Regeling betrouwbaarheidsniveaus authenticatie elektronische dienstverlening

Regeling van de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties van … , nr. , 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;
- *persoonsgegevens en verwerking van persoonsgegevens*: hetgeen daaronder wordt verstaan in artikel 4 van de Algemene verordening gegevensbescherming;
- *bijzondere categorieën van persoonsgegevens*: persoonsgegevens als bedoeld in de begripsbepaling voor "bijzondere categorieën van persoonsgegevens" in artikel 1 van de Uitvoeringswet 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 vierde lid.
2. Een bestuursorgaan of aangewezen organisatie bepaalt dat voor een elektronische dienst authenticatie op betrouwbaarheidsniveau hoog vereist is indien één 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 één 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. Indien geen van de in kolom hoog of substantieel genoemde criteria op de dienst van toepassing is, bepaalt een bestuursorgaan of aangewezen organisatie dat voor de desbetreffende dienst betrouwbaarheidsniveau laag toereikend is.

Artikel 3 Risico verlagende factoren

Onverminderd de toepasselijkheid van wettelijke voorschriften kan, in afwijking van artikel 2, tweede en derde lid, een bestuursorgaan of aangewezen organisatie voor een elektronische dienst authenticatie op een naastlager betrouwbaarheidsniveau 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. bij het inloggen slechts informatie aan het bestuursorgaan of de aangewezen organisatie ter

beschikking wordt gesteld, of
c. het bestuursorgaan of de aangewezen organisatie later in het proces herstelmaatregelen neemt.

Artikel 4 Risico verhogende factoren

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

Artikel 5 Bepalen betrouwbaarheidsniveau voor het registreren van een machtiging

1. Een bestuursorgaan of aangewezen instantie die een dienst verleent bepaalt het betrouwbaarheidsniveau dat voor het registreren van een machtiging voor die dienst ten minste vereist is.
2. Het bestuursorgaan of de instantie kan voor diensten aan burgers bij toepassing van het eerste lid bepalen dat voor het registreren van een machtiging authenticatie op een lager betrouwbaarheidsniveau dan voor de dienst waarop de machtiging ziet, toereikend is.

Artikel 6 Tijdelijk toestaan van naastlager niveau

Onverminderd de toepasselijkheid van wettelijke voorschriften kan een bestuursorgaan of aangewezen organisatie besluiten 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 niveau laag toe te staan.

Artikel 7 Kenbaarheid betrouwbaarheidsniveau

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

Artikel 8 Citeertitel

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

Artikel 9 Inwerkingtreding

Deze regeling treedt in werking op het tijdstip waarop artikel 6 van de Wet digitale overheid in werking treedt.

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

De staatsecretaris van Binnenlandse Zaken en Koninkrijksrelaties,

drs. R.W. Knops

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, eerste 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 Risico's indien de gegevens in verkeerde handen vallen	• Geen bijzondere categorieën van persoonsgegevens • Geen persoonsgegevens van strafrechtelijke aard • Kleinschalige verwerking • Geen of nauwelijks risico op identiteits-fraude en/of misbruik van de betreffende dienst	• 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 • Reëel risico op identiteitsfraude en/of misbruik van de betreffende dienst	• Persoonsgegevens die: *stigmatiserend kunnen werken; *reputatieschade kunnen opleveren; *schade kunnen opleveren aan de gezondheid, of *chanteerbaarheid kunnen opleveren • Gegevens die onder het medisch beroepsgeheim vallen
---	---	---	---
Bedrijfsgegevens	• Algemene bedrijfsgegevens	• Gevoelige bedrijfsgegevens	• Geen criteria/nvt
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 dienst-verlening verstrekt.	• Geen criteria/nvt
Gevolgen voor de gegevens in de basisregistraties	• Geen criteria/nvt	• Controle ingeregeld op de verwerking van gegevens	• Geen controle ingeregeld op de verwerking van gegevens

Economisch belang	• Niet of nauwelijks ingrijpend voor economische positie burgers/bedrijven in de doelgroep • De directe schade voor burgers is lager dan €1000,- • 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/bedrijven in de doelgroep • De directe schade voor burgers is hoger dan €1000,- • 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/bedrijven 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 toegangscontrole tot deze dienstverlening. Hoe risicovoller de dienstverlening is, bijvoorbeeld als veel privacygevoelige gegevens worden verwerkt of het financieel belang groot is, hoe hoger de veiligheid van de dienst moet zijn, waaronder de toegangscontrole tot de dienstverlening. Deze toegangscontrole 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 vaststelling van de mate van toegangscontrole en de keuze voor het toegangsmiddel daarin 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 daarvoor 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 is 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, die op Europees niveau regels stelt aan de veiligheid van inlogmiddelen. Bestuursorganen en aangewezen organisaties moeten op grond van het tweede lid van artikel 6 van de wet bepalen welk betrouwbaarheidsniveau op een door hen aangeboden dienst van toepassing is, met het oog op authenticatie (identificatie/inloggen) terzake. 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 tot 2 jaar na inwerkingtreding 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 authenticatiemiddelen is de hierboven al genoemde eIDAS-verordening. Deze verordening regelt wanneer authenticatie/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 verordening). 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 uitvoeringsverordening 2015/1502 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 betrouwbaarheids-niveaus 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[1] 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.[2]

Benadrukt wordt, dat deze regeling een in de bijlage opgenomen afwegingskader bevat; de factoren, 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 versnelde risico-analyse op veiligheid van de dienstverlening. De regeling bevat – bewust - geen afvink-lijst of *one-size-fits-all* benadering, maar richtsnoeren waarmee de desbetreffende organisatie aan de slag kan om de eigen diensten te classificeren.[3] 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 bijvoorbeeld nodig, omdat in de praktijk 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

[1] 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.
[2] Privacycare – PBLQ, Onderzoek betrouwbaarheidsniveau patiëntenauthenticatie bij elektronische gegevensuitwisseling in de zorg, mei 2016. Meegezonden als bijlage bij Tweede Kamerbrief over Impuls eID, Kamerstuk 26 643, nr. 419.
[3] Zie mbt de vertaalslag door gemeenten: https://www.digitaleoverheid.nl/nieuws/instrument-helpt-gemeenten-om-betrouwbaarheidsniveau-van-digitale-diensten-te-bepalen/

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 organisatie specifieke vraagbaak of ander hulpmiddel te hanteren, waarmee nadere toelichting en praktische ondersteuning (bijvoorbeeld in de vorm van voorbeelden) worden gegeven.

2.2 Belang van vaststelling van het betrouwbaarheidsniveau voor elektronische diensten met een vergelijkbaar risicoprofiel

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 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 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 in het indienen van een klacht of Wob-verzoek, het uitbrengen van een ingebrekestelling, het doorgeven van een adreswijziging, (technisch) 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 beoordelen factoren 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. 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 betrouwbaarheids-niveau 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 informatievoorziening waarbij de vaststelling van de identiteit van een burger of bedrijf (onderneming of rechtspersoon) niet van belang is, zelfs niet op niveau laag. Voor deze diensten is het bepalen van een betrouwbaarheidsniveau voor authenticatie uiteraard niet nodig.

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 betrouwbaarheids-niveau 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.

<u>Minimale specifieke wettelijke eisen</u>
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.

<u>Vaste specifieke wettelijke eisen</u>
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 derhalve 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.[4] 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 als ze in verkeerde handen vallen.

De vorm, digitaal of op papier, is niet relevant: beide vormen zijn van toepassing. Bij het verlenen van de 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

[4] Artikel 4, eerste lid, AVG.

wissen of vernietigen van gegevens"[5]). Verwerking kan meer of minder grootschalig en/of gestapeld geschieden. In dit verband vormt de hoeveelheid te verwerken gegevens per individu een indicatie, alsmede het aantal betrokkenen, de duur van de gegevensverwerking en de geografische reikwijdte van de verwerking.[6]

De dienstaanbieder 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 dienstaanbieders 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 – per ongeluk aan de verkeerde persoon wordt verstrekt.

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 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.

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.

Ook gegevens over gezondheid[7] 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 werken;
- reputatieschade opleveren;
- schade opleveren aan de gezondheid, of
- tot chanteerbaarheid kunnen leiden.

[5] Artikel 4, tweede lid, AVG.
[6] 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
[7] 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.

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

De verwerking van persoonsgegevens van strafrechtelijke aard valt onder niveau substantieel. In 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, alsmede persoonsgegevens betreffende een door de rechter opgelegd verbod naar aanleiding van onrechtmatig of hinderlijk gedrag. De persoonsgegevens inzake een door de rechter opgelegd verbod naar aanleiding van onrechtmatig of hinderlijk gedrag waren in de Wet bescherming persoonsgegevens op één lijn gesteld met de andere persoonsgegevens van strafrechtelijke aard en die lijn is voortgezet in de UAVG (de AVG biedt die ruimte).[8] 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[9] en het transactiebedrag, of geaggregeerde basisgegevens over betalingen.[10] Ook deze gevoelige gegevens niet zijnde bijzondere categorieën van persoonsgegevens of persoonsgegevens van strafrechtelijke aard zijn opgenomen onder niveau substantieel.

Persoonsgegevens - Betrouwbaarheidsniveau Hoog
In deze categorie gaat het om persoonsgegevens of 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 en/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 vallen hieronder, alsmede gegevens over werkprestaties of relatieproblemen.

Om te bepalen of iets stigmatiserend kan zijn of reputatieschade oplevert, kan als maatstaf worden gebruikt dat deze categorie is voorbehouden aan de gevallen waarin het afbreukrisico zo groot is voor de betrokkene(n) dat deelname aan de maatschappij bijna onmogelijk is. 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.[11] De overwegingen bij de AVG zeggen daarover dat het gaat om gegevens die informatie geven over de lichamelijke of geestelijke 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

[8] TK 2017/18, 34 851, nr. 3, blz. 89-90.
[9] De BIC code staat voor: Bank Identificatie Code en wordt gebruikt om een bank te kunnen identificeren.
[10] 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.
[11] Zie artikel 4, vijftiende lid, AVG.

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.[12] Gezondheidsgegevens vallen onder betrouwbaarheidsniveau hoog als deze gegevens in verkeerde handen vallen en daardoor:

- stigmatiserend kunnen werken;
- reputatieschade kunnen opleveren;
- 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.[13] 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 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.[14] Verwerking hiervan rechtvaardigt betrouwbaarheidsniveau substantieel.

---

[12] Overweging 35 bij de AVG.

[13] Privacycare – PBLQ, Onderzoek betrouwbaarheidsniveau patiëntenauthenticatie bij elektronische gegevensuitwisseling in de zorg, mei 2016, p. 40.

[14] 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.

2.3.5 Burgerservicenummer

Het burgerservicenummer is 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. Onder gebruiker wordt ook een eventuele gemachtigde verstaan. Diensten waarbij het BSN van derden (bijv. werknemers) wordt verwerkt zijn eveneens in de tabel meegenomen.

Burgerservicenummer – niveau laag
In de categorie laag wordt het burgerservicenummer bij de dienstverlening uitsluitend opgegeven door de gebruiker van de dienst, maar wordt het niet door de dienstaanbieder 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 dienst op betrouwbaarheidsniveau laag is een digitaal formulier van de dienstverlener waarbij het BSN door de gebruiker moeten worden opgegeven.

Burgerservicenummer – niveau substantieel
Bij niveau substantieel wordt het burgerservicenummer 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 voor ingevuld formulier welke de gebruiker van de dienstverlener ontvangt waarop zijn of haar burgerservicenummer reeds is ingevuld.

Burgerservicenummer- niveau hoog
Er zijn geen specifieke criteria met betrekking tot de verwerking van het burgerservicenummer 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 persoonsgegevens, zoals NAW-gegevens en een rekeningnummer, leiden tot bijvoorbeeld reputatieschade of chanteerbaarheid en is een hoog betrouwbaarheidsniveau gerechtvaardigd.

2.3.6 Basisregistraties

De impact van het wijzigen van een gegeven in een basisregistratie[15] kan groot zijn, aangezien de gegevens aan een grote groep afnemers worden verstrekt. Elke opname of wijziging van een gegeven in een registratie moet met de grootste zekerheid en zorgvuldigheid gebeuren, juist omdat afnemers op deze gegevens moeten kunnen vertrouwen. Deze gegevens zullen in veel gevallen ook bepalend zijn voor veel rechten en verplichtingen van burgers en bedrijven. Daarom is het afhankelijk van de bij de betreffende basisregistratie behorende en gehanteerde procedure of betrouwbaarheidsniveau substantieel of hoog van toepassing is. Deze procedure hangt samen met de aard van de dienst.

Basisregistraties – niveau laag
Er vindt in het kader van de dienstverlening geen verwerking plaats op niveau laag in basisregistraties.

Basisregistraties – niveau substantieel
Niveau substantieel is voldoende indien er op een melding of verzoek, dat tot wijziging van een basisregistratie zou moeten leiden, een controle plaatsvindt (bijvoorbeeld via het zgn '4-ogen principe') op de gegevens die gewijzigd of opgegeven worden.

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

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 controle plaatsvindt op de verwerking van de gegevens.

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. Het gaat om een 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. Bijvoorbeeld: als er meerdere voertuigen met een inlogmiddel op naam worden gezet dan beperkt de schade zich tot die voertuigen die onjuist op dezelfde naam zijn gezet. De vervolgschade van het verkeerd op naam stellen behoort dan niet tot de mee te rekenen schade.

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 €1000,-
- 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 betrouwbaarheids-niveau substantieel te worden gehanteerd. Richtsnoer is dat de directe schade per geval:

- Voor burgers hoger is dan €1000,-
- 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 maar gemiddelden zijn en richting geven. 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 dienstaanbieders 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. De onderhavige regeling bevat daarom 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 (dus: in het vervolgproces) nemen van extra processtappen of mitigerende maatregelen waardoor het risico verminderd wordt.

Zo kan een dienstverlener in plaats van niveau hoog substantieel en in plaats van substantieel laag (dus: het naastlagere niveau) 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 “brengen” van gegevens. Dit is bijvoorbeeld het geval bij de aanlevering van gegevens bij belastingaangifte. Met de aanlevering van de gegevens ontstaat nog niet het gevolg (belastingbetaling) 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 in het voorbeeld gekozen voor vooringevulde 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 verkeerder persoon gebeurt. Overigens zal bij het ter beschikking stellen van privacygevoelige informatie, zoals bijzondere persoonsgegevens, een naastlager niveau niet snel in de rede liggen. Tot slot 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..

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. Omstandigheden waaraan gedacht moet worden, betreffen primair risico's voor 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.
Het uitvoeren van een volledige risicoanalyse behelst een zorgvuldig proces. Hiertoe kan de Baseline Informatiebeveiliging Overheid geraadpleegd worden.[16]

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 zou dan feitelijk een dode letter in de regeling 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 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 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 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.

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 dienstaanbieder 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; hierbij moet ingevolge artikel 6, vierde lid, van de wet dan wel sprake

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

zijn van ten minste twee authenticatiefactoren). Het is de verwachting dat twee jaar na inwerkingtreding van deze regeling sprake zal zijn van voldoende beschikbaarheid en dekkingsgraad van (publieke en private) inlogmiddelen. Mocht dit (veel) eerder het geval zijn, dan zal worden bezien of het opportuun is om de tijdelijke uitzonderingsmogelijkheid te schrappen. Mocht dit onverhoopt later zijn, dan zal worden bezien of het opportuun is om de termijn te verlengen.
Indien een dienstaanbieder 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 dienstaanbieder de betreffende informatie op zijn website actueel houdt.

Vanzelfsprekend ontslaat het gebruik van de tijdelijke afwijkingsbevoegdheid dienstaanbieders er niet van om hun (informatie)beveiliging op orde te hebben.[17] Zij blijven zelfstandig verantwoordelijk voor de beveiliging van hun dienstverlening.

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 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. Dit 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. 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. Dit laat onverlet, dat de dienstverlener er – conform artikel 6 van de onderhavige regeling – voor kan kiezen tijdelijk toe te staan dat een inlogmiddel van een naastlager betrouwbaarheidsniveau wordt gehanteerd (zie 3.1).

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 aard van de verwerking daarvan een

[17] Dit betreft toepassing van de BIO (zie voetnoot 16).
[18] Artikel 5, eerste lid, onderdeel f, van de AVG.

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 dienstaanbieders 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 dienstaanbieders en is deze gericht op zoveel mogelijk uniformiteit bij de classificering van diensten met een vergelijkbaar risicoprofiel. Hoewel de regeling zekere ruimte voor dienstaanbieders biedt, zal deze naar verwachting niet leiden tot grote verschillen tussen dienstaanbieders. Classificering door de dienstaanbieder 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 dienstaanbieder op zijn website - dus: voorafgaand aan het moment van authenticatie van een persoon of registratie van een machtiging voor een elektronische dienst - op toegankelijke wijze inzichtelijk te maken voor welke dienst welk middel tenminste 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: dienstaanbieders 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, hiermee zijn extra kosten, tijd en inspanningen (oa activeringshandelingen, mogelijk specifieke apparatuur) 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.

[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).

Voor dienstaanbieders 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 geringe aanpassing van hun dienstverlening verwacht. Voor hen zullen de extra kosten die aan de invoering van deze regeling verbonden zijn, minimaal uitvallen. Hoe dan ook zullen zij een check op conformiteit met de onderhavige regeling moeten uitvoeren (validatie classificatie); de uitkomsten kunnen tot aangepaste werkprocessen leiden. Voor dienstaanbieders 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 dienstaanbieder 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 worden beschouwd.

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,[22] verloopt het toezicht op de naleving van deze regeling in het publieke domein door decentrale overheden via de reguliere (interbestuurlijke) lijnen (interbestuurlijk toezicht uit de Provincie- en Gemeentewet). Het interbestuurlijk toezicht biedt de naast hoger gelegen bestuurslaag (uitsluitend) de mogelijkheden tot repressief ingrijpen, te weten schorsing en vernietiging bij handelen in strijd met het recht of het algemeen belang (door de Kroon) en in uiterste gevallen indeplaatsstelling (bij taakverwaarlozing).

Voor de naleving door bestuursorganen op het niveau van de Rijksoverheid (ministeries en zelfstandige bestuursorganen) en door de aangewezen organisaties (zie artikel 17, eerste lid) wijst de minister, op wiens beleidsterrein het betreffende (zelfstandige) bestuursorgaan of aangewezen organisatie werkzaam is, 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 de naleving van deze regeling door bestuursorganen op het niveau van de provincies wijst de Minister van BZK ambtenaren aan (artikel 17, tweede lid, van de wet). Het toezicht dat zij houden is in lijn met het reguliere interbestuurlijke toezicht dat de minister houdt op provincies en bestuursorganen op het niveau van provincies (gemeenschappelijke regelingen waaraan provincies deelnemen).

Op de naleving van de deze regeling door gemeenten en waterschappen alsmede de bestuursorganen op het niveau van gemeenten en waterschappen, zoals gemeenschappelijke regelingen, wordt in lijn met het reguliere interbestuurlijke toezicht gehouden door de provincies. Het provinciebestuur

[21] Gebaseerd op de handreiking van het Forum Standaardisatie: *Een handreiking voor overheidsorganisaties,* Betrouwbaarheidsniveaus voor digitale dienstverlening, Versie 4. Forum Standaardisatie, April 2017.
[22] Kamerstukken II, 2019/20, 34 972, nr. 3.

informeert de minister over de (mate van) naleving zodat de minister zijn rol als stelselverantwoordelijke kan vervullen (artikel 17, derde lid, van de wet).

7. Advies en consultatie

PM verwerken uitkomsten AP, ATR, (internet)consultatie incl. U&H toets (indicatie kosten)

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. Overigens ligt het in de rede dat een dienstaanbieder het niet 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

Het is aan de dienstverlener om te bepalen op welk betrouwbaarheidsniveau een gebruiker zich moet identificeren om toegang te krijgen tot een elektronische dienst. Dit geldt ook voor de toegang voor gemachtigden. Met andere woorden: de dienstverlener bepaalt in beginsel ook het betrouwbaarheidsniveau van een machtiging. Het lijkt logisch dat dienstverleners de betrouwbaarheidsniveaus dan zullen koppelen. Dit is echter niet altijd het geval. Reden is dat hoogbetrouwbare machtiging een relatief complex registratieproces meebrengt. Dit doet afbreuk aan het gebruiksgemak voor degene die een elektronische dienst wil afnemen. Deze ervaart dan een hoge drempel om te machtigen. Dit leidt er in de praktijk toe dat een belangrijke, veelal kwetsbare, doelgroep het machtigingsproces niet kiest maar zijn identificatiemiddel ‘uitleent’. Hierdoor wordt feitelijk afbreuk gedaan aan de betrouwbaarheid en nemen de risico’s juist toe.

Om deze paradox te voorkomen is er, om redenen van inclusie, toegankelijkheid en laagdrempeligheid, voor gekozen om dienstverleners de ruimte te geven om, afhankelijk van de aard van hun dienstverlening en de beoogde gebruikers, de betrouwbaarheidsniveaus te koppelen of de totstandkoming van de machtiging op een lager niveau te laten plaatsvinden. Op basis van een risicoafweging kan de dienstverlener na het moment van machtiging nog een andere technische of fysieke vorm van controle laten plaatsvinden, waardoor de identiteitsvaststelling bij het registeren van

de machtigingsrelatie met inbegrip van deze controle op een vergelijkbaar betrouwbaarheidsniveau plaatsvindt als het vereiste niveau voor afname van de dienst. De identiteitsvaststelling dient uiteindelijk met voldoende waarborgen te zijn omkleed, gegeven het betrouwbaarheidsniveau waarop de dienstverlening moet plaatsvinden.

Bovengeschetste bevoegdheid geldt alleen bij (machtigen terzake van) dienstverlening aan burgers. Bij gebruik van een bedrijfsmiddel is inherent sprake van een machtigingsrelatie; een bedrijf machtigt immers per definitie iemand om hem te vertegenwoordigen. Het ligt dan niet in de rede om de betrouwbaarheidsniveaus van dienst en machtiging te ontkoppelen.

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 dienstaanbieders kunnen toepassen van artikel 6 van de wet. Beide moeten derhalve gelijktijdig in werking treden.

De staatsecretaris van Binnenlandse Zaken en Koninkrijksrelaties,

drs. R.W. Knops