FS-20130416.06A

Forum Standaardisatie

Adoptieadvies DNSSEC

18-03-2013

1 Doelstelling adoptieadvies

1.1 Achtergrond

In de Forumvergadering van 5 februari j.l. heeft het Forum ingestemd met het maken van een standaard sjabloon voor een adoptieaanpak per open standaard. De eerste conceptversie van het standaard sjabloon is inmiddels af en reeds toegepast op de open standaard DNSSEC (Domain Name System Security Extensions) van de 'pas toe of leg uit lijst'. Het doel van deze 'adoptiesessie' DNSSEC was om enerzijds het standaard sjabloon te toetsen op waarde en inhoud, en anderzijds om tot een adoptieadvies voor DNSSEC te komen.

1.2 Proces

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

- Het Bureau Forum Standaardisatie heeft een eerste conceptversie van een standaard sjabloon voor een adoptieaanpak op maat otwikkeld.
- Op basis van dit sjabloon is een bijeenkomst georganiseerd met een autoriteit (Marco Davids, SIDN) op de open standaard DNSSEC
- Samen met het Bureau Forum Standaardisatie is DNSSEC toegepast op het standaard sjabloon

De uitkomsten van de adoptiesessie DNSSEC zijn vervolgens in dit document vastgelegd.

1.3 Leeswijzer

Dit document is een samenvatting van de toepassing van het standaard sjabloon op DNSSEC. In dit document zullen kort de geïdentificeerde stakeholders die van belang zijn voor de adoptie van DNSSEC genoemd worden. Daarna zullen de drempels die zijn geconstateerd en de oplossingen en adviezen die de adoptie van DNSSEC kunnen bevorderen, behandeld worden.

2 Adoptieadvies DNSSEC.

2.1 Belangrijkste stakeholders

Voor het identificeren van de belangrijkste stakeholders van DNSSEC moet er onderscheid worden gemaakt tussen 'signing' en 'validation' van DNSSEC. Met 'signing' wordt het domein beveiligd met een DNSSEC handtekening, met 'validation' controleert de provider de validiteit van een DNSSEC handtekening.

2.1.1 Signing

Voor het 'signen' van DNSSEC zijn er voor het Bureau Forum Standaardisatie een aantal belangrijke partners die kunnen helpen bij de adoptie van DNSSEC. Stichting Internet Domeinregistratie Nederland (SIDN), de organisatie die alle .nl domeinnamen beheert, is een belangrijke partner voor adoptie. Zij beheren ook de website DNSSEC.nl waar veel informatie en tools zijn te vinden over de toepassing van DNSSEC. Het registreren van de domeinnamen is echter niet de verantwoordelijkheid van SIDN, maar van zogenaamde 'registrars'1. Dit kunnen grote Internet Service Providers (ISP's) zoals KPN of XS4ALL zijn, maar er zijn ook kleinere onbekendere 'registrars' die domeinnamen signeren voor overheidspartijen. De 'registrars' zijn verenigd in de Vereniging van Registrars. Deze organisatie zou een goed aanspreekpunt en partner kunnen zijn om de adoptie van DNSSEC te bevorderen.

Surfnet, NLnetLabs en PowerDNS zijn belangrijke marktpartijen waar veel kennis over DNSSEC aanwezig is. Met deze partners zou het Bureau Forum Standaardisatie samen moeten optrekken om de kennis en ervaring die hier aanwezig is te delen met nieuwe gebruikers.

Aan de gebruikers kant is voor het Rijk Algemene Zaken, Dienst Publiek en Communicatie (AZ/DPC), een belangrijke stakeholder. AZ/DPC is de Rijksregistrar en biedt DNSSEC ondersteuning aan. Alle rijkspartijen die hun domeinnamen onderbrengen bij AZ/DPC kunnen op deze manier DNSSEC gesigneerd worden. Voor provincies en gemeenten ligt dit anders. Hiervoor is er geen gemeenschappelijke registrar. Een overzicht van alle registrars van gemeenten, provincies etc., welke SIDN kan leveren, zou bijdragen aan het beter inzichtelijk maken welke registrars benaderd moeten worden en welke DNSSEC reeds aanbieden. Tenslotte is de net opgerichte informatiebeveiligingsdienst (IBD) van KING een goede stakeholder om bij aan te haken.

2.1.2 Validation

Voor de validerende kant van DNSSEC ligt net als bij de signerende kant veel kennis en ervaring bij SIDN, Surfnet en NLnetLabs. Daarnaast bieden steeds meer softwareleveranciers ondersteuning aan voor DNSSEC en wordt het in de software ook makkelijker om DNSSEC validation aan te vinken. Belangrijke softwareleveranciers zijn BIND, PowerDNS, Mircrosoft en Secure64.

Aan de gebruikers kant is SSC-ICT een belangrijke stakeholder. Het Bureau Forum Standaardisatie heeft al een kennisbijeenkomst

1 Een registrar is een bedrijf dat in opdracht van bedrijven, instellingen of personen een domeinnaam registreert

georganiseerd samen met SIDN en Surfnet over 'validation' van DNSSEC. SSC-ICT is inmiddels bezig met het aanzetten van DNSSEC waardoor bij succesvolle implementatie direct veel Rijkswerkplekken DNSSEC valideren. Voor de provincies, gemeenten en uitvoeringsorganisaties ligt het ingewikkelder en zal vooral op individueel niveau gecommuniceerd moeten worden. Sommige gemeenten hebben inmiddels DNSSEC succesvol geadopteerd en zij zouden als voorbeeld moeten dienen voor andere gemeenten. Hetzelfde geldt voor provincies en uitvoeringsorganisaties.

2.2 Geïdentificeerde drempels en maatregelen

Aan de hand van het standaard sjabloon zijn een aantal belangrijke drempels geïdentificeerd in volgorde van belangrijkheid:

2.2.1 Bekendheid van DNSSEC

Het ontbreekt bij DNSSEC vooral aan bekendheid (voornamelijk hoe DNSSEC bekend staat). DNSSEC krijgt al snel een technische stempel opgedrukt en de 'sense of urgency' om tot snelle adoptie van DNSSEC over te gaan ontbreekt. DNSSEC is als standaard moeilijk aan de man te krijgen. Communciatie richting de nieuwe gebruikers strandt al snel in een technische discussie waardoor veel beleidsmakers binnen de overheid afhaken.

Maatregelen: Op korte termijn gaat het Bureau Forum Standaardisatie samen met SIDN en andere geïdentificeerde stakeholders die DNSSEC aanjagen (Surfnet, NLnetLabs, ISOC), de standaard als onderdeel van een nieuwe generatie internetstandaarden (NextGen Internet) in de markt zetten. DKIM, IPv6 en DNSSEC maken samen een veiliger en beter schaalbaar internet. Deze manier van communiceren maakt meer duidelijk wat de standaarden precies omvatten en hoe al deze standaarden zich tot elkaar verhouden. De businesscase voor adoptie van deze drie standaarden samen is ook sterker dan voor adoptie van DNSSEC, DKIM of IPv6 alleen. Daarbij sluit deze aanpak aan bij de keuze van het Forum op informatiebeveiliging en indentitymanagement.

Op de langere termijn gaat Het Bureau Forum Standaardisatie een faciliterende rol spelen in het samenbrengen van de partijen (IPv6 Task Force, ISOC, Phishingscorecard etc.) die betrokken zijn bij deze drie standaarden. Het doel zal daarbij zijn om meer samen op te trekken, de drie standaarden in zijn geheel aan te jagen en de informatie, kennis en ervaring van deze standaarden gezamenlijk te beheren. Op de KING leveranciersbijeenkomst van vrijdag 22 maart heeft het Bureau samen met SIDN en de IPv6 Task Force al een presentatie gegeven met deze nieuwe insteek. Ook zijn er artikelen gepubliceerd die hier aan refereren.

Tenslotte gaat SIDN nog een vergelijking tussen Nederland en het buitenland publiceren. Nederland loopt voor in de implementatie van DNSSEC en zulke positieve signalen dragen bij aan de verdere adoptie van DNSSEC.

2.2.2 Kennis van DNSSEC

Het ontbreekt aan kennis van DNSSEC bij veel overheidsorganisaties. Vooral de signerende kant van DNSSEC (met name sleutelbeheer) is ingewikkeld en vereist een bepaald kennisniveau. Verkeerde implementatie van DNSSEC kan als direct gevolg hebben dat de website van de organisatie niet meer bereikbaar is. Er is wel veel kennis van

DNSSEC aanwezig in Nederland, maar deze kennis is verspreid en het is niet inzichtelijk waar de benodigde kennis is te vinden.

Maatregelen: SIDN beheert de website DNSSEC.nl. Het Bureau Forum Standaardisatie wil samen met DNSSEC een overzicht maken van waar de trainingen, cursussen, online hulpmiddelen etc. te vinden zijn en welke organisaties dit aanbieden. Deze informatie moet zowel op de website DNSSEC.nl als op forumstandaardisatie.nl terecht komen.

Daarnaast heeft het Bureau i.s.m. SIDN en Surfnet een kennisbijeenkomst georganiseerd bij SSC ICT over DNSSEC validation. Ter aanvulling hierop zal BFS samen met SIDN op korte termijn een webinar organiseren. Het Bureau wil in de toekomst meer van dit soort kennisbijeenkomsten organiseren.

2.2.3 Organisatorische dimensie

Het gebeurt nog weleens dat een website niet goed gevalideerd wordt doordat de website niet correct (meer) is gesigned. Het is echter heel moeilijk te monitoren of DNSSEC voor problemen zorgt, laat staan te achterhalen wat verkeerd is gegaan bij DNSSEC implementatie. Er zijn wel monitoring tools beschikbaar maar deze zijn ingewikkeld en worden niet of nauwelijks toegepast.

Maatregelen: Er zou meer gedaan moeten worden aan procesondersteuning. Het 'ontzorgen' van organisaties om problemen met DNSSEC te identificeren en op te lossen, zou een belangrijke maatregel zijn om deze obstakels voor nieuwe gebruikers weg te nemen. SIDN wil hier een grotere rol in gaan spelen, maar op korte termijn is hier nog geen directe oplossing voor. Het Bureau gaat samen met SIDN nadenken over hoe hier invulling aan te geven.

2.2.4 Technische dimensie DNSSEC

DNSSEC is geen 'bleeding edge' technologie meer en veel technische problemen zijn met voldoende kennis van DNSSEC (zie 2.2.2.) op te lossen. Daarnaast is er tegenwoordig goede software beschikbaar die veel technische problemen helpen oplossen. Van sommige software is echter bekend dat ze problemen opleveren met DNSSEC. Dit kan gevolgen hebben voor een goede implementatie van DNSSEC

Maatregelen: SIDN gaat i.s.m. het Bureau een overzicht maken van welke softwareleveranciers DNSSEC ondersteunen en van welke software bekend is dat ze problemen kunnen geven met DNSSEC.

2.2.5 Overige adviezen

Naast de oplossingen die het Bureau Forum Standaardisatie in samenwerking met andere partijen kan nemen om de adoptie van DNSSEC te bevorderen en de implementatie van DNSSEC te ondersteunen, zijn er ook nog een aantal adviezen uit de sessie naar voren gekomen.

- De functie die AZ/DPC vervult als Rijksregistrars voor het onderbrengen en daarmee signen van DNSSEC zou als voorbeeld kunnen dienen voor andere overheidslagen. De domeinen van de gemeenten vallen bijvoorbeeld onder verschillende registrars. Dit advies zou vooral richting KING (specifiek de

informatiebeveiligingsdienst) en de provincies moeten worden gecommuniceerd.