Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

> Retouradres Postbus 20011 2500 EA Den Haag

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal
Postbus 20018
2500 EA Den Haag

Directie Dienstverlening, Regeldruk en informatiebeleid
Cluster Informatiebeleid
Basisvoorzieningen Overheid

Schedeldoekshaven 200
2511 EZ Den Haag
Postbus 20011
2500 EA Den Haag
www.rijksoverheid.nl

Contactpersoon
Kim Schamp

T 070-4268269
kim.schamp@minbzk.nl

Datum 13 september 2011
Betreft Beantwoording schriftelijke vragen met de kenmerken 2011Z16610, 2011Z16612 en 2011Z16661.

Bijlagen
1

Hierbij bied ik u, mede namens de minister van Justitie en Veiligheid, de minister van Buitenlandse Zaken en de minister van Defensie de antwoorden aan op de schriftelijke vragen die zijn gesteld door het lid El Fassed (Groenlinks) betreffende internetcertificaten, ingezonden 31 augustus 2011 met kenmerk 2011Z16610, het lid Verhoeven (D66) betreffende de beveiliging van DigiD en overheidswebsites, ingezonden 31 augustus 2011 met kenmerk 2011Z16612 en de leden Elissen, Hernandez en Kortenoeven (allen PVV) betreffende een blunder bij DigiNotar, ingezonden 1 september 2011 met kenmerk 2011Z16661.

De minister van Economische Zaken, Landbouw en Innovatie is, mede gelet op de vragen 3 en 7 van het lid El Fassed, eveneens betrokken bij de beantwoording.

In antwoord op uw brief van 7 september 2011 met kenmerk 2011Z17081 deel ik u mee, mede namens de minister van Veiligheid en Justitie, dat het kabinet uw Kamer, zoals verzocht, per brief nader zal informeren over de gebeurtenissen, voorafgaande aan het plenaire debat hierover. In die brief zal ik ook ingaan op de belangrijkste berichten in de media over de veiligheid van overheidswebsites.

De minister van Binnenlandse Zaken en Koninkrijksrelaties,

J.P.H. Donner

Beantwoording Kamervragen betreffende DigiNotar

2011Z16610

Vragen van het lid El Fassed aan de ministers van Binnenlandse Zaken en Koninkrijksrelaties en van Buitenlandse Zaken over internetcertificaten (ingezonden 31 augustus 2011)

Vraag 1
Kent u het bericht 1) in onder meer Webwereld dat Iran erin is geslaagd om het internetverkeer van haar burgers naar Google.com af te tappen door middel van een vervalst beveiligingscertificaat bij de Nederlandse certificeringsautoriteit DigiNotar?

Antwoord op vraag 1
Ja.

Vraag 2
Bent u ermee bekend dat het zogeheten 'rootcertificaat' van de uitgever van het door Iran vervalste certificaat, het bedrijf DigiNotar, ongeldig is verklaard door Microsoft en Mozilla, en mogelijk door andere softwareleveranciers?

Antwoord op vraag 2
Het is ons bekend dat de certificaten van het bedrijf DigiNotar door de webbrowsers niet meer als betrouwbaar worden aangemerkt. Leveranciers van besturingssystemen en applicatiesoftware kunnen een update doorvoeren van hun systemen met als gevolg dat sommige websites en onderliggende systemen moeilijker - of in het geheel niet - bereikbaar zijn. Een aantal heeft dit ook gedaan.

Vraag 3
Kunt u toelichten op welke wijze door de overheid toezicht werd uitgeoefend op het functioneren van DigiNotar? Doet u onderzoek naar de oorzaken van deze zaak?

Antwoord op vraag 3
In het stelsel van PKI-Overheid is voorzien dat certificaatleveranciers (CA) jaarlijks worden geaudit naar de opzet en werking van de eisen zoals vastgelegd in het Programma van Eisen PKI-Overheid. Deze audits worden uitgevoerd door gecertificeerde auditors. Zij rapporteren aan de Policy Authority (PA) van PKI-Overheid.
Daarnaast vindt er toezicht plaats door de OPTA[1] op basis van de Telecomwet, indien er sprake is van uitgifte van gekwalificeerde[2] certificaten ten behoeve van de elektronische handtekening. De DigiNotar certificaten waarbij het aangetoonde misbruik heeft plaats gevonden, zijn certificaten waar de OPTA geen bevoegdheid heeft om op toe te zien.
Het Kabinet neemt de structurele betekenis van de gebeurtenissen in ogenschouw. In het licht hiervan voert het ministerie van Binnenlandse Zaken en Koninkrijksrelaties onderzoek uit naar het gehele stelsel en proces rondom PKI-Overheid, inclusief het toezicht daarop. Het ministerie van ELI laat aanvullend daarop onderzoeken in hoeverre de problemen rondom DigiNotar ook consequenties hebben voor de wijze van toezicht op uitgifte van gekwalificeerde certificaten. De Tweede Kamer wordt hierover geïnformeerd zodra meer duidelijk is. Zoals in het regeerakkoord is gesteld zal de Staatssecretaris van Veiligheid en

[1] De Onafhankelijke Post en Telecom Autoriteit (OPTA) voert toezicht uit op de aanbieders van gekwalificeerde certificaten. Deze certificatendienstverleners worden geplaatst in een openbaar register.
[2] Gekwalificeerde certificaten zijn bruikbaar in het elektronische verkeer tussen bedrijven onderling en tussen bedrijven en overheid. PKI-overheidscertificaten worden alleen ingezet in het elektronische verkeer van burgers en bedrijven met de overheid en tussen overheidsinstellingen.

Justitie bovendien een wetsvoorstel indienen dat een meldplicht introduceert voor gebeurtenissen zoals deze bij DigiNotar zijn voorgekomen.

Vraag 4
Kunt u de consequenties van deze zaak toelichten voor de dienstverlening en het interne functioneren van de Nederlandse overheid en andere klanten van DigiNotar? Hebben burgers overlast ondervonden van deze zaak en zo ja, in hoeveel gevallen en op welke wijze?

Antwoord op vraag 4
De gevolgen van de reactie door internetdienstverleners op het bekend worden van de door DigiNotar afgegeven gecompromitteerde certificaten voor het vertrouwen in het digitale communicatieverkeer zijn groot, ook al is de materiële betekenis van die afgifte mogelijk veel beperkter. Alleen partijen die gebruik maken van certificaten of diensten van DigiNotar lopen het risico dat systemen of communicatie uitvallen. Tot nu toe is geconstateerd dat sommige websites (tijdelijk) uit de lucht zijn.
DigiNotar is niet het enige bedrijf dat certificaten en diensten voor internetverkeer genereert. De certificaten van andere bedrijven worden niet geraakt door de gebeurtenissen bij DigiNotar.
Het Kabinet heeft het operationele beheer van de systemen voor certificering bij DigiNotar gecontroleerd overgenomen, zodat de certificaten gefaseerd kunnen worden ingetrokken en het gebruik van de door hacker aangemaakt en gebruikte certificaten kan worden gemonitord en kan worden bestreden waar dit wordt waargenomen.

Vraag 5
Acht u het uitgesloten dat Iran of enige andere partij erin kan zijn geslaagd om zich via DigiNotar toegang te verschaffen tot vertrouwelijke communicatie van de Nederlandse overheid? Welke stappen heeft u gezet om zich daarvan te vergewissen?

Antwoord op vraag 5
Het Kabinet onderzoekt wie betrokken zijn bij het hacken van DigiNotar. Voor een beschrijving van genomen besluiten en ingezette acties verwijs ik naar de Kamerbrief “Digitale inbraak DigiNotar” van 5 september 2011.

Vraag 6.
Bent u van plan om Iran op deze zaak aan te spreken?

Antwoord op vraag 6
Het Kabinet onderzoekt momenteel wie betrokken zijn bij het hacken van DigiNotar. Op grond van de uitkomsten van dit onderzoek beraadt het Kabinet zich op passende vervolgstappen.

Vraag 7
Acht u het in het licht van deze zaak verstandig om nieuwe certificaten van de Nederlandse overheid toe te vertrouwen aan particuliere bedrijven? Zo nee, overweegt u om certificaten direct door de Nederlandse overheid te laten uitgeven? Zo ja, welke aanvullende eisen overweegt u te stellen aan deze bedrijven? Kunt u dat toelichten?

Antwoord op vraag 7
Het feit dat de hacker certificaten namens DigiNotar oneigenlijk heeft aangemaakt, heeft geen gevolgen voor andere certificaatleveranciers. Wanneer de certificaten op een juiste, zorgvuldige wijze zijn gegenereerd, ongeacht door welk bevoegd bedrijf, is er op dit moment geen enkele aanleiding om te twijfelen aan de betrouwbaarheid en veiligheid van deze certificaten en al het internetverkeer dat met behulp van deze certificaten heeft plaatsgevonden.

Tegelijkertijd is het Kabinet van oordeel dat de structurele betekenis van de gebeurtenissen in ogenschouw moeten worden genomen. Als onderdeel daarvan voert het ministerie van Binnenlandse Zaken en Koninkrijksrelaties een onderzoek uit naar het gehele stelsel en proces rondom PKI-Overheid, inclusief het toezicht daarop. Daarnaast zal de DigiNotar problematiek ook geëvalueerd worden met het oog op de gewenste betrouwbaarheid van digitale dienstverlening van en aan bedrijven. De Tweede Kamer wordt hierover geïnformeerd zodra hierover meer duidelijkheid is.

1) http://webwereld.nl/nieuws/107747/iran-kan-gmail-aftappen-door-nederlands-certificaat--update-2--.html

2011Z16612

Vragen van het lid Verhoeven (D66) aan de minister van Binnenlandse Zaken en Koninkrijksrelaties over de beveiliging van DigiD en overheidswebsites (ingezonden 31 augustus 2011) Deze vragen dienen ter aanvulling op eerdere vragen ter zake van het lid El Fassed (GroenLinks), ingezonden 31 augustus 2011 (vraagnummer 2011Z16610).

Vraag 1
Heeft u kennisgenomen van het bericht "Browsers dumpen DigiNotar na Iraanse Gmail-tap"en specifiek het in de ban doen van het DigiNotar certificaat door Firefox, IE en Chrome? 1)

Antwoord op vraag 1
Ja.

Vraag 2
Is het zo dat de Nederlandse staat via onder meer DigiD ook gebruik maakt van de diensten en specifiek van certificaten van DigiNotar? Kunt u een opsomming geven van de verschillende websites en diensten die hier gebruik van nemen?

Antwoord op vraag 2
Ja. De DigiNotar certificaten voor DigiD zijn inmiddels vervangen.
Het betreft enkele tienduizenden certificaten van DigiNotar waarvan de betrouwbaarheid thans ter discussie is gesteld. Daaronder valt een substantieel aantal certificaten dat in gebruik is bij de Nederlandse staat en dat wordt ingezet voor diverse overheidswebsites en -diensten. Alle door het bedrijf DigiNotar uitgegeven certificaten voor publieke en semi-publieke organisaties worden of zijn inmiddels vervangen door certificaten van andere (PKI-) certificatenleveranciers. De CIO's (Chief Information Officers) van Rijk en decentrale overheden zijn aangewezen om de omzetting van de certificaten van DigiNotar aan te sturen. In de komende periode gaan alle websites en diensten gefaseerd en gecontroleerd over op nieuwe certificaten.

Vraag 3
Betekent de genoemde inbreuk dat de handtekening van DigiNotar nu de facto waardeloos is geworden, dat browsers ook de beveiliging van DigiD niet meer op waarde kunnen schatten en dat browsers beveiligingswaarschuwingen zullen geven bij veilige overheidswebsites? Biedt dit ruimte voor derde partijen om onveilige kopieën te maken van overheidswebsites die dan dezelfde melding zullen krijgen, maar in tegenstelling tot de originelen niet meer veilig zijn en die burgers kunnen misleiden?

Antwoord op vraag 3
Nee. Uit de omstandigheid dat thans DigiNotar-certificaten gecompromitteerd blijken te kunnen zijn, kan en mag niet worden geconcludeerd dat alle historische transacties van DigiNotar mogelijk gecompromitteerd zijn;
Inmiddels zijn DigiD.nl en mijn.belastingdienst.nl overgegaan naar een andere certificaatleverancier, waarvan de certificaten betrouwbaar zijn en worden vertrouwd door de softwareleveranciers;
Ja, het is mogelijk dat browsers in de omschakelperiode naar andere certificaten beveiligingswaarschuwingen geven bij veilige overheidswebsites en;
Ja, in de omschakelperiode naar andere certificaten is het mogelijk dat derde partijen onveilige kopieën kunnen maken van overheidswebsites (de zgn. omgeleide sites), die gebruik maken van de door de hacker oneigenlijk aangemaakte certificaat van DigiNotar. Om deze reden is het operationele beheer van het systeem voor het verstrekken van certificering

gecontroleerd overgenomen zodat de certificaten gefaseerd kunnen worden ingetrokken en het gebruik van de door hacker aangemaakt en gebruikte certificaten kan worden gemonitord en kan worden bestreden waar dit wordt waargenomen.

Vraag 4
Kunt u via onafhankelijk onderzoek aantonen dat de beveiliging van overheidsdiensten zoals DigiD en beveiligde websites nog altijd afdoende is?

Antwoord op vraag 4
De overheid neemt diverse maatregelen om de beveiliging van overheidsdiensten en -websites te beheersen. Zo heeft het Kabinet, na overleg met het moederbedrijf van DigiNotar, nog in de nacht van vrijdag op zaterdag het operationele beheer van systemen voor certificaten van het bedrijf overgenomen teneinde de schade van de gebleken inbreuk op de integriteit van het internetverkeer en de beheersmaatregelen ter beperking van de gevolgen van de gebeurtenis. Daardoor wordt een beheersbare migratie naar andere certificaten mogelijk zonder dat dit additionele risico's schept voor zover bekend.
Voor een overzicht verwijs ik u naar de Kamerbrief "Digitale inbraak DigiNotar" van 5 september 2011.

1) Webwereld.nl, 30 aug 2011

2011Z16661

Vragen van de Leden Elissen, Hernandez en Kortenoeven (alle drie PVV) aan de minister van Veiligheid en Justitie, de minister van Buitenlandse Zaken, de minister van Binnenlandse zaken en Koninkrijksrelaties en de minister van Defensie over een blunder bij DigiNotar.

Vraag 1
Bent u bekend met het bericht 'Browsermakers geven nieuwe versie uit na DigiNotar blunder? (1)

Antwoord op vraag 1
Ja.

Vraag 2
Heeft deze blunder gevolgen voor het gebruik van DigiD omdat DigiNotar het bedrijf is dat de beveiligingscertificaten levert waardoor burgers veilig gebruik kunnen maken van DigiD?

Antwoord op vraag 2
Het heeft gevolgen gehad voor het gebruik van DigiD. In de loop van dinsdag 6 september is DigiD overgeschakeld naar een andere certificaatleverancier. Voor die tijd kunnen burgers geconfronteerd zijn met waarschuwingen of meldingen dat de site niet langer vertrouwd kan worden.

Vraag 3
Is er aanleiding om DigiNotar en andere 'certificate authorities' aan nadere inspectie te onderwerpen om de privacy van Nederlandse burgers te waarborgen?

Antwoord op vraag 3
Het Kabinet heeft in de nacht van vrijdag op zaterdag het operationele beheer van systemen voor certificaten van DigiNotar overgenomen, teneinde de schade van de gebleken inbreuk op de integriteit van het internetverkeer te beperken en de beheersmaatregelen ter beperking van de gevolgen te kunnen treffen. Daardoor wordt een beheersbare migratie naar andere certificaten mogelijk zonder dat dit voor zover bekend additionele risico's schept.
Op dit moment wordt prioriteit gegeven aan het beheersen van het huidige incident en de gevolgen daarvan. Tegelijkertijd constateert het Kabinet dat de structurele betekenis van de gebeurtenissen in ogenschouw moeten worden genomen. Als onderdeel daarvan voert het ministerie van Binnenlandse Zaken en Koninkrijksrelaties een onderzoek uit naar het gehele stelsel en proces rondom PKI-Overheid, inclusief het toezicht daarop. De Tweede Kamer wordt hierover geïnformeerd zodra hierover meer duidelijkheid is.

Vraag 4
Gaat de blunder bij DigiNotar naar uw verwachting gevolgen hebben voor de elektronische dienstverlening van de overheid? Gaan burgers en/of overheidsonderdelen hier hinder van ondervinden? Zo nee, waarom niet?

Antwoord op vraag 4
De inbraak bij DigiNotar en de door de hacker daarbij aangemaakte en gebruikte certificaten vormen een ernstige aantasting van het vertrouwen in en de integriteit van het digitale communicatieverkeer. De aantasting van het vertrouwen in de certificaten van DigiNotar kan potentieel grote implicaties hebben voor zowel het verkeer tussen mens en machine als voor het verkeer tussen machines onderling.
Voor het digitale communicatieverkeer ontstaat door het aanmaken en gebruik van boven genoemde certificaten het risico dat het voor de internetgebruiker niet meer zichtbaar is of hij

te maken heeft met een betrouwbare website of computer, blijkend uit het certificaat ('slotje') op het scherm. De mogelijke introductie van deze certificaten maakt, dat gebruikers er niet meer in alle gevallen zonder meer van uit kunnen gaan, dat het een veilige internetcommunicatie betreft. In dergelijke gevallen kan de burger worden doorgeleid naar een niet bedoelde site, waarbij de gegevens die de burger verstrekt, in verkeerde handen terechtkomen. Hierdoor wordt het vertrouwen in het digitale communicatieverkeer ernstig aangetast.
Het Kabinet heeft het operationele beheer van de systemen voor certificering bij DigiNotar gecontroleerd overgenomen, zodat de certificaten gefaseerd kunnen worden ingetrokken en het gebruik van de door hacker aangemaakt en gebruikte certificaten kan worden gemonitord en kan worden bestreden waar dit wordt waargenomen.
Er zijn tot dusver echter geen aanwijzingen dat dit in Nederland ook daadwerkelijk heeft plaatsgevonden.

Vraag 5
Heeft het feit dat bedrijven als Mozilla, Microsoft (2) en Google het vertrouwen in DigiNotar hebben opgezegd gevolgen voor de samenwerking tussen de Nederlandse overheid en DigiNotar?

Antwoord op vraag 5
Het Kabinet heeft het vertrouwen in het bedrijf DigiNotar en alle door hen geleverde diensten en certificaten opgezegd en het operationele beheer van het systeem voor het verstrekken van certificering overgenomen. Alle door het bedrijf afgegeven certificaten voor publieke en semi-publieke organisaties worden vervangen door certificaten van andere certificatenleveranciers nadat is gebleken dat de certificaten en diensten van de andere certificatenleveranciers betrouwbaar zijn.

Vraag 6
Klopt de uitspraak van Woordvoerder Jochem Binst dat de blunder van DigiNotar geen gevolgen heeft voor het werk dat DigiNotar voor de overheid doet? Zo ja, kunt u dit toelichten?

Antwoord op vraag 6
Zie het antwoord op vraag 5.

Vraag 7
Klopt het dat DigiNotar gehackt is, zoals op F-secure wordt gemeld? (3)

Antwoord op vraag 7
Er heeft een hack (digitale inbraak) bij DigiNotar plaatsgevonden. Zie feitenrelaas in brief d.d. 5 september.

Vraag 8
Gaat u onderzoeken of Iran achter de (geslaagde) hackpoging van DigiNotar zit? Zo nee, waarom niet? Zo ja, is hier sprake van cybercrime of cyberwarfare?

Antwoord op vraag 8
Het Kabinet onderzoekt momenteel wie betrokken zijn bij het hacken van DigiNotar. Mede in het licht van de uitkomst daarvan zal het Kabinet beslissen over passende vervolgstappen.

Vraag 9
Gaat u onderzoeken of er mensenrechten in Iran zijn geschonden doordat Iran een Nederlands certificaat heeft weten te bemachtigen?

Antwoord op vraag 9
Zie het antwoord op vraag 8.

(1) ‘Browsermakers geven nieuwe versie uit na DigiNotar blunder’
http://tweakers.net/nieuws/76445/browsermakers-geven-nieuwe-versies-uit-nadiginotar-blunder.html

(2) ‘Microsoft Security Advisory (2607712)’
http://www.microsoft.com/technet/security/advisory/2607712.mspx

(3) ‘DigiNotar Hacked by Black.Spook and Iranian Hackers’
http://www.fsecure.com/weblog/archives/00002228.html