IETF66 DNSEXT

Montreal, CA, IETF 66

Jabber: xmpp:dnsext@jabber.ietf.org

http://tools.ietf.org/wg/dnsext

https://datatracker.ietf.org/public/meeting_materials.cgi?meeting_num=66

AGENDA

- Administrivia
  - Appointment of Scribes
    - Official: Robert Martin-Legene
    - Jabber: Marcos Sanz
  - Previous Minutes
  - Agenda Bashing
- Document Status
- Denial of Existence (NSEC3) Status
- Automated Trust Anchor management
- Other Topics
- Milestones

Documents Advanced

- CERT RR bis: RFC4389
- Epsilon: RFC4470
- DS SHA-256: RFC4509
- N-P
  - Derivation of DNS Name Predecessor and Successor In AUTH48
  - draft-ietf-dnsext-dns-name-p-s-02.txt
- Wildcard Clarify
  - RFC-Editor queue
  - draft-ietf-dnsext-wcard-clarify-11.txt
- DHCID
  - RFC-Editor queue (IANA assign state)
    - We checked at the desk: typecode has been assigned)
  - draft-ietf-dnsext-dhcid-rr-13.txt

Documents Advanced(II)

- NSID
  - Name Server Identifier Option
  - In IETF last call
  - draft-ietf-dnsext-nsid-02.txt
- LLMNR
  - Publication Requested as Informational, IESG will dispose of it next meeting.
  - draft-ietf-dnsext-mdns-45.txt
- DNSSEC experiments
  - Publication Requested as Experimental
  - draft-ietf-dnsext-dnssec-experiments-03.txt
- OPT-IN
  - Publication requested as Experimental
  - draft-ietf-dnsext-dnssec-opt-in-09.txt

Last call completed waiting for chair:

- DSA Keying and Signature Information in the DNS
  - Needs more reviewers to say they read it.
  - draft-ietf-dnsext-rfc2536bis-dsa-06.txt
- Storage of Diffie-Hellman Keying Information in the DNS
  - Needs more reviewers to say they read it.
  - draft-ietf-dnsext-rfc2539bis-dhk-06.txt

Drafts (almost) in last calls:

- Transition Mechanisms
  - draft-ietf-dnsext-dnssec-trans-04.txt

Ongoing

- Clarifications and Implementation Notes for DNSSECbis
  - draft-ietf-dnsext-dnssec-bis-updates-03.txt
  - See later presentation
- Domain Name System (DNS) IANA Considerations
  - draft-ietf-dnsext-2929bis-03.txt
- Enhanced Privacy on Negative answers NSEC replacement Requirements
  - draft-ietf-dnsext-signed-nonexistence-requirements-03.txt

Ongoing (II)

- DNSSEC Hash Authenticated Denial of Existence
  - draft-ietf-dnsext-nsec3-06.txt

In holding state

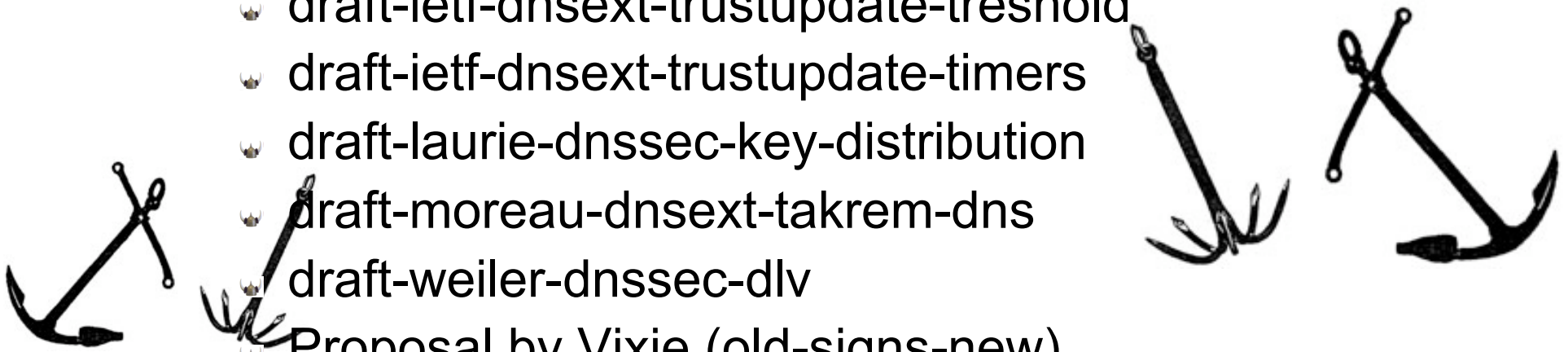
- RSA/SHA256 Algorithm
  - draft-ietf-dnsext-dnssec-rsasha256-00.txt
- ECC KEY
  - needs simplifications
  - draft-ietf-dnsext-ecc-key-09.txt

NSEC3 status and issues

- http://www.nsec3.org contains the issues list.
- David Blacka will lead discussion on open issues and experiences.

Automated DNSSEC Trust anchor management

- Trust Anchor Update requirements in DNSSEC
  - draft-ietf-dnsext-rollover-requirments-02.txt
- Initial set of trust-anchor management proposals
  - draft-ietf-dnsext-trustupdate-treshold
  - draft-ietf-dnsext-trustupdate-timers
  - draft-laurie-dnssec-key-distribution
  - draft-moreau-dnsext-takrem-dns
  - draft-weiler-dnssec-dlv
  - Proposal by Vixie (old-signs-new)

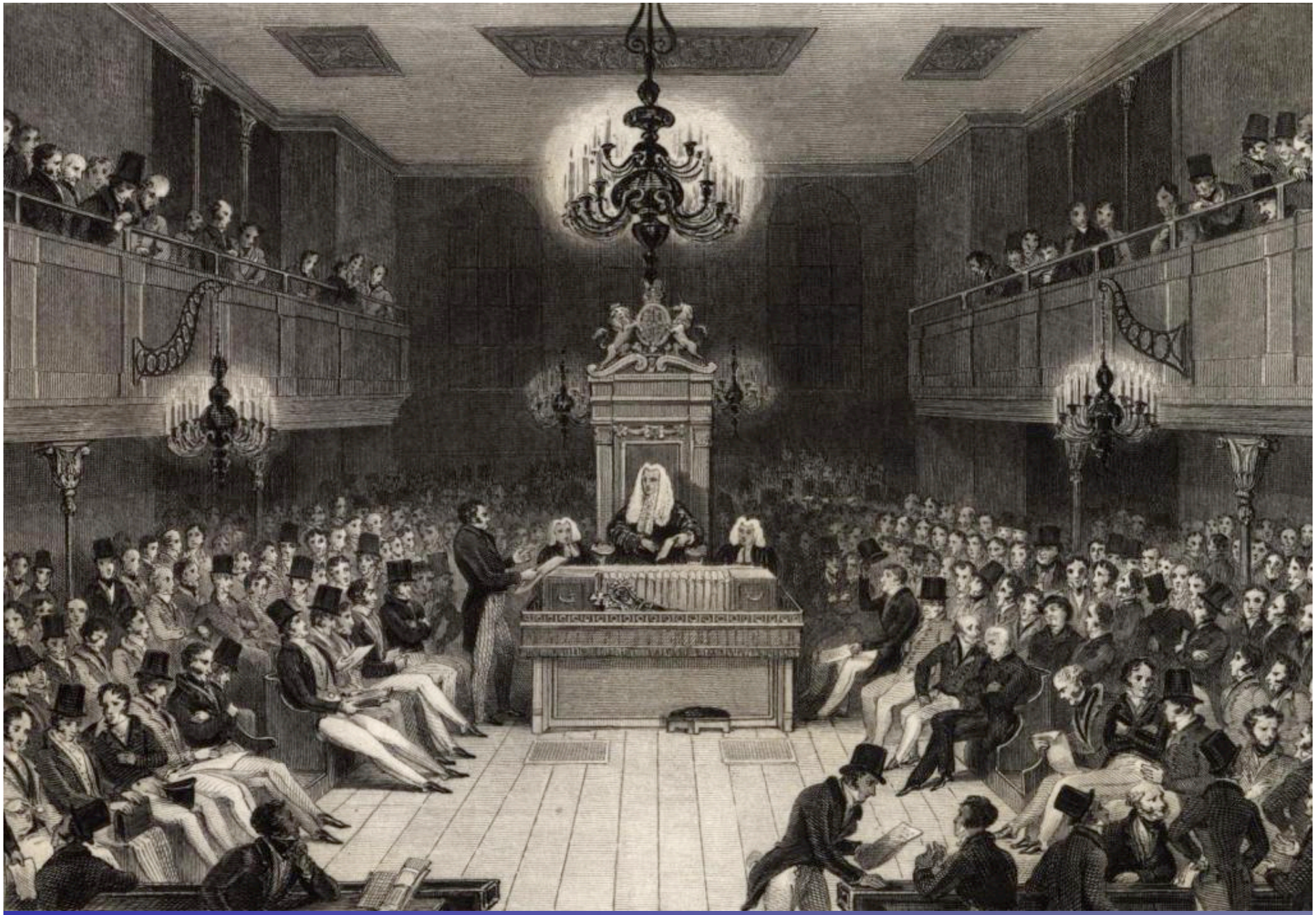


Key rollover scope

- This is about replacing the trust anchor(s) based on existing trust
- Not about efficiently making use of a multitude of islands of trust.
- Is this a fair assessment?
- Do we have consensus to not consider DLV in *this* discussion
- Do we have consensus to consider laurie's dnssec key distribution

Key rollover: Reviews

- Reviews seem to converge to threshold, timers, or threshold-with-modifications
  - Timers has certain security properties that are not available in threshold
  - Reviewers seem to like some of these in threshold too
  - Others prefer the extreme of threshold with minimal parameters (paraphrasing the Vixie proposal)
  - Timers seems to be complete
- Question: if timers seems ready, what are the benefits of further refining threshold?



IETF 66 DNSEXT WG

Other topics

- DNAME-bis: Why update DNAME RFC
  - Matt Larson
- RFC2929-bis Update
  - Donald Eastlake
- DNS Cookies
  - Donald Eastlake
- Identifying and responding to unsolicited queries
  - Peter Koch
  - draft-koch-dns-unsolicited-queries

Milestones

Jul 2006 Finalize trust anchor rollover requirements

Jul 2006 Finalize DNSSEC transition mechanisms

Aug 2006 Finalize Zone Enumeration Requirements

Aug 2006 Version 0 of DNAME clarification (outlined draft)

Aug 2006 Select candidate for working group output for trust anchor rollover

Oct 2006 WGLC trust-anchor rollover

Oct 2006 Submit KEY algorithm documents RFC253[69]bis to IESG for proposed standard

Oct 2006 Version 1 of DNAME clarification

Oct 2006 NSEC3 WGLC

Nov 2006 draft-fleming-007-21 ready for publication

Dec 2006 RFC2672bis (DNAME) to Draft Standard or revision, WGLC

Dec 2006 RFC1982 (Serial Number Arithmetic) interop report

Jan 2007 (placeholder)

RFC2845 (TSIG)to Draft standard, RFC2671bis (EDNS0) to Draft Standard, RFC2136bis (Dynamic Update) to Draft Standard, RFC3007bis (Secure Update) to Draft Standard, RFC1995bis (IXFR) to Draft standard, RFC1996bis (Notify) to Draft Standard, RFC2930bis (TKEY) to Draft standard, RFC2181bis (Clarify) to Draft Standard, RFC2308bis (Neg Caching) to Draft Standard, RFC2782bis (SRV RR) to Draft Standard, RFC3226 (Message Size) to Draft

AOB