

# Signing the Root

AusNOG-04  
Sydney  
September 2010

Dave Knight



# Contents

- DNSSEC History
- Signing the Root
- The Root is Signed!
- Questions?

# DNSSEC History

# First some DNS history

# 1983

- Paul Mockapetris invents the Domain Name System
- Described in RFCs 882 and 883
- Implements the first server: Jeeves

# 1987

- Now a formal Internet Standard, two RFCs describe DNS (obsoleting 882 and 883):
  - ▶ *RFC 1034: Domain Names - Concepts and Facilities*
  - ▶ *RFC 1035: Domain Names - Implementation and Specification*
- DNS begins to catch-on

# 1990

Stephen Bellovin discovers a flaw in the DNS.

As DNS is already widely deployed on the Internet the flaw is kept secret while research is started on a secure replacement for DNS.

# 1995

- Bellovin's paper *Using the Domain Name System for System Break-ins* is published
- DNSSEC becomes a topic within the IETF



The DNSSEC story  
starts here

# 1997

*RFC 2065 Domain Name System Security  
Extensions*

# 1999

- *RFC 2535 Domain Name System Security Extensions*
- Obsoletes RFC 2065
- DNSSEC appears to be complete
- BIND9 is being developed to implement DNSSEC

# 2000

- BIND 9.0.0 is released
  - ▶ First implementation of DNSSEC

# 2001

- Key handling in RFC 2535 is causing operational problems that will make deployment impossible.
- The Delegation Signer resource record is proposed to solve the problems. It only exists in the parent zone, so introduces protocol difficulty of its own.
- BIND9 doesn't understand the new DS RR.
- It's decided to rewrite RFC 2535 in 3 new drafts.

# 2003

- BIND9 snapshots appear that support what is now known as DNSSEC-bis
- NLnet Labs SECREG shows that DNSSEC-bis is ready for deployment

# 2004

- BIND 9.3 and NSD 2 have support for DNSSEC-bis

# 2005

- The DNSSEC-bis RFCs are published
  - ▶ *RFC 4033: DNS Security Introduction and Requirements*
  - ▶ *RFC 4034: Resource Records for the DNS Security Extensions*
  - ▶ *RFC 4035: Protocol Modifications for the DNS Security*
- .SE (Sweden) is the first signed ccTLD
- RIPE NCC begin signing their portion of the in-addr.arpa tree



# DNSSEC-bis

- Adds these new RR types
  - ▶ DNSKEY, DS, RRSIG, NSEC
- Provides
  - ▶ Origin authentication
  - ▶ Data integrity
  - ▶ Authenticated denial of existence
- Doesn't provide confidentiality
- Enables zone enumeration
- Makes zones much bigger

# How DNSSEC-bis works

- Public key crypto, public keys published in-zone in the DNSKEY RRSets
- Signatures made using those keys for each RRSets in the zone, in an RRSIG record
  - ▶ RRSIGs have an inception and expiry time, so must be periodically replaced
- DS record is a hash of the DNSKEY placed in the parent zone and signed by its key, asserting trust across the delegation
- NSEC records point to the Next domain name and lists the types it has

# How DNSSEC-bis works - 2

## EXAMPLE.ORG:

```
example.org. DNSKEY 257 3 8 AwEAAeikvxboZpn9VCxm3YDLHo40SvA9E
```

```
example.org. DNSKEY 256 3 8 AwEAAe+QdjC7q3keM67j6/WzSY+mDM0sM
```

```
example.org. RRSIG DNSKEY 8 2 3600 20100921030003  
20100913172516 31589 example.org. kFlg0Ners5QdT0sKKsfqzm6pZmg
```

## ORG:

```
example.org. DS 31589 8 1 7B8370002875DDA781390A8E586C3149384
```

```
example.org. DS 31589 8 2 3FDC4C11FA3AD3535EA8C1CE3EAF7BFA5CA
```

```
example.org. RRSIG DS 7 2 86400 20100923154605 20100909144605  
37812 org. dTmmpM7+TtMwUZBV7u1lSAgqsC8llAbQ2MjKfQSeFIbwUKjGGh
```

# How DNSSEC-bis works - 3

## THE ROOT:

au. NS a3.audns.net.au.

au. NS b1.audns.net.au.

au. NS b2.audns.net.au.

au. NS ns1.audns.net.au.

au. NS ns2.audns.net.au.

au. NS ns3.audns.net.au.

au. NS ns4.audns.net.au.

au. RRSIG NSEC 8 1 86400 20100919000000 20100911230000  
41248 . c9XQFK36eSGRH3vYASrFJkBk7DYzqw4TEdzubLCQMC8LEvZtfQFFZ

au. NSEC aw. NS RRSIG NSEC

# 2006

- ISC launches their Domain Lookaside Validation Registry: [dlv.isc.org](http://dlv.isc.org)
- .PR (Puerto Rico) is signed

# 2007

- .BR (Brazil) is signed
- .BG (Bulgaria) is signed

# 2008

- .CZ (Czech Republic) is signed
- *RFC 5155: DNS Security (DNSSEC) Hashed Authenticated Denial of Existence*
  - ▶ New RR type: NSEC3
  - ▶ Solves zone enumeration
  - ▶ Opt-in allows incremental growth in delegation-centric zones
- Dan Kaminsky discovers a new cache poisoning vulnerability
- The US DoC NTIA publish a Notice of Inquiry entitled “Enhancing the Security and Stability of the Internet’s Domain Name and Addressing System”

# 2009

- IANA launches the ITAR
- .GOV is signed
  - ▶ First major use of NSEC3
- .ORG is signed
  - ▶ The first gTLD to be signed
- ICANN and VeriSign announce a joint project to sign the root



# Signing the Root

# The Project

A cooperation between ICANN & VeriSign  
with support from the U.S. DoC NTIA



# Roles and Responsibilities

# ICANN

IANA Functions Operator

- Manages the Key Signing Key (KSK)
- Accepts DS records from TLD operators
- Verifies and processes request
- Sends update requests to DoC for authorization and to VeriSign for implementation

# DoC NTIA

U.S. Department of Commerce  
National Telecommunications and Information Administration

- Authorizes changes to the root zone
  - ▶ DS records
  - ▶ Key Signing Keys
  - ▶ DNSSEC update requests follow the same process as other changes
- Checks that ICANN has followed their agreed upon verification/processing policies and procedures

# VeriSign

Root Zone Maintainer

- Manages the Zone Signing Key (ZSK)
- Incorporates NTIA-authorized changes
- Signs the root zone with the ZSK
- Distributes the signed zone to the root server operators

**Design**

The guiding principle  
behind the design is  
that the result must be  
trustworthy



# Transparency

Processes and procedures should be as open as possible for the Internet community to trust the signed root

# Audited

Processes and procedures should  
be audited against industry standards,  
e.g. ISO/IEC 27002:2005

# High Security

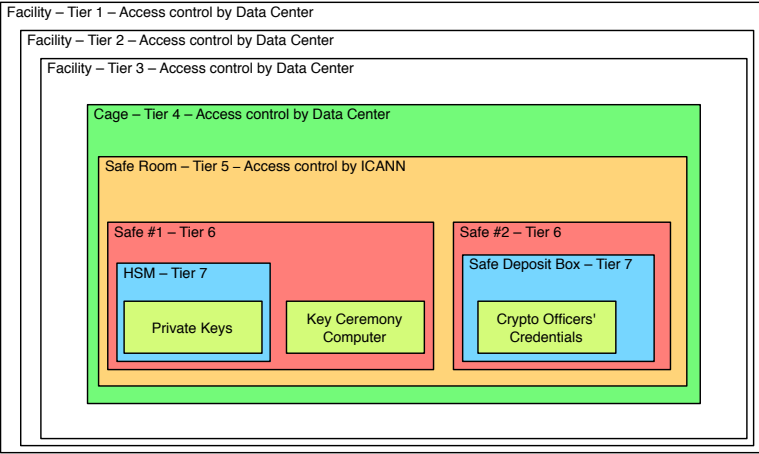
Root system should meet all NIST  
SP 800-53 technical security controls required  
by a HIGH IMPACT system

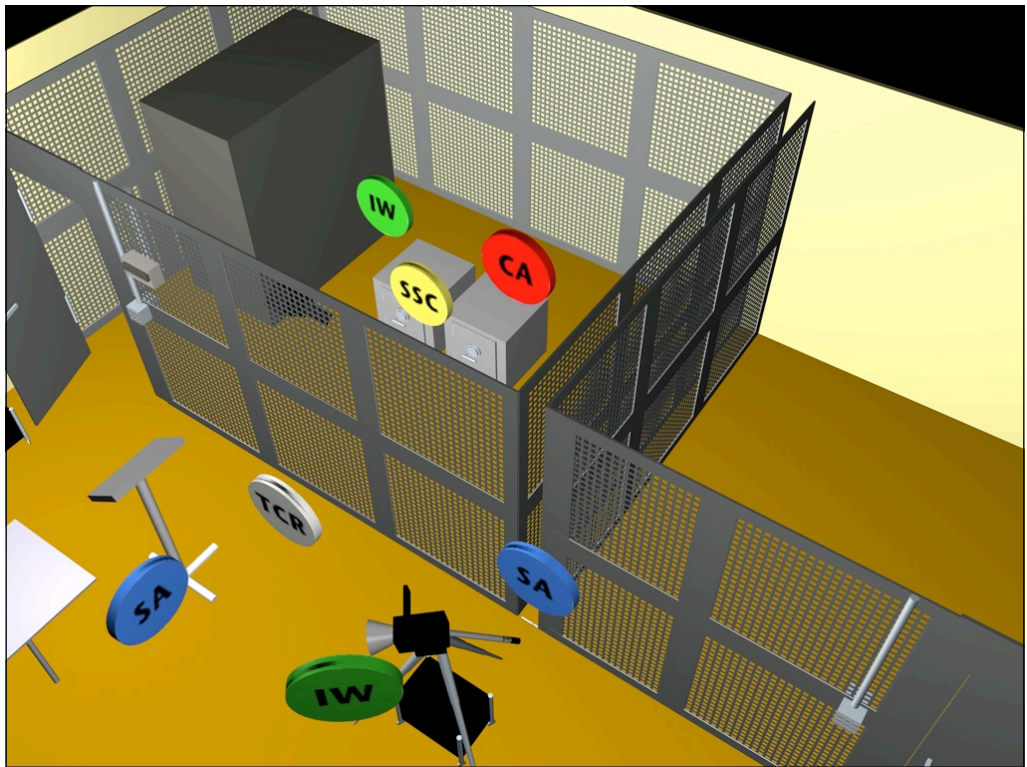
# Community Involvement

Trusted representatives from the community  
are invited to take an active role in the key  
management process

# Approach to Protecting the KSK

# Physical Security





# DPS

## DNSSEC Practice Statement

- States the practices and provisions that are employed in root zone signing and zone distribution services
  - ▶ Issuing, managing, changing and distributing DNS keys in accordance with the specific requirements of the U.S. DoC NTIA
- Comparable to a certification practice statement (CPS) from an X.509 certification authority (CA)



# Auditing & Transparency

- Third-party auditors check that ICANN operates as described in the DPS
- Other external witness may also attend the key ceremonies
- Working toward having a Systrust audit performed later this year

# Trusted Community Representatives (TCRs)

- Have an active roll in the management of the KSK
  - ▶ as Crypto Officers needed to activate the KSK
  - ▶ as Recovery Key Share Holders protecting shares of the symmetric key that encrypts the backup copy of the KSK

# Crypto Officer (CO)

- Have physical keys to safe deposit boxes holding smartcards that activate the HSM
- ICANN cannot generate new key or sign ZSK without 3-of-7 COs
- Able to travel up to 4 times a year to US.

## Recovery Key Shareholder (RKSH)

- Have smartcards holding pieces (M-of-N) of the key used to encrypt the KSK inside the HSM
- If both key management facilities fall into the ocean, 5-of-7 RKSH smartcards and an encrypted KSK smartcard can reconstituted KSK in a new HSM
- Backup KSK encrypted on smartcard held by ICANN
- Able to travel on relatively short notice to US. Hopefully never. Annual inventory.

## CO

---

Alain Aina, BJ  
Anne-Marie  
Eklund Löwinder, SE  
Frederico Neves, BR  
Gaurab Upadhaya, NP  
Olaf Kolkman, NL  
Robert Seastrom, US  
Vinton Cerf, US

Andy Linton, NZ  
Carlos Martinez, UY  
Dmitry Burkov, RU  
Edward Lewis, US  
João Luis Silva Damas, PT  
Masato Minda, JP  
Subramanian Moonesamy, MU

## CO Backup

---

Christopher Griffiths, US  
Fabian Arbogast, TZ  
John Curran, US  
Nicolas Antonello, UY  
Rudolph Daniel, UK  
Sarmad Hussain, PK  
Ólafur Guðmundsson, IS

## RKSH

---

Bevil Wooding, TT  
Dan Kaminsky, US  
Jiankang Yao, CN  
Moussa Guebre, BF  
Norm Ritchie, CA  
Ondřej Surý, CZ  
Paul Kane, UK

## BCK

---

David Lawrence, US  
Dileepa Lathsara, LK  
Jorge Etges, BR  
Kristian Ørmen, DK  
Ralf Weber, DE  
Warren Kumari, US

# DNSSEC Protocol Parameters

# Split keys

- The Zone Signing Key (ZSK) is used to sign the zone
- The Key Signing Key (KSK) is used to sign the ZSK
- This split is not required by the protocol, but it enhances security by reducing access to the key which forms the trust anchor while reducing the importance of the key which must be exercised often to sign the zone.

# Key Signing Key

- KSK is 2048-bit RSA
  - ▶ Rolled as required
  - ▶ RFC 5011 for automatic key rollovers
- Signatures made using SHA-256



# Zone Signing Key

- ZSK is 1024-bit RSA
  - ▶ Rolled once a quarter (four times per year)
- Zone signed with NSEC
- Signatures made using SHA-256

# Signature Validity

- DNSKEY-covering RRSIG (by KSK) validity 15 days
  - ▶ new signatures published every 10 days
- Other RRSIG (by ZSK) validity 7 days
  - ▶ zone generated and resigned twice per day

# Key Ceremonies

- Key Generation
  - ▶ Generation of new KSK
- Processing of ZSK Signing Request (KSR)
  - ▶ Signing ZSK for the next upcoming quarter
  - ▶ Every quarter

# Root Trust Anchor

- Published on a web site by ICANN as
  - ▶ XML-wrapped and plain DS record
    - to facilitate automatic processing
  - ▶ PKCS #10 certificate signing request (CSR)
    - as self-signed public key
    - Allows third-party CAs to sign the KSK
    - ICANN will sign the CSR producing a CERT

Deployment

# Goals

- Deploy a signed root zone
  - ▶ Transparent processes
  - ▶ Audited procedures
  - ▶ Community involvement

**Issues Anticipated  
Which Affected the  
Deployment Strategy**

# DO=1

- A significant proportion of DNS clients send queries with EDNS0 and DO=1
- Some (largely unquantified, but potentially significant) population of such clients are unable to receive large responses
- Serving signed responses might break those clients



# Rollback

- If we sign the root, there will be some early validator deployment
- There is the potential for some clients to break, perhaps badly enough that we need to un-sign the root (e.g., see previous slide)
- Un-signing the root will break the DNS for validators

# Staged Deployment

# Deploy Incrementally

- The goal was to leave the client population with some root servers not offering large responses until the impact of those large responses is better understood
- Relies upon resolvers not always choosing a single server

# DURZ

- Deploy conservatively
  - ▶ It is the root zone, after all
- Prevent a community of validators from forming
  - ▶ This allows us to un-sign the root zone during the deployment phase (if we have to) without collateral damage

# DURZ

- “Deliberately Unvalidatable Root Zone”
- Sign RRSets with keys that are not published in the zone (but with matching keytag...)
- Publish keys in the zone which are not used, and which additionally contain advice for operators (see next slide)
- Swap in actual signing keys (which enables validation) at the end of the deployment process



# Testing

- A prerequisite for this plan was a captive test of the deployment
  - ▶ Test widely-deployed resolvers, with validation enabled and disabled, against the DURZ
  - ▶ Test with clients behind broken networks that drop large responses

# Deploy Incrementally

L	27 January
A	10 February
M, I	March 3rd
D, K, E	March 22nd
B, H, C, G, F	April 12th
J	May 5th

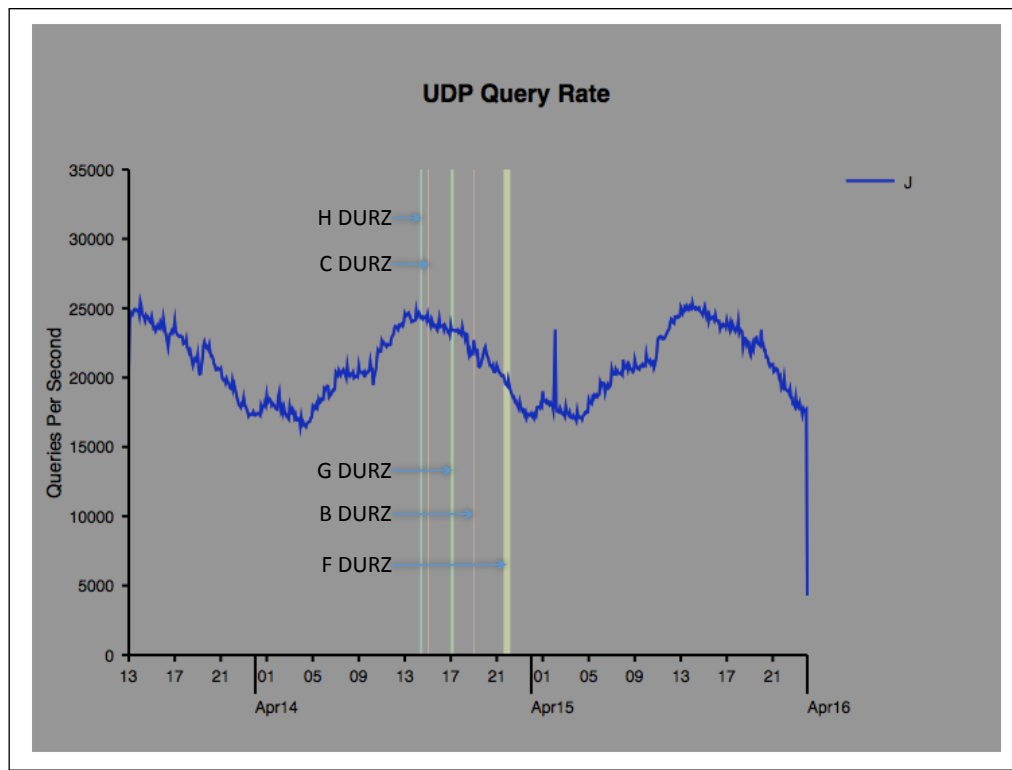


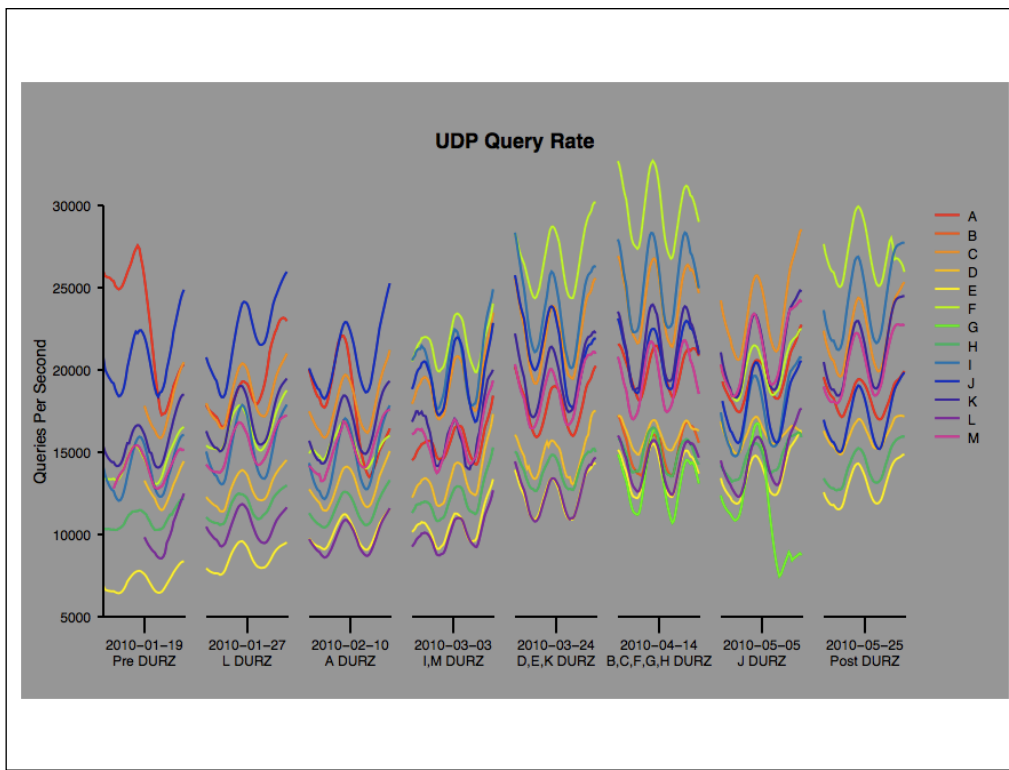
# Measurement

- Full packet captures and subsequent analysis around signing events in addition to long term collection of priming queries
- Dialogue with operator communities to assess real-world impact of changes

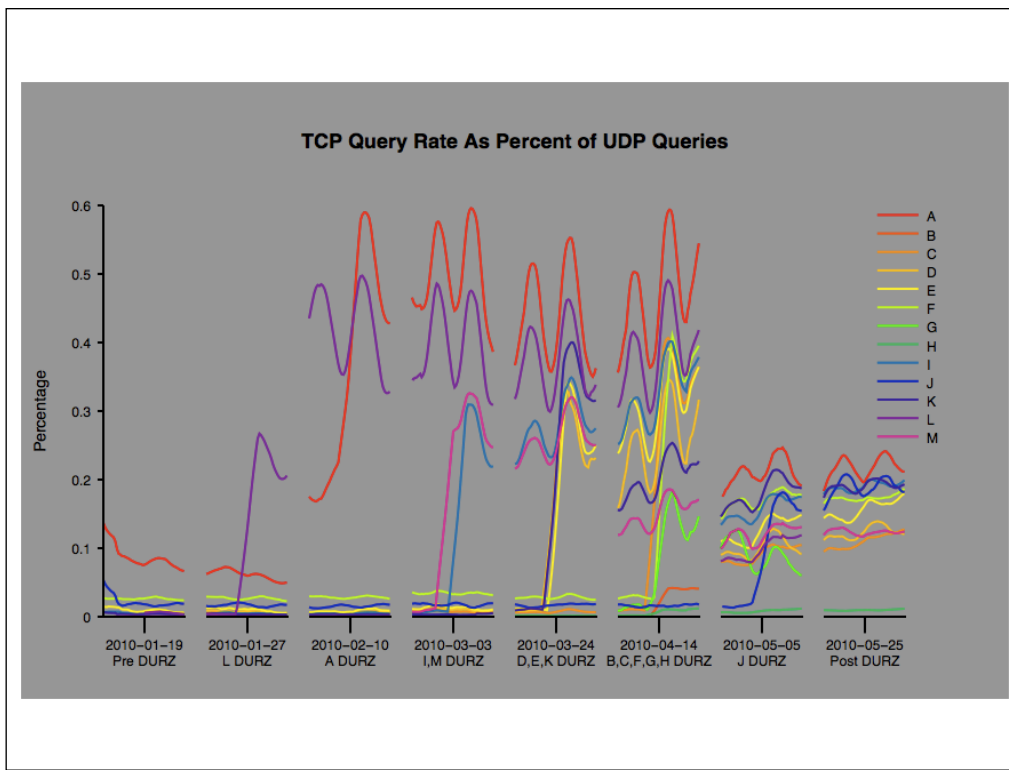
# DURZ Data Analysis

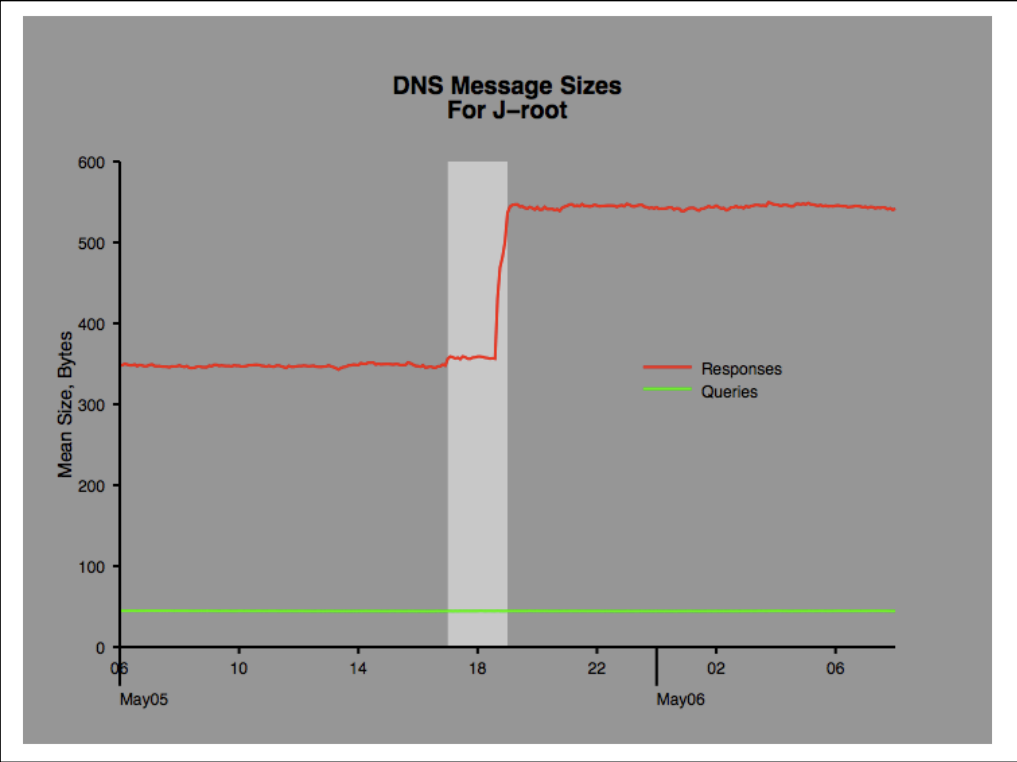
- Looking at the data for indications of problems
  - ▶ Query rates
  - ▶ TCP traffic
  - ▶ Message sizes
  - ▶ Priming queries











# Summary

- No problems evident in the data
- No problems reported by users



**Communication**

# Project Web Page

- <http://www.root-dnssec.org>
  - ▶ Status updates
  - ▶ Documents
  - ▶ Presentation Archive
  - ▶ Contact information

# Communication

- Reaching the technical audiences via mailing lists and other means, such as showing up in person to make presentations
  - ▶ IETF DNS lists (e.g. DNSOP)
  - ▶ non-IETF DNS lists (e.g. DNS-OARC)
  - ▶ General operator lists (e.g. NANOG)

# Milestones

# 2009

- August
  - ▶ Project to sign the root formally announced
- October
  - ▶ The plan receives first public airing at RIPE 59
- December
  - ▶ <http://www.root-dnssec.org> site launched
  - ▶ First signed root zone created internally at VeriSign

# 2010

- January through May
  - ▶ Incremental roll-out of the DURZ to the root servers
- June
  - ▶ First ceremony in Culpeper, Virginia
    - Created initial root zone KSK
    - Processed initial KSR for Q3/2010
  - ▶ First DS records added to the root zone

# Key Ceremony Participants and Attendees



# 2010

- July
  - ▶ Second ceremony in Los Angeles, California
    - Key material from the first ceremony replicated and stored
    - Q4/2010 KSR processed
  - ▶ The fully validatable signed root zone is published to the root servers by VeriSign
  - ▶ The root zone trust anchor is published by ICANN



# Root DNSSEC Design Team

Joe Abley  
Mehmet Akcin  
David Blacka  
David Conrad  
Richard Lamb  
Matt Larson  
Fredrik Ljunggren  
Dave Knight  
Tomofumi Okubo  
Jakob Schlyter  
Duane Wessels

# The root is signed!

DNSSEC is now part of standard operations

# ARPA

- ARPA is signed since March
  - ▶ Keys currently managed by Verisign, will change to a joint model like the root
- E164.ARPA signed by RIPE NCC since 2007
- Other ARPA children, with the exception of IN-ADDR.ARPA are signed by ICANN since April
  - ▶ Addition of DS records to ARPA in progress

# DS Submission

- TLD operators can submit DS records to the IANA for inclusion in the root zone
- Instructions
  - ▶ <http://www.iana.org/procedures/root-dnssec-records.html>

# Secured delegations

As of the start of this week the root zone contains 32 secured delegations

be bg biz br

cat ch cz dk

edu eu info lk

museum na org

pm se tf

tm uk us

...and the 11 test IDN  
TLD zones

# Start your validators!

- The trust anchor is available at
  - ▶ <https://www.iana.org/dnssec/>

# Questions?

[dave.knight@icann.org](mailto:dave.knight@icann.org)