STAATSCOURANT
Officiële uitgave van het Koninkrijk der Nederlanden sinds 1814.
Nr. 13656
17 mei
2023

Regeling van de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties van 8 mei 2023, nr 23-0000244782, houdende regels betreffende de bepaling van het vereiste betrouwbaarheidsniveau van authenticatie voor de verlening van elektronisch diensten en overgangsrecht met betrekking tot betrouwbaarheidsniveaus (Regeling betrouwbaarheidsniveaus authenticatie elektronische dienstverlening)

De Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties;

Gelet op artikel 6, tweede, derde en vierde lid, van de Wet digitale overheid;

Besluit:

Artikel 1 Begripsbepalingen

In deze regeling wordt verstaan onder:
– *basisregistraties:* basisregistraties, genoemd in bijlage 1 bij deze regeling;
– *bedrijfsgegevens:* gegevens die betrekking hebben op een onderneming of rechtspersoon en de uitvoering van het bedrijfsproces;
– *bijzondere categorieën van persoonsgegevens:* persoonsgegevens als bedoeld in de begripsbepaling voor 'bijzondere categorieën van persoonsgegevens' in artikel 1 van de Uitvoeringswet Algemene verordening gegevensbescherming;
– *elektronische dienst:* hetgeen daaronder wordt verstaan in artikel 1 van de wet;
– *identificatiemiddel:* hetgeen daaronder wordt verstaan in artikel 1 van de wet;
– *persoonsgegevens en verwerking van persoonsgegevens:* hetgeen daaronder wordt verstaan in artikel 4 van de Algemene verordening gegevensbescherming;
– *persoonsgegevens van strafrechtelijke aard:* persoonsgegevens als bedoeld in de begripsbepaling voor 'persoonsgegevens van strafrechtelijke aard' in artikel 1 van de Uitvoeringswet Algemene verordening gegevensbescherming;
– *wet:* Wet digitale overheid.

Artikel 2 Bepalen betrouwbaarheidsniveau voor een dienst

1. Indien voor een elektronische dienst niet bij wettelijk voorschrift is bepaald dat een specifieke wijze van authenticatie voor die dienst vereist is of ten minste vereist is, bepaalt een bestuursorgaan of aangewezen organisatie dat niveau overeenkomstig het tweede tot en met vijfde lid.

2. Een bestuursorgaan of aangewezen organisatie bepaalt dat voor een elektronische dienst authenticatie op betrouwbaarheidsniveau hoog vereist is indien voor een van de aspecten van die dienst een van de in bijlage 2 bij deze regeling genoemde criteria in de kolom hoog op die dienst van toepassing is.

3. Een bestuursorgaan of aangewezen organisatie bepaalt dat voor een elektronische dienst authenticatie op betrouwbaarheidsniveau substantieel vereist is indien voor een van de aspecten van die dienst een van de in bijlage 2 bij deze regeling genoemde criteria in de kolom substantieel op die dienst van toepassing is en geen van de in de kolom hoog genoemde criteria.

4. Een bestuursorgaan of aangewezen organisatie bepaalt dat voor een elektronische dienst authenticatie op betrouwbaarheidsniveau laag vereist is indien voor een van de aspecten van die dienst een van de in bijlage 2 bij deze regeling genoemde criteria in de kolom laag op die dienst van toepassing is en geen van de in de kolom substantieel of hoog genoemde criteria

5. Een bestuursorgaan of aangewezen organisatie bepaalt dat geen authenticatie is vereist indien voor geen van de aspecten van die dienst een van de in bijlage 2 bij deze regeling genoemde criteria op de dienst van toepassing is.

Artikel 3 Risico verlagende factoren

1. Onverminderd de toepasselijkheid van een wettelijk voorschrift dat bepaalt dat een specifieke wijze

van authenticatie voor die dienst vereist is of ten minste vereist is, kan, in afwijking van artikel 2, tweede en derde lid, een bestuursorgaan of aangewezen organisatie voor een elektronische dienst authenticatie op één betrouwbaarheidsniveau lager vaststellen, indien:

a. het proces van toegangsverlening voorziet in een adequate aanvullende technische of fysieke controle op de authenticiteit van de gebruiker van het identificatiemiddel na het moment waarop daarmee voor de eerste keer voor de desbetreffende dienst een authenticatie is uitgevoerd;
b. het bestuursorgaan of de aangewezen organisatie in het proces herstelmaatregelen neemt of kan nemen.

2. Toepassing van het eerste lid sluit gelijktijdige toepassing van artikel 6 uit.

Artikel 4 Risicoverhogende factoren

Indien naar het oordeel van het bestuursorgaan of de aangewezen organisatie, gelet op de aard van de dienst, sprake is van risicoverhogende factoren waaronder identiteitsfraude of misbruik van de dienst, wordt een volledige risicoanalyse uitgevoerd teneinde het passende betrouwbaarheidsniveau voor die dienst te kunnen bepalen.

Artikel 5 Machtigen

1. Afgifte en intrekking van een machtiging wordt elektronisch geregistreerd.

2. Bij afgifte van een machtiging is sprake van een kenbare wilsuiting van de machtiginggever om:
   a. de dienst af te nemen, en
   b. dit door de beoogd gemachtigde te laten doen.

3. Afgifte en intrekking van een machtiging kan langs elektronische en niet-elektronische weg.

4. De betrouwbaarheid van een machtigingsregistratie is tenminste gelijk aan het betrouwbaarheidsniveau dat voor de authenticatie voor de dienst is vereist.

5. Bij de registratie van een machtiging die langs elektronische weg is afgegeven gebruiken machtiginggever en gemachtigde een identificatiemiddel op tenminste hetzelfde betrouwbaarheidsniveau als voor de dienst is vereist.

6. Bij de registratie van een machtiging, die niet of niet geheel langs elektronische weg is afgegeven, bepaalt het bestuursorgaan of de aangewezen organisatie of de betrouwbaarheid van de machtiging gewaarborgd is.

7. Het bestuursorgaan of de aangewezen organisatie kan bepalen dat de betrouwbaarheid van een machtigingsregistratie lager mag zijn dan het betrouwbaarheidsniveau dat voor de authenticatie van de dienst vereist is, mits adequate aanvullende maatregelen in het proces van dienstverlening of toegangsverlening worden getroffen.

Artikel 6 Tijdelijk toestaan van een lager niveau

1. Onverminderd de toepasselijkheid van een wettelijk voorschrift dat bepaalt dat een specifieke wijze van authenticatie voor die dienst vereist is of ten minste vereist is, kan een bestuursorgaan of aangewezen organisatie, indiende beschikbaarheid of het gebruik van identificatiemiddelen op de betrouwbaarheidsniveaus substantieel en hoog of de mogelijkheid om deze te gebruiken om toegang te krijgen tot dienstverlening onvoldoende is, voor een elektronische dienst, waarvoor op grond van artikel 2 authenticatie op betrouwbaarheidsniveau hoog respectievelijk substantieel benodigd is, tot twee jaar na inwerkingtreding van deze regeling voor toegang tot die dienst tevens het gebruik van een toegelaten of erkend middel op betrouwbaarheidsniveau substantieel respectievelijk een middel op betrouwbaarheidsniveau laag toestaan.

2. Toepassing van het eerste lid sluit gelijktijdige toepassing van artikel 3 uit.

Artikel 7 Kenbaarheid betrouwbaarheidsniveau

Het bestuursorgaan dat of de aangewezen organisatie die de dienst verleent maakt op de eigen website kenbaar welk betrouwbaarheidsniveau van authenticatie op grond van de artikelen 2 tot en met 6 ten minste vereist is.

Artikel 8 Citeertitel

Deze regeling wordt aangehaald als:Regeling betrouwbaarheidsniveaus authenticatie elektronische dienstverlening.

Artikel 9 Inwerkingtreding

Deze regeling treedt in werking met ingang van 1 juli 2023.

Deze regeling zal met de toelichting in de Staatscourant worden geplaatst.

De Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties Digitalisering en Koninkrijksrelaties,
A.C. van Huffelen

BIJLAGE 1: BASISREGISTRATIES

(bijlage als bedoeld in artikel 1 van de Regeling betrouwbaarheidsniveaus authenticatie elektronische dienstverlening)

- de basisregistraties adressen en gebouwen, bedoeld in artikel 2 van de Wet basisregistraties adressen en gebouwen
- de basisregistratie grootschalige topografie, bedoeld in artikel 2, eerste lid, van de Wet basisregistratie grootschalige topografie
- de basisregistratie inkomen, bedoeld in artikel 21a, eerste lid, van de Algemene wet inzake rijksbelastingen
- de basisregistratie kadaster, bedoeld in artikel 48, eerste lid, van de Kadasterwet
- de basisregistratie ondergrond, bedoeld in artikel 2, eerste lid, van de Wet basisregistratie ondergrond
- de basisregistratie personen, bedoeld in artikel 1.2 van de Wet basisregistratie personen
- de basisregistratie topografie, bedoeld in artikel 98a van de Kadasterwet
- de basisregistratie WOZ, bedoeld in artikel 37a, eerste lid, van de Wet waardering onroerende zaken
- het handelsregister, bedoeld in artikel 2 van de Handelsregisterwet 2007
- het kentekenregister, bedoeld in artikel 42, eerste lid, van de Wegenverkeerswet 1994.

BIJLAGE 2: CRITERIA BETROUWBAARHEIDSNIVEAUS

(bijlage als bedoeld in artikel 2, tweede tot en met vierde lid, Regeling betrouwbaarheidsniveaus authenticatie elektronische dienstverlening)

Aspecten van de dienst	Criteria betrouwbaarheidsniveaus		
	Niveau laag	Niveau substantieel	Niveau hoog
Persoonsgegevens (behoudens het BSN): aard gegevens en aard en omvang van de verwerking	• Geen bijzondere categorieën van persoonsgegevens • Geen persoonsgegevens van strafrechtelijke aard, geen gegevens uit antecedentenonderzoek en geen politiegegevens • Kleinschalige verwerking	• Bijzondere categorieën van persoonsgegevens • Persoonsgegevens van strafrechtelijke aard, gegevens uit antecedentenonderzoek en politiegegevens • Gevoelige persoonsgegevens niet zijnde bijzondere categorieën van persoonsgegevens, persoonsgegevens van strafrechtelijke aard, gegevens uit antecedentenonderzoek of politiegegevens • Grootschalige verwerking	• Persoonsgegevens die: * stigmatiserend kunnen werken * reputatieschade kunnen opleveren * tot uitsluiting kunnen leiden * schade kunnen opleveren aan de gezondheid, of * chanteerbaarheid kunnen opleveren • Gegevens die onder het medisch beroepsgeheim vallen
Risico's indien de gegevens in verkeerde handen vallen Aard van de gegevens van ondernemingen en rechtspersonen	Geen of nauwelijks risico op identiteitsfraude en/of misbruik van de betreffende dienst Algemeen bekende gegevens van ondernemingen en rechtspersonen	Reëel risico op identiteitsfraude en/of misbruik van de betreffende dienst Gevoelige gegevens van ondernemingen en rechtspersonen	Groot risico op identiteitsfraude en/of misbruik van de betreffende dienst Geen criteria
Aard van de verwerking van het BSN	• BSN van degene aan wie de dienst wordt verleend, van zijn gemachtigde, of van een derde wordt door dienstverlener niet verstrekt	• BSN van degene aan wie de dienst wordt verleend, van zijn gemachtigde of van een derde wordt door de dienstverlener tijdens het proces van dienstverlening verstrekt • NB: wanneer dienstverlener reeds opgegeven BSN terugkoppelt: minimaal niveau laag met 2-factor authenticatie nodig	• BSN in combinatie met andere persoonsgegevens
Gevolgen voor de gegevens in de basisregistraties	• Geen criteria	• Controle op de verwerking van gegevens	• Geen controle op de verwerking van gegevens
Economisch belang	• Niet of nauwelijks ingrijpend voor economische positie burgers/ondernemingen en rechtspersonen in de doelgroep, waarbij als richtsnoer geldt: * De directe schade voor burgers is lager dan € 1.000,– * De directe schade voor bedrijven tot 250 werknemers is lager dan € 125.000,– * De directe schade voor grotere bedrijven is lager dan € 500.000,–	• Ingrijpend voor economische positie burgers/ondernemingen en rechtspersonen in de doelgroep, waarbij als richtsnoer geldt: * De directe schade voor burgers is hoger dan € 1.000,– * De directe schade voor bedrijven tot 250 werknemers is hoger dan € 125.000,– * De directe schade voor grotere bedrijven is hoger dan € 500.000,–	• Zodanig ingrijpend voor economische positie burgers/ondernemingen en rechtspersonen dat ongewijzigd welstandsniveau of voortbestaan onmogelijk is

TOELICHTING

I. Algemeen

1. Inleiding

Digitale overheidsdienstverlening moet veilig zijn. Dat geldt zowel voor inrichting van de overheidsdienstverlening zelf, als voor de digitale toegang tot deze dienstverlening.
Hoe risicovoller de dienstverlening is, bijvoorbeeld als veel privacygevoelige gegevens worden verwerkt of het economisch belang groot is, hoe hoger de veiligheid van de dienst moet zijn, waaronder de toegang tot de dienstverlening. Deze is in veel gevallen van groot belang voor de veiligheid van de dienstverlening met achterliggende processen als geheel.
Veilige dienstverlening begint bij de vaststelling of deze aan de juiste persoon wordt geleverd. Gelet hierop is er in de wet voor gekozen om de mate van toegangscontrole en de keuze voor het toegangsmiddel niet langer vrijblijvend te laten zijn, maar daar op basis van de wet een verplichtend karakter aan te geven. Doelstelling is daarbij om over de volle breedte een veiligere toegang tot overheidsdienstverlening te bewerkstelligen en meer eenduidigheid in inlogniveaus voor gelijksoortige dienstverlening bij verschillende overheden. Dit brengt voor burgers en bedrijven een betere voorspelbaarheid met zich mee en draagt daarmee bij aan het vertrouwen in de digitale overheid.

Deze keuze vergt dat de wet voor de vaststelling van de benodigde toegang tot dienstverlening een normatief kader biedt. Dit wordt met deze regeling beoogd. De regeling geeft uitvoering aan artikel 6, tweede, derde en vierde lid, van de Wet digitale overheid (hierna: de wet). In artikel 6, eerste lid, van de wet wordt bepaald dat bestuursorganen en aangewezen organisaties bij elektronische dienstverlening waarvoor authenticatie op betrouwbaarheidsniveau substantieel of hoog vereist is, uitsluitend toegang tot de dienstverlening verlenen indien (door de burger of het bedrijf dat de dienst wil afnemen) gebruik wordt gemaakt van identificatiemiddelen die ten minste het voor de betreffende dienstverlening vereiste betrouwbaarheidsniveau hebben. De betrouwbaarheidsniveaus 'substantieel' en 'hoog' zijn ontleend aan de Europese eIDAS-verordening,[1] die op Europees niveau regels stelt aan de veiligheid van inlogmiddelen. Ter uitwerking bepalen bestuursorganen en aangewezen organisaties op grond van het tweede lid van artikel 6 van de wet welk betrouwbaarheidsniveau op een door hen aangeboden dienst van toepassing is, met het oog op authenticatie (identificatie/inloggen) voor die dienst. De wet schrijft voor dat bij ministeriële regeling regels worden gesteld over de wijze waarop bestuursorganen en aangewezen organisaties dat doen en op welke wijze zij ervoor zorgen dat het vastgestelde betrouwbaarheidsniveau kenbaar is. Het derde lid bepaalt dat dergelijke regels ook worden gesteld over het betrouwbaarheidsniveau voor het afgeven van machtigingen. De onderhavige regeling bevat deze regels.

Artikel 6, vierde lid, van de wet bepaalt dat bij ministeriële regeling regels kunnen worden gesteld over het tijdelijk toestaan van authenticatie met een middel op een lager betrouwbaarheidsniveau dan het niveau dat voor de desbetreffende dienst is bepaald. In deze regeling wordt van die mogelijkheid gebruik gemaakt: dienstverleners kunnen, in de gevallen die in deze regeling zijn bepaald, tot 2 jaar na inwerkingtreding van deze regeling voor elektronische diensten voor burgers en bedrijven, waarvoor voor toegang gebruik moet worden gemaakt van een middel met betrouwbaarheidsniveau substantieel respectievelijk hoog, het gebruik van een toegelaten of erkend middel met een naastlager niveau toestaan, mits sprake is van twee-factor authenticatie (art. 6, vierde lid, WDO).

2. Betrouwbaarheidsniveau

2.1 Afwegingskader en positionering

De betrouwbaarheid van inlogmiddelen

Het Europese kader voor wederzijdse erkenning van identificatiemiddelen is de hierboven al genoemde eIDAS-verordening. Deze verordening regelt wanneer identificatiemiddelen door andere lidstaten dan de lidstaat waarin het middel is uitgegeven moeten worden erkend (artikel 6 eIDAS). Daartoe worden drie betrouwbaarheidsniveaus geïntroduceerd: laag, substantieel en hoog (artikel 8 eIDAS). Een identificatiemiddel met betrouwbaarheidsniveau laag biedt een beperkte mate van zekerheid over iemands opgegeven of beweerde identiteit, niveau substantieel biedt een substantiële mate van vertrouwen en niveau hoog een hoge mate van vertrouwen. In de op eIDAS gebaseerde

[1] 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 (PbEU 2014, L 257).

uitvoeringsverordening 2015/1502[2] is voor de verschillende betrouwbaarheidsniveaus vastgesteld aan welke eisen een middel moet voldoen om in EU (incl. EER)-lidstaten te kunnen worden geaccepteerd.

De betrouwbaarheid van overheidsdienstverlening

De onderhavige regeling schrijft onder meer voor hoe bestuursorganen en aangewezen organisaties de betrouwbaarheid van hun diensten moeten inschalen, gelet op de risico's die aan de diensten zijn verbonden. Want hoe hoger het risico is op schade als de dienst niet aan de juiste persoon wordt geleverd, hoe groter de zekerheid moet zijn dat de juiste persoon inlogt. Voor de inschaling van de overheidsdienstverlening kiest deze regeling voor eenzelfde inschaling met de betrouwbaarheidsniveaus laag, substantieel en hoog, zoals die in eIDAS worden gehanteerd, waardoor het betrouwbaarheidsniveau van de dienst kan worden gekoppeld aan de benodigde betrouwbaarheid van het inlogmiddel. Bij het opstellen van deze regeling is de Handreiking betrouwbaarheidsniveaus voor digitale dienstverlening[3] van het Forum Standaardisatie als vertrekpunt genomen. In dat document zijn uitgangspunten geformuleerd voor het bepalen van betrouwbaarheidsniveaus voor elektronische overheidsdiensten. Dat document hanteert ook de betrouwbaarheidsniveaus uit eIDAS. Verder is bij de totstandkoming van deze regeling gebruik gemaakt van het onderzoek van PrivacyCare naar betrouwbaarheidsniveaus bij patiëntenauthenticatie bij elektronische gegevensuitwisseling in de zorg.[4]

Benadrukt wordt, dat deze regeling een in de bijlage opgenomen afwegingskader bevat; de criteria, op basis waarvan het betrouwbaarheidsniveau moet worden bepaald, vormen houvast waarmee bestuursorganen en aangewezen organisaties (ook wel: 'dienstaanbieders' of 'dienstverleners' genoemd) hun weg kunnen en moeten vinden. Het is in feite een verkorte risico-analyse op veiligheid van de dienstverlening. De regeling bevat – bewust – geen afvinklijst of *one-size-fits-all*-benadering, maar richtsnoeren waarmee de desbetreffende organisatie aan de slag kan om de eigen diensten te classificeren.[5] Van belang daarbij is dat een beredeneerde afweging wordt gemaakt. Hierdoor bestaan voor bestuursorganen en aangewezen organisaties mogelijkheden voor risicoafweging. Een dergelijke ruimte voor eigen inschatting is nodig omdat in de praktijk, bijvoorbeeld bij het gebruik van open tekstvakken, niet altijd op voorhand duidelijk is welke gegevens door de gebruiker worden ingegeven. De onderhavige regeling is normatiever dan de – veeleer adviserende – Handreiking betrouwbaarheidsniveaus en daarmee een meer dwingende opvolger van de handreiking. Hiervoor is gekozen omdat met de bovenliggende wet wordt toegewerkt naar harmonisatie en standaardisatie van het veilig en betrouwbaar inloggen bij de overheid, waarmee verder wordt gegaan dan het aan overheden/publieke dienstverleners opleggen van procesmatige verplichtingen. Wel is het binnen de regeling aan de dienstverleners zelf om een op de eigen organisatie, diensten en context toegespitste 'vertaling' te maken.
Het voorgaande levert een zekere spanning op, omdat enerzijds bij dienstverleners, burgers en bedrijven behoefte bestaat aan zoveel mogelijk eenduidigheid (rechtszekerheid, duidelijkheid, uniformiteit) en bruikbaarheid bij alle gangbare vormen van elektronische dienstverlening die authenticatie vereisen, en anderzijds aan ruimte om recht te doen aan de eigenheid van de uitvoeringspraktijk. Hieraan kan tegemoet worden gekomen door als dienstverlener een organisatiespecifieke vraagbaak of ander hulpmiddel te hanteren, waarmee nadere toelichting en praktische ondersteuning (bijvoorbeeld in de vorm van voorbeelden) worden gegeven.
Naar verwachting zal toepassing van deze regeling in de praktijk leiden tot eenzelfde betrouwbaarheidsniveau voor vergelijkbare overheidsdiensten, waardoor een zekere uniformiteit en voorspelbaarheid wordt bewerkstelligd. Dit zal worden gemonitord en waar nodig op termijn leiden tot aanpassing van de regeling. Voorkomen moet worden dat er onnodig grote verschillen tussen vergelijkbare dienstverleners ontstaan en het vereiste niveau van authenticatie in de loop der tijd aan veel verandering onderhevig is. Duidelijkheid en overzichtelijkheid dragen bij aan de 'doenlijkheid' voor burgers. Ook minder digitaal vaardige burgers zijn daarmee geholpen, omdat zij dan niet steeds een ander middel of andere handelingen hoeven te verrichten.

2.2 Vaststelling betrouwbaarheidsniveau door dienstverlener

Aan het gebruik van elektronische diensten zijn risico's verbonden. Het gaat om risico's voor burgers, bedrijven en dienstverleners die samenhangen met privacybescherming en beveiliging van de gegevens van de gebruiker tegen ongewenste wijzigingen. Bij gebruik van een identificatiemiddel met

[2] Pb EU 2014, L 235.
[3] Een handreiking voor Overheidsorganisaties Forum Standaardisatie, Betrouwbaarheidsniveaus voor digitale dienstverlening, versie 4, april 2017, zie https://www.forumstandaardisatie.nl/nieuws/nieuwe-versie-handreiking-betrouwbaarheidsniveaus, voor de laatste versie.
[4] Privacycare – PBLQ, Onderzoek betrouwbaarheidsniveau patiëntenauthenticatie bij elektronische gegevensuitwisseling in de zorg, mei 2016. Meegezonden als bijlage bij Tweede Kamerbrief over Impuls eID, Kamerstukken II, 2017–2018, 26 643, nr. 419.
[5] Zie mbt de vertaalslag door gemeenten: https://www.digitaleoverheid.nl/nieuws/instrument-helpt-gemeenten-om-betrouwbaarheidsniveau-van-digitale-diensten-te-bepalen/.

een hoger betrouwbaarheidsniveau is de kans op (misbruik van de dienst door) onjuiste authenticatie kleiner dan bij een middel met een lager betrouwbaarheidsniveau, waardoor zich minder snel schade zal voordoen.

De lasten in termen van gebruiksgemak bij het gebruik van identificatiemiddelen nemen echter veelal toe wanneer het betrouwbaarheidsniveau toeneemt. Dat vloeit voort uit het feit dat voor het gebruik van deze middelen bijvoorbeeld meer handelingen moeten worden verricht of specifieke apparatuur moet worden aangeschaft. Het te gebruiken identificatiemiddel moet voldoende betrouwbaar en veilig zijn om de risico's die aan de desbetreffende elektronische dienst verbonden zijn te mitigeren, terwijl onnodig hoge kosten moeten worden voorkomen.

Zoals hierboven is opgemerkt, bepalen verleners van elektronische diensten zelf welk betrouwbaarheidsniveau passend is bij een door hen verleende dienst. De afweging die daaraan ten grondslag ligt, zal bij soortgelijke elektronische diensten in beginsel niet tot verschillende uitkomsten leiden. Dat zou afbreuk doen aan de veiligheid en betrouwbaarheid van de overheidsdienstverlening en aan de rechtszekerheid (verwachtingspatroon) voor gebruikers daarvan. Niettemin kunnen soortgelijke diensten bij verschillende organisaties, bijvoorbeeld het indienen van een klacht of Wob-verzoek, het uitbrengen van een ingebrekestelling, het doorgeven van een adreswijziging, (technisch/functioneel) wezenlijk anders zijn ingericht, waardoor toch andere authenticatie nodig is. Met deze regeling worden regels gesteld over de wijze waarop het betrouwbaarheidsniveau wordt vastgesteld. Deze regels bieden naar verwachting voldoende houvast om zoveel mogelijk uniformiteit te borgen, terwijl er voldoende ruimte blijft om recht te doen aan de specifieke risicokenmerken en eigenschappen van de desbetreffende dienst.

2.3 Te hanteren criteria voor het vaststellen van het betrouwbaarheidsniveau

2.3.1 Uitgangspunt: het voorkomen van schade

De criteria die dienstverleners moeten gebruiken om het vereiste betrouwbaarheidsniveau voor een elektronische dienst vast te stellen, zijn gericht op het voorkomen van – materiële en immateriële – schade voor burgers, bedrijven en de overheid zelf. Hoe groter het risico dat uit ongeautoriseerd of onveilig gebruik van die dienst aanzienlijke schade voortvloeit, hoe groter de zekerheid moet zijn omtrent de identiteit van de gebruiker. Dit is een gangbaar principe van informatiebeveiliging en van de beveiliging van persoonsgegevens in het bijzonder. In dit verband wordt opgemerkt dat de criteria die zijn opgenomen in de regeling zijn te beschouwen als een verkorte risicoanalyse. Waar het uiteindelijk om gaat, is dat aangesloten wordt op een betrouwbaarheidsniveau dat past bij het feitelijke risico dat kleeft aan de dienstverlening.
De regeling biedt daarom ook de mogelijkheid om rekening te houden met mogelijk aanwezige risico-verlagende, maar ook risico-verhogende factoren, en laat uiteindelijk ook de mogelijkheid om een volledige risico-analyse uit te voeren.

Indien in specifieke wettelijke voorschriften voor de desbetreffende dienst is vastgelegd welk betrouwbaarheidsniveau moet worden gehanteerd, is geen nadere beoordeling nodig. In andere gevallen wordt het vereiste niveau aan de hand van de criteria in bijlage 2 bepaald. Als op een dienst één van de criteria voor niveau hoog van toepassing is, moet voor die dienst betrouwbaarheidsniveau hoog worden gehanteerd. Als geen van de criteria voor niveau hoog van toepassing is, maar wel één van de criteria voor substantieel, dan moet dat niveau worden gehanteerd. Als geen van de criteria voor hoog of substantieel van toepassing is op de dienst, dan is niveau laag van toepassing. Dienstverleners kunnen in afwijking van het voorgaande onder bepaalde voorwaarden voor een dienst één niveau lager bepalen. Daarop wordt nader ingegaan in paragraaf 3.1.

Het toepassen van dit systeem zal leiden tot een conclusie over een te hanteren betrouwbaarheidsniveau voor een dienst. De wet voorziet in een acceptatieplicht voor toegelaten middelen voor overheidsdiensten op de betrouwbaarheidsniveaus substantieel en hoog. Het betrouwbaarheidsniveau laag wordt met de wet niet geregeld.

Een groot deel van de elektronische diensten behoeft in het geheel geen authenticatie door de gebruiker. Dat is bijvoorbeeld het geval bij algemene of openbare informatievoorziening waarbij de vaststelling van de identiteit van een burger of bedrijf (onderneming of rechtspersoon) niet van belang is, zelfs niet op niveau laag, zoals bij het bezoeken van een overheidswebsite, het stellen van een vraag over het ophalen van vuilnis of het doen van een melding van losse stoeptegels. Voor deze diensten is het bepalen van een betrouwbaarheidsniveau voor authenticatie niet nodig en ook niet wenselijk om redenen van het voorkomen van het opleggen van onnodige lasten. Voorkomen moet worden dat 'voor de zekerheid' onnodige authenticatie wordt vereist.

2.3.2 Specifieke wettelijke eisen over betrouwbaarheidsniveaus diensten of identificatiemiddelen

Het eerste aspect van een dienst dat beoordeeld moet worden, zijn specifieke wettelijk vastgelegde eisen over het betrouwbaarheidsniveau van diensten of identificatiemiddelen.

Het kader van de onderhavige regeling om voor *diensten* te beoordelen wat het betrouwbaarheidsniveau van authenticatie moet zijn, is een algemeen kader op grond van de wet. Er zijn echter ook eisen die op grond van specifieke wetgeving worden gesteld aan het betrouwbaarheidsniveau van het identificatie*middel* dat vereist is om toegang tot bepaalde elektronische diensten te verkrijgen. Het voor de dienst vast te stellen betrouwbaarheidsniveau moet daarmee in lijn zijn. Niet uitgesloten is voorts dat in de toekomst ook specifieke wettelijke eisen worden gesteld aan het betrouwbaarheidsniveau van een dienst. Als er in specifieke wetgeving eisen worden gesteld ten aanzien van het (al dan niet minimale) niveau van authenticatie voor een identificatiemiddel of een bepaalde dienst, dan moet daarbij rekening worden gehouden met het algemene kader dat in deze regeling wordt gegeven voor het beoordelen van diensten. Een lager niveau vereisen in specifieke wetgeving dan dat op grond van deze regeling vereist is, is uiteraard niet wenselijk. Indien de omstandigheden van het geval hiertoe niettemin nopen, moet de desbetreffende specifieke bepaling dragend gemotiveerd worden. Gelet op het voorgaande ligt het in de rede om bestaande (sectorale) regels over eisen aan toegang tegen het licht te houden.

Minimale specifieke wettelijke eisen

Er zijn enkele voorbeelden van wettelijke eisen aan het betrouwbaarheidsniveau van identificatiemiddelen waarmee diensten ontsloten moeten worden. Deze zijn verwerkt als criteria in de tabel bij artikel 2. Zo is in het Besluit digitale stukken Strafvordering bepaald dat de indiening, toezending, kennisneming, verstrekking en betekening van diverse stukken in het strafproces authenticatie vereisen met een middel dat, naast andere eisen, uitgaat van een tweefactor-authenticatie of hoger (artikel 5 Besluit digitale stukken Strafvordering). Voor de elektronische aangifte of melding bij de burgerlijke stand is bepaald dat de vaststelling van de juistheid van de identiteit van de aangever geschiedt door middel van DigiD op basis van ten minste tweefactor-authenticatie, eHerkenning op basis van minimaal betrouwbaarheidsniveau 2plus, dan wel een opvolgend en minstens even betrouwbaar middel (artikel 2 van het Besluit elektronische dienstverlening burgerlijke stand). Dit soort *minimale* specifieke wettelijke eisen zijn meegenomen in het algemene beoordelingskader in de tabel bij artikel 2 van deze regeling (behoudens bij het hoogste niveau ‘hoog’, dat naar zijn aard niet minimaal kan zijn). Indien bij de beoordeling van een dienst in het kader van deze regeling op grond van specifieke wettelijke eisen minimaal niveau substantieel wordt vereist (zoals in de zojuist genoemde twee voorbeelden) en de beoordeling van andere aspecten van de dienst (zoals de aard van de persoonsgegevens of het economisch belang) uitkomt op niveau hoog, dan zal de hele dienst op grond van deze regeling moeten worden verleend op betrouwbaarheidsniveau hoog. Omdat betrouwbaarheidsniveau ‘hoog’ het hoogste niveau is, is het criterium over specifieke wetgeving voor dat niveau ‘hoog’ zonder meer.

Vaste specifieke wettelijke eisen

Indien de in verband met de te verlenen elektronische dienst gestelde specifieke wettelijke eisen aan het betrouwbaarheidsniveau van een identificatiemiddel of een dienst niet een minimaal niveau vereisen, maar slechts één niveau, dan heeft die specifieke wettelijke eis voorrang op het algemene kader van deze regeling. Een voorbeeld van zo’n specifieke eis die niet een minimumniveau stelt, maar één niveau, is te vinden in het Besluit digitalisering burgerlijk procesrecht en bestuursprocesrecht. Daarin is bepaald dat authenticatie om toegang te krijgen tot een digitaal systeem voor gegevensverwerking van de rechterlijke instanties plaatsvindt met een middel dat, naast andere eisen, uitgaat van tweefactor-authenticatie (artikel 3 van dat besluit). Dit laat overigens onverlet, dat voor deze diensten tevens kan worden ingelogd met identificatiemiddelen op de hogere betrouwbaarheidsniveaus.

2.3.3 Persoonsgegevens

De vereiste betrouwbaarheid en veiligheid van authenticatie van natuurlijke personen hangt samen met de verwerking van persoonsgegevens. Daarvoor zijn de Algemene verordening gegevensbescherming (AVG) en de Uitvoeringswet Algemene verordening gegevensbescherming (UAVG) de geldende Europeesrechtelijke en nationale kaders. In deze regeling worden de begrippen gehanteerd die zijn gebaseerd op die kaders. Van belang zijn de aard van de gegevens en de aard en – relatieve – omvang van de verwerking van de gegevens.
Onder persoonsgegevens wordt alle informatie verstaan over een geïdentificeerde of identificeerbare natuurlijke persoon (de betrokkene); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, aan de hand van een identificator zoals een naam, een

identificatienummer, locatiegegevens, een online identificator of van één of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon.[6] Ook gegevens die op zichzelf niet tot identificatie leiden, kunnen in combinatie wel als identificerend worden beschouwd en (substantiële of hoge) risico's voor betrokkenen opleveren.

Bij het verlenen van de elektronische diensten waarvoor op grond van deze regeling een betrouwbaarheidsniveau van authenticatie moet worden bepaald, worden persoonsgegevens verwerkt (verwerking is 'een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden op ander wijze ter beschikking stellen, aligneren of combineren, afschermen wissen of vernietigen van gegevens'[7]). Verwerking kan meer of minder grootschalig en/of gestapeld geschieden. In dit verband vormt de hoeveelheid te verwerken gegevens per individu (als gevolg van meerdere doelen en vastleggingen) een indicatie, alsmede het aantal betrokkenen, de duur van de gegevensverwerking en de geografische reikwijdte van de verwerking. Voorbeelden van grootschalige persoonsgegevensverwerking betreffen de verwerking van klantgegevens door een verzekeringsmaatschappij of een bank en de verwerking van patiëntgegevens door een ziekenhuis.[8]
De dienstverlener moet weten wat de risico's zijn voor de betrokkene indien diens gegevens bij een ander terecht komen of indien gegevens uit zijn naam door een ander aan een dienstverlener worden verstrekt, hetzij per ongeluk of opzettelijk. Het kan daarbij gaan om het risico op identiteitsfraude en/of misbruik of oneigenlijk gebruik van de betreffende dienst of om een negatief effect op de persoonlijke levenssfeer van betrokkene. Vervolgens moet door dienstverleners de vertaalslag gemaakt worden van die risico's naar het vereiste betrouwbaarheidsniveau van authenticatie bij toegang tot de dienst. Bijvoorbeeld wat is het risico als een bijzonder persoonsgegeven – bijvoorbeeld gegevens over seksueel gedrag of seksuele gerichtheid – aan de verkeerde persoon wordt verstrekt.

Kortom, per dienst moeten aard en omvang van de verwerking, impact voor en kwetsbaarheid van betrokkene en de mate waarin de gegevens bruikbaar zijn voor misbruik in ogenschouw worden genomen.

Persoonsgegevens – Betrouwbaarheidsniveau laag

Betrouwbaarheidsniveau laag is het basisniveau in deze regeling. Dat houdt in dat de risico's voor de betrokkene bij verlies of onbevoegd of onzorgvuldig gebruik van de persoonsgegevens zodanig zijn dat standaard (informatie)beveiligingsmaatregelen, waaraan ook identificatiemiddelen met betrouwbaarheidsniveau laag moeten voldoen op grond van de eIDAS-verordening, toereikend zijn. Bij verwerkingen van persoonsgegevens in deze klasse gaat het om uitsluitend niet bijzondere categorieën van persoonsgegevens en om persoonsgegevens die niet strafrechtelijke veroordelingen en strafbare feiten betreffen. Deze categorie omvat bijvoorbeeld gegevens die reeds algemeen bekend zijn bij een breed publiek zoals naam, adres en woonplaats. Omdat de gegevens algemeen bekend worden geacht, is een hoger betrouwbaarheidsniveau niet noodzakelijk. Voorkomen moet worden dat diensten met een relatief bescheiden risicoprofiel op het niveau substantieel komen. Dit werpt een nodeloos hoge drempel op voor relatief eenvoudige diensten als het aanvragen van een eenvoudige vergunning, bijvoorbeeld een kapvergunning.

Persoonsgegevens – Betrouwbaarheidsniveau substantieel

Persoonsgegevens die door hun aard bijzonder gevoelig zijn wat betreft de grondrechten en fundamentele vrijheden, verdienen specifieke bescherming aangezien de context van de verwerking ervan significante risico's kan meebrengen voor de grondrechten en de fundamentele vrijheden.
Bij bijzondere categorieën van persoonsgegevens worden persoonsgegevens verwerkt waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken. Ook de verwerking van genetische gegevens, biometrische gegevens ter identificatie van een persoon alsmede gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid (art. 9 lid 1 AVG) zijn bijzondere persoonsgegevens.
Al deze gegevens zijn in beginsel geclassificeerd op niveau substantieel.

[6] Artikel 4, eerste lid, AVG.
[7] Artikel 4, tweede lid, AVG.
[8] De AVG bevat een aantal verplichtingen voor organisaties die op grote schaal bijzondere persoonsgegevens verwerken. De AP vult 'grootschalige gegevensverwerking' voor de zorg nader in. De in dat verband gehanteerde factoren zijn evenwel breed bruikbaar. https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-geeft-uitleg-over-grootschalige-gegevensverwerking-de-zorg.

Ook gegevens over gezondheid[9] zijn bijzondere persoonsgegevens. Echter, de risico's als deze gegevens in verkeerde handen vallen is zodanig groot, dat deze gegevens al snel vallen onder categorie hoog (zie verder de toelichting bij hoog). Onder niveau substantieel vallen gezondheidsgegevens die *niet*:

- stigmatiserend kunnen werken;
- reputatieschade kunnen opleveren;
- tot uitsluiting kunnen leiden;
- schade kunnen opleveren aan de gezondheid, of
- tot chanteerbaarheid kunnen leiden.

Betrouwbaarheidsniveau substantieel is bijvoorbeeld van toepassing bij arbeidsongeschiktheidsuitkeringen; zo vallen gegevens over een eerste ziektedag en de uitkeringsperiode hier onder.

De verwerking van persoonsgegevens van strafrechtelijke aard valt in beginsel onder niveau substantieel. In de UAVG gaat het hierbij om persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen als bedoeld in artikel 10 van de AVG. Gegevens uit antecedentenonderzoek (onderzoek van meerdere registers en door gesprekken en huisbezoek met behulp waarvan risico's in kaart worden gebracht zodat problemen met bijvoorbeeld huurders of werknemers worden voorkomen) en politiegegevens (persoonsgegevens die worden verwerkt in het kader van uitvoering van de politietaak, bedoeld in de Politiewet) vallen eveneens onder niveau substantieel.

Er zijn ook gegevens die niet tot bijzondere categorieën van persoonsgegevens worden gerekend, maar volgens de Autoriteit Persoonsgegevens gevoeliger kunnen zijn dan gewone persoonsgegevens en daarom een hoger beschermingsniveau vereisen. Te denken valt aan gegevens over iemands financiële of economische situatie (zoals salarisgegevens), gebruikersnamen en wachtwoorden. Maar volgens de Autoriteit Persoonsgegevens vallen betalingsgegevens hier ook onder. Betalingsgegevens betreffen de IBAN code, de BIC-code[10] en het transactiebedrag, of geaggregeerde basisgegevens over betalingen.[11] Ook deze gevoelige gegevens niet zijnde bijzondere categorieën van persoonsgegevens of persoonsgegevens van strafrechtelijke aard zijn opgenomen onder niveau substantieel.

Gegevens waarbij een reëel risico bestaat op identiteitsfraude – dat wil zeggen het misbruik maken van valse of gestolen identiteitsgegevens – valt in beginsel onder substantieel, tenzij sprake is van de verzwarende omstandigheden zoals hieronder bij hoog genoemd.

Persoonsgegevens – Betrouwbaarheidsniveau Hoog

In deze categorie gaat het om persoonsgegevens die bijzonder van aard kunnen zijn en een hoog risico vormen voor de persoon in kwestie indien deze gegevens in verkeerde handen vallen. Dit kan stigmatiserend werken, uitsluiting (bijvoorbeeld van het verkrijgen van een verzekering) of reputatieschade opleveren, schade opleveren aan de gezondheid, (identiteits)fraude bewerkstelligen, ernstig misbruik of oneigenlijk gebruik van de betreffende dienst opleveren of de betrokkene chantabel maken. Strafrechtelijke gegevens met een dergelijk hoog risico (bijvoorbeeld verband houdend met ernstige misdrijven) vallen in deze categorie, alsmede gegevens over werkprestaties of relatieproblemen.

Om te bepalen of een dienst stigmatiserend kan zijn of reputatieschade oplevert, is een belangrijke maatstaf de maatschappelijke positie van betrokkenen. Ook moet worden bezien of het afbreukrisico zo groot is voor betrokkenen dat deelname aan de maatschappij ernstig wordt bemoeilijkt. Te denken valt aan de volgende voorbeelden:

– Bijzondere gegevens: gegevens over geestelijke gezondheidszorg, gokverslaving, alcoholverslaving etc.
– Strafrechtelijke gegevens: zaken zoals zedenmisdrijven, of gevallen waarin het identificatie van een dader betreft.

Gezondheidsgegevens zijn persoonsgegevens die verband houden met de fysieke of mentale gezondheid van een natuurlijke persoon, waaronder gegevens over verleende gezondheidsdiensten waarmee informatie over zijn gezondheidstoestand wordt gegeven.[12] De overwegingen bij de AVG zeggen daarover dat het gaat om gegevens die informatie geven over de lichamelijke of geestelijke

[9] Gezondheidsgegevens zijn persoonsgegevens die verband houden met de fysieke of mentale gezondheid van een natuurlijke persoon, waaronder gegevens over verleende gezondheidsdiensten waarmee informatie over zijn gezondheidstoestand wordt gegeven, zie artikel 4 lid 15 AVG.
[10] De BIC code staat voor Bank Identificatie Code en wordt gebruikt om een bank te kunnen identificeren.
[11] Verordening (EG) Nr. 924/2009 van het Europees Parlement en de Raad van 16 september 2009, betreffende grensoverschrijdende betalingen in de Gemeenschap en tot intrekking van Verordening (EG) nr. 2560/2001.
[12] Zie artikel 4, vijftiende lid, AVG.

gezondheidstoestand van de betrokkene in het verleden, het heden en de toekomst. Het betreft een aan een natuurlijke persoon toegekend cijfer, symbool of kenmerk dat als unieke identificatie van die natuurlijke persoon geldt voor gezondheidsdoeleinden; informatie die voortkomt uit het testen of onderzoeken van een lichaamsdeel of lichaamseigen stof, met inbegrip van genetische gegevens en biologische monsters; en informatie over bijvoorbeeld ziekte, handicap, ziekterisico, medische voorgeschiedenis, klinische behandeling of de fysiologische of biomedische staat van de betrokkene, ongeacht de bron, zoals bijvoorbeeld een arts of een andere gezondheidswerker, een ziekenhuis, een medisch hulpmiddel of een in-vitrodiagnostiek.[13] Gezondheidsgegevens vallen onder betrouwbaarheidsniveau hoog als deze gegevens in verkeerde handen kunnen vallen en daardoor:

- stigmatiserend kunnen werken;
- reputatieschade kunnen opleveren;
- tot uitsluiting kunnen leiden;
- schade kunnen opleveren aan de gezondheid, of
- tot chanteerbaarheid kunnen leiden.

Een voorbeeld van een gezondheidsgegeven dat, indien in verkeerde handen, stigmatiserend kan werken is een positieve uitslag op HIV. Reputatieschade kan iemand bijvoorbeeld lijden, omdat bekend is geworden dat de persoon bij de GGZ onder behandeling staat. De persoon wordt mogelijk niet stabiel geacht door zijn werkgever en de werkgever kan betwijfelen of als gevolg daarvan zijn werknemer zijn werk nog wel naar behoren kan uitvoeren. Als een patiënt zelf aanvullingen wil aanbrengen op zijn medisch dossier, dan valt dit onder niveau hoog. Bijvoorbeeld het toevoegen van resultaten van zelfmetingen van parameters zoals bloedsuikerspiegel, bloeddruk, gewicht.[14] Een verkeerde invoer kan immers schade opleveren aan de gezondheid. Door verslavingsproblematiek kan een persoon chantabel zijn, bijvoorbeeld een gok- of alcoholverslaving.

Uiteraard zijn de genoemde voorbeelden niet limitatief. Zo valt het inzien van een compleet medisch dossier onder niveau hoog als het dossier informatie bevat dat reputatieschade kan opleveren, stigmatiserend kan werken, schade kan opleveren aan de gezondheid of voor de betrokken persoon chantabel kan zijn. Indien afspraak- en inschrijfgegevens inzicht geven in het specialisme van de zorgaanbieder, dan is betrouwbaarheidsniveau hoog ook wenselijk. In zijn algemeenheid geldt dat bij gegevens die onder het medisch beroepsgeheim vallen sprake is van classificering ‘hoog’.

2.3.4 Aard van de bedrijfsgegevens

Diensten die (mede) door ondernemingen en rechtspersonen worden afgenomen, behoeven ook classificering; de wet, waaronder artikel 6 daarvan, ziet immers op de toegang tot elektronische diensten door burgers en bedrijven. Bij elektronische toegang door een bedrijf zal veelal geen sprake zijn van verwerking van bijzondere persoonsgegevens. Inloggen met niveau laag kan dan echter onwenselijk zijn, in verband met de aard van de betrokken bedrijfsgegevens. Dit kan voor bedrijven -analoog aan burgers – negatieve gevolgen en (financiële) schade opleveren.

Bij bedrijfsgegevens moet worden onderscheiden tussen algemeen bekende (openbare en/of via het Handelsregister gemakkelijk toegankelijke) gegevens, zoals naam, contactgegevens en soort bedrijvigheid, en gevoelige (geheime) informatie, die verband houdt met de uitvoering van het bedrijfsproces. Bij gevoelige bedrijfsgegevens kan gedacht kan worden aan de samenstelling van producten, het klantenbestand en samenwerkingspartners, specialistische kennis en commerciële gegevens, kortom informatie die concurrentiegevoelig is en handelswaarde bezit.[15] Verwerking hiervan rechtvaardigt betrouwbaarheidsniveau substantieel.

2.3.5 Burgerservicenummer

Het burgerservicenummer (BSN) is een uniek persoonsnummer en een persoonsgegeven zoals bedoeld in art. 4 lid 1 AVG. Art. 87 AVG stelt dat lidstaten voor de verwerking van het nationaal identificatienummer zelf specifieke voorwaarden kunnen stellen. Passende waarborgen zijn vereist. Het te verwerken BSN kan betrekking hebben op degene aan wie de dienst wordt verleend of zijn eventuele gemachtigde. Diensten waarbij het BSN van derden (bijv. werknemers) wordt verwerkt zijn eveneens in de tabel meegenomen.

---

[13] Overweging 35 bij de AVG.

[14] Privacycare – PBLQ, Onderzoek betrouwbaarheidsniveau patiëntenauthenticatie bij elektronische gegevensuitwisseling in de zorg, mei 2016, p. 40. Wel moet – in het kader van *remote patient monitoring* – mogelijk worden geacht dat zorgaanbieders na een succesvolle authenticatie op niveau hoog een token uitgeven die voor een bepaalde tijdsduur gebruikt kan worden om zelfmetingen in te sturen. Op deze manier kan bijvoorbeeld een telefoon worden gekoppeld aan een persoon.

[15] Zie artikel 1 van de Wet van 17 oktober 2018, houdende regels ter uitvoering van Richtlijn 2016/943/EU van het Europees Parlement en de Raad van 8 juni 2016 betreffende de bescherming van niet-openbaar gemaakte knowhow en bedrijfsinformatie (bedrijfsgeheimen) tegen het onrechtmatig verkrijgen, gebruiken en openbaar maken daarvan (PbEU 2016, L157) (Wet bescherming bedrijfsgeheimen), Stb. 2018, 369.

Burgerservicenummer – niveau laag

In de categorie laag wordt het BSN bij de dienstverlening uitsluitend opgegeven door degene aan wie de dienst wordt verstrekt, maar wordt het niet door de dienstverlener tijdens het proces van dienstverlening verstrekt aan degene die is ingelogd. Als gevolg daarvan bestaat er geen kans dat een burgerservicenummer wordt verstrekt aan onbevoegden. Een voorbeeld van een dienst op betrouwbaarheidsniveau laag is een digitaal formulier van de dienstverlener waarbij het BSN door de gebruiker moet worden opgegeven.
In de praktijk komt het voor dat in een sessie sprake is van terugkoppeling van identificerende gegevens na verstrekking van het BSN, waarbij de dienstverlener naast naam en/of adresgegevens ook het opgegeven BSN teruggeeft. Dit zou blijkens bijlage 2 op niveau substantieel moeten worden bepaald, terwijl het BSN eerder is verstrekt door de gebruiker van de dienst. In dergelijke gevallen is inschalen op niveau substantieel niet per se logisch. Dit geldt eveneens voor de situatie waarin na inloggen met DigiD een burger welkom wordt geheten en het BSN wordt teruggekoppeld. Immers: in dit geval geeft de burger eigenlijk impliciet een BSN op. Echter: het voor dergelijke situaties toestaan van gebruik van niveau laag *sec* zou niet wenselijk zijn om redenen van tegengaan van misbruik; voorkomen moet worden dat de persoon die inlogt niet de burger zelf is maar een malafide persoon. Daarom ligt het in de rede voor deze gevallen niveau laag met minimaal twee factor authenticatie te eisen.

Burgerservicenummer – niveau substantieel

Bij niveau substantieel wordt het BSN van degene aan wie de dienst wordt verleend in het proces van dienstverlening teruggekoppeld/verstrekt aan degene die is ingelogd zonder dat dat nummer door de gebruiker is opgegeven bij het inloggen. Een voorbeeld hiervan is een vooringevuld formulier dat de gebruiker van de dienstverlener ontvangt en waarop zijn of haar BSN reeds is ingevuld.

Zoals hiervoor reeds is aangegeven, komt het in de praktijk voor dat in een sessie sprake is van terugkoppeling van identificerende gegevens na verstrekking van het BSN, waarbij de dienstverlener naast naam en/of adresgegevens ook het opgegeven BSN teruggeeft. Dit zou blijkens bijlage 2 op niveau substantieel moeten worden bepaald, terwijl het BSN eerder is verstrekt door de gebruiker van de dienst. In dergelijke gevallen ligt het in de rede niveau laag met minimaal twee factor authenticatie te eisen.

Burgerservicenummer- niveau hoog

Er zijn geen specifieke criteria met betrekking tot de verwerking van het BSN die leiden tot de indeling van een dienst in categorie hoog. Niveau hoog is dus niet van toepassing, in die zin dat het gebruik van het BSN in zichzelf niet zal leiden tot inzet van betrouwbaarheidsniveau hoog. Wel kan het BSN in combinatie met andere (al dan niet bijzondere) persoonsgegevens, zoals NAW-gegevens en een rekeningnummer, leiden tot bijvoorbeeld reputatieschade of chanteerbaarheid.

2.3.6 Basisregistraties

Kwaliteit en betrouwbaarheid van de basisregistraties[NaN] zijn essentieel. De impact van het wijzigen van een (authentiek) gegeven in een basisregistratie kan groot zijn, aangezien de gegevens aan een grote groep afnemers worden verstrekt en door hen verplicht moeten worden gebruikt. Elke opname of wijziging van een gegeven in een registratie moet met de grootste zekerheid en zorgvuldigheid gebeuren, juist omdat afnemers, zoals medeoverheden, op deze gegevens moeten kunnen vertrouwen. Deze gegevens zullen in veel gevallen ook ten grondslag liggen aan domeinspecifieke rechten (aanspraken) en verplichtingen van burgers en bedrijven. Afhankelijk van de bij de betreffende basisregistratie behorende en gehanteerde procedure is betrouwbaarheidsniveau substantieel of hoog van toepassing. Deze procedure hangt samen met de aard en de gevolgen van de dienst.

Basisregistraties – niveau laag

Er vindt in het kader van de dienstverlening geen verwerking met gevolgen voor gegevens in de basisregistraties plaats op niveau laag.

Basisregistraties – niveau substantieel

Niveau substantieel is voldoende indien er op een melding die of verzoek dat tot wijziging van een basisregistratie zou moeten leiden, een controle plaatsvindt door de instantie die verantwoordelijk is

Welke registraties aangemerkt zijn als basisregistraties is te vinden in bijlage 1 van deze regeling.

voor de basisregistratie op de juistheid van de gegevens die gewijzigd of opgegeven worden. Zo'n aanvullende controle bestaat uit – doorgaans nog via menselijke tussenkomst te realiseren – technische, organisatorische of andere maatregelen en heeft daarmee mitigerend effect. Inloggen met een middel op niveau hoog is dan niet nodig. Hiervan is sprake bij authentieke gegevens in basisregistraties. Dit zijn gegevens die bij wettelijk voorschrift als zodanig zijn aangemerkt; de status 'authentiek' betekent dat de kwaliteit van het gegeven dusdanig is gegarandeerd, dat de gebruiker op de juistheid daarvan kan vertrouwen. Het bij inschrijving of mutatie toetsen aan wettelijke vereisten (*compliance*), zoals bijvoorbeeld bij het Kadaster plaatsvindt, wordt niet onder de hier bedoelde controle (validatie) begrepen.

Basisregistratie – niveau hoog

Betrouwbaarheidsniveau hoog wordt gebruikt indien de opname of wijziging van gegevens direct in de bron (= de basisregistratie) geschiedt en er dus geen aanvullende controle plaatsvindt op de verwerking van de gegevens. Ook kan door voortschrijdende digitalisering controle steeds minder in de vorm van menselijke tussenkomst plaatsvinden, waardoor een dienstverlener mogelijk eerder op inschaling op niveau hoog uit komt. In de praktijk komt de mogelijkheid van directe opname of wijziging in basisregistraties (nog) alleen voor bij niet-authentieke gegevens.

NB: Een dienstverlener kan met betrekking tot *andere* registraties dan basisregistraties ook tot inschaling overgaan. Zo kent het Kadaster de openbare registers, de schepenregistratie en de luchtvaartregistratie, alle drie met rechtsgevolgen. Dit onderdeel van de regeling/tabel geldt dan naar zijn aard niet, maar de wegingsfactoren bedrijfsgegevens (zie 2.3.4) en/of economisch belang (zie 2.3.7) zullen dan soelaas kunnen bieden, waarbij het element controle/mitigerende maatregelen de facto een rol kan spelen.

2.3.7 Economisch belang

Bij de toegang tot een dienst kan ingeval van onjuiste identificatie, identiteitsfraude of verkeerde verwerking van gegevens financiële schade ontstaan. Hierbij kan gedacht worden aan schade door misbruik of fraude, verlies van geld of economische positie, aansprakelijkheidsstelling, onbevoegden die toegang krijgen tot concurrentiegevoelige informatie of koersgevoelige informatie die uitlekt. Voor het classificeren van het betrouwbaarheidsniveau van de dienst zijn de mate van ingrijpendheid voor de economische positie van burgers/bedrijven (kwalitatief) en directe schade (kwantitatief) uitgangspunt. Voor het bepalen van de impact moet rekening worden gehouden met de (feitelijke) omstandigheden van het geval, oftewel de verhouding tussen de geleden schade en de draagkracht van de doelgroep die van een bepaalde dienst gebruikmaakt. Zo levert misgelopen subsidie directe schade op, niet de gederfde inkomsten als gevolg van het niet kunnen uitvoeren van het plan waarvoor de subsidie was aangevraagd (dit is vervolgschade). Voor het bepalen van de directe schade is de frequentie van misbruik van die specifieke dienst niet van belang.

Economisch belang – niveau laag

Indien onjuiste identificatie, fraude of misbruik niet of nauwelijks ingrijpend is voor de economische positie van burgers/bedrijven – de gevolgen voor degene wiens identiteit wordt misbruikt zijn weliswaar vervelend, maar leiden niet tot gedwongen aanpassing van activiteiten of welstandsniveau – kan voor classificering van de dienst volstaan worden met betrouwbaarheidsniveau laag. Richtsnoer is dat de directe schade per geval:
- Voor burgers lager is dan € 1.000,–
- Voor bedrijven tot 250 werknemers (MKB) lager is dan € 125.000,–
- Voor grotere bedrijven lager is dan € 500.000,–

Economisch belang – niveau substantieel

Indien onjuiste identificatie, fraude of misbruik ingrijpend is voor de economische positie van burgers/bedrijven – de gevolgen zijn van (tijdelijke) invloed op activiteiten of welstandsniveau van degene wiens identiteit wordt misbruikt – dient voor classificering van de dienst betrouwbaarheidsniveau substantieel te worden gehanteerd. Richtsnoer is dat de directe schade per geval:
- Voor burgers hoger is dan € 1.000,–
- Voor bedrijven tot 250 werknemers (MKB) hoger is dan € 125.000,–
- Voor grotere bedrijven hoger is dan € 500.000,–

Benadrukt wordt, dat de genoemde bedragen niet absoluut zijn, maar gemiddelden en richting gevend. Binnen de categorie burgers bestaan immers grote verschillen in draagkracht en doelgroepen. Dit geldt ook voor bedrijven; de omstandigheden van een groot MKB-bedrijf zijn anders dan die van een zzp'er. Veelal wordt bij de (toegang tot) dienstverlening zelf geen onderscheid gemaakt naar

bedrijfsgrootte. Voorts kan de specifieke aard van de dienst met zich brengen, dat onjuiste identificatie of identiteitsfraude ingrijpende gevolgen heeft voor de economische positie van burgers/bedrijven. Om die reden moeten dienstverleners een dienst op niveau substantieel kunnen kwalificeren.

Economisch belang – niveau hoog

Indien onjuiste identificatie, fraude of misbruik zodanig ingrijpend is voor de economische positie van bedrijven/burgers dat het ongewijzigd voortbestaan van het bedrijf (bijvoorbeeld schade ter grootte van de jaaromzet) of het doorleven op hetzelfde welstandsniveau (bijvoorbeeld schade ter grootte van een jaarinkomen) ernstig bedreigd wordt, dan is niveau hoog het passende betrouwbaarheidsniveau.

2.4 Risico verlagende factoren

Het door dienstverleners toepassen van de hiervoor geschetste classificatiesystematiek zal in de meeste gevallen leiden tot een door de systematiek gedragen conclusie over het te hanteren betrouwbaarheidsniveau voor authenticatie inzake door hen aangeboden diensten. Echter, op basis hiervan zal niet voor alle situaties een passend niveau bepaald kunnen worden; er zijn omstandigheden denkbaar die tot minder strikte toepassing kunnen nopen. Zo is het mogelijk om de authenticatie (artikel 3) of de registratie van een machtiging (artikel 5) voor een elektronische dienst op een naastlager niveau vast te stellen. De onderhavige regeling bevat inzake authenticatie een aantal mogelijkheden om het niveau naar beneden bij te stellen, indien evident kan worden beargumenteerd dat het feitelijke risico van de toegangsverlening tot een dienst lager ligt, mits specifieke wettelijke eisen hier niet aan in de weg staan. In deze gevallen is sprake van het door de organisatie (in het vervolgproces) nemen van extra processtappen of mitigerende maatregelen waardoor het risico verminderd wordt. Verlaging kan vanzelfsprekend slechts aan de orde zijn indien deze passend is binnen de integrale verantwoordelijkheid van de dienstverlener.

Een dienstverlener kan in plaats van niveau hoog substantieel en in plaats van substantieel laag (dus: het naastlagere niveau oftewel maximaal een stap lager) bepalen, als het authenticatieproces voorziet in een extra waarborg. Deze moet bestaan uit een aanvullende technische of fysieke vorm van controle van de authenticiteit van de gebruiker van het identificatiemiddel. Deze controle moet plaatsvinden na de eerste authenticatie. Deze aanvullende stap biedt voldoende waarborgen dat de persoon die inlogde daadwerkelijk de persoon is die hij zegt te zijn. Een voorbeeld is het proces van trouwen of het aangaan van een geregistreerd partnerschap. Na een elektronische melding van het voornemen van een huwelijk of geregistreerd partnerschap, verschijnen de beide partners fysiek voor een trouwambtenaar om het huwelijk te voltrekken of het partnerschap te registreren. Het risico op het ten onrechte aangaan van het huwelijk is dan niet afhankelijk van de inloggen bij de aanvraag.

Ook kan een naastlager niveau worden vastgesteld, indien bij inlog uitsluitend informatie aan het bestuursorgaan of de aangewezen organisatie wordt ‘gebracht’. Dit is het geval bij op transactie georiënteerde diensten, waarbij de eerste stap in een proces bestaat uit een digitale aanvraag, aanlevering van gegevens of een aangifte door een burger of bedrijf, waarna via een ander (digitaal of papieren) kanaal een vervolgstap door de overheid volgt (terugkoppeling, besluit, verstrekking van documenten etc.). Het gaat dan om het louter ‘brengen’ van gegevens. Met de aanlevering van de gegevens ontstaat nog niet het gevolg (bijvoorbeeld: betaling) en er worden ook geen gegevens door de dienst zelf vrijgegeven. Eventuele schade vindt dan niet onherroepelijk na het inloggen plaats. Bepalend is hoe de dienst feitelijk wordt ingericht. Wordt gekozen voor vooringevulde (belasting)aangifte, dan betekent inloggen dat gegevens worden vrijgegeven, en dat van een lager niveau geen sprake (meer) kan zijn. Immers, na inloggen worden dan direct persoonsgegevens vrijgegeven en ontstaat onherroepelijk schade als dat aan de verkeerde persoon gebeurt. Overigens zal bij het ter beschikking stellen van privacygevoelige informatie, zoals bijzondere persoonsgegevens, een naastlager niveau niet snel in de rede liggen.

Voorts werkt het risicoverlagend als de dienstverlener later in het proces herstelmaatregelen neemt, bijvoorbeeld in de vorm van aanvullende controles in het achterliggende proces waartoe toegang is verleend. Voorbeeld is een proces van aangifte en een daaropvolgende beschikking die via een ander kanaal wordt toegestuurd.

In het geval van het opvragen of weergeven van privacygevoelige informatie die niet door de gebruiker ‘gebracht’ is, ligt het niet in de rede om het niveau te verlagen, daar er dan geen risicobeperkende factoren zullen zijn. Authenticatie ‘aan de voordeur’ zal dan direct van het juiste niveau moeten zijn, om tot een betrouwbare en praktisch werkbare dienst te komen.

2.5 Risico verhogende factoren

Zoals in 2.1 wordt aangegeven, behelst het toepassen van de classificatiesystematiek in feite een

snelle, vereenvoudigde risicoanalyse. Naast risico verlagende factoren (zie 2.4), zijn er ook omstandigheden denkbaar die juist tot hogere classificering kunnen nopen. De onderhavige regeling bevat daarom ook de mogelijkheid om aard, kenmerken en context van de dienst nader te beschouwen in de vorm van het uitvoeren van een volledige risicoanalyse. Dit hoeft dan niet per definitie te leiden tot een verhoogde classificatie (en dus: authenticatie) niveau, maar dient ertoe het passende betrouwbaarheidsniveau voor de betreffende dienst beter te kunnen bepalen en te onderbouwen, omdat toepassing van de criteria gezien de specifieke omstandigheden niet tot een dragende motivering leiden. Indicatoren voor het vermoeden van een verhoogd risico liggen primair op het terrein van de overheid zelf, zoals verlies van vertrouwen in een publieke dienstverlener als gevolg van onvoldoende authenticatie, (structurele) identiteitsfraude of grootschalig misbruik van diensten en grote bestuurlijk-politieke gevoeligheid. Ook maatschappelijke effecten kunnen een indicator vormen. Het uitvoeren van een volledige risicoanalyse behelst een zorgvuldig proces. Hiertoe kan de Baseline Informatiebeveiliging Overheid geraadpleegd worden.[17] De onderhavige regeling stelt geen specifieke (vorm)vereisten aan een dergelijke risicoanalyse.

2.6 Machtigen

Normaal gesproken is bij elektronische dienstverlening alleen de identiteit van de gebruiker (de afnemer van de dienst oftewel belanghebbende) van belang. In de praktijk komt het echter vaak voor, dat een belanghebbende niet zelf de dienst van het bestuursorgaan of de aangewezen organisatie afneemt, maar zich – vrijwillig – laat vertegenwoordigen; de belanghebbende geeft daartoe dan een, al dan niet digitale, machtiging af aan een derde. Hierbij wordt de bevoegdheid verleend om in naam van belanghebbende (rechts)handelingen te verrichten (vgl. art. 3:60 ev BW). Vanzelfsprekend geldt dan onverminderd dat de betrouwbaarheid van de elektronische dienstverlening gewaarborgd moet zijn en dat machtiging niet de zwakke schakel in dit proces mag zijn. Uitgangspunt is dat de betrouwbaarheid van een machtigingsregistratie tenminste gelijk is aan het betrouwbaarheidsniveau dat voor de authenticatie voor de dienst is vereist. In de praktijk wordt vaak gebruik gemaakt van niet (uitsluitend) langs digitale weg afgegeven machtigingen. Deze regeling houdt daar rekening mee door uit te gaan van het principe dat het totale dienstverleningsproces, dus inclusief de toegangsverlening, min of meer dezelfde waarborgen kent. De machtiging moet met voldoende betrouwbaarheid zijn afgegeven, waardoor de wil en de betrokkenheid van de belanghebbende oftewel de machtiginggever met voldoende zekerheid kan worden vastgesteld.

3. Tijdelijk toestaan van lager betrouwbaarheidsniveau

3.1 Achtergrond en voorwaarden

Het voorgaande deel van de toelichting heeft betrekking op de inschaling van het betrouwbaarheidsniveau van de overheidsdiensten zelf, op basis waarvan kan worden bepaald welk inlogmiddel met corresponderende betrouwbaarheid moet worden ingezet voor toegang tot de dienstverlening. Echter, de ontwikkeling van de digitale overheid en het breed beschikbaar maken van inlogmiddelen op hogere betrouwbaarheidsniveaus is een proces dat continu doorloopt, en zich stapsgewijs voltrekt. Het ligt in de verwachting dat op het moment van inwerkingtreding van de wet nog een aanloopperiode nodig is, omdat nog niet op alle betrouwbaarheidsniveaus de benodigde inlogmiddelen direct breed beschikbaar zullen zijn. Onverkorte verplichtstelling van hoogbetrouwbare middelen zou dan feitelijk een dode letter in de wet zijn. Er is daarom voor gekozen om met deze omstandigheid in de regeling rekening te houden en termijn te stellen waarin de beweging naar de hogere betrouwbaarheidsniveaus moet en ook redelijkerwijs kan worden gemaakt.

Op grond van artikel 6, vierde lid, van de wet kan voor een bepaalde periode authenticatie met een aangewezen middel met een lager betrouwbaarheidsniveau worden toegestaan dan het niveau dat voor die dienst is bepaald. Deze bepaling is om verschillende redenen opgenomen. Allereerst is onzeker of het middel tijdig door voldoende afnemers van elektronische diensten zal (kunnen) worden gebruikt. Dat is afhankelijk van de bereidheid van burgers/bedrijven (gebruikers) om een dergelijk middel te verwerven en van het tempo waarop dienstverleners op de benodigde infrastructuur (gdi-voorzieningen) kunnen worden aangesloten. Zolang de beschikbaarheid en dekkingsgraad (incl. aansluitingsgraad) van identificatiemiddelen op de betrouwbaarheidsniveaus substantieel en hoog nog niet op een adequaat niveau zijn, zal het toepassen van de in deze regeling vervatte regels over betrouwbaarheidsniveaus ertoe leiden dat toegang tot elektronische dienstverlening onevenredig wordt beperkt. Het is niet opportuun om dienstverleners te verplichten tot het hanteren van een bepaald betrouwbaarheidsniveau, als er door onvoldoende brede beschikbaarheid van inlogmiddelen eenvoudigweg niet aan kan worden voldaan.

[17] BIO, toepasselijk voor alle overheidslagen. Stct. 2020, 7857.

In dat verband ligt het tijdelijk toestaan van authenticatie met een middel met een naastlager betrouwbaarheidsniveau in de rede. Artikel 6 bepaalt daarom dat een dienstverlener (bestuursorgaan of aangewezen organisatie) voor een elektronische dienst, waarvoor authenticatie op betrouwbaarheidsniveau hoog respectievelijk substantieel nodig is, kan toestaan dat tot twee jaar na inwerkingtreding van deze regeling voor toegang tot die dienst tevens gebruik kan worden gemaakt van een toegelaten of erkend middel op niveau substantieel (als alternatief voor hoog) respectievelijk een middel op niveau laag (als alternatief voor substantieel). Van deze bevoegdheid kan de dienstverlener alleen gebruik maken indien de beschikbaarheid of het gebruik van identificatiemiddelen op de betrouwbaarheidsniveaus substantieel en hoog, of de mogelijkheid om deze te gebruiken om toegang te krijgen tot dienstverlening, onvoldoende is. Of hiervan daadwerkelijk sprake is, zal in overleg met de Minister van BZK moeten worden bepaald; laatstgenoemde heeft immers – gezien zijn verantwoordelijkheid voor het gehele stelsel – het beste inzicht in landelijke uitrol/beschikbaarheid en gebruik.

In het laatste geval geldt, ingevolge artikel 6, vierde lid, van de wet, als voorwaarde dat sprake moet zijn van een middel op niveau laag met ten minste twee authenticatiefactoren zoals bedoeld in de eIDAS-verordening. Het is de verwachting dat twee jaar na inwerkingtreding van deze regeling sprake zal zijn van voldoende beschikbaarheid en dekkingsgraad van toegelaten (publieke en private) inlogmiddelen gezamenlijk. Deze termijn is mede afgestemd op het feit dat na inwerkingtreding van de wet en bijbehorende uitvoeringsregelgeving, aanbieders van inlogmiddelen door de Minister van BZK moeten worden getoetst en daartoe een toelatingsprocedure moeten doorlopen. Naar verwachting zullen stapsgewijs toegelaten (erkende) middelen beschikbaar komen. Mocht dit (veel) eerder dan binnen twee jaar het geval zijn, dan zal worden overwogen om de tijdelijke uitzonderingsmogelijkheid te schrappen. Mocht dit onverhoopt later zijn, dan zal worden overwogen om de termijn te verlengen.

De periode van 2 jaar biedt voorts de mogelijkheid om op basis van veranderde inzichten vast te stellen of er diensten zijn waarvoor het lagere niveau van authenticatie blijkt te volstaan. Door ervaringen te monitoren en de regeling eventueel op basis daarvan te actualiseren, bestaat de gelegenheid om onnodige lasten in de toekomst, als gevolg van een te hoog voorgeschreven authenticatieniveau te voorkomen. Overigens behoort ook aanscherping/verhoging van het betrouwbaarheidsniveau tot de mogelijkheden, waarbij de lastenverhoging die daarmee gepaard zal kunnen gaan in de afweging wordt betrokken.

Er is niet voor gekozen in de regeling bepaalde (nieuwe) vormen van dienstverlening op niveau hoog uit te sluiten van de mogelijkheid van een tijdelijk lager niveau. Het is aan de dienstverlener om, bijvoorbeeld indien de ontwikkeling van die diensten belemmerd zou worden of wegens de risico's van het toelaten van identificatiemiddelen op het naastlagere niveau, zijn diensten volgens de hoofregel (artikel 2) te classificeren en een lager authenticatieniveau niet toe te staan.

Indien een dienstverlener van artikel 6 gebruik maakt, dient dit kenbaar te zijn voor burgers/bedrijven (zie artikel 7 en hoofdstuk 5 van deze toelichting). Het is van belang dat de dienstverlener de betreffende informatie op zijn website actueel houdt.

Vanzelfsprekend ontslaat het gebruik van de tijdelijke afwijkingsbevoegdheid dienstverleners er niet van om hun (informatie)beveiliging op orde te hebben; zo geldt voor Rijk, gemeenten en provincies in dit verband de Baseline Informatiebeveiliging Overheid (BIO). Dienstverleners blijven zelfstandig verantwoordelijk voor de beveiliging van hun dienstverlening en van de toegang daartoe.
De beveiliging van de toegang tot elektronische diensten is verankerd in de bovenliggende wet (artikel 4 WDO) en de op grond daarvan vastgestelde informatiebeveiligingsbepalingen in het Besluit digitale overheid.

Vanzelfsprekend is stapeling van de artikelen 3 en 6 niet mogelijk. Gebruikmaking van de mogelijkheid tot lagere inschaling van een dienst door de toepassing van risicoverlagende factoren, sluit uit dat nog eens – tijdelijk – een stap omlaag wordt gemaakt en vice versa.
Dit wordt expliciet benoemd in het tweede lid van genoemde artikelen.

3.2 Verhouding tot artikel 24 (overgangsrecht bedrijfsmiddel) en artikel 29 (aansluitschema) WDO

Artikel 24 van de wet bevat een regeling voor bedrijfs- en organisatiemiddelen die op het moment van inwerkingtreden van de wet onderdeel uitmaakten van een stelsel van afspraken aangaande elektronische toegangsdiensten waarvan ook de Staat deel uitmaakte. Met dit artikel is geregeld dat deze (private) middelen gedurende een periode van 18 maanden worden aangemerkt als een erkend middel in de zin van artikel 11 van de wet. In het derde lid wordt geregeld voor welk betrouwbaarheidsniveau de desbetreffende middelen geacht worden te zijn erkend. Artikel 24 van de wet voorziet dus in de tijdelijke toelating van bepaalde middelen die al in gebruik zijn. Dat wetsartikel gaat niet over

het betrouwbaarheidsniveau van elektronische diensten of het accepteren van bepaalde middelen op een lager niveau.

Artikel 29, derde lid, van de wet voorziet in gefaseerde inwerkingtreding van de artikelen 7 en 15 WDO; bepaald is dat de acceptatieplicht voor een dienstverlener inzake toegelaten/erkende inlogmiddelen niet eerder van toepassing is dan nadat de betreffende dienstverlener is aangesloten op de generieke digitale infrastructuur. Het moment van feitelijke aansluiting is opgenomen in een (ministeriële regeling met) aansluitschema. Gevolg daarvan is, dat de dienstverlener tot dat moment ook niet-toegelaten/-erkende inlogmiddelen, zoals eigen domeinspecifieke authenticatiemethoden en middelen op niveau laag, voor het afnemen van zijn diensten kan laten gebruiken.

4. Verhouding tot de Algemene verordening gegevensbescherming

Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming) (PbEU 2016, L 119) (AVG) is van toepassing op de verwerking van persoonsgegevens zoals die plaatsvindt in het kader van elektronische dienstverlening door bestuursorganen en aangewezen organisaties. Ter bescherming van de rechten en vrijheden van natuurlijke personen in verband met de verwerking van persoonsgegevens zijn passende technische en organisatorische maatregelen nodig om een passende beveiliging te waarborgen.[18] Onder dergelijke maatregelen valt ook het hanteren/toepassen van het juiste betrouwbaarheidsniveau van authenticatie bij het verlenen van toegang tot elektronische diensten, zoals bepaald in deze regeling. Gelet op de AVG spelen de aard van de persoonsgegevens en de omvang van de verwerking daarvan een rol in het beoordelingskader dat in deze regeling is opgenomen. Zo leidt de verwerking van bijzondere categorieën van persoonsgegevens bijvoorbeeld tot een hoger betrouwbaarheidsniveau dan vereist is indien enkel niet-bijzondere categorieën van persoonsgegevens worden verwerkt. Het doorwerken van de AVG in deze regeling sluit ook aan bij dezelfde doorwerking van de AVG in de eIDAS-verordening[19], met name bij de op grond van artikel 8 van die verordening vastgestelde technische specificaties voor de betrouwbaarheidsniveaus laag, substantieel en hoog voor elektronische identificatiemiddelen.

5. Gevolgen en uitvoering

Bij de voorbereiding van deze regeling, die onlosmakelijk samenhangt met de uitgangspunten in de bovenliggende wet, is voor wat betreft de uitvoerbaarheid niet alleen het perspectief van de dienstverleners betrokken, maar ook dat van de doelgroep(en). Burgers en bedrijven moeten de nieuwe regels niet alleen kennen, maar ook 'kunnen'. Voor wat betreft de mate waarin de uitvoering voor hen 'doenlijk' is (gesproken wordt in dit verband van 'doenvermogen'[20]) is het volgende van belang.
Zoals hiervoor in 2.1 en 2.2 wordt aangegeven, beoogt deze regeling stroomlijning voor dienstverleners en is deze gericht op zoveel mogelijk uniformiteit bij de classificering van diensten met een vergelijkbaar risicoprofiel. Hoewel de regeling zekere ruimte voor dienstverleners biedt, zal deze naar verwachting niet leiden tot grote verschillen tussen dienstverleners. Classificering door de dienstverlener naar drie niveaus, betekent dat voor gebruikers vast staat voor welke dienst welk niveau inlogmiddel moet worden gebruikt; burgers/bedrijven hebben terzake geen keuzemogelijkheid – en ook geen keuzestress. Classificering moet worden beschouwd als besluit van algemene strekking in de zin van de Awb, waarop de Bekendmakingswet van toepassing is.
Duidelijkheid en kenbaarheid zijn van groot belang. Naast reguliere (elektronische) bekendmaking dient de dienstverlener op zijn website – dus: voorafgaand aan het moment van authenticatie van een persoon of bedrijf of registratie van een machtiging voor een elektronische dienst – op toegankelijke wijze inzichtelijk te maken voor welke dienst welk middel ten minste moet worden gebruikt en wat het gevolg is van het niet beschikken over het juiste niveau inlogmiddel: dan kan de dienst niet digitaal worden afgenomen. Benadrukt wordt dat gebruik van een middel van een hoger niveau is toegestaan.
Kortom: dienstverleners moeten informatie verschaffen over de digitale diensten die zij aanbieden, hoe deze kunnen worden afgenomen, wat daarvoor nodig is, wat van gebruikers verwacht wordt, welke processtappen moeten worden doorlopen, waar/hoe de benodigde inlogmiddelen kunnen worden aangeschaft en waar men terecht kan voor vragen (helpdesk). In termen van mentale belasting betekent dit dat gebruikers nieuwe informatie moeten gaan verwerken: bij de overheid kan niet langer voor alle diensten met (DigiD) laag worden ingelogd. Dat betekent dat nieuwe en/of meerdere middelen moeten worden aangeschaft, waarmee extra kosten, tijd en inspanningen (oa

[18] Artikel 5, eerste lid, onderdeel f, van de AVG.
[19] Artikel 5, eerste lid, van de eIDAS-verordening in samenhang met artikel 94, tweede lid, van de AVG.
[20] Zie: WRR, Weten is nog geen doen: Een realistisch perspectief op redzaamheid. Rapport nr. 97, 2017. Kabinetsreactie op dit rapport d.d. 22 januari 2018 (*Kamerstukken II* 2017/18, 34775 VI, nr. 88) en Voortgangsbericht (*Kamerstukken II* 2017/18, 34775 VI, nr. 113 en *Kamerstukken I* 2017/18, 34775, AE).

activeringshandelingen, mogelijk specifieke apparatuur) zijn gemoeid. Hoewel een zekere mate van oplettendheid door gebruikers nodig is, is naleving eenvoudig en is de verwachting dat routine wordt ontwikkeld; eenmaal aangeschaft en gebruikt, wijst het proces zich vanzelf. Er staat iets tegenover: burgers en bedrijven kunnen veiliger en betrouwbaarder inloggen bij de overheid.
Voor dienstverleners die hun elektronische dienstverlening nu al op een adequaat betrouwbaarheidsniveau aanbieden – conform de handreiking van het Forum Standaardisatie[21]waarop de onderhavige regeling in belangrijke mate is gebaseerd – wordt een beperkte aanpassing van hun dienstverlening verwacht. Voor hen zullen de extra kosten die aan de invoering van deze regeling verbonden zijn, minimaal uitvallen. Bij hen is de vereiste inspanning beperkt tot een check op de conformiteit (validatie van classificatie); de uitkomsten kunnen tot (enigszins) aangepaste werkprocessen leiden.
Voor dienstverleners die hun dienstverlening nog niet geclassificeerd hebben, is extra inspanning vereist en zal het beoordelen van hun diensten op basis van deze regeling en de gevolgen daarvan voor de uitvoering extra kosten met zich meebrengen.
Met deze regeling wordt een evenwichtig kader geboden voor het classificeren van het betrouwbaarheidsniveau van authenticatie bij elektronische dienstverlening. Enerzijds verhoogt een hoger betrouwbaarheidsniveau de betrouwbaarheid van overheidshandelen en de veiligheid van de communicatie met die overheid. Anderzijds leiden diezelfde hogere eisen tot extra lasten voor burgers en bedrijven vanwege aan te schaffen middel(en) en extra lasten bij het inloggen en tot meer handelingen voor de dienstverlener om met zekerheid iemands identiteit te kunnen vaststellen. Bij het formuleren van criteria op grond waarvan het betrouwbaarheidsniveau van de dienst moet worden beoordeeld, is een kader gegeven waarbij niet per definitie steeds gekozen moet worden voor het hoogste niveau van betrouwbaarheid. Daarbij is gelet op de passendheid van de criteria binnen de eisen die de AVG stelt in het kader van bescherming van persoonsgegevens. Alles afwegend moeten de extra lasten als verantwoord en proportioneel, ook in termen van gebruiksvriendelijkheid worden beschouwd. Immers onnodig hoge drempels zullen het gebruik van een middel door burgers remmen, of leiden tot ‘work arounds’ (alternatieve oplossingen), zoals het afgeven van middelen, wat dan de facto leidt tot minder veiligheid.
Deze regeling treedt tezamen met haar wettelijke grondslag in werking, op 1 juli 2023. Omdat de acceptatieplicht terzake van toegelaten inlogmiddelen op een later moment in werking treedt (artt. 7 en 15 jo artikel 6, eerste lid, en 29, derde lid, WDO) en voorkomen moet worden dat voor burgers en bedrijven onduidelijkheid ontstaat, is het raadzaam bij de kennisgeving van classificering te vermelden dat gebruikers tot nader order nog met meerdere inlogmiddelen/lagere niveaus terecht kunnen; deze kunnen nog worden gebruikt tot het moment dat voor de desbetreffende dienstverlener de acceptatieplicht gaat gelden.

6. Toezicht en handhaving

Zoals beschreven in paragraaf 6.2 van het algemeen deel van de memorie van toelichting bij het wetsvoorstel digitale overheid en de toelichting bij artikel 17 daarvan, verloopt het toezicht op de naleving van deze regeling door bestuursorganen op het niveau van de rijksoverheid (ministeries en zelfstandige bestuursorganen) en door de aangewezen organisaties (zie artikel 17, eerste lid, van de wet) als volgt: de minister, op wiens beleidsterrein het betreffende (zelfstandige) bestuursorgaan of aangewezen organisatie werkzaam is, wijst een toezichthouder aan. Het gaat daarbij in de regel om het terzake van de desbetreffende organisaties reeds functionerende toezicht. Voor wat betreft het toezicht op de ministeries zelf wijst de Minister van BZK de toezichthouder aan.
Voor wat betreft de naleving van deze regeling door provincies, gemeenten en waterschappen zal, in aansluiting op de bestaande praktijk, het toezicht er in bestaan dat zij bij de aansluiting op het stelsel van publieke voorzieningen de naleving van de verplichtingen moeten aantonen. In dit verband zij verwezen naar de Kamerbrief Interbestuurlijk toezicht onder de Wet digitale overheid.[22]

7. Advies en (internet)consultatie

Naar aanleiding van het advies van de Autoriteit Persoonsgegevens zijn de regeling, bijlage 2 en de toelichting aangevuld en verduidelijkt. Zo is artikel 6 voorzien van de voorwaarde waaronder de dienstverlener van de afwijkingsbevoegdheid gebruik kan maken en is het in de bijlage opgenomen afwegingskader aangevuld op het punt van verwerking van het BSN (niveau hoog). Voor wat betreft het advies om een gegevensbeschermingseffectbeoordeling (geb) uit te voeren, wordt gewezen op het feit dat doorlopend geb’s op het eID-stelsel worden uitgevoerd. Dit wordt beschouwd als een continu proces.

Naar aanleiding van het advies van het Forum Standaardisatie zijn regeling en bijlage 2 aangepast: het

[21] Gebaseerd op de handreiking van het Forum Standaardisatie: *Een handreiking voor overheidsorganisaties*, Betrouwbaarheidsniveaus voor digitale dienstverlening, Versie 4. Forum Standaardisatie, April 2017.
[22] Brief van 23 september 2022, Kamerstukken II 2022–2023, 35 868 nr 16.

bepaalde inzake machtigen (artikel 5) is aangescherpt en verduidelijkt en de wegingsfactor 'uitsluiting' is in bijlage 2 toegevoegd. De toelichting is op meerdere punten aangevuld en verduidelijkt, onder meer op het punt van risico verlagende factoren en ongewenste stapeling.
Ook wordt in hoofdstuk 5 van de toelichting aangegeven hoe de dienstverleners ruimte wordt gegeven om zich op de uitvoering voor te bereiden. Het advies om afspraken te maken over het beheer van de regeling en het bieden van centrale implementatie-ondersteuning (bijvoorbeeld het faciliteren van regelhulpen) zal worden opgevolgd.

Naar aanleiding van het advies van het Adviescollege Toetsing Regeldruk is een aantal verduidelijkingen aangebracht. Onder meer is de toelichting aangevuld op het punt van de 2-jaarstermijn in artikel 6. Ook is het vierde lid van artikel 2 gewijzigd, waardoor wordt voorkomen dat dienstverleners authenticatie vereisen waar dat, gelet op de aard van de dienst, in het geheel niet nodig is. Ook de Unie van Waterschappen en het Kadaster hebben hier om verzocht.
Inzake het advies om de baten en kosten in beeld te brengen teneinde een (kwantitatief) onderbouwde uitspraak te kunnen doen over de regeldrukeffecten, te bepalen op basis van de huidige situatie en wijze van authenticatie en de frequentie waarmee bepaalde diensten worden afgenomen, het volgende. Het afgelopen jaar is door burgers honderden miljoenen keren met DigiD ingelogd. Meest benaderde instanties zijn de Belastingdienst, DUO, UWV, SVB, CBR, gemeenten en de zorg. Het overgrote deel van de succesvolle authenticaties (dit varieert tussen 2/3 en 4/5) wordt gedaan met DigiD laag, de rest vindt plaats middels niveau substantieel/laag met 2-factor authenticatie. Op basis hiervan is de verwachting dat in de toekomst voor het overgrote deel (60%) zal (moeten) worden ingelogd met een middel op niveau substantieel en voor een deel (20%: het zal vooral gaan om dienstverleners in de zorg) met een middel op niveau hoog. Rond de 20% zal naar verwachting op niveau laag kunnen blijven. Aan bedrijven zijn de afgelopen jaren enkele honderdduizenden (eHerkenningsmiddelen uitgegeven, waarvan het overgrote deel op niveau 2+ (laag) en 3 (substantieel). De verwachting is dat bedrijven in de toekomst primair zullen (moeten) inloggen met een middel op niveau substantieel. Aan een *upgrade* van eHerkenning zijn voor het desbetreffende bedrijf kosten verbonden. Bedacht moet worden dat de onderhavige regeling onlosmakelijk samenhangt met de bovenliggende wet en de daarin gemaakte keuzes. In (hoofdstuk 9 van) de memorie van toelichting bij de WDO wordt ingegaan op de (regeldruk)gevolgen (baten en lasten) voor burgers en bedrijven. Tevens zij verwezen naar hetgeen hiervoor in hoofdstuk 5 van de toelichting is opgemerkt over uitvoering(sgevolgen).
Op verzoek van een aantal zorginstanties is steviger verankerd dat gezondheidsgegevens op hoog ingeschaald moeten worden. Op verzoek van het UWV en RVO is 'grootschalige verwerking' nader toegelicht. Naar aanleiding van de input van de Kamer van Koophandel, het Kadaster en de RDW is het bepaalde omtrent basisregistraties nader toegelicht. Op verzoek van Justis is het in de toelichting gestelde omtrent strafrechtelijk gegevens verduidelijkt.

Voorts hebben enkele organisaties gevraagd naar de status en mate van bindendheid van de regeling. Hierop wordt, in aansluiting op hoofdstuk 1 en hoofdstuk 2.1-2.2 van deze toelichting, opgemerkt dat de beveiliging van elektronische diensten van publieke dienstverleners op orde moet zijn. Onderdeel daarvan is het vaststellen van het juiste betrouwbaarheidsniveau van de identificatie en authenticatie bij de toegang tot die diensten. Met deze regeling wordt beoogd dienstverleners beter te ondersteunen bij het bepalen daarvan en daartoe het vaststellen van het betrouwbaarheidsniveau meer te normeren dan op dit moment het geval is. Naar verwachting zal hierdoor een duidelijke vraag naar hogere betrouwbaarheidsniveaus van middelen ontstaan. Deze regeling brengt niet met zich mee dat het Ministerie van BZK op de stoel van de publieke dienstverleners gaat zitten; zij zijn en blijven zelf verantwoordelijk voor het vaststellen van het noodzakelijke betrouwbaarheidsniveau voor hun elektronische diensten, als onderdeel van de beveiliging ervan. Dit levert een spanningsveld op tussen 'willen normeren en harmoniseren' enerzijds en 'eigen verantwoordelijkheid met ruimte voor een eigen afweging' anderzijds. Het werken met deze regeling moet in de praktijk gestalte gaan krijgen; praktijkervaringen zullen worden verzameld en zullen dienen als input voor toekomstige doorontwikkeling van de regeling, waaraan in gezamenlijkheid zal worden gewerkt.

II Artikelsgewijs

Artikel 1

Voor de inhoud en betekenis van de begripsbepalingen wordt verwezen naar de paragrafen 2.3.3 en 2.3.4 van het algemeen deel van de toelichting.

Artikelen 2–4

Het bepalen van het betrouwbaarheidsniveau van een dienst wordt toegelicht in paragraaf 2.3.2 (artikel 2, eerste lid), de paragrafen 2.1 – 2.3.7 (artikel 2, tweede tot en met vierde lid) en de paragrafen

2.4 (artikel 3) en 2.5 (artikel 4) van het algemeen deel van de toelichting. Het is gelet op tekst en strekking van de WDO niet toegestaan dat een dienstverlener het onmogelijk maakt om voor gekwalificeerde diensten in te loggen met een middel op het bijbehorende betrouwbaarheidsniveau. Voorkomen moet worden dat met een enkele inloghandeling via een *portal* toegang wordt gegeven tot verschillende diensten, wanneer dit zou betekenen dat voor alle diensten feitelijk hetzelfde – te hoge – niveau (nl dat van de hoogst ingeschaalde dienst) gaat gelden. Wel is het mogelijk om meerdere betrouwbaarheidsniveaus te hanteren in een portal, en na de toegang tot het portal alleen de diensten te laten zien waartoe gebruiker met dat middel toegang heeft. Tot de diensten met een hoger betrouwbaarheidsniveau heeft hij dan geen toegang; wil hij deze toch afnemen, dan moet hij opnieuw inloggen.

Artikel 5

De waarborgen omtrent de identiteit en wilsuiting die nodig zijn in de situatie dat iemand een elektronische dienst zelf afneemt, zijn ook maatgevend voor de situatie dat er sprake is van een machtiging. Vermeden moet worden dat in het geval van machtiging wezenlijk zwaardere of lichtere waarborgen worden gevraagd en geboden. Zwaardere waarborgen leiden tot ongewenste drempels in het registreren van een machtiging, wat elektronische dienstverlening onnodig belemmert. Lichtere waarborgen kunnen ertoe leiden dat machtigingen het 'afvoerputje' dreigen te worden waar oneigenlijk gebruik van zou kunnen worden gemaakt. Dit kan, los van de gevolgen voor individuele burgers, leiden tot verlies van vertrouwen in elektronische dienstverlening in het algemeen en in machtigingen in het bijzonder. Hoofdregel is daarom dat de betrouwbaarheid van een machtigingsregistratie, ongeacht of deze elektronisch of niet (geheel) elektronisch plaatsvindt, tenminste gelijk is aan het betrouwbaarheidsniveau dat voor de authenticatie van die dienst is vereist. De dienstverlener kan evenwel bepalen dat de betrouwbaarheid van een machtigingsregistratie lager mag zijn dan het betrouwbaarheidsniveau dat voor de authenticatie van de dienst vereist is. Voorwaarde is dat door de dienstverlener zelf risicoverlagende maatregelen worden getroffen (vergelijkbaar met die genoemd in artikel 3, onder a en c), die maken dat de dienst toe kan met het lagere betrouwbaarheidsniveau 'aan de voordeur'. Waar het om gaat is los van de registratie van een machtiging een andere – aanvullende – vorm van controle te laten plaatsvinden, waardoor de dienstverlening via een gemachtigde van een vergelijkbare betrouwbaarheid is als het vereiste niveau voor afname van de dienst. Het geheel dient uiteindelijk met voldoende waarborgen te zijn omkleed.

Deze bevoegdheid geldt zowel bij (machtigen terzake van) dienstverlening aan burgers, als bij (machtigen terzake van) dienstverlening aan bedrijven. Benadrukt wordt dat deze regeling *vrijwillige* machtiging betreft; andere vormen van (wettelijke) vertegenwoordiging, zoals ouderlijk gezag, curatele, bewindvoering en mentorschap worden niet door deze regeling beslagen.

Lid 1

Dit lid expliciteert dat, hoewel een machtiging *als zodanig* niet elektronisch tot stand hoeft te komen (zie lid 3), de *registratie* ervan elektronisch dient te geschieden. De dienstverlener (bestuursorgaan of aangewezen organisatie) moet kunnen vertrouwen op hetgeen de registratie vermeldt. Over de wijze van elektronisch registreren (hoe, waarin) stelt deze regeling, afgezien van het equivalentievereiste (zie leden 4 en 5), geen regels. Sprake is van voorziening-onafhankelijkheid; zo kan bijvoorbeeld de publieke voorziening DigiD Machtigen worden gebruikt, maar ook een eigen registratie. Reden hiervoor is de diversiteit en sectorspecificiteit in diensten; dienstverleners hebben ruimte om de wijze van registratie af te stemmen op aard en kenmerken van hun eigen dienstverlening. Een papieren registratiesysteem is onwenselijk om redenen van efficiency en continuïteit. Registratie kan worden gedaan door de machtiginggever of de gemachtigde.
De intrekking van een machtiging behoeft eveneens elektronische registratie. De intrekking hoeft echter *als zodanig* niet elektronisch te geschieden en kan, om redenen van toegankelijkheid en gebruiksgemak, bijvoorbeeld ook telefonisch. Indien intrekking wel elektronisch geschiedt, hoeft dit niet op hetzelfde betrouwbaarheidsniveau te geschieden.

Lid 2

Machtigen is het namens een ander verrichten van (rechts)handelingen. Hiertoe is (uitdrukkelijke of stilzwijgende) toestemming van de machtiginggever, de belanghebbende bij de dienst, aan de gemachtigde nodig (art. 3:60 ev BW). De dienstverlener moet (de betrouwbaarheid van) deze wilsuiting in relatie tot de betreffende elektronische dienst kunnen bepalen; er moeten voldoende waarborgen terzake zijn. Deze waarborgen kunnen worden ingericht in een elektronisch proces (lid 5) of een niet-elektronisch proces (lid 6). Van belang is dat de omschrijving van de betrokken dienst duidelijk is en de machtiging niet te ruim is dwz zich beperkt tot de betrokken dienst.

Lid 3

Machtiging is vormvrij; een wilsuiting kan op diverse manieren tot stand komen. Dit kan elektronisch, via e-mail of een machtigingsvoorziening zoals DigiD machtigen, of niet-elektronisch. Het is vanuit een oogpunt van toegankelijkheid en inclusiviteit van belang om digitaal minder vaardigen te faciliteren. Dit sluit aan bij de bestaande praktijk, waarin machtiging vaak tot stand komt of wordt ingetrokken via *face-to-face* (bijvoorbeeld balie-) contact, telefonisch of op papier. Zie voorts lid 6.

Lid 4

Dit lid betreft het equivalentievereiste. Dit houdt in dat uitgangspunt is dat het totale dienstverleningsproces altijd min of meer dezelfde waarborgen kent, ongeacht hoe de dienst wordt verleend; direct aan de belanghebbende of (na een afgegeven machtiging) via een gemachtigde.

Lid 5

Indien machtiging langs elektronische weg plaatsvindt en hiertoe ingelogd wordt in een machtigingsvoorziening, brengt het equivalentievereiste met zich dat zowel de machtiginggever als gemachtigde een elektronisch identificatiemiddel gebruiken dat tenminste hetzelfde betrouwbaarheidsniveau heeft als voor de dienst is vereist. Zekerheid omtrent wilsuiting is dan eenvoudig af te leiden; deze is in feite geïncorporeerd in het gebruik van het identificatiemiddel. Wordt een machtiging via e-mail afgegeven, dan is het onderhavige lid naar zijn aard niet van toepassing (bij een mailbericht wordt immers niet ingelogd) en geldt, om redenen van veiligheid en betrouwbaarheid, het zesde lid.
Om een machtiging in te trekken hoeft geen identificatiemiddel gebruikt te worden met tenminste hetzelfde betrouwbaarheidsniveau als voor de dienst is vereist. Om redenen van toegankelijkheid en gebruiksgemak kan intrekken ook op een andere (bijvoorbeeld niet digitale) wijze.

Lid 6

In de praktijk geschiedt machtiging niet altijd (geheel) elektronisch. Vaak wordt in het geval sprake is van gebruikers die minder digivaardig zijn gebruik gemaakt van *face-to-face* machtiging (een 'helpende hand', bijvoorbeeld aan een fysieke balie) en/of papier, waarvan het betrouwbaarheidsniveau onduidelijk is. Indien machtiging niet (geheel) langs elektronische weg heeft plaatsgevonden, is het aan de dienstverlener om te bepalen of deze betrouwbaar genoeg is (m.a.w. de wilsuiting voldoende kenbaar is) om op basis hiervan toegang tot de dienst te verlenen.

Vanuit een oogpunt van inclusiviteit en toegankelijkheid is het wenselijk dat een laagdrempelig en tegelijkertijd voldoende betrouwbaar niet-(geheel) elektronisch machtigingsproces mogelijk is. De formulering van lid 6 biedt de dienstverlener ruimte om met specifieke situaties of omstandigheden rekening te houden, opdat enerzijds zekerheid omtrent wilsuiting (zie lid 2) kan worden verkregen en anderzijds maatwerk mogelijk is. Het is aan de dienstverlener om, gelet op de aard en risico's van zijn dienst, te bepalen of de betrouwbaarheid van de machtiging gewaarborgd is en welke aanvullende procedures bij de toegangsverlening van een gemachtigde of later in het proces hij adequaat acht en hoe hij deze inschaalt. Bij de invulling van deze discretionaire ruimte kunnen de volgende factoren in acht worden genomen, teneinde de betrouwbaarheid van een *niet-digitale* machtiging te kunnen bepalen.

1. *Kanaal of kanalen waarlangs de machtiging wordt afgegeven*
   Het gebruik van kanalen waarlangs identiteitsverificatie en -controle van de wilsuiting/ondertekening kan plaatsvinden is van belang. Van machtigingen die via een papieren proces tot stand komen is het moeilijker om de juiste wilsuiting/ondertekening te verifiëren. Voor een hogere betrouwbaarheid verdient face-to-face verificatie de voorkeur.
2. *Kenbaarheid van de wil van machtiginggever*
   Het is zaak dat de wil van de machtiginggever (belanghebbende) omtrent de machtiging kenbaar is. Voor een hoger betrouwbaarheidsniveau, zullen ook hieraan hogere eisen worden gesteld. Het beste is daarbij als er sprake is van een expliciete wilsuiting die bovendien als wilsuiting voorhanden is, denk aan een ondertekende verklaring of een op video opgenomen verklaring. Voor een lager betrouwbaarheidsniveau zou kunnen worden volstaan met aanvullende zekerheid aan de hand waarvan kan worden aangenomen dat de machtiging overeenkomt met de wil van de machtiginggever. Hierbij kan worden gedacht aan codes die zijn verstrekt aan de machtiginggever en die deze aan de gemachtigde heeft gegeven.
   Bij de wilsuiting moet de belanghebbende op een voldoende betrouwbare wijze zijn geïdentificeerd. Regels die het Europees Telecommunicatie en Standaardisatie Instituut (ETSI, een standaardiseringsorganisatie) medio 2021 heeft geformuleerd in ETSI TS 119 461 (*identity proofing*) zijn hiervoor relevant.
3. *Omstandigheden waaronder machtiginggever zijn wil kenbaar heeft gemaakt*
   De machtiginggever dient zijn wil tot het afgeven van een machtiging zonder dwang of drang te

kunnen uiten. In het geval van een *face-to-face* proces zijn hier de omstandigheden het gunstigst voor. In een videoproces, waarbij machtiginggever en gemachtigde beiden aanwezig zijn, zijn hier al meer twijfels bij denkbaar. Het is een overweging om machtigingen, die op een wijze tot stand komen waarbij er twijfels mogelijk zijn, de registratie van de machtiging schriftelijk te laten bevestigen, met *opt-out* mogelijkheid. Verder is aan te bevelen een termijn aan te geven voordat de machtiging ingaat.

4. *Specificiteit van de machtiging*
   Machtigingen dienen te worden afgegeven met eenduidig bepaalde identificerende gegevens van de gemachtigde en met een eenduidig bepaald bereik ten aanzien van af te nemen diensten en geldigheidstermijn. Wanneer de gemachtigde een machtiging laat registreren op basis van een voorafgaande schriftelijke machtiging (bijvoorbeeld een notariële volmacht) wordt hier een specifieke machtiging voor een of meer elektronische diensten van afgeleid. Ook in dit geval is een schriftelijke bevestiging aan de machtiginggever aan te bevelen.

Lid 7

Mitigerende maatregelen zijn nodig voor die gevallen dat een dienstverlener machtiging toestaat die minder betrouwbaar is geregistreerd voor de desbetreffende dienst vereist. Het gaat daarbij om maatregelen die meer zekerheid geven over de betrouwbaarheid ‘aan de poort’ (dus: omtrent wil en betrokkenheid van machtiginggever en de betrouwbaarheid van de machtiging) en maatregelen verderop in het dienstverleningsproces (dus: aanvullende maatregelen met compenserend effect in relatie tot machtiginggever). Het bepaalde geldt met betrekking tot elektronische en niet-(geheel) elektronische machtigingen en is niet beperkt tot specifieke diensten. Het staat dienstverleners vrij om, gelet op aard en kenmerken van hun eigen dienstverlening, invulling te geven aan het bepaalde en aanvullende maatregelen in het proces van dienstverlening en/of toegangsverlening te treffen. Het bepaalde omvat tevens reeds afgegeven machtigingen, waardoor in feite een overgangsregime voor ‘oude gevallen’ wordt gerealiseerd.

Voorbeelden van aanvullende maatregelen in het dienstverleningsproces zelf:

Controleren van aanvraag aan de hand van andere registraties
In dit geval toetst de dienstverlener de gegevens op de aanvraag aan de hand van andere registraties, bijvoorbeeld controle van de gegevens van een onderneming aan de hand van het Handelsregister of controle op het opgegeven bankrekeningnummer ('is dat van de machtiginggever?').

Contacteren van de machtiginggevervanuit het (digitale) primaire proces
Het primaire proces kent stappen waarin contact met de machtiginggever tot stand komt, zoals vragen om aanvullende gegevens en informeren over een genomen besluit/verleende vergunning.

Uitstellen van het gevraagde besluit/wachttijd inbouwen
Dit geeft de dienstverlener ruimte om aanvullende verificaties uit te voeren, in bijvoorbeeld publieke registers. Bij twijfel verleent de dienstverlener geen toegang tot de dienst; ten onrechte weigeren heeft minder negatieve gevolgen dan ten onrechte toegang verlenen.

Mogelijkheid bieden de dienst terug te draaien
Als blijkt dat een gemachtigde ten onrechte een dienst heeft afgenomen, is het soms mogelijk de dienst terug te draaien in die zin dat de dienstverlener de genomen beslissing en de daaruit resulterende gevolgen ongedaan maakt.

Notificeren van het gebruik van de machtiging aan de machtiginggever
In dit geval ontvangt de machtiginggever een kennisgeving van het gebruik van de machtiging.

Gebruik maken van vertrouwde tussenpersonen
De dienstverlener accepteert in dit geval alleen aanvragen en verzoeken die afkomstig zijn van een vertrouwde partij. Daarbij kan het bijvoorbeeld gaan om een notaris die zelf de identiteit van de aanvrager/verzoeker controleert.

Vastleggen van het gebruik van de machtiging
De dienstverlener legt vast welke persoon gebruik heeft gemaakt van een machtiging. Dit maakt het mogelijk bij oneigenlijk gebruik van de machtiging achteraf verhaal te halen bij de gemachtigde.

NB
Bij ondernemingen geldt dat soms de doelgroep zo beperkt is, dat dienstverleners de leden ervan kennen, bijvoorbeeld bij de aanvraag voor subsidie voor vissersschepen. In sectoren waarin sprake is van inhoudelijk complexe regelingen is soms sprake van een beperkt aantal intermediairs die namens ondernemingen in die sectoren optreden. Dat maakt het mogelijk deze intermediairs te vertrouwen op basis van een zogenoemde zelfverklaring.

Voorbeelden van aanvullende maatregelen in het proces van toegangsverlening:

Persoonlijk contact
In persoonlijk contact met de machtiginggever kan de dienstverlener expliciet vaststellen of de gemachtigde daadwerkelijk namens de belanghebbende mag handelen. Een voorbeeld hiervan is het 'keukentafelgesprek'. Daarbij is wel de vraag hoe deze aanvullende check wordt vastgelegd en of daar inzage en herstel op mogelijk is. Het is van belang om hier prudent mee om te gaan zodat schaduwlijsten worden voorkomen.

Beperken van de acceptatie van machtigingen
Dit houdt in dat de dienstverlener alleen machtigingen accepteert die bijvoorbeeld niet langer geleden dan een vooraf bepaalde termijn zijn uitgegeven, dan wel juist voor een bepaalde datum zijn aangegaan.

De keuze om een of meer van de aanvullende maatregelen toe te passen is aan de dienstverlener. Die maakt zijn keuze op basis van een (verkorte) risicoanalyse van de elektronische dienst(en). Daarbij geldt dat de grootste risico's zich zullen voordoen in situaties waarin sprake is van grote aantallen gebruikers van de dienst en/of een groot financieel belang en/of risico's op het terrein van privacy en gegevensbescherming. Aandachtspunt bij deze maatregelen is verder dat de beschreven maatregelen invloed hebben op de balans tussen enerzijds het gemak van het gebruik van machtigingen en anderzijds de veiligheid daarvan. Bij de beantwoording van de vraag of de dienstverlener de mogelijkheid wil bieden om een lager betrouwbaarheid van de machtigingsregistratie te accepteren in combinatie met aanvullende maatregelen zijn de volgende criteria van belang:

- de aard van de verwerkte persoonsgegevens en de gevolgen voor de privacy van betrokkene;
- de omvang van de (rechts)gevolgen van het gebruik van de dienst;
- de vraag of de dienst gegevens uit basisregistraties wijzigt;
- economisch belang van de machtiginggever;
- publiek belang en imagorisico van de dienstverlener.

Artikel 6

Verwezen wordt naar paragraaf 3.1 van het algemeen deel van de toelichting.

Artikel 7

Verwezen wordt naar hoofdstuk 5 van het algemeen deel van de toelichting.

Artikel 9

Deze regeling is noodzakelijk voor het door dienstverleners kunnen toepassen van artikel 6, tweede tot en met vierde lid, van de wet. De regeling treedt daarom in werking wanneer artikel 6, tweede tot en met vierde lid, van de Wet digitale overheid in werking treedt, te weten op 1 juli 2023.

Zie tevens hoofdstuk 5 van het algemeen deel van de toelichting.

De Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties Digitalisering en Koninkrijksrelaties
A.C. van Huffelen