Revised IANA Considerations for DNSSEC

draft-ietf-dnsop-dnssec-iana-cons

Paul Hoffman
DNSOP working group
IETF 111, virtual
2021-07-26
Document status

• Adopted as WG work item after IETF 109
• 1.5 pages of text, plus normal front and back stuff
• Little discussion on the list
• May be ready for WG Last Call?
Motivations: GOSTbis, post-quantum

- draft-ietf-dnsop-rfc5933-bis currently needs to be on Standards Track because the algorithms in DS records are “standard required”
- But some disagree with making every national crypto algorithm need an IETF standard just for DS records
- There are already many proposals for quantum-resistant signing algorithms
  - NIST is now proposing to have multiple algorithms, not just one
What preceded this draft

- RFC 6014 (passed by DNSEXT in 2010) made all the new DNSSEC registries “RFC required
  - Forgot to back-port DS and NSEC records
  - No justification given for the difference

- RFC 8624 (algorithm implementation requirements and usage guidelines) talks about GOST as “MAY”, doesn’t say anything about other national algorithms
What this draft does

• Update RFC 6014 to have DS and NSEC3 be “RFC required” like the rest of the RRtypes
• Update RFC 8624 to automatically make these non-standards-track algorithms “MAY implement”
• That’s all