



DNSSEC voor .nl

1 Inleiding

1.1 Rol van het DNS

Domeinnamen hebben een belangrijke functie in het internetverkeer. Door middel van domeinnamen kan op een makkelijke manier contact gelegd worden met computers, websites en elektronische postbussen van instellingen, bedrijven en individuele personen. Via een domeinnaam kan men bijvoorbeeld de site van een bedrijf bereiken en vervolgens: informatie opvragen, een catalogus bekijken, advertenties opgeven, financiële transacties verrichten en bestellingen doen. Daarnaast worden domeinnamen ook gebruikt voor e-mail en ftp-verkeer, en vele andere netwerkgerelateerde toepassingen. Domeinnamen vormen een soort handvat op het internet en de goede werking ervan is van cruciaal belang voor de werking van het internet.

De oorsprong van de domeinnaam heeft te maken met een uniek nummer dat elke computer op internet heeft. Dat nummer heet IP-adres (Internet Protocol). Het bestaat uit een combinatie van cijfers. Omdat woorden makkelijker zijn te onthouden dan cijfers, is ervoor gekozen deze nummers te vertalen naar namen. Omdat het internet nog wel steeds werkt via de nummers worden de namen in een Domain Name Server (DNS) weer terugvertaald naar nummers. Iedere domeinnaam is opgebouwd uit minimaal twee onderdelen. De meest rechtse component (bijvoorbeeld .com) wordt het 'top level domain' (TLD) genoemd. De country code top level domain names (ccTLD) verwijzen naar landen, zoals .nl voor Nederland, .be voor België of .de voor Duitsland.

1.2 Kwetsbaarheden in het DNS

Het huidige DNS-protocol bevat een aantal kwetsbaarheden en is hierdoor niet voldoende beschermd tegen bijvoorbeeld aanvallen van een onbekende 'man-in-the-middle' die een foutief IP-adres teruggeeft bij een DNS-bevraging. Op deze manier kunnen potentieel zeer gevoelige gegevens in verkeerde handen komen doordat gebruikers denken dat ze op een veilige website zijn, maar in werkelijkheid op een nagemaakte website nepsite zijn aanbeland. Op deze manier kan ook e-mail- of ftp-verkeer worden onderschept zonder dat de gebruiker iets merkt.

Deze kwetsbaarheden van het DNS zijn al heel lang bekend, maar tot voor kort was de veronderstelling dat het niet gemakkelijk is om daar misbruik van te maken. In de zomer van 2008 heeft Dan Kaminsky aangetoond dat het gebruik maken van deze kwetsbaarheden helemaal niet zo ingewikkeld is. Hierdoor is er veel aandacht in de media ontstaan over de veiligheid van het DNS en is dit onderwerp hoger op de agenda komen te staan. Een consequentie hiervan is dat het gevoel van urgentie om maatregelen te nemen om het DNS veiliger te maken groter is geworden.

1.3 DNSSEC als oplossing

De meest complete en veilige oplossing om de kwetsbaarheden in het DNS op te lossen is de grootschalige implementatie van DNSSEC. Hiermee wordt een digitale handtekening gekoppeld aan het antwoord op een DNS-vraag zodat de internetgebruiker kan controleren of hij het onversleutelde antwoord inderdaad heeft teruggekregen van degene die dat antwoord terug mag geven in plaats van een antwoord van willekeurig iemand die hem probeert te misleiden.



De introductie van DNSSEC is in alle opzichten géén kant-en-klaar project. Het DNSSEC-protocol is dusdanig opgebouwd dat de invoering ervan een grote impact heeft op de bedrijfsprocessen, het beleid en de algemene voorwaarden van registries en registrars. Dit geldt zowel voor de zonefilepublicatie in het DNS als voor de domeinnaamregistratieprocessen. Daarnaast geldt dat de introductie van DNSSEC met zich meebrengt dat het DNS-systeem veel gevoeliger wordt voor (menselijke) fouten. Het huidige DNS is tamelijk tolerant voor verkeerd geconfigureerde DNS-systemen, maar met DNSSEC zal een verkeerde configuratie vaker leiden tot het disfunctioneren van het DNS. De consequentie van deze twee zaken is dat het belangrijk is om zeer voorzichtig en weloverwogen met de introductie van DNSSEC om te gaan omdat fouten bij de implementatie een grote impact kunnen hebben op de stabiliteit en de betrouwbaarheid van de .nl-zone.

2 Operationele issues bij de invoering van DNSSEC

De invoering van DNSSEC voor .nl leidt dus tot een veiligere .nl-zone. Er zijn echter nog een aantal operationele issues die moeten worden opgelost voordat DNSSEC voor de .nl-zone kan worden ingevoerd zonder de stabiliteit in gevaar te brengen. Deze issues worden hieronder kort uitgelegd en besproken.

2.1 Vraag naar DNSSEC

De vraag naar DNSSEC is op dit moment nog erg laag. Hiervoor zijn een aantal redenen zoals de bekendheid van de kwetsbaarheden van het DNS bij het grote publiek en de consequenties die dat heeft op de internetveiligheid. Daarnaast spelen de kosten die met de introductie van DNSSEC gepaard gaan en de kennis die nodig is om DNSSEC te implementeren ook een rol.

Het belang van een veilig DNS wordt echter steeds groter omdat het belang van het internet steeds meer toeneemt en het DNS een kritisch onderdeel van het internet is. Omdat de kwetsbaarheden van het DNS al jaren bekend zijn en de technieken om er misbruik van te maken steeds geavanceerder worden is het dan ook een kwestie van tijd voordat er op grotere schaal misbruik hiervan gemaakt gaat worden. Op dat moment zal de roep naar DNSSEC snel heel groot kunnen worden, waardoor er minder tijd is om de implementatie van DNSSEC zorgvuldig te doen.

Een aantal landen en TLD's heeft inmiddels DNSSEC geïmplementeerd of heeft vergaande vorderingen gemaakt in de aanloop daar naartoe. Dit betekent dat de implementatie van DNSSEC in een stroomversnelling is gekomen, zeker nu ICANN heeft aangekondigd dat DNSSEC in 2010 voor de root geïmplementeerd wordt. Voor veel registries is de geringe vraag naar DNSSEC wel een issue, maar wordt het veiligheidsprobleem als dusdanig groot ervaren dat ze er toch voor kiezen om DNSSEC in te voeren.

2.2 Signing software

DNSSEC werkt met Public Key Infrastructure (PKI) technologie. Dit houdt in dat elke DNSSEC-domeinnaam een publieke- en een privésleutel heeft. Met de privésleutel wordt de domeinnaam ondertekend en met behulp van de bijbehorende publieke sleutel kan een gebruiker controleren of het antwoord op een DNS-vraag door de juiste instantie is ondertekend. Het ondertekenen met de sleutels is een administratief proces wat het beste kan worden geautomatiseerd om fouten te voorkomen en de extra werkdruk op beheerders zo laag mogelijk te houden.



Op dit moment zijn er verschillende 'signing software-pakketten' beschikbaar, maar ontbreekt nog een goed open-source alternatief. De beperkte beschikbaarheid van DNSSEC-software is voor veel partijen een probleem bij de invoering van DNSSEC. Met name omdat een foutloze publicatie van de zonefile een vereiste is en deze software daarvoor noodzakelijk is. Ook voor SIDN is het een vereiste dat er goede DNSSEC-signing-software beschikbaar is voordat de .nl-zone ondertekend kan worden. Daarbij kiest SIDN ervoor om zoveel mogelijk met open-source-software te werken om vendor lock-in te voorkomen en om aanpassingen aan de software te kunnen doen indien nodig. Om die reden dragen wij, samen met een aantal andere partijen, bij aan de ontwikkeling van OpenDNSSEC.org software (www.opendnssec.org).

2.3 Wijzigen van registratieprocessen en het registratiesysteem

De invoering van DNSSEC brengt met zich mee dat er meer informatie over een domeinnaam bij de registry bekend moet zijn. De publieke sleutels van een .nl-domeinnaam moeten namelijk bij SIDN bekend zijn zodat SIDN deze kan publiceren in de .nl-zonefile.

Om deze publieke sleutels te kunnen ontvangen en wijzigen zijn extra processen nodig, bovenop de bestaande processen. Binnen de EPP-standaard, die de communicatie tussen registries en registrars beschrijft, is hier al rekening mee gehouden, maar in de praktijk blijkt dat een aantal zaken in deze standaard nog niet optimaal werken. Bovendien geldt dat er nog veel zaken zijn waar nog geen 'best practises' voor bestaan omdat DNSSEC nog niet veel is geïmplementeerd. De invoering van DNSSEC zal dus een aantal nieuwe processen met zich meebrengen en SIDN zal deze afstemmen met haar registrars om te komen tot optimale processen voor het .nl-domein.

2.4 Key roll-overs

De DNSSEC-sleutels zijn, om veiligheidsredenen, niet onbeperkt houdbaar en moeten periodiek, of eenmalig in geval van een veiligheidslek (emergency key roll-over), worden veranderd. Dit betekent dat er voor elke DNSSEC-domeinnaam extra administratieve handelingen moeten worden verricht ook al verandert er niks aan de domeinnaam waardoor de beheerslasten toenemen. De wijzigingen in de sleutels moeten worden gepubliceerd in het DNS en als hier fouten in ontstaan zal een DNSSEC-domeinnaam niet meer werken. Hierdoor wordt de fouttolerantie van het DNS flink verkleind en neemt de stabiliteit van het DNS mogelijk af. Zolang de root nog niet is ondertekend met DNSSEC is het bovendien niet mogelijk om sleutels van top level domeinen (TLD's), en wijzigingen daarop, in het DNS te publiceren. Tot die tijd zal er gebruik moeten worden gemaakt van interim oplossingen zoals ITAR van IANA en DLV van ISC. Deze oplossingen leiden tot extra beheerslasten bij key roll-overs en emergency key roll-overs.

Ook voor key roll-overs geldt dat deze het beste kunnen worden geautomatiseerd om zo min mogelijk problemen te veroorzaken. Daarnaast zal de procedure voor key roll-overs eenvoudiger worden op het moment dat de root DNSSEC heeft geïmplementeerd omdat SIDN dan haar sleutels alleen bij ICANN hoeft te wijzigen. ICANN heeft aangekondigd dat dit vanaf 1 juli 2010 het geval is.

2.5 Key roll-overs van meerdere domeinen, ondertekend met één sleutel

In de DNSSEC-standaard is het toegestaan om meerdere domeinen met één privésleutel te ondertekenen. Dit kan zijn voordelen hebben als er maar een beperkt aantal privésleutels tegelijkertijd kan worden beheerd. Typisch werken Hardware Security Module (HSM's, kluizen voor digitale sleutels) met een licentiemodel waarvoor per sleutel moet worden betaald en bovendien is er een maximum gesteld aan het aantal sleutels dat er in een HSM kan worden opgeslagen. Voor TLD's zoals .nl is dit geen groot probleem omdat er maar één zone hoeft te worden ondertekend. Registrars of name server



operators die echter grote aantallen domeinen beheren en toch hun sleutels in een HSM willen opslaan zouden dus meerdere HSM's nodig kunnen hebben voor het sleutelbeheer als ze per domein één sleutel gebruiken en zij zullen dus wellicht meerdere domeinen met één sleutel willen ondertekenen.

Op het moment dat er echter een wijziging plaatsvindt in de privésleutel zullen ook alle publieke sleutels moeten worden gewijzigd. Deze staan opgeslagen bij de 'parent' (SIDN in het geval van domeinnamen in de .nl-zone) en worden normaal gesproken gespreid gewijzigd omdat de geldigheid van elke publieke sleutel op een ander moment afloopt. Als er echter heel veel domeinen met dezelfde privésleutel zijn ondertekend loopt de geldigheid van alle daaraan verbonden publieke sleutels op hetzelfde moment af. Dit betekent dat er dan in zeer korte tijd veel communicatie met de 'parent' ontstaat. Het huidige EPP-protocol houdt hier geen rekening mee en er is op dit moment geen mogelijkheid om de sleutels op een andere manier bij de registry te wijzigen. Het protocol zal dus moeten worden aangepast of er zal een niet-standaard oplossing moeten worden gebouwd. Een andere optie is het om een grens te stellen aan het aantal domeinen dat met één privésleutel mag worden ondertekend. Er zijn dus nog een aantal zaken die hiervoor (in een internationaal verband) uitgezocht moeten worden.

2.6 Verhuizen van DNSSEC-domeinen

Eén van de belangrijkste middelen om concurrentie tussen registrars mogelijk te maken is een goed werkend verhuisproces. Vaak gaat een verhuizing van registrar A naar registrar B gepaard met een verhuizing van de name server operator. Als een domeinnaam met DNSSEC is ondertekend moet de privésleutel die hiervoor gebruikt wordt ook meeverhuizen. Vanuit veiligheidsoverwegingen is het echter niet toelaatbaar dat de privésleutel zelf meeverhuist. Dit betekent dat er voor een DNSSEC-domeinnaam twee mogelijke opties zijn om te verhuizen:

1. De name server operator die de domeinnaam kwijtraakt werkt mee met de verhuizing door de publieke sleutel van de nieuwe name server operator in het DNS te publiceren. Hiermee blijft een domeinnaam gedurende het hele verhuisproces bereikbaar en beveiligd met DNSSEC. Dit kost de 'oude' name server operator echter tijd en moeite en het is de vraag of hij dit wil doen voor een vertrekkende klant. Het is echter mogelijk om hiervoor voorzieningen te treffen, maar dat vereist additioneel beleid en kan leiden tot extra administratieve lasten.
2. DNSSEC wordt tijdens de verhuizing tijdelijk uitgezet. Hierdoor kan de verhuizing makkelijk plaatsvinden, maar is de domeinnaam tijdelijk niet beveiligd. Deze oplossing is dan wel simpel, maar gaat in tegen het principe dat DNSSEC er juist is om domeinen te beveiligen tegen aanvallen.

Beide opties hebben specifieke vóór- en nadelen. SIDN wil, in overleg met de lokale internetgemeenschap, uiteindelijk tot een standpunt komen over het proces dat de voorkeur geniet. Hierover zal dus nog afstemming met de lokale internetgemeenschap plaatsvinden.

2.7 Aanpassen van DNS resolving infrastructuur

Om te kunnen controleren of het antwoord op een vraag aan een DNSSEC-domein correct is moet de resolver (degene die de DNS-vraag stelt) kunnen controleren of het antwoord met de juiste privésleutel is ondertekend. Hiervoor gebruikt hij de publieke sleutel die bij die domeinnaam hoort (trust anchor). In het ontwerp van DNSSEC is het mogelijk om een verwijzing naar een trust anchor één niveau hoger in de DNS-hiërarchie te publiceren en die verwijzing vervolgens ook te ondertekenen. Hierdoor is het niet nodig elk trust anchor van elke domeinnaam te kennen, maar volstaat het om enkel het trust anchor van de root zone te kennen om alle andere op een beveiligde manier te kunnen achterhalen.



DNS-resolvers moeten wel DNSSEC 'aan' hebben staan om te kunnen controleren of het antwoord met de juiste privésleutel is ondertekend. Hiervoor zullen alle internet server providers en andere partijen die resolving name servers hebben hun infrastructuur moeten aanpassen. Het gaat hierbij om het wijzigen van hun configuratie in de name serversoftware, maar in veel gevallen ook om het aanpassen van de hardware omdat het controleren van de DNSSEC-sleutels een rekenintensieve taak is. Daarnaast zal de beheerslast voor name server operators ook toenemen. Als de resolvers echter DNSSEC niet 'aan' hebben staan heeft de invoering van DNSSEC weinig toegevoegde waarde. Een aantal partijen heeft inmiddels het voortouw genomen en heeft hun infrastructuur gereed gemaakt voor DNSSEC. Het zal echter nog wel een tijd duren voordat >95% van alle name servers DNSSEC compatibel is.

3 Standpunt en plan van aanpak SIDN

SIDN heeft in haar missie staan dat ze werkt aan een stabiele en veilige .nl-zone. Wij zijn daarom voorstander van DNSSEC. De operationele issues moeten echter wel worden opgelost voordat DNSSEC voor de .nl-zone kan worden ingevoerd zonder de stabiliteit van de .nl-zone in gevaar te brengen. Daarnaast geldt dat er gewerkt moet worden aan bekendheid met het veiligheidsprobleem van het huidige DNS en het belang van DNSSEC als oplossing hiervoor. SIDN hanteert rondom de invoering van DNSSEC voor de .nl-zone een pro-actieve en gefaseerde aanpak. Concreet betekent dat dat SIDN:

- Werkt aan software om DNSSEC 'signing' te automatiseren middels het OpenDNSSEC.org project (www.opendnssec.org)
- Participeert in het DNSSEC.nl platform (www.dnssec.nl) om met andere partijen die bij DNSSEC in Nederland betrokken zijn de invoering van DNSSEC voor de .nl-zone te stimuleren
- Actief het belang van DNSSEC promoot en ernaar streeft om DNSSEC op een zo groot mogelijke schaal voor de .nl-zone in te voeren.
- Participeert in internationale fora zoals ICANN en IETF om te komen tot standaarden en best practices
- Participeert in de DNSSEC Industry Coalition om DNSSEC-zaken met collega-registries af te stemmen
- DNSSEC in verschillende stappen invoert waarbij eerst de .nl-zone wordt ondertekend (DNSSEC tier 1) en daarna, als alle issues zijn opgelost, de mogelijkheid wordt geboden om .nl-domeinen met DNSSEC te ondertekenen.

3.1 Invoering van DNSSEC voor de .nl-zone

SIDN kiest voor een gefaseerde invoering van DNSSEC in vier stappen. Deze staan hieronder kort weergegeven:

1. *Afstemming met stakeholders over implementatievorm van DNSSEC*
SIDN werkt, samen met een aantal partijen uit de Nederlandse internetgemeenschap, aan oplossingen voor de operationele issues die hierboven beschreven staan. Hiervoor is onder andere het DNSSEC.nl platform opgericht. Indien er op basis van de invoering van DNSSEC belangrijke beleidswijzigingen zullen moeten worden doorgevoerd zal SIDN hierover met de lokale internetgemeenschap afstemming zoeken. SIDN zal daarnaast ook met haar registrars overleggen over de manier waarop DNSSEC-processen (technisch en operationeel) worden ingevuld.
2. *Ondertekenen van .nl-zone met DNSSEC, één maand nadat de root DNSSEC invoert.*
Door de .nl-zone te ondertekenen en dit besluit publiek te maken neemt SIDN het voortouw bij de invoering van DNSSEC voor de .nl-zone. SIDN kiest er bewust voor om te wachten tot ICANN de root heeft ondertekend omdat hiermee meteen een de gewenste eindsituatie kan worden



geïmplementeerd welke significante voordelen bij (emergency) key roll-overs met zich meebrengt. Hierdoor is de kans op fouten bij key roll-overs aanzienlijk kleiner wat de stabiliteit van de .nl-zone vergroot.

3. *Publiceren van .nl publieke sleutel in de root (DNSSEC tier 1)*

Zodra het mogelijk is (afhankelijk van ICANN) publiceert SIDN haar DNSSEC-sleutels in de root. Vanaf dit moment kan worden geverifieerd door resolvers of een antwoord op een .nl-domeinnaamvraag daadwerkelijk van SIDN afkomstig is. SIDN zal haar sleutels alleen in de root publiceren en geen gebruik maken van ITAR of DLV.

4. *Implementatie DNSSEC voor .nl-domeinen (DNSSEC tier 2)*

Op het moment dat alle issues rondom DNSSEC zijn opgelost en het duidelijk is op welke manier DNSSEC voor de .nl-zone het beste kan worden ingevoerd zal SIDN hiervoor een project opzetten om DNSSEC tier 2 te implementeren.