Staatsblad
van het Koninkrijk der Nederlanden

Jaargang 2013

362

Besluit van 17 september 2013 tot wijziging van het Besluit elektronische handtekeningen in verband met een meldingsplicht voor veiligheidsinbreuken en integriteitsverlies betreffende gekwalificeerde certificaten

Wij Willem-Alexander, bij de gratie Gods, Koning der Nederlanden, Prins van Oranje-Nassau, enz. enz. enz.

Op de voordracht van Onze Minister van Economische Zaken van 15 juli 2013, nr. WJZ / 13121672, gedaan in overeenstemming met Onze Minister van Veiligheid en Justitie;

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

De Afdeling advisering van de Raad van State gehoord (advies van 31 juli 2013, nr. W15.13.0245/IV);

Gezien het nader rapport van Onze Minister van Economische Zaken van 12 september 2013, nr. WJZ / 13152145, gedaan in overeenstemming met Onze Minister van Veiligheid en Justitie;

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 van door hem aangeboden of afgegeven gekwalificeerde certificaten voor een melding van die inbreuk of dat verlies aan de Autoriteit Consument en Markt, bedoeld in artikel 2, eerste lid, van de Instellingswet Autoriteit Consument en Markt, 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 vermoedelijke 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

Het advies van de Afdeling advisering van de Raad van State wordt niet openbaar gemaakt op grond van artikel 26, zesde lid jo vijfde lid, van de Wet op de Raad van State, omdat het zonder meer instemmend luidt.

Dit besluit treedt in werking op 1 november 2013.

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

Wassenaar, 17 september 2013

Willem-Alexander

De Minister van Economische Zaken,
H.G.J. Kamp

Uitgegeven de *zevenentwintigste* september 2013

De Minister van Veiligheid en Justitie,
I.W. Opstelten

stb-2013-362
ISSN 0920 - 2064
's-Gravenhage 2013

NOTA VAN TOELICHTING

I. Algemeen

1. Aanleiding

De in het najaar van 2011 vastgestelde digitale inbraak en de gevolgen die dit had voor de betrouwbaarheid van certificaten die door het bedrijf DigiNotar werden uitgegeven, leverden grote risico's op voor de beveiliging van elektronisch dataverkeer en daarmee voor de continuïteit van de overheidsdienstverlening langs elektronische weg. In reactie op 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 met inbegrip van de controle daarop 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).

Voor de diverse toepassingen kunnen bedrijven (en personen) gebruik maken van verschillende soorten certificaten. Certificaten kunnen voor verschillende toepassingen gebruikt worden, zoals voor authenticatie, voor het versleutelen van bestanden zodat deze vertrouwelijk zijn, en voor het plaatsen van een elektronische handtekening. De kwaliteit van certificaten is afhankelijk van twee zaken: de sterkte van de door het certificaat gebruikte cryptografische sleutels en de kwaliteit van het uitgifteproces. Uiteraard is de betrouwbaarheid van een certificaat ook sterk afhankelijk van de wijze van gebruik. Zoals het sterkste slot nutteloos is als de sleutel ernaast hangt, moet ook zorgvuldig met certificaten en de eventueel daarbij behorende middelen omgegaan worden. Wie daar onbevoegd over kan beschikken, kan zich voordoen als de rechtmatig eigenaar van het certificaat.

Er zijn allerlei soorten certificaten met verschillende functies en toepassingen. Gekwalificeerde certificaten zijn geschikt voor elektronische handtekeningen, waarbij zowel die certificaten, de certificatiedienstverleners als de wijze waarop deze certificaten worden verstrekt aan bij en krachtens de wet gestelde eisen moeten voldoen. Certificatiedienstverleners hebben op grond van de Telecommunicatiewet voor deze certificaten een registratieplicht bij de Autoriteit Consument & Markt (ACM). Ook het toezicht door ACM op de certificatiedienstverleners van gekwalificeerde certificaten is in de Telecommunicatiewet geregeld. Voor andere certificaten geldt een dergelijk wettelijk kader niet. Echter, om bijvoorbeeld certificaten geaccepteerd te laten worden in browsers (van belang voor SSL (*Secure Socket Layer*)-certificaten die voor het beveiligen van websites worden gebruikt), moeten aanbieders van die certificaten wel aan eisen vanuit de markt voldoen.

2. Inhoud en betekenis

Dit besluit bevat een meldplicht voor certificatiedienstverleners ten aanzien van gekwalificeerde certificaten. 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 van door hem beheerde gekwalificeerde certificaten heeft of kan hebben, onverwijld te melden aan ACM en aan de Minister

van Veiligheid en Justitie die voor het Nationale Cyber Security Centrum (NCSC) verantwoordelijk is. Een certificatiedienstverlener die ook andere diensten verleent, hoeft geen melding te doen van incidenten die enkel die andere dienstverlening betreffen. Echter, wanneer bijvoorbeeld ingebroken wordt op informatiesystemen die zelf niet betrokken zijn bij de verstrekking van gekwalificeerde certificaten, maar waarbij het mogelijk is om via die systemen toegang te krijgen tot systemen die wel betrokken zijn bij de uitgifte van gekwalificeerde certificaten, geldt daarvoor een verplichting tot melden. In dat geval kunnen als gevolg van een inbreuk ook aanzienlijke gevolgen voor de betrouwbaarheid van de aangeboden of afgegeven gekwalificeerde certificaten optreden. Tot afgegeven gekwalificeerde certificaten worden naast geldende certificaten, ook verlopen en ingetrokken gekwalificeerde certificaten gerekend. De meldplicht strekt zich ook tot die laatste certificaten uit, zolang een certificatiedienstverlener bij of krachtens de wet een verantwoordelijkheid ten aanzien van die certificaten heeft. Tot de incidenten, die aanzienlijke gevolgen kunnen hebben, dient bijvoorbeeld elke inbraak (fysiek in het bedrijfspand of online) gerekend te worden voor zover het bedrijfspand of systeem op welke manier dan ook gebruikt wordt voor dienstverlening rond gekwalificeerde certificaten. Ook de ontdekking van virussen, malware of andere ongeautoriseerde software die op een van de betreffende systemen van de certificatiedienstverlener aanwezig is, valt hier onder. Uiteraard moet het hier wel gaan om virussen, malware enz. die aanzienlijke gevolgen kunnen hebben voor de betrouwbaarheid van de gekwalificeerde certificaten. Een virus waarvan direct bekend is dat het volstrekt onschuldig is voor de betrouwbaarheid hoeft dus niet gemeld te worden. Ook onvolkomenheden in de toegangsbeveiliging of bijvoorbeeld gedragingen van het personeel die het begaan van een misdrijf betreffen (zie in dit verband ook artikel 4, eerste lid, onderdeel s, en tweede lid, van het Besluit elektronische handtekeningen), vallen onder de meldplicht. Indien er gerede twijfel is over de omvang van de gevolgen, waarbij die gevolgen ook groot zouden kunnen zijn dient gemeld te worden. Inbreuken met geringe gevolgen hoeven niet gemeld te worden. Wanneer bijvoorbeeld procedures niet (volledig) correct zijn doorlopen of sluitend zijn, maar de integriteit of betrouwbaarheid nooit in het geding is geweest of kan zijn, hoeft er niet gemeld te worden. Als een gekwalificeerd certificaat ten onrechte op de zwarte lijst wordt gezet, dit wordt ontdekt en bij contact met de certificaathouder blijkt dat die het certificaat in die periode niet heeft gebruikt, zal de impact ook gering kunnen zijn.

Met dit besluit wordt een aantal doelstellingen beoogd. Als toezichthouder dient ACM er op toe te zien dat certificatiedienstverleners voldoen aan de bij of krachtens de wet gestelde eisen, die onder andere de betrouwbaarheid van gekwalificeerde certificaten moeten waarborgen. Incidenten zoals hier bedoeld, zijn bij uitstek momenten waarop eventuele gebreken daarin aan het licht komen. ACM kan nadere informatie opvragen en indien nodig maatregelen treffen waartoe de wet haar bevoegdheid geeft (artikelen 2.2, vierde lid, 15.2, 15.4 en 18.7 van de Telecommunicatiewet). De certificatiedienstverlener zal daaraan dan uitvoering dienen te geven. Daarnaast kan ACM er door een onverwijlde melding van een incident op toezien dat – mede op basis van adviezen van NCSC – zo snel mogelijk actie wordt ondernomen om de maatschappelijke gevolgen van de inbreuk zoveel als mogelijk in te perken of te voorkomen. Een andere doelstelling is het continu verbeteren van de veiligheid en betrouwbaarheid ten aanzien van gekwalificeerde certificaten. Zwakheden in procedures worden vaak door incidenten kenbaar. Door middel van meldingen kan systematisch gewerkt worden aan het verbeteren van deze procedures. Wanneer ACM vaststelt dat vergelijkbare procedures bij verschillende certificatiedienstverleners in gebruik zijn, en daar worden zwakheden in ontdekt, kan ACM dit aankaarten bij de

bezoeken die zij in het kader van het toezicht aflegt. Ook NCSC kan in het kader van haar voorlichtende taak aandacht besteden aan dergelijke zwakheden. Een vierde doelstelling is het preventief vergaren van informatie over incidenten die mogelijk grote gevolgen kunnen hebben voor de dienstverlening. Door deze centraal bij NCSC te verzamelen, wordt het mogelijk om bijvoorbeeld reeds eerder (bij anderen) gesignaleerde incidenten te herkennen en gericht de getroffen certificatiedienstverlener bij te staan met technische en functionele hulp en ondersteuning door NCSC. Doel van dit alles moet uiteraard zijn de betrouwbaarheid van gekwalificeerde certificaten op een zo hoog mogelijk niveau te houden.

3. Toepassingsgebied

Het besluit bevat enkel de plicht tot melding van veiligheidsinbreuken of integriteitsverlies met (potentieel) aanzienlijke gevolgen voor 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 denkbaar dat de op zich gescheiden systemen voor gekwalificeerde en niet-gekwalificeerde certificaten van een certificatiedienstverlener op eenzelfde of vergelijkbare wijze zijn beveiligd. Wanneer dan een succesvolle aanval plaatsvindt op informatiesystemen die een certificatiedienstverlener gebruikt voor niet-gekwalificeerde certificaten, bestaat er ook gerede twijfel over de informatiebeveiliging van de systemen waarmee gekwalificeerde certificaten worden uitgegeven. 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.

4. Betrokken organen

Het besluit bepaalt dat een melding dient plaats te vinden aan ACM en aan de Minister van Veiligheid en Justitie die verantwoordelijk is voor NCSC. Ten aanzien van meldingen aan 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 NCSC (Kamerstukken II 2011/12, 26 643, nr. 247).

Dit besluit bevat een afzonderlijke plicht tot melding aan 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.

5. Uitvoerings- en handhavingstoets

Het ontwerp-besluit is op 7 mei 2013 voor een Uitvoeringstoets voorgelegd aan de Autoriteit Consument & Markt (ACM), welke hier op 5 juni 2013 op heeft gereageerd. ACM is van oordeel dat het voorstel de effectiviteit van het toezicht kan verbeteren. ACM zie ook enkele knelpunten voor de doeltreffendheid van haar toezicht en doet daartoe enkele verbetervoorstellen, zoals het verduidelijken en aanvullen van de Nota van Toelichting op diverse punten. De belangrijkste voorstellen betreffen de reikwijdte van de meldplicht, de vertrouwelijkheid van de meldingen en de ongewijzigde eigen verantwoordelijkheid van de certificatiedienstverleners. Verder benadrukt ACM dat zij onafhankelijk toezicht zal houden en handhaven met het oog op het waarborgen van de betrouwbaarheid van het totale stelsel in het algemeen maatschappelijk belang. Deze voorstellen van ACM hebben geleid tot enkele aanpassingen en aanvullingen op die punten in de Nota van Toelichting.

6. Regeldruk

De regeldruk zal licht toenemen voor certificatiedienstverleners die gekwalificeerde certificaten aanbieden. Op jaarbasis worden gemiddeld vier 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 400 Euro per bedrijf en maximaal 4.000 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, maar dit zal zich alleen bij hoge uitzondering voordoen.

Daarnaast zal er eenmalig geïnvesteerd moeten worden in het aanpassen van de procedures met betrekking tot incidenten. Dat zal per bedrijf enkele mandagen kunnen kosten en daarom in totaliteit ca. 40.000 euro bedragen. Het toezicht op meldplicht zal onderdeel zijn van de jaarlijkse externe audit op veiligheidsaspecten en zal naar verwachting niet tot extra toezichtslasten leiden.

De regeldruk voor burgers en de inhoudelijke nalevingskosten voor bedrijven blijven ongewijzigd.

7. Consultatie

Dit besluit is geconsulteerd door middel van een internetconsultatie op Overheid.nl. De consultatie startte op 20 februari 2013 en eindigde op 20 maart 2013. Er zijn drie reacties ontvangen, waarvan er twee inhou-

delijk commentaar bevatten. Uit de consultatie bleek dat de doelstellingen van het besluit door deze partijen worden onderschreven.

Er zijn vraagtekens geplaatst bij de concrete invulling van de meldplicht bij zowel ACM als NCSC en over hoe dit zich verhoudt tot het reeds bestaande gezamenlijke meldpunt van ACM en Agentschap Telecom voor meldingen van inbreuken op persoonsgegevens (hoofdstuk 11 Telecommunicatiewet) en inbreuken op de continuïteit van de dienstverlening (hoofdstuk 11A Telecommunicatiewet). Daarnaast is in de consultatie opgemerkt dat er bij de inschatting van de administratieve lasten alleen is gekeken naar de kosten voor het doen van de meldingen, en niet naar de kosten voor het aanpassen van de interne bedrijfsprocessen naar aanleiding van dit besluit. Door in de praktijk een samenwerking te realiseren tussen ACM en NCSC over de wijze waarop gemeld moet worden, zullen de structurele kosten worden beperkt. Verder wordt er van uitgegaan dat betrokken bedrijven de meldingen zullen integreren in hun eigen aanpak van incidenten, maar eenmalige kosten qua aanpassing van procedures zijn niet te vermijden.

In de consultatiebijdragen werd verder gewezen op ongewenste (mogelijke) verschillen met de voorgestelde Europese Verordening. Hier is zoveel mogelijk bij aangesloten, maar gelet op het in paragraaf 1 van deze toelichting beschreven belang van de meldplicht voor de snelle onderkenning en effectieve aanpak van incidenten, en de onzekerheid over de definitieve inhoud en het moment van inwerkingtreding van de Verordening, is besloten hier niet op te wachten.

Verder werd in de reacties op de consultatie opgemerkt dat bepaalde begrippen en bewoordingen, zoals «inbreuk», «veiligheid», «systemen niet in alle gevallen consistent worden gebruikt of niet nader worden toegelicht. Naar aanleiding van deze opmerkingen is de toelichting getoetst op consistentie en eenduidigheid van de gehanteerde begrippen en waar nodig op enkele onderdelen aangepast.

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 ACM. De verplichting heeft betrekking op gekwalificeerde certificaten en niet op andersoortige certificaten, zoals bijvoorbeeld SSL-certificaten die gebruikt worden voor website-authenticatie.

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 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 veiligheidsinbreuk of integriteitsverlies slechts beperkte impact heeft. 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. Het is niet mogelijk en niet zinvol een uitputtende omschrijving van alle mogelijk voorkomende gevallen van meldingsplichtige inbreuken of verliezen te geven. 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 gerede 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. Onverwijld betekent hier zo snel mogelijk, maar zeker niet later dan 24 uur na ontdekking. 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 en NCSC 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. Een tijdige reactie van de toezichthouder en NCSC laat de eigen en primaire verantwoordelijkheid van de certificatiedienstverlener onverlet, waaronder het zo spoedig mogelijk verhelpen van een incident en de gevolgen daarvan.

De verplichting tot onverwijlde melding is ook van belang voor de certificatiedienstverlener die derden heeft ingeschakeld voor bepaalde aspecten van zijn dienstverlening. Hij zal met die derden afspraken dienen te maken, die er toe leiden dat hun inschakeling een onverwijlde melding mogelijk maken. Bij een melding is een kennisgeving van specifieke informatie vereist die inzicht biedt in de aard, start, gevolgen en te verwachten onderzoeksduur 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. Bij de melding van de mogelijke gevolgen is van belang dat zowel gevolgen op de korte als langere termijn, voor zover althans in te schatten, worden gemeld, en ook de minder waarschijnlijke maar niet uit te sluiten gevolgen. De met betrekking tot de melding verstrekte informatie betreft in het algemeen bedrijfs- en fabricagegegevens als bedoeld in artikel 10, eerste lid, onder c, van de Wet openbaarheid van bestuur.

De verstrekte informatie is voor ACM 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 aan integriteit 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. Voor het naderhand inwinnen van

verdere informatie kan ACM op grond van artikel 18.7, eerste lid, van de Telecommunicatiewet van een ieder te allen tijde inlichtingen vorderen voor zover dit redelijkerwijs voor de vervulling van haar taak nodig is.

Artikel II

Ingevolge het kabinetsbeleid inzake Vaste Verandermomenten treedt nieuwe regelgeving in beginsel in werking op 1 januari of 1 juli van enig jaar. In dit besluit wordt hiervan afgeweken. De kwetsbaarheid van de samenleving voor veiligheidsinbreuken op gekwalificeerde certificaten vereist onverwijlde betrokkenheid van ACM en van NCSC bij incidenten. Zij beschikken over bevoegdheden en expertise die belangrijk zijn voor het beperken van ongewenste private en publieke nadelen als gevolg van een inbreuk. Een meldplicht als bedoeld in dit besluit waarborgt die tijdige betrokkenheid. Voortvarendheid bij de invoering van een meldplicht is vereist gelet op het belang van het verminderen van de kwetsbaarheid van de samenleving voor veiligheidsinbreuken. Als gevolg daarvan is het gewenst dat dit besluit zo spoedig mogelijk in werking zal treden zodra het meldpunt ten behoeve van ACM en NCSC operationeel is. Dit zal op 1 november 2013 het geval zijn.

De Minister van Economische Zaken,
H.G.J. Kamp