BRUSSELS

© vzw Atomium

ICANN

No.38 | 20-25 June 2010

DNSSEC Workshop

ICANN Meeting, Brussels, Belgium

23 June 2010

Agenda

1. Welcome and Introductions: Steve Crocker, Co-Chair DNSSEC Deployment Initiative, DNSSEC Deployment Around the World
2. Operational Issues with DNSSEC:
   - Draft Request for Comment on DNSSEC Policy & Practice Statement, Fredrik Ljunggren, Kirei AB
   - Obtaining and Maintaining Data – Registry and Registrar Issues, Moderator, Russ Mundy
     - Technical Presentations: Olafur Gudmundsson, Shinkuro; Dan Kaminsky, Recursive Ventures
     - Panel Discussion: Ondrej Filip, CZ.NIC; Jim Galvin, Afilias; Jeremy Hitchcock, Dyn Inc.; Peter Larsen, Larsen Data ApS; Michele Neylon, Blacknight; Frederico Neves, NIC.br; Patrik Wallström, Internet Infrastructure Foundation (.SE); Chris Wright, AusRegistry

Agenda

2. Operational Issues with DNSSEC, Cont.
   - Using Data and Getting it Out – ISP and Resolver Issues, Moderator, Russ Mundy
     - Technical Presentation: Jason Livingood, Comcast; Roland van Rijswijk, SurfNet
     - Panel Discussion: Mats Dufberg, Telia; Bert Hubert, PowerDNS; Normen Kowalewski, Deutsche Telecom; Jason Livingood; Comcast; Roland van Rijswijk, SurfNet
3. DNSSEC Tool Development
   - Open Source Tools, Russ Mundy, Co-Chair, DNSSEC Deployment Initiative
   - DNSSEC Deployment in PowerDNS, Bert Hubert, PowerDNS
   - Open DNSSEC, Roy Arends, Nominet

Agenda

4. Activities from the Region:
   Julien Adam, AFNIC; Tim Verhoeven, .be; Peter Koch, DENIC; Peter Janssen, .eu; Sara Monteiro. FCCN/.pt; Alexander Ilin, .ru
5. Completing the DNSSEC Chain of Trust -- Panel Discussion: Lance Wolak, Public Interest Registry (moderator); Olaf Kolkman, IETF; Rick Lamb, ICANN; Lauren Price, Public Interest Registry; Jim Galvin, Afilias; Rajesh Kothari, NamesBeyond; Jeremy Hitchcock, Dyn Inc.; James Bladel, GoDaddy; Jason Livingood, Comcast; Leslie Daigle, ISOC

Lunch Break: 12:15 to 1:00 pm in Room 100 (tickets required for entry)

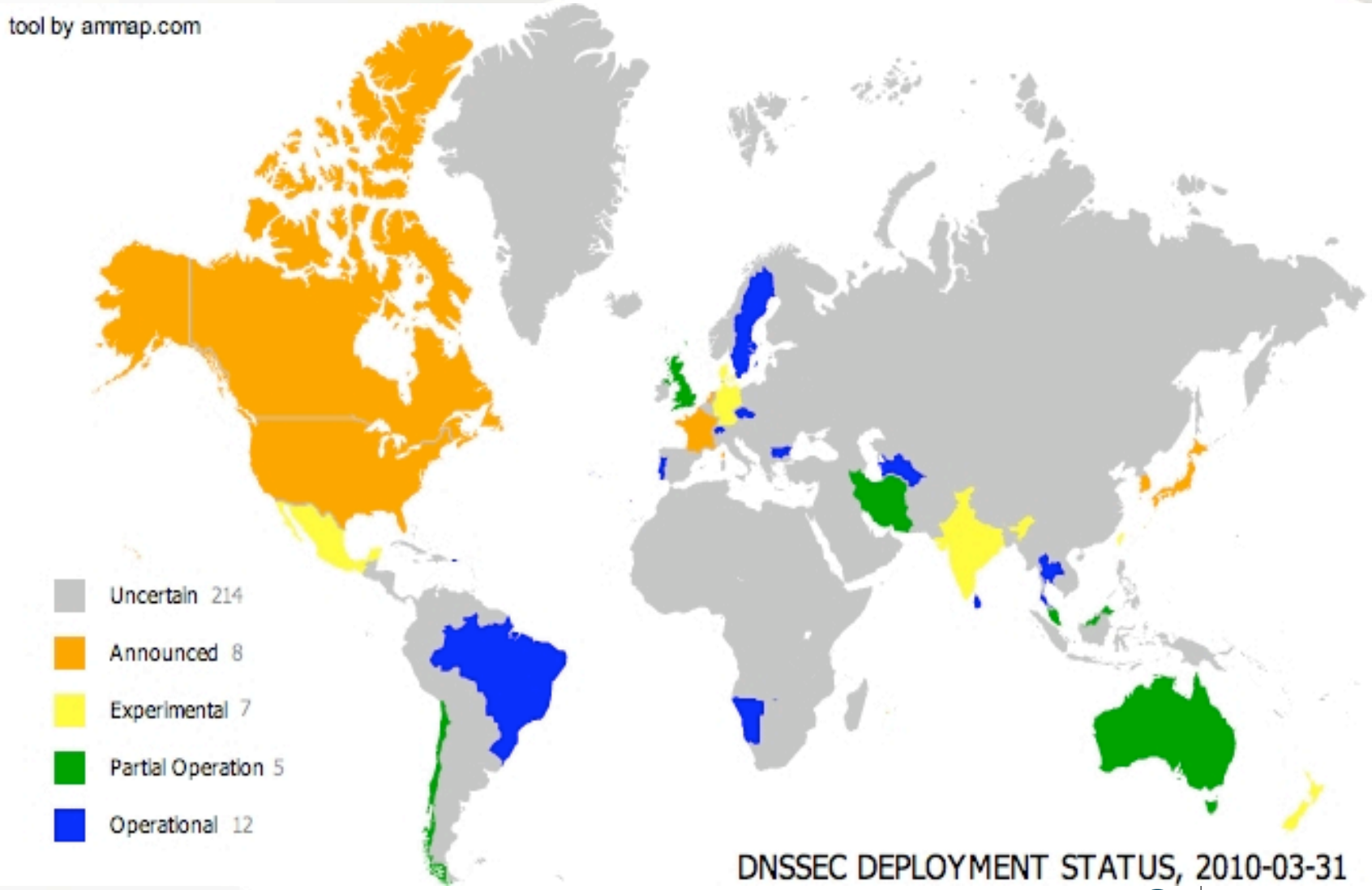
6. Implementation of DNSSEC at the Root:
   Ashley Heineman, National Telecommunications and Information Administration; Matt Larson, VeriSign, Inc.; and Rick Lamb, ICANN

ccTLD DNSSEC Deployment Mar 2010 through Dec 2011

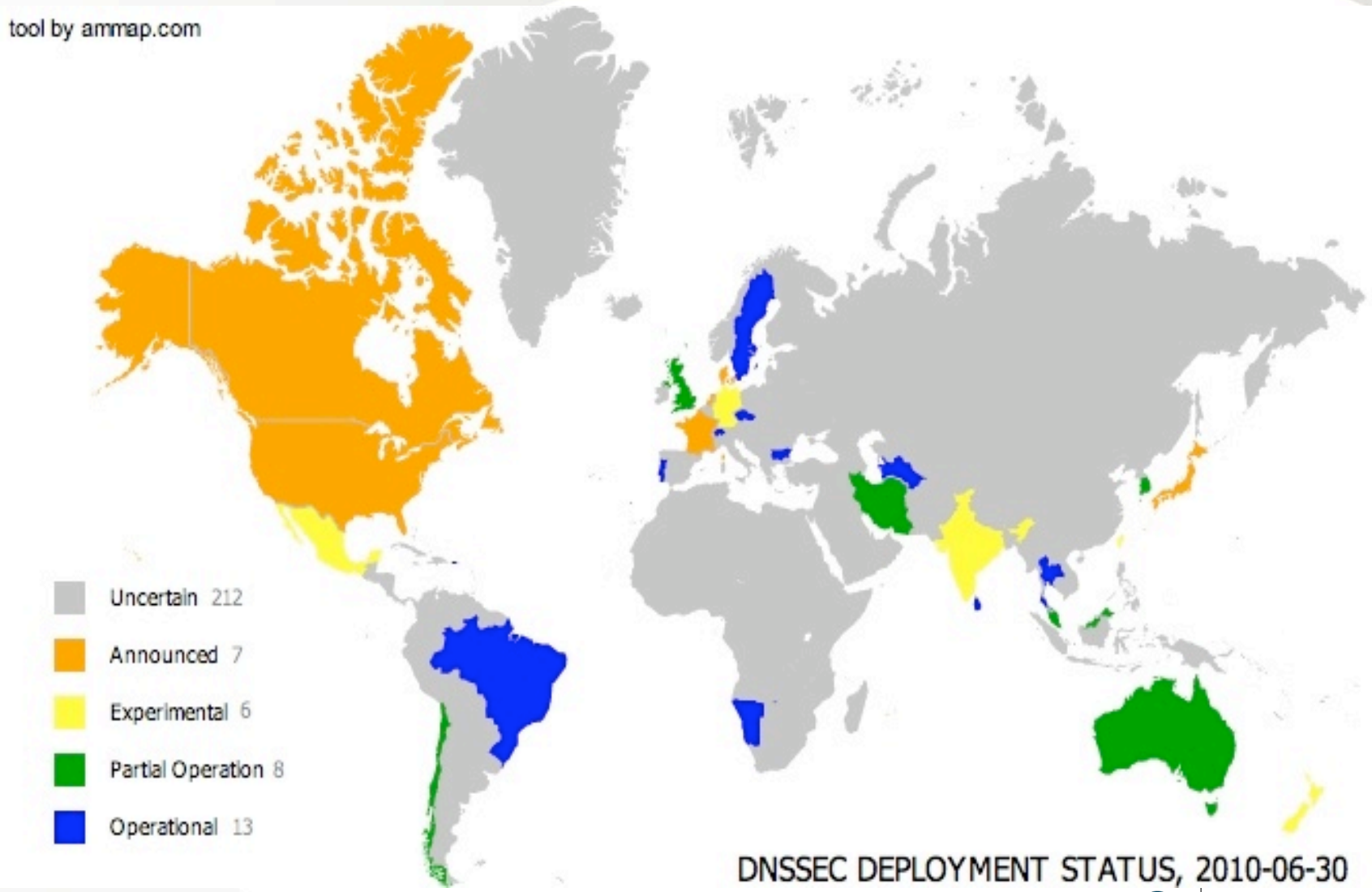
Steve Crocker

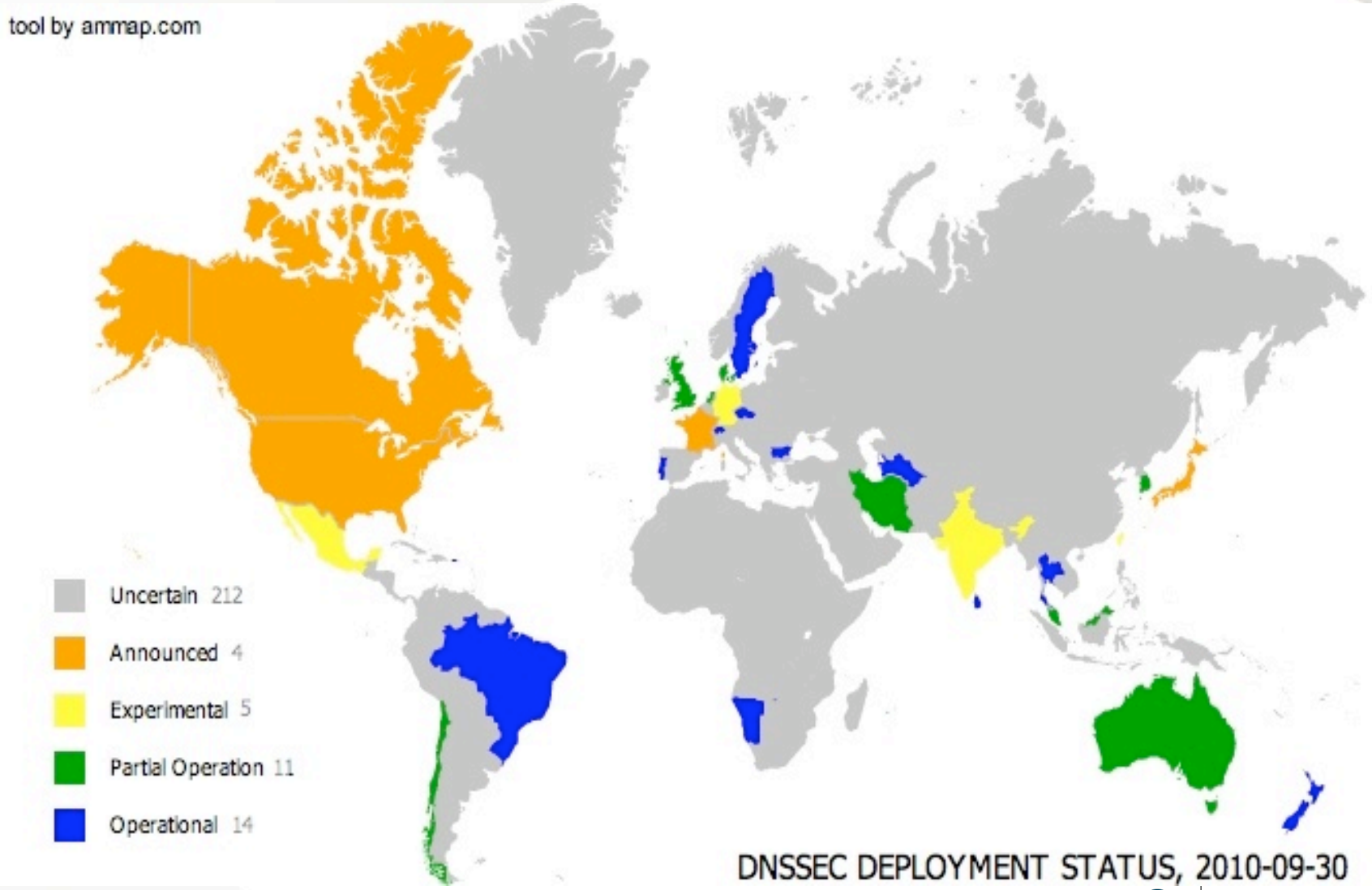
June 23, 2010

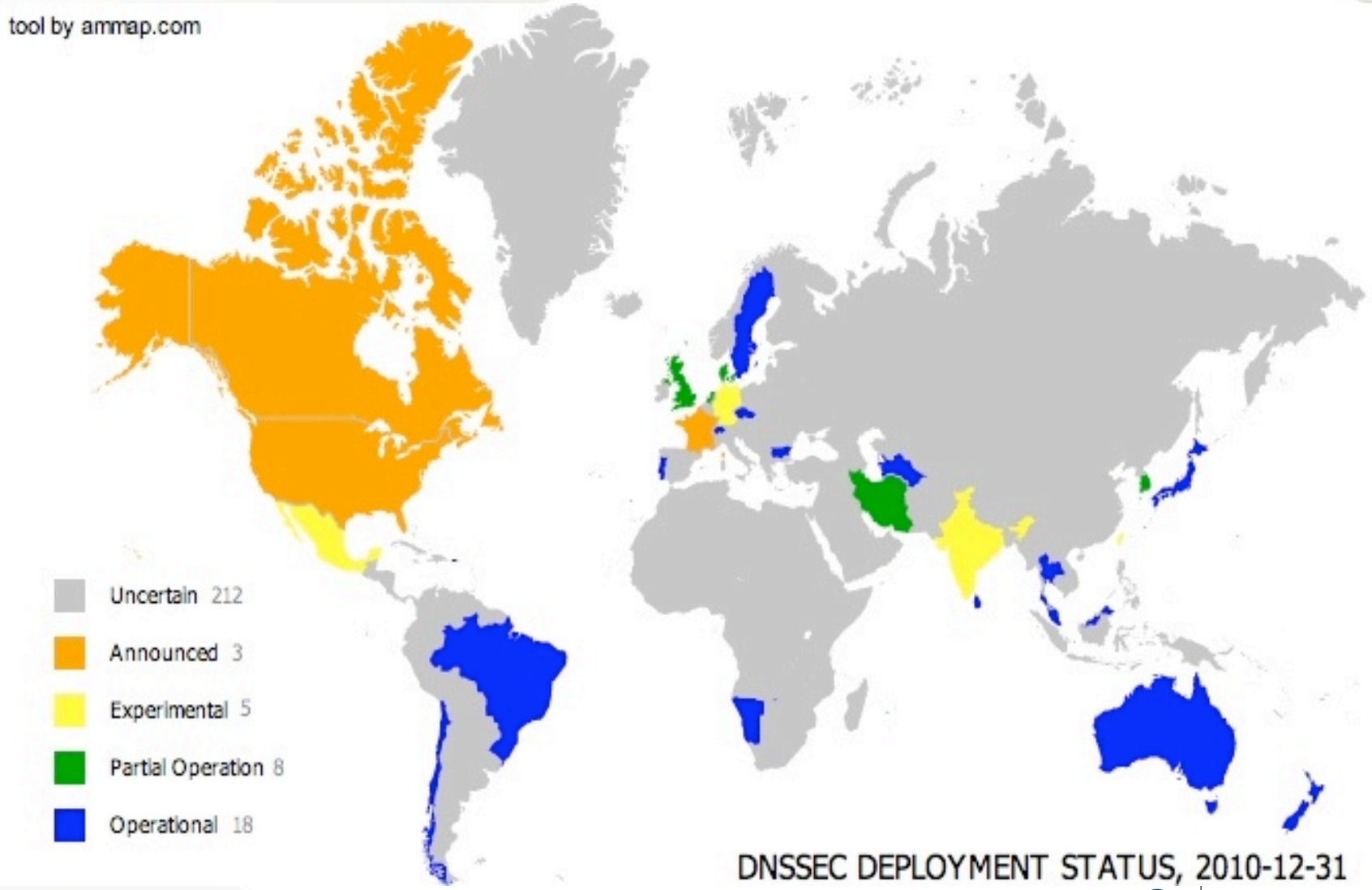
ICANN BRUSSELS No.38 | 20-25 June 2010

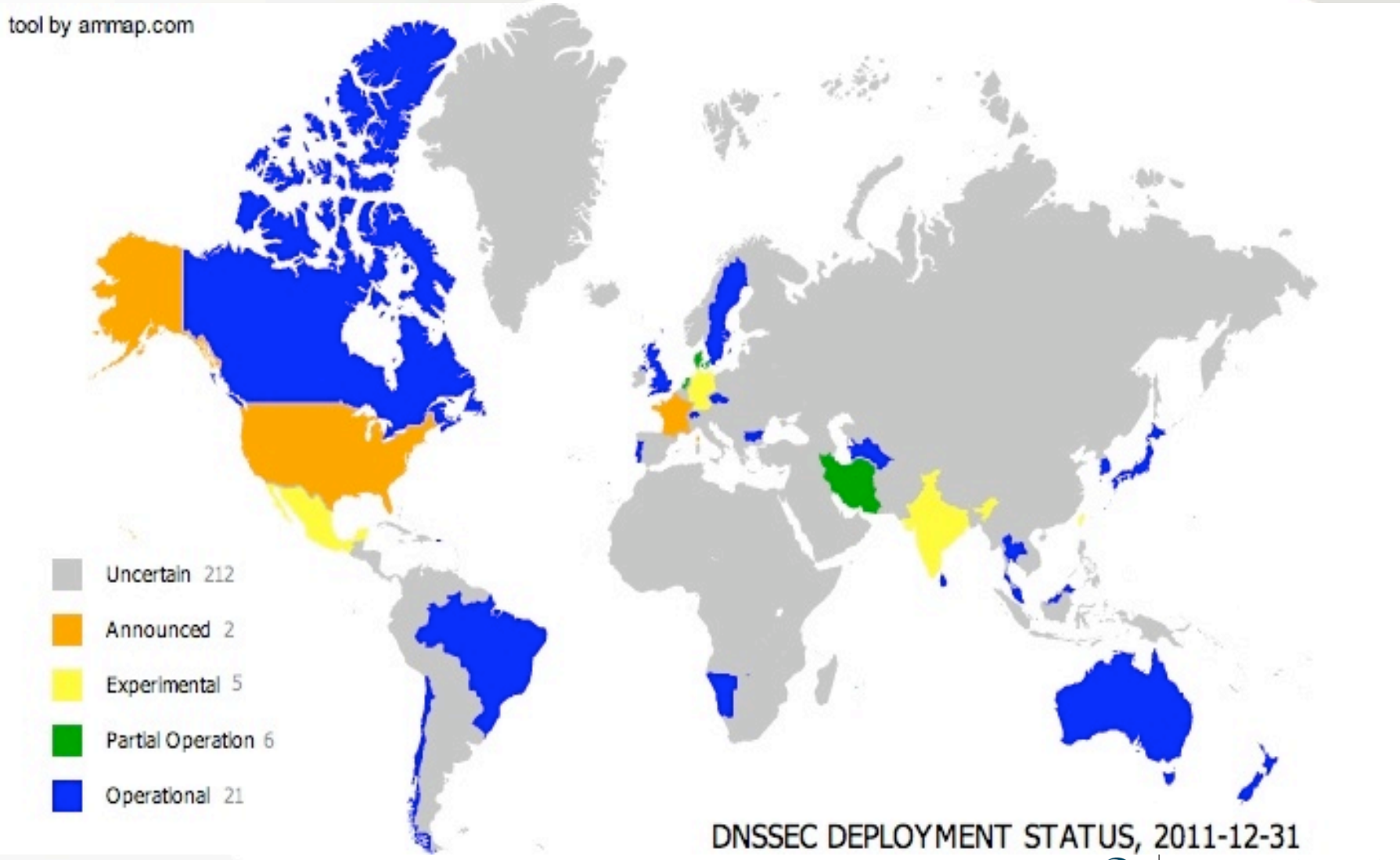


DNSSEC DEPLOYMENT STATUS, 2010-03-31

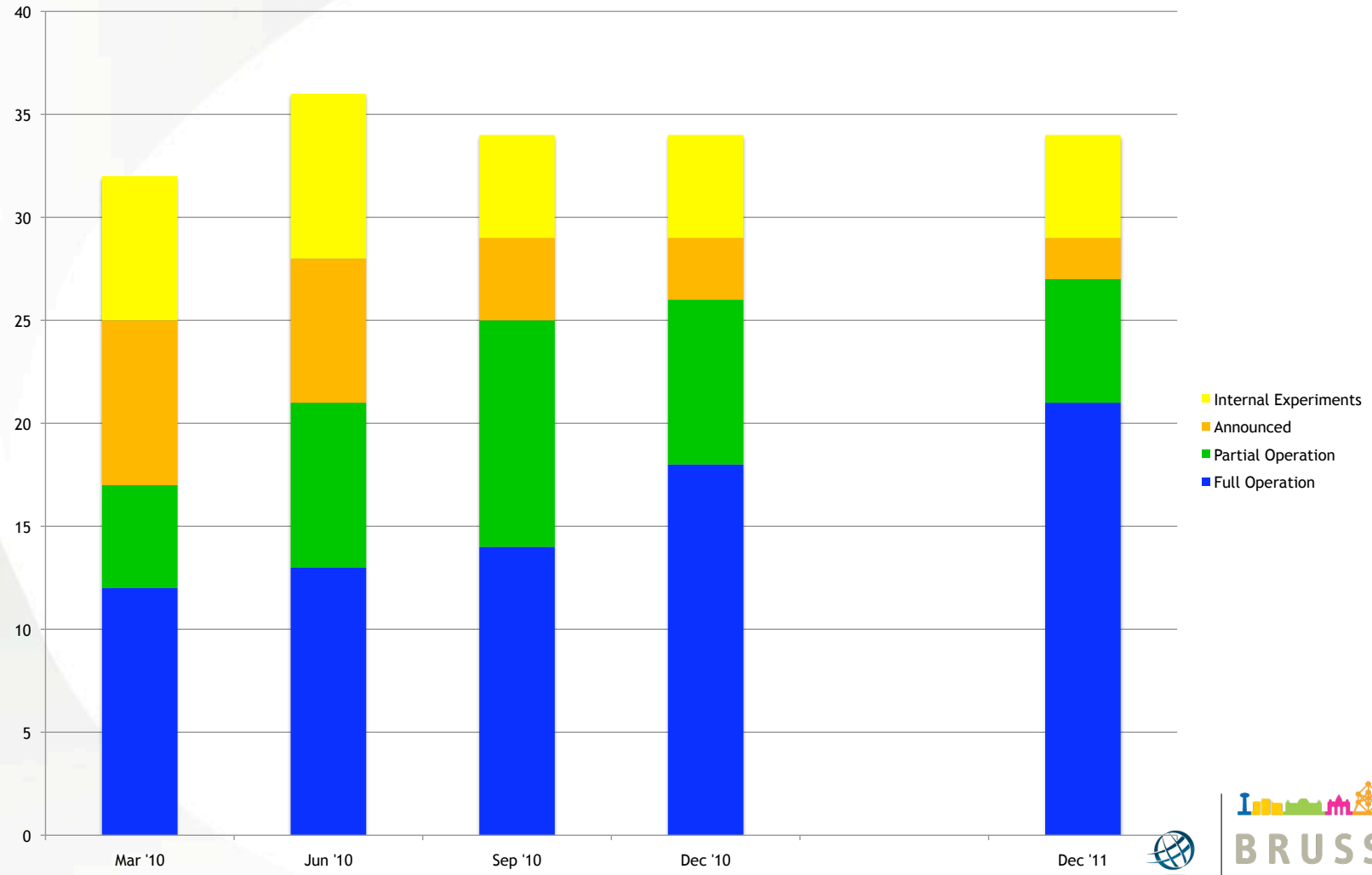

tool by ammap.com
Uncertain 212
Announced 7
Experimental 6
Partial Operation 8
Operational 13
DNSSEC DEPLOYMENT STATUS, 2010-06-30


tool by ammap.com
Uncertain 212
Announced 4
Experimental 5
Partial Operation 11
Operational 14
DNSSEC DEPLOYMENT STATUS, 2010-09-30


tool by ammap.com
Uncertain 212
Announced 3
Experimental 5
Partial Operation 8
Operational 18
DNSSEC DEPLOYMENT STATUS, 2010-12-31


tool by ammap.com
Uncertain 212
Announced 2
Experimental 5
Partial Operation 6
Operational 21
DNSSEC DEPLOYMENT STATUS, 2011-12-31

ccTLD DNSSEC Adoption



Operational Issues with DNSSEC: Panel Discussions

Panel: Obtaining and Maintaining Data – Registry and Registrar Issues, Russ Mundy, Moderator

Panelists and Some Key Points for Discussion:

- Ondrej Filip, CZ.NIC
  - CZ.NIC has about 100.000 signed domains, the highest number in all TLDs.;
  - DNSSEC: special services or standard part of domain registration?
  - End user adoption - end user tools (such as Mozilla add on); and
  - Next step: Validation at end user side - CPE DNSSEC compatibility.
- Jim Galvin, Afilias
  - DNSSEC Best Practices
    - Must support the import and export of the public key;
    - Must provide a mechanism to unsign a domain;
    - Must functionally separate DNS services from registration services;
    - Must support the import of a new NS resource record set without; discontinuing existing DNS services;
    - Must continue DNS services until explicitly told to stop;
    - Must setup new DNS services in advance of transfer; and
    - Must support export of domain's zone file.

Panel: Obtaining and Maintaining Data – Registry and Registrar Issues, Russ Mundy, Moderator, Cont.

Some Points for Discussion From Panelists, Cont.:

- Jeremy Hitchcock, Dyn Inc.
  - Registrar adoption: Small ecosystem of registrars to start, EPP and DNS being more tied together;
  - Registrant adoption: technical users and high value domains are going to be first, education going to be key; and
  - Caching/recursive DNS and application adoption: applications and OS awareness of DNSSEC validation.
- Peter Larsen, Larsen Data ApS
- Michele Neylon, Blacknight
- Frederico Neves, NIC.br
  - Operational DNSSEC validation;
  - Chain of thrust validation at DS update time; and
  - APEX continue signature verification.

Panel: Obtaining and Maintaining Data – Registry and Registrar Issues, Russ Mundy, Moderator, Cont.

Some Points for Discussion From Panelists, Cont.:

- Patrik Wallström, Internet Infrastructure Foundation (.SE)
  - ".SE's registry-registrar model we now have launched on the 9th of March 2009. Before that, all DNSSEC administration could be done from our own registry interface by anybody.
  - We identified the problem of transfers of DNSSEC enabled domains early, and monitored what happened to the domains that were transferred from a DNSSEC enabled domain to a non-DNSSEC registrar.
  - In the agreement with all the registrars, there is a paragraph that states that all registrars must be able to remove DS records from the registry. We only had four incidents within the first month where DS records was not removed so that the domains did not work. Since then we have not had any incidents with registrars and DNSSEC.
  - The major problem in .SE is still for the name server operator to send keys to the registry. And we are also looking into making it a requirement for registrars to be able to communicate DNSSEC keys from the registrant to the registry."
  - Registry - registrar model with DNSSEC
  - DNSSEC and Transfers
  - Sending keys to the parent
  - Making DNSSEC a requirement?

Panel: Obtaining and Maintaining Data – Registry and Registrar Issues, Russ Mundy, Moderator, Cont.

Some Points for Discussion From Panelists, Cont.:

- Chris Wright, AusRegistry
  - Transfers – yes they are ugly, but we have to work with what we've got;
  - Policy – Exactly how much should the Regulator dictate, and how much should be left to the industry / market to sort out?
  - What exactly IS the 'business case' for deploying/supporting DNSSEC for:
    - Registries;
    - Registrars;
    - Registrants;
    - Software Vendors;
  - DNSSEC, its only one link in the chain!

Panel: Obtaining and Maintaining Data – Registry and Registrar Issues, Russ Mundy, Moderator, Cont.

Questions to Frame the Discussion:

- Are you aware of the issues concerning DNSSEC domain transfers and if so, how do you intend to solve them for your TLD/domains?
- Are you aware risks and benefits associated to key rollovers and what is your policy/position on this?
- For which types of domains does DNSSEC create additional (economic or security) value?
- How expensive is implementation of DNSSEC and how does it fit into your budget? Is it purely an expense, or does it also improve your revenue?
- How do you convince/help your registrars/customers to deploy DNSSEC?
- How do you send the keys to the parent?

Panel: Using Data and Getting it Out – ISP and Resolver Issues, Russ Mundy, Moderator

Panelists and Some Key Points for Discussion:

- Mats Dufberg, Telia
  - DNSsec resolving for the customers
    - TeliaSonera Sweden has one dedicated, redundant and distributed DNS resolving system for various customers types (broadband, corporate backbone circuits, mobile broadband, 3G/GPRS).
    - In total 1.5-2 million users depend on our DNS resolving system.
    - We have run DNSsec resolving for three years.
  - Levels of DNSsec resolving
    - To understand the affect of DNSsec resolving one has to understand the levels of DNSsec resolving.
      1. Dedicated DNSsec resolver does the job, the client is not aware of DNSsec.
      2. Dedicated DNSsec resolver does the job, but the client request DNSsec answer.
      3. The client does the validation itself.
    - DNSsec resolving is backward compatible with DNS resolvning when the client is not DNSsec aware, i.e. level 1

Panel: Using Data and Getting it Out – ISP and Resolver Issues, Russ Mundy, Moderator

Panelists and Some Key Points for Discussion:

- Mats Dufberg, Telia
  - Instability, bugs…
    - Problems with DNS resolving are know. What can we expect from DNSsec resolving?
    - Everything that can happen with DNS resolving can happen with DNSsec resolving. Plus more.
  - Areas that we should look at are:
    - Stability;
    - Network requirements;
    - Performanc;e
    - Resource requirement;
    - Support calls from users (customers);
    - Troubleshooting;
    - Key management (trust anchors).

Panel: Using Data and Getting it Out – ISP and Resolver Issues, Russ Mundy, Moderator

Panelists and Some Key Points for Discussion:

- Bert Hubert, PowerDNS
  - At 10 euros/dollars per user interaction, how will we deal with DNSSECs policy if "rather no data than suspect data";
  - Do we need facilities to allow a zone to rapidly go insecure?
  - Should end-user software become more DNSSEC aware before ISPs resolvers start to validate for them?
- Norman Kowalewski, Deutsche Telecom
  - Impact of signing the root/measures are you taking: We expect no unpredictable behavior in any systems or resolving infrastructure by the fact that the root gets signed.
  - Plan to sell DNSSEC to your customers or add it as a free extra security service: We can and will make respective offerings, including differentiated approaches, as soon as demand warrants it. Certainly this also includes to have a differentiated approach across the different vertical industries, as usual in the groups enterprise solution business.
  - We have not deployed DNSSEC in our resolvers at this time due to balancing effort and benefits.
  - Do certain national laws/regulations rely on implementation presumptions that are removed by DNSSEC (e.g. child protection)?

Panel: Using Data and Getting it Out – ISP and Resolver Issues, Russ Mundy, Moderator, Cont.

Panelists and Some Key Points for Discussion:

- Jason Livingood, Comcast
  - Are there any potential operational issues between registries and TLD operators to sort out?
  - Is addition load expected on resolvers, and how will that be handled?
  - Does equipment or software need to be upgraded to support DNSSEC?
  - How will you know if DNSSEC is functioning well?

- Roland van Rijswijk, SurfNet
  - What (if any) monitoring solutions do you use to monitor your validating resolvers and signing infrastructure/signed zones?
  - Concerned about the approachability of owners of signed zones; sometimes reporting issues to them is like talking to a wall. Does anyone see a way to improve this?
  - Those who do validation using DLV: will you drop this when the root gets signed
  - Handling helpdesk calls for "disappeared" (invalid) domains

Panel: Using Data and Getting it Out – ISP and Resolver Issues, Russ Mundy, Moderator, Cont.

Panelists and Some Key Points for Discussion:

- Questions to Frame the Discussion:
  - What is your opinion regarding the impact of signing the root with DNSSEC on the behavior of your resolving infrastructure and what measures are you taking?
  - Do you plan to sell DNSSEC to your customers or add it as a free extra security service?
  - What are your reasons for (not) deploying DNSSEC in your resolvers?

Thank you and Questions