Wijziging van de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg en de Jeugdwet in verband met digitale identificatie en authenticatie in de zorg

Voorstel van wet

Wij Willem-Alexander, bij de gratie Gods, Koning der Nederlanden, Prins van Oranje-Nassau, enz. enz. enz.

Allen, die deze zullen zien of horen lezen, saluut! doen te weten:

Alzo, Wij in overweging genomen hebben, dat het wenselijk is om regels te stellen over het veilig digitaal kunnen raadplegen van informatie door zorgaanbieders, zorgmedewerkers, indicatieorganen, zorgverzekeraars, jeugdhulpaanbieders en medewerkers van jeugdhulpaanbieders, met behulp van registers en door middel van inlogmiddelen die voldoen aan het betrouwbaarheidsniveau hoog;

Zo is het, dat Wij, de Afdeling advisering van de Raad van State gehoord, en met gemeen overleg der Staten-Generaal, hebben goedgevonden en verstaan, gelijk Wij goedvinden en verstaan bij deze:

Artikel I

De Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg wordt als volgt gewijzigd:

A

Aan artikel 1 wordt na onderdeel # [waarvan de letteraanduiding alfabetisch aansluit op het laatste onderdeel], onder vervanging van de punt aan het slot van dat onderdeel door een puntkomma, drie onderdelen toegevoegd, luidende:

#. *inlogmiddel:* elektronisch middel voor identificatie en authenticatie ten behoeve van onder meer elektronische gegevensuitwisseling in de zorg;

#. *betrouwbaarheidsniveau hoog:* betrouwbaarheidsniveau hoog als bedoeld in artikel 8, tweede lid, onder c, van Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG (PbEU 2014, L 257) en de krachtens deze verordening vastgestelde uitvoeringshandelingen;

#. *zorgmedewerker*:
a. zorgverlener als bedoeld in artikel 1 van de Wet kwaliteit, klachten en geschillen zorg; en
b. eenieder die werkzaamheden verricht of gaat verrichten voor een zorgaanbieder, indicatieorgaan of zorgverzekeraar en daarbij cliëntgegevens verwerkt.

B

Hoofdstuk 3 komt te luiden:

Hoofdstuk 3. Identificatie en authenticatie

Artikel 14
1. Er wordt een register ingesteld van zorgaanbieders, zorgmedewerkers, indicatieorganen en zorgverzekeraars, ten behoeve van:
a. het verlenen van toegang tot de voorzieningen, bedoeld in artikel 3, eerste lid, onder c en d, van de Wet algemene bepalingen burgerservicenummer; en

b. de identificatie en authenticatie van zorgaanbieders of zorgmedewerkers in verband met onder meer het gebruik van elektronische uitwisselingssystemen en zorginformatiesystemen.

2. Het register wordt ingesteld en beheerd door Onze Minister.

3. Bij of krachtens algemene maatregel van bestuur worden regels gesteld over:
a. de inschrijving van een zorgaanbieder, zorgmedewerker, indicatieorgaan of zorgverzekeraar in het register;
b. de procedure en gronden voor weigering, schorsing of intrekking van een inschrijving in het register;
c. het verwerken van gegevens van zorgaanbieders, zorgmedewerkers, indicatieorganen of zorgverzekeraars in het register, waaronder kan worden verstaan het verwerken van persoonsgegevens zoals burgerservicenummer;
d. het verlangen van bijdragen van de in het register opgenomen zorgaanbieders, zorgmedewerkers, indicatieorganen en zorgverzekeraars in de kosten van het betreffende register.

Artikel 14a
1. Onze Minister verleent goedkeuring aan een inlogmiddel of categorieën van inlogmiddelen als dit middel en indien van toepassing, de koppeling van dit middel aan een in het register geregistreerde, voldoet of voldoen aan het betrouwbaarheidsniveau hoog.

2. Bij of krachtens algemene maatregel van bestuur worden regels gesteld over:
a. de wijze waarop met een bewijsmiddel aangetoond kan worden of een inlogmiddel, of de koppeling van dit middel aan een geregistreerde, voldoet aan het betrouwbaarheidsniveau hoog;
b. het indienen van een aanvraag voor goedkeuring en de gegevens die hierbij worden verstrekt;
c. het verlenen, weigeren, schorsen of intrekken van goedkeuring;
d. het aan Onze Minister of de Inspectie, op verzoek of uit eigen beweging, verstrekken van alle gegevens die nodig zijn om te beoordelen of het betreffende goedgekeurde inlogmiddel op dat moment voldoet aan het betrouwbaarheidsniveau hoog, door:
1º. een in het register, bedoeld in artikel 14, geregistreerde;
2º. diegene van wie het inlogmiddel is goedgekeurd;
3º. de verstrekker van een bewijsmiddel als bedoeld in onderdeel a.
e. de verwerking van persoonsgegevens die noodzakelijk is voor de uitvoering van dit artikel.

Artikel 15
1. Voor zover onder meer de voorzieningen en systemen, bedoeld in artikel 14, eerste lid, gebruikt worden met een overeenkomstig artikel 14a, eerste lid, goedgekeurd inlogmiddel, wordt een geregistreerde door de beheerder van deze voorziening of dit systeem in staat gesteld om ook gebruik te maken van ieder ander goedgekeurd inlogmiddel.

2. Een zorgaanbieder kan onder door hem te stellen voorwaarden onder andere elektronische uitwisselingssystemen of zorginformatiesystemen geheel of gedeeltelijk gebruiken of laten gebruiken met ieder goedgekeurd inlogmiddel door een in het register ingeschreven zorgaanbieder of zorgmedewerker.

3. Ten behoeve van de koppeling van het inlogmiddel aan een in het register geregistreerde kunnen persoonsgegevens worden verwerkt, waaronder het burgerservicenummer.

4. Bij of krachtens algemene maatregel van bestuur worden regels gesteld over:
a. de toegang tot en het gebruik van voorzieningen, elektronische uitwisselingssystemen en zorginformatiesystemen met ieder goedgekeurd inlogmiddel;
b. de koppeling van een inlogmiddel aan een geregistreerde en de benodigde gegevensverwerking.

C

In de artikelen 16 en 16a wordt na ‘artikelen 5 tot en met 12,’ ingevoegd ’14a,’.

D

Na artikel 17b wordt een artikel ingevoegd, luidende:

Artikel 18
Op een in een register als bedoeld in artikel 14 ingeschreven zorgaanbieder, indicatieorgaan of zorgverzekeraar aan wie vóór de inwerkingtreding van de Wet van [datum] tot wijziging van de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg en de Jeugdwet in verband met digitale identificatie en authenticatie in de zorg (*Stb.* 20XX, XXX) een middel is verstrekt als bedoeld in artikel 15, derde lid, zoals dat artikel luidde voor de inwerkingtreding van de hiervoor genoemde wet, blijft dat artikel van toepassing tot een bij of krachtens algemene maatregel van bestuur te bepalen moment.

E

Artikel 18 vervalt.

Artikel II

Artikel 7.2.7 en 7.2.8 van de Jeugdwet komen als volgt te luiden:

Artikel 7.2.7
1. Er wordt een register ingesteld van jeugdhulpaanbieders, jeugdhulpverleners en medewerkers die werkzaamheden verrichten of gaan verrichten voor jeugdhulpaanbieders, ten behoeve van:
   a. het verlenen van toegang tot de voorzieningen, bedoeld in artikel 3, eerste lid, onder c en d, van de Wet algemene bepalingen burgerservicenummer; en
   b. de identificatie en authenticatie van jeugdhulpaanbieders, jeugdhulpverleners of medewerkers in verband met onder meer het gebruik van elektronische systemen waarin gegevens van jeugdigen worden verwerkt.

2. Het register wordt ingesteld en beheerd door Onze Minister.

3. Bij of krachtens algemene maatregel van bestuur worden regels gesteld over:
   a. de inschrijving van een jeugdhulpaanbieder, jeugdhulpverlener of medewerker, in het register;
   b. de procedure en gronden voor weigering, schorsing of intrekking van een inschrijving in het register;
   c. het verwerken van gegevens van jeugdhulpaanbieders, jeugdhulpverleners of medewerkers in het register, waaronder kan worden verstaan het verwerken van persoonsgegevens zoals burgerservicenummer;
   d. het verlangen van bijdragen van de in het register opgenomen jeugdhulpaanbieders, jeugdhulpverleners of medewerkers in de kosten van het betreffende register.

Artikel 7.2.8
1. Voor zover onder meer de voorzieningen en systemen, bedoeld in artikel 7.2.7, eerste lid, gebruikt worden met een overeenkomstig artikel 14a, eerste lid, van de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg goedgekeurd inlogmiddel, wordt een geregistreerde door de beheerder van deze voorziening of dit systeem in staat gesteld om ook gebruik te maken van ieder ander goedgekeurd inlogmiddel.

2. Een jeugdhulpaanbieder kan onder door hem te stellen voorwaarden onder andere zijn systemen als bedoeld in artikel 7.2.7, eerste lid, onder b, geheel of gedeeltelijk gebruiken of laten gebruiken met ieder goedgekeurd inlogmiddel door een in het register ingeschreven jeugdhulpaanbieder, jeugdhulpverlener of een medewerker als bedoeld in artikel 7.2.7, eerste lid.

3. Ten behoeve van de koppeling van het inlogmiddel aan een in het register geregistreerde jeugdhulpaanbieder, jeugdhulpverlener of medewerker, kunnen persoonsgegevens worden verwerkt, waaronder het burgerservicenummer.

4. Bij of krachtens algemene maatregel van bestuur worden regels gesteld over:
   a. de toegang tot en het gebruik van voorzieningen en systemen;
   b. de koppeling van een inlogmiddel aan een geregistreerde en de benodigde gegevensverwerking.

C

Aan artikel 10.2 wordt een lid toegevoegd, luidende:

5. Op een in de autorisatielijst, bedoeld in artikel 7.2.7, ingeschreven jeugdhulpaanbieder aan wie vóór de inwerkingtreding van de Wet van [datum] tot wijziging van de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg en de Jeugdwet in verband met digitale identificatie en authenticatie in de zorg (*Stb.* 20XX, XXX) een middel is verstrekt als bedoeld in artikel 7.2.8, derde lid, zoals dat artikel luidde voor de inwerkingtreding van de hiervoor genoemde wet, blijft dat artikel van toepassing tot een bij of krachtens algemene maatregel van bestuur te bepalen moment.

Artikel III
Deze wet treedt in werking op een bij koninklijk besluit te bepalen tijdstip, dat voor de verschillende artikelen of onderdelen daarvan verschillend kan worden vastgesteld.

Lasten en bevelen dat deze in het Staatsblad zal worden geplaatst en dat alle ministeries, autoriteiten, colleges en ambtenaren die zulks aangaat, aan de nauwkeurige uitvoering de hand zullen houden.

De Minister van Volksgezondheid,
Welzijn en Sport,

Inhoudsopgave

Algemeen deel

1. Inleiding

Om passende zorg en jeugdhulp te kunnen leveren, moeten medewerkers op het juiste moment kunnen beschikken over de juiste informatie op de juiste plek. Door meer gegevens elektronisch uit te wisselen worden administratieve lasten verminderd en worden fouten voorkomen. Dat is nu lang niet altijd het geval. Met dit wetsvoorstel wordt daarom een belangrijke randvoorwaarde ingevuld om gegevens elektronisch te kunnen uitwisselen: veilige en betrouwbare digitale toegang[1] van zorgmedewerkers, oftewel identificatie en authenticatie.

In het coalitieakkoord is de ambitie opgenomen om de standaardisatie van elektronische gegevensuitwisseling in de zorg te intensiveren. Om maximale elektronische gegevensuitwisseling in de zorg te realiseren moeten echter meer randvoorwaarden worden ingevuld waarbij meer regie vanuit de overheid noodzakelijk is. Hiertoe wordt opgeroepen vanuit de Tweede Kamer[2] en vanuit het zorgveld. Eén van die randvoorwaarden betreft de totstandkoming van generieke functies. Denk hierbij aan functionaliteiten voor de toestemming van de cliënt/patiënt, adressering (vindbaarheid zorgaanbieders), lokalisatie (vindbaarheid cliëntgegevens) en de toegang tot digitale gegevens. Deze functies zijn nodig voor alle elektronische gegevensuitwisselingen, vandaar de naam generieke functies. In dit wetsvoorstel staan de generieke functies identificatie en authenticatie centraal. In het Integraal Zorgakkoord (hierna: IZA) is afgesproken dat deze functies uiterlijk in 2025 ingevuld zijn met afspraken, standaarden of voorzieningen, met als belangrijke toevoeging dat zij sectoroverstijgend beschikbaar zijn en in de praktijk gebruikt kunnen worden. Daar wordt mede met dit wetsvoorstel invulling aan gegeven.

Op dit moment vindt identificatie en authenticatie plaats aan de hand van het Unieke Zorgverlener Identificatie register (hierna: UZI-register) voor toegang tot de Sectorale Berichtenvoorziening in de zorg (hierna: SBV-Z). Daarmee kunnen zorgaanbieders, jeugdhulpaanbieders, indicatieorganen en zorgverzekeraars persoonsgegevens van cliënten verifiëren bij de basisregistratie personen (hierna: BRP). Na registratie in het UZI-register kunnen passen worden aangevraagd en verstrekt aan de medewerkers. De pas is een soort elektronisch paspoort waarmee gegevens geraadpleegd en uitgewisseld kunnen worden. Daarnaast wordt ook een elektronische identiteit uitgegeven voor systemen van zorgaanbieders, jeugdhulpaanbieders, indicatieorganen en zorgverzekeraars; een servercertificaat. Dit alles is echter onvoldoende om te komen tot grootschalig gebruik van inlogmiddelen op het juiste betrouwbaarheidsniveau. Het huidige UZI-register en de bijbehorende inlogmiddelen kunnen namelijk niet breed in de zorg worden gebruikt voor de verschillende systemen waarmee gewerkt wordt. De passen worden daarnaast als gebruiksonvriendelijk en duur ervaren.

1.1 Het wetsvoorstel in het kort

Om uniforme, veilige en betrouwbare digitale toegang tot gegevens van cliënten te realiseren voorziet het wetsvoorstel in de instelling van één register van zorgaanbieders, jeugdhulpaanbieders, jeugdhulpverleners, indicatieorganen, zorgverzekeraars en medewerkers. Medewerkers zijn natuurlijke personen die werkzaamheden verrichten of gaan verrichten voor zorgaanbieders, jeugdhulpaanbieders, indicatieorganen en zorgverzekeraars en daarbij cliëntgegevens verwerken. De in hiervoor genoemde in het register ingeschrevenen worden hierna gemakshalve aangeduid als zorg- en jeugdhulpaanbieders en hun medewerkers. Zij krijgen de keuze tussen verschillende goedgekeurde inlogmiddelen die voldoen aan het betrouwbaarheidsniveau hoog. Met deze middelen kunnen alle geverifieerde ingeschrevenen toegang krijgen tot de SBV-Z wanneer deze over de juiste autorisatie beschikken. Ingeschrevenen kunnen deze inlogmiddelen daarnaast gebruiken om onder andere elektronische uitwisselingssystemen te raadplegen. Het UZI-register verstrekt voor deze toepassingen identificerende kenmerken van ingeschrevenen bij het gebruik van inlogmiddelen. Met dit register en deze inlogmiddelen worden identificatie en authenticatie gebruiksvriendelijk en flexibel en kunnen kosten worden gereduceerd. Dit draagt bij aan het invullen en geschikt maken van de

[1] Toegang verkrijgen of inloggen is een vorm van autorisatie op basis van identificatie en authenticatie. De termen toegang en inloggen worden in deze toelichting gebruik t.b.v. de leesbaarheid.
[2] Zie de moties Van den Berg en Kerstens Kamerstukken II 2020/21, 27 529, nr. 222 en nr. 223.

generieke functie voor identificatie en authenticatie voor grootschalig en breed gebruik in de zorg. Daarmee wordt een belangrijke randvoorwaarde ingevuld om meer gegevens veilig digitaal uit te wisselen.

1.2 Digitalisering in de zorg en het belang van identificatie en authenticatie

De digitale transformatie van de zorg en het toenemend volume van elektronische uitwisseling (het delen en benaderen van medische gegevens van cliënten) maakt een betrouwbare en veilige gegevensuitwisseling in de zorg noodzakelijk. De toegang van zorgaanbieders en hun medewerkers tot deze gegevens is hierbij een belangrijke randvoorwaarde. Voor veilige gegevensuitwisseling moeten zij zich kunnen identificeren (identiteit bekend maken) en authentiseren (identiteit bewijzen) zodat onweerlegbaar vastgesteld kan worden wie medische gegevens deelt of benadert. Dit doen zij met een inlogmiddel. Voor digitale gegevensuitwisseling tussen zorgaanbieders en hun medewerkers is vertrouwen namelijk essentieel. Zij moeten erop kunnen vertrouwen dat andere zorgaanbieders de digitale toegang van hun medewerkers veilig en betrouwbaar hebben geregeld. De behoefte aan een uniforme en veilige manier van identificeren en authentiseren is dan ook groot.

1.3 Het huidige UZI-register en de inlogmiddelen

Op dit moment vindt identificatie en authenticatie van zowel zorg- als jeugdhulpaanbieders en hun medewerkers plaats aan de hand van het Unieke Zorgverlener Identificatie register (UZI-register). Het UZI-register is wettelijk ingesteld om de ingeschrevenen toegang te verlenen tot een voorziening waarmee cliëntgegevens geverifieerd kunnen worden, waaronder het burgerservicenummer (hierna: BSN). Deze voorziening is de SBV-Z. Voor opname in het UZI-register wordt geverifieerd of de aanvrager gebruik mag maken van de SBV-Z. Na registratie in het register en verificatie worden zogenoemde UZI-passen aan medewerkers van zorg- en jeugdhulpaanbieders verstrekt. De UZI-pas wordt uitgelezen met behulp van een kaartlezer en is een soort elektronisch paspoort. Een zorg- of jeugdhulpmedewerker kan de UZI-pas gebruiken voor digitale identificatie, authenticatie, autorisatie, en het verzegelen alsmede ondertekenen van digitale (medische) gegevens. Verzegelen en ondertekenen gebeurt door het zetten van een gekwalificeerde elektronische handtekening. Dat is een digitale handtekening die juridisch gelijk staat aan het zetten van een natte handtekening. Naast het uitgeven van UZI-passen kan ook een servercertificaat worden uitgegeven voor systemen van organisaties die de SBV-Z benaderen. Het servercertificaat waarborgt betrouwbare uitwisseling van (zorg)informatie tussen systemen. UZI-passen en UZI-servercertificaten worden tezamen UZI-middelen genoemd. Het UZI-register en de UZI-middelen zijn onlosmakelijk met elkaar verbonden. Het UZI-register koppelt namelijk de fysieke identiteit van een gebruiker aan een elektronische identiteit en legt deze vast in een certificaat of inlogmiddel. Het aanvragen van UZI-middelen kan dan ook niet zonder opname in het UZI-register.

Het register en de middelen zijn primair bedoeld om gebruik te kunnen maken van de SBV-Z. Inmiddels worden het register en de middelen breder gebruikt dan enkel voor toegang tot de SBV-Z. Ook kan met dit register en deze middelen onder andere toegang worden verkregen tot het Landelijk Schakelpunt (LSP) en enkele registers zoals het Landelijk Implantatenregister. Hiermee wordt toegang verleend op het hoogste betrouwbaarheidsniveau. Onder het huidige wettelijk kader kunnen het UZI-register en de bijbehorende middelen evenwel niet breder worden ingezet, het register is immers primair gericht op het kunnen raadplegen van de SBV-Z. Voor toegang tot zorginformatiesystemen zoals elektronische patiëntendossiers (hierna: EPD's) mogen het register en de middelen strikt genomen dan ook niet gebruikt worden. Dit terwijl deze middelen een veilige wijze van inloggen bieden, die voor zorgaanbieders niet eenvoudig op een andere manier te realiseren is. Nu worden naast de UZI-middelen daarom veel verschillende andere methoden van inloggen gebruikt, zoals verschillende gebruikersnamen en wachtwoorden, eventueel met een tweede authenticatiefactor. Inloggen gebeurt dan ook niet uniform en vaak niet op het vereiste betrouwbaarheidsniveau hoog.

De Europese eIDAS-Verordening[3] (hierna: eIDAS) is de basis voor een betrouwbare digitale dienstverlening in de EU. eIDAS staat voor 'Electronic Identities And Trust Services'. eIDAS maakt onderscheid tussen drie niveaus van betrouwbaarheid: 'laag', 'substantieel' en 'hoog'. Er zijn verschillende betrouwbaarheidsniveaus omdat inlogmiddelen worden gebruikt voor toegang tot verschillende gegevens. Sommige gegevens zijn bijvoorbeeld extra privacygevoelig, zoals gezondheidsgegevens. De betrouwbaarheidsniveaus geven aan met welke zekerheid de identiteit is vastgesteld en door de gebruiker kan worden bewezen. Om de identiteit te bewijzen worden zogenaamde authenticatiefactoren toegepast. Voorbeelden zijn: iets dat je weet (gebruikersnaam en wachtwoord), iets dat je bent (biometrische gegevens), iets dat je hebt (token, SMS/e-mail code).

Het UZI-register is momenteel een Trusted Service Provider (hierna: TSP). Het register wordt beheerd door de minister, deze taak wordt uitgevoerd door het CIBG. Het CIBG verstrekt en beheert hiertoe certificaten en sleutelinformatie. Certificaten worden op dragers gezet (de UZI-pas en het UZI-servercertificaat) en uitgegeven aan natuurlijke personen en systemen. De technologie/standaard achter de certificaten is Public Key Infrastructure (PKI[4]). Het UZI-register voldoet hiertoe aan de normen van de Public Key Infrastructure voor de overheid (PKI-o). Dat maakt het certificaat hoogwaardig en betrouwbaar. PKI is bovendien gebaseerd op Europese standaarden en voldoet aan internationaal geaccepteerde richtlijnen. De huidige inrichting van het UZI-register en de UZI-middelen (het huidige UZI-stelsel[5]) schiet evenwel tekort voor grootschalig en breed gebruik in de zorgsector. De PKI-o-certificaten blijven evenwel ook in de toekomst van belang, zie hierover uitgebreider paragraaf 2.5.3.

Om te controleren of uitgegeven UZI-middelen nog geldig zijn en niet zijn ingetrokken worden er zogenaamde CRL-lijsten (Certificate Revocation List) beschikbaar gesteld aan vertrouwende partijen. Daarmee kunnen partijen die de UZI-middelen gebruiken controleren of de middelen nog geldig zijn.

2. Hoofdlijnen van het voorstel

In deze paragraaf worden de hoofdlijnen van dit wetsvoorstel toegelicht. Daarbij wordt eerst nader geschetst welke problemen bestaan bij het huidige UZI-register en de huidige middelen (paragraaf 2.1), vervolgens wordt toegelicht waarom het noodzakelijk is dit met wetgeving op te lossen en welke oplossing is gekozen (paragraaf 2.2). Daarna wordt nader ingegaan op de uitbreiding van het toepassingsbereik van het UZI-register en de bijbehorende middelen naar elektronische uitwisselingssystemen (paragraaf 2.3) en ten slotte wordt toegelicht welke inlogmiddelen in de toekomst gebruikt kunnen gaan worden (paragraaf 2.4).

2.1 Probleembeschrijving

Een uniforme en betrouwbare identificatie en authenticatie van zorg- en jeugdhulpaanbieders en hun medewerkers was altijd al van belang, maar is door de opkomst van netwerkzorg en digitalisering in toenemende mate noodzakelijk. Voor het veilig uitwisselen van gezondheidsgegevens is inloggen op het hoogste betrouwbaarheidsniveau vereist (eIDAS niveau 'hoog').[6] Echter, inloggen op het hoogste betrouwbaarheidsniveau gebeurt nauwelijks in de zorg- en jeugdhulpsector en beperkt zich vrijwel alleen tot toepassingen waar de huidige UZI-middelen worden gebruikt. In deze sectoren worden namelijk veel verschillende inlogmethoden gebruikt die vaak niet aan het vereiste betrouwbaarheidsniveau voldoen. Daarnaast worden zorg- en jeugdhulpaanbieders en hun medewerkers op verschillende manieren geïdentificeerd. Zo worden verschillende identificerende nummers gebruikt en is de zorgidentiteit van een professional niet uniform opgebouwd. Dat maakt identificatie voor elektronische gegevensuitwisseling niet interoperabel. Met interoperabiliteit wordt

[3] Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG.
[4] Het PKI-overheid-certificaat (Public Key Infrastructure) is een computerbestand dat werkt als een digitaal paspoort.
[5] Een stelsel is een geheel aan afspraken op gebied van organisatie, besturing, toezicht, beheer, architectuur, toepassingen, techniek, procedures en regels aangaande het systeem in een bepaalde vastgestelde versie.
[6] De AVG vereist technische en organisatorische maatregelen voor het beveiligen van gevoelige persoonsgegevens. Medische gegevens zijn bijzondere en geheime persoonsgegevens. Toegang tot deze gegevens moet plaatsvinden met inlogmiddelen van het hoogste, breed beschikbare betrouwbaarheidsniveau.

bedoeld: het vermogen van organisaties (en hun processen en systemen) om effectief en efficiënt gegevens uit te wisselen met hun omgeving.

Het zorg- en jeugdhulpveld[7] ziet het UZI-register als een zeer bruikbaar instrument om zorg- en jeugdhulpaanbieders en hun medewerkers uniform en uniek te identificeren, maar ervaart obstakels in het gebruik van de UZI-middelen. De UZI-middelen worden als niet flexibel, gebruiksonvriendelijk en te duur ervaren. Een UZI-pas kost 255 euro en een servercertificaat 450 euro. De UZI-middelen zijn 3 jaar geldig. Het gevolg van deze hoge kosten is dat een groot gedeelte van het zorgveld geen UZI-pas aanvraagt. Doordat uit de wet volgt dat UZI-middelen uitgegeven moeten worden door de beheerder van het register, namelijk de minister, is het niet goed mogelijk dat andere gebruiksvriendelijke inlogmiddelen aangesloten kunnen worden op het UZI-register. De huidige UZI-middelen worden dan ook niet omarmd en daarmee niet grootschalig en zorgbreed gebruikt. Het UZI-register is daarnaast niet compleet en fungeert daarmee niet als een landelijk register voor het identificeren van zorg- en jeugdhulpaanbieders en hun medewerkers. Hierdoor kan het niet bijdragen aan het veilig raadplegen van cliëntgegevens op het betrouwbaarheidsniveau hoog. Ook bestaat het risico dat UZI-passen tussen medewerkers uitgeleend worden. In dat geval gebruiken meerdere medewerkers één identiteit.

De beperkte adoptie van de UZI-pas wordt versterkt doordat de huidige UZI-pas niet gebruiksvriendelijk is en niet past binnen elk werkproces. De UZI-pas (met bijbehorende kaartlezer) werkt namelijk niet op mobiele apparaten zoals een smartphone of tablet en is daarmee niet voor ieder werkproces geschikt. Te denken valt aan zorgprocessen in de ambulancezorg en de ambulante zorg (thuiszorg) waar met mobiele apparaten gewerkt wordt. De desbetreffende zorgaanbieders kiezen in de praktijk daarom voor andere inlogmethoden. Daarnaast is het huidige UZI-stelsel niet flexibel. De zorgidentiteit van de professional in het UZI-register, bestaande uit een uniek nummer, de werkgever-werknemer relatie en de rolcode op basis van het beroep dat een professional uitoefent, wordt fysiek op de chip van de UZI-pas geprint. Als er een wijziging plaatsvindt in werkgever-werknemer relatie of beroep, is er een nieuw middel nodig. Dat brengt naast administratieve lasten ook de nodige kosten met zich mee.

Tot slot ervaart het veld de UZI-middelen gezien de inflexibiliteit en het beperkte toepassingsbereik als te duur. De kosten voor de UZI-middelen komen bovenop de kosten die voor andere inlogmethoden gemaakt worden. In de praktijk worden immers verschillende methoden van inloggen gebruikt zoals verschillende gebruiksnamen met wachtwoord, eventueel aangevuld met een tweede authenticatiefactor. Uit artikel 14 van de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (hierna: Wabvpz) en artikel 7.2.3 van de Jeugdwet volgt daarnaast dat de UZI-middelen in principe enkel gebruikt kunnen worden voor het raadplegen van SBV-Z. Dit maakt dat de dure UZI-middelen niet breed binnen de zorg gebruikt kunnen worden.

Kortom; de aanleiding voor de herziening van het huidige UZI-register en de UZI-middelen is dat de huidige inrichting van het UZI-register en de koppeling van het register aan UZI-middelen tekort schiet voor grootschalig gebruik in de zorgsector. De middelen zijn niet breed toepasbaar, niet geschikt voor mobiel gebruik en niet flexibel bij wijziging van beroep of werkgever. Daarmee zijn de middelen niet geschikt voor de invulling van de generieke functie en vormt het een obstakel voor meer en veilige digitale gegevensuitwisseling.

2.2 Doelstelling en noodzaak wetgeving

In de afgelopen jaren is gebleken dat landelijke oplossingen voor generieke functies zonder enige vorm van overheidsinterventie onvoldoende tot stand komen. Ook in dit geval is wetgeving noodzakelijk om te komen tot goede identificatie en authenticatie in de zorg. Binnen het bestaande wettelijk kader is het namelijk niet mogelijk om het toepassingsbereik van het UZI-register uit te breiden naar elektronische uitwisselingssystemen. In onder meer artikel 14 van de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (Wabvpz) is namelijk bepaald dat het UZI-

[7] Onder het zorg- en jeugdhulpveld verstaan wij zorgaanbieders, jeugdhulpaanbieders, medewerkers, koepelorganisaties, leveranciers, programma's voor gegevensuitwisseling en belanghebbende organisaties. Het veld is o.a. geconsulteerd via het Informatieberaad zorg, klankbordgroepen en expertsessies.

register bedoeld is voor het raadplegen van SBV-Z. De wet biedt geen duidelijke grondslag voor het breed gebruiken van het UZI-register voor andere toepassingen. Een dergelijke grondslag is evenwel noodzakelijk om de gegevens die vastliggen in dit register ook te gebruiken om bijvoorbeeld veilig inloggen in systemen van zorgaanbieders mogelijk te maken.

Net als de Wabvpz bevat de Jeugdwet een tweetal bepalingen, artikelen 7.2.7 en 7.2.8, op basis waarvan, kort gezegd, jeugdhulpaanbieders met een door de minister verstrekt middel toegang kunnen krijgen tot SBV-Z, waarmee het burgerservicenummer geraadpleegd kan worden. Jeugdhulpaanbieders worden hiertoe ingeschreven op een autorisatielijst. Met dit wetsvoorstel worden ook de artikelen in de Jeugdwet in lijn gebracht met de nieuwe artikelen in de Wabvpz.

Ook is het van belang dat de wet wordt gewijzigd zodat niet langer de beheerder van het register inlogmiddelen uitgeeft. Momenteel worden deze middelen uitgegeven door de minister, deze taak wordt uitgevoerd door het CIBG. Het CIBG geeft dan ook in de praktijk onder meer UZI-passen uit aan diegenen die zijn ingeschreven in het UZI-register en gerechtigd zijn de SBV-Z te raadplegen. Zoals toegelicht in paragraaf 2.1 is de UZI-pas niet geschikt voor grootschalig gebruik in de zorg. Het is dan ook van belang dat er andere middelen komen die geschikt zijn voor verschillende zorgprocessen en breed in zorg gebruikt kunnen worden. Voor de beveiliging van cliëntgegevens is het immers van belang dat gewerkt wordt met inlogmiddelen die over het juiste beveiligingsniveau beschikken. Zoals toegelicht wordt in paragraaf 2.5.1 is één van de beoogde nieuwe inlogmiddelen DigiD. Dit middel wordt uitgegeven door het ministerie van Binnenlandse zaken en koninkrijksrelaties en kan niet door het CIBG worden uitgegeven. Ook de zorgspecifieke middelen en PKI-o-certificaten worden, zoals wordt toegelicht in paragraaf 2.5.2 en 2.5.3, uitgegeven door andere partijen. Om deze middelen aan te sluiten op het UZI-register is dan ook wetswijziging nodig. Met de onderhavige wijziging worden tevens regels gesteld die borgen dat deze middelen voldoen aan het betrouwbaarheidsniveau hoog. De taak van minister wordt hierdoor beperkt tot het beheer van het UZI-register en het bewaken van de kwaliteit van de inlogmiddelen, het ontwikkelen van deze middelen wordt overgelaten aan partijen die hiervoor over de juiste expertise beschikken.

Met dit wetsvoorstel wordt dan ook mogelijk gemaakt dat:

1) Zorgaanbieders, jeugdhulpaanbieders, jeugdhulpverleners, indicatieorganen, zorgverzekeraars en hun medewerkers (ingeschrevenen) gebruik kunnen maken van inlogmiddelen op het hoogste betrouwbaarheidsniveau. Dat betreft in ieder geval onder de Wet digitale overheid (hierna: Wdo) erkende publieke en private inlogmiddelen, zorgspecifieke inlogmiddelen, PKI-o-middelen en onder de eIDAS-verordening genotificeerde middelen.
2) Het register wordt ingezet voor het verstrekken van identificerende kenmerken (attributen) ten behoeve van het digitaal identificeren van ingeschrevenen voor toegang tot onder meer uitwisselings- en zorginformatiesystemen (naast de al bestaande toegang tot de SBV-Z).

Door het mogelijk te maken met verschillende goedgekeurde middelen in te loggen ontstaat keuzevrijheid. Ingeschrevenen kunnen kiezen voor een middel dat goed in het werkproces en bij hun persoonlijke voorkeuren past. Dat kan bijvoorbeeld een pas zijn, maar ook een digitale wallet op een mobiele telefoon. Hiermee wordt het obstakel van de huidige gebruiksonvriendelijke UZI-pas die niet in ieder werkproces past weggenomen. Ook wordt het nieuwe UZI-stelsel flexibeler door het register en de middelen te ontkoppelen. Doordat de zorgidentiteit uit het UZI-register niet langer fysiek op het inlogmiddel staat, zoals dat bij de UZI-pas gebeurt, kunnen wijzigingen in het register eenvoudig doorgegeven worden zonder dat middelen ingetrokken hoeven te worden. Tot slot kunnen kosten voor identificatie en authenticatie gereduceerd worden door synergie-mogelijkheden. Verschillende systemen die zorg- en jeugdhulpaanbieders nu al gebruiken voor verschillende applicaties en toepassingen kunnen mogelijk worden geharmoniseerd op het vlak van authenticatie. Hiermee kunnen verborgen kosten van identificatie en authenticatie in allerlei systemen worden geëlimineerd.

Bezien is ook of er alternatieve oplossingsrichtingen denkbaar zijn. Eén alternatief is het niet reguleren van de digitale identiteit van de zorg- en jeugdhulpaanbieders en hun medewerkers. Dit is echter niet wenselijk, omdat daarmee geen interoperabiliteit tot stand komt en de generieke functies

identificatie en authenticatie niet optimaal ingevuld worden. Ook komt de regering daarmee niet tegemoet aan de oproep vanuit de zorgsector om actie te ondernemen vanuit de overheid en aan de gemaakte afspraken in het IZA. Een ander alternatief is dat de minister zelf nieuwe inlogmiddelen gaat ontwikkelen om de huidige UZI-middelen te vervangen. Voor dit alternatief is niet gekozen omdat er reeds andere middelen op de markt zijn of worden ontwikkeld die gebruikt kunnen worden in de zorg. Hierbij kan gedacht worden aan DigiD, maar ook aan de zorgspecifieke inlogmiddelen die momenteel worden ontwikkeld. Aangezien er reeds een ander geschikt inlogmiddel is en er naar verwachting nieuwe zorgspecifieke middelen bijkomen, is het niet langer nodig dat het de minister eigen middelen ontwikkelt. De noodzaak ontbreekt dan ook om de taak van het verstrekken van inlogmiddelen nog langer aan de minister toe te kennen. Ook ontstaat er door het niet langer vanuit de overheid aanbieden van middelen ruimte voor verschillende partijen om diverse inlogmiddelen te ontwikkelen die aansluiten bij de verschillende behoeften van het zorgveld.

De in dit wetsvoorstel gekozen oplossingsrichting is afgestemd met het zorgveld. Hiervoor zijn zorg- en jeugdhulpaanbieders, koepels, leveranciers en programma's geconsulteerd. Dat is gebeurd in het Informatieberaad Zorg (IB), klankbordgroepen, expertsessies en individuele gesprekken met het zorgveld. Ook zij zien het voordeel van verschillende erkende inlogmiddelen waarmee de zorgidentiteit van de zorgmedewerker uit het UZI-register wordt opgehaald en gebruikt wordt om toegang te verkrijgen tot onder meer elektronische uitwisselings- of zorginformatiesystemen. Deze oplossing is in samenwerking met het zorgveld tot stand gekomen en door hen goed ontvangen.[8] Met deze invulling van de generieke functies identificatie en authenticatie zal een groot gedeelte van het zorgveld naar verwachting snel overgaan tot implementatie. Met zogenaamde 'Proof of Concepts' (PoC's) is de oplossingsrichting in een testomgeving technisch beproefd. De beproefde techniek is vervolgens met pilots naar de praktijk gebracht om ervaring in het zorgveld op te doen. Hiermee wordt het zorgveld voorbereid op implementatie en kan in delen van de zorgsector vooruitlopend op grootschalige implementatie perspectief worden geboden. Daarnaast is deze aanpak van strategisch belang en noodzakelijk voor acceptatie in het zorgveld.[9] In aanloop naar grootschalige implementatie worden verschillende pilots uitgevoerd in delen van het zorgveld waarbij zorg- en jeugdhulpmedewerkers ervaring op kunnen doen met verschillende inlogmiddelen. Begin 2023 is een eerste pilot afgerond waarbij een groep artsen de mogelijkheid heeft gekregen met DigiD in te loggen via het UZI-register om toegang te verkrijgen tot een applicatie waarmee vaccinatiegegevens naar het RIVM gestuurd kunnen worden. Later in 2023 is een digitale wallet als inlogmiddel toegevoegd en kan ook toegang worden verkregen tot het Nationaal Contactpunt voor e-Health (NCPeH). Het NCPeH is een Europees netwerk waar zorgverleners onderling medische gegevens kunnen uitwisselen. Een volgende pilot is voorbereid waarbij in 2024 toegang tot de SBV-Z mogelijk zal worden via het nieuwe stelsel. Hiermee is in de praktijk beproefd of de voorgestelde oplossingsrichting werkbaar is. De deelnemende artsen hebben een positieve gebruikerservaring gedeeld.[10] Zo is aangegeven dat het gebruiksvriendelijker is en er altijd snel toegang verkregen kan worden via de app op de telefoon. Ook zorgt het beschikbaar stellen van verschillende inlogmiddelen ervoor dat er een back-up is.

2.3 Identificatie en authenticatie voor toegang tot cliëntgegevens

Zoals toegelicht in paragraaf 2.2 vloeit uit artikel 14 van de Wabvpz voort dat het UZI-register bedoeld is om het raadplegen van de SBV-Z mogelijk te maken voor diegenen die in het register zijn ingeschreven. Momenteel is er dan ook geen heldere grondslag om het UZI-register en de bijbehorende middelen te gebruiken voor het inloggen in elektronische uitwisselingssystemen. Hierdoor kunnen de huidige en nieuwe inlogmiddelen niet voldoende gebruikt worden voor toegang tot andere systemen die zorg- en jeugdhulpaanbieders gebruiken. Dit is problematisch omdat er

[8] Dat is gebeurd in het Informatieberaad Zorg (IB), klankbordgroepen, expertsessies en individuele gesprekken met het zorgveld.
[9] TNO rapport "Toekomstbestendig maken van UZI middelen" Zie hierover: https://www.gegevensuitwisselingindezorg.nl/uzi-middelen/nieuws/2022/07/05/onderzoek-tno-naar-gebruik-inlogmiddelen
[10] Zie hierover: "Succesvolle pilot met inloggen via DigiD in plaats van UZI-pas", raadpleegbaar via: https://www.uziregister.nl/actueel/nieuws/2023/03/09/succesvolle-pilot-met-inloggen-via-digid-in-plaats-van-uzi-pas.

momenteel nauwelijks andere inlogmiddelen met het betrouwbaarheidsniveau hoog voor handen zijn. In de praktijk wordt daarom nog vaak gebruik gemaakt van inlogmiddelen die beschikken over een lager betrouwbaarheidsniveau. Dit beperkt evenwel de mogelijkheden voor veilige toegang tot cliëntgegevens.

Aangezien een hoog betrouwbaarheidsniveau van groot belang is voor het beveiligen van gegevens van cliënten maakt het onderhavige wetsvoorstel daarom mogelijk dat het UZI-register en de nieuwe inlogmiddelen met het betrouwbaarheidsniveau hoog breed ingezet kunnen worden voor toegang tot elektronische uitwisselings- of zorginformatiesystemen. Daarmee kan het register en de inlogmiddelen breed in het zorgveld worden ingezet en geschikt gemaakt worden voor de invulling van de generieke functies identificatie en authenticatie. Met het wetsvoorstel wordt het UZI-register dan ook hét register voor identificerende kenmerken van zorg- en jeugdhulpaanbieders en hun medewerkers om elektronisch gegevens uit te kunnen wisselen.

Behoudens het gebruik van de SBV-Z is het aan zorg- en jeugdhulpaanbieders om te bepalen in hoeverre zij de nieuwe inlogmiddelen willen gebruiken voor eigen elektronische uitwisselingssystemen. Er is niet voor gekozen het gebruik van het UZI-register en de bijbehorende middelen verplicht te stellen voor gegevensuitwisseling of toegang tot alle uitwisselingssystemen van de zorg- en jeugdhulpaanbieders. Zij kunnen namelijk ook eigen inlogmiddelen gebruiken die over het juiste betrouwbaarheidsniveau beschikken. Het is immers in beginsel aan de zorgaanbieder te bepalen hoe hij zijn organisatie vormgeeft en op welke wijze hij voldoet aan de verplichtingen die voortvloeien uit de AVG. Daarnaast brengt een verplichting om het UZI-register en de bijbehorende middelen te gebruiken voor alle eigen elektronische uitwisselingssystemen grote lasten met zich voor zorg- en jeugdhulpaanbieders. Zij zouden dan immers alle elektronische uitwisselingssystemen die zij gebruiken verplicht moeten aanpassen voor gebruik met de nieuwe inlogmiddelen. Voor systemen waar dit niet mogelijk is zouden zij moeten overstappen naar een ander systeem. Gezien het voorgaande is ervoor gekozen zorg- en jeugdhulpaanbieders de mogelijkheid te geven de nieuwe inlogmiddelen breed te gebruiken, maar ook ruimte te laten voor de aanbieder om zelf te bepalen hoe hij borgt dat veilig ingelogd wordt in zijn eigen elektronische uitwisselingsystemen. Met dit wetsvoorstel wordt dan ook beoogd om eraan bij te dragen dat op termijn enkel cliëntgegevens geraadpleegd worden met inlogmiddelen met het betrouwbaarheidsniveau hoog.

Het wetsvoorstel stelt inlogmiddelen op het betrouwbaarheidsniveau hoog beschikbaar, neemt huidige obstakels weg en moedigt het gebruik aan. Totdat er verschillende alternatieve inlogmiddelen op het hoogste betrouwbaarheidsniveau beschikbaar zijn blijven de huidige UZI-middelen beschikbaar zodat er in ieder geval één inlogmiddel is dat voldoet aan het betrouwbaarheidsniveau hoog. De verwachting is dat het wetsvoorstel bewerkstelligt dat het zorgveld de overstap kan maken naar veilige en werkbare inlogmiddelen, zonder dat te verplichten. Vanzelfsprekend wordt de overstap gestimuleerd, gemonitord en geëvalueerd. Zo nodig kan op een later moment worden overwogen om over te gaan op verplicht gebruik van het register en de goedgekeurde middelen en daarmee inlogmiddelen te gebruiken met betrouwbaarheidsniveau eIDAS hoog, indien blijkt dat zorg- en jeugdhulpaanbieders niet zelf de overstap maken naar veilige inlogmiddelen.

Als zorg- en jeugdhulpaanbieders besluiten gebruik te maken van het register en de bijbehorende middelen, geldt er een acceptatieplicht van alle goedgekeurde inlogmiddelen. Keuzevrijheid voor inlogmiddelen is een belangrijk uitgangspunt bij het wetsvoorstel. De gedachte is dat zorg-jeugdhulpaanbieders en hun medewerkers kunnen kiezen voor een middel dat past bij het werkproces en persoonlijke voorkeuren. Dat middel moet dan ook overal te gebruiken zijn; zorginformatie- en uitwisselingssystemen zouden niet moeten afdwingen één bepaald middel te gebruiken. Hiermee wordt een mogelijke 'vendor lock-in' beperkt en kan de zorg- of jeugdhulpaanbieder niet volledig afhankelijk worden gemaakt van één leverancier. Daarnaast wordt interoperabiliteit gewaarborgd en wordt voorkomen dat een medewerker een sleutelbos met veel verschillende inlogmiddelen nodig heeft om cliëntgegevens in te kunnen zien en uit te wisselen. Het CIBG zal zorg- en jeugdhulpaanbieders, namens de minister, voorzien van een gestandaardiseerd koppelvlak waarmee alle goedgekeurde inlogmiddelen beschikbaar komen. Hiermee ontzorgt het CIBG het veld. Door op het koppelvlak van het CIBG aan te sluiten wordt voldaan aan de

acceptatieplicht. Daarmee komen in de basis alle goedgekeurde middelen beschikbaar, maar niet eventueel vereiste randapparatuur om deze te kunnen gebruiken. Het is niet verplicht om eventueel benodigde hardware of randapparatuur zoals kaartlezers of mobiele telefoons te faciliteren. De zorg- of jeugdhulpaanbieder kan wat dat betreft kiezen voor een specifiek middel.

Ook met de nieuwe inlogmiddelen blijft digitaal ondertekenen en verzegelen mogelijk. Met alle goedgekeurde inlogmiddelen kan een gekwalificeerde digitale handtekening worden gezet.

2.4 Medewerkers registeren in het UZI-register

Met dit wetsvoorstel kunnen medewerkers van zorg- en jeugdhulpaanbieders zich laagdrempelig inschrijven in het UZI-register. Met medewerker wordt eenieder bedoeld die werkzaam is of wil zijn in de zorg of jeugdhulp en daarbij cliëntgegevens verwerkt. Om een UZI-nummer te verkrijgen wordt een hoog betrouwbare koppeling gemaakt met het BSN van de medewerker. Het besluit om toegang te verlenen (autorisatie) is een verantwoordelijkheid van de zorg- of jeugdhulpaanbieder. Doorgaans kan met alleen een UZI-nummer geen toegang tot medische gegevens verkregen worden. Daarvoor zijn aanvullende kenmerken (attributen) nodig. Aanvullende (autorisatie)kenmerken (zoals bevoegdheden vanuit de wet BIG) worden met grote zorgvuldigheid toegekend. Nadat een zorg- of jeugdhulpmedewerker is ingeschreven verifieert de zorg- of jeugdhulpaanbieder of de medewerker bij hem werkzaam is en of hij toegang moet kunnen krijgen tot SBV-Z of andere elektronische uitwisselingssystemen die de zorg- of jeugdhulpaanbieder gebruikt. Er is dus nadrukkelijk een extra handeling van de zorg- of jeugdhulpaanbieder noodzakelijk alvorens een medewerker toegang kan krijgen tot de SBV-Z. Louter de inschrijving in het UZI-register is niet voldoende om cliëntgegevens te kunnen raadplegen, die toegang moet verstrekt worden door de werkgever van de medewerker, namelijk de zorg- of jeugdhulpaanbieder. Het is van belang dat de medewerker desgewenst continue ingeschreven kan staan in het UZI-register. Het is dan namelijk niet nodig dat hij zich telkens opnieuw inschrijft als hij van baan wisselt of even niet werkzaam is in de zorg. De nieuwe zorg- of jeugdhulpaanbieder waar de medewerker voor gaat werken, kan vervolgens immers aangeven dat de medewerker die reeds staat ingeschreven bijvoorbeeld toegang moet krijgen tot de SBV-Z of bepaalde eigen elektronische uitwisselingssystemen. Een voortdurende inschrijving voorkomt dan ook administratieve lasten voor de medewerker.

Laagdrempelige inschrijving van medewerkers is tevens van belang omdat dit eraan bijdraagt dat de bijbehorende veilige inlogmiddelen gebruikt kunnen worden door deze professionals. Het is van belang dat alle medewerkers die bijvoorbeeld de SBV-Z moeten raadplegen dit doen met hun eigen inlogmiddelen en niet bijvoorbeeld met een geleend middel van een ander. Het is immers van belang dat enkel diegenen die hiertoe gerechtigd zijn cliëntgegevens kunnen raadplegen. Dit wordt geborgd met persoonsgebonden inlogmiddelen waarmee geverifieerd wordt of diegene die inlogt in een systeem ook gerechtigd is om het betreffende systeem te raadplegen. Om te borgen dat alle zorgmedewerkers veilig kunnen inloggen met een eigen inlogmiddel wordt dan ook met dit wetsvoorstel mogelijk gemaakt dat zij zich laagdrempelig kunnen inschrijven in het UZI-register en vervolgens laagdrempelig een veilig inlogmiddel met het betrouwbaarheidsniveau hoog kunnen gebruiken. Dit draagt bij aan het veilig digitaal toegankelijk maken van cliëntgegevens.

Net als met de huidige verstrekking van CRL-lijsten (Certificate Revocation List), waarmee vertrouwende partijen kunnen controleren of uitgegeven middelen nog geldig zijn, moeten vertrouwende partijen kunnen blijven controleren of de registraties in het register nog actueel zijn. Daarom worden vanuit het register lijsten ter beschikking gesteld met registraties die niet meer actueel zijn. Het gaat om een beperkt aantal gegevens die gehasht zijn. Het hashen van deze gegevens betekent dat ze in een onbegrijpelijke reeks tekens worden omgezet.

2.5 Inlogmiddelen met het betrouwbaarheidsniveau hoog

Het wetsvoorstel voorziet in het gebruik van (verschillende) goedgekeurde inlogmiddelen op het betrouwbaarheidsniveau hoog. Hiermee wordt geborgd dat gezondheidsgegevens van cliënten veilig geraadpleegd kunnen worden. Alvorens een inlogmiddel aangesloten kan worden op het UZI-register moet het middel door de Minister worden goedgekeurd. Tot goedkeuring wordt overgegaan als

aangetoond kan worden dat het betreffende middel beschikt over het vereiste betrouwbaarheidsniveau. Dit kan aangetoond worden door het overleggen van een bewijsmiddel. Beoogd wordt om bij of krachtens algemene maatregel van bestuur te bepalen dat in ieder geval vier verschillende bewijsmiddelen kunnen leiden tot goedkeuring van een inlogmiddel, namelijk erkenning onder de Wdo, certificering op basis van de NEN 7518[11] van zorgspecifieke middelen, een PKI-o-certificering en een door Europa erkend middel (genotificeerd) onder de eIDAS-verordening. Hierdoor zullen via verschillende wegen verschillende middelen goedgekeurd kunnen worden die allen beschikken over het betrouwbaarheidsniveau hoog, en wat betreft techniek kunnen aansluiten op de werkprocessen en persoonlijke voorkeuren van gebruikers.

Zoals hiervoor al benoemd kan een inlogmiddel enkel op het UZI-register aangesloten worden indien met een bewijsmiddel aangetoond kan worden dat met dit middel ingelogd kan worden op betrouwbaarheidsniveau hoog. Voor de aansluiting van het middel op het register wordt goedkeuring verleend door de minister. In de praktijk zal deze taak gemandateerd worden aan het CIBG. Een verstrekker van een inlogmiddel kan bij de minister een aanvraag indienen om voor goedkeuring in aanmerking te komen. Die aanvraag dient vergezeld te gaan van een bewijsmiddel en bij of krachtens algemene maatregel van bestuur aangewezen bescheiden aan de hand waarvan bepaald kan worden dat het inlogmiddel beschikt over het juiste betrouwbaarheidsniveau. Beoogd is dat als een inlogmiddel beschikt over erkenning onder de Wdo, certificering op basis van de NEN 7518, leverancier is van PKI-o-certificaten of Europees genotificeerd is, dit middel goedgekeurd kan worden voor gebruik in de zorg. Met deze bewijsmiddelen kan namelijk genoegzaam aangetoond worden dat het middel voldoet aan het hoogste betrouwbaarheidsniveau. De minister gaat dan ook in beginsel niet zelf nogmaals onderzoek doen naar het middel. Over de aanvraag tot goedkeuring worden bij of krachtens algemene maatregel van bestuur nadere regels gesteld. Ook is het mogelijk om in de toekomst bij algemene maatregel van bestuur andere bewijsmiddelen op te nemen aan de hand waarvan een inlogmiddel goedgekeurd kan worden.

Met de invoering van deze nieuwe inlogmiddelen, zal het CIBG niet langer namens de minister UZI-middelen hoeven te verstrekken. Het CIBG gaat kan dan ook terug naar haar kerntaak van registerhouder en stopt met het uitgeven van UZI-passen en servercertificaten. Daarmee fungeert het CIBG niet meer als Trusted Service Provider (hierna: TSP). De afgifte van inlogmiddelen wordt overgelaten aan publieke en private leveranciers van middelen. In de volgende paragrafen wordt uitgebreider ingegaan op de verschillende middelen.

2.5.1 Wdo erkende inlogmiddelen

De Wdo regelt dat Nederlandse burgers en bedrijven veilig en betrouwbaar kunnen inloggen bij de (semi-)overheid. Daarmee wordt bedoeld dat burgers elektronische identificatiemiddelen (eID) krijgen met een substantiële of hoge mate van betrouwbaarheid. Deze identificatiemiddelen geven publieke dienstverleners meer zekerheid over iemands identiteit. De Wdo biedt hiertoe grondslagen voor de verwerking van persoonsgegevens in het authenticatieproces bij het geven van de digitale toegang, waaronder het burgerservicenummer.[12] Met de Wdo wordt ruimte gecreëerd om onder strikte voorwaarden een publiek identificatiemiddel ter uitoefening van een private taak te gebruiken. In de zorg- en jeugdhulpsector gaat het concreet om het gebruik van DigiD voor de identificatie en authenticatie van medewerkers. Voor het gebruik van dit publieke inlogmiddel biedt de Wdo een juridische grondslag. De Wdo biedt geen juridische grondslag voor het gebruik van een onder de Wdo erkend privaat inlogmiddel voor de identificatie en authenticatie van medewerkers. Met het onderhavige wetsvoorstel wordt dit opgelost. Het wordt hierdoor mogelijk dat publieke Wdo-middelen, namelijk DigiD, en private Wdo-middelen in de zorg gebruikt kunnen worden om veilig in te loggen om gegevens van cliënten te raadplegen of uit te wisselen. Hiertoe moet de minister het

[11] NEN 7518 identificatie en authenticatie EGIZ
[12] Ter verduidelijking: Wdo erkende inlogmiddelen genereren een BSN. Het BSN wordt niet gebruikt om natuurlijke personen te identificeren voor toegang tot uitwisselingssystemen of zorginformatiesystemen. Met het BSN kan de zorgidentiteit (wie ben je?: UZI-nummer, waar werk je?: URA-nummer en wat zijn je bevoegdheden?: rolcode) uit het UZI-register opgehaald worden.

middel goedkeuren. Aangezien deze middelen reeds onder de Wdo erkend zijn als middel kan de minister desgewenst direct overgaan tot goedkeuring.

2.5.2 Zorgspecifieke inlogmiddelen (gecertificeerd op basis van de NEN 7518)

Gezien de grote diversiteit aan zorg en jeugdhulp die in Nederland verleend wordt, is het van belang dat er verschillende zorgspecifieke middelen beschikbaar komen die identificatie en authenticatie van medewerkers in verschillende werkomgevingen mogelijk maakt. Een verpleegkundige die werkt op een ambulance stelt andere eisen aan een inlogmiddel dan een tandarts die in een eigen praktijk werkzaam is. Om de verschillende behoeften in het veld te kunnen dekken zijn verschillende middelen nodig. In zorgprocessen binnen instellingen kan bijvoorbeeld een pas goed werken, maar in de thuiszorg is een digitale wallet op een mobiele telefoon beter werkbaar. Gezien de specifieke behoeften van het veld, zullen de middelen die onder de Wdo beschikbaar komen niet in alle gevallen uitkomst bieden.

Met dit wetsvoorstel wordt daarom mogelijk gemaakt dat, naast de Wdo-middelen, ook zorgspecifieke middelen erkend kunnen worden om te gebruiken voor toegang tot de SBV-Z. Een zorgspecifiek middel is een elektronisch middel voor identificatie en authenticatie, dat onder de verantwoordelijkheid van de zorg- of jeugdhulpaanbieder wordt uitgereikt aan zijn medewerkers.

De zorgspecifieke middelen voldoen op onderdelen niet aan de eisen vanuit de Wdo aan de middelen worden gesteld. Zorgspecifieke middelen zullen dus niet onder de Wdo erkend (kunnen) worden. Zo is de toepasbaarheid van de zorgspecifieke middelen beperkt tot de zorg door het gebruik van het UZI-nummer als identificerend nummer. Daardoor is het middel niet breed bruikbaar bij de organisaties die onder het regime van de Wdo vallen (zoals een gemeente of de Belastingdienst) en het BSN als identificerend nummer hanteren. Daarbij komt dat niet iedere Nederlander een zorgspecifiek middel kan krijgen: de uitgifte van de zorgspecifieke middelen is beperkt tot diegenen die staan ingeschreven in het UZI-register en daarbij werkzaam zijn voor een zorg- of jeugdhulpaanbieder. De Wdo vereist evenwel dat private middelen voor eenieder beschikbaar gesteld kunnen worden. Aangaande het betrouwbaarheidsniveau zullen dezelfde strenge eisen worden gesteld aan zorgspecifieke middelen als aan de Wdo-middelen.

Een groot deel van het zorgveld maakt reeds gebruik van zorgspecifieke middelen, zoals bijvoorbeeld een ziekenhuispas. Uit gesprekken met het veld is gebleken dat zij ook in de toekomst van deze zorgspecifieke middelen gebruik willen blijven maken. Medewerkers werken namelijk met een veelheid aan applicaties en op verschillende soorten apparaten (bv PC, laptop, tablet, smartphone). Voor al deze applicaties moet een bruikbaar en gebruiksvriendelijk inlogmiddel komen dat gebruikt kan worden op al deze apparaten. De inzet van zorgspecifieke middelen kan bijdragen aan de realisatie hiervan. Het inzetten van de zorgspecifieke middelen, naast de Europees genotificeerde middelen, Wdo-middelen en de PKI-o-certificaten, heeft een aantal voordelen.

Ten eerste sluiten de zorgspecifieke middelen goed aan bij bestaande werkprocessen. In het ziekenhuis is een ziekenhuispas bijvoorbeeld een geschikt inlogmiddel. Deze pas voldoet bijvoorbeeld aan daar geldende eisen omtrent hygiëne in de steriele OK-omgeving, is ook bruikbaar in de nabijheid van een MRI-scanner (inloggen op de telefoon kan hier bijvoorbeeld niet in verband met straling) en kunnen hier ook deuren mee worden geopend. Daarnaast kan de patiënt de arts met een pas herkennen aan de pasfoto en naam op de pas. Een ziekenhuispas is dan ook een voorbeeld van een zorgspecifiek middel dat bijzonder geschikt is voor gebruik in een bepaalde zorgomgeving. In de tweede plaats is het van belang dat er een set aan diverse authenticatiemiddelen beschikbaar komt voor medewerkers. Hoe meer verschillende authenticatiemiddelen kunnen worden ingezet, hoe meer keuzevrijheid en adaptatie van de oplossingsrichting in het zorgveld. Ten derde kunnen medewerkers blijven werken met de zorgspecifieke middelen waarmee zij nu al inloggen, mits deze aan het betrouwbaarheidsniveau hoog voldoen. Deze middelen moeten overigens wel eerste worden goedgekeurd door de minister aan de hand van een certificaat.

<u>Certificering en goedkeuring van zorgspecifieke middelen</u>

Zoals hiervoor toegelicht is het van belang dat, naast de Europees genotificeerde middelen, Wdo-middelen en PKI-o-certifcaten, ook zorgspecifieke middelen gekoppeld kunnen worden aan het UZI-register. Om een zorgspecifiek middel te koppelen moet het door de minister goedgekeurd worden, wat mogelijk is als het middel voldoet aan de eisen die worden gesteld door de NEN 7518. Bij zorgspecifieke middelen moet dit worden aangetoond aan de hand van een certificering op basis van NEN 7518. Het certificaat dat hiermee verkregen wordt fungeert als bewijsmiddel op basis waarvan de minister het middel kan goedkeuren zodat aangesloten kan worden op het UZI-register.

Om middels certificering voor goedkeuring in aanmerking te komen doorlopen zorgspecifieke middelen de normale werkwijze van certificering aan de hand van een NEN-norm. Daarbij wordt door een NEN-werkgroep een norm en bijbehorend certificeringsschema opgesteld, vervolgens kunnen door de Raad voor Accreditatie (hierna: RvA) certificerende instellingen (hierna: CI's) worden geaccrediteerd om inlogmiddelen te mogen certificeren. In het certificeringsschema van de NEN 7518 is beschreven aan welke eisen certificerende instellingen moeten voldoen om aan de hand van deze norm te certificeren en welk proces certificerende instellingen moeten doorlopen om door de RvA geaccrediteerd te worden.

Om voor goedkeuring in aanmerking te komen moet het certificaat van een zorgspecifiek middel zijn verstrekt door een CI die door de RvA is geaccrediteerd. Het is dan ook van belang dat de RvA beoordeelt welke CI's gerechtigd zijn de certificering voor de zorgspecifieke middelen uit te voeren. Hiermee wordt geborgd dat enkel CI's die over de juiste kennis beschikken zorgspecifieke middelen kunnen certificeren. De door de RvA geaccrediteerde CI's beoordelen uiteindelijk of de zorgspecifieke authenticatiemiddelen voldoen aan deze NEN-norm. Bij een positieve beoordeling ontvangt een product of organisatie een certificaat.

Bij of krachtens algemene maatregel van bestuur worden regels gesteld waaraan een certificaat moet voldoen om voor goedkeuring van de minister in aanmerking te komen. Met deze goedkeuring kan het inlogmiddel gebruikmaken van het UZI-register. Deze regels zien onder meer toe op welke versie van de NEN 7518 de zorgspecifieke middelen moeten voldoen, de informatie die de minister moet hebben om over te gaan tot goedkeuring van het middel, de gevolgen van vrijwillige of gedwongen beëindiging van de werkzaamheden van een certificerende instelling, de duur van geldigheid van het certificaat en tussentijdse controles.

<u>Certificering in twee rollen</u>

In de NEN 7518 is vastgelegd aan welke eisen de middelen moeten voldoen voor de kwalificatie op het hoogste betrouwbaarheidsniveau. Hierbij wordt inhoudelijk zoveel als mogelijk aangesloten bij, en verwezen naar, de eisen uit de eIDAS-verordening en de Wdo. De eisen aangaande het betrouwbaarheidsniveau hebben zowel betrekking op de techniek van het authenticatiemiddel als op de identificatie van de medewerker, het registratie- en beheerproces van deze (digitale) identiteit en de uitgifte van het zorgspecifieke middel aan een medewerker. Het is namelijk van belang dat de koppeling van een middel aan een gebruiker zorgvuldig en op de juiste wijze wordt uitgevoerd. Zonder een valide koppeling van het middel aan de gebruiker zou iemand die niet gerechtigd hiertoe is over een middel kunnen beschikken en daarmee bepaalde systemen kunnen raadplegen. Om een middel op het betrouwbaarheidsniveau hoog te certificeren worden daarom ook hoge eisen gesteld aan de koppeling van het middel aan de gebruiker. Bij deze koppeling wordt het BSN van de gebruiker eenmalig verwerkt om te verifiëren dat de identiteit van de gebruiker overeenkomt met de UZI-registratie. Op het gebruik van dit persoonsgegeven wordt dieper ingegaan in paragraaf 6.

Op basis van de NEN 7518 kunnen partijen voor twee rollen worden gecertificeerd. Ten eerste voor de rol van leverancier van het inlogmiddel. Dit is de partij die de techniek voor het inlogmiddel levert. De partij wordt er hoofdzakelijk op beoordeeld of de techniek aan de juiste betrouwbaarheidseisen voldoet en of de partij voldoet aan eisen die worden gesteld aan technische interoperabiliteit. Ten tweede kan een partij worden erkend in de rol van middelenuitgever. In deze rol wordt beoordeeld of de partij die het middel uitreikt dit op een juiste manier doet. De eisen voor deze rol hebben betrekking op de identificatie van de medewerker, het registratie- en beheerproces van deze (digitale) identiteit en de uitgifte van het zorgspecifieke middel aan een zorgmedewerker.

Ter illustratie een voorbeeld van een zorgaanbieder die wil gaan werken met een zorgspecifiek middel. Eerst zal de zorgaanbieder een middel inkopen, of zelf ontwikkelen, dat gecertificeerd moet wordenop het onderdeel 'leverancier van het authenticatiemiddel'. Vervolgens is het aan de zorgaanbieder in de rol van middelenuitgever om te borgen dat onder andere de uitgifte van het middel volgens de NEN-norm 7518 wordt uitgevoerd. Ook op het uitgifteproces moet een certificering plaatsvinden. Als dit is gebeurd, kan het middel worden aangesloten op het UZI-register en worden ingezet voor identificatie en authenticatie in de zorg. Het is ook mogelijk dat een andere partij dan een zorgaanbieder de uitgifte van het middel uitvoert zoals een koepelorganisatie onder verantwoordelijkheid van een groep zorgaanbieders.

2.5.3 PKI-o-certificaten

Het UZI-register koppelt de fysieke identiteit van een zorg- of jeugdhulpmedewerker aan een elektronische identiteit en legt deze vast in een certificaat. Deze certificaten worden aan natuurlijke personen en systemen uitgegeven en werkt op basis van de PKI-o technologie/standaard. Het CIBG (UZI-register) vervult hiermee in de huidige situatie de rol van Trusted Service Provider (TSP).

Op termijn zal het CIBG geen UZI-middelen meer uitgeven en de huidige middelen uitfaseren. Dat betekent niet dat PKI-o middelen niet bruikbaar zijn voor elektronische gegevensuitwisseling in de zorg. De PKI-o servercertificaten kunnen gebruikt blijven worden maar zullen in de toekomst uitgegeven worden door andere TSP's. Deze TSP's moeten voldoen aan strenge eisen om PKI-o servercertificaten uit te mogen geven. Hierop vinden op verschillende momenten in het jaar audits plaats. Dat maakt het een hoogwaardig en betrouwbaar certificaat. Het is bovendien gebaseerd op Europese standaarden en voldoet aan internationaal geaccepteerde richtlijnen.

2.5.4 Onder de eIDAS-verordening genotificeerde inlogmiddelen

Europese (eIDAS genotificeerde) middelen die aan het hoogste betrouwbaarheidsniveau voldoen zijn in de basis geschikt om te gebruiken in combinatie met het UZI-register. Om een zorgidentiteit uit het register op te kunnen halen is het evenwel noodzakelijk dat het gebruikte Europese middel een (versleuteld) BSN kan ontsluiten. Dat betekent dat de gebruiker die dat Europese middel gebruikt, in een eerder stadium een BSN door de Nederlandse overheid moet zijn toegekend.

Het BSN is de sleutel om via het UZI-register een identiteit te verkrijgen. Voor middelen die onder de Wdo worden erkend en voor zorgspecifieke middelen is een grondslag gecreëerd om een BSN te verwerken. Dat geldt niet voor eIDAS genotificeerde middelen: deze middelen leveren een ander identificerend kenmerk (de 'PersonIdentifier') dat door de lidstaat is toegekend. In sommige gevallen kan dit Europese identificerende nummer worden omgezet in een BSN. Daarbij zijn het Nederlandse nationale eIDAS-knooppunt en het BSN-koppelregister betrokken. Als er een relatie bestaat tussen het Europese identificerende kenmerk en een BSN, dan levert het eIDAS-knooppunt in de authenticatieverklaring het (versleutelde) BSN aan dat gerelateerd is aan het Europese middel dat is gebruikt voor de authenticatie.

3. Verhouding tot hoger recht

In deze paragraaf wordt toegelicht hoe dit wetsvoorstel zich verhoudt tot het hoger recht. Hiertoe wordt eerst ingegaan op de eIDAS-verordening (paragraaf 3.1) en vervolgens wordt ingegaan op het vrij verkeer van diensten en goederen (paragraaf 3.2). Dit wetsvoorstel raakt daarnaast aan de Algemene verordening gegevensbescherming (AVG). Op de verwerking van gegevens en de relatie met de AVG wordt separaat ingegaan in paragraaf 6.

3.1 eIDAS-verordening

Met dit wetsvoorstel wordt voor wat betreft het betrouwbaarheidsniveau van inlogmiddelen aangesloten bij het betrouwbaarheidsniveau hoog, zoals vastgelegd in artikel 8, derde lid, van de eIDAS-verordening. Hiermee is geregeld dat de inlogmiddelen een hoge mate van vertrouwen moeten bieden in iemands identiteit. Waar een dergelijk inlogmiddel precies aan moet voldoen is nader uitgewerkt in de Uitvoeringsverordening betrouwbaarheidsniveaus. In deze verordening zijn de minimale technische specificaties en procedures voor de verschillende betrouwbaarheidsniveaus

vastgelegd. Zoals uitgebreider toegelicht in paragraaf 2 kan aan de hand van verschillende bewijsmiddelen aangetoond worden dat een inlogmiddel voldoet aan het betrouwbaarheidsniveau hoog.

Met de eIDAS-verordening wordt onder meer beoogd te regelen dat burgers en bedrijven met hun nationale elektronische identificatiesystemen, zoals in Nederland DigiD, kunnen inloggen bij diensten van openbare instanties in andere lidstaten. Nederlandse regels hierover worden vastgesteld in de Wdo, zie hierover uitgebreider paragraaf 4.2. De Nederlandse en buitenlandse middelen die onder de Wdo zijn erkend kunnen eveneens goedgekeurd worden voor gebruik in combinatie met het UZI-register.

3.2 Verhouding tot het vrij verkeer van goederen en diensten

De eisen aan inlogmiddelen die met dit wetsvoorstel worden gesteld raken aan het vrij verkeer van goederen en diensten. Uit het wetsvoorstel vloeit namelijk voort dat een inlogmiddel enkel aangesloten kan worden op het UZI-register, en aldus gebruikt kan worden voor het raadplegen van SBV-Z, als dit middel voldoet aan het betrouwbaarheidsniveau hoog. Voor het betrouwbaarheidsniveau hoog is gekozen in aansluiting met de AVG. Uit artikel 5, eerste lid, onder f, van de AVG vloeit namelijk voort dat persoonsgegevens passend beveiligd moeten worden. Voor wat betreft het raadplegen van SBV-Z – en in het verlengde het BSN van cliënten – is dit het betrouwbaarheidsniveau hoog.

Het betrouwbaarheidsniveau hoog borgt ook dat veilige uitwisseling van medische gegevens kan plaatsvinden. Het met dit wetsvoorstel stellen van eisen aan inlogmiddelen gebeurt dan ook in het kader van de bescherming van de gezondheid van personen. Zoals reeds toegelicht is in paragraaf 1 kan zonder veilige uitwisseling van gegevens namelijk niet gekomen worden tot goede zorg. De eis dat een inlogmiddel moet voldoen het betrouwbaarheidsniveau hoog is, mede in het licht van de AVG en de eIDAS-verordening, dan ook proportioneel. Ook is aan het beginsel van subsidiariteit voldaan. Zoals toegelicht in paragraaf 2.2 zijn andere mogelijkheden gezocht om te komen tot een veilige manier van inlogmiddelen, maar zijn die mogelijkheden niet werkbaar gebleken. Ten slotte is van belang dat niet dwingend of exclusief wordt voorgeschreven op welke wijze aangetoond kan worden dat een inlogmiddel voldoet aan het betrouwbaarheidsniveau hoog. Ook wordt geen onderscheid gemaakt naar afkomst van het betreffende middel. Er wordt beoogd om bij of krachtens algemene maatregel van bestuur verschillende bewijsmiddelen aan te wijzen op grond waarvan aangetoond kan worden dat een middel voldoet aan het betrouwbaarheidsniveau, waaronder middelen uit een andere lidstaat die onder de Wdo zijn erkend.

4. Verhouding tot nationale wetgeving

Met dit wetsvoorstel wordt de Wabvpz en de Jeugdwet aangepast. Deze wijziging raakt daarnaast aan de Wdo en de Wet elektronische gegevensuitwisseling in de zorg (hierna: Wegiz). Op de verhouding van het onderhavige wetsvoorstel met deze drie wetten wordt hierna achtereenvolgend ingegaan.

4.1 Aanpassing Wabvpz en Jeugdwet

Het onderhavige wetsvoorstel vervangt hoofdstuk 3 van de Wabvpz over de registers van zorgaanbieders, indicatieorganen en zorgverzekeraars en wijzigt artikel 7.2.7 en 7.2.8 van de Jeugdwet. Deze registers zijn ingesteld zodat zorg- en jeugdhulpaanbieders – via de SBV-Z – het BSN van de cliënt kunnen raadplegen (artikel 14, eerste lid, Wabvpz en 7.2.7 van de Jeugdwet). Hiertoe worden door de beheerder van het register inlogmiddelen en servercertificaten verstrekt aan diegenen die in het register zijn ingeschreven (artikel 15, derde lid, Wabvpz en 7.2.8, derde lid, van de Jeugdwet). Op grond van dit wetsvoorstel worden deze middelen en certificaten niet langer verstrekt door de beheerder. Een ingeschrevene kan in plaats daarvan gebruik gaan maken van goedgekeurde identificatiemiddelen met een hoog beveiligingsniveau.

Met dit wetsvoorstel wordt tevens het doel van het register van zorgaanbieders uitgebreid. Dit register wordt op grond van dit wetsvoorstel tevens ingesteld met het oog op de identificatie en authenticatie van zorgaanbieders en zorgmedewerkers ten behoeve van elektronische

gegevensuitwisseling in de zorg. Zoals toegelicht in paragraaf 2.2 wordt hiermee bewerkstelligd dat de identificatiemiddelen met het betrouwbaarheidsniveau hoog ook gebruikt kunnen worden om veilig cliëntgegevens te raadplegen via andere systemen van de zorgaanbieder. Om dit te bewerkstelligen kunnen in vervolg ook zorgmedewerkers die werkzaam zijn voor een zorgaanbieder zich in het register laten inschrijven. Van de gelegenheid is ten slotte gebruik gemaakt om het nieuwe hoofdstuk 3 van de Wabvpz en de artikelen 7.2.7 en 7.2.8 van de Jeugdwet redactioneel te verbeteren. Gezien de hiervoor beschreven wijzigingen in de Wabvpz, moeten ook het Besluit gebruik burgerservicenummer in de zorg, Besluit elektronische gegevensverwerking door zorgaanbieders, het Besluit Jeugdwet en de Regeling gebruik burgerservicenummer in de zorg gewijzigd worden om deze regelgeving met dit wetsvoorstel in lijn te brengen.

4.2 Verhouding met de Wdo

Met de Wdo wordt de basis gelegd voor een generieke digitale infrastructuur in het publieke domein.[13] Hiertoe wordt onder meer gefaciliteerd dat een inlogmiddel, zoals DigiD, dat voldoet aan een hoog betrouwbaarheidsniveau, gebruikt kan worden ter identificatie bij bestuursorganen of aangewezen organisaties om zo toegang krijgen tot hun dienstverlening. Op grond van artikel 2, tweede lid, onder a, in verbinding met de bijlage van de Wdo, zijn zorgaanbieders, indicatieorganen, en zorgverzekeraars die vallen onder Wabvpz reeds aangewezen organisaties voor het raadplegen van het BSN door middel van de SBV-Z.

Met dit wetsvoorstel wordt het daarnaast voor zorg- en jeugdhulpaanbieders en hun medewerkers mogelijk om bepaalde cliëntgegevens te raadplegen met een goedgekeurd inlogmiddel met het betrouwbaarheidsniveau hoog. Dit kan een middel zijn dat als zodanig is erkend onder de Wdo. De onderhavige wet biedt Onze Minister namelijk de mogelijkheid om inlogmiddelen goed te keuren als ten aanzien van deze middelen met een bewijsmiddel aangetoond kan worden dat dit middel over het betrouwbaarheidsniveau hoog beschikt. Beoogd wordt om bij of krachtens algemene maatregel van bestuur te bepalen dat een erkenning onder de Wdo een dergelijk bewijsmiddel is. Wdo-middelen kunnen dan ook gebruikt worden door zorgaanbieders, zorgmedewerkers, indicatieorganen en zorgverzekeraars om onder meer SBV-Z te raadplegen. Daarnaast kunnen zorgaanbieders en zorgmedewerkers Wdo-middelen breed gebruiken om veilig cliëntgegevens te raadplegen.

4.3 Verhouding met de Wegiz

Met de Wegiz is beoogd te komen tot volledige interoperabiliteit als het gaat om elektronische gegevensuitwisseling tussen zorgverleners[14] aan de hand van eenduidige eisen aan taal en techniek. Dit doel wordt mede bereikt door het inzetten van certificering van informatieproducten en -diensten door certificerende instellingen aan de hand van NEN-normen. Met dit wetsvoorstel worden, anders dan onder de Wegiz, inlogmiddelen niet exclusief verplicht om aan een NEN-norm te voldoen. Wel wordt beoogd om bij of krachtens algemene maatregel van bestuur te bepalen dat een identificatiemiddel goedgekeurd kan worden als dit middel onder meer beschikt over een certificaat van een certificerende instelling waaruit blijkt dat dit middel voldoet aan de NEN 7518. Anders dan in de Wegiz wordt niet exclusief voorgeschreven dat een middel enkel voldoet als aan deze norm wordt voldaan. Er zijn namelijk andere mogelijkheden voorhanden aan de hand waarvan aangetoond kan worden dat een middel voldoet aan het betrouwbaarheidsniveau hoog. Het is daarnaast voor veilige uitwisseling van gegevens van een cliënt niet noodzakelijk dat de te gebruiken identificatiemiddelen voldoen aan dezelfde NEN-norm, maar enkel dat het betrouwbaarheidsniveau hoog bereikt is. Om onnodige administratieve lasten tegen te gaan kunnen identificatiemiddelen die onder de Wdo of het PKI-overheidsstelsel zijn erkend, ook door Onze minister goedgekeurd worden voor gebruik in de zorg. Bij de goedkeuring van een inlogmiddel aan de hand van een bewijsmiddel van een certificerende instelling op basis van de NEN 7518 wordt waar mogelijk aangesloten worden bij de Wegiz.

[13] Kamerstukken II 2017/18, 34 972, nr. 3, p. 1.
[14] De Wegiz is van toepassing op zorgverleners als bedoeld in artikel 1, eerste lid, van de Wet kwaliteit, klachten en geschillen zorg en derhalve niet van toepassing op jeugdhulpverleners.

5. Toezicht en handhaving

Met het wetsvoorstel Verzamelwetgegevens II wordt het toezicht van de inspectie Volksgezondheid en jeugd (hierna: Inspectie) op de Wabvpz verduidelijkt. Hiertoe wordt expliciet bepaald dat de Inspectie toezicht kan houden en zo nodig handhavend kan optreden bij overtreding van delen van de Wabvpz. In het uiterste geval kan de Inspectie een herstelsanctie opleggen, namelijk een schriftelijke aanwijzing, schriftelijk bevel of een last onder dwangsom. Met het onderhavige wetsvoorstel wordt het toezicht- en handhavingsinstrumentarium van de Inspectie uitgebreid ten aanzien van de intrekking of schorsing van identificatiemiddelen met het betrouwbaarheidsniveau hoog.

Op grond van het nieuwe artikel 14a Wabvpz kan de minister goedkeuring verlenen aan een identificatiemiddel, indien dit middel voldoet aan het betrouwbaarheidsniveau hoog. Hiermee wordt geborgd dat gegevens van cliënten veilig geraadpleegd worden en wordt invulling gegeven aan de stelselverantwoordelijkheid van de minister. Zoals uitgebreider toegelicht in paragraaf 2.5 kan met een bewijsmiddel zoals een Wdo-erkenning, certificaat van een certificerende instelling verstrekt op basis van de NEN 7518, een PKI-overheidscertificaat of Europese notificatie aangetoond worden dat het middel aan dit betrouwbaarheidsniveau voldoet. Zoals ook toegelicht in de hiervoor genoemde paragraaf beoordeelt de verstrekker van het betreffende bewijsmiddel geregeld of het middel nog aan de gesteld eisen voldoet. Indien dit niet langer het geval is vervalt het bewijsmiddel en wordt vervolgens tevens de goedkeuring voor het middel ingetrokken in bij of krachtens algemene maatregel van bestuur te bepalen termijn. De kwaliteit van de identificatiemiddelen wordt dan ook in beginsel geborgd door middel van de reeds bestaande stelsels waarmee bewezen wordt of het middel aan het juiste betrouwbaarheidsniveau voldoet.

Voor het uitzonderlijke geval waarbij een identificatiemiddel niet langer voldoende veilig is én de continuïteit en daarmee de kwaliteit van zorg in gevaar kan komen, bevat het wetsvoorstel een grondslag voor de Inspectie om informatie op te vragen en om zo nodig toezicht te houden. De kwaliteit van zorg kan in gevaar komen na de intrekking van de goedkeuring van een inlogmiddel omdat de zorgaanbieder niet meer aan zijn wettelijke plicht om het BSN van de cliënt te registreren kan voldoen en mogelijk ook niet langer zijn elektronische uitwisselingsystemen of zorginformatiesystemen kan raadplegen indien hiervoor goedkeurede inlogmiddelen gebruikt worden. In een dergelijk uitzonderlijk geval is het aan de minister om te bepalen hoe en wanneer de goedkeuring wordt ingetrokken. De Inspectie kan hier een ondersteunende rol inspelen door een inschatting te maken van hoe de intrekking van het middel de kwaliteit van zorg kan beïnvloeden. In een zeer uitzonderlijk geval kan de Inspectie haar bevoegdheden inzetten om te bewerkstelligen dat de betreffende zorgaanbieder informatie verschaft of om hem ertoe te bewegen maatregelen te treffen om de inlogmiddelen te vervangen opdat de continuïteit van de zorg niet in gevaar komt. Een dergelijke situatie zal zich doorgaans niet voor doen omdat zorgaanbieders normaliter zelf en in goed overleg al de benodigde maatregelen treffen.

Indien een inlogmiddel onveilig blijkt te zijn en van tijdig herstel naar het betrouwbaarheidsniveau hoog geen sprake is of kan zijn en de veiligheid van cliëntgegevens – en in het verlengde daarvan de kwaliteit van de zorg – in gevaar blijft, kan de minister over gaan tot intrekking van de goedkeuring van het betreffende middel. Het intrekken van de goedkeuring is een ultimum remedium met grote gevolgen voor zowel de verstrekker van het middel als voor diegenen die dit middel gebruiken. Intrekking moet dan ook aan de beginselen van proportionaliteit en subsidiariteit voldoen, ook zal in beginsel onder bepaalde voorwaarden een redelijke termijn gegeven moeten worden aan de gebruikers van de betreffende middelen om over te stappen naar een ander identificatiemiddel. Hoe lang die termijn is en welke voorwaarden van toepassing zullen zijn zal mede afhangen van het risico dat bestaat voor de veiligheid van cliëntgegevens. Over de intrekking van identificatiemiddelen worden nadere regels gesteld bij of krachtens algemene maatregel van bestuur. De intrekking van de goedkeuring van een identificatiemiddel is een besluit in de zin van de Awb, waartegen bezwaar en beroep openstaat.

6. Gegevensbeschermingseffectbeoordeling

Om de privacy-aspecten van het wetsvoorstel te onderzoeken is een gegevensbeschermings-effectbeoordeling uitgevoerd. Het wetsvoorstel voorziet in een aantal nieuwe gegevensverwerkingen:

- Authenticatieverklaringen vanuit het UZI-register waarbij met erkende middelen de zorgidentiteit uit het UZI-register wordt opgehaald. Hierbij wordt onder andere het BSN verwerkt.
- Het verwerken van het BSN door zorgaanbieders zodat identiteiten sterk gekoppeld worden om zorgspecifieke middelen uit te kunnen geven.
- De koppeling van een HR-systeem aan het UZI-register ten behoeve van het geautomatiseerd beheren van de relaties van de zorgaanbieder met zorgmedewerkers in het register.

6.1 Authenticatieverklaringen CIBG

Iedere keer dat de zorgidentiteit met een inlogmiddel uit het UZI-register wordt opgehaald, verkrijgt het CIBG een versleuteld BSN, ontsleutelt deze en geeft daarvoor een versleutelde zorgidentiteit terug. Dat is noodzakelijk om een sterke koppeling te maken tussen de identiteit die vanuit het inlogmiddel wordt verstrekt en de zorgidentiteit vanuit het UZI-register. Daarmee kan een hoog betrouwbare relatie tot stand komen. Het BSN wordt omgezet in een UZI-nummer. Bij zorgspecifieke middelen wordt niet het BSN maar het UZI-nummer gebruikt om de zorgidentiteit op te halen uit het register. Deze gegevensverwerking vindt centraal plaats voor de zorgsector en beschikt het CIBG over gegevens bij welke zorgaanbieder een zorgmedewerker inlogt. Er vindt logging t.b.v. een beveiligingsincident / oneigenlijk gebruik plaats. Voor deze logging worden de bewaartermijnen in het BIO-OP product ‘Handreiking Dataclassificatie’ onder de verschillende eisen voor integriteit en vertrouwelijkheid van gegevens gehanteerd.

6.2 Verwerken van het BSN door de middelenuitgever zorgspecifieke middelen

Het is van belang dat gegevens van cliënten enkel geraadpleegd kunnen worden met het gebruik van inlogmiddelen die voldoen aan het juiste betrouwbaarheidsniveau. Voor het raadplegen van deSBV-Z is dit het betrouwbaarheidsniveau hoog. Dat betekent dat zowel de techniek van het middel als het uitgifteproces moeten voldoen aan de betrouwbaarheid eIDAS hoog. Om de uitgifte van een persoonlijk Wdo of zorgspecifiek inlogmiddel op Hoog in te regelen, is de verwerking van het BSN nodig. Het is dus nodig dat de middelenuitgevers een BSN-verwerkingsgrondslag hebben. Voor de Wdo-middelen wordt dit geregeld in de Wdo. Voor de zorgspecifieke middelen wordt dit geregeld middels deze wetswijziging.

Om de koppeling tussen de door de middelenuitgever vastgestelde identiteit van de medewerker en de identiteit in het door de overheid beheerde UZI-register met de hoogste betrouwbaarheid te kunnen maken, moet een gedeelde unieke sleutel worden gebruikt. Het UZI-register hanteert het BSN als sleutel om de zorgmedewerker en het sectorspecifieke UZI-nummer uniek te relateren. Dat betekent dat de middelenuitgever het BSN (als gedeelde unieke sleutel) van de zorgmedewerker moet aanleveren aan het CIBG, zodat deze kan worden gebruikt om het bijbehorende UZI-nummer te vinden. Dit UZI-nummer en de bijbehorende attributen (zoals URA en rolcode) worden vervolgens naar de middelenuitgever gestuurd en op het zorgspecifieke middel gezet. Deze wordt dan persoonlijk aan de zorgmedewerker uitgegeven. Op deze manier wordt een hoog betrouwbare relatie tot stand gebracht tussen de medewerker en het UZI-nummer en kan persoonsverwisseling worden voorkomen. De BSN-verwerking bij de middelenuitgever is noodzakelijk in dit proces.

De vraag kan worden gesteld of bij de beoogde eenmalige verwerking van het BSN, de tussenkomst van de middelenuitgever noodzakelijk en gerechtvaardigd is of dat de identiteitskoppeling door de zorgmedewerker zelf tot stand gebracht kan worden. Het is namelijk praktisch mogelijk dat de eenmalige identiteitskoppeling wordt gerealiseerd door de medewerker zelf. In dat geval verifieert de zorgmedewerker zelf de koppeling van zijn middel aan zijn UZI-registratie. Echter, doordat de koppeling door de medewerker zelf wordt gemaakt en er geen gedeelde sleutel is voor zijn identiteit

tussen de twee administraties (het UZI-register en het register bij de zorgaanbieder), is het complex deze (moedwillig) verkeerd gemaakte koppeling te detecteren en te voorkomen. Door deze risico's zijn de zorgspecifieke middelen niet of erg lastig als eIDAS Hoog te classificeren. Het is daarom niet werkbaar om op deze oplossing in te zetten.

6.3 Vergelijkbaar met de Wdo

Het beoogde proces voor deze eenmalige verwerking van het BSN, lijkt op de verwerking van het BSN door middelenuitgevers die werken onder de Wdo. Deze middelenuitgevers krijgen op grond van de Wdo de bevoegdheid eenmalig het BSN te verwerken en deze tijdens het uitgeven van het authenticatiemiddel 'om te ruilen' in een van het BSN afgeleid nummer (concept van de 'polymorfe pseudonimisering'). Na deze omwisseling mag het BSN door de Wdo middelenuitgever niet meer worden verwerkt, moet het BSN worden 'vernietigd' in de administratie en wordt alleen nog een afgeleid nummer gebruikt. Voor zorgspecifieke middelen zal een soortgelijk proces worden gevolgd: het BSN zal door de middelenuitgever eenmalig worden gebruikt om het UZI-nummer op te halen uit het door de overheid beheerde UZI-register. Na deze omwisseling wordt het UZI-nummer door de middelenuitgever hard gekoppeld aan het zorgspecifieke middel. Daarna mag het BSN niet meer worden gebruikt ten behoeve van het genoemde doel en moet het worden verwijderd uit de administratie. Vaak zal de eenmalige BSN-verwerking worden uitgevoerd door de zorg- of jeugdhulpaanbieder voor wie de betreffende medewerker werkzaam is. De zorgaanbieder is immers doorgaans degene die een inlogmiddel uitgeeft. Het kan evenwel voorkomen dat de uitgifte van de middelen niet plaatsvindt bij de zorgaanbieder, maar bijvoorbeeld bij de leverancier van het authenticatiemiddel of bij een koepelorganisatie die middelen uitgeeft voor meerdere zorgaanbieders. Ook dan geldt dat het BSN slechts eenmaal gebruikt mag worden bij de koppeling van het middel aan de ingeschrevene.

6.4 BSN verwerkingsgrondslag bij de zorgaanbieder

In deze wetswijziging wordt een grondslag voor de verwerking van het BSN ten behoeve van het uitgeven van zorgspecifieke middelen voor de zorgaanbieder geregeld. Deze BSN-verwerkingsgrondslag wordt voor de zorgaanbieder, en niet voor iedere uitgever van zorgspecifieke middelen, gecreëerd om ervoor te zorgen dat de zorgspecifieke middelen alleen worden gebruikt in het zorgdomein.

Het kan voorkomen dat de uitgifte van de middelen en de certificering in de rol van middelenuitgever niet plaatsvindt bij de zorgaanbieder, maar bijvoorbeeld bij de leverancier van het authenticatiemiddel of bij een koepel. In deze gevallen moet de middelenuitgever een contract zijn aangegaan met een zorgaanbieder. De middelenuitgever is dan de verwerker en de zorgaanbieder de verwerkingsverantwoordelijke. De grondslag van de verwerking ligt in dat geval bij de zorgaanbieder, maar de daadwerkelijke verwerking van het BSN wordt gedaan door de middelenuitgever. Hierdoor ontstaan mogelijkheden voor de middelenuitgever de zorgspecifieke middelen op eIDAS substantieel en/of eIDAS hoog uit te geven.

6.5 Koppeling HR-systeem aan UZI-register

Zorgaanbieders en jeugdhulpaanbieders kunnen een koppeling vanuit een HR-systeem maken met het UZI-register. Deze systeemkoppeling maakt het mogelijk geautomatiseerd nieuwe medewerkers aan te melden op basis van het BSN van de medewerker en deze relatie te muteren in het register. Daarmee kunnen inschrijvingen en mutaties gemakkelijk en snel doorgegeven worden aan het CIBG. Om dit veilig te laten verlopen worden er eisen gesteld aan de wijze waarop inschrijvingen en mutaties vanuit het HR-systeem van de zorgaanbieder worden doorgegeven. Er moet aangesloten worden op een gestandaardiseerd koppelvlak en het systeem moet voldoen aan relevante NEN-normen zoals de NEN 7518.

6.6 Geïnventariseerde risico's: het uitlenen van inlogmiddelen en gebruik privételefoon

Bij het uitvoeren van de DPIA zijn een aantal risico's naar voren gekomen bij het verwerken van gegevens in het kader van dit wetsvoorstel. De belangrijkste daarvan is het uitlenen van inlogmiddelen, daar wordt in deze paragraaf kort op ingegaan. In de praktijk gebeurt het nog wel

eens dat een eigenaar van een inlogmiddel het middel door een derde laat gebruiken. Hierbij kan bijvoorbeeld gedacht worden aan een arts die een digitaal document laat ondertekenen door een derde. In het kader van informatiebeveiliging is het uitwisselen van inlogmiddelen onwenselijk omdat zo mogelijk medewerkers bij gegevens kunnen waar zij niet toe gerechtigd zijn. Een medewerker is minder snel geneigd een inlogmiddel uit te lenen dat voor meerdere toepassingen gebruikt kan worden. Een mobiele telefoon wordt waarschijnlijk minder snel gedeeld omdat daarop vaak ook zeer persoonlijk gegevens staan (bijvoorbeeld foto's, sms, WhatsApp-berichten, e-mail, applicaties voor bankieren en andere apps). Dit uitlenen is minder comfortabel, dit geldt ook voor het uitlenen van DigiD. Vanuit een beveiligingsoogpunt vormen de inloggegevens in combinatie met een telefoon namelijk een grotere drempel tegen misbruik dan het uitlenen van een specifieke werkpas. Daarnaast is van belang dat het uitlenen van een Wdo inlogmiddel bijzonder onwenselijk is omdat hiermee potentieel toegang kan worden verkregen tot overheidsdiensten namens de medewerker.

Medewerkers kunnen naast een pas bijvoorbeeld ook kiezen voor een digitale wallet op een smartphone of tablet. Als daarvoor een werktelefoon wordt gebruikt, zijn daarop mogelijk al diverse beveiligingsmaatregelen ingesteld. Het gebruik van een privételefoon neemt een aantal risico’s met zich mee. Zo kan het voorkomen dat de gebruiker op een privételefoon per ongeluk malafide of gecompromitteerde software installeert die verborgen zit in ogenschijnlijk veilige applicaties. Ook kunnen risico’s ontstaan als gevolg van het niet (meer kunnen) uitvoeren updates van het besturingssysteem van de telefoon, softwarebibliotheken of applicaties zelf. Hoewel middelen op betrouwbaarheidsniveau hoog bestand zouden moeten zijn tegen dit soort aanvalspatronen, blijft er een risico. Dit is (deels) op te lossen door de privételefoon centraal te laten beheren door de zorgaanbieder, jeugdhulpaanbieder of middelenleverancier. De privételefoon wordt dan een ‘managed device’. Het is echter de vraag of gebruikers deze vorm van beheer wenselijk vinden. Bovendien ontstaat een complexe situatie wanneer deze telefoon door twee of meer zorgaanbieders beheerd zou moeten worden om aan de gebruiksvoorwaarden van de verschillende (zorgspecifieke) middelen te voldoen. Een ‘managed device’ is veiliger en een privételefoon niet per definitie onveilig. Het is aan de zorg- of jeugdhulpaanbieders hierover afspraken te maken met hun medewerkers.

7. Gevolgen (m.u.v. financiële gevolgen)

Hieronder wordt aangegeven wat de gevolgen zijn van deze wetswijziging zijn voor de betrokken partijen.

7.1 Overheid

Het toekomstbestendig maken van de UZI-middelen heeft gevolgen voor de taken en verantwoordelijkheden van het CIBG. Het CIBG is verantwoordelijk voor het beheer van het UZI-register en het digitaal beschikbaar stellen van de attributen uit het UZI-register (de authenticatieverklaring). Het CIBG zal tevens namens de minister verantwoordelijk worden voor de goedkeuring van de eIDAS-, Wdo-, zorgspecifieke- of PKI-o servercertificaten. Indien dit het geval is, keurt het CIBG de middelen goed.

Om deze taken uit te voeren moeten zowel technische als procesmatige wijzigingen worden geïmplementeerd. Technische wijzigingen betreffen het verstrekken van identificerende attributen uit het UZI-register door middel van erkende inlogmiddelen voor identificatie en authenticatie van zorgmedewerkers. Procesmatig verandert het registratieproces van het CIBG. Daarnaast zal een proces moeten worden ingericht voor het beoordelen van de authenticatiemiddelen die onderdeel (willen) worden van het stelsel. Het CIBG is nauw betrokken bij het wetsvoorstel en heeft een uitvoeringstoets gedaan (zie paragraaf 11.2).

7.2 Zorg- en jeugdveld

Door de generieke functies identificatie en authenticatie in te vullen krijgt het veld de mogelijkheid een uniforme, veilige en gebruiksvriendelijke manier van inloggen te implementeren. Hiermee kan een belangrijke randvoorwaarde voor elektronische gegevensuitwisseling worden ingevuld.

Met de voorgenomen wijziging ontstaat een (migratie)periode waarin de zorg- en jeugdhulpaanbieders en hun medewerkers gebruik kunnen maken van de huidige UZI-middelen én de nieuwe erkende inlogmiddelen. Hiervoor moeten er keuzes gemaakt worden met betrekking tot software en inlogmiddelen. Zorg- en jeugdhulpaanbieders zullen hiervoor gesprekken moeten voeren met hun ICT- en middelenleveranciers.

Doordat bij een registratie in het UZI-register geen UZI-pas meer hoeft worden uitgegeven, wordt het UZI-register toegankelijker voor zorg- en jeugdhulpaanbieders en hun medewerkers. Initiële aanvragen en wijzigingen kunnen veel sneller worden doorgevoerd. Daarmee wordt het UZI-register geschikt gemaakt om breed te kunnen worden ingezet in het veld.

7.3 Bedrijven

Met bedrijven worden de leveranciers van inlogmiddelen en zorginformatie- en uitwisselingssystemen (zoals een EPD) bedoeld.

Om in aanmerking te komen voor een goedkeuring wordt beoogd dat middelenleveranciers moeten zorgen voor een middel dat is erkend onder de Wdo, NEN (7518), PKI-O of eIDAS. Hiervoor wordt een audit doorlopen waarbij vastgesteld wordt of het middel aan de gestelde eisen voldoet. Zij leveren een verklaring af (auditrapport) waaruit blijkt dat door een derde partij (auditor) is vastgesteld, dat het middel voldoet aan de gestelde eisen van de Wdo, NEN 7518, PKI-O ofwel eIDAS. Hierover worden regels bij of krachtens algemene maatregel van bestuur.

Leveranciers van informatie- en uitwisselingssystemen kunnen erkende inlogmiddelen en UZI-attributen integreren in hun systemen. Hiervoor moet doorgaans de inlogmodule in het systeem worden aangepast en aangesloten worden op het koppelvlak van het CIBG. Daarmee komen de verschillende goedgekeurde inlogmiddelen beschikbaar die de zorgidentiteit uit het UZI-register kunnen ophalen.

7.4 Burgers

Het is voor burgers belangrijk om te weten dat er zorgvuldig met hun medische gegevens wordt omgegaan. Door toe te werken naar breed gebruik van inlogmiddelen op het hoogste betrouwbaarheidsniveau wordt het gegevensuitwisselingsproces veiliger en de privacy van burgers beter gewaarborgd. Ook wordt transparanter wie welke zorggegevens heeft ingezien door een breder gebruik van de identiteiten uit het UZI-register in verschillende toepassingsgebieden.

8. Uitvoering

Het wetsvoorstel heeft gevolgen voor de uitvoering door het CIBG. Het CIBG zal teruggaan naar haar kerntaak van registerhouder en stopt op termijn met het uitgeven van UZI-passen en servercertificaten. Daarmee fungeert het CIBG niet meer als verlener van vertrouwensdiensten (TSP). Het CIBG is verantwoordelijk voor het beheer van het UZI-register en het digitaal beschikbaar stellen van de authenticatieverklaring. Een nieuwe taak voor het CIBG wordt het goedkeuren van de inlogmiddelen namens de minister. Hiervoor wordt beoogd dat het CIBG beoordeelt of een middel beschikt over een bewijs waaruit blijkt dat het middel voldoet aan de eisen voor het betrouwbaarheidsniveau hoog. Dit brengt systeem- en procesmatige aanpassingen met zich mee. Het CIBG heeft op basis van het wetsvoorstel een uitvoeringstoets uitgebracht, hierop is dieper ingegaan in paragraaf 11.2.

Het CIBG krijgt middels onderhavig wetsvoorstel eveneens de mogelijkheid tot het weigeren of intrekken van een inschrijving in het UZI-register indien de middelen niet (meer) voldoen of indien een ingeschrevene in het register niet voldoet aan de hiervoor geldende eisen. Hierbij is bijvoorbeeld gedacht aan situaties waarbij een ingeschrevene niet langer aan de eisen hiervoor voldoet of als de betreffende ingeschrevene zijn inschrijving misbruikt door via de SBV-Z onrechtmatig het BSN of andere persoonsgegevens te raadplegen.

In het kader van het evenredigheidsbeginsel is het van belang om ruimte te laten voor de afweging van belangen in het concrete geval. In het huidige stelsel is gebleken dat een besluit onredelijk zwaar

kan uitvallen voor een betrokken zorg- of jeugdhulpaanbieder. Dit kan mogelijk ook het geval zijn in het nieuwe stelsel. Zo zullen er financiële belangen gemoeid zijn met het goedkeuren van een inlogmiddel. Indien de goedkeuring van de middelen wordt ingetrokken, dan zal de zorgaanbieder mogelijk nieuwe middelen moeten aanvragen. Deze kosten kunnen hoog oplopen. Een ander belang van zorgaanbieders is gelegen in het feit dat een middel breder wordt gebruikt dan alleen voor de toegang tot de SBV-Z. De intrekking van een goedkeuring of de wijziging van autorisatiekenmerken kan ook andere werkzaamheden van de zorgaanbieder verstoren. In de huidige situatie kan dit tot gevolg hebben dat een zorg- of jeugdhulpaanbieder bijvoorbeeld geen toegang meer heeft tot een uitwisselingssysteem van medische gegevens van cliënten.

9. Regeldruk

Het wetsvoorstel heeft gevolgen voor zorgaanbieders, jeugdhulpaanbieders en leveranciers op een aantal aspecten van regeldruk. Tegelijkertijd zorgt het wetsvoorstel voor duidelijkheid, uniformiteit en verlichting van regeldruk. De regeldrukeffecten voor zorgaanbieders en leveranciers worden per onderdeel van het wetsvoorstel weergegeven. Verder zorgt de manier van invoeren ervoor dat de situatie werkbaar is voor het zorgveld.

9.1 Werkbare invoering in de praktijk

De verwachting is dat het wetsvoorstel in 2025 in werking treedt. Er geldt een verplichting voor het gebruik van erkende inlogmiddelen voor de toegang tot de SBV-Z. Er geldt geen directe verplichting om gebruik te maken van de erkende inlogmiddelen en het UZI-register voor toegang tot uitwisselings- en/of zorginformatiesystemen. Naar verwachting zullen een aantal zorgketens snel overgaan tot implementatie omdat de behoefte aan de invulling van de generieke voorziening voor identificatie en authenticatie groot is in het zorgveld. Voorbeelden zijn zorgketens in de geboortezorg, verpleegkundige-overdracht, medicatieoverdracht en het LSP. Gegevensuitwisseling komt tot stand in zorgketens en hiermee ontstaat een indirecte verplichting tot implementatie. Vertrouwen en interoperabiliteit in de zorgketen zijn essentieel en daarom kan een partij binnen de keten niet kiezen voor een andere manier van inloggen.

De behoefte in het zorgveld aan een oplossing voor uniforme, veilige en betrouwbare identificatie en authenticatie van de zorgmedewerker is groot. Zorgaanbieders, leveranciers en programma's voor gegevensuitwisseling (VIPP en focus) hebben aangegeven snel tot implementatie te willen overgaan. Er is gekozen voor een ingroeimodel en geen 'big bang' implementatie. Zodra het wetsvoorstel in werking treedt zullen een aantal (grote) zorgketens gaan implementeren. Vanaf dan begint een overgangsperiode waarbij de huidige UZI-middelen op termijn worden uitgefaseerd en het zorgveld moet overstappen op nieuwe middelen. De overgangsperiode geeft het zorgveld ruimschoots de tijd om van de UZI-middelen over te stappen op een erkend middel dat op persoonlijke titel wordt gebruikt. Op termijn worden de nieuwe middelen en het UZI-register mogelijk verplicht gesteld zodat de gehele zorgsector veilig, betrouwbaar en uniform toegang verkrijgt tot medische gegevens van cliënten.

De generieke oplossing voor identificatie en authenticatie is met zorgveld tot stand gekomen en goed ontvangen. Hiervoor zijn zorg- en jeugdhulpaanbieders, koepels, leveranciers en programma's geconsulteerd. VWS zal dat blijven doen in het Informatieberaad Zorg (IB), klankbordgroepen, expertsessies en individuele gesprekken met het zorgveld. Ook blijven praktijkchecks gedaan worden door techniek te beproeven en pilots uit te voeren.

Tot grootschalige implementatie in 2025 mogelijk is wordt techniek beproefd met behulp van PoC's en beproefde techniek in delen van de zorgsector naar de praktijk gebracht met pilots. Deze aanpak is essentieel voor acceptatie in de zorgsector. Hiermee wordt technische ervaring en gebruikerservaring opgedaan. Details van de oplossingsrichting kunnen verder ingevuld en bijgeschaafd worden. Zo wordt voorgesorteerd op grootschalige implementatie.

Een eerste pilot bij wijze van praktijkcheck heeft aangetoond dat de oplossing technisch werkt en werkbaar is voor zorgaanbieders, zowel voor grote instellingen als voor kleine zorgaanbieders en solistisch werkende zorgverleners. Hieruit kwam naar voren dat het publieke middel DigiD

gebruiksvriendelijker is dan de huidige UZI-middelen en er altijd snel toegang verkregen kan worden via de app op de telefoon. Ook zorgt het beschikbaar stellen van verschillende inlogmiddelen ervoor dat er een back-up is.[15] Met meer pilots worden nog meer praktijkchecks gedaan en is VWS constant in gesprek met het zorgveld. De oplossing wordt daarmee verder ingevuld en bijgeschaafd.

De technische implementatie kan omschreven worden als het vervangen van het slot op de deur van de zorgapplicatie. Dat gebeurt door de softwareleverancier van de zorgaanbieder en betreft een module binnen het zorgsysteem. Om gebruik te kunnen maken van de verschillende erkende inlogmiddelen waarmee de professionele zorgidentiteit uit het UZI-register wordt opgehaald, moet worden aangesloten op een koppelvlak van het CIBG. De specificaties zijn beschikbaar en aansluiten wordt door leveranciers niet als ingrijpend beoordeeld.

In 2025 worden een aantal zorgketens vanuit de Wegiz verplicht gegevens elektronisch uit te wisselen. Hiervoor zijn verschillende werkende generieke functies nodig. Bij het verder vormgeven van de implementatie moet rekening gehouden worden met de samenloop van verschillende implementaties door leveranciers en zorgaanbieders. Dat gebeurt vanuit VWS (de Wegiz en generieke functies) in afstemming met leveranciers en zorgaanbieders.

9.2 Inloggen met Wdo middelen

Met het wetsvoorstel wordt het voor zorg- en jeugdhulpmedewerkers mogelijk gemaakt gebruik te maken van inlogmiddelen met het betrouwbaarheidsniveau hoog. Beoogd om bij of krachtens algemene maatregel van bestuur te bepalen dat dit onder meer de middelen zijn die onder de Wet digitale overheid (Wdo) zijn erkend. Leveranciers van middelen kunnen het middel met een audit laten certificeren. VWS sluit hiermee aan bij het Wdo stelsel dat onder verantwoordelijkheid van het ministerie van BZK wordt opgesteld.

Door Wdo middelen beschikbaar te stellen voor de zorg- en jeugdhulpmedewerker is het gebruik van de huidige UZI-middelen niet meer verplicht en kunnen die worden uitgefaseerd. Daarmee komen de administratieve lasten te vervallen. De UZI-pas kost 255 euro per 3 jaar en het UZI-servercertificaat 450 euro per 3 jaar. Als medewerker hoef je niet meer nieuwe UZI-middelen aan te vragen als er een wijziging plaatsvindt in je beroep of werkgever. De wijziging moet alleen nog doorgevoerd worden in het UZI-register. Daarnaast kunnen andere inlogmiddelen uitgefaseerd worden. Denk aan inloggen op verschillende systemen met verschillende gebruikersnamen, wachtwoorden, eventueel aangevuld met een tweede factor zoals een code via SMS of e-mail. Ook het beheer van deze identiteiten komt te vervallen. Evenals het resetten van toegangscodes door een helpdesk. Zorgmedewerkers kunnen kiezen voor een middel en deze overal gebruiken. Deze inlogmiddelen zijn veiliger dan bijvoorbeeld een gebruiksnaam en wachtwoord. Een sterkere authenticatie betekent mogelijk wel dat inloggen enkele seconden langer duurt. Voor het gebruiksgemak kan de authenticatieverklaring worden hergebruikt zodat gebruiksvriendelijkheid en veiligheid beter samen gaat. Overigens volgt de noodzaak tot het inloggen op het betrouwbaarheidsniveau eIDAS Hoog niet uit het wetsvoorstel en levert daarmee geen nieuwe regeldruk op.

De exacte administratieve lasten en kosten voor identificatie en authenticatie zijn voor een groot deel afhankelijk van het inlogmiddel. Zo is DigiD gratis voor burgers en wordt al breed gebruikt onder Nederlandse inwoners. Met een Nederlandse identiteitskaart met e-functionaliteit (eNIK) kan via de DigiD app ingelogd worden op betrouwbaarheidsniveau eIDAS Hoog. Een eNIK kost 71,53 euro en is 10 jaar geldig.[16] Voor andere middelen geldt dat ze nog moeten worden aangevraagd en daar kunnen kosten aan verbonden zijn. De werkgever van een zorgmedewerker kan ervoor kiezen kosten voor een middel te vergoeden. De kosten voor een middel op het hoogste betrouwbaarheidsniveau worden ingeschat tussen de 20 en 70 euro per jaar.[17] Kanttekening hierbij is dat verschillende inlogmiddelen op het hoogste betrouwbaarheidsniveau nog volop in ontwikkeling zijn en nog niet op grote schaal voor deze prijs te koop zijn. Met de middelen kan op termijn wel overal in de zorg ingelogd worden.

[15] Nieuwsbericht pilot BRBA: Succesvolle pilot met inloggen via DigiD in plaats van UZI-pas | Nieuwsbericht | Gegevensuitwisseling in de zorg
[16] Eindrapport Herijking MKBA Digitale Toegang naar aanleiding van de Wet digitale overheid, p. 49.
[17] TNO rapport "Toekomstbestendig maken van UZI middelen".

Daardoor kunnen andere middelen en manieren van inloggen komen te vervallen. Hiermee kunnen verborgen kosten van authenticatie in allerlei systemen worden geëlimineerd.

Uitgaande van de 90.000 zorgmedewerkers die nu in het UZI-register geregistreerd staan, gaat het in de toekomstige situatie om totale gemiddelde kosten van € 4.500.000 per jaar (gemiddeld € 50 per zorgmedewerker per jaar) voor het inlogmiddel. Daarnaast wordt jaarlijks een bijdrage gevraagd voor de registratie in het UZI-register. De financiële lasten voor inschrijvingen in het register vallen buiten de definitie van regeldruk en worden in paragraaf 10.2 verder toegelicht. In de huidige situatie gaat het om gemiddelde kosten van € 7.650.000 per jaar (€ 85 per zorgmedewerker per jaar) en de kosten die gemaakt worden voor alle andere methoden van inloggen zoals gebruiksnamen en wachtwoorden. Dit betreft dus een minimale regeldrukreductie van € 3.150.000 per jaar. Hierbij zijn de kosten andere methoden van authenticatie in allerlei systemen en bijbehorende functies zoals beheer en uitgifte niet meegenomen.

9.3 Inloggen met zorgspecifieke middelen

Het wetsvoorstel voorziet naast het gebruik van Wdo erkende middelen ook in het gebruik van zorgspecifieke middelen. Dat zijn middelen die onder de verantwoordelijkheid van de zorg- of jeugdhulpaanbieder aan hun medewerkers worden uitgereikt en niet onder de Wdo erkend kunnen worden. Het gebruik van zorgspecifieke middelen, zoals een ziekenhuispas, is facultatief en de middelen zijn alleen geschikt voor gebruik in de zorgsector. Om ervoor te zorgen dat deze middelen veilig en betrouwbaar zijn moeten zorgaanbieders die zelf middelen uitgeven het middel laten certificeren volgens NEN 7518. Dat is noodzakelijk om onafhankelijk vast te laten stellen dat de zorgspecifieke middelen het juiste betrouwbaarheidsniveau hebben. Nevendoel van deze verplichting is geen Wdo-ondermijnende ingang te creëren voor middelen die in de zorg gebruikt kunnen worden. De NEN certificering wordt verkregen door een audit uit te laten voeren en daar gaan administratieve lasten en kosten mee gepaard. Deze mogelijkheid is daarmee vooral interessant voor grote instellingen met veel medewerkers. Kleinere zorgaanbieders, jeughulpaanbieders en solistisch werkende zorgverleners kunnen gebruik maken van de Wdo middelen.

Zorgaanbieders die zelf middelen uitgeven moeten de technische werking van het middel, de (initiële) identificatie, de registratie en het beheer van de identiteit en het uitgifteproces laten beoordelen. Deze factoren bepalen hoe veilig en betrouwbaar het uitgegeven middel is. Voor certificering van de technische werking van een middel kan de leverancier zijn product certificeren en deze certificering voor meerdere zorg- en jeugdhulpaanbieders hergebruiken. Het uitgifteproces moet per zorg- of jeugdhulpaanbieder beoordeeld worden.

NEN audits en certificering bestaat al voor bestaande normen zoals de NEN 7510, 7512 en 7513. Grote zorginstellingen die zelf middelen willen uitgeven kunnen de nieuwe norm hierin meenemen.

9.4 De identiteit van een medewerker in het UZI-register

Het UZI-register wordt hét register voor het verstrekken van de identiteit van medewerkers en zorg- en jeugdhulpaanbieders. Daarmee moeten medewerkers en aanbieders zich inschrijven in het register en eventuele mutaties doorgeven. Nu staan ongeveer 90.000 medewerkers geregistreerd in het UZI-register. Potentieel zal het UZI-register doorgroeien naar 1,5 miljoen mensen die werkzaam zijn in de zorg.[18] De doelgroep die momenteel geen UZI-middelen gebruikt zal zich in de jaren na het inwerking treden van het wetsvoorstel inschrijven in het register. In de berekeningen wordt in de eerste jaren na het in werking treden van het wetsvoorstel uitgegaan van een groei van 100.000 registraties per jaar.

[18] In Nederland werkten in 2020 circa 1,4 miljoen mensen in de sector zorg en welzijn. Het gaat om werknemers en zelfstandigen met een hoofdbaan bijvoorbeeld als medisch specialist, pedagogischmedewerker, verpleegkundige of verzorgende, die werken in het ziekenhuis of verpleeghuis, in de wijkverpleging, de thuiszorg, de kinderopvang of de jeugdzorg. Ook personeel in de gehandicaptenzorg, geestelijke gezondheidszorg, huisartsenzorg en sociaal werk valt hieronder. En het gaat niet alleen om mensen die met cliënten, patiënten en kinderen werken, ook al het personeel met een administratieve of leidinggevende functie valt hieronder.

Medewerkers kunnen zich digitaal registreren door in te loggen en een aantal gegevens door te geven aan het CIBG. Voor zorg- en jeugdhulpaanbieders wordt het mogelijk gemaakt om een koppeling met een HR-systeem te maken voor geautomatiseerd aanmelden van medewerkers en muteren van relaties in het register. Daarmee kunnen inschrijvingen en mutaties gemakkelijk en snel doorgegeven worden aan het CIBG. Een inschrijving van een natuurlijk persoon kost maximaal 3 minuten en de inschrijving van een rechtspersoon maximaal 5 minuten. Verder zal naar schatting jaarlijks 10% van de medewerkers een mutatie doorgeven. Een mutatie doorgeven in het UZI-register kost maximaal 2 minuten. Per 100.000 (nieuwe) registraties kost dat 5.000 uur. Uitgedrukt in een geldbedrag is dat (5.000 x 47) € 235.000,- per 100.000 nieuwe inschrijvingen. De mutaties per 100.000 registraties nemen jaarlijks ongeveer 333 uur in beslag. Dat komt neer op € 15.651,- per 100.000 ingeschreven zorgmedewerkers.

Het CIBG zal een jaarlijkse bijdrage in rekening brengen voor de registratie in het UZI-register.

Tot slot moeten zorgaanbieders kennis nemen van de nieuwe wet- en regelgeving; zogenaamde kennisnamekosten. Hiervoor moeten ongeveer 20.000 zorgaanbieders een half uur investeren. Daarmee komen de kennisnamekosten uit op 470.000 euro (10.000 uur x 47,00 euro)

10. Financiële gevolgen

Financiële gevolgen zijn te verdelen in eenmalige (implementatie)kosten en structurele kosten.

10.1 Eenmalige kosten

Om de UZI-pas door een stelsel van eIDAS genotificeerde, Wdo-conforme, zorgspecifieke inlogmiddelen en PKI-o middelen te vervangen zal er eenmalig geïnvesteerd moeten worden in het bouwen van de technische oplossing en het inrichten van het stelsel.

Bouw (VWS/CIBG)

De eenmalige kosten zullen hoofdzakelijk bestaan uit productontwikkeling (bouw) en bijkomende beleidsmatige- en juridische ondersteuning ten aanzien van uitwerking van het stelsel. Daarnaast zal de UZI-pas op termijn uitgefaseerd moeten worden. Dit brengt systeem- en procesmatige aanpassingen met zich mee. De vervanging en daarmee gepaard gaande uitfasering zal iteratief door een multidisciplinair team worden gerealiseerd. De hieruit volgende eenmalige uitgaven worden op € 8 miljoen geraamd. Dit bedrag is ingegeven op basis van de op dit moment bekende indicatoren. De implementatiekosten zijn meerjarig (t/m 2025) opgenomen op de begroting van VWS.

Daarnaast wordt de oplossing beproefd en worden pilots uitgevoerd. Met het beproeven van de techniek worden parallel verdere details van de oplossing ingevuld en kan voorgesorteerd worden op implementatie in het zorgveld. Om de proof of concepts en pilots vanuit VWS te ondersteunen is een volledig ICT team beschikbaar.

Zowel de vernieuwingen van het systeem, de wijzigingen vanuit het wetsvoorstel, de pilots en procesmatige aanpassingen worden ondergebracht in één programma binnen het CIBG. Onder het programma zijn vier projectlijnen gedefinieerd.

Adoptie (Zorgaanbieders)

Naast de bouw van de nieuwe oplossing waardoor uitfasering van de huidige oplossing mogelijk wordt, zullen (ICT-leveranciers van) zorgaanbieders de oplossing moeten implementeren. De technische implementatie kan omschreven worden als het vervangen van het slot op de deur van de zorgapplicatie. Dat gebeurt door de softwareleverancier van de zorgaanbieder en betreft een module binnen het zorgsysteem. Binnen de module wordt aangesloten op een koppelvlak van het CIBG. De specificaties zijn beschikbaar en aansluiten wordt door leveranciers niet als ingrijpend beoordeeld. Exacte implementatiekosten zijn nog niet bekend en worden nader onderzocht en inzichtelijk gemaakt door o.a. pilots uit te voeren. Op basis van de op dit moment bekende informatie wordt de

implementatie(impact) door (leveranciers van) zorgaanbieders als minimaal en daarmee kosten neutraal beschouwd. De exacte implementatie-impact is situationeel en kan per leverancier en zorgaanbieder verschillen. Zo is de implementatie van een zorgspecifiek inlogmiddel zoals een personeelspas ingrijpend omdat hierbij zowel persoonspassen als bijbehorende randapparatuur (bijvoorbeeld kaartlezers) vervangen moeten worden.

10.2 Structurele kosten

Eenmaal gebouwd en geadopteerd zullen de technische oplossing en het stelsel beheerd moeten worden. De ambitie is om het UZI-register zorgbreed in te zetten voor identificatie en authenticatie van de zorg- en jeugdhulpaanbieders en hun medewerkers, de schaal van inzet is afhankelijk van in welke mate het zorgveld welwillend is om de nieuwe oplossing te adopteren.

Beheer product (CIBG)

Het CIBG is verantwoordelijk voor het productbeheer en heeft in de uitvoeringstoets de structurele kosten ingeschat op 6 miljoen euro per jaar. Voorzien wordt dat het UZI-register zal blijven bestaan en dat de registraties zullen toenemen in aantal. Zodra het wetsvoorstel in werking treedt zal er een periode ontstaan waarin het nieuwe product wordt beheerd én UZI-middelen nog uitgegeven worden. Op termijn geeft het CIBG geen (nieuwe) passen en certificaten (UZI-middelen) meer uit. De reeds uitgegeven passen moeten nog wel ondersteund blijven worden voor zolang ze geldig zijn.

Het CIBG beheert het register, geeft authenticatieverklaringen af en keurt middelen op het hoogste betrouwbaarheidsniveau goed. De toename van het aantal registraties in het register is geen aanleiding tot hoge aanvullende structurele kosten. De diensten die samenhangen met de uitvoering en instandhouding gebeuren grotendeels automatisch en zijn niet of minder afhankelijk van het aantal gebruikers. Naast registraties zal de oplossing onderhevig zijn aan regulier onderhoud. Het CIBG zal een bijdrage aan de zorg- en jeugdhulpaanbieder vragen voor een registratie in het UZI-register. Er wordt geen bijdrage gevraagd als er een UZI-pas of servercertificaat is afgenomen. Het totaal aan bijdragen van het zorgveld mag de kosten voor de uitvoering door het CIBG niet overstijgen. Afhankelijk van het groeiscenario van het aantal registraties in het UZI-register en de bijdrage per registratie draagt het zorgveld het volgende bij:

Bijdrage derden (ingeschrevenen) UZI-register (20 euro per medewerker per jaar) Jaarlijkse kosten UZI-register 6 miljoen			
Jaar	**Aantal registraties** (zonder UZI-middel)	**Bijdrage derden**	**Bijdrage VWS**
2025	0	0	6.000.000
2026	100.000	2.000.000	4.000.000
2027	200.000	4.000.000	2.000.000
2028	300.000	6.000.000	0

Beheer stelsel

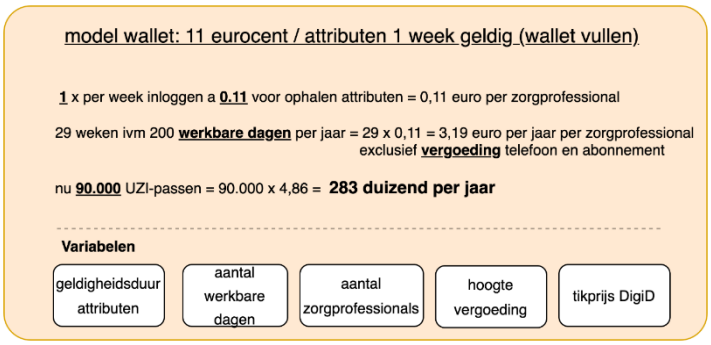
Naast het onderhouden van het product zal het stelsel up-to-date moeten blijven. Het moet duidelijk zijn en blijven wat de spelregels zijn in de omgang tussen de betrokken partijen en het product. Denk aan informatie over rechten en plichten, financiën, normenkaders en eisen aan techniek. Beheer van het stelsel zal onderdeel zijn van de bestaande formatieplekken binnen VWS zoals nu reeds al het geval is voor wat betreft de ontwikkeling van het stelsel.

Gebruikskosten Product (zorgveld)

Het uitvoeren van een authenticatie brengt kosten met zich mee, zowel voor publieke als private inlogmiddelen onder de Wet digitale overheid (Wdo), evenals voor zorgspecifieke middelen, eIDAS-genotificeerde middelen en PKI-O-certificaten. Zelfs het gebruik van authenticatiemiddelen van zorgaanbieders die geen deel uitmaken van het UZI-stelsel is niet kosteloos. Zoals toegelicht in paragraaf 9 worden er veel methoden van inloggen gebruikt voor verschillende systemen met

verschillende gebruikersnamen, wachtwoorden, eventueel aangevuld met een tweede factor zoals een code via SMS of e-mail. Er zijn kosten verbonden aan het beheer van deze identiteiten. Evenals het resetten van toegangscodes door een helpdesk.

De kosten zijn afhankelijk van verschillende factoren, waaronder initiële verificatiekosten, registratiekosten van de identiteit, uitgiftekosten van een middel, en eventuele kosten voor benodigde hard- en software of abonnementen. Beheer-, technische- en beveiligingskosten dragen ook bij aan de totale kosten. Daarnaast kan het gebruik van een middel door leveranciers, als onderdeel van hun verdienmodel, extra (commerciële) kosten met zich meebrengen. De financiering van deze kosten moet op een of andere manier worden gedekt.



Voor authenticatiemiddelen onder de Wdo lijkt de financiering waarschijnlijk te gebeuren op basis van het aantal gebruikers (abonnementsprijs) of het aantal transacties (tikprijs), hoewel hier momenteel nog geen definitieve duidelijkheid over bestaat.

In tegenstelling tot het centraal gefinancierde publieke middel DigiD, is het nog niet duidelijk hoe de financiering zal plaatsvinden voor de (aankomende) private middelen onder de Wdo. Het Ministerie van Volksgezondheid, Welzijn en Sport (VWS) geeft de voorkeur aan een abonnementsprijs om te voorkomen dat een tikprijs leidt tot een beperking van het aantal transacties/inlogpogingen. Om de totale kosten voor de gezondheidszorg inzichtelijk te maken, worden verschillende kostenscenario's overwogen. Het gebruik van het publieke Wdo middel DigiD kost ongeveer 11 cent per transactie. Deze kosten worden niet doorberekend aan burgers maar door verschillende ministeries betaald. Voor private Wdo middelen is onduidelijk of een abonnementsprijs of prijs per transactie gehanteerd wordt. Daarom zijn er een aantal scenario’s uitgewerkt waarin de bekostiging plaatsvindt per inlog.

Huidige DigiD 0,11 per inlog/ 0,01 per inlog

De kosten voor DigiD bedragen op dit moment 11 cent per inlog. Deze kosten worden niet doorbrekend aan de gebruiker maar worden afgekocht door ministeries. Zakelijk gebruik door zorgmedewerkers wordt niet afgekocht. Per medewerker die 200 werkdagen per jaar 10 keer per dag inlogt kost een inlogmiddel 220 euro per jaar. Als door volume-effecten de prijs per inlog afneemt naar 1 cent kost dat 20 euro per jaar per gebruiker.

Wallet geldigheid 1 dag/1week

Digitale wallets zijn inlogmiddelen die de zorgidentiteit (een combinatie van een aantal attributen/kenmerken) uit het UZI register in de 'wallet' opslaan en daarmee niet met iedere inlog langs het UZI-register gaan. Afhankelijk van de geldigheid van de ingeladen zorgidentiteit worden kosten gemaakt. Als de zorgidentiteit bijvoorbeeld 1 werkdag geldig is kost het per gebruiker 22 euro per jaar. Een geldigheid van bijvoorbeeld een week leidt tot jaarlijkse kosten van 3,19 euro per gebruiker.

In het scenario van een bekostiging per transactie zijn digitale wallets financieel aantrekkelijker omdat deze minder frequent gebruikt worden om de zorgidentiteit uit het UZI-register op te halen.

VWS streeft ernaar de kosten van het laden van een digitale wallet met een zorgidentiteit centraal te financieren. Hierdoor worden de kosten voor het gebruik van zowel publieke als private middelen onder de Wdo centraal gefinancierd evenals voor het gebruik van eIDAS genotificeerde middelen (mits die een BSN ontsluiten). Dit geldt enkel wanneer het gaat om het verkrijgen van een verklaring van de digitale zorgidentiteit van een zorgmedewerker die in een digitale wallet kan worden opgeslagen. Aangezien deze verklaring een bepaalde geldigheidsduur heeft, is het niet noodzakelijk dat de zorgmedewerker frequent met een Wdo-middel of eIDAS-middel moet authentiseren om een nieuwe verklaring te verkrijgen. Hiermee probeert VWS negatieve prikkels voor het gebruik van authenticatiemiddelen te verminderen en tegelijkertijd de centraal ontstane kosten beheersbaar te houden. Een zorgspecifiek middel kan niet worden gebruikt om een EDI-wallet te vullen met een verklaring van een zorgidentiteit (tenzij dit middel ook Wdo-erkend zou zijn, dan volgt echter de lijn van een Wdo-middel). Dit omdat een zorgspeificiek middel geen BSN zal kunnen aanbieden dat geaccepteerd wordt binnen het UZI-stelsel. De kosten voor het centraal financieren van digitale wallets zijn de komende jaren beperkt. Naar verwachting komen de wallets in 2026 ter beschikking en zal niet iedere medewerker gelijk overstappen. Uitgaande van de huidige 90.000 inschrijvingen in het register die vijf keer per jaar hun wallet laden bedraagt dat € 49.500 per jaar.

Het wordt verwacht dat, met name met het oog op de EDI-wallet als gevolg van de eIDAS-herziening, elke zorgmedewerker op termijn over een digitale wallet kan beschikken en daarmee zijn/haar verklaring van de zorgidentiteit zelf kan opslaan en gebruiken bij zorgaanbieders in het nieuwe UZI-stelsel.

Wanneer een zorgmedewerker een publiek of privaat Wdo-middel gebruikt voor directe toegang tot de dienstverlening van een zorgaanbieder, zullen deze transactiekosten echter wel worden doorberekend aan de zorgaanbieder. De hierboven geschetste modellen, die een vereenvoudigde weergave zijn van hoe de kosten zich manifesteren, laten zien dat bij een beperkt aantal gebruikers (90.000) en een beperkt aantal inlogtransacties op een werkdag (10x), de kosten van de authenticaties aanzienlijk hoger zijn dan bij het gebruik van digitale wallet-oplossingen.

Middel type	Doel	Financiering
Wdo publiek	Vullen van een EDI-wallet met zorgidentiteit	Centraal gefinancierd
Wdo privaat	Vullen van een EDI-wallet met zorgidentiteit	Centraal gefinancierd
eIDAS genotificeerd	Vullen van een EDI-wallet met zorgidentiteit	Centraal gefinancierd
Zorgspecifiek (NEN 7518)	Vullen van een EDI-wallet met zorgidentiteit	Functioneel niet mogelijk
Wdo publiek	Authenticatie directe toegang	Geen: doorbelast

Wdo privaat	Authenticatie directe toegang	Geen: doorbelast
eIDAS genotificeerd	Authenticatie directe toegang	Geen: doorbelast
Zorgspecifiek (NEN 7518)	Authenticatie directe toegang	Geen: kosten (al) gedragen door zorgaanbieder

VWS is voornemens de komende jaren de gebruikskosten te financieren zoals in deze paragraaf beschreven. Echter is veel afhankelijk van onder andere hoe snel en breed digitale wallets in de zorg beschikbaar komen en hoe snel de inschrijvingen in het register zullen toenemen. Afhankelijk van hoe de markt zich ontwikkelt kan VWS bijstellen.

11. Advies en consultatie

Het wetsvoorstel is ter internetconsultatie aangeboden. Op de reacties wordt ingegaan in paragraaf 11.1.

Daarnaast zijn er een aantal toetsen uitgevoerd en adviezen gevraagd over het wetsvoorstel, waar eveneens in deze paragraaf op wordt ingegaan. Het CIBG heeft een uitvoeringstoets gedaan (paragraaf 11.2), de Inspectie Gezondheidszorg en Jeugd (IGJ) heeft een Toezicht- en Handhaafbaarheidstoets opgeleverd (paragraaf 11.3), het Adviescollege toetsing regeldruk (ATR) heeft het wetsvoorstel beoordeeld op regeldruk (paragraaf 11.4) en de Autoriteit Persoonsgegevens (AP) heeft advies uitgebracht (paragraaf 11.5).

11.1 Internetconsultatie

De internetconsulatie van het wetsvoorstel digitale identificatie en authenticatie in de zorg (DIAZ) is gestart op 7 juli 2023 en is gesloten op 18 augustus 2023. Daarmee heeft de internetconsultatie 6 weken open gestaan. De consultatie heeft 25 reacties opgeleverd. In hoofdlijnen zijn de reacties positief over de richting van het wetsvoorstel. Er zijn een aantal aandachtpunten meegegeven die nadere duiding, dan wel aanpassing van het voorstel vragen. Op de hoofdlijnen uit de internetconsultatie en de veranderingen die naar aanleiding hiervan in het wetsvoorstel zijn aangebracht, wordt hierna ingegaan. Na afloop van de internetconsultatie is van de gelegenheid gebruik gemaakt om de wijzigingen die met dit wetsvoorstel worden aangebracht in de Wabvpz ook aan te brengen in de Jeugdwet. Ook voor de Jeugdsector is namelijk van belang dat de UZI-passen worden uitgefaseerd en dat deze sector kan gaan beschikken over diverse inlogmiddelen met het betrouwbaarheidsniveau hoog, die desgewenst breed ingezet kunnen worden. De artikelen en de toelichtingen zijn op dit punt aangevuld.

11.1.1 Scope wetsvoorstel

Uit de reacties op de internetconsultatie is gebleken dat er onduidelijkheid bestaat over de scope van het wetsvoorstel. In het wetsvoorstel staat dat het register en de inlogmiddelen gebruikt kunnen worden voor toegang tot zorginformatie- en uitwisselingssystemen ten behoeve van elektronische gegevensuitwisseling in de zorg. Het laatstgenoemde roept de vraag op of het register en de middelen ook gebruikt kunnen worden als er niet direct gegevens uitgewisseld worden. Bijvoorbeeld voor lokale toegang tot een EPD binnen één zorg- of jeugdhulpaanbieder. Hiermee kan een extra drempel van aparte authenticatie voor gegevensuitwisseling weggenomen worden.

Het doel van het wetsvoorstel is de inlogmiddelen en het register zorg breed in te kunnen zetten voor onder meer toegang tot zorginformatie- en uitwisselingssystemen. Zorginformatie- en uitwisselingssystemen omvatten alle systemen in de zorg waarbij persoons- en medische gegevens worden verwerkt. Authenticatie op het betrouwbaarheidsniveau eIDAS hoog is ook noodzakelijk voor lokale toegang.

Hoewel het wetsvoorstel zich primair richt op toegang tot het BSN-register via de SBV-Z en toegang tot zorginformatie- en uitwisselingssystemen, wordt breder gebruik voor bijvoorbeeld toegang tot interne systemen of gebouwen niet uitgesloten. Sterker nog; door de inlogmiddelen en de identiteiten uit het register zowel voor interne als externe doeleinden te gebruiken kan meer uniformiteit en efficiëntie behaald worden. In de toelichting is dit verduidelijkt.

11.1.2 Verplichting wetsvoorstel DIAZ

Uit verschillende reacties op de internetconsultatie blijkt dat er uit wordt gegaan van een verplichting om de goedkeurde inlogmiddelen breed te gaan gebruiken in de zorg. Vanuit de verplichting gedacht zijn er grote zorgen over de implementatie, overgangstermijn en kosten.

Het wetsvoorstel DIAZ betreft evenwel geen verplichting voor het gebruik van het register en de inlogmiddelen voor toegang tot alle zorginformatie- en uitwisselingssystemen die een zorgaanbieder gebruikt. Deze verplichting geldt alleen voor toegang tot de SBV-Z, waar nu uitsluitend UZI-middelen voor kunnen worden gebruikt.

Vanuit bestaande wet- en regelgeving bestaat ook zonder de wet DIAZ de plicht om medische gegevens goed te beveiligen en de toegang tot deze gegevens op het hoogste betrouwbaarheidsniveau in te regelen. Met het wetsvoorstel wordt het mogelijk gemaakt andere (erkende) inlogmiddelen te gebruiken dan de huidige UZI-middelen en het register breder in te zetten dan voor toegang tot de SBV-Z. Bij het in werking treden van de wet ontstaat een overgangstermijn waar huidige inlogmiddelen gebruikt kunnen blijven worden, en de mogelijkheid wordt gecreëerd om de overstap te maken naar de nieuwe inlogmiddelen. Op dit moment is nog niet bepaald wanneer de huidige UZI-middelen (de UZI-pas) uitgefaseerd worden. Dat is sterk afhankelijk van de beschikbaarheid van voldoende verschillende alternatieve erkende inlogmiddelen op het betrouwbaarheidsniveau eIDAS hoog. Onder de Wdo zijn DigiD en eHerkenning beschikbaar. Nieuwe (private) inlogmiddelen worden verwacht wanneer erkenning onder het Wdo stelsel of certificering op basis van NEN 7518 mogelijk is.

Zorgspecifieke middelen (zoals personeelspassen) die op dit moment al gebruikt worden voor toegang tot medische gegevens vallen onder de verantwoordelijkheid van de zorgaanbieder en kunnen gebruikt blijven worden. Het gebruik van de onder dit wetsvoorstel goedgekeurde inlogmiddelen en het register voor die doeleinden is immers niet verplicht. Wanneer deze middelen toetreden tot het UZI-stelsel en daarmee identiteiten vanuit het UZI-register gebruiken zullen de middelen aan de eisen van NEN 7518 moeten voldoen en goedgekeurd moeten worden door de minister. Vanaf dat moment kunnen deze middelen ook gebruikt worden om SBV-Z te raadplegen.

11.1.3 Gekwalificeerde elektronische handtekening

Verschillende reacties vragen om meer duidelijkheid ten aanzien van de gekwalificeerde elektronische handtekening, een huidige functionaliteit van de UZI-pas. Het kunnen zetten van een gekwalificeerde elektronische handtekening is noodzakelijk om het zorgproces soepel te laten verlopen.

Terecht is opgemerkt dat de toelichting van het wetsvoorstel meer duidelijkheid over de gekwalificeerde elektronische handtekening moet scheppen. Met de huidige UZI-pas kan een zogenaamde gekwalificeerde elektronische handtekening worden gezet. Ook in de toekomstige situatie met de verschillende goedgekeurde inlogmiddelen die onder het UZI-stelsel beschikbaar komen, blijft dit mogelijk. Het gebruik van de gekwalificeerde elektronische handtekening wordt in paragraaf 1.3 en 2.3 nader toegelicht.

11.1.4 Goedkeuren inlogmiddelen

Het CIBG zal na inwerkingtreding van dit wetsvoorstel de bevoegdheid krijgen om namens de minister inlogmiddelen goed te keuren, te schorsen of in te trekken. Dat betreft in ieder geval onder de Wdo erkende publieke en private inlogmiddelen, zorgspecifieke inlogmiddelen en PKI-o-servercertificaten. Deze middelen voldoen aan de eisen vanuit eIDAS. Verschillende reacties op de consultatie pleiten ook voor het toestaan van middelen die onder de eIDAS verordening zijn erkend (genotificeerd) door andere lidstaten van de Europese Unie.

eIDAS genotificeerde middelen die aan het hoogste betrouwbaarheidsniveau voldoen zijn in de basis geschikt. Echter, om een zorgidentiteit uit het register op te kunnen halen is het noodzakelijk dat het gebruikte Europese middel een (versleuteld) BSN kan ontsluiten. Dat betekent dat de gebruiker die dat Europese middel gebruikt, in een eerder stadium een BSN door de Nederlandse overheid moet zijn toegekend. Het BSN is de sleutel om via het UZI-register een zorgidentiteit te verkrijgen

(UZI/URA/Rolcode). Onder de Wdo en het zorgspecifieke stelsel is een grondslag gecreëerd om een BSN te kunnen verwerken. Dat geldt per definitie niet voor eIDAS middelen: deze middelen leveren een ander identificerend kenmerk dat in sommige gevallen, via het Nederlandse nationale eIDAS-knooppunt, kan worden omgezet in een BSN. Vandaar dat in het wetsvoorstel erkenning onder de Wdo of certificering onder NEN 7518 is opgenomen om tot het UZI-stelsel toe te kunnen treden. Een genotificeerd eIDAS middel dat een BSN bevat, moet gebruikt kunnen worden in de zorgsector. Daarom wordt deze categorie middelen nader toegelicht in onder andere in paragraaf 2.2.

11.1.5 eIDAS herziening (EDI-wallet)

Verschillende reacties op het wetsvoorstel wijzen op de herziening van eIDAS en de komst van de EDI-wallet. Het wetsvoorstel dient in lijn te zijn met deze Europese ontwikkeling en daarmee ook de rol die het CIBG gaat vervullen. Ook is het gebruik van de gekwalificeerde elektronische handtekening opgenomen als verplichte basisfunctionaliteit in de EDI-wallet onder de eIDAS-herziening.

Met dit wetsvoorstel wordt rekening gehouden met de herziening van eIDAS en de ontwikkeling van de Wdo. Het wetsvoorstel past binnen deze ontwikkelingen en is toekomstbestendig. Digitale wallets hebben de potentie om inlogmiddelen veilig én gebruiksvriendelijk te maken. Echter, de behoeften in het zorgveld zijn divers en digitale wallets zullen (voorlopig) niet de enige bruikbare inlogmiddelen in de zorg zijn. Het wetsvoorstel voorziet in het gebruik van wallets en 'niet-wallets' zoals het huidige DigiD.

Het register van zorgaanbieders wordt als authentieke bron ingezet voor het verstrekken van attributen van zorgaanbieders en zorgmedewerkers. Deze attributen kunnen in wallets worden opgeslagen, op inlogmiddelen worden gezet of eenmalig worden afgegeven. In dat laatste geval is het noodzakelijk bij iedere inlogpoging het BSN om te wisselen voor de zorgidentiteit. Voor 'niet-wallet'-gebaseerde inlogmiddelen zoals het huidige DigiD wordt altijd het UZI-register bevraagd. Bij het gebruik van dit type middel verwerkt het CIBG alle inlogpogingen.

11.1.6 Zorgspecifieke middelen NEN 7518

Het wetsvoorstel gaat uit van een NEN-norm (7518) voor de erkenning van zorgspecifieke middelen. De norm is nog niet beschikbaar en daarmee niet te beoordelen. In de reacties worden zorgen geuit over het effect op reeds in de praktijk gehanteerde inlogmiddelen. Ook wordt de bereidheid van leveranciers op certificering conform NEN 7518 in twijfel getrokken. Tegelijkertijd wordt het belang van het gebruik van zorgspecifieke middelen zoals een personeelspas benadrukt.

Beoogd is voor het certificeren van zorgspecifieke middelen naar de NEN 7518 te verwijzen. Terecht wordt opgemerkt dat deze norm nog niet beschikbaar is. Voor wat betreft de eisen aan inlogmiddelen zal de NEN 7518 zoveel mogelijk aansluiten bij de eisen vanuit eIDAS en de Wdo. Daarmee wordt geborgd dat er geen eIDAS/Wdo ondermijnende ingang wordt gecreëerd voor zorgspecifieke middelen en dat middelen aan dezelfde strenge eisen voldoen. Afwijkende eisen worden voorzien op het toepassingsdomein (uitsluitend voor de zorgsector, waar Wdo-middelen overheidsbreed ingezet moeten kunnen worden) en technische eisen om aan te kunnen sluiten op het koppelvlak van het CIBG. De norm wordt in lijn met bestaande eisen vanuit normen zoals de 7510, 7512 en 7513 opgeleverd.

De verwachting is dat de NEN 7518 in het tweede kwartaal van 2024 in publieke consultatie gaat en later in 2024 kan worden vastgesteld. NEN normen voor de zorg zoals de NEN 7510, 7512 en 7513 zijn door VWS afgekocht en daarmee gratis beschikbaar voor het veld. Hiervoor is een licentieovereenkomst met NEN afgesloten. Jaarlijks wordt vastgesteld welke normen binnen deze overeenkomst worden afgekocht.

11.1.7 Zorgmedewerker en het register

Diverse reacties op de internetconsultatie pleiten voor een inperking van de definitie van zorgmedewerker. Met de huidige definitie van zorgmedewerker (eenieder die werkzaamheden verricht of gaat verrichten voor een zorgaanbieder) bestaat de kans dat onbevoegden toegang krijgen tot gevoelige (persoons)gegevens. Registratie zou alleen mogelijk moeten zijn met een opleiding in de zorg. Daarnaast wordt meer duidelijkheid gevraagd omtrent de regeling voor het inschrijven, intrekken en uitschrijven in het register. Hierbij moeten de administratieve lasten voor zorgaanbieders worden beperkt.

Het UZI-register wordt hét register voor het verstrekken van identiteiten van zorgaanbieders en zorgmedewerkers. Hierbij maakt het register waar mogelijk gebruik van andere bronregisters zoals de BRP, KVK, LRZA en BIG. Hiermee worden administratieve lasten beperkt. Daarnaast wordt er een HRM-koppelingen ontwikkeld die zorgaanbieders kunnen gebruiken om de in-/door- en uitstroomprocessen van zorgmedewerkers geautomatiseerd te koppelen aan het register. Per AMvB worden de eisen aan inschrijvingen, intrekkingen en uitschrijvingen verder uitgewerkt.

De gedachte achter de definitie van zorgmedewerker is dat iedereen een UZI-nummer kan verkrijgen. Iedereen die medische gegevens elektronisch raadpleegt en/of uitwisselt moet uniek herkenbaar zijn. Dat zorgt voor transparantie voor de patiënt/cliënt die kan zien welke zorgmedewerker er in een dossier toegang heeft gehad of gegevens heeft uitgewisseld. Beperkingen op de definitie zorgmedewerker leiden tot minder flexibiliteit. Ook in de huidige situatie worden passen aan medewerkers zonder opleiding verstrekt. Een UZI-nummer kan alleen verkregen worden nadat een betrouwbare koppeling met de natuurlijk persoon (het BSN) is gemaakt. Van belang is echter dat met louter alleen een UZI-nummer geen toegang tot medische gegevens verkregen kan worden. Daarvoor zijn aanvullende kenmerken (attributen) nodig. Zo kan de koppeling van het UZI-nummer aan de rechtspersoon, de zorgaanbieder waar namens gehandeld wordt, worden gebruikt om een toegangsbesluit (door die zorgaanbieder) op te baseren. Dat geldt ook voor de koppeling van bevoegdheden (de zogenoemde rolcode) aan het UZI-nummer. Maatregelen die zijn opgelegd door tuchtcollege, strafrechter of IGJ kunnen leiden tot het intrekken van één of meer attributen (bijvoorbeeld een bevoegdheid). Het besluit tot toegang is een verantwoordelijkheid van de zorgaanbieder. In paragraaf 2.4 van deze toelichting is de keuze voor de definitie zorgmedewerker nader toegelicht.

11.1.8 Acceptatieplicht inlogmiddelen

Verschillende reacties roepen op tot waarborgen van de keuzevrijheid voor inlogmiddelen. Medewerkers gebruiken verschillende systemen en kunnen voor verschillende aanbieders werken. Daarbij zou het mogelijk moeten zijn om éénzelfde middel voor alle systemen te gebruiken. Als dat niet kan worden medewerkers alsnog verplicht over verschillende inlogmiddelen te beschikken.

Keuzevrijheid voor inlogmiddelen is een belangrijk uitgangspunt bij dit wetsvoorstel. De gedachte is dat medewerkers kunnen kiezen voor een middel dat past bij het werkproces en persoonlijke voorkeuren. Dat middel moet dan ook overal te gebruiken zijn; zorginformatie- en uitwisselingssystemen zouden niet moeten kunnen afdwingen dat één bepaald middel gebruikt moet worden. Hiermee wordt een ‘vendor lock-in’ beperkt en is de zorg- of jeugdhulpaanbieder niet volledig afhankelijk van één leverancier. Daarnaast wordt interoperabiliteit gewaarborgd en wordt voorkomen dat een medewerker een sleutelbos met veel verschillende inlogmiddelen nodig heeft om medische gegevens in te kunnen zien en uit te wisselen. Aan het wetsvoorstel is daarom de plicht toegevoegd dat wanneer van het UZI-register gebruik wordt gemaakt, ieder goedgekeurd middel gebruikt kan worden. Het CIBG zal zorg- en jeugdhulpaanbieders voorzien in een gestandaardiseerd koppelvlak waarmee alle goedgekeurde inlogmiddelen beschikbaar komen. Hiermee ontzorgt het CIBG het zorgveld. Voor de Wdo-middelen wordt daartoe het (technische) koppelvlak gebruikt dat voor de Wdo-middelen vereist is. Voor zorgspecifieke middelen een zorgspecifiek koppelvlak. In

paragraaf 2.3 is de acceptatieplicht toegelicht en artikel 15, eerste lid, is aangepast naar 'ieder goedgekeurd inlogmiddel'.

11.1.9 Gebruiksvriendelijkheid

Vanuit verschillende reacties op de internetconsultatie wordt het belang van gebruiksvriendelijke inlogmiddelen benadrukt. Dat geldt voor alle werkprocessen en in het bijzonder voor werkprocessen waar snel handelen van levensbelang is zoals op de SEH. Inloggen op het betrouwbaarheidsniveau eIDAS hoog vereist vaak meer handelingen en kan daarmee afdoen aan gebruiksvriendelijkheid.

Het belang van gebruiksvriendelijke inlogmiddelen die goed passen binnen het werkproces wordt onderschreven. Tegelijkertijd is het noodzakelijk met hoge mate van zekerheid te kunnen vaststellen wie medische gegevens heeft geraadpleegd, dan wel heeft uitgewisseld. Door authenticatieverklaringen op het betrouwbaarheidsniveau eIDAS hoog te herbruiken kan een werkbare én veilige situatie worden gerealiseerd.

Verder wordt opgemerkt dat inlogmiddelen op het hoogste betrouwbaarheidsniveau op dit moment nog niet op grote schaal beschikbaar zijn. Mede door de herziening van de eIDAS verordening en de nadere detaillering van de regelingen onder de Wdo vindt ontwikkeling van deze middelen nog volop plaats. Er wordt van uitgegaan dat deze middelen op eIDAS hoog gaan komen. De vraag is op welke termijn. De ontwikkelingen worden nauwlettend in de gaten gehouden. Totdat er verschillende alternatieve middelen op het betrouwbaarheidsniveau eIDAS hoog zijn, blijven de huidige UZI-middelen tevens beschikbaar.

11.1.10 Implementatie en financiële gevolgen

Uit de internetconsulatie blijkt dat er veel vragen zijn omtrent de financiële gevolgen van het wetsvoorstel. Zo wordt gevreesd voor hogere kosten door een toename in het gebruik van de nieuwe inlogmiddelen. Dat geldt ook voor het geschikt maken van personeelspassen zodat deze als zorgspecifiek middel ingezet kunnen worden.

In de toelichting is een ruwe kosteninschatting opgenomen van de financiële gevolgen van dit wetsvoorstel die nader onderzocht worden. De verwachting is dat de totale kosten die een zorgaanbieder kwijt is voor de authenticatie van de zorgmedewerkers zullen afnemen. Wanneer de middelen breder gebruikt worden, hoeft dat dus niet tot hogere verbruikskosten te leiden. Daarnaast kunnen andere methoden van inloggen die in het applicatielandschap van de zorgaanbieder voorkomen, vervangen worden door één oplossing. Dit spaart kosten uit van bijbehorende authenticatiemiddelen en taken en ondersteunende processen gericht op de (ICT-)ondersteuning van zorgmedewerkers gericht op die inlogmethoden.

Zodra het wetsvoorstel is aangenomen wordt bepaald wanneer de huidige UZI-middelen worden uitgefaseerd. Om de UZI-middelen te kunnen uitfaseren moeten er voldoende alternatieve middelen op het betrouwbaarheidsniveau eIDAS hoog beschikbaar zijn. Tot die tijd kunnen de UZI-middelen gebruikt worden zoals dat nu ook gebeurt. Continuïteit is het uitgangspunt. Bij uitfasering moet er een realistische overgangstermijn vastgesteld worden. Dat gebeurt in samenspraak met het zorgveld.

Het wetsvoorstel DIAZ betreft een wijziging in de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (Wabvpz) en de Jeugdwet. Met het wetsvoorstel wordt het mogelijk gemaakt verschillende erkende inlogmiddelen te gebruiken in het UZI-stelsel en het UZI-register zorg breed in te zetten voor het verstrekken van zorgidentiteiten aan zorgaanbieders en zorgmedewerkers. Deze verbreding is nodig omdat het huidige UZI-register bedoeld is om toegang te verlenen tot de SBV-Z.

Volgens de huidige planning kan de wet in 2025 in werking treden. Zodra het wetsvoorstel is aangenomen, is grootschalige implementatie mogelijk en kunnen - bij verschillende alternatieve inlogmiddelen – de huidige UZI-middelen worden uitgefaseerd.

11.2 Uitvoeringstoets CIBG

Het CIBG heeft het wetsvoorstel DIAZ als haalbaar en uitvoerbaar beoordeeld. Echter ziet het CIBG wel een aantal aandachtspunten. In deze paragraaf wordt ingegaan op de voornaamste punten van het CIBG.

Uitgifte van attributen

Het uitgeven van attributen is een nieuwe taak voor het CIBG. De regelgeving m.b.t. deze uitgifte is daarnaast nog in ontwikkeling. Het is nog niet te zeggen welke effecten (inrichting processen, systemen en financiën) deze regelgeving te weeg zullen brengen. Wel signaleert het CIBG dat beide factoren gevolgen kunnen hebben voor de uitvoering van de taak in de brede zin van het woord. Aangaande de onzekerheid omtrent de regelgeving, wenst het CIBG daarnaast het volgende aan te stippen. Het CIBG bemerkt in het huidige stelsel dat het stringente karakter van een privaat normenkader zich soms lastig verhoudt tot publiekrechtelijke normen als evenredigheid en zorgvuldigheid. Het CIBG voorziet dat ze met het nog te ontwikkelen regelgeving omtrent attributen mogelijk ook tegen uitdagingen op het snijvlak publiek- en privaatrecht zal aanlopen. Dit tezamen brengt een marge van onzekerheid met zich mee voor de uitvoering (in de brede zin) van deze specifieke taak. In regelgeving en met beleidsregels worden eventuele uitdagingen op het snijvlak publiek- en privaatrecht uitvoerbaar gemaakt.

Bevoegdhedenverdeling binnen het stelsel

Er dient een heldere afbakening te zijn van de stelselrollen en de bijbehorende verantwoordelijkheden. Denk hierbij o.a. aan de rol van (stelseleigenaar, uitvoerder en toezichthouder). Het CIBG vindt het bijvoorbeeld van belang om vast te leggen welke rollen de andere actoren zullen spelen bij besluiten, zoals het besluit tot intrekken van de goedkeuring van een (categorie van een) toegangsmiddel, waartoe het CIBG gemandateerd zal worden of bij het wijzigen van de norm waaraan een zorgspecifiek middel moet voldoen teneinde toegelaten te worden. In het nieuwe UZI afsprakenstelsel wordt een heldere afbakening van rollen opgenomen.

11.3 Toezicht- en Handhaafbaarheidstoets IGJ

De inspectie ziet vanuit het perspectief van toezicht en handhaafbaarheid en de uitvoering in de praktijk redenen tot aanpassing van het wetsvoorstel. Ten eerste vraagt de inspectie meer duiding bij de definities van de begrippen ‘inlogmiddel’ en ‘zorgmedewerker’. Ten tweede wordt meer duidelijkheid gevraagd ten aanzien van een aantal artikelen. Op basis van de toelichting is het voor de IGJ niet duidelijk hoe zorgmedewerkers aan inlogmiddelen komen en hoe de registraties in het register, in het bijzonder de werkgeversverificatie, uitgevoerd worden. Voor wat betreft het toezicht op de procedure en gronden voor weigering, schorsing of intrekking van een inschrijving in het register is het de IGJ niet duidelijk waarop in de praktijk wordt toegezien. Voor wat betreft het goedkeuren van inlogmiddelen vraagt de IGJ zich af waarom het noodzakelijk is zorgaanbieders de mogelijkheid te geven zorginformatiesystemen toegankelijk te maken. Daarnaast acht de IGJ zich niet de aangewezen toezichthouder op de goedgekeurde inlogmiddelen. De IGJ heeft namelijk geen deskundigheid om te beoordelen of goedgekeurde inlogmiddelen op enig moment (nog) voldoen aan betrouwbaarheidsniveau hoog. Wel ziet de IGJ een taak bij toezicht op de regels over het gebruik van inlogmiddelen als deze gebruikt worden voor toegang tot zorginformatiesystemen, omdat dit een relatie kan hebben tot de kwaliteit van zorg.

De begrippen ‘inlogmiddel’ en ‘zorgmedewerker’ zijn aangepast. Gebruik van een inlogmiddel wordt, zoals toegelicht in 11.1.1, niet beperkt tot elektronische gegevensuitwisseling in de zorg. Voor wat

de zorgmedewerker betreft gaat het om het verwerken van cliëntgegevens. Tevens is het doel van het register aangepast, zoals in 11.1.1 toegelicht.

In de toelichting (hoofdstuk 9) is nader beschreven hoe zorgmedewerkers aan een inlogmiddel komen en hoe initiële registraties en mutaties in het register plaatsvinden. Het verkrijgen van de inlogmiddelen is aan de zorgaanbieders en zorgmedewerkers. Initiële registraties en mutaties in het register kunnen gemakkelijk en laagdrempelig worden doorgegeven. Hierbij wordt zoveel mogelijk gebruik gemaakt van koppelingen met andere bronregisters zoals de BRP, KVK en BIG. De koppeling van de zorgmedewerker met de werkgever is net als in de huidige situatie een verantwoordelijkheid van de zorgaanbieder. Het CIBG zorgt ervoor dat actuele koppelingen inzichtelijk zijn voor zorgaanbieders.

De beheerder (het CIBG) zal op grond van artikel 14 en AMvB de procedure volgen voor inschrijving, weigering, schorsing of intrekking. De AP houdt toezicht op het misbruik van (persoons)gegevens door een ingeschrevene.

Toezicht op en handhaving van artikel 14a gaat over de goedgekeurde inlogmiddelen. In de basis beoordeelt een certificerende instelling of een middel aan het betrouwbaarheidsniveau hoog voldoet. Desalniettemin kunnen er signalen zijn van een inlogmiddel dat niet voldoende veilig is. In een dergelijk uitzonderlijk geval is het aan de minister om te bepalen hoe en wanneer de goedkeuring wordt ingetrokken. De Inspectie kan hier een ondersteunende rol in spelen. Niet door zelf de veiligheid van het middel te beoordelen maar door een inschatting te maken van hoe de intrekking van het middel de kwaliteit van zorg kan beïnvloeden. In een zeer uitzonderlijk geval kan de Inspectie haar bevoegdheden inzetten om te bewerkstelligen dat de betreffende zorgaanbieder informatie verschaft of om hem ertoe te bewegen maatregelen te treffen om de inlogmiddelen te vervangen opdat de continuïteit van de zorg niet in gevaar komt. Een dergelijke situatie zal zich doorgaans niet voor doen omdat zorgaanbieders normaliter zelf en in goed overleg al de benodigde maatregelen treffen. Paragraaf 5 is hierop aangepast.

11.4 Advies Adviescollege toetsing regeldruk (ATR)

Het ATR heeft de regeldrukgevolgen beoordeeld aan de hand van een toetsingskader. Zo is er gekeken naar nut en noodzaak, minder belastende alternatieven, werkbaarheid voor doelgroepen en of de gevolgen voor regeldruk volledig en juist in beeld zijn gebracht. Op dit laatstgenoemde heeft het ATR een opmerking gemaakt. De andere onderdelen van het toetsingskader geven geen aanleiding tot opmerkingen.

De opmerking van het ATR betreft de beschrijving en berekening van de regeldrukgevolgen. De toelichting vermeldt niet de omvang van extra regeldruk t.a.v. de inschrijvingen in het register in een geldbedrag (die bedraagt 5.000 x € 47,- = € 235.000,-). Hetzelfde geldt voor de mutaties die medewerkers moeten doorgeven. Het tijdsbeslag per mutatie is 2 minuten, zodat de totale regeldruk van de mutaties € 15.651 per 100.000 ingeschreven medewerkers bedraagt (2 minuten x 100.000 medewerkers x 10% x € 47,-).

De opmerking van het ATR is overgenomen en verwerkt in de toelichting paragraaf 9.4.

11.5 Advies Autoriteit Persoonsgegevens (AP)

De AP adviseert tot krachtiger overheidsoptreden om zorgaanbieders en zorgmedewerkers gebruik te laten maken van inlogmiddelen met betrouwbaarheidsniveau hoog om toegang te krijgen tot elektronische uitwisselingssystemen en zorginformatiesystemen. De AP adviseert hier een concrete termijn op te nemen, waarna zorgaanbieders verplicht de betreffende middelen moet gebruiken. Daarnaast heeft de AP opmerkingen over maatregelen die het gebruiksgemak verhogen maar tegelijkertijd het beveiligingsniveau kunnen verlagen, over het risico bij gebruik van privételefoons,

over het toelaten van zorgmedewerkers tot het register, over toegang tot andere diensten dan elektronische uitwisselingssystemen en zorginformatiesystemen, over de koppeling van HR-systemen, over de te grote nadruk op gegevensuitwisseling en over de verruiming van bevoegdheden van de IGJ.

Zorgaanbieders moeten op grond van bestaande wet- en regelgeving passende technische en organisatorische maatregelen treffen om medische gegevens van cliënten te beveiligen. Het wetsvoorstel richt zich op identificatie en authenticatie als onderdeel van de maatregelen die getroffen moeten worden. Zowel de regering als de AP hechten belang aan authenticatie op betrouwbaarheidsniveau hoog door zorg- en jeugdhulpaanbieders en medewerkers bij het raadplegen van cliëntgegevens.[19] Echter ziet de regering nu geen aanleiding om de inlogmiddelen die onder deze wet goedgekeurd kunnen worden, verplicht te stellen aan zorg- en jeugdhulpaanbieders voor gebruik van andere systemen dan de SBV-Z. Het wetsvoorstel stelt inlogmiddelen op het betrouwbaarheidsniveau hoog beschikbaar, neemt huidige obstakels weg en moedigt het gebruik aan. Totdat er verschillende alternatieve inlogmiddelen op het hoogste betrouwbaarheidsniveau beschikbaar zijn worden de huidige UZI-middelen in stand gehouden zodat er in ieder geval één inlogmiddel is dat voldoet aan betrouwbaarheidsniveau hoog. De verwachting is dat het wetsvoorstel bewerkstelligt dat het zorgveld de overstap kan maken naar veilige en werkbare inlogmiddelen, zonder daar een termijn aan te koppelen. Het stellen van een dergelijke termijn is op dit moment niet proportioneel. Het is immers aan zorgaanbieders om te bepalen hoe zij passende maatregelen treffen om cliëntgegevens te beveiligen op het betrouwbaarheidsniveau hoog. Dit kan met behulp van goedgekeurde inlogmiddelen, maar het staat zorgaanbieders vrij om dit, met uitzondering van het raadplegen van de SBV-Z, met andere inlogmiddelen te doen. Een plicht tot het gebruik van goedgekeurde inlogmiddelen grijpt dan ook te diep in op de ondernemingsvrijheid van zorgaanbieders. Een dergelijke plicht is daarnaast overbodig om dat zorgaanbieders reeds op grond van de AVG verplicht zijn om passende maatregelen te treffen. Ten slotte brengt een dergelijke plicht en termijn hoge kosten met zich mee voor de zorgaanbieders. Alle systemen met cliëntgegevens moeten immers aangepast worden. Vanzelfsprekend wordt de overstap naar inlogmiddelen op het betrouwbaarheidsniveau hoog gestimuleerd, gemonitord en geëvalueerd. Indien blijkt dat de overstap naar inlogmiddelen met het betrouwbaarheidsniveau hoog niet wordt gemaakt, kan worden overwogen om het gebruik van de onder dit wetsvoorstel goedgekeurde inlogmiddelen te verplichten voor andere systemen dan de SBV-Z.

In de toelichting is niet beoogd tot uitdrukking te brengen dat veilig inloggen omzeild zou mogen worden ten behoeve van het gebruiksgemak. De toelichting is hierop aangepast in paragraaf 9.2. Ook zijn de risico's bij het gebruik van een privételefoon opgenomen en nader toegelicht in paragraaf 6.6. Ook de beveiligingsrisico's die gepaard gaan met een koppeling tussen het UZI-register en HR-systemen voor het doorgeven van werkgever-werknemers relaties zijn toegelicht in 6.6.

Voor wat betreft het advies om het register zo in te richten dat alleen natuurlijke personen die aantoonbaar werkzaam zijn in de zorgsector, of dat binnen afzienbare tijd zullen zijn, kunnen worden ingeschreven wordt het advies niet overgenomen. Zoals toegelicht in 11.1.7 blijft het begrip zorgmedewerker ongewijzigd. De regering ziet niet in hoe de definitie van zorgmedewerker deuren opent voor misbruik. Om een UZI-nummer te verkrijgen wordt een hoog betrouwbare koppeling gemaakt met het BSN van de zorgmedewerker. Aanvullende (autorisatie)kenmerken (zoals bevoegdheden vanuit de wet BIG) worden met grote zorgvuldigheid toegekend. De zorgaanbieder is verantwoordelijk voor het verlenen van toegang van medewerkers en het toekennen van de juiste autorisaties die nodig zijn om het werk uit te kunnen voeren.

[19] De AP handhaaft op ten minste 2 factor authenticatie, betrouwbaarheidsniveau laag/substantieel. Volgt o.a. uit: Haga beboet voor onvoldoende interne beveiliging patiëntendossiers | Autoriteit Persoonsgegevens en Boete OLVG | Autoriteit Persoonsgegevens

Tot slot stelt de AP, net als verschillende reacties op de internetconsultatie, dat het wetsvoorstel een te grote nadruk legt op gegevensuitwisseling. Zoals toegelicht in 11.1.1 wordt dit advies overgenomen. Artikel 14, eerste lid is aangepast en ook de toelichting is hierop aangepast.

Artikelsgewijze toelichting

Artikel I: Wijziging van de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg

Onderdeel A – Artikel 1 (begripsbepaling)
Aan artikel 1 worden drie begripsbepalingen toegevoegd. In de begripsbepaling "inlogmiddel" wordt een middel omschreven waarmee een in het register als bedoeld in artikel 14 geregistreerde kan aantonen dat hij gerechtigd is toegang te verkrijgen tot bepaalde elektronische systemen die worden gebruikt voor gegevensuitwisseling in de zorg. Met het begrip "betrouwbaarheidsniveau hoog" is aangesloten bij artikel 8 van de eIDAS-verordening. Ten slotte wordt met "zorgmedewerker" eenieder bedoeld die werkzaamheden verricht voor een zorgaanbieder en daarbij client gegevens verwerkt. Hierbij is niet relevant of het gaat om een vrijwilliger, werknemer of ZZP'er. Ook kan het hier zowel gaan om zorgverleners als ondersteunend personeel. Onder zorgmedewerker wordt ten slotte ook verstaan diegene die werkzaam is geweest of in de toekomst werkzaam gaat zijn als zorgmedewerker. Beoogd wordt dat een zorgmedewerker desgewenst voortdurend ingeschreven kan staan in het register van zorgaanbieders, zodat het niet nodig is om na een wisseling van functie opnieuw ingeschreven te worden. Om te voorkomen dat in periodes dat een persoon niet werkzaam is als zorgmedewerker misbruik kan maken van de inschrijving, kan diegene die ingeschreven staat in het register pas cliëntgegevens raadplegen nadat zijn werkgever heeft geverifieerd dat hij hiertoe gerechtigd is. Zie hierover uitgebreider paragraaf 2.4 van het algemeen deel van deze toelichting.

De nieuw in te voegen begripsbepalingen zijn conform aanwijzing 5.69 geletterd met een #. Dit symbool wordt in de drukproeffase van het Staatsblad vervangen door de juiste lettering, op dat moment is namelijk duidelijk op welk onderdeel het nieuwe onderdeel zal aansluiten. Er zijn namelijk meerdere wetsvoorstellen die aan artikel 1 nieuwe onderdelen beogen toe te voegen, zoals de Verzamelwet gegevensverwerking VWS I.

Onderdeel B – Artikelen 14, 14a en 15 (registers en inlogmiddelen)

Artikel 14 (nieuw) – Het register van zorgaanbieders, zorgmedewerkers, indicatieorganen en zorgverzekeraars
In het nieuwe eerste en tweede lid van artikel 14 is, net als in het oude artikel 14, geregeld dat een register wordt ingesteld van zorgaanbieders, indicatieorganen en zorgverzekeraars, die worden beheerd door onze minister, ten behoeve van het verkrijgen van toegang tot de Sectorale Berichten Voorziening in de Zorg (SBV-Z) (artikel 3 Wabpvz). Met de SBV-Z kan toegang verkregen worden tot het burgerservicenummerregister. In het nieuwe artikel 14 is bepaald dat er één register is van zowel zorgaanbieders, zorgmedewerkers, indicatieorganen als zorgverzekeraars, in plaats van afzonderlijke registers per groep. Nieuw is daarnaast dat het register ook wordt ingesteld met het oog op de identificatie en authenticatie van zorgaanbieders en zorgmedewerkers in verband met onder meer het gebruik van elektronische uitwisselingssystemen en zorginformatiesystemen. In dat kader bevat artikel 14, derde lid, een grondslag om in het register ook zorgmedewerkers op te nemen, zij maken immers gebruik van deze systemen.

Het oude eerste en tweede lid van artikel 15 zijn met een aantal redactionele wijzigingen opgenomen in het nieuwe artikel 14, derde lid. Artikel 14, derde lid, onder b, bevat daarnaast een grondslag om nadere regels te stellen over het intrekken van een inschrijving in de registers. Hiervan kan bijvoorbeeld sprake zijn als de geregistreerde misbruik maakt van zijn inschrijving door onrechtmatig de SBV-Z te raadplegen. Op grond van het nieuw voorgestelde artikel 14, derde lid, onder c, kunnen bij of krachtens algemene maatregel van bestuur regels worden gesteld over het verwerken van persoonsgegevens, waaronder het burgerservicenummer, van diegenen die in het register worden ingeschreven. Ten slotte kunnen, net als in het huidige artikel 15, vijfde lid, bij of krachtens algemene maatregel van bestuur regels worden gesteld over het verlangen van een bijdrage van een in het register geregistreerde voor de kosten die met het register gepaard gaan.

Artikel 14a (nieuw) – Goedkeuring inlogmiddelen

In het eerste lid is bepaald dat de Minister goedkeuring verleend aan een inlogmiddel indien dit middel en de koppeling van dit middel aan de gebruiker voldoet aan het betrouwbaarheidsniveau hoog. De minister kan tevens goedkeuring geven aan bepaalde categorieën van inlogmiddelen. Hierbij kan gedacht worden aan het gelijktijdig goedkeuren van de onder de Wet digitale overheid erkende identificatiemiddelen of de identificatiemiddelen die door een lidstaat van de Europese Unie ingevolge de eIDAS-verordening zijn goedgekeurd. In het tweede lid is bepaald dat bij of krachtens algemene maatregel van bestuur regels worden gesteld over de wijze waarop aangetoond kan worden dat dit betrouwbaarheidsniveau is bereikt. Zoals toegelicht in paragraaf 2.5 van het algemeen deel van deze toelichting kan dit in ieder geval door erkend te zijn onder de Wdo, gecertificeerd te zijn onder de NEN 7518 of door te beschikken over een PKI-overheidscertificaat. Over de wijze waarop een aanvraag tot goedkeuring ingediend kan worden en het verstrekken van de hierbij benodigde gegevens, worden bij of krachtens algemene maatregel van bestuur regels gesteld.

Bij of krachtens algemene maatregel van bestuur worden tevens regels gesteld over het verlenen, weigeren, schorsen of intrekken van goedkeuring. Van schorsing of intrekking kan sprake zijn als het betreffende inlogmiddel niet langer voldoet aan het betrouwbaarheidsniveau hoog. Voor inlogmiddelen die categoraal zijn goedgekeurd, zullen bij of krachtens algemene maatregel van bestuur regels worden gesteld die mogelijk maken dat die goedkeuring zo nodig per individueel inlogmiddel ingetrokken of geschorst kan worden. Als er aanwijzingen zijn dat een middel hier niet langer aan voldoet wordt hierover op verzoek of uit eigen beweging informatie verstrekt door de in een register ingeschreven zorgaanbieder, indicatieorgaan of zorgverzekeraar die het betreffende middel in gebruik heeft, door diegene aan wie goedkeuring verleend is en door de verstrekker van het bewijsmiddel op basis waarvan de goedkeuring is verleend.

Artikel 15 (nieuw) – Inlogmiddelen
In het eerste lid is bepaald dat in het geval een voorziening of systeem door een geregistreerde wordt gebruik in combinatie met het register, dat in dat geval deze voorziening of dit systeem gelijkelijk gebruikt kan worden met ieder goedgekeurd inlogmiddel (zie uitgebreider paragraaf 2.5 van het algemeen deel van de toelichting). Het woord ‘gebruikt’ heeft een brede betekenis, zo kan hieronder worden verstaan het gebruik van een inlogmiddel om toegang te krijgen tot een systeem, het gebruik van dit middel om een elektronische handtekening te zetten, het raadplegen van een voorziening of systeem, maar ook nu nog niet voorziene toepassingen die mogelijk in de toekomst ontstaan en raken aan de identificatie en authenticatie van een zorgaanbieder of zorgmedewerker.

Tevens is in het tweede lid bepaald dat zorgaanbieders en zorgmedewerkers de goedgekeurde inlogmiddelen kunnen gebruiken met onder meer elektronische uitwisselingssystemen en zorginformatiesystemen indien de zorgaanbieder zijn systemen hiervoor openstelt. Het is hiermee ook mogelijk om de inlogmiddelen te gebruiken voor systemen waarbij niet het verwerken of uitwisselen van gegevens centraal staat. Het is aan de zorgaanbieder om te bepalen aan wie en onder welke voorwaarden toegang tot zijn systemen wordt verleend.

Toegang tot de systemen van de zorgaanbieder en de SBV-Z kan verkregen worden met een goedgekeurd inlogmiddel. Dit middel wordt gekoppeld aan een in het register geregistreerde (derde lid). Indien een inlogmiddel wordt gekoppeld aan een natuurlijk persoon kunnen hierbij persoonsgegevens verwerkt worden, waaronder het burgerservicenummer. Zoals toegelicht in paragraaf 6 van het algemeen deel van deze toelichting is deze gegevensverwerking noodzakelijk om te garanderen dat het middel aan de juiste inschrijving in het register wordt gekoppeld.

Bij of krachtens algemene maatregel van bestuur kunnen regels worden gesteld over de toegang met een goedgekeurd inlogmiddel tot de SBV-Z, en elektronische uitwisselings- en zorginformatiesystemen, het koppelen van deze middelen aan een in het register geregistreerde en de verwerking van gegevens bij deze koppeling (vierde lid). Een voorbeeld hiervan is dat bij algemene maatregel van bestuur bepaald kan worden dat een zorg- of jeugdhulpmedewerker enkel SBV-Z kan raadplegen indien door de zorgaanbieder geverifieerd is dat dit noodzakelijk is.

Onderdeel C – artikel 16 en 16a (toezicht)
Met het wetsvoorstel Verzamelwet gegevensverwerking VWS II wordt voorgesteld een nieuw hoofdstuk 3b toe te voegen aan de Wabvpz, waarin toezicht en handhaving wordt geregeld. Hiermee gaat de Inspectie toezicht houden op een deel van de Wabvpz. De Minister kan tevens zo nodig een dwangsom opleggen of een schriftelijke aanwijzing geven. Met onderdeel C van dit wetsvoorstel worden de artikelen 16 en 16a gewijzigd, zodat ook toezicht gehouden kan worden op het nieuwe artikel 14a. Zoals nader is toegelicht in paragraaf 5 van het algemeen deel van deze toelichting, wordt hiermee beoogd dat in uitzonderlijke situaties toezicht gehouden kan worden op het borgen dat de goedgekeurde inlogmiddelen blijvend beschikken over het betrouwbaarheidsniveau hoog. Indien van toepassing zullen op een later moment in dit wetsvoorstel de benodigde samenloopbepalingen met het wetsvoorstel Verzamelwet gegevensverwerking VWS II opgenomen worden.

Onderdeel D – Artikel 18 (overgangsrecht)
Het nieuwe artikel 18 voorziet in een overgangsperiode waarmee artikel 15, zoals dit artikel luidde voor de inwerkingtreding van de onderhavige wet, van toepassing blijft op middelen die zijn verstrekt vóór de inwerkingtreding van deze wet. De exacte duur van deze overgangsperiode wordt bij of krachtens algemene maatregel van bestuur bepaald. Beoogd wordt dat deze periode in ieder geval zo lang is dat reeds verstrekte middelen gebruikt kunnen blijven worden voor de termijn waarvoor zij zijn verstrekt. Mogelijk wordt de overgangsperiode langer indien dit noodzakelijk is voor overstap van de huidige inlogmiddelen naar de nieuwe middelen.

Onderdeel E – (vervallen overgangsrecht)
In onderdeel E is bepaald dat het nieuwe artikel 18 vervalt. Beoogd wordt dit onderdeel bij koninklijk besluit in werking te laten treden – en dus artikel 18 (nieuw) te laten vervallen – nadat het overgangsrecht is uitgewerkt.

Artikel II: Wijziging van de Jeugdwet

Net als de Wabpvz bevat de Jeugdwet een tweetal bepalingen, artikelen 7.2.7 en 7.2.8, op basis waarvan, kort gezegd, jeugdhulpaanbieders met een door de minister verstrekt middel toegang kunnen krijgen tot de SBV-Z, waarmee het burgerservicenummer geraadpleegd kan worden. Jeugdhulpaanbieders worden hiertoe ingeschreven op een autorisatielijst. Met dit wetsvoorstel worden deze artikelen in lijn gebracht met de nieuwe artikelen 14 en 15 Wabpvz. Voor een toelichting op deze wijzigingen wordt verwezen naar de toelichting bij artikel I. Anders dan in de Wabpvz kent de Jeugdwet geen definities van elektronische uitwisselingssystemen en zorginformatiesystemen, daarom wordt in, artikel 7.2.7, eerste lid, onder b, in het algemeen gesproken over elektronische systemen waarin gegevens van jeugdigen worden verwerkt. Het gaat hier om systemen waarin bijvoorbeeld dossiers van jeugdigen worden bijgehouden of uitgewisseld. Daarnaast is van belang dat in de Jeugdwet geen afzonderlijke bepaling wordt opgenomen over de goedkeuring van inlogmiddelen. Hiervoor wordt verwezen naar artikel 15 van de Wabpvz, hierin is de goedkeuring van deze middelen reeds afdoende geregeld. Ten slotte wordt in artikel 10.2 een overgangsbepaling opgenomen voor reeds op grond van artikel 7.2.7 verstrekte middelen, voor een toelichting hierop wordt verwezen naar de toelichting bij artikel 18 van de Wabpvz.

Artikel III: Inwerkingtreding

Beoogd wordt om deze wet, met uitzondering van artikel I, onderdeel E, bij koninklijk besluit in werking te laten treden op 1 januari 2025. Het hiervoor genoemde onderdeel kan inwerkingtreden als het overgangsrecht zoals opgenomen in artikel 18 van de Wabpvz is uitgewerkt.

De Minister van Volksgezondheid,
Welzijn en Sport

C. Helder