DNSSEC at ARIN

Mark Kosters
ARIN Chief Technology Officer

What do RIRs do?

- Allocates Internet Resources
  - IP Addresses (v4 and V6)
  - Autonomous Numbers
- Publishes Information
  - Whois
  - Resource Certification
  - DNS

Reverse DNS

- Maps an address to a name
- Answers what is the name given this address?
- DNS parlance
  - Give me the name for 192.149.252.33
  - "dig 33.252.149.192.in-addr.arpa ptr"
  - Answer: smtp1.arin.net
- Used for mail, web, ftp, ssh and other services

Problem

- Needed to sign reverse zones
- Parent not signed (in-addr.arpa or ip6.arpa)
- What to do?
  - Not the first – RIPE has been doing this for years
  - Provide static trust anchors with KSKs on the website for each delegation

Staged Approach

- Made sure our DNSSEC secondaries were DNSSEC Capable
- Began signing the zones in Q2 of 2009
- Allowed registrants to place their DS records in our system in Q1 2011

ARIN Online and DNSSEC

- Main way of interfacing with the community
- Also provide a RESTful registration interface
- Video tutorial on how to manage DNS and DNSSEC:
  - https://www.arin.net/knowledge/dnssec/dnssec_full.html

Concurrent Complications

- In-addr.arpa was on the root servers
  - Needed to be moved off to a new set of servers independent of the root servers – completed in Feb 2011
  - In-addr.arpa was signed in March 2011
- ip6.arpa was signed earlier (Sept 2010)
- ARIN DS records for allocations we control were placed in our parent zones March 2011

Now What?

- Since in-addr.arpa and ip6.arpa are now signed there is no need for static-configured trust anchors; you can follow the chain of trust
- No way of knowing how many servers use statically configured trust anchors
- Have not done a key roll in fear of breaking them

Takeaways

- Publishing trust anchors outside the root leads to complications
- No way of really measuring the damage if you do a key roll of the KSK