Root Zone KSK Roll

A Brief and Early Update

IETF 87, Berlin, August 2013

Joe Abley, ICANN; David Blacka, Verisign

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 this week to start this work
    - still digesting input received from public consultation
    - 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

Plausible Timeline

- Direction to proceed, draft documentation published by end of 2013
- Outreach throughout 2014
- New trust anchors published around July 2014
- Testing complete and final revisions of documentation published by October 2014
- Execute KSK rollover January-July 2015

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

Talk to Us

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