

Vergaderjaar 2011–2012

33 331

EU-voorstel: Verordening betreffende elektronische identificatie en diensten voor elektronische transacties in de interne markt COM(2012) 238¹

A

BRIEF AAN DE VICEVOORZITTER VAN DE EUROPESE COMMISSIE

Den Haag, 9 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.² Graag legt de commissie een aantal vragen en opmerkingen over deze ontwerpverordening aan u voor.

In de toelichting op de ontwerpverordening wordt gesteld dat de technologische onpartijdigheid van het wetgevingskader behouden blijft. Nu is de huidige Europese richtlijn elektronische handtekening bepaald niet technologieonafhankelijk. Alleen als PKI-technologie wordt toegepast kan de huidige richtlijn worden begrepen en toegepast, en kunnen elektronische handtekeningen worden geplaatst die dezelfde rechtskracht hebben als handgeschreven handtekeningen. Deze handtekeningen hebben dwingende bewijskracht. Ook voor deze ontwerpverordening geldt dat deze uit lijkt te gaan van de toepassing van PKI-technologie. Klopt deze veronderstelling? Kent de Europese Commissie nog andere identificatiemiddelen waarop deze richtlijn van toepassing is, waarbij geen gebruik wordt gemaakt van digitale certificaten?

Artikel 5 van de ontwerpverordening bepaalt dat de wederzijdse erkenning en aanvaarding van elektronische identificatiemiddelen onder een regeling vallen die bij de Europese Commissie aangemeld wordt door de lidstaten. De voorwaarden voor aanmelding van nationale stelsels van elektronische identificatie waarop deze regelingen van toepassing zijn, zijn opmerkelijk te noemen. De elektronische identificatiemiddelen moeten zijn afgegeven door, namens of onder de verantwoordelijkheid van de aanmeldende lidstaat. Dit gaat veel verder dan het stellen van voorwaarden aan de afgifte van identificatiemiddelen, zoals we die nu kennen in de Europese richtlijn elektronische handtekening en de (Nederlandse) Wet elektronische handtekening of Wet elektronisch bestuurlijk verkeer. Waarom wordt deze eis gesteld? Kan niet volstaan worden met het stellen van eisen aan de afgifte van elektronische identificatiemiddelen zelf of eisen aan de partijen die deze identificatie-

¹ Zie E120015 op www.europapoort.nl

² COM(2012)238; het COM-document is ter inzage gelegd op de afdeling Inhoudelijke ondersteuning onder griffie nr. 150924.01u

middelen afgeven? Hoe wordt voorkomen dat er oneigenlijke concurrentie plaatsvindt met marktpartijen?

Hoe reëel is het dat online authenticatiemogelijkheden op ieder moment en gratis beschikbaar worden gesteld? Bedoelt de Europese Commissie met «ieder moment» een 100% beschikbaarheid? Of is 98% beschikbaarheid ook aanvaardbaar? Kunnen dienstverleners in hun algemene voorwaarden uitzonderingen opnemen op deze beschikbaarheidseis? Voor wiens rekening komen de kosten van het op ieder moment en gratis beschikbaar stellen van online authenticatiemogelijkheden? Aan wie mogen dienstverleners hun kosten doorberekenen voor het gebruikmaken van authenticatiemogelijkheden? Hoe wordt voorkomen dat er oneigenlijke concurrentie optreedt met marktpartijen?

De aansprakelijkheid van lidstaten onder artikel 6 lid 1 sub e is onbeperkt. Is dat inderdaad de bedoeling? Hebben lidstaten de vrijheid om deze aansprakelijkheid in contracten te beperken? Hoe wordt voorkomen dat deze onbeperkte aansprakelijkheid wordt afgewenteld op de aanbieder van elektronische identificatiemiddelen, dan wel wordt doorberekend in de tarieven aan eindgebruikers? Hebben aanbieders van elektronische identificatiediensten de vrijheid om hun aansprakelijkheid in hun algemene voorwaarden, Certificate Policies of Certification Practice Statements en/of contracten te beperken?

Voor de verleners van vertrouwensdiensten geldt dat op hem controle wordt uitgeoefend door de nationale toezichthouder. In artikel 13 lid 2 sub c wordt verwezen naar artikel 19 lid 2 onder g). Moet dit niet onder h) zijn?

Artikel 11 verwijst naar Richtlijn 95/46/EG. Deze richtlijn bevat minder waarborgen voor de betrouwbaarheid van de gegevensverwerking dan de voorgestelde Europese privacyverordening (COM(2012)11). Is de Europese Commissie bereid de relevante bepalingen van bedoelde verordening in de onderhavige verordening op te nemen?

Artikel 16 lid 1 spreekt van een verplichte jaarlijkse audit voor dienstverleners zodat zij kunnen bevestigen dat zij voldoen aan de eisen van de verordening, hetgeen vastgelegd wordt in een veiligheidsaudit. Klopt het dat het woord «veiligheidsaudit» niet helemaal gelukkig is gekozen en dat het verslag van de audit verder gaat dan alleen die eisen van de verordening die op de veiligheid van de dienstverlening betrekking hebben?

Ten slotte, artikel 19 lid 2 sub d bepaalt dat gekwalificeerde verleners van vertrouwensdiensten gebruikmaken van betrouwbare systemen en producten die de betrouwbaarheid garanderen van de processen die zij ondersteunen. Moet deze bepaling zo worden opgevat dat als de betrouwbaarheid van die processen met technologie kan worden afgedwongen deze ook met technologie moet worden afgedwongen? Is deze bepaling te vergelijken met de verplichting van *privacy by design* en *default* uit de voorgestelde Europese privacyverordening?

De vaste commissie voor Binnenlandse Zaken en de Hoge Colleges van Staat / Algemene Zaken en Huis der Koningin verheugt zich op het antwoord van de Europese Commissie in het kader van de politieke dialoog en vertrouwt erop dat de Europese Commissie binnen de door haarzelf gestelde termijn van drie maanden zal reageren.

Een afschrift van deze brief is verstuurd aan de Nederlandse regering

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