Beleidsregel aanwijzing certificatieorganisaties elektronische handtekeningen

Beleidsregel van de Staatssecretaris van Economische Zaken met betrekking tot de aanwijzing van organisaties die certificatiedienstverleners toetsen op de overeenstemming met de bij of krachtens de Telecommunicatiewet gestelde eisen, op grond van artikel 18.16 van de Telecommunicatiewet (Beleidsregel aanwijzing certificatieorganisaties elektronische handtekeningen)

6 mei 2003/nr. WJZ/03/02264

De Staatssecretaris van Economische Zaken,

Besluit:

Artikel 1
In deze beleidsregel wordt verstaan onder:
a. minister: de Minister van Economische Zaken;
b. wet: Telecommunicatiewet.

Artikel 2
1. Een aanvraag voor een aanwijzing als organisatie als bedoeld in artikel 18.16 van de wet, die certificatiedienstverleners beoordeelt onder een vrijwillige accreditatieregeling, wordt ingediend bij:
Ministerie van Economische Zaken
Directoraat-Generaal
Telecommunicatie en Post
Postbus 20101
2500 EC Den Haag.
2. De aanvraag gaat vergezeld van bewijsstukken waaruit blijkt dat de organisatie ten minste:
a. een toetsingskader hanteert dat garandeert dat de getoetste certificatiedienstverleners en de certificaten die zij afgeven voldoen aan de wettelijke eisen;
b. voorwaarden hanteert die objectief, transparant, evenredig en niet-discriminerend zijn;
c. geaccrediteerd is op basis van de norm EN 45011 of EN 45012 of een gelijkwaardige norm, welke accreditatie het vakgebied 'gekwalificeerde certificaten' dient te omvatten, door een instantie die aantoonbaar voldoet aan de norm EN 45010 of een gelijkwaardige norm;
d. voldoet aan artikel 3.

Artikel 3
1. Het personeel dat door de organisatie als auditor wordt ingezet om een conformiteitsbeoordeling uit te voeren van een certificatiedienstverlener:
a. heeft een opleiding op minimaal HBO-niveau dan wel een daaraan gelijkwaardige aanmerkelijke ervaring en aanvullende beroepsopleiding en -training;
b. beschikt over een equivalent van ten minste vier jaar voltijds praktijkervaring met betrekking tot informatietechnologie, waarvan tenminste twee jaar in een functie met betrekking tot Public Key Infrastructure en informatiebeveiliging;
c. heeft voldoende begrip van de technische technische specificatie ETSI TS 101 456 of een daarmee gelijkwaardige technische specificatie;
d. heeft voldoende begrip van de concepten van managementsystemen in het algemeen;
e. heeft voldoende begrip van onderwerpen die zijn gerelateerd aan Public Key Infrastructure, management van informatiebeveiliging en organisatorische betrouwbaarheid;
f. heeft voldoende kennis van de principes en processen gerelateerd aan risicobeoordeling en risicomanagement;
g. heeft een training van ten minste 5 dagen afgerond over het beoordelen van managementsystemen en het management van beoordelingsprocessen;
h. beschikt over de volgende persoonlijke eigenschappen: integer, onbevooroordeeld, volwassen houding, onderscheidingsvermogen, analytisch, vasthoudend en realistisch;
i. kan complexe operaties in een breed perspectief plaatsen en de rol van individuele eenheden in grote organisaties begrijpen;
j. heeft kennis en eigenschappen om beoordelingsprocessen te managen;
k. zorgt ervoor dat de eigen kennis en vaardigheden op het gebied van Public Key Infrastructure, management van informatiebeveiliging en beoordeling van managementsystemen voortdurend op peil worden gehouden;
l. heeft voorafgaand aan zelfstandig optreden als auditor ervaring opgedaan in het hele proces van beoordeling van certificatiedienstverleners, welke ervaring is verkregen door onder supervisie van een ervaren auditor deel te nemen aan minimaal vier beoordelingen bestaande uit totaal ten minste 20 dagen, hierbij inbegrepen toetsing van documentatie, implementatiebeoordeling en opstelling beoordelingsrapport.
2. In aanvulling op de eisen, genoemd in het eerste lid, voldoet een auditor die als leider van een auditteam optreedt, aan de volgende eisen:
a. hij heeft opgetreden als een gekwalificeerd auditor in ten minste drie complete beoordelingen van certificatiedienstverleners;
b. hij beschikt over adequate kennis en eigenschappen om het beoordelingsproces te managen;
c. hij beschikt over de capaciteit om effectief te communiceren, zowel mondeling als schriftelijk.
3. Een beoordelingsteam als geheel voldoet aan de volgende eisen:
a. in elk van de volgende kennisgebieden is tenminste één auditor binnen het beoordelingsteam gekwalificeerd om de verantwoordelijkheid te dragen voor:
1°. de benodigde kennis van wetgeving en regelingen waaraan binnen het specifieke veld van certificatiedienstverlening en informatiebeveiliging moet zijn voldaan;
2°. de benodigde kennis van de laatste stand van de techniek betreffende Public Key Infrastructure;
3°. De benodigde kennis om een aan informatiebeveiliging gerelateerde risicobeoordeling uit te voeren om kwetsbaarheden te ontwaren bij de certificatiedienstverlener, het begrijpen van hun betekenis voor de dienstverlening en het verminderen en onder controle brengen van deze kwetsbaarheden, en
4°. de benodigde kennis van kwesties

van organisatorische betrouwbaarheid.
b. het beoordelingsteam is competent om indicaties van kwetsbaarheden in de certificatiedienstverlening terug te leiden naar de desbetreffende elementen van het managementsysteem van de certificatiedienstverlener opdat deze verbeterd kunnen worden.
4. Om er voor te zorgen dat het beoordelingsteam alle noodzakelijke expertise tot zijn beschikking heeft, mogen technisch deskundigen met specifieke kennis over de onderwerpen, genoemd in het derde lid, onder a, 1° tot en met 4°, worden ingeschakeld om het beoordelingsteam te assisteren, ook al voldoen zij niet aan alle criteria voor een individuele auditor.
5. De technisch deskundigen, bedoeld in het vierde lid, zijn te allen tijde verantwoording schuldig aan de leider van het auditteam en functioneren niet onafhankelijk van de auditors in het team die wel gekwalificeerd zijn als auditor.

Artikel 4
De organisatie verleent de Minister alle medewerking bij de beoordeling of het gestelde in het tweede artikel wordt voldaan, door ten minste inzage te verstrekken in alle bescheiden, voorzover die nodig is in verband met deze beoordeling.

Artikel 5
1. De aangewezen certificatieorganisatie deelt de Minister de namen en adressen van certificatiedienstverleners mee die door de organisatie zijn gecertificeerd dan wel van wie de certificatie is ingetrokken.
2. De melding, bedoeld in het eerste lid, vindt plaats binnen een maand na de datum van de certificatie of de datum van intrekking.
Artikel 6
Een aanwijzing kan worden ingetrokken indien de certificatieorganisatie niet meer voldoet aan de artikelen 2 tot en met 5.

Artikel 7
Deze beleidsregel wordt aangehaald als: Beleidsregel aanwijzing certificatieorganisaties elektronische handtekeningen

Deze beleidsregel treedt in werking op het tijdstip waarop de Wet elektronische handtekeningen in werking treedt.

's-Gravenhage, 6 mei 2003.
De Staatssecretaris van Economische Zaken,
J.G. Wijn.

Toelichting

I.1 Inleiding

Ingevolge artikel 18.16 van de Telecommunicatiewet kan de Minister van Economische Zaken organisaties aanwijzen die certificatiedienstverleners toetsen op de overeenstemming met de bij of krachtens de Telecommunicatiewet gestelde eisen. Deze beleidsregel geeft aan onder welke voorwaarden een aanvraag om aanwijzing als een zogenoemde certificatieorganisatie wordt toegewezen.

I.2 Advisering

Deze beleidsregel is in oktober 2002 aan de leden van het Permanent Overlegorgaan Post en Telecommunicatie (OPT), de Onafhankelijke Post- en Telecommunicatieautoriteit (OPTA), de Taskforce PKI Overheid en het Electronic Commerce Platform Nederland (ECP.NL) gezonden. Het OPT had geen opmerkingen.
Hieronder wordt op het belangrijkste commentaar ingegaan.
OPTA geeft aan dat uit de beleidsregel niet blijkt of de Minister na aanwijzing van een organisatie die certificatiedienstverleners toetst, op een regelmatige basis deze organisatie blijft controleren. OPTA acht dit wel wenselijk. Naar aanleiding hiervan is in de toelichting bij artikel 2 nader op dit punt ingegaan.
De Taskforce PKI Overheid heeft opgemerkt dat de eisen die in artikel 3, eerste lid, zijn opgenomen, in sommige gevallen zwaar zijn in een zich ontwikkelende markt waarin nog weinig certificatiedienstverleners opteren voor een vrijwillige accreditatie. De gestelde eisen komen echter overeen met de in Europa inmiddels aanvaarde eisen. Handhaving van die eisen is met het oog op certificatiedienstverlening binnen de hele Europese Unie nodig.

I.3 Notificatie

De beleidsregel is op 17 oktober 2002 (kennisgeving 2002/398) ter notificatie toegezonden aan de Europese Commissie. Van de zijde van de Europese Commissie is opgemerkt dat het voorschrift dat de instellingen die door de Minister van Economische Zaken worden aangewezen moeten zijn geaccrediteerd door de Raad voor de Accreditatie een belemmering kan betekenen voor instellingen uit andere lidstaten die wensen te worden aangewezen. In verband hiermee is in artikel 2, tweede lid, onderdeel c de verwijzing naar deze Raad vervangen door een verwijzing naar de toepasselijke norm (EN45010) waaraan de instelling moet voldoen.

I.4 Administratieve lasten

Er zijn momenteel drie organisatie die in aanmerking wensen te komen voor een aanwijzing. De administratieve lasten die samenhangen met het voldoen aan de eisen die deze beleidsregel stelt om in aanmerking te komen voor aanwijzing worden begroot op € 300,-. Het gaat daarbij om het samenstellen en opsturen van de informatie die binnen die organisaties al voorhanden is. Tevens moeten wijzigingen in de opgegeven informatie worden doorgegeven. De totale administratieve lasten voor deze groep op grond van deze beleidsregel worden daarom geraamd op € 1000,-. Gelet op het belang voor de certificatiedienstverleners om gebruik te kunnen maken van vrijwillige accreditatieregelingen en op de belangen van de toezichthouder en de gebruikers van certificatiediensten moet de Minister een goed inzicht hebben in de betrouwbaarheid van de organisaties. De gestelde eisen vormen daarvoor een adequaat toetsingskader.
Het Adviescollege toetsing administratieve lasten heeft op 25 april 2003 laten weten dat het heeft besloten geen advies uit te brengen over deze beleidsregel.

II. Artikelen

Artikelen 2 en 3
In artikel 2, tweede lid, onderdeel c, wordt een accreditatie gevraagd die het vakgebied gekwalificeerde certificaten dient te omvatten. Dit betekent

dat uit deze accreditatie moet blijken dat minimaal voldaan is aan de eisen van de artikelen 2 en 3 van deze beleidsregel. Bij de aanwijzing zal de Minister de aan te wijzen organisatie verplichten ermee in te stemmen dat de accreditatieorganisatie, die de aan te wijzen organisatie heeft geaccrediteerd, de Minister met redenen omkleed informeert over eventuele afwijkingen ten opzichte van de oorspronkelijke accreditatie die tijdens de door haar uitgevoerde (jaarlijkse) herbeoordelingen worden geconstateerd. Dit is belangrijke informatie voor de Minister om te kunnen beoordelen of de aangewezen organisatie blijft voldoen aan het gestelde in de artikelen 2 en 3, en indien dit niet het geval is, een aanwijzing in te kunnen trekken op grond van artikel 6 van de beleidsregel. De normering van de eisen die in artikel 3 zijn gesteld, is gebaseerd op CEN Workshop Agreement CWA 14172-2.

Artikel 4
Voor zover de geldigheidsduur van de aanwijzing bij de aanwijzingsbeschikking niet is beperkt, moet een aangewezen certificatieorganisatie steeds de informatie verschaffen aan de Minister waaruit blijkt dat nog steeds aan de gestelde eisen voor aanwijzing wordt voldaan. De Minister toetst deze overeenstemming met de eisen ten minste een keer per jaar. Vooralsnog wordt uitgegaan van een periode van vier jaar binnen welke de gestelde eisen en voorwaarden niet worden aangepast. Deze termijn is gelijk aan de gangbare termijn dat een accreditatie geldig is.

Artikel 5
De Minister moet, ingevolge van artikel 11 van de richtlijn nr. 1999/93/EG van het Europees Parlement en de Raad van de Europese Unie van 13 december 1999 betreffende een gemeenschappelijk kader voor elektronische handtekeningen (PbEG 2000, L 13), de namen en adressen van alle gecertificeerde nationale certificatiedienstverleners notificeren. Om adequaat aan deze plicht te voldoen, is dit artikel opgenomen.

De Staatssecretaris van Economische Zaken,
J.G. Wijn.