KSK Futures BoF
IETF 104, Prague

Paul Hoffman
Why we are here

• The process of rolling over KSK for the root zone was begun in 2015
• The new key was put into use on 11 October 2018, and the old key will be removed on 22 March 2019
• A lot of surprising things were found during the rollover process
• What have we learned about rolling over the KSK that we can apply to future rollovers?
  – There is already a wide variety of views expressed
What’s already happening

• White paper covering the process

• Discussion is already happening on the mailing list
  – Subscribe and review the archives at https://mm.icann.org/mailman/listinfo/ksk-rollover
Next steps

• Saying things here today is definitely useful, but it will be even more useful if whatever you say is also brought to the mailing list so that a wider audience can see it and discuss it
  – This can be more about group discussion than individual’s statements

• In the second half of 2019, IANA will review the discussion, evaluate the proposals, prepare a draft plan, and bring that plan to the community for public review
Validating resolvers and ./IN/DNSKEY

- A validating resolver needs to have the DNSKEY RRset for the root zone in order to validate.
- This RRset expires after 48 hours, so all validating resolvers send a request for ./IN/DNSKEY to a root server at least every 48 hours.
- If they get a response that cannot be validated against their trust anchor, they will retry the request.
DNSKEY queries seen at most of the root servers

- Increases in the volume of root DNSKEY requests after the rollover, and again after the revocation
- No seeming impact: there have been no complaints
- Not clear if these systems have any users making queries or if they are just on autopilot
- 40,000 QPS is about 8% of the total query volume seen by the root servers
Before and after the revocation of KSK-2010

- This chart shows the change in root DNSKEY query rates before and after 11 January 2019.
- The green band are hosts asking for the root DNSKEY at about the same rate before and after the revocation.
- There are a lot of hosts asking for the DNSKEY (pink area) that were not asking before, and only a few asking less frequently.
Some of the previous comments (1)

• Why roll at all? What are the motivations?
• How often to roll?
  – Every $X$ years
  – Wait until it is proven to be needed
  – Roll every year
    • Some vendors express concern about systems sitting on a shelf for more than a year
• Need better tools to say when resolvers are ready for an upcoming rollover
Some of the previous comments (2)

- Need better bootstrapping for the resolvers that are running up-to-date software
- Adding standby keys makes rollovers easier for systems using RFC 5011
  - Standby key is planned just for normal rollovers, not when the active key is lost or compromised
- Should there be standby keys? If so, what are the important considerations?
- Should the signing algorithm change? If so, what are the important considerations?
Today’s discussion

• Make your proposal or ask your question, but also consider responding to earlier discussion
• It’s OK to bring up something completely new
• Getting DNSSEC widely deployed has been difficult: will your suggestion cause it to be easier or harder to get more zones signing and more resolvers validating?
• Again: after this meeting, please take your ideas to the mailing list