CS-20120615.06D

notitie

Opname DNSSEC op de lijst voor 'pas toe of leg uit'

Forum Standaardisatie

Wilhelmina v Pruisenweg 52
2595 AN Den Haag
Postbus 96810
2509 JEDen Haag
www.forumstandaardisatie.nl

FORUM STANDAARDISATIE

Agendapunt:	6. Open Standaarden		
Bijlagen:	Expertadvies en consultatiereacties		
Aan:	College Standaardisatie		
Van:	Forum Standaardisatie		
Datum:	23 mei 2012	**Versie**	1.0
Betreft:	Opname DNSSEC op de lijst voor 'pas toe of leg uit'		

Waarom is een keuze belangrijk?
Domain Name System (DNS) wordt gebruikt om internet-domeinnamen (bijv. 'www.rijksoverheid.nl') te koppelen aan IP-adressen (bijv. 94.228.135.80). DNS wordt daarom vaak het 'telefoonboek van internet' genoemd. DNS kent een kwetsbaarheid die het mogelijk maakt dat een kwaadwillende een domeinnaam koppelt aan een ander IP-adres. Gebruikers kunnen hierdoor worden misleid naar een frauduleuze website. De standaard DNS Security Extensions (DNSSEC) neemt deze kwetsbaarheid weg. DNSSEC voegt daarvoor aan DNS-registraties een digitale handtekening toe. Deze handtekening kan dan door de bevragende partij (de bezoeker van de website) worden geverifieerd. DNSSEC zorgt voor een beter beveiligd fundament van het internet. De standaard draagt ertoe bij dat identiteitsfraude en internetdiefstal inclusief bijbehorende kosten beter kunnen worden voorkomen. Buitenlandse overheden (o.a. USA en Zweden) bevorderen het gebruik reeds. Opname op de 'pas toe of leg uit'-lijst zorgt ervoor dat Nederlandse overheden zullen investeren in systemen die overweg kunnen met DNSSEC en daarmee zal de adoptie van DNSSEC in Nederland worden bevorderd.

Waarom kunt u met een 'gerust hart' ja zeggen?
Op 27 januari 2012 is een expertgroep met vertegenwoordigers uit het bedrijfsleven en overheid bijeen gekomen. Op basis van de discussie tijdens de bijeenkomst en schriftelijke input van een tweetal andere experts is het expertadvies opgesteld. De experts concludeerden dat DNSSEC voldoet aan de toetsingscriteria die College Standaardisatie hanteert. Het expertadvies is publiekelijk geconsulteerd hetgeen heeft geleid tot een zevental reacties. Een vijftal respondenten onderschrijft de opname en één respondent plaatst een aantal opmerkingen. Een respondent (BKWI) stelt dat zij DNSSEC wel graag op de lijst ziet, maar met een nog breder toepassingsgebied. Deze reacties zijn betrokken bij de opstelling van dit Forumadvies

Zijn er risico's verbonden aan de keuze?
Het DNS-systeem wordt door invoering van DNSSEC weliswaar veiliger, maar ook complexer en gevoeliger voor fouten door systeembeheerders. Het risico bestaat dat websites door fouten niet meer bereikbaar zijn. Om de invoering goed te laten verlopen en de kosten te minimaliseren adviseert het Forum om validatie van domeinnamen alleen verplicht te stellen voor systemen die direct aan het publieke internet gekoppeld zijn, terwijl de signing verplichting van domeinnamen alleen geldt als deze geautomatiseerd aangevraagd kunnen worden. Daarnaast wordt opgeroepen tot het opstellen van een handreiking.

Beslispunt

Het College Standaardisatie wordt gevraagd in te stemmen met:

Datum
23 mei 2012

1. de opname van DNSSEC op de lijst voor 'pas toe of leg uit',
2. het functionele toepassingsgebied:
   "*Systemen en diensten voor:*
   - *Het registreren en in DNS publiceren van internet-domeinnamen ('signing'). De registratieverplichting geldt enkel indien 'signed domain names' bij een registerhouder van een top-level domein (zoals SIDN voor .NL) geautomatiseerd aangevraagd kunnen worden; (NB. dit is sinds 15 mei het geval)*
   - *Het vertalen van domeinnamen naar internetadressen en vice versa ('validation enabled resolving'). 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)."*
3. het organisatorische werkingsgebied:
   "Overheden (Rijk, provincies, gemeenten en waterschappen) en instellingen uit de (semi-) publieke sector";

4. de additionele adviezen ten aanzien van de adoptie van de standaard:
   - het oproepen van het "DNSSEC.nl platform" en het Nationaal Cyber Security Centrum (NCSC) om gezamenlijk een handreiking te ontwikkelen voor overheidsorganisaties ter ondersteuning van de invoering en het beheer van DNSSEC.
   - het oproepen van het NCSC om in de "ICT-Beveiligingsrichtlijnen voor webapplicaties" uitgebreider stil te staan bij DNSSEC en een heldere richtlijn voor het gebruik van DNSSEC op te stellen.
   - het oproepen van de verantwoordelijke ministeries om hun domeinen z.s.m., conform het besluit van het ICBR[1], door de Dienst Publiek en Communicatie van Min. AZ te laten registeren en beheren. Hiermee is ondersteuning van DNSSEC voor die domeinen gegarandeerd en is bovendien het beheer van Rijksdomeinen in handen van een centrale gespecialiseerde partij.

Reikwijdte 'pas toe of leg uit' regime

Het 'pas toe of leg uit' regime heeft betrekking op de aanschaf van producenten of diensten waarbij de betreffende standaarden toegepast kunnen worden. Dit betekent concreet dat overheidsorganisaties worden opgeroepen om bij de aanschaf van nieuwe hard- en software (en eventuele bijbehorende diensten) tenminste die producten aan te schaffen die geschikt zijn voor het gebruik van de DNSSEC standaard. Het besluit over wanneer deze standaard het best kan worden toegepast, ligt daarmee alsnog bij de individuele organisaties.

In het geval van DNSSEC wordt voor Rijksoverheden een uitzondering gemaakt op deze regel. Rijksoverheden dienen conform een besluit van het ICBR hun domeinnamen onder te brengen bij de Dienst Publiek en Communicatie van Min. AZ . DPC ondersteund het gebruik van DNSSEC (maar bijvoorbeeld ook 'pas toe of leg uit' -standaard IPv6) en regelt zowel het signen als de validatie van de domeinen. Bijkomend voordeel van dit besluit is dat alle Rijksdomeinen overzichtelijk door één partij beheerd worden en bovendien worden voor deze service geen kosten in rekening gebracht.

[1] *http://www.rijksoverheid.nl/onderwerpen/ict/domeinnamen/domeinnamen-bij-de-rijksoverheid*

Toelichting

Waar gaat het inhoudelijk over?
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. Zo is www.rijksoverheid.nl bijvoorbeeld gekoppeld aan het IPv4-adres 94.228.135.80 en aan het IPv6-adres 2a00:d00:3:2::162. 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. DNS staat momenteel op de lijst met gangbare open standaarden (en blijft daar ook staan; DNSSEC is een aanvullende standaard).

In de DNS-standaard zijn in de afgelopen jaren tekortkomingen ontdekt die het mogelijk maken voor hackers om deze verwijzingen aan te passen. 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.

DNSSEC werkt aanvullend aan PKI(overheid). PKI(overheid) zorgt voor integriteit en vertrouwelijkheid van gegevensuitwisseling met een bepaalde domeinnaam, maar kan in tegenstelling tot DNSSEC niet garanderen dat met het correcte IP-adres wordt gecommuniceerd. Op de langere termijn kan PKI(overheid) zelfs aan kracht winnen door koppeling aan DNSSEC (via de in ontwikkeling zijnde standaard 'DANE'). DNSSEC is ook complementair aan DKIM (betrouwbare herkomst e-mail) dat momenteel in procedure is.

Hoe is het proces verlopen?
Op basis van de intake is besloten tot het instellen van een expertgroep. Op 27 januari 2012 is een expertgroep bijeengekomen om de bevindingen in het algemeen en de geïdentificeerde knelpunten in het bijzonder te bespreken. De expertgroep adviseerde positief over opname op de lijst. Het expertadvies is publiekelijk geconsulteerd hetgeen heeft geleid tot een zevental reacties:

- Vijf van de respondenten (KvK, Belastingdienst, UWV, EL&I, PROXY Laboratories) onderschrijven de opname van DNSSEC op de 'pas toe of leg uit'-lijst.
- De Belastingdienst toont zich groot voorstander van opname van DNSSEC, maar merkt tevens op dat er wel een zekere afhankelijkheid lijkt te bestaan m.b.t. keuze van browsers en dat dit in de toekomst een aandachtspunt zou kunnen worden.
  Reactie: Juist om deze reden is de 'client' uitgezonderd. Niet alle browsers en andere internetapplicaties bieden standaard ondersteuning DNSSEC. De verplichting wordt gelegd op het 'koppelvlak' tussen een organisatie en het internet. Door daar te controleren wordt het gehele achterliggende netwerk in voldoende mate beveiligd, zonder dat aanpassingen nodig zijn op individuele clients.

- UWV geeft de opmerking mee dat het in IPv6 bij RIPE mogelijk wordt voor bedrijven om een IP-reeks voor een organisatie te reserveren.

Reactie: Dit zal de beheerlast voor IP-adressen en DNSSEC kunnen verlagen maar zorgt niet voor beveiliging van DNS.

- EL&I stelt dat de ondersteuning van de standaard door gangbare software en de kosten van DNSSEC (invoering en exploitatie) nog onvoldoende duidelijk zijn.
  Reactie:
  - *Er moet onderscheid worden gemaakt tussen valideren (het controleren van DNSSEC gegevens bij het bezoeken van een website) en ondertekenen (het vastleggen van DNSSEC informatie aan de aanbiederskant).*
  - *In de meeste netwerksoftware is het valideren op DNSSEC inmiddels een standaardoptie. De extra kosten zijn hier dus minimaal.*
  - *Voor het ondertekenen is het gewenst dat het proces tussen dienstaanbieder en registratiepartij (uiteindelijk SIDN) zoveel mogelijk geautomatiseerd kan plaatsvinden. Dit is dan ook als eis opgenomen. Daarnaast zijn Rijksoverheden d.m.v. van het ICBR besluit[2] verplicht hun domeinen onder te brengen bij Dienst Pulbiek en Communicatie van Min. AZ. DPC ondersteund DNSSEC en brengt bovendien voor het domeinnaambeheer geen kosten in rekening.*
  - *DNSSEC maakt het registeren van systemen op het internet ontegenzeggelijk complexer en foutgevoeliger. Daar waar het huidige DNS-systeem nog enigszins fouttolerant is, is DNSSEC dat (vanuit veiligheidsoogpunt) niet meer. Dit maakt het netwerkbeheer een kritieke factor. Op het moment dat dit nu nog niet goed geregeld is, moeten mogelijk kosten worden gemaakt om dit goed in te richten. BKWI geeft in de consultatie hier enkele handvatten voor.*
- Stichting NLnet plaats een aantal opmerkingen, met name bij het buiten het toepassingsgebied laten vallen van de lokale werkplek en stelt dat er in de aanbevelingen ook aandacht gegeven dient te worden aan hoe gebruikers en interne toepassingen aan de ontvangende zijde kunnen profiteren van de beveiliging die DNSSEC biedt.
  Reactie: Op termijn kan een verruiming inderdaad zinvol zijn. De expertgroep heeft echter bewust gekozen tot beperking van het functioneel toepassingsgebied, omdat de clientondersteuning op dit moment nog onvoldoende is. Bovendien: door op het koppelpunt tussen de organisatie en het internet te controleren op DNSSEC wordt de interne organisatie in belangrijke mate beschermd.
- BKWI ondersteunt de opname van DNSSEC op de lijst voor 'pas toe of leg uit', maar maakt wel enkele opmerkingen. Kort samengevat betreft het de volgende punten:
  - Men pleit voor een meer technische definitie van het toepassingsgebied.
    Reactie: er is bewust gekozen voor een meer 'leesbare' definitie. De technische definitie kan gezien worden als een uitwerking hiervan, die een plek kan krijgen in een handreiking rondom DNSSEC (vergelijk de toepassingsgebieden voor PDF en ODF, die ook in een handreiking verder zijn uitgewerkt).
  - Men wijst op de wens om ook het gebruik van DNSSEC te verplichten.
    Reactie: om invulling te geven aan dit punt is een extra adoptieadvies opgenomen om – beginnend bij belangrijke internetdiensten van de overheid – het gebruik van DNSSEC te verplichten.

Datum
23 mei 2012

[2] *http://www.rijksoverheid.nl/onderwerpen/ict/domeinnamen/domeinnamen-bij-de-rijksoverheid*

- BKWI suggereert een shared service op te richten voor DNS beheer bij de overheid. In dit verband wijst men op de kosten die gemaakt moeten worden voor goed netwerk/DNS-beheer.
- *Reactie: Voor Rijksoverheden is er reeds één centrale domeinbeheerder waar iedere Rijksoverheid domeinnamen moeten onderbrengen: Dienst Publiek en Communicati3e van min. AZ.*

  Voor alle overheidspartijen wordt bovendien ter ondersteuning voorgesteld om een handreiking m.b.t het gebruik van DNSSEC op te stellen. . Men wijst er op dat DNSSEC geen 'oplossing voor alles' is en dat de kennis rondom DNSSEC niet overal aanwezig is.
  Reactie: hier heeft BKWI een duidelijk punt. De oproep voor het opstellen van een handreiking wordt daarom in dit Forumadvies niet alleen gedaan aan de DNSSEC community maar ook aan het Nationaal Cyber Security Centrum. Dit betekent dat in de handreiking in de volle breedte naar het vraagstuk gekeken kan worden.

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. Het DNS-systeem wordt door invoering van DNSSEC weliswaar veiliger, maar ook complexer en gevoeliger voor fouten door systeembeheerders. Het risico bestaat dat websites door fouten niet meer bereikbaar zijn. Om de invoering goed te laten verlopen en de kosten te minimaliseren adviseert het Forum om validatie van domeinnamen alleen verplicht te stellen voor systemen die direct aan het publieke internet gekoppeld zijn, terwijl de signing verplichting van domeinnamen alleen geldt als deze geautomatiseerd aangevraagd kunnen worden.
  Ten aanzien van de kosten kunnen de volgende opmerkingen worden gemaakt:
  1. SIDN gaat geen kosten in rekening brengen voor DNSSEC aan registratie dienstverleners. SIDN overweegt om DNSSEC registratiehouders te belonen voor het gebruik van DNSSEC.
  2. Op basis van ervaringen en buitenland en Nederland blijkt dat de commerciële registratie-dienstverleners geen of nauwelijks extra kosten in rekening brengen aan domeinnaamhouders voor DNSSEC. Op dit moment is het grootste deel van de overheidsdomeinnamen onder gebracht bij dergelijke dienstverleners.
  3. Een overheidsorganisatie kan er voor kiezen om zelf te signen of om zelf registratiedienstverlener te worden (bijv. Belastingdienst en DPC/AZ). In dat geval zijn er kosten verbonden aan 'sleutel-beheer'. Naarmate een organisatie meer domeinnamen beheert, zijn de kosten per domeinnaam lager. Door toename van ervaring en ondersteuning van DNSSEC in software en automatisering van de registratie, zijn deze kosten gedaald. Daarnaast zijn Rijksoverheden d.m.v. het ICBR besluit[3] verplicht hun domeinen onder te brengen bij Dienst Publiek en Communicatie van Min.

[3] *http://www.rijksoverheid.nl/onderwerpen/ict/domeinnamen/domeinnamen-bij-de-rijksoverheid*

AZ. DPC ondersteund DNSSEC en brengt bovendien voor het domeinnaambeheer geen kosten in rekening.

4. Veel van de huidige netwerkapparatuur biedt reeds ondersteuning voor validatie van DNSSEC. Doordat validatie niet verplicht is voor systemen die niet direct aan het publieke internet gekoppeld zijn, zijn de implementatiekosten relatief beperkt. Daarnaast kunnen de kosten voor validatie verder worden beperkt door validatie te implementeren op centrale, gemeenschappelijke systemen zoals Digitale Werkplek Rijk.

   Toegevoegde waarde voor bedrijven
   Net als overheden zijn bedrijven (bijvoorbeeld banken) gebaat bij een standaard die helpt om de afkomst van een website te valideren. Dit zowel in de rol van afnemer van informatie en diensten van andere partijen, als in de rol van aanbieder van informatie en diensten naar de eigen afnemers en gebruikers. DNSSEC werk pas optimaal als in alle lagen de internetinfrastructuur (van domeinbeheerder via internet service provider tot de eigen netwerkapparatuur) deze standaard ondersteunen. Door als overheid DNSSEC de 'pas toe of leg uit' status te verlenen, en actief te gaan gebruiken, wordt de adoptie van deze standaard, naar verwachting aanzienlijk versneld en wordt het voor bedrijven eenvoudiger om deze standaard effectief in te zetten.

- *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). Andere voorbeelden van top-level domeinen die DNSSEC ondersteunen zijn Europa (.eu), Zweden (.se) en Tsjechië (.cz). In Nederland hebben SIDN, SURFnet en NCSC ervaring met en expertise over DNSSEC. Voor de verdere adoptie is nog wel stimulans nodig, temeer omdat de meerwaarde stijgt naar mate de adoptiegraad toeneemt.

- *Opname bevordert adoptie*
  De waarde van DNSSEC neemt enorm toe naarmate de standaard meer gebruikt wordt. Voor de adoptie van DNSSEC is het van belang dat er kritieke massa ontstaat. De overheid kan hieraan bijdragen door DNSSEC op de 'pas toe of leg uit'-lijst op te nemen. Daardoor kunnen overheden en gebruikers straks profiteren van een beter beveiligd fundament van het internet.

Wat is de conclusie van de expertgroep en de consultatie?

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'.

Het toepassingsgebied omvat het ondertekenen van domeinnamen en het valideren van opgevraagde domeinen. Voor het toepassingsgebied gelden twee beperkingen waarmee een aantal praktische bezwaren worden weggenomen en de kosten voor invoering worden verlaagd. De registratieverplichting geldt alleen indien de registerhouder het ondertekenen van domeinnamen geautomatiseerd heeft.. Inmiddels heeft het Forum Standaardisatie vastgesteld dat SIDN deze functionaliteit sinds 15 mei 2012 aanbiedt, waardoor deze beperking de opname van DNSSEC op de 'pas toe of leg uit'-lijst niet meer in de weg staat. Daarnaast geldt de plicht tot validatie niet voor systemen die niet direct aan het publieke internet gekoppeld zijn. Met de twee gestelde beperkingen wordt een aantal praktische bezwaren weggenomen en worden de kosten voor invoering verlaagd.

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. 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 'pas toe of leg uit'-lijst een handreiking komt . Deze handreiking moet overheidsorganisaties helpen om te gaan met invoering van de standaard. Als basis voor deze handleiding is in ruime mate best-practice materiaal beschikbaar. Op basis van de consultatiereactie van BKWI wordt voorgesteld bij het opstellen van deze handreiking ook het Nationaal Cyber Security Centrum te betrekken, zodat de veiligheidsproblematiek in de breedte belicht kan worden in deze handreiking.

Datum
23 mei 2012

Bijlagen
(zie: https://lijsten.forumstandaardisatie.nl/open-standaard/dnssec)

- Expertadvies DNSSEC, versie 1.0 d.d. 13 februari 2012
- Overzicht reacties consultatieronde
    1. Belastingdienst
    2. BKWI
    3. Kamer van koophandel
    4. Ministerie van Economische Zaken, Landbouw en Innovatie
    5. PROXY Laboratories
    6. Stichting NLnet
    7. UWV