

# Practicalities

# Bind with DNSSEC?

```
$ ./configure --with-openssl
```

```
$ head config.log
```

This file contains any messages produced by compilers while running configure, to aid debugging if configure makes a mistake.

It was created by configure, which was generated by GNU Autoconf 2.61. Invocation command line was

```
$ ./configure --prefix=/usr/local --with-openssl
```

# DNSSEC aware config

```
options {  
    ...  
    dnssec-enable yes;  
    ....  
};
```

- BIND: dnssec-enable
- NSD: As default

# Generate keys

## Usage:

```
dnssec-keygen -a alg -b bits [-n type] [options] name
```

Version: 9.6-ESV

## Required options:

-a algorithm: RSA | RSAMD5 | DH | DSA | RSASHA1 | RSASHA256 | RSASHA512 | NSEC3DSA | NSEC3RSASHA1 |  
HMAC-MD5 | HMAC-SHA1 | HMAC-SHA224 | HMAC-SHA256 | HMAC-SHA384 | HMAC-SHA512

-b key size, in bits:

RSAMD5: [512..4096]

RSASHA1: [512..4096]

NSEC3RSASHA1: [512..4096]

RSASHA256: [512..4096]

RSASHA512: [1024..4096]

DH: [128..4096]

DSA: [512..1024] and divisible by 64

NSEC3DSA: [512..1024] and divisible by 64

HMAC-MD5: [1..512]

HMAC-SHA1: [1..160]

HMAC-SHA224: [1..224]

HMAC-SHA256: [1..256]

HMAC-SHA384: [1..384]

HMAC-SHA512: [1..512]

-n nametype: ZONE | HOST | ENTITY | USER | OTHER

(DNSKEY generation defaults to ZONE)

name: owner of the key

## Other options:

-c <class> (default: IN)

-d <digest bits> (0 => max, default)

-e use large exponent (RSAMD5/RSASHA1 only)

-f keyflag: KSK

-g <generator> use specified generator (DH only)

-t <type>: AUTHCONF | NOAUTHCONF | NOAUTH | NOCONF (default: AUTHCONF)

-p <protocol>: default: 3 [dnssec]

-s <strength> strength value this key signs DNS records with (default: 0)

-r <randomdev>: a file containing random data

-v <verbose level>

-k : generate a TYPE=KEY key

## Output:

K<name>+<alg>+<id>.key, K<name>+<alg>+<id>.private

# Generate two keys

```
$ dnssec-keygen -a RSASHA1 -b 2048 -n zone -f KSK example.com  
Kexample.com.+005+41863
```

```
$ dnssec-keygen -a RSASHA1 -b 1024 -n zone example.com  
Kexample.com.+005+58803
```

- Generate a Key Signing Key and Zone Signing Key

# \$include the keys

```
$TTL 100
@      100      IN      SOA      ns      (
                                zonemaster      ;
                                2008091600
                                100      ; These values
                                200      ; are to unrealistic for
                                604800   ; production zones
                                100
                                )

                                NS      ns
ns      A      192.0.2.1
demo    A      192.0.2.3

$include Kexample.com.+005+41863.key
$include Kexample.com.+005+58803.key
```

# Sign the lot

```
$ dnssec-signzone -o example.com zonefile.txt
```

Creates a ds-set as a bonus!

# Serve your zone

```
zone "example.com" {  
    type master;  
    file "example.com.signed";  
};
```

- Just point to it in your masterfile



```

; <<>> DiG 9.5.0-P2 <<>> @192.168.1.11 example.com SOA +dnssec
; (1 server found)
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 53425
;; flags: qr aa rd; QUERY: 1, ANSWER: 0, AUTHORITY: 4, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 4096
;; QUESTION SECTION:
;example.com.                IN SOA

;; AUTHORITY SECTION:

example.com.                100      IN SOA      ns.example.com. zonemaster.example.com. (
                                2008091600 ; serial
                                100      ; refresh (1 minute 40 seconds)
                                200      ; retry (3 minutes 20 seconds)
                                604800   ; expire (1 week)
                                100      ; minimum (1 minute 40 seconds)
                                )
example.com.                100      RRSIG       SOA 5 2 100 20081017184752 (
                                20080917184752 58803 example.com.
                                mMS8by7l09SKFv+zQHB/dd0czsmZpsvwrwil
                                gBh12tqK/9kGtuID8f5OvERqwSDhE4e462yF
                                sS8839JlKYndgMJU/cCY1qGIW34tad83P/yl
                                lPWdZ00bDGB8d0BeE4Sj8TbUtSrnbJb1ZvByG
                                0IIB0JKZHRe009SBQAKfXqUnr/E= )

example.com.                100      NSEC        demo.example.com. NS SOA RRSIG NSEC DNSKEY
example.com.                100      RRSIG       NSEC 5 2 100 20081017184752 (
                                20080917184752 58803 example.com.
                                ROta6SMQWFoRrmEAdPaHIbViqNJAwySPZYCG
                                iGodUKVDxGPw/E77rkMdwIKJZk3n/IMHleM+
                                ce/8v2zU3cBXtJ2BjFKiJ3quDWaJRb33DGWH
                                +SaIOJgc4lHMwctGzdogGdznCJ0xpbYmV9g8
                                rCZV59qWJ3sferRYTvrMBEokBh0= )
                                100      DNSKEY      256 3 5 (
                                AwEAAbMW4ddT7IZ+xHcPkbyimnQEVd/h4lPm
                                VI2ghRdMoy3vY+Y4m0jg4YKL6DSRaWppZpF4
                                YGVvrL/jWngKUaUOeEDjDLx3e79K9t4ncL66
                                jKFgB1pOxUKxNSKda9nm4JbjoGZwU+AH4aGc
                                94fKVb12+jwSx6Y9UNN4E13JHIMEQvnt
                                ) ; key id = 58803;; Query time: 1 msec

;; SERVER: 192.168.2.202#53(192.168.2.202)
;; WHEN: Wed Sep 17 22:36:49 2008
;; MSG SIZE rcvd: 452

```

# Publish at Parent

Go Daddy My Account > DOMAINMANAGER Welcome: okolkman Log Out My Account GoDaddy.com

Domains Buy/Sell Tools Help Discount Domain Club: Not Active Register Domains Feedback

Domain Details New .COMs Just 9.99\* Save on the world's most popular domain! SHOP NOW! New! Mobile Domain Management See More...

Great news! The new DNS Manager is live.

All Domains NET-DNS.ORG GO Advanced View Quick View Diagnostic View

Organize Locking Cash in Upgrade Renew Forward Control Nameservers Account Change Delete Selected

### Domain Information

Registered: 4/2/2002  
Locked: Locked [Manage](#)  
Expires On: 4/2/2012 [Renew Now](#)  
Auto Renew: On [Manage](#)  
Extended Auto Renew: Off [Get Extended Auto-Renew!](#)  
Status: Active [Refresh Page](#)  
Authorization Code: [Send by Email](#)  
Forwarding: Off [Manage](#)

### Nameservers

Nameservers: (Last update 4/27/2011)  
NS.HACTRN.NET  
NS1.NET-DNS.ORG  
SEC2.AUTHDNS.RIPE.NET  
MCVAX.NLNETLABS.NL [Set Nameservers](#) [Manage DS Records](#)

### DNS Manager

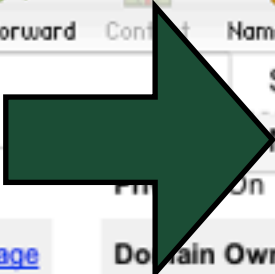
DNS Manager: Not hosted here

### Related Products

Hosting: Not hosted here [Learn More/Add](#)  
WebSite Tonight®: Off [Learn More/Add](#)  
Email Accounts: None [Manage](#)  
InstantPage: Not activated [Manage](#)  
Domain Variations Bundle: Options available [Learn More/Add](#)

### TLD Specific

Not Applicable



Manage DS Records

# Records for NET-DNS.ORG

Key Tag	Algorithm	Digest Type	Digest	MaxSigLife	Flags	Protocol	Public Key	Updates
▶ 43393	7	1	2FE...	NA	NA	NA	NA	<a href="#">Edit</a> <a href="#">Remove</a>
▶ 43393	7	2	F1A...	NA	NA	NA	NA	<a href="#">Edit</a> <a href="#">Remove</a>

[Add new DS record](#)

[Cancel](#)

 **What is DNSSEC?**

 DNSSEC is a security measure that uses digital signatures to authenticate the origin of DNS data and prevent the use of forged DNS data. [Learn more.](#)

[LEARN MORE](#)

Re

## Add DS Records

Step 1 of 2

## Create Records for NET-DNS.ORG

[Switch to basic mode](#) \* Required

Enter up to 10 DS records \*

Example: COOLEXAMPLE.COM 3600 IN DS 12345 2 1 3489c4a6930c385a00e797d1f9a7051eea4ab85d ;comments

- ☐ Replace all existing DS records
- ☒ Append to existing DS records

[Add](#)[Cancel](#)

Next

authenticate the origin of DNS data  
and prevent the use of forged DNS  
data. [Learn more.](#)

Home

Domain Renew

Update Contact

Update Nameserver

DNS Management

Domain Forwarding

Request Client  
Transfer

Domain Transfer In

DNSSEC Control Panel

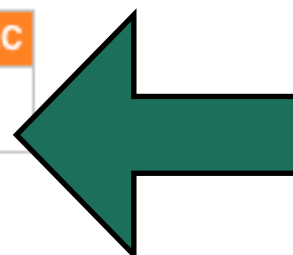
DNSSEC TOOLS

Change Password

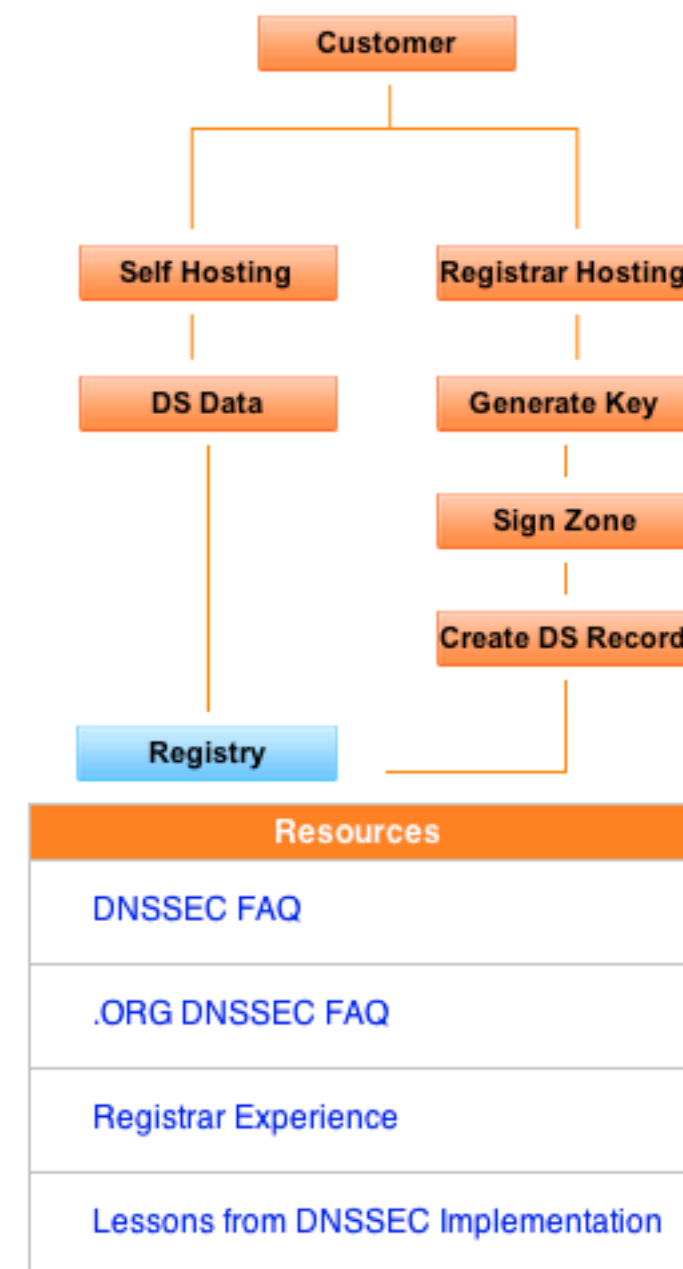
Login to Hosting  
Server

Logout

Domain Name	Nameserver 1	Nameserver 2	DNSSEC
dns-school.org	ns.secret-wg.org	open.nlnetlabs.nl	



## DNSSEC



Home

Domain  
Renew

Update  
Contact

Update  
Nameserver

DNS  
Management

Domain  
Forwarding

Request  
Client  
Transfer

Domain Name : dns-school.org

#### Self Hosting

If the customers hosting provider is supporting DNSSEC and they have ds data, click "Add DS Record" button and no need to go Namesbeyond NS section.

Domain	Created	Key Tag	Algorithm	Digest Type	Digest	
dns-school.org	2011-04-27 11:39:54	13554	7	2	9aec0b1cdafe41243ed5d85f6849bf1fe8e9d25898a196c632ff193c5b4586b3	<a href="#">Remove</a>
dns-school.org	2011-04-27 11:39:32	13554	7	1	840cdbb4e8739c7c19edefb5f09876cf4667314c	<a href="#">Remove</a>

[Add DS Record](#)

If Your hosting provider does not support DNSSEC then you can change your Nameservers to our Nameservers. To Change Nameservers click edit. [Edit](#)

#### DNSSEC





This was the essence

Now

Automate

# Automate using Bind

- Configure your zones to work with dynamic update (IMPORTANT)
- Add “auto-dnssec” to you configuration
  - allow: use the keys when told to sign (in combination with cron maintained rndc resign)
  - maintain: have the name daemon maintain the signatures (recommended)
- Use dnssec-settime to prepare your keys



# Or



But first let us try to understand keys and timing