DNSSEC for the Root Zone – Update

IETF 78, Maastricht, The Netherlands
27 July 2010

Joe Abley, ICANN and 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)

Deployment Status

- **Done!**
- Full production on July 15, 2010
  - Already had DURZ at every root server
  - Keys became unobscured
- No problems reported

DS Record Change Requests

- DS record requests being accepted by IANA now
- TLD change template now includes DS records
- DS RRsets for *bg*, *br*, *cat*, *cz*, *lk*, *na*, *org*, *tm*, *uk* already in the root

Trusted Community Representatives (TCRs)

- Crypto Officers (CO)
- Recovery Key Shareholders (RKSH)
- Not from an organization affiliated with the root zone management process
  - ICANN, VeriSign or the U.S. Department of Commerce

TCRs

- Crypto Officers (COs)
  - 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
  - Don't lose the (physical) key

TCRs

- Recovery Key Share Holders (RKSHs)
  - 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 reconstitute KSK in a new HSM
    - Backup KSK encrypted on smartcard held by ICANN
  - Able to travel on relatively short notice to US, but hopefully never
  - Annual inventory

Crypto Officers (COs)

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

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

Backup COs

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

Recovery Key Shareholders (RKSHs)

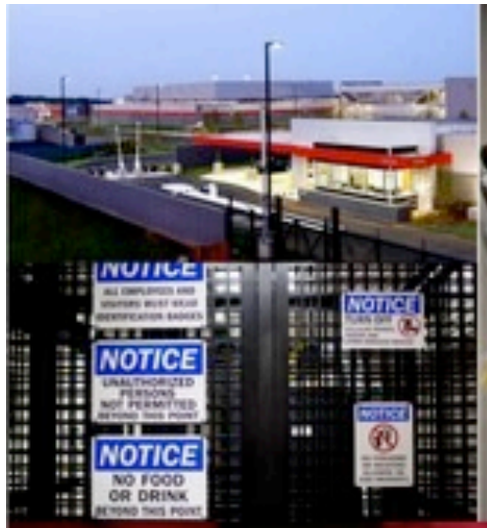
Bevil Wooding, TT
Dan Kaminsky, US
Jiankang Yao, CN
Moussa Guebre, BF
Norm Ritchie, CA
Ondřej Surý, CZ
Paul Kane, UK

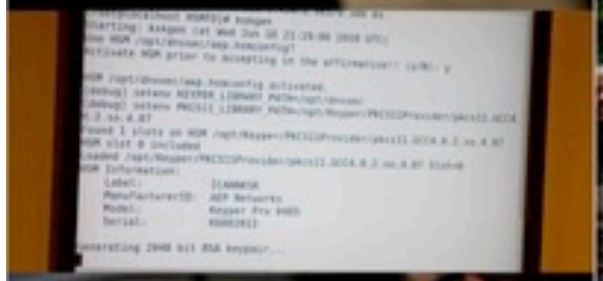
Backup RKSHs

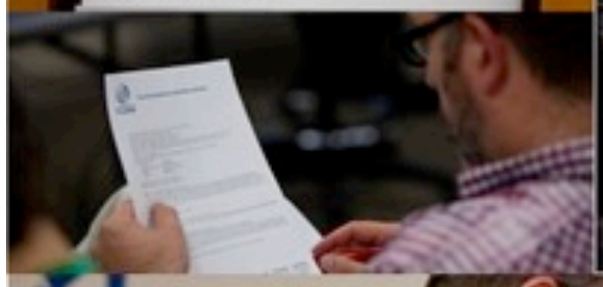
David Lawrence, US
Dileepa Lathsara, LK
Jorge Etges, BR
Kristian Ørmen, DK
Ralf Weber, DE
Warren Kumari, US

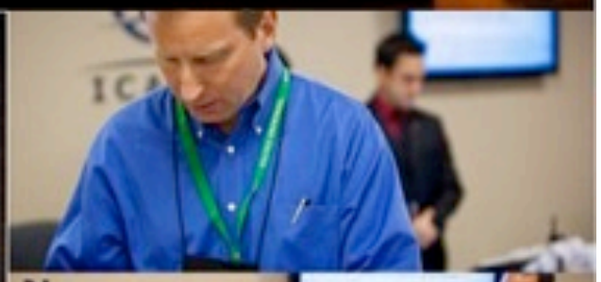
Key Ceremonies

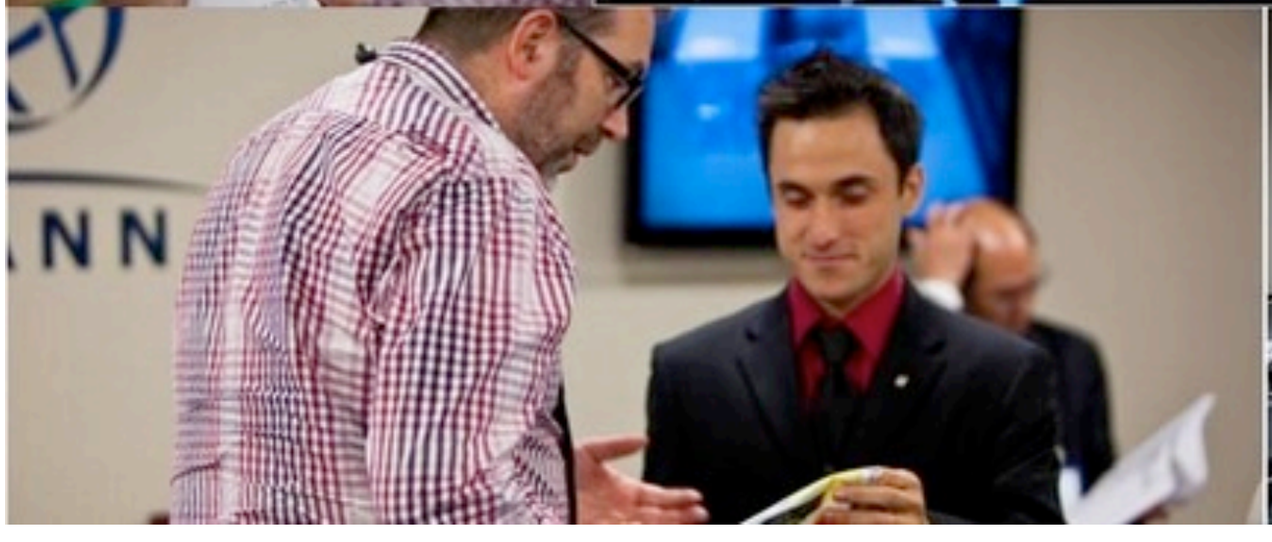
- Ceremony #1: June 16, 2010, Culpeper, VA
  - KSK created, Q3 root DNSKEY RRsets signed
  - Recovery Key Shareholders and East Coast Crypto Officers enrolled
- Ceremony #2: July 12, 2010, Los Angeles, CA
  - KSK installed, Q4 root DNSKEY RRsets signed
  - West Coast Crypto Officers enrolled


NOTICE
NOTICE
NOTICE
NOTICE
NO FOOD
OR DRINK










One World. One Internet. Everyone Connected.
19036

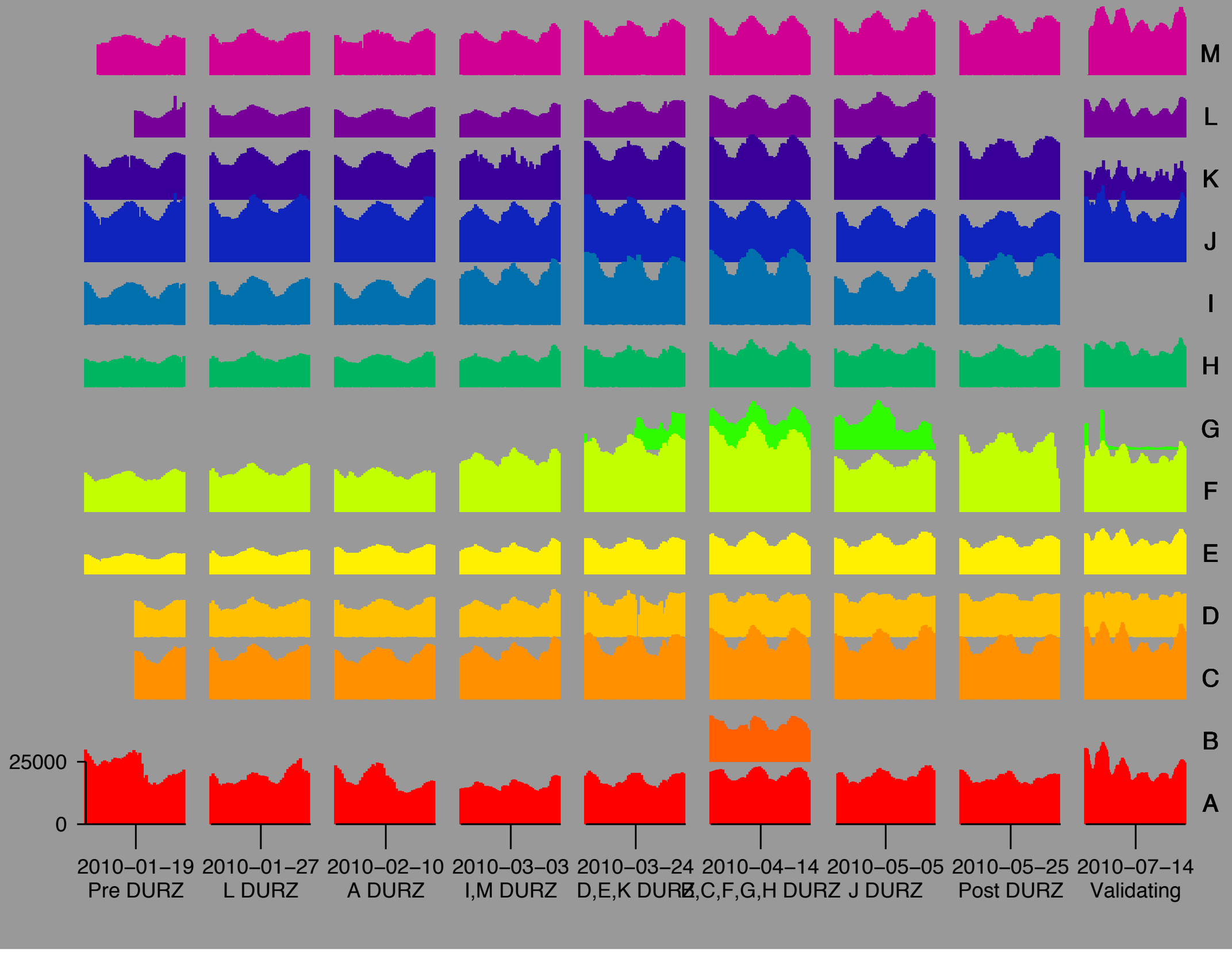
Key Ceremony Video

- To be inserted here

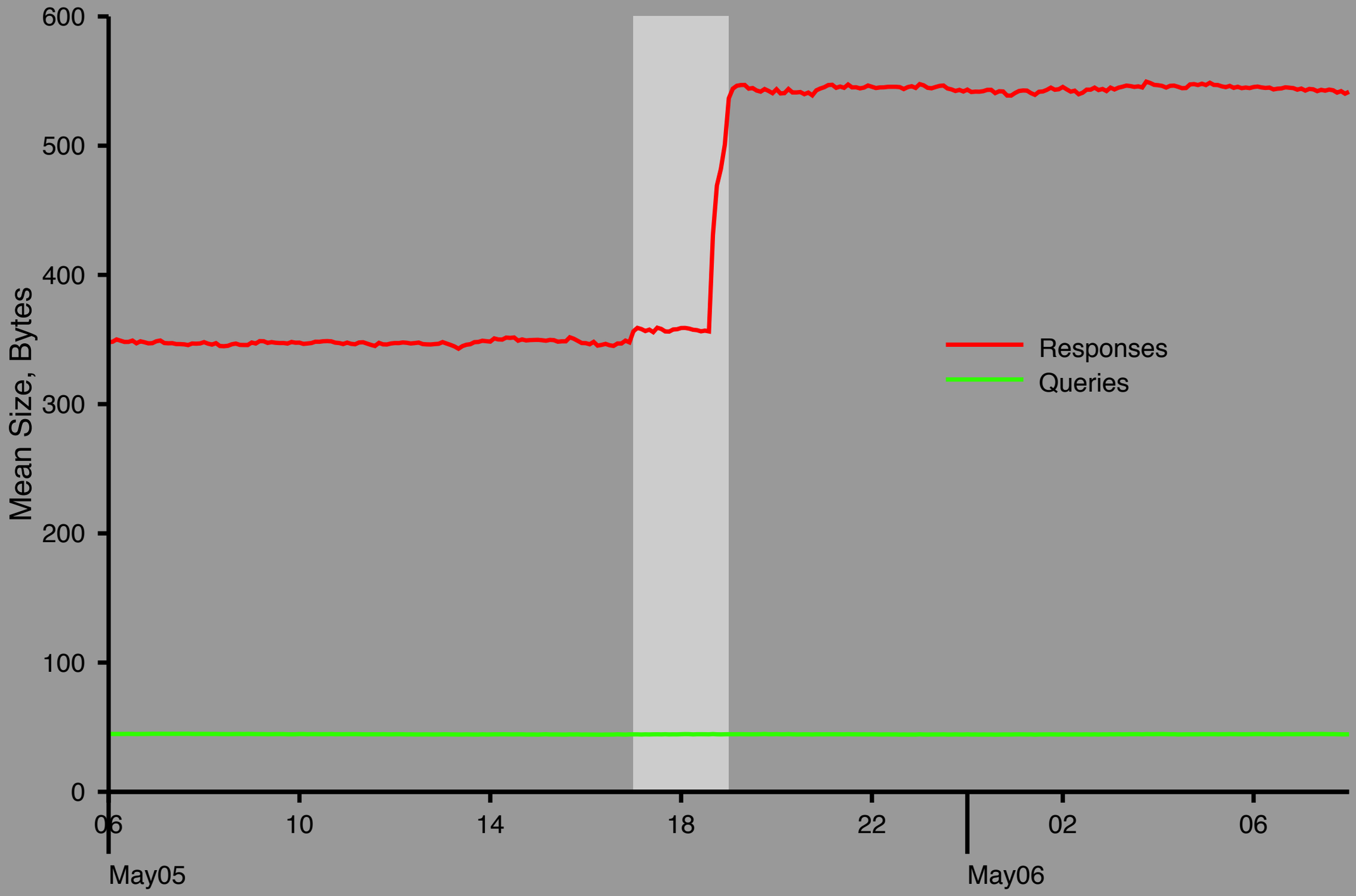
DURZ/DITL Data

- Nine separate data collection events
- Usually 48 hours (most recent was 120 hours)
- DNS Queries only
- Some 20TB of data
- Asked all root operators to participate

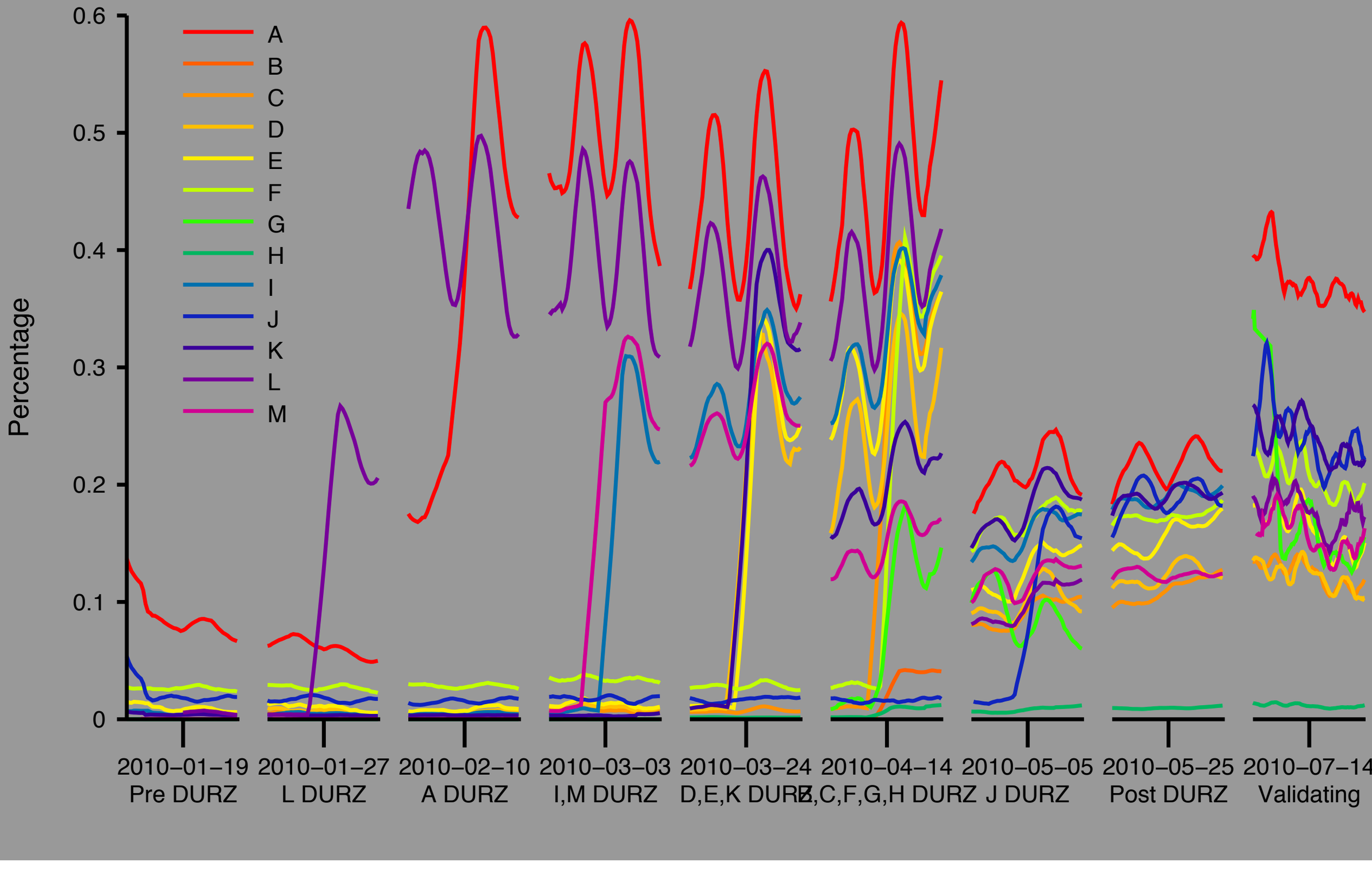
UDP Query Rate



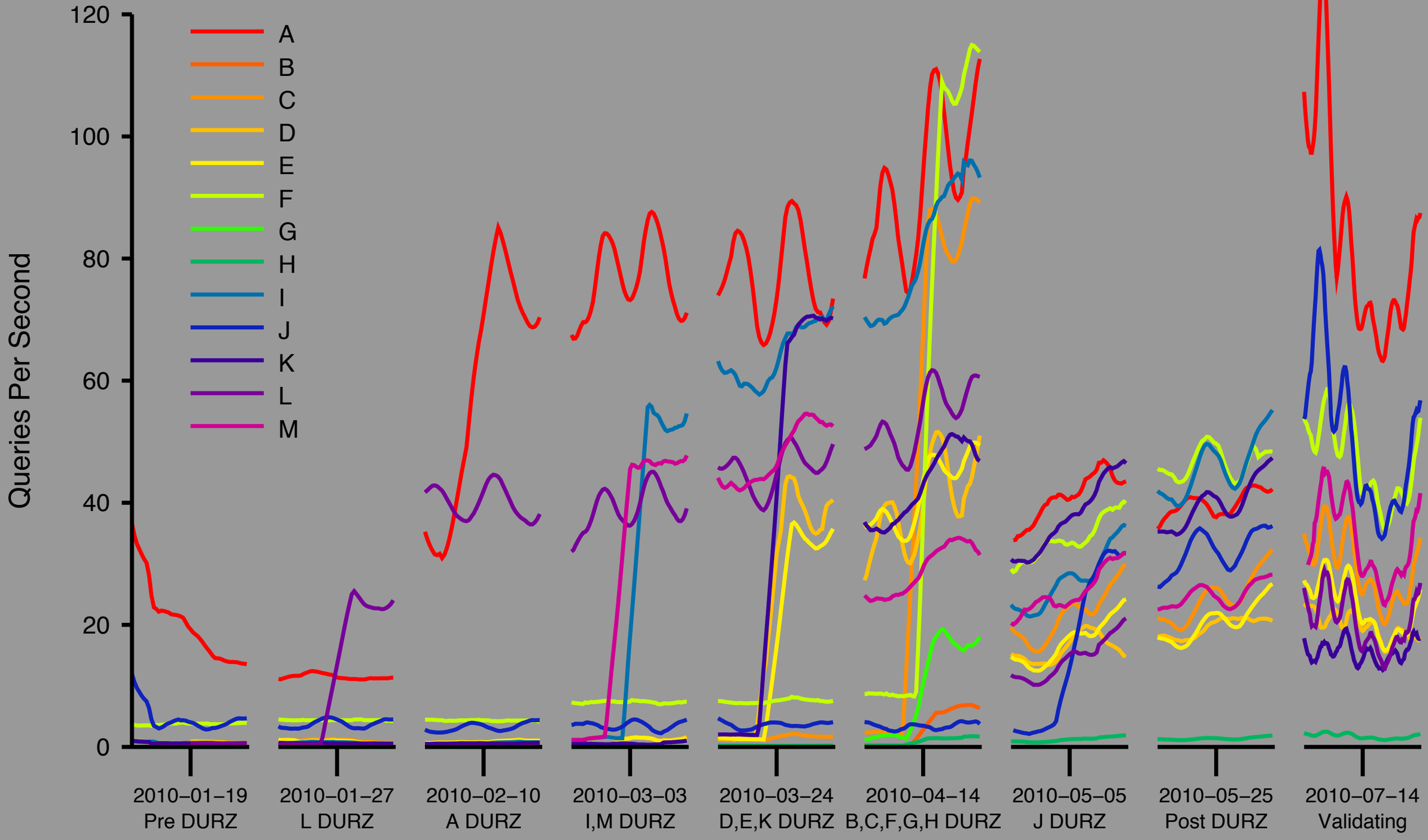
DNS Message Sizes
For J–root



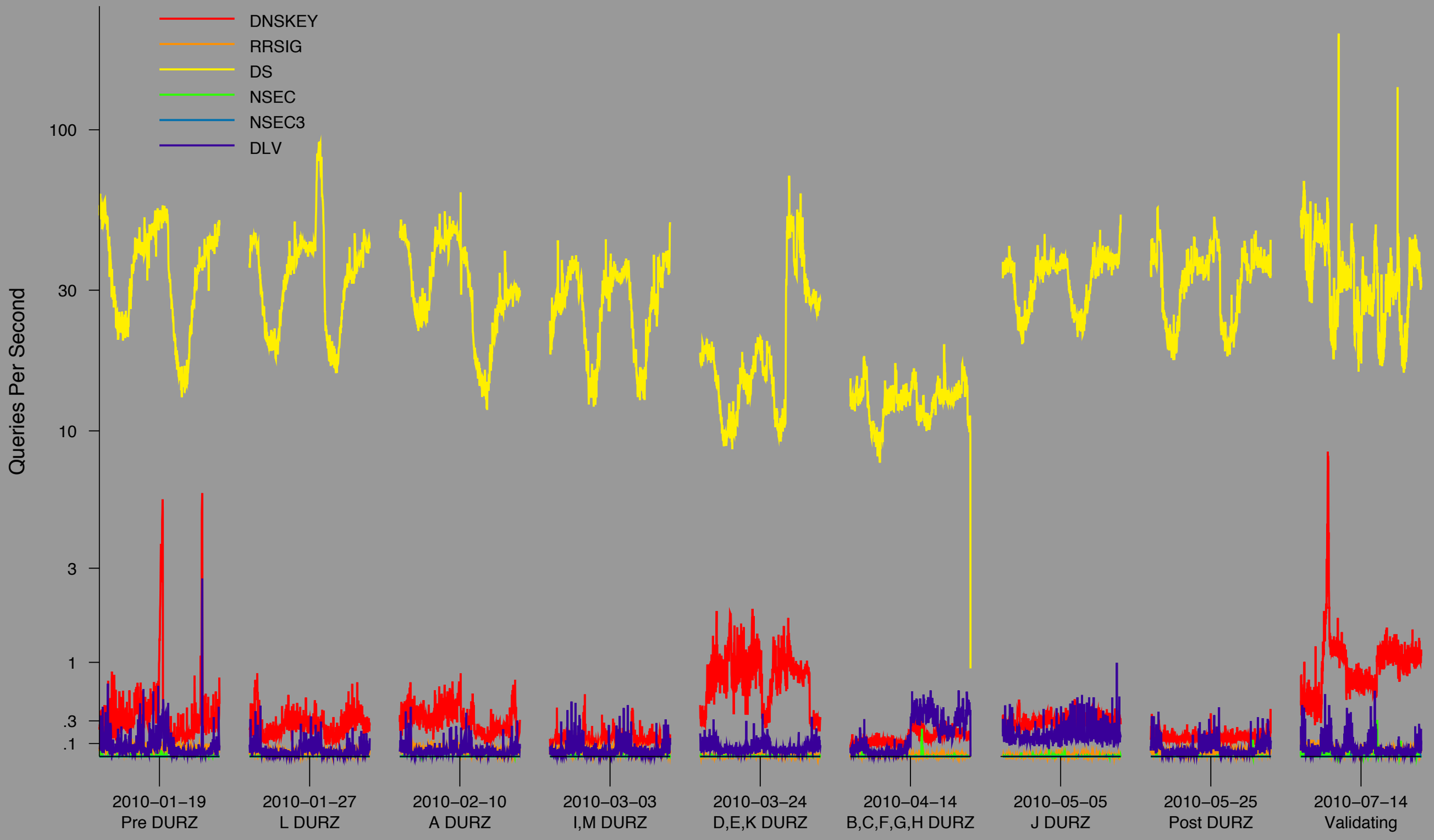
TCP Query Rate As Percent of UDP Queries



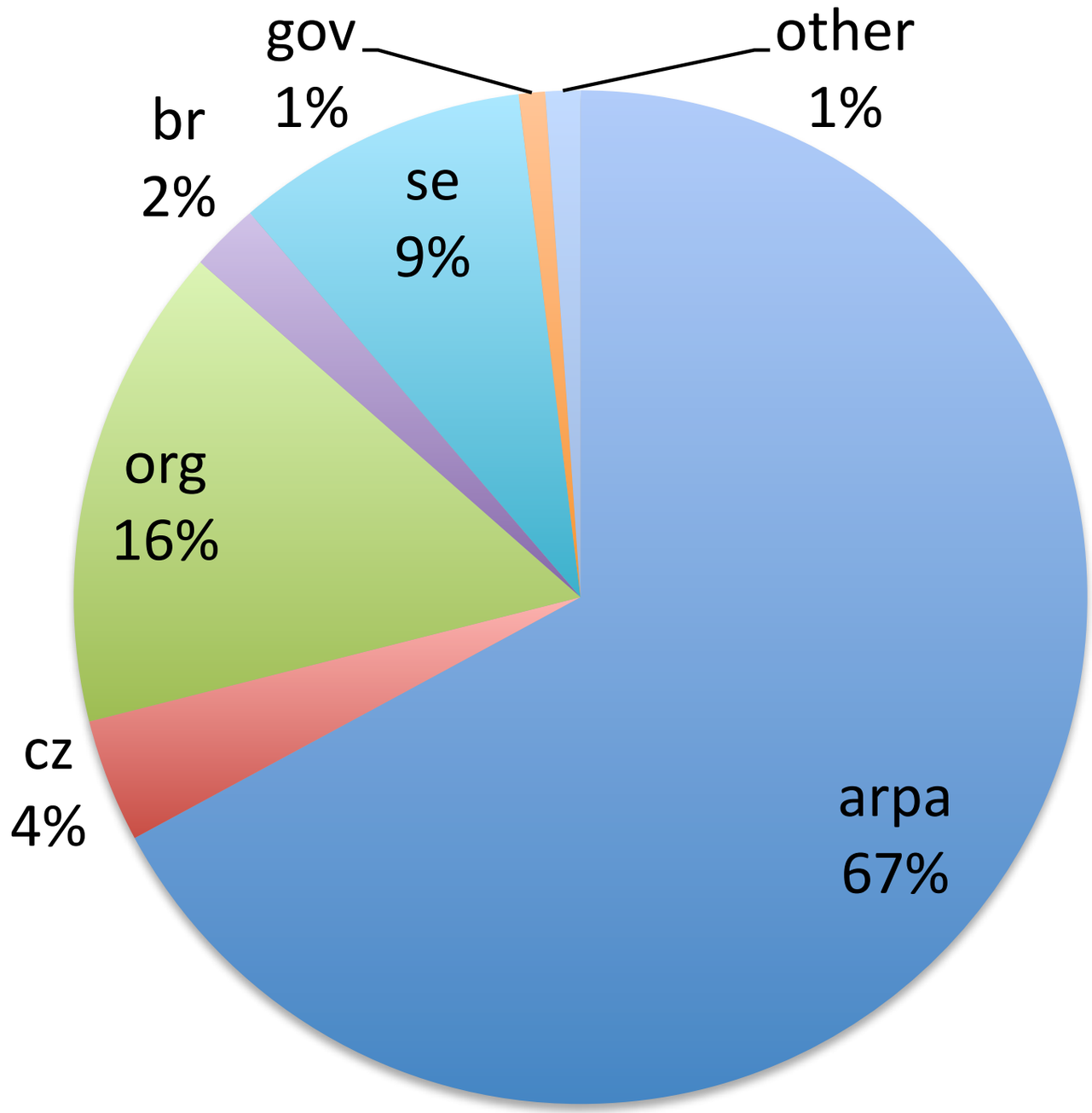
TCP Query Rate



DNSSEC Query Types
For A–root



TLDs of DS Queries



(Based on data from 2010-07-14 through 2010-07-19)

Documentation

Available at 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