

Revised IANA Considerations for DNSSEC

draft-hoffman-dnssec-iana-cons

Paul Hoffman
DNSOP working group
IETF 109, virtual
2020-11-16

Motivations: GOSTbis, post-quantum

- draft-ietf-dnsop-rfc5933-bis needs to be on Standards Track because the algorithms in DS records are “standard required”
- In the coming years, there will be many proposals for quantum-resistant signing algorithms
- Other IETF WGs have all their registries either “expert review” or “RFC required”

This draft

- RFC 6014 (passed by DNSEXT in 2010) made all the new DNSSEC registries “RFC required”
- We forgot DS records
- Also, NSEC3 decided to go with “standard required”
- Currently makes them all “RFC required”

Three choices for requirements

- Standard
 - Must have full IETF review
 - Probably will require DNSOP review
- RFC
 - Can be done through the Independent Series Editor (ISE), no IETF review
 - IESG gets a preview and comment
- Specification
 - External document, particular Internet Draft, RFC
 - Always has expert review

Expert review

- Experts work at the behest of the IESG
 - IESG can replace the expert if they aren't meeting expectations (too slow, too conservative, too liberal)
- All decisions by the expert can be appealed to the IESG
- TLS, IPsec, S/MIME, ..., tend to be going toward specification required with expert review

Next step

- Do nothing
 - draft-ietf-dnsop-rfc5933-bis has to be a standard
- Adopt draft-hoffman-dnssec-iana-cons, choose “RFC required”
 - draft-ietf-dnsop-rfc5933-bis can be moved forward as an informational RFC, like most other national crypto RFCs in the IETF
- Adopt draft-hoffman-dnssec-iana-cons, choose “specification required”
 - draft-ietf-dnsop-rfc5933-bis could be used, or it could be moved forward as an informational RFC