Proposal to revise RFC 4641 on DNSSEC Operational Practices

Paul Hoffman

Why revise RFC 4641

- We have learned a bunch in the past two years
- The cryptography that was added after WG LC is flawed
- The discussion of key rollover times has no justification for the times chosen
- It mixes the discussion of publishing trust anchors and publishing keys in a signed parent zone

What have we learned

- Deployment issues from .br, .se, and RIPE's part of inaddr.arpa
- Picky investigation of the stability issues of PIR's proposal to start signing .org before the DNS root is signed

4641's crypto is flawed

- The size choices is mostly handwaving not supported by analysis
- Key signatures are very different than document signatures because keys are relatively short-lived; this changes the sizes needed
- Maybe also include NIST guidance
- We can simplify the choices

Key rollover is misunderstood

- There is no justification for “one year”: it could just as well have been “ten minutes” or “100 years”
- Regular rollover period is directly related to perceived attacks, the cost of such attacks, and the cost of botched updates
- Much more description is needed
- Likely outcome: many zones will only need to do emergency rollovers

Publishing trust anchors is very different than publishing child keys

- When you have a parent signing your keys, you can make very different choices
- Prime example: rollover strategies
- Another big difference: experimenting with different key signing algorithms
- Divide the relevant content into two clearly-delineated sections

Next steps

- See if the WG cares (already started)
- If so, ask Olaf and Miek to open the doc up again
- Maybe make this a WG item