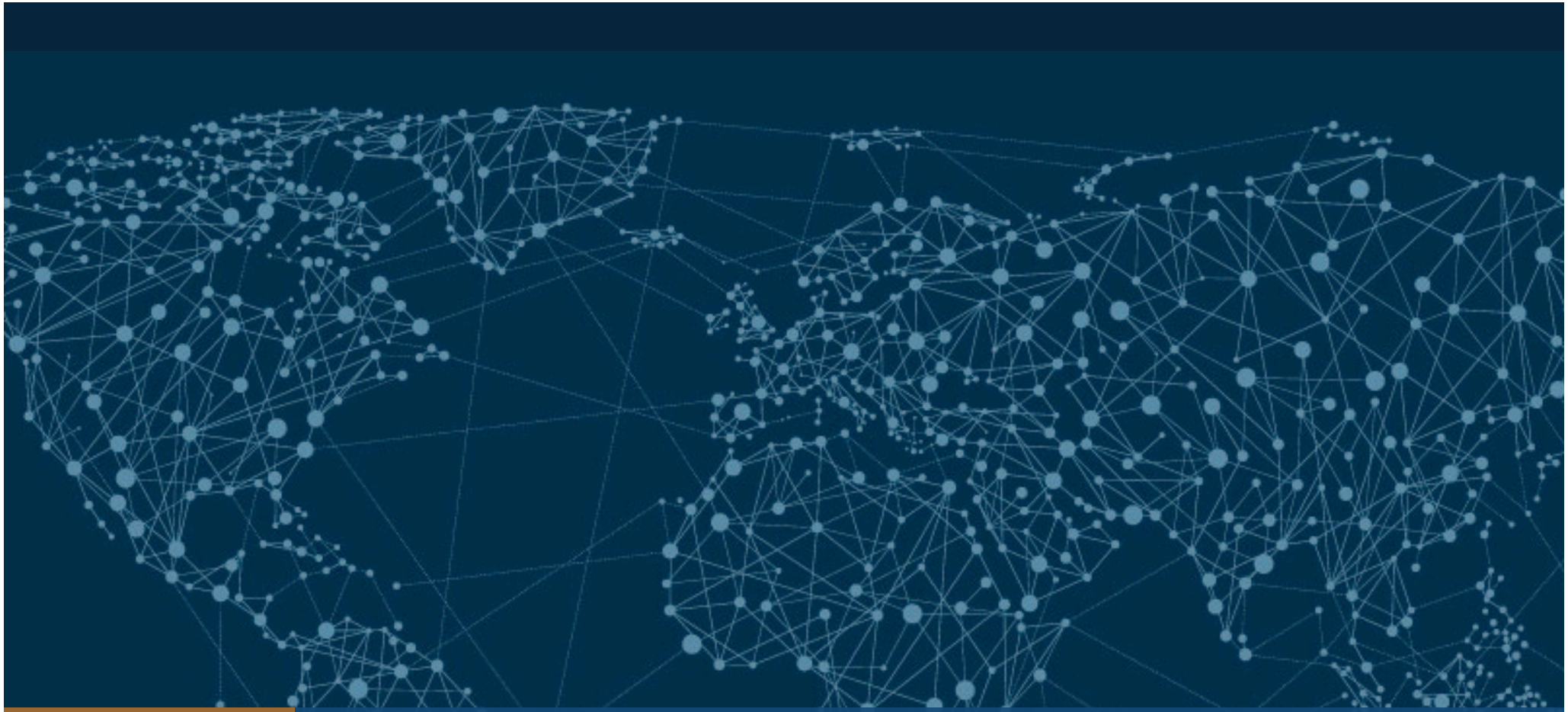

Rolling the KSK

Edward Lewis | NANOG 67 | 14 June 2016
edward.lewis@icann.org

Agenda

- Root Zone DNSSEC operations
- Dates of the KSK Roll
- Related Activities

DNSSEC in the Root Zone

- DNSSEC in the Root Zone is managed jointly
  - ICANN, as the IANA Functions Operator (IFO)
  - Verisign, as the Root Zone Maintainer (RZM)
  - Coordinated via NTIA arrangements

DNSSEC Key Management in the Root Zone

- DNSSEC key management is divided into
  - Key Signing Key, self-signs the key set
  - Zone Signing Key, signs other zone data

- These roles are meaningful to the operators of signed zones
  - The significance is that the roles are separated

KSK and ZSK

- ICANN, as IANA operator, manages the KSK
  - Same KSK since operations began in 2010
  - Quarterly the KSK signs the ZSK in a ceremony

- Verisign, as RZM, manages the ZSK
  - ZSK is changed quarterly
  - The DNSKEY set in the DNS is managed in 10-day slots

Activities underway

- The ZSK will be lengthened
  - Activity managed by Verisign, covered elsewhere
  - This activity will happen before...
- The KSK will be changed
  - A new trust anchor is needed by all DNSSEC validating DNS caches/clients
- Separate but coordinated activities

Why Change the KSK?

- Primary reason – Operational Preparedness
  - KSK has no expiration date, currently no weakness
  - No key should live forever: bad crypto practice
  - Prefer to exercise process in normal conditions
    - As opposed to abnormal, such as key compromise
- Big challenge
  - Involves countless/uncountable participants
  - No test environment can cover all possibilities

Planned KSK Roll Dates

- **Assuming ZSK lengthening progresses to plan**
- Publically viewable plan available, July 2016
- In KSK Ceremonies
  - October/November 2016, initial generation of KSK
  - January/February 2017, operationally ready
- In DNS
  - New KSK appearance in DNS on July 11, 2017
  - New KSK signs beginning October 11, 2017
  - Revoke current KSK on January 11, 2018

Upcoming Activities

- Presenting the plan (July to December 2016)
  - Informal feedback
- Presenting the new KSK (January to July 2017)
  - New key will be introduced and publicized
- Follow *Automated Updates* (RFC 5011)
  - July 11, 2017 through early 2018

Changing Trust Anchors

- Trust Anchors are configured data in DNSSEC validators
  - If *Automated Updates of DNSSEC Trust Anchors* (RFC 5011) is enabled and working, the roll is automatic
  - Else, manual intervention to add the new KSK before October 11, 2017 (assuming all is on track) and to remove the old KSK at a later date

Testing Resources

- Resources targeted for software developers
  - Two environments with “sped up clocks”
  - http://icksk.dnssek.info/fauxroot.html
  - http://keyroll.systems
- Resources more suitable for operators
  - Will be forthcoming

For More Information

- Join the mailing list:
  - https://mm.icann.org/listinfo/ksk-rollover

- Follow on Twitter
  - @ICANN
  - Hashtag: #KeyRoll

- Visit the web page:
  - https://www.icann.org/kskroll

Engage with ICANN

Thank You and Questions

Reach me at:
Email: edward.lewis@icann.org
Website: icann.org

twitter.com/icann

gplus.to/icann

facebook.com/icannorg

weibo.com/ICANNorg

linkedin.com/company/icann

flickr.com/photos/icann

youtube.com/user/icannnews

slideshare.net/icannpresentations