

# DNSSEC for the Root Zone

UKNOF 16, London, April 2010

Richard Lamb, ICANN



This design is the result of a cooperation  
between ICANN & VeriSign with  
support from the U.S. DoC NTIA

# Quick Recap

- 2048-bit RSA KSK, 1024-bit RSA ZSK
- Signatures with RSA/SHA-256
- Split ZSK/KSK operations
- Incremental deployment
- Deliberately Unvalidatable Root Zone (DURZ)

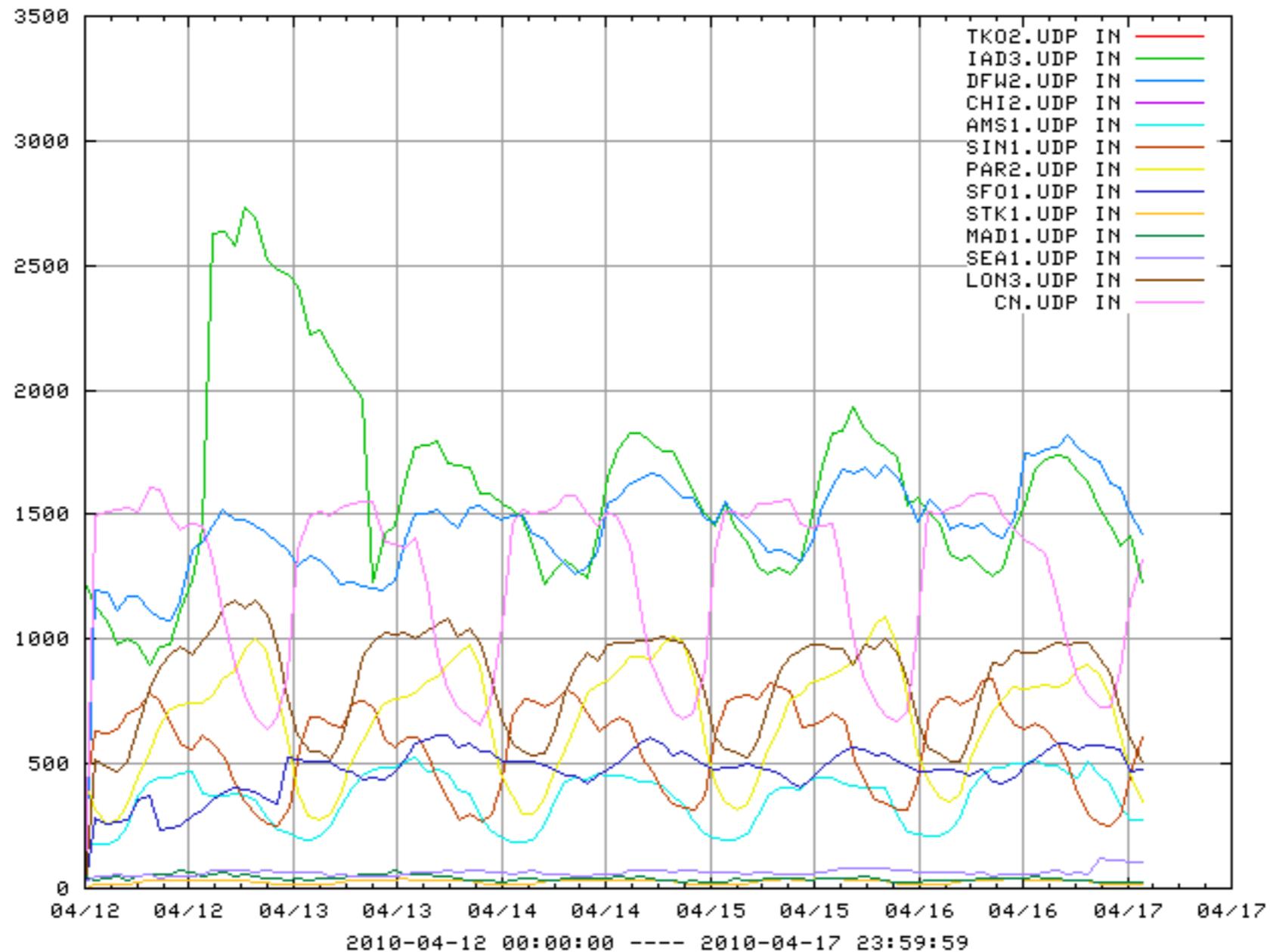
# DURZ Deployment

- The Deliberately Unvalidatable Root Zone (DURZ) deployment started on January 27.
- As of today – 12 root server operators are serving the DURZ.

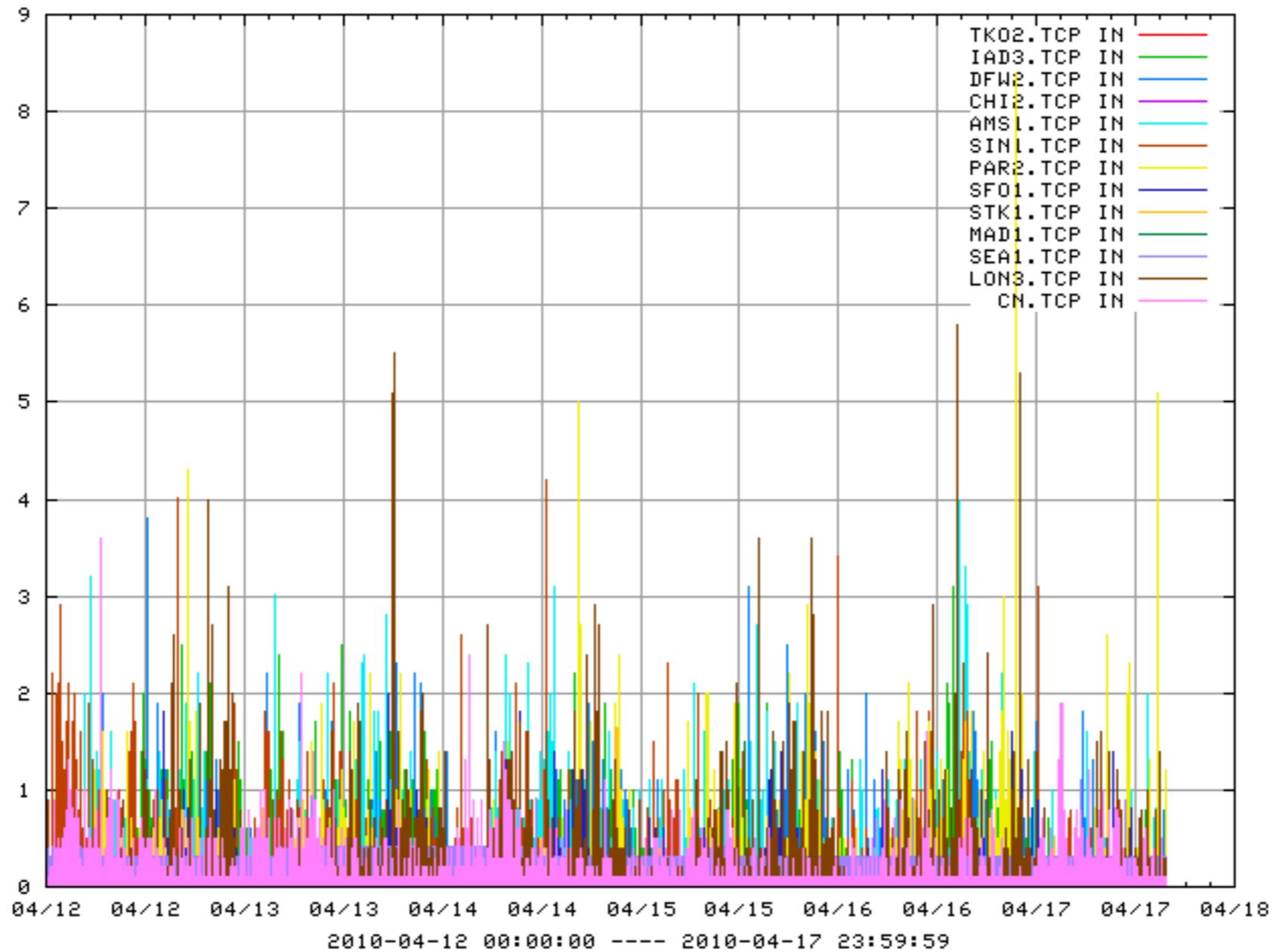
# Root Server Status

Root Server	Operated by	Signed ARPA	DURZ	LTQC	DITL
A	VeriSign	2010-03-16	2010-02-10	submitting	submitting
B	ISI	2010-03-16	2010-04-14	unknown	unknown
C	Cogent	2010-03-16	2010-04-14	submitting	submitting
D	UMD	2010-03-16	2010-03-24	submitting	submitting
E	NASA	2010-03-16	2010-03-24	submitting	submitting
F	ISC	2010-03-17	2010-04-14	submitting	submitting
G	US DoD	2010-03-16	2010-04-14	submitting	submitting
H	US Army	2010-03-16	2010-04-14	submitting	submitting
I	Autonomica	2010-03-15	2010-03-03	submitting	submitting
J	VeriSign	N/A	2010-05-05	submitting	submitting
K	RIPE NCC	2010-03-15	2010-03-24	submitting	submitting
L	ICANN	2010-03-15	2010-01-27	submitting	submitting
M	WIDE	2010-03-15	2010-03-03	submitting	submitting

# UDP Traffic @ J-Root



# TCP Traffic @ J-Root



# Key Ceremonies

- Key ceremonies tested and exercised during January and February.
  - ▶ See [Root Zone DNSSEC KSK Ceremonies Guide](#) for more information.
- The secure facilities are being fine tuned to meet the requirements set by DoC and the expectations set by the community.

# TCR Proposal

- Draft document describing how recognized members of the DNS technical community could be part of the key management process has been published.
- ▶ Visit <http://www.root-dnssec.org/tcr/> for more information

# DS Change Requests

- Approach likely to be based on existing methods for TLD managers to request changes in root zone.
- Anticipate being able to accept DS requests 1-2 months before the validatable signed root zone is in production.

# Policy Update

- Updated versions of the draft KSK and ZSK DNSSEC Practice Statements (DPS) will be published shortly.
  - ▶ Not much has changed substantively, but please read these practice statements – answers to most questions regarding DNSSEC for the Root Zone can be found in the DPS.

# Documentation

Available at [www.root-dnssec.org](http://www.root-dnssec.org)

- Requirements
- High Level Technical Architecture
- DNSSEC Practice Statements (DPS)
- Trust Anchor Publication
- Deployment Plan
- KSK Ceremonies Guide
- TCR Proposal
- Resolver Testing with a DURZ

# Questions & Answers

**rootsign@icann.org**

# 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