Uitvoeringswet in verband met de uitvoering van EU-verordening elektronische identiteiten en vertrouwensdiensten

MEMORIE VAN TOELICHTING

Inhoudsopgave

1. Inleiding

Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG (PbEU 2014, L 257) (hierna verder genoemd: de verordening of de eidas-verordening) is een van de initiatieven ter uitvoering van de Digitale agenda voor Europa van de Europese Commissie voor de jaren 2010 tot en met 2015. Doel van de verordening is het vertrouwen in elektronische transacties te vergroten door te voorzien in een gemeenschappelijke grondslag voor veilige elektronische interactie tussen burgers, bedrijven en overheden, en bijgevolg ook de doeltreffendheid van publieke en private onlinediensten en elektronische handel in de interne markt van de Europese Unie te verhogen. De verordening regelt daartoe het grensoverschrijdend gebruik van elektronische identificatiemiddelen en vertrouwensdiensten tussen de lidstaten van de Europese Unie. De verordening is in september 2014 in werking getreden. Vanaf 1 juli 2016 is het onderdeel vertrouwensdiensten inclusief het toezicht daarop van toepassing en vanaf 18 september 2018 de verplichte erkenning van elektronische identificatiemiddelen uit andere lidstaten. De richtlijn 1999/93/EG van het Europees Parlement en de Raad van 13 december 1999 betreffende een gemeenschappelijk kader voor elektronische handtekeningen (PbEG 2000, L 13) (hierna: de richtlijn of de Richtlijn elektronische handtekeningen) is met ingang van 1 juli 2016 ingetrokken. Voor uitvoering van de verordening is ook wijziging van wetgeving noodzakelijk. Aan het einde van de artikelsgewijze toelichting is een omzettingstabel van de verordening opgenomen. Deze memorie van toelichting wordt uitgebracht mede namens de Minister van Veiligheid en Justitie en de Minister van Binnenlandse Zaken en Koninkrijksrelaties.

2. De eidas-verordening en gewaarborgd vertrouwen bij digitaal verkeer

2.1 Elektronische identificatie en elektronische identificatiemiddelen

Dienstverlening is vaak persoonlijk. Een dienstaanbieder wil dan ook weten wie de dienst wil afnemen. In de fysieke wereld worden hier identiteitsbewijzen, zoals het paspoort, de identiteitskaart of het rijbewijs voor gebruikt. Die bevatten identificerende gegevens van een persoon zoals een voornaam, achternaam, geboortedatum, geboorteplaats, foto en mogelijk een uniek identificerend nummer, zoals in Nederland het Burgerservicenummer (BSN). Het document bevat eveneens echtheidskenmerken zoals een speciaal bewerkte foto, een zegel of hologram. Daardoor weet iemand die het identiteitsdocument controleert met wie hij te maken heeft, dat het om een echt document gaat en daardoor dat de gegevens op het document authentiek zijn.

Elektronische identificatie is digitaal en verloopt anders. Preciezer gesteld is elektronische identificatie een proces waarbij persoonsidentificatiegegevens in elektronische vorm worden gebruikt. Met die gegevens wordt een persoon uniek aangeduid. (artikel 3, onderdeel 1, van de verordening). Unieke aanduiding maakt onderscheid tussen personen mogelijk. Het voorkomt dat de ene persoon wordt verward of verwisseld met een andere. In de verordening gaat het hierbij niet enkel om elektronische identificatie van natuurlijke personen, maar ook om rechtspersonen die zijn opgericht naar of worden beheerst door het recht van een lidstaat. Elektronische identificatie in de zin van de verordening kan voorts ook betrekking hebben op natuurlijke personen die bevoegd voor deze rechtspersonen handelen, zoals op basis van wettelijke vertegenwoordiging of een volmacht. Geen elektronische identificatie die in de verordening is geregeld, is bijvoorbeeld identificatie van een natuurlijke persoon die een andere natuurlijke persoon vertegenwoordigt of identificatie van apparaten, systemen of computerprogrammatuur.

Bij elektronische identificatie kan gebruik worden gemaakt van elektronische identificatiemiddelen (artikel 3, onderdeel 2, van de verordening). De persoonsidentificatiegegevens zijn dan bijvoorbeeld opgeslagen in een chip die is geïntegreerd in een pasje of zijn aanwezig in een beveiligde omgeving binnen een informatiesysteem. De controle over het gebruik van persoonsidentificatiegegevens berust bij de persoon van wie de identiteit is. Het gebruik kan met kennis die geheim blijft voor anderen, bijvoorbeeld een zelfgekozen wachtwoord of pincode. Het kan ook met een middel in combinatie met (wisselende) gegevens, bijvoorbeeld voortkomend uit een nummercalculator, token of mobiele telefoon. Tenslotte kan het gebruik van de persoonsidentificatiegegevens fysiek gebonden zijn, aan biometrische kenmerken, zoals een vingerafdruk, stemherkenning of irisscan. Een combinatie van methoden leidt tot meer veiligheid en minder kans op identiteitsfraude. Bijvoorbeeld het invullen van een gebruikersnaam, wachtwoord op een website, waarna vervolgens een verificatiecode afkomstig van een nummercalculator op een telefoon moet worden ingevoerd. Dit wordt meerfactorauthenticatie genoemd. De kans dat een derde over beide geheime en persoonsgebonden factoren beschikt is kleiner dan bij gebruik van een enkelvoudige methode. Voorwaarde daarvoor is het zorgvuldig gebruik en bewaren van geheime gegevens en bijbehorende middelen.

De functie van het gebruik van elektronische identificatiemiddelen is dat een persoon elektronisch duidelijk kan maken aan een ander wie hij is en dat hij het echt is. Het is gericht op het creëren van gewaarborgd vertrouwen bij een ander. Dit gebeurt doordat het gebruik van een elektronisch identificatiemiddel via een elektronisch proces leidt tot een bevestiging van de echtheid van een aan een ander opgegeven of kenbaar gemaakte identiteit. Die elektronische bevestiging van echtheid die de vertrouwende partij ontvangt, is in veel situaties afkomstig van een derde partij die de identiteit op echtheid heeft gecontroleerd en vastgelegd. Het proces dat bevestiging mogelijk maakt, heeft een specifieke naam: authenticatie (artikel 3, onderdeel 5, van de verordening).

De betrouwbaarheid van elektronische identificatiemiddelen kan verschillend zijn. Dit hangt af van de betrouwbaarheid van de keten die op het elektronisch identificatiemiddel is gericht. Bij deze keten kunnen meerdere partijen betrokken zijn. De betrouwbaarheid van het middel wordt bepaald door onder meer de koppeling tussen persoonsidentificatiegegevens met de persoon, het uitgifteproces van een elektronisch identificatiemiddel, het beheer van het middel, de gebruikte techniek en de inrichting van het authenticatieproces.

Het gebruik van een elektronisch identificatiemiddel kan in de nabijheid van een vertrouwende partij plaatsvinden. Bijvoorbeeld elektronische identificatie in onmiddellijke nabijheid om vervolgens een fysiek product in ontvangst te kunnen nemen. Het creëren van gewaarborgd vertrouwen is echter bij uitstek ook geschikt voor partijen die elektronisch en op afstand met elkaar in contact staan. Voor elektronische identificatiemiddelen als bedoeld in de verordening is het zelfs een voorwaarde dat die worden gebruikt voor authenticatie bij een onlinedienst, en dus elektronisch op afstand.

2.2. Vertrouwensdiensten

Onder vertrouwensdiensten worden samengevat elektronische handtekeningen, elektronische zegels, elektronische tijdstempels, diensten voor aangetekende elektronische bezorging en elektronische certificaten voor authenticatie van websites verstaan. Deze diensten worden gewoonlijk tegen betaling verricht. Er wordt bij vertrouwensdiensten een verbinding met andere gegevens gelegd. Dit wordt associatie genoemd. Met een elektronische handtekening kan bijvoorbeeld een digitale overeenkomst worden ondertekend. Met een elektronisch zegel kan een diploma of uittreksel door een instantie elektronisch gewaarmerkt worden. Een certificaat voor de authenticatie van een website maakt een gebruiker duidelijk of een website echt is en dat hij daadwerkelijk met de bedoelde website communiceert. Vertrouwensdiensten dragen bij aan het vertrouwen in elektronisch verkeer.

De meest bekende vertrouwensdienst is de elektronische handtekening. Een elektronische handtekening bestaat uit gegevens in elektronische vorm die gehecht zijn aan of logisch verbonden zijn met andere gegevens in elektronische vorm en die door de ondertekenaar worden gebruikt om te ondertekenen (artikel 3, onderdeel 10, van de verordening). Ondertekenaar is een natuurlijke persoon die een elektronische handtekening aanmaakt (artikel 3, onderdeel 9, van de verordening). Door ondertekening drukt de ondertekenaar iets uit ten aanzien van de vastgelegde gegevens. Bijvoorbeeld: "ik ben de auteur van dit document" of "ik heb dit document in ontvangst genomen", of "ik ben akkoord met de inhoud van dit document".

Een elektronisch zegel kan worden gebruikt door een rechtspersoon die is opgericht naar of worden beheerst door het recht van een lidstaat. Het zegel betreft gegevens in elektronische vorm die gehecht zijn aan of logisch verbonden zijn met andere gegevens in elektronische vorm en die worden gebruikt om de oorsprong en integriteit daarvan te waarborgen (artikel 3, onderdeel 25, van de verordening). Een rechtspersoon die bijvoorbeeld elektronisch een diploma, een getuigschrift of een uittreksel uit een administratie verstrekt, kan dit van een elektronisch zegel voorzien. Daarmee wordt beoogd te waarborgen dat het elektronisch document van een bepaalde entiteit afkomstig is. De organisatie van een rechtspersoon is verantwoordelijk voor een zorgvuldig en bevoegd gebruik van een elektronisch zegel. Voor de vertrouwende partij is niet herkenbaar wie de natuurlijke persoon is die de rechtspersoon vertegenwoordigt bij het aanmaken van het zegel. Daardoor kan een vertrouwende partij de bevoegdheid tot vertegenwoordiging door de natuurlijke persoon op grond van de wet, statuten of een volmacht niet controleren. Dit is enkel anders indien aanvullende gegevens (attributen) over de identiteit van de natuurlijke persoon onderdeel zijn van het elektronisch zegel. Het voorzien van een elektronisch document van een elektronisch zegel is te onderscheiden van de ondertekening daarvan. Voor de totstandkoming van bijvoorbeeld een elektronische onderhandse akte, zoals een elektronische verzekeringspolis, is op grond van artikel 932, eerste lid, van Boek 7 van het BW ondertekening daarvan met een elektronische handtekening vereist.

Een elektronisch tijdstempel betreft gegevens in elektronische vorm die andere gegevens in elektronische vorm verbinden aan een bepaald tijdstip en die bewijzen dat die laatstgenoemde gegevens op dat tijdstip bestonden (artikel 3, drieëndertigste lid, van de verordening). Dit kan belangrijk zijn bij processen waaraan tijdslimieten zijn verbonden voor het indienen van stukken en aanvragen. Aanbestedingsprocedures, subsidieaanvragen en belastingaangiftes zijn hier voorbeelden van.

Een dienst van aangetekende elektronische bezorging verschaft bewijs over het verzenden van elektronische gegevens en de ontvangst daarvan. Daarbij zijn de verzonden gegevens beschermd tegen het risico van verlies, diefstal, beschadiging en onbevoegde wijziging (artikel 3, onderdeel 36, van de verordening). Net als aangetekende post kan de dienst van aangetekende elektronische bezorging worden gebruikt voor verzending en ontvangst van belangrijke documenten. Bij het verlenen van een dienst voor elektronisch aangetekende bezorging geldt niet als vereiste dat de geadresseerde of iemand voor hem de ontvangst van een bericht elektronisch 'in persoon' moet bevestigen. Een bewijs van ontvangst kan zich bij een dergelijke dienst ook beperken tot de bevestiging dat een bericht op een account is afgeleverd. Indien met een bepaalde mate van betrouwbaarheid moet worden vastgesteld of de geadresseerde daadwerkelijk kennis heeft genomen

van de ontvangst van een bericht, dan hangt het van de inrichting van de dienst af of dit is gewaarborgd. Bij de zogenoemde gekwalificeerde elektronisch aangetekende bezorging wordt bijvoorbeeld de eis gesteld dat de identiteit van de geadresseerde wordt bevestigd, alvorens de gegevens worden bezorgd.

Door gebruik van een certificaat voor authenticatie van websites weet een burger of bedrijf dat hij zich echt op de gewenste website bevindt en niet op een namaaksite (artikel 3, onderdeel 38, van de verordening). Het stelt bezoekers van een website in staat met een bepaalde mate van betrouwbaarheid vast te stellen welke persoon of organisatie achter de website zit die ze online bezoeken. Visueel wordt dit gewoonlijk zichtbaar door het tonen van een slotje, vaak in combinatie met de groene kleur van de adresbalk. Websitecertificaten worden veel gebruikt als bron van vertrouwen in websites, onder meer voor internetbankieren, overheidswebsites en webwinkels. Het gebruik daarvan is essentieel voor betrouwbare toegang tot een website.

Aanvullende vertrouwensdiensten zien op de validering en bewaring van elektronische handtekeningen en –zegels. Validering is het proces waarmee wordt nagegaan of en bevestigd dat een elektronische handtekening of zegel geldig is (artikel 3, onderdeel 41, van de verordening). Bewaringsdiensten zorgen ervoor dat ook na verloop van tijd nog kan worden vastgesteld of een indertijd gebruikte elektronische handtekening of -zegel echt en geldig was. Dit waarborgt de bewijsfunctie van bijvoorbeeld ondertekende of gewaarmerkte elektronische documenten die gearchiveerd zijn en waarbij de technologische geldigheid van de elektronische handtekening of het zegel inmiddels is verlopen. Dit vereist maatregelen die het bijvoorbeeld mogelijk maken na te gaan of de betreffende vertrouwensdienst indertijd geldig was gebruikt en of gegevens achteraf niet aangepast zijn. Elektronische overeenkomsten, zoals koopcontracten die langs digitale weg tot stand zijn komen is een voorbeeld van mogelijke toepassing van deze dienst.

Vertrouwensdiensten worden vaak gebruikt bij het verzenden en ontvangen van elektronische documenten. Onder elektronische documenten wordt elke inhoud verstaan die in elektronische vorm is opgeslagen. Hier valt tekst onder maar ook geluid, beeld en zelfs audiovisuele opnames. De verordening bepaalt dat elektronische documenten rechtsgevolgen kunnen hebben en als bewijsmiddel gebruikt kunnen worden in gerechtelijke procedures.

2.3. Certificaten onderdeel van vertrouwensdiensten

Certificaten kunnen onderdeel zijn van een vertrouwensdienst, maar bijvoorbeeld ook van een elektronisch identificatiemiddel. Een certificaat is een gegevensbestand waarin onder meer identiteitsgegevens staan vermeld van degene op naam van wie het certificaat staat, de geldigheidsduur ervan en de partij die het certificaat heeft afgegeven. Voorafgaand aan de afgifte van het certificaat controleert de verstrekkende derde partij de identiteit van de persoon voor wie het certificaat bestemd is en registreert dit. Na afgifte kan de houder van het certificaat met behulp van unieke (geheime) private sleutel het certificaat gebruiken. Om deze sleutelgegevens onder zijn controle te houden, kan een middel zoals een smartcard, USB-stick, mobiele telefoon of token worden gebruikt. Een certificaat kan door de houder ervan gekoppeld worden aan door hemzelf gekozen of aangemaakte andere gegevens, bijvoorbeeld aan een elektronisch document. Hierdoor wordt de integriteit of herkomst, of eventueel ook de vertrouwelijkheid van dat document gewaarborgd. Degene die elektronisch en op afstand vertrouwt op een certificaat gekoppeld aan bijvoorbeeld een document, zal bepaalde gegevens in een certificaat moeten kunnen inzien en bevestigd krijgen dat het certificaat nog geldig en niet ingetrokken is. Daarvoor moet de vertrouwende partij beschikken over unieke publieke sleutelgegevens. Die sleutelgegevens zijn vastgelegd in het publieke deel van het certificaat of zijn bijvoorbeeld via een webbrowser toegankelijk. In de toelichting op het wetsvoorstel Wet elektronische handtekeningen is de werking van certificaten in verband met asymmetrische cryptologie toegelicht (Kamerstukken II 27 743 2000/01, nr. 3, blz. 2 en 3).

In de verordening worden specifieke eisen gesteld aan het verlenen van gekwalificeerde certificaten voor elektronische handtekeningen, voor elektronische zegels en voor website-authenticatie (artikel 3, vijftiende lid, dertigste lid en achtendertigste lid). Dit zijn certificaten waaraan door de daarvoor geldende specifieke eisen en het toezicht daarop een hoog betrouwbaarheidsniveau wordt toegekend. Een eis die bij de afgifte van een dergelijk gekwalificeerd certificaat van toepassing is, is dat verificatie van de identiteit in fysieke aanwezigheid moet plaatsvinden. Anders dan onder de richtlijn geldt dit alleen bij de eerste afgifte en kan verificatie bij een vervolgverzoek onder voorwaarden online en op afstand plaatsvinden. Daarmee worden de mogelijkheden voor het op afstand verkrijgen van een gekwalificeerd certificaat in de praktijk vereenvoudigd.

3. De inhoud en gevolgen van de eidas-verordening op hoofdlijnen

3.1 Inhoud

Indien een lidstaat van de Europese Unie de onlinetoegang tot publieke diensten afhankelijk stelt van een elektronisch identificatiemiddel dat nationaal is uitgegeven, belemmert dit de toegang tot die onlinedienst voor burgers of bedrijven uit andere lidstaten. Bijvoorbeeld de toegang tot een onlineportal of persoonlijke omgeving om bepaalde administratieve processen af te kunnen wikkelen. Om hierin verandering te brengen bevat de verordening een verplichte erkenning van elektronische identificatiemiddelen uit andere lidstaten waarvan het onderliggende stelsel is aangemeld bij de Europese Commissie. Met aangemelde elektronische identificatiemiddelen kunnen burgers en bedrijven zich ook toegang verschaffen tot onlinediensten die onder de in nationale wetgeving gestelde voorwaarden door openbare instanties uit andere lidstaten worden aangeboden en waarvoor het gebruik van een elektronisch identificatiemiddel vereist is. Deze verplichte erkenning door openbare instanties van aangemelde elektronische identificatiemiddelen beperkt zich tot die het betrouwbaarheidsniveau substantieel of hoog hebben. Een openbare instantie hoeft geen elektronisch identificatiemiddel te erkennen dat een lager betrouwbaarheidsniveau heeft dan voor de onlinedienst vereist is. Voorbeelden waarbij erkenning aan de orde kan zijn, is het met behulp van een aangemeld elektronisch identificatiemiddel in een andere lidstaat doen van online belastingaangifte of het realiseren van een elektronische inschrijving bij een universiteit. Een lidstaat is niet verplicht tot het melden van een stelsel over te gaan. De verordening preciseert de verantwoordelijkheid van een lidstaat voor onderdelen van een aangemeld stelsel en de aansprakelijkheid die daarbij geldt.

De verordening is tevens van toepassing op vertrouwensdiensten die aan het publiek worden aangeboden (zie hiervoor verder de toelichting bij artikel I, onderdeel F). Uitgangspunt in de verordening is dat de verlener van vertrouwensdiensten gevestigd in de ene lidstaat niet wordt belemmerd in het verlenen van zijn diensten in een andere lidstaat. In de verordening wordt verder onderkend dat betrouwbaar elektronisch verkeer wezenlijk is. De verordening regelt de eisen waaraan moet worden voldaan bij het verlenen van vertrouwensdiensten aan het publiek en waaraan het toezicht hierop moet voldoen. De verordening maakt hierbij onderscheid tussen het verlenen van niet-gekwalificeerde en gekwalificeerde vertrouwensdiensten. De functie van de dienst is steeds dezelfde. Het verschil is dat aan het verlenen van gekwalificeerde vertrouwensdiensten en de verleners daarvan specifieke eisen worden gesteld en het toezicht daarop specifieker en verdergaand is geregeld. Iedere verlener van vertrouwensdiensten aan het publiek is gehouden tot het treffen van passende organisatorische en technische veiligheidsmaatregelen. De lidstaten dienen te voorzien in een beperkte vorm van toezicht achteraf op de naleving hiervan bij niet-gekwalificeerde vertrouwensdiensten. Verder dient iedere verlener van vertrouwensdiensten te voldoen aan informatieverplichtingen, indien sprake is van een veiligheidsinbreuk of integriteitsverlies met aanzienlijke gevolgen voor de vertrouwensdienst. Voorts regelt de verordening dat gekwalificeerde vertrouwensdiensten niet eerder als zodanig mogen worden aangeboden, dan nadat daarvoor de status gekwalificeerd is toegekend door het door een lidstaat aangewezen toezichthoudend orgaan. Het toezichthoudend orgaan dient in de verordening vastgestelde taken te vervullen, waaronder die ten aanzien van de uitoefening van toezicht op verleners van vertrouwensdiensten en hun diensten, het delen van gegevens met andere toezichthouders, het verlenen van bijstand, samenwerking met

toezichthoudende organen uit andere lidstaten van de Europese Unie en het opstellen en bijhouden van vertrouwenslijsten. De mogelijkheid van vrijwillige accreditatie, die de richtlijn bood, komt niet terug in de verordening. Ook certificaten voor de authenticatie van websites worden gerekend tot vertrouwensdiensten. Die zijn, zoals uit het incident DigiNotar najaar 2011, is gebleken voor het realiseren van digitale betrouwbaarheid bij online-verkeer essentieel.

Er kunnen met behulp van vertrouwensdiensten rechtshandelingen tot stand komen en de bewijsvoering kan ermee worden vergemakkelijkt. De verordening bevat regels die gaan over de rechtsgevolgen die aan het gebruik van vertrouwensdiensten zijn verbonden en over het gebruik van vertrouwensdiensten als bewijs in gerechtelijke procedures. Daarnaast is de grensoverschrijdende erkenning van bepaalde elektronische handtekeningen/zegels door openbare instanties die onlinediensten aanbieden onderwerp van de verordening, evenals de positie van verleners van vertrouwensdiensten uit derde landen en aansprakelijkheid.

De verordening doet geen afbreuk aan nationaal of Unierecht dat betrekking heeft op de totstandkoming en geldigheid van contracten of andere wettelijke of procedurele verplichtingen inzake vormvereisten. In dat verband is Richtlijn 2000/31/EG van het Europees Parlement en de Raad van 8 juni 2000 betreffende bepaalde juridische aspecten van de diensten van de informatiemaatschappij, met name de elektronische handel, in de interne markt („richtlijn inzake elektronische handel") (PbEG L 178, 2000) relevant. Een van de uitgangspunten van die richtlijn is dat lidstaten ervoor zorgen dat hun rechtsstelsel het sluiten van overeenkomsten langs elektronische weg mogelijk maakt. Dit laat onverlet dat de richtlijn het toelaat dat een lidstaat in sommige gevallen een vormvereiste mag stellen, bijvoorbeeld dat een door de notaris opgemaakt authentieke akte op (bepaald) papier gesteld dient te zijn. De voorschriften over vertrouwensdiensten in de verordening respecteren dit.

3.2 Gevolgen

Een verordening werkt rechtstreeks en lidstaten van de Europese Unie zijn verplicht om alle maatregelen te nemen die nodig zijn voor de volledige verwezenlijking van een verordening. Gelet op het rechtstreekse karakter, maakt een verordening automatisch deel uit van de nationale rechtsorde en is het verboden om bepalingen ervan in het nationale recht over te nemen (arrest van het Hof van 7 februari 1973, C-39/72, Slachtpremies, ECLI:EU:C:1973:13). Voorkomen moet worden dat een nationale regeling opnieuw datgene bepaalt dat reeds in een rechtstreeks toepasselijke verordening wordt bepaald. Daartoe moeten de met de desbetreffende verordening strijdige bepalingen uit het nationale recht als ook de bepalingen uit de nationale regeling die hetzelfde regelen als de verordening worden geschrapt (arrest van het Hof van de Europese Gemeenschap van 7 februari 1973, C-39/72, ECLI:EU:C:1973:13). Wel kan het voor de operationalisering van een verordening nodig zijn om bepalingen met betrekking tot handhaving, rechtsbescherming en aanwijzing van uitvoeringsorganen op te nemen in nationale regelgeving. Daarnaast kan het noodzakelijk zijn feitelijke maatregelen te treffen. De eidas-verordening maakt zowel feitelijke uitvoeringswerkzaamheden als aanpassing van regelgeving noodzakelijk. Het deel van de eidas-verordening over elektronische identificatie vereist feitelijke uitvoering. Hierbij vervult de ontwikkeling van een landelijke technische voorziening die grensoverschrijdende elektronische identificatie mogelijk maakt een belangrijke rol. Voor het deel van de verordening dat over vertrouwensdiensten gaat, wordt wijziging van wetgeving voorgesteld. Deze wijzigingen hebben betrekking op de diverse hoofdstukken van de Telecommunicatiewet (hierna verder ook: Tw), de artikelen 3:15 a tot met c en artikel 6:196b, van het Burgerlijk Wetboek (hierna verder: BW), artikel 2.16 van de Algemene wet bestuursrecht (hierna verder: Awb), artikel 34a van de Wet bescherming persoonsgegevens en artikelen in verscheidene andere wetten die verwijzen naar artikelen met begrippen die door de rechtstreekse werking van de verordening worden vervangen.

De voorgestelde aanpassingen van de Tw zijn het gevolg van de voorschriften in de verordening over de eisen waaraan voldaan moet zijn bij het aanbieden van vertrouwensdiensten aan het publiek en over het toezicht daarop. Een van de voorgestelde wijzigingen heeft betrekking op een overgang van

het toezicht door de Autoriteit Consument en Markt (hierna verder: ACM) naar Agentschap Telecom, een dienstonderdeel van het Ministerie van Economische Zaken (hierna verder ook: AT). De voorgestelde wijzigingen in Boek 3 van het BW en de Awb hangen samen met de rechtsgevolgen verbonden aan het gebruik van de elektronische handtekening. De voorgestelde veranderingen in Boek 3 respectievelijk Boek 6 van het BW houden verder het vervallen van bestaande bepalingen over certificatiedienstverleners uit derde landen en over aansprakelijkheid certificatieverleners in. De verordening voorziet daarin met rechtstreekse werking, waardoor genoemde bepalingen overbodig worden. Voor zover in andere wetgeving naar de desbetreffende bepalingen uit deze wetten wordt verwezen, voorziet dit wetsvoorstel tevens in aanpassing daarvan.

De voorschriften in de verordening over de erkenning van vertrouwensdiensten door openbare instanties die onlinediensten aanbieden, vereisen dat openbare instanties met inachtneming daarvan handelen. Afhankelijk van de inhoud van bepaalde uitvoeringshandelingen van de Europese Commissie gebaseerd op de verordening die tijdens de voorbereiding van dit wetsvoorstel nog niet bekend zijn, in combinatie met eventuele aanpassing van enkele andere besluiten van de Europese Commissie gebaseerd op Richtlijn 2006/123/EG van het Europees Parlement en de Raad van 12 december 2006 betreffende diensten op de interne markt (PbEG L 376, 2006) (hierna verder: de dienstenrichtlijn), is het wenselijk de voorziening die thans onderdeel uitmaakt van het Ondernemersplein en die bevoegde instanties als bedoeld in de Dienstenwet faciliteert bij het valideren van elektronische handtekeningen te bezien op de gevolgen van de verordening. Voorts kan op een later moment een beperkte wijziging van de Dienstenwet noodzakelijk zijn die op de erkenning van elektronische handtekeningen bij procedures en formaliteiten via het centraal loket als bedoeld in die wet betrekking heeft. Tot slot bevat het wetsvoorstel artikelen die de samenloop met enkele andere wetsvoorstellen regelt alsmede voorzien in overgangsrecht.

4. Erkenning elektronische identificatiemiddelen

4.1 Grensoverschrijdende erkenning elektronische identificatiemiddelen

De verplichting tot erkenning van elektronische identificatiemiddelen is van toepassing op openbare instanties die toegang bieden tot onlinediensten waarvoor op grond van nationaal recht of gangbare bestuursrechtelijke praktijk elektronische identificatie met gebruikmaking van een elektronisch identificatiemiddel en authenticatie vereist is. De verplichting tot erkenning kan alleen van toepassing zijn op openbare instanties die online diensten aanbieden. Het begrip openbare instantie is gedefinieerd in de verordening en sluit overwegend aan bij de definitie van het begrip 'aanbestedende dienst' als bedoeld in de richtlijn 2014/24/EU van het Europees Parlement en de Raad van 26 februari 2014 betreffende het plaatsen van overheidsopdrachten en tot intrekking van Richtlijn 2004/18/EG (PbEU L 94, 2014). Voor de praktijk biedt het begrip aanbestedende dienst daarmee een belangrijk aanknopingspunt voor instellingen en organen om bepalen of zij een openbare instantie in de zin van de verordening zijn. Of een dienst online door een openbare instantie moet worden aangeboden en in hoeverre een elektronische identificatiemiddel daarbij vereist is, is geen onderwerp van de verordening. De verordening regelt niet de door openbare instanties geboden toegang tot elektronische dienstverlening als zodanig. Dit is een aangelegenheid van de lidstaten zelf en van eventuele andere toepasselijke Europese regelgeving. Bij online-diensten die door openbare instanties aangeboden kunnen worden, kan onder meer worden gedacht aan het online kunnen inzien van voor een burger of bedrijf bestemde (persoonlijke) informatie, het aanvragen van een vergunning, het doen van meldingen of aangiftes, het aanbrengen van wijzigingen in gegevens, de opgave van een registratie, de afwikkeling van allerlei ander opvolgend en te ontvangen retourverkeer en te verrichten handelingen. Een openbare instantie die weliswaar onlinediensten aanbiedt maar voor het gebruik waarvan geen elektronisch identificatiemiddel vereist is, hoeft geen elektronische identificatiemiddelen uit andere lidstaten te erkennen.

Niet alle elektronische identificatiemiddelen uit andere lidstaten hoeven erkend te worden. Voorwaarde voor erkenning is dat het elektronische identificatiemiddelen betreft waarvan een lidstaat het stelsel,

waartoe de elektronische identificatiemiddelen behoren, heeft gemeld bij de Europese Commissie. Om grensoverschrijdend te kunnen erkennen, dienen elektronische identificatiemiddelen namelijk aan bepaalde interoperabiliteits- en veiligheidseisen te voldoen. Deze eisen zijn op het niveau van de verordening en in uitvoeringshandelingen van de Europese Commissie gedefinieerd. Indien een lidstaat een stelsel niet heeft aangemeld, hoeven de openbare instanties uit een andere lidstaat de tot dat stelsel behorende elektronische identificatiemiddelen derhalve niet te erkennen.

De verplichting tot erkenning van elektronische identificatiemiddelen uit andere lidstaten, waarvan het stelsel is aangemeld bij de Commissie, is beperkt tot middelen met een vrij hoge betrouwbaarheid. De verordening onderscheidt drie betrouwbaarheidsniveaus, namelijk laag, substantieel en hoog. De Europese Commissie zal uitvoeringshandelingen vaststellen die nader bepalen wat die niveaus inhouden. Alleen elektronische identificatiemiddelen met een substantieel of hoog betrouwbaarheidsniveau moeten worden erkend door openbare instanties uit andere lidstaten. Daarbij geldt dat een openbare instantie nooit een elektronisch identificatiemiddel met een lager betrouwbaarheidsniveau hoeft te erkennen dan voor toegang tot de online dienst wordt geëist.

De verplichting tot erkenning heeft tot slot betrekking op elektronische identificatiemiddelen bestemd voor natuurlijke personen, rechtspersonen of natuurlijke personen die rechtspersonen vertegenwoordigen. Rechtspersonen zijn in de zin van het Verdrag betreffende de Werking van de Europese Unie (hierna verder: VWEU) zijn alle entiteiten die zijn opgericht naar of worden beheerst door het recht van een lidstaat, ongeacht hun rechtsvorm. Geen onderdeel van deze opsomming is de vertegenwoordiging door de ene natuurlijke persoon van een andere, zoals vertegenwoordiging in het geval van handelingsonbekwaamheid of van een onder curatele gestelde.

4.2 Uitvoeringsmaatregelen

Om grensoverschrijdend gebruik van elektronische identificatiemiddelen mogelijk te maken, is een technische voorziening nodig die berichten kan versturen over elektronische identiteiten verstrekt in Nederland en berichten kan ontvangen over elektronische identiteiten verstrekt in andere lidstaten. Deze voorziening stuurt persoonsidentificatie gegevens van burgers en bedrijven uit andere lidstaten naar Nederlandse openbare instanties die deze nodig hebben voor online dienstverlening aan deze groep. Andersom stuurt de voorziening persoonsidentificatie gegevens van Nederlandse burgers en bedrijven naar openbare instanties in andere lidstaten, waar deze burgers en bedrijven online diensten willen afnemen, indien althans tot melding van een Nederlands stelsel bij de Europese Commissie wordt overgegaan. In voorkomend geval gaan er dan persoonsidentificatie gegevens van de Nederlandse technische voorziening naar de technische voorziening van de betreffende lidstaat. De Nederlandse technische voorziening, in feite een koppelpunt, wordt aangesloten op de nationale infrastructuur elektronische identiteiten, het eID-stelsel. De technische voorziening stelt Nederlandse openbare instanties in staat om vast te stellen of het een elektronisch identificatiemiddel betreft dat is gemeld bij de Europese Commissie, over welk betrouwbaarheidsniveau dat middel beschikt en levert de authenticatie van de persoon, zodat de openbare instantie kan bepalen of toegang tot de online dienst wordt verleend. Door middel van aansluiting van het koppelpunt op de bestaande Nederlandse identiteitsinfrastructuur kan het internationale berichtenverkeer via een reeds bestaande beveiligde verbinding plaatsvinden en worden onnodige inspanningen en kosten bij openbare instanties vermeden. Aangezien er wordt gewerkt met gegevens tot persoonsidentificatie is dataprotectie een vereiste. Op de verplichte erkenning van elektronische identiteiten door openbare instanties is de Wet Naleving Europese regelgeving publieke entiteiten van toepassing.

4.3 De melding van een stelsel tot bewerkstelliging van erkenning

Lidstaten bepalen zelf of een stelsel, dat kan overigens ook een specifiek identificatiemiddel op een bepaald veiligheidsniveau zijn, wordt aangemeld bij de Europese Commissie. Na afronding van het notificatieproces kunnen de burgers en bedrijven hun nationale elektronische identiteit dan gebruiken voor toegang tot online diensten in andere lidstaten. De lidstaten moeten er zelf voor zorgen dat stelsels van elektronische identificatiemiddelen aan de bij of krachtens de verordening gestelde eisen

voldoen. Een stelsel kan betrekking hebben op een elektronisch identificatiemiddel dat door of in opdracht van een lidstaat wordt uitgegeven. Een aanmelding kan ook betrekking hebben op een stelsel waarvan de daaronder vallende elektronische identificatiemiddelen onafhankelijk van de aanmeldende lidstaat worden uitgegeven, maar die door de lidstaat zijn erkend. Een stelsel kan daarmee (tevens) betrekking hebben op door de markt aangeboden elektronische identificatiemiddelen.

Bij de totstandkoming en het gebruik van een elektronisch identificatiemiddel kunnen meerdere partijen betrokken zijn met ieder een eigen verantwoordelijkheid. De partij die voor een koppeling van persoonsidentificatiegegevens aan de persoon zorg draagt, kan een andere zijn dan degene die een elektronisch identificatiemiddel uitgeeft of degene die het authenticatieproces verzorgt. De verordening bepaalt dat als tot melding bij de Europese Commissie wordt overgegaan, de lidstaat de juistheid van de persoonsidentificatiegegevens waarborgt (artikel 7d, van de verordening) en de partij die het elektronische identificatiemiddel uitgeeft verantwoordelijk is voor de koppeling tussen het middel en de identificatiegegevens van een persoon (artikel 7e, van de verordening). Daarnaast dient de aanmeldende lidstaat te voorzien in de werking en beschikbaarheid van een online authenticatievoorziening, het koppelpunt, waardoor partijen die werken met elektronische identificatiemiddelen uit andere lidstaten de echtheid daarvan bevestigd kunnen krijgen op het daaraan verbonden betrouwbaarheidsniveau (artikel 7f, van de verordening). Openbare instanties moeten daarvan kosteloos gebruik kunnen maken bij hun online-dienstverlening aan burgers en bedrijven uit andere lidstaten. Ingeval van opzet of door nalatigheid toegebrachte schade die te wijten is aan een verzuim in de naleving van deze specifieke verplichtingen, is de lidstaat daarvoor aansprakelijk overeenkomstig de nationale regels inzake aansprakelijkheid. Voor andere in de verordening vastgestelde delen in de keten betreffende elektronische identificatiemiddelen berust aansprakelijkheid onder dezelfde voorwaarden bij de partijen die voor die delen verantwoordelijk zijn (artikel 11 van de verordening). Lidstaten moeten elkaar en de Europese Commissie informeren over veiligheidsproblemen met elektronische identiteiten van een genotificeerd stelsel. Een door veiligheidsinbreuk of integriteitsverlies getroffen lidstaat dient de grensoverschrijdende authenticatie geheel of gedeeltelijk op te schorten of in te trekken (artikel 10, van de verordening).

4.4 Uitvoeringsmaatregelen

Burgers en bedrijven met een in Nederland uitgegeven elektronisch identificatiemiddel kunnen hiermee alleen in andere lidstaten terecht, indien het onderliggende stelsel hiervoor door Nederland is aangemeld bij de Europese Commissie. Of en wanneer Nederland een stelsel voor elektronische identificatie gaat aanmelden voor wederzijdse erkenning, is ten tijde van het opstellen van dit wetsvoorstel nog aan besluitvorming onderhevig. De besluitvorming hierin voor Nederland hangt af van nationale ontwikkelingen, in het bijzonder de totstandkoming van het eID-stelsel waarin publieke en private aanbieders van elektronische identificatiemiddelen actief zullen zijn. Dit stelsel is thans nog in ontwikkeling. Aanmelding is voor een lidstaat facultatief en daarmee geen vereiste voor een tijdige omzetting van de verordening. De verplichting tot erkenning van aangemelde stelsels geldt voor alle lidstaten uiterlijk vanaf september 2018.

5. Het verlenen van vertrouwensdiensten

5.1 Het treffen van passende veiligheidsmaatregelen

Verleners van zowel niet-gekwalificeerde als gekwalificeerde vertrouwensdiensten aan het publiek verlenen diensten waarbij vertrouwen centraal staat. Gelet hierop bevat de verordening een algemeen uitgangspunt. Zij dienen passende technische en organisatorische maatregelen te treffen om veiligheidsrisico's van de door hen te verlenen diensten te beheersen. Het zal per vertrouwensdienst en van de beoogde betrouwbaarheid die daarmee wordt nagestreefd, afhangen op welke wijze aan deze verplichting invulling dient te worden gegeven.

5.2 Uitvoeringsmaatregelen

De verordening biedt lidstaten geen grondslag nadere voorschriften in nationale wetgeving vast te stellen over het treffen van passende veiligheidsmaatregelen. De Europese Commissie kan door middel van uitvoeringshandelingen passende veiligheidsmaatregelen nader specificeren. Voor gekwalificeerde vertrouwensdiensten zijn de eisen in de verordening waaraan voldaan dient te zijn specifieker, zodat het eenvoudiger dan voor niet-gekwalificeerde vertrouwensdiensten vast te stellen is wat passend is. Het door een lidstaat aan te wijzen toezichthoudend orgaan dat verantwoordelijk is voor het toezicht op de naleving van deze en andere eisen uit de verordening kan hierin een ondersteunende rol vervullen, door waar dat mogelijk is richtinggevend daarover te communiceren op basis van bijvoorbeeld opgedane ervaringen ook in andere lidstaten. Bij de invulling en uitvoering van deze norm kunnen ook algemeen geaccepteerde beveiligingsstandaarden binnen de praktijk van informatiebeveiliging, zoals de Code voor Informatiebeveiliging (NEN-ISO/IEC 27002:2007 nl) van betekenis zijn. Het 'richtsnoer Beveiliging persoonsgegevens' van het College bescherming persoonsgegevens gaat in op passende en organisatorische maatregelen bij de beveiliging van persoonsgegevens.

5.3 Meldplichten bij inbreuk op veiligheid of verlies van integriteit

Maatregelen die tot doel hebben de veiligheid van vertrouwensdiensten op passende wijze te waarborgen, kunnen het risico op veiligheidsinbreuken of verlies van integriteit verminderen maar niet uitsluiten. Indien zich een incident met vertrouwensdiensten voordoet, dient vertrouwen zoveel mogelijk behouden te blijven of te worden hersteld. De verordening bepaalt dat aanbieders van gekwalificeerde en niet-gekwalificeerde vertrouwensdiensten verplicht zijn een veiligheidsinbreuk of integriteitsverlies met aanzienlijke gevolgen voor de verleende vertrouwensdienst of voor de persoonsgegevens die daarmee worden beheerd binnen vierentwintig uur na ontdekking te melden bij het door een lidstaat aangewezen toezichthoudend orgaan van de lidstaat waar de verlener gevestigd is. Waar passend dienen andere relevante organen, zoals het bevoegde nationale orgaan voor informatieveiligheid of de gegevensbeschermingsautoriteit op de hoogte te worden gesteld van iedere veiligheidsinbreuk of ieder integriteitsverlies met aanzienlijke gevolgen voor de verleende vertrouwensdienst of voor de persoonsgegevens die daarmee worden beheerd. Als de veiligheidsinbreuk of het integriteitsverlies waarschijnlijk negatieve gevolgen heeft voor de gebruikers, moeten deze hierover door de vertrouwensdienstverlener onmiddellijk worden geïnformeerd. Indien het algemeen belang daarmee wordt gediend, kan het toezichthoudend orgaan bepalen dat het publiek wordt of moet worden geïnformeerd over een veiligheidsinbreuk of integriteitsverlies. Doel van deze verplichtingen is het bevestigen en waar nodig herstellen van het vertrouwen van het publiek, de klanten, de markt, de overheid en de toezichthouders in de desbetreffende instelling of het desbetreffende bedrijf.

Meldplichten zijn ook onderwerp van andere toekomstige Europese regelgeving, waaronder de meldplicht in de ontwerprichtlijn van de Europese Commissie houdende maatregelen om een hoog gemeenschappelijk niveau van netwerk- en informatiebeveiliging in de Unie te waarborgen (COM (2013) 48 finaal) en in het voorstel van de Europese Commissie voor een Algemene verordening gegevensbescherming (COM (2012)11 def) ter vervanging van richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (PbEG 1995, L 281). Bij de implementatie en uitvoering van deze meldplichten zal voor zover noodzakelijk op de verhouding tot de meldplicht in de eidas-verordening worden ingegaan.

5.4 Uitvoeringsmaatregelen

De plicht tot melden van een inbreuk of integriteitsverlies is in de verordening geregeld. In het wetsvoorstel worden de in de verordening genoemde organen en autoriteit aangewezen tot wie een verplichte melding zich dient te richten. Dit zijn:

- de Minister van Economische Zaken als toezichthoudend orgaan, bedoeld in de verordening;

- de Minister van Veiligheid en Justitie als nationale orgaan voor informatieveiligheid, bedoeld in de verordening;
- het College bescherming persoonsgegevens (hierna verder: Cbp) als gegevensbeschermingsautoriteit, bedoeld in de verordening.

De aanwijzing van de Minister van Economische Zaken als toezichthoudend orgaan wordt in paragraaf 7.8 toegelicht. De minister is op grond van het wetsvoorstel bevoegd ambtenaren van Agentschap Telecom te belasten met het toezicht op het verlenen van vertrouwensdiensten. De aanwijzing van de Minister van Veiligheid en Justitie als nationale orgaan voor informatieveiligheid volgt uit zijn verantwoordelijkheid voor het Nationaal Cyber Security Center (hierna verder: NCSC). De aanwijzing van het Cbp als gegevensbeschermingsautoriteit is gelegen in de verantwoordelijkheid van het Cbp voor het toezicht op de verwerking van persoonsgegevens overeenkomstig het bepaalde bij of krachtens de Wet bescherming persoonsgegevens (hierna verder: Wbp) en andere wetgeving inzake de verwerking van persoonsgegevens bepaalde (zoals art. 11.3a Tw). Met het oog daarop beschikt het Cbp over toezichthoudende en handhavende bevoegdheden.

Een melding aan AT en NCSC is aangewezen indien een veiligheidsinbreuk of integriteitsverlies aanzienlijke gevolgen voor de verleende vertrouwensdienst heeft. Ten algemene geldt dat niet te snel wordt aangenomen dat een melding achterwege kan blijven. Dat wil zeggen dat ook sprake is van aanzienlijke gevolgen als bedoeld in de verordening indien een incident aanzienlijke gevolgen voor de verleende vertrouwensdienst *kan* hebben, ongeacht of het zeker is dat die zullen intreden. Gelet op de ernst en omvang van de gevolgen die een incident met vertrouwensdiensten kan veroorzaken, wordt aangenomen dat de verordening hierin ruim opgevat dient te worden. En in geval van gerede twijfel over de vraag hoe groot de gevolgen daadwerkelijk zouden kunnen zijn, dient eveneens tot melding te worden overgegaan. Indien daarentegen vaststaat dat een veiligheidsinbreuk of integriteitsverlies slechts beperkte impact heeft, kan een melding achterwege blijven. De verlener van vertrouwensdiensten zal in dat geval in staat zijn de inbreuk snel en adequaat te herstellen. Naarmate meer onzekerheid bestaat omtrent de aard en omvang van gevolgen van een incident voor de betrouwbaarheid of indien direct duidelijk is dat de gevolgen van een veiligheidsinbreuk of integriteitsverlies vertrouwensdiensten op grotere schaal treffen of zullen treffen, is een melding noodzakelijk. Vanuit oogpunt van duidelijkheid, voorzienbaarheid en kenbaarheid kan het noodzakelijk zijn omstandigheden en criteria aan te duiden waaronder een melding vereist is. De Minister van Economische Zaken kan hierin door middel van beleidsregels en/of richtsnoeren voorzien uit hoofde van het toezicht op de naleving van de verordening en de Minister van Veiligheid en Justitie voor een melding aan het NCSC.

Een melding aan het Cbp is op grond van de verordening vereist, indien een inbreuk of integriteitsverlies aanzienlijke gevolgen heeft voor de persoonsgegevens die met een vertrouwensdienst worden beheerd. Deze meldplicht aangaande persoonsgegevens is daarmee specifieker en beperkter in toepassingsbereik dan die als geregeld in de Wet tot wijziging van de Wbp inzake een meldplicht datalekken Die wet bevat in het nieuwe artikel 34a Wbp, eerste lid, een verplichting tot melding aan het Cbp van een inbreuk op de beveiliging als bedoeld in de Wbp, die leidt tot de aanzienlijke kans op ernstige nadelige gevolgen dan wel ernstige nadelige gevolgen heeft. Ingevolge artikel 34a, tweede lid, stelt de verantwoordelijke de betrokken personen in kennis indien de inbreuk waarschijnlijk ongunstige gevolgen zal hebben voor diens persoonlijke levenssfeer. Het Cbp zal door middel van beleidsregels de praktijk nader houvast bieden.

Te onderscheiden van de materiële plicht tot melden van bepaalde incidenten met vertrouwensdiensten aan de aangewezen organen, zijn de daarbij te overleggen gegevens. De Europese Commissie kan op grond van de verordening door middel van uitvoeringshandelingen formaten en procedures, met inbegrip van termijnen, vaststellen over de bij een melding aan de relevante organen of een betroffene te overleggen gegevens. Bijvoorbeeld door formulieren vast te stellen met een algemene of specifieke duiding van wat een melding voor vertrouwensdiensten aan organen dient te behelzen. Duiding van te overleggen gegevens in nationale regelgeving is daarmee

uitsluitend aan de orde, indien krachtens de verordening hierin niet is voorzien. Gelet hierop voorziet het wetsvoorstel in een grondslag in de Telecommunicatiewet om aan de Minister van Economische Zaken, de Minister van Justitie, het Cbp en in voorkomend geval aan degene die van een inbreuk of verlies negatieve gevolgen ondervindt, te overleggen gegevens bij algemene maatregel van bestuur vast te stellen, indien een goede uitvoering van de verordening dit vereist. Daarmee blijft er ruimte om in het geval dat noodzakelijk mocht zijn de te overleggen gegevens in nationale regelgeving vast te stellen. Uiteraard zal de Minister van Economische Zaken dit in voorkomend geval in overeenstemming met de Minister van Veiligheid en Justitie doen. De aan AT, NCSC en Cbp te melden gegevens kunnen op die wijze waar mogelijk onderling afgestemd worden vastgelegd.

De in de verordening geregelde meldplicht heeft gevolgen voor bestaande regelgeving. Het Besluit elektronische handtekeningen bevat een meldplicht voor aanbieders van gekwalificeerde certificaten voor elektronische handtekeningen aan het publiek. Een melding van certificatiedienstverleners dient op dit moment gericht te zijn aan ACM en aan de Minister van Veiligheid en Justitie. Ook zijn in dat besluit de gegevens geduid die bij een melding verstrekt dienen te worden. Deze meldplicht is na het DigiNotarincident tot stand gekomen in afwachting van de verordening. Doordat het wetsvoorstel bepaalt aan wie gemeld dient te worden en de verordening zelfstandig en met een breder toepassingsbereik bepaalt wat een meldplicht inhoudt, is het niet passend dit nog in nationale regelgeving vast te leggen. Ook voorziet het wetsvoorstel in de mogelijkheid bij algemene maatregel van bestuur de te overleggen gegevens te benoemen, indien dat voor een goede uitvoering van de verordening vereist is. Mede in het licht hiervan zal het Besluit elektronische handtekeningen worden heroverwogen.

Bij de totstandkoming van het wetsvoorstel is rekening gehouden met het respecteren van de rechtstreekse werking van de verordening in verhouding tot de Wet tot wijziging van de Wbp inzake een meldplicht datalekken. De verordening regelt met rechtstreekse werking de meldplicht ook aan de nationale gegevensbeschermingsautoriteit, de mogelijkheid voor de Commissie tot duiding van daarbij te overleggen gegevens krachtens de verordening en de melding aan een betrokkene en eventueel het publiek. Dit zijn zaken die ook in de Wet tot wijziging van de Wbp inzake een meldplicht datalekken worden geregeld, zodat wordt voorgesteld vertrouwensdiensten van het toepassingsbereik van die wet uit te sluiten. Om zeker te stellen dat het Cbp toezicht kan houden op de naleving van de meldplichten uit de verordening wordt een benadering aangehouden die ook ten aanzien van aanbieders van openbare elektronische communicatiediensten is gevolgd. Voor die aanbieders geldt op grond van artikel 11.3a van de Tw een meldplicht die op persoonsgegevens betrekking heeft, waarbij die melding omwille van doelmatigheidsoverwegen bij het Cbp dient plaats te vinden. In het onderhavige wetsvoorstel is voor vertrouwensdiensten op vergelijkbare wijze een bepaling aan de Tw toegevoegd waarin het toezicht op de meldplicht ingevolge de verordening bij het Cbp wordt belegd.

Anders dan Agentschap Telecom en het Cbp is NCSC geen toezichthouder. De activiteiten van het NCSC liggen in de sfeer van het bieden van ondersteuning en bijstand bij het waarborgen en herstellen van vitale ICT-systemen, bijvoorbeeld naar aanleiding van een vrijwillige melding. Op activiteiten van het NCSC volgend op een melding zijn bestaande wettelijke kaders van toepassing, zoals die inzake de Wbp en de Wet openbaarheid van bestuur. Naar aanleiding van de motie Hennis-Plasschaert c.s. (Kamerstukken II 2011/12, 26 643, nr. 202) is een wettelijke regeling in voorbereiding, waarin de taken van de minister op het terrein van cybersecurity worden vastgesteld, een meldplicht wordt geregeld voor een inbreuk op de veiligheid of een verlies van integriteit van elektronische informatiesystemen en ook het verwerken van gegevens ten behoeve van de uitvoering van die taken aan bod komen. Het vooruitlopend hierop wettelijk vastleggen van taken en bevoegdheden van de minister in relatie tot het NCSC specifiek in verband met een meldplicht voor vertrouwensdiensten, is voor een strikte omzetting van de verordening niet noodzakelijk[1].

[1] De verhouding tussen het wetsontwerp Wet gegevensverwerking en meldplicht cybersecurity en de in de eidas-verordening geregelde meldplicht aan het nationale orgaan voor informatieveiligheid, wordt nog nader bezien op

5.5 Gekwalificeerde vertrouwensdiensten en vertrouwenslijsten

Naast de algemene voorschriften die gelden voor alle verleners van vertrouwensdiensten, zijn er specifieke eisen die uitsluitend van toepassing zijn op de verleners van gekwalificeerde vertrouwensdiensten en hun diensten. Deze eisen hebben betrekking op de verlener van de vertrouwensdienst, zoals onder meer eisen betreffende personeel, procedures en betrouwbare systemen en daarnaast op de specifieke vertrouwensdienst die hij voornemens is te verlenen aan het publiek. Laatstbedoelde eisen zijn per vertrouwensdienst verschillend vastgesteld. Voor veel eisen in de verordening, waaronder ook voor gekwalificeerde vertrouwensdiensten, kan de Europese Commissie verwijzen naar private referentienormen die invulling geven aan gestelde eisen. Het voldoen aan deze normen levert het vermoeden op dat aan die eisen van de verordening is voldaan. Normen maken de algemene eisen specifiek, controleerbaar en toetsbaar. Normen worden opgesteld door internationale en Europese normalisatie organisaties zoals ISO en ETSI. Het is niet verplicht de normen waarnaar wordt verwezen na te leven. Andere werkwijzen die een vergelijkbaar resultaat opleveren zijn ook toegestaan.

Een verlener van vertrouwensdiensten die het voornemen heeft gekwalificeerde vertrouwensdiensten aan het publiek te verlenen dient een kennisgeving van zijn voornemen te doen aan het toezichthoudend orgaan. Doordat aan gekwalificeerde vertrouwensdiensten een hoge mate van betrouwbaarheid wordt toegekend, is van belang dat deskundige externe toetsing op de in de verordening gestelde eisen plaatsvindt onverminderd de noodzaak van publiekrechtelijk toezicht. Bij de kennisgeving van het voornemen dient een conformiteitsbeoordelingsverslag van een conformiteitsbeoordelingsinstantie worden overgelegd dat op de verlener en de dienst betrekking heeft. Bij een conformiteitsbeoordelingsinstantie zijn auditors werkzaam die deskundig zijn op het terrein van vertrouwensdiensten. Een dergelijke instantie moet geaccrediteerd zijn overeenkomstig Verordening (EG) nr. 765/2008 van het Europees Parlement en de Raad van 9 juli 2008 tot vaststelling van de eisen inzake accreditatie en markttoezicht betreffende het verhandelen van producten en tot intrekking van Verordening (EEG) nr. 339/93 (PbEU 2008, L 218) (hierna verder: verordening 765/2008). Accreditatie vindt plaats aan de hand van geharmoniseerde accreditatienormen. De Europese Commissie is bevoegd vast te stellen welke van deze normen geschikt zijn voor de accreditatie van conformiteitsbeoordelingsinstanties die de hiervoor genoemde audit willen uitvoeren. Tevens kan de Europese Commissie regels vaststellen voor uitvoering van de audit en het conformiteitsbeoordelingsverslag. In Nederland vindt accreditatie plaats door de Raad voor Accreditatie.

Als naar het oordeel van het door de lidstaat aangewezen toezichthoudend orgaan voldaan is aan de eisen uit de verordening, kent die de status van gekwalificeerd toe aan de verlener en zijn vertrouwensdiensten en wordt die status opgenomen in de vertrouwenslijst. De vertrouwenslijst is een instrument met behulp waarvan een ieder elektronisch op afstand kan nagaan of de status van 'gekwalificeerd' nog geldig is. Momenteel bestaan er al vertrouwenslijsten voor de elektronische handtekening. Deze zullen worden uitgebreid met andere vertrouwensdiensten. Een gekwalificeerde dienstverlener die is opgenomen op de vertrouwenslijst, mag het vertrouwensmerk van de Europese Unie voor gekwalificeerde vertrouwensdiensten voeren. Dit keurmerk is een eenvoudige, herkenbare en duidelijke manier om in de hele Europese Unie aan te geven dat een vertrouwensdienst gekwalificeerd is. Ook na opname in de vertrouwenslijst moet de gekwalificeerde verlener en de gekwalificeerde dienst aan de eisen uit de verordening blijven voldoen.

5.6 Uitvoeringsmaatregelen

Doordat in de verordening specifieke eisen worden gesteld aan gekwalificeerde verleners van vertrouwensdiensten en hun diensten, is het niet langer mogelijk in nationale regelgeving eisen voor

---

samenloop. Hierbij wordt rekening gehouden met de rechtstreekse werking van de verordening. Dit kan tot aanpassingen in het wetsontwerp en de memorie van toelichting leiden.

te schrijven waaraan voldaan dient te worden. In het wetsvoorstel vervalt de grondslag die de Tw biedt om bij of krachtens algemene maatregel van bestuur eisen te stellen aan certificatiedienstverleners van gekwalificeerde certificaten voor het publiek en aan hun gekwalificeerde certificaten. Dit zal gevolgen hebben voor het Besluit elektronische handtekeningen. De verordening biedt nog wel ruimte voor nationale regelgeving als het gaat om de verificatie van de identiteit van degene aan wie een gekwalificeerd certificaat wordt afgegeven. De huidige Tw regelt de verificatie van de identiteit voor gekwalificeerde certificaten die op naam van natuurlijke personen worden gesteld, die bestemd zijn voor elektronische handtekeningen en waarbij identificatie in fysieke aanwezigheid plaatsvindt. Dat dient plaats te vinden aan de hand van de bij de Wet op de identificatieplicht aangewezen geldige documenten. Als gevolg van de verordening strekt verificatie zich voortaan ook uit tot andere soorten gekwalificeerde certificaten en ook tot rechtspersonen en daarnaast voor de gevallen waarin online-identificatie en authenticatie toegestaan is. Voorgestelde wijzigingen van de Tw bepalen hoe verificatie in die gevallen dient plaats te vinden. Dit omvat ook de verificatie van zogenoemde attributen, extra specifieke gegevens die op een persoon betrekking hebben, en die van een certificaat deel kunnen uitmaken.

Te onderscheiden van in de verordening vastgestelde eisen zijn normen die eisen specifiek en controleerbaar maken. Voor het waarborgen van de betrouwbaarheid en de rechtszekerheid is noodzakelijk dat bij de toepasselijkheid van de verordening vanaf 1 juli 2016 in voldoende mate is voorzien in dergelijke veelal technische normen, waaraan een vermoeden van overeenstemming met de eisen kan worden ontleend. Aangezien het aanwijzen van normen geen verplichting maar een bevoegdheid van de Europese Commissie is, kan het voorkomen dat er wel normen zijn maar dat deze niet zijn aangewezen. Gelet hierop bepaalt het wetsvoorstel dat bij of krachtens algemene maatregel van bestuur hierin kan worden voorzien, voor zover dit voor een goede uitvoering van de verordening is vereist.

Op grond van de huidige Tw kan de Minister van Economische Zaken een of meer organisaties aanwijzen die bevoegd zijn certificatiedienstverleners te toetsen op overeenstemming met eisen die bij en krachtens deze wet aan hen en hun diensten zijn gesteld, en die daartoe een bewijs van toetsing kunnen afgeven. Het betreft een ingevolge het Besluit elektronische handtekeningen geaccrediteerde organisatie. De aangewezen organisatie onderhoudt samen met andere belanghebbenden een certificatieschema dat het TTP.NL-schema wordt genoemd. Dit schema is op basis van zelfregulering tot stand gekomen. Het bewijs van toetsing van een aangewezen organisatie wordt gelet hierop ook wel de TTP-verklaring genoemd. Indien een certificatiedienstverlener over een dergelijk bewijs van toetsing van een door de Minister aangewezen organisatie beschikt, wordt daaraan het vermoeden ontleend dat aan de krachtens de Telecommunicatiewet gestelde eisen is voldaan. In plaats daarvan kan een certificatiedienstverlener ook zelf bewijs aandragen waaruit blijkt dat aan de krachtens de wet gestelde eisen is voldaan. In de praktijk wordt van deze laatste mogelijkheid geen gebruik gemaakt.

Deze in de Tw geregelde systematiek is niet langer houdbaar onder de verordening. Het door de minister kunnen aanwijzen van certificeringsorganisaties vervalt in het wetsvoorstel. De verordening biedt onvoldoende ruimte om te voorzien in aanwijzing van conformiteitsbeoordelingsinstanties op basis van nationale toelatingseisen. De toezichthouder dient zich er bewust van te zijn dat hierdoor tussen conformiteitsbeoordelingsinstanties verschillen kunnen zijn. Daarnaast is er niet langer sprake van vrijwillige maar van verplichte inschakeling van een dergelijke instantie door een verlener van vertrouwensdiensten die de status gekwalificeerd wil hebben of heeft verkregen. De verordening kent bovendien aan de beschikbaarheid van een verslag of verklaring van een conformiteitsbeoordelingsinstantie geen vermoeden toe dat sprake is van overeenstemming met de in de verordening gestelde eisen. Vanuit de behoefte aan beter en meer direct toezicht op verleners van vertrouwensdiensten naar aanleiding van het incident met DigiNotar in 2011, is continuering van toekenning van een bewijsvermoeden aan een verslag of verklaring van de conformiteitsbeoordelingsinstantie ook niet wenselijk. In het wetsvoorstel komen de bepalingen over dit bewijsvermoeden te vervallen. Voorgestelde wijzigingen in de Telecommunicatiewet hebben

daarnaast betrekking op het opstellen en bijhouden van een nationale vertrouwenslijst door het toezichthoudend orgaan.

De verordening bepaalt dat lidstaten regelgeving kunnen vaststellen over de tijdelijke schorsing van gekwalificeerde certificaten voor gekwalificeerde elektronische handtekeningen en gekwalificeerde elektronische zegels. In de internationale ETSI standaarden wordt de mogelijkheid van het opschorten van certificaten – naast het intrekken- feitelijk nu al geboden, maar het ondersteunen daarvan door gekwalificeerde vertrouwensdienstverleners is optioneel. De gedachte achter het opschorten is dat iemand de status van een certificaat niet vertrouwt en de vertrouwensdienstverlener daarover inlicht. De vertrouwensdienstverlener wil deze melding verifiëren bij de certificaathouder en gedurende die tijd schort de vertrouwensdienstverlener het certificaat op. Wanneer er niets aan de hand blijkt te zijn dan wordt het certificaat weer geldig gemeld en anders definitief ingetrokken. In Nederland wordt van de mogelijkheid tot het opschorten van certificaten geen gebruik gemaakt. Er is geen behoefte om deze lijn te wijzigen. In het (private) programma van eisen PKI-overheid is vastgelegd dat het niet toegestaan is certificaatopschorting te ondersteunen.

5.7 Toezicht

Lidstaten zijn verplicht een toezichthoudend orgaan aan te wijzen. Een toezichthoudend orgaan moet toezien op de naleving van de eisen uit de verordening over vertrouwensdiensten, maar bijvoorbeeld ook de vertrouwenslijst opstellen en bijhouden. De verordening maakt onderscheid in toezicht op niet-gekwalificeerde en gekwalificeerde vertrouwensdiensten. Het toezicht op niet-gekwalificeerde vertrouwensdiensten is beperkt tot het toezicht op de algemene eisen en vindt uitsluitend achteraf plaats in reactie op klachten, kennisgeving, incidenten of in voorkomend geval op basis van eigen onderzoek. Aan deze vorm van beperkt toezicht liggen onder meer overwegingen van uitvoerbaarheid en beperking van administratieve lasten ten grondslag.

Het toezicht op gekwalificeerde verleners van vertrouwensdiensten is zwaarder ingericht. Toezicht vindt vooraf en vervolgens structureel plaats en strekt zich uit tot de specifieke eisen. Voordat een verlener een gekwalificeerde vertrouwensdienst mag verlenen, dient hij het voornemen hiertoe kenbaar te maken aan het toezichthoudend orgaan. Daarbij moet een conformiteitsbeoordelingsverslag worden overgelegd en beoordeelt het toezichthoudend orgaan of de status gekwalificeerd kan worden toegekend. Nadat een gekwalificeerde verlener van vertrouwensdiensten en zijn diensten eenmaal die status heeft, dient de verlener op grond van de verordening verplicht ten minste eens in de 24 maanden een nieuwe conformiteitsbeoordeling laten uitvoeren door een conformiteitsbeoordelingsorgaan. Het toezichthoudend orgaan kan daarnaast zelf ook op elk moment een audit uitvoeren of dit op kosten van de verlener van vertrouwensdiensten laten doen. Indien er door een toezichthoudend orgaan wordt vastgesteld dat de eisen uit de verordening niet worden nageleefd, kan hij herstel daarvan binnen een gestelde termijn vorderen. Indien daaraan geen gevolg wordt gegeven kan dit leiden tot intrekking van de status gekwalificeerd. Indien er sprake blijkt te zijn van een inbreuk op de bescherming van persoonsgegevens moet de nationale gegevensbeschermingsautoriteit hierover worden geïnformeerd. Een inbreuk met mogelijk grensoverschrijdende gevolgen moet aan het betreffende land en het Europees Agentschap voor Informatieveiligheid (ENISA) worden gemeld.

Toezichthoudende organen zijn onder voorwaarden verplicht op verzoek bijstand aan elkaar te verlenen, in het bijzonder door uitwisseling van informatie. Het is mogelijk dat toezichthouders uit verschillende landen samenwerken bij een inbreuk met grensoverschrijdende gevolgen door middel van de uitvoering van een gezamenlijk onderzoek.

De lidstaten zijn verplicht voorschriften vast te stellen inzake de sancties die van toepassing zijn op inbreuken op de verordening en daarmee ook ten aanzien van vertrouwensdiensten. De vastgestelde sancties moeten doeltreffend, evenredig en afschrikkend zijn.

5.8 Uitvoeringsmaatregelen

Het toezicht op gekwalificeerde certificaten voor elektronische handtekeningen wordt momenteel op grond van de Telecommunicatiewet uitgevoerd door de Autoriteit Consument en Markt (hierna: ACM). Zoals hiervoor is toegelicht biedt de verordening in tegenstelling tot de richtlijn geen basis meer voor vrijwillige conformiteitsbeoordeling met toekenning van een wettelijk vermoeden dat aan eisen is voldaan. Dit heeft gevolgen voor de positie van het TTP.NL-schema dat momenteel als beoordelingsschema wordt gebruikt door (geaccrediteerde) instanties. Daarbij is door het incident met DigiNotar in 2011 duidelijk geworden dat structurele aanpassingen in het toezicht gewenst en nodig zijn. De Onderzoeksraad voor Veiligheid heeft in zijn onderzoeksrapport naar aanleiding van het incident met DigiNotar de huidige toezichtconstructie onverantwoord genoemd. Een aanbeveling van de Onderzoeksraad voor Veiligheid aan de Minister van Economische Zaken was om de rol van de toezichthouder aan te passen zodat er meer sprake is van daadwerkelijk toezicht. Concreet krijgt de opvolging van deze aanbeveling gestalte door het loslaten van het wettelijk geregelde vermoeden van overeenstemming (artikel 18.16a Tw). Het oordeel of al dan niet aan de eisen uit de verordening wordt voldaan is aan de toezichthouder en kan niet louter op een verslag van een conformiteitsbeoordelingsinstantie worden gebaseerd. Periodieke conformiteitsbeoordeling blijft niettemin een belangrijke rol spelen bij de uitoefening van het toezicht en is daarom verplicht gesteld in de verordening. De audit dient door een conformiteitsbeoordelingsinstantie te worden verricht en binnen drie werkdagen na afronding daarvan door de gekwalificeerde verlener van vertrouwensdiensten aan het toezichthoudend orgaan te worden verstrekt. De conformiteitbeoordelingsinstantie heeft daarbij een andere rol en verantwoordelijkheid dan de toezichthouder. De conformiteitbeoordelingsinstantie is geen verlengstuk van de toezichthouder en de audit is geen vervanging van het toezicht en de eigen oordeelsvorming van de toezichthouder. Het betekent ook dat niet de conformiteitsbeoordelingsinstantie, maar de toezichthouder bestuursorgaan is dat besluiten neemt over toelating en handhaving. Als de toezichthouder zich bijvoorbeeld voor een besluit mede baseert op de inhoud van een conformiteitsbeoordelingsverslag en de vertrouwensdienstverlener de inhoud daarvan in bezwaar of beroep ter discussie stelt, dient de toezichthouder zich hierover een zelfstandig oordeel te vormen.

De mate waarin voor het toezicht betekenisvolle conformiteitsbeoordelingsverslagen worden overlegd is mede afhankelijk van de nadere uitwerking van de verplichte conformiteitsbeoordeling en de normen waarop deze is gebaseerd. Nu is nog niet duidelijk welke vorm van conformiteitsbeoordeling, certificatie of keuring, er in Europees verband gekozen zal worden. In opdracht van de Europese Commissie wordt gewerkt aan een conformiteitbeoordelingsschema voor de verordening. Het gebruik van dit schema zal niet verplicht zijn. Er is niet voor gekozen op nationaal niveau de minister de bevoegdheid te geven een door de markt aangeboden conformiteitsbeoordelingsschema aan te wijzen. Een dergelijke aanwijzing is alleen zinvol, indien daaraan enig wettelijk vermoeden van overeenstemming kan worden ontleend. Een wettelijk vermoeden betreffende het voldoen aan eisen uit de verordening of het op juiste wijze beoordelen op het voldoen aan de eisen daaruit zou echter de mogelijkheden voor het uitoefenen van daadwerkelijk toezicht door de toezichthouder belemmeren. Dat wordt niet wenselijk geacht. De beheerder van het conformiteitbeoordelingschema en het conformiteitsbeoordelingsorgaan zijn ervoor verantwoordelijk dat het schema en het daarop gebaseerde conformiteitsbeoordelingsverslag een volledige toetsing van de eisen van de verordening inhouden. Voor de toezichthouder moet de waarde van het verslag duidelijk zijn, zodat daarmee rekening kan worden gehouden bij de uitoefening van het toezicht. Dubbele lasten door dubbele toetsing van normen moet worden voorkomen en tegelijkertijd moet het toezicht voldoende zijn om de naleving van wet- en regelgeving effectief te borgen. Daarbij heeft de toezichthouder op grond van de verordening de bevoegdheid om ten allen tijde zelf een audit uit te voeren. Wanneer de toezichthouder dit nodig acht, zal die van deze mogelijkheid gebruik maken.

Aanpassingen in de structuur hebben ook tot heroverweging van de belegging van het toezicht geleid. Het toezicht op gekwalificeerde certificaten voor de elektronische handtekening is een taak van ACM, die tamelijk los van zijn overige activiteiten op het terrein van telecommunicatie staat. Die taak is bij de implementatie van de Richtlijn elektronische handtekeningen destijds bij de Onafhankelijke Post en Telecommunicatie Autoriteit belegd waarbij een beperkte vorm van markttoezicht uitgangspunt was

en waaraan in sterke mate invulling werd gegeven door de TTP-certificering. De meer centrale positie die in de verordening aan de uitoefening van toezicht op (gekwalificeerde) vertrouwensdiensten is toebedeeld, vereist een verschuiving naar meer inhoudelijk toezicht en minder accent op toezicht dat uitsluitend procesmatig of in tweede instantie is. De ervaringen met het incident DigiNotar benadrukken de noodzaak hiervan. Een meer inhoudelijke en proactieve vorm van toezicht op het gebied van vertrouwensdiensten sluit beter aan bij de bestaande kennis, expertise en andere taken van Agentschap Telecom, een dienstonderdeel van het Ministerie van Economische Zaken. De werkzaamheden van het Agentschap in het kader van toezicht zijn vaak al gericht op specifieke technische beoordelingen –en processen, certificering, middelen/apparaten. Agentschap Telecom is bereid om hierin actief en snel te investeren. In het wetsvoorstel zijn bepalingen opgenomen die de Minister van Economische Zaken aanwijzen als toezichthoudend orgaan in de zin van de verordening, waarbij voorts is bepaald dat met het toezicht worden belast de door Minister daartoe bij besluit aangewezen ambtenaren. Deze aan te wijzen ambtenaren van Agentschap Telecom beschikken over de bevoegdheden, waarover zij ook voor andere toezichtstaken beschikken, zoals het opleggen van een boete en, indien aan de daaraan gestelde voorwaarden is voldaan, de toepassing van bestuursdwang. Voorts voorziet het wetsvoorstel in bepalingen betreffende bescherming van gegevens, indien in het kader van het verplicht verlenen van bijstand gegevens worden uitgewisseld met een toezichthoudend orgaan in een andere lidstaat die betrekking hebben op een verlener van vertrouwensdiensten of zijn vertrouwensdiensten. Een lidstaat kan voorts ervoor kiezen te bepalen onder welke voorwaarden het eigen toezichthoudend orgaan gezamenlijk met een toezichthoudend orgaan uit een andere lidstaat onderzoek kan doen naar bijvoorbeeld een grensoverschrijdend incident. Gelet op het belang van grensoverschrijdend toezicht op vertrouwensdiensten, is in het wetsvoorstel voorzien onder welke voorwaarden dit mogelijk is.

Een inhoudelijker benadering van de uitoefening van toezicht door de toezichthouder laat onverlet dat de verordening de inzet van geaccrediteerde conformiteitsbeoordelingsorganen voorschrijft (artikel 20, eerste lid verordening). Daarbij is van belang op welke wijze de expertise van conformiteitsbeoordelingsorganen wordt ingezet. Een goede motivering in een verslaglegging die inzicht biedt in de wijze waarop een beoordeling tot stand is gekomen, biedt meer aanknopingspunten om tot zelfstandige oordeelsvorming op basis van een verslag te komen dan een verslag waarin dit ontbreekt (zie het Onderzoeksrapport van de Raad voor de Veiligheid, het DigiNotarincident, Waarom digitale veiligheid de bestuurstafel te weinig bereikt, 2012). De mate waarin voor het toezicht betekenisvolle conformiteitsbeoordelingsverslagen worden overgelegd, is mede afhankelijk van de aanwijzing van referentienormen door de Europese Commissie, zowel ten aanzien van accreditatie, auditregels als verslagen. Hierbij kan een conformiteitsbeoordelingsorgaan een audit baseren op een nog te ontwikkelen Europees conformiteitsbeoordelingschema of het TTP-certificatieschema. Indien een schema voldoet aan de door de Europese Commissie aangewezen normen biedt dat voor AT een bepaald inzicht in de kwaliteit daarvan bij de beoordeling of aan de in de verordening gestelde eisen is voldaan. Aangezien ontwikkelingen op het gebied van informatiebeveiliging snel verlopen, is het van belang dat certificatieschema's op basis van ervaringen en inzicht in nieuwe dreigingen worden bijgehouden.

5.9 Aansprakelijkheid

Verleners van vertrouwensdiensten bieden diensten aan die het vertrouwen in het elektronisch verkeer waarborgen. Indien een verlener van vertrouwensdiensten de verplichtingen in de verordening niet of niet volledig naleeft kan dit vertrouwen in gevaar komen of aangetast worden. Het kan tot schade voor anderen leiden. De verordening bevat voorschriften over aansprakelijkheid en bewijslast van verleners van vertrouwensdiensten. Verleners van niet-gekwalificeerde verleners van vertrouwensdiensten zijn aansprakelijk voor opzettelijk of uit onachtzaamheid toegebrachte schade aan een natuurlijke persoon of rechtspersoon die is te wijten aan een verzuim de verplichtingen uit hoofde van deze verordening na te leven. De bewijslast hiervoor ligt bij de natuurlijke persoon of de rechtspersoon. Voor verleners van gekwalificeerde verleners van vertrouwensdiensten gelden andere

aansprakelijkheidsregels. De opzet of nalatigheid van een gekwalificeerde verlener van vertrouwensdiensten wordt vermoed, tenzij die bewijst dat de schade zonder opzet of nalatigheid van zijn kant is ontstaan. Teneinde de beoordeling te vergemakkelijken van het financiële risico dat verleners van vertrouwensdiensten misschien moeten dragen of dat zij zouden moeten dekken met verzekeringspolissen, laat de verordening toe dat verleners van vertrouwensdiensten, onder bepaalde voorwaarden, beperkingen verbinden aan het gebruik van de door hen verleende diensten en dat zij niet aansprakelijk zijn voor schade die het gevolg is van het gebruik van diensten dat deze beperkingen te buiten gaat. De klanten moeten vooraf terdege worden geïnformeerd over de beperkingen. Deze beperkingen moeten herkenbaar zijn voor een derde partij, bijvoorbeeld doordat er informatie over de beperkingen wordt opgenomen in de voorwaarden met betrekking tot de verleende dienst, of via andere herkenbare middelen. Om uitvoering te geven aan deze beginselen, moet deze verordening overeenkomstig de nationale aansprakelijkheidsregels worden toegepast. Daarom laat deze verordening nationale regels inzake bijvoorbeeld de definitie van schade, opzet, nalatigheid, of de toepasselijke procedurele regels, onverlet.

5.10 Uitvoeringsmaatregelen

Het ter implementatie van de Richtlijn elektronische handtekeningen opgenomen artikel 6:196b BW regelt thans de aansprakelijkheid van certificatiedienstverleners die gekwalificeerde certificaten afgegeven aan het publiek. Dit artikel legt op deze dienstverleners een gekwalificeerde schuldaansprakelijkheid met omgekeerde bewijslast (Kamerstukken II 2000/01 27 743, nr. 3, blz. 18). Indien de desbetreffende certificatiedienstverlener aan kan tonen dat hij niet nalatig heeft gehandeld, is die van zijn aansprakelijkheid ontheven. Voor dienstverleners van niet-gekwalificeerde certificaten gelden thans de nationale aansprakelijkheidsregels (het algemene aansprakelijkheidsregime van Boek 6 BW). Daar de verordening de richtlijn intrekt en in artikel 13 eigen regels geeft op het terrein van de aansprakelijkheid, dient artikel 6:196b BW te vervallen.

5.11 Derde landen

In derde landen gevestigde verleners van vertrouwensdiensten kunnen binnen de Europese Unie vertrouwensdiensten verlenen. De verordening bevat geen voorschriften die daar in de weg aan staan. Een vertrouwensdienst verstrekt door een aanbieder uit een derde land wordt rechtens erkend als gelijkwaardig aan een gekwalificeerde vertrouwensdienst verstrekt door gekwalificeerde in de Europese Unie gevestigde verleners van vertrouwensdiensten, indien die vertrouwensdienst wordt erkend op grond van een overeenkomst, gesloten tussen de Europese Unie en het betrokken derde land of een internationale organisatie, overeenkomstig een daartoe in het VWEU vastgestelde procedure (artikel 14 van de verordening). Onderwerp van die overeenkomst dient in het bijzonder te zijn dat de in een derde land gevestigde verleners van vertrouwensdiensten de binnen de Europese Unie geldende voorschriften voor gekwalificeerde verleners van vertrouwensdiensten en hun gekwalificeerde vertrouwensdiensten naleven. Ook het uitgangspunt van de wederkerigheid dient onderdeel van een dergelijke overeenkomst te zijn. Anders dan onder de richtlijn voor gekwalificeerde certificaten wordt in de verordening niet materieel geregeld aan welke eisen een verlener van vertrouwensdienst uit een derde land dient te voldoen om vertrouwensdiensten als gelijkwaardig aan gekwalificeerd te mogen aanbieden binnen de Europese Unie. Onder de verordening zijn de mogelijkheden hiervoor afhankelijk van het sluiten van een overeenkomst met de Europese Unie en van de inhoud daarvan.

5.12 Uitvoeringsmaatregelen

In artikel 3:15b BW is de regeling van de Richtlijn elektronische handtekeningen over het afgeven aan het publiek van gekwalificeerde certificaten door een certificatiedienstverlener gevestigd in een derde land, geïmplementeerd. Dit artikel noemt een aantal situaties waarin erkenning van gekwalificeerde certificaten afgegeven aan het publiek door een certificatiedienstverlener gevestigd in een derde land kan plaatsvinden. Daar de verordening de richtlijn intrekt en, zoals hierboven aangegeven, in artikel

14 regelt dat erkenning plaatsvindt op grond van een overeenkomst tussen de EU en het derde land of internationale organisatie, dient artikel 15b te worden geschrapt.

5.13 Toegankelijkheid voor personen met een handicap

Waar dat haalbaar is, zullen op grond van de verordening vertrouwensdiensten en eindgebruikersproducten die worden gebruikt bij de verlening van deze diensten toegankelijk worden gemaakt voor personen met een handicap. Voor de overheid is het voldoen aan de webrichtlijnen, waar de toegankelijkheid, ook voor mensen met een handicap, wordt geborgd verplicht en valt dit onder het daarin geregelde pas-toe-of leg-uit regime. Voor niet-overheden geldt deze regel niet. Bedrijven zullen het toegankelijk maken van vertrouwensdiensten voor personen met een handicap afwegen tegen bedrijfseconomische belangen. Naarmate de vraag naar toegankelijkheid van vertrouwensdiensten voor personen met een handicap groter wordt, zal de economische haalbaarheid voor specifieke aanpassingen groter zijn. Bedrijven zullen met ontwikkelingen hierin rekening dienen te houden.

6. Rechtsgevolgen en vertrouwensdiensten

6.1 Rechtsgevolgen en bewijs

De verordening bevat voor verschillende vertrouwensdiensten voorschriften over het rechtsgevolg en het gebruik als bewijsmiddel daarvan. Uitgangspunt van die voorschriften is dat het rechtsgevolg van een vertrouwensdienst en de toelaatbaarheid ervan als bewijsmiddel in gerechtelijke procedures niet louter ontkend mag worden op grond van het feit dat die niet aan de eisen voor een gekwalificeerde vertrouwensdienst voldoen. Dit is niet anders dan onder de Richtlijn elektronische handtekeningen. Of enige vertrouwensdienst, daargelaten of die gekwalificeerd is, tot een rechtsgevolg leidt of kan leiden is afhankelijk van nationaal recht (overweging 22). Hierop is een uitzondering. Specifiek voor de gekwalificeerde elektronische handtekening bepaalt de verordening dat die hetzelfde rechtsgevolg heeft als een handgeschreven handtekening (artikel 25, tweede lid, van de verordening). Voor andere elektronische handtekeningen dient het nationaal recht te bepalen welke rechtsgevolgen daaraan verbonden zijn (overweging 49 van de verordening). De verordening heeft het naast rechtsgevolgen ook over de toelaatbaarheid van vertrouwensdiensten als bewijsmiddel in gerechtelijke procedures. Aan verschillende gekwalificeerde vertrouwensdiensten kent de verordening voor bepaalde aspecten daarvan een vermoeden van betrouwbaarheid toe. Dit vermoeden richt zich op de integriteit of juistheid van bepaalde gegevens/functies die een bepaalde vertrouwensdienst biedt. Binnen een gerechtelijke procedure is dat van invloed op de bewijspositie tussen partijen en de bewijskracht van deze gekwalificeerde vertrouwensdiensten. Een rechtens toegekend vermoeden van juistheid en integriteit kan weerlegd worden. Tegenbewijs is dus mogelijk.

6.2 Uitvoeringsmaatregelen

In het BW is een algemene regeling opgenomen over de rechtsgevolgen van elektronische handtekeningen. Het eerste lid van 3:15a BW bepaalt dat een elektronische handtekening dezelfde rechtsgevolgen heeft als een handgeschreven handtekening indien de methode die daarbij is gebruikt voor authentificatie voldoende betrouwbaar is, gelet op het doel waarvoor de elektronische handtekeningen werden gebruikt en op alle overige omstandigheden van het geval. In het tweede lid is het vermoeden van voldoende betrouwbaarheid neergelegd ten aanzien van de gekwalificeerde elektronische handtekening.

Daar de verordening voor de gekwalificeerde handtekening in artikel 25, tweede lid, het rechtsgevolg bepaalt, wordt de huidige regeling in artikel 3:15a over de rechtsgevolgen van de elektronische handtekening beperkt tot de geavanceerde elektronische handtekening of enig andere elektronische handtekening.

Voor andere vertrouwensdiensten dan de elektronische handtekening, te weten de elektronische zegels, tijdstempels en diensten voor elektronische aangetekende bezorging, geldt dat de gekwalificeerde elektronische methode daarvan het vermoeden van integriteit en juistheid oplevert. Voor deze elektronische diensten kent ons nationaal recht geen algemene regeling over rechtsgevolgen of over het vermoeden van integriteit en juistheid. Er hoeft dan ook geen aanpassing van wetgeving plaats te vinden. De verordening vereist voor deze diensten verder geen nadere uitwerking.

7 Erkenning van vertrouwensdiensten

7.1 Erkenning van elektronische handtekeningen en zegels

Het gebruik van een door of namens een openbare instantie aangeboden onlinedienst zoals het doorlopen van een administratieve procedure kan afhankelijk zijn gesteld van ondertekening met een elektronische handtekening (natuurlijke persoon) of het aanmaken van een elektronisch zegel (rechtspersoon). De technische invulling daarvan kan verschillen, doordat in regelgeving of door een openbare instantie zelf daaraan eisen worden gesteld. Indien een openbare instantie om technische of betrouwbaarheidsredenen uitsluitend een specifieke methode accepteert, belemmert dit de grensoverschrijdende toegang tot andere lidstaten. Burgers en bedrijven uit een andere lidstaat beschikken vaak niet over precies die methode die aan alle gestelde vereisten voldoet of het is lastig en wellicht onmogelijk die te verkrijgen. De verordening bepaalt wanneer en welke methodes grensoverschrijdend erkend dienen te worden.

De verplichting tot erkenning is van toepassing op openbare instanties die onlinediensten aanbieden, en die het gebruik daarvan afhankelijk stellen van ondertekening met een geavanceerde elektronische handtekening of het aanmaken met een geavanceerde elektronisch zegel. Deze geavanceerde vertrouwensdiensten dienen aan bepaalde in de verordening gestelde eisen te voldoen. Als voor een onlinedienst een bepaalde geavanceerde elektronische handtekening of elektronisch zegel wordt geëist of voorgeschreven, dient een openbare instantie in ieder geval ook andere geavanceerde handtekeningen en zegels te erkennen die voldoen aan door de Europese Commissie hiertoe op basis van uitvoeringshandelingen vastgestelde formats en alternatieve methodes. Een openbare instantie die online-diensten aanbiedt hoeft niet altijd alle geavanceerde elektronische handtekeningen en zegels te erkennen die aan de door de Commissie vastgestelde formats en technisch specificaties voldoen. Uitgangspunt is dat de erkenning zich niet uitstrekt tot geavanceerde elektronische handtekeningen en zegels met een lagere betrouwbaarheid dan het geëiste of voorgeschreven niveau, waarbij in de verordening hieraan op een specifieke wijze invulling wordt gegeven. Een lidstaat mag verder voor grensoverschrijdend verkeer van openbare instanties die online-diensten aanbieden geen elektronische handtekening van een hoger betrouwbaarheidsniveau dan een gekwalificeerde elektronische handtekening vereisen.

Deze in de verordening gevolgde opzet sluit aan bij de krachtens Richtlijn 2006/123/EG van het Europees Parlement en de Raad van 12 december 2006 betreffende diensten op de interne markt (PbEG L 376, 2006) gevolgde benadering ten aanzien van de afwikkeling van procedures en formaliteiten via het één-loket als bedoeld in die richtlijn waarvoor een elektronische handtekening wordt geëist. Zie hiervoor Besluit nr. 2011/130/EU van de Commissie van 25 februari 2011 tot vaststelling van minimumvoorschriften voor de grensoverschrijdende verwerking van documenten die door de bevoegde autoriteiten elektronisch zijn ondertekend krachtens Richtlijn 2006/123/EG van het Europees Parlement en de Raad betreffende diensten op de interne markt (PbEU L 53), alsmede Beschikking nr. 2009/767/EG van de Europese Commissie van 16 oktober 2009 inzake maatregelen voor een gemakkelijker gebruik van elektronische procedures via het ‘één-loket’ in het kader van Richtlijn nr. 2006/123/EG van het Europees Parlement en de Raad betreffende diensten op de interne markt (PBEU L 274/36). De op grond hiervan vastgestelde formats houden in dat documenten moeten kunnen worden verwerkt die voldoen aan de technische specificaties uit de bijlage van het

eerstgenoemde besluit van de Commissie. Ten tijde van de voorbereiding van dit wetsvoorstel is nog niet bekend in hoeverre hierbij volledig wordt aangesloten.

Een van de eisen die aan een geavanceerde elektronische handtekening wordt gesteld heeft betrekking op de uitsluitende controle van de aanmaakgegevens door de ondertekenaar. In de richtlijn spitst deze eis zich toe op de uitsluitende controle door de ondertekenaar over een middel, zoals een smartcard of token waarin op cryptografie gebaseerde sleutels zijn opgeslagen waarmee een elektronische handtekening kan worden aangemaakt. Dit impliceert dat de controle zich ook mede op het beheer van de drager waarin sleutelgegevens zijn opgeslagen richt. Als gevolg van de ontwikkelingen op internet, zoals cloudoplossingen hoeft de omgeving waarin sleutelgegevens worden bewaard niet altijd onder beheer van de ondertekenaar te staan. Dit kan ook een door een derde partij beheerde omgeving zijn, zoals een informatiesysteem dat elektronisch en op afstand door de ondertekenaar te benaderen is. Het beheer en de controle over de omgeving met de sleutelgegevens verschuift hiermee naar controle op afstand van sleutelgegevens die door een ander worden beheerd. De verordening biedt hiervoor ruimte, maar stelt als voorwaarde voor een geavanceerde elektronische handtekening dat de ondertekenaar de aanmaakgegevens 'met een hoog vertrouwensniveau' onder zijn uitsluitende controle kan gebruiken. In de handreiking Betrouwbaarheidsniveaus voor elektronische overheidsdiensten (versie 3) van het Forum Standaardisatie wordt op verschillende mogelijkheden nader ingegaan.

7.2 Uitvoeringsmaatregelen

In 2011 is ter uitvoering van het hiervoor aangehaalde Besluit 2011/130/EU een voorziening gerealiseerd die bevoegde instanties als bedoeld in de Dienstenwet onder meer in staat stelt elektronische handtekeningen die aan de in dat besluit gestelde standaarden voldoet te kunnen valideren. Die voorziening is ondergebracht bij het digitaal Ondernemersplein. Als gevolg van de verordening zullen openbare instanties in voorkomend geval tot erkenning moeten overgaan ten aanzien van verkeer dat langs andere kanalen dan via het digitaal Ondernemersplein wordt afgewikkeld en strekt erkenning zich ook uit tot elektronische zegels. Afhankelijk van de door de Europese Commissie op grond van de verordening vast te stellen formats en andere methodes waaraan geavanceerde elektronische handtekeningen en zegels voor erkenning dienen te voldoen, zal de huidige voorziening daarmee in overeenstemming worden gebracht. Het voornemen is openbare instanties die het aangaat op deze wijze te faciliteren bij het kunnen voldoen aan de verplichtingen in de verordening over erkenning van de bedoelde vertrouwensdiensten. Dit laat onverlet dat openbare instanties zelf verantwoordelijk zijn voor de naleving van de verplichtingen inzake erkenning. Afhankelijk van de wijze waarop de bestaande voorziening wordt aangepast en gepositioneerd, kan dit inhouden dat een openbare instantie met een onlinedienst waarvoor een geavanceerde elektronische handtekening of zegel is vereist van die voorziening gebruik kan maken om aan de verordening te kunnen voldoen. Op de naleving van de verplichtingen inzake de erkenning van genoemde elektronische handtekeningen en zegels is de Wet Naleving Europese regelgeving publieke entiteiten van toepassing.

8. Gegevensbescherming

Op de verwerking van persoonsgegevens is de Wet bescherming persoonsgegevens van toepassing. De verordening bevestigt dat in overeenstemming hiermee gehandeld dient te worden. Persoonsgegevens worden verwerkt bij het gebruik van het koppelpunt dat grensoverschrijdende authenticatie in het online-verkeer met openbare instanties mogelijk moet maken. Via dat koppelpunt worden persoonsidentificatiegegevens vanuit andere lidstaten omgezet naar gegevens die leesbaar zijn voor in Nederland aanwezige openbare instanties en andersom. De inhoud van een minimale set aan gegevens voor grensoverschrijdend gebruik van elektronische identiteiten, wordt door de Europese Commissie in een uitvoeringshandeling op grond van de verordening vastgesteld. De gegevens van natuurlijke personen die het koppelpunt moet verwerken zijn naar verwachting de voor- en achternaam, geboortedatum en een uniek identificeerbaar nummer. Dit unieke nummer bestaat uit

de landcode van de Lidstaat van herkomst, de landcode van de Lidstaat van bestemming, gevolgd door een aantal leesbare karakters. Dit nummer kan per transactie verschillen en is géén Europees uniek identificerend persoonsnummer. Daarnaast zal de uitvoeringshandeling het naar verwachting mogelijk maken aanvullende gegevens van de natuurlijke persoon met de minimale dataset mee te sturen, te weten voor- en achternaam bij geboorte, geboorteplaats, huidige adres en geslacht. Voor rechtspersonen zijn de minimale gegevens de huidige wettelijke naam en een uniek identificerend nummer. Op vrijwillige basis kunnen rechtspersonen aanvullende gegevens meesturen zoals het huidige adres en het fiscaal nummer.

De openbare instantie die een dienst elektronisch verleent, is gerechtigd aanvullende gegevens te vragen om te bepalen of een ingezetene binnen de Europese Unie daadwerkelijk recht heeft om de dienst af te nemen. Deze aanvullende gegevens worden alleen verzonden na toestemming van de gebruiker. Dit laat onverlet dat, indien gegevens niet behorend tot de genoemde verplichte of aanvullende set van gegevens, het mogelijk is andersoortige gegevens buiten het koppelpunt om aan de desbetreffende overheidsdienst aan te leveren.

Net als bij elektronische identiteiten worden bij vertrouwensdiensten persoonsgegevens verwerkt. Tijdens de registratiefase legt de vertrouwensdienstverlener persoonsgegevens van de gebruiker met de uitdrukkelijke toestemming van die gebruiker vast. De vertrouwensdienstverlener is hierbij verantwoordelijke in de zin van artikel 1 sub d, van de Wet bescherming persoonsgegevens. Het gaat hierbij om een minimale gegevensset waaruit blijkt aan wie de vertrouwensdienst wordt verleend. Bij persoonsgebonden vertrouwensdiensten, zoals een elektronische handtekening, verstrekt de gebruiker zelf persoonsgegevens aan de ontvangende partij. Het gaat daarbij om minimale gegevens, zoals de voor- en achternaam. Daardoor weet de ontvangende partij wie de handtekening heeft gezet. Indien er aanwijzingen zijn voor een inbreuk op de bescherming van persoonsgegevens bij het verlenen van vertrouwensdiensten door een gekwalificeerde verlener van vertrouwensdiensten, brengt Agentschap Telecom het Cbp op de hoogte van de resultaten van de audits die ten aanzien van die verlener en zijn diensten zijn uitgevoerd. De bevoegdheid en verplichting hiertoe volgt uit de rechtstreekse werking van artikel 17, vierde lid, onderdeel f, van de verordening. Een vertrouwensdienstverlener moet zelf de gegevensbeschermingsautoriteit op de hoogte stellen van een veiligheidsinbreuk of integriteitsverlies met aanzienlijke gevolgen voor de persoonsgegevens die daarmee worden beheerd. En als de inbreuk of het verlies naar verwachting negatieve gevolgen zal hebben voor een natuurlijke persoon of een rechtspersoon aan wie een vertrouwensdienst is verleend, dan moet die eveneens worden geïnformeerd.

PM De 'Privacy impact assesment' landelijk koppelpunt is nog in voorbereiding en de resultaten daarvan zullen na de consultatie worden verwerkt.

9. Aanpassingen in andere wetgeving en overgangsrecht

9.1 Aanpassingen in andere wetgeving

In een aantal bepalingen in de wetgeving wordt verwezen naar de handtekening die voldoet aan de eisen van (het eerste en) tweede lid van artikel 3:15a BW (de eisen die worden gesteld aan de gekwalificeerde handtekening) en naar artikel 3:15b BW (afgeven van gekwalificeerde certificaten door dienstverleners uit derde landen. Deze bepalingen dienen te worden aangepast. Verwezen dient te worden naar de gekwalificeerde elektronische handtekening van artikel 3, onderdeel 12, van de verordening. De verwijzing naar het in dit wetsvoorstel geschrapte artikel 15b dient te vervallen. Het betreft aanpassingen in Boek 7 van het Burgerlijk Wetboek, het Wetboek van Burgerlijke Rechtsvordering, de Kadasterwet, de Wet handhaving consumentenbescherming en de Wet op de omzetbelasting 1968.

9.2 Overgangsrecht

De verordening bevat overgangsrechtelijke voorschriften voor veilige middelen als bedoeld in de Richtlijn elektronische handtekeningen en voor gekwalificeerde certificaten als bedoeld in die richtlijn (artikel 51 van de verordening). Veilige middelen die door een door de Minister van Economische Zaken onder de huidige Telecommunicatiewet aangewezen instelling op overeenstemming met daaraan bij en krachtens de wet gestelde eisen zijn beoordeeld, worden als gekwalificeerde middelen voor het aanmaken van elektronische handtekeningen in de zin van de verordening aangemerkt. En gekwalificeerde certificaten die zijn afgegeven door een certificatiedienstverlener met inachtneming van het bepaalde bij en krachtens de huidige Telecommunicatiewet worden aangemerkt als gekwalificeerde certificaten voor elektronische handtekeningen in de zin van de verordening.
Voor certificatiedienstverleners die onder de huidige wet gekwalificeerde certificaten afgeven geldt op grond van de verordening vanaf 1 juli 2016 een specifiek overgangsregime. Zij worden tijdelijk aangemerkt als gekwalificeerde verleners van vertrouwensdiensten in de zin van de verordening. Deze status geldt minimaal totdat de dienstverlener een conformiteitsbeoordelingsverslag heeft ingediend dat door het door de lidstaat aangewezen toezichthoudend orgaan is beoordeeld. Dat verslag dient zo spoedig mogelijk doch uiterlijk 1 juli 2017 te worden ingediend. Wordt een conformiteitsbeoordelingsverslag niet tijdig overgelegd, dan wordt de aanbieder op grond van de verordening vanaf 2 juli 2017 niet langer beschouwd als gekwalificeerde verlener van vertrouwensdiensten in de zin van de verordening. De verlener beschikt dan van rechtswege niet langer over de status gekwalificeerd voor hemzelf en zijn diensten en de registratie op de vertrouwenslijst van de desbetreffende verlener van vertrouwensdiensten zal dan door het toezichthoudend orgaan ongedaan worden gemaakt. Is de uitkomst van de beoordeling van een tijdig ingediend verslag positief dan wordt de status van gekwalificeerde verlener van vertrouwensdiensten voor het verlenen van gekwalificeerde certificaten voor elektronische handtekeningen aan het publiek gehandhaafd. Totdat een tijdig ingediend verslag door het toezichthoudend orgaan is beoordeeld, is niet integraal vastgesteld dat de verlener daadwerkelijk voldoet aan de eisen die de verordening stelt aan gekwalificeerde verleners van vertrouwensdiensten en aan het verlenen van gekwalificeerde certificaten voor elektronische handtekeningen. Dat neemt niet weg dat zij als gekwalificeerde verleners van vertrouwensdiensten zijn aangemerkt, zodat de verordening op hen van toepassing is vanaf 1 juli 2016. Dat geldt ook voor dit wetsvoorstel als het tot wet is verheven en in werking is getreden. Dit betekent dat certificatiedienstverleners vanaf 1 juli 2016 aan de bij en krachtens de verordening gestelde eisen moeten voldoen, met dien verstande dat zij een overgangsperiode hebben ten aanzien van het indienen van het conformiteitsbeoordelingsverslag. Indien een gekwalificeerde verlener van vertrouwensdiensten die voorheen een certificatiedienstverlener was aan bepaalde eisen die bij of krachtens de verordening of dit wetsvoorstel niet voldoet, dan kan de toezichthouder in het kader van de handhaving van de naleving van die eisen daartegen optreden met inachtneming van hetgeen daaromtrent in de verordening en het wetsvoorstel is bepaald.

10. Administratieve lasten en verdere effecten voor het bedrijfsleven

De bepalingen uit de verordening kunnen gevolgen hebben voor de administratieve lasten van aanbieders van vertrouwensdiensten. Voor aanbieders van niet-gekwalificeerde vertrouwensdiensten betekent de verordening een lichte stijging van de toezichtslasten. Deze lasten treden voor de niet-gekwalificeerde aanbieders alleen op wanneer er sprake is van een vertrouwensinbreuk of integriteitsverlies bij een aanbieder. Voor aanbieders van gekwalificeerde vertrouwensdiensten betekent de verordening eveneens een stijging van administratieve lasten als gevolg van de verbreding van de scope van de verordening, de vertrouwenslijst en de meldplicht.

10.1 Elektronische identiteiten

De verplichte erkenning van elektronische identiteiten uit andere lidstaten geldt alleen voor openbare instanties in de publieke sector. De private sector kan zich aansluiten maar is dat niet verplicht. Om met elektronische identiteiten van burgers en bedrijven uit andere lidstaten om te kunnen gaan, is aansluiting op koppelpunt dat inkomende en uitgaande authenticatie regelt nodig. Dit koppelpunt zal

worden aangesloten op de Nederlandse infrastructuur van elektronische identiteiten (eID-structuur). Op deze wijze wordt voorkomen dat openbare instanties en gebruikers uit de private sector aparte aansluitingen nodig hebben voor Nederlandse elektronische identiteiten en elektronische identiteiten uit andere lidstaten. Aansluiting van de private sector op de Nederlandse eID-infrastructuur is vrijwillig en gebeurt door een contract af te sluiten met een zogeheten herkenningsmakelaar. Het gaat hier om een contract met een privaat bedrijf. Daarnaast dient een zogeheten koppelvlak te worden gerealiseerd voor technische aansluiting. Private partijen zullen waarschijnlijk in eerste instantie op het eID-stelsel aansluiten om Nederlandse burgers en bedrijven te kunnen authentiseren. Via deze aansluiting op het eID-stelsel kan ook het berichtenverkeer van elektronische identiteiten van inwoners en bedrijven uit andere lidstaten worden afgehandeld. Dit veroorzaakt geen extra administratieve lasten of nalevingskosten.

10.2 Vertrouwensdiensten

De verordening maakt grensoverschrijdend gebruik van elektronische handtekeningen, -zegels, -tijdstempels, -diensten voor elektronisch aangetekende bezorging en certificaten voor websiteauthenticatie mogelijk, maar verplicht Nederlandse burgers of bedrijven niet tot aanschaf of tot het gebruik van deze vertrouwensdiensten. De aanbieder van een elektronische dienst of proces bepaalt of hierbij gebruik moet worden gemaakt van een elektronische handtekening, -zegel, tijdstempel, dienst voor aangetekende elektronische bezorging. De verordening bepaalt alleen dat gelijkwaardige elektronische handtekeningen, -zegels, -tijdstempels, en diensten voor aangetekende elektronische bezorging uit andere lidstaten ook moeten worden geaccepteerd. Het ontvangen van een elektronische handtekening, -zegel, -tijdststempel, dienst voor aangetekende bezorging of gebruik van een certificaat voor authenticatie van websites veroorzaakt in de regel geen extra lasten of nalevingskosten. De controle van de vertrouwensdienst verloopt meestal automatisch. Indien een ontvanger dit wenst kan hij extra controles uitvoeren, bijvoorbeeld door het gebruik van valideringsdiensten. Valideringsdiensten controleren vertrouwensdiensten op een aantal extra kenmerken waardoor extra zekerheid kan worden verkregen.

10.3 Toezichtlasten

Voor verleners van niet-gekwalificeerde vertrouwensdiensten is er sprake van stijging van lasten vanuit het nieuwe Europeesrechtelijk kader, omdat deze diensten tot nu toe niet gereguleerd zijn. De toezichtlasten vanuit de verordening worden veroorzaakt door de meldplicht bij veiligheidsinbreuken en integriteitsverlies. De hoogte van deze lasten zal samenhangen met de ernst van de inbreuk en zijn moeilijk van tevoren in te schatten. Bij een lichte inbreuk is het wellicht voldoende om de toezichthouder te informeren over de corrigerende maatregelen en zijn de lasten nihil. Een ernstige inbreuk zal gepaard gaan met hogere lasten, niet alleen door intensieve betrokkenheid van de toezichthouder, maar ook over het informeren van de klanten en het publiek.

Verleners van gekwalificeerde vertrouwensdiensten krijgen eveneens te maken met stijgende toezichtlasten. Deze worden veroorzaakt doordat de verordening meer diensten reguleert dan de Richtlijn elektronische Handtekeningen en doordat de verordening nieuwe verplichtingen introduceert. De verordening bevat een aantal verplichtingen, zoals verplichte toetsing vooraf door de toezichthouder, de periodieke conformiteitbeoordeling en meldplicht bij veiligheidsinbreuken. Daarnaast kan de toezichthouder zelf een conformiteitbeoordeling uitvoeren, vragen stellen of een controle ter plaatse uitvoeren. De tijd die de aanbieder van gekwalificeerde vertrouwensdiensten kwijt is aan registratie, de periodieke conformiteitbeoordelingen, meldingen van veiligheidsinbreuken, de periodieke bedrijfsbezoeken, meldingen van veiligheidsinbreuken en periodieke bedrijfsbezoeken, telt als administratieve lasten. Echter gelet op de huidige invulling het wettelijk kader door certificering bestonden deze lasten al voor aanbieders van gekwalificeerde elektronische handtekeningen. In de praktijk is de huidige vrijwillige accreditatieregeling dusdanig ingevuld dat voor TTP-certificatie een jaarlijkse audit bij de aanbieders van gekwalificeerde elektronische handtekeningen nodig is. Deze audit moet momenteel ook al aan de toezichthouder worden verstrekt. Daarnaast geldt voor

aanbieders van gekwalificeerde elektronische handtekeningen op grond van de Telecommunicatiewet nu reeds een registratieplicht. Het Besluit Elektronische handtekeningen kent bovendien een meldplicht voor veiligheidsinbreuken en integriteitsverlies bij gekwalificeerde elektronische handtekeningen. Tot slot legde de toezichthouder onder het huidige wettelijke regime ook bedrijfsbezoeken af. Gekwalificeerde elektronische zegels, -tijdstempels, diensten van aangetekende elektronische bezorging en certificaten voor de authenticatie van websites zijn tot nu toe niet gereguleerd. Doordat deze onder de verordening komen te vallen, wordt het toezichtregime van toepassing. Dit betekent voor de aanbieders van deze diensten administratieve lasten die men tot nu toe niet heeft. Deze lasten worden, net als bij de gekwalificeerde elektronische handtekening, veroorzaakt door toetsing van de toezichthouder voordat de dienst mag worden verleend, periodieke conformiteitbeoordelingen, de vertrouwenslijst en de melding van veiligheidsinbreuken. In Nederland zijn er momenteel vier private partijen die gekwalificeerde vertrouwensdiensten leveren en drie overheidsorganisaties. Op dit moment is niet bekend in hoeverre deze partijen gekwalificeerde diensten, naast de elektronische handtekening, gaan aanbieden. Daarnaast wordt het toezichtinstrumentarium voor de nieuwe vertrouwensdiensten nog ingericht. Hierdoor is een kwantitatieve onderbouwing van de stijging van de lasten nog niet mogelijk.

11. Financiële gevolgen voor medeoverheden

Gemeenten en provincies moeten hun technische en organisatorische processen zodanig aanpassen dat het mogelijk is dat een burger/bedrijf zich met een elektronisch identificatiemiddel uit een andere lidstaat kan authentiseren bij een onlinedienst die voor hen toegankelijk is. Zoals in paragraaf 2 is uiteengezet, regelt de verordening niet de feitelijke toegang tot onlinediensten. De kosten voor het toegankelijk maken van processen worden dan ook niet veroorzaakt door de verordening en kunnen hier niet aan worden toegerekend. Uit onderzoek (Financiële gevolgen Europese verordening elektronische identiteiten en vertrouwensdiensten voor medeoverheden, Ecorys, 2013) blijkt dat de financiële gevolgen voor gemeenten en overheden afhangen van het implementatiescenario dat wordt gekozen. Er wordt gekozen om het berichtenverkeer, dat samenhangt met grensoverschrijdende authenticatie, af te handelen via de reeds aanwezige voorzieningen van het toekomstige eID-stelsel. Concreet betekent dit dat het koppelpunt dat het grensoverschrijdend berichtenverkeer regelt, wordt aangesloten op de zogeheten herkenningsmakelaar. Aangezien gemeenten en provincies op het in ontwikkeling zijn eID-stelsel zullen aansluiten om te kunnen werken met Nederlandse elektronische identiteiten, zullen de financiële gevolgen voor het kunnen authenticeren van burgers en bedrijven uit andere lidstaten gering zijn. Het onderzoek wijst uit dat het gaat om eenmalige kosten ter hoogte van ongeveer driehonderdduizend Euro en jaarlijkse kosten die minder dan honderdduizend Euro voor alle gemeenten en provincies bedragen. Conform de verplichtingen uit de Financiële Verhoudingswet zal het Ministerie van Economische Zaken deze kosten in 2018 via het Gemeente- en Provinciefonds compenseren. Vanaf september 2018 is erkenning van elektronische identiteiten uit andere lidstaten namelijk verplicht.

12. Uitvoeringstoets, consultatie (en adviezen)

Paragraaf over notificatie wordt ingevoegd na consultatie ivm met eventuele wijzigingen nav consultatie.

II. ARTIKELEN

Onderdeel A, artikel 1.1, onderdeel ss
Voor de toepassing van het wetsvoorstel betreft het begrip vertrouwensdienst een belangrijk begrip. De definitie verwijst voor de omschrijving daarvan naar de eidas-verordening (artikel 3, onderdeel 16, van de verordening). Een vertrouwensdienst is volgens de verordening een elektronische dienst die gewoonlijk tegen betaling wordt verricht en het onderstaande inhoudt:

a) het aanmaken, verifiëren en valideren van elektronische handtekeningen, elektronische zegels of elektronische tijdstempels, diensten voor elektronisch aangetekende bezorging en op deze diensten betrekking hebbende certificaten, of
b) het aanmaken, verifiëren en valideren van certificaten voor authenticatie van websites, of
c) het bewaren van elektronische handtekeningen, zegels of certificaten die op deze diensten betrekking hebben.
In paragraaf 2.2 van het algemeen deel van de toelichting zijn kenmerken van verschillende vertrouwensdiensten nader toegelicht.

Onderdeel A, artikel 1.1, onderdeel tt
De verordening maakt onderscheid tussen gekwalificeerde en niet-gekwalificeerde vertrouwensdiensten. Aan gekwalificeerde vertrouwensdiensten kan door de daaraan in de verordening gestelde eisen een hoog niveau van betrouwbaarheid worden toegekend. Voor niet-gekwalificeerde vertrouwensdiensten kan het niveau van betrouwbaarheid verschillend zijn.

Onderdeel A, artikel 1.1, onderdeel uu
De verlener van een vertrouwensdienst is in het wetsvoorstel gedefinieerd door te verwijzen naar de definitie die daarvan in de verordening wordt gegeven (artikel 3, onder 19, van de verordening). Het betreft een natuurlijke persoon of rechtspersoon die een of meer vertrouwensdiensten verleent.

Onderdeel A, artikel 1.1, onderdeel vv
Een gekwalificeerde verlener van vertrouwensdiensten als bedoeld in het wetvoorstel wordt in de verordening gedefinieerd als: een verlener van vertrouwensdiensten die één of meerdere gekwalificeerde vertrouwensdiensten verleent en van het toezichthoudende orgaan de status van gekwalificeerde heeft gekregen (artikel 3, onderdeel 20, van de eidas-verordening). Het is met andere woorden niet voldoende dat de verlener van vertrouwensdiensten feitelijk voldoet aan de gestelde eisen, maar noodzakelijk is ook dat de status gekwalificeerd door het toezichthoudend orgaan is toegekend. De eisen die in de verordening aan een gekwalificeerde verlener van vertrouwensdiensten worden gesteld, zijn gericht op het waarborgen van de betrouwbaarheid van een dergelijke verlener.

Onderdeel A, artikel 1.1, onderdelen ww
Evenals er gekwalificeerde vertrouwensdiensten zijn, zijn er ook gekwalificeerde certificaten. Het begrip gekwalificeerd certificaat wordt in de verordening als verzamelnaam gebruikt voor gekwalificeerde certificaten voor elektronische handtekeningen, voor elektronische zegels en voor websiteauthenticatie (artikel 3, onderdelen 15, 30 en 39). Een vertrouwensdienst waarvan een gekwalificeerd certificaat deel uitmaakt draagt bij aan een hogere betrouwbaarheid van die vertrouwensdienst.

Onderdeel A, artikel 1.1, onderdeel xx
In Verordening (EG) nr. 765/2008 van het Europees Parlement en de Raad van 9 juli 2008 tot vaststelling van de eisen inzake accreditatie en markttoezicht betreffende het verhandelen van producten en tot intrekking van Verordening (EEG) nr. 339/93 (PbEU 2008, L 218) (hierna verder te noemen: accreditatieverordening) is een conformiteitsbeoordelingsinstantie een instantie die conformiteitsbeoordelingsactiviteiten verricht, zoals onder meer ijken, testen, certificeren en inspecteren. In de eidas-verordening dient een dergelijke instantie geaccrediteerd te zijn om een conformiteitsbeoordeling te verrichten van een gekwalificeerde verlener van vertrouwensdiensten en van de door hem verleende vertrouwensdiensten (artikel 3, onder 18, van de eidas-verordening). De accreditatie dient hierop betrekking te hebben. Daarvoor is nodig dat een nationale accreditatie-instantie op verzoek van een conformiteitsbeoordelingsinstantie beoordeelt of deze bekwaam is dit soort conformiteitsbeoordelingsactiviteiten uit te voeren. Wanneer zij bekwaam wordt bevonden, geeft de nationale accreditatie-instantie daartoe een accreditatiecertificaat af. In de Wet aanwijzing nationale accreditatie-instantie is voor Nederland de Raad voor Accreditatie als nationale accreditatie-instantie aangewezen.

Onderdeel A, artikel 1.1, onderdeel yy
In de verordening wordt het begrip gekwalificeerd middel voor het aanmaken van elektronische handtekeningen gedefinieerd. Ditzelfde geldt voor het begrip gekwalificeerd middel voor het aanmaken van elektronische zegels. In het wetsvoorstel worden deze begrippen telkens in samenhang gebruikt, zodat die in een gezamenlijk begrip zijn ondergebracht. Het onderscheidende bestanddeel 'middel voor het aanmaken van elektronische handtekeningen' respectievelijk 'middel voor het aanmaken van elektronische zegels' is in de verordening afzonderlijk gedefinieerd. Het dient te gaan om geconfigureerde software of hardware die wordt gebruikt om een elektronische handtekening of elektronisch zegel aan te maken, zoals een smartcard of een token (artikel 3, onder 22 en onder 31, van de verordening). Indien een dergelijk middel voldoet aan daaraan in de verordening gestelde eisen die op de betrouwbaarheid van dat middel betrekking hebben, is sprake van een gekwalificeerd middel (artikel 3, onder 23 en onder 32, van de verordening). Het aanbieden van gekwalificeerde middelen is alleen toegestaan door daartoe gecertificeerde aanbieders.

Onderdeel A, artikel 1.1, onderdeel lll
Ieder lidstaat van de Europese Unie dient een toezichthoudend orgaan als bedoeld in de verordening aan te wijzen voor de in de eigen lidstaat gevestigde verleners van vertrouwensdiensten. De taken van een toezichthoudend orgaan staan in de verordening opgesomd (artikel 17, van de verordening). Die taken beperken zich niet tot het terrein van toezicht op de naleving van de eisen uit de verordening. Dit omvat onder meer ook het verlenen van bijstand aan toezichthoudende organen uit andere lidstaten en het beoordelen of de status gekwalificeerd aan een verlener van vertrouwensdiensten en zijn vertrouwensdiensten kan worden toegekend. Elders in dit wetsvoorstel wordt de Minister van Economische Zaken aangewezen als toezichthoudend orgaan voor in Nederland gevestigde verleners van vertrouwensdiensten.

Onderdeel A, artikel 1.1, onderdeel mmm
Aan de hand van een vertrouwenslijst is voor het publiek zichtbaar welke gekwalificeerde verleners van vertrouwensdiensten en hun vertrouwensdiensten geregistreerd staan of geregistreerd zijn geweest. Een lidstaat dient een vertrouwenslijst op een veilige manier op te stellen, bij te houden en te publiceren (artikel 22 van de verordening). Een vertrouwenslijst wordt met behulp van een digitaal certificaat elektronisch ondertekend of verzegeld. Het begrip vertrouwenslijst is niet nieuw en te herleiden tot beschikking nr. 2009/767/EG van de Europese Commissie van 16 oktober 2009 inzake maatregelen voor een gemakkelijker gebruik van elektronische procedures via het 'één-loket' in het kader van Richtlijn nr. 2006/123/EG van het Europees Parlement en de Raad betreffende diensten op de interne markt (PbEU L 274/36)). De beschikking verplichtte lidstaten om een menselijk leesbare versie van hun vertrouwenslijst aan te bieden. Er bleek vervolgens onder meer behoefte te bestaan aan een machinaal verwerkbare versie van de vertrouwenslijst en een koppeling tussen vertrouwenslijsten. De Europese Commissie heeft daarop de beschikking gewijzigd (Wijziging van de beschikking één-loket middels het besluit nr. 2010/425/EU van de Europese Commissie van 28 juli 2010 tot wijziging van Beschikking 2009/767/EG wat betreft het opstellen, bijwerken en publiceren van vertrouwenslijsten van certificatiedienstverleners die onder toezicht staan of zijn geaccrediteerd in een lidstaat (PBEU L 199/30)). Naar verwachting zal de Europese Commissie bij het vaststellen van de uitvoeringshandelingen op grond van de eidas-verordening ten aanzien van de vertrouwenslijsten het bepaalde in de aangehaalde beschikkingen als uitgangspunt nemen.

Onderdeel A, artikel 1.1, onderdeel nnn
De term 'eidas-verordening' is een veelvuldig in de praktijk gebruikte en aan de Engelse taal ontleende afkorting van de verordening. In het wetsvoorstel is deze aanduiding van de verordening overgenomen. Op vergelijkbare wijze heeft ook de roaming-verordening in de Telecommunicatiewet een plaats gekregen. De eidas-verordening biedt grondslag voor een groot aantal door de Europese Commissie vast te stellen gedelegeerde handelingen en uitvoeringshandelingen. Indien in het wetsvoorstel wordt verwezen naar de eidas-verordening is dit gelet op de gebruikte definitie daarvan met inbegrip van vastgestelde gedelegeerde handelingen en uitvoeringshandelingen.

Onderdeel B, opschrift paragraaf 2.1
In het wetsvoorstel wordt de verantwoordelijkheid voor de toekenning van de status gekwalificeerd voor vertrouwensdiensten en het opstellen en bijhouden van de vertrouwenslijst gelegd bij de Minister van Economische zaken. Die belast vervolgens ambtenaren van Agentschap Telecom met de uitvoering daarvan. De ACM blijft onverminderd verantwoordelijk voor de registratie en het bijhouden van een register voor het aanbieden van een openbaar elektronisch communicatienetwerk, een openbare elektronische communicatiedienst, dan wel bijbehorende faciliteiten. Door deze verdeling in verantwoordelijkheden en het verschil in voorschriften voor de te onderscheiden activiteiten, is in het wetsvoorstel hoofdstuk 2 van de Telecommunicatiewet opgedeeld in twee paragrafen. De eerste paragraaf heeft betrekking op openbare elektronische communicatienetwerken en –diensten, dan wel bijbehorende faciliteiten. Dit betreft de artikelen 2.1 tot en met 2.5. De tweede paragraaf heeft betrekking op gekwalificeerde vertrouwensdiensten. De artikelen in die paragraaf zijn in het wetsvoorstel nieuw toegevoegd.

Onderdeel C, artikel 2.1
Het huidige vijfde tot en met zevende lid hebben betrekking op diverse aspecten van de aanvraag van een certificatiedienstverlener tot registratie van het mogen aanbieden of afgeven van gekwalificeerde certificaten. Deze leden vervallen als gevolg van de herschikking in paragrafen en de rechtstreekse werking van de verordening. Voor zover dit voor de uitvoering van de verordening noodzakelijk is, zijn voorschriften over de toekenning van de status gekwalificeerd en de vertrouwenslijst onderdeel van de paragraaf over gekwalificeerde vertrouwensdiensten.

Onderdeel D, artikel 2.2
Het huidige tweede tot en met vijfde lid gaan over het weigeren, beëindigen of wijzigen van een registratie betreffende certificatiedienstverleners en gekwalificeerde certificaten. Doordat artikel 2.2 onderdeel is van paragraaf 2.1 van het wetsvoorstel en die paragraaf niet op deze doelgroep betrekking heeft, vervallen in het wetsvoorstel het derde tot en met het vijfde lid. Verder komt het tweede lid anders te luiden. In het tweede lid komt te staan wat nu is bepaald in artikel 2.2, vierde lid, onderdeel a. Daarin staat dat de ACM de registratie eindigt of wijzigt, indien de grond tot registratie is vervallen. Dit voorschrift is ook van betekenis voor aanbieders van openbare elektronische communicatienetwerken en –diensten, of bijbehorende faciliteiten. Te denken valt aan de situatie waarin een aanbieder zijn activiteiten waarop de registratie betrekking heeft uit eigener beweging beëindigt. Voor zover dit voor de uitvoering van de verordening noodzakelijk is, zijn voorschriften in verband met weigering, beëindiging of wijziging van de status gekwalificeerd bij vertrouwensdiensten onderdeel van de nieuwe in te voegen paragraaf over gekwalificeerde vertrouwensdiensten.

Onderdeel E, artikel 2.3
In de hier voorgestelde wijziging worden eerdere wijzigingen van de Telecommunicatiewet tot implementatie van het besluit van de Europese Commissie ter uitvoering van de dienstenrichtlijn over vertrouwenslijsten (zie hiervoor de toelichting bij onderdeel A, onder lll) ongedaan gemaakt. In plaats daarvan worden de vertrouwenslijsten rechtstreeks werkend door de eidas-verordening geregeld. Noodzakelijke voorschriften ten aanzien van de vertrouwenslijst en de verantwoordelijkheid daarvoor zijn, zijn in het wetsvoorstel onderdeel van de nieuwe paragraaf over het verlenen van gekwalificeerde vertrouwensdiensten.

Onderdeel F, Artikel 2.5a
Dit artikel beperkt de toepasselijkheid van de Telecommunicatiewet tot de verlening van vertrouwensdiensten aan samengevat het publiek. Deze beperking sluit aan op het toepassingsbereik van de eidas-verordening voor vertrouwensdiensten. De verordening bepaalt dat die zich niet uitstrekt tot vertrouwensdiensten die uitsluitend in systemen die gesloten zijn als gevolg nationaal recht of overeenkomsten tussen een welbepaalde groep deelnemers worden verleend (artikel 2, tweede lid). Deze omschrijving wordt in de overwegingen van de verordening toegelicht. De verordening mag volgens die overwegingen met name niet voorzien in de verlening van diensten die uitsluitend binnen gesloten systemen gebruikt worden tussen een welbepaalde groep deelnemers, en die geen gevolgen

hebben voor derden. Systemen die zijn opgezet bij bedrijven of overheden voor het beheer van interne procedures waarbij gebruik wordt gemaakt van vertrouwensdiensten, behoren bijvoorbeeld niet onder deze verordening te vallen. Alleen vertrouwensdiensten die aan het publiek verleend worden en gevolgen hebben voor derden moeten voldoen aan de vereisten van deze verordening (overweging 21 van de richtlijn). Ook onder de richtlijn elektronische handtekeningen werd het toepassingsbereik ervan beperkt en wel tot systemen die berusten op vrijwillige privaatrechtelijke overeenkomsten tussen een vastgesteld aantal deelnemers (overweging 16 van de richtlijn). In de nadere memorie van antwoord bij de Wet elektronische handtekeningen is vervolgens aan de hand van verschillende concrete voorbeelden toegelicht hoe deze uitzondering opgevat dient te worden (Kamerstukken I 2002/03, 27 743, nr. 35b, blz. 8 tot en met 10; zie voorts ook voor gekwalificeerde certificaten en het vermelden van het toepassingsbereik daarvan in het certificaat: Kamerstukken II 2000/2001, 27 743, nr. 3, blz. 19). Daarbij is tevens aangegeven dat het uiteindelijk ook het Europese Hof van Justitie is om te oordelen of sprake is van certificaten aan het publiek of niet. De desbetreffende voorbeelden en het daarbij gemaakte voorbehoud zullen naar wordt aangenomen ook onder de verordening nog steeds van betekenis zijn, met dien verstande dat die niet enkel voor gekwalificeerde certificaten voor elektronische handtekeningen relevant zijn maar voor alle vertrouwensdiensten.

Onderdeel F, Artikel 2.5b
Dit artikel betreft een nadere uitwerking van de in de eidas-verordening beschreven procedure om als gekwalificeerde verlener van vertrouwensdiensten gekwalificeerde vertrouwensdiensten te mogen aanbieden (artikel 21, van de eidas-verordening). Verleners van vertrouwensdiensten die niet over de status gekwalificeerd beschikken en gekwalificeerde vertrouwensdiensten willen gaan leveren, dienen op grond van de verordening bij het aangewezen toezichthoudend orgaan een kennisgeving van hun voornemen in, en daarbij een door een conformiteitsbeoordelingsorgaan afgegeven conformiteitsbeoordelingsverslag. Het toezichthoudend orgaan is na ontvangst daarvan verplicht te verifiëren of de verlener van vertrouwensdiensten en de door hem verleende vertrouwensdiensten in overeenstemming zijn met de in de verordening vastgestelde eisen, en in het bijzonder met de eisen die worden gesteld aan gekwalificeerde verleners van vertrouwensdiensten en aan de gekwalificeerde vertrouwensdiensten die zij verlenen. Indien het toezichthoudend orgaan vervolgens na verificatie vaststelt dat de verlener van vertrouwensdiensten en de door hem verleende vertrouwensdiensten in overeenstemming met deze eisen zijn, kent het toezichthoudend orgaan de status van gekwalificeerde toe aan de verlener van vertrouwensdiensten en aan de door hem verleende vertrouwensdiensten. De aanvang van het verlenen van gekwalificeerde vertrouwensdiensten is toegestaan nadat de status van gekwalificeerde door het toezichthoudend orgaan is opgenomen in de vertrouwenslijst. Opname daarin moet binnen drie maanden plaatsvinden na de kennisgeving door de verlener van vertrouwensdiensten van zijn voornemen. Indien de verificatie door het toezichthoudend orgaan niet binnen die drie maanden is afgerond, brengt het toezichthoudend orgaan de verlener van vertrouwensdiensten op de hoogte van de redenen voor de vertraging en van de termijn waarbinnen de verificatie zal zijn afgerond.

Ter uitvoering van artikel 21 van de verordening zijn in het voorgestelde artikel voorschriften opgenomen over de kwalificatie, inhoud en behandeling van een kennisgeving van een voornemen. Uit het eerste lid volgt dat een mededeling aan de Minister van Economische Zaken van het voornemen om de status gekwalificeerd te krijgen als een aanvraag wordt aangemerkt. Er wordt niet over kennisgeving maar over mededeling gesproken. Hiermee wordt hetzelfde bedoeld. Voor mededeling is gekozen vanuit oogpunt van eenheid in terminologie in hoofdstuk 2 van de Telecommunicatiewet. De kwalificatie van een mededeling als aanvraag is noodzakelijk doordat dit de basis is voor een daarop volgende inhoudelijke beoordeling door de Minister die uitmondt in een op rechtsgevolg gerichte beschikking: de toekenning respectievelijk de weigering van de status gekwalificeerd.

Het voorgestelde tweede lid vloeit voort uit het vereiste in de verordening dat de taken van het toezichthoudend orgaan, inclusief de toekenning van de status gekwalificeerd, uitsluitend betrekking hebben op de verleners van vertrouwensdiensten die gevestigd zijn in de lidstaat waarvoor het

toezichthoudend orgaan is aangewezen (artikel 17, derde lid, van de verordening). Het derde lid laat de verdere toepasselijkheid van artikel 4:5, eerste lid, Awb onverlet. De onderdelen a en b, benoemen twee situaties waarbij Agentschap Telecom een aanvraag niet in behandeling mag nemen, indien de aanvraag niet binnen een gestelde termijn is aangevuld met de in dat lid omschreven ontbrekende informatie. De vereiste overlegging van een conformiteitsverslag als bedoeld in onderdeel b, kan ook in een vreemde taal zijn opgesteld. In dat geval kan het voor de beoordeling van de aanvraag noodzakelijk zijn dat het desbetreffende verslag is vertaald en aan de kwaliteit van die vertaling eisen worden gesteld. Artikel 4:5, tweede lid, van de Algemene wet bestuursrecht, is hierop van toepassing. Het vierde lid gaat over de bij een aanvraag te voegen gegevens die in een vertrouwenslijst opgenomen moeten worden. Dit stelt de Minister in staat om na toekenning van de status gekwalificeerd de vertrouwenslijst hiermee bij te werken. De Minister kan zo nodig een formulier vaststellen waarin de te overleggen gegevens worden benoemd. Uit het vijfde lid volgt onder meer dat de Minister ook andere gegevens mag eisen bij het indienen van de aanvraag. Hierbij kan bijvoorbeeld worden gedacht aan gegevens ten aanzien van de gevolgde auditregels bij het opstellen van een verslag. Hierover kan de Europese Commissie referentienormen vaststellen (artikel 20, vierde lid, van de verordening). De aanvraag wordt door het toezichthoudend orgaan, voor Nederland is dat de Minister, beoordeeld op overeenstemming met de eisen, bedoeld in de verordening. Deze verplichting volgt rechtstreeks uit de verordening, zodat dit niet in het wetsvoorstel is overgenomen. Uit de verordening volgt voorts dat als aan die eisen naar het oordeel van het toezichthoudend orgaan is voldaan, de status van gekwalificeerd wordt verleend. Hieruit kan worden afgeleid dat als aan die eisen niet is voldaan, de toekenning van de status wordt geweigerd. De bevoegdheid tot weigering voor de Minister valt daarmee binnen de rechtstreekse werking van de verordening, zodat dit niet separaat in het wetsvoorstel is vastgelegd. Het betreft een weigeringsbesluit waartegen bezwaar en beroep kan worden ingesteld.

Onderdeel F, Artikel 2.5c
In het eerste lid wordt de Minister van Economische Zaken aangewezen als verantwoordelijke voor het opstellen, bijhouden en openbaar elektronisch toegankelijk maken van de vertrouwenslijst voor Nederland. In de huidige Tw berust die verantwoordelijkheid bij ACM. Doordat de Minister in het wetsvoorstel voor de vertrouwenslijst verantwoordelijk wordt, is de verwachting dat de toegankelijkheid van deze lijst via de website van Agentschap Telecom wordt gerealiseerd. Uiterlijk op 18 september 2015 specificeert de Commissie door middel van uitvoeringshandelingen de informatie die in de vertrouwenslijsten van lidstaten moet worden opgenomen en omschrijft zij de technische specificaties en formaten daarvan (artikel 22, vijfde lid, van de verordening). De Minister kan deze informatie uitsluitend opnemen en bijhouden, indien de gekwalificeerde verleners van vertrouwensdiensten de daarvoor benodigde gegevens verstrekken. Het tweede tot en met zevende lid zien op verschillende te onderscheiden situaties waarbij gegevens verstrekt moeten worden en op het bijhouden van de vertrouwenslijst door de Minister. Het derde lid is hierbij aan te merken als een bepaling die artikel 24, eerste lid, onderdeel a, van de verordening in het belang van een goede uitvoering nader concretiseert. Binnen het huidig wettelijk kader zijn de in de vertrouwenslijst op te nemen informatie en technische specificaties van de lijst geregeld in de Regeling vertrouwenslijst. Naar verwachting zal de uitvoeringshandeling van de Europese Commissie over de vertrouwenslijsten bij deze praktijk aansluiten. De Regeling vertrouwenslijst zal als gevolg van de rechtstreekse werking van de eidas-verordening vermoedelijk worden heroverwogen.

Onderdeel F, Artikel 2.5d
De eidas-verordening bevat voorschriften over het intrekken van de status gekwalificeerd door het toezichthoudend orgaan en over het daarvan in kennis stellen van de gekwalificeerde verlener van vertrouwensdiensten (artikel 20, derde lid, van de verordening). Onverminderd deze voorschriften bevat het wetsvoorstel tevens enkele concretiserende voorschriften die voor de goede uitvoering van de verordening vereist zijn. Uit het eerste lid volgt dat Agentschap Telecom is gehouden de status gekwalificeerd te beëindigen, indien daarvoor niet langer een grond aanwezig is. In dat geval is Agentschap Telecom verplicht tot beëindiging van de status over te gaan. Hiermee wordt voor een specifieke situatie nadere invulling gegeven aan de nationale afwegingsvrijheid die de verordening ten

aanzien van intrekking aan het toezichthoudend orgaan biedt. In het tweede lid wordt geregeld dat het Agentschap onverminderd hetgeen over intrekking in de verordening is bepaald, de status gekwalificeerd ook om de in dat lid genoemde gevallen kan beëindigen. In onderdeel a betreft dit het handelen in strijd met het bij of krachtens de wet bepaalde. Daarvan kan bijvoorbeeld sprake zijn indien niet aan de eisen is voldaan die in dit wetsvoorstel aan de vaststelling van de identiteit bij de uitgifte van een gekwalificeerd certificaat worden gesteld. Die eisen mogen ingevolge de verordening met inachtneming van het daaromtrent bepaalde overeenkomstig het nationale recht worden bepaald. Een redelijke uitleg van de verordening staat in dat geval toe dat ingeval van strijd met die eisen wettelijk wordt bepaald dat dit beëindiging van de status gekwalificeerd tot gevolg kan hebben. Dit geldt onverminderd de mogelijkheden tot beëindiging op grond van de rechtstreekse werking van de verordening. Op grond van onderdeel b kan het Agentschap tot beëindiging overgaan indien na een daartoe gestelde termijn de gegevens waarnaar in dat onderdeel wordt verwezen niet alsnog zijn verstrekt. Het betreft gegevens die op grond van het wetsvoorstel door de gekwalificeerde verleners van vertrouwensdiensten verstrekt dienen te worden aan het Agentschap, zodat die aan zijn verplichtingen ten aanzien van het opstellen en bijhouden van de vertrouwenslijst kan voldoen. Ook hiervoor geldt dat een redelijke uitleg van de verordening met zich brengt dat bij niet-naleving van deze verplichting, na een daartoe gestelde termijn, tot beëindiging van de status gekwalificeerd moet kunnen leiden. Anders kan het vertrouwen van het publiek in de vertrouwenslijst of in relatie tot de betrokken verlener geschaad worden.

Onderdeel F, Artikel 2.5e en onderdeel G, artikel 11.5b
De in het kader van een aanvraag ontvangen gegevens kunnen persoonsgegevens bevatten. Voor zover dat het geval is en die gegevens onderdeel worden van een gegevensverzameling, is op grond van het voorgestelde onderdeel F de Minister daarvoor verantwoordelijke in de zin van de Telecommunicatiewet. Dit geldt ook met betrekking tot de persoonsgegevens die in de vertrouwenslijst voorkomen. De in onderdeel G voorgestelde wijzigingen hebben betrekking op het verbreden van de werkingssfeer van artikel 11.5b tot verleners van vertrouwensdiensten. Naast de toepasselijkheid van de Wet bescherming persoonsgegevens, wordt met de voorgestelde onderdelen tevens nadere invulling gegeven aan artikel 5, van de eidas-verordening.

Onderdeel H, artikel 11.5c
De verordening bevat een rechtstreeks werkende meldplicht voor verleners van vertrouwensdiensten ingeval van incidenten met vertrouwensdiensten die zich ook uitstrekt tot het doen van een melding aan de nationale gegevensbeschermingsautoriteit. Die meldplicht is aan de orde bij een inbreuk op de veiligheid of verlies van integriteit met aanzienlijke gevolgen voor de persoonsgegevens die met een vertrouwensdienst worden beheerd (zie artikel 19, tweede lid, van de eidas-verordening). Ook de melding aan een natuurlijke persoon of rechtspersoon die naar verwachting negatieve gevolgen zal hebben van een inbreuk of integriteitsverlies is rechtstreeks werkend in de verordening vastgesteld. Over de bij een melding te overleggen gegevens kan de Europese Commissie uitvoeringshandelingen vaststellen. Het voorgestelde artikel respecteert de rechtstreekse werking van de verordening. In dit onderdeel wordt het Cbp als nationale gegevensbeschermingsautoriteit aangewezen. Voor de bij een melding te overleggen gegevens, indien de Europese Commissie geen uitvoeringshandelingen hierover vaststelt, wordt verwezen naar de toelichting bij onderdeel P.

Onderdeel I, artikel 15.1
Het huidige artikel 15.1, bepaalt wie met het toezicht op de naleving van het bij of krachtens de Telecommunicatiewet bepaalde belast is. Voor de in het eerste lid opgesomde activiteiten en onderwerpen worden met het toezicht op de naleving van de daarop betrekking hebbende voorschriften belast de bij besluit van Onze Minister aangewezen ambtenaren (voor zover het althans bevoegdheden van de Minister aangaat). De daarvoor aangewezen ambtenaren maken deel uit van het dienstonderdeel Agentschap Telecom. De voorgestelde wijzigingen hebben tot gevolg dat de opsomming aan activiteiten en onderwerpen in het eerste lid wordt verruimd tot het toezicht op de naleving van de bepalingen in het deel van de eidas-verordening dat over vertrouwensdiensten gaat

en tot enkele bepalingen in het wetsvoorstel over vertrouwensdiensten. Dit toezicht beperkt zich tot in Nederland gevestigde verleners van vertrouwensdiensten en hun vertrouwensdiensten aan het publiek. Bij de uitoefening van het toezicht zal Agentschap Telecom onderscheid dienen te maken tussen verleners van gekwalificeerde respectievelijk niet-gekwalificeerde vertrouwensdiensten. Ten aanzien van niet-gekwalificeerde verleners van vertrouwensdiensten is Agentschap Telecom op grond van de verordening uitsluitend bevoegd achteraf te handhaven op basis van een signaal dat een niet-gekwalificeerde verlener van vertrouwensdiensten of de door hem verleende vertrouwensdienst niet zou voldoen aan de vereisten van de verordening (artikel 17, derde lid, onderdeel b, van de verordening).

Het voorgestelde artikel 15.1, derde lid, breidt het toezicht van het Cbp uit tot de meldplicht als geregeld in de verordening voor een inbreuk op de veiligheid of het verlies van integriteit van persoonsgegevens.

Onderdeel J, artikel 15.3b
Aan het verlenen van vertrouwensdiensten zijn vaak grensoverschrijdende aspecten verbonden. Een verlener van vertrouwensdiensten kan bijvoorbeeld in de ene lidstaat van de Europese Unie gevestigd zijn en in een andere lidstaat zijn diensten aanbieden. Of de servers waarvan gebruikt wordt gemaakt, bijvoorbeeld voor het aanmaken van certificaten, staat niet in de lidstaat van vestiging van de verlener van vertrouwensdiensten maar in een andere lidstaat (zie overweging 42 van de verordening). De eidas-verordening bepaalt dat toezichthoudende organen verplicht zijn samen te werken voor het uitwisselen van goede praktijken met betrekking tot vertrouwensdiensten (artikel 18 van de verordening). Een verzoek tot bijstand dient gemotiveerd zijn. Wederzijdse bijstand kan in het bijzonder betrekking hebben op informatieverzoeken en toezichthoudende maatregelen, zoals verzoeken om inspecties uit te voeren in verband met de conformiteitsbeoordelingsverslagen. Een toezichthoudend orgaan mag een verzoek om bijstand weigeren vanwege een limitatief aantal in de verordening opgesomde redenen.

Uit het eerste lid volgt dat de ambtenaren die belast zijn met het toezicht op de in Nederland gevestigde verleners van vertrouwensdiensten ook belast zijn met het verlenen van bijstand als een verzoek daartoe door de Minister van Economische Zaken is ingewilligd. Inwilliging hangt af van de beoordeling door de Minister van de in artikel 18, tweede lid, van de eidas-verordening, genoemde weigeringsgronden tot het verlenen van bijstand. Het verlenen van bijstand zal zich in het bijzonder concentreren op het verschaffen van informatie en gegevens die voor een toezichthoudend orgaan uit een andere lidstaat behulpzaam zijn bij de uitoefening van het toezicht door dat orgaan op de in die andere lidstaat gevestigde verleners van vertrouwensdiensten. Om deze bijstand te kunnen te verlenen in overeenstemming met de verordening, dienen de aangewezen ambtenaren van Agentschap Telecom over de daarvoor benodigde bevoegdheden te beschikken ten aanzien van verleners van vertrouwensdiensten die in Nederland actief zijn, maar hier niet gevestigd zijn en waarop het verzoek tot bijstand betrekking heeft. Het betreft bevoegdheden zoals het vorderen van inlichtingen, het inzien of kopiëren van gegevens en bescheiden, onderzoek van apparatuur en voorzieningen, en zo nodig door inspectie ter plaatse. Deze bevoegdheden en de voorwaarden waaronder die gebruikt mogen worden zijn in titel 5.2 van de Awb geregeld voor toezichthouders als bedoeld in artikel 5.11 van die wet. De ambtenaren belast met het verlenen van bijstand, treden evenwel strikt genomen niet op als toezichthouder voor in andere lidstaten gevestigde verleners van vertrouwensdiensten waarop een verzoek tot bijstand betrekking heeft. Door in het voorgestelde tweede lid de aangewezen ambtenaren die belast zijn met het verlenen van bijstand als toezichthouder in de zin van de Awb aan te merken, verkrijgen zij de voor het verlenen van bijstand benodigde bevoegdheden. Hiervan is uitgezonderd artikel 5:19 van de Awb dat betrekking heeft op het onderzoeken van vervoermiddelen. Het is niet aannemelijk dat het gebruik van deze bevoegdheid noodzakelijk is.

Op grond van artikel 5:20, van de Awb, is een ieder verplicht aan een toezichthouder binnen de door hem gestelde redelijke termijn alle medewerking te verlenen die deze redelijkerwijs kan vorderen bij

de uitoefening van zijn bevoegdheden. Indien overtreding van dat voorschrift plaatsvindt, kunnen de ambtenaren belast met het verlenen van bijstand op grond van de overeenkomstige toepassing in het tweede lid van artikel 5.14, eerste lid, van de Telecommunicatiewet een bestuurlijke boete opleggen van ten hoogste € 450 000. Daarmee wordt aangesloten bij het algemene regime voor bestuurlijke boete in de Telecommunicatiewet. Voorts zijn in het voorgestelde derde lid enkele andere artikelen van de Telecommunicatiewet van overeenkomstige toepassing verklaard.

Onderdeel J, artikel 15.3c
Bij een verzoek tot het verlenen van bijstand stelt de Minister van Economische Zaken vast of een weigeringsgrond in de verordening van toepassing is. Bij die beoordeling dient de Minister op grond van het voorgestelde eerste lid tevens het daarin bepaalde onder a tot en met c te betrekken. Deze onderdelen hebben tot doel geheimhouding van bedrijfsvertrouwelijke gegevens en inlichtingen te waarborgen, doelbinding zeker te stellen en vast te stellen of het gegevens en inlichtingen betreft waarvoor bevoegdheid tot verstrekking bestaat. Dit zal de Minister aan de hand van het gemotiveerde verzoek tot bijstand dienen te beoordelen.

Onderdeel J, artikel 15.3d
Indien van toepassing kunnen lidstaten hun toezichthoudende organen toestaan gezamenlijke onderzoeken uit te voeren waarbij personeelsleden van toezichthoudende organen van andere lidstaten betrokken zijn. De regelingen en procedures voor dergelijke gezamenlijke acties worden door de betrokken lidstaten overeenkomstig hun wetgeving overeengekomen en vastgelegd (artikel 18, derde lid, van de verordening). De verordening verplicht lidstaten niet tot het bieden van de mogelijkheid tot het doen van gezamenlijk onderzoek. Gelet op het grensoverschrijdend karakter van het verlenen van vertrouwensdiensten, is het van belang dat deelname door ambtenaren van Agentschap Telecom aan een gezamenlijk onderzoek openstaat. Het voorgestelde artikel bepaalt wanneer dat kan en wat daarbij geldt.

Voorwaarde voor een gezamenlijk onderzoek is dat tussen het toezichthoudend orgaan in de andere lidstaat en de Minister van Economische Zaken hierover overeenstemming bereikt. Hierop hebben het eerste en tweede lid betrekking. Het kan gaan om situaties waarin een incident heeft plaatsgevonden bij een verlener van vertrouwensdiensten die grensoverschrijdend actief is. Onder omstandigheden kan het dan zinvol zijn dat ambtenaren van Agentschap Telecom in nauw en direct overleg met collega's van een toezichthoudend orgaan uit een andere lidstaat treden over de aanpak van een onderzoek, de uitvoering daarvan en het uitwisselen van informatie die tijdens en na een onderzoek wordt verkregen. Bij ernstige incidenten waarbij behoefte is aan snelle en hoogwaardige kennisuitwisseling, kan er bovendien behoefte aan bestaan dat een ter zake deskundige persoon werkzaam bij een ander toezichthoudend orgaan op locatie informatie kan inzien, beoordelen en vervolgvragen kan voorleggen aan Agentschap Telecom en omgekeerd ook zelf nieuwe informatie kan delen met het Agentschap. Gelet hierop beschikken de ambtenaren van Agentschap Telecom die aan een gezamenlijk onderzoek deelnemen op grond van het derde lid over dezelfde bevoegdheden als bij het verlenen van bijstand. Ook kan een ambtenaar van Agentschap Telecom met een beroep op artikel 5:15, derde lid, van de Awb, zijn bevoegdheden uitoefenen in aanwezigheid van een persoon die werkzaam is bij een toezichthoudend orgaan uit een andere lidstaat. Een persoon die voor een toezichthoudend orgaan uit een andere lidstaat aan een gezamenlijk onderzoek deelneemt mag vervolgens van gegevens en inlichtingen kennis nemen onder de voorwaarden die daaraan zijn verbonden. De bevoegdheid tot het vorderen van gegevens en inlichtingen en de verantwoordelijkheid voor inspectie ter plaatse blijft uitsluitend berusten bij de betrokken ambtenaren van Agentschap Telecom.

Onderdeel K, artikel 16.1
De Minister van Economische Zaken dient werkzaamheden of diensten te verrichten ter uitvoering van het bepaalde in de eidas-verordening. De Minister wordt in het wetsvoorstel aangewezen als toezichthoudend orgaan en is daarmee verantwoordelijk voor het vervullen van in de verordening aan dat orgaan toegekende taken. De inhoud van die taken zijn echter niet bij of krachtens dit

wetsvoorstel bepaald, maar in de eidas-verordening zelf. Daardoor kan onduidelijkheid bestaan of de werkzaamheden of diensten die de Minister ter uitvoering van de eidas-verordening verricht eveneens onder het toepassingsbereik van de algemene vergoedingsregeling kunnen vallen. De voorgestelde wijzigingen in dit artikel geven hierover uitdrukkelijk uitsluitsel. Ten aanzien van niet-gekwalificeerde vertrouwensdiensten vindt geen registratie plaats van de verleners van die diensten en zijn de verdere werkzaamheden van een andere omvang en orde dan in verband met gekwalificeerde vertrouwensdiensten.

Onderdeel L, artikel 18.2a
Met het voorgestelde artikel wordt uitvoering gegeven aan artikel 17, eerste lid, van de eidas-verordening. Op grond daarvan moeten lidstaten een toezichthoudend orgaan aanwijzen. De rol en taken van de Minister van Economische Zaken als toezichthoudend orgaan omvatten meer dan enkel het houden van toezicht op de naleving van hoofdstuk 3 van de eidas-verordening. Het toezichthoudende orgaan dient ook bijstand en samenwerking te verlenen aan andere toezichthoudende organen en de status gekwalificeerd toekennen of in voorkomend geval intrekken. Voorts is de Minister tevens verantwoordelijk voor het opstellen en bijhouden van de vertrouwenslijst. Met het toezicht op de naleving zijn op grond van dit wetsvoorstel de door de Minister aangewezen ambtenaren belast. Die aangewezen ambtenaren zijn tevens belast met het verlenen van bijstand en bevoegd om deel te nemen aan een gezamenlijk onderzoek met andere toezichthoudende organen onder de daaraan in het wetsvoorstel gestelde voorwaarden. Het voornemen is dat de Minister ambtenaren van Agentschap Telecom hiermee zal belasten. Ditzelfde geldt voor het opstellen en bijhouden van de vertrouwenslijst en het behandelen van aanvragen tot het verleend krijgen van de status gekwalificeerd dan wel het beëindigen van die status.

Onderdeel M, artikel 18.3a en onderdeel N, artikel 18.7
De verstrekking van gegevens door andere bestuursorganen dan de Autoriteit Consument en Markt aan de Minister is in de voorgestelde wijziging ook toegestaan indien dit noodzakelijk is voor de uitvoering van en het toezicht op de eidas-verordening (onderdeel L). En voorts is het vorderen van inlichtingen ook toegestaan voor een juiste uitvoering van de verordening (onderdeel M).

Onderdeel O, artikel 18.15
De eisen waaraan in Nederland gevestigde verleners van vertrouwensdiensten en hun vertrouwensdiensten moeten voldoen, zijn in de verordening met rechtstreekse werking vastgelegd. Ditzelfde geldt voor aanbieders van gekwalificeerde middelen voor elektronische handtekeningen of elektronische zegels. Voor veel van die eisen geldt dat de Europese Commissie de bevoegdheid heeft door middel van uitvoeringshandelingen referentienormen vast te stellen op basis van de comitologieprocedure. Indien aan een dergelijke norm, bijvoorbeeld een Europese vastgestelde technische norm, is voldaan, wordt aangenomen dat er overeenstemming is met de daarop betrekking hebbende eis die in de verordening staat vermeld. Het vaststellen van een norm sluit niet uit dat ook op andere wijze dan met inachtneming van die norm aan een eis uit de verordening kan worden voldaan.

De Europese Commissie is niet verplicht uitvoering te geven aan de vaststelling van referentienormen in alle gevallen waarvoor die bevoegdheid bestaat. Bij de voorbereiding van dit wetsvoorstel is onduidelijk in hoeverre op alle onderdelen waar dit nodig is (tijdig) referentienormen vastgesteld zullen worden. Voor het waarborgen van de betrouwbaarheid en de rechtszekerheid is evenwel noodzakelijk dat bij de toepasselijkheid van de verordening vanaf 1 juli 2016 in voldoende mate is voorzien in dergelijke technische normen. Gelet hierop biedt het voorgestelde artikel de mogelijkheid dit bij of krachtens algemene maatregel van bestuur te doen, voor zover dit voor een goede uitvoering van de eidas-verordening is vereist.

De Europese Commissie is voorts bevoegd referentienormen vast te stellen voor de accreditering van conformiteitsbeoordelingsinstanties, auditregels en het conformiteitsbeoordelingsverslag (artikel 20, vierde lid, van de eidas-verordening). Indien aan deze referentienormen wordt voldaan verbindt e

verordening hier niet het vermoeden aan dat aan eisen uit de eidas-verordening is voldaan. Dit verschil met de andere referentienormen, zoals die onder meer in de artikelen 34, tweede lid, 38, zesde lid, 42, tweede lid, 44, tweede lid, 45, tweede lid, heeft tot gevolg dat het stellen van regels over deze referentienormen zich niet goed lenen voor vastlegging in een algemeen verbindend voorschrift. De referentienormen zijn niet meer en ook niet minder dan een richtlijn bij de beoordeling van conformiteitsbeoordelingsverslagen. Indien de Europese Commissie dergelijke referentienormen niet vaststelt, kan Agentschap Telecom als dat voor een goede uitvoering van de verordening noodzakelijk is overwegen hieromtrent beleidsregels vast te stellen.

Onderdeel P, artikel 18.15a
De Europese Commissie kan uitvoeringshandelingen vaststellen met rechtstreekse werking betreffende formaten en procedures vaststellen voor doeleinden van de meldplicht (artikel 19, vierde lid, van de verordening). Dit kunnen ook formulieren zijn met een duiding van de bij een melding te overleggen gegevens. Daarbij kan die aanduiding zowel gelden voor een melding aan het toezichthoudend orgaan, het nationale orgaan voor informatieveiligheid, de gegevensbeschermingsautoriteit als de natuurlijke persoon of rechtspersoon die van een inbreuk of integriteitsverlies negatieve gevolgen ondervindt. Indien of zolang de Europese Commissie niet of eventueel in onvoldoende mate voorziet in een duiding van de bij een melding te overleggen gegevens, kunnen op grond van het voorgestelde artikel 18.15a voor een goede uitvoering van de verordening bij algemene maatregel van bestuur hierover regels worden gesteld voor een melding aan AT, NCSC en, voor zover het persoonsgegevens betreft, het Cbp, alsmede aan degene aan wie een vertrouwensdienst is verleend die naar verwachting ongunstige gevolgen ondervindt van een inbreuk die op grond van de verordening aan die organen moet worden gemeld. Bij de op grond van een algemene maatregel van bestuur te melden gegevens kan worden gedacht aan maatregelen die de aanbieder voorstelt of heeft getroffen om de inbreuk aan te pakken, de aard van de inbreuk of het verlies, vermoedelijke tijdstip van de aanvang van de inbreuk of het verlies en de mogelijke gevolgen en instanties waar meer informatie over de inbreuk kan worden verkregen.

Onderdeel P, artikel 18.15b
Dit artikel bepaalt dat het bevoegde nationale orgaan voor informatieveiligheid, bedoeld in artikel 19, tweede lid, van de eidas-verordening de Minister van Veiligheid en Justitie is, die verantwoordelijk is voor het Nationaal Cyber Security Center (NCSC).

Onderdeel P, artikel 18.15c
Voorafgaand aan afgifte van een gekwalificeerd certificaat is identiteitsverificatie met daartoe geschikte middelen verplicht. Dit dient overeenkomstig de nationale wetgeving plaats te vinden (artikel 24, eerste lid, eerste alinea, van de eidas-verordening). Identiteitsverificatie kan betrekking hebben op een natuurlijke persoon of op een natuurlijke persoon die een rechtspersoon vertegenwoordigt. In het laatste geval is het de bedoeling een gekwalificeerd certificaat dat daarvoor geschikt is op naam van een rechtspersoon te stellen. Rechtspersonen zijn in de zin van het VWEU alle entiteiten die zijn opgericht naar of worden beheerst door het recht van een lidstaat, ongeacht hun rechtsvorm. Voor Nederland worden voor de toepassing van de verordening hiertoe de rechtspersonen als bedoeld in de artikelen 1 tot en met 3 van Boek 2 van het Burgerlijk Wetboek gerekend. Voorts worden tot rechtspersonen ook gerekend de Europese naamloze vennootschap, bedoeld in Verordening (EG) nr. 2157/2001 van de Raad van 8 oktober 2001 betreffende het statuut van de Europese Vennootschap (SE) (PbEG 2001, L 294), het Europees economisch samenwerkingsverband, bedoeld in Verordening nr. 2137/85 van de Raad van de Europese Gemeenschappen van 25 juli 1985 tot instelling van Europese economische samenwerkingsverbanden (PbEG L 199/1) en de Europese coöperatieve vennootschap, bedoeld in verordening (EG) Nr. 1435/2003 van de Raad van de Europese Unie van 22 juli 2003 betreffende het statuut voor een Europese Coöperatieve Vennootschap (SCE) (PbEU 2003, L 207). Indien bij een eenmanszaak, maatschap, vennootschap onder firma of commanditaire vennootschap onder firma behoefte bestaat aan een gekwalificeerd certificaat voor website-authenticatie richt identiteitsverificatie zich op de natuurlijke persoon, waarbij door middel

van vermelding van aanvullende attributen in een certificaat duidelijk kan worden gemaakt dat die natuurlijke persoon voor een van deze rechtsvormen optreedt.

De verordening somt limitatief enkele manieren op die voor identiteitsverificatie van een natuurlijke persoon of rechtspersoon geschikt zijn. Identificatie in fysieke aanwezigheid is er daar één van. Dit is onderwerp van artikel 18.15c, zoals uit het eerste lid blijkt. Indien een certificaat op naam van een natuurlijke persoon wordt gesteld, volgt uit het tweede lid met welke bescheiden de identiteit van die persoon moet worden vastgesteld. Dit dient een in artikel 1 van de Wet op de identificatieplicht aangewezen geldig document te zijn. Bij rechtspersonen heeft identificatie in fysieke aanwezigheid betrekking op natuurlijke personen die vertegenwoordigingsbevoegd zijn. Dit is onderwerp van het derde tot en met zesde lid. De meest voorkomende situatie zal zijn dat een natuurlijk persoon bevoegd is een rechtspersoon te vertegenwoordigen bij de aanschaf van een op naam van die rechtspersoon te stellen gekwalificeerd certificaat. Identificatie omvat dan zowel identificatie van de natuurlijke persoon als identificatie van de rechtspersoon en de bevoegdheid tot vertegenwoordiging door de natuurlijke persoon van die rechtspersoon. De vertegenwoordigingsbevoegdheid van de natuurlijke persoon van wie in fysieke aanwezigheid de identiteit is vastgesteld, dient te worden gecontroleerd aan de hand van de gegevens in het handelsregister. In plaats daarvan kan ook de identiteit van een natuurlijke persoon worden vastgesteld die over een volmacht beschikt van een bestuurder van de rechtspersoon die over een in het handelsregister vastgelegde vertegenwoordigingsbevoegdheid beschikt. In dat geval hoeft die bestuurder niet in persoon te verschijnen, maar dient aan de hand van de gegevens in het handelsregister te worden vastgesteld dat de bestuurder die de volmacht heeft verleend vertegenwoordigingsbevoegd is. Dit vereist dat met een hoge mate van betrouwbaarheid wordt vastgesteld dat die bestuurder inderdaad degene is geweest die de volmacht heeft ondertekend. De gevolmachtigde natuurlijke persoon vervangt immers de fysieke aanwezigheid van de bestuurder als natuurlijke persoon bij identificatie. Gelet hierop wordt in het derde lid, onderdeel c, bepaald dat een volmacht met een gekwalificeerde elektronische handtekening of een door een notaris gelegaliseerde handtekening ondertekend dient te zijn. Het vierde lid heeft betrekking op vertegenwoordiging via een of meer tussenliggende rechtspersonen. De natuurlijke rechtspersoon vertegenwoordigt in dat geval een rechtspersoon, die weer de rechtspersoon vertegenwoordigt op wie de tenaamstelling betrekking heeft. En hierbij kan zelfs sprake zijn van een keten aan tussenliggende rechtspersonen, zoals bij concerns met achterliggende dochtermaatschappijen. In dat soort situaties dient een verificatie van de gehele keten ononderbroken terug te voeren zijn op de natuurlijke persoon van wie in fysieke aanwezigheid de identiteit wordt vastgesteld, en wel op dezelfde wijze met behulp van het handelsregister als bij rechtstreekse vertegenwoordiging. Afgezien van vertegenwoordiging van rechtspersonen kan het zich voordoen dat de natuurlijke persoon bijvoorbeeld een vennootschap onder firma vertegenwoordigt en voor die vennootschap bevoegd is de rechtspersoon te vertegenwoordigen op naam van wie het certificaat wordt gesteld. Uit het vijfde lid volgt dat ten aanzien van identificatie dan hetzelfde geldt als voor rechtspersonen. Het zesde lid houdt rekening met rechtspersonen en met als zelfstandige eenheid naar buiten werkende samenwerkingsverbanden die niet in het handelsregister staan ingeschreven. Voor verificatie van gegevens kan in dat geval worden afgegaan op een buitenlandse register waarin de entiteit of eenheid staat ingeschreven dat soortgelijk is aan het handelsregister.

Onderdeel P, artikel 18.15d
De eidas-verordening somt drie mogelijkheden op voor identificatie die elektronisch en/of op afstand kan worden uitgevoerd voorafgaand aan de afgifte van een gekwalificeerd certificaat.

De eerste mogelijkheid is dat identificatie op afstand plaatsvindt door middel van een geldig elektronisch identificatiemiddel met het betrouwbaarheidsniveau substantieel of hoog als bedoeld in de verordening. Bij het gebruik van dit identificatiemiddel is geen fysieke aanwezigheid vereist, maar vereist is in dat geval dat ten tijde van de uitgifte van dat middel identificatie in fysieke aanwezigheid wel heeft plaatsgevonden (artikel 24, eerste lid, onder b, van de verordening). Verificatie aan de hand van een elektronisch identificatiemiddel dat aan de daarin in de verordening gestelde eisen voldoet, vindt overeenkomstig nationale wetgeving plaats. Gelet hierop is in het eerste lid bepaald dat afgifte

van een dergelijk middel met inachtneming van de aan identificatie of vertegenwoordiging gestelde eisen, bedoeld in artikel 18.15c moet zijn uitgegeven.

De tweede mogelijkheid voor elektronische identificatie voorafgaand aan de afgifte van een gekwalificeerd certificaat, bestaat uit verificatie van de identiteit aan de hand van een eerder afgegeven, geldig gekwalificeerd certificaat (artikel 24, eerste lid, onderdeel c, van de verordening). Het kan gaan om certificaten voor de gekwalificeerde elektronische handtekening (natuurlijke personen) of voor het gekwalificeerde elektronisch zegel (rechtspersonen). Identificatie met behulp van een dergelijk eerder afgegeven certificaat is alleen toegestaan, indien dat eerdere certificaat ofwel in fysieke aanwezigheid is afgegeven ofwel met een elektronisch identificatiemiddel dat voldoet aan de eisen die hiervoor bij de eerste mogelijkheid zijn genoemd. Het tweede lid bevestigt dat voorwaarde hierbij is dat afgifte van die identificatiemiddelen met inachtneming van respectievelijk overeenkomstig artikel 18.15c, heeft plaatsgevonden.

De derde mogelijkheid voor elektronische identificatie op afstand bij een afgifte van een gekwalificeerd certificaat is voor lidstaten optioneel (artikel 24, eerste lid, onderdeel d, van de verordening). Lidstaten kunnen er voor kiezen andere op nationaal niveau erkende identificatiemethoden die een mate van betrouwbaarheid verschaffen die gelijkwaardig is als fysieke aanwezigheid te accepteren als alternatief voor identificatie in fysieke aanwezigheid. Hierbij zou bijvoorbeeld wellicht kunnen worden gedacht aan identificatie met behulp van beeldverbindingen, die voldoende zekerheid bieden dat een persoon daadwerkelijk live in beeld is en zijn identiteit met voldoende zekerheid aan de hand van authentieke documenten kan worden vastgesteld. Hierbij geldt als eis dat het gelijkwaardige betrouwbaarheidsniveau door een conformiteitsbeoordelingsinstantie bevestigd dient te zijn. Gelet op het uitgangspunt van minimumomzetting van de verordening, is in het voorstel er vanaf gezien deze mogelijkheid nader te onderzoeken.

Onderdeel P artikelen 18.15e
De gegevens die in een gekwalificeerd certificaat vermeld moeten staan, zijn in enkele bijlagen van de verordening voorgeschreven. Dit is een set aan basisgegevens die onverlet laat dat in een dergelijk certificaat eventueel ook andere, facultatieve, gegevens kunnen staan die gekoppeld zijn aan degene die het certificaat identificeert. Een voorbeeld hiervan zijn gegevens die bevestigen dat een persoon bevoegd is een ander te vertegenwoordigen, zoals bij een certificaat voor een elektronische handtekening waaruit tevens de bevoegdheid tot wettelijke vertegenwoordiging, volmacht of lastgeving blijkt. Deze aan een persoon gekoppelde aanvullende gegevens worden attributen genoemd. Bij natuurlijke personen betreft dit naar hun aard persoonsgegevens. Ook de inhoud van specifieke attributen moeten op grond van de verordening op juistheid worden geverifieerd overeenkomstig de nationale wetgeving. Doordat attributen in beginsel op allerlei gegevens betrekking kunnen hebben, is het niet goed mogelijk een procedure voor te schrijven op basis waarvan verificatie van al die gegevens ongeacht de achtergrond daarvan, kan plaatsvinden. Dit zal per geval verschillen, zodat als algemene eis geldt dat verificatie op een niveau plaatsvindt dat past bij de betrouwbaarheid die aan de status gekwalificeerd wordt toegekend. In het tweede lid wordt dit voor bepaalde specifieke gegevens nader geconcretiseerd.

Onderdeel P, artikel 18.15f
Een certificaat kan een gefingeerde naam bevatten in plaats van te zijn gesteld op de echte naam van een natuurlijke persoon. De houder van het certificaat maakt gebruik van een pseudoniem. De verordening voorziet evenals onder de Richtlijn elektronische handtekening in de mogelijkheid van het gebruik van een pseudoniem bij een gekwalificeerd certificaat voor elektronische handtekeningen. Ook bij een gekwalificeerd certificaat voor website-authenticatie kan van een pseudoniem gebruik worden gemaakt. Op grond van de verordening moet in een certificaat vermeld worden als de naamgeving een pseudoniem betreft. Degene die op een dergelijk certificaat vertrouwt als ontvanger ervan, kan in dat geval door controle van het certificaat nagaan dat het een pseudoniem betreft. De vertrouwende partij weet dat het om een gefingeerde naam gaat, maar weet ook dat de identiteit van de persoon die heeft ondertekend voor hem onzichtbaar is geverifieerd door de verlener van vertrouwensdiensten.

Hij krijgt de bevestiging dat het certificaat afkomstig is van een bepaalde echt bestaande persoon. Het gebruik van pseudoniemen kan een instrument zijn ter bescherming van persoonsgegevens in het kader van 'privacy by design' of dataminimalisatie. De vertrouwende partij weet niet wie er achter het pseudoniem zit en hoeft dat bij sommige transacties ook niet te weten.

Onderdeel Q, artikelen 18.16 en 18.16a
Op grond van de huidige Telecommunicatiewet is de Minister van Economische Zaken bevoegd een of meer organisaties aan te wijzen die bevoegd zijn certificatiedienstverleners te toetsen op overeenstemming met de bij en krachtens deze wet gestelde eisen en daartoe een bewijs van toetsing af te geven. Het door de minister kunnen aanwijzen van certificeringsorganisaties vervalt in het wetsvoorstel. De verordening stelt zelf eisen aan instanties die deze verleners en hun diensten moeten toetsen. Deze instanties worden conformiteitsbeoordelingsinstanties genoemd. Conformiteitsbeoordelingsinstanties moeten geaccrediteerd zijn in overeenstemming met de accreditatieverordening om een conformiteitsbeoordeling te verrichten van een gekwalificeerde verlener van vertrouwensdiensten en van de door hem verleende vertrouwensdiensten (artikel 3, onder 18, van de verordening). Over de accreditering, toe te passen auditregels en verslagen van die instanties kan de Europese Commissie referentienormen vaststellen. Voor Nederland is de instantie die bevoegd is tot accreditatie de Raad voor Accreditatie.

Bij een kennisgeving van het voornemen gekwalificeerde vertrouwensdiensten te verlenen dient aan het toezichthoudend orgaan een conformiteitsbeoordelingsverslag te worden overgelegd. Ook na het verkrijgen van de status gekwalificeerd dient een dergelijk verslag ten minste eens in de 24 maanden aan het toezichthoudend orgaan te worden toegezonden (artikelen 20, tweede lid, en 21, eerste lid, van de verordening). Er bestaat voor verleners van vertrouwensdiensten niet de vrijheid zelf te bepalen af te zien van overlegging van een dergelijk verslag, en bijvoorbeeld te volstaan met overlegging van andere bescheiden waaruit overeenstemming met de eisen in de verordening zou moeten blijken. Evenmin bepaalt de verordening dat aan de overlegging van een positief conformiteitsbeoordelingsverslag het vermoeden mag worden ontleend dat inderdaad aan die eisen is voldaan. De toezichthouder draagt onverminderd de overlegging van een dergelijk verslag zelf verantwoordelijkheid voor de beoordeling of aan de in de verordening en het wetsvoorstel gestelde eisen wordt voldaan. Daarbij is de toezichthouder op grond van de verordening bevoegd zelf een audit uit te voeren of dit op kosten van de betrokken verlener van vertrouwensdiensten te doen. Het handhaven van een wettelijk vermoeden als bedoeld in artikel 18.16a vervalt in het wetsvoorstel.

Onderdeel R, artikel 18.17
De bewoordingen in dit artikel zijn aangepast aan de in de eidas-verordening gebruikte begrippen. Onder de richtlijn elektronische handtekeningen werd het gebruik van een veilig middel voor elektronische handtekeningen geregeld. In de verordening is het begrip veilig middel vervangen door gekwalificeerd middel, waarbij dit ook betrekking kan hebben op een elektronisch zegel.

Onderdeel S, artikel 18.17a
Bij het aanmaken van een elektronische handtekening kan gebruik worden gemaakt van een gekwalificeerd middel. De instellingen die een aanbieder van een middel mogen certificeren om het als gekwalificeerd middel te mogen aanbieden, moeten door de lidstaten worden aangewezen. Die aanwijzing mag zowel op openbare als private organen betrekking hebben. De Europese Commissie is bevoegd gedelegeerde handelingen vast te stellen met betrekking tot het opstellen van specifieke criteria waaraan die organen moeten voldoen (artikel 30, eerste en vierde lid, van de eidas-verordening).

Deze in de verordening gevolgde benadering sluit goeddeels aan bij de wijze waarop dit in de huidige Telecommunicatiewet is geregeld. Op grond van artikel 18.17a, eerste lid, is de Minister bevoegd een of meer instellingen aan te wijzen die zijn belast met het beoordelen van de overeenstemming van een veilig middel voor het aanmaken van elektronische handtekeningen met de eisen bedoeld in artikel 18.17 en het daartoe afgeven van verklaringen. Als gevolg van de verordening wordt de

werking van dit artikel verbreed tot gekwalificeerde middelen voor het aanmaken van elektronische handtekeningen en elektronische zegels. Daarnaast mogen ook in de nieuwe situatie bij of krachtens algemene maatregel van bestuur regels worden gesteld over de eisen waaraan instellingen moeten voldoen om voor een aanwijzing door de Minister in aanmerking te komen. Daar wordt evenwel in het tweede lid aan toegevoegd dat dit niet kan als de Europese Commissie specifieke criteria vaststelt waaraan door de lidstaten aangewezen organen moeten voldoen. In dat geval wordt dan op basis van de verordening met rechtstreekse werking al voorzien in die eisen.

De door de Minister aangewezen organen die bevoegd zijn verleners van middelen te certificeren, moeten hun certificering baseren op een veiligheidsbeoordeling uitgevoerd in overeenstemming met door de Europese Commissie vastgestelde normen inzake de veiligheidsbeoordeling van producten op het gebied van informatietechnologie. Die normen zijn in een door de Commissie vastgestelde lijst opgenomen. In plaats van de veiligheidsbeoordeling uit te voeren aan de hand van die vastgestelde normen, mag een gecertificeerde instelling dit ook doen op basis van een ander proces. Voorwaarde daarbij is dat er geen vastgestelde normen zijn of wanneer een veiligheidsbeoordeling op grond van vastgestelde normen gaande is. Verder dient dit proces vergelijkbare beveiligingsniveaus te hanteren en de gecertificeerde instelling de Commissie van dat andere proces op de hoogte stellen.

De door de Minister aangewezen certificeringsinstellingen zijn op grond van het nieuw ingevoegde zesde lid gehouden binnen twee weken nadat een veiligheidsbeoordeling resulteert in een positief oordeel de Minister daarover te informeren. En ingevolge het zevende lid kunnen over de daartoe te verstrekken gegevens en wijze van verstrekking bij of krachtens algemene maatregel van bestuur regels worden gesteld. Deze informatieverplichting is noodzakelijk om de Minister in staat te stellen te voldoen aan verplichtingen tot informatieverstrekking aan de Europese Commissie over gekwalificeerde middelen voor het aanmaken van elektronische handtekeningen en elektronische zegels. Over de inhoud van die informatieverplichtingen kan de Commissie op basis van uitvoeringshandelingen formaten en procedures vaststellen. De ontvangen informatie gebruikt de Commissie voor het opstellen van een lijst van gecertificeerde gekwalificeerde middelen als aangeduid. Deze lijst publiceert de Commissie en wordt bijgehouden (artikel 31 en 39, derde lid, van de eidas-verordening)

Onderdeel T, artikel 18.18
De verordening bepaalt dat verleners van vertrouwensdiensten die niet over de status gekwalificeerd beschikken en die de intentie hebben gekwalificeerde vertrouwensdiensten te gaan leveren, bij het toezichthoudend orgaan een kennisgeving van hun voornemen moeten indienen, evenals een door een conformiteitsbeoordelingsorgaan afgegeven conformiteitsbeoordelingsverslag (artikel 21, eerste lid). En zij mogen vervolgens niet eerder beginnen met het verlenen van de gekwalificeerde vertrouwensdienst nadat de status van gekwalificeerde is opgenomen in de vertrouwenslijst (artikel 21, derde lid). Deze voorschriften zijn ook van toepassing op een verlener van gekwalificeerde vertrouwensdiensten waarvan de status gekwalificeerd is beëindigd. Die verlener zal dan wederom de gehele procedure voor de toekenning van de status gekwalificeerd met succes dienen te doorlopen. Gelet hierop is handhaving van een met artikel 18.18 vergelijkbare bepaling voor gekwalificeerde verleners van vertrouwensdiensten niet nodig en niet goed verenigbaar met de rechtstreekse werking van de verordening. Tegen verleners van vertrouwensdiensten die zich niet aan deze bepalingen houden kunnen bestuurlijke maatregelen worden getroffen. Het toezicht op de naleving strekt zich uitdrukkelijk ook uit tot de artikelen 21, eerste en derde lid, van de eidas-verordening. Dit omvat daarmee tevens verleners van vertrouwensdiensten die hun diensten als gekwalificeerd aanbieden, terwijl zij niet of niet langer over de status gekwalificeerd beschikken voor henzelf en voor hun diensten. Tegen verleners van vertrouwensdiensten die moedwillig zich als gekwalificeerd presenteren of hun vertrouwensdiensten als zodanig aanbieden kunnen derhalve bestuurlijke maatregelen worden getroffen, zoals het opleggen van een boete. Er is vanaf gezien de mogelijkheid van strafrechtelijk sanctioneren op grond van de Wet op de economische delicten met dit wetsvoorstel te herintroduceren. In het kader van de Instellingswet Autoriteit Consument en Markt is afgezien van de mogelijkheid van strafrechtelijke handhaving naast bestuursrechtelijke handhaving door ACM. Dit

heeft geleid tot het schrappen van enkele verwijzingen in de Wet op de Economische Delicten die betrekking hadden op onder meer de eisen die gesteld worden aan het mogen aanbieden van gekwalificeerde certificaten. In dit wetsvoorstel berust het toezicht op het verlenen van vertrouwensdiensten niet bij ACM maar bij de Minister. Dit enkele verschil heeft in dit geval niet geleid tot het alsnog herintroduceren in het wetsvoorstel van strafrechtelijke handhaving ten aanzien van gekwalificeerde vertrouwensdiensten. Daarbij is meegewogen dat anders dan onder de huidige Telecommunicatiewet het toezicht zich tevens uitstrekt tot niet-gekwalificeerde verleners van vertrouwensdiensten. Bevoegdheden zoals het vorderen van inlichtingen (artikel 18.7) of het opvragen daarvan bij andere bestuursorganen in het kader van toezicht (artikel 18.3a) strekken zich ten principale ook uit tot verleners van niet-gekwalificeerde vertrouwensdiensten die zich ten onrechte voordoen als gekwalificeerde verleners. Er is voorts in de praktijk niet gebleken dat er behoefte bestaat aan verdergaande onderzoeksbevoegdheden zoals het strafrecht die biedt.

Onderdeel U, artikel 18.22
In dit onderdeel wordt geregeld dat de eidas-verordening kenbaar is te raadplegen via de in de Staatscourant opgegeven vindplaats.

Onderdeel V, artikel 20.15a
Door de voorgestelde wijziging in het toezicht zal de verantwoordelijkheid voor verschillende activiteiten, waaronder het toezicht overgaan van ACM op door de Minister aangewezen ambtenaren (Agentschap Telecom). Dit artikel bevat overgangsrecht ten aanzien van aanvragen, besluiten, bezwaar- en beroepschriften, rechtsgedingen, overeenkomsten en diverse andere zaken. Het overgangsrecht beperkt zich ingevolge het eerste lid uitsluitend tot hetgeen betrekking heeft op certificatiedienstverleners of gekwalificeerde certificaten.

Onderdeel W, artikel 20.16
Het bestaande artikel 20.16 voorziet in voorschriften betreffende de verstrekking van gegevens ten behoeve van de registratie van certificatiedienstverleners, waarbij tevens verschillende situaties inzake overgangsrecht worden onderscheiden. Doordat de registratie op de vertrouwenslijst met rechtstreekse werking is geregeld in de verordening en bestaande certificatiedienstverleners ingevolge artikel 51, derde lid, van de verordening worden aangemerkt als gekwalificeerde verleners van vertrouwensdiensten, zullen reeds geregistreerde certificatiedienstverleners op de door Agentschap Telecom op te stellen en bij te houden vertrouwenslijst geregistreerd worden als gekwalificeerde verleners van vertrouwensdiensten voor gekwalificeerde certificaten voor elektronische handtekeningen. Artikel 20.16 vervalt in het wetsvoorstel.

Onderdeel Y, artikel 20.15a
Dit onderdeel betreft een verbetering van een technische omissie.

Artikel II (artikelen 3:15a tot en met 15c BW)

De artikelen 3:15a tot en met c BW betreffen de implementatie van enkele bepalingen uit de Richtlijn elektronische handtekeningen. Artikel 3:15a geeft regels met betrekking tot de elektronische handtekening en bepaalt onder meer de voorwaarden voor het bestaan van rechtsgevolgen van elektronische handtekeningen en bevat definities. Artikel 3:15b BW bevat een regeling voor de erkenning van gekwalificeerde certificaten die buiten de Europese Gemeenschappen (hierna verder: EG) en Europese Economische Ruimte (hierna verder: EER) zijn afgegeven. Ingevolge artikel 3:15c BW zijn buiten het vermogensrecht de bepalingen van de artikelen 3:15a en 3:15b BW van overeenkomstige toepassing, voor zover de aard van de rechtshandeling of van de rechtsbetrekking zich daartegen niet verzet.

De intrekking van de richtlijn door de verordening en het geven van eigen regels op het terrein van de elektronische handtekening betekent dat de artikelen ter implementatie van de richtlijn dienen te vervallen. De verordening onderscheidt een elektronische handtekening, een geavanceerde

elektronische handtekening en een gekwalificeerde elektronische handtekening. Een elektronische handtekening is in de verordening gedefinieerd als gegevens in elektronische vorm die gehecht zijn aan of logisch verbonden zijn met andere gegevens in elektronische vorm en die door de ondertekenaar worden gebruikt om te ondertekenen (artikel 3, onder 10, van de verordening). Een geavanceerde elektronische handtekening is ingevolge artikel 3, onderdeel 11, een elektronische handtekening die voldoet aan de eisen van artikel 26. Dit houdt in dat de handtekening dient te voldoen aan de volgende eisen:
a)zij is op unieke wijze aan de ondertekenaar verbonden;
b)zij maakt het mogelijk de ondertekenaar te identificeren;
c)zij komt tot stand met gegevens voor het aanmaken van elektronische handtekeningen die de ondertekenaar, met een hoog vertrouwensniveau, onder zijn uitsluitend controle kan gebruiken,
d)zij is op zodanige wijze aan de daarmee ondertekende gegevens verbonden, dat elke wijziging achteraf van de gegevens kan worden opgespoord.
Een gekwalificeerde elektronische handtekening is een geavanceerde elektronische handtekening die is aangemaakt met een gekwalificeerd middel voor het aan maken van elektronische handtekeningen en die gebaseerd is op een gekwalificeerd certificaat voor elektronische handtekeningen (art. 3, onderdeel 12).
Zoals in het algemeen deel van de toelichting is aangegeven, bepaalt de verordening dat een gekwalificeerde elektronische handtekening hetzelfde rechtsgevolg heeft als een handgeschreven handtekening. De rechtsgevolgen van de overige handtekeningen zijn ter bepaling aan de lidstaten (zie paragraaf 6.1 en 6.2 van het algemeen deel). Voor de geavanceerde elektronische handtekening en enig andere gewone elektronische handtekening zijn de rechtsgevolgen in artikel 3:15a BW (nieuw) opgenomen. Hiervoor is aangesloten bij het huidige eerste lid van artikel 15a. Een geavanceerde elektronische handtekening als bedoeld in onderdeel 11, en een andere elektronische handtekening als bedoeld in onderdeel 10, van artikel 3 van de verordening hebben dezelfde rechtsgevolgen als een geschreven handtekening, indien de methode voor ondertekening die gebruikt is voldoende betrouwbaar is, gelet op het doel waarvoor de elektronische handtekening is gebruikt en op alle overige omstandigheden van het geval.

Het tweede lid van het huidige artikel 3:15a BW inzake het vermoeden van het bestaan van een rechtsgevolg van de gekwalificeerde elektronische handtekening dient te worden geschrapt, nu de verordening zoals gezegd bepaalt dat de gekwalificeerde elektronische handtekening hetzelfde rechtsgevolg heeft als een handgeschreven handtekening. De overige leden 3 tot en met 5 van artikel 3:15a BW hebben evenmin bestaansrecht meer. Het derde lid bepaalt dat een methode die voor authentificatie wordt gebruikt niet enkel op de in dit lid aangegeven gronden als onvoldoende betrouwbaar kan worden aangemerkt. De verordening geeft in artikel 25, eerste lid, een eigen regeling op dit punt en bepaalt dat het rechtsgevolg van een elektronische handtekening en de toelaatbaarheid ervan als bewijsmiddel in gerechtelijke procedures niet mogen worden ontkend louter op grond van het feit dat de handtekening elektronisch is of niet aan de eisen voor gekwalificeerde handtekeningen voldoet.

Het vierde lid en vijfde lid van het huidige artikel 3:15a BW geven definities van de begrippen elektronische handtekening en ondertekenaar op grond van de richtlijn. De verordening geeft omschrijvingen van deze begrippen in artikel 3, onderdeel 10 en onderdeel 9. Het zesde lid bepaalt dat van de leden 2 en 3 kan worden afgeweken. Zoals hiervoor is aangegeven vervallen deze leden en dient derhalve ook het zesde lid te vervallen.

Artikel 3:15b BW noemt drie voorwaarden voor de erkenning van gekwalificeerde certificaten afgegeven aan het publiek door een certificatiedienstverlener gevestigd in een derde land. Certificaten worden gelijkgesteld aan gekwalificeerde certificaten die door een in de EG of EER gevestigde certificatiedienstverlener worden afgegeven indien a) de certificatiedienstverlener voldoet aan de eisen in de richtlijn en in het kader van een in een lidstaat van de EG of EER ingestelde vrijwillige-accreditatieregeling is geaccrediteerd, danwel b) een in de EG of EER gevestigde certificatiedienstverlener die voldoet aan de richtlijn in staat voor dit certificaat of c) het certificaat of

de certificatiedienstverlener is erkend in het kader van een bilaterale of multilaterale overeenkomst tussen de EG of EER en derde landen of internationale organisatie. Zoals ook in paragraaf 5.11 en 5.12 is aangegeven, bevat de verordening in artikel 14 een eigen regeling inzake de verlening van vertrouwensdiensten door aanbieders uit derdelanden: erkenning vindt plaats op grond van een overeenkomst tussen de EU en een derdeland of internationale organisatie. Artikel 3:15b dient dan ook te vervallen.

Ingevolge artikel 3:15c BW vinden de artikelen van de betreffende afdeling (artikelen 15a en 15b) buiten het vermogensrecht van overeenkomstige toepassing, voor zover de aard van de rechtshandeling of van de rechtsbetrekking zich daartegen niet verzet. Het artikel ziet primair op privaatrechtelijke verhoudingen buiten de sfeer van het vermogensrecht, maar toepassing op andere rechtsgebieden is niet uitgesloten (Kamerstukken II 27 743 2001/01, nr. 3, blz. 11). Op verschillende plaatsen in de wetgeving wordt naar artikel 3:15a verwezen.
De regeling van de vertrouwensdiensten van de verordening strekt zich uit tot in beginsel alle domeinen. De regeling van de elektronische handtekening van de verordening geldt dan ook voor zowel het private als publieke domein. De voorgestelde bepaling in artikel 3:15a over de rechtsgevolgen voor de gewone en geavanceerde elektronische handtekening kan in beginsel eveneens van overeenkomstige toepassing worden verklaard voor andere rechtsgebieden buiten het vermogensrecht. In artikel 3:15c BW wordt daarom, op dezelfde voet als thans het geval is, bepaald dat artikel 3:15a BW buiten het vermogensrecht van overeenkomstige toepassing is.

Artikel III (artikel 6:196b BW)

Artikel 6:196b BW geeft een specifiek aansprakelijkheidsregime voor de certificatiedienstverlener die gekwalificeerde certificaten afgeeft aan het publiek. Met dit artikel is artikel 6 van de Richtlijn elektronische handtekening geïmplementeerd.
Doordat de verordening de Richtlijn elektronische handtekening intrekt, dient dit artikel ter implementatie van de richtlijn te vervallen. De verordening geeft in artikel 13 een eigen regeling voor aansprakelijkheid voor verleners van vertrouwensdiensten (zie paragraaf 5.9 en 5.10 van het algemeen deel van de toelichting).

Artikel IV (artikelen 7:655 en 932 BW)

Onderdeel A
Artikel 7:655 BW, derde lid, ziet op het verstrekken van een opgave door de werkgever aan de werknemer van elementen van de arbeidsovereenkomst. Wanneer dit elektronisch wordt gedaan, dient deze opgave te zijn voorzien van een handtekening die voldoet aan de eisen, bedoeld in artikel 3:15a, tweede lid, BW. Dit tweede lid bevat de onderdelen a tot en met f, dat wil zeggen de voorwaarden voor een gekwalificeerde elektronische handtekening. Het tweede lid van artikel 3:15a, dient te vervallen (zie paragraaf 6.2 van het algemeen deel en hiervoor bij artikel II). In artikel 3, onderdeel 12, van de verordening wordt de gekwalificeerde handtekening omschreven.
De verwijzing naar alle onderdelen van het tweede lid van artikel 3:15a BW dient derhalve te worden vervangen door een verwijzing naar artikel 3, onderdeel 12, van de verordening.

Onderdeel B
Artikel 7:932 BW ziet op het afgeven van een polis door de verzekeraar. Als dit een polis betreft die is opgemaakt op een wijze als bedoeld in artikel 156a lid 1 van het Wetboek van Burgerlijke Rechtsvordering (op elektronische wijze) moet de polis zijn voorzien van een elektronische handtekening die voldoet aan de eisen, bedoeld in het tweede lid van artikel 3:15a BW. Ook hier geldt dat met de inwerkingtreding van de verordening verwezen dient te worden naar de gekwalificeerde elektronische handtekening van artikel 3, onderdeel 12, van de verordening.

Artikel V (artikel 2:16 Awb)

Sinds de opname van Afdeling 2.3 van de Algemene wet bestuursrecht (hierna: Awb) over verkeer langs elektronische weg in de Awb, sluit de Awb wat betreft de elektronische handtekening aan bij het BW (Kamerstukken II 2001/02, 28 483, nr. 3, p. 18). Artikel 2:16 Awb strekt ertoe de elektronische handtekening gelijk te stellen met de handgeschreven handtekening, geeft een nadere uitwerking aan de betrouwbaarheid van de elektronische handtekening en maakt het mogelijk om aanvullende eisen te stellen bij wettelijk voorschrift. De mogelijkheid om nadere eisen te stellen volgde uit artikel 3, zevende lid, van de richtlijn inzake elektronische handtekeningen. De intrekking van de richtlijn door de verordening en de nieuwe regels over elektronische handtekeningen die de verordening geeft, nopen tot wijziging van artikel 2:16 Awb.

Onder een elektronische handtekening verstaat de verordening "gegevens in elektronische vorm die gehecht zijn aan of logisch verbonden zijn met andere gegevens in elektronische vorm en die door de ondertekenaar worden gebruikt om te ondertekenen." (artikel 3, onderdeel 10). De verordening onderscheidt drie soorten elektronische handtekeningen: gewone, geavanceerde en gekwalificeerde. Een geavanceerde elektronische handtekening is een elektronische handtekening die voldoet aan de eisen genoemd in artikel 26 van de verordening (te weten: a. zij is op unieke wijze aan de ondertekenaar verbonden, b. zij maakt het mogelijk de ondertekenaar te identificeren, c. zij komt tot stand met gegevens voor het aanmaken van elektronische handtekeningen die de ondertekenaar, met een hoog vertrouwensniveau, onder zijn uitsluitende controle kan gebruiken, en d. zij is op zodanige wijze aan de daarmee ondertekende gegevens verbonden, dat elke wijziging achteraf van de gegevens kan worden opgespoord (artikel 3, onderdeel 11). Een gekwalificeerde elektronische handtekening, ten slotte, is een geavanceerde elektronische handtekening die is aangemaakt met een gekwalificeerd middel voor het aanmaken van elektronische handtekeningen en die gebaseerd is op een gekwalificeerd certificaat voor elektronische handtekeningen (artikel 3, onderdeel 12).

Het eerste lid stelt buiten twijfel dat aan het vereiste van ondertekening niet alleen kan worden voldaan door een handgeschreven handtekening, maar ook door een elektronische handtekening. De tekst van deze volzin is zoveel mogelijk ongewijzigd gebleven. Aangezien het begrip elektronische handtekening in de verordening anders is gedefinieerd dan in de richtlijn, is het woord "authentificatie" vervangen door "ondertekening". Hierdoor is het artikel in overeenstemming gebracht met de nieuwe definitie uit de verordening. Uit artikel 25, tweede lid, van de verordening volgt dat een gekwalificeerde elektronische handtekening hetzelfde rechtsgevolg heeft als een handgeschreven handtekening. Een dergelijke handtekening die op een in een lidstaat afgegeven gekwalificeerd certificaat is gebaseerd, moet in alle lidstaten als een gekwalificeerde elektronische handtekening worden erkend (artikel 25, derde lid, verordening). De rechtsgevolgen van de andere elektronische handtekeningen dienen te worden vastgesteld door het nationale recht (zie overweging 22). Ook geavanceerde en andere elektronische handtekeningen kunnen hetzelfde rechtsgevolg hebben als een handgeschreven handtekening, indien de methode voor ondertekening die gebruikt is, voldoende betrouwbaar is, gelet op de aard en inhoud van het elektronische bericht en het doel waarvoor het is gebruikt . Op grond van het eerste lid van artikel 25 van de Verordening mogen het rechtsgevolg van een elektronische handtekening en de toelaatbaarheid ervan als bewijsmiddel in gerechtelijke procedures, niet worden ontkend louter op grond van het feit dat de handtekening elektronisch is of niet aan de eisen voor gekwalificeerde elektronische handtekeningen voldoet. Voor geavanceerde en gewone elektronische handtekeningen geldt dat om te beoordelen of in een bepaald geval een elektronische handtekening voldoende betrouwbaar is, dient te worden gelet op de aard en de inhoud van het bericht en het doel waarvoor het wordt gebruikt. Indien gelet op deze omstandigheden sprake is van een voldoende betrouwbare handtekening, heeft deze hetzelfde rechtsgevolg als een handgeschreven handtekening en kan deze derhalve niet door een bestuursorgaan worden geweigerd. In geval bij wettelijk voorschrift de gewone elektronische handtekening wordt voorgeschreven kunnen uiteraard in aanvullende voorschriften eisen worden gesteld aan de betrouwbaarheid van deze handtekening. Daaraan kan dan het bestuursorgaan de zekerheid ontlenen of de elektronische handtekening voldoende betrouwbaar is gelet de omstandigheden waarin deze wordt toegepast of moet worden gevraagd. Zo kunnen bijvoorbeeld eisen worden gesteld aan het niveau van authenticatie op basis waarvan de elektronische handtekening wordt aangemaakt. Ook kunnen eisen

worden gesteld aan de onafhankelijkheid en veiligheid van het mechanisme waarmee de gegevens die dienen ter ondertekening, aan het te ondertekenen document, bericht of de gestandaardiseerde gegevensset worden gehecht Evenzo kunnen bijvoorbeeld aanvullende eisen worden gesteld aan de elektronische handtekening die door middel van een tablet wordt gezet.

De verwijzing in artikel 2:16 Awb naar artikel 3:15a, tweede tot en met zesde lid, en artikel 3:15b BW is komen te vervallen omdat deze bepalingen in het BW eveneens vervallen. De verordening geeft eigen regels over de onderwerpen die in deze artikelen geregeld waren.
Er bestaan vele soorten elektronische handtekeningen, maar niet elke handtekening is in het licht van het doel waarvoor de elektronische gegevens werden gebruikt, de aard van de rechtsverhouding tussen de ondertekenaar en het bestuursorgaan of de overige omstandigheden van het geval geschikt om in aanmerking te komen voor juridische gelijkstelling met een handgeschreven handtekening. Daarom maakt het tweede lid het mogelijk dat bij wettelijk voorschrift het gebruik van een bepaald type elektronische handtekening wordt voorgeschreven (vlg. ook artikel 27, eerste en tweede lid, van de verordening). Het tweede lid vervangt de volzin in het artikel waarin werd bepaald dat bij wettelijk voorschrift aanvullende eisen kunnen worden gesteld. Deze volzin werd destijds opgenomen omdat dit uit de richtlijn volgde. Nu de richtlijn is ingetrokken en een vergelijkbare bepaling niet is teruggekomen in de verordening, komt de mogelijkheid om aanvullende eisen te stellen dan ook te vervallen.

Volledigheidshalve wordt hier opgemerkt dat de nadere eisen die op grond van artikel 2:15,eerste lid, Awb kunnen worden gesteld aan het gebruik van de elektronische weg, geen betrekking kunnen hebben op elektronische handtekeningen.

Artikel VI (artikel 1072b Wet boek van Burgerlijke Rechtsvordering)

In artikel 1072b is mogelijk gemaakt dat het arbitrale vonnis van artikel 1057, tweede lid, Rv ook kan worden opgemaakt in elektronische vorm door het te voorzien van een elektronische handtekening die voldoet aan het bepaalde in artikel 3:15a, eerste en tweede lid, BW. Er moet voldaan zijn aan de vereisten voor een gekwalificeerde elektronische handtekening. Daar artikel 3:15a, tweede lid, vervalt (zie paragraaf 6.2 van het algemeen deel en hiervoor bij artikel II) en de verordening in artikel 3, onderdeel 12, een omschrijving van de gekwalificeerde elektronische handtekening bevat, dient voortaan te worden verwezen naar dit artikel 3, onderdeel 12, van de verordening.

Artikelen VII tot en met IX (artikel 7e, Kadasterwet, artikel 8.2, Wet handhaving consumentenbescherming, artikel 35, vierde lid, Wet op de omzetbelasting 1968)

In artikel 7e van de Kadasterwet, eerste lid, is bepaald dat indien in die wet wordt voorgeschreven dat een document van een elektronische handtekening wordt voorzien, een elektronische handtekening wordt gebruikt die voldoet aan de eisen, genoemd in artikel 15a, tweede lid, onderdelen a tot en met f, van Boek 3 van het Burgerlijk Wetboek. Steeds moet voldaan zijn aan de voorwaarden gesteld aan een elektronische gekwalificeerde handtekening. Artikel 3:15a, tweede lid, vervalt (zie paragraaf 6.2 van het algemene deel van de toelichting en hiervoor bij artikel II). Verwezen dient in dit artikel te worden naar artikel 3, onderdeel 12, van de verordening.
Het derde lid van artikel 7e van de Kadasterwet vervalt. Destijds volgde uit de richtlijn dat de lidstaten aanvullende eisen konden stellen aan de elektronische handtekening. Nu de richtlijn is ingetrokken en een vergelijkbare bepaling niet is teruggekomen in de verordening, dient de mogelijkheid om aanvullende eisen te stellen dan ook te vervallen.

In artikel 8.2, eerste lid, van de Wet handhaving consumentenbescherming is bepaald dat degene die een dienst van een informatiemaatschappij verleent als bedoeld in de artikelen 15d, eerste en tweede lid, van Boek 3 BW, de artikel 15a tot en met 15c in acht dient te nemen. In dit lid wordt rekening gehouden met het vervallen van artikel 15b van Boek 3 van het Burgerlijk Wetboek (zie paragraaf 5.12 van het algemeen deel van de toelichting).

In het vierde lid van artikel 35b van de Wet op de omzetbelasting 1968 wordt aangegeven met welke technologieën de authenticiteit van de herkomst en de integriteit van de inhoud van een elektronische factuur kunnen worden gewaarborgd. In onderdeel a van dit lid wordt verwezen naar een geavanceerde handtekening van de Richtlijn elektronische handtekeningen die gebaseerd is op een gekwalificeerd certificaat en aangemaakt wordt met een veilig middel, derhalve naar een gekwalificeerde elektronische handtekening. Deze verwijzing dient vervangen te worden door een verwijzing naar de gekwalificeerde elektronische handtekening van de verordening.

Artikel X (artikel 34a Wet bescherming persoonsgegevens)

In het voorgestelde artikel worden verleners van vertrouwensdiensten uitgezonderd van de meldplicht op grond van het nog in werking te treden artikel 34a van de Wet bescherming persoonsgegevens. De meldplicht door verleners van vertrouwensdiensten aan het Cbp op basis van de verordening is in het wetsvoorstel door middel van een wijziging van de Telecommunicatiewet geregeld. Dit biedt de mogelijkheid specifiek rekening te houden met de rechtstreekse werking van de verordening ten aanzien van de norm op basis waarvan gemeld dient te worden, degenen aan wie gemeld dient te worden, en indien de Europese Commissie hiervoor uitvoeringshandelingen vaststelt ook de bij een melding te overleggen gegevens.

Artikelen XI en XII
PM samenloop met wetsvoorstellen die de Telecommunicatiewet wijzigen; aanpassen na consultatie op basis van actuele stand van zaken.

PM aanpassen 30c Rv en 8:36d Awb in wv 34059

Artikelen XIII

Dit artikel regelt diverse situaties van overgangsrechtelijke aard. Het betreft gevallen waarin een aanvraag door een certificatiedienstverlener is ingediend tot registratie onder de huidige Telecommunicatiewet of tot aanwijzing van een instelling die veilige middelen op overeenstemming beoordeeld met wettelijke eisen, en de behandeling van die aanvraag nog niet is afgerond als dit wetsvoorstel tot wet wordt verheven en in werking is getreden. Deze aanvragen worden dan behandeld als aanvragen onder het nieuwe wettelijk kader. Het betreft voorts situaties van bezwaar of beroep waarvoor is bepaald dat het recht van toepassing is zoals dat gold voordat dit wetsvoorstel tot wet wordt verheven en inwerking treedt. Ook wordt voorzien in de continuering van de aanwijzing van instellingen die veilige middelen op overeenstemming beoordelen met wettelijke eisen, zodat die niet hiervoor een nieuwe aanvraag hoeven in te dienen.

III. IMPLEMENTATIETABEL

Verordening 2014/910/EU	**Telecommunicatiewet, Burgerlijk Wetboek en Algemene wet bestuursrecht**	**Omschrijving beleidsruimte**	**Toelichting op keuze bij invulling beleidsruimte**
Artikel 1	Rechtstreekse werking volstaat.		
Artikel 2	Artikel I, onderdeel F (artikel 2.5a, Telecommunicatiewet)		
Artikel 3	Artikel I, onderdeel A		

	(artikel 1.1, Telecommunicatiewet), alsmede artikelen VI, artikel VII, eerste lid, artikel VIII, artikel IX		
Artikel 4	Rechtstreekse werking volstaat.		
Artikel 5, eerste lid	Artikel I, onderdeel G (artikel 11.5b, Telecommunicatiewet), alsmede artikel I, onderdeel F (artikel 2.5e, Telecommunicatiewet) en paragraaf 8 van het algemeen deel van de memorie van toelichting.		
Artikel 6, eerste lid	Feitelijke uitvoering m.b.v. een technische voorziening, een koppelpunt. Waarborging naleving op basis Wet Naleving Europese regelgeving publieke entiteiten.		
Artikel 6, tweede lid	Rechtstreekse werking volstaat.		
Artikel 7	Van mogelijkheid is (nog) geen gebruik gemaakt.	Mogelijkheid voor lidstaat stelsel voor elektronische identificatie aan te melden bij de Europese Commissie	De verplichte erkenning van aangemelde stelsels is van toepassing vanaf september 2018. Ten tijde van de totstandkoming van dit wetsvoorstel heeft besluitvorming over het aanmelden van een stelsel door Nederland nog niet plaatsgevonden.
Artikel 8, eerste en tweede lid	Rechtstreekse werking volstaat.		
Artikel 8, derde lid	De bepalingen richten zich tot de Europese Commissie		
Artikel 9, eerste lid	Rechtstreekse werking volstaat.		
Artikel 9, tweede en derde lid	De bepalingen richten zich tot de Europese Commissie		
Artikel 9, vierde lid	Rechtstreekse werking volstaat.		
Artikel 9, vijfde lid	De bepalingen richten zich tot de Europese Commissie		
Artikel 10	Rechtstreekse werking volstaat.		
Artikel 11, eerste tot en met derde lid	Rechtstreekse werking volstaat.		
Artikel 11, vierde en vijfde lid	Rechtstreekse werking volstaat. Regels inzake aansprakelijkheid zijn		

	onderdeel van Boek 6 van het Burgerlijk Wetboek		
Artikel 12, eerste tot en met zesde lid	Rechtstreekse werking volstaat.		
Artikel 12, zevende tot en met negende lid	De bepalingen richten zich tot de Europese Commissie.		
Artikel 13, eerste en tweede lid	Artikel III (artikel 196b, van Boek 6 BW).		
Artikel 13, derde lid	Regels inzake aansprakelijkheid zijn onderdeel van Boek 6 van het Burgerlijk Wetboek		
Artikel 14	Artikel II, onderdeel B (artikel 15b van Boek 3 BW)		
Artikel 15	Rechtstreekse werking volstaat.		
Artikel 16	Bevoegdheden tot handhaving van naleving zijn gekoppeld aan het zijn van toezichthouder (Artikel I, onderdeel I (artikel 15.1, Telecommunicatiewet); voorts Wet naleving Europese regelgeving publieke entiteiten voor voorschriften gericht tot openbare instanties.		
Artikel 17, eerste lid, eerste volzin	Artikel I, onderdeel L (artikel 18.2a, tweede lid, Telecommunicatiewet)		
Artikel 17, eerste lid, tweede volzin	Artikel I, onderdeel I (artikel 15.1, eerste lid, Telecommunicatiewet), onderdeel J (artikelen15.3b, tweede en derde lid en 15.3d, derde lid, Telecommunicatiewet), onderdeel M (artikel 18.3a, Telecommunicatiewet), onderdeel N (artikel 18.7, eerste lid, Telecommunicatiewet)		
Artikel 17, tweede lid	Feitelijke uitvoering.		
Artikel 17, derde lid	Rechtstreekse werking volstaat.		
Artikel 17, vierde lid, onderdeel a	Artikel I, onderdeel J (artikelen 15.3b tot en met 15.3d, Telecommunicatiewet)		
Artikel 17, vierde lid, onderdeel b	Artikel I, onderdeel Q		
Artikel 17, vierde lid, onderdeel c	Rechtstreekse werking volstaat.		
Artikel 17, vierde lid, onderdeel d	Rechtstreekse werking volstaat.		

Artikel 17, vierde lid, onderdeel e	Artikel I, onderdeel Q		
Artikel 17, vierde lid, onderdeel f	Rechtstreekse werking volstaat.		
Artikel 17, vierde lid, onderdeel g	Artikel I, onderdeel F (artikelen 2.5b en 2.5d, Telecommunicatiewet)		
Artikel 17, vierde lid, onderdeel h		Het toezichthoudend orgaan brengt het voor de nationale vertrouwenslijst verantwoordelijke orgaan op de hoogte van statustoekenning of –intrekking, tenzij dit orgaan ook het toezichthoudend orgaan is.	De Minister van Economische Zaken is verantwoordelijk voor de vertrouwenslijst en is tevens toezichthoudend orgaan.
Artikel 17, vierde lid, onderdeel i	Rechtstreekse werking volstaat.		
Artikel 17, vierde lid, onderdeel j	Artikel I, onderdeel I (artikel 15.1, Telecommunicatiewet)		
Artikel 17, vijfde lid	Van mogelijkheid is geen gebruik gemaakt.	Mogelijkheid dat het toezichthoudend orgaan een vertrouwensinfrastructuur opzet en onderhoudt	
Artikel 17, zesde lid	Rechtstreekse werking volstaat.		
Artikel 17, zevende en achtste lid	Bepaling richt zich tot de Europese Commissie.		
Artikel 18, eerste lid	Artikel I, onderdeel J (artikel 15.3b, Telecommunicatiewet)		
Artikel 18, tweede lid	Artikel I, onderdeel J (artikel 15.3c, Telecommunicatiewet)		
Artikel 18, derde lid	Artikel I, onderdeel J (artikel 15.3d, Telecommunicatiewet)		
Artikel 19, eerste lid	Behoeft naar zijn aard geen implementatie in wetgeving		
Artikel 19, tweede lid, eerste alinea	Artikel I, onderdeel H (artikel 11.5c, Telecommunicatiewet), onderdeel L (artikel 18.2a, tweede lid, Telecommunicatiewet), onderdeel P (artikelen 18.15a. eerste lid en 18.15b, Telecommunicatiewet)		
Artikel 19, tweede lid, tweede alinea	Artikel I, onderdeel P (artikel 18.15a. tweede lid, Telecommunicatiewet)		
Artikel 19, tweede lid, derde alinea	Rechtstreekse werking volstaat.		
Artikel 19, tweede	Rechtstreekse werking		

lid, vierde alinea	volstaat.		
Artikel 19, derde lid	Rechtstreekse werking volstaat.		
Artikel 19, vierde lid	Artikel I, onderdeel P (artikelen 18.15a. eerste lid en 18.15b, Telecommunicatiewet)		
Artikel 20, eerste en tweede lid,	Artikel I, onderdeel Q		
Artikel 20, derde lid	Artikel I, onderdeel F (artikel 2.5d, Telecommunicatiewet)		
Artikel 20, vierde lid	Bepaling richt zich tot Europese Commissie.		
Artikel 21, eerste lid	Artikel I, onderdeel F (artikel 2.5b) en Q (Telecommunicatiewet)		
Artikel 21, tweede lid	Artikel I, onderdeel Q (Telecommunicatiewet)		
Artikel 21, derde lid	Rechtstreekse werking volstaat. Voorts onderdeel T (artikel 18.18 van de Telecommunicatiewet)		
Artikel 21, vierde lid	Bepaling richt zich tot Europese Commissie.		
Artikel 22 , eerste lid	Artikel I, onderdeel F (artikel 2.5c, Telecommunicatiewet)		
Artikel 22, tweede lid	Rechtstreekse werking volstaat.		
Artikel 22, derde lid	Artikel I, onderdeel F (artikel 2.5c, Telecommunicatiewet)	Het verantwoordelijk orgaan is de Minister van Economische Zaken	
Artikel 22, vierde lid	Bepaling richt zich tot Europese Commissie.		
Artikel 22, vijfde lid	Bepaling richt zich tot Europese Commissie.		
Artikel 23	Rechtstreekse werking volstaat.		
Artikel 24, eerste lid, aanhef en onder a	Artikel I, onderdeel P (artikelen 18.15c, 18.15e, 18.15f, Telecommunicatiewet)		
Artikel 24, eerste lid, aanhef en onder b	Artikel I, onderdeel P (artikelen 18.15d, eerste lid, 18.15e, 18.15f, Telecommunicatiewet)		
Artikel 24, eerste lid, aanhef en onder c	Artikel I, onderdeel P (artikelen 18.15d, tweede lid, 18.15e, 18.15f, Telecommunicatiewet)		
Artikel 24, eerste lid, aanhef en onder d		Van mogelijkheid tot verificatie op basis van andere op nationaal niveau erkende identificatiemethoden is geen geen gebruik gemaakt	

Artikel 24, tweede tot en met vierde lid	Artikel I, onderdeel O (artikel 18.15, Telecommunicatiewet)		
Artikel 24, vijfde lid	Bepaling richt zich tot Europese Commissie.		
Artikelen 25 en 26	Artikel II, onderdelen A en C (artikelen 15a en 15c, Boek 3 BW) en artikel V (artikel 2:16, Awb)		
Artikel 27, eerste en tweede lid	Feitelijke uitvoering voor openbare instanties mogelijk met behulp van valideringsdienst Ondernemersplein. Waarborgen naleving op basis van Wet naleving Europese regelgeving publieke entiteiten.		
Artikel 27, derde lid	Rechtstreekse werking volstaat. Voorts artikel VII (artikel 7e, Kadasterwet)		
Artikel 27, vierde en vijfde lid	Bepaling richt zich tot Europese Commissie.		
Artikel 28, eerste lid	Artikel I, onderdeel O (artikel 18.15, Telecommunicatiewet)		
Artikel 28, tweede tot en met vierde lid	Rechtstreekse werking volstaat.		
Artikel 28, vijfde lid	Van mogelijkheid is geen gebruik gemaakt.	Van mogelijkheid tot vaststellen regels inzake tijdelijke schorsing gekwalificeerd certificaat voor elektronische handtekeningen is geen gebruik gemaakt.	
Artikel 28, zesde lid	Bepaling richt zich tot Europese Commissie.		
Artikel 29, eerste lid	Artikel I, onderdeel O (artikel 18.15, Telecommunicatiewet)		
Artikel 29, tweede lid	Bepaling richt zich tot Europese Commissie		
Artikel 30, eerste lid	Onderdelen R (artikel 18.17, Telecommunicatiewet) en S (artikel 18.17a, Telecommunicatiewet)		
Artikel 30, tweede lid	Rechtstreekse werking volstaat.		
Artikel 30, derde lid	Onderdeel S (artikel 18.17a, Telecommunicatiewet)		
Artikel 30, vierde lid	Bepaling richt zich tot Europese Commissie		
Artikel 31, eerste lid	Onderdeel S (artikel 18.17a, zesde en zevende lid, Telecommunicatiewet)		
Artikel 31, tweede en derde lid	Bepaling richt zich tot de Europese Commissie.		

Artikel 32, eerste en tweede lid	Rechtstreekse werking volstaat.		
Artikel 32, derde lid	Artikel I, onderdeel O (artikel 18.15, onder a, van de Telecommunicatiewet)	Indien Commissie geen referentienummers vaststelt, dan mogelijkheid dit nationaal te doen.	Vanuit belang van veiligheid is het wenselijk nationaal referentienummers vast te stellen, zolang de Europese Commissie hierin niet voorziet.
Artikel 33, eerste lid	Rechtstreekse werking volstaat		
Artikel 33, tweede lid	Artikel I, onderdeel O (artikel 18.15, onder a, van de Telecommunicatiewet)	Indien Commissie geen referentienummers vaststelt, dan mogelijkheid dit nationaal te doen.	Vanuit belang van veiligheid is het wenselijk nationaal referentienummers vast te stellen, zolang de Europese Commissie hierin niet voorziet.
Artikel 34, eerste lid	Rechtstreekse werking volstaat		
Artikel 34, tweede lid	Artikel I, onderdeel O (artikel 18.15, onder a, van de Telecommunicatiewet)	Indien Commissie geen referentienummers vaststelt, dan mogelijkheid dit nationaal te doen.	Vanuit belang van veiligheid is het wenselijk nationaal referentienummers vast te stellen, zolang de Europese Commissie hierin niet voorziet.
Artikel 35	Rechtstreekse werking volstaat		
Artikel 36	Rechtstreekse werking volstaat		
Artikel 37, eerste tot en met derde lid	Rechtstreekse werking volstaat; Wet Naleving Europese regelgeving publieke entiteiten		
Artikel 37, vierde en vijfde lid	Bepaling richt zich tot de Europese Commissie		
Artikel 38, eerste tot en met vierde lid	Rechtstreekse werking volstaat		
Artikel 38, vijfde lid	Van mogelijkheid geen gebruik gemaakt.	Mogelijkheid voor lidstaten nationale regels vast te stellen inzake tijdelijke schorsing van gekwalificeerde certificaten voor elektronische zegels	Zie paragraaf 5.6, laatste alinea van het algemeen deel van de memorie van toelichting.
Artikel 38, zesde lid	Artikel I, onderdeel O (Artikel 18.15, onder a, van de Telecommunicatiewet)	Indien Commissie geen referentienummers vaststelt, dan mogelijkheid dit nationaal te doen.	Vanuit belang van veiligheid is het wenselijk nationaal referentienummers vast te stellen, zolang de Europese Commissie hierin niet voorziet.

Artikel 39 , eerste lid	Artikel I, onderdeel O (artikel 18.15, onder b, van de Telecommunicatiewet)	Indien Commissie geen referentienummers vaststelt, dan mogelijkheid dit nationaal te doen.	Vanuit belang van veiligheid is het wenselijk nationaal referentienummers vast te stellen, zolang de Europese Commissie hierin niet voorziet.
Artikel 39, tweede lid	Artikel I, onderdelen R (artikel 18.17, Telecommunicatiewet) en S (artikel 18.17a, Telecommunicatiewet)		
Artikel 39, derde lid	Artikel I, onderdeel S (artikel 18.17a, zesde en zevende lid, Telecommunicatiewet)		
Artikel 40	Artikel I, onderdeel O, (artikel 18.15, onder a, van de Telecommunicatiewet)	Indien Commissie geen referentienummers vaststelt, dan mogelijkheid dit nationaal te doen.	Vanuit belang van veiligheid is het wenselijk nationaal referentienummers vast te stellen, zolang de Europese Commissie hierin niet voorziet.
Artikel 41	Rechtstreekse werking volstaat.		
Artikel 42, eerste lid	Rechtstreekse werking volstaat.		
Artikel 42, tweede lid	Artikel I, onderdeel O (artikel 18.15, onder a, van de Telecommunicatiewet)	Indien Commissie geen referentienummers vaststelt, dan mogelijkheid dit nationaal te doen.	Vanuit belang van veiligheid is het wenselijk nationaal referentienummers vast te stellen, zolang de Europese Commissie hierin niet voorziet.
Artikel 43	Rechtstreekse werking volstaat.		
Artikel 44, eerste lid	Rechtstreekse werking volstaat.		
Artikel 44, tweede lid	Artikel I, onderdeel O (artikel 18.15, onder a, van de Telecommunicatiewet)	Indien Commissie geen referentienummers vaststelt, dan mogelijkheid dit nationaal te doen.	Vanuit belang van veiligheid is het wenselijk nationaal referentienummers vast te stellen, zolang de Europese Commissie hierin niet voorziet.
Artikel 45, eerste lid	Rechtstreekse werking volstaat.		
Artikel 45, tweede lid	Artikel I, onderdeel O (artikel 18.15, onder a, van de Telecommunicatiewet)	Indien Commissie geen referentienummers vaststelt, dan mogelijkheid dit nationaal te doen.	Vanuit belang van veiligheid is het wenselijk nationaal referentienummers vast te stellen, zolang de Europese Commissie hierin

			niet voorziet.
Artikel 46	Rechtstreekse werking volstaat.		
Artikel 47	Bepalingen richten zich tot de Europese Commissie.		
Artikel 48	Bepalingen richten zich tot de Europese Commissie.		
Artikel 49	Bepalingen richten zich tot de Europese Commissie.		
Artikel 50	Rechtstreekse werking volstaat.		
Artikel 51	Rechtstreekse werking volstaat (zie paragraaf 9.2 van het algemeen deel van de memorie van toelichting)		
Artikel 52	Rechtstreekse werking volstaat.		
Bijlage I	Rechtstreekse werking volstaat.		
Bijlage II	Rechtstreekse werking volstaat.		
Bijlage III	Rechtstreekse werking volstaat.		
Bijlage IV	Rechtstreekse werking volstaat.		

De Minister van Economische Zaken,

De Minister van Veiligheid en Justitie,

De Minister van Binnenlandse Zaken en Koninkrijksrelaties