Ministerie van Economische Zaken,
Landbouw en Innovatie

> Retouradres Postbus 20401 2500 EK Den Haag

De Voorzitter van de Eerste Kamer
der Staten-Generaal
Binnenhof 22
2513 AA 's-GRAVENHAGE

Directoraat-generaal Bedrijfsleven & Innovatie
Directie Regeldruk en ICT-beleid

Bezoekadres
Bezuidenhoutseweg 20
2594 AV Den Haag

Postadres
Postbus 20401
2500 EK Den Haag

Factuuradres
Postbus 16180
2500 BD Den Haag

Overheidsidentificatienr
00000001003214369000

T 070 379 8911 (algemeen)
www.rijksoverheid.nl/eleni

Datum 3 september 2012

Betreft Reactie brief Verordening elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt (COM(2012)238)

Ons kenmerk
DGBI-R&I / 12096937

Uw kenmerk
150924u

Geachte Voorzitter,

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.

[1] Kamerstukken I 2011–2012, 22 112, FL

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 genomen van de brief aan de Tweede Kamer van 14 maart, waarin de lessen van de DigiNotarzaak zijn beschreven[4]. 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.

[2] Kamerstukken II, 2011–2012, 26 643, nr. 247

[3] Kamerstukken II, 2011–2012, 26 643, nr. 222

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

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

---

[5] 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

Directoraat-generaal
Bedrijfsleven & Innovatie
Directie Regeldruk en ICT-beleid

Ons kenmerk
DGBI-R&I / 12096937

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.

(w.g.) drs. M.J.M. Verhagen
Minister van Economische Zaken Landbouw en Innovatie