevens					
Er is een verwerkingsregister met mogelijkheid tot inzage		x	N.v.t.	Effectief	Effectief
Gegevensbeschermingseffectbeoordeling (GEB) en regelmatige actualisatie		x	N.v.t.	Deels effectief	Effectief
Dataminimalisatie, het zo min mogelijk verzamelen van persoonsgegevens		x	N.v.t.	Effectief	Effectief
De grondslag voor verwerking en verantwoordelijkheden is vastgelegd		x	N.v.t.	Effectief	Effectief
Melding van incidenten met (potentieel) aanzienlijke gevolgen	x		N.v.t.	Effectief	Effectief

We constateren dat het overgrote deel van de kwaliteitsbevorderende maatregelen bij DigiD effectief is. Bij eHerkenning valt op dat we veel maatregelen als deels effectief beoordelen bij de clusters IT-operations en Information Security. Dit komt omdat er wel processen en procedures zijn uitgewerkt, maar het niet navolgbaar is hoe deze in praktijk zijn gebracht. De minister van BZK moet voor eHerkenning beter aantonen dat de maatregelen ook in de praktijk gevolgd worden.

Bij de component BSNk PP is 1 beheersmaatregel niet effectief. Dit betreft de outsourcing van Logius aan ICTU (ICT-Uitvoeringsorganisatie). Stichting ICTU is een advies- en projectenorganisatie voor de Rijksoverheid. Zij verzorgt de ontwikkeling van BSNk. Een omschrijving wat ICTU in het kader van BSNk PP doet voor Logius staat niet beschreven. Hierover zijn in de geleverde documentatie geen formele afspraken aangetroffen.

Bij DigiD constateerden we dat er geen samenvattend uniform vastgesteld beeld is van het IT-landschap. Er zijn verschillende visuele weergaven aangeleverd door organisaties zoals BZK, Logius en Capgemini. Deze weergaven verschilden steeds weer wat van elkaar. Voor eHerkenning werd niet duidelijk hoe componenten zich tot elkaar verhouden. De beschikbare rapportages zijn niet altijd een-op-een te matchen met specifieke componenten. Voor BSNk PP geldt dat de IT-architectuurplaten sinds 2018 niet meer zijn geactualiseerd. Dit brengt het volgende risico met zich mee. Het wijzigen van IT-onderdelen kan invloed hebben op aanpalende IT-onderdelen. Als niet bekend is welke dit zijn, kan dit gevolgen hebben voor de uiteindelijke IT-dienstverlening.

We constateren dat er geen actuele en eenduidige IT-architectuur is voor zowel eHerkenning als DigiD. We verwachtten meer duidelijkheid over hoe alle IT-onderdelen met elkaar samenhangen. We kregen geen goed zicht op de onderliggende IT van de authenticatiedienstverlening. Dit is met name belangrijk vanuit het externe perspectief dat bijvoorbeeld een volksvertegenwoordiger heeft of vanuit een controle- of auditorganisatie. Als de samenhang bekend is, is de dienstverlening beter te controleren en zijn IT-wijzigingen beter door te voeren. Verder is een gedeeld inzicht en overzicht nodig om het nieuwe authenticatiestelsel onder de Wdo goed in te richten en te laten werken.

5. Wet digitale overheid en Europese digitale identiteit

5.1 Conclusies

- De Wet digitale overheid (Wdo) verandert het stelsel voor digitale toegang met ingang van 1 juli 2023. Er komen authenticatiemiddelen naast DigiD en eHerkenning. Daarom moet er een technisch aansluitpunt komen waar alle authenticatiemiddelen samenkomen. Dan hoeven uitvoerende organisaties zoals UWV, Belastingdienst en gemeenten alleen op één centraal punt aan te sluiten. Dit aansluitpunt is er niet.
- Ook de Europese digitale identiteit is in voorbereiding. Concreet is dit de *wallet*. Dit is een digitale portemonnee met (identiteits)gegevens, die een burger of bedrijf kan delen met publieke en private partijen. Met de *wallet* kunnen burgers en bedrijven ook inloggen, net als met DigiD en eHerkenning. Het zou in de toekomst kunnen dat veel authenticaties met de *wallet* worden gedaan en minder met DigiD of eHerkenning. Belangrijk is dat de *wallet* kwalitatief dezelfde authenticatie biedt als DigiD en eHerkenning. Over hoe de *wallet* er uit komt te zien en hoe deze past in het stelsel voor digitale authenticatie, is nog veel onduidelijkheid.

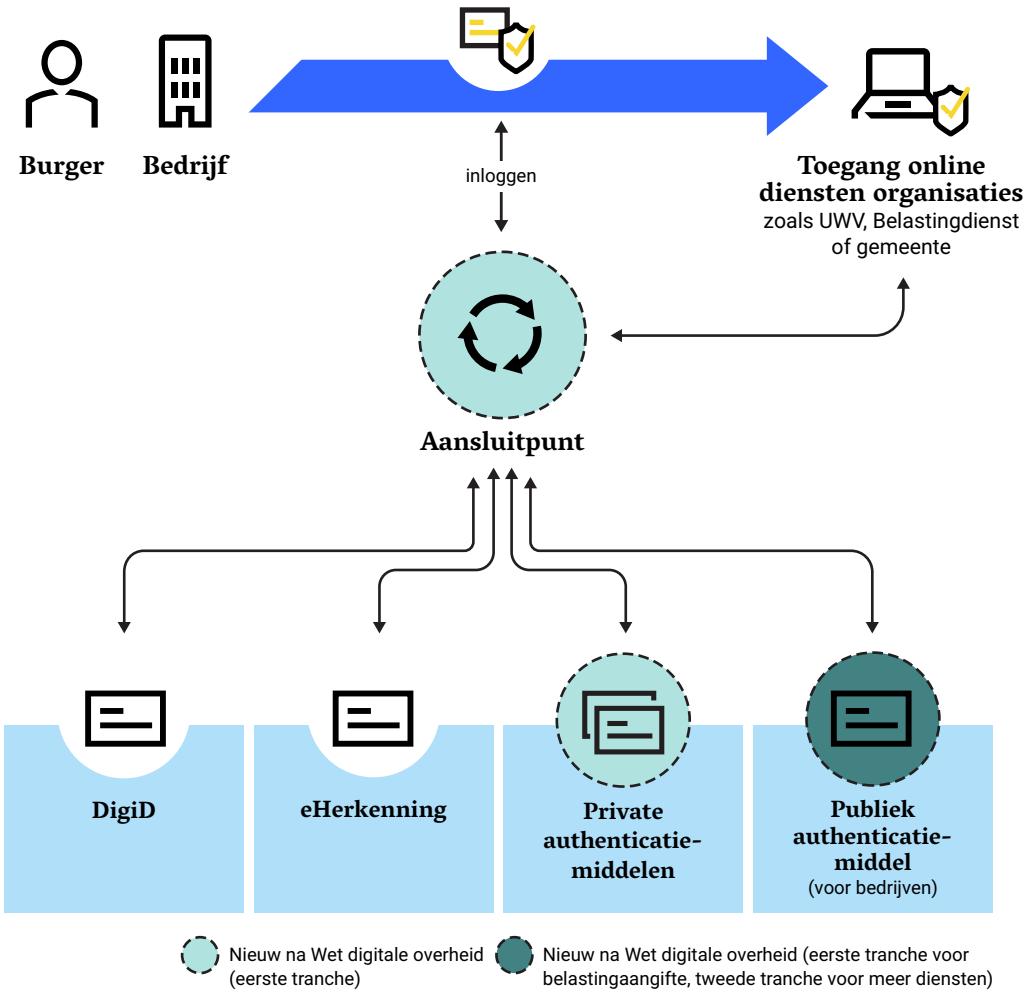
5.2 Wet digitale overheid

De aanzet voor de Wet digitale overheid (Wdo) dateert uit 2016. Onder de initiële naam Wet Generieke Digitale Infrastructuur (GDI) ging deze toen in internetconsultatie. Na aanpassingen is de Wdo in het voorjaar van 2023 aangenomen in beide Kamers van de Staten-Generaal. Per 1 juli 2023 gaat deze in. De Wdo bestaat uit de wet en een aantal lagere besluiten en regelingen.[15]

De Wdo legt het fundament voor de verdere digitalisering van de overheid. De Wdo zorgt ervoor dat er zoveel mogelijk standaarden worden gehanteerd. De wet bevat regels over veiligheid en de controle daarop. Ook wordt in de Wdo de digitale toegang tot publieke dienstverlening voor burgers en bedrijven behandeld. Er staan regels in over veilig inloggen bij (semi)overheidsinstanties om gebruik te maken van hun dienstverlening. Figuur 3 toont de meest in het oog springende veranderingen door de Wdo voor het onderwerp authenticatie.

Figuur 3 *Stelsel toegang na inwerkingtreding Wdo*

Na invoering van de Wdo verandert het authenticatiestelsel



Uit figuur 3 blijkt dat de Wdo de mogelijkheid biedt om private authenticatiemiddelen toe te laten (naast het publieke DigiD). Om als authenticatiemiddel toegelaten te worden tot het stelsel, moet het voldoen aan de eisen zoals deze in de Wdo staan. Overheidspartijen moeten de toegelaten authenticatiemiddelen verplicht accepteren. Verder moeten zij hun dienstverlening indelen naar betrouwbaarheidsniveau.

De wet treedt niet op 1 juli 2023 al volledig in werking, maar gefaseerd. Het Ministerie van BZK stelt een aansluitschema voor uitvoerende overheidspartijen op, in samenwerking met Logius, departementen en publieke dienstverleners. Naar verwachting kunnen potentiële aanbieders van authenticatiemiddelen zich vanaf 1 juli 2023 aanmelden. Dit betekent dat ruim voor deze datum de exacte voorwaarden helder moeten zijn. Bij de afronding van dit rapport (februari 2023) was dit nog niet het geval.

In de Wdo is ook voorzien dat voor uitvoeringspartijen een routeringsvoorziening wordt ingericht. De minister van BZK is daarvoor verantwoordelijk. Deze routeringsvoorziening sluit alle authenticatiemiddelen aan en is dus een belangrijk onderdeel van het nieuwe authenticatiestelsel. In figuur 3 is dit gevisualiseerd als het 'aansluitpunt'. Ten tijde van dit schrijven is dit centrale aansluitpunt nog niet gerealiseerd.[16]

De minister van BZK wil ook zorgen voor een publiek authenticatiemiddel voor bedrijven. In eerste instantie zal dit authenticatiemiddel gericht zijn op het doen van belastingaangifte. Dit laatste wordt geregeld in het reeds aangenomen wetsvoorstel Wdo dat vanaf 1 juli 2023 gefaseerd in werking treedt. De minister van BZK werkt nog aan een tweede wetsvoorstel voor de Wdo. De beoogde invoeringsdatum daarvan is onbekend. In dit tweede deel van de Wdo beoogt de minister van BZK te zorgen voor een publiek authenticatiemiddel voor bedrijven, breder dan alleen voor het doen van belastingaangifte. Na invoering van de 2 delen - de minister van BZK spreekt over 'tranches' - ziet het stelsel eruit zoals weergegeven in figuur 3.

5.3 Europese digitale identiteit en 'wallet', eIDAS2

5.3.1 eIDAS2

In 2014 heeft het Europese Parlement de zogenaamde eIDAS-verordening aangenomen. In september 2018 trad deze in werking. eIDAS staat voor *Electronic Identities And Trust Services*. Het biedt een kader voor Europees gebruik van elektronische identiteiten en diensten. Met eIDAS hebben de Europese lidstaten afspraken gemaakt om dezelfde begrippen, betrouwbaarheidsniveaus en onderlinge digitale infrastructuur te gebruiken.

Met eIDAS kun je met nationale middelen zoals DigiD dezelfde zaken regelen in een ander Europees land. Dit betekent dat een Nederlandse burger in Duitsland hetzelfde zou moeten kunnen regelen als een Duitse burger.

Deze verordening was in eerste instantie geen succes. De implementatie in lidstaten liet te wensen over en te weinig lidstaten lieten hun elektronisch identificatiemiddel aanmelden om op de eIDAS-infrastructuur te kunnen. Ook waren te weinig dienstverleners

aangesloten op eIDAS, waardoor onvoldoende diensten beschikbaar waren. De Europese Commissie zelf concludeerde na een evaluatie dat de bestaande eIDAS-verordening niet in alle opzichten voldeed (Europese Commissie, 2021).

De Europese Commissie diende daarom een voorstel in bij de Raad van de Europese Unie en het Europees Parlement om de eIDAS-verordening aan te passen, om de werking ervan te versterken: eIDAS2 (Europese Commissie, 2021). eIDAS2 biedt ook een verdere invulling van een raamwerk voor een digitale Europese identiteit. Volgens de Europese Commissie wordt hiermee 'de digitale autonomie van de Europese burger versterkt'. eIDAS2 wil burgers en bedrijven in staat stellen digitale zaken simpeler en veiliger te regelen. Ook speelt eIDAS2 in op ontwikkelingen in de markt en beschikbare technologie voor *wallets*.

5.3.2 Wallets

Een *wallet* is kort gezegd een digitale portemonnee met persoonsgegevens. Die portemonnee bevat bijvoorbeeld je rijbewijs, NAW-gegevens, diploma's en medische gegevens. Het idee is dat je alleen die gegevens deelt die echt nodig zijn voor de andere partij. Dat kan bij zowel overheid als bij bedrijven. Niet meer een kopie van je paspoort, maar bijvoorbeeld alleen maar het gegeven laten zien dat je 18+ bent bij een drankenhandel. Burgers kunnen zo eenvoudig bepalen hoeveel informatie ze over zichzelf verstrekken aan partijen die daarom vragen.

De Europese Commissie ziet in zo'n *wallet* nieuwe kansen als het gaat om gemak, dataminimalisatie, betrouwbaarheid, veiligheid en efficiëntie. Iedere inwoner van de Europese Unie die recht heeft op een nationale identiteitskaart, zal met de invoering van eIDAS2 recht krijgen op genoemde digitale identiteit en de daarbij behorende *wallet*.

Iedere lidstaat zal minimaal 1 *wallet* 'gratis'[17] beschikbaar stellen aan haar burgers. Deze *wallet* moet minimaal de identiteit bevatten[18] en een authenticatiemechanisme waarmee de houder zich digitaal online kan authenticeren. Daarmee concurreert de wallet dus ook mogelijk met andere authenticatiemiddelen onder Wdo, zoals DigiD en eHerkenning. Hier gaan we in de volgende paragraaf uitgebreider op in.

De *wallets* zullen nationaal erkend moeten worden door daartoe aangewezen instanties. Dat is in Nederland de Rijksinspectie Digitale Infrastructuur. Een nationaal erkende *wallet* moet in alle lidstaten geaccepteerd worden. Burgers en bedrijven kunnen hiermee hun gegevens met andere burgers, bedrijven en organisaties delen. De *wallet* zal niet alleen in het publieke maar ook in het private domein gebruikt kunnen worden.

Tot slot bieden *wallets* ook functionaliteiten zoals een elektronische handtekening. Deze functionaliteit maakt nu geen onderdeel uit van DigiD en eHerkenning, zie ook § 4.2.2.

5.3.3 DigiD en eHerkenning en eIDAS2

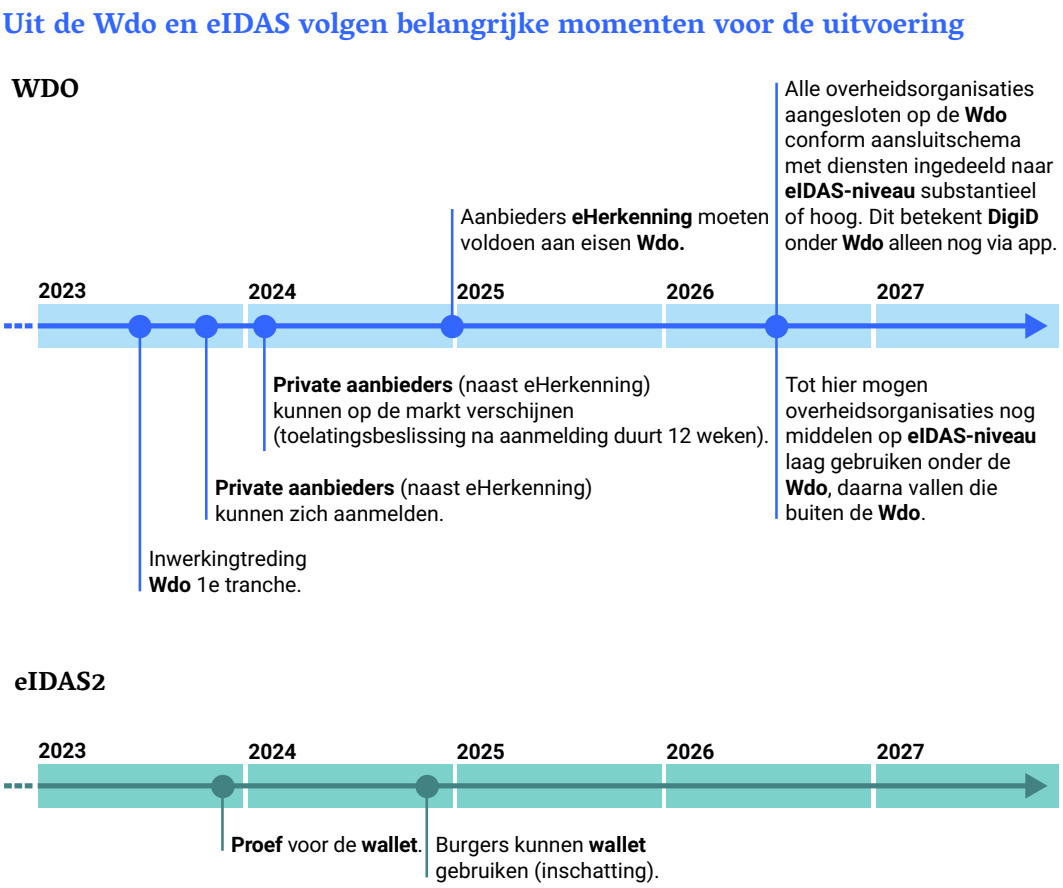
Het gebruik van de *wallet* is vrijwillig. Hoe snel deze ingeburgerd zal raken, is niet te voorspellen. Het ligt niet in de lijn der verwachting dat DigiD en eHerkenning binnen enkele jaren overbodig worden. In de verre toekomst bestaat die mogelijkheid wel. De beoogde *wallets* bieden namelijk straks mogelijkheden voor identificatie, authenticatie en regie op gegevens door de burger zelf.

Theoretisch kunnen DigiD en/of eHerkenning zich ook transformeren tot een *wallet* met dezelfde naam. Het Nederlandse kabinet kiest hier niet voor. Eind 2022 gaf de staatssecretaris van Koninkrijksrelaties en Digitalisering aan dat DigiD niet uitgebouwd zal worden tot de publieke voorbeeld*wallet*, maar apart zal blijven bestaan als het authenticatiemiddel dat het nu is. Het kabinet onderzoekt wel de mogelijkheden om op basis van DigiD een Nederlandse *id-wallet* te activeren. Het kabinet draagt in dit kader ook aan dat DigiD als grensoverschrijdend eID-middel in online interacties met overheidsdiensten van andere lidstaten gebruikt kan worden (BZK, 2022b).

5.4 Tijdslijn Wdo en eIDAS2

De invoering van de Wdo, eIDAS2 en de *wallet* kennen gedeeltelijke samenloop en overlap. In figuur 4 zijn de belangrijkste momenten indicatief weergegeven.

Figuur 4 *Indicatieve tijdslijnen Wdo en eIDAS2*



Aanvullend op de beschreven momenten in figuur 4 merken wij op:

- Er is geen datum benoemd in de Wdo wanneer het centrale aansluitpunt voor uitvoerende organisaties (zoals beschreven in § 5.2) beschikbaar moet zijn.
- Er wordt in 2023 een aansluitschema voor uitvoerende organisaties als UWV, Belastingdienst en gemeenten gemaakt om aan te sluiten op het nieuwe authenticatiestelsel. Het aansluiten moet binnen 3 jaar na inwerkingtreding Wdo gebeuren.

Voor beide bovenstaande punten geldt dat het onduidelijk is wat er gebeurt als burgers met een nieuw authenticatiemiddel al over een jaar willen inloggen. Als een burger bijvoorbeeld begin 2024 al beschikt over een nieuw authenticatiemiddel en een gemeente pas eind juni 2026 aansluit op het stelsel onder de Wdo, kan de burger dit authenticatiemiddel ruim 2 jaar niet gebruiken bij die gemeente.

Bij de tijdslijn zien wij verder de volgende risico's:

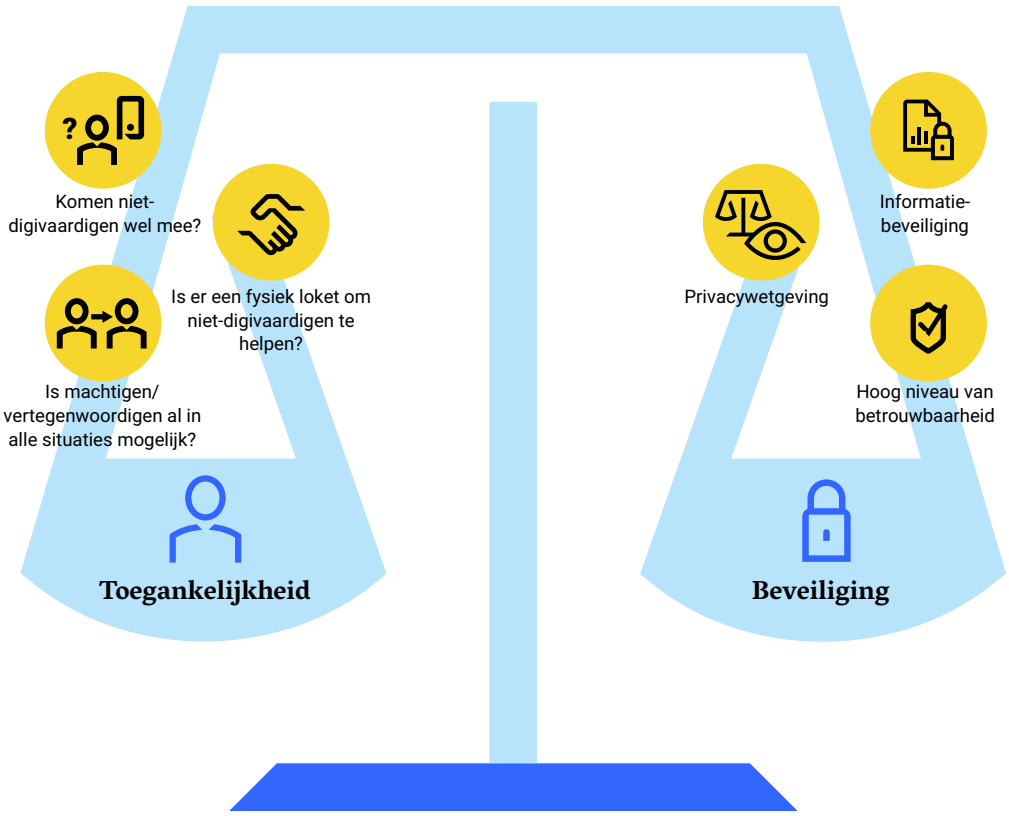
- De continuïteit en kwaliteit van de bestaande dienstverlening komt mogelijk in gevaar door deze stelselveranderingen. De vraag is of er genoeg implementatietijd is voor de huidige authenticatiemiddelenleveranciers (tot januari 2025) en voor uitvoerende organisaties (tot uiterlijk juli 2026) om aan te sluiten.
- Medewerkers van het Ministerie van BZK en Logius moeten zich zowel richten op de continuïteit van de huidige diensten DigiD en eHerkenning als op de realisatie van de Wdo en eIDAS2 en de *wallet*. Veel activiteiten lopen parallel en vragen om inzet van dezelfde schaarse expertise en capaciteit op dit vlak.
- Zoals ook in § 4.4.1 benoemd is er nu weinig zicht op de totaalarchitectuur van het toegangsstelsel. Hiermee bedoelen we de samenhang van alle componenten die nodig zijn voor dit stelsel. Een gedeeld inzicht en overzicht is belangrijk om het nieuwe stelsel goed in te richten, te laten werken en onnodige kosten te vermijden.

6. Afweging tussen veiligheid en toegankelijkheid

In dit hoofdstuk beschrijven we de afweging tussen veiligheid en toegankelijkheid van dienstverlening. Strengere eisen aan de veiligheid zorgen voor minder toegankelijke dienstverlening. Dit kan vooral voor niet-digivaardige burgers problemen opleveren. Die problemen kunnen worden tegengegaan wanneer niet-digivaardigen goed ondersteund worden. Dit kan door digitaal belangen te laten behartigen door op eigen verzoek andere personen te machtigen en wettelijke vertegenwoordiging te regelen. De problemen voor niet-digivaardigen kunnen ook worden tegengegaan als er een fysiek loket is, waar ook burgers terecht kunnen die wel digivaardig zijn, maar die een probleem hebben dat te complex is om digitaal af te handelen. In figuur 5 is de afweging gevisualiseerd.

Figuur 5 *Afweging voor betrouwbaarheidsniveau DigiD*

De waarden beveiliging en toegankelijkheid moeten worden afgewogen



We beperken ons in dit hoofdstuk tot DigiD, omdat de niet-digivaardige burger daar het meest mee te maken heeft.

6.1 Conclusies

De minister van BZK moet afwegen hoe veilig en hoe toegankelijk digitale voorzieningen moeten zijn. De volgende punten zijn hierbij van belang:

- Overheid en uitvoerende organisaties kiezen ten behoeve van betere beveiliging voor steeds hogere betrouwbaarheidsniveaus. Meer veiligheid gaat ten koste van toegankelijkheid. Daardoor bestaat het risico dat niet-digivaardigen worden uitgesloten.
- Dit risico kan worden verminderd door met name niet-digivaardigen te ondersteunen.
  - Enerzijds wanneer niet-digivaardigen op eigen verzoek andere personen machtigen om namens hen in te loggen. Deze mogelijkheid bestaat reeds met DigiD Machtigen. Wettelijk vertegenwoordigers zouden ook namens een niet-digivaardige moeten kunnen inloggen. Dit is nog niet mogelijk.

- Anderzijds kan een fysiek loket de niet-digivaardige burger ondersteunen. De minister van BZK financiert daartoe al de Informatiepunten Digitale Overheid (IDO's). We constateren dat de beperkte mogelijkheden en bevoegdheden van medewerkers van IDO's een effectieve ondersteuning van de bezoekers in de weg staat. Zo'n fysiek loket is ook nodig voor burgers die wel digivaardig zijn, maar die een probleem hebben dat te complex is om digitaal af te handelen.

6.2 Veiligheid en toegankelijkheid

6.2.1 Betrouwbaarheidsniveaus DigiD

DigiD kent verschillende betrouwbaarheidsniveaus. Een hoger betrouwbaarheidsniveau betekent dat je met steeds meer zekerheid kan zeggen dat degene die probeert in te loggen ook daadwerkelijk die persoon is. Het betrouwbaarheidsniveau stijgt wanneer je met meer 'factoren' inlogt. 1 factor is bijvoorbeeld 'iets dat je weet'. Dit is bijvoorbeeld gebruikersnaam en wachtwoord. Een tweede factor kan zijn 'iets dat je hebt', bijvoorbeeld een mobieltje, via een app. Het betrouwbaarheidsniveau stijgt verder wanneer ook het fysiek identiteitsdocument - middels een daarin aanwezige chip - gecheckt wordt. Uitvoerende partijen als het UWV en gemeenten moeten voor hun diensten zelf bepalen welk betrouwbaarheidsniveau nodig is. De indeling in betrouwbaarheidsniveaus op nationaal niveau is niet dezelfde als die op EU/eIDAS-niveau.

Figuur 6 *Betrouwbaarheidsniveaus DigiD*

Tabel 7 toont de aantallen authenticaties via DigiD per betrouwbaarheidsniveau over de jaren 2018 t/m 2021. We constateren een stijging van het totaal aantal authenticaties en van authenticaties met betrouwbaarheidsniveaus midden, substantieel en hoog. We zien een daling van authenticaties met DigiD-betrouwbaarheidsniveau basis. Burgers loggen dus steeds minder vaak in met alleen gebruikersnaam en wachtwoord.

Tabel 7 *Aantal authenticaties per* DigiD-*betrouwbaarheidsniveau (ICTU, 2022)*[19]

	2018	2019	2020	2021
Totaal	**307.956.118**	**340.758.404**	**402.519.872**	**557.008.812**
Basis	260.066.132	223.949.536	161.210.552	121.523.951
Midden	47.703.384	111.453.266	195.229.103	281.825.661
Substantieel	186.601	5.355.566	46.080.130	153.649.114
Hoog	1	36	87	10.086

Tabel 8 toont vervolgens hoe de rij 'midden' uit tabel 7 is opgebouwd. Er zijn 2 mogelijkheden voor 'midden', via sms of via de app. Bij beide mogelijkheden constateren we een stijgende lijn.

Tabel 8 *Berekening authenticaties op niveau Midden, verdeeld naar app en (ook ingesproken) sms (op basis van ICTU, 2022)*

	2018	2019	2020	2021
Midden (totaal)	**47.703.384**	**111.453.266**	**195.229.103**	**281.825.661**
Midden (app)	10.866.602	46.830.118	95.633.971	132.008.570
Midden (sms)	36.836.782	64.623.148	99.595.132	149.817.091

6.2.2 Uitfasering betrouwbaarheidsniveaus

Overheidspartijen kiezen voor steeds hogere betrouwbaarheidsniveaus. Zo kan sinds 1 oktober 2022 bij Mijn Belastingdienst niet meer met alleen gebruikersnaam en wachtwoord worden ingelogd. Nu is er ook een extra sms-controle nodig. Voor MijnOverheid zal vanaf begin 2023 hetzelfde gelden en op 8 mei 2023 zal ook de Sociale Verzekeringsbank (SVB) overstappen. Op een later moment volgt ook Belastingdienst Toeslagen. De staatssecretaris van Koninkrijksrelaties en Digitalisering meldt overigens wel dat de mogelijkheid om in te loggen met sms-authenticatie voorlopig nog behouden blijft. Dit vanwege de grote groep mensen die hier nog gebruik van maakt (BZK, 2022c).

Uit de Wdo volgt dat 3 jaar na inwerkingtreding van de Wdo het gebruik van DigiD op eIDAS-niveau laag niet meer wordt erkend.[20] Dit is dus per 1 juli 2026. Alleen de

eIDAS-niveaus substantieel en hoog worden dan nog erkend. Inloggen via DigiD onder de Wdo kan dan alleen nog maar via de app inclusief een (eenmalige) fysieke ID-check. Tabel 7 en tabel 8 laten zien dat van alle 557 miljoen authenticaties er ongeveer 150 miljoen keer *van sms gebruik is gemaakt. Dat betekent dan ook dat mogelijk veel burgers moeten overstappen van sms naar app.*

Of dit daadwerkelijk zo zal zijn, is nog niet geheel duidelijk. Het Ministerie van BZK geeft aan dat er in de praktijk nog dienstverlening op eIDAS-niveau laag kan plaatsvinden. Deze wordt dan feitelijk niet gereguleerd door de Wdo, maar de Wdo verbiedt dat niet expliciet.

Het is belangrijk goed af te wegen of mogelijkheden kunnen worden uitgefaseerd. Een van die factoren is of niet-digivaardigen goed ondersteund kunnen worden, bijvoorbeeld door machtigen en vertegenwoordigen en ondersteuning bij een fysiek overheidsloket.

6.3 Machtigen en wettelijk vertegenwoordigen

In § 4.2.2 gingen we al kort in op machtigen en wettelijk vertegenwoordigen. In deze paragraaf gaan we dieper op deze onderwerpen in. Een van de factoren bij de afweging veiligheid en toegankelijkheid is namelijk of niet-digivaardigen goed ondersteund kunnen worden, bijvoorbeeld machtigen op eigen verzoek of wettelijk vertegenwoordigen.

6.3.1 Machtigen

DigiD Machtigen is er sinds 1 januari 2010. De eerdere naam was Gemeenschappelijke machtigingsvoorziening (GMV) (BZK, 2010). Met DigiD Machtigen kun je als burger ‘machtigen op eigen verzoek’. Je kunt andere personen of organisaties machtigen voor een bepaalde dienst, bijvoorbeeld voor de belastingaangifte. Die persoon mag in dit voorbeeld dan namens jou inloggen met DigiD Machtigen bij de Belastingdienst.

Ondanks dat deze mogelijkheid er is, wordt er momenteel nog op een niet-legitieme wijze ‘gemachtigd’. Zonder gebruik te maken van DigiD Machtigen verstrekken bijvoorbeeld familieleden DigiD-gegevens aan elkaar en loggen met elkaars DigiD in. De ingezette ontwikkeling richting hogere betrouwbaarheidsniveaus maken dit op termijn onmogelijk. Als je via de app moet inloggen, moet je op het moment van inloggen beschikken over de smartphone behorend bij een bepaalde DigiD. Dit kan bij bepaalde groepen burgers tot problemen leiden.

6.3.2 Wettelijk vertegenwoordigen

Er zijn situaties waar je niet op eigen verzoek kunt of wilt machtigen. Ook dan is inloggen namens een persoon belangrijk. Die situaties kun je scharen onder 'wettelijk vertegenwoordigen'.

Ouder-kindrelaties

Wettelijke vertegenwoordiging is bijvoorbeeld het geval bij ouder-kindrelaties. Volgens de wet is de ouder de wettelijke vertegenwoordiger totdat het kind 18 is. Dat de ouder namens het kind kan inloggen met DigiD is nog niet ingeregeld. Dit is voor veel dienstverlening wel belangrijk, zeker als een kind medische zorg nodig heeft.

Sinds 8 november 2022 loopt er een proef bij ziekenhuis Maastricht UMC+. In deze proef kan de ouder met de eigen DigiD – zonder tussenkomst van het ziekenhuis – inloggen op het patiëntportaal van het kind. Het ziekenhuis checkt of de ouder bevoegd is. De ouder krijgt vervolgens toegang tot het dossier van het kind. Of - en zo ja wanneer - deze proef verbreed of landelijk uitgerold wordt, was bij het schrijven van dit rapport (februari 2023) onbekend.

Bewindvoerders en curatoren

Er zijn ook volwassenen die bijvoorbeeld niet handelingsbekwaam zijn en gebruikmaken van bewindvoerders. Denk aan verstandelijk beperkten. Of denk aan curatoren die beheer moeten voeren over iemands bezittingen. Bewindvoerders en curatoren kunnen nog niet inloggen namens een persoon. De reden is dat de registers nog niet ontsloten zijn waarin staat wie de bewindvoerder of curator voor wie is.
Daar wordt ondertussen aan gewerkt. Op 26 september 2022 meldt de staatssecretaris van Koninkrijksrelaties en Digitalisering aan de Tweede Kamer dat ze het register van wettelijke vertegenwoordigers ontsluit samen met de Raad voor de rechtspraak. Ze maakt de zogenoemde 'bevoegdheidsverklaringsdienst'. Deze verstrekt een verklaring over de bevoegdheid van iemand om namens een ander te handelen. Het is een generieke voorziening waarop alle overheidsdienstverleners kunnen aansluiten. Haar planning is om dit in 2024 gereed te hebben (BZK, 2022d). Vooralsnog is dit niet mogelijk.

6.4 Informatiepunten digitale overheid

Burgers die vragen hebben over online overheidsdienstverlening, waaronder DigiD, kunnen onder meer terecht bij Informatiepunten Digitale Overheid (IDO's). Eind 2022 zijn er ruim 650 IDO's, vooral gehuisvest in bibliotheken. Dit is nu een bijna landelijk dekkend netwerk, met alleen op het platteland enkele witte vlekken.

Het aantal vragen bij de IDO's is relatief laag als je kijkt naar de mogelijke doelgroep: burgers met onvoldoende (digitale) basisvaardigheden. Het totaal geregistreerde vragen ligt op ongeveer 55.000 (Koninklijke Bibliotheek, 2022).[21] Het Ministerie van BZK schat in dat er 2,5 miljoen Nederlanders met onvoldoende (digitale) basisvaardigheden zijn en dat er ongeveer 4 miljoen Nederlanders onvoldoende digitale en bureaucratische vaardigheden hebben om zelfstandig zaken te doen met de overheid (BZK, 2021d).[22]

Uit tabel 9 blijkt dat zo'n 20% van de vragen expliciet over DigiD gaat.

Tabel 9 *Soorten vragen bij Informatiepunten Digitale Overheid van 2021 t/m 3e kwartaal 2022 (Koninklijke Bibliotheek, 2022)*[23]

Soort vragen bij Informatiepunten Digitale Overheid	
Anders	34%
DigiD: app installeren, DigiD aanvragen, activeren of aanmeldhulp	20%
Coronavragen (check-app, afspraak vaccinatie/testen)	16%
Hulp bij vragen over computers/tablets/smartphones	14%
Hulp bij aanvraag gemeentelijke regeling (bijvoorbeeld algemene bijstand, WMO)	10%
Belastingzaken	10%
Overheidsdienstverlening 'Manifestgroep' (minus Belastingdienst en DigiD)	4%
Online bankieren	3%

IDO-medewerkers mogen geen DigiD aanvragen voor klanten. In de wet is namelijk bepaald dat je alleen voor jezelf een DigiD mag aanvragen, en niet voor anderen. De medewerkers mogen de klant wel helpen bij de aanvraag en 'over de schouder meekijken' (Probiblio, z.d). We constateren dan ook dat IDO-medewerkers niet-digivaardigen maar tot op bepaalde hoogte kunnen helpen, omdat de medewerkers over beperkte mogelijkheden en bevoegdheden beschikken. We bevelen de minister van BZK aan te onderzoeken of meer bevoegdheden voor IDO-medewerkers rond het aanvragen van DigiD passen in de doorontwikkeling van de IDO's, zodat burgers beter ondersteund kunnen worden.

Over IDO's rapporteren wij uitgebreider in ons rapport 'Resultaten verantwoordingsonderzoek 2022 Ministerie van Binnenlandse Zaken en Koninkrijksrelaties', dat op 17 mei 2023 verschijnt.

In dit kader is het verder van belang dat ook digivaardige burgers een (fysiek) loket nodig hebben. Bijvoorbeeld bij complexe zaken die niet via digitale formulieren zijn af te handelen. Te denken valt dan aan onterechte vermeldingen van burgers in fraude-registers, genderveranderingen, immigratie-/emigratieproblemen, et cetera. Naast IDO's kunnen ook gemeenteloketten hiervoor een goede plaats zijn.

7. Reactie en nawoord

Op 10 maart 2023 ontvingen we van de staatssecretaris van Koninkrijksrelaties en Digitalisering, mede namens de minister van BZK, een reactie op ons conceptrapport. Hieronder geven we haar reactie integraal weer. We sluiten af met ons nawoord.

7.1 Reactie staatssecretaris van Koninkrijksrelaties en Digitalisering

“Hierbij stuur ik u mede namens de minister van Binnenlandse Zaken een reactie op de uitkomsten van uw onderzoeksrapport *Digitale identiteit vraagt veel van DigiD en eHerkenning*.

De beleidsdoelstellingen van DigiD en eHerkenning
U heeft afgelopen periode de digitale authenticatiemiddelen DigiD (voor burgers) en eHerkenning (voor bedrijven) onderzocht. Allereerst constateert u in het rapport dat de beleidsdoelstellingen van DigiD en eHerkenning grotendeels zijn bereikt. Daarnaast constateert u dat de baten van de middelen opwegen tegen de kosten en dat de kwaliteit van DigiD en eHerkenning voldoende wordt beheerst.
Ik ben blij met uw constateringen. Uw adviezen neem ik mee bij de verdere verbetering en doorontwikkeling van de authenticatiemiddelen.

U geeft aan dat de doelen voor machtigen en vertegenwoordigen gedeeltelijk zijn bereikt. Ik streef ernaar, zoals in mijn Werkagenda Waardengedreven Digitalisering staat beschreven, dat iedereen mee kan doen in de digitale samenleving. In dat kader werk ik aan de brede beschikbaarheid van voorzieningen om iemand anders langs

digitale weg te kunnen vertegenwoordigen (zowel voor gemachtigden als voor wettelijk vertegenwoordigen). Verder geeft u aan dat de beheersing van fraude verspreid is over verschillende partijen. De Wet digitale overheid (Wdo) biedt grondslagen om misbruik en fraude integraal aan te pakken. Functies rondom detectie en aanpak van fraude hebben mijn volle aandacht.

Inclusie en toegankelijkheid

Hogere betrouwbaarheidsniveaus maken de dienstverlening veiliger en maken een nauwkeuriger identiteitsvaststelling mogelijk, maar vragen altijd nadrukkelijke aandacht voor digitale toegankelijkheid voor burgers. De afweging tussen veiligheid en toegankelijkheid staat daarom centraal bij de doorontwikkeling van inlogmiddelen en bij het onderzoek naar de toepassing van hogere betrouwbaarheidsniveaus.

Voor burgers kan het lastig zijn om volwaardig digitaal mee te doen. Er moet om die reden altijd een fysiek alternatief zijn om in contact te treden met publieke dienstverleners. Ondersteuning kan onder meer gevonden worden bij de Informatiepunten Digitale Overheid (IDO's) en de helpdesk van DigiD en eHerkenning. Daarnaast ben ik, zoals eerder al benoemd, bezig met het verder ontwikkelen van digitaal vertegenwoordigen.

Hulp aan burgers moet voorop staan en de IDO's zijn hierin een belangrijk middel. De loketten zijn ingericht voor (tijdelijk) niet zelfredzame burgers. Zij geven invulling aan de loketfunctie voor publieke dienstverlening, met name in de 'wegwijzerfunctie'. Op dit moment ben ik bezig met de doorontwikkeling van de IDO's tot Informatiepunten voor publieke dienstverlening. Uiteraard komen de rol en taken van de IDO-medewerkers hierbij aan de orde, ook in het kader van het DigiD-aanvraagproces. In de reactie op uw rapport over IDO's, dat binnenkort zal verschijnen, zal ik hier nader op reageren. Voor digitaal vaardige burgers wordt gewerkt aan de ontwikkeling van het project 'Eén Overheid': een overheidsbrede, landelijke informatievoorziening met informatie over publieke dienstverlening.

Het nieuwe stelsel Toegang en de wallet

U geeft aan dat de implementatie van het stelsel Toegang nog de nodige aanpassingen van DigiD en eHerkenning zullen vragen. Daarnaast is er volgens u nog onduidelijkheid over hoe de wallet in het stelsel van digitale authenticatie gaat passen. Ik wil hierbij opmerken dat er onderscheid gemaakt moet worden tussen het stelsel Toegang en de wallet, zoals opgenomen in het voorstel tot revisie van de eIDAS-verordening.

Met de beoogde wallet wordt niet enkel authenticatie mogelijk. Burgers en bedrijven kunnen met de wallet zelf bepalen welke gegevens zij van zichzelf verzamelen en welke zij daarvan zullen delen en met wie. Ik vind het belangrijk dat het gebruik van een wallet altijd vrijwillig blijft. Burgers en bedrijven kunnen daarom ook niet verplicht worden om zich door middel van een wallet te authentiseren bij overheidsdienstverlening.

Bij het stelsel Toegang gaat het om een stelsel van authenticatiemiddelen. DigiD en eHerkenning dienen in het nieuwe stelsel, net als nieuwe middelen, te voldoen aan de wettelijke eisen zoals vormgegeven in de Wdo. Daarnaast wordt er op dit moment hard gewerkt aan randvoorwaardelijke toegangsservices. U geeft hierbij aan dat een centraal aansluitpunt ontbreekt. In plaats van een centraal aansluitpunt wordt gewerkt aan een standaard koppelvlak. Deze standaardisatie zorgt ervoor dat dienstverleners zelf een aansluitmethode kunnen kiezen.

Belangrijk is dat de aansluiting van publieke dienstverleners op het nieuwe stelsel Toegang niet in één keer, maar geleidelijk gaat. Dienstverleners sluiten zich na de inwerkingtreding van de Wdo geleidelijk aan op het stelsel Toegang. De Wdo die hiervoor de basis legt zal, naar verwachting, op 1 juli gefaseerd in werking treden."

7.2 Nawoord

We concluderen dat DigiD en eHerkenning op dit moment toereikend functioneren. De staatssecretaris geeft aan de inhoud van het rapport mee te nemen bij verdere verbetering en doorontwikkeling van de authenticatiemiddelen. We volgen met belangstelling hoe de staatsecretaris omgaat met de uitdagingen voor de nabije toekomst die er ook zijn. Ons valt op dat het doel om iemand anders wettelijk digitaal te kunnen vertegenwoordigen er is sinds 2013. Er is ons geen concrete planning bekend voor het realiseren van de landelijke uitrol van digitaal wettelijk vertegenwoordigen. Zolang dit nog niet kan, is de overheid minder digitaal toegankelijk voor diverse groepen burgers. De staatsecretaris geeft aan dat er onderscheid gemaakt moet worden tussen het stelsel toegang (onder de Wdo) en de wallet (eIDAS2). Maar het is ons bijvoorbeeld onduidelijk hoe de wallet zich verhoudt met huidige en nieuwe authenticatiemiddelen onder de Wdo. En of de Wdo-eisen voor de wallet gaan gelden. Uitvoeringsorganisaties moeten makkelijk kunnen aansluiten op de nieuwe authenticatiemiddelen die kunnen voortvloeien uit de Wdo. Daarvoor is het in dit rapport beschreven aansluitpunt belangrijk.

Bijlagen

Bijlage 1 Onderzoeksverantwoording

We lichten in deze bijlage de gebruikte onderzoeksmethoden en -activiteiten toe.

Probleemstelling

De centrale probleemstelling voor dit onderzoek luidt:
"In hoeverre zijn de doelen in relatie tot digitale identiteit en de daarbij nu beschikbare authenticatiemiddelen DigiD en eHerkenning gerealiseerd? Zijn deze authenticatiemiddelen doelmatig en in hoeverre worden de beschikbaarheid, integriteit en exclusiviteit van genoemde authenticatiemiddelen in voldoende mate beheerst?"

Onderzoeksvragen

We hebben het onderzoek uitgevoerd aan de hand van de volgende vragen:

1. *In hoeverre zijn de doelen voor digitale identiteit en voor de nu beschikbare diensten DigiD en eHerkenning gerealiseerd?*
2. *Hoe doelmatig zijn eHerkenning en DigiD vergeleken met elkaar en in vergelijking met een ander authenticatiemiddel of vergelijkbare dienst in binnen- of buitenland?*
3. *In hoeverre beheerst de overheid de kwaliteit van DigiD en eHerkenning?*

We beschouwden DigiD en eHerkenning ook in het kader van de Wdo en eIDAS2.

Aanpak, toetsing en normen

De aanpak, toetsing en normen verschilden per onderzoekvraag.

Onderzoeksvraag 1

Voor onderzoeksvraag 1 onderzochten we in hoeverre de doelen gerealiseerd zijn, die de minister van BZK zich vanaf 10 jaar terug heeft gesteld. We onderzochten doelen voor gebruik/adoptie, functionaliteit en veiligheid, zoals de minister deze formuleerde in Kamerstukken en internationale verklaringen. Sommige doelen waren niet concreet genoeg geformuleerd om te toetsen, deze doelen hebben we geconcretiseerd in het toetsingskader dat te vinden is in bijlage 2.

Om te toetsen of de doelen zijn bereikt, verzamelden we documentatie en hielden we interviews. Vervolgens beoordeelden we of de minister de doelen geheel, gedeeltelijk of niet heeft bereikt.

Onderzoeksvraag 2

Voor onderzoeksvraag 2 brachten we de kosten in beeld voor de authenticatiemiddelen DigiD en eHerkenning. Dit deden we specifiek voor de jaren 2018 t/m 2021. Ook onderzochten we de mogelijke baten. We wilden DigiD en eHerkenning met een authenticatiemiddel in het buitenland kunnen vergelijken. Hiervoor hebben we een enquête uitgezet bij rekenkamers van Europese landen. We kregen 12 reacties op een enquête bij de rekenkamers van 25 Europese landen. Slechts 1 land had cijfers over de afgelopen 4 jaar en een authenticatiemiddel dat enigszins vergelijkbaar is met DigiD.

Onderzoeksvraag 3

Voor onderzoeksvraag 3 keken we naar de beheersing van de kwaliteit van DigiD en eHerkenning. Met kwaliteit bedoelen we de beschikbaarheid, integriteit en exclusiviteit van DigiD en eHerkenning. De definities hiervan staan in de begrippenlijst.

Om onderzoeksvraag 3 te beantwoorden maakten we gebruik van een door ons opgesteld toetsingskader. Bij de samenstelling van het toetsingskader hebben we gebruikgemaakt van verschillende bronnen zoals de Baseline Informatiebeveiliging Overheid (BIO – daarmee ook de internationale normen ISO27001 en ISO27002), de Nederlandse Overheids Referentie Architectuur (NORA) en het afsprakenstelsel eHerkenning. Daarnaast is verschillende wet- en regelgeving relevant, in ieder geval de Wet digitale overheid, Wet Beveiliging Netwerk en Informatiesystemen (Wbni) en verschillende EU-regelgeving, zoals de eIDAS-verordening.

Het toetsingskader is in lijn met (delen van) het GITC-kader van de Auditdienst Rijk (ADR), het 'Handbook on IT-audit for supreme audit institutions' en het 'Studierapport Algemene beheersing van IT-diensten' van NOREA, de beroepsorganisatie van IT-auditors.

We hebben het toetsingskader ook gebruikt voor activiteiten die uitbesteed worden binnen de dienstverlening van DigiD en/of eHerkenning. Hiervoor geldt namelijk dat de verantwoordelijkheid niet kan worden uitbesteed. De leverancier waaraan activiteiten zijn uitbesteed moet voldoende *assurance* kunnen verschaffen.

De Algemene Rekenkamer geeft geen *assurance*verklaring af volgens het stramien voor *assurance*-opdrachten van NOREA. Wel is voor beantwoording van onderzoeksvraag 3 een IT-audit uitgevoerd waarbij de kwaliteitsrichtlijnen van NOREA worden nageleefd. De normen in het toetsingskader toetsten we voor DigiD en eHerkenning. We wilden bijvoorbeeld weten of er processen en procedures zijn uitgewerkt voor IT-beheer. Ook wilden we kunnen vaststellen of dit in praktijk wordt toegepast. In auditthermen toetsten we de normen op basis van *opzet* en *bestaan*.
Wij beoordeelden de effectiviteit van de beheersmaatregelen aan de hand van aangeleverde documentatie, gesprekken en waarneming tijdens gesprekken.

DigiD en eHerkenning in het kader van de Wdo en eIDAS2
We beschouwden DigiD en eHerkenning ook in het kader van de Wdo en eIDAS2. Dit is gedaan door wetsteksten en documentatie te analyseren en interviews te houden.

Activiteiten
De beantwoording van de onderzoeksvragen vond plaats door het bestuderen van verschillende documenten. We hebben hiervoor openbare bronnen bekeken, zoals rapporten van onderzoeksbureaus, Kamerbrieven en documenten van de Europese Commissie. Daarnaast gebruikten we interne bronnen van het Ministerie van BZK en specifiek Logius.

Verder hebben we interviews afgenomen bij verschillende betrokkenen. Zo hebben we onder andere gesproken met medewerkers van het Ministerie van BZK, Logius, DICTU (Dienst ICT Uitvoering), RvIG (Rijksdienst voor Identiteitsgegevens) en Agentschap Telecom. Ook spraken we onder andere met vertegenwoordigers van de VNG, de Waag, SIDN, Currence en Itsme. In bijlage 3 is een lijst opgenomen met organisaties waar interviews zijn afgenomen en/of waar informatie vanuit verstrekt is.

Ook organiseerden we een interactieve workshop met een vertegenwoordiging van betrokkenen binnen het vakgebied. Mede naar aanleiding van output van de workshop hebben we ons toetsingskader verder aangescherpt en de scope verder bepaald.

Tot slot hebben we een aantal visualisaties gecreëerd, onder andere om de architectuur in beeld te brengen.

Bijlage 2 Toetsingskader doelen

In deze bijlage staan doelen voor digitale identiteit en authenticatie in detail uitgeschreven in onderstaande tabel. De minister van BZK stelde deze doelen de afgelopen 10 jaar. We verwijzen naar de bronnen waar deze doelen waren geformuleerd door de minister van BZK. Deze bronnen zijn te vinden in de literatuurlijst. In de tabel is opgenomen in hoeverre het doel is bereikt met de uitleg voor deze beoordeling.

Tabel 10 *Toetsingskader doelen digitale identiteit*

Nr.	Onderwerp	Doelstelling	Doel bereikt?	Uitleg
B.01a	Gebruik: reikwijdte Nederland	De voorzieningen bieden toegang tot digitale interactie met de overheid en organisaties met een publieke taak, in Nederland (BZK, 2021b).	Bereikt	Er is in Nederland digitale toegang/interactie/dienstverlening mogelijk, middels eHerkenning en DigiD, met publieke partijen, private partijen met een publieke taak alsook private partijen (ICTU, 2022). We hebben voor zowel DigiD als eHerkenning daarbij geen gedetailleerd inzicht aangetroffen in welke mate partijen nog moeten aansluiten.
B.01b	Gebruik: reikwijdte EU	De voorzieningen bieden toegang tot digitale interactie met de overheden en organisaties met een publieke taak in andere EU-lidstaten (BZK, 2021b, 2021c) (Europese Commissie 2014) .	Deels bereikt	Voor toegang tot dienstverlening in andere EU-lidstaten geldt dat het aantal transacties laag is evenals het aantal beschikbare diensten. Vandaar gedeeltelijk bereikt.
B.02	Gebruik: reikwijdte (eIDAS)	Nederlandse overheidsorganisaties en private organisaties met een publieke taak moeten sinds 29 september 2018 Europees erkende inlogmiddelen accepteren in hun digitale dienstverlening (Europese Commissie 2014).	Deels bereikt	Er zijn uitvoeringsorganisaties die genoemde genotificeerde middelen accepteren en diensten voor andere inwoners van EU-lidstaten aanbieden, er is echter geen beeld van welke nog niet zijn aangesloten en nog zouden moeten volgen. Wel is vastgesteld dat nog niet alle overheidsorganisaties Europees erkende inlogmiddelen accepteren. Vandaar gedeeltelijk bereikt.
B.03	Gebruik: reikwijdte (eIDAS)	Europese burgers en bedrijven die de beschikking hebben over een erkend inlogmiddel moeten dezelfde zaken kunnen regelen als alle andere burgers en bedrijven in een lidstaat (Europese Commissie 2014).	Niet vast te stellen	DigiD en eHerkenning zijn beschikbaar, Europees genotificeerd en kunnen ook in de EU worden gebruikt,[24] maar of dat in voldoende mate kan, voor dezelfde diensten als de inwoner van een land is niet vast te stellen.

Nr.	Onderwerp	Doelstelling	Doel bereikt?	Uitleg
B.04	Gebruik: reikwijdte (eIDAS)	Identificatiemiddelen kennen verschillende betrouwbaarheidsniveau's in relatie tot de classificatie van de gegevens en de aard van de diensten die er mee worden ontsloten (Europese Commissie 2014).	Bereikt	DigiD en eHerkenning kennen verschillende betrouwbaarheidsniveaus. Dienstaanbieders zijn zelf verantwoordelijk om het juiste niveau voor dienstverlening te bepalen.
B.05	Gebruik: toegankelijkheid	De voorzieningen zijn gebruiksvriendelijk en geschikt voor mobiele apparaten (zonder concessies te doen aan veiligheid) (Europese Raad 2017, 2018).	Bereikt, met kanttekening	Belangrijkste instrument bij DigID hiervoor zijn de toegankelijkheidseisen / toegankelijkheidsverklaringen. DigiD is bruikbaar vanuit een browser, waar nodig of gewenst in combinatie met een (eventueel gesproken) sms-code (onder niveau substantieel) en/of de DigiD-app. Daarnaast kan op mobiele apparaten de DigiD-app worden gebruikt. De DigiD-app is nodig vanaf het niveau substantieel en hoger. Genoemde app is alleen beschikbaar op het platform van Google of Apple. Om de app te kunnen gebruiken moet de burger zich registreren bij Google of Apple. Er is geen alternatief. Vandaar genoemde kanttekening. Nog niet alle eHerkenningsaanbieders werken met apps. eHerkenningsaanbieders hebben afspraken met betrekking tot toegankelijkheid geformuleerd en tonen dit aan middels een zelfverklaring.
B.06	Gebruik: toegankelijkheid	De voorzieningen zijn door allen op gelijke manier te gebruiken, waaronder door mensen met een lichamelijke beperking, met gepaste assistentie wanneer nodig (Europese Raad 2017, 2018).	Deels bereikt	Belangrijkste instrument bij DigiD hiervoor zijn de toegankelijkheidseisen / toegankelijkheidsverklaringen. Uit genoemde verklaringen blijkt dat een aantal voorzieningen nog niet 'volledig toegankelijk' is. Daarom gedeeltelijk bereikt. eHerkenningsaanbieders hebben afspraken met betrekking tot toegankelijkheid geformuleerd en tonen dit aan middels een zelfverklaring.
B.07	Functionaliteit	De voorzieningen stellen de identiteit vast van een partij (authenticatie) (BZK, 2013).	Bereikt	Met behulp van DigiD en eHerkenning kunnen dienstaanbieders de identiteit vaststellen.
B.08	Functionaliteit	De voorzieningen ondersteunen het bewijzen van bevoegdheden t.a.v. een specifieke dienst (autorisatie) (BZK, 2013).	Deels bereikt	Voor eHerkenning is dit doel gehaald. Voor DigiD niet geheel. De functionaliteit met betrekking tot machtigen en vertegenwoordigen is nog in ontwikkeling en nog niet afgerond.

Nr.	Onderwerp	Doelstelling	Doel bereikt?	Uitleg
B.09	Functionaliteit	Een ieder kan zich digitaal door een gemachtigde laten vertegenwoordigen (BZK, 2013).	Bereikt, met kanttekening	eHerkenning biedt deze functionaliteit en DigiD Machtigen bestaat. Kanttekening is dat dit niet in 1 keer kan voor alle diensten die met DigiD worden ontsloten, maar alleen per dienst. Vandaar de kanttekening.
B.10	Functionaliteit	Een ieder kan zich digitaal door een wettelijke vertegenwoordiger laten vertegenwoordigen (BZK, 2013).	Deels bereikt	Voor eHerkenning is dit doel bereikt. Voor DigiD geldt dat dit voor personen onder curatele, personen onder bewindvoering en voor minderjarige kinderen nog niet volledig is gerealiseerd. Proeven / eerste uitvoering lopen, maar realisatie is naar verwachting over enkele jaren afgerond (BZK, 2022d).
B.11	Functionaliteit	Een ieder kan digitaal een wilsuiting bevestigen of instemmen met de inhoud van een transactie (ondertekenen) (BZK, 2013).	Bereikt, met kanttekening	De functionaliteit is er voor burgers en bedrijven in de markt, onderdeel van 'vertrouwensdiensten', maar andere diensten dan DigiD en eHerkenning. De dienst DigiD bevat geen gekwalificeerde digitale handtekening. Wel kan er een wilsuiting worden gegeven, middels een authenticatie met DigiD of eHerkenning.[25] Een aantal van de eHerkenningspartijen biedt ook de functionaliteit digitale handtekening aan.
B.12	Functionaliteit	De voorzieningen ondersteunen de mogelijkheid tot *single-sign-on* voor naadloze toegang tot publieke dienstverlening (Europese Raad 2017)	Bereikt	Functionaliteit is er voor zowel DigiD als eHerkenning, volledige invoering is niet altijd opportuun vanuit beveiligingsoptiek en geldende wet/regelgeving.
B.13	Veiligheid	Helpt identiteitsfraude c.q. oneigenlijk gebruik voorkomen (BZK, 2013 en 2021c)	Deels bereikt	Het voorkomen van fraude, voor DigiD en eHerkenning, is verspreid over verschillende partijen, er ontbreekt een goed kwalitatief en kwantitatief beeld. Voor eHerkenning is er geen centraal fraudemeldpunt. Daarom gedeeltelijk bereikt.

Bijlage 3 Lijst geïnterviewde organisaties

We hebben tijdens ons onderzoek de volgende partijen geïnterviewd of we hebben informatie van hen ontvangen.

1. ADR (Auditdienst Rijk)
2. Agentschap Telecom
3. Belastingdienst
4. Capgemini
5. Commissie van Deskundigen voor het Toezicht op het ETD-stelsel
6. Currence
7. De Waag
8. DICTU (Dienst ICT Uitvoering)
9. Digidentity
10. Itsme (België)
11. KPN
12. Logius
13. Ministerie van BZK
14. Ministerie van EZK
15. Ministerie van VWS
16. Nationale Ombudsman
17. RvIG (Rijksdienst voor Identiteitsgegevens)
18. RVO (Rijksdienst voor Ondernemend Nederland)
19. SER (Sociaal Economische Raad)
20. SIDN (Stichting Internet Domeinregistratie Nederland)
21. Stichting Fraudehelpdesk
22. UWV
23. VNG (Vereniging van Nederlandse Gemeenten)
24. De rekenkamers van België, Duitsland, Estland, Finland, Italië, Letland, Litouwen, Noorwegen, Slovenië, Spanje, Tsjechië en Zwitserland

Bijlage 4 Begrippenlijst

Authenticatie: het *"bevestigen van de door de entiteit geclaimde identiteit [..]: i s het inderdaad de entiteit die het claimt te zijn?"* (ICTU, z.d.)

Autorisatie: het *"bepalen of iemand [..] in aanmerking komt om toegang te krijgen tot een dienst of informatie etc."* (BZK, 2021c).

Beschikbaarheid: de mate waarin een object (informatie, IT-dienst of IT-middel) continu beschikbaar is en de gegevensverwerking ongestoord voortgang kan hebben.

DigiD: de naam DigiD is een afkorting van 'Digitale Identiteit'. Met DigiD kunnen burgers inloggen om toegang te verkrijgen tot online dienstverlening van onder meer overheidsorganisaties.

Digitale identiteit: een verzameling van betrouwbare gegevens die een entiteit (persoon, organisatie) representeert in het digitale domein (BZK, 2021c).

eHerkenning: eHerkenning is een afsprakenstelsel met een netwerk van publieke en private partijen. eHerkenning regelt in de basis de herkenning (authenticatie) en controleert de bevoegdheid (autorisatie) van personen die online een dienst willen afnemen. Dit is een middel specifiek voor bedrijven.

eIDAS: eIDAS staat voor *Electronic Identities And Trust Services*. Het biedt een kader voor Europees gebruik van elektronische identiteiten en vertrouwensdiensten.

eIDAS-netwerk: door middel van het eIDAS-netwerk is het mogelijk om bij aangesloten dienstverleners, zoals gemeenten of de nationale belastingdienst, in andere Europese landen in te loggen met een Nederlands authenticatiemiddel zoals DigiD. Andersom is dit ook mogelijk. Een Duitse burger kan op die manier met diens Duitse authenticatiemiddel bijvoorbeeld bij de Nederlandse Belastingdienst inloggen.

Exclusiviteit: de mate waarin uitsluitend geautoriseerde personen of apparatuur via geautoriseerde procedures en beperkte bevoegdheden gebruikmaken van een object (IT-dienst of IT-middel) of toegang hebben tot een object (creëren, wijzigen, verwijderen of lezen van gegevens).

Identificatie: het *"uniek duiden van een entiteit in een bepaalde context [en het] antwoord op de vraag: welke entiteit is het?"* (ICTU, z.d.).

Integriteit: de mate waarin het object (gegevens, IT-dienst of IT-middel) in overeenstemming is met de beoogde werkelijkheid.

Machtigen: voor DigiD is een machtigingsdienst (DigiD Machtigen) beschikbaar. Hiermee kun je als burger 'machtigen op eigen verzoek'. Je kunt andere personen machtigen voor een bepaalde dienst, bijvoorbeeld belasting aangeven. Die persoon mag dan namens jou inloggen met DigiD Machtigen bij de Belastingdienst.

Wallet: een wallet is kort gezegd een digitale portemonnee met persoonsgegevens. Die portemonnee bevat bijvoorbeeld je rijbewijs, NAW-gegevens, diploma's, medische gegevens, et cetera. Het idee is dat je alleen die gegevens laat zien die echt nodig zijn. Dat kan bij zowel overheid als bij bedrijven.

Wettelijk vertegenwoordigen: er zijn situaties waarbij machtigen op eigen verzoek niet kan of wordt gewenst. Ook dan is inloggen namens een persoon belangrijk. Die situaties kun je scharen onder 'wettelijk vertegenwoordigen'. Wettelijke vertegenwoordiging is bijvoorbeeld het geval bij ouder-kindrelaties of volwassenen die niet handelingsbekwaam zijn en gebruikmaken van bewindvoerders.

Wdo: de Wet digitale overheid (Wdo) legt het fundament voor de verdere digitalisering van de overheid. De Wdo zorgt ervoor dat er zoveel mogelijk standaarden worden gehanteerd. Ook behandelt de Wdo de digitale toegang tot publieke dienstverlening voor burgers en bedrijven. De Wdo biedt ook de mogelijkheid om private authenticatiemiddelen aan te bieden (naast DigiD).
De minister van BZK wil ook zorgen voor een publiek authenticatiemiddel voor bedrijven. In eerste instantie zal dit authenticatiemiddel gericht zijn op het doen van belastingaangifte. Dit laatste wordt geregeld in het reeds aangenomen wetsvoorstel Wdo dat vanaf 1 juli 2023 gefaseerd in werking treedt. De minister van BZK werkt nog aan een tweede wetsvoorstel voor de Wdo. De invoeringsdatum daarvan is onbekend. In dit tweede deel van de Wdo beoogt de minister van BZK te zorgen voor een publiek authenticatiemiddel voor bedrijven, breder dan alleen voor het doen van belastingaangifte.

Bijlage 5 Literatuurlijst

Literatuur

Algemene Rekenkamer. (2016). *Aanpak van laaggeletterdheid*. Den Haag: Eigen Beheer. Bijlage bij Kamerstuk 28760, nr. 56, Tweede Kamer, vergaderjaar 2015-2016.

BZK (2010). Brief van de staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties. *Modernisering van de overheid*. Tweede Kamer, vergaderjaar 2009-2010, 29 362, nr. 177.

BZK (2013). Brief van de ministers van Binnenlandse Zaken en Koninkrijksrelaties en Economische Zaken. *Informatie- en communicatietechnologie (ICT)*. Tweede Kamer, vergaderjaar 2013-2014, 26 643, nr. 299.

BZK (2019). *Jaarverslag en slotwet ministerie van Binnenlandse Zaken en Koninkrijksrelaties 2018*. Den Haag: eigen beheer.

BZK (2020). *Jaarverslag en slotwet ministerie van Binnenlandse Zaken en Koninkrijksrelaties 2019*. Den Haag: eigen beheer.

BZK (2021a). *Jaarverslag en slotwet ministerie van Binnenlandse Zaken en Koninkrijksrelaties 2020*. Den Haag: eigen beheer.

BZK (2021b). Brief van de staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties. Tweede Kamer, vergaderjaar 2020-2021, 26 643, nr. 750.

BZK (2021c). Brief van de staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties. Tweede Kamer, vergaderjaar 2020-2021, 26 643, nr. 743.

BZK (2021d). Brief van de staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties. Tweede Kamer, vergaderjaar 2021-2022, 26643, nr. 809.

BZK (2022a). *Jaarverslag en slotwet ministerie van Binnenlandse Zaken en Koninkrijksrelaties 2021*. Den Haag: eigen beheer.

BZK (2022b). *Beantwoording van de vragen van de Tweede Kamer der Staten-Generaal over de Voortgangsrapportage Europese Digitale Identiteit* (26643-902). Bijlage bij Kamerbrief met kenmerk: 2022-0000604333.

BZK (2022c). Brief van de staatssecretaris van Koninkrijksrelaties en Digitalisering. *Informeren burgers over verhoging authenticatieniveau aantal afnemers DigiD*. Kenmerk: 2022-0000585495.

BZK (2022d). Brief van de staatssecretaris van Koninkrijksrelaties en Digitalisering. *Voortgangsrapportage domein Toegang najaar 2022*. Tweede Kamer, vergaderjaar 2022-2023, 26 643, nr. 914.

Ecorys (2016). Business Case Inloggen in het BSN- domein. *De kosten en baten van het eID-stelsel*. Rotterdam: eigen beheer.

Ecorys (2018). *Maatschappelijke kosten-batenanalyse Machtigingsstelsel*. Rotterdam: eigen beheer.

Ecorys (2023). *Concept Herijking MKBA Digitale Toegang: Naar aanleiding van de Wet digitale overheid*. Rotterdam: eigen beheer.

Europese Commissie (2014). *Verordening (EU) Nr. 910/2014 van het Europees Parlement en de Raad betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG.*

Europese Commissie (2021). *Voorstel voor een Verordening van het Europees Parlement en de Raad tot wijziging van Verordening (EU) nr. 910/2014 betreffende een Europees kader voor een digitale identiteit*. COM(2021) 281 final, 2021/0136(COD).

Europese Raad (2017), *Tallinn Declaration on E-Government*.

Europese Raad (2018), B*erlin Declaration on Digital Society and Value-Based Digital Government*.

ICTU (2022). *Monitor Digitale Overheid 2022*. Bijlage bij Kamerstuk 26 643, nr. 945, Tweede Kamer, vergaderjaar 2022-2023.

ICTU (z.d.). *NORA: Identificatie en authenticatie*. Via website www.noraonline.nl.

Koninklijke Bibliotheek (2022). *Outputregistratietool Q3 2022, september 2022.*

Probiblio (z.d.). *Omgaan met DigiD in het IDO*. Via website www.probiblio.nl.

Internetbronnen

Afsprakenstelsel Elektronische Toegangsdiensten
https://afsprakenstelsel.etoegang.nl/

CBS
https://www.cbs.nl/

DigiD
https://www.digid.nl/

DigiD Machtigen
https://machtigen.digid.nl/

Digitale Overheid
https://www.digitaleoverheid.nl/

EDI Pleio (community voor Europese Digitale Identiteit georganiseerd door BZK)
https://edi.pleio.nl/

eHerkenning
https://eherkenning.nl/

eIDAS verordening 2014
https://eur-lex.europa.eu/legal-content/NL/TXT/HTML/?uri=CELEX%3A32014R0910

Elektronische handtekening
https://www.rijksoverheid.nl/onderwerpen/digitale-overheid/vraag-en-antwoord/wat-is-een-elektronische-handtekening

Europese Digitale Identiteit
https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_nl

Forum Standaardisatie
https://www.forumstandaardisatie.nl/

Logius
https://logius.nl/

ICTU
https://ictu.nl/

Kamer van Koophandel
https://kvk.nl/

NORA (Nederlandse Overheid Referentie Architectuur)
http://noraonline.nl

Probiblio.nl
https://www.probiblio.nl/omgaan-met-digid-in-het-ido

Register van toegangelijkheidsverklaringen
https://www.toegankelijkheidsverklaring.nl/register

Rijksinspectie Digitale Infrastructuur (RDI), voorheen Agentschap Telecom
https://www.rdi.nl/

Rijksoverheid
https://www.rijksoverheid.nl/

Trusted List Netherlands, Trust Service Providers (eIDAS Dashboard)
https://esignature.ec.europa.eu/efda/tl-browser/#/screen/tl/NL

Verordening van het Europees Parlement en de Raad tot wijziging van Verordening (EU) nr. 910/2014 betreffende een Europees kader voor een digitale identiteit (eIDAS2)
https://eur-lex.europa.eu/legal-content/NL/TXT/HTML/?uri=CELEX:52021PC0281&from=E

Bijlage 7 Eindnoten

1. Meer specifiek: dit authenticatiemiddel zal eerst gericht zijn op het doen van belastingaangifte. Dit wordt reeds in de eerste tranche van de Wdo geregeld. In de tweede tranche van de Wdo zal dit authenticatiemiddel breder inzetbaar zijn dan alleen voor het doen van belastingaangifte.
2. Dit afsprakenstelsel is openbaar beschikbaar op internet (Bron: Afsprakenstelsel Elektronische Toegangsdiensten).
3. De figuur is een versimpelde weergave, eHerkenning kent bijvoorbeeld verschillende betrouwbaarheidsniveaus, net als DigiD. Deze zijn in de figuur niet opgenomen voor de leesbaarheid van de figuur. De betrouwbaarheidsniveaus van eHerkenning liggen momenteel tussen niveau eH2 en eH4. eH2 is momenteel het laagste niveau met gebruikersnaam en wachtwoord, het hoogste betrouwbaarheidsniveau is eH4. Bij eH4 worden persoonsgegevens gecheckt door fysieke verschijning en legitimatie met een origineel identiteitsbewijs.
4. Ter vergelijking: in 2021 telde Nederland 17,48 miljoen inwoners (Bron: CBS). Overigens kunnen Nederlanders die in het buitenland wonen ook een DigiD-account hebben.
5. Ter vergelijking: eHerkenning is beschikbaar voor alle rechtspersonen die ingeschreven staan in het Handelsregister. In 2021 waren dit er 2.199.387 (Bron: KVK).
6. T/m jaar 2020 werden sommige gebruikers meerdere malen geteld met meerdere accounts. Vanaf 2021 is in de Monitor Digitale Overheid een keuze gemaakt om alleen de unieke accounts weer te geven op basis van het hoogst geactiveerde inlogmiddel.
7. Er zijn meerdere soorten elektronische handtekeningen. Namelijk de gewone, geavanceerde en gekwalificeerde elektronische handtekening. Alleen de zogenaamde gekwalificeerde elektronische handtekening voldoet aan alle wettelijke eisen en is altijd rechtsgeldig, gelijkgesteld aan de handtekening met pen. Bron: Rijksoverheid (subpagina) Voorbeelden van partijen die deze functionaliteit aanbieden zijn KPN, Cleverbase en Digidentity. Bron: Trusted List Netherlands, Trust Service Providers (eIDAS Dashboard)
8. Er bestaat wel een Centraal Meldpunt Identiteitsfraude (CMI), maar hier komen geen meldingen binnen over fraude met eHerkenning en heel weinig fraudemeldingen met DigiD.
9. Vanuit de maatschappij gezien spreken we over ‘kosten’. Vanuit BZK gezien zijn het ‘uitgaven’ en vanuit Logius gezien gaat het om ‘omzet’. We verkiezen in ons rapport de term ‘kosten’, omdat dit ons inziens het meeste aansluit bij de beleving van burgers en bedrijven en omdat het aansluit bij de terminologie van maatschappelijke kosten- en batenanalyses.

10. DigiD Machtigen wordt binnen de rijksoverheid vaak als aparte entiteit gezien, los van DigiD en eHerkenning. Vanuit een burger- en bedrijvenperspectief beschouwen wij dit als onontbeerlijk onderdeel voor digitale authenticatie. Om die reden vermelden wij deze kosten.
11. Hier zijn begrote kosten opgenomen omdat de realisatiekosten niet gemeld zijn in het jaarverslag van Logius en niet binnen de onderzoekstermijn aan ons zijn opgeleverd.
12. De schatting is als volgt tot stand gekomen. We hebben een benadering gemaakt van de kosten voor het uitgeven van eHerkenningsaccounts op basis van een gemiddelde prijs (exclusief btw) bij eHerkenningsleveranciers en het aantal uitgegeven eHerkenningsaccounts. De kosten die uitvoerende partijen zoals UWV en gemeenten maken om aan te sluiten op eHerkenning via eHerkennings-makelaars zijn niet bekend en niet in dit bedrag opgenomen. Voor DigiD zijn deze aansluitkosten voor uitvoerende partijen ook niet bekend.
13. Alleen Letland kon deze gegevens tijdig in de onderzoeksperiode aanleveren. Het exacte aantal unieke gebruikers is niet bekend bij de rekenkamer van Letland zonder aanvullende gegevensanalyses uit te voeren. Deze rekenkamer geeft aan dat het mogelijk het grootste deel van de 1,9 miljoen inwoners van Letland zou kunnen bereiken. Dit is ongeveer een tiende van het aantal inwoners in Nederland. Al met al zijn er te veel variabelen anders, waardoor een internationale vergelijking niet te maken is.
14. Deze redeneerwijze is in lijn met studies zoals de 'Business Case Inloggen in het BSN- domein. De kosten en baten van het eID-stelsel.' Ecorys (2016):
    "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. 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." Pagina 43.
    Voor het uurtarief wordt uiteindelijk als bron het gemiddelde uurtarief in 2015 van salarisnet.nl gebruikt. Wij gebruiken als bron voor het uurloon in 2021 het gemiddelde uurloon. Bron: CBS (subpagina). De 'ruim 550 miljoen transacties' is te vinden in tabel 1.
    Overigens is de burger ook tijd kwijt aan het installeren van DigiD, hoeveel minuten is niet in te schatten. Relevant bij deze opmerking is dat de beredenering ook stand houdt als we in plaats van een kwartier tijdsbesparing voor de burger slechts 5 minuten aanhouden. Daarnaast is de tijdsbesparing voor bedrijven en uitvoerende organisaties niet gekwantificeerd, potentieel zou die besparing groot kunnen zijn.

15. Wanneer we het in dit rapport het over de Wdo hebben, bedoelen we dit geheel: de wet en een aantal lagere besluiten en regelingen.
16. In de rapporttekst spreken wij over ‘aansluitpunt’ als we de ‘routeringsvoorziening’ bedoelen. Deze routeringsvoorziening is als volgt geformuleerd in de consultatieversie van het “Besluit Digitale overheid”, uitgewerkte regelgeving van de Wdo:
    “Beleidsuitgangspunt en wens van overheidsdienstverleners is om op eenvoudige wijze en eenmalig op de voorzieningen voor elektronische toegang te kunnen aansluiten. Daartoe wordt ingevolge de wet digitale overheid een nieuwe voorziening ingericht, de routeringsvoorziening, waarvoor de minister verantwoordelijk is. De routeringsvoorziening heeft tot doel (semi-) publieke dienstverleners te ontzorgen in hun aansluiting op wettelijk verplichte authenticatielandschappen (DigiD, eIDAS, etc.). De routeringsvoorziening biedt de afnemer/dienstverlener hiertoe één koppelvlak, één aanspreekpunt en één factuur. De routeringsvoorziening voorziet hierin door te fungeren als tussenpartij die elektronisch berichtenverkeer met de authenticatielandschappen enerzijds vertolkt naar de dienstverlener anderzijds. Technisch bestaat de routeringsvoorziening uit één of meerdere publieke en mogelijk één of meerdere private routeringsdiensten.”
17. We merken op dat ‘gratis’ niet bestaat. Financiering zal bijvoorbeeld uit algemene middelen, uit heffingen op aansluitende dienstverleners of anderszins geregeld moeten worden. Gegeven dit feit is ook onduidelijk wat de businesscase voor private partijen zal zijn, die mogelijk een *wallet zullen aanbieden.*
18. De wallet moet ook een wettelijk erkend identificatiemiddel worden (WID).
19. De vermelde aantallen komen overeen met wat Logius heeft aangeleverd aan ICTU t.b.v. de Monitor Digitale Overheid. De aantallen zijn in de Monitor niet volledig correct overgenomen. Per e-mail hebben wij van Logius de correcte getallen ontvangen.
20. Zie als onderdeel van de Wdo de Memorie van toelichting wet GDI, onderdeel 13, overgangsrecht, pagina 52:
    “Dit wetsvoorstel ziet op het gebruik van erkende authenticatiemiddelen in het elektronisch verkeer met bestuursorganen en aangewezen organisaties. Alleen middelen op het betrouwbaarheidsniveau ‘substantieel’ of ‘hoog’ kunnen in aanmerking komen voor het verkrijgen van een erkenning. Bestuursorganen en aangewezen organisaties mogen slechts toegang tot hun elektronische diensten op betrouwbaarheidsniveau ‘substantieel’ of ‘hoog’ verlenen, indien de gebruiker met een erkend middel inlogt. Zij zijn verplicht vanaf de inwerkingtreding van dit wetsvoorstel erkende middelen te accepteren. Niet-erkende middelen mogen niet geaccepteerd worden voor elektronische diensten op betrouwbaarheidsniveau ‘substantieel’ of ‘hoog’. Hiervoor geldt geen overgangsrecht. Middelen op een

lager betrouwbaarheidsniveau dan substantieel of hoog, zoals het uit te faseren middel DigiD, zullen niet worden erkend ingevolge dit wetsvoorstel. Bij wijze van overgangsperiode mogen bestuursorganen en aangewezen organisaties deze middelen met betrouwbaarheidsniveau laag nog drie jaar na de inwerkingtreding van dit wetsvoorstel accepteren voor diensten waarvoor een laag betrouwbaarheidsniveau geldt."

21. Dit betreft de periode van het ontstaan van de IDO's in 2019 t/m derde kwartaal 2022.
22. Deze aantallen van 4 miljoen en 2,5 miljoen mensen zijn gebaseerd op onderzoeken gepubliceerd in 2013 en 2016. Het aantal van 2,5 miljoen is afkomstig uit het rapport 'Aanpak van laaggeletterdheid' (2016). De Algemene Rekenkamer stelde in dat rapport: "Er zijn in Nederland 2,5 miljoen mensen van 16 jaar en ouder die moeite hebben met één of twee van deze vaardigheden [lezen en rekenen]". Het aspect 'digitale vaardigheden' is een paar keer ter sprake gekomen in dit rapport, maar de Algemene Rekenkamer heeft geen uitspraken gedaan over het aantal niet-digivaardigen.
23. De percentages tellen niet op tot 100%. Dit heeft te maken met het feit dat de vragen betrekking kunnen hebben op meerdere categorieën.
24. DigiD en eHerkenning kennen een hoge mate van acceptatie/gebruik en zijn door de EU genotificeerd.
25. Het 'ondertekenen' van de aangifte Inkomstenbelasting met DigiD is hiervan het bekendste voorbeeld.

Algemene Rekenkamer
Afdeling Communicatie
Postbus 20015
2500 EA Den Haag
070 342 44 00
voorlichting@rekenkamer.nl
www.rekenkamer.nl

Foto: ANP, Koen van Weel.

De tekst in dit document is
vastgesteld op 24 maart 2023.
Dit document is op 29 maart 2023
aangeboden aan de
Tweede Kamer.

Den Haag, maart 2023