DNSSEC for the Root Zone

Questions & Answers Session at
IETF'77 Anaheim, March 2010

Jakob Schlyter

Richard Lamb, ICANN Matt Larson, VeriSign

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)

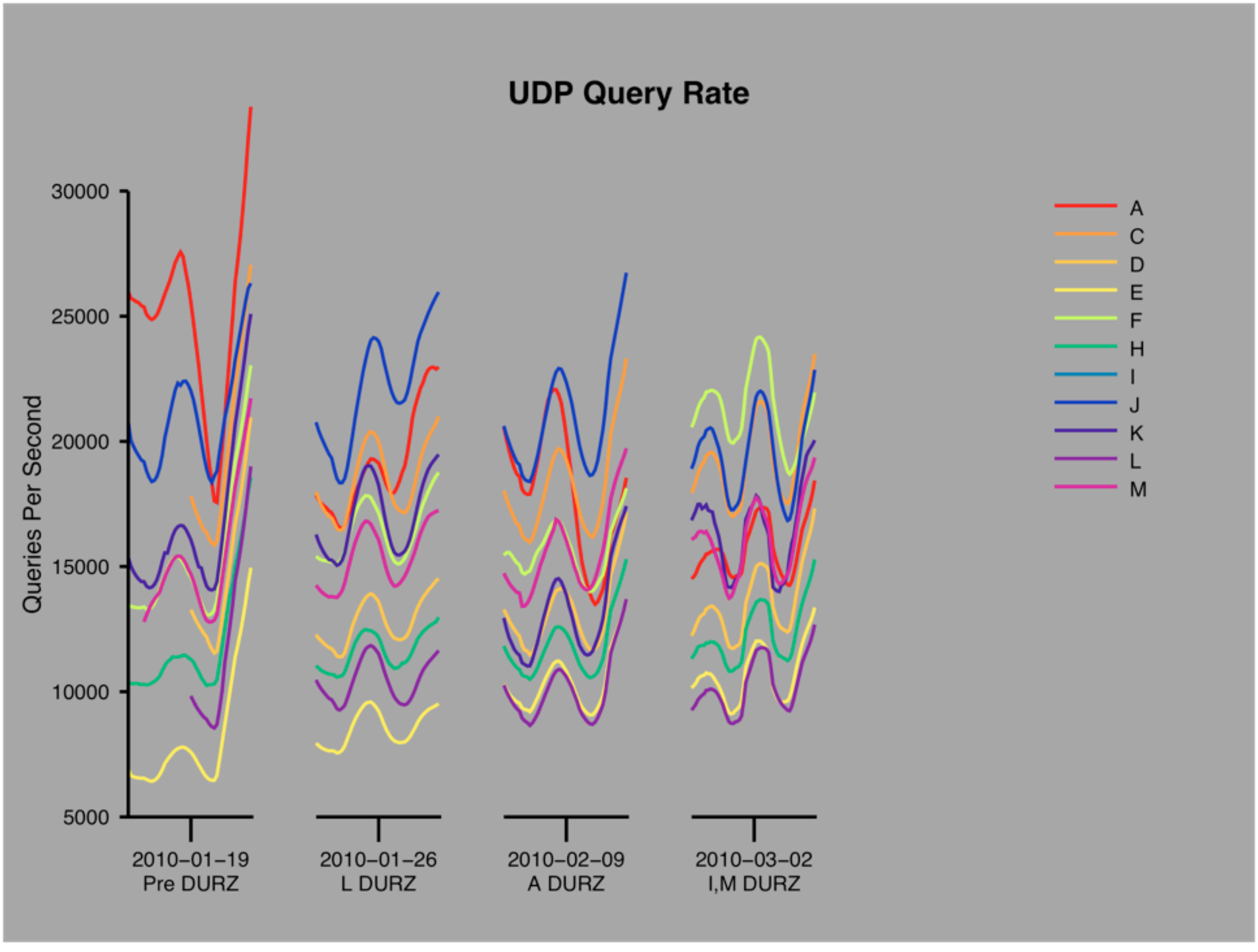
What's happened since IETF'76 ?

DURZ Deployment

- The Deliberately Unvalidatable Root Zone (DURZ) deployment started on January 27.
- As of today – 4 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 Query Rate
Queries Per Second
30000
25000
20000
15000
10000
5000
2010–01–19
Pre DURZ
2010–01–26
L DURZ
2010–02–09
A DURZ
2010–03–02
I,M DURZ
A
C
D
E
F
H
I
J
K
L
M


TCP Query Rate
Queries Per Second
100
80
60
40
20
0
2010–01–19
Pre DURZ
2010–01–26
L DURZ
2010–02–09
A DURZ
2010–03–02
I,M DURZ
A
C
D
E
F
H
I
J
K
L
M

Key Ceremonies

- Key ceremonies has been 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 NTIA 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.
  - See Trusted Community Representatives – Proposed Approach to Root Key Management 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

- An minor update of the DNSSEC Practice Statements (DPS) for the KSK and ZSK will be published shortly.
  - Not much has changed, but please read this policy – answers to most questions regarding DNSSEC for the Root Zone can be found in the DPS.

Documentation

Available at www.root-dnssec.org

- Requirements
- High Level Technical Architecture
- Policy and Practice Statements
- 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