Root Zone KSK Roll

ICANN 48, Buenos Aires, 20 Nov 2013

Root Zone KSK Roll

- Starting planning to develop an approach and relevant documentation to execute a (non-emergency) scheduled KSK rollover, based on input received and contractual obligation

Early Stages

- Root Zone Partners met in Berlin IETF to start this work
  - digesting input received from public consultation and community
  - identifying types of research, testing and outreach necessary

Parameters

- Do not expect any changes to signing parameters for the root zone
  - no algorithm roll
  - no change in key sizes

Mechanisms

- Early publication of trust anchors for incoming KSKs
- RFC 5011 semantics with generous timing

Outreach

- Anticipate widespread communication to a technical/operational audience
  - IETF, *NOG, RIPE, APRICOT, DEFCON, RSA, others?
- Envision continued formal and informal consultations throughout the process

RFC 5011 Testing

- Deployment of a public testbed
- Directed engagement of prominent validator operators, mobile device vendors, browser/plugin vendors, others?
- Extensive testing of known software including unbound, BIND9, Power Recursor, Vantio, others?

Response Size Testing

- Can expect DNSKEY response sizes to grow during the rollover event
  - fragmentation of responses using UDP/IPv6 greater than 1280 bytes is a particular concern
- Plan a widespread survey of tolerance of real-world validators to response size

Rollback

- We expect to retain the ability to roll back to known safe states during the execution of the KSK rollover
- A key open question is how to detect breakage and gauge its severity, to inform any decision to rollback

Future Rollovers

- Anticipate a regular KSK roll schedule, perhaps every 3-5 years
  - sufficiently frequent to facilitate operational currency
  - not so frequent that the operational cost for the Root Zone Partners and validator operators is excessive
- Future rollovers are dependent on a successful first rollover

Status

- Consider recommendations from SSAC Advisory on DNSSEC Key Rollover in the Root Zone (SAC 063)
- Summarize input received from public consultation and other community input
- Seek to fully understand the impact the new delegations will have on the overall stability and security of the DNS
- Reassess potential KSK rollover timeline in light of above

Talk to Us

- Usual suspects from ICANN and Verisign
  - David Blacka, Al Bolivar, Terry Manderson, Tomofumi Okubo, Brad Verd, Duane Wessels, Rick Lamb
- rootsign@icann.org