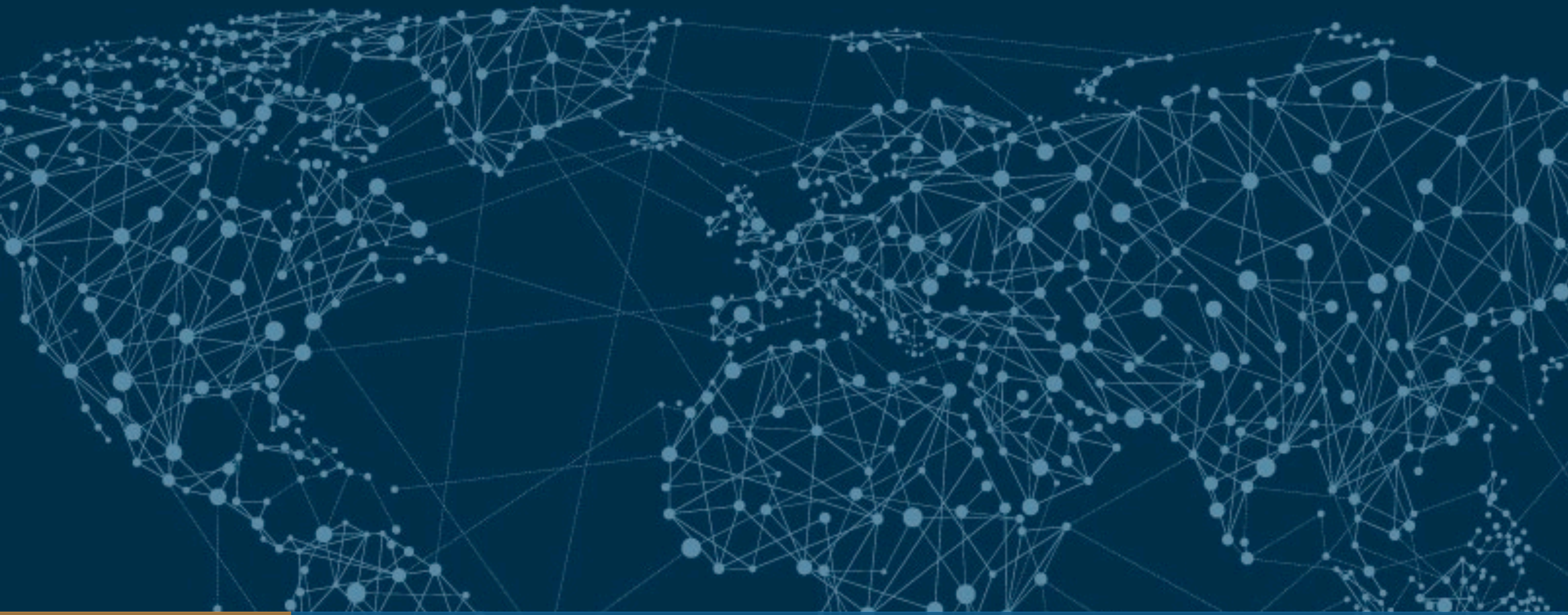

Root Zone KSK Maintenance

Jaap Akkerhuis | ENOG -10 | October 2015

What I’m doing here

- Channeling IANA
- Make people aware this is happening
- Member of design team

Agenda

- Change of Hardware Security Modules (HSMs)
- Roll (change) the Key Signing Key (KSK)

Background

- Root Zone KSK
  - The trust anchor in the DNSSEC hierarchy
  - Has been in operation since June 2010
- "After 5 years of operation"
  - Concerns over original HSM battery life
  - Requirement to roll the KSK
- What's a HSM? What's a KSK? (We'll get to that.)

The Players

- Root Zone Management (RZM) Partners
  - Internet Corporation for Assigned Names and Numbers (ICANN)
  - U.S. Department of Commerce, National Telecommunications and Information Administration (NTIA)
  - Verisign
- External Design Team for KSK roll

- ICANN
  - Performs DNSSEC and KSK functions (plus others) in accordance with the IANA functions contract

What is a...

- KSK?
    - Key-Signing Key signs DNSKEY RR set
    - Root Zone KSK
        - Public key in DNS Validator Trust Anchor sets
            - Copied everywhere - "configuration data"
        - Private key used only inside HSM

KSK ???

What is a...

- HSM?
    - Hardware Security Module
    - Specialized hardware
    - Operates KSK
        - Prevents exposure of private key

Public Impact

- HSM change
  - Happened with no impact

- KSK roll
  - Large impact (on those DNSSEC validating)
  - Anybody operating a validator has the KSK now
  - All copies need to be updated
  - Trusting the new KSK is work to be done

HSM Change (or "Tech Refresh")

- Culpeper, Virginia, USA on April 9, 2015
- El Segundo, California, USA on August 13, 2015

- Plan
  - https://www.icann.org/news/announcement-3-2015-03-23-en
- Archived
  - https://www.iana.org/dnssec/ceremonies
  - "21" and "22" plus the HSM Acceptance Testing for each site

KSK Roll

- Compared to HSM change
    - Greater public impact
    - Various options to consider

- Approach
    - ICANN Public Consultation (2012)
    - Previous engineering effort (2013)
    - Current external design team (2015)
        - Final report due in December
    - RZM Partners follow with a plan

Design Team Roster

- Joe Abley
- John Dickinson
- Ondrej Sury
- Yoshiro Yoneya
- Jaap Akkerhuis
- Geoff Huston
- Paul Wouters

- Plus participation of the aforementioned Root Zone Management Partners

In theory

- On paper...

- The industry collective wisdom is fairly mature
  - There have been many KSK rolls before
  - What works, breaks has been experienced

- The Root Zone KSK is different
  - Other KSK rolls inform the parent (or DLV)
  - A new root KSK has to be updated everywhere
  - Mitigated by RFC5011's trust anchor management

In practice

- …but…

- Any plan will face external challenges
  - Will validators have trouble receiving responses during the roll? (Fragmentation issues)
  - Are automated trust anchor updates implemented correctly?
  - Will operators know how to prepare, how to react?
  - Will all DNSSEC code paths perform correctly?

Challenges

- Coordination is the central theme
  - "What to go to and when to go"
  - Uniquely distributed (management) effort
  - DNSSEC Validator Operators and RZM partners will have to act in concert
    - Build trust in new KSK
    - Deciding when to take the next step
    - Whether going forward or backward

Participate

- **Join the mailing list:**
  https://mm.icann.org/mailman/listinfo/root-dnssec-announce

- **Join the conversation on Twitter:**
  Hashtag: #KeyRollover
  Follow @ICANNtech for the most up to date news