

# DNSSEC

Sebastian Castro



# This presentation is not...

- A DNSSEC introductory course
  - But ask any question you like
- A DNSSEC tutorial
- An HSM showcase or sales pitch

# This presentation IS

- A snapshot of current status of deployment
- A review of NZRS DNSSEC architecture
  - Technical components
  - Policy components
  - Procedures
- A review of DNSSEC potential
  - DANE, for example

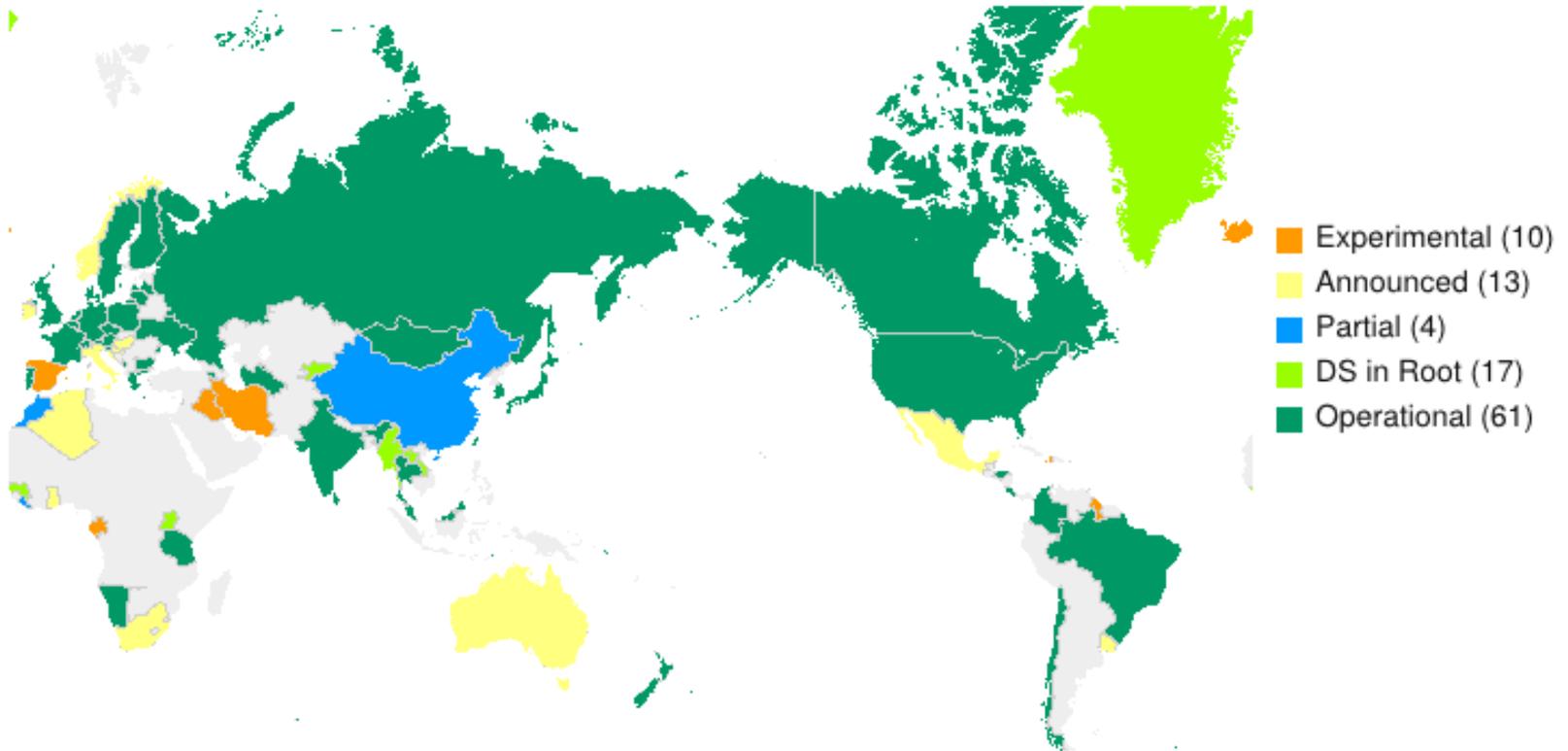
# A short “detour”

- DNSSEC
  - Authentication and integrity to DNS data by adding cryptographic signatures
  - Requires cryptographic keys
  - Makes DNS errors more visible
  - New set of potential errors: bogus data due to missing keys, missing sigs, etc.

# Current deployment status

- Globally

ccTLD DNSSEC Status on 2013-09-09



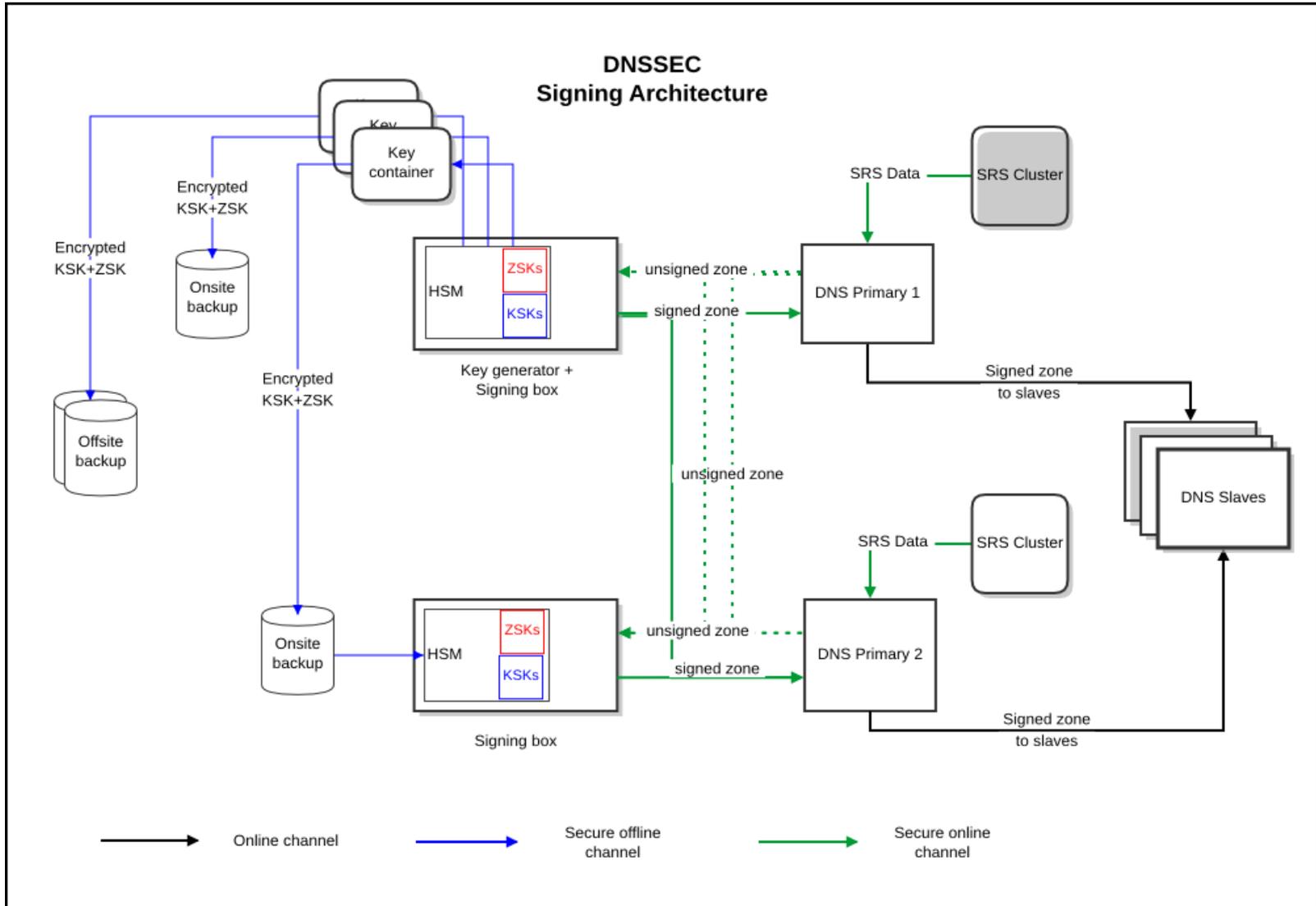
# Current deployment status

- Locally
  - 115 domains signed
    - Several from geeks, with some organizations as Unleashed, GodZone, RadioNZ
  - 94 with DS records (includes the second level domains)
  - 2 registrars DNSSEC-friendly

# NZRS DNSSEC Architecture

- Main features
  - Resilient: built with BC and DR in mind (in line with company policy)
  - Robust
  - Bump in the wire
  - Separations of roles (operators, security officers)

# Overview



# Architectural decisions

- KSK/ZSK or CSK?
- Online/Offline KSK
- How to feed the zones for signing? Zone transfers, copying files, database backend
- How to distribute the zones?

# Policy Components

- DNSSEC Practice Statement
  - Prepared based on RFC 6841
  - Defines policies around keys, responsibilities, roles, security controls, etc.
  - Our DPS publicly available at <http://www.nzrs.net.nz/dns/dnssec/dps>

# DPS: a glimpse

- ZSK
  - 1024 bits, RSA
  - Lifetime: 3 months
  - Automatic rollovers
- KSK
  - 2048 bits, RSA
  - Lifetime: 12 months
  - Manual rollovers

# DPS (2)

## Roles

- System Administrator (SA)
- Keystore Security Officer (KSO)
- Device Security Officer (DSO)
- Key Generation Administrator (KGA)
- Witness (WI)

## Zone Signing Params

- Signature validity period: 12 to 16 days
- Refresh time: 3 days
- TTLs
- Authenticated denial of existence

# Key Generation Procedure

- Key Generation Procedure
  - Create new keys for the next period
  - Remove used keys
  - Create HSM backup
- Requires a SA, SO, KGA, audit trails, etc
- Material available at <http://www.nzrs.net.nz/dns/dnssec>
- We've done two so far

# HSM

- Hardware Security Modules
  - Provide protection to private component of keys
  - Operate as blackboxes: provide them with data to sign, the id of the key and they will sign
  - Different certifications:
    - FIPS 140-2
    - CC-EAL

# HSM (2)

- Many many alternatives:
  - Going from USD\$0 to 100K
  - Differentiation points: level of certification, speed, algorithm support, key size support
- Do I need an HSM to do DNSSEC?
  - Not necessarily, depends on how much do you value your keys.
  - There are TLDs not using HSM for DNSSEC. Risk management has been done differently

# Is there value on DNSSEC?

- The IETF DANE WG is working on standards to publish data that will enable trust
  - TLSA records for SSL Certificates, which will affect Web, Mail, XMPP, SIP, etc.
  - Fingerprint for PGP keys
  - SSH fingerprints for servers (SSHFP)
- During IETF88, the commitment was to bring encryption to all protocols, as much as possible.
- DNS (with DNSSEC) will serve as bootstrap for trust

# Status of DNS tools

- **For signing:** pretty much done. BIND, PowerDNS, OpenDNSSEC do signing. KnotDNS will add it soon
- **For validation:** done. BIND, Unbound, major DNS vendors support validation
- **For applications:** getting there.
  - DNSSEC validator for the browser
  - OpenSSH in FreeBSD 10 will silently trust valid signed SSHFP records
  - Postfix support added
  - A DNS API is being discussed that will provide secure signalling to applications.

# Some examples

Internet Engineering Task Force (IETF) - Google Chrome

Internet Engineering Task Force (IETF) - Google Chrome

www.ietf.org



## The Internet Engineering Task Force (IETF)

**The goal of the IETF is to make the Internet work better.**

The mission of the IETF is to make the Internet work better by producing high quality, relevant technical documents that influence the way people design, use, and manage the Internet. Newcomers to the IETF should [start here](#).

**News**      **Next Meeting: IETF 89, March 2-7, 2014**

[Open](#) • [Leading Engineers Agree to Upgrade](#)      IETF 89, London, England (UTC+0)

[Home](#)  
[About the IETF](#)  
[Mission](#)  
[Standards Process](#)  
[Info Wall](#)

[Chat Live with the IETF Community](#)

**www.ietf.org Secured by DNSSEC**

Domain name www.ietf.org is correctly secured by DNSSEC.

Information about the IP address of this domain name was validated using DNSSEC. Because this domain name is secured by DNSSEC, you are protected against domain name spoofing.

[Go to plugin homepage for additional information](#)

Unleash - Data Centre and Internet Services - New Zealand Colocation, Internet Access and Business ISP Services - Google Chrome

Unleash - Data Centre and Internet Services - New Zealand Colocation, Internet Access and Business ISP Services - Google Chrome

www.unleash.co.nz

Connected via IPv6 · Customer Login · Contact Us



## Unleash

Data Centre and Internet Services



**www.unleash.co.nz Secured by DNSSEC**

Domain name www.unleash.co.nz is correctly secured by DNSSEC.

Information about the IP address of this domain name was validated using DNSSEC. Because this domain name is secured by DNSSEC, you are protected against domain name spoofing.

[Go to plugin homepage for additional information](#)

Radio New Zealand - Google Chrome

Radio New Zealand - Google Chrome

www.radionz.co.nz

Wednesday 13 November - 8:48 a



## RADIO NEW ZEALAND

TE REO IRIRANGI O AOTEAROA

[HOME](#)   [NATIONAL](#)   [CONCERT](#)   [NEWS](#)   [INTERNATIONAL](#)  

[Listen Live to National](#)   [Listen Live to Concert](#)   [Listen Live to International](#)

**www.radionz.co.nz Secured by DNSSEC**

Domain name www.radionz.co.nz is correctly secured by DNSSEC.

Information about the IP address of this domain name was validated using DNSSEC. Because this domain name is secured by DNSSEC, you are protected against domain name spoofing.

[Go to plugin homepage for additional information](#)

Questions?



Internet Access: