Eerste Kamer der Staten-Generaal

1

Vergaderjaar 2011–2012

33 331 EU-voorstel: Verordening betreffende elektronische identificatie en diensten voor elektronische transacties in de interne markt COM(2012) 238

B

VERSLAG VAN EEN SCHRIFTELIJK OVERLEG

Vastgesteld 3 september 2012

De vaste commissie voor Binnenlandse Zaken en de Hoge Colleges van Staat / Algemene Zaken en Huis der Koningin[1] heeft met belangstelling kennisgenomen van het voorstel voor een verordening betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt.[2] Naar aanleiding daarvan heeft zij onder andere de minister van Binnenlandse Zaken en Koninkrijksrelaties op 4 juli 2012 een brief gestuurd.

De minister van Economische Zaken, Landbouw en Innovatie heeft op 3 september 2012 gereageerd.

De commissie brengt bijgaand verslag uit van het gevoerde schriftelijk overleg.

De griffier van de vaste commissie voor Binnenlandse Zaken en de Hoge Colleges van Staat / Algemene Zaken en Huis der Koningin,
Fred Bergman

[1] Samenstelling:
Holdijk (SGP), Dupuis (VVD), Kox (SP), Sylvester (PvdA) *(vice-voorzitter),* Engels (D66) *(voorzitter),* Thissen (GL), Nagel (50PLUS), Ruers (SP), Van Bijsterveld (CDA), Duthler (VVD), Huijbregts-Schiedon (VVD), Van Kappen (VVD), Koffeman (PvdD), Kuiper (CU), Meurs (PvdA), Vliegenthart (SP), De Vries-Leggedoor (CDA), Lokin-Sassen (CDA), Th. de Graaf (D66), De Boer (GL), De Lange (OSF), Barth (PvdA), Ter Horst (PvdA), Koole (PvdA), Van Dijk (PVV), Klever (PVV), Sörensen (PVV), Schouwenaar (VVD)

[2] COM(2012)238. Zie ook dossier **E120015** op www.europapoort.nl

kst-33331-B
ISSN 0921 - 7371
's-Gravenhage 2012

BRIEF AAN DE MINISTER VAN ECONOMISCHE ZAKEN, LANDBOUW EN INNOVATIE

Den Haag, 4 juli 2012

De vaste commissie voor Binnenlandse Zaken en de Hoge Colleges van Staat / Algemene Zaken en Huis der Koningin heeft met belangstelling kennisgenomen van het voorstel voor een verordening betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt.[1] Graag legt de commissie een aantal vragen en opmerkingen over deze ontwerpverordening aan u voor. Bijgevoegd is tevens een afschrift van de brief die de commissie aan de Europese Commissie heeft gestuurd[2].

In artikel 6 van de ontwerpverordening wordt bepaald dat stelsels voor elektronische identificatie in aanmerking komen voor aanmelding als de elektronische identificatiemiddelen zijn afgegeven door, namens of onder de verantwoordelijkheid van de aanmeldende staat. Klopt het dat de stelsels die worden aangemeld ook van toepassing kunnen zijn op elektronische identificatiemiddelen die niet uitsluitend worden gebruikt om online toegang te krijgen tot een dienst van een bestuursorgaan in de zin van de Algemene wet bestuursrecht? De commissie acht het onwenselijk dat uitsluitend elektronische identificatiemiddelen kunnen worden gebruikt die zijn afgegeven door, namens of onder de verantwoordelijkheid van de aanmeldende lidstaat. Waarom kan niet worden volstaan met het stellen van eisen aan de dienstverleners die deze identificatiemiddelen uitgeven? Wordt de eis van het afgeven van elektronische identificatiemiddelen door, namens of onder de verantwoordelijkheid van de aanmeldende lidstaat – in casu de Nederlandse staat – gesteld om te voorkomen dat een gebruiker die geconfronteerd wordt met schade als gevolg van onbetrouwbare elektronische identificatiemiddelen, deze niet meer kan verhalen op de dienstverlener zelf omdat deze mogelijk opgehouden is te bestaan vanwege het niet kunnen voldoen van aansprakelijkheidsclaims? Is de regering het met de commissie eens dat de Nederlandse staat met deze bepaling min of meer een «waarborgfonds» wordt voor oninbare claims? Voor de commissie is een dergelijk gevolg onwenselijk en zij verzoekt de Nederlandse regering dan ook de in artikel 6 lid 1 genoemde voorwaarde te veranderen in: «de elektronische identificatiemiddelen zijn afgegeven door een dienstverlener, die namens of onder de verantwoordelijkheid van de aanmeldende lidstaat is gecontroleerd op de naleving van de in deze verordening gestelde eisen aan deze dienstverlener».

Voor de verlener van vertrouwensdiensten geldt dat op hem controle wordt uitgeoefend door de nationale toezichthouder. Gaat deze controle verder dan het toezicht door de OPTA zoals dat nu in de Telecommunicatiewet is geregeld? Kan de regering bevestigen dat de door de dienstverleners zelf ingevulde formulieren, zonder dat zij een derdenverklaring hoeven te overleggen, van de baan zijn? Als deze verordening van kracht wordt, is deze rechtstreeks toepasselijk. Is de Nederlandse regering van plan om de Telecommunicatiewet aan te passen in die zin dat de regeling van het toezicht door de OPTA in lijn wordt gebracht met de eisen die de onderhavige verordening stelt?

In artikel 15 lid 2 worden verleners van vertrouwensdiensten verplicht gesteld om zonder onnodige vertragingen en waar mogelijk binnen 24 uur nadat zij hiervan op de hoogte zijn, het bevoegde toezichthoudende orgaan, het bevoegde nationale orgaan voor informatieveiligheid en andere relevante derde partijen zoals gegevensbeschermingsautoriteiten

[1] COM(2012)238. Zie ook dossier **E120015** op www.europapoort.nl
[2] EK 33 331, A

op de hoogte te stellen van iedere veiligheidsinbreuk of ieder integriteitsverlies. Wie wordt in Nederland het bevoegde nationale orgaan voor informatieveiligheid geacht te zijn?

In artikel 19 wordt bepaald dat gekwalificeerde verleners van vertrouwensdiensten die gekwalificeerde vertrouwensdiensten verlenen het risico van aansprakelijkheid dragen door er voor te zorgen dat zij voldoende financiële middelen tot hun beschikking hebben of door middel van een toereikende aansprakelijkheidsverzekering. De zogenaamde DigiNotar-affaire heeft tot het faillissement van DigiNotar geleid. Had deze bepaling het risico op dit faillissement verminderd?
Had de onderhavige verordening sowieso het risico op de veiligheidsinbreuken op de systemen van DigiNotar verminderd? Hoe beoordeelt de Nederlandse regering dat?

Verder wenst de commissie de volgende vragen aan de regering voor te leggen. Om welke e-ID's gaat het precies in de ontwerpverordening, hoeveel landen kennen hoeveel en welke e-ID's? Gaat het om het veiliger maken van handelingen die nu grensoverschrijdend al plaatsvinden of gaat het om het uitbreiden van de mogelijkheden daarvan? Welke belemmeringen zijn er nu zonder dat deze verordening er is en kan de regering voorbeelden geven van het praktische nut ervan? Welke zekerheid hebben verschaffers van e-ID's dat hun gegevens door ontvangers op een juiste wijze worden beschermd? Verder zou de commissie graag vernemen wat de Nederlandse regering in de brede oriëntatiefase in de richting van de Europese Commissie heeft geantwoord over de wenselijkheid en het nut van de onderhavige verordening. Tot slot, kan de regering aangeven hoeveel geld er met toezicht gemoeid zal zijn?

De commissie voor Binnenlandse Zaken en de Hoge Colleges van Staat / Algemene Zaken en Huis der Koningin zien met belangstelling uit naar de antwoorden van de regering en ontvangt deze graag binnen **vier weken** na dagtekening van deze brief.

Voorzitter van de vaste commissie voor Binnenlandse Zaken en de Hoge Colleges van Staat / Algemene Zaken en Huis der Koningin,
J. W. M. Engels

BRIEF VAN DE MINISTER VAN ECONOMISCHE ZAKEN, LANDBOUW EN INNOVATIE

Aan de Voorzitter van de Eerste Kamer der Staten-Generaal

Den Haag, 3 september 2012

Bij brief van 4 juli 2012 heeft uw vaste commissie voor Binnenlandse Zaken een aantal vragen gesteld en opmerkingen gemaakt over de Verordening betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt (COM(2012)238), hierna de Verordening. In deze reactie ga ik, mede namens mijn collega van Binnenlandse Zaken en Koninkrijksrelaties, in op uw punten. Daarbij merk ik op dat de Verordening de status heeft van een voorstel van de Europese Commissie en nog niet de definitieve status heeft bereikt. Als gevolg van nieuwe inzichten en onderhandelingen in het Raadstraject zal de tekst nog wijzigen waardoor gedetailleerde antwoorden op sommige vragen op dit moment niet te geven zijn.

Reikwijdte verordening
Uw commissie vraagt of de stelsels die worden aangemeld ook van toepassing kunnen zijn op elektronische identificatiemiddelen die niet uitsluitend worden gebruikt om online toegang te krijgen tot een dienst van een bestuursorgaan in de zin van de Algemene wet bestuursrecht. Artikel 6, eerste lid, sub b, van de ontwerpverordening heeft betrekking op de wederzijdse erkenning van aangemelde stelsels van elektronische identificatiemiddelen. Die wederzijdse erkenning geldt uitsluitend voor het gebruik van identificatiemiddelen voor toegang tot elektronische overheidsdiensten. Dit sluit een breder gebruik van aangemelde stelsels voor identificatiemiddelen niet uit. Aangemelde stelsels voor identificatie kunnen ook buiten het domein van toegang tot elektronische overheidsdiensten worden gebruikt. De wederzijdse erkenning voor overheidsdiensten doet daar op zichzelf niet aan af.

Verantwoordelijkheid en aansprakelijkheid
De regering heeft in zijn BNC-fiche de vereiste dat een elektronisch identificatiemiddel «door, namens of onder de verantwoordelijkheid van de aanmeldende lidstaat wordt uitgegeven» als specifiek aandachtspunt aangemerkt. Met de keuze voor deze formulering sluit de ontwerpverordening inderdaad in potentie de wederzijdse erkenning van bepaalde private elektronische identificatiemiddelen uit, die op grond van nationale wetgeving of gangbare bestuursrechterlijke praktijk online toegang tot overheidsdiensten zouden kunnen verschaffen. Doel van het kabinet is dat wederzijdse erkenning zich in de praktijk ook uitstrekt tot andere oplossingen voor identificatie dan die gebaseerd op gekwalificeerde certificaten.

De Verordening stelt eisen aan de dienstverleners en stelt deze aansprakelijk voor de naleving daarvan. De aanmeldende lidstaat wordt alleen aansprakelijk gesteld voor de ondubbelzinnige koppeling van de (elektronische) persoonsidentificatiegegevens aan de natuurlijke persoon of de rechtspersoon (artikel 6, lid 1 punt e). Daarnaast wordt de lidstaat aansprakelijk voor een online-authenticatiemogelijkheid waarmee afhankelijke partijen ontvangen elektronische persoonsidentificatiegegevens kunnen valideren. De regering is met uw commissie van opvatting dat de dienstverleners verantwoordelijk en aansprakelijk zouden moeten zijn voor al hun activiteiten, waaronder de koppeling tussen de persoonsidentificatiegegevens aan een elektronisch identificatiemiddel.
Dit laat echter onverlet dat een lidstaat wel verantwoordelijk is voor een juiste uitgifte van unieke identificerende nummers, zoals – in Nederland –

het BSN en KvK-nummer. De regering is geen voorstander van het overnemen van verantwoordelijkheden en aansprakelijkheden van (private) dienstverleners (BNC-fiche[1] onder punt 9). Nederland zal zijn standpunt aangaande aansprakelijkheid inbrengen in de raadswerkgroep waar de Verordening wordt besproken.

Wetgeving en toezicht
Op grond van de Telecommunicatiewet houdt OPTA momenteel toezicht op de zogeheten gekwalificeerde certificaten die voor het zetten van een gekwalificeerde elektronische handtekening worden gebruikt. Naast elektronische handtekeningen omvat de Verordening ook andere vertrouwensdiensten zoals; elektronische zegels, -tijdstempels, -bezorgdiensten, – documenten, en websitecertificaten. Deze vertrouwensdiensten vallen momenteel in het geheel niet onder het toezicht van OPTA. In de tekst van de Verordening, zoals deze nu luidt, zullen genoemde vertrouwensdiensten wel onder het toezicht van OPTA gaan vallen. Bij dat verruimde toezicht wordt onderscheid gemaakt tussen gekwalificeerde en niet-gekwalificeerde vertrouwensdiensten. Een aanbieder van een gekwalificeerde vertrouwendienst mag niet eerder daarmee starten dan nadat zij het voornemen daartoe hebben gemeld bij het toezichtorgaan en daarbij een verslag hebben overgelegd van een door een erkend onafhankelijk orgaan uitgevoerde veiligheidsaudit. Deze derdenverklaring is daarmee niet langer optioneel. Een dergelijke derdenverklaring dient bovendien jaarlijks te worden overgelegd. Ook in andere opzichten krijgt het toezicht meer aandacht, zoals bij veiligheidsincidenten, het melden daarvan en wederzijdse bijstand tussen toezichthoudende organen.
De inrichting van het toezicht door OPTA wordt in het licht van de Verordening opnieuw bezien. De met het toekomstige toezicht samenhangende kosten zijn op dit moment moeilijk te kwantificeren. Wel is duidelijk dat door de toename van scope en intensiteit van de toezichtstaak de kosten voor het toezicht significant zullen toenemen.
Zo stellen artikel 15 en 16 een aantal veiligheidseisen aan verleners van vertrouwensdiensten en het toezicht daarop. Als gevolg van de rechtstreekse werking van de Verordening zal het toezicht van OPTA in lijn met de eisen van de Verordening worden gebracht.

Meldplicht
Bij brief van 6 juli 2012[2] heeft de minister van Veiligheid en Justitie de Kamer geïnformeerd over meldplichten en interventiemogelijkheden bij veiligheidsinbreuken. Voor de in de Verordening opgenomen meldplicht zal worden aangesloten bij de uitgangspunten die in deze brief genoemd zijn. Dit betekent dat verleners van vertrouwensdiensten verplicht worden om een veiligheidsinbreuk bij de OPTA te melden en dat de OPTA, indien nodig, het Nationaal Cyber Security Centrum (NCSC) informeert.

Aansprakelijkheid en veiligheidsrisico's
De in artikel 19 genoemde verplichte indekking tegen aansprakelijkheid komt ook voor in bijlage II van de huidige Richtlijn Elektronische Handtekeningen voor certificatiedienstverleners van gekwalificeerde certificaten. De reikwijdte van die verplichting is in de Verordening verruimd tot dienstverleners van gekwalificeerde vertrouwensdiensten. In de praktijk hebben vertrouwensdienstverleners een aansprakelijkheidsverzekering. De aandeelhouder van DigiNotar heeft zelf het faillissement van DigiNotar aangevraagd. Omdat het vertrouwen in het bedrijf was verdwenen, cq. opgezegd, viel het grootste deel van de klanten en dus ook inkomsten weg, terwijl de kosten van de bedrijfsvoering doorliepen.
Uit de onderzoeken[3] naar aanleiding van de DigiNotarzaak blijkt dat de veiligheid kan worden verhoogd door een samenhangend pakket maatregelen. De Europese Commissie heeft met belangstelling kennis

[1] Kamerstukken I 2011–2012, 22 112, FL
[2] Kamerstukken II, 2011–2012, 26 643, nr. 247
[3] Kamerstukken II, 2011–2012, 26 643, nr. 222

genomen van de brief aan de Tweede Kamer van 14 maart, waarin de lessen van de DigiNotarzaak zijn beschreven[1]. Op verzoek van de Commissie heeft inmiddels een vervolggesprek over de lessen plaatsgevonden. De Verordening kan op een aantal punten als verbetering ten opzichte van de Richtlijn Elektronische Handtekeningen worden beschouwd. Zo is de scope breder, waarmee meer vertrouwensdiensten een basis in het recht krijgen, waardoor toezicht houden mogelijk wordt. Daarnaast biedt het instrument van een Verordening de mogelijkheid om zaken eenduidig en helder te regelen voor verleners van vertrouwensdiensten in alle lidstaten. Een voorbeeld hiervan is de verplichte veiligheidsaudit (artikel 16, eerste lid). Een reductie van complexiteit, stevig toezicht, transparante juridische en technische eisen dragen bij aan het reduceren van de kans op veiligheidsinbreuken bij vertrouwensdienstverleners. Daarmee zijn we er echter nog niet. De DigiNotarzaak heeft geleerd dat informatiebeveiliging topprioriteit dient te zijn bij het management van vertrouwensdienstverleners.

Overige vragen

De Verordening omvat alle elektronische identiteiten die toegang bieden tot elektronische overheidsdiensten. Een lidstaat bepaalt zelf of het zijn elektronische identiteit(en) notificeert. Van de 27 lidstaten zijn de volgende Lidstaten aanwijsbaar in staat om hun elektronische identiteiten technisch grensoverschrijdend te laten werken, te weten: Oostenrijk, België, Estland, Frankrijk, Finland, Duitsland, Litouwen, Italië, Luxemburg, Portugal, Slovenië, Spanje, Verenigd Koninkrijk, Zweden[2]. Veelal betreft het een (gekwalificeerd) certificaat op een nationale identiteitskaart waarmee identificatie en authenticatie op een hoog betrouwbaarheidsniveau mogelijk is en een (gekwalificeerde) elektronische handtekening kan worden gezet. Naast (nationale) identiteitskaarten worden ook andere dragers, zoals een USB-stick of bankpasjes gebruikt. Genoemde landen hebben de interoperabiliteit van hun elektronische identificatie beproefd en een aantal van hen zal naar verwachting snel tot notificatie overgaan. Als Nederland zijn stelsel voor elektronische identiteiten notificeert en dit door de Europese Commissie wordt geaccepteerd, betekent dit voor Nederlandse burgers en bedrijven op termijn een aanzienlijke uitbreiding van de mogelijkheden om veilig grensoverschrijdend elektronisch te kunnen communiceren. Zo regelt de Verordening de wederzijdse erkenning van elektronische identiteiten, iets dat nu nog geen wettelijke basis in de interne markt heeft. Daarnaast zijn lessen getrokken uit de praktijk van de Richtlijn Elektronische Handtekeningen en wordt het toezicht eenduidiger geregeld dan onder deze Richtlijn het geval was. De Verordening levert daarmee ook een basis voor grensoverschrijdend gebruik van veilige elektronische identiteiten en vertrouwensdiensten. De praktijk onder de Richtlijn heeft belemmeringen op het gebied van grensoverschrijdende interoperabiliteit van elektronische handtekeningen aan het licht gebracht. Deze konden ondermeer ontstaan doordat de lidstaten de Richtlijn op verschillende manieren technisch implementeerden. Hierdoor bleek grensoverschrijdend gebruik van elektronische handtekeningen in de praktijk lastig. Zo is het niet eenvoudig om de echtheid van een handtekening te controleren in het land van herkomst. De toegevoegde waarde van het instrument Verordening is de rechtstreekse werking waarmee uiteenlopende nationale implementaties moeten worden voorkomen. Processen waarbij elektronische handtekeningen reeds grensoverschrijdend worden gebruikt, bijvoorbeeld Europese aanbestedingen, hebben baat bij eenduidige regelgeving, technische standaardisatie, en gelijktijdige inwerkingtreding.

Artikel 11 van de Verordening bevat de bepalingen voor gegevensverwerking- en bescherming. Deze bepalingen zien vooral op de verleners van vertrouwensdiensten. Ontvangers van vertrouwensdiensten

[1] Kamerstukken II, 2011–2012, 26 643, nr. 230

[2] Bronvermelding:
https://www.eid-stork.eu/index.php?option=com_processes&Itemid=&act=streamDocument&did=1846
https://www.eid-stork.eu/index.php?option=com_processes&Itemid=&act=streamDocument&did=1852

zijn gebonden aan de nationale privacywetgeving die in lijn moet zijn met de Europese Dataprotectierichtlijn (95/46/EG).

Deze richtlijn wordt momenteel vervangen door een verordening die ook van toepassing zal zijn op de ontvangers van vertrouwensdiensten. De nationale dataprotectietoezichthouders hebben de taak de huidige en toekomstige dataprotectiewetgeving te handhaven. Toepassing van het beginsel van dataminimalisatie bij elektronische identiteiten en vertrouwensdiensten kan de kans op misbruik van gegevens door de ontvangende partij aanzienlijk verminderen.
Nederland onderschrijft het nut van de Verordening en de keuze voor dit instrument. Nederland meent dat de Verordening kansen biedt voor aanbieders en afnemers van elektronische diensten. De regering plaatst, gelet op de gangbare praktijk in Nederland, echter kanttekeningen bij de focus die de Verordening legt op «gekwalificeerde certificaten». Hierdoor komt het principe van technologische neutraliteit in het gedrang. Een uitgebreide uitwerking van het Nederlandse standpunt ten aanzien van de Verordening vindt u in het reeds genoemde BNC-fiche.

Minister van Economische Zaken Landbouw en Innovatie,
M. J. M. Verhagen