Besluit van …….tot wijziging van het Besluit elektronische handtekeningen in verband met een meldingsplicht voor veiligheidsinbreuken en integriteitsverlies betreffende gekwalificeerde certificaten

Consultatieversie 20-02-2013

Wij Beatrix, bij de gratie Gods, Koningin der Nederlanden, Prinses van Oranje-Nassau, enz. enz. enz.

Op de voordracht van Onze Minister van Economische Zaken van ……, nr. WJZ…….;

Gelet op artikel 18.15, eerste lid, van de Telecommunicatiewet;

De Afdeling advisering van de Raad van State gehoord (advies van ……nr. W…….);

Gezien het nader rapport van Onze Minister van Economische Zaken van ……., nr. WJZ……;

Hebben goedgevonden en verstaan:

Artikel I

Artikel 2, eerste lid, van het Besluit elektronische handtekeningen wordt gewijzigd als volgt:

A

In onderdeel r wordt onder 4° ",en" vervangen door een puntkomma.

B

Onder vervanging van de punt aan het slot van onderdeel s door ", en" wordt een onderdeel toegevoegd, luidende:

t. hij zorgt onverwijld na iedere veiligheidsinbreuk die of ieder integriteitsverlies dat aanzienlijke gevolgen heeft of kan hebben voor de betrouwbaarheid of het vertrouwen van door hem aangeboden of afgegeven gekwalificeerde certificaten voor een melding van die inbreuk of dat verlies aan het college, bedoeld in artikel 2, eerste lid, van de Wet Onafhankelijke post- en telecommunicatie autoriteit, en aan Onze Minister van Veiligheid en Justitie, met een kennisgeving aan beiden van:

1°. de aard en omvang van de inbreuk of het verlies;

2°. het tijdstip van de aanvang van de inbreuk of het verlies;

3°. de mogelijke gevolgen van de inbreuk of het verlies;

4°. een prognose van de tijd nodig om de inbreuk te onderzoeken;

5°. zo mogelijk de door de certificatiedienstverlener genomen of te nemen maatregelen om de gevolgen van de inbreuk of het verlies te beperken of herhaling hiervan te voorkomen;

6°. de contactgegevens van de in Nederland gevestigde functionaris die verantwoordelijk is voor het doen van de kennisgeving.

Artikel II

Dit besluit treedt in werking met ingang van de dag na de datum van uitgifte van het Staatsblad waarin het wordt geplaatst.

Lasten en bevelen dat dit besluit met de daarbij behorende nota van toelichting in het Staatsblad zal worden geplaatst.

De Minister van Economische Zaken,

NOTA VAN TOELICHTING
(concept-datum)

I. ALGEMEEN

Aanleiding
De in het najaar van 2011 vastgestelde digitale inbreuk op de veiligheid van certificaten die door het bedrijf DigiNotar werden uitgegeven, leverde grote risico's op voor de continuïteit van de overheidsdienstverlening langs elektronische weg. Als gevolg van onder meer dit incident hebben diverse onderzoeken op het gebied van digitale veiligheid plaatsgevonden. Op basis van de uitkomsten van die onderzoeken zijn maatregelen aangekondigd en deels inmiddels uitgevoerd, die de digitale veiligheid dienen te verbeteren. Specifiek ten aanzien van digitale certificaten is één van de conclusies dat een meldplicht van incidenten de toezichthouder helpt bij het uitoefenen van zijn taak omdat de impact van een incident sneller wordt onderkend en

er vervolgens effectiever kan worden opgetreden (Kamerstukken II 2011/12, 26 643, nr. 230, blz. 3). Bij brief van 6 juli 2012 heeft het kabinet bevestigd aan een wettelijke meldplicht voor veiligheidsincidenten te werken (Kamerstukken II 2012/2013, 26 643, nr. 246).

Inhoud en betekenis

Dit besluit bevat een meldplicht voor certificatiedienstverleners ten aanzien van gekwalificeerde certificaten. Dit zijn certificaten waarvoor certificatiedienstverleners een registratieplicht hebben en waarop het toezicht in de Telecommunicatiewet betrekking heeft. Het betreft certificaten die geschikt zijn voor elektronische handtekeningen en waarbij die certificaten en de certificatiedienstverleners aan bij en krachtens de wet gestelde eisen moeten voldoen. Het besluit legt aan een certificatiedienstverlener de verplichting op een inbreuk op de veiligheid die of een verlies van integriteit dat aanzienlijke gevolgen voor de betrouwbaarheid of vertrouwelijkheid van door hem beheerde gekwalificeerde certificaten heeft of kan hebben onverwijld te melden aan de Onafhankelijke Post en Telecommunicatie Autoriteit (OPTA) en aan de Minister van Veiligheid en Justitie die voor het Nationale Cyber Security Centrum (NCSC) verantwoordelijk is. Tot de incidenten, die aanzienlijke gevolgen kunnen hebben dient bijvoorbeeld elke inbraak (fysiek in het bedrijfspand of online) gerekend te worden. Ook de ontdekking van virussen, malware of andere ongeautoriseerde software die op een van de systemen van de certificatiedienstverlener aanwezig is, valt hier bijvoorbeeld onder. Uiteraard moet het hier wel gaan om de ontdekking van virussen, malware enz. die aanzienlijke gevolgen kunnen hebben. Maar ook andere onvolkomenheden in de toegangsbeveiliging of bijvoorbeeld gedragingen van het personeel die de beroepsintegriteit of het begaan van een misdrijf betreffen, vallen onder de meldplicht. Ook indien er twijfel is over de vraag hoe groot de gevolgen daadwerkelijk zouden kunnen zijn, dient gemeld te worden.

Het besluit leidt op een specifiek punt tot een verbetering die relevant is voor het toezicht op gekwalificeerde certificaten en voor hulp ingeval van incidenten. Een onverwijlde melding van een incident aan toezichthouder OPTA, stelt hem in staat tijdig vast te stellen welke vervolgacties nodig zijn. OPTA kan bijvoorbeeld nadere informatie opvragen over een incident om te toetsen of door een certificatiedienstverlener aan de eisen die bij of krachtens de wet zijn gesteld, is voldaan en kan in voorkomend geval een last onder bestuursdwang of een bestuurlijke boete opleggen om noodzakelijke vervolgacties tijdig af te dwingen (artikelen 18.7, 15.2 en 15.4, van de Telecommunicatiewet). En indien aan de daarvoor geldende eisen is voldaan, kan de registratie van een certificatiedienstverlener worden gewijzigd of beëindigd (artikel 2.2, vierde lid, van de Telecommunicatiewet). Een onverwijlde melding aan de Minister van Veiligheid en Justitie en daarmee aan het NCSC kan tot technische en functionele hulp en ondersteuning aan de certificatiedienstverlener

leiden om de gevolgen van een incident te beperken en op te lossen. Onverwijld betekent hier zo snel mogelijk, maar zeker niet later dan 24 uur na ontdekking.

Toepassingsgebied

Het besluit bevat geen plicht tot melding van veiligheidsinbreuken of van integriteitsverlies van andersoortige certificaten dan gekwalificeerde certificaten. Een uitbreiding tot andere certificaten zou een wijziging van de Telecommunicatiewet vereisen. De Telecommunicatiewet is op andere soorten certificaten niet van toepassing. Overigens is niet ondenkbaar dat bijvoorbeeld een succesvolle aanval op informatiesystemen die een certificatiedienstverlener gebruikt voor andersoortige certificaten tot twijfel leidt over de informatiebeveiliging van de systemen waarmee gekwalificeerde certificaten worden uitgegeven. De inbreuk leidt dan tot onzekerheid of de integriteit van de gekwalificeerde certificaten hierdoor is of zal worden aangetast. Een meldplicht op grond van dit besluit kan dan eveneens aan de orde zijn. Eenzelfde situatie kan zich bijvoorbeeld voordoen in het geval een medewerker die verantwoordelijk is voor de verwerking van vertrouwelijke of gevoelige gegevens binnen de certificatiedienstverlener betrokken blijkt te zijn bij frauduleuze activiteiten. Een verdere uitbreiding van een meldplicht is afhankelijk van de uiteindelijke inhoud van en het moment waarop het voorstel voor een verordening van het Europees Parlement en de Raad van de Europese Unie betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt (voorstel van 4 juni 2012, COM(2012) 238 final; hierna: de voorgestelde verordening of de verordening) wordt vastgesteld. Die verordening heeft betrekking op elektronische identiteiten en elektronische vertrouwensdiensten, waaronder diensten ten aanzien van certificaten. De verordening bevat een groot aantal voorschriften over het aanbieden van elektronische vertrouwensdiensten, waaronder ook een plicht tot melding van veiligheidsinbreuken daarop (artikel 15, tweede lid, van het voorstel). Naar verwachting zal de voorgestelde verordening over anderhalf tot drie jaar zijn aangenomen en in werking zijn getreden. De daarin opgenomen verplichtingen zullen dan rechtstreeks doorwerken in de nationale rechtsorde. Daarom is er nu voor gekozen om een uitdrukkelijke meldingsplicht door middel van dit besluit vast te stellen die bij het huidig wettelijk kader past. Dit besluit geeft daar uitvoering aan door een meldplicht vast te stellen ten aanzien van gekwalificeerde certificaten.

Betrokken organen

Het besluit bepaalt dat een melding dient plaats te vinden aan OPTA en aan de Minister van Veiligheid en Justitie die verantwoordelijk is voor het NCSC. Ten aanzien van meldingen aan het NCSC heeft de Minister van Veiligheid en Justitie een wetsvoorstel aangekondigd dat strekt tot invoering van een verplichting tot het melden van ernstige cyberincidenten in de vitale infrastructuur aan het NCSC (Kamerstukken II 2011/12, 26 643, nr. 247).

Dit besluit bevat een afzonderlijke plicht tot melding aan het NCSC. Het is niet wenselijk met een dergelijke verplichting te wachten totdat dit aangekondigde wetsvoorstel kracht van wet heeft en in werking is getreden. Zodra de voorgestelde verordening definitief is vastgesteld en in werking is getreden geldt door de rechtstreekse werking daarvan naar verwachting een meldplicht aan meerdere instanties, waaronder aan het bevoegde nationale orgaan van informatie en veiligheid. Bij de voorbereiding van het wetgevingstraject dat noodzakelijk is om de verenigbaarheid van Nederlandse wet- en regelgeving met de eenmaal vastgestelde verordening te waarborgen, zal nagegaan worden of de meldplicht in de verordening tot aanpassing van wet- en regelgeving dient te leiden. Het door de Minister van Veiligheid en Justitie aangekondigde wetsvoorstel, of indien dit tot wet is verheven die wet, zal samen met het Besluit elektronische handtekeningen bij die beoordeling betrokken worden.

Uitvoerings- en handhavingstoets
PM

Administratieve Lasten
De administratieve lasten zullen licht toenemen voor certificatiedienstverleners die gekwalificeerde certificaten aanbieden. Op jaarbasis worden maximaal twee meldingen per bedrijf verwacht bij maximaal tien bedrijven. De melding op zich (inclusief de updates) zal maximaal twee uur in beslag nemen. Intern zal er onderzoek en overleg nodig zijn om het management te informeren, maar dat hoort tot de normale bedrijfsvoering. En de kosten daarvan vallen daarom buiten de definitie van het begrip administratieve lasten. Bij een uurtarief van 50 Euro komen de administratieve lasten uit op 200 Euro per bedrijf en maximaal 2.000 Euro op jaarbasis.
De bestuurlijke lasten van de afhandeling van de melding zullen ook licht toenemen en in dezelfde orde van grootte liggen. Bij omvangrijke incidenten vallen de administratieve lasten hoger uit en zullen extra inspanningen van de toezichthouder nodig zijn.

II. ARTIKELEN

Artikel I

Artikel 2 van het Besluit elektronische handtekeningen stelt eisen waaraan een certificatiedienstverlener die certificaten als gekwalificeerde certificaten aanbiedt of afgeeft aan het publiek en in Nederland een vestiging heeft, dient te voldoen. Aan deze eisen wordt toegevoegd dat de certificatiedienstverlener inbreuken op de veiligheid of verlies van integriteit van door hem beheerde gekwalificeerde certificaten dient te melden bij OPTA. De verplichting heeft betrekking op gekwalificeerde certificaten en niet op andersoortige certificaten, zoals bijvoorbeeld certificaten die

gebruikt worden voor website-authenticatie (bijvoorbeeld SSL-certificaten herkenbaar aan het gele 'slotje' bovenaan een website).

De meldingsplicht geldt voor een inbreuk die of verlies dat aanzienlijke gevolgen heeft of kan hebben voor de betrouwbaarheid van door de certificatiedienstverlener aangeboden en afgegeven gekwalificeerde certificaten. Deze bewoordingen sluiten niet geheel aan bij de letterlijke bewoordingen van de voorgestelde EU-verordening. De verordening bepaalt dat sprake dient te zijn van aanzienlijke gevolgen. Dit wordt hier aldus uitgelegd dat dit ook omvat een inbreuk of integriteitsverlies met *het risico* op aanzienlijke gevolgen voor de betrouwbaarheid van de afgegeven en aangeboden certificaten. Gelet hierop geldt ook een meldplicht als door een inbreuk of integriteitsverlies aanzienlijke gevolgen voor de betrouwbaarheid van de afgegeven en aangeboden certificaten kunnen optreden maar die gevolgen nog niet zijn ingetreden. De meldplicht is niet van toepassing, indien vaststaat dat een inbreuk overduidelijk een beperkt aantal certificaten aantast zonder enig risico van uitbreiding daarvan. De certificatiedienstverlener zal in dat geval in staat zijn de inbreuk snel en adequaat te herstellen. Naarmate meer onzekerheid bestaat omtrent de aard en omvang van gevolgen van een incident voor de betrouwbaarheid of indien direct duidelijk is dat de gevolgen van een veiligheidsinbreuk of integriteitsverlies certificaten op grotere schaal treffen of zullen treffen, is de meldingsplicht wel van toepassing . Hiervoor zal op basis van ervaringen een praktijk ontwikkeld moeten worden. Voor de praktijk dient daarbij zoveel mogelijk het uitgangspunt van een ruimhartige melding te gelden. In geval van twijfel over de vraag hoe groot de gevolgen daadwerkelijk zouden kunnen zijn, moet tot melding worden overgegaan.

Een verplichte melding dient altijd onverwijld plaats te vinden. De voorgestelde verordening is hierin specifieker en bepaalt dat de melding zonder onnodige vertragingen en waar mogelijk binnen 24 uur nadat de dienstverlener hiervan op de hoogte is, dient te worden gedaan. Aangezien de verordening nog niet is vastgesteld, is er voor gekozen in het besluit niet te specifiek hierin te zijn. Niettemin kan het afhankelijk van de omstandigheden van het geval nodig zijn al na het verstrijken van enkele uren na een incident tot melding over te gaan. Een melding die snel wordt gedaan, biedt de toezichthouder de mogelijkheid vlot te reageren. Dit kan bijdragen aan het beperken van een aantasting van het vertrouwen in certificaten en de maatschappelijke schade die het gevolg van een incident kan veroorzaken.

Bij een melding is een kennisgeving van specifieke informatie vereist die inzicht biedt in de aard, omvang, start en te verwachten duur van het incident alsmede van de getroffen of te nemen maatregelen om de gevolgen van de inbreuk of het verlies te beperken en contactgegevens. Tot de te treffen maatregelen wordt onder meer het informeren van afnemers van de certificaten over het incident gerekend Die informatie is voor OPTA relevant in het kader van het toezicht en voor NCSC voor het kunnen

verlenen van bijstand. Het is mogelijk dat niet alle gevraagde informatie beschikbaar is op het moment dat een melding wordt gedaan. Zo kan het zijn dat er eerst nader onderzoek moet worden gedaan, om bijvoorbeeld de omvang van het verlies vast te stellen. Juist om die reden is ook opgenomen dat een prognose moet worden gegeven om de inbreuk te onderzoeken, Het niet beschikbaar hebben van alle gevraagde informatie is dus geen reden om niet onverwijld te melden.

Artikel II

Ingevolge het kabinetsbeleid inzake Vaste Verandermomenten treedt inwerkingtreding van nieuwe regelgeving in beginsel in werking op 1 januari of 1 juli van enig jaar. In dit besluit wordt hiervan afgeweken. Er is een groot belang gemoeid met het verminderen van de kwetsbaarheid van de samenleving voor veiligheidsinbreuken in een digitale omgeving. Dit vereist voortvarendheid bij het treffen van maatregelen die daaraan bijdragen. Als gevolg daarvan is het gewenst dat dit besluit zo spoedig mogelijk na plaatsing in het Staatsblad in werking zal treden.

De Minister van Economische Zaken,