

# DNSSEC for the Root Zone

DNSSEC Session at  
ICANN38, Brussels, Belgium, June 2010

Ashley Heineman, U.S. DoC NTIA

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

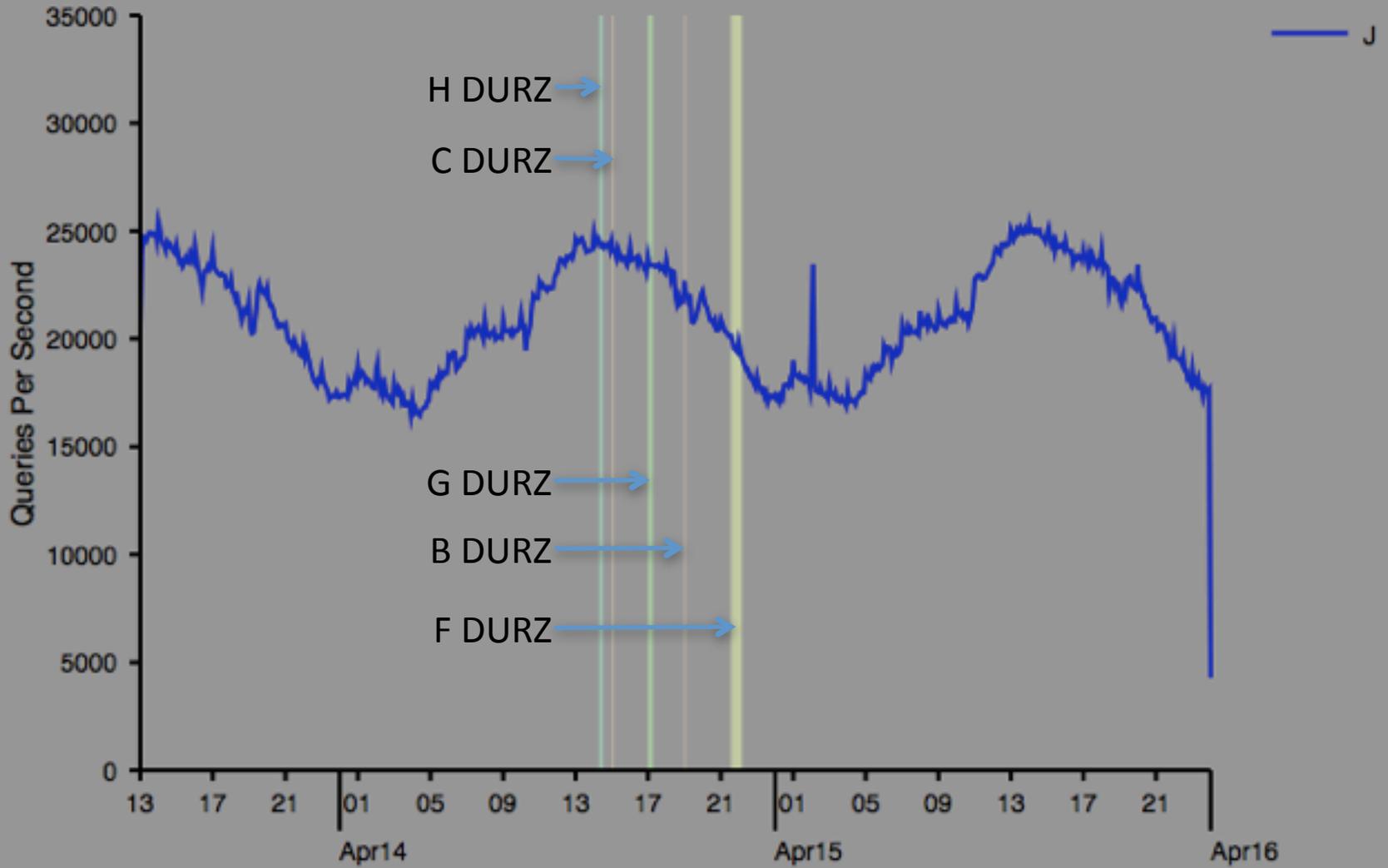
# The DURZ

- The 13 root servers were incrementally converted to a signed, but unvalidatable, zone beginning in January and finishing in May
- Root server operators collaborated with DNS-OARC to collect DNS queries 24 hours before and after each switchover

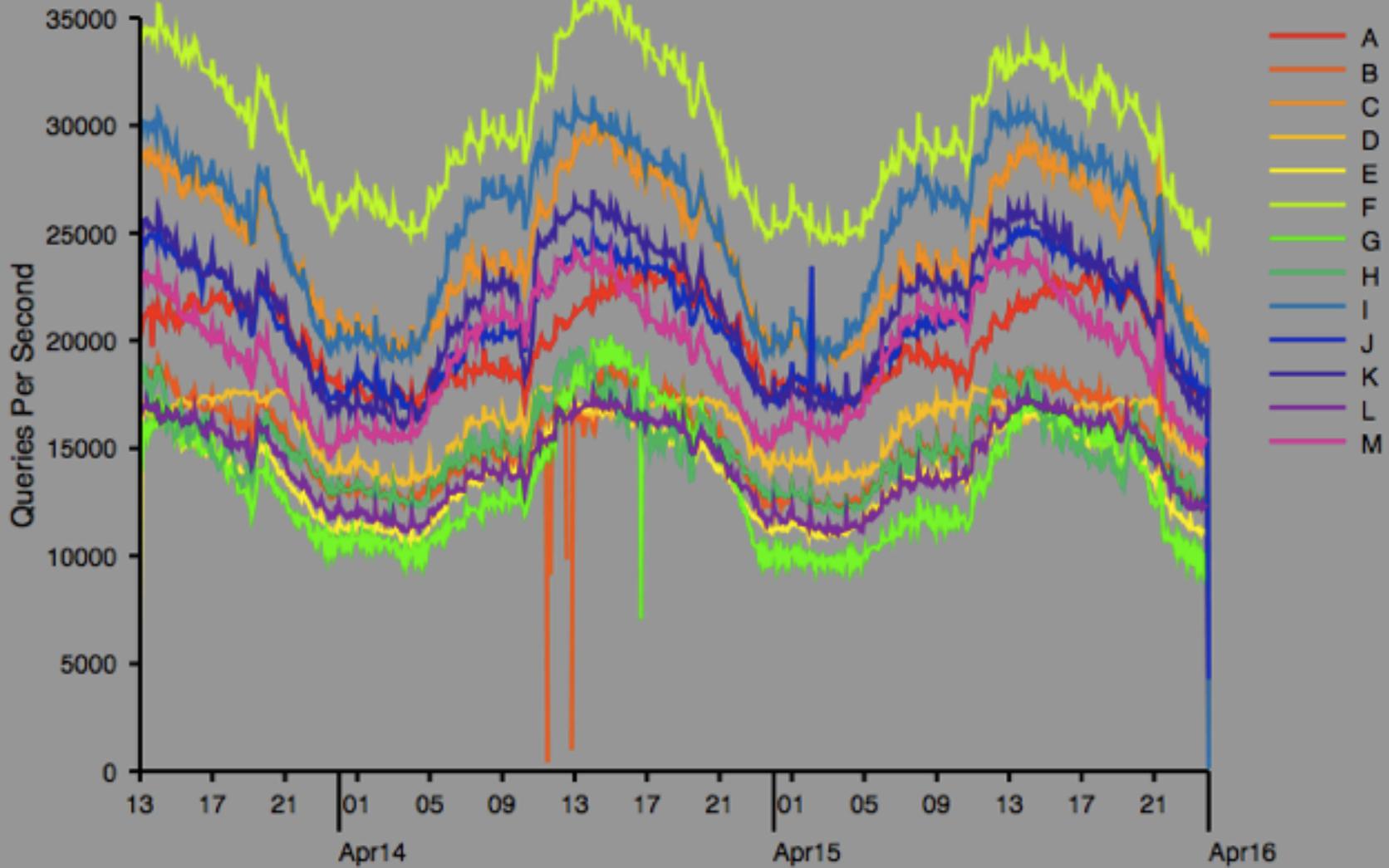
# DURZ Data Analysis

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

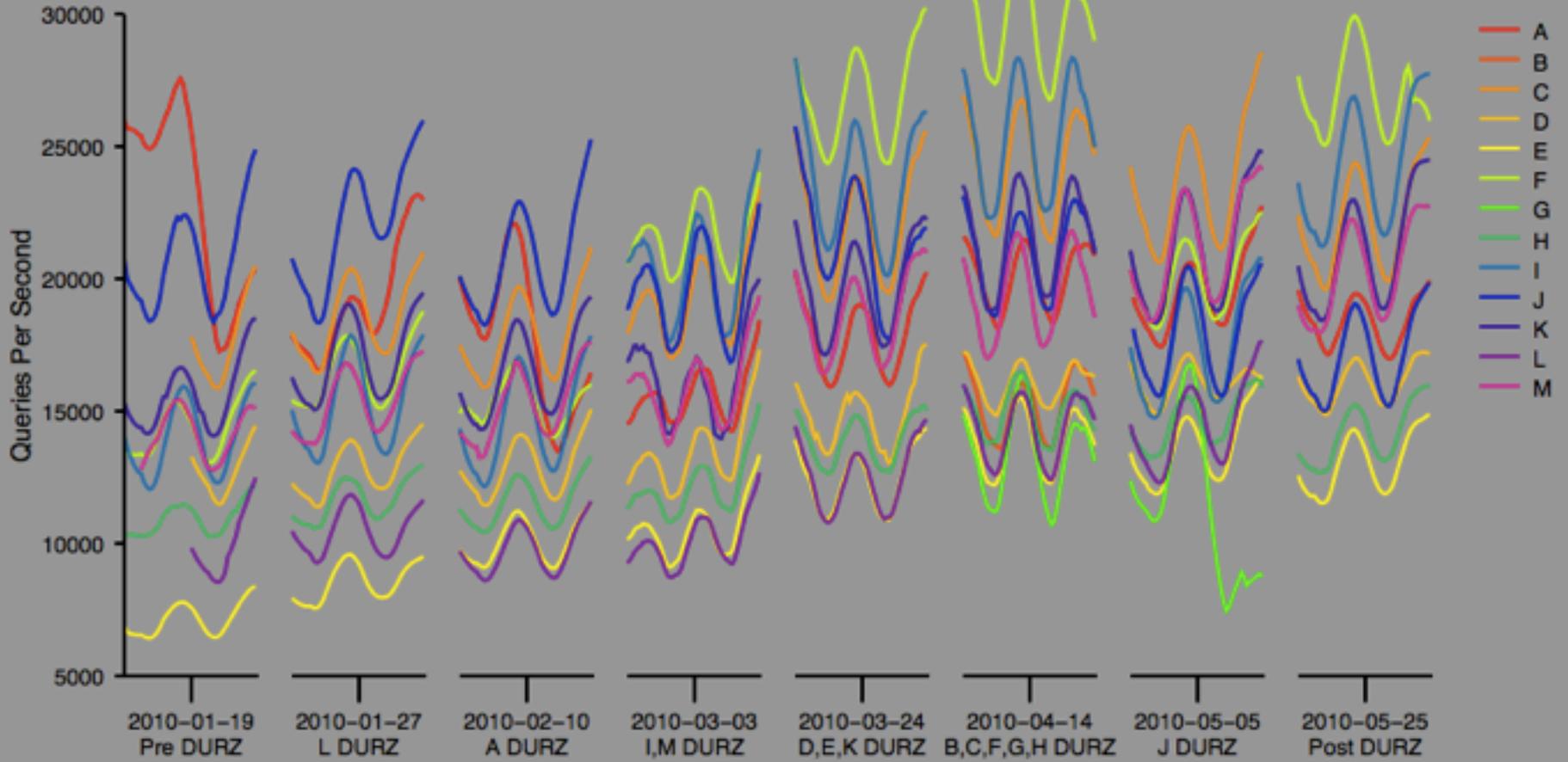
# UDP Query Rate



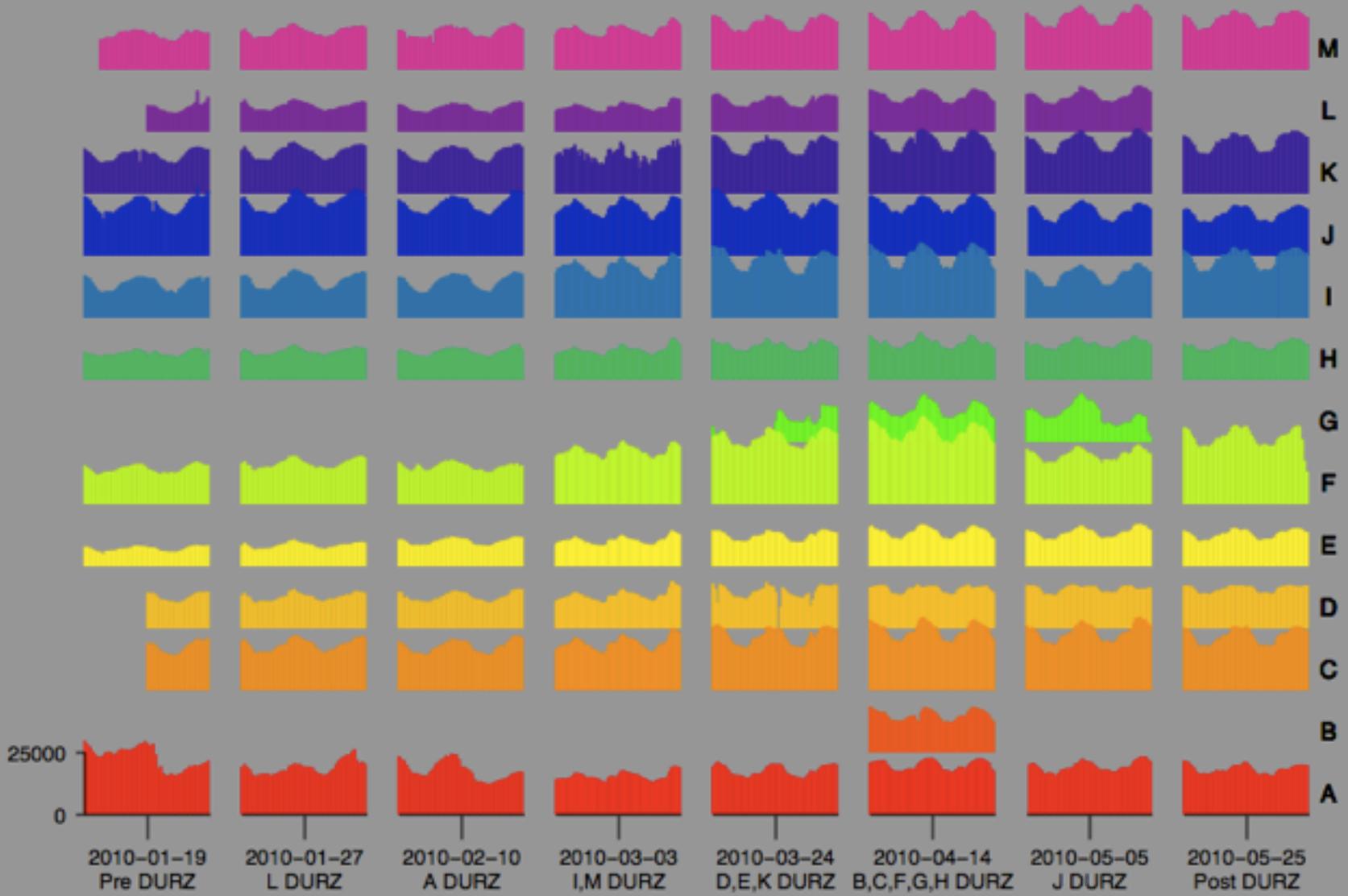
# UDP Query Rate



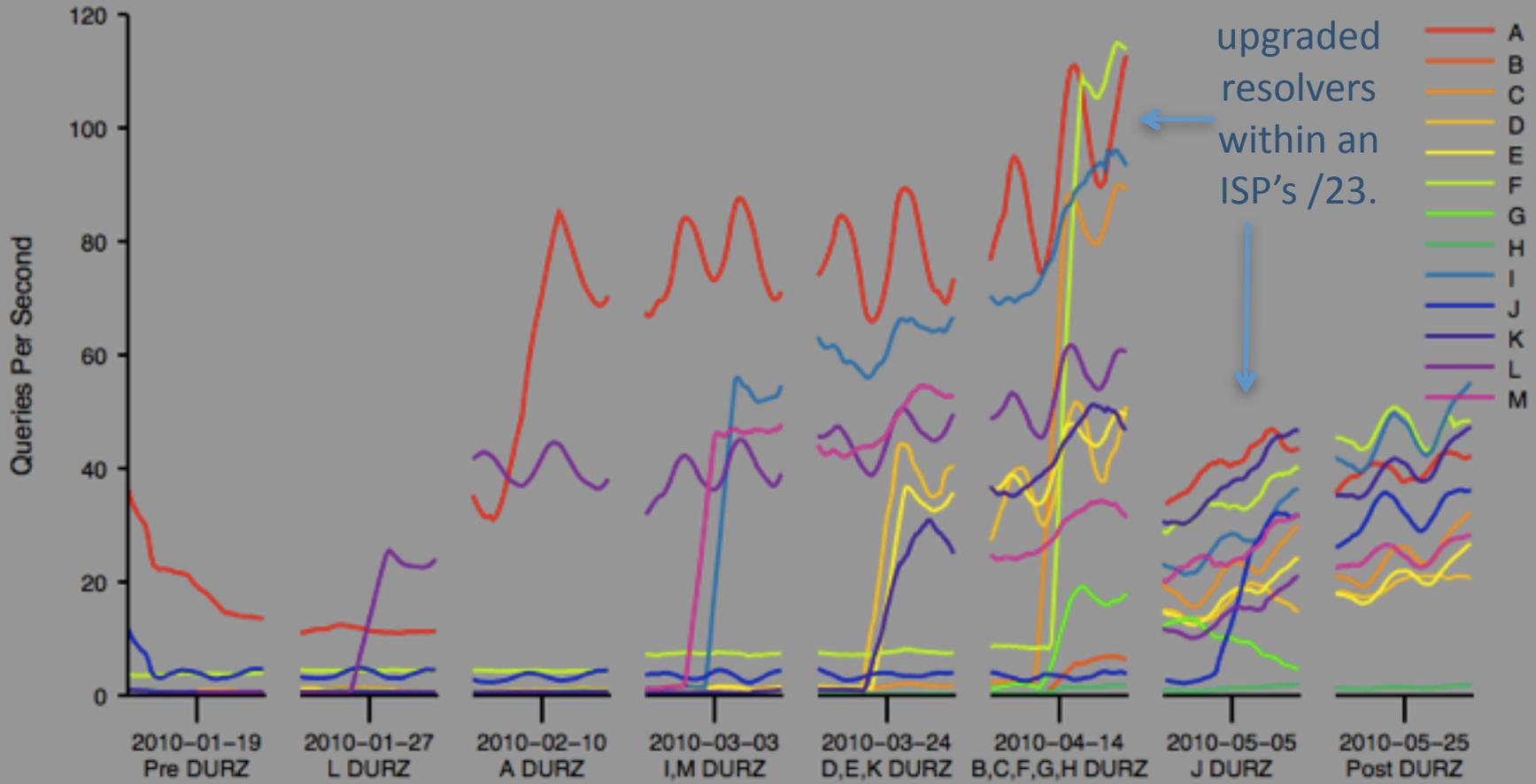
### UDP Query Rate



# UDP Query Rate

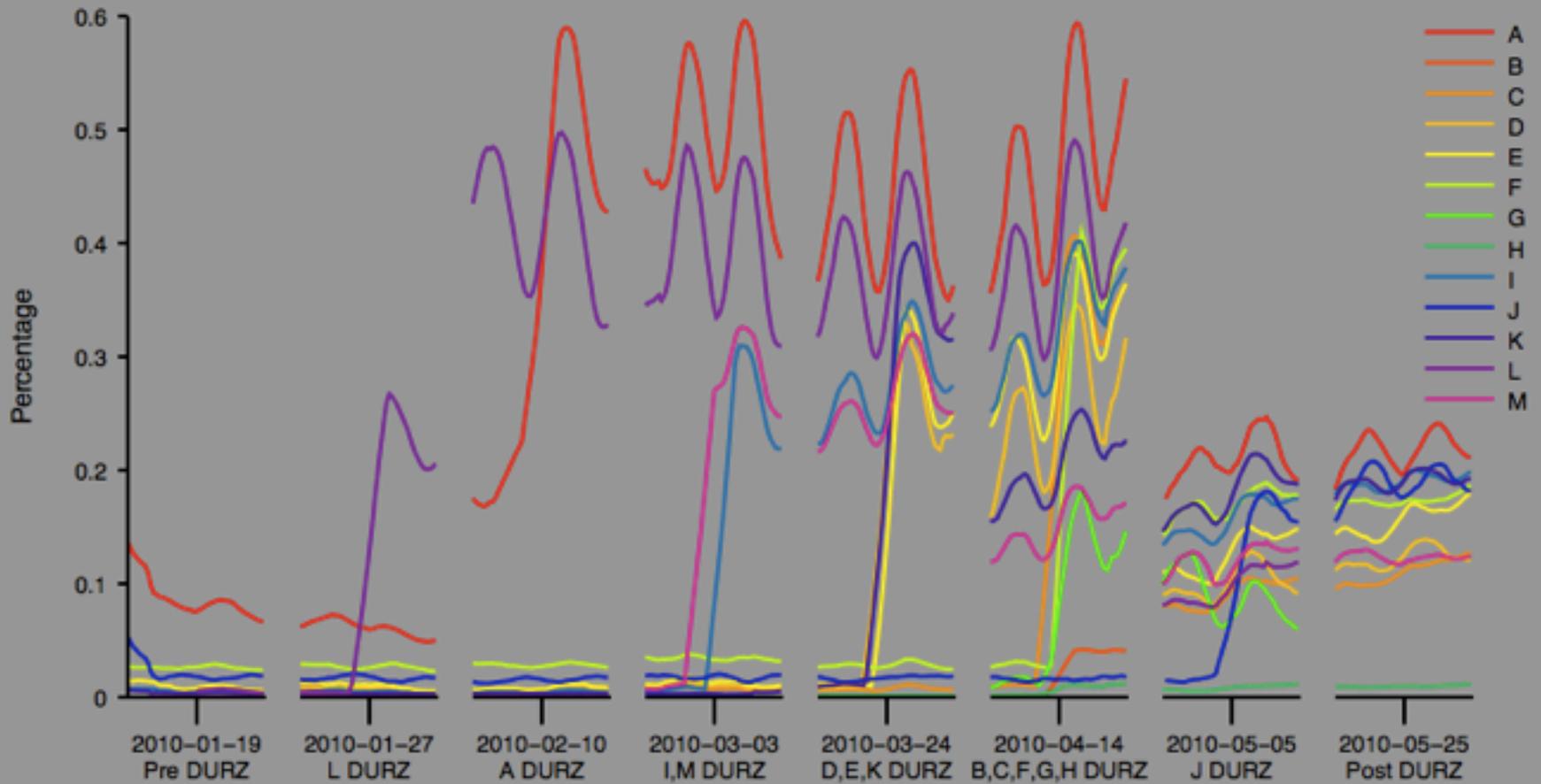


# TCP Query Rate

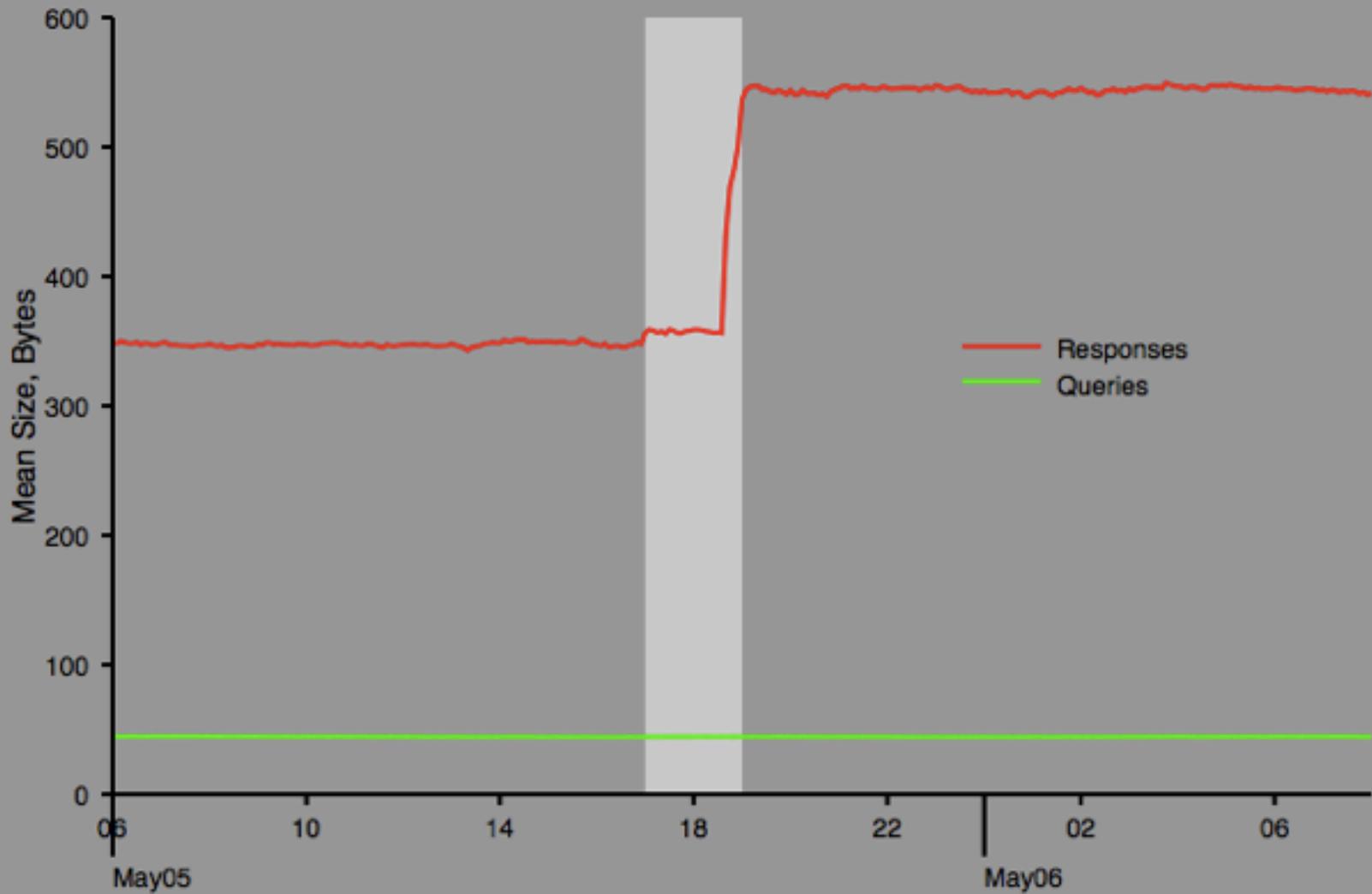


This drop is due to upgraded resolvers within an ISP's /23.

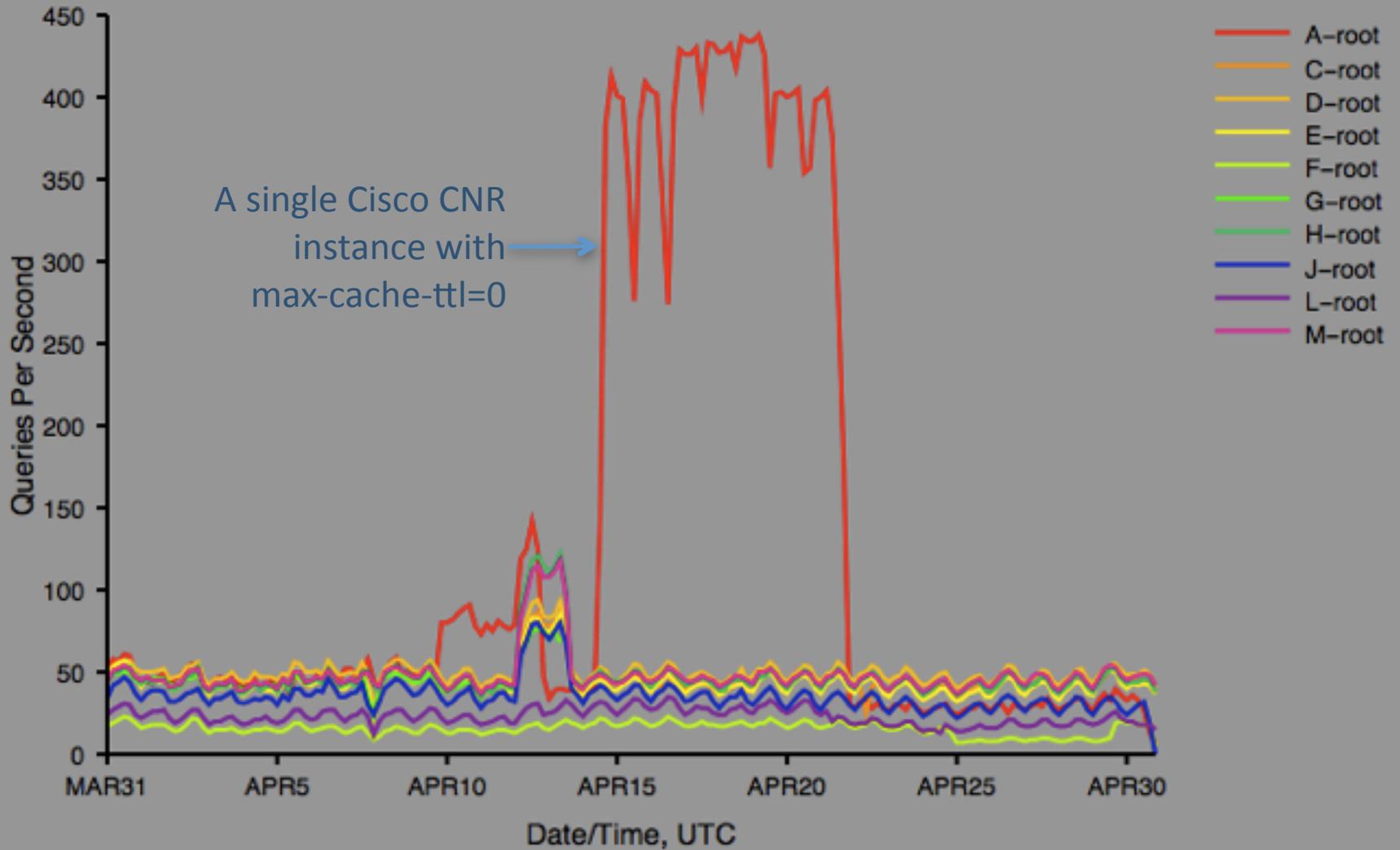
### TCP Query Rate As Percent of UDP Queries



## DNS Message Sizes For J-root



# UDP Priming Query Rate for the previous month as of 2010-05-01 00:00:00



# Generating a Root Key

***Done.***

# DNSSEC Root Zone KSK Ceremony I

Where: 16 June 2010 in Culpeper, Virginia (outside the nuclear blast zone of Washington, DC)

When: Started at 17:25 UTC, ended at 00:25 UTC (1:25-8:25 PM)

Who: 30 people in a small room for 7 hours (without laptops!):

- 16 Trusted Community Representatives (TCRs) acting as Crypto Officers, Recovery Key Share Holders and backups
- 11 ICANN staff and contractors
- 1 external auditor
- 1 VeriSign representative to verify the KSR/ZSK (Matt!!)
- 1 external camera man

What: **19036** (DNSSEC Key Tag for KSK)

# DNSSEC Root Zone KSK Ceremony | TCRs

- Sacrificed time and money to improve the confidence in and acceptance of DNSSEC in the root
- 14 Crypto Officers (CO) – 7 for US East and 7 for US West key management facilities
- 7 Recovery Key Share Holders (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 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. 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

# Quick Recap

- 2048-bit RSA KSK, 1024-bit RSA ZSK
- Signatures with RSA/SHA-256
- Split ZSK/KSK operations
- KSK and ZSK policies and other documents published on <http://www.root-dnssec.org>

# DS Change Requests

- Accepting DS records NOW
- DS records handling document at <http://www.root-dnssec.org/documentation/>

# Next....

- Key Ceremony on 12 July 2010 in Los Angeles, California, completes the process
- Key material then replicated and stored in the West coast facility
- At L.A. ceremony, KSR for Q4 will also be signed
- See <http://dns.icann.org/ksk>

# **15 July 2010**

## **Finally...the DVRZ**

- A fully validatable production root zone is currently planned to be published
- Another data collection (five days)
- Root zone trust anchor to be published by ICANN (the IANA Functions Operator)

# Key Ceremony Participants and Attendees



# Acknowledgements

## Design Team:

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

## ICANN Staff:

Anand Mishra, Francisco  
Arias, Reed Quinn, Alex  
Kulik, Joyce Thomas,  
Marilyn Vernon, Leo  
Vegoda, Naela Saras,  
Michael Cashin, Perl Liang,  
Kim Davies, Michele  
Jourdan, Naveed Tahir-  
Kheli, Carol Cornell, Khalil  
Rasheed, Cathy Cornejo,  
Patrick Jones, Geoff  
Bickers, Doug Brent, Sara  
Stohl

## VeriSign Staff:

Too many people to  
mention, from all over the  
company and the world

## Community:

Roy Arends, Patrik  
Fältström, Tim Polk,  
Scott Rose, Doug  
Montgomery,  
Steve Crocker, John  
Dickinson, David  
Soltero, David Miller,  
Don Davis and so many  
others from Internet  
and security  
communities