IETF 77 REPORTS

DNSEXT
DNSOP

Matthijs Mekking


ANAHEIM
Cars Land
Disney Way

DNSEXT

- Support for Internationalized Domain Names
- Rollover and Die
- draft-ietf-dnsext-dnssec-bis-updates-11
- draft-dempsky-dnscurve-01

Internationalized Domain Names

- Example:
  - Russia has the ccTLD ru.
  - ru. == RU. == rU. == Ru.
  - Proposed Internationalized TLD рф (Российская Федерация or Rossiyskaya Federatsiya, Russian Federation)
  - DNS representation: xn-p1ai.
  - ru. == xn-p1ai. ?
- Equivalence gets a different meaning

Internationalized Domain Names

- How to make ru. equal to xn-p1ai.?
- Clone zone
- Redirection (BNAME)
- Still struggling with the problem definition
  - What is the equality function?
  - What is a name?

Rollover and Die

- How do resolvers behave if configured with an invalid trust anchor?
- Aggressive:
  - mis-configured trust anchors cause large increases in the DNS query load;
  - responses to these additional queries are themselves large.
- Resolvers need to be more conservative
- RFC 5011? Trust Anchor History Service?

draft-ietf-dnsext-dnssec-bis-updates-11

- Technical clarifications to DNSSEC
- CD bit handling logic needs to be sorted out
- Changes due to "rollover and die"?

draft-dempsky-dnscurve-01

- “DNSCurve uses high-speed high-security elliptic-curve cryptography to drastically improve every dimension of DNS security”:
  - Confidentiality
  - Integrity
  - Availability
- WG has not made up their mind if this should be adopted

DNSOP

- NSEC3 Hash Performance
- IPv6 and Recursive Resolvers
- draft-ietf-dnsop-dnssec-dps-framework-01
- draft-ietf-dnsop-dnssec-trust-history-01
- draft-ietf-dnsop-rfc4641bis-02
- draft-morris-dnsop-dnssec-key-timing-02
- draft-howard-isp-ip6rdns-03

NSEC3 Hash Performance

- Research by Yuri Schaeffer, NLnet Labs
- “What is the worst case effect of the number of NSEC3 hash iterations on the query load of a recursive name server?”
- Observations:
  - Key length has more impact than hash iterations for resolver; 150+ iterations halves performance.
  - Authoritative server suffers more than the resolver; 100 iterations halves performance.

IPv6 and Recursive Resolvers

- Turn on IPv6 breaks 0.078% of the users: 470.000 users
- How do we make the transition less painful?
- Don't let users with broken IPv6 connectivity about AAAA records
- NANOG, ISOC, OARC: “Ugly, necessary hack”
- BIND9 implemented it, PowerDNS and Secure64 plan to

draft-ietf-dnsop-dnssec-dps-framework-01

- A framework to assist writers of DNSSEC Signing Policy and Practice Statements
- .SE revised the document.
- “Please read it!”

draft-ietf-dnsop-dnssec-trust-history-01

- Service to help resolvers recover from stale trust anchors
- RRtype: TALINK (58)
- Rollover and Die issue?

draft-ietf-dnsop-dnssec-trust-history-01

- Lifetime of keys, if expired:
  - No Connectivity
  - No DNSSEC
  - Out-of-band Software Update
- No hold-down timer when adding a key to the history, if not using 5011
  - Follow regular rollovers, warn operators in case of updates

draft-ietf-dnsop-rfc4641bis-02

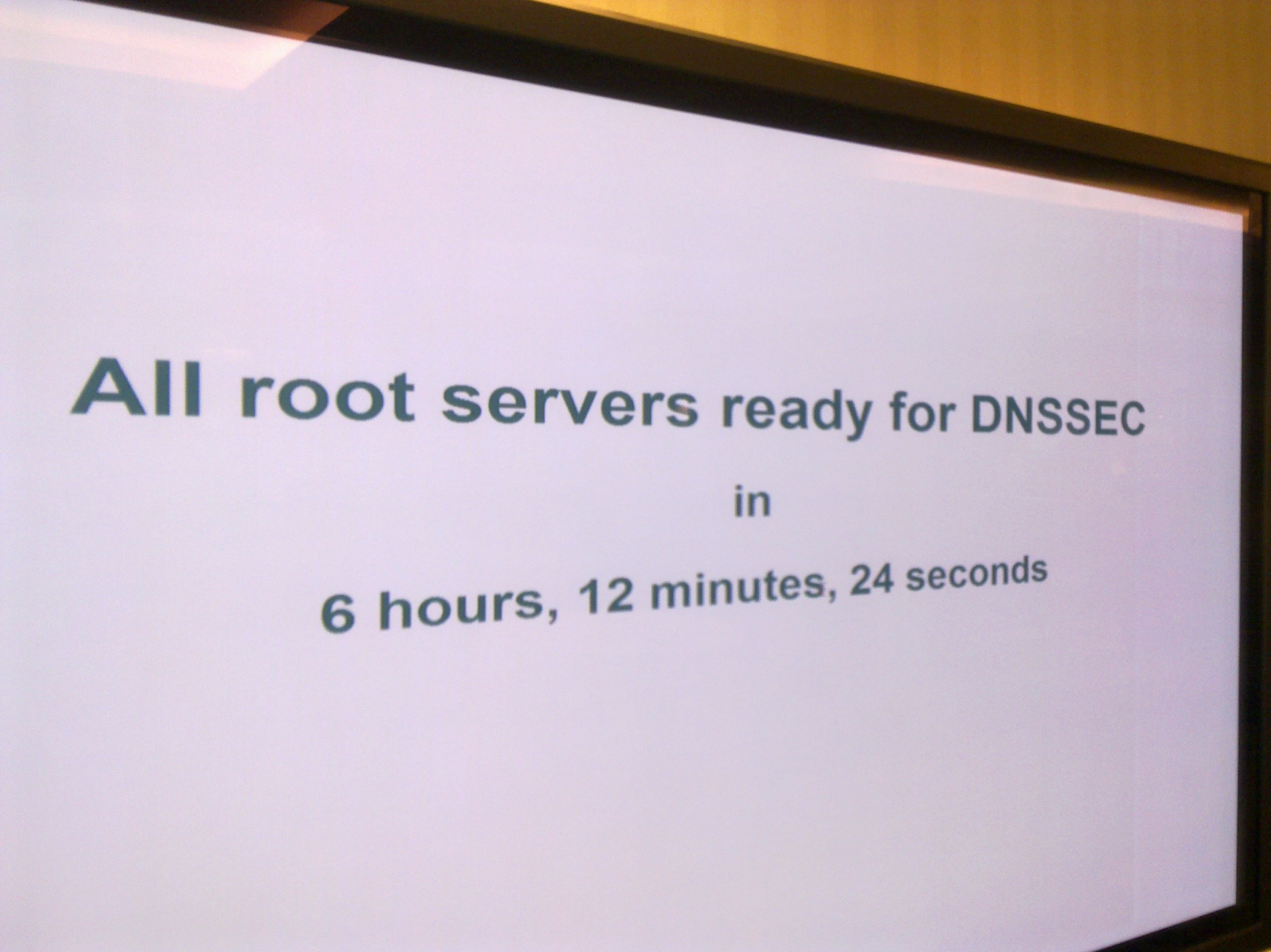
- HSM
- NSEC or NSEC3?
- Review of NIST by Scott Rose
- Switching DNS Operators
- Still a bunch of open issues:
  - Key rollover frequency
  - Target audience: Large TLD vs. “Mom and Pop”
  - http://www.nlnetlabs.nl/svn/rfc4641bis/trunk/open-issues/

draft-morris-dnsop-dnssec-key-timing-02

- Described all rollover mechanisms in detail
- Algorithm rollover in a different document
- Keep separate from 4641 bis
- Adopted by the WG

draft-howard-isp-ip6rdns-03

- Analyse possible ways for IPv6 Reverse DNS
- No recommendations, just list possible ways
- Small changes
- Discussion about having recommendations
- What's the purpose of the document


All root servers ready for DNSSEC
in
6 hours, 12 minutes, 24 seconds

Root Signing Q&A

- UDP query rate of A going down, no real explanation
- Small increase in TCP query rate (up to 80 QPS)

Root Signing Q&A

- Issue “Improper maintenance of trust anchors”
  - Needs more research
  - RFC 5011
- Frequency of KSK Rollover?
  - 5 year, lifetime of HSM
- Statistics for IPv6
- OARC's DNS Reply Size Test Server

- http://tools.ietf.org/wg/dnsext
- http://tools.ietf.org/wg/dnsop
- http://www.root-dnssec.org