F-Root's DNSSEC Signing Plans

- Keith Mitchell
- Internet Systems Consortium
- UKNOF15, Rochdale, 21st Jan 2010

Background

- DNSSEC has been around for many years
- Allows for cryptographic verification that DNS records are authentic
- Its time has finally come:
  - Standards and implementations are now mature
  - “Kaminsky” etc vulnerabilities
  - Many TLDs now signed or signing soon: e.g. *.org, .gov, .se, .pt, .br*

Background

- DNSSEC is based upon a hierarchy of "trust anchors"
- The apex of these is the root
- Signing the root is necessary for full deployment
- Will allow DNSSEC-aware clients to follow a completely signed and verified delegation path
- ICANN finally agreed to have this happen in 2010

Background

- IANA and VeriSign, with oversight from ICANN and the US Government DoC, get to control what is published in the root zone
- They have come up with the root signing plan and time-line, available at:
  - http://www.root-dnssec.org/
- The 12 operators of the 13 root server instances will be implementing this plan
- ISC is involved both as **F-root** operator and supplier of BIND software to several others

Possible Side-Effects

- Responses from root servers for "." will include signatures, so will become larger:
  - greater than 512-byte UDP limit
- EDNS0 allows up to 4096-byte responses via UDP over IP fragments
- EDNS0 is now widely implemented in DNS software
- But not so well understood by middleware (e.g. firewall, CPE) devices

Testing Side-Effects

- Testing tool provided by OARC at:
  - https://www.dns-oarc.net/oarc/services/replysizetest
- If you see issues, best to address them on your network now, or there will likely be performance issues when signed root goes live
- The “Deliberately Unvalidatable Root Zone” (DURZ) is a transition measure during this testing phase

The DURZ

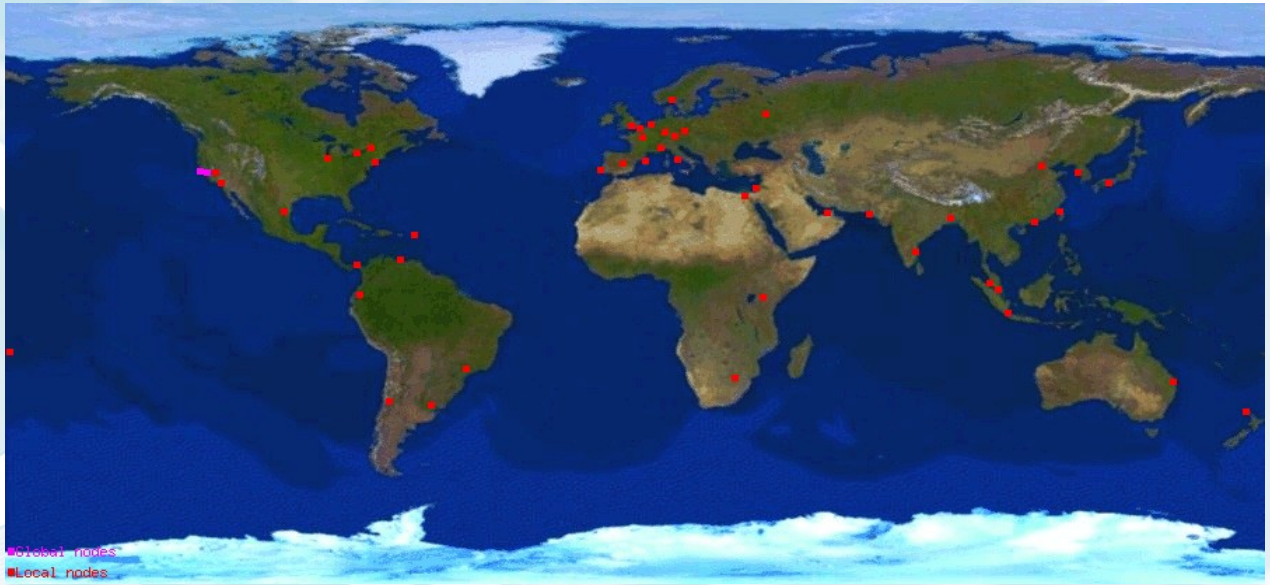
- Between 01-Dec-09 and 25-Jan-10, signed root for internal IANA/VeriSign testing only
- Between 25-Jan-10 and 01-Jul-10, signed root will be served by some operators
- In order to avoid issues during the transition period, the root zone will be signed with a “dummy” KSK and ZSK, the *DURZ*
- The fully signed root will go live on 01-Jul-10, when all operators have transitioned

Tentative Time-Line

- 01-Dec-09: Root zone signed for internal use by VeriSign and ICANN.
- Week of 25-Jan-10: L starts to serve DURZ
- Week of 08-Feb-10: A starts to serve DURZ
- Week of 01-Mar-10: M, I start to serve DURZ
- Week of 22-Mar-10: D, K, E start to serve DURZ
- Week of 12-Apr-10: B, H, C, G, **F** start to serve DURZ
- Week of 03-May-10: J starts to serve DURZ
- May/Jun-10: results studied, final deployment decision
- 01-Jul-10: Distribution of validatable, production, signed root zone; publication of root zone trust anchor

F-root Plans

- There are over 50 anycast instances of F-root globally, each with 2 servers:
  - https://www.isc.org/community/f-root



- We have a 3-hour window in the week defined above to enable all these

BIND Versions

- ISC will be upgrading the version of BIND it uses on its F-root servers to a minimum consistent version:
  - BIND 9.6.2, released in February
- This has support for the SHA-2 DNSSEC algorithm used to sign the root
  - not strictly needed as root servers only serve signed zone as content, not validate it
- Other root operators who use BIND are being encouraged to Beta test this version early

BIND Versions

- Latest version of BIND is 9.7.0, just coming out of Beta
- It has many features to make deployment of DNSSEC within your network much more user-friendly
- Strongly recommend this version for your authoritative servers, validating resolvers etc

Data Gathering

- During the transition, most root operators will be gathering data to monitor for possible issues
- This will be uploaded and shared via
- DNS-OARC (http://www.dns-oarc.net)
- Various tools will be used to capture both long-term trends, and short-term snapshots during changes

Data Gathering Tools

- Continuous Domain Statistics Collector (DSC) summary stats
- Long-Term Query Capture (LTQC) will look at changes in the cache-priming queries to root servers
- tcpdump/dnscap packet capture of all queries during transition windows (DITL)

What About DLV ?

- ISC's DNSSEC-Lookaside Validation service:
  https://www.isc.org/solutions/dlv
  was conceived as a transition tool to connect trust-anchor islands until the root downwards is signed
- We will continue to operate it as long as there are islands that need it, but will be very happy when the need goes away !

Summary

- Full plans/documents available at:
  http://www.root-dnssec.org/
- ISC will be working with other root operators to transition F-root to the DURZ during the week of 12-Apr-10
  - More info at http://blog.isc.org
- BIND 9.6.2 will be available during February to support root operators
- Signed root planned to go live 01-Jul-10
- Try BIND 9.7.0 if you haven't deployed DNSSEC yet !