DNSSEC Workshop

Update on Root Key Rollover

Russ Mundy, Parsons (Sparta)

ICANN

Overview

- This SSAC Work Party is considering issues relating to the rollover of the Domain Name System Security Extensions (DNSSEC) Key-Signing Key (KSK).

- This work is not meant to result in a definitive advisory, but will provide an inventory and study of the issues related to a key rollover.

- The Work Party is exploring:

  - Possible root zone KSK rollover scenarios; and

  - Complications and complexities unique to the handling of root zone keys.

- IANA also held a recent public consultation on the contract requirement to perform a scheduled root zone KSK rollover. The Public Comment period ended on 31 May. Further consultation with the community is expected in the next few months.

Issues

- The Work Party is considering the following issues:
  - Key Management in the Root Zone
    - Zone-Signing Key (ZSK) Operational Role; and
    - Key-Signing Key (KSK) Operational Role.
  - Motivations for KSK Rollover.
  - Risks Associated with Key Rollover
  - Available Mechanisms for Key Rollover:
    - RFC 5011 Rollover;
    - Non-RFC 5011 Rollover; and
    - Common Resolver Rollover Requirements.
  - DNS Response Size Considerations.

ICANN

Next Steps

- The Work Party will produce a document for the review of the full SSAC.

- The SSAC will decide whether and/or when to publish the final document.

ICANN