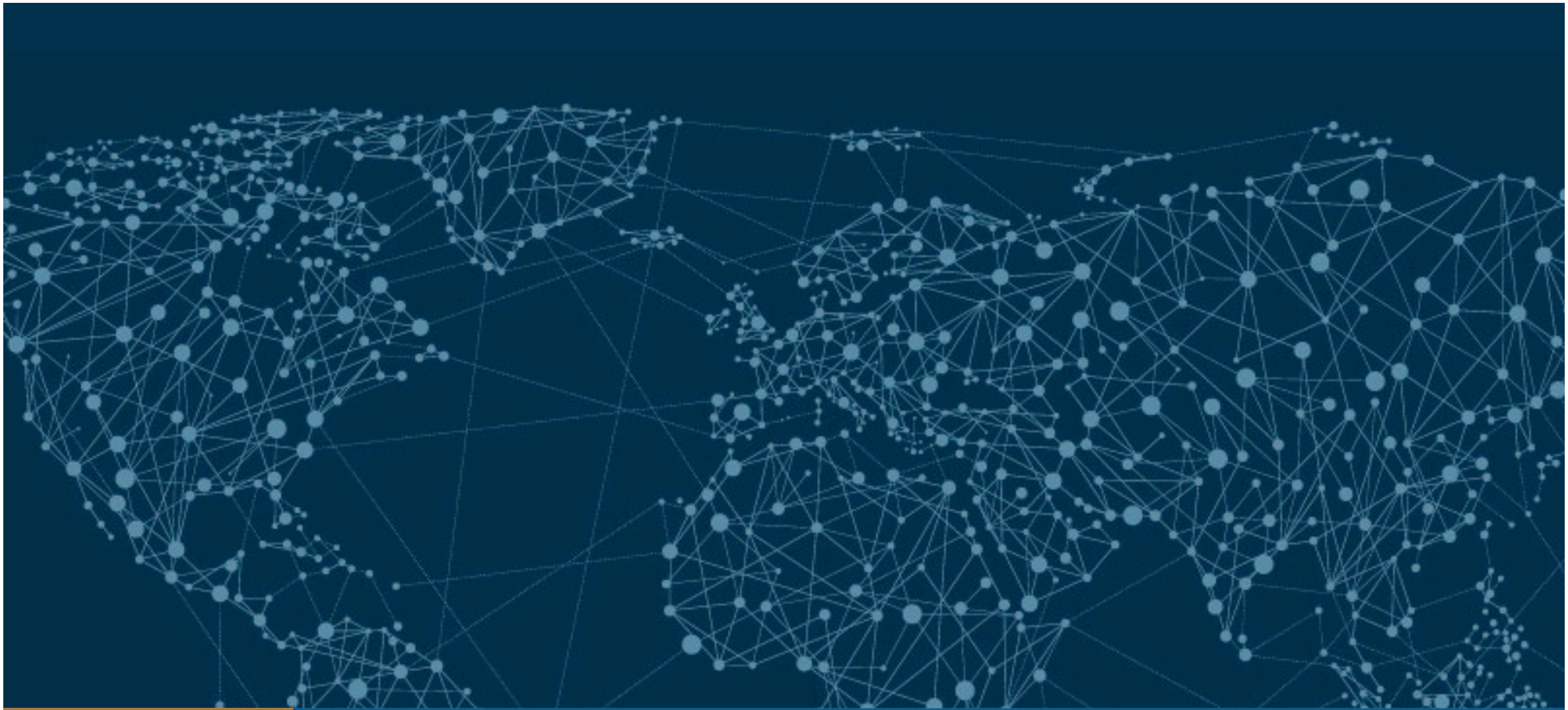

Root Zone KSK: After ICANN 53

Edward Lewis | ICANN 53 | June2015
edward.lewis@icann.org

Agenda

- Setting the scene
- Change of Hardware Security Modules (HSMs)
- Roll (change) the Key Signing Key (KSK)
- The big finish

Background

- Root Zone KSK
  - The trust anchor in the DNSSEC hierarchy
  - Has been in operation since June 2010
    - With no roll of key itself
    - And with no change of HSM (until April 2015)

- "After 5 years of operation"
  - Concerns over HSM (hardware) battery life
  - Requirement to roll the KSK

The Players

- Root Zone Management 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

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

Public Impact

- HSM change
    - Not much impact to the public
        - So long as they work, they are unseen
    - Concerns that existing set is growing old
        - Specifically the internal battery

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

Goal for today

- This presentation is intended to
  - Inform
  - Call attention to a coming ICANN Public Comment Period on KSK roll

- Two means for feedback
  - Informal via mic and mail list, comments picked up by KSK roll Design Team
  - Formal via an upcoming ICANN Public Comment period

HSM Change (or "Tech Refresh")

- Straightforward Replacement
  - Same brand, newer model

- Culpeper, Virginia, USA Facility
  - Ceremony XXI on April 9, 2015 (went flawlessly)
- El Segundo, California, USA Facility
  - Ceremony XXII planned for August 13, 2015

- Documented Plan
  - https://www.icann.org/news/announcement-3-2015-03-23-en

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)

Milestones

- Current Design Team Plan
  - Study, discussion through June
  - Present report for ICANN Public Comment
    - 40 days, opening right after ICANN 53 ends
  - One month to prepare final report

- Root Zone Management Partners then develop a plan and execute

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?

Design Team Document (Rough) Preview

- History, scope, motivations
- Cryptographic considerations
- Protocol considerations
- Operational coordination
- Impact on DNSSEC validation
- Trust Anchor publication
- Testing
- The plan itself
- Analysis of risks

- This list is meant to whet your appetites

In Summary: DNSSEC Links

- http://www.iana.org/dnssec
- http://www.root-dnssec.org
- http://www.verisigninc.com/assets/dps-zsk-operator-1527.pdf