EPP keyrelay: oplossing voor de laatste DNSSEC deployment hobbel

Antoin Verschuren
SIDN Labs
antoin.verschuren@sidn.nl

DNSSEC is de beveiligingsuitbreiding op het Domain Name System (DNS) die op dit moment op verschillende plaatsen ter wereld wordt uitgerold, bijvoorbeeld in het .nl-domein. Het kent echter nog één onopgelost probleem: hoe verhuis je een met DNSSEC beveiligde domeinnaam op een veilige manier naar een andere DNS-operator? Hiervoor bestaat op dit moment geen eenvoudige oplossing en dat vormt een significante hobbel voor de verdere adoptie van DNSSEC.

In dit whitepaper stellen we onze oplossing voor dit probleem voor. Die draait om een 'key relay', een nieuw concept waarbij we gebruik maken van de registry als centraal punt om key-materiaal van de verkrijgende naar de latende DNS operator te sturen. Dit mechanisme is nodig omdat de latende DNS-operator sleutelmateriaal van de toekomstige DNS-operator nodig heeft voor pre-publicatie. Onze aanpak is onafhankelijk van specifieke businessrollen en communicatieprotocollen, heeft een groot draagvlak onder de .nl-registrars, en is daarnaast eenvoudig te implementeren. Om key relays te realiseren introduceren we een nieuw commando voor het EPP-protocol: EPP keyrelay.

I. Introductie

Het Domain Name System (DNS) [1] is een basisprotocol van het Internet. Het zet gemakkelijk te onthouden namen om in adressen van computers waar applicaties zich technisch bevinden. DNS wordt zowel zichtbaar als onzichtbaar door vrijwel elke internetapplicatie gebruikt, en vormt daarmee een kritiek protocol als het gaat om de werking van het internet.

DNSSEC [2] is de beveiligingsuitbreiding op het DNS. Het zorgt ervoor dat gebruikers niet via DNS ongemerkt kunnen worden 'omgeleid' naar een andere computer zonder dat ze dat in de gaten hebben. DNSSEC draagt zo direct bij aan het vergroten van de internetveiligheid en vormt een belangrijk element in het palet van mechanismen om het vertrouwen van gebruikers in het internet te maximaliseren. DNSSEC beveiligt DNS-antwoorden door handtekeningen (signatures) toe te voegen die gemaakt zijn met behulp van private sleutels (keys). Deze kunnen worden gecontroleerd (validated) met publieke sleutels. Zo'n gecontroleerd DNS-antwoord noemen we dan veilig (secure).

DNSSEC wordt op dit moment door verschillende partijen uitgerold, bijvoorbeeld door Google, Comcast en door verschillende landendomeinen zoals .br (Brazilië), .cz (Tsjechië) en .se (Zweden). SIDN heeft in 2012 DNSSEC op grote schaal uitgerold en het .nl-domein kent daardoor inmiddels meer dan 1,5 miljoen domeinnamen die met DNSSEC zijn beveiligd (stand juni 2013 [3]). Hiermee heeft .nl wereldwijd het grootste aantal DNSSEC-domeinnamen, maar loopt daardoor ook als eerste tegen een tot nu toe onopgelost probleem aan: het verhuizen van een met DNSSEC beveiligde domeinnaam van de ene DNS-operator naar de andere. Veel DNSSEC-domeinnamen betekent immers ook dat er veel van die domeinnamen worden verhuisd. In de experimentele fase van DNSSEC deployment was het nog acceptabel om DNSSEC voor een domeinnaam korte tijd uit te zetten bij een aanpassing in de infrastructuur, maar met toekomstige uitbreidingen op basis van DNSSEC zoals DANE [4] zullen domeinnamen continue veilig moeten zijn, ook tijdens wijzigingen aan de DNS-infrastructuur of van leveranciers. Als DNSSEC tijdelijk uitstaat tijdens een verhuizing, dan zullen protocollen als DANE helemaal niet werken en zal een dienst of website die voor zijn werking afhankelijk is van DANE dus niet beschikbaar zijn.

Het niet veilig kunnen verhuizen van een DNSSEC-domeinnaam vormt dus een significante hobbel voor de verdere uitrol van DNSSEC en hindert de verdere verhoging van de internetveiligheid. In dit whitepaper introduceren we onze oplossing voor dit probleem, die draait om een zogenaamde 'key relay'. Dit is een nieuw concept waarbij we gebruik maken van de registry als centraal punt om DNSSEC-sleutelmateriaal van de verkrijgende naar de latende DNS-operator te sturen en zo de verhuizing van begin tot eind veilig uit te voeren. Het unieke aan onze aanpak is dat het onafhankelijk is van specifieke businessrollen en communicatieprotocollen, een groot draagvlak onder de .nl-registrars heeft, en eenvoudig te realiseren is. Op protocol-niveau introduceren we voor key relays een nieuw commando voor het Extensible Provisioning Protocol (EPP) [5]: EPP keyrelay.

In de rest van dit paper beschrijven we de randvoorwaarden van veilig verhuizen (Sectie II) en hoe we dat hebben toegepast op het verhuisproces (Sectie III). Daarna gaan we in op hoe we key relays hebben gerealiseerd (Sectie IV) en we sluiten af met conclusies en toekomstig werk (Sectie V).

II. De domeinnaamindustrie

A. Verhuizen van domeinnamen

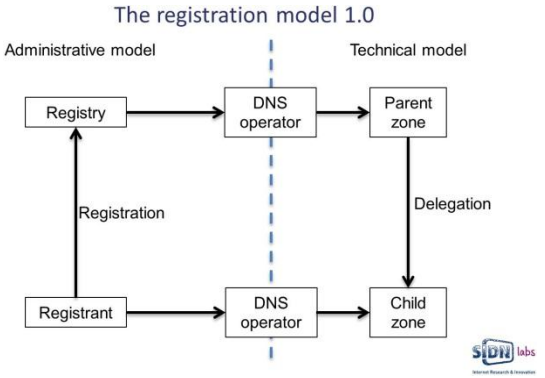
Ook zonder DNSSEC is het verhuizen van een domeinnaam naar een andere DNS-operator altijd al een probleem geweest. Wanneer een dienst overgaat naar een andere leverancier is het wenselijk dat beide leveranciers samenwerken om de overgang voor de eindklant zo geruisloos mogelijk te laten verlopen. Voor DNS-verhuizingen zonder DNSSEC moet de latende DNS-operator zijn nameserver nog enige tijd secondary laten draaien voor een zone om zo (a) bevragende nameservers (resolvers) die nog op de oude authoritative nameservers uitkomen te leren wat de nieuwe authoritative nameservers zijn en (b) om dezelfde antwoorden te geven als die nieuwe nameservers. Resolvers komen meteen na een nameserverwijziging nog vaak uit bij die oude nameservers vanwege het bewaren (cachen) van antwoorden in resolvers.

In de praktijk is DNS zonder DNSSEC zeer vergevingsgezind en bestand tegen veel operationele onvolkomenheden. Veel DNS-operators laten daarom na om deze wenselijke samenwerking uit te voeren voor klanten die vertrokken zijn, en die klanten hebben slechts minimaal last van die niet samenwerkende operators. De oude operator stopt zijn dienst abrupt, en DNS zonder DNSSEC accepteert zonder meer elk nieuw antwoord dat de resolver krijgt van de nameserver van de nieuwe operator, zij het met enige vertraging. Helaas accepteert zo'n resolver zonder DNSSEC ook elk antwoord van een willekeurige andere nameserver van een man-in-the-middle.

Met DNSSEC is dit verhaal duidelijk anders. Met DNSSEC moet de 'chain of trust' namelijk intact blijven, wil een resolver het DNS-antwoord accepteren [2]. Niet zomaar elk antwoord wordt geaccepteerd door een validerende resolver, om man-in-the-middle aanvallen te voorkomen. Er is tot nu toe één oplossing bekend voor het veilig verhuizen van een DNSSEC-domeinnaam die onder alle omstandigheden werkt zonder dat de domeinnaam tijdelijk insecure hoeft te worden [6]. Voor die oplossing is het echter nodig dat beide operators elkaars publieke DNSSEC-sleutels hebben, en dus samenwerken in de procedure om te zorgen dat een resolver de oude en nieuwe antwoorden accepteert gedurende de verhuisperiode. Om te begrijpen waarom die samenwerking tussen operators als moeizaam wordt gezien leggen we eerst kort uit welke rollen er bestaan in het registratiemodel van domeinnamen.

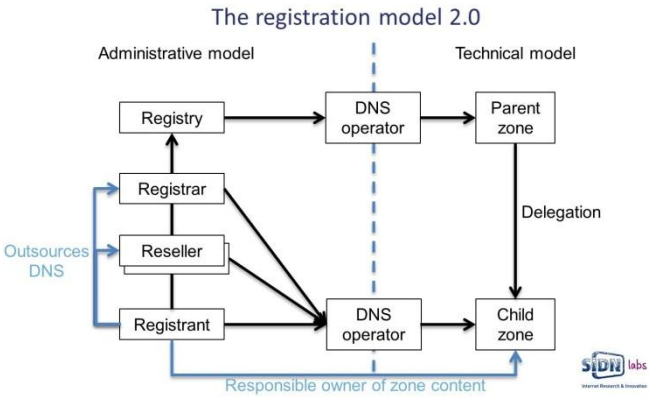
B. Rollen in de domeinnaamsector

In de jaren dat DNS bestaat is er behoorlijk wat veranderd aan de manier waarop er wordt omgegaan met het beheer van domeinnamen. Op technisch vlak is het model betrekkelijk eenvoudig gebleven (zie Figuur 1): er is een 'parent zone' en 'child zone'. De parent zone wordt administratief beheerd door een 'registry' en de child zone wordt administratief beheerd door een 'registrant'.



Figuur 1. Het traditionele registratiemodel.

Op het administratieve vlak is er echter door groeiende concurrentie en commercie een behoorlijk complex speelveld ontstaan van partijen die allemaal iets met een domeinnaam te maken willen hebben. Naast de registry en de registrant zijn er allerlei rollen ontstaan voor administratieve tussenpartijen of dienstverleners, zoals registrars, resellers, 3rd party hosters en DNS-operators (zie Figuur 2). Omdat één partij vaak meerdere rollen kan vervullen in de keten zijn er in discussies over dit onderwerp vaak misverstanden over de rol die wordt vervuld, en is men bang om verantwoordelijkheden, controle en omzet te verliezen.



Figuur 2. Het hedendaagse registratiemodel.

Bij het bedenken van een oplossing voor het samenwerken in het DNSSEC-verhuisprobleem is het dus belangrijk ervoor te zorgen dat alle combinaties van rollen geen afbreuk doen aan het model, en geen aannames te doen over wie welke rol vervult. Het vervelende van het bespreken van een 'DNSSEC-operator change' is dat de

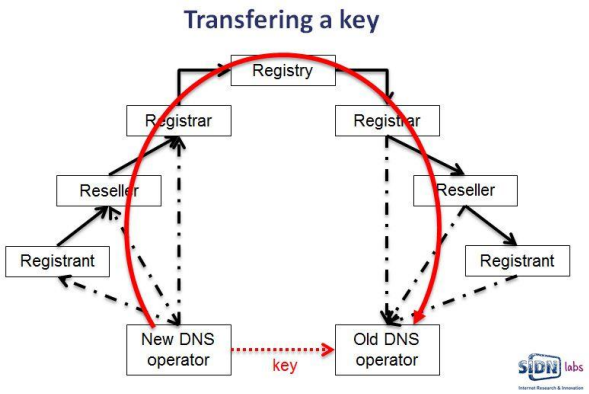
belangrijkste rol in dit proces, die van de DNS-operator, een rol is die tot nu toe nog niet goed is onderkend in de bestaande processen. In het verleden werd ervan uitgegaan dat de registrant vanzelfsprekend ook de DNS-operator was van zijn eigen child zone, maar die rol wordt nu meestal ingevuld door de registrar, reseller, website hoster of een andere derde partij. Die partijen gaan ervan uit dat het vanzelfsprekend is dat die rol bij hun activiteit hoort, maar in feite wordt die rol uitbesteed door de registrant en is het dus belangrijk om die rollen goed te scheiden.

III. Secure verhuizen

A. Mechanisme

Voor het veilig verhuizen van een DNSSEC-domeinnaam is het nodig dat beide DNS-operators tijdelijk elkaars publieke 'Zone Signing Key' (ZSK) opnemen in de zone [6]. De verkrijgende operator kan deze ZSK van de latende operator veilig opvragen via DNS met DNSSEC. Maar de latende operator heeft geen veilig kanaal om de ZSK van de verkrijgende operator op te vragen. De toekomstige zone is immers nog niet gedelegeerd, en er is daardoor nog geen 'chain of trust' aanwezig waarmee die key met DNSSEC-validatie uit die zone gehaald kan worden. Omdat het aantal DNS-operators zeer groot is, is het niet schaalbaar om die allemaal onderling veilig met elkaar te laten communiceren.

De innovatie die wij voorstellen is om DNS-operators daarom te laten communiceren via het kanaal dat ze toch al gebruiken om domeinnamen te registreren en te onderhouden: het administratieve kanaal via de registry. We noemen deze interactie een 'key relay'. De key wordt hierbij 'gerelayed' door deze naar de registry te sturen. De registry stuurt deze door naar de huidige registrar, die er op zijn beurt weer voor kan zorgen dat de key terecht komt bij de latende DNS-operator (zie Figuur 3).



Figuur 3. Versturen van de ZSK naar de latende DNS operator via de registry.

Het voordeel van een key relay is dat het een stateless mechanisme is, waardoor het schaalbaar is, eenvoudig te realiseren door de registry en eenvoudig te automatiseren voor registrars en resellers (zie Sectie IV.A). Daarnaast kan de registry of registrar controleren of het verhuisverzoek is geautoriseerd door de registrant, zodat de latende DNS-operator de key geautomatiseerd in zijn zone kan plaatsen. Ook is het proces agnostisch voor de verschillende rollen die al dan niet aanwezig zijn, of wie de rol van DNS-operator inneemt.

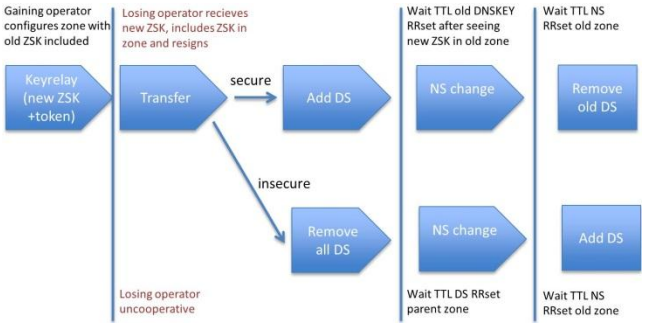
B. Inventarisatie bij stakeholders

Om tot een breed gedragen oplossing voor DNSSEC-operator changes te komen hebben we de wensen van de belangrijkste registrars, resellers, DNS-experts en collega-registries in kaart gebracht. We hebben geluisterd naar alle wensen en oog gehad voor de risico's die mensen zagen.

Zo wil de registry liever geen moeilijke timers bijhouden, mag de database niet veranderd worden door een willekeurige registrar, moet de registrant vrij zijn in de keuze van zijn registrar en moet altijd duidelijk zijn wie zijn huidige 'registrar of record' is. De registrars en resellers willen alles eenvoudig kunnen automatiseren, zonder handmatige controle, en ze willen ook in controle blijven indien de latende partij niet (snel genoeg) meewerkt. De DNS-operators willen weten of de key die zij opnemen in de zone echt wel door de registrant is goedgekeurd en hoe lang die dan in de zone moet blijven staan indien de hele verhuizing uiteindelijk toch niet doorgaat.

C. Procesoverzicht verhuizen DNSSEC-domeinnaam

Figuur 4 laat zien dat het totale proces van het verhuizen van een DNSSEC-domeinnaam uit meerdere stappen bestaat. De key relay is een losstaande stap, die in de toekomst ook voor andere doeleinden gebruikt zou kunnen worden.



Figuur 4. Procesdiagram DNSSEC operator change.

Nadat de key relay stap is uitgevoerd kunnen de andere stappen in het proces gevolgd worden. Dit zijn

allemaal bestaande registry-processen waar niets aan gewijzigd wordt. Het enige wat er dus verandert in het hele DNSSEC-verhuisproces (indien er sprake is van een DNS-operator change) is dat er eerst een key relay wordt uitgevoerd waarmee de key van de verkrijgende naar de latende DNS-operator wordt gestuurd.

De stappen daarna zijn losse stappen omdat het tijdstip van uitvoering daarvan afhankelijk is van diverse TTL-instellingen, waarmee de toekomstige registrar controle houdt over de kwaliteit en snelheid van de verhuizing. Of er nu wel of geen verandering van registrar plaatsvindt, een key relay is alleen nodig wanneer de DNS-operator die het DNSSEC sleutelmateriaal beheert wijzigt. Indien de registrar niet wijzigt, kan de transfer in dit proces worden weggelaten.

Indien de latende DNS-operator meewerkt, wordt gekozen voor het 'secure-traject' (bovenste helft van Figuur 4). Als dat niet het geval is kan de verkrijgende registrar altijd nog kiezen voor het 'insecure-traject', zodat hij te allen tijde de controle houdt.

Merk op dat indien een domeinnaam voor het verhuisproces al met DNSSEC beveiligd is, het verhuizen in zowel het secure als insecure traject evenveel stappen kent. De wachttijd tussen de individuele stappen is nodig omdat het tijd kost een eenmaal opgebouwde chain of trust uit de caches van alle resolvers te krijgen. Zonder die wachttijden zou de domeinnaam in validerende resolvers als 'bogus' worden gezien en zou de domeinnaam niet meer werken. Dit is waarom het verhuizen van een domeinnaam met DNSSEC altijd meer stappen kent dan een domeinnaam die geen DNSSEC heeft.

IV. KEY RELAY

A. *Afhandeling*

Om een key relay uit te voeren onderscheiden we twee processen:

1. Van toekomstig DNS-operator naar registry:
   Ontvang je een key relay verzoek van een partij onder je (vergelijk Figuur 3), bijvoorbeeld; een reseller ontvangt een key relay verzoek van een registrant, dan stuur je die door naar de toekomstige partij boven je; bijvoorbeeld je registrar, net zolang tot die de registry heeft bereikt. Een key relay verzoek wordt vergezeld van de autorisatiecode van de huidige registrant. De registry of latende registrar kan dan controleren of het verzoek is geautoriseerd door de huidige registrant.

2. Van registry naar latende DNS-operator:
   Ontvang je een key relay verzoek van een partij boven je, dan stuur je die door naar de latende (op dat moment huidige) verantwoordelijke partij onder je, totdat die de latende DNS-operator bereikt. De latende DNS-operator weet dat het verzoek geautoriseerd is door de huidige registrant omdat de registry of registrar de autorisatiecode heeft gecontroleerd. Hij kan de key daarom direct opnemen in de huidige zone voor de domeinnaam.

Deze twee stappen werken ook als de registrar of één van de andere partijen dezelfde blijft, of als er bijvoorbeeld geen reseller in het spel is, en werkt ook onafhankelijk van welke partij de DNS-operator rol inneemt. In ieder geval één partij in de keten weet immers wie de rol van DNS-operator vervult, anders had de domeinnaam nooit gedelegeerd kunnen zijn.

Het proces is volledig te automatiseren, mits elke partij zijn administratie en provisioning op orde heeft. De communicatie tussen de registrars en registry vindt meestal plaats in de vorm van EPP-berichten, maar tussen de andere partijen onderling (DNS-operator, registrant, reseller) meestal niet. Voor het model maakt het echter niet uit of de communicatie over EPP of een ander communicatieprotocol verloopt, zolang de beveiliging van het kanaal dat wordt gebruikt maar minstens zo veilig is als het kanaal dat is gebruikt om de domeinnaam te registreren of te onderhouden. Ons concept van key relays is hiermee algemeen toepasbaar.

Ook voor de registry is het proces eenvoudig. De registry ontvangt een key relay verzoek van een willekeurige registrar. De registry controleert de autorisatiecode van de registrant in het key relay verzoek, zoekt de huidige registrar of record op van de domeinnaam in het key relay verzoek in de registry database, en stuurt het key relay verzoek dan direct door naar die registrar. Dat is alles wat er gebeurt. Er wordt niets gewijzigd in de database en er hoeft geen state of timer te worden bijgehouden. De registry faciliteert alleen de communicatie tussen de registrars.

B. *EPP keyrelay-commando*

Zoals gezegd verloopt de communicatie tussen registry en registrars veelal via het provisioning protocol EPP [5]. Om het keyrelay mechanisme bij de registry te realiseren hebben wij daarom een nieuw EPP-commando geformuleerd: EPP keyrelay [7].

Naast de gebruikelijke EPP-velden zijn de belangrijkste velden in het EPP keyrelay-commando:

- de domeinnaam;
- de publieke key die wordt 'gerelayed';
- de autorisatiecode van de huidige registrant;
- hoe lang de key in de oude zone moet staan;
- de registrar die de keyrelay indient.

Deze gegevens worden door de verkrijgende registrar naar de registry verstuurd middels een EPP keyrelay-commando en worden door de registry één-op-één doorgezet in de EPP message queue van de huidige 'registrar of record' voor de betreffende domeinnaam.

EPP kent voornamelijk commando's om objecten te wijzigen in de registry database door de huidige 'registrar of record' voor een domeinnaam. Alleen de door de registrant aangewezen registrar mag daarbij wijzigingen aanbrengen aan de domeinnaam bij de registry. Daarnaast kent EPP het 'transfer' commando (het wijzigen van de registrar voor een domeinnaam) dat ook een object in de database wijzigt, maar door een willekeurige registrar aan de registry kan worden aangeboden. De registrant beveiligt een transfer-commando daarom door een door de huidige 'registrar of record' verstrekte autorisatiecode mee te geven bij een transfer, zodat de registry kan controleren of de willekeurige registrar handelt namens de huidige registrant.

Het keyrelay-commando lijkt op het transfer-commando, maar dan voor het wijzigen van de DNS-operator van een domeinnaam. Het wordt net als een transfer-commando ook door een willekeurige registrar aan de registry aangeboden, maar verandert niets aan de database. Het leidt echter wel tot een actie en meestal bij een andere registrar dan die het commando heeft uitgevoerd. Om te voorkomen dat deze actie onterecht wordt uitgevoerd, wordt ook het keyrelay-commando beveiligd met een autorisatiecode van de registrant

Het door ons voorgestelde EPP keyrelay-commando is hiermee voor het EPP protocol naast een nieuw commando ook een nieuwe commando categorie naast de drie betaande categorieën van 'session management commands', 'query commands' en 'object transform commands' [5]. Het EPP keyrelay-commando valt in geen van deze 3 categorieën en kan het beste worden omschreven als een 'communication command'.

Het kan voorkomen dat een verhuizing van een zone uiteindelijk niet doorgaat, of wordt teruggedraaid door de registrant nadat het key relay-verzoek al is uitgevoerd. Ook willen sommige DNS-operators zorgvuldig het proces beheren en voor belangrijke domeinnamen handmatig controleren of het proces volgens plan verloopt. Daardoor kan het proces bij sommige operators langer duren dan bij andere. Om te voorkomen dat keys door de geautomatiseerde toevoeging te lang of te kort in de zone bij de latende operator blijven staan kan de verkrijgende operator in een key relay-verzoek een indicatie meegeven hoe lang de key in de zone moet blijven. De latende operator kan dan na deze tijd de key veilig uit de zone verwijderen als de verhuizing onverwacht toch niet door gaat.

Tenslotte was het een wens van operators om te kunnen zien wie het key relay-verzoek heeft ingediend, zodat er door de latende operator contact opgenomen kan worden indien deze technische onvolkomenheden in het sleutelmateriaal constateert of andere technische vragen heeft. Om deze reden bevat een EPP keyrelay-commando ook de ID van de registrar die de key relay indient.

Door van het EPP keyrelay-commando een los commando te maken en niet te kiezen voor een complex gecombineerd verhuis- en transferproces kunnen alle andere EPP-commando's blijven zoals ze nu zijn. Ook kan het EPP keyrelay-commando hierdoor in de toekomst worden gebruikt in andere processen waarvoor het nodig is om sleutelmateriaal uit te wisselen.

C. Implementatie in DRS

SIDN heeft, als registry voor .nl, dit voorstel geïmplementeerd in haar domeinnaamregistratiesysteem (DRS). Door het proces voor DNSSEC-operator changes te faciliteren nemen we een belangrijk obstakel voor DNSSEC-adoptie weg en leveren wij een bijdrage aan de verdere beveiliging van de .nl-zone.

De implementatie in het registratiesysteem van SIDN was betrekkelijk eenvoudig, omdat het EPP keyrelay-commando niets wijzigt aan de database. Er hoeven geen nieuwe tabellen te worden gemaakt of bestaande tabellen te worden veranderd. Simpel gezegd is EPP keyrelay enkel een database query en de afhandeling van het hele proces kan volledig buiten de database om plaatsvinden. Daarnaast is EPP keyrelay een faciliterend commando. Het is niet verplicht om een key relay uit te voeren via de registry. Als DNS-operators onderling met elkaar willen communiceren kan dat ook nog steeds.

De meeste .nl-registrars die zich bezighouden met DNSSEC hebben toegezegd deze methode van veilig verhuizen te gaan ondersteunen, zodra EPP keyrelay gestandaardiseerd is in de IETF. De reden is dat ze zonder keyrelays hun klanten verhinderen hun domeinnaam veilig weg te verhuizen, maar daarmee ook geen nieuwe klanten naar zich toe kunnen verhuizen. Zeker met toekomstige toepassingen als DANE [4] wordt een geruisloze verhuizing nog belangrijker en de partijen in de markt willen ook daar hun klanten kunnen ondersteunen.

V. CONCLUSIES EN TOEKOMSTIG WERK

In dit whitepaper hebben we onze oplossing besproken voor DNSSEC-operator changes, het laatste onopgeloste probleem voor DNSSEC. De innovatie van ons werk is het concept van een 'key relay', waarbij we gebruik maken van de registry als centraal trust anchor om de publieke ZSK op een veilige manier van de toekomstige naar de latende DNS-operator te sturen. Onze aanpak is onafhankelijk van

specifieke businessrollen en communicatieprotocollen, heeft een groot draagvlak onder de .nl-registrars en is daarnaast eenvoudig te realiseren. Wij geloven daarom dat keyrelays dé aanpak zijn voor een DNSSEC-operator change en dat we hiermee de laatste hobbel voor de verdere uitrol van DNSSEC wegnemen.

We hebben het key relay-proces en de bijbehorende EPP syntax ingediend bij de IETF als een internet draft [7] en spannen ons in om die samen met de internet community tot RFC te bevorderen. Commentaar, maar ook support zonder commentaar, is welkom via de publieke IETF provreg mailinglist [8], waar EPP-extensies worden besproken. Tot nu toe is de draft daar enthousiast ontvangen.

Toekomstig werk voor de verdere adoptie van DNSSEC bestaat hierdoor aan de authoritieve kant enkel nog uit beleid en marktwerking. Enkele registries waaronder die van Nieuw Zeeland hebben registrars in hun beleid al verplicht gesteld om mee te werken aan het verhuizen van domeinnamen die met DNSSEC zijn ondertekend. Technisch gezien moet SIDN het keyrelay-proces behalve voor de EPP-interface ook nog implementeren in haar webinterface voor het registratiesysteem. Wat overblijft is de validatie van DNSSEC bij ISP's om er voor te zorgen dat DNSSEC ook voor gewone eindgebruikers van het DNS daadwerkelijk beschikbaar is en zo het internet veiliger maakt.

Acknowledgements

Met dank aan Miek Gieben, Marc Groeneweg, Rik Ribbers, Marco Davids en Cristian Hesselman.

Referenties

[1] Mockapetris, P., "Domain names - concepts and facilities", STD 13, RFC 1034, "Domain names - implementation and specification", STD 13, RFC 1035, November 1987.

[2] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "DNS Security Introduction and Requirements", RFC 4033, "Resource Records for the DNS Security Extensions", RFC 4034, "Protocol Modifications for the DNS Security Extensions", RFC 4035, March 2005.

[3] https://www.sidn.nl/kennisbank/statistieken/

[4] Hoffman, P., and J. Schlyter, "The DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS) Protocol: TLSA", RFC 6698, August 2012

[5] Hollenbeck, S., "Extensible Provisioning Protocol (EPP)", STD 69, RFC 5730, August 2009.

[6] Koch, P. and M. Sanz, "Changing DNS Operators for DNSSEC signed Zones", draft-koch-dnsop-dnssec-operator-change-04 (work in progress), March 2012.

[7] Gieben, R., Groeneweg, M., Ribbers, R., and A.L.J. Verschuren "Key Relay Mapping for the Extensible Provisioning Protocol" draft-gieben-epp-keyrelay-02 (work in progress), April 2013.

[8] PROVREG mailing list, https://www.ietf.org/mailman/listinfo/provreg