Forum Standaardisatie

Expertadvies DNSSEC

Datum 13 februari 2012

Colofon

Projectnaam	Expertadvies DNSSEC
Versienummer	1.0
Locatie	
Organisatie	Forum Standaardisatie Postbus 96810 2509 JE Den Haag forumstandaardisatie@logius.nl

Auteurs	Bart Gijsen Matthijs Punter Diederik Rothengatter

Inhoud

Managementsamenvatting

Waar gaat het inhoudelijk over?
DNS (Domain Name System) wordt gebruikt om internet-domeinnamen om te zetten naar IP-adressen en vice versa. Als zodanig is het DNS een belangrijke component in de werking van het internet. De standaard DNSSEC maakt het mogelijk om een belangrijke kwetsbaarheid van het DNS-systeem weg te nemen, die het mogelijk maakt bezoekers ongemerkt om te leiden naar een IP-adres waarachtig een valse pagina schuilgaat.

De standaard DNSSEC werkt bovenop de bestaande DNS. De standaard werkt door aan bestaande DNS-registraties (de z.g.n. records) van een domeinnaam extra informatie toe te voegen in de vorm van een digitale handtekeningen. Deze kunnen dan door de bevragende partij (de bezoeker van de website) geverifieerd worden.

Door als overheid de eigen websites van dergelijke handtekeningen te voorzien ('signing') en door de handtekening van andere DNS records te controleren ('validation') neemt de betrouwbaarheid sterk toe.

Hoe is het proces verlopen?
Op 27 januari 2012 is een expertgroep met vertegenwoordigers uit bedrijfsleven en overheid bijeen gekomen. Vooraf zijn zij, en enkele anderen die niet aanwezig konden zijn, in de gelegenheid gesteld input te leveren. Op basis van deze input en de discussie tijdens de bijeenkomst is dit adviesrapport opgesteld.

Hoe scoort de standaard op de toetsingscriteria?

- *Open standaardisatieproces*
  DNSSEC is gestandaardiseerd binnen de IETF (Internet Engineering Task Force). Het standaardisatieproces van de IETF voldoet aan de gestelde criteria voor een open standaardisatieproces.

- *Toegevoegde waarde*
  De expertgroep meent dat de voordelen van DNSSEC opwegen tegen de extra kosten die gemaakt moeten worden. De voordelen zitten vooral op het vlak van een betere betrouwbaarheid van overheidswebsites. De kans op door kwaadwillenden vervalste overheidswebsites neemt door het gebruik van DNSSEC af. Naarmate meer schakels in de keten voorzien zijn van DNSSEC nemen deze voordelen toe. Er zijn geen voor de hand liggende alternatieven voor de standaard.

- *Draagvlak*
  Er is wereldwijd draagvlak voor DNSSEC onder relevante belanghebbende groepen. De Amerikaanse overheid heeft reeds enkele jaren geleden het beleidsbesluit genomen om DNSSEC toe te passen voor domeinen onder het top-level domein van de federale overheid (.gov). In de verdere adoptie is nog wel

stimulans nodig, temeer omdat de meerwaarde stijgt naar mate de adoptiegraad toeneemt.

- *Opname bevordert adoptie*
  Het DNS-systeem wordt door invoering van DNSSEC weliswaar veiliger, maar ook complexer en gevoeliger voor fouten door systeembeheerders. Dit is een potentiële drempel voor de adoptie.

  Het is daarom wenselijk dat er naast opname van de standaard op de lijst voor 'pas toe of leg uit' - een handreiking komt voor overheidsorganisaties m.b.t. de inzet van DNSSEC. Deze handreiking moet overheidsorganisaties helpen om te gaan met invoering van de standaard.

Wat is de conclusie van de expertgroep
De expertgroep concludeert dat de standaard in voldoende mate scoort aan de gestelde toetsingscriteria en adviseert DNSSEC op te nemen op de lijst voor 'pas toe of leg uit'.

Als toepassingsgebied wordt voorgesteld:

"Systemen en diensten voor:
- *Het registreren en in DNS publiceren van internet-domeinnamen ('signing').*
- *Het vertalen van domeinnamen naar internetadressen en vice versa ('validation enabled resolving').*

Hierbij gelden twee beperkingen:
- *De registratieverplichting geldt enkel indien 'signed domain names' bij een registry van een top-level domein geautomatiseerd aangevraagd kunnen worden.*
- *DNSSEC validatie is niet verplicht voor systemen die niet direct aan het publieke internet gekoppeld zijn (bijvoorbeeld clients/werkplekken binnen een LAN en interne DNS systemen)."*

Met de twee gestelde beperkingen wordt een aantal praktische bezwaren weggenomen. Dit betreft het (nog) niet aanwezig zijn van de mogelijkheid om automatisch een domeinnaam te registreren binnen een top-level domein (dit is bijvoorbeeld nog niet mogelijk voor het .cw van Curaçao). Daarnaast zouden niet alle systemen *verplicht* voorzien hoeven te worden van DNSSEC, maar enkel die systemen die direct gekoppeld zijn het publieke internet.

Welke additionele adviezen zijn er ten aanzien van de adoptie van de standaard?
Bij de beoordeling heeft de expertgroep benadrukt dat enkel opname van DNSSEC op de lijst van open standaarden niet voldoende is.

Omdat DNS met DNSSEC complexer is dan 'legacy' DNS, vergt deze standaard meer van de beheer- en implementatieaanpak. De expertgroep adviseert een handreiking op te stellen voor overheidsorganisaties waarin wordt beschreven hoe met deze extra complexiteit omgegaan moet worden.

1 Doelstelling expertadvies

1.1 Achtergrond

Het kabinet stelt via de Digitale Agenda.nl en i-NUP open standaarden als norm. Doel van dit ICT-beleid is om informatievoorziening toegankelijker te maken, om elektronische dienstverlening van de overheid te verbeteren, om onafhankelijkheid van ICT-leveranciers te vergroten, en om een krachtige impuls te geven aan economische groei en innovatie.

Eén van de maatregelen van het actieplan is het gebruik van een lijst met standaarden, die vallen onder het principe "pas toe of leg uit" (comply-or-explain) [1]. Het College Standaardisatie, dat in 2006 door het kabinet is ingesteld, spreekt zich uit over de standaarden die op de lijst zullen worden opgenomen, o.a. op basis van een expertbeoordeling van de standaard [2]. Het College Standaardisatie wordt geadviseerd door het Forum Standaardisatie. Bureau Forum Standaardisatie ondersteunt beide instellingen.

Onderwerp van dit expertadvies is DNSSEC. Deze standaard is aangemeld door dhr. Marco Davids, technisch adviseur bij de Stichting Internet Domeinregistratie Nederland (SIDN) voor opname op de lijst met open standaarden voor 'pas toe of leg uit'.

Een negental experts is verzameld in een expertgroep, die de DNSSEC standaard heeft beoordeeld aan de hand van een aantal criteria. Deze criteria – vooraf vastgesteld door het College Standaardisatie [3] en uitgewerkt in de vorm van concrete vragen - worden in het hier voorliggende expertadvies genoemd en behandeld. De opdracht aan de expertgroep was om een advies op te stellen over het wel of niet opnemen van deze standaard op de lijst, al dan niet onder bepaalde voorwaarden.

1.2 Proces

Voor het opstellen van dit advies is de volgende procedure doorlopen:

- Door het Bureau Forum Standaardisatie is een intakegesprek gevoerd met de indiener. Hierin is de standaard getoetst op uitsluitingscriteria ('criteria voor in behandelname') en is een eerste inschatting gemaakt van de kansrijkheid voor opname.
- Op basis van de intake is besloten tot het instellen van een expertgroep. Op basis van dit besluit is door het Bureau Forum Standaardisatie een groep samengesteld en een voorzitter aangezocht. Op basis van de aanmelding en de intake is een voorbereidingsdossier opgesteld voor leden van de expertgroep.
- De expertgroep is begonnen met het individueel scoren van de DNSSEC standaard aan de hand van een spreadsheet met vragen in het voorbereidingsdossier. Op basis van de verkregen antwoorden hebben voorzitter en begeleider van de expertgroep de verschillende knelpunten geïdentificeerd.
- Vervolgens is de expertgroep op 27 januari 2012 bijeengekomen om de bevindingen in het algemeen en de geïdentificeerde knelpunten in

het bijzonder te bespreken. Tijdens deze bijeenkomst zijn ook het toepassings- en werkingsgebied vastgesteld.

De uitkomsten van de expertgroep zijn door de voorzitter en begeleider verwerkt in dit advies rapport. Een eerste conceptversie is aan de leden van de expertgroep gestuurd met verzoek om reactie. Na verwerking van de reacties is het rapport afgerond, nogmaals toegestuurd aan de experts en ingediend voor de publieke consultatieronde.

1.3 Vervolg

Dit expertadvies zal ten behoeve van een publieke consultatie openbaar worden gemaakt door het Bureau Forum Standaardisatie. Eenieder kan gedurende de consultatieperiode op dit expertadvies zijn/haar reactie geven. Het Bureau Forum Standaardisatie legt vervolgens de reacties voor aan de voorzitter en indien nodig aan de expertgroep.

Het Forum Standaardisatie zal op basis van het expertadvies en relevante inzichten uit de openbare consultatie een advies aan het College Standaardisatie opstellen. Het College Standaardisatie bepaalt uiteindelijk op basis van het advies van het Forum of de standaard wordt opgenomen op de lijst voor 'pas toe of leg uit'.

1.4 Samenstelling expertgroep

Voor de expertgroep zijn personen uitgenodigd die vanuit hun persoonlijke expertise of werkzaamheden bij een bepaalde organisatie direct of indirect betrokken zijn bij de standaard. Daarnaast is een onafhankelijke voorzitter aangesteld om de expertgroep te leiden en als verantwoordelijke op te treden voor het uiteindelijke expertadvies.

Als voorzitter is opgetreden Bart Gijsen, senior consultant bij TNO op het gebied van Vitale Infrastructuren.

De expertgroep is in opdracht van het Forum Standaardisatie begeleid door Matthijs Punter.

Aan de expertgroep hebben deelgenomen:
- Dhr. Miek Gieben (SIDN)
- Dhr. Peter van Dijk (Netherlabs)
- Dhr. Olaf Kolkman (NLnet Labs)
- Dhr. Casper Gielen (Universiteit van Tilburg)
- Dhr. Jelte Jansen (Internet systems Consortium - ISC)
- Dhr. Klaus Spithost (IT-works)
- Dhr. Rolf Sonneveld (Sonnection)
- Dhr. René Schut (DUO)
- Dhr. Theo van Diepen (Logius)

Daarnaast is door een aantal mensen voorafgaand aan de expertgroepbijeenkomst een inhoudelijke bijdrage geleverd door het individueel scoren van de standaard of door het geven van een reactie in algemene zin:
- Dhr. Roland van Rijswijk (SURF)
- Dhr. Rob Weemhoff (IBM Nederland)

1.5 Toelichting DNSSEC

DNS staat voor 'Domain Name System' en is een set aan afspraken voor het vertalen van een internetdomeinnaam naar een IP-adres; deze koppeling wordt een DNS-record genoemd. Hiermee weet een computer welke server bij een domeinnaam hoort op het internet. Een computer vraagt dit op bij een zogenaamde 'DNS-server' (doorgaans van de internetprovider), die dit eventueel recursief via 'bovengelegen' DNS-servers kan opzoeken.

In de DNS-standaard zijn in de afgelopen jaren tekortkomingen ontdekt die het mogelijk maken voor hackers om deze verwijzingen aan te passen. Kwaadwillenden kunnen gebruikers die op zoek zijn naar een website dan naar een willekeurige web server sturen. Door een nep website op zo'n server te installeren kan vertrouwelijke informatie van de gebruiker worden verkregen, zonder dat de gebruiker dit kan detecteren. Dit is uiteraard zeer onwenselijk.

De standaard DNSSEC maakt het mogelijk om dit te voorkomen door aan een DNS-record een digitale handtekening toe te voegen en deze bij uitwisseling te verifiëren.

SIDN beheert het topleveldomein .NL en heeft DNSSEC aangemeld met twee doeleinden:

- Om te bevorderen dat netwerkapparatuur van de overheid de standaard gaat ondersteunen.
- Om te bevorderen dat domeinen van de Nederlandse overheid voorzien worden van een DNSSEC record, in het bijzonder websites als DigiD, MijnOverheid, etc.

Op een langere termijn zijn gebruikmakend van DNSSEC ook mogelijkheden voor de verbetering van bestaande authenticatiediensten, bijvoorbeeld de PKI-keten (via de in ontwikkeling zijnde standaard 'DANE') en DKIM voor beveiligde e-mail.

DNSSEC kan worden beschouwd als een verzamelnaam voor een aantal samenhangende standaarden, die zijn vastgelegd in zogenaamde RFC's (Request for Comments). Dit betreft:

- RFC 3833 A Threat Analysis of the Domain Name System
- RFC 4033 DNS Security Introduction and Requirements (DNSSEC-bis)
- RFC 4034 Resource Records for the DNS Security Extensions (DNSSEC-bis)
- RFC 4035 Protocol Modifications for the DNS Security Extensions (DNSSEC-bis)
- RFC 4398 Storing Certificates in the Domain Name System (DNS)
- RFC 4470 Minimally Covering NSEC Records and DNSSEC On-line Signing
- RFC 4509 Use of SHA-256 in DNSSEC Delegation Signer (DS) Resource Records (RRs)
- RFC 4641 DNSSEC Operational Practices
- RFC 5155 DNSSEC Hashed Authenticated Denial of Existence
- RFC 5702 Use of SHA-2 Algorithms with RSA in DNSKEY and RSIG Resource Records for DNSSEC.

1.6 Relatie met andere standaarden

Er is een functionele relatie op netwerkniveau met onder meer:

- IPv4 en IPv6
- HTTP en HTTPS
- TLS

Dit zijn belangrijke protocollen die 'bovenop' DNSSEC werken. Met name IPv6 is relevant, aangezien dit via 'pas toe of leg uit' wordt afgedwongen.

Op functioneel niveau is er daarnaast een relatie met DKIM (op dit moment in procedure). Deze standaard maakt het mogelijk om zeker te stellen dat de afzender van een e-mailbericht ook daadwerkelijk toebehoort aan een bepaald domein. Hiervoor worden gegevens uit DNS gebruikt. DNSSEC waarborgt vervolgens dat deze gegevens niet zijn gemanipuleerd.

Tenslotte is er een technische relatie met beveiligingsalgoritmes (voor de beveiliging van de sleutel). Hierbij gaat het o.a. om SHA2 op de lijst met gangbare standaarden.

1.7 Leeswijzer

In hoofdstuk 2 wordt beschreven in welke gevallen de standaard functioneel gezien gebruikt zou moet worden (functioneel toepassingsgebied) en door welke organisaties deze gebruikt zou moeten worden (organisatorisch werkingsgebied).

Om te bepalen of de standaard opgenomen moet worden op de lijst met open standaarden voor 'pas toe of leg uit' zijn deze getoetst aan een viertal door het College Standaardisatie vastgestelde criteria. In hoofdstuk 3 staat het resultaat van deze toetsing. Hoofdstuk 4 bevat een samenvatting van de toets resultaten en het advies van de expertgroep aan het Forum Standaardisatie.

2 Toepassings– en werkingsgebied

Van overheidsorganisaties wordt verwacht dat zij de lijst met open standaarden hanteren bij aanbestedingstrajecten volgens het "pas toe of leg uit"-regime. Afhankelijk van de aan te schaffen functionaliteit zal bepaald moeten worden welke koppelvlakken geïmplementeerd moeten worden, en welke standaarden uit de lijst hiervoor ingezet dienen te worden. Om dit te kunnen doen heeft de expertgroep gekeken in welke gevallen de standaard functioneel gezien gebruik moeten worden (functioneel toepassingsgebied), en door welke organisaties deze gebruikt zou moeten worden (organisatorisch werkingsgebied).

2.1 Functioneel toepassingsgebied

Als functioneel toepassingsgebied wordt voorgesteld:

Systemen en diensten voor:
- **Het registreren en in DNS publiceren van internet-domeinnamen ('signing').**
- **Het vertalen van domeinnamen naar internetadressen en vice versa ('validation enabled resolving').**

Hierbij gelden twee beperkingen:
- **De registratieverplichting geldt enkel indien 'signed domain names' bij een registry van een top-level domein geautomatiseerd aangevraagd kunnen worden.**
- **DNSSEC validatie is niet verplicht voor systemen die niet direct aan het publieke internet gekoppeld zijn (bijvoorbeeld clients/werkplekken binnen een LAN en interne DNS systemen)."**

In eenvoudige termen gesteld:
- Bij het registreren van een domeinnaam zou gekozen moeten worden voor een registratie die door middel van DNSSEC 'ondertekend' is. Hiermee krijgen bezoekers meer zekerheid over de authenticiteit van de pagina / het IP-adres (van de overheid) die men bezoekt.
- Systemen en netwerkdiensten zouden zo moeten zijn ingericht dat ze de ondertekening van sites, indien aanwezig, controleren. Hiermee wordt voorkomen dat gebruikers binnen een overheidsorganisatie terecht komen op een vervalste website

Er zijn uit praktisch oogpunt een aantal beperkingen opgenomen:
- Hoewel voor de meeste 'top level' domeinen een ondertekende domeinnaam kan worden aangevraagd, wordt dit voor sommige top level domeinnamen nog niet ondersteund. Voor deze domeinnamen zou de verplichting dan ook niet moeten gelden.

  Daarbij gaat het ondermeer om de domeinnamen van de andere landen in het koninkrijk en de bijzondere Nederlandse gemeenten in de Antillen:

  .an – voormalige Nederlandse Antillen
  .aw – Aruba

.cw – Curaçao
.sx – Sint Maarten (Nederlands deel)

Voor het top level domein .bq – Bonaire, Sint Eustatius en Saba – geldt dat hiervoor nog geen domeinnamen aangevraagd kunnen worden. DNSSEC is daarbij dan ook nog niet aan de orde.

- Niet in alle gevallen kan een ondertekening automatisch worden uitgevoerd en worden onderhouden tussen de registrar (degene die de registratie uitvoert) en de registry (de beheerder van het top-level domein). Er zijn dan handmatige handelingen nodig, wat registratie en bijhouden complexer maakt.

  Voor het .NL-domein is de verwachting dat de automatische verwerking vanaf het tweede kwartaal 2012 beschikbaar is bij SIDN. De verplichting voor 'pas toe of leg uit' voor het .NL-domein geldt dan ook pas zodra deze automatische verwerking beschikbaar is.

- Er zijn verschillende stappen in de keten waar DNSSEC validatie kan plaatsvinden. Dit kan bijvoorbeeld plaatsvinden op de lokale werkplek, in het lokale netwerk of op de server van de provider. In de meest ideale situatie vindt DNSSEC validatie in al deze schakels plaats. Er zijn dan echter veel situaties waar deze validatie extra complexiteit met zich meebrengt, terwijl de betrouwbaarheidswinst minimaal is. Zo is het valideren met DNSSEC op de werkplek nog geen gemeengoed. Zo controleert de browser Chrome op dit moment DNSSEC automatisch, Internet Explorer nog niet en Firefox enkel met een plugin.

  Daarom stelt de expertgroep voor om de DNSSEC validatie enkel te verplichten in die situaties waar er sprake is van een netwerkelement dat een verbinding verzorgt met het publieke internet. Denk bijvoorbeeld aan de centrale DNS-server van een organisatie. Achter dit netwerkelement kunnen meerdere interne netwerkelementen zitten (waaronder lokale werkplekken). Voor deze interne netwerkelementen geldt dat DNSSEC optioneel is.

2.2 Organisatorisch werkingsgebied

De expertgroep adviseert om het organisatorisch werkingsgebied overeen te laten komen met het werkingsgebied, waarop het 'pas toe of leg uit' principe van toepassing is, te weten:

Overheden (Rijk, provincies, gemeenten en waterschappen) en instellingen uit de (semi-) publieke sector.

3 Toetsing van standaard aan criteria

Om te bepalen of de standaard opgenomen moet worden op de lijst met open standaarden zijn deze getoetst aan een aantal criteria. Er zijn vier hoofdcriteria:

1. Open standaardisatieproces
2. Toegevoegde waarde
3. Draagvlak
4. Opname bevordert adoptie

Deze criteria staan beschreven in het rapport, *"Toetsingsprocedure en criteria voor lijsten met open standaarden"* [3] en staan op de website www.forumstandaardisatie.nl. Het resultaat van de toetsing zal in dit hoofdstuk per criterium beschreven worden. Voor de volledigheid is tevens de definitie van elk criterium opgenomen (in een kader).

3.1 Open standaardisatieproces

De ontwikkeling en het beheer van de standaard zijn op een open, onafhankelijke, toegankelijke, inzichtelijke, zorgvuldige en duurzame wijze ingericht.

3.1.1 Is de documentatie voor een ieder drempelvrij beschikbaar?

Is het specificatiedocument beschikbaar zonder dat er sprake is van onacceptabele belemmeringen (zoals te hoge kosten en te hoge lidmaatschapseisen)?

Ontwikkelingen van DNSSEC worden beheerd door de Internet Engineering Task Force (IETF). De IETF is een grote, internationale, open community van netwerk ontwikkelaars, beheerders, vendors, en onderzoekers die zich bezig houdt met de ontwikkeling van de Internet architectuur, en de werking van het Internet. IETF is toegankelijk voor elke geïnteresseerde individu. Alle specificaties met betrekking tot DNSSEC zijn kosteloos beschikbaar als RFC documenten via de website van de IETF (http://www.ietf.org/)

Is de documentatie over het ontwikkel- en beheerproces (bijv. het voorlopige specificatiedocument, notulen en beschrijving besluitvormingsprocedure) beschikbaar zonder dat er sprake is van onacceptabele belemmeringen (zoals te hoge kosten en te hoge lidmaatschapseisen)?

De standaarden zijn ontwikkeld door de DNSEXT werkgroep van de IETF; verslagen van alle overleggen zijn vrij beschikbaar via de website van de IETF (http://www.ietf.org/).

3.1.2 Is het intellectuele eigendomsrecht voor eenieder beschikbaar, zodat de standaard vrij implementeerbaar en te gebruiken is

Stelt de standaardisatieorganisatie het intellectueel eigendomsrecht op de standaard m.b.t. bijvoorbeeld eventuele patenten- onherroepelijk royalty-free voor eenieder beschikbaar?

De IETF Policy geeft geen garanties met betrekking tot IPR, maar eenieder die mee-ontwikkelt aan de standaard moet IPR aanmelden. Er is voor DNSSEC geen claim op IPR en er zijn meerdere open source-implementaties.

Garandeert de standaardisatieorganisatie dat partijen die bijdragen aan de ontwikkeling van de standaard hun intellectueel eigendomsrecht onherroepelijk royalty-free voor eenieder beschikbaar stellen?

De rechten en plichten van RFC auteurs en de daaruit voortvloeiende vrije beschikbaarheid van de standaard wordt vastgesteld in RFC 5378 (http://tools.ietf.org/html/rfc5378).

3.1.3 Is de inspraak van eenieder in voldoende mate geborgd?

Is het besluitvormingsproces toegankelijk voor alle belanghebbenden (bijv. gebruikers, leveranciers, adviseurs, wetenschappers)?

De IETF is open en drempelloos, het staat een ieder vrij om deel te nemen in het standaardisatie- en besluitvormingsproces (zie bijv. http://www.ietf.org/newcomers.html).

Vindt besluitvorming plaats op een wijze die zoveel mogelijk recht doet aan de verschillende belangen?

De IETF heeft een lange traditie van "rough consensus"; een grote meerderheid moet het eens zijn met een besluit voor het genomen wordt. Voor diepgaande informatie zie http://www.ietf.org/tao.html

Kan een belanghebbende formeel bezwaar aantekenen tegen de gevolgde procedure?

Binnen de werkgroepen kunnen bezwaren kenbaar gemaakt worden. Ook buiten de werkgroepen om kunnen bezwaren gemeld worden aan Internet Engineering Steering Group (IESG) stuurgroep-leden.

Organiseert de standaardisatieorganisatie regelmatig overleggen met belanghebbenden over doorontwikkeling en beheer van de standaard? (geen harde voorwaarde)

De IETF organiseert jaarlijks 3 open bijeenkomsten, telkens op een andere locatie wereldwijd. De volgende IETF is in Parijs van 25-30 maart 2012. Daarnaast is er een rijke traditie aan mailinglists en andere informele communicatiekanalen zoals Jabber.

Organiseert de standaardisatieorganisatie een publieke consultatie voordat (een nieuwe versie van) de standaard wordt vastgesteld? (geen harde voorwaarde)

Voordat een nieuwe RFC geaccordeerd wordt is er een open comments proces georganiseerd door de relevante werkgroep (in het geval van DNSSEC is dat de DNSEXT werkgroep).

3.1.4 Is de standaardisatieorganisatie onafhankelijk en duurzaam?

Is de ontwikkeling en het beheer van de standaard belegd bij een onafhankelijke non-profit standaardisatieorganisatie?

De IETF Trust is een non-profit organisatie onder Amerikaans recht in de staat Virginia (zie http://iaoc.ietf.org/docs/TrustFAQv1.2.txt).

Is de financiering van de ontwikkeling en het onderhoud van de standaard voor tenminste drie jaar gegarandeerd?

De continuïteit van de IETF wordt gegarandeerd door ISOC, de Internet Society, een wereldwijd genootschap met veel profit en non-profit leden. Daarnaast is de werkgroep waar de DNSSEC standaard onder valt actief en gezond met leden van diverse belangrijke en kapitaalkrachtige spelers op het wereldwijde internet.

3.1.5 Is het (versie) beheer van de standaard goed geregeld?

Heeft de standaardisatieorganisatie gepubliceerd beleid met betrekking tot versiebeheer van de standaard? (met o.a. aandacht voor migratie van gebruikers)

Er is binnen IETF veel aandacht voor operationele aspecten, zie onder andere http://www.ietf.org/about/process-docs.html. In 1.3 en 1.4 is aangetoond dat het standaardisatieproces open, eerlijk, onafhankelijk en duurzaam is.

3.1.6 Conclusie

DNSSEC is gestandaardiseerd binnen de IETF (Internet Engineering Task Force). Het standaardisatieproces van de IETF voldoet aan de gestelde open standaardisatie criteria. Specifiek voor de DNSSEC standaard zijn geen IPR claims bekend bij de experts.

3.2 Toegevoegde waarde

De interoperabiliteitswinst en andere voordelen van adoptie van de standaard wegen overheidsbreed en maatschappelijk op tegen de risico's en nadelen.

3.2.1 Is het toepassings- en werkingsgebied van de aanmelding goed gedefinieerd?

Is het functioneel toepassingsgebied goed gedefinieerd?

Is het organisatorisch werkingsgebied goed gedefinieerd?

Zie het vorige hoofdstuk.

Is de standaard generiek toepasbaar en niet alleen bedoeld voor gegevensuitwisseling met één of een beperkt aantal specifieke voorzieningen?

DNSSEC is een uitbreiding op het DNS protocol, wat aan de basis ligt van het internet. DNSSEC is niet geschreven voor specifieke toepassing maar heeft het generieke doel om vertrouwen toe te voegen aan het bestaande DNS protocol.

3.2.2 Verhoudt de standaard zich goed tot andere standaarden?

Kan de standaard naast of in combinatie met reeds opgenomen standaarden worden toegepast (d.w.z. de standaard conflicteert niet met reeds opgenomen standaarden)?

DNSSEC is backward compatible met DNS; dat wil zeggen: DNS servers die geen notie hebben van DNSSEC zullen geen "last" hebben van DNSSEC. Kanttekening hierbij is wel dat bepaalde achterhaalde praktijken, zoals bijv. het blokkeren van TCP voor DNS op firewalls of het tegenhouden van DNS berichten groter dan 512 bytes dan wel gefragmenteerde DNS berichten kan leiden tot problemen in communicatie en dat dit dus aandacht behoeft bij gebruik van DNSSEC. Hierover is voldoende publiek beschikbare documentatie te vinden op internet en het mag dan ook als bekend worden verondersteld hoe hier correct mee om te gaan [4].

Biedt de aangemelde standaard meerwaarde boven reeds opgenomen standaarden met een overlappend functioneel toepassings- en organisatorisch werkingsgebied? (Dit kan ook om een nieuwe versie van dezelfde standaard gaan.)

DNSSEC is een uitbreiding op DNS en voegt hieraan integriteit en vertrouwen toe; in tegenstelling tot bij traditionele DNS is het met DNSSEC mogelijk om vast te stellen dat een DNS antwoord betrouwbaar en ongewijzigd gegeven is door de beheerder van een domein. Hiermee wordt falsificatie van DNS antwoorden m.b.v. het zogenoemde "cache poisoning" effectief voorkomen. Daarnaast is DNSSEC een "enabling technology" die het in de toekomst mogelijk maakt om additionele

informatie op te nemen in DNS die vereist dat de integriteit en betrouwbaarheid van DNS antwoorden gegarandeerd is (bijv. het DANE initiatief waarbij informatie over PKI certificaten in DNS wordt opgenomen)

Biedt de aangemelde standaard meerwaarde boven bestaande concurrerende standaarden die in aanmerking zouden kunnen komen voor opname?

DNSSEC is een algemeen geaccepteerde (want breed ingevoerd en ondersteund door de IETF) standaard waarvan bovendien meerdere open implementaties beschikbaar zijn. De enige gerelateerde standaard, DNSCurve (http://dnscurve.org), is (nog) niet als open standaard beschikbaar en voldoet bovendien niet aan de eis dat er meerdere algemeen beschikbare en geaccepteerde open implementaties van beschikbaar zijn.

Is de standaard een internationale standaard of sluit de standaard aan bij relevante internationale standaarden?

DNSSEC is een internationale standaard, ontwikkeld en beheerd door de internationale non-profit organisatie IEFT. DNSSEC kan worden gezien als een bouwsteen in een internet security architectuur, en biedt een goede basis voor andere standaarden zoals DKIM en DANE.

Draagt de standaard voldoende bij aan interoperabiliteit zonder dat aanvullende standaardisatieafspraken (zoals lokale profielen) noodzakelijk zijn?

DNSSEC is backward compatible en is een uitbreiding op de huidig gebruikte DNS standaard. In tegenstelling tot traditioneel DNS is het met DNSSEC mogelijk om vast te stellen dat een DNS antwoord betrouwbaar en ongewijzigd gegeven is door de beheerder van een domein. DNSSEC voegt authenticiteit toe aan berichtenuitwisseling en daarmee meer vertrouwen in interoperabiliteit. Daarvoor kan DNSSEC worden geadopteerd zonder dat aanvullende standaardisatieafspraken (zoals profielen) noodzakelijk zijn.

3.2.3 Wegen de kwantitatieve en kwalitatieve voordelen van adoptie van de standaard, voor de (semi-)overheid als geheel en voor de maatschappij, op tegen de nadelen?

Draagt de adoptie van de standaard bij aan de oplossing van een bestaand, relevant interoperabiliteitsprobleem?

Het is reeds lange tijd (sinds de jaren ‘90 van de vorige eeuw) bekend dat DNS kwetsbaar is voor falsificatie van antwoorden. Meer recent is gebleken dat dit ook in de praktijk misbruikt wordt. DNSSEC biedt hier een oplossing voor door het toepassen van digitale handtekeningen aan de kant van de beheerder van DNS zones die te controleren zijn door clients die DNS antwoorden opvragen. Hierdoor draagt de standaard bij aan een betere structurele beveiliging van Internet Infrastructuur.

Draagt de standaard bij aan het voorkomen van een vendor lock-in (leveranciersafhankelijkheid)?

Van vendor lock-in met betrekking tot DNS producten is geen sprake, omdat de meest gebruikte producten zijn vrij beschikbaar zijn. DNSSEC wijzigt hier weinig aan. Het aanbod van managed DNS diensten zonder DNSSEC is nog wel uitgebreider, dan met DNSSEC. Naar verwachting zal het DNSSEC aanbod - net als in andere landen - toenemen. DNSSEC veroorzaakt dus ook geen vendor lock-in aangezien er meerdere open implementaties van hoge kwaliteit beschikbaar zijn.

Wegen de overheidsbrede en maatschappelijke baten voor de informatievoorziening en de bedrijfsvoering op tegen de kosten?

DNSSEC *validatie* is zonder noemenswaardige kosten in te voeren (zie ook [4] voor uitgebreidere argumentatie). Vaak kan volstaan worden met het aanvinken van enkele opties in de software.

DNSSEC *signing* brengt ontegenzeggelijk kosten met zeg mee, en zal - zeker in het begin - leiden tot hogere operationele kosten:

- Indien het gaat om een extern gehoste website zal de provider mogelijk (beperkte) meerkosten in rekening brengen voor het in stand houden van de registratie.
- Daar waar het gaat om DNS-registraties die verwijzen naar de eigen infrastructuur (intern gehoste servers), dan zal er meer tijd gaan zitten in het zorgvuldig opzetten en beheren van de registraties.

Deze beperkte extra operationele kosten wegen echter ruimschoots op tegen de baten. Deze baten liggen in een verhoogd vertrouwen in de echtheid van de bezochte (overheids-)website. Gezien het vaak vertrouwelijke karakter van overheidsdienstverlening op internet is dit vertrouwen van onschatbare waarde.

De waarde neemt over de tijd toe wanneer meer partijen hun DNS registratie ondertekenen met DNSSEC en internetproviders hierop gaan valideren. Dit is al het geval bij een aantal toonaangevende providers zoals T-Mobile, XS4ALL, BIT en doelgroepnetwerken zoals SURFnet).

Aanvankelijk kan invoering van DNSSEC (net als elke andere technologie) ook gepaard gaan met technische / configuratie issues die tot verstoring van berichtuitwisseling leiden. Dit is echter een operationeel aspect dat los staat van de open standaard en waarvan het risico wordt ingeschat als niet groter dan voor andere technologie, zoals bijv. IPv6.

Gezien het grote belang van een betrouwbaar internetverkeer verplicht de Amerikaanse overheid het gebruik van DNSSEC al sinds geruime tijd voor overheidssites binnen het .gov-domein [5].

Zijn de beveiligingsrisico's aan overheidsbrede adoptie van de standaard acceptabel?

DNSSEC biedt toegevoegde waarde door vertrouwen toe te voegen aan DNS; het enige echt relevante beveiligingsrisico dat DNSSEC met zich meebrengt is dat het zgn. Distributed Denial of Service (DDoS) aanvallen op basis van "DNS amplificatie" makkelijker maakt. De waarde die

DNSSEC biedt door het toevoegen van vertrouwen weegt zwaarder dan dit toegenomen risico. Bovendien: een Denial of Service (DoS; non-distributed) aanval kan met DNSSEC worden voorkomen. Door adoptie van DNSSEC verbetert de beveiliging van berichtenuitwisseling door het wegnemen van één van de huidige kwetsbaarheden.

Zijn de privacyrisico's aan overheidsbrede adoptie van de standaard acceptabel?

Er zijn mogelijke privacy risico's indien gebruik wordt gemaakt van de zgn. "NSEC" variant van DNSSEC (bij gebruikmaking hiervan is het triviaal voor derden om de volledige inhoud van een DNS zone op te vragen). Het is echter ook goed mogelijk om dit voor te zijn door gebruik te maken van de "NSEC3" variant die het met gebruikmaking van cryptografische technieken moeilijker zo niet onmogelijk maakt om dit te doen. Daarom zal naar verwachting invoering van de standaard geen consequenties hebben voor privacy van personen.

3.2.4 Conclusie

De expertgroep meent dat de voordelen van DNSSEC opwegen tegen de extra kosten die gemaakt moeten worden.

De voordelen zitten vooral op het vlak van een betere betrouwbaarheid van overheidswebsites. De kans op door kwaadwillenden vervalste overheidswebsites neemt door het gebruik van DNSSEC af. Naarmate meer schakels in de keten voorzien zijn van DNSSEC nemen deze voordelen toe.

Er zijn geen voor de hand liggende alternatieven voor de standaard.

3.3 Draagvlak

Aanbieders en gebruikers moeten voldoende ervaring hebben bij het ondersteunen, implementeren en gebruiken van de standaard.

3.3.1 Bestaat er voldoende marktondersteuning voor de standaard?

Bieden meerdere leveranciers ondersteuning voor de standaard?

Er zijn een groot aantal concurrerende open implementaties van DNSSEC beschikbaar (bv. BIND, Unbound, NSD, PowerDNSSEC, OpenDNSSEC, etc.). Daarnaast zijn er ook een groot aantal commerciële leveranciers die DNSSEC ondersteunen (bv. Xelerance, Secure64, BlueCat, Men & Mice, InfoBlox, Microsoft, etc.). DNS producten (resolvers, authoritatieve servers) zijn dus ruim voldoende beschikbaar.

Management tooling (b.v. ten behoeve van signing) is ook aanwezig en wordt verder ontwikkeld.

In de hoek van managed DNS services is DNSSEC ondersteuning nog niet ver, maar zal naar verwachting ontwikkelen net als in andere landen waar DNSSEC al eerder geïntroduceerd is. Het tempo hiervan hangt af van adoptie van DNSSEC door het grote aantal stakeholders. Juist hierin kan de "pas toe of leg uit" lijst een rol spelen.

Kan een gebruiker de conformiteit van de implementatie van de standaard (laten) toetsen?

Er zijn diverse eenvoudige tools om DNSSEC werking op hoofdlijn te toetsen.

3.3.2 Kan de standaard rekenen op voldoende draagvlak?

Wordt de aangemelde versie van de standaard binnen het organisatorische werkingsgebied door meerdere organisaties gebruikt?

DNSSEC in de huidige vorm wordt door een groot aantal top-level domeinen en door de root zone van het internet gebruikt. Daarnaast wordt de standaard ook in Nederland toegepast door partijen als SURFnet, SIDN, NLnet Labs, T-Mobile, XS4ALL, BIT, de Universiteit van Tilburg, de Erasmus Universiteit, etc.

Recentelijk heeft GovCert via het NCSC ook DNSSEC opgenomen op haar lijst van mogelijkheden ter beveiliging van webapplicaties [6]

Wordt een vorige versie van de standaard binnen het organisatorische werkingsgebied door meerdere organisaties gebruikt?

Er worden verscheidene signing algoritmes gebruikt en bijv. de NSEC en NSEC3 varianten van de standaard. Alle gangbare implementaties ondersteunen de standaard in volledige breedte en zullen hier geen moeite mee hebben. Oudere, experimentele versies van de standaard worden in praktijk niet (meer) gebruikt.

Is de aangemelde versie backwards compatible met eerdere versies van de standaard?

DNSSEC is backward compatible met de originele DNS standaard uit 1983.

Zijn er voldoende positieve signalen over toekomstige gebruik van de standaard door (semi-)overheidsorganisaties, het bedrijfsleven en burgers?

DNSSEC wordt reeds toegepast in het (semi-)publieke domein en in de commerciële markt. Er dienen nog wel 'hindernissen' in de adoptie van de standaard genomen te worden, maar dat lijkt op dit moment meer een kwestie van tijd dan dat het onoverkomelijke business of technische hindernissen zijn. Kijkend naar adoptie in het buitenland zal toekomstig gebruik ook in Nederland gaan toenemen.

3.3.3 Conclusie

Er is wereldwijd draagvlak voor DNSSEC onder relevante belanghebbende groepen. De Amerikaanse overheid heeft reeds enkele jaren geleden het beleidsbesluit genomen om DNSSEC toe te passen voor domeinen onder het top-level domein van de federale overheid (.gov). In de verdere adoptie is nog wel stimulans nodig, temeer omdat de meerwaarde stijgt naar mate de adoptiegraad toeneemt.

3.4 Opname bevordert adoptie

De opname op de lijst is een geschikt middel om de adoptie van de standaard te bevorderen.

Er zijn twee lijsten: de lijst met gangbare standaarden en de lijst voor 'pas toe of leg uit'. Deze laatste lijst is bedoeld om standaarden een extra stimulans te geven wanneer:
1. Hun huidige adoptie binnen de (semi-)overheid beperkt is;
2. Opname bijdraagt aan de adoptie door te stimuleren o.b.v. het 'pas toe of leg uit' regime.

De lijst met gangbare standaarden vormt een referentie voor standaarden die veel gebruikt worden. Als standaarden voldoen aan enkele basisvoorwaarden (voor o.a. openheid), er is geen discussie over en de standaarden worden breed gebruikt, dan vindt opname op die lijst plaats.

Voor DNSSEC geldt dat een opname op de lijst voor 'pas toe of leg uit' wordt voorzien.

3.4.1 Is de "pas toe of leg uit"-lijst het passende middel om de adoptie van de standaard binnen de (semi)overheid te bevorderen?

DNSSEC is een enabling technology; de mogelijkheden om bv. DNSSEC in te zetten om via een alternatieve weg trust establishment in certificaten (PKI) te regelen (beter bekend als het DANE initiatief) zijn alleen realistisch indien er een goede DNSSEC uitrol is gerealiseerd. Dit is dan zowel van waarde voor de overheid als voor burgers en bedrijven die van overheidsdiensten gebruik maken. Zonder een serieuze aanmoediging, zoals de "pas toe of leg uit" lijst is het niet waarschijnlijk dat een DNSSEC uitrol van voldoende omvang binnen redelijke tijd tot stand komt om direct van dit soort state-of-the-art ontwikkelingen te kunnen profiteren. DNSSEC heeft dus een steuntje in de rug nodig om een kritieke massa te bereiken. Gezien het belang van beveiliging van DNS en het gebrek aan adoptie, dient de standaard op de lijst te komen.

3.4.2 Zijn er naast opname op de lijst aanvullende adoptiemaatregelen nodig?

De toepassing van DNSSEC maakt een correct gebruik van DNS belangrijk. Daar waar het huidige DNS-systeem een fout van een systeembeheerder toelaat, is dit bij DNSSEC veel minder het geval. Een recent voorbeeld, waarbij door een fout van een beheerder de website van NASA.gov niet langer beschikbaar was [7], illustreert dit.

Overheidsorganisaties zullen dus zeer bewust DNSSEC moeten gaan inzetten. De expertgroep acht het wenselijk dat er een handreiking komt met praktische tips en aandachtspunten. Dit verlaagt de drempel tot adoptie en draagt bij aan een groter gebruik in de praktijk.

Een dergelijke handreiking zou in moeten gaan op ondermeer de volgende aspecten:

- de implicaties van toevoegen van DNSSEC op het domeinnaam registratiebeleid, de DNS architectuur en beheerprocessen bij de digitale overheid;
- formulering van eisen m.b.t. DNSSEC in aanbestedingen;
- aandachtspunten bij initiële configuratie van DNSSEC;
- aandachtspunten bij reguliere beheer van DNSSEC (specifiek key roll-over beleid)

Als basis voor deze handleiding is in ruime mate best-practice materiaal publiek beschikbaar. [8]

3.4.3 Is de inzet van aanvullende adoptie-instrumenten (communicatief, financieel, juridisch), door andere partijen dan het Forum/College Standaardisatie, noodzakelijk?

Semi-publieke partijen als SURFnet en SIDN communiceren al op vrij brede schaal over de technologie wat in ieder geval zorgt voor voldoende beschikbare informatie. Daarnaast is ook GOVCERT.NL (opgegaan in het Nationaal CyberSecurity Centre) actief geweest in het communiceren over DNSSEC en beschikken zij over de nodige expertise. Het is voorstelbaar dat experts van deze (semi-)publieke partijen door middel van een bijdrage leveren aan de in de vorige paragraaf gesuggereerde handreiking.

3.4.4 Kan een uitgebreid adoptieadvies van het Forum Standaardisatie helpen bij het wegnemen van knelpunten in de adoptie?

DNSSEC opereert, net als DNS en IPv4 / IPv6 onder de motorkap, onttrokken aan het zicht van de gemiddelde gebruiker. Daar vervult het een belangrijke rol, maar die is lastig uit te leggen. Bovendien is er sprake van een 'kip-ei' situatie; waarom zou ik signeren als er toch niemand valideert?

Een verplichting via 'pas toe of leg uit' en een handreiking voor overheidsorganisatie zullen zeker een stimulans voor adoptie van DNSSEC zijn en kunnen de vicieuze cirkel te doorbreken.

3.4.5 Conclusie

Het DNS-systeem wordt door invoering van DNSSEC weliswaar veiliger, maar ook complexer en gevoeliger voor fouten door systeembeheerders. Dit is een potentiële drempel voor de adoptie.

Het is daarom wenselijk dat er – naast opname van de standaard op de lijst voor 'pas toe of leg uit' - een handreiking komt voor overheidsorganisaties m.b.t. de inzet van DNSSEC. Deze handreiking moet overheidsorganisaties helpen om te gaan met invoering van de standaard.

4 Advies aan Forum en College

4.1 Samenvatting van de toetsingscriteria

Samengevat is het oordeel op de toetsingscriteria als volgt:

4.1.1 *Open standaardisatieproces*
DNSSEC is gestandaardiseerd binnen de IETF (Internet Engineering Task Force). Het standaardisatieproces van de IETF voldoet aan de gestelde open standaardisatie criteria. Specifiek voor de DNSSEC standaard zijn geen IPR claims bekend bij de experts.

4.1.2 *Toegevoegde waarde*
De expertgroep meent dat de voordelen van DNSSEC opwegen tegen de extra kosten die gemaakt moeten worden. De voordelen zitten vooral op het vlak van een betere betrouwbaarheid van overheidswebsites. De kans op door kwaadwillenden vervalste overheidswebsites neemt door het gebruik van DNSSEC af. Naarmate meer schakels in de keten voorzien zijn van DNSSEC nemen deze voordelen toe. Er zijn geen voor de hand liggende alternatieven voor de standaard.

4.1.3 *Draagvlak*
Er is wereldwijd draagvlak voor DNSSEC onder relevante belanghebbende groepen. De Amerikaanse overheid heeft reeds enkele jaren geleden het beleidsbesluit genomen om DNSSEC toe te passen voor domeinen onder het top-level domein van de federale overheid (.gov). In de verdere adoptie is nog wel stimulans nodig, temeer omdat de meerwaarde stijgt naar mate de adoptiegraad toeneemt.

4.1.4 *Opname bevordert adoptie*
Het DNS-systeem wordt door invoering van DNSSEC weliswaar veiliger, maar ook complexer en gevoeliger voor fouten door systeembeheerders. Dit is een potentiële drempel voor de adoptie.

Het is daarom wenselijk dat er naast opname van de standaard op de lijst voor 'pas toe of leg uit' - een handreiking komt voor overheidsorganisaties m.b.t. de inzet van DNSSEC. Deze handreiking moet overheidsorganisaties helpen om te gaan met invoering van de standaard.

4.2 Advies aan Forum en College

Voeg DNSSEC toe aan de "pas toe of leg uit" lijst.

Met als toepassingsgebied:

Systemen en diensten voor:
- *Het registreren en in DNS publiceren van internet-domeinnamen ('signing').*
- *Het vertalen van domeinnamen naar internetadressen en vice versa ('validation enabled resolving').*

Hierbij gelden twee beperkingen:
- *De registratieverplichting geldt enkel indien 'signed domain names' bij een registry van een top-level domein geautomatiseerd aangevraagd kunnen worden.*
- *DNSSEC validatie is niet verplicht voor systemen die niet direct aan het publieke internet gekoppeld zijn (bijvoorbeeld clients/werkplekken binnen een LAN en interne DNS systemen).*

En als werkingsgebied:

Overheden (Rijk, provincies, gemeenten en waterschappen) en instellingen uit de (semi-) publieke sector.

4.3 Aanbevelingen ten aanzien van de adoptie van de standaard

DNSSEC is een beveiligingstoevoeging aan de gangbare DNS systemen en diensten. Deze toevoeging vergt een secure werkwijze bij de invoering en extra beheerhandelingen.

Om de drempel te verlagen is het wenselijk dat er een handreiking komt voor overheidsorganisaties, die hen helpt bij deze invoering. Deze handreiking zou moeten ingaan op
- de implicaties van toevoegen van DNSSEC op het domeinnaam registratiebeleid, de DNS architectuur en beheerprocessen bij de digitale overheid;
- formulering van eisen m.b.t. DNSSEC in aanbestedingen;
- aandachtspunten bij initiële configuratie van DNSSEC;
- aandachtspunten bij reguliere beheer van DNSSEC (specifiek key roll-over beleid)

Als basis voor deze handleiding is in ruime mate best-practice materiaal publiek beschikbaar.

5 Referenties

[1] "Pas toe of leg uit" is vastgelegd in de "Instructie rijksdienst bijaanschaf ICT-diensten of ICT-producten" van 8 november 2008, en daarnaast in convenanten en afspraken met decentrale overheden. Zie: http://www.open-standaarden.nl/open-standaarden/het-pas-toe-of-leg-uit-principe/

[2] " Instellingsbesluit College en Forum Standaardisatie 2010". Zie: https://zoek.officielebekendmakingen.nl/stcrt-2010-4499.html

[3] Criteria en procedure voor 'pas toe of leg uit', vastgesteld door het College Standaardisatie op 23 juni 2011. Zie: http://www.forumstandaardisatie.nl/fileadmin/os/images/Toetsingsprocedure_en_criteria_v1_0.pdf

[4] Zie bijvoorbeeld: http://www.surfnet.nl/Documents/rapport_201106_DeployingDNSSECvalidationv10.pdf

[5] Executive Office Of The President
Office Of Management And Budget - Memorandum for chief information officers. Zie: http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2008/m08-23.pdf

[6] NCSC beveiligingsrichtlijnen, zie: https://www.ncsc.nl/actueel/nieuwsberichten/ict--beveiligingsrichtlijnen.html

[7] DNSSEC, Comcast en NASA.gov, zie: http://www.dnssec.comcast.net/DNSSEC_Validation_Failure_NASAGOV_20120118_FINAL.pdf

[8] Bijvoorbeeld handreikingen van NIST, zie: http://csrc.nist.gov/publications/nistpubs/800-81r1/sp-800-81r1.pdf