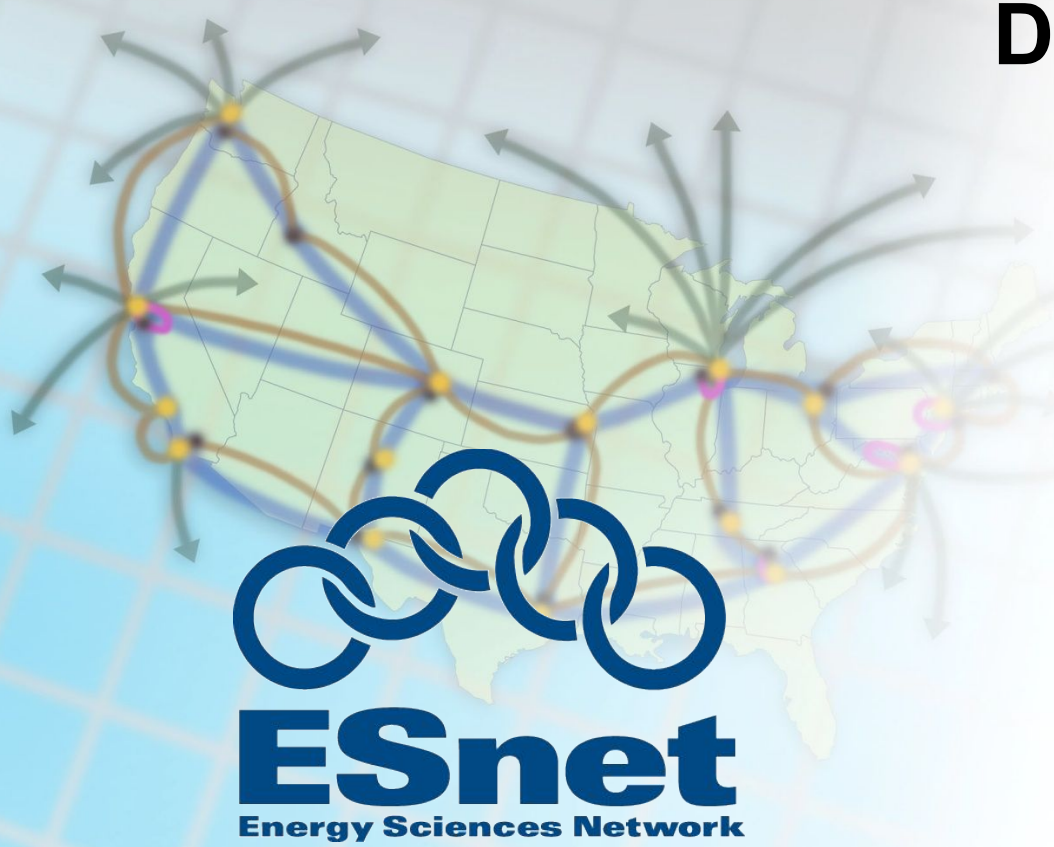


Supporting Advanced Scientific Computing Research • Basic Energy Sciences • Biological and Environmental Research • Fusion Energy Sciences • High Energy Physics • Nuclear Physics

Don't Fear the Signer
DNSSEC and You

R. Kevin Oberman
Sr. Network Engineer

October 20, 2009

NANOG47
Dearborn, MI

Berkeley Lab

U.S. Department of Energy | Office of Science

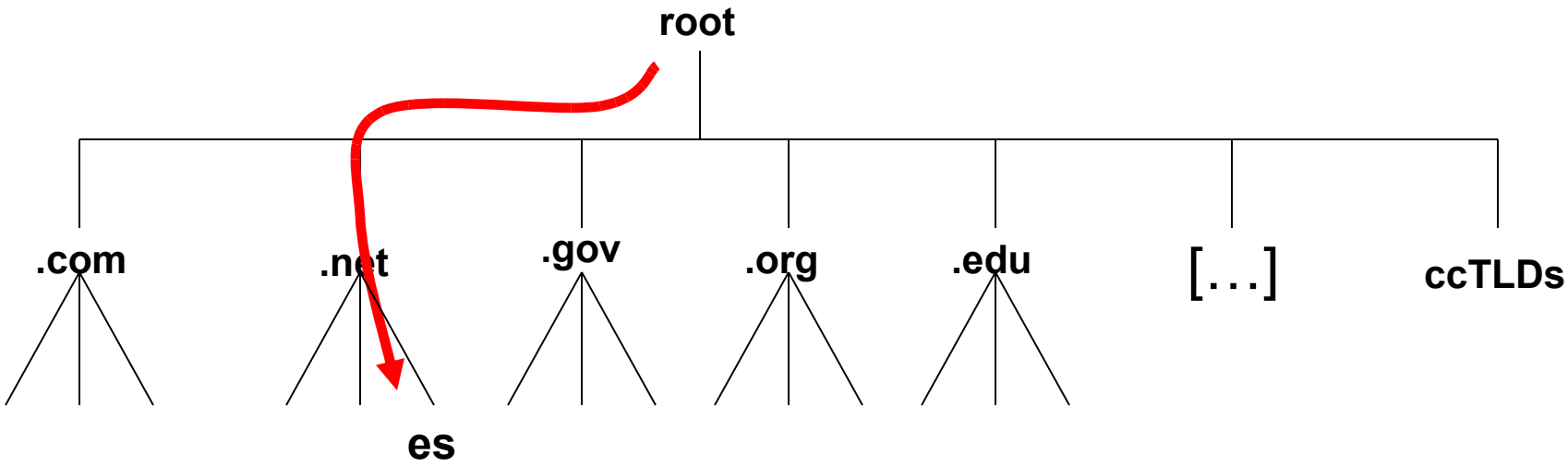
Overview

- DNSSEC Basics—A quick look under the hood
- Why you should sign your data soon
- Implementation status
- Your implementation
- Signing Policies
- How to sign data—Multiple approaches
- Operational Concerns

DNSSEC Basics

- DNSSEC uses public key cryptography
- Similar to SSH
- DNSSEC uses an anchored trust system
- NOT PKI! No certificates
- Trust must start at the root and follow the DNS hierarchy
- You generate key pairs and sign your data
- You make keys available to your parent

DNSSEC Basics



- Root key must be well known
- Root servers know net public KSK
- net servers know es public KSK
- es servers sign *.es.net records with private ZSK

Why You Should Sign Soon

- This is the perfect time to test and experiment as you are free to make mistakes and tweak both policies and procedures
- Once you publish keys, you really don't want to mess up!
- Mistakes can make you service disappear to anyone using a validating server!
- This is a one time offer! Don't pass it up.
  - Once you publish you keys, playtime is over
  - Signing alone has no external impact

Implementation Status

It really IS getting closer!

- Root should be signed next year
- org and gov are signed now
- com, edu and net should be signed in 2012
- Several ccTLDs are signed and more are coming
- Registration issues still being worked on
  - Transfers are of particular concern
    - An unhappy losing registrar could take you down!

Implementation

Until your parent is ready. . .

- Develop signing policies and procedures
- Test, test, and test some more
  - key re-signing
  - key rolls
  - management tools
- Find out how to transfer the initial key to your parent (when the parent decides)
  - This is a trust issue. Are you REALLY big-bank.com?

Implementation

If you are brave…

- Test validation
  - Best done on an internal test server
    - If something breaks, this can hurt you
- Give your key(s) to the DLV or ITAR
  - DNSSEC will then be live and your data subject to validation
  - Playtime will be over

What to Sign

- Forward zones are the big win
  - Reverse zone signing has value
    - Less than the forward zones
- You may not want to sign some or all reverse zones
  - Maybe not some forward zones, either
    - Cases for not signing forward zones are few and far between

How to Sign

- Signing usually involves two 'types” of keys
  - One for signing zone data (ZSK)
  - One for signing keys passed to parent (KSK)
- Keys need to be changed (rolled) regularly
- Signatures (not keys) expire
  - Expired signatures mean no DNS availability

Signing Policy

- Use two active keys (for both ZSK and KSK)
  - Data is re-signed by two newest keys
- Sign at short intervals compared to expiration times
  - Provides a buffer to deal with failures
  - Signing every 24 hours with 14 day expiration
    - Average 13 days to fix a problems

Signing Policy [2]

- New KSKs require that the parent be notified
- Limited use of KSKs mean that it is considered safe to use them for longer intervals
  - ZSKs should be rolled (updated) monthly
    - 1024 bits **(New!)**
  - KSKs should be rolled (updated) annually
    - 2048 bits

Signing systems

- Do it yourself
  - Cheap
    - Assuming that your time is free!
  - Not easy
    - Though not excessively complex
    - Hard part is to ensure reliability
  - Will get MUCH easier
    - BIND 9.7 is intended to largely automate the system
    - Third alpha release is available for testing

Signing systems (2)

Free tools to ‘Do It Yourself’

- DNSSEC-tools (http://www.dnssec-tools.org)
  - Suite of tools that can be used to create a system
- OpenDNSSEC (http://www.opendnssec.org)
  - Turnkey software
  - Support HSMs
  - Not yet completed (Goal is now February)
- BIND (https://www.isc.org/software/bind/)
  - Limited automation, but should be much enhanced in next version

Signing systems (3)

Commercial tools/appliances

- Believed to be available
  - Secure64 (www.secure64.com)
  - Xelerance (www.xelerance.com)
  - Infoblox (www.infoblox.com)
  - Bluecat (www.bluecatnetworks.com)

HSMs and DNSSEC

Hardware Security Modules provide a very secure means of generating key pairs, random numbers, and performing standard cryptographic operations with them

- Use standard APIs (usually PKCS11)
- Vary a lot in terms of cost and capability
- Look for FIPS 140-2 Level 2 or higher certification

Operational Concerns

- You need at least two people able to work with your system
- You need a backup system
- You need a maximum restoration time of less than the shortest possible interval between signing and signature expiration

References

- NIST Special Publication SP800-81
  - SP800-81r1 is available for comment
  - Excellent overview of DNSSEC with detailed examples for BIND and NSD
- Why Deploy DNSSEC?
- DNSSEC HOWTO, a tutorial in disguise
- DNSSEC in 6 Minutes
- BIND Administrator's Reference Manual
- Lots of RFCs! (See above for numbers)