Wijziging van de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg 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 en zorgverzekeraars, 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 ingevoegd, luidende:

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

#. *betrouwbaarheidsniveau hoog:* het 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*: eenieder die werkzaamheden verricht of gaat verrichten voor een zorgaanbieder en daarbij clientgegevens raadpleegt met behulp van een goedgekeurd inlogmiddel.

B

Hoofdstuk 3 komt als volgt te luiden:

Hoofdstuk 3. Identificatie en authenticatie

Artikel 14

1. Er wordt een register van zorgaanbieders, zorgmedewerkers, indicatieorganen en zorgverzekeraars ingesteld, om:
   a. hen toegang te kunnen verlenen tot voorzieningen waarmee het burgerservicenummer van een cliënt opgevraagd kan worden ten behoeve van het vaststellen van zijn identiteit; en
   b. de identificatie en authenticatie van de in het register ingeschreven zorgaanbieders en zorgmedewerkers mogelijk te maken bij elektronische gegevensuitwisseling in de zorg.
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 en zorgverzekeraar in het register;
b. de procedure en gronden voor weigering of intrekking van een inschrijving in het register;
c. het verwerken van gegevens van zorgaanbieders, zorgmedewerkers, indicatieorganen en zorgverzekeraars in het register, waaronder kan worden verstaan het verwerken van persoonsgegevens zoals burgerservicenummer;
d. het verlangen van bijdragen van de in een register opgenomen zorgaanbieders, zorgmedewerkers, indicatieorganen en zorgverzekeraars in de kosten van het betreffende register.

Artikel 14a
1. Een in het register, bedoeld in artikel 14 ingeschrevene kan, met een op grond van artikel 15 goedgekeurd inlogmiddel, toegang krijgen tot de voorzieningen, bedoeld in artikel 3, eerste lid, onder c en d, van de Wet algemene bepalingen burgerservicenummer.

2. Een in het register ingeschreven zorgaanbieder of zorgmedewerker kan met een goedgekeurd inlogmiddel toegang krijgen tot elektronische uitwisselingssystemen en zorginformatiesystemen.

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

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

Artikel 15
1. Onze Minister verleent goedkeuring aan een inlogmiddel als dit middel en indien van toepassing, de koppeling van dit middel aan een in een register ingeschrevene, 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 ingeschrevene voldoet aan het betrouwbaarheidsniveau hoog, zoals een aan te wijzen certificaat of toelating;
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, ingeschrevene;
    2º. diegene van wie het inlogmiddel is goedgekeurd;
    3º. de verstrekker van een bewijsmiddel als bedoeld in onderdeel a.
e. de verwerking van gegevens die noodzakelijk is voor de uitvoering van dit artikel.

C

In de artikelen 16 en 16a wordt na ‘artikelen 5 tot en met 12,’ ingevoegd ’14 tot en met 15,’.

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 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
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 te kunnen leveren, moeten zorgmedewerkers 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 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[1] 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 patiëntgegevens) 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, indicatieorganen en zorgverzekeraars persoonsgegevens van patiënten verifiëren bij de basisregistratie personen (hierna: BRP). Na registratie van de zorgaanbieder 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, 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 hebben 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, zorgmedewerkers, indicatieorganen en zorgverzekeraars. Ingeschrevenen krijgen de keuze tussen verschillende goedgekeurde inlogmiddelen die voldoen aan het betrouwbaarheidsniveau hoog. Met deze middelen kunnen alle geverifieerde ingeschrevenen toegang krijgen tot SBV-Z. Zorgaanbieders en zorgmedewerkers kunnen deze inlogmiddelen daarnaast gebruiken om elektronische uitwisselingssystemen te raadplegen. Het UZI-register verstrekt voor deze toepassingen identificerende kenmerken van ingeschrevenen bij het gebruik van inlogmiddelen. De ingeschrevenen zijn zorgaanbieders, zorgmedewerkers, indicatieorganen en zorgverzekeraars. Met dit register en deze inlogmiddelen wordt identificatie en authenticatie gebruiksvriendelijk, flexibel en kunnen kosten worden gereduceerd. Dit draagt bij aan het invullen en geschikt maken van de 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

[1] Zie de moties Van den Berg en Kerstens Kamerstukken II 2020/21, 27 529, nr. 222 en nr. 223.

gegevensuitwisseling in de zorg noodzakelijk. De toegang van zorgaanbieders en zorgmedewerkers 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 is vertrouwen namelijk essentieel. Zorgaanbieders moeten erop kunnen vertrouwen dat andere zorgaanbieders de digitale toegang van zorgmedewerkers 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 zorgaanbieders, zorgmedewerkers, indicatieorganen en zorgverzekeraars 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 patiëntgegevens 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 SBV-Z. Na registratie in het register en verificatie worden zogenoemde UZI-passen aan gebruikers verstrekt. De UZI-pas wordt uitgelezen met behulp van een kaartlezer en is een soort elektronisch paspoort. Daarnaast kan ook een servercertificaat worden uitgegeven voor systemen van organisaties die 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[2] (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 medische gegevens. De betrouwbaarheidsniveaus geven aan met welke zekerheid de identiteit is vastgesteld. 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). Het UZI-register voldoet hiertoe aan de normen van de Public Key Infrastructure voor de overheid (PKI-o). Dat maakt

[2] 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.

het een hoogwaardig en betrouwbaar certificaat. Het 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[3]) 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.

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 zorgaanbieders en zorgmedewerkers was altijd al van belang, maar is door de opkomst van netwerkzorg en digitalisering in toenemende mate noodzakelijk. Voor het veilig uitwisselen van medische gegevens is inloggen op het hoogste betrouwbaarheidsniveau vereist (eIDAS niveau 'hoog').[4] Echter, inloggen op het hoogste betrouwbaarheidsniveau gebeurt nauwelijks in de zorgsector en beperkt zich vrijwel alleen tot toepassingen waar de huidige UZI-middelen worden gebruikt. In de zorgsector worden namelijk veel verschillende inlogmethoden gebruikt die vaak niet aan het vereiste betrouwbaarheidsniveau voldoen. Daarnaast worden zorgaanbieders en zorgmedewerkers 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 bedoeld: het vermogen van organisaties (en hun processen en systemen) om effectief en efficiënt gegevens uit te wisselen met hun omgeving.

Het zorgveld[5] ziet het UZI-register als een zeer bruikbaar instrument om zorgaanbieders en zorgmedewerkers 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 zorgaanbieders en zorgmedewerkers. Hierdoor kan het niet bijdragen aan het veilig raadplegen van cliëntgegevens op het betrouwbaarheidsniveau hoog. Ook bestaat het risico dat UZI-passen tussen zorgmedewerkers uitgeleend worden. In dat geval gebruiken meerdere zorgmedewerkers één identiteit.

De beperkte adoptie van de UZI-pas wordt versterkt doordat de huidige UZI-pas niet gebruiksvriendelijk is en niet past binnen elk zorgproces. De UZI-pas (met bijbehorende kaartlezer) werkt namelijk niet op mobiele apparaten zoals een smartphone of tablet en is daarmee niet voor ieder zorgproces 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,

[3] 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.
[4] 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.
[5] Onder het zorgveld verstaan wij zorgaanbieders, zorgmedewerkers, koepelorganisaties, leveranciers, programma's voor gegevensuitwisseling en belanghebbende organisaties. Het zorgveld is o.a. geconsulteerd via het Informatieberaad zorg, klankbordgroepen en expertsessies.

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 zorgveld 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, wachtwoorden, eventueel aangevuld met een tweede authenticatiefactor. Uit de artikel 14 van de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (hierna: Wabvpz) 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 (de UZI-pas voor zorgmedewerkers en het servercertificaat voor systemen) 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 – dat identificatie en authenticatie van onder meer zorgaanbieders en zorgmedewerkers mogelijk maakt – uit te breiden naar elektronische uitwisselingssystemen. In artikel 14 van de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (Wabvpz) is namelijk bepaald dat het UZI-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.

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 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 clientgegevens 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 een 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, zorgmedewerkers, zorgverzekeraars en indicatieorganen 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 en PKI-o-middelen.

2) Het UZI-register wordt ingezet voor het verstrekken van identificerende kenmerken (attributen) ten behoeve van het digitaal identificeren van zorgaanbieders en zorgmedewerkers voor toegang tot uitwisselings- en zorginformatiesystemen (naast de al bestaande toegang tot SBV-Z) ten behoeve van elektronische gegevensuitwisseling in de zorg. Dit onderdeel is niet van toepassing op zorgverzekeraars en indicatieorganen omdat zij geen gebruik mogen en kunnen maken van deze uitwisselings- en zorginformatiesystemen.

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. Wijzigingen in het register kunnen 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 zorgaanbieders 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 zorgaanbieders en zorgmedewerkers. 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 zelf 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 zorgaanbieders, 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 elektronische uitwisselings- of zorginformatiesystemen ten behoeve van elektronische gegevensuitwisseling in de zorg. Deze oplossing is in samenwerking met het zorgveld tot stand gekomen en door hen goed ontvangen.[6] 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.[7] In aanloop naar grootschalige implementatie worden verschillende pilots uitgevoerd in delen van het zorgveld waarbij verschillende zorgmedewerkers 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

[6] Dat is gebeurd in het Informatieberaad Zorg (IB), klankbordgroepen, expertsessies en individuele gesprekken met het zorgveld.
[7] TNO rapport "Toekomstbestendig maken van UZI middelen" Zie hierover: https://www.gegevensuitwisselingindezorg.nl/uzi-middelen/nieuws/2022/07/05/onderzoek-tno-naar-gebruik-inlogmiddelen

verkrijgen tot een applicatie waarmee vaccinatiegegevens naar het RIVM gestuurd kunnen worden. Hiermee is in de praktijk beproefd of de voorgestelde oplossingsrichting werkbaar is. De deelnemende artsen hebben een positieve gebruikerservaring gedeeld.[8] 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 elektronische gegevensuitwisseling in de zorg

Zoals toegelicht in paragraaf 2.2 vloeit uit artikel 14 van de Wabvpz dat het UZI-register bedoeld is om het raadplegen van SBV-Z mogelijk te maken voor diegenen die in het register zijn ingeschreven. Momenteel is het dan ook niet mogelijk om het UZI-register en de bijbehorende middelen te gebruiken voor het inloggen in elektronische uitwisselingssystemen ten behoeve van elektronische gegevensuitwisseling in de zorg. Hierdoor kunnen de huidige en nieuwe inlogmiddelen – die veilig inloggen op het betrouwbaarheidsniveau hoog mogelijk maken – niet gebruikt worden voor de andere systemen die een zorgaanbieder of zorgmedewerker gebruiken. Dit is problematisch omdat er momenteel nauwelijks andere inlogmiddelen met het betrouwbaarheidsniveau hoog voor handen zijn. In de zorg wordt daarom nog vaak gebruik gemaakt van inlogmiddelen die beschikken over een lager beveiligingsniveau. Dit beperkt evenwel de mogelijkheid om veilig clientgegevens uit te wisselen.

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 ten behoeve van elektronische gegevensuitwisseling in de zorg. 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 zorgaanbieders en zorgmedewerkers om elektronisch gegevens uit te kunnen wisselen.

Behoudens het gebruik van SBV-Z is het aan zorgaanbieders om te bepalen in hoeverre zij de nieuwe inlogmiddelen willen gebruiken voor eigen elektronische uitwisselingssystemen. Er is dan ook niet voor gekozen om het gebruik van het UZI-register en de bijbehorende middelen verplicht te stellen voor het raadplegen van alle uitwisselingssystemen van de zorgaanbieders. Zorgaanbieders kunnen namelijk ook eigen inlogmiddelen gebruiken die over het juiste betrouwbaarheidsniveau beschikken. Het is immers in beginsel aan de zorgaanbieder om 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 van zorgaanbieders grote lasten met zich voor de zorgaanbieders. Zij zouden dan immers alle elektronische uitwisselingssystemen die zij gebruiken 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 om zorgaanbieders de mogelijkheid te geven om de nieuwe inlogmiddelen breed te gebruiken, maar om ook ruimte te laten voor de zorgaanbieder 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 clientgegevens geraadpleegd worden met inlogmiddelen met het betrouwbaarheidsniveau hoog.

2.4 Zorgmedewerkers registeren in het UZI-register

Met dit wetsvoorstel kunnen zorgmedewerkers zich laagdrempelig inschrijven in het UZI-register. Met zorgmedewerker wordt eenieder bedoeld die werkzaam is of wil zijn in de zorg. Nadat een zorgmedewerkers is ingeschreven verifieert de zorgaanbieder of de zorgmedewerker bij hem werkzaam is en of hij toegang moet kunnen krijgen tot SBV-Z of andere elektronische uitwisselingssystemen die de zorgaanbieder gebruikt. Er is dus nadrukkelijk een extra handeling van de zorgaanbieder noodzakelijk alvorens een zorgmedewerker toegang kan krijgen tot SBV-Z. Louter de inschrijving in het UZI-register is dan ook niet voldoende om clientgegevens te kunnen raadplegen, die toegang moet verstrekt worden door de werkgever van de zorgmedewerker,

[8] 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.

namelijk de zorgaanbieder. Het is van belang dat de zorgmedewerker 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 zorgaanbieder waar de zorgmedewerker voor gaat werken, kan vervolgens immers aangeven dat de zorgmedewerker die reeds staat ingeschreven bijvoorbeeld toegang moet krijgen tot SBV-Z of bepaalde eigen elektronische uitwisselingssystemen. Een voortdurende inschrijving voorkomt dan ook administratieve lasten voor de zorgmedewerker.

Laagdrempelige inschrijving van zorgmedewerkers 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 zorgmedewerkers die bijvoorbeeld 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 clientgegevens 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 clientgegevens.

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 medische gegevens 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 drie verschillende bewijsmiddelen kunnen leiden tot goedkeuring van een inlogmiddel, namelijk erkenning onder de Wdo, certificering onder de NEN 7518[9] van zorgspecifieke middelen en een PKI-o-certificering. Hierdoor zullen via verschillende wegen verschillende middelen goedgekeurd worden die allen beschikken over het betrouwbaarheidsniveau hoog, maar qua 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 Onze 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 of het inlogmiddel beschikt over het juiste betrouwbaarheidsniveau. Beoogd wordt dat als een inlogmiddel beschikt over erkenning onder de Wdo, certificering onder de NEN 7518 of een PKI-o-certificaat, 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. Onze 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. Toegang tot de SBV-Z kan in vervolg verkregen worden met Wdo-middelen, zorgspecifieke middelen en met servercertificaten die worden

[9] NEN 7518 identificatie en authenticatie EGIZ

uitgegeven door een TSP welke is erkend onder het PKI-o stelsel.[10] Deze servercertificaten voldoen aan dezelfde strenge eisen ten aanzien van betrouwbaarheid als de servercertificaten die het CIBG op dit moment uitgeeft. 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.[11] Met de Wdo wordt ruimte gecreëerd om onder strikte voorwaarden een publiek identificatiemiddel ter uitoefening van een private taak te gebruiken. In de zorgsector gaat het concreet om het gebruik van DigiD voor de identificatie en authenticatie van zorgmedewerkers. Voor het gebruik van dit publieke inlogmiddel biedt de Wdo een juridische grondslag. Op dit moment is er geen juridische grondslag voor het gebruik van een onder de Wdo erkend privaat inlogmiddel voor de identificatie en authenticatie van zorgmedewerkers. 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. Hiertoe moet Onze Minister het middel goedkeuren, aangezien deze middelen reeds onder de Wdo erkend zijn al middel kan Onze Minister vervolgens desgewenst direct overgaan tot goedkeuring.

2.5.2 Zorgspecifieke inlogmiddelen (gecertificeerd onder de NEN 7518)

Gezien de grote diversiteit aan zorg die in Nederland verleend wordt, is het van belang dat er verschillende zorgspecifieke middelen beschikbaar komen die identificatie en authenticatie van zorgmedewerkers 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 zorgveld 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 zorgveld, 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 gebruikt kunnen worden. Een zorgspecifiek middel is een elektronisch middel voor identificatie en authenticatie ten behoeve van digitale gegevensuitwisseling in de zorg, dat onder de verantwoordelijkheid van de zorgaanbieder wordt uitgereikt aan zijn zorgmedewerkers.

Deze zorgspecifieke middelen voldoen op onderdelen niet aan de eisen die aan de Wdo-middelen worden gesteld en zullen dus niet onder de Wdo erkend worden. Zo is bijvoorbeeld de toepasbaarheid van deze middelen beperkt tot de zorg (door het gebruik van het UZI-nummer als identificerend nummer) en zal het middel daarmee niet breed bruikbaar zijn bij de organisaties die onder het regime van de Wdo vallen (zoals een gemeente of de Belastingdienst). Ook kan niet iedere Nederlander een zorgspecifiek middel verkrijgen: de uitgifte van de zorgspecifieke middelen is beperkt tot diegenen die staan ingeschreven in het UZI-register. 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 zorgveld is gebleken dat zij ook in de toekomst van deze zorgspecifieke middelen gebruik willen blijven maken. Zorgmedewerkers werken namelijk met een

[10] Het PKIoverheid-certificaat (Public Key Infrastructure) is een computerbestand dat werkt als een digitaal paspoort.
[11] Ter verduidelijking: Wdo erkende inlogmiddelen genereren een BSN. Het BSN wordt niet gebruikt om natuurlijke personen te identificeren voor toegang tot uitwisselingssystemen of zorginformatiesysteem. 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.

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 Wdo-middelen en de PKI-o-certificaten, heeft een aantal voordelen.

Ten eerste sluiten de zorgspecifieke middelen goed aan bij bestaande zorgprocessen. 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 zorgmedewerkers. Hoe meer verschillende authenticatiemiddelen kunnen worden ingezet, hoe meer keuzevrijheid en adaptatie van de oplossingsrichting in het zorgveld. Ten derde kunnen zorgmedewerkers blijven werken met de zorgspecifieke middelen waarmee zij nu al inloggen. Deze middelen moeten natuurlijk wel eerste worden goedgekeurd aan de hand van een certificaat. Het is immers van belang dat middelen gebruikt worden met het betrouwbaarheidsniveau hoog.

Certificering en goedkeuring van zorgspecifieke middelen

Zoals hiervoor toegelicht is het van belang dat, naast de 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 het betrouwbaarheidsniveau hoog. Bij zorgspecifieke middelen kan dit onder meer aangetoond worden aan de hand van certificering onder de NEN 7518. Het certificaat dat hiermee verkregen wordt kan fungeren als bewijsmiddel op basis waarvan Onze 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. Voor zorgspecifieke middelen is de NEN 7518 ontwikkeld. In het certificeringsschema is daarnaast 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 gebruik gaan maken van het UZI-register. Deze regels gaan zien op onder meer welke versie van de NEN 7518 de zorgspecifieke middelen moeten voldoen, de informatie die het 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, en de duur van geldigheid van het certificaat en tussentijdse controles.

Certificering in twee rollen

In de NEN 7518 is in ieder geval 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 zorgmedewerker, het registratie- en beheerproces van deze (digitale) identiteit en de uitgifte van het zorgspecifieke middel aan een zorgmedewerker. Het is namelijk van belang dat de koppeling van een middel aan een gebruiker zorgvuldig en op de juiste wijze wordt uitgevoerd, anders ontstaat mogelijk een risico voor de veiligheid van cliëntgegevens. Zonder 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. Aanvullend daarop kunnen ook nog eisen worden gesteld aan de technische interoperabiliteit.

Onder de NEN 7518 kunnen partijen voor twee rollen worden olp0gecertificeerd. 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 zorgmedewerker, het registratie- en beheerproces van deze (digitale) identiteit en de uitgifte van het zorgspecifieke middel aan een zorgmedewerker. De werkgroep van de NEN-norm 7518 heeft voor deze twee rollen een set met eisen opgesteld.

Ter illustratie een voorbeeld van een zorgaanbieder die wil gaan werken met een zorgspecifiek middel en dit zelf uitgeeft. Eerst zal de zorgaanbieder een middel inkopen dat is gecertificeerd op 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 zorgmedewerker 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).

Na inwerkingtreding van het wetsvoorstel 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. Deze middelen 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 middelen 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.

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 beschikt over 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 tussen het van afkomst van het betreffende middelen. Er wordt beoogd om bij of krachtens algemene maatregel van bestuur verschillende bewijsmiddelen aan te wijzen op grond waarvan aangetoond kan worden of 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 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

Het onderhavige wetsvoorstel vervangt hoofdstuk 3 van de Wabvpz over de registers van zorgaanbieders, indicatieorganen en zorgverzekeraars. Deze registers zijn ingesteld zodat zorgaanbieders – via SBV-Z – het BSN van de client kunnen raadplegen (artikel 14, eerste lid, Wabvpz). 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). 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 patiëntgegevens 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 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 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.[12] 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 SBV-Z.

Met dit wetsvoorstel wordt het daarnaast voor zorgaanbieders, zorgmedewerkers, indicatieorganen en zorgverzekeraars 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 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.

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 naar de nieuwe artikelen 14 tot en met 15 Wabvpz. In deze artikelen wordt mogelijk gemaakt dat

[12] Kamerstukken II 2017/18, 34 972, nr. 3, p. 1.

zorgmedewerkers, zorgaanbieders, indicatieorganen en zorgverzekeraars aan de hand van een inschrijving in een register en met behulp van een inlogmiddel gegevens van cliënten, waaronder het BSN, kunnen raadplegen. Om te voorkomen dat gegevens in verkeerde handen vallen is van belang dat deze gegevens 1) enkel geraadpleegd kunnen worden door diegenen die daartoe gerechtigd zijn en in zoverre dit voor de noodzakelijk is en dat 2) de identificatiemiddelen die worden gebruikt voldoen aan het betrouwbaarheidsniveau hoog.

5.1 Toezicht op raadplegen patiëntgegevens

Om met een goedgekeurd inlogmiddel onder meer het BSN van een cliënt te raadplegen moet een zorgmedewerker, zorgaanbieder, indicatieorgaan of zorgverzekeraar ingeschreven staan in het register en zijn geverifieerd. Uit de AVG vloeit voort dat de zorgaanbieder, het indicatieorgaan en de zorgverzekeraar borgen dat de inschrijving in het register niet wordt misbruikt om onrechtmatig gegevens te raadplegen. De zorgaanbieder kan bijvoorbeeld loggen welke gegevens uit elektronische uitwisselingssystemen door welke zorgmedewerkers worden geraadpleegd en zo nodig ingrijpen bij misstanden. De zorgaanbieder moet dan ook het veilig gebruik van gegevens door zijn eigen zorgmedewerkers borgen. Het is immers aan de verwerkingsverantwoordelijke om de AVG na te leven en zo nog maatregelen te nemen om datalekken te voorkomen. Op gegevensverwerking in de zorg wordt reeds door zowel de Autoriteit Persoonsgegevens (AP) als de Inspectie toezicht gehouden.[13] De AP richt zich daarbij op de vraag of de betreffende gegevensverwerking conform de wet plaatsvindt, de Inspectie houdt daarnaast toezicht op de verwerking van gegevens in zoverre dit raakt aan de kwaliteit en veiligheid van de zorgverlening. Als een zaak valt op het terrein van beide toezichthouders dan overleggen zij zo nodig met elkaar over de uitoefening van hun bevoegdheden. De Inspectie zal zich daarnaast voornamelijk richten op de kwaliteit van zorg, terwijl de AP het zwaartepunt legt op de verwerking van gegevens.

In een uitzonderlijk geval waarbij een zorgaanbieder, zorgmedewerker, indicatieorgaan of zorgverzekeraar niet zelf de veiligheid van de betreffende persoonsgegevens borgt die via het register kunnen worden geraadpleegd, kan Onze Minister op basis van dit wetsvoorstel over gaan tot intrekking van de inschrijving in het register. Dit heeft voor de ingeschrevene grote gevolgen omdat diegene in elk geval niet langer SBV-Z kan raadplegen en dus niet langer toegang heeft tot het BSN van cliënten. Hierdoor kan diegene niet langer de wettelijke plicht uitvoeren om het BSN van een client te verifiëren (artikel 4 tot en met 7 Wabvpz). Dit heeft mogelijk grote gevolgen voor de mogelijkheid om zijn beroep uit te oefenen. Van intrekking bij misbruik kan daarom enkel sprake zijn als in redelijkheid niet verwacht kan worden dat de ingeschrevene, of de organisatie waarvoor hij werkzaam is, de veiligheid van patiëntgegevens borgt. Intrekking moet dan ook evenredig zijn aan de gevolgen voor de ingeschrevene en voldoen aan de beginselen van proportionaliteit en subsidiariteit. Het besluit tot intrekking van de inschrijving is een besluit in de zin van de Awb, hier tegen staat bezwaar en beroep open.

5.2 Toezicht op betrouwbaarheidsniveau identificatiemiddelen

Op grond van het nieuwe artikel 15 Wabvpz kan Onze Minister goedkeuring verlenen aan een identificatiemiddel, indien dit middel voldoet aan het betrouwbaarheidsniveau hoog. Hiermee wordt geborgd dat gegevens van cliënten veilig geraadpleegd worden. Zoals uitgebreider toegelicht in paragraaf 2.5 kan met een bewijsmiddel zoals een Wdo-erkenning, certificaat van een certificerende stelling verstrekt onder de NEN 7518 of een PKI-overheidscertificaat 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 de verstrekker van een bewijsmiddel of de gebruiker van een identificatiemiddel niet adequaat optreedt in het geval een identificatiemiddel niet langer voldoende veilig is, bevat het wetsvoorstel een grondslag voor de Inspectie om toezicht te houden en zo nodig handhavend op te treden. De Inspectie kan in een dergelijk geval onderzoek doen naar het

[13] Zie hierover het Samenwerkingsprotocol AP- IGJ io, Autoriteit Persoonsgegevens (*Stcr.* 2018, 7023)

betreffende middel. Hiertoe wordt zo nodig informatie verschaft aan de Inspectie over degene aan wie goedkeuring is verleend of de verstrekker van het bewijsmiddel. De Inspectie kan na het vaststellen van een overtreding een herstelsanctie opleggen. Indien van tijdig herstel naar het betrouwbaarheidsniveau hoog geen sprake is of kan zijn en de veiligheid van patiëntgegevens – en in het verlengde daarvan de kwaliteit van de zorg – in gevaar blijft, kan Onze 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 patiëntgegevens. 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.

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 (UZI/URA/Rolcode) 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. Het CIBG verwerkt daarmee alle inlogpogingen (authenticatieverklaringen) van zorgmedewerkers op zorginformatiesystemen en -uitwisselingssystemen. Daarmee vindt deze gegevensverwerking 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 SBV-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 zorgmedewerker 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 zorgmedewerker 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 zorgmedewerker zelf. In dat geval verifieert de zorgmedewerker zelf de koppeling van zijn middel aan zijn UZI-registratie. Echter, doordat de koppeling door de zorgmedewerker 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 Substantieel of 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 zorgaanbieder voor wie de betreffende zorgmedewerker 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 Geïnventariseerde risico's: het uitlenen van inlogmiddelen

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 zorgmedewerker is minder snel geneigd een inlogmiddel uit te lenen dat voor meerdere toepassingen gebruikt kan worden. Een mobiele telefoon wordt minder snel gedeeld omdat daarop vaak zeer persoonlijk gegevens (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. Inlogmiddelen met het betrouwbaarheidsniveau kunnen daarnaast minder eenvoudig uitgeleend worden, wat de veiligheid van gegevens ten goede komt. 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 zorgmedewerker.

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 verantwoordelijk worden voor de goedkeuring van de Wdo-, zorgspecifieke- of PKI-o middelen. 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 project 'Toekomstbestendig maken UZI' en zal nog een uitvoeringstoets doen.

7.2 Zorgveld

Door de generieke functies identificatie en authenticatie in te vullen krijgt het zorgveld 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 zorgsector gebruik kan maken van de huidige UZI-middelen én de nieuwe erkende inlogmiddelen. Hiervoor moeten er keuzes gemaakt worden met betrekking tot software en inlogmiddelen. Zorgaanbieders 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 zorgaanbieders en zorgmedewerkers. Initiële aanvragen en wijzigingen kunnen veel sneller worden doorgevoerd. Daarmee wordt het UZI-register geschikt gemaakt om breed te kunnen worden ingezet in het zorgveld.

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) of PKI-O. 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 ofwel PKI-O. 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 gaat terug naar haar kerntaak van registerhouder en stopt met het uitgeven van UZI-passen en servercertificaten. Daarmee fungeert het CIBG niet meer als TSP. Het CIBG is verantwoordelijk voor het beheer van het UZI-register en het digitaal beschikbaar stellen de authenticatieverklaring. Een nieuwe taak voor het CIBG is het goedkeuren van de inlogmiddelen. Hiervoor wordt beoogd dat het CIBG beoordeeld of een middel beschikt over bewijsmiddel waaruit blijkt dat middel beschikt over het betrouwbaarheidsniveau hoog. Dit brengt systeem- en procesmatige aanpassingen met zich mee. Het CIBG zal op basis van het wetsvoorstel een uitvoeringstoets doen.

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 SBV-Z onrechtmatig het BSN 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 de betrokken zorgaanbieder. Zo zullen er financiële belangen gemoeid zijn met het goedkeuren van een inlogmiddel. Indien de goedkeuring van de UZI-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 UZI-middel breder wordt gebruikt dan alleen voor het 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 zorgaanbieder bijvoorbeeld geen toegang meer heeft tot een uitwisselingssysteem van medische gegevens van patiënten.

9. Regeldruk

Het wetsvoorstel heeft gevolgen voor zorgaanbieders 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 werking treedt per 2025. Er geldt geen directe verplichting om gebruik te maken van de erkende inlogmiddelen en het UZI-register voor toegang tot uitwisselings- en/of zorginformatiesystemen ten behoeve van elektronische gegevensuitwisseling in de zorg. 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, het LSP en de SBV-Z. 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. Per 2025 zullen een aantal (grote) zorgketens implementeren. Vanaf dan begint een overgangsperiode waarbij UZI-middelen worden uitgefaseerd en het zorgveld binnen 3 jaar moet overstappen op nieuwe middelen. De overgangsperiode geeft het zorgveld ruimschoots de tijd tot uiterlijk 2028 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 elektronische gegevensuitwisseling.

De generieke oplossing voor identificatie en authenticatie is met zorgveld tot stand gekomen en goed ontvangen. Hiervoor zijn zorgaanbieders, 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.[14] 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 zorgmedewerkers 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 zorgmedewerker 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 zorgmedewerker 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 alle andere inlogmiddelen uitgefaseerd worden. Denk

[14] Nieuwsbericht pilot BRBA: Succesvolle pilot met inloggen via DigiD in plaats van UZI-pas | Nieuwsbericht | Gegevensuitwisseling in de zorg

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. 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 sterkere authenticatie bijvoorbeeld eenmaal per dag en buiten het zorgproces om gevraagd worden. Ook kan de frequentie van het inloggen op verschillende zorgapplicaties worden teruggebracht. Overigens volgt 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.[15] 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.[16] 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. 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 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 zorgaanbieder aan hun medewerkers worden uitgereikt en niet onder de Wdo erkend worden omdat ze dan ook in andere sectoren gebruikt moeten 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 en solistisch werkende zorgverleners kunnen gebruik maken van de Wdo middelen.

Zorgaanbieders die zelf middelen uitgeven moeten de technische werking van het middel 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 voor meerdere zorgaanbieders hergebruiken. Het uitgifteproces moet per zorgaanbieder beoordeeld worden.

[15] Eindrapport Herijking MKBA Digitale Toegang naar aanleiding van de Wet digitale overheid, p. 49.
[16] TNO rapport "Toekomstbestendig maken van UZI middelen".

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 zorgidentiteit van een professional in het UZI-register

Het UZI-register wordt hét register voor het verstrekken van de identiteit van zorgmedewerkers en zorgaanbieders. Daarmee moeten zorgmedewerkers en zorgaanbieders zich inschrijven in het register en eventuele mutaties doorgeven. Nu staan ongeveer 90.000 zorgmedewerkers geregistreerd in het UZI register. Potentieel zal het UZI-register doorgroeien naar 1,5 miljoen mensen die werkzaam zijn in de zorg.[17] 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 uitgegaan van een groei van 100.000 registraties per jaar.

Zorgmedewerkers kunnen zich digitaal registreren door in te loggen en een aantal gegevens door te geven aan het CIBG. Voor zorgaanbieders wordt het mogelijk gemaakt om een koppeling met een HR-systeem te maken voor geautomatiseerd aanmelden in 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 zorgmedewerkers een mutatie doorgeven. Een mutatie doorgeven in het UZI-register kost maximaal 2 minuten. Per 100.000 (nieuwe) registraties kost dat 5.000 uur. De mutaties per 100.000 registraties nemen jaarlijks ongeveer 333 uur in beslag.

Het CIBG zal een jaarlijkse bijdrage in rekening brengen voor de registratie in het UZI-register. De bijdrage zal ongeveer 20 euro per ingeschrevene bedragen.

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 Wdo-conforme, zorgspecifieke inlogmiddelen en PKI-o middelen te vervangen zal er eenmalig geïnvesteerd moeten worden in het bouwen van de oplossing cq. 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 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 € 2 miljoen geraamd. Dit bedrag is ingegeven op basis van de op dit moment bekende indicatoren en vooruitlopend op de door het CIBG te realiseren uitvoeringstoets waar validatie zal plaatsvinden. De implementatiekosten zijn meerjarig (t/m 2024) opgenomen op de reguliere begroting van VWS (inclusief de eenmalige kosten van het CIBG).

[17] 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.

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. Hiervoor is in 2024 een bedrag van 2 miljoen euro vanuit de reguliere begroting van VWS beschikbaar.

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.

10.2 Structurele kosten

Eenmaal gebouwd en geadopteerd zal de oplossing cq. stelsel beheerd moeten worden. De ambitie is om het UZI-register zorgbreed in te zetten voor identificatie en authenticatie van de zorgmedewerker, 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 zal de structurele kosten in de uitvoeringstoets nader specificeren. Voorzien wordt dat het UZI-register zal blijven bestaan en dat de registraties zullen toenemen in aantal. Per 2025 geeft het CIBG geen (nieuwe) passen en certificaten (UZI-middelen) meer uit. De reeds uitgegeven passen moeten nog wel drie jaar ondersteund blijven worden.

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 huidige product zal uitgefaseerd worden en een nieuw product wordt geïntroduceerd. Uit een eerste verkenning worden de jaarlijkse kosten ingeschat op maximaal 8 miljoen euro.[18] Op basis van de op dit moment bekende informatie wordt de beheer(impact) door het CIBG als kosten neutraal beschouwd, waarmee het uitgangspunt is dat de totale onderhoudskosten van het bestaande product de onderhoudskosten van het nieuwe product zullen benaderen. Het CIBG zal een bijdrage aan de zorgaanbieder en/of zorgmedewerker vragen voor een registratie in het UZI-register. Het totaal aan bijdragen van het zorgveld mogen 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 (zorgaanbieders) UZI-register (20 euro per zorgmedewerker per jaar) Jaarlijkse kosten UZI-register 8 miljoen			
Jaar	**Aantal registraties**	**Bijdrage derden**	**Bijdrage VWS**
2025	90.000	1.800.000	6.200.000
2026	200.000	4.000.000	4.000.000
2027	300.000	6.000.000	2.000.000
2028	400.000	8.000.000	0

[18] TNO rapport "Toekomstbestendig maken van UZI middelen".

Beheer Stelsel (VWS)

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 (voor Zorgaanbieders/professionals)

Zorgaanbieders maken kosten voor het gebruik van inlogmiddelen. Kosten voor de eventuele aanschaf en het gebruik van ondersteunende techniek van een middel, bijvoorbeeld een mobiele telefoon, zijn niet meegenomen. Deze kosten zijn niet toe te schrijven aan identificatie en authenticatie. Voor inlogmiddelen onder de Wdo vindt de financiering naar alle waarschijnlijkheid plaats op basis aantal gebruikers (abonnementsprijs) of aantal transacties (tikprijs). Onder de Wdo is niet duidelijk hoe private middelen bekostigd worden. VWS prefereert een abonnementsprijs omdat een tikprijs zorgt voor een prikkel tot minder transacties/inloggen. Private middelenleveranciers berekenen de kosten door aan zorgaanbieders.

Er zijn een aantal kostenscenario's denkbaar.

- Abonnementsprijs
  De jaarlijkse kosten voor een inlogmiddel op het hoogste betrouwbaarheidsniveau worden ingeschat tussen de 20 en 70 euro.[19] Kanttekening hierbij is dat verschillende inlogmiddelen op het hoogste betrouwbaarheidsniveau nog volop in ontwikkeling zijn en nog niet voor die prijs op grote schaal beschikbaar zijn.

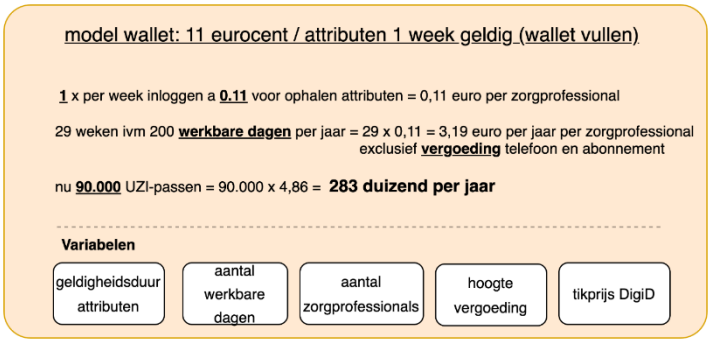
  Uitgaande van de 90.000 huidige UZI-registraties komt dat totaal neer op 1.8 miljoen bij een abonnementsprijs van 20 euro per jaar. Bij 70 euro per jaar gaat het om 6.3 miljoen.

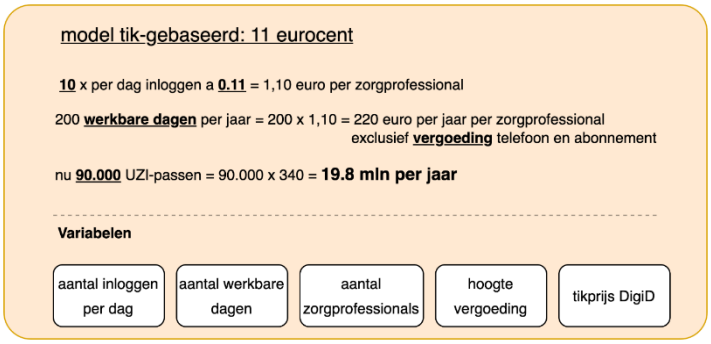
- Prijs per transactie
  Het gebruik van het publieke middel DigiD kost ongeveer 11 cent per transactie. Deze kosten worden niet doorberekend aan burgers maar door verschillende ministeries betaald. Voor private middelen is onduidelijk of een abonnementsprijs of prijs per transactie gehanteerd wordt. 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 zorgmedewerker 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.

  - 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 de gebruiker 22 euro per jaar. Een geldigheid van bijvoorbeeld een week leidt tot jaarlijkse kosten van 3,19 euro.

[19] TNO rapport "Toekomstbestendig maken van UZI middelen".





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.

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 van € 20 waarmee de totale jaarlijkse kosten op € 6.300.000 komen. In de huidige situatie gaat het om gemiddelde kosten van € 7.650.000 per jaar (€ 85 per zorgmedewerker per jaar). Dit betreft dus een besparing van € 1.350.000 per jaar. In deze vergelijking is het uitfaseren van andere huidige manieren van inloggen niet meegenomen. Als de nieuwe inlogmiddelen zorg-breed gebruikt kunnen worden i.p.v. enkel de huidige meest gebruikte toepassingen (SBV-Z en LSP), is de kostenbesparing vele malen hoger.

11. Advies en consultatie

PM

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 ingeschrevene 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 zorggerelateerde werkzaamheden verricht voor een zorgaanbieder. 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 namelijk 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 clientgegevens 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 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 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 het veilig kunnen raadplegen van andere elektronische uitwisselingssystemen die in de zorg gebruikt worden. 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 ingeschrevene misbruik maakt van zijn inschrijving door onrechtmatig 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 ingeschrevene voor de kosten die met het register gepaard gaan.

Artikel 14a (nieuw) – Inlogmiddelen
Net als in het oude artikel 14, eerste lid, is in het nieuwe artikel 14a, eerste lid, geregeld dat een in een register ingeschrevene toegang kan krijgen tot SBV-Z. Tevens is in het tweede lid bepaald dat de zorgaanbieders en zorgmedewerkers toegang kan krijgen tot elektronische

uitwisselingssystemen en zorginformatiesystemen. Toegang tot deze systemen en SBV-Z kan verkregen worden met een goedgekeurd inlogmiddel. Dit middel wordt gekoppeld aan een in het register ingeschrevene (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 SBV-Z, en elektronische uitwisselings- en zorginformatiesystemen, het koppelen van deze middelen aan een in het register ingeschrevene en de verwerking van gegevens bij deze koppeling (vierde lid).

Artikel 15 (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. 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. Als er aanwijzingen zijn dat het 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.

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 de nieuwe artikelen 14 tot en met 15. 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 misbruik van de inschrijving in een van de registers door het onrechtmatig raadplegen van het burgerservicenummer en 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: Inwerkingtreding

Beoogd wordt om deze wet, met uitzondering van onderdeel E, bij koninklijk besluit in werking te laten treden op 1 januari 2025.

De Minister van Volksgezondheid,
Welzijn en Sport,