# Impactanalyse Wet digitale overheid

## 1e analyse op de onderdelen informatiebeveiliging, acceptatieplicht, en betrouwbaarheidsniveaus

## Eindrapport

April 2021

Auteurs: Anneleen van Beek, Ewout Bückmann, Felicia Flamm en Hedzer Uulders

# Samenvatting

De Wet digitale overheid (Wdo) – voorheen Wet generieke digitale infrastructuur – vormt de eerste tranche van regelgeving ten behoeve van de verdere digitalisering van de overheid op verschillende niveaus[1]. De wet bevat de meest urgente onderwerpen van regelgeving voor de digitale overheid, te weten:

- de bevoegdheid om bepaalde (open) standaarden te verplichten in het elektronisch verkeer van de overheid;
- het stellen van regels over informatieveiligheid en het verwerken van persoonsgegevens;
- de verantwoordelijkheid voor het beheer van de voorzieningen en diensten binnen de generieke digitale overheidsinfrastructuur (GDI);
- regels voor de digitale toegang tot publieke dienstverlening voor inwoners (natuurlijke personen) en organisaties (rechtspersonen en ondernemingen).

De wet is op 18 februari 2020 door de Tweede Kamer aangenomen. Naar aanleiding van de vragen in de Eerste Kamer is onlangs besloten tot een wetswijziging, die de inwerkingtreding van de wet (opnieuw) zal vertragen[2]. De wet zelf is een zogeheten kaderwet: de wet regelt algemene principes, verantwoordelijkheden en procedures, maar bevat geen gedetailleerde regels. De uitwerking vindt plaats in lagere regelgeving, zoals in algemene maatregelen van bestuur (AMvB's) en ministeriële regelingen (MR's)[3].

*Beschrijving onderzoek*

Dit rapport biedt een analyse naar de impact van de Wdo aan de hand van de reeds beschikbaar gekomen onderdelen van de wet (Besluit digitale overheid, Regeling betrouwbaarheidsniveaus, Besluiten burger- en bedrijfsmiddelen). Dit onderzoek richt zich daarmee op enkele onderdelen van de Wdo die inmiddels zijn uitgewerkt, te weten de informatiebeveiliging, acceptatieplicht en betrouwbaarheidsniveaus betreffende inlogmiddelen voor publieke dienstverlening. De samenhang van deze drie onderdelen met nog niet beschikbare lagere regelgeving kon nog niet op impact worden getoetst. Hierdoor kan alleen op hoofdlijnen inzicht gegeven worden in de uitvoeringsconsequenties. De uitkomsten van dit onderzoek geven daarbij inzicht in de randvoorwaarden en afhankelijkheden die een rol spelen met de nog niet beschikbare regelgeving zodat op een later moment, wanneer de totstandkoming van de lagere regelgeving verder gevorderd is, de daadwerkelijke (samenhangende) impact kan worden bepaald.

*Conclusie*

Onder de huidige omstandigheden is de Wdo voor gemeenten niet goed uitvoerbaar. Hier zijn in deze analyse verschillende redenen voor aangegeven. Om de wet voor gemeenten uitvoerbaar te maken zijn de belangrijkste aandachtspunten en randvoorwaarden:

- Gemeenten moeten de informatiebeveiliging op de toegang tot het stelsel op orde hebben, voordat de wet daadwerkelijk in werking treedt. Omdat het nog niet duidelijk is op welke manier er op het stelsel aangesloten kan worden, is ook niet duidelijk hoe de toegangsbeveiliging er precies uit gaat zien. Voorbereidingen kunnen dan ook nog niet getroffen worden.

[1] MvT Wdo
[2] https://www.rijksoverheid.nl/documenten/kamerstukken/2021/02/19/memorie-van-antwoord-bij-wetsvoorstel-digitale-overheid
[3] Een overzicht hiervan is te vinden in de bijlage bij de Kamerbrief over de Wdo van 13 mei 2020: https://www.rijksoverheid.nl/documenten/publicaties/2020/05/13/uitvoeringsregelgeving-onder-de-wet-digitale-overheid

- Gemeenten moeten in staat zijn de digitale toegang op de juiste betrouwbaarheidsniveaus te bieden. Nog niet alle middelen met hogere betrouwbaarheidsniveaus zijn beschikbaar of bekend bij de inwoners (voor organisaties is dit wel al mogelijk). Ook is nog niet duidelijk hoe moet worden omgegaan met verschillende betrouwbaarheidsniveaus bij gemeenten die gebruik maken van *Single Sign-On* (SSO) en portalen. De Wdo hanteert een gefaseerde inwerkingtreding. Deze fasering komt niet goed overeen met de afhankelijkheden tussen onderlinge onderdelen. Voor het succesvol en verantwoord kunnen overstappen naar hogere betrouwbaarheidsniveaus is de beschikbaarheid van de machtigingsvoorziening een belangrijke randvoorwaarde.
- Gemeenten moeten alle toegelaten burger- en bedrijfsmiddelen accepteren, maar zijn hiervoor afhankelijk van een publieke routeringsvoorziening, tenzij gemeenten tijdig zelf iets kunnen regelen. Omdat functionaliteit en planning hiervan onduidelijk is, kunnen gemeenten hier niet op anticiperen.

Bij gebrek aan duidelijkheid hierover ontstaat onrust bij gemeenten omdat niet duidelijk is wat er op welk moment van ze verwacht wordt en of dat technisch en organisatorisch haalbaar is. Ook zijn er zorgen dat inwoners en organisaties hierdoor niet goed worden meegenomen in het proces. Het risico is dat de overgang naar het beoogde stelsel van de Wdo niet soepel verloopt en er problemen ontstaan in de continuïteit van de digitale dienstverlening van gemeenten (en andere bestuursorganen). Gemeenten maken zich met name zorgen over wat het voor inwoners betekent, het inloggen wordt met hogere betrouwbaarheidsniveaus ingewikkelder en er komen nieuwe (onbekende) inlogmiddelen beschikbaar. Als de transitie niet goed verloopt kan dit nadelige gevolgen hebben voor inwoners die op onderdelen van deze digitale dienstverlening afhankelijk zijn.

### *Aanbevelingen*

Op grond van het onderzoek worden een aantal aanbevelingen gedaan. Als eerste is meer duidelijkheid nodig om een goede voorbereiding op de Wdo te kunnen treffen. Maak op korte termijn een gedegen en haalbare planning voor de inwerkingtreding van de wet en de technische oplevering van voorzieningen. Geef ook zo spoedig mogelijk duidelijkheid over de kosten die worden doorbelast, of maak hier een prognose voor die periodiek wordt geüpdate. Planning en kostenprognose helpt gemeenten om ook financieel te kunnen anticiperen op de wet.

Neem de randvoorwaarden en afhankelijkheden tussen de verschillende regelgeving en bijbehorende voorzieningen in deze planning nadrukkelijk mee zodat de Wdo goed uitvoerbaar wordt. Zorg bijvoorbeeld dat voor de acceptatieplicht zowel een routeringsvoorziening als ook een machtigingsdienst beschikbaar is. Het vraagstuk machtigen kan niet los worden gezien van de inlogmiddelen en de bijbehorende betrouwbaarheidsniveaus, omdat wijzigingen in de betrouwbaarheidsniveaus van inlogmiddelen weerslag hebben op de vraag naar machtiging. Om problemen in de uitvoering te vermijden moeten deze vraagstukken gezamenlijk en op hetzelfde moment worden opgelost.

Richt een proces in om telkens bij het beschikbaar komen van nieuwe onderdelen van de Wdo de impact te bepalen en daarbij ook terug te kijken naar de impact zoals die eerder op andere onderdelen bepaald is. De losse elementen van de Wet zullen getrapt beschikbaar komen. Deze elementen staan echter niet los van elkaar. De impact van een los bekeken AMvB of Regeling kan flink veranderen door bepalingen die in een ander onderdeel worden opgenomen. Risico is dat bij het doen van losse impactanalyses samenhang en onderling doorwerking niet goed wordt onderkend. Heb hier als opdrachtgever van de analyses ook nadrukkelijk aandacht voor.

# Inhoud

# 1. Inleiding

Dit onderzoek is een eerste analyse naar de impact van de Wet digitale overheid en richt zich in het bijzonder op enkele onderdelen van de Wet digitale overheid die inmiddels zijn uitgewerkt, te weten de informatiebeveiliging, acceptatieplicht en betrouwbaarheidsniveaus met betrekking op de inlogmiddelen voor publieke dienstverlening. Dit onderzoek geeft inzicht in wat deze onderdelen van de wet betekenen voor de gemeentelijke uitvoering en in de stappen die gemeenten moeten nemen om eraan te voldoen en worden aanbevelingen gedaan voor een goede implementatie. Daarnaast beoogt dit onderzoek het bredere kader van de Wdo te schetsen waarbinnen deze onderdelen vallen, om zo zicht te bieden op de randvoorwaarden en afhankelijkheden die bij de Wdo een rol spelen. Hieronder wordt eerst ingegaan op de aanleiding van het onderzoek, vervolgens op de scope en onderzoeksvraagstelling en tenslotte op de aanpak.

## 1.1. Achtergrond/Aanleiding

De Wet digitale overheid kent een lange aanlooptijd. De wet heette oorspronkelijk Wet generieke digitale infrastructuur. Deze wet beoogde met name overheidsbreed open standaarden verplicht te kunnen maken; de veiligheid en betrouwbaarheid van de digitale overheidsdienstverlening te versterken; eenvoudige, veilige en betrouwbare toegang van inwoners en organisaties tot elektronische overheidsdienstverlening te realiseren en een terugvaloptie voor toegang tot digitale dienstverlening te creëren door het toelaten van verschillende inlogmiddelen[4]. Deze wet creëerde hiermee ook delen van het bredere stelsel van digitale basisvoorzieningen van de overheid: de generieke digitale infrastructuur (GDI). Mede door dynamische technische ontwikkelingen werd het wetgevingsproces voor de Wet GDI tranchegewijs opgezet. Parallel hieraan is in 2018 de Europese eIDAS-verordening ingegaan, waardoor publieke organisaties in Nederland Europees erkende inlogmiddelen, inclusief de bijbehorende beveiligingsniveaus, moeten accepteren binnen hun digitale dienstverlening.

In 2017 kreeg de wet GDI de naam Wet digitale overheid (Wdo). De doelstellingen van de wet bleven in grote lijnen dezelfde. De wet is opgebouwd als een kaderwet, die voor de eerste tranche wordt uitgewerkt in meer dan tien onderliggende besluiten en regelingen op het gebied van onder meer standaarden, toegankelijkheid, betrouwbaarheidsniveaus, inlogmiddelen, erkenning, aansluiting en bekostiging. Na enkele jaren voorbereiding is op 18 februari 2020 de kaderwet Wdo – met algemene regels over open standaarden, het inloggen door inwoners en organisaties bij de overheid en over informatieveiligheid en privacy – aangenomen door de Tweede Kamer. Als ingangsdatum werd 1 juli 2020 aangehouden. Bij behandeling in de Eerste Kamer heeft de staatssecretaris n.a.v. Kamervragen besloten de wet te wijzigen door het toevoegen van een wettelijk verhandelverbod voor gegevens en door het opnemen in de wet van de principes *privacy by design* en *open source*[5]. De novelle die hierdoor ontstaat zal het wetgevingsproces opnieuw doorlopen, zodat de Wdo voorlopig niet in werking zal treden. Het is onduidelijk wat dit betekent voor de nog niet beschikbare regelgeving.

[4] Zie de Memorie van Toelichting bij het Wetsvoorstel GDI (https://www.internetconsultatie.nl/wetgdi/details)
[5] Zie Memorie van antwoord van 19 februari 2021. https://www.rijksoverheid.nl/documenten/kamerstukken/2021/02/19/memorie-van-antwoord-bij-wetsvoorstel-digitale-overheid

## 1.2. Scope

Dit onderzoek richt zich op de volgende besluiten en regelingen als uitwerkingen van artikelen uit de kaderwet Wdo:

- Besluit digitale overheid (grondslag Wdo art. 4 en 16)
- Regeling classificering betrouwbaarheidsniveaus dienstverlening (grondslag Wdo art. 6)

Daarnaast worden in dit onderzoek ook die artikelen betrokken die niet nader in een regeling uitgewerkt gaan worden maar wel gevolgen hebben voor gemeenten, in het kader van de acceptatieplicht (Wdo art.7 en 15). Verder worden in dit onderzoek bredere randvoorwaarden en afhankelijkheden benoemd die een rol (zullen) spelen bij de toekomstige invoering van de Wdo. Daarmee wordt ook de impact van de Wdo in bredere zin verkend.

Dit onderzoek raakt op punten (indirect) aan het Besluit burgermiddelen en erkende diensten en het Besluit bedrijfsmiddelen en erkende diensten, voor zover deze zien op regels en (technische) eisen waaraan private en publieke middelen moeten voldoen en die impact hebben op de gemeentelijke aansluiting hierop. De nadere uitwerking van deze regels en eisen – in de vorm van de Regeling toelating burger- en bedrijfsmiddelen en erkende diensten – is echter nog niet beschikbaar.

Dit onderzoek richt zich niet op artikelen uit de Wdo die worden uitgewerkt in regelingen die nog niet klaar zijn, en betrekking hebben op bijvoorbeeld bekostiging en standaarden.

Samenvattend gaat dit onderzoek in essentie dus over Wdo artikel 4, 6, 7, 15 en 16 en daarmee over drie onderwerpen die impact hebben op de gemeentelijke uitvoeringspraktijk, te weten:

- De informatiebeveiligingsplicht met betrekking tot de toegang tot digitale dienstverlening die het Besluit digitale overheid op grond van Wdo art. 4 en 16 met zich meebrengt voor gemeenten;
- De noodzaak voor gemeenten om hun digitale dienstverleningsprocessen in te schalen aan de hand van de benodigde betrouwbaarheidsniveaus, die op grond van Wdo art.6 voortvloeit uit de Regeling classificering betrouwbaarheidsniveaus dienstverlening en
- De plicht voor gemeenten om publieke en private inlogmiddelen te accepteren op grond van Wdo art.7 en 15.

De navolgende hoofdstukken zijn dan ook gestructureerd langs deze drie lijnen. De samenhang van deze drie onderdelen met nog niet beschikbare lagere regelgeving is nog niet op impact is getoetst. Hierdoor kan alleen op hoofdlijnen inzicht gegeven worden in de uitvoeringsconsequenties. De uitkomsten van dit onderzoek geven daarbij inzicht in de randvoorwaarden en afhankelijkheden die een rol spelen met de nog niet beschikbare regelgeving zodat op een later moment, wanneer de totstandkoming van de lagere regelgeving verder gevorderd is, de daadwerkelijke (samenhangende) impact kan worden bepaald. Daardoor is het onderzoek ook een verkenning naar impact van de Wdo in bredere zin.

## 1.3. Vraagstelling

Deze analyse moet inzicht geven in de uitvoerbaarheid van bovenstaande onderdelen van de Wet digitale overheid, in de impact hiervan op de gemeentelijke organisatie en in de randvoorwaarden en

afhankelijkheden die daarbij van belang zijn. Tevens geeft het onderzoek aanbevelingen voor een implementatie van (onderdelen van) de nieuwe wet bij gemeenten.

De onderzoeksvragen voor deze analyse zijn:

- Wat wijzigt er in de werkwijze van de gemeente door de Wet digitale overheid?
- Wat betekenen deze veranderingen voor de gemeentelijke organisatie?
- Is de gemeente voldoende toegerust voor een doeltreffende uitvoering?
- Welke kosten en besparing voor de gemeentelijke uitvoering zijn aan deze wijziging van de wet verbonden?
- Wat zijn de verwachte effecten van de wet voor gemeenten?
- Hoe deze kunnen veranderingen worden geïmplementeerd en wat zijn de randvoorwaarden en risico's?

## 1.4. Aanpak & methodologie

In het najaar van 2020 is een plan van aanpak opgesteld voor dit onderzoek. Hierin worden onder andere de onderzoeksaanpak en scope toegelicht. Dit plan van aanpak is in januari 2021 met de begeleidingscommissie afgestemd en akkoord bevonden. De begeleidingscommissie bestaat uit vertegenwoordigers van het ministerie van BZK (als opdrachtgever) en vertegenwoordigers van VNG en VNG Realisatie.

In deze impactanalyse is een onafhankelijke en objectieve toets op de impact van de Wdo op gemeenten. Hiervoor is eerst de huidige situatie beschreven van de onderdelen van de gemeentelijke organisatie die door de onderzochte onderdelen van de Wdo geraakt worden. Vervolgens is een juridische analyse van de Wdo uitgevoerd van de betreffende onderdelen van de Wdo. Hierbij hebben is gebruik gemaakt van de kennis die binnen VNG Realisatie aanwezig is op deze onderdelen. Ook zijn er enkele verdiepende vragen gesteld aan betrokkenen bij BZK.

Vervolgens is in totaal met elf gemeenten en gemeentelijke samenwerkingsverbanden over de verschillende onderdelen van de Wdo gesproken. In eerste instantie is er gesproken met een groep gemeenten die al wat dieper in de materie was ingewerkt, om ons eigen beeld nog te toetsen en aan te scherpen. Vervolgens hebben is er voor de tweede groep gemeenten een selectie gemaakt, waarbij rekening is gehouden met een goede afspiegeling in grootte en spreiding in het land. Er is bij deze gemeenten gesproken met medewerkers publieke dienstverlening, informatiemanagers, architecten, privacy-adviseurs en informatiebeveiligers.

De informatie, eerste conclusies en aanbevelingen die uit deze gesprekken zijn vervolgens weer bij de gesprekspartners geverifieerd in een gezamenlijke klankbordsessie. Aan de hand van deze validatie is de conceptrapportage opgesteld en voorgelegd aan de begeleidingscommissie. Na bespreking van dit concept is deze eindrapportage opgesteld.

## 1.5. Leeswijzer

Hoofdstuk 2 beschrijft de verplichtingen die op gemeenten afkomen door de onderdelen van de Wdo die in de analyse centraal staan en de veranderingen die deze wetsonderdelen met zich meebrengen voor gemeenten.

Hoofdstuk 3 beschrijft de uitvoerbaarheid van deze onderdelen en de impact die zij hebben op de gemeentelijke organisatie op hoofdlijnen.

Hoofdstuk 4 beschrijft kort de (mogelijke) financiële consequenties van de onderzochte onderdelen van de Wdo aan de hand van de verschillende kostencomponenten.

In hoofdstuk 5 tot slot zijn de conclusies en aanbevelingen opgenomen en worden de antwoorden op de onderzoeksvragen gegeven.

# 2. Wet digitale overheid

Dit hoofdstuk kijkt naar de veranderingen die de onderdelen van de Wdo, die in deze analyse centraal staan, met zich meebrengen voor gemeenten. Allereerst wordt de Wet digitale overheid in een algemeen overzicht beschreven. De tweede paragraaf geeft inzicht in de relevante ontwikkelingen op gebied van wetgeving en normen die een relatie hebben met de Wdo. Daarna wordt voor de onderwerpen uit de Wdo, die in scope zijn, een schets van de huidige situatie gegeven. Tot slot beschrijft dit hoofdstuk concreet welke wijzigingen er op gemeenten afkomen door de onderzochte onderdelen van de wet.

## 2.1. De Wet digitale overheid nader uitgelegd

In deze paragraaf is op basis van de 7 w's (wat, wie, waarom, op welke wijze, wanneer en met welke middelen?) een beschrijving gemaakt van de Wet digitale overheid.

### *Wat?*

De Wet digitale overheid (Wdo) – voorheen Wet generieke digitale infrastructuur – vormt, in zijn huidige vorm, een eerste tranche van regelgeving ten behoeve van de verdere digitalisering van de overheid op verschillende niveaus[6]. De wet bevat, volgens de memorie van toelichting, de meest urgente onderwerpen van regelgeving voor de digitale overheid, te weten:

- de bevoegdheid om bepaalde (open) standaarden te verplichten in het elektronisch verkeer van de overheid;
- het stellen van regels over informatieveiligheid en het verwerken van persoonsgegevens;
- de verantwoordelijkheid voor het beheer van de voorzieningen en diensten binnen de generieke digitale overheidsinfrastructuur (GDI);
- regels voor de digitale toegang tot publieke dienstverlening voor inwoners (natuurlijke personen) en organisaties (rechtspersonen en ondernemingen).

De wet is op 18 februari 2020 door de Tweede Kamer aangenomen. Naar aanleiding van de vragen in de Eerste Kamer is onlangs besloten tot een wetswijziging, die de inwerkingtreding van de wet (opnieuw) zal vertragen[7]. De wet zelf is een zogeheten kaderwet: de wet regelt algemene principes, verantwoordelijkheden en procedures, maar bevat geen gedetailleerde regels. De uitwerking vindt plaats in lagere regelgeving, zoals in algemene maatregelen van bestuur (AMvB's) en ministeriële regelingen (MR's)[8].

### *Wie?*

Bij de Wet digitale overheid zijn verschillende partijen in uiteenlopende rollen betrokken. In de verschillende wetsartikelen wordt aangeven welke partijen door de bepaling in het artikel worden aangesproken. De minister van BZK is verantwoordelijk voor het beheer van de Generieke Digitale Infrastructuur. Logius is de uitvoerende organisatie onder aansturing van het ministerie van BZK. Logius is ontwikkelaar en beheerder van de publieke middelen en van de routeringsvoorziening Identity Bridge. Daarnaast is ook DICTU (ministerie van EZK) betrokken als ontwikkelaar van de routeringsvoorziening Toegangsverleningsservice (TVS).

[6] MvT Wdo
[7] https://www.rijksoverheid.nl/documenten/kamerstukken/2021/02/19/memorie-van-antwoord-bij-wetsvoorstel-digitale-overheid
[8] Een overzicht hiervan is te vinden in de bijlage bij de Kamerbrief over de Wdo van 13 mei 2020: https://www.rijksoverheid.nl/documenten/publicaties/2020/05/13/uitvoeringsregelgeving-onder-de-wet-digitale-overheid

De wet stelt regels voor de aanbieders van publieke digitale dienstverlening: bestuursorganen in de zin van de Algemene wet bestuursrecht (Awb), zoals gemeenten (en gemeentelijke samenwerkingsverbanden), uitvoeringsinstanties (UWB, SVB, Belastingdienst, DUO, RDW, etc.), aangewezen organisaties (de zorgsector, onderwijsinstellingen, pensioenfondsen) en de rechterlijke macht.

Ook stelt de wet regels voor private partijen, de zogenaamde 'erkende diensten': middelenuitgever, authenticatiedienst, ontsluitende dienst of machtigingsdienst. Deze diensten hebben een rol in de technische ontwikkeling en moeten daarbij voldoen aan de aan hen gestelde regels en voorwaarden om te worden toegelaten tot het stelsel als erkende dienst.

Tenslotte stelt de wet regels voor de inwoners en organisaties: om toegang te hebben tot de online diensten van publieke dienstverlening, moeten inwoners en organisaties middelen aanschaffen, in overeenstemming met het betrouwbaarheidsniveau van die dienstverlening.

*Waar?*
De Wdo heeft alleen betrekking op de Nederlandse digitale dienstverlening. Daarnaast op alle inwoners van Nederland met een BSN (voorwaarde om een DigiD te krijgen).

*Waarom?*
In het Regeerakkoord Vertrouwen in de toekomst (2017 – 2021) is aangegeven dat aanpassing aan de digitale samenleving van de overheid niet alleen noodzakelijk is, maar dat het ook mogelijkheden biedt voor een betere dienstverlening. Het demissionaire kabinet ontwikkelt daartoe een brede agenda voor de verdere digitalisering van het openbaar bestuur op verschillende niveaus. De Wdo past in die ambitie en legt de basis voor die verdere digitalisering, waaronder regulering van de digitale overheid en meer in het bijzonder de generieke digitale voorzieningen in een gemeenschappelijke infrastructuur van de overheid. In dit hoofddoel van verdere digitalisering van de overheid zijn een aantal andere uitgangspunten opgenomen, zoals regels voor het betrouwbaarheidsniveau van de inlogmiddelen die in de Europese verordening eIDAS zijn vastgelegd.

*Op welke wijze?*
De wet bakent de rollen en verantwoordelijkheden af van de verschillende partijen die bij deze wet betrokken zijn. Het stelsel van afspraken en regelgeving valt onder het beheer van de minister van BZK. Ook is BZK verantwoordelijk voor de technische ontwikkeling en het beheer van de generieke digitale infrastructuur, zoals het publieke inlogmiddel voor inwoners (DigiD), een machtigingsvoorziening en een routeringsvoorziening waarmee de publieke dienstverleners via één punt aansluiten op de verschillende inlogmiddelen. Daarnaast vindt een deel van de technische ontwikkeling plaats in de 'vrije markt'. In de markt zijn private voorzieningen beschikbaar, zoals inlogmiddelen of ontsluitende diensten. Deze kunnen door de minister van BZK worden toegelaten tot het stelsel, zodat ze een 'erkende dienst' worden. Toelating vindt plaats op basis van nader te stellen regels en standaarden.

Voor het inschalen van het betrouwbaarheidsniveau voor de digitale dienstverlening is de Regeling betrouwbaarheidsniveaus. Hierin zijn de regels opgenomen voor het bepalen van het betrouwbaarheidsniveau van authenticatie en machtiging voor een elektronische dienst en de communicatie hierover naar de inwoners. Voor de verplichting tot het accepteren van verschillende middelen worden bestuursorganen 'ontzorgd' door het ministerie van BZK, in de vorm van een routeringsvoorziening. Maar ze hebben ook de optie om voor een andere 'ontsluitende dienst' uit de markt te kiezen. Voor het onderdeel informatiebeveiliging op de toegang tot de elektronische

dienstverlening volgen publieke dienstverleners zo veel mogelijk de huidige systematiek (volgens de normen uit de BIO en ENSIA voor het afleggen van verantwoording). Dit geldt ook voor het toezicht op de acceptatieplicht en de inschaling van de betrouwbaarheidsniveaus van de dienstverlening.

*Wanneer?*

In artikel 29 zijn bepalingen voor de inwerkingtreding van de wet en enkele afzonderlijke artikelen opgenomen. De Wdo treedt gefaseerd in werking; het definitieve tijdspad is nog niet bekend. De datum van inwerkingtreding is al enige malen opgeschoven, onder andere door vertraging in het besluitvormend proces rondom de wet; zoals eerder is aangegeven is dit zeer recent opnieuw het geval geweest.

Ook is er een aantal technische afhankelijkheden waardoor nog onduidelijk is wanneer de wet ook daadwerkelijk uitvoerbaar wordt. De departementen en de publieke dienstverleners stellen hiervoor in samenwerking met het ministerie van BZK een aansluitschema op. Dit schema bevat data waarop de acceptatieplicht voor bestuursorganen en aangewezen organisaties geldt.

Een belangrijk onderdeel hierbij is de acceptatieplicht van verschillende middelen via een routeringsvoorziening/ontsluitende dienst. In artikel 29 van de Wdo staat aangegeven dat artikel 7 en 15 pas in werking treden als kan worden aangesloten op de voorzieningen waar de minister van BZK verantwoordelijk is (artikel 5) en het bijbehorende aansluitschema bekend is. Hier is dus naast de inwerkingtreding van de wet zelf ook de beschikbaarheid van voorzieningen een afhankelijkheid.

Een ander belangrijk onderdeel is het toepassen van het juiste betrouwbaarheidsniveau. Dit is afhankelijk van de beschikbaarheid van identificatiemiddelen op de betrouwbaarheidsniveaus substantieel en hoog, en van de mogelijkheid deze te gebruiken om toegang te krijgen tot publieke dienstverlening. Als deze middelen niet op juiste niveau beschikbaar of te gebruiken zijn, is het gebruik van een toegelaten of erkend middel op betrouwbaarheidsniveau substantieel respectievelijk een middel op niveau laag toegestaan, tot twee jaar na inwerkingtreding van de Regeling betrouwbaarheidsniveaus.

*Met welke middelen?*

In artikel 20, 21 en 22 van de Wdo zijn financiële bepalingen opgenomen. Deze zouden in een ministeriële regeling over de bekostiging nader worden uitgewerkt. Deze regeling was ten tijde van dit onderzoek nog niet beschikbaar en op dit moment is onduidelijk of deze er nog wel komt. Indien deze er niet komt zullen in elk geval op een andere wijze afspraken over de kosten moeten worden gemaakt. Op hoofdlijnen staat in de artikelen uit de kaderwet het volgende aangegeven:

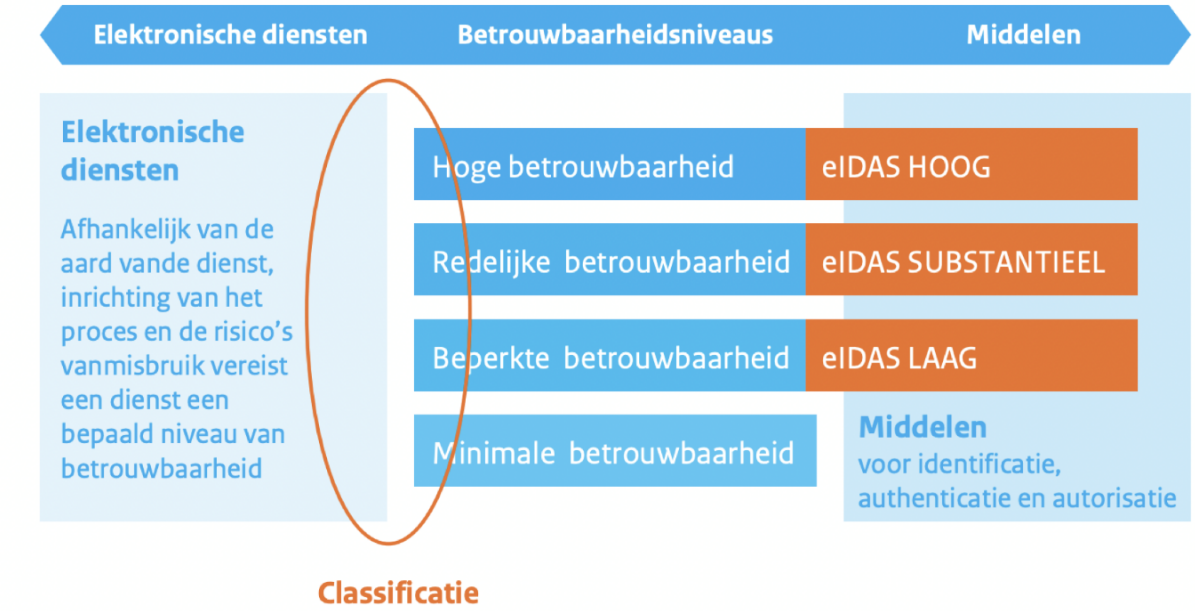
- De kosten die gemaakt worden voor het publieke middel, zullen ten laste komen van de gebruiker (artikel 20). De bedoeling is dat inwoners betalen via leges op het rijbewijs of Nationale Identiteitskaart voor hun publieke middelen. Ook private middelen zullen (naar verwachting) tegen kosten aan inwoners worden aangeboden, maar dat speelt zich ‘in de markt’ af.
- De kosten die gemaakt worden voor de inrichting en het beheer van de GDI (artikel 5) en het toelaten van middelen en diensten (artikel 9) worden doorberekend aan de dienstverleners, waaronder gemeenten (artikel 21). De bedoeling is dat de dienstverleners betalen voor de aansluiting, via een routeringsvoorziening. Daarnaast betalen dienstverleners voor het gebruik van een middel naar rato van gebruik.
- Aan het erkennen van middelen en diensten en het toezicht houden hierop worden ook kosten verbonden aan de hand van vastgestelde tarieven voor de aanvrager (artikel 22).

## 2.2. Samenhangende regelgeving en ontwikkelingen

Er zijn een aantal Europese verordeningen, nationale wetten en kaders die raken aan de Wdo. Hieronder volgt een korte toelichting op de meest relevante juridische kaders.

*eIDAS-verordening*

Met eIDAS hebben de Europese lidstaten afspraken gemaakt om dezelfde begrippen, betrouwbaarheidsniveaus en onderlinge digitale infrastructuur te gebruiken. eIDAS staat voor 'Electronic Identities And Trust Services'. Een onderdeel van de verordening is het grensoverschrijdend gebruik van Europees erkende inlogmiddelen. Maar in de eIDAS-verordening zijn ook de mogelijke betrouwbaarheidsniveaus voor inlogmiddelen vastgelegd. Binnen dit wettelijke kader zijn drie verschillende niveaus te onderscheiden: laag, substantieel en hoog. De eIDAS-verordening verplicht organisaties om een inlogmiddel te hanteren voor toegang tot een elektronische dienst dat past bij het betrouwbaarheidsniveau van die dienst. Deze niveaus worden ook in de Wdo toegepast. Onderstaand figuur 1 geeft aan welke eIDAS-middelen passen bij de verschillende betrouwbaarheidsniveaus.[9]




*Figuur 1 eIDAS-middelen bij de verschillende betrouwbaarheidsniveaus.*

*Single Digital Gateway*

De Single Digital Gateway (SDG) is de Europese toegangspoort die Europeanen toegang gaat geven tot informatie en procedures. Een aantal diensten moet volledig digitaal beschikbaar worden gesteld voor grensoverschrijdend verkeer binnen de EU. Ook de SDG is een Europese verordening die onderdeel uitmaakt van een verdere digitaliseringsslag binnen de overheid.

*Algemene Verordening Gegevensbescherming (AVG)*

Vanuit de Algemene Verordening Gegevensbescherming is voor het gebruik maken van het Burgerservicenummer (BSN) en sommige andere gegevens een wettelijke grondslag nodig. De Wdo

[9] https://www.gemmaonline.nl/images/gemmaonline/7/75/GEMMA_Gegevenslandschap_-_Autorisatie_en_authenticatie_v1_0.pdf

biedt deze wettelijke grondslag, ook aan private partijen die gegevens nodig hebben als erkende dienst voor de publieke elektronische dienstverlening.

*Wet modernisering elektronisch bestuurlijk verkeer*
In 2022 zal de Wet modernisering elektronisch bestuurlijk verkeer in werking treden. Het wetsvoorstel geeft de burger recht om elektronisch berichten aan een bestuursorgaan te zenden op een door het bestuursorgaan bepaalde wijze.

*Algemene wet bestuursrecht (Awb)*
De Algemene wet bestuursrecht (Awb) vereist dat elektronisch verkeer tussen burger en bestuursorgaan 'voldoende betrouwbaar en vertrouwelijk' verloopt en dat eenieder zich moet kunnen laten bijstaan of vertegenwoordigen.

*Paspoortwet*
De paspoortwet is gewijzigd, omdat per 4 januari 2021 in de chip van de Nationale identiteitskaart e(NIK) een applet is opgenomen die kan worden gebruikt voor het inloggen via DigiD hoog.

*Wegenverkeerswet*
De wegenverkeerswet wordt volgens Artikel 27 uit de Wdo aangepast voor het gebruik van het eID (publiek identificatiemiddel) op het rijbewijs. Sinds de eerste helft van 2018 is op rijbewijzen een publiek identificatiemiddel geplaatst.

*Wet Revitalisering Generiek Toezicht*
Het interbestuurlijk toezicht, het toezicht tussen gemeenten en provincies, is geregeld in de Wet Revitalisering Generiek Toezicht. Gemeenten hebben te maken met een toezichthouder per beleidsdomein. De provincie is de toezichthouder voor ruimtelijke ordening, bouwen, milieu, huisvesting, monumenten, archieven (overheidsinformatie) en constructieve veiligheid van bouwwerken. Het Rijk blijft toezichthouder voor de gemeenten op die terreinen, waar provincies geen taak en expertise hebben. Dit geldt bijvoorbeeld voor onderwijswetten en sociale zaken.

*Baseline Informatiebeveiliging Overheid (BIO)*
Vanaf 1 januari 2020 is de Baseline Informatiebeveiliging Overheid (BIO) van kracht. De BIO vervangt de bestaande baselines informatieveiligheid voor Gemeenten, Rijk, Waterschappen en Provincies. Van BIG, BIR, BIR2017, IBI en BIWA naar BIO. Hiermee is één gezamenlijk normenkader ontstaan voor informatiebeveiliging binnen de gehele overheid, gebaseerd op de internationaal erkende en actuele ISO-normatiek (ISO 27001/2). Vanuit de BIO worden eisen gesteld aan de inrichting van de toegang van gebruikers tot informatie en informatie verwerkende faciliteiten. Deze eisen worden ook binnen de Wdo toegepast bij het onderdeel informatiebeveiliging.

## 2.3. De huidige situatie bij gemeenten

Deze paragraaf kijkt naar de huidige situatie van de verschillende onderdelen die de Wet digitale overheid raakt en in scope zijn van dit onderzoek.

*Informatiebeveiliging van de toegang tot de elektronische dienstverlening*
Gemeenten moeten voor de informatiebeveiliging voor de bedrijfsvoering en primaire processen in algemene zin voldoen aan de Baseline Informatiebeveiliging Overheid (BIO). Verantwoording over de informatiebeveiliging wordt jaarlijks afgelegd via het verantwoordingsstelsel ENSIA. 'Uitgangspunt is

het horizontale verantwoordingsproces aan de gemeenteraad. Dit vormt de basis voor het verticale verantwoordingsproces aan nationale partijen die een rol hebben in het toezicht op informatieveiligheid. Bij het afleggen van verantwoording wordt het principe van single information single audit toegepast; alle informatie die noodzakelijk is voor verticale verantwoording is ook onderdeel van het horizontale verantwoordingsproces'[10].

Specifiek voor de toegang tot elektronische dienstverlening wordt jaarlijks het DigiD-zelfassessment uitgevoerd. Ook deze valt onder het ENSIA-stelsel. De DigiD-audit wordt door een onafhankelijk auditor gedaan. In het verticale verantwoordingsproces wordt verantwoording aan Logius afgelegd met betrekking tot de aansluiting op DigiD. Logius stelt de regels voor de beveiliging en gemeenten moeten aantoonbaar voldoen aan deze regels. In onderstaande figuur 2 is de verantwoordingswijze weergegeven (naast DigiD, wordt er ook voor andere voorzieningen verantwoording afgelegd aan toezichthouders van het Rijk; die zijn voor dit onderzoek buiten scope).[11]


*Figuur 2 Verantwoordingswijze gemeenten informatiebeveiliging*

### *Betrouwbaarheidsniveaus digitale diensten*

Op dit moment bepalen gemeenten de betrouwbaarheidsniveaus van hun digitale diensten op het moment van de overgang naar of uitbreiding van de online dienstverlening. Denk hierbij aan het inrichten van portalen of het inzetten van webformulieren. Een andere aanleiding is op het moment dat in het kader van informatiebeveiliging een risicoanalyse wordt gemaakt en bij de dataclassificatie een inschaling wordt gegeven voor het betrouwbaarheidsniveau.

### *DigiD als inlogmiddel voor inwoners*

Inwoners gebruiken DigiD als ze gebruik willen maken van de digitale dienstverlening van gemeenten. Gemeenten mogen DigiD gebruiken omdat zij een publieke taak uitvoeren en in hun administratie gebruik mogen maken van het BSN. Met DigiD kun je uitsluitend gebruik maken van publieke dienstverlening, niet van private diensten zoals online winkelen. Ongeveer 14 miljoen Nederlanders gebruiken DigiD. Logius is verantwoordelijk voor de ontwikkeling en het beheer van dit middel. DigiD is beschikbaar in de betrouwbaarheidsniveau *Basis*, *Midden, Substantieel en Hoog.*

- DigiD Basis: de gebruiker logt in met een gebruikersnaam en wachtwoord.
- DigiD Midden: dit is een tweefactorauthenticatie. De gebruiker kiest voor inloggen met de DigiD app of voor gebruikersnaam/wachtwoord aangevuld met een sms-controle. De DigiD app heeft tweefactorauthenticatie.

[10] https://www.ensia.nl/#!/

[11] https://www.vngrealisatie.nl/ensia

- DigiD Substantieel: dit is een toevoeging van een eenmalige ID-check. Gebruikers kunnen met de DigiD-app een eenmalige ID-check van een rijbewijs of identiteitskaart toevoegen. Hierna is de DigiD-app geschikt om in te loggen op betrouwbaarheidsniveau Substantieel.
- DigiD Hoog: een structurele combinatie van uitlezen van een chip op een identiteitsbewijs (vanaf 4 januari 2021 via de eNIK, bij inwerkingtreding van Wdo ook het rijbewijs) met de DigiD app voor het hoogste niveau van betrouwbaarheid

Op dit moment wordt alle gemeentelijke onlinedienstverlening op niveau Basis of Midden aangeboden. Dit komt overeen met het eIDAS-betrouwbaarheidsniveau Laag, dat ten minste uitgaat van tweefactor authenticatie. Daarmee voldoet het niveau DigiD Basis niet aan het eIDAS Laag niveau en zal dit na inwerkingtreding van de Wet digitale overheid uitgefaseerd worden. Het streven is om ook het gebruik van DigiD tweefactor authenticatie met sms-authenticatie zoveel mogelijk te gaan uitfaseren. Op termijn zal het minimaal vereiste niveau de DigiD tweefactorauthenticatie met app zijn, of een vergelijkbare private oplossing.

Voor DigiD Substantieel is een pilot opgestart om het 'activeren aan de balie' te onderzoeken. Zo kunnen inwoners bij de gemeentebalie worden geholpen door de baliemedewerker met het scannen van hun ID-bewijs om DigiD Substantieel te activeren. De praktijkbeproeving wordt in opdracht van het ministerie van BZK uitgevoerd, is in voorbereiding en start in het tweede kwartaal van 2021. Hierbij zijn 5 gemeenten betrokken en VNG Realisatie zal een impactanalyse uitvoeren op dit proces.

### *DigiD machtigen*

Organisaties met een aansluiting op DigiD, kunnen ook aansluiten op DigiD Machtigen. Met DigiD Machtigen kunnen inwoners die gebruik maken van gemeentelijke digitale diensten, iemand vrijwillig machtigen. Deze persoon, die namens hen optreedt, is bijvoorbeeld een familielid, een zorgverlener of een belastingadviseur.

DigiD Machtigen is een voorziening die al langer beschikbaar is voor het registreren van vrijwillige machtigingen voor digitale dienstverlening, maar deze werkt nog niet optimaal. Al enige tijd vindt doorontwikkeling plaats naar een breder inzetbare machtigingsvoorziening. Doel is enerzijds om een gebruiksvriendelijkere voorziening te ontwikkelen die meer toekomstbestendig is dan de huidige voorziening. Daarnaast moet het mogelijk worden dat ook wettelijk vertegenwoordigers (zoals ouders, bewindvoerders, curators) lang digitale weg zaken kunnen doen voor de personen die zij vertegenwoordigen. Hiervoor is het nodig om informatie uit het curatele- en bewindregister, de BRP en het ouderlijkgezagregister te kunnen ontsluiten. Aan deze oplossing wordt nu gewerkt [12]. Tenslotte is digitaal machtigen op dit moment alleen op een laag betrouwbaarheidsniveau mogelijk en dat sluit in sommige gevallen niet aan bij het betrouwbaarheidsniveau van de dienstverlening. In toekomst moet niet alleen het inloggen op een hoger betrouwbaarheidsniveau mogelijk zijn, maar ook het machtigingsproces zelf. Indien er voldoende risico-verlagende maatregelen worden getroffen, is ook een naastgelegen lager betrouwbaarheidsniveau toegestaan.

Op dit moment is niet duidelijk wat de planning voor de doorontwikkeling is en wanneer de voorziening voldoet aan bovenstaande doelstellingen. Ook zal er een aanvullende regeling nodig zijn om het gebruik van de machtigingsvoorziening (met name op het gebied van gegevensuitwisseling) uit te werken, naar verwachting wordt dit later nog uitgewerkt in het Besluit machtigen.

[12] https://www.vngrealisatie.nl/producten/digitaal-machtigen

*eHerkenning als inlogmiddel voor organisaties*

Waar inwoners DigiD gebruiken in het contact met de overheid, gebruiken organisaties een eHerkenning middel. Ook eHerkenning is persoonsgebonden en mag niet worden overgedragen of gedeeld. Iedereen binnen een organisatie die wil inloggen met eHerkenning, moet beschikken over een persoonsgebonden eHerkenningsmiddel met machtiging. eHerkenning is een publiek-private samenwerking, dat onderdeel is van het eID-stelsel. Er bestaan verschillende eHerkenningsmiddelen, dit zijn allemaal private middelen. Er zijn op dit moment zes leveranciers erkend door de Rijksoverheid om eHerkenning als inlogmiddel te mogen leveren. Daarnaast zijn er eHerkenningsmakelaars die gemeenten helpen bij de aansluiting op eHerkenning, op dit moment zijn vijf makelaars erkend door de Rijksoverheid. eHerkenningsmiddelen worden op verschillende betrouwbaarheidsniveaus uitgegeven. Deze niveaus zijn *EH1*, *EH2*, *EH2+, EH3* en *EH4*. Overigens maken niet alle gemeenten gebruik van een eHerkenningsmakelaar omdat ze op dit moment niet allemaal digitale dienstverlening aan organisaties aanbieden.

Gemeenten zijn naast dienstverlener, zelf ook gebruiker van eHerkenning. Gemeentelijke medewerkers kunnen voor de uitvoering van hun taak gebruik maken van elektronische (web)diensten van andere organisaties. Op het moment dat een gemeentelijke medewerker een dergelijke dienst van een andere organisatie wil gebruiken, bijvoorbeeld een inzageportaal van een keten- of netwerkpartij, is de afspraak binnen de overheid dat deze medewerker daarvoor een eHerkenningsmiddel gebruikt. Het betrouwbaarheidsniveau van het eHerkenningsmiddel dat gebruikt wordt voor het afnemen van de dienst is afhankelijk van het betrouwbaarheidsniveau dat door de dienstverlener aan de dienst is toegekend.

## 2.4. De toekomstige situatie: wat wijzigt er voor gemeenten?

Op basis van de huidige situatie en de veranderingen die de Wdo met zich meebrengt, beschrijft deze paragraaf wat er wijzigt voor gemeenten. Hieronder wordt ingegaan op de verplichtingen die op hoofdlijnen gelden voor gemeenten na inwerkingtreding van de onderzochte wetsonderdelen.

*De informatiebeveiliging van de toegang tot de elektronische dienstverlening*

Artikel 4 gaat over informatiebeveiliging van de toegang (identificatie en authenticatie) van de elektronische dienstverlening. Artikel 16 over het verwerken van persoonsgegevens. Dit artikel geeft grondslagen voor de verwerking van persoonsgegevens in het authenticatieproces, waaronder het BSN. Gegevensverwerking in het kader van de gemeentelijke elektronische dienstverlening als zodanig wordt niet onder dit lid begrepen. In het Besluit digitale overheid worden beide onderdelen nader uitgewerkt.

Gemeenten zijn straks verplicht om maatregelen te nemen op de informatiebeveiliging van de toegang tot de digitale dienstverlening. Deze verplichtingen zijn er nu ook voor het huidige inlogmiddel DigiD, met de Wdo wordt dit wettelijk vastgelegd voor de huidige en alle toekomstige inlogmiddelen. Toezicht hierop vindt plaats volgens de systematiek die vanuit de DigiD-assessment bekend is. Hiervoor moeten gemeenten middels een zelf-assessment en een verklaring van een onafhankelijke auditor verantwoording afleggen aan BZK. ‘Over het uitvoeren van de audits (proces, periodiciteit etc.) worden nadere regels gesteld, waarbij zoveel mogelijk zal worden aangesloten bij de door de dienstverleners in de desbetreffende sectoren reeds gehanteerde systemen en gebruiken’[13]. Deze regels zijn op dit moment nog niet tot in detail bekend. Het niet kunnen voldoen

[13] MvT Wet digitale overheid.

aan deze verplichting heeft gevolgen. Indien gemeenten niet aan de regels voldoen of dit niet kunnen aantonen middels een audit, heeft BZK de bevoegdheid ze af te sluiten (op basis van artikel 18).

In de Wdo is de scope van het Besluit digitale overheid niet helemaal eenduidig. Zo is het onduidelijk of de informatiebeveiligingsregels uit het besluit gaan over het onderdeel dat nu wordt afgedekt door de huidige DigiD-assessment en de audit hierop, of dat het gaat over een groter onderdeel van informatiebeveiliging en dat het daarmee deels de interne bedrijfsvoering van de gemeente raakt (informatiebeveiliging van de digitale diensten binnen een gemeente). Tijdens ons onderzoek is deze onduidelijkheid voorgelegd aan de juridische beleidsadviseur bij BZK. Samenvattend is het antwoord dat de reikwijdte van het Besluit digitale overheid de digitale toegang betreft, dat wil zeggen de verbinding(en) met de generieke digitale infrastructuur (GDI). BZK geeft daarbij aan dat met het Besluit digitale overheid sprake is van 'stroomlijning en codificering van bestaande informatiebeveiligingsnormering en richtlijnen; materieel gaan er niet of nauwelijks nieuwe verplichtingen gelden'.

Ondanks de toelichting is het nog lastig om de verandering goed vast te stellen. In het nieuwe stelsel dat de Wdo behelst, zullen er toch wijzigingen optreden die impact hebben op het onderdeel informatiebeveiliging. Zo zullen er naast (of in de plaats van) de huidige DigiD-aansluiting, andere aansluitingen met meerdere middelen zijn. Daardoor verandert mogelijk ook het stelsel van wie aan wie verantwoording af moet leggen over de toegang. Omdat de informatiebeveiliging aangepast moet worden aan het toekomstige (informatievoorzienings)stelsel dat nu nog niet helemaal uitgewerkt is, kan ook nog niet precies worden vastgesteld hoe dit onderdeel er straks uit gaat zien.

*Digitale diensten moeten worden ingedeeld naar betrouwbaarheidsniveaus*

In artikel 6 van de Wdo is deze bepaling opgenomen en deze wordt verder uitgewerkt in de Regeling betrouwbaarheidsniveaus[14]. Hierin zijn de regels opgenomen voor het bepalen van het betrouwbaarheidsniveau van authenticatie en machtiging voor een elektronische dienst en de communicatie hierover naar de inwoner.

Gemeenten zijn verplicht om hun aangeboden dienstverlening in te schalen op betrouwbaarheidsniveau. Op basis van deze inschaling wordt vastgesteld welk niveau van beveiliging het aan de dienstverlening gekoppelde inlogmiddel moet hebben. Dit geldt ook voor machtiging. Daar is een naastgelegen lager betrouwbaarheidsniveau toegestaan, indien er voldoende risico-verlagende maatregelen worden getroffen. Gemeenten moeten op de eigen website kenbaar maken welk betrouwbaarheidsniveau van authenticatie vereist is voor welke diensten.

De Wdo hanteert hiervoor de drie Europese eIDAS-betrouwbaarheidsniveaus Laag, Substantieel en Hoog. Het eIDAS-betrouwbaarheidsniveau Laag gaat uit van tenminste een tweefactor authenticatie. Op termijn vervalt DigiD Basis omdat deze geen tweefactor authenticatie heeft en vooruitlopend hierop vervalt per 1 juli 2021 eHerkenning niveau EH1. Gemeenten die digitale diensten aanbieden op EH1 moeten op korte termijn deze diensten aanbieden op minimaal EH2 en mogelijk EH2+ niveau.

Om betrouwbaarheidsniveaus van diensten vast te stellen en te borgen dat de gehanteerde inlogmiddelen passend zijn bij deze betrouwbaarheidsniveaus heeft VNG Realisatie eind 2019 met een aantal gemeenten een analyse van de gemeentelijke producten/diensten uitgevoerd. Het

[14] Regeling Betrouwbaarheidsniveaus versie na consultatie panel datum 15 december 2020

resultaat is een overzicht van betrouwbaarheidsniveaus[15] voor de gemeentelijke dienstverlening, dat gemeenten helpt bij het bepalen van het juiste betrouwbaarheidsniveau per product en/of dienst. Voor deze analyse is de Uniforme productnamenlijst (UPL) voor gemeenten van standaarden.overheid.nl als uitgangspunt genomen. De uitkomsten zijn getoetst en besproken met een aantal gemeenten, juristen en de Informatiebeveiligingsdienst (IBD). Daarbij is er ook een Handreiking machtigingsvoorziening beschikbaar met afwegingen voor een lager betrouwbaarheidsniveau voor registratie van vrijwillige machtiging[16].

### *Ontwikkeling DigiD Hoog*

Het DigiD-middel op betrouwbaarheidsniveau *Hoog* is vanaf begin 2021 beschikbaar. Om op DigiD Hoog over te kunnen gaan is er een speciale chip, een 'applet', nodig op het rijbewijs of de Nederlandse Identiteitskaart (NIK). Sinds eind 2014 zijn hiervoor door de RDW bijna 5 miljoen van deze *eRijbewijzen* uitgegeven. Vanwege het ontbreken van een juridische basis, zolang de Wet digitale overheid nog niet in werking is getreden, kunnen deze rijbewijzen hiervoor echter nog niet gebruikt worden. Sinds januari 2021 wordt hiervoor ook de *eNIK* uitgegeven. De wijziging van de Paspoortwet met bijbehorende uitvoeringsregelgeving is wel in werking getreden, waardoor de eNIK wel gebruikt kan worden. Na de introductie van de eNIK is echter gebleken dat er een onregelmatigheid optreedt in de werking van de chip van de identiteitskaart zodra de inlogfunctie wordt geactiveerd. De mogelijkheid tot activeren is daarom op 28 januari jl. tijdelijk stopgezet. Sinds 17 maart jl. worden de aangepaste kaarten uitgegeven waarbij dit verholpen is. Op dit moment zijn er echter nog geen diensten waarvoor DigiD hoog vereist is.

### *Er is een acceptatieplicht met betrekking tot toegelaten inlogmiddelen*

Met de Wdo worden naast DigiD ook private middelen voor inwoners toegestaan als inlogmiddel. Voor organisaties is dat met eHerkenning al het geval, het aansluiten hierop verloopt nu via eHerkenningsmakelaars. De Wdo schrijft in artikel 7 en 15 voor dat alle toegelaten authenticatiediensten dienen te worden ontsloten bij alle dienstverleners met interactie met inwoners en organisaties. Gemeenten zijn straks dus verplicht om alle publieke en alle erkende inlogmiddelen te accepteren.

Voor gemeenten geldt dat ze als bestuursorganen in principe ontzorgd worden door de minister die verantwoordelijk is voor de ontwikkeling van de routeringsvoorziening. Overigens wordt in de wet zelf gesproken van een 'voorziening' om identificatiemiddelen te ontsluiten (Artikel 5). In de MvT (blz. 21) wordt het de routeringsvoorziening genoemd, als generieke voorziening waar de minister van BZK verantwoordelijk voor is. Op dit moment is Logius bezig met de ontwikkeling van de Routeringsvoorziening[17] die in artikel 5 van de Wdo bedoeld wordt. De eerste versie van deze voorziening is in productie, maar biedt vooralsnog alleen de ontsluiting van DigiD en eIDAS (voor EU-inwoners met een BSN in Nederland). Het is onduidelijk wat de toekomstplannen voor de doorontwikkeling van deze routeringvoorziening zijn en wat de oplevertermijn hiervoor is. Het is ook niet duidelijk of in toekomst ook eHerkenning (al dan niet via eHerkenningsmakelaars) hieraan wordt toegevoegd.

Daarnaast kunnen gemeenten er ook voor kiezen om een leverancier te contracteren die onder verantwoordelijkheid van de gemeente zelf een routeringsvoorziening inricht of aanbiedt. Dit is dan

[15] https://www.vngrealisatie.nl/producten/betrouwbaarheidsniveaus-digitale-dienstverlening geraadpleegd op 6 februari 2021

[16] https://www.vngrealisatie.nl/sites/default/files/2020-10/20201002%20Handreiking%20bij%20machtigingsvoorziening%200.97.pdf, met in de bijlage Afwegingen lager betrouwbaarheidsniveau voor registratie vrijwillige machtiging

[17] https://www.logius.nl/diensten/routeringsvoorziening

een voorziening onder eigen beheer en verantwoordelijkheid. Een derde optie voor gemeenten die door VNG verkend wordt is of eHerkenningsmakelaars als routeringsvoorziening voor alle toegestane middelen en de machtigingsvoorziening kunnen fungeren. Vanuit de VNG zijn in het kort de voor- en nadelen[18] geduid van deze oplossing als input voor het beleidstraject. Voor organisaties in de zorg, zoals ziekenhuizen en apotheken, in nu al de ToegangsVerleningsService (TVS)[19] beschikbaar. Gemeenten kunnen hier (vooralsnog) niet op aansluiten.

Er is wel wat onduidelijkheid of de routeringsvoorziening van BZK zowel voor inlogmiddelen in het burgerdomein, als ook voor inlogmiddelen in het bedrijvendomein is. Want naast de routeringsvoorziening van BZK is er in de wet en MvT ook sprake van 'ontsluitende diensten'. De overeenkomst en het verschil tussen de routeringsvoorziening en ontsluitende diensten is onduidelijk. Naar aanleiding hiervan zij er ook hierover aanvullende vragen gesteld aan de juridische beleidsadviseur bij BZK. Ook na beantwoording blijven er onduidelijkheden bestaan, hieronder wordt aangegeven welke dat zijn.

Het ministerie geeft aan dat 'een ontsluitende dienst' gebruikt wordt in het bedrijvendomein. Dit is een private dienst die erkend moet worden. Een routeringsvoorziening is een publieke voorziening onder verantwoordelijkheid van de minister van BZK en wordt nu ingezet in het burgerdomein. Privaat ontsluitende diensten zijn nu bekend als eHerkenningsmakelaars, private partijen die de eHerkenningsmiddelen ontsluiten. In de Wdo is aangegeven dat private erkende ontsluitende diensten kunnen worden toegelaten tot het burgerdomein, als dit nodig is voor de continuïteit van de dienstverlening (artikel 9, lid 3). Aanvullend op de acceptatieplicht van alle inlogmiddelen, is in artikel 15 (acceptatie van bedrijfs- en organisatiemiddelen) aangegeven dat bestuursorganen en aangewezen organisaties in elk geval één van de erkende ontsluitende diensten accepteren. Dit betekent dat gemeenten in elk geval verplicht zijn om via een ontsluitende dienst aan te sluiten op de bedrijfsmiddelen (nu eHerkenningsmakelaar).

Daarnaast wordt ook in de MvT (blz. 40) de indruk gewekt dat de routeringsvoorziening alleen voor de burgermiddelen is, en de ontsluitende dienst voor de bedrijfsmiddelen: 'Voor rekening van de dienstverleners komen in de eerste plaats de kosten voor het aansluiten op de routeringsvoorziening in het geval dat sprake is van digitale dienstverlening (op betrouwbaarheidsniveau substantieel of hoog) aan inwoners. Indien sprake is van digitale dienstverlening aan organisaties zijn er kosten voor aansluiting op de ontsluitende dienst.' Dit betekent dat elke gemeente 1 routeringsvoorziening en 1 ontsluitende dienst zal moeten hebben om aan de acceptatieplicht te kunnen voldoen.

Samengevat maken deze verschillende onderdelen niet zonder meer duidelijk hoe de nieuwe situatie bij gemeenten er precies uit gaat zien.

### *Randvoorwaarden van de ontwikkeling en het beheer van stelsel onder de Wdo*

In een aantal artikelen van de Wdo zijn randvoorwaarden beschreven die gevolgen hebben voor gemeenten. Het gaat dan bijvoorbeeld om het beheer van de GDI door de minister van BZK (artikel 5), toezicht en handhaving (artikel 17), de bijzondere bevoegdheden van de minister van BZK (artikel 18), de onderlinge verplichting tot informatieverstrekking voor het waarborgen van veilige toegang (artikel 19) en de financiële bepalingen (artikel 20, 21 en 22).

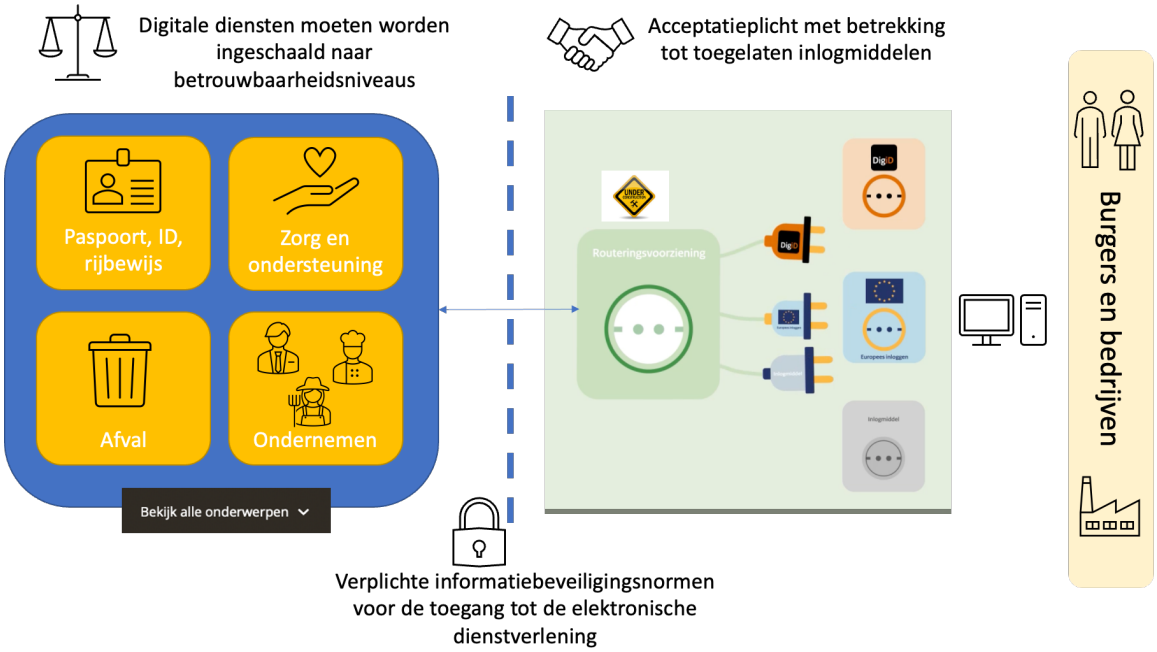
[18] https://www.vngrealisatie.nl/sites/default/files/2020-09/190225_Commerciele%20makelaars%20als%20routeringsvoorziening%20toegangsdiensten%20burger%20en%20bedrijven.pdf

[19] https://www.digitaleoverheid.nl/dossiers/tvs/

Binnen de Wdo is er daarnaast een groot aantal afhankelijkheden. Gemeenten moeten een aantal dingen zelf regelen, maar zijn ook afhankelijk van het beheer van BZK, keuzes die daarbij gemaakt worden en de technische realisatie van noodzakelijke onderdelen. BZK bepaalt welke erkende diensten volgens de regels worden toegelaten.

*Samenvattend: Wat wijzigt er voor gemeenten?*
In onderstaande figuur 4 is samenvattend weergegeven wat er wijzigt voor gemeenten:

- Er zijn verplichte informatiebeveiligingsnormen voor de toegang tot de elektronische dienstverlening;
- Digitale diensten moeten worden ingeschaald naar betrouwbaarheidsniveaus;
- Er is een acceptatieplicht met betrekking tot de toegelaten inlogmiddelen en voor de elektronische machtigingsverklaringen.




*Figuur 4 Samenvatting: Wat wijzigt er voor gemeenten?*

# 3. Impact Wdo voor gemeenten

Dit hoofdstuk gaat in op de impact die de onderzochte onderdelen van de Wdo hebben op de gemeentelijke uitvoeringspraktijk. Basis voor het bepalen van deze impact is de wijziging die de Wdo oplevert in de werkwijze van gemeenten. Vervolgens zijn in de gesprekken met de gemeenten deze veranderingen getoetst en de verschillende onderdelen van de uitvoeringsconsequentie besproken. Om een goede afspiegeling te krijgen is zowel rekening gehouden met de grootte en spreiding van gemeenten in het land en met de verschillende rollen van de gesprekspartners binnen de gemeenten. De bevindingen, eerste conclusies en aanbevelingen zijn geverifieerd in een klankbordsessie met de gesproken gemeenten. Voordat wordt ingegaan op de impact op de onderdelen informatiebeveiliging, betrouwbaarheidsniveaus en acceptatieplicht wordt eerst ingegaan op algemene bevindingen. Aan het eind van dit hoofdstuk komen ook de bredere randvoorwaarden en afhankelijkheden aan de orde.

## 3.1. Algemene bevindingen

Wat als eerste opvalt in deze analyse is dat de Wdo niet een makkelijke wet is om te overzien. Het gaat over veel verschillende onderdelen van het eID-stelsel die veelal in elkaar grijpen. Maar soms zijn er ook onderdelen die juist los lijken te staan van het geheel, zoals de standaarden en toegankelijkheid (beide overigens niet in scope bij dit onderzoek). Het is daarom niet makkelijk te overzien wat de samenhang van de losse onderdelen is en of daar bij het ingaan van de wet rekening mee is gehouden. In onderstaande paragrafen wordt specifieker ingegaan op de samenhang tussen onderdelen die nu veelal afzonderlijk worden aangepakt

Ook de inwerkingtreding roept vragen op. De inwerkingtreding is al meerdere malen uitgesteld, en het is nog niet duidelijk wanneer de wet zelf in werking treedt. Gemeenten geven aan dat ze wel vaker over deze onderwerpen gehoord hebben, maar eigenlijk niet goed weten wat nu wanneer verwacht wordt. Gemeenten geven hierbij ook aan dat het ‘niet te doen is’ om telkens bij te houden wat de status is, en horen het graag als duidelijk is wat wanneer verwacht wordt. Gemeenten moeten tijdens de gefaseerde inwerkingtreding van de verplichtingen uit de Wdo bovendien zorgen voor de continuïteit van de dienstverlening.

De wet is al lang in ontwikkeling en de informatievoorziening over de wet is op dit moment niet voldoende voor gemeenten om goed aangehaakt te blijven. Mede door de onduidelijkheid die is beschreven in bovenstaande punten en door de grote druk op gemeenten door invoering van andere wetgeving (rond informatievoorziening, het sociaal domein en de Omgevingswet) zijn er nog nauwelijks gemeenten gestart met de voorbereiding op de implementatie van de Wdo. Hieronder wordt de situatie specifieker bekeken op de afzonderlijke onderdelen.

## 3.2. De informatiebeveiliging van de toegang tot de elektronische dienstverlening

Gemeenten zijn straks verplicht om maatregelen te nemen op de informatiebeveiliging van de toegang tot de digitale dienstverlening en hierover verantwoording af te leggen. Zoals aangeven in paragraaf 2.4 bleek tijdens de analyse enige onduidelijkheid te zijn over de precieze invulling van dit onderdeel. Dit is ook in de gesprekken met gemeenten aan bod geweest. Ook gemeenten gaven aan dat ze nog niet helemaal goed konden inschatten wat de impact zou zijn. Met name omdat het stelsel waar het onderdeel informatiebeveiliging betrekking op heeft, nog niet duidelijk is vastgelegd.

*Impact monitoring en verantwoording informatiebeveiliging*

Gemeente moeten met de Wdo verantwoording afleggen over passende informatiebeveiligingsmaatregelen voor verbindingen met de Generiek Digitale Infrastructuur (GDI) die lopen via de beschikbare inlogmiddelen. Gemeenten leggen nu verantwoording af via de ENSIA-methodiek (in deze context: de DigiD-assessment), waarin de BIO-normen zijn verwerkt. Informatiebeveiliging, en de verantwoording hierover, is voor gemeenten een belangrijk thema. Als voor het onderdeel informatiebeveiliging op de toegang tot de elektronische dienstverlening de huidige systematiek (volgens de normen uit de BIO en ENSIA) voor het afleggen van verantwoording passend is bij de toekomstige beoogde door de WDO, levert de verplichting een beperkte extra lastendruk. De extra lastendruk zit dan in de extra inlogmiddelen waarover informatiebeveiligingsverantwoording moet worden afgelegd. Gemeenten gaan er daarbij vanuit dat relevante informatie kan worden hergebruikt. Nog onduidelijk is wat de invloed op de inhoud van de audit is in het geval van aansluiten via de routeringsvoorziening of rechtstreeks via een eigen opdracht aan een marktpartij.

Uit deze analyse komt verder naar voren dat in de huidige zelf-assessment op de DigiD-aansluiting (met check door externe auditor) deels dubbel werk zit, omdat normen die al in het 'algemene' deel aan bod komen hier ook nog eens gevraagd worden. In de audit die met de Wdo op de toegang tot digitale dienstverlening wordt uitgevoerd, zou op dit onderdeel kritisch moeten worden toegezien. Uitgangspunt moet hier ook zijn om geen dubbele informatie aan te leveren.

*Logging*

Teneinde onbevoegde informatieverwerking en systeemtechnische fouten bij de toegang tot digitale dienstverlening te kunnen ontdekken, maken gemeentelijke ICT-voorzieningen gebruik van logbestanden. De logbestanden betreffen o.a. de uitgevoerde authenticaties, de daarbij gebruikte identificatiemiddelen, de tijdstippen waarop is ingelogd en uitgelogd, de systeemtechnische gegevens, waaronder het IP-adres en, indien van toepassing, machtigingsgegevens. Het Besluit Digitale overheid wijzigt het Besluit verwerking persoonsgegevens generieke digitale infrastructuur. In dit laatste besluit staan al passages opgenomen over bewaartermijn van persoonsgegevens van inlogmiddelen. Artikel 23 van het besluit Digitale overheid voegt hieraan toe dat ook de betreffende logbestanden van ICT-systemen 5 jaar bewaard moeten worden. Dit is om de traceerbaarheid door de keten heen te borgen. De IBD heeft voor gemeenten een handreiking Logging[20] opgesteld, waarin volgens de dataclassificatiesystematiek de bewaartermijnen zijn bepaald. Hier worden de bewaartermijnen van een log bepaald door de verschillende eisen voor integriteit en vertrouwelijkheid van gegevens. Deze bewaartermijnen kunnen door deze systematiek afwijken van de bewaartermijn van maximaal 5 jaar die in de wet is opgenomen. Gemeenten hebben hier mogelijk een extra inspanning door het technisch aanpassen van de bewaartermijnen in de logging.

## 3.3. Digitale diensten moeten worden ingeschaald naar betrouwbaarheidsniveaus

Gemeenten zijn verplicht om hun dienstverlening in te schalen op betrouwbaarheidsniveau. Op dit onderdeel hebben gemeenten het meeste concrete beeld bij wat er moet gebeuren; enkele gemeenten hebben al actie ondernomen. Deze gemeenten geven aan dat zij al aan de slag zijn

[20] https://www.informatiebeveiligingsdienst.nl/kennisproducten-ibd/

gegaan met het goed in kaart brengen van de digitale processen en actuele proceseigenaren of al zijn begonnen met het indelen van de processen op het juiste betrouwbaarheidsniveau.

### *Inschaling van digitale dienstverlening*

Gemeenten verschillen in de mate waarop ze digitale dienstverlening aanbieden. Uit de gesprekken blijkt dat voor de grote steden dit kan oplopen naar ongeveer 400-600 producten voor inwoners en organisaties. Bij kleine gemeenten gaat het om tientallen. Op dit moment wordt alle gemeentelijke online dienstverlening op niveau Laag aangeboden (DigiD Laag of Midden: beiden vallen onder eIDAS Laag)[21]. Totaal zijn 309 van de 355 gemeenten aangesloten op eHerkenning, het gebruikte betrouwbaarheidsniveau is heel divers[22]. Een deel van de gemeenten zit nog op eH1, maar enkele gemeenten zijn al actief aan de slag om eHerkenning 1 uit te faseren of hebben dit al gedaan.

De belangrijkste impact zit in het herzien van de digitale dienstverlening. Allereerst moeten gemeenten de onlinediensten in beeld brengen en nagaan welke gegevens daarbij verwerkt worden. Daarvoor moeten processen opnieuw beoordeeld worden. Per dienst zal de afweging gemaakt worden of voor deze dienst authenticatie noodzakelijk en wenselijk is. Voor de diensten waarvoor dit het geval is, moet er vervolgens een risicoafweging worden gemaakt voor het bepalen van de betrouwbaarheidsniveaus van de onlinedienstverlening, zeker als het gaat om medische en inkomensgegevens. Een aantal gemeenten geeft aan dat een hoger betrouwbaarheidsniveau ook verwachtingen schept bij de gebruikers, dat de gemeente geen informatie vraagt die al binnen de systemen beschikbaar is. Om dit de realiseren zal ook een slag op procesoptimalisatie moeten worden uitgevoerd bij gemeenten. Gemeenten geven aan dat machtigen ook een belangrijke rol speelt bij de digitale dienstverlening en het inschalen van betrouwbaarheidsniveaus. Paragraaf 3.5 gaat hier verder op in.

### *De impact voor gemeenten*

De meeste impact is eenmalig voor het bepalen van de betrouwbaarheidsniveaus. Als de informatiehuishouding op orde is, kan binnen een project met de betrokkenen per digitaal proces het betrouwbaarheidsniveau worden afgestemd en kunnen de relevante personen binnen de gemeente worden geïnformeerd. Hier zijn veel verschillende rollen bij betrokken: proceseigenaren, CISO, FG en dienstverlening. Binnen de geïnterviewde gemeenten is hier nog nauwelijks ervaring mee opgedaan en is er nog geen goed zicht op de te zetten stappen. Hierdoor is het op dit moment nog niet mogelijk om deze impact te ramen. De verwachting is dat de tijd en capaciteit die het kost om de dienstverlening op het juiste niveau in te schalen vooral gerelateerd is aan het aanbod van onlinedienstverlening. Dit zal dus ook verschillen per gemeente.

Qua techniek is het omzetten van de betrouwbaarheidsniveaus van de dienstverlening goed te doen. Voor eHerkenning geldt dat een aantal gemeenten en de softwareleveranciers al de aanpassing naar niveau 2 van eHerkenning hebben gemaakt. Uiteraard moeten hier wel middelen voor vrijgemaakt worden. Gemeenten leggen nu de wijze van inloggen nergens vast, omdat ze maar één betrouwbaarheidsniveau hebben. Met meerdere betrouwbaarheidsniveaus wordt het loggen van de inlogactiviteiten daarom mogelijk een aanpassing in ICT, omdat gemeenten het niveau van inloggen moeten gaan vastleggen. Ook hier zijn enige kosten mee gemoeid.

[21] https://www.vngrealisatie.nl/producten/digid

[22] https://www.eherkenning.nl/aansluiten-op-eherkenning/aangesloten-organisaties

Ook structureel is er een impact. Voor het structureel beheer van de betrouwbaarheidsniveaus is het nodig deze onderdeel uit te laten maken van het reguliere proces, bijvoorbeeld aansluitend bij het dataclassificatieproces. Hiervoor zijn ook aanpassingen van de werkinstructies voor medewerkers nodig. De extra tijdsinspanning hiervoor is op dit moment niet te bepalen.

### *Communicatie aan inwoners en organisaties*

Allereerst zullen gemeenten bij hun digitale diensten teksten moeten toevoegen over het verplichte betrouwbaarheidsniveau. Zeker bij gemeenten met een Single Sign On (SSO) of een portaal is goede communicatie belangrijk. Hoewel de verwachting is dat de communicatie over betrouwbaarheidsniveaus landelijk wordt uitgevoerd en pas gaat gebeuren als de geschikte inlogmiddelen beschikbaar zijn, zullen de vragen van inwoners en organisaties over het aanvragen en gebruiken van de nieuwe middelen bij de gemeente terecht komen. De verwachting is dat dit voor organisaties minder ingewikkeld zal zijn. Gemeenten geven aan dat ze zich wel zorgen maken of de bedachte oplossingen wel aansluiten bij de wensen en beleving van de inwoner. Het voorbeeld dat wordt gegeven is van de nieuwe eNIK die per 4 januari wordt uitgegeven. Ze krijgen soms vragen van inwoners (wat kan ik ermee? hoe werkt het? en hoe zit het met de kosten?), maar de toepassing voor de inwoner is nu nog minimaal. De verwachting is dat inwoners meer bij gemeenten aan gaan kloppen voor vragen bij grote veranderingen rondom het inloggen. Een gevolg kan zijn dat ze meer capaciteit bij het Klant Contact Centrum (KCC) moeten inrichten om inwoners bij te staan, terwijl in veel gevallen het antwoord moet komen van de (private) partij die het inlogmiddel heeft uitgegeven. In eerdere analyses m.b.t. inlogmiddelen werd deze impact ook geconstateerd.

### *Impact op de digitale dienstverlening aan inwoners*

De inschaling heeft ook gevolgen voor de digitale dienstverlening aan inwoners en organisaties. Inwoners moeten zich voorbereiden op het gebruik van een ander middel met in veel gevallen een hoger betrouwbaarheidsniveau dan ze gewend zijn. Naast de risicoafweging op het gebruik van persoonsgegevens zoals via de Regeling betrouwbaarheidsniveaus wordt opgelegd, maken gemeenten ook afwegingen in wat het betekent voor de dienstverlening aan inwoners. Gemeenten zijn zich ervan bewust dat een hoger betrouwbaarheidsniveau ook hogere drempels kan opwerpen voor de inwoners, met name voor dienstverlening in het sociaal domein. Dit zou betekenen dat sommige inwoners minder goed gebruik kunnen maken van de digitale dienstverlening en (meer) afhankelijk worden van dan wel dienstverlening op locatie of machtigingen.

Sommige gemeenten hebben Single Sign On (SSO) voor DigiD. Daarmee kunnen inwoners direct naar gelijksoortige betrouwbaarheidsniveau dienstverlening, mits de sessie het toelaat. Andere gemeenten hebben een portaalfunctie waarin je een overzicht hebt van al je ‘zaken’. Tenslotte hebben veel gemeenten ‘losse formulieren’, waarbij digitale processen afzonderlijk doorlopen moeten worden. Gemeenten vragen zich af hoe het in praktijk werkt met SSO en een portaalfunctie. Moet je altijd op hoogste niveau inloggen zodat je zeker weet dat je alle diensten kunt doorlopen? Of moet je meerdere keren inloggen afhankelijk van niveau? Of moet je duidelijk communiceren wat met welk inlogniveau wel en niet kan? Dit heeft impact op de inwoners en gemeenten zullen dit nog nader moeten uitwerken. De gesproken gemeenten hebben hier nog geen keuzes in gemaakt.

### *Veilige digitale dienstverlening*

In de Memorie van Toelichting op de wet is aangegeven dat dienstverleners baten genereren door het gebruik van een generieke, betrouwbare infrastructuur voor het digitaal inloggen. Zij kunnen hierdoor meer diensten aan inwoners of organisaties digitaal verlenen en door de hogere betrouwbaarheid van de inlogmethoden minder risico’s lopen. Uit de analyse blijkt dat gemeenten het belang van veilige en betrouwbare dienstverlening onderschrijven. Wel geven ze aan dat dit ook

in verhouding moet staan tot toegankelijke dienstverlening. Uit de analyse blijkt niet dat gemeenten door de hogere betrouwbaarheidsniveaus verwachten hierdoor diensten die ze nu niet digitaal aanbieden, straks wel digitaal kunnen aanbieden. Eerder nog is het omgekeerde het geval: door hogere drempels bij de digitale dienstverlening verwachten ze dat de vraag om analoge dienstverlening kan toenemen. Een aanzienlijke groep inwoners is niet digitaal vaardig en kan moeilijk of niet meekomen als het gaat om communicatie met de overheid[23]. Dit kan mogelijk ook tot uitvoeringsproblemen leiden, bijvoorbeeld omdat inwoners dan niet gemakkelijk en snel de informatie kunnen leveren die nodig is voor de uitvoering van de gemeentelijke taken.

*Impact op de digitale dienstverlening aan organisaties*

Door de meeste organisaties zal de drempel van een hoger betrouwbaarheidsniveau niet als problematisch worden ervaren. Van gemiddelde ondernemingen mag verwacht worden dat ze de nodige eHerkenningsmiddelen aanschaffen om zaken te doen. Wel zijn hierbij specifieke doelgroepen te onderscheiden voor wie dit anders is. Dit is lastiger voor zelfstandigen, stichtingen en verenigingen. De eerste categorie heeft een uitzondering gekregen en mag van DigiD gebruik blijven maken voor zakelijke dienstverlening. De laatste twee groepen zijn vaak organisaties bestaande uit vrijwilligers, die met gemeenten vooral van doen hebben voor het aanvragen van bijvoorbeeld subsidies, en dan nog vaak een enkele keer per jaar. Gemeenten geven aan dat het omslachtig voelt om hen kosten te laten maken voor het aanvragen van een inlogmiddel alleen hiervoor. Ze moeten zich inschrijven bij KvK en het middel beheren als vrijwilligersorganisatie. Het gaat om 40 à 50 euro per jaar. Voor bedrijven valt dit mee, maar voor verenigingen is dit nog best veel geld. Enkele gemeenten geven aan bij het inschalen van de dienstverlening aan dergelijke partijen hier rekening mee te gaan houden, dus zonder eHerkenning.

*Randvoorwaarde: informatiehuishouding gemeenten op orde*

Een belangrijke voorwaarde voor het inschalen van de betrouwbaarheidsniveaus is dat de informatiehuishouding op orde is: er moet overzicht zijn over alle digitale diensten, proceseigenaren, verantwoordelijken voor de dienstverlening, etc. Ook geven gemeenten aan dat de huidige processen nog geen onderscheid maken tussen bijvoorbeeld een aanvraag door een inwoners zelf of door een gemachtigde, terwijl dat wel nodig is voor de toekomstige dienstverlening.

Gemeenten geven aan dat een bijkomend effect van de risicoafweging in het bepalen van de betrouwbaarheidsniveaus is, om nog eens te kijken naar dataminimalisatie. Hierbij moeten proceseigenaren aangeven wat minimaal nodig is om de aanvraag in behandeling te nemen. Bij het verzamelen en verwerken van persoonsgegevens mogen niet meer gegevens worden gebruikt dan nodig is om het doel waarvoor ze gebruikt zullen worden, te bereiken. Soms is er een tegengesteld belang (meer data voor verantwoording, bijvoorbeeld) en wordt dataminimalisatie daarmee een moeilijke afweging.

Gemeenten zetten de continuïteit van de dienstverlening aan inwoners en organisaties bovenaan. Bij het implementeren van de juiste betrouwbaarheidsniveaus is het een belangrijke voorwaarde dat deze continuïteit gewaarborgd is.

[23] 20 tot 25% van de Nederlandse bevolking heeft moeite zonder hulp digitaal zaken te doen met de overheid. Dialogic (2013), De digitale (zelf)redzaamheid van de burger: ondersteuning bij de Digitale Overheid 2017.

*Technische voorzieningen voor onderdeel betrouwbaarheidsniveaus zijn nog niet klaar*
Verder is duidelijk dat een aantal voorzieningen randvoorwaardelijk zijn voor het toepassen van de betrouwbaarheidsniveaus. Voor de hand liggend is dat er publieke middelen op niveau substantieel en hoog beschikbaar moeten zijn. Op dit moment lopen er ontwikkelingen, pilots en onderzoeken op deze onderdelen. Sommige gemeenten zijn hierbij betrokken maar veel gemeenten zitten ook in de wachtstand hierop. Daarnaast kunnen sommige CMS-systemen van gemeenten het onderscheid in meerdere betrouwbaarheidsniveaus niet aan. In die systemen is er maar één niveau beschikbaar voor alle producten: laag, substantieel of hoog.

## 3.4. Er is een acceptatieplicht met betrekking tot toegelaten inlogmiddelen

Gemeenten zijn straks verplicht om naast DigiD ook andere burgermiddelen toe te laten. Dit geldt ook voor verschillende middelen voor organisaties, maar omdat dit nu al de praktijk is, wordt dit als minder ingrijpend ervaren. Gemeenten gaan hiervoor waarschijnlijk gebruik maken van een routeringsvoorziening om niet op alle middelen afzonderlijk aan te sluiten. Zoals eerder aangegeven was er tijdens de analyse onduidelijkheid over de begrippen routeringsvoorziening en ontsluitende diensten. Gemeenten hebben het, indien bekend met de wet, vooral over een routeringsvoorziening. Ze geven hierbij aan dat zij verwachten dat ook eHerkenning, eIDAS en machtigingen via deze voorziening lopen, en dat ze dus gebruik zullen maken van één centraal aansluitpunt. Omdat overeenkomst en onderscheid tussen routeringsvoorziening en ontsluitende dienst niet duidelijk was, en omdat gemeenten het begrip routeringsvoorziening hanteerden, is deze analyse in deze paragraaf daartoe beperkt.

Op dit moment zijn er nog geen private inlogmiddelen toegelaten en is de routeringsvoorziening van BZK nog in ontwikkeling en is planning onduidelijk. Hierdoor is de impactbepaling van de acceptatie van deze nieuwe middelen door gemeenten ook nog niet precies vast te stellen. In deze paragraaf wordt vooral ingegaan op randvoorwaarden, wensen en eisen voor de toegelaten inlogmiddelen en routeringsvoorziening zoals in de analyse naar voren is gekomen.

*Dienstverlening en communicatie*
Gemeenten vrezen dat inwoners straks door de bomen het bos niet meer zien, wanneer er naast DigiD verschillende inlogmiddelen beschikbaar komen. Voorbeelden van middelen die nu al beschikbaar zijn, zijn ITSme, IRMA en IDin. Gemeenten verwachten dat er (onbedoeld) wel meer taken op ze afkomen in de communicatie hierover, omdat inwoners bij onduidelijkheden of problemen eerder contact op zullen nemen met de dienstverlenende instantie dan met de partij die het inlogmiddel voor dienstverlening levert – hoewel dat dan de juiste route is.

Het toelaten van meerdere middelen en de keuze die met name inwoners hier straks in hebben, kunnen een rol spelen in de bredere wens voor ‘meer regie op gegevens’. De inwoner kan dan zelf kiezen voor het middel waarmee zij het overzicht houdt. Sommige gemeenten hebben hier wel een visie op, maar lang niet iedereen heeft er op deze manier over nagedacht. Daarbij is er ook twijfel of inwoners op deze vrije keuze zitten te wachten en het straks niet allemaal ingewikkelder wordt voor sommige groepen. Wel verwachten gemeenten positieve reacties op de optie om met één en hetzelfde middel bij zowel publieke als private dienstverleners in te loggen.

*Technische aanpassingen en continuïteit*
Op dit moment zijn bij veel gemeenten de inlogmiddelen een onderdeel van de software van systemen, zoals voor bijvoorbeeld burgerzaken, die worden verzorgd door leveranciers. Gemeenten

zijn hierdoor afhankelijk van de aanpassingen en de kosten die leveranciers moeten maken om de toegelaten middelen toe te laten of moeten kiezen voor een andere leverancier of oplossing. Daarvoor moet eerst duidelijk worden wat de technische eisen zijn waaraan gemeenten moeten voldoen. Om de impact van het technisch aansluiten te beperken zou een gelijkblijvende werking (koppelvlakken standaarden en kostenniveau) randvoorwaardelijk moeten zijn. Bovendien geldt ook voor dit onderdeel dat bij deze transitie de continuïteit van de digitale gemeentelijke dienstverlening een belangrijke voorwaarde is.

### *Routering als randvoorwaarde*

Belangrijkste voorwaarde om te kunnen voldoen aan de acceptatieplicht is de routeringsvoorziening. Hoewel het in theorie mogelijk lijkt om op alle middelen afzonderlijk aan te sluiten, is dit in praktijk een onaantrekkelijke optie, en ligt het voor dienstverleners voor de hand om alleen aan te sluiten op een routeringsvoorziening. Veruit de meeste gemeenten geven dan ook aan alleen nieuwe middelen te kunnen accepteren als deze zijn ontsloten via de routeringsvoorziening. Hierdoor is het accepteren van verschillende publieke en private middelen echter afhankelijk van de beschikbaarheid van een routeringsvoorziening.

Zoals opgenomen in de Wdo en eerder beschreven in hoofdstuk 2, is het ministerie van BZK onder de organisatie van Logius bezig met het ontwikkelen van een publieke routeringsvoorziening. Uit de analyse blijkt dat de meeste gemeenten nog niet goed hebben voor ogen hebben over hoe aan te sluiten op de verschillende middelen. Het liefst maken zij gebruik van de routeringsvoorziening. Ook zijn gemeenten nog niet goed op de hoogte van deze ontwikkelingen van de routeringsvoorziening en de planning hiervoor. Dit komt omdat veel nog onduidelijk is en er weinig concrete informatie beschikbaar is over de voortgang, planning en resultaten. De reputatie van BZK en Logius blijkt op dit vlak ook niet heel goed. Meestal moeten gemeenten ‘achteraan de rij aansluiten’ en de ervaring van de afgelopen jaren is dat de voorziening lang op zich wachten. Gemeenten hebben er daardoor niet veel vertrouwen in dat hier tijdig de oplossing uitkomt die gemeenten hierbij goed kunnen ontzorgen.

### *Pilot met routeringsvoorziening* Logius

In de eerste helft van 2019 heeft een pilot met vier gemeenten plaatsgevonden. In deze pilot is door de gemeenten een aansluiting gerealiseerd met een proefversie van de routeringsvoorziening van Logius. In de pilot is met name de technische werking van de routeringsvoorziening beproefd. Gemeenten hebben daarnaast input geleverd op het schermverloop dat was ingericht door Logius. Dit is nog wel een aandachtspunt voor gemeenten. Met de implementatie van de routeringsvoorziening verandert het schermverloop, de routeringsvoorziening gaat dan het schermverloop voor een belangrijk deel bepalen. Het wel of niet toepassen van de routeringsvoorziening heeft dus impact op de inrichting van het digitaal portaal of de digitale formulieren bij de gemeente, en wat daarbij voor schermverloop geregeld moet worden. De proefversie van de routeringsvoorziening bood op dat moment alleen de functionaliteit voor DigiD en op een later moment in de pilot ook eIDAS (voor EU-burgers met een BSN in Nederland).

VNG realisatie heeft een review[24] uitgevoerd op de pilot en aanbevelingen ingebracht bij Logius en opdrachtgever ministerie van BZK en samen met een aantal gemeenten en softwareleveranciers de

[24] https://www.vngrealisatie.nl/sites/default/files/2020-09/20190618%20concept%20Notitie%20Quickscan%20Routeervoorziening%200.95%20v2.pdf

wensen en eisen[25] opgehaald van gemeenten voor een routeringsvoorziening. Tot nu toe is onbekend wat precies met de eisen en wensen is gedaan. Voor enkele gemeenten is dit ook de aanleiding geweest om zelf aan de slag te gaan met het ontwikkelen van een routeringsdienst in samenwerking met hun leverancier. Rotterdam en Den Haag hebben het initiatief genomen om zelf met een leverancier een ontwikkeltraject in te gaan. Zij geven aan tevreden te zijn over de gekozen oplossing. Voor de toekomst betekent dit dat ook andere gemeenten hiervan gebruik zouden kunnen maken. Tegelijk is dit wel een extra aandachtspunt voor de routeringsvoorziening die Logius ontwikkelt. Een zorg is namelijk dat de hoge ontwikkel- en beheerkosten hiervan straks over een kleiner aantal kleinere spelers moeten worden verdeeld, omdat grote gemeenten en andere overheden zelf een routeringsvoorziening gaan ontwikkelen en oplossingen vanuit de markt mogelijk aantrekkelijker zijn.

Daarnaast geven gemeenten aan dat het belangrijk is dat straks alle gemeentelijke diensten achter één routeringsvoorziening zitten. En dat dus alle inlogmiddelen, maar ook eHerkenning en machtigen met deze ene routeringsvoorziening kunnen worden ontsloten. Gemeenten geven daarbij wel aan dat met een dergelijke allesomvattende routeringsvoorziening een ‘single point of failure’ kan ontstaan dat men met de toelating van meerdere inlogmiddelen tot het stelsel nu juist wilde voorkomen.

*Georganiseerde aansluiting als randvoorwaarde*
Voor de aansluiting op de verschillende inlogmiddelen gelden, zoals gezegd, organisatorische en technische randvoorwaarden. Niet alle publieke dienstverleners kunnen gelijktijdig aan worden gesloten. Het ministerie van BZK stelt hiervoor een aansluitschema op, op grond van de input die publieke dienstverleners, waaronder gemeenten, hiervoor zelf aan dragen. De beschikbaarheid van de publieke voorziening is essentieel voor gemeenten om duidelijkheid te hebben over de aansluittermijn om aan de wet te kunnen voldoen.

## 3.5. Overige randvoorwaarden en afhankelijkheden

De nieuwe regels en plichten voor gemeenten die uit de Wdo voortkomen staan niet op zichzelf, maar zijn onderdeel van een stelstel. Zoals geschetst in hoofdstuk 2 bevat dit stelsel verantwoordelijkheden, afspraken, toezicht en technische componenten die ontwikkeld en beheerd worden. Om bovenstaande stappen te kunnen uitvoeren zijn gemeenten, zoals eerder aangegeven, afhankelijk van de uitwerking en planning binnen dit stelsel. Samenvattend zijn gemeenten nog niet in staat om aan de Wdo te voldoen zonder dat aan deze voorwaarden is voldaan. In de paragrafen hiervoor zijn bij de verschillende onderdelen al specifiek randvoorwaarden genoemd. Hieronder wordt nog ingegaan op enkele aanvullende onderdelen.

*Machtigingen is belangrijke voorwaarde voor onderdeel betrouwbaarheidsniveaus*
Uit de analyse blijkt dat ook het ‘machtigingen’ een belangrijke voorwaarde is voor het overstappen op hogere betrouwbaarheidsniveaus. Nu is digitaal machtigen beperkt mogelijk, alleen voor vrijwillige machtigingen. Voor het kunnen voldoen aan de Wdo is een bredere inzetbaarheid van de machtigingsvoorziening voorwaardelijk. Zoals aangegeven in hoofdstuk 2 is op dit moment niet duidelijk wat de planning voor de doorontwikkeling is en wanneer de voorziening voldoet aan bovenstaande doelstellingen.

[25] https://www.vngrealisatie.nl/sites/default/files/2020-09/PVE%20routeringsvoorziening%20concept%200.4%20%28minimale%20variant%20RV%29.pdf

De machtigingsvoorziening is ten eerste noodzakelijk omdat de drempel van een hoger betrouwbaarheidsniveau er mogelijk toe leidt dat meer mensen hulp nodig hebben met digitale dienstverlening: veilig inloggen bij de overheid vraagt straks wat meer dan nu van inwoners, waardoor er mogelijk meer inwoners zijn die anderen willen machtigen om dit voor hen te doen. Ook zegt de Awb dat eenieder zich moet kunnen laten bijstaan of vertegenwoordigen.

Ten tweede speelt hierbij dat er geen 'workaround' meer is. Met de ontwikkeling van DigiD naar hogere betrouwbaarheidsniveaus wordt het moeilijker voor een inwoner om de eigen DigiD-code aan een andere persoon door te geven. Het afstaan van de persoonlijke DigiD wordt door de overheid weliswaar ontraden, maar er zijn veel situaties waarin inwoners hun persoonlijke DigiD doorgeven aan een ander persoon om voor hen zaken te regelen met de overheid. De verwachting is dat het belang van (digitaal) machtigen voor het afnemen van diensten bij de overheid door een gemachtigde verder gaat toenemen. Mensen die het niet kunnen en willen vallen dan terug op dienstverlening aan de balie. Die optie is er natuurlijk altijd, maar het drukt wel flink op de capaciteit als dit ineens sterk toeneemt.

Ten derde is naast het betrouwbaarheidsniveau van het inloggen, het net zo belangrijk dat het betrouwbaarheidsniveau van de digitale machtiging zelf voldoet aan het vereiste niveau. De machtiging moet dus, afhankelijk van de dienstverlening waarvoor de machtiging is, mogelijk op een hoger betrouwbaarheidsniveau worden uitgevoerd. Anders is 'machtigen' alsnog een achterdeur waarlangs met een lager betrouwbaarheidsniveau kan worden volstaan.

Tenslotte is naast de technische mogelijkheid, ook een uniforme productlijst (UPL) noodzakelijk voor meer standaardisatie. Hiermee worden de verschillende producten en diensten van gemeenten op eenzelfde eenduidige wijze omschreven. Hier zit nu bij gemeenten veel variatie in, wat bijvoorbeeld voor bewindvoerders die met meerdere gemeenten te maken hebben, lastig is. Voor elke gemeente moet dan apart worden nagegaan onder welke omschrijving het betreffende product of dienst staat. Gemeenten hebben veel vragen over het onderdeel machtigen en zijn met name bezorgd dat dit niet in samenhang met de andere onderdelen opgepakt gaat worden.

### *Gemeenten moeten toestemming krijgen om met BSN's te mogen werken*

Voor het gebruik van BSN, inclusief ontvangst van het BSN, zijn technische beveiligingsmaatregelen en juridische procedures ingericht om onbevoegde kennisneming van het BSN te voorkomen. Onderdeel van de juridische procedure is dat voorafgaand aan de verstrekking van het sleutelmateriaal wordt geverifieerd of de aanvrager het recht op het gebruik van het BSN ontleent aan wet- en regelgeving. Er wordt gekeken of een organisatie als een BSN-gerechtigde aangemerkt kan worden. Er moet hiervoor een verzoek worden ingediend bij de Rijksdienst voor Identiteitsgegevens (RvIG), het zogenoemde AutorisatieLijst BSN's (ALB)-proces[26]. Gemeenten moeten dit per product regelen. Ook voor eIDAS moe(s)ten gemeenten eerst als BSN-gerechtigde organisatie aangemerkt worden. Uit de analyse is gebleken dat de doorlooptijd van dit verificatieproces lang duurt. Deze lange doorlooptijd heeft mogelijk een vertragende impact op de aanvragen in het kader van de voorzieningen vanwege de Wdo. Het is nodig dat de ALB-procedure dienend is aan de uitvoering van de Wdo om mogelijke vertraging te beperken.

[26] https://www.logius.nl/sites/default/files/public/bestanden/diensten/BSNk/Toelichting-ALB-proces_0.pdf

*Planning is nog steeds niet definitief*

Doordat de inwerkingtreding van de wet ‘sluimert’ blijkt uit de analyse dat het urgentiebesef van de wet minder wordt. Daarnaast komen de onderliggende besluiten en regelingen van de Wdo in tranches beschikbaar en zijn de beschreven generieke voorzieningen en diensten nog niet beschikbaar. De verschillende onderdelen staan echter niet los van elkaar. Dit betekent dat het los verplichten van regelgeving en voorzieningen een risico vormt voor gemeenten. Zo kan er een verplichting zijn om inlogmiddelen te accepteren, maar is er nog geen landelijk routeringsvoorziening waarmee deze inlogmiddelen kunnen worden ontsloten. Of is er een inlogmiddel met betrouwbaarheidsniveau hoog, maar geen machtingsvoorziening die hiermee om kan gaan waardoor mogelijk gemachtigden individuen niet kunnen helpen en de individuele inwoners dus geen gebruik kunnen maken van de individuele dienstverlening. Voor digitalisering is er binnen gemeenten veel aandacht. De uitdaging zit erin om de losse wetten die over digitalisering gaan in samenhang te implementeren zodat er voordelen te halen zijn en de beperkte capaciteit efficiënt kan worden ingezet.

# 4. Financiële consequenties

Op dit moment is de financiële impact van de onderzochte wetsonderdelen nog erg moeilijk in te schatten. Dit komt mede doordat de oorspronkelijk beoogde Regeling bekostiging niet beschikbaar was tijdens het onderzoek. Zoals eerder aangegeven is er tijdens het schrijven van dit rapport onduidelijkheid ontstaan of deze regeling nog onderdeel gaat uitmaken van de Wdo. Dat betekent voor nu in elk geval dat onder meer artikel 21 Wdo nog niet is uitgewerkt. Volgens dit artikel worden de kosten die samenhangen met de uitvoering van de GDI (artikel 5 t/m 9) doorberekend aan publieke dienstverleners, waaronder gemeenten. Om toch een beeld te kunnen schetsen van de (mogelijke) financiële impact worden de *kostencomponenten* benoemd van de drie onderwerpen die centraal staan in deze analyse[27]. Dit maakt het ook mogelijk om in een later stadium, zodra de wet verder uitgekristalliseerd is, een zo volledig mogelijk beeld te krijgen van de financiële impact van de Wdo.

*Informatiebeveiliging toegang*

De kosten voor het onderdeel informatiebeveiliging van de toegang vallen uiteen in drie delen. Ten eerste moeten er mogelijk technische aanpassingen gedaan worden om aan de nieuwe eisen te voldoen; er moet immers een nieuwe toegangspoort beveiligd worden. Technische aanpassing van de logging en bijbehorende bewaartermijnen is hierbij bijvoorbeeld een aandachtspunt. Dit zijn eenmalige kosten om van de oude naar de nieuwe situatie te komen. Daarnaast zijn er eenmalige kosten te verwachten voor de implementatie-inspanning om van de oude naar de nieuwe situatie te komen (projectkosten, inhuur, etc.). Tenslotte zijn er de kosten die nu al gemaakt worden en straks nog steeds gemaakt moeten worden. Hieronder vallen de zelf-assessment voor de toegang (nu DigiD, straks naar verwachting de routeringsvoorziening), de externe audit hierop en de kosten voor de informatiebeveiliging zelf. Het is de vraag op dit onderdeel wat de verandering is die de nieuwe situatie met zich meebrengt ten opzichte van de huidige situatie. De verwachting is dat door verschuivingen er toch extra kosten gemaakt moeten worden op deze onderdelen. Dit zijn structurele kosten die jaarlijks gemaakt moeten worden.

*Inschaling betrouwbaarheidsniveaus*

De inschaling van de gemeentelijke dienstverlening naar de verschillende betrouwbaarheidsniveaus brengt incidentele kosten met zich mee. Deze zijn afhankelijk van de uitgangssituatie van de gemeente. Niettemin kan de inschaling de nodige kosten met zich meebrengen. Ter indicatie: uit het onderzoek blijkt dat dit voor een grote gemeente maanden in beslag nemen. Het is niet alleen noodzakelijk de proceseigenaren van de verschillende (niet zelden honderden) werkprocessen te achterhalen en een actuele lijst hiervan maken, maar ook om met alle eigenaren het gesprek voeren over het juiste betrouwbaarheidsniveau van de verschillende diensten volgens verschillende criteria (zoals veiligheid enerzijds en toegankelijkheid anderzijds). Hiervoor is waarschijnlijk een projectleider nodig, en extra inzet van bijvoorbeeld de FG. Ook zal er extra communicatie moeten worden georganiseerd richting inwoners en organisaties over de nieuwe betrouwbaarheidsniveaus, mede naar aanleiding van vragen die hierover bij de gemeente binnen zullen komen. Hiernaast moeten er mogelijk eenmalig kosten worden gemaakt door gemeenten om de inschaling vorm te geven in hun ICT-omgeving en deze mogelijk aan te passen (bijvoorbeeld door oplossingen als single sign on, portalen of webformulieren aan te passen of te herzien). Tenslotte zullen voor het beheer van de betrouwbaarheidsniveaus door de verschillende proceseigenaren structureel kosten worden gemaakt.

[27] Zie hiervoor ook MvT Wdo, paragraaf 7.3 betreffende de financiële gevolgen van de wet.

*Acceptatieplicht*

De plicht om verschillende middelen te accepteren, maakt het, zoals gezegd, voor gemeenten noodzakelijk om aan te sluiten op een routeringsvoorziening en/of een ontsluitende dienst. In de MvT bij de Wdo is hierover het volgende aangegeven (p. 40): 'Voor rekening van de dienstverleners komen in de eerste plaats de kosten voor het aansluiten op de routeringsvoorziening in het geval dat sprake is van digitale dienstverlening (op betrouwbaarheidsniveau substantieel of hoog) aan inwoners. Indien sprake is van digitale dienstverlening aan organisaties zijn er kosten voor aansluiting op de ontsluitende dienst.' Op dit moment is nog niet precies duidelijk of het hierbij om twee losse aansluitingen gaat, of dat burger- en bedrijvenmiddelen wel via één punt kunnen verlopen.

Dit brengt allereerst incidentele aansluitkosten met zich mee. Ook de aanpassingen in de interne digitale infrastructuur van gemeenten (om met de berichten van de routeringsvoorziening en/of ontsluitende dienst te kunnen werken) brengen incidentele kosten met zich mee. Daarnaast zijn er beheerkosten van zowel de aansluiting als van de aangebrachte aanpassingen in het interne digitale landschap (voor zover dit meer kosten met zich meebrengt dan de kosten van het beheer van het huidige landschap). Nog onduidelijk is of het op een later moment ontsluiten van nieuwe middelen via de routeervoorziening altijd kan zonder veranderingen voor de aansluiting van de gemeente op de routeervoorziening. Mogelijk zijn hier ook kosten mee gemoeid. Verder zullen gemeenten hun website moeten aanpassen en moeten communiceren met inwoners en organisaties over de verschillende middelen die kunnen worden gebruikt in het kader van hun digitale dienstverlening. Dit laatste zal vooral het geval zijn in de eerste fase na implementatie, en dus incidenteel kosten met zich meebrengen, maar mogelijk ook structureel, omdat ten opzichte van de huidige situatie een structureel bredere keuze aan inlogmiddelen ontstaat.

Hiernaast is het gebruik van de verschillende identificatiemiddelen een structurele kostenpost voor gemeenten. Zij gaan betalen naar rato van het gebruik van de middelen. Over dit gebruik, maar ook over de tariefstelling is op dit moment echter nog niets bekend, en ook is nog onduidelijk of de toelating van één of meer private middelen gevolgen gaat hebben voor de kosten van DigiD en de doorberekening hiervan. Gemeenten hebben hier bovendien geen enkele invloed op. Dit komt er op dit moment op neer dat voor de extra inlogmiddelen een blanco check uitgeschreven moet worden.

Ook zijn de ontwikkel- en beheerkosten van de benodigde voorzieningen, die doorberekend worden aan dienstverleners op grond van Wdo art. 21, een structurele kostenpost voor gemeenten. Ook hiervoor geldt dat de hoogte van deze kosten nog onbekend is. Dat is bovendien (mede) afhankelijk van het aantal partijen waaronder ze verdeeld moeten worden. Bij gemeenten bestaat de vrees dat bijvoorbeeld voor de routeringsvoorziening van Logius straks meer betaald moet worden, omdat sommige gemeenten en andere bestuursorganen hiervoor een eigen voorziening gaan gebruiken en dus niet meedelen in de kosten. Te zijner tijd kan een vergelijkbare situatie ontstaan voor de kosten van de ontwikkeling en het beheer van de machtigingsdienst.

*Andere kosten onderdelen*

Ook met de machtigingenvoorziening, die voorwaardelijk is voor het toepassen van de acceptatieplicht, zijn kosten gemoeid. Ook die voorziening kent (net als de routeringsvoorziening) aansluitkosten, implementatievraagstukken en inschalen van machtiging.

Tenslotte verwachten gemeenten met het ingaan van de Wdo ook meer vragen van inwoners en organisaties te krijgen over inloggen op de eigen dienstverlening. Bij de overgang naar de Wdo moet

ook worden meegenomen dat er (tijdelijk) meer inzet op communicatie nodig is van gemeenten, bijvoorbeeld op het Klant Contact Centrum. Aan opschaling hiervan zitten ook kosten verbonden.

## 4.1. Samenvatting financiële consequenties in kostencomponenten

In onderstaande tabel 1 is vanuit de vorige paragraaf een samenvatting gegeven van de (mogelijke) financiële impact door deze uit te drukken in incidentele en structurele kostencomponenten bij de drie onderwerpen die centraal staan in deze analyse.

| **Wijziging** | **Kostencomponent** | **Incidenteel** | **Structureel** |
|---|---|---|---|
| Informatiebeveiliging toegang | Technische aanpassing Waaronder logging en bewaartermijnen | X | |
| | Projectkosten voor de implementatie | X | |
| | Beheer van de informatiebeveiliging van de toegang | | X |
| | Zelf-assessment extra inlogmiddelen/routeringsvoorziening | | X |
| | Externe audit op de extra aansluitingen | | X |
| Inschaling betrouwbaarheids-niveaus | Proceseigenaren vaststellen digitale diensten | X | |
| | Samen met eigenaren betrouwbaarheidsniveau inschalen | X | |
| | Projectkosten voor implementatie | X | |
| | Extra inzet Functionaris gegevensbescherming | X | |
| | Communicatie met inwoners en organisaties over hogere betrouwbaarheidsniveaus | X | |
| | Aanpassen gemeentelijk ICT-omgeving om deze passend te laten zijn aan de ingeschaalde betrouwbaarheidsniveaus | X | |
| | Beheer betrouwbaarheidsniveaus door de verschillende proceseigenaren | | X |
| Acceptatieplicht | Aansluiten op nieuwe generieke voorzieningen | X | |
| | Aanpassen gemeentelijke infrastructuur om aan te sluiten op nieuwe generieke voorzieningen | X | |
| | Beheer aansluiting en aangepaste infrastructuur | | X |
| | Communicatie over de verschillende inlogmiddelen aan inwoners en organisaties | X | X |
| | Betalen naar rato van gebruik van de nieuwe inlogmiddelen | | X |
| | Doorbelasting ontwikkelen- en beheer kosten van de generieke voorzieningen | | X |

*Tabel 1 Samenvatting financiële consequenties in kostencomponenten*

# 5. Conclusies en aanbevelingen

In dit laatste hoofdstuk beschrijft eerst de conclusies van het onderzoek. Dat gebeurt door de onderzoeksvragen uit paragraaf 1.3 te beantwoorden. Op basis hiervan wordt na de laatste onderzoeksvraag over gegaan naar de aanbevelingen die op basis van de conclusies worden gedaan.

## 5.1. Beantwoording onderzoeksvragen

*Wat wijzigt er in de werkwijze van de gemeente door de Wet digitale overheid?*
In scope van dit onderzoek zijn er voor gemeenten concreet de volgende wijzigingen:

- Gemeenten zijn straks verplicht om maatregelen te nemen op de informatiebeveiliging van de toegang tot de digitale dienstverlening;
- Gemeenten moeten het betrouwbaarheidsniveau inschalen van authenticatie en machtiging voor een elektronische dienst en hierover communiceren naar de inwoners en organisaties;
- Gemeenten hebben een acceptatieplicht met betrekking tot alle toegelaten inlogmiddelen.

Naast bovenstaande onderdelen zijn in Wdo randvoorwaarden beschreven die gevolgen hebben voor gemeenten. Deze randvoorwaarden en de afhankelijkheden voor gemeenten zijn in hoofdstuk 3 specifiek beschreven en zijn aan het eind van dit rapport vertaald naar specifieke aanbevelingen om de Wdo uitvoerbaar te maken.

*Wat betekenen deze veranderingen voor de gemeentelijke organisatie?*
De verplichte informatiebeveiliging van de toegang tot de elektronische dienstverlening en de monitoring en verantwoording daarvan leidt tot beperkte aanpassingen binnen de gemeentelijke uitvoering als wordt aangesloten op de bestaande door gemeenten gehanteerde normering en systematiek. Als het toezicht (de audit) binnen de Wdo hierbij aansluit levert de verplichting een beperkte extra lastendruk op. Maar dit moet wel nog bevestigd worden door meer duidelijkheid over de scope van dit onderdeel te krijgen.

Gemeenten moeten voor het inschalen van de betrouwbaarheidsniveaus de onlinediensten in beeld brengen en nagaan welke gegevens daarbij verwerkt worden en per dienst bepalen of authenticatie noodzakelijk en wenselijk is. Voor het structureel beheer van de betrouwbaarheidsniveaus is het nodig deze onderdeel uit te laten maken van het reguliere proces. Vragen van inwoners en organisaties over de betrouwbaarheidsniveaus zullen bij de gemeente terecht komen. De taak van de gemeente is om te zorgen voor een goede communicatie op maat.

Acceptatie van nieuwe middelen is nog niet voor alle gemeenten mogelijk bij uitblijven van routeringsvoorziening. Veruit de meeste gemeenten geven aan alleen nieuwe middelen te kunnen accepteren aks deze zijn ontsloten via de routeringsvoorziening. Op dit moment zijn er nog geen private inlogmiddelen toegelaten en is de routeringsvoorziening nog in ontwikkeling. Hierdoor is de impact van de acceptatie van deze nieuwe middelen door gemeenten op dit moment niet goed vast te stellen. Wel is het duidelijk dat er belangrijke randvoorwaarden, wensen en eisen zijn aan de toegelaten inlogmiddelen en routeringsvoorziening die nog niet ingevuld zijn. Deze volgen uit de analyse en komen terug in de antwoorden op onderstaande vragen.

*Is de gemeente voldoende toegerust voor een doeltreffende uitvoering van de Wdo?*
Nee, de gemeenten zijn op dit moment niet voldoende toegerust om de wet doeltreffend uit te voeren. Onder de huidige omstandigheden is de Wdo voor gemeenten niet goed uitvoerbaar. Hier zijn in deze analyse verschillende redenen voor aangegeven. Om de wet voor gemeenten uitvoerbaar te maken zijn de belangrijkste aandachtspunten en randvoorwaarden:

- Gemeenten moeten de informatiebeveiliging op de toegang tot het stelsel op orde hebben, voordat de wet daadwerkelijk in werking treedt. Omdat het nog niet duidelijk is op welke manier er op het stelsel aangesloten kan worden, is ook niet duidelijk hoe de toegangsbeveiliging er precies uit gaat zien. Voorbereidingen kunnen dan ook nog niet getroffen worden.
- Gemeenten moeten in staat zijn de digitale toegang op de juiste betrouwbaarheidsniveaus te bieden. Nog niet alle middelen met hogere betrouwbaarheidsniveaus zijn beschikbaar of bekend bij de inwoners (voor organisaties is dit wel al mogelijk). Ook is nog niet duidelijk hoe moet worden omgegaan met Single Sign-On (SSO) en portalen. Voor het succesvol en verantwoord kunnen overstappen naar hogere betrouwbaarheidsniveaus is de beschikbaarheid van de machtigingsvoorziening een belangrijke randvoorwaarde.
- Gemeenten moeten alle toegelaten burger- en bedrijfsmiddelen accepteren, maar zijn hiervoor afhankelijk van een publieke routeringsvoorziening, tenzij gemeenten tijdig zelf iets kunnen regelen. Omdat functionaliteit en planning hiervan onduidelijk is, kunnen gemeenten hier niet op anticiperen.

De inwerkingtreding is al meerdere malen uitgesteld, en het is nog niet duidelijk wanneer de wet zelf in werking treedt. Gemeenten geven aan dat ze wel vaker over deze onderwerpen gehoord hebben, maar eigenlijk niet goed weten wat nu wanneer verwacht wordt. Gemeenten geven hierbij ook aan dat het 'niet te doen is' om telkens bij te houden wat de status is, en horen het graag als duidelijk is wat wanneer verwacht wordt. Gemeenten moeten tijdens de gefaseerde inwerkingtreding van de verplichtingen uit de Wdo zorgen voor de continuïteit van de dienstverlening. Mede door de onduidelijkheid die is beschreven in bovenstaande punten en door de grote uitvoeringsdruk op gemeenten door invoering van andere wetgeving (rond informatievoorziening, het sociaal domein en de omgevingswet) zijn er nog nauwelijks gemeenten gestart met de voorbereiding op de implementatie van de Wdo.

*Welke kosten en besparing voor de gemeentelijke uitvoering zijn aan deze wijziging van de wet verbonden?*
Op dit moment is de financiële impact van de onderzochte wetsonderdelen nog niet in te schatten. Dit komt vooral omdat de Regeling Bekostiging nog niet beschikbaar is. Volgens artikel 21 van de Wdo worden de kosten die samenhangen met de uitvoering van de GDI (artikel 5 t/m 9) doorberekend aan publieke dienstverleners, waaronder gemeenten. Zij betalen voor de aansluiting, via een routeringsvoorziening of op alle middelen afzonderlijk. Daarnaast betalen dienstverleners voor het gebruik van een middel door inwoners en organisaties, waarschijnlijk per inlog. Dit zijn de directe kosten voor het gebruik.

Naast de kosten die direct uit de wet of uit de op te stellen regeling zelf voortkomen zijn er ook nog kosten die gemeenten moeten maken voor bijvoorbeeld de implementatie, inschaling en voorlichting aan inwoners en organisaties. Hieronder vallen structurele kosten, waaronder kosten voor de informatiebeveiliging (beheer, zelf-assessment extra inlogmiddelen/ routeringsvoorziening, externe audit op de extra aansluitingen), beheer betrouwbaarheidsniveaus, beheer van de aansluiting(en) en communicatie naar inwoners en organisaties. En er zijn voor de implementatie verschillende incidentele kosten bij gemeentes. Ook hiervoor geldt dat eerst meer duidelijkheid moet zijn over de

manier waarop aansluiten op de voorzieningen er uit gaat zien, voordat deze kunnen worden berekend.

Om een beeld te kunnen schetsen van de (mogelijke) financiële impact zijn de *kostencomponenten* van de drie onderwerpen die centraal staan in deze analyse[28] beschreven. Op dit moment is echter nog niet duidelijk welke bedragen voor een gemeente zijn gekoppeld aan de afzonderlijke componenten. In een later stadium, zodra de wet verder uitgekristalliseerd is en kosten bekend zijn, zal de financiële impact van de Wdo moeten worden berekend.

*Wat zijn de verwachte effecten van de Wdo voor gemeenten?*
De wet is geschreven vanuit het perspectief van de overheid en gaat over de inrichting van het stelsel voor toegang tot de digitale dienstverlening. De Wdo beschrijft de verantwoordelijkheden van de minister van BZK en de verplichtingen voor bestuursorganen en private partijen met betrekking tot de aansluiting op de generieke voorzieningen, maar gaat nauwelijks in op het effect op inwoners en organisaties. In deze analyse komt naar voren dat gemeenten wel effect verwachten op inwoners en organisaties. Dit effect wordt veroorzaakt doordat een hoger betrouwbaarheidsniveau hogere drempels, maar ook hogere verwachtingen, kan opwerpen voor de inwoners en organisaties, met name voor dienstverlening in het sociale domein.

Er is ook twijfel of inwoner en organisaties op vrije keuze van inlogmiddelen zitten te wachten en het straks niet allemaal ingewikkelder wordt. Aan de andere kant geeft de analyse aan dat mogelijk, door het beschikbaar komen van private middelen, de optie om met een en hetzelfde middel bij zowel publieke als ook private dienstverleners te kunnen inloggen positief zal worden ontvangen door inwoners. Daarnaast kan het voor sommige inwoners bijdragen aan hun wens voor meer regie op eigen gegevens.

*Hoe kan de Wdo worden geïmplementeerd en wat zijn de randvoorwaarden en risico's?*
Samenvattend is de Wdo op dit moment voor gemeenten niet uitvoerbaar, gezien het feit dat een aantal belangrijke randvoorwaarden niet ingevuld is. Er is op alle fronten behoefte aan een duidelijke aanpak en planning voor de Wdo. Ten eerste over onduidelijkheden die in de wet zelf zitten en over de planning van de inwerkingtreding (zie de aanbevelingen). Ten tweede over de specificaties voor de (publieke) voorzieningen en de planning van oplevering hiervan. De Wdo hanteert een gefaseerde inwerkingtreding. Deze fasering komt niet goed overeen met de afhankelijkheden tussen onderlinge onderdelen. Ten derde is er nog niets duidelijk over de te verwachten kosten voor gemeenten van de nieuwe voorzieningen en inlogmiddelen.

Bij gebrek aan duidelijkheid ontstaat onrust. Het risico is dat door deze onrust de overgang naar het beoogde stelsel van de Wdo niet soepel verloopt en er problemen ontstaan in de continuïteit van de digitale dienstverlening van gemeenten (en andere bestuursorganen). Gemeenten maken zich met name zorgen over wat het voor inwoners betekent, het inloggen wordt met hogere betrouwbaarheidsniveaus ingewikkelder en er komen nieuwe (onbekende) inlogmiddelen beschikbaar. Als de transitie niet goed verloopt kan dit nadelige gevolgen hebben voor inwoners die op onderdelen van deze digitale dienstverlening afhankelijk zijn. De dienstverlening aan die inwoners komt dan in het gedrang.

[28] Zie hiervoor ook MvT Wdo, paragraaf 7.3 betreffende de financiële gevolgen van de wet.

## 5.2. Aanbevelingen

Om de Wdo succesvol te kunnen implementeren door gemeenten en de wet uitvoerbaar te maken is het belangrijk dat de volgende aanbevelingen worden overgenomen. De belangrijkste aanbevelingen van algemene aard worden als eerste gegeven, gevolgd door een aantal specifieke aanbevelingen voor de drie onderdelen, informatiebeveiliging, betrouwbaarheidsniveaus en acceptatieplicht.

*Geef meer duidelijkheid over inhoud (wettekst), planning en kosten*
Als eerste is meer duidelijkheid nodig om een goede voorbereiding op de Wdo te kunnen treffen. Maak op korte termijn een gedegen een haalbare planning voor de inwerkingtreding van de wet en de technische oplevering van voorzieningen. Geef ook zo spoedig mogelijk duidelijkheid over de door te belasten kosten, of maak hier een prognose van die periodiek wordt geüpdate. Dit helpt gemeenten om ook financieel te kunnen anticiperen op de wet. Geeft tenslotte ook duidelijkheid over de onderdelen in de wetteksten waar nu verwarring over is. Gemeenten mogen niet voor verassingen komen te staan omdat de onderdelen in de wet niet duidelijk omschreven zijn.

*Faciliteer door het gelijktijdig beschikbaar maken van routeringsvoorziening en machtigingsdienst*
Neem de randvoorwaarden en afhankelijkheden tussen de verschillende regelgeving en bijbehorende voorzieningen in deze planning nadrukkelijk mee zodat de Wdo uitvoerbaar wordt. Zorg bijvoorbeeld dat voor de acceptatieplicht zowel een routeringsvoorziening als ook een machtigingsdienst beschikbaar is. Het vraagstuk machtigen kan niet los worden gezien van de inlogmiddelen en de bijbehorende betrouwbaarheidsniveaus, omdat wijzigingen in de betrouwbaarheidsniveaus van inlogmiddelen weerslag hebben op de vraag naar machtiging. Om problemen in de uitvoering te vermijden moeten deze vraagstukken gezamenlijk en op hetzelfde moment worden opgelost. Maak hierbij ruimte om praktijkervaring op te doen met deze voorzieningen.

*Bepaal de impact van de wet integraal bij elke nieuw uitgewerkt onderdeel*
Faciliteer het proces om telkens bij het beschikbaar komen van nieuwe onderdelen van de Wdo de impact te bepalen en daarbij ook terug te kijken naar de impact zoals die eerder op andere onderdelen is bepaald. Vanwege het getrapt beschikbaar komen van de nadere uitwerking van de Wet zullen telkens elementen van de Wet worden onderzocht. Deze elementen staan echter niet los van elkaar. De impact van een los bekeken AMvB of Regeling kan flink veranderen door bepalingen die in een ander onderdeel opgenomen worden. Risico is dat bij het doen van losse impactanalyses samenhang en onderling doorwerking niet goed wordt onderkend. Heb hier nadrukkelijk aandacht voor in het opdrachtgeverschap op de analyses. Gebruik alle uitvoeringstoetsen als input voor het opstellen van het aansluitschema.

*Zorg voor goede en tijdige communicatie naar inwoners en organisaties*
Communiceer naar inwoners en organisaties op het moment dat hogere betrouwbaarheidsniveaus worden toegepast en nieuwe middelen beschikbaar komen. Een publiciteitscampagne vanuit de Rijksoverheid kan veel vragen wegnemen en de druk op de gemeentelijke organisatie bij de invoering verminderen. Gemeenten maken zich zorgen dat met name sommige inwoners in deze ontwikkeling niet goed kunnen meekomen.

Voor de onderdelen van de Wdo die inmiddels zijn uitgewerkt zijn hieronder nog aanvullend specifieke aanbevelingen opgenomen.

*Aanbevelingen beveiliging van de toegang*

- Het is nodig om bij het Besluit digitale overheid, als toelichting op de scope, op te nemen dat het gaat over informatiebeveiliging van toegang tot de GDI zodat deze scope niet voor meerdere uitleg vatbaar is. Bovendien is duidelijkheid gewenst over de inhoud van de audit in het geval van aansluiten via de routeringsvoorziening of rechtstreeks via een eigen opdracht aan een marktpartij.
- Om de extra lastendruk in de monitoring en verantwoording beperkt te houden is het nodig om de auditsystematiek en normering vanuit de Wdo (aanvullende regelgeving is nog niet beschikbaar) passend te laten zijn bij de huidige periodiciteit en proces van informatie aanleveren, risicogerichte aanpak en normering uit de BIO van gemeenten.
- De Informatiebeveiligingsdienst heeft voor gemeenten een *Handreiking Aanwijzing Logging*[29] opgesteld waarin volgens de dataclassificatie systematiek de bewaartermijnen zijn bepaald. Hier worden de bewaartermijnen van een log bepaald door de verschillende eisen voor integriteit en vertrouwelijkheid van gegevens. Deze bewaartermijnen zijn afwijkend van de maximaal 5 jaar van de wet. Aanbevolen wordt om op dit punt aan te sluiten bij de door gemeenten gehanteerde systematiek.

*Aanbeveling inschaling van de betrouwbaarheidsniveaus*

- Gemeenten zetten het belang van de continuïteit van de dienstverlening aan inwoners en organisaties bovenaan. Zorg ervoor dat de voorzieningen die randvoorwaardelijk zijn voor het toepassen van de betrouwbaarheidsniveaus tijdig gereed zijn. Het is daarbij nodig dat de ALB-procedure dienend is aan de uitvoering van de Wdo om mogelijke vertraging te beperken. Voor de hand liggend is dat er publieke middelen op niveau substantieel en hoog beschikbaar moeten zijn. Maar ook het onderdeel machtigen is een belangrijke randvoorwaarde voor het kunnen toepassen van de hogere betrouwbaarheidsniveaus. Zorg ervoor dat deze voorziening gereed is met alle specifieke eisen die hiervoor voorzien zijn.
- Zorg dat gemeenten op tijd kunnen beginnen met het inschalen van de betrouwbaarheidsniveaus door duidelijkheid te geven over de inwerkingtreding. Gemeenten geven aan dat een bijkomend effect van deze risicoafweging is dat zij nog eens goed kijken naar dataminimalisatie. Bovendien kunnen nog niet alle ICT-systemen verschillende betrouwbaarheidsniveaus aan. Mede hierdoor neemt dit onderdeel mogelijk veel tijd in beslag.

*Aanbevelingen acceptatieplicht*

- Zorg voor duidelijkheid in de wetteksten op de onderdelen routeringsvoorziening en ontsluitende diensten, zodat gemeenten weten wat er van ze verwacht wordt en hoe het informatielandschap er in toekomst precies uit gaat zien.
- Zorg ervoor dat de voorzieningen die randvoorwaardelijk zijn voor de acceptatieplicht tijdig gereed zijn. De precieze status van de routeringsvoorziening is op dit moment onduidelijk, terwijl het voor gemeenten een belangrijke voorwaarde is om te kunnen werken met de verschillende middelen. Gemeenten hebben duidelijkheid nodig over de functie en reikwijdte van deze voorziening, over de relatie tot ontsluitende diensten en de technische specificaties ervan. Ook is het belangrijk duidelijkheid te krijgen over de mogelijkheid zelf een routeringsvoorziening te (laten) ontwikkelen. Maak hierbij ook gebruik van de al aangereikte aanbevelingen over de routeringsvoorzieningen door de VNG.

[29] https://www.informatiebeveiligingsdienst.nl/kennisproducten-ibd/

# Bijlage A: Gesprekspartners

| Gemeente | Gesprekspartners | Rol |
|---|---|---|
| Rotterdam | Marco Smit | Adviseur Dienstverlening/DigiD/eHerkenning |
| | Rob Bruijnzeels | Programmamanager Toegankelijk |
| Den Haag | Vincent van Beek | Product Owner MijnDenHaag |
| | John Agterdenbos | Chief Enterprise architect |
| | Jan Verbeek | Solution Architect |
| Montferland | Marco Robins | Informatiemanager |
| | Paul Deimann | CISO/FG |
| Groningen | Bram Scholtens | Adviseur Dienstverlening |
| | Bas Verheijen | CISO |
| | Michiel Klok | Sr. Informatieadviseur |
| Almere | Joël Koeckhoven | Sr. Beleidsadviseur informatievoorziening |
| | Peter van der Wel | Strategisch Beleidsadviseur |
| | Barbara Buitenhuis-Vis | Sr. Beleidsadviseur Burgerzaken |
| Samenwerkingsverband Oisterwijk, Hilvarenbeek en Goirle | Marion Denissen | Projectleider Dienstverlening |
| | Marco de Bruin | CISO |
| | Ronald van Andel | Informatiemanager Goirle |
| | Barbara Hooijmakers | Webmaster Oisterwijk |
| | Rene Koks | Manager Dienstverlening Oisterwijk |
| | Marja Kuijpers | Afdelingshoofd burgerzaken en KCC |
| | Leo van Herk | Informatiemanager |
| | Bas Emmen | Informatie beheerder |
| | Noortje van Gils | ENSIA coördinator |
| | Gerry de Vaan | Informatiemanagement |
| Aa en Hunze/Assen Assen | Arnoud Bijvoet | CISO (gecombineerd) |
| | Jan Ekke de Vries | Strategisch Informatiemanager |
| Deventer/Olst-Wijhe/ Raalte (DOWR) | Hessel Bremer | CISO DOWR en Zwolle |
| | Martine Kolk | Informatiemanager DOWR |
| | Lotte Schieving | FG DOWR |
| | Wessel Hemels | ISO DOWR |
| | Lucas Klekamp | Privacy Officer DOWR |
| | Eric Grotenhuis | ENSIA Coördinator DOWR |
| Lingewaard | Lenie van der Horst | Teammanager Informatievoorziening |
| | Marco ten Bohmer | Informatiemanager |
| | Victoria Lamers | Informatieadviseur |
| | Eric-Hans Bais | CISO |
| Medemblik | Kim Engel-de Koning | Informatiemanager |
| | Erik Müller | Informatie Architect |
| | Koosje Bozelie | Adviseur e-dienstverlening |
| | Ferry Posno | CISO (Koggenland, Opmeer, Medemblik) |
| | Dick Sijm | Informatieadviseur |
| Stichtse Vecht | Aad Verboom | Architect |
| | Sander Nagtegaal | CISO |