# Operational Aspects of Root Zone KSK Rollover

ICANN 46 Beijing

Joe Abley

# Current Root Zone KSK

- The current KSK was generated in Ceremony 1 and brought into service in Ceremony 2 in July 2010
    - Physically stored in four HSMs
        - two HSMs in secure storage in each of two Key Management Facilities
- Exercised during every ceremony (quarterly) to produce a signed DNSKEY RRSet
    - provided to the Root Zone Maintainer for service

# KSK Management Systems are Rollover-Ready

- The transition from a Deliberately-Unvalidatable Root Zone (DURZ) to production in July 2010 was carried out as a KSK rollover

- Software used to exercise the KSK is published at http://data.iana.org/

  - source code for ICANN software is available

  - DVD image used in ceremonies is available (currently based on CentOS)

# KSK Rollover Initiated in a KSK Ceremony

- All key management actions are performed during ceremonies so that they can be audited
  - four ceremonies per year
  - each ceremony involves ICANN staff and also Trusted Community Representatives who travel to the KMF to participate

# Impact of KSK Rollover

- No direct impact on zone administrators (TLD or otherwise)
- No direct impact on the root zone partners (the change is managed using the existing processes; ceremonies accommodate key rollover)
- Possible widespread impact on validators as soon as signatures generated using the outgoing KSK are withdrawn

# Mitigation of Validator Impact

- Root zone KSK rollover follows RFC5011
  - but with no standby key
- Reaction to the rollover was tested in 2010 by a third-party contractor
  - some bugs were found in validator implementations, were reported and fixed
  - report concluded that properly-configured validators would accommodate a root zone KSK rollover

# Trust Anchor Retrieval

- A validator that has been off-line full the full duration of a KSK rollover will not be able to make use of RFC 5011 semantics
- This case is effectively that of a newly-deployed validator
  - bootstrap required

# Existing Committments

- ICANN will perform a KSK Rollover within the first five years of production operation
  - precise timing was not specified since the extent of RFC5011 implementation in validators was unknown, and expected to be low
  - consultation through the ICANN Public Comment Process is open, right now

# Consultation

- Open Public Comment on Root Zone KSK Rollover
  - comment period closes on 13 April
  - 8 responses received so far (2013-04-07)
- If you have an opinion, please submit a comment

# Questions?

ICANN46 Beijing
Joe Abley