



DNSSEC in .nl

Antoin Verschuren, Technical policy advisor, SIDN

To Sign or not to Sign

3-12-2009

SIDN Relatiedag

Utrecht



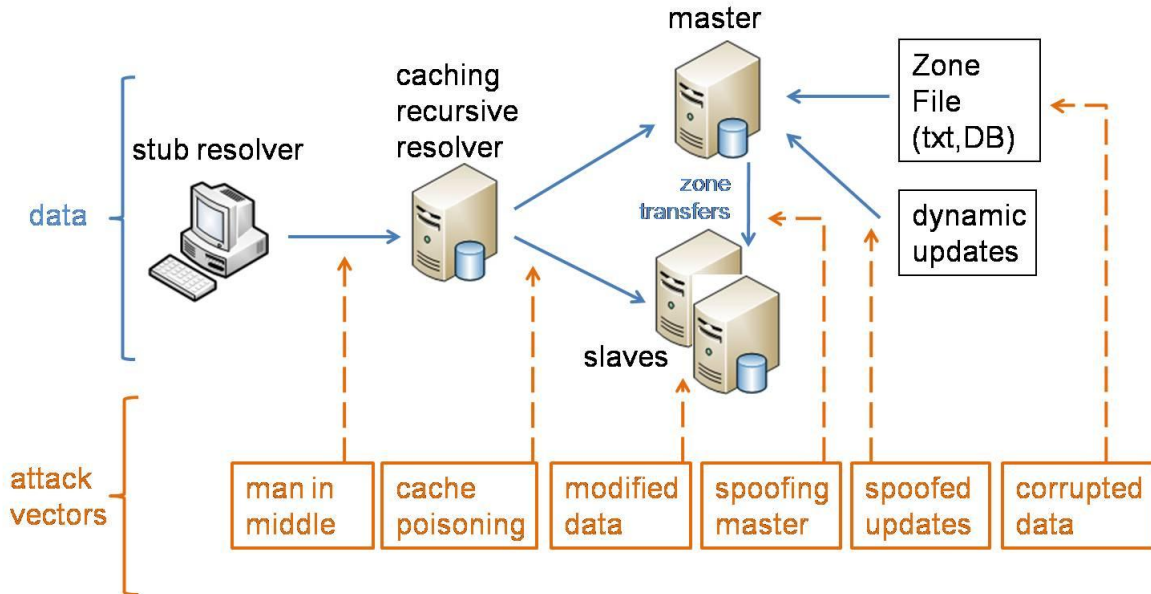
Agenda

- Wat is DNSSEC en waarom is het nodig?
- Wat is de status van DNSSEC?
- Wat doet SIDN?
- DNSSEC openstaande issues
- Signing software
- Issues tussen tier-1 en tier-2
- Overige zaken

Wat is DNSSEC en waarom is het nodig?



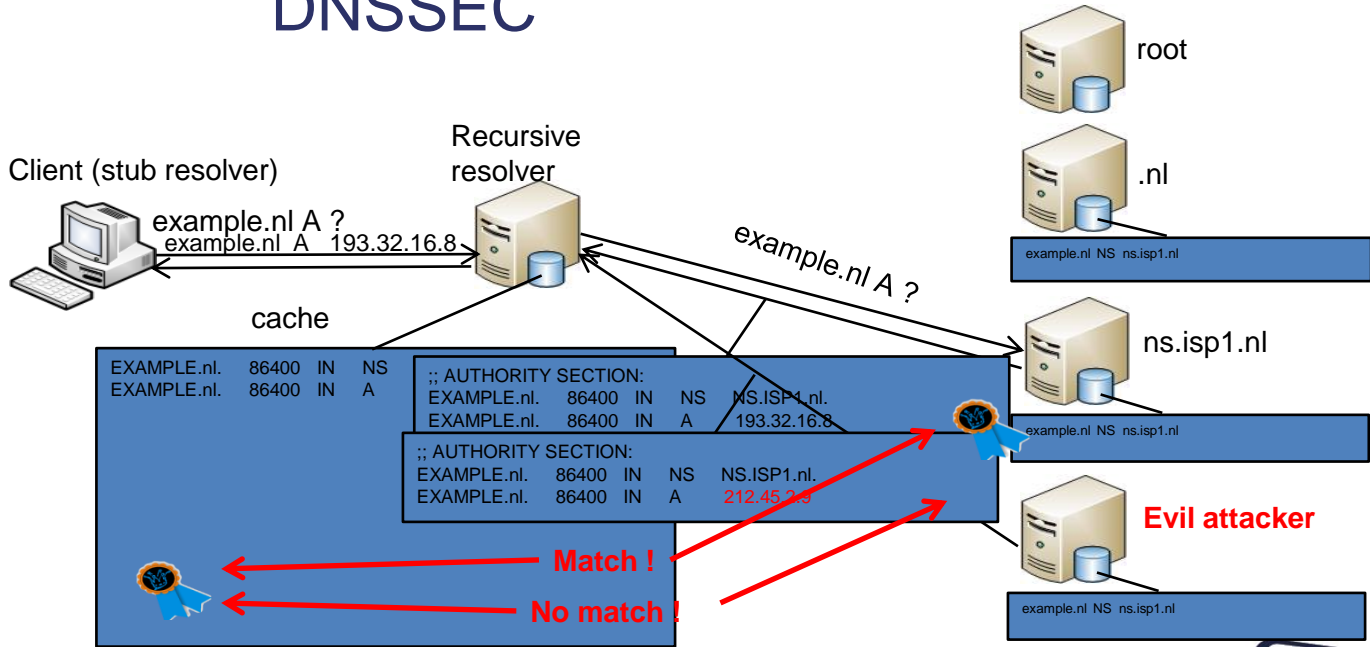
DNS attack vectors



DNSSEC

- Gebruikt public key cryptografie voor het valideren van de authenticiteit van de data
- De DNS-data wordt gesigneerd met een private key
- De resolver kan met behulp van de public key de integriteit van de gesigneerde data controleren

DNSSEC



DNSSEC helpt niet tegen

- Bedreigingen tegen een host (DDOS, buffer overruns, etc.)
- Schermt data niet af (privacy)
- Garandeert niet de correctheid van de DNS-data (garbage in, garbage out)
- Phishing, typosquatting
- DNSSEC garandeert enkel de authenticiteit van de DNS-data die ontvangen wordt.

Wat is de status van DNSSEC?

DNSSEC Status (wat is klaar)

- Protocol is technisch klaar
- Er is name server-software beschikbaar
- Enkele TLD's hebben DNSSEC geïmplementeerd
- De root wordt DNSSEC ondertekend (1 juli 2010)
- Verschillende TLD's hebben DNSSEC aangekondigd

DNSSEC status (wat is er nog niet)

- Proven technology voor signing
- Efficiënte schaalbare methode voor key management tussen parent en veel childs
- Processen voor day-to-day domain management
- Kennis en kunde bij registrars en registrants
- Marktvraag, maar die komt er aan

DNSSEC in de root

- Grootste wijziging aan de root zone file sinds tijden
- Huidige discussie: algoritme rollovers, capaciteit
- SHA-1 of SHA-256?
- TCP vs UDP
- Grotere responses
- Meer capaciteit
- Herziening infrastructuur
- Conflicterend met IDN, nieuwe TLD's?

Waarom duurt het zo lang?

- DNS werkt toch?
 - (aanvallen nemen toe sinds Kaminsky)
- DNSSEC is moeilijk
 - Zelfs voor DNS-experts. Klein foutje funest
- DNSSEC kost investering
 - DNS-infrastructuur kosten (data, capaciteit, traffic) verdubbelen
- Protocol is nu klaar, nu operationele implementatie nog
 - (standaard tools, proven technology, BCP's, software)
- Politieke discussie over wie de sleutel van het internet heeft
- Wie beheert de sleutel van jouw domein?
 - Registries/registrars moeten orderstraten aanpassen
- Awareness/vraag onder mainstream domeinnaamhouders

Wat doet SIDN?



Standpunt SIDN

- Beter zorgvuldig dan snel
 - Geen groot risico nemen, eerst de issues oplossen
- Maar, DNSSEC is nodig en komt er
 - SIDN project invoering DNSSEC gestart
- Dus actief bijdragen aan issues, niet afwachten
 - Bijdrage aan OpenDNSSEC signer
- Samenwerking tussen registries voor tier-1 oplossingen
 - DNSSEC industry coalition, DNSSEC-deployment initiative, IETF, ICANN
- Samenwerking tussen experts, registrars en dns-operators voor tier-2 oplossingen
 - dnssec.nl platform

Aankondiging

- SIDN gaat .nl (tier-1) ondertekenen!
 - 1 maand nadat de root is ondertekend
 - Dus augustus 2010 (afhankelijk van root)
 - Vanwege: geen DLV, ITAR, key publicatie
 - Geen 2 grootschalige wijzigingen tegelijkertijd
 - Mogelijk nog geen DS in root (IANA/ICANN)
- Daarna tier-2: secure delegaties
 - Processen en procedures
 - Aanpassing DRS

DNSSEC

openstaande issues



DNSSEC tier-1 issues

- Infrastructuur en capaciteit
 - SIDN intern, DNS infrastructuur, HSM's
- Software om processen te automatiseren
 - Signing software
 - Key management software
- Beleid, processen en procedures
 - Key management
 - Emergency key rollover
 - Trust anchor publicatie

Tier-2 issues

- Hoe vermarkt je DNSSEC?
- DNS-infrastructuur
- DNSSEC-provisioning
- **Signing software (voor iedereen)**
- Processen en procedures richting registrants
 - Key management
 - Contracten met registrants en DNS-operators

Issues tussen tier-1 & tier-2

- Wijzigen van DNS-operator (bijv. bij verhuizing)
- Key roll-overs
- Key management
- Registry/registrar system security

Signing software



Hardware/Software signers



Secure64 DNS Signer

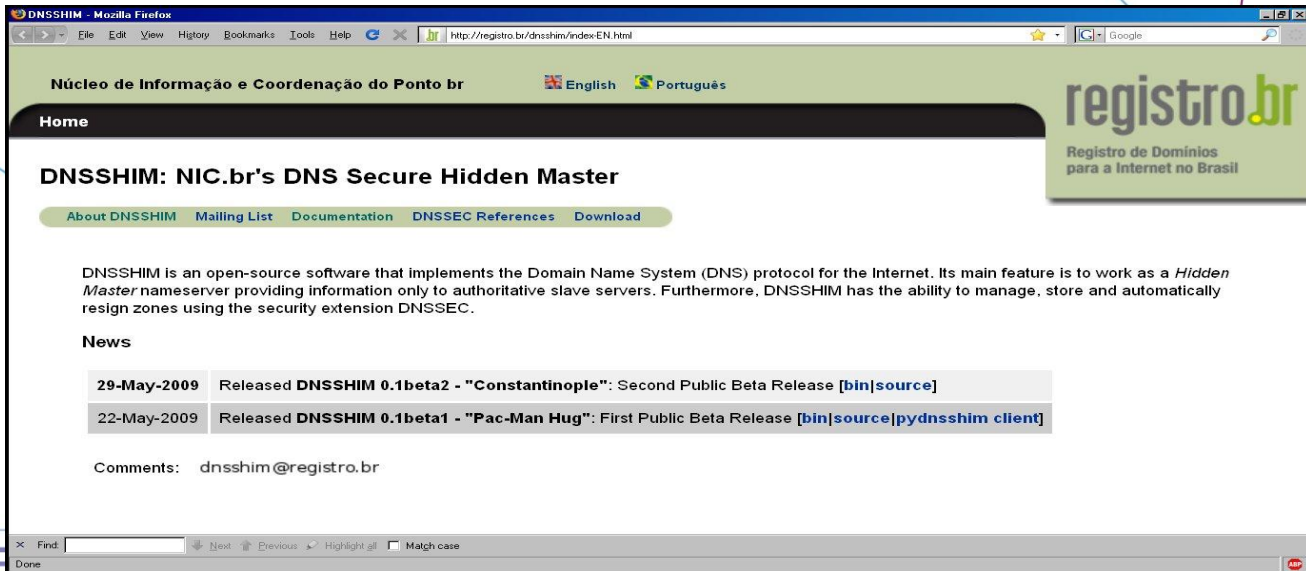


Hardware/Software signers



DNSX
DNSX SECURE SIGNER
DNSSEC MANAGEMENT SOLUTION

Hardware/Software signers



The screenshot shows a Mozilla Firefox browser window displaying the DNSSHIM website. The browser's address bar shows the URL `http://registro.br/dnsshim/index-EN.html`. The website header includes the text "Núcleo de Informação e Coordenação do Ponto br" and language options for "English" and "Português". The "registro.br" logo is visible in the top right corner, with the tagline "Registro de Domínios para a Internet no Brasil".

The main content area features a "Home" navigation bar and a title "DNSSHIM: NIC.br's DNS Secure Hidden Master". Below the title is a menu with links for "About DNSSHIM", "Mailing List", "Documentation", "DNSSEC References", and "Download".

The main text describes DNSSHIM as an open-source software implementing the DNS protocol for the Internet, highlighting its role as a *Hidden Master* nameserver and its support for DNSSEC.

A "News" section lists two releases:

29-May-2009	Released DNSSHIM 0.1beta2 - "Constantinople": Second Public Beta Release [bin][source]
22-May-2009	Released DNSSHIM 0.1beta1 - "Pac-Man Hug": First Public Beta Release [bin][source][pydnsshim client]

At the bottom, there is a "Comments:" section with the email address `dnsshim@registro.br`.

The browser's status bar at the bottom shows a search function with a "Find" input field and options for "Next", "Previous", "Highlight all", and "Match case". The status is "Done".

Signing software

- Software voor automatisering processen
- Bij voorkeur open source (geen vendor lock-in)
- Robuust, betrouwbaar en toekomstbestendig
- Geschikt voor:
 - Grote TLD's (> 10M records)
 - Kleine/grote dns-operator met enkele of veel kleine zones
- Push the button technologie

Waarom OpenDNSSEC?

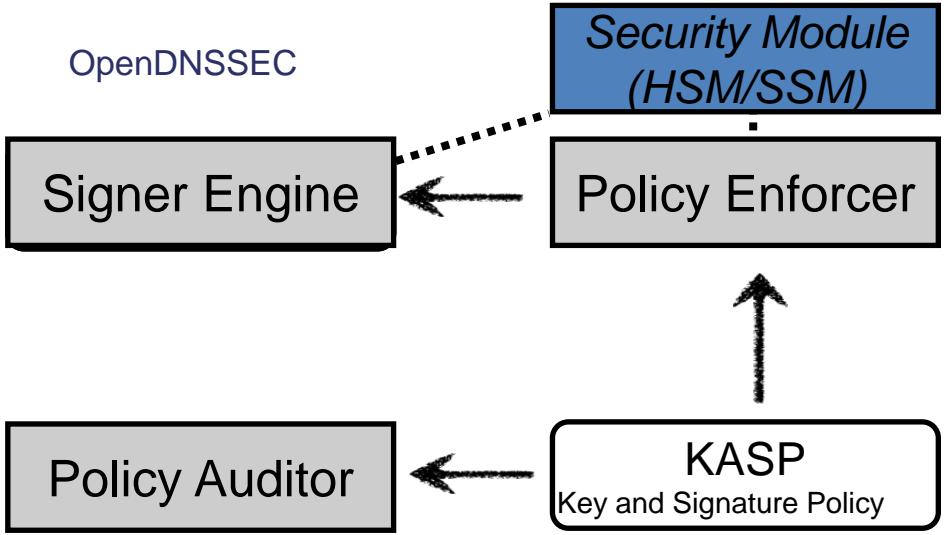
- SIDN wil een goede signer
- Voor zichzelf en DNS-community
- SIDN draagt bij aan OpenDNSSEC:
 - Requirements en review
 - Testplan en uitvoering
 - Geen bouwen (conflicteert met testen)
 - Samen met: .SE, Nominet, Kirei, NLnetLabs, Surfnets

Hardware/software signers





OpenDNSSEC



Issues tussen tier-1 en tier-2


Wijzigen DNS-operator: issue beschrijving


- Hoe verhuis je een DNSSEC-zone van de ene DNS-operator naar een andere
- Wetende dat registrars in een competitieve markt niet al te beste vrienden zijn
- Huidige registratie regels stellen dat een registrant altijd de 'controle' over zijn domein heeft

Wijzigen DNS-operator: betrokken partijen

- O = Observer i.e. DNS resolver
- L = Loosing DNS operator
- G = Gaining DNS operator
- P = Parent of Registry
- NI = Name servers van L (voor transfer)
- Ng = Name servers van G (na transfer)

Wijzigen DNS-operator in DNS, zonder DNSSEC

L	NI	NI	NI	
P	NI	NI	Ng	Ng
G		Ng	Ng	Ng
O	NI	NI	NI or Ng	Ng
	Before	Xfer req	Right after Xfer	Final




Alle twee de antwoorden zijn geldig in DNS

Wijzigen DNS-operator: hoe doen we dit met DNSSEC?

- Alle experts hebben naar de volgende vraag gekeken:
 - Wijzigen DNS-operator voor een DNSSEC-zone met als voorwaarde:
 - *Geen Outage !!*
 - *Handhaven bestaande processen*
 - Dat is niet gelukt
 - In elk scenario was er een mogelijke fout in het resollen

Wijzigen DNS-operator: waarom is er een probleem?

L	NI	NI	NI		
P	NI	NI	Ng		Ng
G		Ng	Ng		Ng
O	NI	NI	NI or Ng		Ng
	Before	Xfer req	Right after Xfer		Final

Als er slechts één sleutel is, is er slechts één van de twee antwoorden geldig.

Wijzigen DNS-operator: mogelijke oplossingen (1)

- Insecure worden tijdens de verhuizing
- Mogelijke oplossing voor eenvoudige domeinen
- Geen oplossing voor bank.nl
- Attack window tijdens de verhuizing
- Niet erg wenselijk

Wijzigen DNS-operator: mogelijke oplossingen (2) (althans in theorie)

- Vraag private key aan de loosing DNS-operator
- Registrant geeft private key aan de gaining operator om de nieuwe data en keys te signen
- Dit is een no-go wat security betreft
- HSM's staan niet eens toe dat de private key gekopieerd kan worden
- HSM (keycard) overdragen?

Wijzigen DNS-operator: mogelijke oplossingen (3)

- Gaining operator maakt nieuwe zone and keys
- Stuur de nieuwe public keys naar de losing operator (via registrant of registry)
- Losing operator signeert de nieuwe public keys met de oude private key (key rollover)
- Registry neemt zowel oude als nieuwe DS op
- Een DS TTL na signing, kan transfer doorgaan

Wijzigen DNS-operator: oplossing

L	NI	NI	NI	
P	NI	NI	Ng	Ng
G		Ng	Ng	Ng
O	NI	NI	NI or Ng	Ng
	Before	Xfer req	Right after Xfer	Final



- Beide versies zijn geldig met DNSSEC als:**
- de nieuwe zone ondertekend is met oude private key
 - de oude zone de nieuwe public key bevat

Wijzigen DNS-operator: conclusies en aanbevelingen

- Wijzigen DNS-operator van DNSSEC-domeinen werkt enkel indien de losing dns-operator meewerkt, en nog veranderingen aan het domein toestaat nadat de klant heeft opgezegd en niets meer betaalt
- Hoe gaan we dit voor de .nl-zone oplossen?
 - Regelgeving?
 - Overlaten aan de markt en bewustzijn promoten in de markt?
 - Andere opties?

Key rollovers

- 1x in de zoveel tijd nieuwe keys genereren
- Keys moeten worden verstuurd naar parent
- Verschillende key rollover scenario's
- Timing issues van groot belang
 - Risico: domein werkt niet

HSM's en rollovers (multiple zones)

- Meeste HSM's kunnen slechts beperkt aantal keys aan
- Incentive voor hosters om keys te hergebruiken voor meerdere zones
- Tot wel meer dan 100.000 zones met 1 key
- Wat doe je dan met verhuizingen? (timing issues)
- Wat doe je dan met key rollovers? (registry)
- Hergebruiken geen goed idee-> 1 key per zone

Vragen

- Hoe moet dit worden opgelost voor .nl?
 - Regelgeving (bijv. 1 key per domein)?
 - SLA op EPP-interface?
 - Bulkproces bij parent? Is dat mogelijk/wenselijk?

Key management

- DNS werkt parent-child
- Domein registratie werkt Registry-Registrar-Reseller-Registrant-DNS-operator
- Key updates zijn time-critical
- Liefst rechtstreeks via DNS, bijv. via notify
- EPP voor bootstrapping
- ICANN policy wordt fout geïnterpreteerd, hoe zit dat voor .nl?

Registry system security

- Als DNS straks waterdicht is wordt het registry systeem de weakest link
- Meer aanvallen te verwachten, security verhogen
- Voorbeelden in Nieuw Zeeland, Afrika
- Zowel registry als registrar kwetsbaar
- Zoek een betrouwbare registrar, onthoudt je credentials, en houd je gegevens goed bij

Overige zaken



Laatste hobbel: resolvers

- Alle resolvers moeten DNSSEC doen
 - Bij ISP's, bedrijven, etc.
 - Maar ook die in DSL-routers!
- Onderzoek heeft aangetoond dat 75% van CPE-routers 'DNS-dingetjes' doen die mogelijk fout gaan met DNSSEC (EDNS0, TCP)

WAARSCHUWING: DNSSEC gaat er komen

- Ook al wilt u zelf nog geen DNSSEC hosting gaan doen, het signen van de root en .nl gaat invloed hebben!
- Resolvers gaan grotere responses krijgen als u of uw klanten daar DNSSEC aanzetten
- Bereid uw infrastructuur voor op DNSSEC
 - Dus ook de firewalls/routers voor uw nameservers (EDNS0/TCP)
 - En ook de CPE's van klanten met eigen resolvers/validators

Meepraten

- dnssec.nl platform
 - Discussieplatform over DNSSEC invoering
 - Kenniscentrum en adviserende rol naar alle bij DNSSEC betrokken partijen
 - Zoekt o.a. oplossingen voor aangedragen issues
 - Op zoek naar DNS(SEC)-experts vanuit alle disciplines
- Kijk op www.dnssec.nl

Questions?

Antoin Verschuren
SIDN
antoin.verschuren@sidn.nl

