

DNSEXT @ IETF-76

Olafur Gudmundsson
Andrew Sullivan

Note Well

Any submission to the IETF intended by the Contributor for publication as all or part of an IETF Internet-Draft or RFC and any statement made within the context of an IETF activity is considered an "IETF Contribution". Such statements include oral statements in IETF sessions, as well as written and electronic communications made at any time or place, which are addressed to:

- The IETF plenary session
- The IESG, or any member thereof on behalf of the IESG
- Any IETF mailing list, including the IETF list itself, any working group or design team list, or any other list functioning under IETF auspices
- Any IETF working group or portion thereof
- The IAB or any member thereof on behalf of the IAB
- The RFC Editor or the Internet-Drafts function

All IETF Contributions are subject to the rules of RFC 5378 and RFC 3979 (updated by RFC 4879).

Statements made outside of an IETF session, mailing list or other function, that are clearly not intended to be input to an IETF activity, group or function, are not IETF Contributions in the context of this notice.

Please consult RFC 5378 and RFC 3979 for details.

A participant in any IETF activity is deemed to accept all IETF rules of process, as documented in Best Current Practices RFCs and IESG Statements.

A participant in any IETF activity acknowledges that written, audio and video records of meetings may be made and may be available to the public.

WG status

- See:
 - <http://ops.ietf.org/lists/namedroppers/namedroppers.2009/msg02861.html>
- New charter:
 - <http://tools.ietf.org/wg/dnsext/charters>
- Presentations:
 - <http://tools.ietf.org/wg/dnsext/agenda>
- Scribes:
 - Minutes:
 - Jabber:
 - Slide Monkey: Ed Lewis

DNSSEC drafts

- DNSKEY registry states Scott Rose
(proxy: Olafur)
- DNSKEY registration rules Paul Hoffman
DNSSEC GOST WG/LC comments
- DNSSEC-bis-updates

DNSSECbis Trust Anchor “selection”

- Options:
 - Closest
 - All must work
 - Try all; all must be SECURE
 - Any may work
 - Try until you get (any) SECURE
 - If any yield BOGUS, and all the others are INSECURE, result is BOGUS
 - If all INSECURE, result is INSECURE

Drafts in adoption queue

- Documents asking to become WG documents:
 - draft-hoffman-dnssec-ecdsa
 - draft-hoffman-dnssec-dsa-sha2
 - draft-barwood-transport-signal

DNS and TCP transport

- DNS TCP transport
 - TCP Transport Required
 - Ray Bellis
- TCP security considerations
 - Fernando Gont
- Stateless TCP
 - Geoff Huston

DNS Transport model

- Answer size =
- 1..512 UDP sufficient Standard DNS
- 1..1480 EDNS0 Enhanced DNS over UDP
 - Some fire walls block EDNS0 or EDNS0 > 1024
- 1500 EDNS0
 - EDNS0 unreliable for many due to fragmentation, middle boxes, firewalls, bad DNS software
- Fallback == TCP
 - It is required currently but not frequently used, we expect it to become used more frequently.

Other