OPENBAAR

Ons kenmerk: OPTA/ACNB/2011/202084_OV
Zaaknummer: 11.0038.29
Datum: 13 september 2011

Besluit van het College van de Onafhankelijke Post en Telecommunicatie Autoriteit op grond van artikel 2.2, vierde lid, sub b van de Telecommunicatiewet tot het beëindigen van de registratie van Diginotar B.V. als certificatiedienstverlener wegens verrichten van activiteiten en diensten in strijd met artikel 2 van het Besluit elektronische handtekeningen.

1. Samenvatting

1. In dit besluit concludeert het college van de Onafhankelijke Post en Telecommunicatie Autoriteit (hierna: het college) dat Diginotar B.V. (hierna: Diginotar) activiteiten of diensten heeft verricht in strijd met het bepaalde in artikel 2, eerste lid, sub c en d, van het Besluit elektronische handtekeningen en artikel 18.15, eerste lid, van de Telecommunicatiewet (hierna: Tw). Het college besluit daarom op grond van artikel 2.2, vierde lid, sub b, van de Tw om de registratie van Diginotar als certificatiedienstverlener in te trekken.

2. Verloop van de procedure

2. Diginotar staat conform artikel 2.1, vijfde lid, van de Tw bij het college geregistreerd als certificatiedienstverlener die gekwalificeerde certificaten aanbiedt.[1]

3. Op maandag 29 augustus 2011 verschenen in de diverse media de eerste berichten over door Diginotar ten onrechte uitgegeven (valse) SSL-certificaten. Het college houdt geen toezicht op SSL-certificaten.

4. Op 30 augustus 2011, heeft Diginotar het bedrijf Fox-IT (hierna: Fox-IT) verzocht om een onderzoek in te stellen naar het beveiligingsincident dat bij Diginotar heeft plaatsgevonden en daarover een rapport op te stellen. Het doel van het rapport van Fox-IT is om relevante informatie te delen met belanghebbenden van Diginotar. Aan het rapport liggen drie onderzoeksvragen ten grondslag:

    - Hoe drongen de inbrekers binnen op het netwerk van Diginotar?
    - Wat is de omvang en status van het beveiligingsincident?
    - Kan er meer worden ontdekt over de impact van het beveiligingsincident?

    Het onderzoek van Fox-IT is uitgevoerd door een team van forensisch IT specialisten, cybercrime experts, malware analisten en een beveiligingsexpert met PKI ervaring. Fox-IT heeft in het verleden meerdere malen werkzaamheden voor de (rijks)overheid uitgevoerd.[2]

[1] Diginotar staat sinds 18 november 2003 bij het college geregistreerd onder registratienummer 940266.
[2] https://www.fox-it.com/nl/over-fox-it/referenties

Ook het college heeft Fox-IT in het verleden ingehuurd om onderzoek te verrichten. Dat maakte het onderzoek van Fox-IT voor het college een geschikte potentiële eerste informatiebron.

5. Op 31 augustus 2011 heeft het college per e-mail de volgende informatie opgevraagd bij Diginotar:
    - Het onderzoeksrapport dat in opdracht van Diginotar door Fox-IT wordt opgesteld of een conceptversie daarvan.
    - Het laatste auditrapport van PriceWaterhouseCoopers.

6. Omdat het college op vrijdag 2 september 2011 nog geen reactie van Diginotar had ontvangen op zijn e-mailbericht van 31 augustus 2011, heeft het college zijn verzoek herhaald in de schriftelijke informatievordering van 2 september 2011.

7. Omdat het college de bij Diginotar gevorderde informatie op maandagochtend 5 september 2011 nog niet had ontvangen, heeft het college de betreffende informatie tevens direct bij Fox-IT B.V. respectievelijk PriceWaterhouseCoopers gevorderd.

8. Op 5 september 2011 hebben medewerkers van het college een bezoek gebracht aan Fox-IT. Ten kantore van Fox-IT hebben onderzoekers van Fox-IT hun bevindingen uit het onderzoek bij Diginotar aan de medewerkers van het college toegelicht, waaronder in het bijzonder voor zover deze bevindingen betrekking hadden op de systemen die werden gebruik voor de uitgifte van gekwalificeerde certificaten.

9. Op dinsdag 6 september 2011 heeft het college om 11.17 uur de gevorderde informatie van Diginotar ontvangen.

10. Het rapport van Fox-IT en de toelichting van Fox-IT op dit rapport zijn vervolgens door het college onderzocht om vast te stellen of Diginotar de relevante regels die gelden voor aanbieders van gekwalificeerde certificaten heeft overtreden.

11. Op 7 september 2011 heeft het college Diginotar een brief gestuurd waarin Diginotar wordt bericht dat het college voornemens is de registratie van Diginotar als certificatiedienstverlener in te trekken.[3] In de hiervoor bedoelde brief wordt Diginotar tevens in de gelegenheid gesteld om voor vrijdag 9 september 2011 12.00 uur schriftelijk haar zienswijze bij het college in te dienen.

12. Op 9 september 2011 omstreeks 11 uur heeft Diginotar via haar gemachtigde een zienswijze bij het college ingebracht.

13. Op 9 september 2011 heeft de gemachtigde van Diginotar op verzoek van het college

[3] Kenmerk OPTA/ACNB/2011/202066. Deze brief is tevens per fax en per e-mail aan Diginotar verstuurd.

aangegeven waar de voorlopige bedenkingen van Diginotar ten aanzien van het Fox-IT rapport uit bestaan.

14. Op 9 september 2011 heeft Fox-IT een nadere verklaring afgelegd ten aanzien van de hacker activiteit op de CA-server van Diginotar die werd gebruikt voor de uitgifte van gekwalificeerde certificaten.

3. Feiten

15. Diginotar is een certificatiedienstverlener die in Nederland een vestiging heeft en gekwalificeerde certificaten aanbiedt aan het publiek.[4] Tot op heden kan Diginotar gekwalificeerde certificaten uitgeven aan het publiek .

16. Op grond van artikel 2.1, vijfde lid, van de Tw bestaat voor Diginotar de verplichting zich te laten registreren door het college.

17. Diginotar heeft er voor gekozen om gebruik te maken van de mogelijkheid om zich te laten accrediteren door een op grond van artikel 18.16 Tw aangewezen certificatie instelling (hierna: CI). Op grond van artikel 18.16a van de Tw wordt een certificatiedienstverlener die in het bezit is van een geldig bewijs van toetsing van een CI vermoed te voldoen aan artikel 18.15, eerste lid, van de Tw en worden de door de desbetreffende certificatiedienstverlener aan het publiek aangeboden certificaten vermoed te voldoen aan artikel 18.15, tweede lid, van de Tw.

18. Eén maal in de drie jaar wordt door de CI een certificatieaudit uitgevoerd bij Diginotar, waarbij de CI vaststelt of Diginotar voldoet aan de eisen, onder andere, uit ETSI-norm 101 456. Indien Diginotar voldoet aan de hiervoor genoemde eisen wordt door de CI daarvoor een bewijs van toetsing afgegeven. Tussentijds wordt door de CI minimaal één maal per jaar een surveillanceaudit uitgevoerd om te controleren of Diginotar nog voldoet aan de vereisten uit ETSI-norm 101 456.[5]

19. Voor de aanmaak van gekwalificeerde certificaten maakte Diginotar gebruik van verschillende door haar zelf aangemaakte Certification Authorities (CA's). Een CA geeft een digitaal certificaat uit, waarin de CA verklaart dat de publieke sleutel gevat in het certificaat toebehoort aan de persoon die in het certificaat vermeld wordt.[6]

20. Uit onderzoek dat door Fox-IT is uitgevoerd aan de systemen van Diginotar blijkt dat onbevoegde derden ("hackers") in juni 2011 de (administratieve) rechten van de Windows-domeinserver van Diginotar hebben verkregen.[7] Omdat alle CA-servers onderdeel uitmaakten van hetzelfde Windows-domein, kon met de administratieve rechten op de domeinserver

[4] In 2010 heeft Diginotar [vertrouwelijk] gekwalificeerde certifcaten aan het publiek uitgegeven.
[5] Het laatste bewijs van toetsing dateert op 1 november 2010.
[6] Voor een populaire uitleg zie wikipedia: http://nl.wikipedia.org/wiki/Certificaatautoriteit
[7] Interim report DigiNotar Certificate Authority breach, Fox-IT, 5 september 2011, pagina 6.

toegang worden verkregen tot de verschilende CA-servers van Diginotar.

21. Door Fox-IT zijn sporen van 'hackeractiviteit' (met gebruikmaking van administratieve rechten) gevonden op de CA-server die wordt gebruikt voor de uitgifte van gekwalificeerde certificaten.[8] Dit betekent dat een onbevoegde derde ('hacker') actief is geweest op de CA-server die wordt gebruikt voor de uitgifte van gekwalificeerde certificaten. Met gebruik van de administratieve rechten van een server kunnen gegevens op deze server worden gemanipuleerd, onttrokken of verwijderd. De integriteit van de gegevens op de CA-server die wordt gebruikt voor de aanmaak en uitgifte van gekwalificeerde certificaten is dan ook niet meer te garanderen.

22. Daarnaast heeft Fox-IT vastgesteld dat in ieder geval twee serienummers van certificaten op de CA server, die werd gebruikt voor de aanmaak van gekwalificeerde certificaten, niet kunnen worden gekoppeld aan vertrouwde certificaten. Daarom kan niet worden uitgesloten dat deze serienummers gekoppeld zijn aan ten onrechte uitgegeven (valse) certificaten.[9]

23. Op de door Fox-IT onderzochte servers, waaronder de CA-server gebruikt voor het aanmaken van gekwalificeerde certificaten, is geen antivirus software aangetroffen.[10]

24. De CA-servers van Diginotar bevonden zich fysiek in een goed beveiligde omgeving. Zoals hiervoor reeds aangegeven maakte de verschillende CA-servers echter onderdeel uit van hetzelfde Windows-domein en is een onbevoegde derde er in geslaagd om de administratieve rechten van deze server te verkrijgen. Daarnaast heeft Fox-IT sterke aanwijzingen aangetroffen om aan te nemen dat de CA-servers, naast de eerder genoemde domeinserver, ook bereikbaar waren via het managementnetwerk van Diginotar.[11]

25. Door Fox-IT is eveneens vastgesteld dat op 1 en 2 juli 2011 in de nachtelijk uren met de administratieve rechten is ingelogd op de CA- server die werd gebruikt voor uitgifte van gekwalificeerde certificaten ([vertrouwelijk]). Tevens is vastgesteld dat op de hiervoor genoemde tijdstippen is gewerkt met twee bestanden ([vertrouwelijk]) die sindsdien verdwenen zijn. Tijdens deze inlogsessies is ook de webpagina geopend die waarschijnlijk door een onbevoegde derde ("hacker") is gebruikt om in te breken op de systemen van Diginotar, de zogenaamde "Backdoor". [12]

4. Zienswijze van Diginotar op voornemen tot beëindiging registratie

26. Kort en zakelijk weergegeven voert Diginotar de volgende punten aan in haar zienswijze.

27. Allereerst is Diginotar van mening dat het college de conclusies uit het Fox-IT rapport

[8] Interim report DigiNotar Certificate Authority breach, Fox-IT, 5 september 2011, pagina 6 .
[9] Interim report DigiNotar Certificate Authority breach, Fox-IT, 5 september 2011, pagina 9.
[10] Interim report DigiNotar Certificate Authority breach, Fox-IT, 5 september 2011, pagina 9
[11] Interim report DigiNotar Certificate Authority breach, Fox-IT, 5 september 2011, pagina 9
[12] Dit blijkt uit de in randnummer 14 genoemde verklaring.

overneemt zonder zelf onderzoek te verrichten. De bevindingen van Fox-IT zijn volgens Diginotar voor een groot gedeelte twijfelachtig.

28. Ook al maakten de verschillende CA-servers onderdeel uit van één Windows-domein, er zijn volgens Diginotar geen aanwijzingen dat er op de server die werd gebruikt om gekwalificeerde certificaten aan te maken regels zijn verwijderd. Volgens Diginotar levert dit overtuigend bewijs op dat geen vervalste of illegale gekwalificeerde certificaten zijn aangemaakt.

29. Ten aanzien van de twee serienummers van certificaten die zijn gevonden op de server die werd gebruikt voor de uitgifte van gekwalificeerde certificaten en welke niet kunnen worden gekoppeld aan vertrouwde certificaten, merkt Diginotar het volgende op. Deze serienummers kunnen tijdelijk zijn gegenereerd door de CA software zonder dat deze gebruikt zijn, ook kunnen deze serienummers zijn aangemaakt door een “bug” in de software. Verder onderzoek is nodig om te verklaren waarom deze serienummers zijn aangemaakt.

30. Diginotar stelt zich ten aanzien van de door het college in zijn voornemen opgenomen overtredingen op het standpunt dat haar systemen onderdeel uitmaken van een ETSI gecertificeerd kwaliteitssysteem. Er is op dit moment volgens Diginotar geen bewijs aanwezig waaruit volgt dat Diginotar niet voldeed aan de certificatievereisten. Daar komt bij dat Diginotar altijd in het bezit is geweest van een bewijs van certificering van de CI.

31. Diginotar heeft OPTA niet direct geïnformeerd over het beveiligingsincident. Toen door Diginotar is ontdekt dat er via haar systemen ten onrechte (valse) SSL-certificaten zijn uitgegeven, is zij overgegaan tot het intrekken van deze certificaten en het treffen van beveiligingsmaatregelen. Diginotar heeft vervolgens een externe adviseur ingeschakeld en geconstateerd dat door het beveiligingsincident de systemen die gebruikt worden voor de aanmaak van gekwalificeerde certificaten niet zijn geraakt. Er bestond volgens Diginotar dan ook geen verplichting om OPTA te informeren. Uiteindelijk heeft Diginotar op 29 augustus 2011 de AIVD geïnformeerd, communicatie met de rest van de overheid heeft diginotar via GOVCERT.NL laten verlopen.

32. Diginotar stelt ten slotte dat het beëindigen van haar registratie tot gevolg zal hebben dat Diginotar de verplichtingen richting haar klanten niet kan nakomen. Het beëindigen van de registratie zal dan ook, in de visie van Diginotar, zeer waarschijnlijk het faillissement van Diginotar tot gevolg hebben.

5. Juridisch Kader

33. Artikel 2.2, vierde lid van de Tw luidt, voor zover relevant als volgt:

“4. Het college beëindigt of wijzigt de registratie:
a. indien de grond voor registratie is vervallen;
b. indien een certificatiedienstverlener activiteiten of diensten verricht in strijd met het bepaalde bij

of krachtens deze wet,
c. indien het college heeft vastgesteld dat de certificatiedienstverlener niet of niet geheel voldoet aan de eisen bedoeld in artikel 18.15, eerste en tweede lid, en de certificatiedienstverlener niet binnen de door het college gestelde termijn heeft aangetoond aan deze eisen te voldoen. Indien de certificatiedienstverlener aantoont redelijkerwijs niet binnen de gestelde termijn aan de eisen te kunnen voldoen, kan het college de termijn verlengen; of
d. indien het college heeft vastgesteld dat de certificatiedienstverlener de gegevens, bedoeld in artikel 2.1, vijfde lid, onder b, of wijzigingen daarin niet, onvolledig of niet juist heeft verstrekt, en de certificatiedienstverlener niet binnen de door het college gestelde termijn de volledige of juiste gegevens alsnog verstrekt."

34. Artikel 18.15 van de Tw luidt, voor zover relevant:

"1.Een certificatiedienstverlener die certificaten als gekwalificeerde certificaten aanbiedt of afgeeft aan het publiek en in Nederland een vestiging heeft, voldoet aan de eisen, gesteld bij of krachtens algemene maatregel van bestuur.

2. Certificaten die als gekwalificeerd certificaat aan het publiek worden aangeboden of afgegeven, voldoen aan de eisen gesteld bij of krachtens algemene maatregel van bestuur.

3. (…)"

35. Artikel 18.16 van de Tw luidt, voor zover relevant:

"1.Onze Minister kan een of meer organisaties aanwijzen die bevoegd zijn certificatiedienstverleners te toetsen op overeenstemming met de bij en krachtens deze wet gestelde eisen en daartoe een bewijs van toetsing af te geven.
(…)"

36. Artikel 18.16a van de Tw luidt, voor zover relevant:

"1. Een certificatiedienstverlener die in het bezit is van een geldig bewijs van toetsing van een op grond van artikel 18.16, eerste lid, aangewezen organisatie, wordt vermoed te voldoen aan artikel 18.15, eerste lid.

2. De certificaten die als gekwalificeerd aan het publiek worden aangeboden of afgegeven door een certificatiedienstverlener als bedoeld in het eerste lid, worden vermoed te voldoen aan artikel 18.15, tweede lid."

37. Artikel 2 van het Besluit elektronische handtekeningen luidt, voor zover relevant:

"1.Een certificatiedienstverlener als bedoeld in artikel 18.15, eerste lid, van de wet voldoet aan de

volgende eisen:
a. hij beschikt over betrouwbare middelen en hanteert betrouwbare procedures voor het aanbieden van certificatiediensten aan het publiek;
b. hij past procedures en processen op het gebied van administratie en beheer toe overeenkomstig een beschreven kwaliteitssysteem dat in overeenstemming is met de laatste ontwikkelingen op het gebied van kwaliteitssystemen;
c. hij maakt uitsluitend gebruik van betrouwbare systemen en producten die procedureel of overeenkomstig de stand der techniek beveiligd zijn en die de technische en cryptografische veiligheid van de processen die zij ondersteunen garanderen;
d. hij neemt adequate maatregelen tegen het vervalsen van de gekwalificeerde certificaten die hij heeft uitgegeven en tegen het uitgeven van illegale gekwalificeerde certificaten en, indien hij gegevens voor het aanmaken van handtekeningen genereert, garandeert hij de vertrouwelijkheid van het proces waarmee dit gebeurt;
e. hij houdt voldoende financiële middelen ter beschikking om in overeenstemming met de eisen van de wet te kunnen functioneren;
f. hij heeft personeel in dienst dat deskundig is op het gebied van de aangeboden diensten, met name op het gebied van beheer, van de technologie voor elektronische handtekeningen, en van de beveiligingsprocedures die worden toegepast;
g. hij verifieert, alvorens een gekwalificeerd certificaat af te geven, de identiteit en eventuele specifieke attributen van de persoon die als ondertekenaar in dat certificaat wordt aangeduid door de geldigheid van de aangeboden documenten te controleren alsmede door de overeenstemming tussen de documenten en de kenmerken van de persoon te controleren door middel van visuele controle en zonodig met behulp van andere daartoe geschikte middelen;
h. hij stelt de datum en het tijdstip van afgifte en van intrekking van een gekwalificeerd certificaat vast met een nauwkeurigheid van één minuut of korter;
i. hij slaat tijdens de geldigheidsduur van het gekwalificeerde certificaat en gedurende een periode van ten minste zeven jaar na de datum waarop de geldigheid van het gekwalificeerde certificaat is verlopen alle relevante gegevens met betrekking tot dat gekwalificeerde certificaat op, met name de gegevens die benodigd zijn om in gerechtelijke procedures de certificatie te kunnen bewijzen, waaronder ten minste:
1°. het gekwalificeerde certificaat;
2°. alle gegevens waarmee de verificatie van de ide ntiteit en van de attributen van de aanvrager bewezen kan worden, en
3°. alle historische gegevens over de afgifte en in trekking van het gekwalificeerde certificaat;
j. hij slaat ten behoeve van eigen gebruik en beheer certificaten zodanig op, in verifieerbare vorm en met gebruikmaking van betrouwbare systemen, dat:
1°. alleen bevoegde personen gegevens kunnen invoer en en wijzigen;
2°. de authenticiteit van de informatie kan worden gecontroleerd;
3°. de certificaten uitsluitend publiekelijk beschi kbaar zijn in de gevallen waarvoor de ondertekenaar toestemming heeft gegeven, en
4°. elke technische wijziging die de genoemde bevei ligingsvoorschriften in gevaar kan brengen, voor de gebruiker duidelijk is;

k. hij zorgt, met inachtneming van de door hem bekendgemaakte tijdsduur tussen verzoek tot intrekking en publicatie van die intrekking, voor een veilige en prompte intrekking van de door hem beheerde gekwalificeerde certificaten na ontvangst van een daartoe strekkend verzoek van de ondertekenaar of van een door hem aangewezen persoon of instantie, welk verzoek voldoet aan de door de certificatiedienstverlener bekendgemaakte procedure voor de intrekking van een gekwalificeerd certificaat;
l. hij publiceert, gedurende de geldigheid van het afgegeven gekwalificeerde certificaat, en tot ten minste zes maanden na het tijdstip waarop de geldigheid van het gekwalificeerde certificaat is verlopen of, indien dat tijdstip eerder valt, na het tijdstip waarop de geldigheid is beëindigd door intrekking, langs elektronische weg en zodanig dat die publicatie door alle gebruikers van de desbetreffende certificatiedienst alsmede door alle partijen die vertrouwen op de uitgegeven gekwalificeerde certificaten geraadpleegd kan worden:
1°. actuele en betrouwbare informatie over de statu s van de afgegeven gekwalificeerde certificaten, en
2°. afgegeven gekwalificeerde certificaten voor zov er de ondertekenaar daarvoor toestemming heeft gegeven;
m. hij slaat de gegevens voor het aanmaken van elektronische handtekeningen van de personen aan wie hij sleutelbeheerdiensten heeft verleend niet op, en hij kopieert deze gegevens evenmin;
n. hij beschikt over beschreven klachtenafhandeling- en geschillenbeslechtingprocedures, en hanteert deze;
o. hij treft maatregelen om bij beëindiging van de dienstverlening de gegevens voor het aanmaken van de elektronische handtekening, waarmee de desbetreffende certificatiedienstverlener de uitgegeven gekwalificeerde certificaten tekent, te vernietigen op het vroegst mogelijke moment dat de publicatieverplichting, bedoeld in onderdeel l, dit mogelijk maakt;
p. hij treft zodanige voorzieningen dat bij beëindiging van de dienstverlening:
1°. de door hem afgegeven gekwalificeerde certifica ten door een andere geregistreerde certificatiedienstverlener worden overgenomen en dat te dien aanzien voldaan wordt aan dit artikel, tenzij dit redelijkerwijze niet mogelijk is, alsmede de ondertekenaars daarvan in kennis worden gesteld;
2°. indien overneming als bedoeld in onderdeel 1° r edelijkerwijze niet mogelijk is, de gekwalificeerde certificaten uiterlijk op het tijdstip waarop de dienstverlening wordt beëindigd worden ingetrokken, de ondertekenaars daarvan in kennis worden gesteld en voor het overige ten aanzien van de ingetrokken gekwalificeerde certificaten door een geregistreerde certificatiedienstverlener voldaan wordt aan de onderdelen i, j en q;
q. hij treft, ongeacht de reden en omstandigheden van beëindiging van de dienstverlening en voor zover de gekwalificeerde certificaten niet worden overgenomen door een andere certificatiedienstverlener, in ieder geval voorzieningen voor de voortzetting van de publicatie overeenkomstig onderdeel l, zulks op de tot dan gebruikelijke wijze en tot ten minste zes maanden na het tijdstip waarop de dienstverlening is beëindigd;
r. hij stelt schriftelijk, met behulp van een duurzaam communicatiemiddel en uit eigen beweging de persoon die een gekwalificeerd certificaat ter ondersteuning van zijn elektronische handtekening wenst en met wie hij een overeenkomst wil aangaan, en desgevraagd de derden, die op het

gekwalificeerde certificaat vertrouwen, ten minste op de hoogte van:
1°. de exacte voorwaarden voor het gebruik van het gekwalificeerde certificaat met inbegrip van eventuele beperkingen inzake dit gebruik, alsmede van de wijzigingen van de voorwaarden;
2°. het bestaan van een vrijwillige accreditatie;
3°. de procedure voor intrekking van het gekwalific eerde certificaat zowel op verzoek van de gebruiker als door hem zelf, en
4°. de procedures voor klachtenbehandeling en gesch illenbeslechting, en
(…)"

38. Artikel 2 van de Regeling elektronische handtekeningen luidt, voor zover relevant:

"1.Een certificatiedienstverlener wordt vermoed te voldoen aan de eisen, gesteld in artikel 2, eerste lid, onderdelen a tot en met m, o en r van het besluit, indien hij voldoet aan de technische specificatie ETSI TS 101 456.
2.De tijdsduur tussen het ontvangen van een verzoek tot intrekking van een gekwalificeerd certificaat en publicatie van die intrekking, als bedoeld in artikel 2, eerste lid, onderdeel k, van het besluit, bedraagt ten hoogste 24 uur.
3.Een certificatiedienstverlener zorgt ervoor dat belanghebbenden gedurende de periode dat de verplichting, bedoeld in artikel 2, eerste lid, onderdeel l, van het besluit, om statusgegevens te publiceren aanwezig is, deze gegevens van afgegeven gekwalificeerde certificaten op elk tijdstip kunnen raadplegen."

6. Overwegingen van het college

6.1 Overtreding

39. Volgens artikel 18.15, eerste lid van de Tw moet een certificatiedienstverlener, die certificaten als gekwalificeerde certificaten aanbiedt aan het publiek en in Nederland een vestiging heeft, voldoen aan de eisen gesteld bij of krachtens algemene maatregel van bestuur. De eisen waar in artikel 18.15, eerste lid aan wordt gerefereerd, staan in artikel 2 van het Besluit elektronische handtekeningen.

6.1.1 Artikel 2, eerste lid, sub d, van het Besluit elektronische handtekeningen

40. Op grond van artikel 2, eerste lid, sub d, van het Besluit elektronische handtekeningen neemt een certificatiedienstverlener die gekwalificeerde certificaten aanbiedt aan het publiek adequate maatregelen tegen het vervalsen van de gekwalificeerde certificaten die hij heeft uitgegeven en tegen het uitgeven van illegale gekwalificeerde certificaten en, indien hij gegevens voor het aanmaken van handtekeningen genereert, garandeert hij de vertrouwelijkheid van het proces waarmee dit gebeurt.

41. Het college stelt op grond van het Fox-IT rapport vast dat er sporen van hacker activiteiten met gebruikmaking van de administrator rechten zijn aangetroffen op de CA-server die werd gebruikt voor de uitgifte van gekwalificeerde certificaten. Omdat een hacker met de hoogst

mogelijke toegangsrechten toegang heeft verkregen tot de CA-server die werd gebruikt voor de uitgifte van gekwalificeerde certificaten, kan het college niet anders dan vaststellen dat de vertrouwelijkheid van het uitgifteproces van deze certificaten niet meer door Diginotar kan worden gegarandeerd.

42. Door alle CA-servers op te nemen in één windows-domein waarvan het voor een onbevoegde derde ("hacker") mogelijk was om de administratieve rechten te bemachtigen, heeft Diginotar nagelaten om adequate maatregelen te nemen tegen het vervalsen van de reeds uitgegeven gekwalificeerde certificaten en de uitgifte van illegale gekwalificeerde certificaten.

43. Op grond van het bovenstaande concludeert het college dat Diginotar niet aan artikel 2, eerste lid, sub d, van het Besluit elektronische handtekeningen voldoet en dat Diginotar in strijd met artikel 18.15, eerste lid, van de Tw handelt.

6.1.2 Artikel 2, eerste lid, sub c, van het Besluit elektronische handtekeningen

44. Naast hetgeen in de vorige paragraaf is beschreven ten aanzien van het handelen in strijd met artikel 2, eerste lid, sub d, van het Besluit elektronische handtekeningen – wat een zelfstandige grond voor de beëindiging van de registratie vormt – is het college van oordeel dat Diginotar tevens artikel 2, eerste lid, sub c, van het Besluit elektronische handtekeningen heeft overtreden.

45. Op grond van artikel 2, eerste lid, sub c, van het Besluit elektronische handtekeningen maakt een certificatiedienstverlener die gekwalificeerde certificaten aanbiedt uitsluitend gebruik van betrouwbare systemen en producten die procedureel of overeenkomstig de stand der techniek beveiligd zijn en die de technische en cryptografische veiligheid van de processen die zij ondersteunen garanderen.

46. Het college is van oordeel dat de beveiliging van de systemen en producten die door Diginotar werden gebruikt bij de uitgifte van gekwalificeerde certificaten niet overeenkomstig de stand der techniek beveiligd zijn. In het Fox-IT rapport wordt immers vastgesteld dat de CA servers, hoewel fysiek gescheiden, wel onderdeel uitmaken van één netwerk. De domeinserver is beveiligd met een zwak wachtwoord. De software op de webserver is gedateerd en er is geen antivirus software op de CA-servers geïnstalleerd. Ook is er geen centraal systeem aanwezig dat de netwerkactiviteit registreert en opslaat.

47. Op grond van bovenstaande oordeelt het college dat Diginotar niet voldoet aan artikel 2, eerste lid, sub c, van het Besluit elektronische handtekeningen en Diginotar ook daarmee artikel 18.15, eerste lid, van de Tw. overtreedt.

6.1.3 Conformiteit met ETSI en certificering door auditor

48. Uit artikel 2, eerste lid van de Regeling elektronische handtekeningen volgt dat wanneer een

certificatiedienstverlener voldoet aan de vereisten van ETSI-norm 101 456, dat wordt vermoed dat ook wordt voldaan aan de vereisten uit artikel 2, eerste lid, onderdelen a tot en met m, o en r van het Besluit elektronische handtekeningen.

49. Het college is van oordeel dat ondanks dat Diginotar regelmatig werd gecontroleerd op conformiteit aan de ETSI-normen, niet kan worden gesteld dat de systemen en procedures van Diginotar in de praktijk geheel voldeden aan de ETSI-norm.

50. Het college stelt vast dat enkele van de door Fox-IT geconstateerde feiten aantonen dat bepaalde procedures en systemen in de praktijk niet werden toegepast, ondanks dat deze mogelijk wel aanwezig waren. Ten aanzien van de volgende ETSI-normen stelt het college vast dat Diginotar daaraan in de praktijk niet heeft voldaan.

51. Artikel 7.4.5.a van ETSI-norm 101 456 (2006) stelt als vereiste dat de integriteit van CA systemen en informatie zal worden beschermd tegen virussen en ongeautoriseerde software. Uit het rapport van Fox-IT blijkt dat er geen antivirus software is aangetroffen op de verschillende CA-servers en dat de netwerkstructuur en /of de beveiligprocedures van Diginotar niet afdoende waren om een inbraak te voorkomen.

52. Artikel 7.4.5.j van ETSI-norm 101 456 (2006) stelt als vereiste dat audit logs regelmatig moeten worden onderzocht om bewijs van onrechtmatige activiteit te identificeren. Uit het rapport van Fox-IT blijkt dat er geen netwerklogging werd gebruikt door Diginotar en dat er verschillende sporen van onrechtmatige toegang te vinden waren op de systemen van Diginotar.

53. Artikel 7.4.6.b van ETSI-norm 101 456 (2006) stelt als vereiste dat gevoelige data moet worden beschermd tegen ongeautoriseerde toegang of bewerking. Uit het rapport van Fox-IT blijkt onbevoegde derden toegang hebben gehad tot de CA-server waarop gekwalificeerde certificaten werden uitgegeven. Uit aanvullende informatie van Fox-IT blijkt eveneens dat het zeer waarschijnlijk is dat onbevoegde derden (“hackers”) gegevens hebben onttrokken van de CA-server die werd gebruikt voor de uitgifte van gekwalificeerde certificaten.

54. Artikel 7.4.6.d van ETSI-norm 101 456 (2006) stelt als vereiste dat de toegang tot informatie en applicatie systeemfuncties afgeschermd moeten zijn in overeenstemming met het toegangsbeleid. De systemen bieden voldoende computer beveiliging controles voor de scheiding van de vertrouwde rollen binnen de organisatie, waaronder scheiding van de beveiligingsbeheerder en de operationele functies. Vooral het gebruik van systeem programma’s zal worden beperkt en strikt worden gecontroleerd. Toegang zal worden beperkt, waarbij alleen diegene toegang hebben tot gegevens die deze gegevens nodig hebben voor de uitvoer van de rol die hun binnen de organisatie is toegewezen. Uit het Fox-IT rapport blijkt dat alle CA-severs onderdeel uitmaakten van één Windows domeinserver. Met de administratieve rechten van de domeinserver was het mogelijk om administratieve taken op

alle CA-servers uit te voeren.

55. Artikel 7.4.6.k van ETSI-norm 101 456 (2006) stelt als vereiste dat er continue monitorings- en alarminrichtingen aanwezig zijn die het mogelijk maken om ongeautoriseerde en/of onregelmatige pogingen om toegang te verkrijgen tot gegevens te detecteren, te registreren en daar tijdig op te reageren. Uit het Fox-IT rapport volgt dat bij Diginotar geen centrale netwerklogging aanwezig was, waardoor ongeautoriseerde toegang tot de gegevens niet tijdig is gedetecteerd.

56. Artikel 7.4.8.e van ETSI-norm 101 456 (2006) stelt als vereiste dat in geval van een compromittering de certificatie autoriteit (hier: Diginotar) een aantal acties moet ondernemen. Eén van deze acties is dat de certificatie autoriteit moet aangeven dat zijn certificaten en de intrekkingsstatusinformatie mogelijk niet meer geldig is. Tot op heden heeft Diginotar dit nagelaten.

6.2 Overwegingen van het college ten aanzien van de zienswijze van Diginotar.

57. Het college heeft Diginotar verzocht om aan te geven op welke punten het rapport van Fox-IT door Diginotar in twijfel wordt getrokken. De gemachtigde van Diginotar heeft op dit verzoek van het college gereageerd. [13] De reactie van Diginotar op het rapport van Fox-IT heeft slechts betrekking op de (onterechte) uitgifte van SSL-certifcaten en de maatregelen die Diginotar ten aanzien daarvan heeft genomen. Uit de reactie van Diginotar blijkt niet dat ter discussie staat dat een onbevoegde derde (“hacker”) administratieve rechten van de domeinserver heeft verkregen en daarmee toegang heeft gehad tot de CA-server die werd gebruikt voor de uitgifte van gekwalificeerde certificaten. Ook andere conclusies uit het rapport van Fox-IT worden niet betwist, laat staan dat dit met feiten wordt onderbouwd.

58. Ten aanzien van de stelling van Diginotar dat er geen aanwijzingen zijn dat er op de server die werd gebruikt om voor de uitgifte van gekwalificeerde certificaten regels zijn verwijderd, merkt het college het volgende op. Naar het oordeel van het college is niet relevant dat (nog) niet is aangetoond dat er gegevens van de CA-server die werd gebruikt voor de uitgifte van gekwalificeerde certificaten zijn verwijderd. Het feit dat onbevoegde derden (“hackers”) met de administratieve rechten van de Windows-domeinserver ook de toegang hebben verkregen tot de CA-server die werd gebruikt voor de uitgifte van gekwalificeerde certificaten is voldoende om vast te stellen dat Diginotar activiteiten heeft uitgevoerd in strijd met artikel 2, eerste lid sub c en d van het Besluit elektronische handtekeningen en daarmee tevens in strijd heeft gehandeld met artikel 18.15, eerste lid van de Tw.[14] Er bestaat immers de mogelijkheid dat gegevens zijn gemanipuleerd of verwijderd door onbevoegde derde(n).

[13] Zie randnummer 13.
[14] Ook Diginotar stelt in haar zienswijze overigens dat alle CA-servers onderdeel uitmaakte van één Windows-domein. Diginotar heeft niet betwist dat een onbevoegde derde toegang heeft verkregen tot de administratieve rechten van de Windows-domeinserver.

59. Ten aanzien van het gedeelte van de zienswijze van Diginotar waarin wordt gesteld dat haar systemen onderdeel uitmaken van een ETSI gecertificeerd kwaliteitssysteem en dat op dit moment geen bewijs aanwezig is waaruit volgt dat Diginotar niet voldeed aan de certificatievereisten, verwijst het colllege naar hetgeen daarover hiervoor in paragraaf 6.1.3. is opgemerkt.

60. Diginotar merkt op dat zij tussen 19 en 29 juli 2011 voor het eerst ontdekte dat vanuit haar CA's onterecht valse (SSL) certificaten werden uitgegeven. Op dat moment is door Diginotar de assistentie van een externe adviseur ingeroepen. De hoofdconclusie van deze externe adviseur was op 27 juli 2011:

    A number of servers were compromised. The hackers have obtained administrative rights to the outside webservers, the CA server "Relaties-CA" and also to "Public-CA". Traces of hacker activity started on June 17th and ended on July 22nd.

    Weliswaar volgt uit de bovenstaande conclusie niet dat er op de servers van Diginotar die werden gebruikt voor de uitgifte van gekwalificeerde certificaten sporen van hackeractiviteit zijn aangetroffen, wel was op dat moment voor Diginotar duidelijk dat een onbevoegde derde ("hacker") toegang had verkregen tot verschillende CA-servers. Aangezien de verschillende CA-servers - waaronder de CA-server die werd gebruikt voor de uitgifte van gekwalificeerde certificaten - via een Windows-domeinserver met elkaar in verbinding stonden, was op dat moment niet uit te sluiten dat een onbevoegde derde ("hacker") toegang had verkregen tot de CA-server die werd gebruikt voor de uitgifte van gekwalificeerde certificaten. In ieder geval had het op de weg van Diginotar gelegen daar direct aanvullend onderzoek naar te laten doen en maatregelen te treffen om de betrouwbaarheid van haar processen en systemen te waarborgen.

61. Wat betreft hetgeen Diginotar in haar zienswijze naar voren heeft gebracht over de gevolgen van het beëindigen van de registratie van Diginotar, merkt het college het volgende op. Diginotar heeft aangevoerd dat het beëindigen van de registratie zeer waarschijnlijk het faillissement van Diginotar tot gevolg zal hebben. Het college constateert dat in dit verband de beëindiging van de registratie in juridische zin alleen gevolgen zal hebben voor een gedeelte van de dienstverlening van Diginotar, namelijk de mogelijkheid om gekwalificeerde certificaten aan te bieden. Het beëindigen van de registratie van Diginotar sluit niet uit dat Diginotar op een later moment, wanneer zij kan aantonen dat wordt voldaan aan de gestelde eisen uit de Tw en het Besluit elektronische handtekeningen, opnieuw door het college kan worden geregistreerd.

62. Het college stelt vast dat door de beëindiging van de registratie van Diginotar circa 4200 gebruikers van de gekwalificeerde certificaten van Diginotar, geen gebruik meer kunnen maken van deze certificaten. Omdat PKIoverheid in deel 2 van zijn programma van eisen heeft opgenomen dat een certificatiedienstverlener onder PKIoverheid geregistreerd dient te zijn bij het college, kan de beëindiging van de registratie van Diginotar door het college ook van

invloed zijn op andere dan gekwalificeerde certificaten.[15] Voor het college staat zijn toezicht op de certificatiedienstverlener en de uitgegeven certificaten voorop. In geval van twijfel over de betrouwbaarheid en integriteit van de systemen van Diginotar en daarmee de uitgegeven certificaten, is interventie door het college noodzakelijk. Een eventueel faillissement van Diginotar, al dan niet veroorzaakt door het beëindigen van de registratie, is geen relevant feit in de beoordeling of de gekwalificeerde certificaten van Diginotar nog te vertrouwen zijn. Zoals eerder aangegeven, kan de integriteit van deze certificaten niet meer worden gegarandeerd. Dit is de relevante afweging voor het al dan niet beëindigen van de registratie.

6.3 Bevoegdheid college

63. Op grond van artikel 2.2, vierde lid sub b van de Tw is het college bevoegd om de registratie van een certificatiedienstverlener (direct) te beëindigen indien deze activiteiten of diensten verricht in strijd met het bepaalde bij of krachtens de Tw.

6.4 Beëindiging registratie

64. Beëindiging van de registratie is een ultimum remedium dat het college kan inzetten wanneer wordt geconstateerd dat de certificatiedienstverlener niet of niet geheel voldoet aan de vereisten uit het Besluit elektronische handtekeningen of diensten of activiteiten verricht in strijd met het Besluit elektronische handtekeningen.

65. Artikel 2.2, vierde lid, sub c geeft het college de mogelijkheid om wanneer een certificatiedienstverlener niet volledig aan de vereisten voldoet, hem een termijn te stellen waarbinnen de certificatiedienstverlener kan aantonen dat hij wel aan de vereisten uit het Besluit elektronische handtekeningen voldoet. Volgens de memorie van toelichting op dit artikel wordt het stellen van een termijn "*noodzakelijk geacht in verband met de mogelijke niet-naleving van bepaalde vereisten die de betrouwbaarheid van een gekwalificeerd certificaat niet direct in twijfel trekken. Het (tijdelijk of incidenteel) niet naleven van een dergelijke vereiste betekent niet zonder meer dat een certificaat tussen de partijen die het gebruiken onbetrouwbaar is geworden (…).*"[16]

66. In het onderhavige geval is er sprake van een ernstige inbraak in en compromittering van de systemen die door Diginotar werden gebruikt voor de aanmaak van gekwalificeerde certificaten. Door deze inbraak is de betrouwbaarheid van de door Diginotar uitgegeven gekwalificeerde certificaten in twijfel te trekken. Omdat de betrouwbaarheid van de door Diginotar uitgegeven gekwalificeerde certificaten niet meer te garanderen is, is het stellen van een termijn waarbinnen Diginotar kan aantonen aan de gestelde eisen te voldoen zinloos. Het college besluit dan ook de registratie van Diginotar als certificatiedienstverlener te beëindigen. Dit heeft feitelijk tot gevolg dat het Diginotar verboden is nog langer gekwalificeerde certificaten aan het publiek aan te bieden zolang zij niet opnieuw geregistreerd is.

15 Programma van Eisen deel 2: Toetreding tot en toezicht binnen de PKI voor de overheid, paragraaf 2.2.1 onder 3, te vinden op: http://www.logius.nl/fileadmin/logius/product/pkioverheid/documenten/pve/PvE_deel2_v3.1.pdf
16 Tweede Kamer, vergaderjaar 2000–2001, 27 743, nr. 3.

Besluit
Openbaar

7. Dictum

67. Omdat Diginotar activiteiten of diensten heeft verricht in strijd met artikel 2, eerste lid, sub c en d, van het Besluit elektronische handtekeningen en daarmee artikel 18.15 van de Tw heeft overtreden, beëindigt het college op grond van artikel 2.2, vierde lid, sub b, van de Tw, de registratie van Diginotar als certificatiedienstverlener per 14 september om 12.00 uur.

HET COLLEGE VAN DE ONAFHANKELIJKE POST EN TELECOMMUNICATIE AUTORITEIT,
namens het college,

prof.dr. M.W. de Jong
Plv. voorzitter

Bezwaar

Belanghebbenden die zich met dit besluit niet kunnen verenigen, kunnen binnen zes weken na de dag waarop dit besluit is bekendgemaakt bezwaar maken bij het College van de OPTA.
Het postadres is: College van de OPTA, Postbus 90420, 2509 LK Den Haag.
Het bezwaarschrift moet zijn ondertekend en moet ten minste de naam en het adres van de indiener, de dagtekening en een omschrijving van het besluit waartegen het bezwaar is gericht bevatten. Voorts moet het bezwaarschrift de gronden van het bezwaar bevatten.

Het college wijst u op de mogelijkheid die de Algemene wet bestuursrecht de indiener van een bezwaarschrift biedt, om in dat geschrift het college te verzoeken de bezwaarschriftenfase over te slaan. Indien het college uw verzoek inwilligt, zal uw bezwaarschrift worden doorgezonden naar de rechtbank en daar als beroepschrift worden behandeld. De procedure kan daardoor worden verkort. Indien het college uw verzoek niet inwilligt, staat tegen deze beslissing geen beroep open en zal uw bezwaarschrift door het college worden behandeld.