Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2011–2012

22 112 Nieuwe Commissievoorstellen en initiatieven van de lidstaten van de Europese Unie

Nr. 1439 **BRIEF VAN DE STAATSSECRETARIS VAN BUITENLANDSE ZAKEN**

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 13 juli 2012

Overeenkomstig de bestaande afspraken heb ik de eer u hierbij zes fiches aan te bieden die werden opgesteld door de werkgroep Beoordeling Nieuwe Commissievoorstellen (BNC).

Fiche 1: Verordening elektronische identificatie en vertrouwensdiensten
Fiche 2: Verordening gebruik EURODAC voor strafrechtelijke onderzoeken (Kamerstuk 22 112, nr. 1440)
Fiche 3: Mededeling hernieuwbare energie (Kamerstuk 22 112, nr. 1441)
Fiche 4: Mededeling vangstmogelijkheden 2013 (Kamerstuk 22 112, nr. 1442)
Fiche 5: Mededeling EU-strategie uitroeiing mensenhandel 2012–2016 (Kamerstuk 22 112, nr. 1443)
Fiche 6: Mededeling ultraperifere regio's van de Europese Unie (Kamerstuk 22 112, nr. 1444)

De staatssecretaris van Buitenlandse Zaken,
H. P. M. Knapen

kst-22112-1439
ISSN 0921 - 7371
's-Gravenhage 2012

Fiche: verordening elektronische identificatie en vertrouwensdiensten

1. Algemene gegevens

Titel voorstel
Verordening van het Europees Parlement en de Raad betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt

Datum Commissiedocument
4 juni 2012

Nr. Commissiedocument
COM(2012) 238

Prelex
http://ec.europa.eu/prelex/detail_dossier_real.cfm?CL=nl&DosId=201689

Nr. Impact Assessment Commissie en Opinie Impact Assessment Board
SWD (2012) 135

Behandelingstraject Raad
Raad voor Vervoer, Telecom en Energie.

Eerstverantwoordelijk ministerie
Ministerie van Economische Zaken, Landbouw en Innovatie in nauwe samenwerking met de ministeries van Binnenlandse Zaken en Koninkrijksrelaties en van Veiligheid en Justitie.

Rechtsbasis, besluitvormingsprocedure Raad, rol Europees Parlement, gedelegeerde en/of uitvoeringshandelingen

a) *Rechtsbasis*
   Artikel 114 VWEU
b) *Besluitvormingsprocedure Raad en rol Europees Parlement*
   Gewone wetgevingsprocedure conform art. 294 VWEU. De Raad stemt met gekwalificeerde meerderheid; het Europees Parlement heeft medebeslissingsrecht.
c) *Gedelegeerde en/of uitvoeringshandelingen*
   Er is voorzien in de vaststelling van een groot aantal gedelegeerde handelingen (art. 290 VWEU) en in de vaststelling van uitvoeringshandelingen door de Commissie (art. 291 VWEU). Gedelegeerde handelingen worden aangekondigd in de artikelen 8 lid 3, 13 lid 5, 15 lid 5, 16 lid 5, 18 lid 5, 20 lid 6, 21 lid 4, 23 lid 3, 25 lid 2, 27 lid 2, 28 lid 6, 29 lid 4, 30 lid 2, 31, artikel 35 lid 3, en artikel 37 lid 3.
   Uitvoeringshandelingen zijn voorzien op grond van de artikelen 7 lid 4, 8 lid 2, 13 lid 6, 14 lid 4, 15 lid 5, 16 lid 6, 17 lid 5, 18 lid 6, 19 lid 5, 20 lid 7, 21 lid 5, 22 lid 2, 23 lid 1, 24 lid 3, 25 lid 3, 26 lid 2, 27 lid 4, 28 lid 7, 29 lid 5, 33 lid 2, 34 lid 4, 36 lid 2, 37 lid 4.

2. Samenvatting BNC-fiche

• Korte inhoud voorstel

De verordening heeft tot doel het vertrouwen in het elektronisch verkeer tussen burgers, bedrijven en overheden binnen Europa te vergroten door dit onbelemmerd en veilig te laten plaatsvinden.

De verordening regelt de wederzijdse erkenning tussen lidstaten van elektronische identiteiten en van vertrouwensdiensten (elektronische handtekeningen, -documenten -tijdstempels, -zegels, bezorgdiensten en webcertificaten). Ook bevat het voorstel regels ten aanzien van aanbieders van vertrouwensdiensten en het toezicht daarop. Er wordt onderscheid gemaakt tussen vertrouwensdiensten met een hoog, zogenoemd gekwalificeerd betrouwbaarheidsniveau, en andere vertrouwensdiensten. Het voorstel vervangt de Richtlijn Elektronische Handtekeningen, die een aanmerkelijk beperkter toepassingsbereik heeft.

Nederlandse positie

Nederland verwelkomt het voorstel. Vertrouwen in grensoverschrijdende elektronische communicatie is noodzakelijk voor elektronische dienstverlening van de overheid aan burgers en bedrijven en aan de totstandkoming van de digitale interne markt. Borging van de veiligheid middels grensoverschrijdend bruikbare elektronische identiteiten en vertrouwensdiensten levert een belangrijk bijdrage aan het benodigde vertrouwen. Hoewel Nederland verheugd is over de strekking en het doel van het voorstel, zijn er ook punten van aandacht: veiligheidsoplossingen en daaraan gestelde eisen moeten aansluiten op de praktijk; het toezicht dient robuust en afdoende te zijn geregeld met voldoende mogelijkheden om in geval van veiligheidsincidenten effectief op te kunnen treden; wederzijdse erkenning dient uitsluitend mogelijk te zijn indien de betrouwbaarheid van veiligheidsoplossingen afdoende is gewaarborgd en deze minimaal gelijkwaardig zijn aan het niveau dat in Nederland wordt gehanteerd bij de betreffende dienst; er dient voldoende aandacht te zijn voor wederzijdse erkenning van nu en in de toekomst veel gebruikte oplossingen die niet op gekwalificeerde certificaten zijn gebaseerd; het voorstel dient niet teveel op delegatie geënt te zijn en de implementatiekosten dienen proportioneel te zijn. De eisen die de verordening stelt aan elektronische certificaten dienen afgestemd te worden met de eisen die de browserleveranciers stellen. Dit coördinatievraagstuk zal tussen de EU en internetoverlegorganen op het mondiale niveau moeten worden opgepakt.

Bevoegdheidsvaststelling en subsidiariteits- en proportionaliteitsoordeel

Bevoegdheid:
Artikel 114 VWEU. Nederland onderschrijft de bevoegdheid van de Unie op dit terrein.
Subsidiariteit: positief
Proportionaliteit: positief

• Implicaties/kansen/risico's

Implicaties
- Nederlandse aanbieders van elektronische diensten zullen om moeten kunnen gaan met buitenlandse elektronische identiteitsvoorzieningen en vertrouwensdiensten. Er is een technische voorziening nodig om dit mogelijk te maken.
- Het betrouwbaarheidsniveau van veiligheidsoplossingen moet omhoog. Dit brengt kosten met zich mee.
- De verordening betekent een uitbreiding van de taken van de toezichthouder (OPTA). De capaciteit (Fte en middelen) bij OPTA zal moeten worden uitgebreid.

Kansen
- Vergroting van de markt en doelgroep voor Nederlandse aanbieders en afnemers van elektronische diensten.

- Aandacht voor veiligheid bij nationale en grensoverschrijdende elektronische transacties en afstemming van vertrouwensdiensten op de risico's.
- Vergroting van de markt voor Nederlandse aanbieders van elektronische identiteiten en vertrouwensdiensten. Samenhang met eerste punt.

Risico's

- Een mismatch tussen hetgeen de verordening expliciet regelt en hetgeen in Nederland in de praktijk wordt gebruikt.
- Geen aansluiting bij STORK[1]-betrouwbaarheidsclassificatie en de systematiek die bij de Dienstenrichtlijn is uitgewerkt. Deze systematiek houdt in dat op basis van een risicoanalyse wordt bepaald welk betrouwbaarheidsniveau noodzakelijk is voor toegang of afname van een elektronische dienst.
- Door de focus op gekwalificeerde elektronische certificaten worden vertrouwensdiensten die niet op deze techniek zijn gebaseerd uitgesloten. Dit kan een rem op innovatie zijn.

3. Samenvatting voorstel

Inhoud voorstel:

De verordening heeft tot doel het vertrouwen in het elektronisch verkeer tussen burgers, bedrijven en overheden binnen Europa te vergroten door dit onbelemmerd en veilig te laten plaatsvinden.

Om dit te realiseren regelt de verordening de wederzijdse erkenning en aanvaarding tussen de lidstaten van elektronische identiteiten en vertrouwensdiensten, zoals elektronische handtekeningen, documenten, tijdstempels, zegels, bezorgdiensten en webcertificaten. Elektronische identificatie kan in de verordening niet op dezelfde generieke manier worden behandeld als de andere elektronische vertrouwensdiensten, omdat het uitreiken van identificatiemiddelen voor publieke doeleinden een nationale aangelegenheid is. Daarom bevat de verordening specifieke voorschriften over de wederzijdse erkenning van de elektronische identiteiten. Die houden in dat lidstaten een elektronische identiteit uit een andere lidstaat moeten accepteren, indien het stelsel waaronder deze is uitgegeven bij de Europese Commissie volgens een procedure is aangemeld. Er is geen verplichting voor een lidstaat zijn eigen stelsel voor elektronische identiteiten aan te melden.
Door de verordening zullen elektronische identiteiten en vertrouwensdiensten ook kunnen worden gebruikt voor elektronische diensten en transacties die in een andere lidstaat worden aangeboden.

Ten behoeve van het veilig verkeer regelt de verordening ondermeer de eisen waaraan vertrouwensdiensten en hun dienstverleners moeten voldoen, het toezicht op de vertrouwensdiensten, ondermeer door een meldplicht aan de nationale toezichthouder in geval van een veiligheidsincident, een verplichte jaarlijkse veiligheidsaudit voor sommige vertrouwensdiensten, de aansprakelijkheid en de bescherming van persoonsgegevens, de mogelijkheid van bindende instructies van de toezichthouder aan de verlener van vertrouwensdiensten en de wederzijdse hulp en bijstand tussen toezichthouders in de lidstaten.
Het voorstel vervangt de Richtlijn Elektronische Handtekeningen. Het toepassingsbereik van de verordening is aanmerkelijk breder dan de Richtlijn en het toezicht op vertrouwensdiensten wordt intensiever ten opzichte van het toezicht zoals dat nu geregeld is. Het voorstel legt de nadruk op elektronische identiteiten en vertrouwensdiensten met een hoog, zogenoemd gekwalificeerd, betrouwbaarheidsniveau. De veror-

[1] De letters staan voor Strong Identity Across Borders Linked. STORK is een grootschalige Europese pilot waarbij grensoverschrijdend gebruik van elektronische identiteiten is gerealiseerd. Nederland nam deel aan dit project en was projectleider van een betrouwbaarheidsclassificatieschema dat bij de verordening gebruikt kan worden.

dening gaat tot slot nader in op de rechtsgevolgen en de aanvaarding van verschillende vertrouwensdiensten.

Impact assessment Commissie

Er werden drie soorten beleidsopties beoordeeld op het gebied van respectievelijk (1) de reikwijdte van het nieuwe kader, (2) het rechtsinstrument en (3) het vereiste niveau van toezicht. Optie 2, die de voorkeur genoot, bleek te leiden tot grotere rechtszekerheid, betere coördinatie van nationaal toezicht, waarborging van de wederzijdse erkenning en aanvaarding van elektronische identificatieregelingen en omvatte tevens essentiële verwante vertrouwensdiensten. De conclusie van de effectbeoordeling was dat dit leidt tot een aanzienlijke verbetering van de rechtszekerheid, de veiligheid van en het vertrouwen in grensoverschrijdende elektronische transacties, met als gevolg minder fragmentering van de markt.

4. Bevoegdheidsvaststelling en subsidiariteits- en proportionaliteitsoordeel

a) Bevoegdheid

De interne markt is een gedeelde bevoegdheid van de Unie en de lidstaten (Art. 4, lid 2, sub a VWEU). De Unie is bevoegd om maatregelen vast te stellen op het gebied van de interne markt en de werking ervan te verzekeren (art. 26 VWEU). De rechtsgrondslag voor het voorstel is artikel 114 VWEU. Het centrale doel van het voorstel is het vergroten van de betrouwbaarheid en het vertrouwen in elektronische transacties in het belang van een goede werking van de interne markt (artikel 1, eerste lid). Omdat het uitreiken van identificatiemiddelen een nationale aangelegenheid is, ziet dit voorstel voor wat betreft elektronische identiteiten enkel op de grensoverschrijdende aspecten. Nederland acht de Unie bevoegd voor zover de verordening zich beperkt tot het vergroten van het vertrouwen in en de betrouwbaarheid van elektronische transacties en het voorstel zich niet uitstrekt over het vaststellen van de identiteit van personen.

b) Subsidiariteits- en proportionaliteitsoordeel

Subsidiariteitsoordeel: positief
De verordening beoogt de erkenning en aanvaarding van elektronische identiteiten en vertrouwensdiensten in andere lidstaten te vereenvoudigen. Hiervoor is wetgeving op Europees niveau gepast en wenselijk. Zonder een verordening komt de wederzijdse erkenning van nationaal uitgegeven elektronische identificatie, elektronische handtekeningen, en overige vertrouwensdiensten op de Europese markt moeilijk van de grond en blijven deze veelal slechts bruikbaar binnen de landsgrenzen. De praktijk van de huidige Europese Richtlijn elektronische handtekeningen heeft dit uitgewezen. De met deze richtlijn beoogde harmonisatie tussen de lidstaten is in het afgelopen decennium niet gerealiseerd, waardoor grensoverschrijdend gebruik van elektronische handtekeningen in de praktijk niet van de grond gekomen is.

Proportionaliteit: positief
De verordening harmoniseert onder meer eisen op het gebied van toezicht, aansprakelijkheid en rechtsgevolgen voor het aanbod en gebruik van elektronische vertrouwensdiensten. Betrouwbaarheid is cruciaal in grensoverschrijdend digitaal verkeer. Onder meer de DigiNotarzaak heeft duidelijk gemaakt dat het noodzakelijk is om steviger toezicht te houden en meer directief te kunnen optreden bij incidenten in de vertrouwens-

dienstverlening. Door de rechtstreekse werking draagt het instrument van de verordening er aan bij dat lidstaten eenzelfde invulling geven aan vertrouwensdiensten waardoor burgers en bedrijven worden geconfronteerd met specifieke nationale (juridische) eisen en technische interoperabiliteitsproblemen. Met een verordening biedt de Commissie een kader voor elektronische identiteiten en vertrouwensdiensten, waardoor betrouwbare grensoverschrijdende dienstverlening en transacties worden bevorderd en de rechtszekerheid wordt vergroot.

Een richtlijn kent het nadeel dat verschillende implementaties of andere tijdstippen van inwerkingtreding ongewenst vertrouwensrisico met zich meebrengen, alsmede het risico op discrepanties in aansprakelijkheidsregimes tussen lidstaten. De burger of ondernemer weet dan niet waar hij aan toe is en zal aarzelen om elektronische diensten van een aanbieder uit een andere lidstaat af te nemen.

Gelet op de belangen bij het elektronisch verkeer en de Nederlandse ervaring met DigiNotar is de nu voorgestelde verordening proportioneel.

c) Nederlands oordeel over de voorstellen op het gebied van gedelegeerde en/of uitvoeringshandelingen

Ten aanzien van de gedelegeerde handelingen betreft het onder meer de bevoegdheid om handelingen vast te stellen ten aanzien van de interoperabiliteit van elektronische identificatie; eisen die aan verleners van vertrouwensdiensten worden gesteld met betrekking tot veiligheidsmaatregelen; erkende onafhankelijke organen die verantwoordelijk zijn voor het houden van audits van dienstverleners; vertrouwenslijsten; eisen met betrekking tot de veiligheidsniveaus van elektronische handtekeningen; eisen met betrekking tot de validering en bewaring van gekwalificeerde certificaten voor elektronische handtekeningen; de organen die verantwoordelijk zijn voor de certificering van middelen voor het aanmaken van gekwalificeerde elektronische handtekeningen; de eisen met betrekking tot de veiligheidsniveaus van elektronische zegels en met betrekking tot gekwalificeerde certificaten voor elektronische zegels; en de interoperabiliteit tussen bezorgdiensten.

Uitvoeringshandelingen kunnen onder andere worden vastgesteld om de voorwaarden van de notificaties van elektronische identificatiesystemen vast te leggen; de samenwerking tussen lidstaten te stroomlijnen in het bijzonder voor uitwisseling van informatie, goede voorbeelden, en peer pressure; de kenmerken van de jaarrapportage van de toezichthouder; de samenwerking tussen toezichthouders; de vereisten waar veiligheidsdienstverleners aan dienen te voldoen; de kenmerken van de audit voor veiligheidsdienstverleners; de bindende aanwijzing die toezichthouders kunnen geven; de startmelding van een veiligheidsdienstverlener, vertrouwenslijsten; standaarden voor betrouwbare systemen en producten. De Commissie stelt in al deze gevallen het gebruik van de onderzoeksprocedure voor.

Het Nederlandse kabinet onderschrijft dat voor Europese veiligheidsoplossingen gedetailleerde eisen, betrouwbaarheidsniveaus en standaarden nodig zijn. Dit voorkomt verschillen tussen lidstaten en daarmee onzekerheid over het niveau van veiligheid van in afzonderlijke lidstaten uitgegeven diensten en producten. Gelet op het technische karakter van dit soort zaken is het van belang dat die relatief eenvoudig kunnen worden aangepast in regelgeving. In dat geval kan het gewenst zijn die niet allemaal op het niveau van de verordening zelf vast te leggen. Tegelijkertijd stelt Nederland vast dat sprake is van een zeer uitgebreid voorgesteld gebruik van gedelegeerde en uitvoeringshandelingen. Daar

zitten zaken tussen die een essentieel deel zijn van de verplichtingen uit de verordeningen en daardoor beter op het niveau van de verordening kunnen worden geregeld gelet op het belang daarvan voor de praktijk. Dit draagt ook beter bij aan de praktische uitvoerbaarheid en kenbaarheid van de verordening. Marktpartijen zullen anders niet enkel de bepalingen van de verordening moeten kennen, maar ook alle daarop gebaseerde regelgeving. Het is daarom naar de overtuiging van Nederland beter dat bepaalde zaken, zoals vereiste minimale betrouwbaarheidsniveau voor de acceptatie van stelsels voor elektronische identiteiten en de eisen die betrekking hebben op het veiligheidsniveau, beter in de verordening zelf vastgelegd kunnen worden.

Daarnaast stelt de Commissie in een aantal gevallen gedelegeerde handelingen voor, waar Nederland de voorkeur zou geven aan uitvoeringshandelingen, omdat goede kennis van de nationale situatie onontbeerlijk is om tot een goede Europese oplossing te komen en de beleidskeuzes significante gevolgen kunnen hebben voor de uitvoering. Hierbij kan bijvoorbeeld gedacht worden aan de organen die verantwoordelijk zijn voor de certificering van middelen voor het aanmaken van gekwalificeerde elektronische handtekeningen en de interoperabiliteit tussen bezorgdiensten.

5. Financiële implicaties, gevolgen voor regeldruk en administratieve lasten

a) Consequenties EU-begroting

Administratieve uitgaven van de Europese Commissie worden geschat op 9,4 mln. (2014–2020). Dit bedrag maakt onderdeel uit van de onderhandelingen over het Meerjarig Financieel Kader (MFK) 2014–2020. Nederland hecht eraan dat met de besprekingen over deze verordening niet vooruit wordt gelopen op de integrale besluitvorming betreffende het MFK. Het voorstel heeft verder geen financiële implicaties.

b) Financiële consequenties (incl. personele) voor rijksoverheid en/ of decentrale overheden

– Het verbreden, verdiepen en intensiveren van de toezichtfunctie op nationaal niveau, de uitbreiding van reeds bestaande nationale vertrouwenslijsten en de notificatie van vertrouwensinbreuken leiden tot een taakverbreding en verzwaring voor de toezichthouder (OPTA). De formatie en het budget van OPTA zullen vergroot moeten worden om het toezicht conform de verordening uit te kunnen voeren.
– De verplichting tot het openstellen van elektronische diensten van overheidsdienstverleners voor (buitenlandse) elektronische vertrouwensvoorzieningen zal kosten met zich meebrengen voor Nederlandse aanbieders van elektronische diensten, zoals uitvoeringsorganisaties en gemeenten. Deze kosten worden veroorzaakt doordat dienstverleners daadwerkelijk buitenlandse elektronische identiteiten en vertrouwensdiensten moeten kunnen verwerken. Dienstverleners zullen hiertoe aan moeten sluiten op een technische voorziening die de echtheid van dergelijke diensten controleert in het land van herkomst en bevestigt.[1] De koepels van de medeoverheden worden bij de implementatie van de verordening betrokken.
– De budgettaire gevolgen hiervan worden ingepast op de begroting van de beleidsverantwoordelijke departementen, conform de regels van de budgetdiscipline.

[1] Indien de Wet op de Financiële verhoudingen van toepassing is, zullen de kosten voor gemeenten van het realiseren van deze verplichting tot het openstellen van elektronische diensten in kaart moet worden gebracht.

c) Financiële consequenties (incl. personele) voor bedrijfsleven en burger

– Het voorstel verplicht bedrijven en burgers niet om een digitale identiteit of vertrouwensdienst aan te schaffen. Het voorstel leidt dan ook niet direct tot financiële lasten voor bedrijfsleven en burgers. Doordat het voorstel de nadruk legt op de hoge betrouwbaarheidsniveaus zal wel een druk ontstaan om tot aanschaf van hogere (en veelal duurdere) vertrouwensdiensten over te gaan. Daarbij kan worden aangetekend dat deze trend ook zonder de verordening al zichtbaar is vanwege de toenemende veiligheidseisen om inbreuken en incidenten te voorkomen. Daarnaast zal een burger of bedrijf ook zonder de verordening moeten voldoen aan de eisen die lidstaten stellen voor toegang tot elektronische dienstverlening en transacties.

d) Gevolgen voor regeldruk/administratieve lasten voor rijksoverheid, decentrale overheden, bedrijfsleven en burger

Nederlandse bedrijven die vertrouwensdiensten verlenen krijgen te maken met extra verplichtingen tot het aanleveren van informatie bij de toezichthouder. Dit betekent een verzwaring van administratieve lasten voor bedrijven die deze vertrouwensdiensten leveren. Het gaat om een kleine tien bedrijven. Deze informatie zal veelal al bij de bedrijven beschikbaar zijn waardoor verwacht wordt dat de extra kosten beperkt zullen zijn.
Het is op dit moment nog niet mogelijk om de administratieve lasten te kwantificeren. In de praktijk worden processen waarin papieren documenten worden gebruikt, steeds meer vervangen door elektronisch verkeer. Deze trend is onder de huidige Europese wetgeving al zichtbaar. Elektronische Dienstverlening levert enerzijds efficiëntievoordelen, gebruikersgemak en besparingen op het gebied van administratieve lasten op. Het brengt aan de andere kant kosten en administratieve lasten voor burgers en bedrijven met zich mee die samenhangen met de aanschaf van elektronische identiteiten en vertrouwensdiensten. Met de voorgestelde verordening wordt verwacht dat met name extra efficiencywinsten mogelijk worden bij elektronische transacties met het buitenland. Hiervoor zal veelal het hoogste veiligheidsniveau van elektronische identiteit of vertrouwensdienst nodig zijn. Dit zijn vanwege de hoge betrouwbaarheidseisen aan techniek en uitgifteproces ook de duurste oplossingen. Er wordt daarom geen groot extra effect verwacht op kosten en besparingen op nationaal niveau.

De transitie zal ook kosten met zich meebrengen voor overheidsorganisaties die elektronische diensten aanbieden. Partijen zullen met elektronische vertrouwensdiensten uit andere lidstaten moeten kunnen omgaan, indien ze de elektronische weg voor nationaal verkeer hebben opengesteld en daarbij om een vertrouwensdienst vragen. Zo moeten aan Nederlandse zijde technische voorzieningen worden getroffen, die de uitwisseling tussen Nederlandse en andere Europese elektronische identiteiten mogelijk maken. Deze voorziening moet worden gerealiseerd en beheerd. Daarnaast ontstaan er kosten door de aansluiting van dienstverlenende organisaties op deze voorziening. Verder zullen steeds maatregelen nodig zijn om de betrouwbaarheid op peil te houden en te verhogen om cybercrime te voorkomen en te bestrijden. Een hoger niveau van elektronische identiteiten en vertrouwensdiensten is duurder en brengt, door een zwaarder uitgifteproces, lastenverzwaring voor burgers en bedrijven met zich mee.

6. Implicaties juridisch

a) Consequenties voor nationale en decentrale regelgeving en/of sanctionering beleid (inclusief toepassing van de lex silencio positivo)

De Telecommunicatiewet, het Burgerlijk Wetboek en de Algemene Wet Bestuursrecht moeten worden aangepast. De verordening maakt uitvoeringswetgeving noodzakelijk die tot wijziging van de Telecommunicatiewet leidt, onder meer ten aanzien van betrouwbaarheidslijsten en het toezicht. Ook zal nagegaan dienen te worden in hoeverre voorschriften bij of krachtens de Telecommunicatiewet verenigbaar zijn met de rechtstreekse werking van de verordening, zoals ten aanzien van certificaten en veilige middelen. Ook ten aanzien van de Algemene Wet Bestuursrecht en het Burgerlijk Wetboek dient te worden bezien of uitvoeringswetgeving noodzakelijk is. Tevens dient nagegaan te worden of in bijzondere wetten met de verordening strijdige bepalingen zijn die moeten worden aangepast of ingetrokken. Er zijn geen gevolgen voor de decentrale regelgeving. Daarnaast heeft het voorstel mogelijk invloed op de in de Digitale Implementatieagenda aangekondigde Wet op het Elektronisch Zakendoen.

b) Voorgestelde implementatietermijn (bij richtlijnen), dan wel voorgestelde datum inwerkingtreding (bij verordeningen en beschikkingen) met commentaar t.a.v. haalbaarheid

De verordening treedt 20 dagen na publicatie in werking. Gelet op de noodzakelijke uitvoerings- en aanpassingswetgeving is het noodzakelijk dat er een realistische termijn wordt geboden voordat de uit de richtlijn voortvloeiende verplichtingen gaan gelden, hetgeen nu nog niet het geval is. Daarnaast zijn uitvoeringsmaatregelen noodzakelijk die echter nog niet overzienbaar zijn vanwege de grote hoeveelheid delegatiebepalingen in de verordening. Elektronische identiteiten die bij de Europese Commissie zijn aangemeld moeten door alle Nederlandse overheden geaccepteerd kunnen worden. De termijn van 6 maanden die in de verordening wordt genoemd is daarvoor te kort. Ditzelfde geldt voor het door alle Nederlandse overheden kunnen accepteren van gekwalificeerde vertrouwensdiensten en van originele of gewaarmerkte elektronische documenten. Een realistischer termijn voor het nemen van uitvoeringsmaatregelen is 24 maanden.

c) Wenselijkheid evaluatie-/horizonbepaling

Artikel 40 van de ontwerpverordening bevat een evaluatiebepaling. Een evaluatie vindt elke 4 jaar plaats. Dit is wenselijk om bijtijds te kunnen onderkennen of de verordening inderdaad bewerkstelligt waar deze voor is bedoeld.

7. Implicaties voor uitvoering en handhaving

a) Uitvoerbaarheid

De verantwoordelijkheid voor de uitvoering van de verordening ligt primair bij de overheid. Nederland moet een voorziening realiseren die het omgaan met erkende elektronische identiteiten in Nederland en de rest van Europa mogelijk maakt. Daarnaast moet deze voorziening het gebruik van Nederlandse elektronische identiteiten in het buitenland mogelijk maken. De technieken en voorzieningen hiervoor bestaan al. Op een later tijdstip moet worden gekozen onder verantwoordelijkheid van welke organisatie dit knooppunt wordt gerealiseerd en bij wie het beheer van dit knooppunt wordt belegd.

Overheidsorganisaties moeten in een vroeg stadium al worden geïnformeerd dat voorstel gevolgen voor hen heeft. Naast aansluiting op de voorziening die het mogelijk moet maken om met buitenlandse elektronische identiteiten te kunnen omgaan zullen er waarschijnlijk ook aanpassingen in de back-office nodig zijn. Er zullen bijvoorbeeld processen moeten worden ingeregeld om naast de identiteit ook andere zaken te controleren, bijvoorbeeld of een persoon een bepaalde rol, zoals bijvoorbeeld arts of advocaat heeft of geautoriseerd is tot het verrichten van de transactie. De verordening regelt dit overigens niet. Door uitvoeringsorganisaties en het Dienstenloket vroeg te betrekken wordt de uitvoerbaarheid van het voorstel geborgd.

Burgerservicenummer en omnummering
De Nederlandse overheid beraadt zich erop om de authenticatievoorziening DigiD op grond van het bepaalde in artikelen 5 en 7 als authenticatiemiddel te notificeren, zodat acceptatie van DigiD door andere lidstaten is geborgd.

Het gebruik/acceptatie van DigiD in de huidige vorm door andere lidstaten stuit vooralsnog op een blokkade, omdat DigiD bij authenticatie in grensoverschrijdende situaties een persoonsidentificerend nummer, in casu het Burgerservicenummer (BSN), zou uitwisselen met de buitenlandse dienstaanbieder. Dit is op grond van nationale wetgeving niet toegestaan. De Wet Algemene Bepalingen Burgerservicenummer (Wabb) bepaalt in artikel 1 onder d, dat het gebruik van het BSN alleen is toegestaan voor (nationale) overheidsorganisaties[1] en een ieder ander dan een overheidsorgaan of degene aan wie het BSN is toegekend, voor zover deze werkzaamheden verricht waarbij het gebruik door hem of haar van het BSN bij of krachtens de wet is toegestaan.

Om DigiD als authenticatiemiddel te notificeren moet bij grensoverschrijdend gebruik van DigiD er geen BSN maar een pseudoniem worden uitgewisseld met de buitenlandse dienstaanbieder, danwel gebruik gemaakt worden van een voorziening die de identiteit in het land van herkomst controleert. Daarvoor zal een omnummerfaciliteit en -autoriteit moeten worden ingericht, tevens om zo nodig de relatie met de authentieke persoon te kunnen leggen. In het ontwerp voor een toekomstige eNIK, waarbij een elektronische identiteit op de Nederlandse identiteitskaart wordt geplaatst, is al rekening gehouden met de inrichting van een omnummerfaciliteit en -autoriteit.

Uit een studie[2] – in het kader van de grote Europese STORK-pilot – is gebleken dat dit probleem zich niet alleen in Nederland voordoet, maar ook in bijv. België, Oostenrijk, Frankrijk en Denemarken. Vrijwel alle EU-lidstaten hebben nationale wetgeving voor het gebruik van persoonsidentificerende nummers. Deze levert belemmeringen op bij het grensoverschrijdend gebruik van nationale authenticatiemiddelen waarin dit nummer is verwerkt.

b) Handhaafbaarheid

De reikwijdte van het toezicht is op dit moment nog niet helemaal duidelijk. In het verlengde van de toezichtstaken die OPTA al had op grond van de Richtlijn Elektronische handtekeningen, ligt het in de rede dat de toezichtstaken waarin de verordening voorziet, worden belegd bij de OPTA. OPTA zal te maken gaan krijgen met een aanmerkelijke verbreding en verzwaring van zijn taken vanwege uitbreiding en intensivering van de toezichtstaak. Het toezicht zal zich over meer diensten uitstrekken en de verordening zal ook gevolgen hebben voor de uitvoering van het toezicht. Voorts zullen samenwerking en afstemming met de andere toezicht-

[1] Als bedoeld in de Algemene wet bestuursrecht, artikel 1:1 onder 1.
[2] Stork, D2.2 – Report on Legal Interoperability. d.d. 24 February 2009.

houders uit de lidstaten op EU-niveau belangrijker worden. Daarnaast zal gekeken moeten worden naar de verhouding tussen de taken van OPTA en de taken van Logius als policiy authority in het kader van het PKIoverheid-stelsel.

c) Communicatie

Het onderwerp elektronische identiteiten en vertrouwensdiensten wordt als ingewikkeld ervaren. Veelal hebben partijen geen juist beeld van wat er wel en niet geregeld wordt en ontstaan misverstanden over begrippen zoals identificatie, authenticatie, autorisatie en privacyvraagstukken. Er zal goed moeten worden gecommuniceerd dat de voorgestelde verordening Nederland niet zal verplichten tot invoering van een Europese identiteitsoplossing, noch burgers of bedrijven verplicht om deze te hebben. Ook wordt er geen centrale database ingericht en worden er zeer beperkt persoonsgegevens uitgewisseld. De verordening schrijft bovendien voor dat het vastleggen van persoonsgegevens tijdens de registratiefase, wanneer een elektronische identiteit wordt aangemaakt, altijd met toestemming van de betrokkene dient te geschieden.

8. Implicaties voor ontwikkelingslanden

Geen.

9. Nederlandse positie

Doelstelling

Het kabinet verwelkomt deze verordening. De verordening heeft tot doel veilige elektronische transacties in Europa via het internet mogelijk te maken. Dit kan worden bereikt door de onderlinge erkenning en acceptatie van elektronische identiteiten en vertrouwensdiensten. Dit is een belangrijk punt uit zowel de Europese als de nationale Digitale Agenda. Burgers en ondernemers moeten bij onderlinge digitale communicatie en met de overheid, zoals het versturen van belastingaangiften, gebruik kunnen maken van betrouwbare identiteitsoplossingen en diensten die de veiligheid verhogen.

Burgers en ondernemers hoeven dan niet voor iedere verschillende lidstaat een separate elektronische identiteit meer aan te vragen, maar kunnen gebruik maken van hun eigen nationale middelen voor elektronische identificatie en authenticatie. Hiermee draagt dit voorstel bij tot versterking van de digitale interne markt en tot het groeivermogen van de Europese economie.

Reikwijdte

De reikwijdte is ruimer dan die van de Richtlijn Elektronische Handtekeningen. Het ontwerp is van toepassing op elektronische identificatie- en authenticatiesystemen (eID's), op elektronische vertrouwensdiensten die de integriteit en authenticiteit van documenten, elektronische handtekeningen en websites verzorgen (tijdstempels, documenten, bezorgdiensten, websitecertificaten, zegels, gekwalificeerde certificaten) en op producten waarmee deze kunnen worden aangemaakt, de zogenoemde veilige middelen.

Voor Nederland is website-authenticatie een belangrijke uitbreiding ten opzichte van de Richtlijn elektronische handtekeningen. Website-authenticatie biedt een bezoeker de zekerheid dat de website daadwerkelijk van de veronderstelde aanbieder van de site is (bijvoorbeeld met het

«gele slotje op de website»). Daarbij wordt veelal gebruik gemaakt van servercertificaten, zoals SSL-certificaten. Op Europees niveau bestaan voor website-authenticatie nu geen wettelijke betrouwbaarheidseisen en is toezicht daarop ook niet verplicht. Het ontwerp brengt daar verandering in. Het kabinet is hier gelet op de betekenis en afhankelijkheid van het elektronisch verkeer van deze diensten voorstander van. Een belangrijke kanttekening die bij de afbakening van de reikwijdte van het voorstel wordt geplaatst, is dat die voldoende helder dient te zijn. De inhoud van bepaalde definities in het voorstel is nu niet altijd even helder (zoals de definitie van knooppunten).

Anders dan bij vertrouwensdiensten, spitst het toepassingsgebied omtrent elektronische identificatie zich in het voorstel vooral toe op het gebruik ervan binnen de overheidssector. Bovendien kan door de directe werking van de verordening een situatie ontstaan dat bepaalde diensten, die momenteel niet gebruikt worden in Nederland (bijvoorbeeld elektronische zegels), maar die in andere landen wel worden gebruikt, in elektronisch verkeer terecht zouden kunnen komen en rechtskracht moet worden toegekend.

Elektronische identificatie (eID)

Het ontwerp regelt de wederzijdse erkenning van elektronische identificatiestelsels[1] [2] die door, namens of onder verantwoordelijkheid van een lidstaat zijn uitgegeven en die voor communicatie met de overheid worden gebruikt. Elektronische identiteiten zijn onderdeel van een stelsel en kunnen bijvoorbeeld de vorm hebben van een elektronische identiteit(skaart) die kan worden gebruikt bij het aanvragen van vergunningen, aangifte doen, etc. Indien een lidstaat een dergelijk identiteitsstelsel bij de Europese Commissie op een juiste wijze heeft aangemeld, moeten andere lidstaten die buitenlandse identiteiten, die onder dat stelsel vallen aanvaarden, bij elektronisch verkeer met hun overheid. Dit maakt het voor ondernemers en burgers eenvoudiger om langs elektronische weg met overheden in andere lidstaten allerlei bestuurlijk verkeer af te wikkelen. Het is voor Nederland en andere lidstaten niet verplicht om over een identiteitsstelsel te beschikken of om die verplicht aan te melden bij de Europese Commissie. Indien een lidstaat een stelsel niet notificeert, betekent dit dat andere lidstaten de elektronische identiteiten uit dat stelsel niet hoeven te erkennen. Dit laat echter onverlet dat de lidstaten buitenlandse identiteiten(stelsels), die wel genotificeerd zijn, moet accepteren.

Het kabinet wil dat wederzijdse erkenning tussen lidstaten zich in de praktijk niet enkel beperkt tot op gekwalificeerde certificaten gebaseerde elektronische identiteiten en vertrouwensdiensten. Grensoverschrijdend gebruik van andere oplossingen voor identificatie, zoals bijvoorbeeld DigiD en eHerkenning, zou mits deze voldoende betrouwbaar zijn voor de dienst die men ermee wil afnemen, mogelijk moeten zijn. Hergebruik van reeds bekende en door de burger en bedrijven vertrouwde middelen vergemakkelijkt en stimuleert het grensoverschrijdend elektronisch verkeer. Daarbij hecht het kabinet er sterk aan dat het recht voor de keuze voor nationale identificatiemiddelen en de persoonsgegevens die daarin opgeslagen zijn, volledig bij de lidstaten zelf blijft. De verordening treedt hier als zodanig ook niet in. Het voorstel regelt niet de aanvullende eisen die gesteld kunnen worden aan een afnemer van elektronische diensten. Zo zal in bepaalde gevallen informatie nodig zijn over de autorisatie, rol of functie van een persoon voordat elektronisch toegang tot een dienst of informatie wordt gegeven. Denk bijvoorbeeld aan advocaten voor toegang tot elektronische dossiers bij de rechtbank of artsen voor toegang tot medische informatie. Het voorstel sluit ook niet uit dat dergelijke

[1] Een stelsel is een samenhangend geheel van processen, voorzieningen, toezicht en afspraken dat, in dit geval, elektronische identificatie en authenticatie mogelijk maakt. Een elektronische identiteit functioneert binnen een stelsel.

[2] Het huidige voorstel is niet consistent in het gebruik van de begrippen stelsel, elektronische identiteit en middel. Daardoor is niet altijd duidelijk wat het voorstel precies bedoelt. Nederland zal op dit punt verheldering vragen aan de commissie.

informatie moet worden overlegd voordat toegang tot informatie of een dienst wordt gegeven.

Niettemin plaatst het kabinet de volgende belangrijke kanttekeningen bij de gekozen benadering:

- Ten aanzien van eID's is belangrijk dat afdoende is gewaarborgd dat Nederland alleen die stelsels van eID's van andere lidstaten hoeft te accepteren die voldoende betrouwbaar zijn voor de dienstverlening die Nederland aanbiedt. Dit betekent dat de acceptatieplicht van een buitenlandse eID zich zou moeten beperken tot minimaal het gelijkwaardige betrouwbaarheidsniveau van de Nederlandse variant van de elektronische identiteit die voor de betreffende dienst wordt gevraagd. De Europese Commissie lijkt vooral in te zetten op eID's van een hoog betrouwbaarheidsniveau, maar uit de verordening blijkt vooralsnog onvoldoende duidelijk welke eisen en criteria gelden die dit waarborgen. Lidstaten zijn weliswaar aansprakelijk ten aanzien van de kwaliteit van identificatie en validatie van door hen aangemelde eID's, maar het is maar de vraag in hoeverre dit tot het gewenste resultaat leidt.
- De waarborg dat identificatiemiddelen uit andere lidstaten voldoende betrouwbaar zijn, is sterk gebaseerd op de aansprakelijkheid van een lidstaat voor een correcte wijze van identificatie. Dit kan echter alleen achteraf worden vastgesteld waardoor dit ingewikkeld is.
- De kosten van uitvoerbaarheid moeten binnen aanvaardbare proporties blijven.
- Om de voorstellen haalbaar te laten zijn, zullen ruime invoeringstermijnen moeten worden gehanteerd.
- De verordening dient de reikwijdte van privaatrechtelijke overeenkomsten niet te beperken.
- Specifieke aandachtspunten bij de verordening vanuit Nederlandse identificatie- en authenticatiestelsels, zoals het afsprakenstelsel eHerkenning en PKI-overheid[1], zijn het kostenaspect bij verificatie, het vereiste dat een elektronisch identificatiemiddel wordt afgegeven door, namens of onder de verantwoordelijkheid van de aanmeldende lidstaat en dat de Staat zich aansprakelijk stelt voor de ondubbelzinnige koppeling van de elektronische identiteit met (rechts-)persoonsidentificatiegegevens. Nederland is geen voorstander van het overnemen van verantwoordelijkheden door de overheid van het bedrijfsleven. Nederland wil hierover duidelijkheid van de Europese Commissie.

Betrouwbaarheid gekwalificeerde vertrouwensdiensten

Bij de vertrouwensdiensten wordt onderscheid gemaakt tussen gekwalificeerde en niet-gekwalificeerde diensten. Aan het aanbieden van gekwalificeerde vertrouwensdiensten (hoog betrouwbaarheidsniveau) worden specifiekere en zwaardere eisen gesteld dan aan het aanbod van niet-gekwalificeerde diensten. Die eisen zijn niettemin vrij algemeen geformuleerd en moeten voor een belangrijk deel nog nader worden ingevuld door gedelegeerde handelingen en/of uitvoeringshandelingen van de Europese Commissie. Het is nog niet duidelijk hoe daar precies invulling aan wordt gegeven. Mede gelet op de rechtstreekse werking van een verordening is het belangrijk dat daaraan een zo gedetailleerde en volledig mogelijke invulling wordt gegeven. Het gaat om vaak technische normen (bijvoorbeeld ETSI-normen[2]) die breed geaccepteerd dienen te zijn om Europees en internationaal toepasbaar te zijn. Hierin zit ook een spanningsveld ten aanzien van wat wenselijk en (op kortere termijn) mogelijk is gelet op het belang van afspraken hierin ook buiten de grenzen van de Europese Unie. De eisen die in het ontwerp worden opgesomd brengen niet goed tot uitdrukking dat veiligheid zowel betrekking dient te hebben op veiligheidsproces- en managementsystemen als ook op

[1] Een stelsel is een samenhangend geheel van processen, voorzieningen, toezicht en afspraken dat, in dit geval, elektronische identificatie en authenticatie mogelijk maakt. Een elektronische identiteit functioneert binnen een stelsel.

[2] ETSI is een Europees Standaardisatie Instituut dat technische standaarden, de ETSI-normen, ontwikkelt en vaststelt op ondermeer het vlak van elektronische certificaten waarop identiteiten en vertrouwensdiensten kunnen worden gebaseerd. Deze standaarden zijn belangrijk bij interoperabiliteit en toezicht.

inhoudelijke veiligheidspecificaties. Veiligheid is meer dan alleen procesbeheersing. Dit dient in de verordening zelf tot uitdrukking te worden gebracht.

Betrouwbaarheid van niet-gekwalificeerde diensten

Het ontwerp richt zich ook op de betrouwbaarheid van diensten met een lager niveau van betrouwbaarheid (niet-gekwalificeerde diensten). Voor alle aanbieders van vertrouwensdiensten geldt een verplichting tot het nemen van passende maatregelen tot risicobeheersing en geldt een verzwaard aansprakelijkheidsrisico hiervoor. Het kabinet staat positief tegenover dit uitgangspunt in het ontwerp. Het kabinet is van opvatting dat de kwaliteit van alle vertrouwensdiensten voor de afnemers en het publiek binnen de Europese Unie voldoende gewaarborgd moet zijn. Dit geldt ook voor vertrouwensdiensten met een lager betrouwbaarheidsniveau. Die worden veel afgenomen (zoals bij website-certificaten) en het belang voor de betrouwbaarheid van het elektronisch verkeer daarvan is dan ook aanzienlijk. Voor zowel afnemers als aanbieders van elektronische diensten moet duidelijk zijn welke betrouwbaarheidsniveau een dienst heeft. Dit kan worden bereikt door gebruik te maken van de STORK-classificatie van betrouwbaarheidsniveaus. Tegelijkertijd dient bij het aanbod van die diensten het belang van ruimte voor innovatie, betaalbaarheid voor de afnemer en concurrentiekracht met derde landen niet uit het oog verloren te worden.

Veiligheidsincidenten

Ondanks waarborgen voor betrouwbaarheid, kunnen zich veiligheidsincidenten voordoen. Het is belangrijk dat de verordening met die mogelijkheid eveneens rekening houdt. Aanbieders moeten passende maatregelen treffen om de gevolgen van veiligheidsincidenten zoveel mogelijk te beperken, hebben een informatieverplichting daarover, en moeten een veiligheidsinbreuk met aanzienlijke gevolgen voor de verleende dienst binnen 24 uur melden bij de betrokken toezichthouders. De toezichthouder kan hierover bindende instructies geven aan verleners van vertrouwensdiensten.
Een probleem dat de verordening zelf niet kan oplossen maar in dit verband eveneens belangrijk is, betreft de ontwrichting die kan optreden indien bij een veiligheidsincident de acceptatie van een betrouwbaarheidsdienst onmiddellijk onbruikbaar wordt. Indien bijvoorbeeld webbrowsers buiten de Europese Unie gecompromitteerde oplossingen per direct niet meer accepteren, kan dat grote gevolgen hebben. De veiligheid kan met uitsluiting gediend zijn, maar de vraag is of dit altijd even proportioneel is gelet op de effecten die uitsluiting per direct kan hebben voor de elektronische dienstverlening aan burgers en bedrijven. Een afweging is altijd maatwerk. Het is van belang dat, zowel op Europees als mondiaal niveau, coördinatiemechanismen worden ingericht waarin dergelijke afwegingen kunnen worden gemaakt.

Het voorstel legt onvoldoende relaties met wereldwijde instituties op het gebied van internetveiligheid, zoals het Cerfificate and Browserforum. Dit soort, veelal buitenlandse, organisaties stelt eisen aan vertrouwensdiensten opdat deze vertrouwd worden door de, veelal Amerikaanse, browsers. De eisen die de verordening stelt dienen afgestemd te worden met de eisen die de browserleveranciers stellen. Dit coördinatievraagstuk zal tussen de EU en mondiale internetoverleggremia moeten worden opgelost.

Toezicht

Het toezicht strekt zich uit tot alle aanbieders van vertrouwensdiensten die in de eigen lidstaat gevestigd zijn. Het toezicht op aanbieders van niet-gekwalificeerde vertrouwensdiensten is gericht op de controle op het nemen van passende maatregelen tot risicobeheersing (en op incidentpreventie en -beheersing). Aanbieders die een gekwalificeerde dienst willen starten dienen het voornemen daartoe bij de toezichthouder te melden en een veiligheidsaudit van een onafhankelijk erkend orgaan te overleggen. Positief is ook dat aanbieders van gekwalificeerde diensten telkens jaarlijks een dergelijke veiligheidsaudit moeten indienen bij de toezichthouder. De toezichthouder kan op ieder moment zelf een audit uitvoeren. De toezichthouder moet voorts beoordelen of een aanbieder op de vertrouwenlijst met betrouwbare aanbieders en diensten kan worden geplaatst en draagt daar dan zorg voor. Nederland is er geen voorstander van dat aanbieders van gekwalificeerde vertrouwensdiensten daarmee al van start mogen gaan voordat door de toezichthouder is gecontroleerd of zij aan de eisen daarvoor voldoen (wel moeten zij het voornemen tot dienstverlening bij de toezichthouder melden en daarbij een verslag van een veiligheidsaudit van een onafhankelijk erkend orgaan overleggen). Evenmin bepaalt de verordening uitdrukkelijk wat de consequenties zijn, indien een dienstverlener c.q. zijn gekwalificeerde diensten worden geschrapt uit vertrouwenlijst. Er moet geen onduidelijkheid over bestaan dat in een dergelijk geval de dienstverlening voor die geschrapte diensten (tijdelijk) moeten worden beëindigd en het predicaat «gekwalificeerd» niet mag worden gebruikt.
Belangrijk is dat het ontwerp er in voorziet dat toezichthouders uit verschillende lidstaten elkaar bijstand verlenen, waarbij ook inspecties in een andere lidstaat tot de mogelijkheden behoren. Het toezicht wordt kortom niet enkel verbreed (alle vertrouwensdiensten), maar krijgt op Europees niveau ook meer profiel en inhoud. Daarnaast is belangrijk dat de betrouwbaarheid van elektronische identiteiten en vertrouwensdiensten, die bij de Europese Commissie worden genotificeerd, is gecontroleerd en dat lidstaten (nood)maatregelen kunnen nemen ingeval er toch sprake lijkt van misstanden bij buitenlandse genotificeerde vertrouwensdiensten. Met betrokkenheid van de toezichthouders moeten lidstaten de mogelijkheid krijgen om diensten die niet meer worden vertrouwd te weren. Nederland wil inspraak bij de delegatiebepalingen die de opnamecriteria op de Europese lijst regelen.

Wederzijdse erkenning en rechtsgevolgen

De verordening regelt verder de wederzijdse erkenning, acceptatie en rechtsgevolgen van vertrouwensdiensten (naast een regeling voor wederzijdse erkenning van eID's). Dit stimuleert grensoverschrijdend elektronisch verkeer met waarborgen voor betrouwbare oplossingen. Dat is een doelstelling waar Nederland voorstander van is. Een vraag is in hoeverre de voorschriften hierover ook praktisch voldoende uitvoerbaar zullen zijn voor de lidstaten. Dit is in het bijzonder het geval bij de erkenning en aanvaarding van elektronische handtekeningen met de lagere veiligheidsniveaus die door een overheid bij het aanbieden van online-toepassingen van de gebruikers worden geëist. Die overheid moet dan ook elektronische handtekeningen uit andere lidstaten met ten minste hetzelfde veiligheidsniveau erkennen. Gelet op de veelheid aan technische oplossingen kan een dergelijk brede acceptatieplicht alleen worden geïmplementeerd door gebruik te maken van de in STORK gedefinieerde betrouwbaarheidsniveaus en door te controleren of de oplossingen daadwerkelijk aan het geclaimde betrouwbaarheidsniveau voldoen.