

DNSSEC: Domain Signing in 10 Minutes

Derek McUumber, CEO
<http://www.datamtn.com>
.gov TLD – System Architect
March 12, 2009

Agenda

Domains

Keys

Zone Files

Signatures

Test

Learn

Host

- ✓ www.dotgov.gov DNSSEC Interface
- ✓ DNS Administrator Expectations
- ✓ Tools and Tips

www.dotgov.gov Interface

[Click here for .gov TLD DNSSEC Features](#)

BASIC DNS Security (DNSSEC)

Upload DNSKEY file(keyset file): Sign one or more domain(s) and upload the public keyset file(s) to enable DNSSEC.

Tip: Multiple domains will be updated if *dnssec-signzone* KEYSET files are merged into a single file.

[CLICK HERE TO PRACTICE DNSSEC DOMAIN PROCEDURES BY USING THIS INTERFACE TO PUBLISH TO THE DNSSEC TESTBED \(SNIP\)](#)

[Signzone Instructions](#)

[DNSSEC FAQs](#)

Optional DNS Security (DNSSEC)

Select your DNSSEC Option: You may choose to allow dotgov.gov to generate, monitor, and automatically update DS Resource Records for none, some, or all of your domains.

- No, thanks. I will manually upload my keysets after I have pre-published my KSK (bi-annually).**
- Yes, but only for domains I select below. I will manually upload keysets for unchecked domains.**
- Yes. Monitor and automatically publish DS RRs for all my domains.**

www.dotgov.gov Interface

Domains

Keys

Zone Files

Signatures

Test

Learn

Host

- ✓ Upload the one KSK per domain to establish initial trust
- ✓ www.dotgov.gov will monitor name servers for future changes
- ✓ Key changes will trigger email to Admin POC and Technical POC

DNS Admin: Best Practice

Domains

Keys

Zone Files

Signatures

Test

Learn

Host

- ✓ 1 Active KSK per domain (2 yr cycle)
- ✓ 1 Active/1 Pre-pub ZSK per domain (90 day cycle)
- ✓ RSASHA1 2048 bit keys (NSEC or NSEC3)
- ✓ www.dotgov.gov will monitor and email when cycles are due after initial upload

10 Minute DNSSEC: Steps

Domains

Keys

Zone Files

Signatures

Test

Learn

Host

- ✓ Offline Key Generation
- ✓ Offline DNSSEC Zone Signing
- ✓ www.dotgov.gov communications
- ✓ Offline Key Rolling and Maintenance

Offline DNSSEC Application

Domains

Keys

Zone Files

Signatures

Test

Learn

Host

- ✓ Client application contained on CDROM
- ✓ Useful to rapidly learn the steps and get domains signed
- ✓ Limits options to acceptable lengths and types
- ✓ Tabs from left to right are the steps
- ✓ Generates all keys with one click
- ✓ Stores repository in \$HOME directory
- ✓ Signs zone files and generates a www.dotgov.gov keyset upload file

Example Zone Signing Output

Domains

Keys

Zone Files

Signatures

Test

Learn

Host

fed.gov Signatures:

Last dnssec-signzone parameters and results:

```
-k Kfed.gov.+007+00171 -o fed.gov -e +7776000 fed.gov.hosts Kfed.gov.+007+08345  
fed.gov.hosts.signed
```

Active Signatures:

FileName: fed.gov.hosts.signed
Last Signed: 3/4/2009 1:31:04 PM [View](#)

Prior Signatures:

 nbsp;FileName: fed.gov.hosts.signed
Retired on: 3/4/2009 1:31:04 PM [View](#)

Re-sign fed.gov zone:

Re-sign all Zone Files:

Current Zone Signing Status

- [nic.gov](#) Unsigned Zone File
- [fed.gov](#) Last Signed: 3/4/2009 1:31:04 PM with KSK: 171
- [fbi.gov](#) Unsigned Zone File

Additional Resources

Domains

Keys

Zone Files

Signatures

Test

Learn

Host

- www.dotgov.gov/Quickstart.html
- www.dotgov.gov/DNSSECFaq.html
- www.dnssecreport.com – tests and tips

Questions?

Domains

Keys

Zone Files

Signatures

Test

Learn

Host

