



# DNSSEC / DANE demo

Paul Wouters

Senior software engineer,

Red Hat

October 17, 2015

# Generating TLSA, SSHFP and OPENPGPKEY records

- yum install hash-slinger
- tlsa --create [www.example.com](https://www.example.com) (for https)
- sshfp -a (known\_hosts)
- sshfp -a -d -d nohats.ca -n ns0.nohats.ca (axfr+scan)
- openpgpkey --create pwouters@fedoraproject.org

```
Terminal - paul@bofh:/vol/home/paul
File Edit View Terminal Go Help

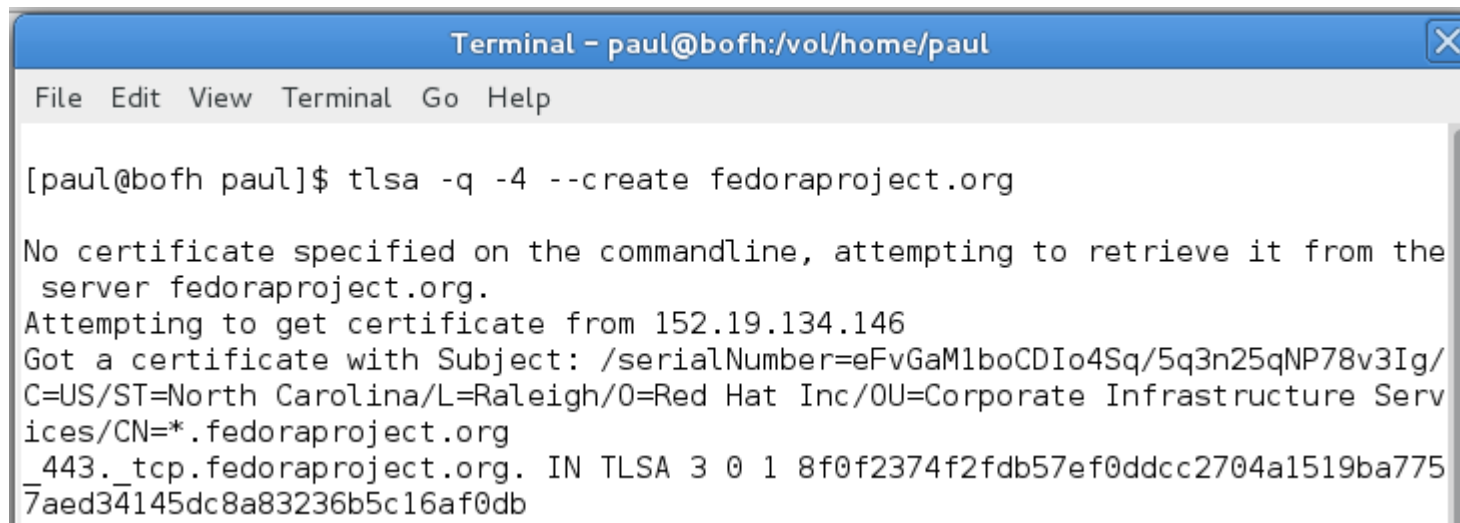
[paul@bofh paul]$ tlsa -q -4 --create fedoraproject.org

No certificate specified on the commandline, attempting to retrieve it from the
server fedoraproject.org.
Attempting to get certificate from 152.19.134.146
Got a certificate with Subject: /serialNumber=eFvGaM1boCDIo4Sq/5q3n25qNP78v3Ig/
C=US/ST=North Carolina/L=Raleigh/O=Red Hat Inc/OU=Corporate Infrastructure Serv
ices/CN=*.fedoraproject.org
_443._tcp.fedoraproject.org. IN TLSA 3 0 1 8f0f2374f2fdb57ef0ddcc2704a1519ba775
7aed34145dc8a83236b5c16af0db
```



# Verifying TLSA, SSHFP and OPENPGPKEY records

- `tlsa --verify www.example.com`
- `openpgpkey --verify pwouters@fedoraproject.org`
- `openpgpkey --fetch pwouters@fedoraproject.org`



```
Terminal - paul@bofh:/vol/home/paul
File Edit View Terminal Go Help

[paul@bofh paul]$ tlsa -q -4 --create fedoraproject.org

No certificate specified on the commandline, attempting to retrieve it from the
server fedoraproject.org.
Attempting to get certificate from 152.19.134.146
Got a certificate with Subject: /serialNumber=eFvGaM1boCDIo4Sq/5q3n25qNP78v3Ig/
C=US/ST=North Carolina/L=Raleigh/O=Red Hat Inc/OU=Corporate Infrastructure Serv
ices/CN=*.fedoraproject.org
_443._tcp.fedoraproject.org. IN TLSA 3 0 1 8f0f2374f2fdb57ef0ddcc2704a1519ba775
7aed34145dc8a83236b5c16af0db
```



# Configure postfix to use TLS

- Generate TLS key, certificate and CA-certificate
- Enable TLS in postfix:
  - `postconf -e "smtpd_tls_security_level = may"`
  - `postconf -e "smtpd_tls_key_file = /etc/postfix/ssl/server.key"`
  - `postconf -e "smtpd_tls_cert_file = /etc/postfix/ssl/server.pem"`
  - `postconf -e "smtpd_tls_CAfile = /etc/postfix/ssl/cacert.pem"`
  - `postconf -e "smtpd_tls_security_level = may"`
  - `postfix reload`



# Configure postfix to use DNSSEC and DANE

- `postconf -e "smtp_dns_support_level = dnssec"`
- `postconf -e "smtp_tls_security_level = dane"`
- Ensure the server postfix runs on is configured to use a DNSSEC capable server specified in `/etc/resolv.conf` (you can point to 8.8.8.8 or 193.110.157.123)



# Postfix now requires TLS when a TLSA record is present

```
Activities Terminal Sat 16:08
root@mx:/etc
File Edit View Search Terminal Help
[root@mx etc]# tail -f /var/log/maillog
Oct 17 22:05:24 mx postfix/smtpd[28105]: connect from whisk.cs.uwaterloo.ca[198.96.155.11]
Oct 17 22:05:24 mx postfix/smtpd[28105]: Anonymous TLS connection established from whisk.cs.uwaterloo.ca[198.96.155.11]
Oct 17 22:05:28 mx postfix/smtpd[28105]: NOQUEUE: reject: RCPT from whisk.cs.uwaterloo.ca[198.96.155.11]: 451 4.7.4 Requested action not found; from=<d1m@upzeqbep.com.tw> to=<cypherpunks@nohats.ca> proto=ESMTP helo=<mail.paip.net>
Oct 17 22:05:28 mx postfix/smtpd[28105]: disconnect from whisk.cs.uwaterloo.ca[198.96.155.11] ehlo=2 st=28105
Oct 17 22:06:39 mx postfix/pickup[27540]: 3ndb336nTzzChB: uid=0 from=<root>
Oct 17 22:06:39 mx postfix/cleanup[28304]: 3ndb336nTzzChB: message-id=<3ndb336nTzzChB@mx.nohats.ca>
Oct 17 22:06:40 mx opendkim[11693]: 3ndb336nTzzChB: no signing table match for 'root@mx.nohats.ca'
Oct 17 22:06:40 mx opendkim[11693]: 3ndb336nTzzChB: no signature data
Oct 17 22:06:40 mx postfix/qmgr[27541]: 3ndb336nTzzChB: from=<root@mx.nohats.ca>, size=448, nrcpt=1 (queue entry)
Oct 17 22:06:41 mx postfix/smtp[28310]: 3ndb336nTzzChB: to=<paul@bofh.nohats.ca>, orig to=<paul@bofh.nohats.ca>, relay=bofh.nohats.ca, status=deferred (TLS is required, but was not offered by host bofh.nohats.ca)
^C
```



# Postfix validates the TLSA record before sending email

```
Activities Terminal Sat
root@mx etc]#
root@mx etc]#
root@mx etc]#
root@mx etc]# mail paul@bofh.nohats.ca
Subject: test
test

EOT
root@mx etc]# tail -f /var/log/maillog
Oct 17 22:22:33 mx postfix/anvil[28708]: statistics: max connection count 1 for (smtp:1
Oct 17 22:22:33 mx postfix/anvil[28708]: statistics: max cache size 1 at Oct 17 22:20:2
Oct 17 22:22:50 mx postfix/pickup[28750]: 3ndbPk5GY3zChB: uid=0 from=<root>
Oct 17 22:22:50 mx postfix/cleanup[28756]: 3ndbPk5GY3zChB: message-id=<3ndbPk5GY3zChB@n
Oct 17 22:22:50 mx opendkim[11693]: 3ndbPk5GY3zChB: no signing table match for 'root@mx
Oct 17 22:22:50 mx opendkim[11693]: 3ndbPk5GY3zChB: no signature data
Oct 17 22:22:50 mx postfix/qmgr[28751]: 3ndbPk5GY3zChB: from=<root@mx.nohats.ca>, size=
Oct 17 22:22:51 mx postfix/smtp[28763]: Verified TLS connection established to bofh.noh
Oct 17 22:22:51 mx postfix/smtp[28763]: 3ndbPk5GY3zChB: to=<paul@bofh.nohats.ca>, relay
atus=sent (250 2.0.0 0k: queued as AAE1E8009C)
Oct 17 22:22:51 mx postfix/qmgr[28751]: 3ndbPk5GY3zChB: removed
^C
root@mx etc]#
```

# Publishing an OPENPGPKEY:

- Generate a new gpg key, for example using gnupg

```
[demo@thinkpad ~]$ ls -a
.  ..  .bash_logout  .bash_profile  .bashrc  .lessht  .mozilla  .xauthKRKwe1
[demo@thinkpad ~]$ gpg --gen-key
gpg (GnuPG) 1.4.19; Copyright (C) 2015 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

gpg: directory `/home/demo/.gnupg' created
gpg: new configuration file `/home/demo/.gnupg/gpg.conf' created
gpg: WARNING: options in `/home/demo/.gnupg/gpg.conf' are not yet active during
gpg: keyring `/home/demo/.gnupg/secring.gpg' created
gpg: keyring `/home/demo/.gnupg/pubring.gpg' created
Please select what kind of key you want:
  (1) RSA and RSA (default)
  (2) DSA and Elgamal
  (3) DSA (sign only)
  (4) RSA (sign only)
Your selection?
RSA keys may be between 1024 and 4096 bits long.
What keysize do you want? (2048)
Requested keysize is 2048 bits
Please specify how long the key should be valid.
    0 = key does not expire
    <n> = key expires in n days
    <n>w = key expires in n weeks
    <n>m = key expires in n months
    <n>y = key expires in n years
Key is valid for? (0) 60
Key expires at Wed 16 Dec 2015 03:25:27 PM EST
Is this correct? (y/N) y
```

```
You need a user ID to identify your key; the software constructs the user ID
from the Real Name, Comment and Email Address in this form:
```

```
"Heinrich Heine (Der Dichter) <heinrichh@duesseldorf.de>"
```





# Publishing an OPENPGPKEY:

- Generate a new gpg key, for example using gnupg

```
Real name: Demo User
Email address: demo@nohats.ca
Comment: Demo User
You selected this USER-ID:
    "Demo User (Demo User) <demo@nohats.ca>"

Change (N)ame, (C)omment, (E)mail or (O)kay/(Q)uit? 0
You need a Passphrase to protect your secret key.

We need to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
.....+++++
....+++++
We need to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
....+++++
.....+++++
gpg: /home/demo/.gnupg/trustdb.gpg: trustdb created
gpg: key B9346B91 marked as ultimately trusted
public and secret key created and signed.

gpg: checking the trustdb
gpg: 3 marginal(s) needed, 1 complete(s) needed, PGP trust model
gpg: depth: 0  valid:   1  signed:   0  trust: 0-, 0q, 0n, 0m, 0f, 1u
gpg: next trustdb check due at 2015-12-16
pub   2048R/B9346B91 2015-10-17 [expires: 2015-12-16]
      Key fingerprint = 7524 CABB 911E 7899 B987 4725 B541 B908 B934 6B91
uid           Demo User (Demo User) <demo@nohats.ca>
sub   2048R/A8BE9C30 2015-10-17 [expires: 2015-12-16]
```



# Publishing an OPENPGPKEY:

- Create an OPENPGPKEY record (in generic format)

```
Activities Terminal Sat 16:26 demo@thinkpad:~
File Edit View Search Terminal Help
generator a better chance to gain enough entropy.
....+++++
.....+++++
gpg: /home/demo/.gnupg/trustdb.gpg: trustdb created
gpg: key B9346B91 marked as ultimately trusted
public and secret key created and signed.

gpg: checking the trustdb
gpg: 3 marginal(s) needed, 1 complete(s) needed, PGP trust model
gpg: depth: 0 valid: 1 signed: 0 trust: 0-, 0q, 0n, 0m, 0f, 1u
gpg: next trustdb check due at 2015-12-16
pub 2048R/B9346B91 2015-10-17 [expires: 2015-12-16]
    Key fingerprint = 7524 CABB 911E 7899 B987 4725 B541 B908 B934 6B91
uid                               Demo User (Demo User) <demo@nohats.ca>
sub 2048R/A8BE9C30 2015-10-17 [expires: 2015-12-16]

[demo@thinkpad ~]$ openpgpkey --create demo@nohats.ca
8b1c1cleae6c650485e77efbc336c5bfb84ffe0b0bea65610b721762._openpgpkey.nohats.ca. IN TYPE61 \# 1201 9901
109c46160929f28261e179940ce13760ee032482ce00c0c1f52d64d32c5747b7d34a069e593670be171d7f372d0d4507496b61
0601a5d8cc0358be7822da785e37f264d0036b9b14f1dc88267bfe799b1b5996037514c24b8bc99b6ecd082427b538eb311005
c11c7116716f4c7bc1745cf7c0202c0dc65d8b2101c757095c00522ff0605f0c5b42067c50576f2bf06ff1c62d2711cfff08c1d
```



# Publishing an OPENPGPKEY:

- Create an OPENPGPKEY record (in rfc format)

```
Activities Terminal Sat 16:27
demo@thinkpad:~
File Edit View Search Terminal Help
[demo@thinkpad ~]$ openpgpkey --create demo@nohats.ca --output rfc
8b1c1c1eae6c650485e77efbc336c5bfb84ffe0b0bea65610b721762._openpgpkey.nohats.ca. IN OPENPGPKEY mQ
M4Tdg7gMkgs4AwMH1LWTTLFdHt9NKBp5ZNNc+Fxl/Ny0NRQdJa2GSX1lYgwPFRYo4NZM1qh43cGAaXyZANYvngi2nheN/Jk0
00sxEXEzM9AHio1vUv+warPtLs0nBHHEWcW90e6F0XPepKT4Nx12LMQHVV5heyVIv8GBfzltCBnpYV2878G/x5i03Ec//jN
IzdpBVkhTRPzASZRI8ceHi9XVgSwLh4rMjB/S1gGK8qL7ABEBAAG0JkR1bW8gVXN1ciAoRGVtbyBVc2VyKSA8ZGVtb0Bub2h
oABgsJCAcDAgYVCAIJCgsEFgIDAQIeAQIXgAAKCRC1QbkIuTRrkXoIB/9t0B9He9kBPMQmBNu2z0cgZv0ZKM1XkMQp4HTesB
iryj320AVgmBUQ6M72AwoeotjBU2xD71LwzJ1PszhVdfHTIZMf25Bg5ZNDDqUGWCsmQXiJ0/Ps00jy5hGDEfiy+tX1lv+M4X
r/owxbrMUknESZtP14c9X+xoWYP016un9K8H0JVU1LRbvczaA0yRLNe+SMQCcCpe6ZY7/UAnEmC6YQ1XpwK0EZ+Sw2iyRkz4
irugBCADbMY4vI+f7WjDZQKG/CjXv0aguTuaJ6Gq/VHFnaKsuDTDgBDG5H6GF5m0+AqIJdwcGJpbnti3LX2FwWDVfpiN8va/
1NWyXtgHqSIp0n6BeBrKS2JyvNcIIjSg5p8awXj+zumjloZYujhM5dYcpube0LkyDyRPBJ3Yfxl7oKNzePqS0tQ49CPu3UH+
sxvuMzX8/+sYziQ8aRmQUTExrK4Uso6azrkpwez4DZNBsb2s5K2dN/dtHr78fMzzJrAeahKDVhaJrobABEBAAGJASUEGAECA
Hwf+0AH/V0y0sszIhD0cymopRj+zKwhHCNLqMvknR6UxcAdmaq0U1/eKRmt20ReyMQ7DiklLCg6lEbgQ5iULi4quqYt7mm
c++kG7wvsBUzgzAhRgCe5QsASezzvs3cQ4v5EnaGEXuBF1mIDMU3URfgNo1DIhgwyLGkZZNwI9/5SUE0490JRn/3KZM1v6j
P1Q2YCKp0q0LXv2ioteEf0vyXILHPZodsC/mxoPp0sUCZuQbJY0dTb11ArRf8X9ucu5EPHC2qflg==
[demo@thinkpad ~]$
```



## Publish your OPENPGPKEY and verify it:

- Add record to zone, re-sign and propagate zone, then:

```
[demo@thinkpad ~]$ openpgpkey --fetch demo@nohats.ca
-----BEGIN PGP PUBLIC KEY BLOCK-----
Comment: demo@nohats.ca key obtained from DNS
Comment: key transfer was protected by DNSSEC
Version: GnuPG v1

mQENBFYi rugBCADqh1lNam3SgQnEYWCSnygmHheZQM4Tdg7gMkgs4AwMH1LWTTLF
dHt9NKBp5ZNNc+Fx1/Ny0NRQdJa2GSX1lYgwPFRYo4NZM1qh43cGAaXYzANYvngi
azrkpwez4DZNBSb2s5K2dN/dtHr78fMzzJrAeahKDVhaJrobABEBAAGJASUEGAEC
AA8FA1Yi rugCGwwFCQBPGgAACgkQtUG5CLk0a5HBHwf+0AH/V0y0sszIhD0cymop
Rj+zKwhHCNLqMvkpNr6UxcAdmaq0U1/eKRmt20ReyMQ7Dik1LCg61EbgQ5iULi4q
kuqYt7mmTwPM10qSY6zk+ZM4DEyx+0KcTy0BvsHDX02kcknc++kG7wvsBUzgzAhR
gCe5QsASezzvs3cQ4v5EnaGEXuBF1mIDMU3URfgNo1DIhgwyLGkZZnXwI9/5SUE0
490JRn/3KZM1v6jLfbvNE1XRNrphjB8/rtxUZoCMsKow32pFRRdcF0P1Q2YCKp0q
0LXv2ioteEf0vyXILHPZodsC/mxoPp0sUCZuQbJY0dTb11ArRf8X9ucu5EPHC2qf
lg==
=LGuo
-----END PGP PUBLIC KEY BLOCK-----
```



# openpgpkey tool warns about email mismatch

```
[demo@thinkpad ~]$ openpgpkey --fetch paul@bofh.nohats.ca
openpgpkey: Received OpenPGP data does not contain a key with keyid paul@bofh.nohats.ca
(add --uid <uid> to override with any of the below received uids)
# Paul Wouters (migration only, use new key) <paul@nohats.ca>
# Paul Wouters <paul@xtdnet.nl>
# Paul Wouters <paul@freeswan.nl>
# Paul Wouters <paul@freeswan.org>
# Paul Wouters <paul@xelerance.com>
# Paul Wouters <paul@cypherpunks.ca>
# Paul Wouters (migration only, use new key) <pwouters@redhat.com>
[demo@thinkpad ~]$ openpgpkey --fetch paul@bofh.nohats.ca --uid paul@nohats.ca | head -15
-----BEGIN PGP PUBLIC KEY BLOCK-----
Comment: paul@bofh.nohats.ca key obtained from DNS
Comment: key transfer was protected by DNSSEC
Version: GnuPG v1

mQENAz97DD0AAAEH/2hrtp4YrNMc0AAF8YbM8rywL8uH/dTFzV2pLMt+CVh7V5EG
N7icm8n+aXUJeY+pvftjiXj0kvEJmc0llfbvG+4Bus4cn2NtM7Yy0kZLSE050bkn
0E+WX9/ffbnXQcnk/E6DBnosIaxPCxnmL2SV6UtGNkbeC3tDcUWfrMtQaqkUhhqN
gfd1p47HIRbPGnr4EX+Ck52HPe7/neo9WZ6XR4pWNQ50cLJXJfBpwZVpedx9f0ys
ARbH6uk4BQbxDGVUBj5S2n2oopnz4L+GvDW7ltcfZLjmaCoZUoH9eWMW35fJ4phr
a4k3CINDF8pquC+66kLEabffvEHW5xgGprXMJ+EABRG0HVBhdWwgV291dGVycyA8
cGF1bEB4dGRuZXQubmw+iQEVAwUTP3tGiucYBqa1zCfhAQHBowf/Qd57/Ag1Sf4S
J1w9wyzm4KxeQs8ds318FDvrdXixLhBGdUz6ErFIMMkT5wYag2lrBjP4f06fg4H6
90Pj+TSjN6DULnvtJRGYYASC53m9DTYbnNIKVBr/VmyrCtGzEyhZm11L1lxLx0PB
U1Q4+K9z1/SIFqcfm8e6lZQ2y7zADD+K7w7bG0xE8tfr0BXZSRpDpi/R8ATmjFDZ
[demo@thinkpad ~]$
```



# Demo of openpgpkey-milter using OPENPGPKEY

```
[root@mx ~]# jobs
[1]+  Running                  tail -f /var/log/messages &
[root@mx ~]# mail paul@bofh.nohats.ca
Subject: test icann
testing icann demo
.
EOT
[root@mx ~]# Oct 17 22:52:14 mx openpgpkey-milter: connect from localhost at ('127.0.0.1', 0)
Oct 17 22:52:14 mx openpgpkey-milter: Received DNSSEC secured OPENPGPKEY for paul@bofh.nohats.ca:
Key-ID:E71806A6B5CC27E1 Fingerprint:FC0C977F4724D0EA06E31C2AE3BA29CE
Oct 17 22:52:14 mx openpgpkey-milter: Will encrypt message to fingerprints:FC0C977F4724D0EA06E31C2AE3BA29CE
```



# View of email send via postfix + openpgpkey-milter

```
paul@bofh:/home/paul
File Edit View Search Terminal Help
ALPINE 2.20 MESSAGE TEXT Folder: INBOX

Date: Sat, 17 Oct 2015 16:52:14
From: root <root@mx.nohats.ca>
To: paul@bofh.nohats.ca
Subject: [openpgpkey-milter encrypted message]

-----BEGIN PGP MESSAGE-----
Version: GnuPG v2.0.14 (GNU/Linux)

hQEMA+cYBqa1zCfhAQf/WBtaZjQsc7EKIEtwhy7ox5tr10izCIsXCGvmbiV1Q+M1
mZIKVF81DAGVSUo5PMuU1GrTAtwaItY5C50CYgEFcFgFCy8LRt0LPoT50WkDb0df
QbCbYbuB3RFenZHGAVxRRoUSHI99EzDq72HzfaUVJkFofoc1cBCYM6er7ImwYAg6
Ua7YXouR7qRlMCshfDF48MWhJeapnMfl71p7C+wGPo3xefzrBvT5G47rVwXDvnN5
0S/1tFTHwEe6r1UI9xTieYENlNZV8V1UvckBA7Fq6lCg73GAwcBGwpnED8L9V1+R
cPBGqNcZs7mLo1w0ppp3ZT3gWl2TuNa0bZqoy+cPa8nAXfBiRoa/JcQRB rQR+mCy
hq+rzyUu+FUQVnEoCcVl9AR3UDcW0T+rxfxMuPGfITEXvXs8+mJb50wqRLnpsNuq
Rwpx3FGyG3ItqRBC+211DqwnzjKsgSp7QYHB2wDx7Ryb+t60756MxGhiP3gfnKIj
PTuxCDtF9B0TNaXXD0WkzquY0rQ7lk7Btiv+svFdmUpgAT6ovJlXkftZ5ZIVhwqY
gCmqdzp0Y+lpJeBuJk9M4gGIbWo6m/itLA8fw2X8WZlWrcYGKsK0SlYPxNaulQtz
0dKqmWdgqHSewEN2I0WS/iyXRk7qqLffnn8rxZX44EUKeCZXbsegAWo/TYy7c1qW
79X1qHqhlsL2mImN0wib6TyYogw5q6q99lwR1kQviA==
=fFWC
-----END PGP MESSAGE-----

[ALL of message]
? Help < MsgIndex P PrevMsg - PrevP
0 OTHER CMDS > ViewAttch N NextMsg Spc NextP
```



# SSHFP record: enable DNSSEC in ssh client

- Can be done in user's own `~/.ssh/ssh_config`
- Can be done globally in `/etc/ssh/ssh_config`
- To only display extra informational text for ssh, use:

`VerifyHostKeyDNS ask`

- To automatically accept the key when found in DNS

`VerifyHostKeyDNS yes`





# Connecting with ssh using VerifyHostKeyDNS ask

```
[root@ns0 ~]# dig +dnssec sshfp bofh.nohats.ca

; <<>> DiG 9.8.2rc1-RedHat-9.8.2-0.37.rc1.el6_7.4 <<>> +dnssec sshfp bofh.nohats.ca
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 64517
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 3, ADDITIONAL: 3

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;bofh.nohats.ca.                IN      SSHFP

;; ANSWER SECTION:
bofh.nohats.ca.                3600    IN      SSHFP   1 1 C5B3A4D944A2973F3FEBFFB6592E34E295C44F79
bofh.nohats.ca.                3600    IN      SSHFP   2 1 41E9A94810955E22CB437704D8F7F7DED08ECFAF

;; AUTHORITY SECTION:
nohats.ca.                      86393   IN      NS      ns0.nohats.ca.
nohats.ca.                      86393   IN      NS      ns1.nohats.ca.
nohats.ca.                      86393   IN      NS      ns2.foobar.fi.

[root@ns0 ~]# ssh root@bofh.nohats.ca
The authenticity of host 'bofh.nohats.ca (76.10.157.69)' can't be established.
RSA key fingerprint is 2b:11:2d:7f:56:bc:ae:8c:e9:dd:5d:10:7e:bd:3e:28.
Matching host key fingerprint found in DNS.
Are you sure you want to continue connecting (yes/no)? 
```



# Connecting with ssh using VerifyHostKeyDNS yes

```
[root@ns0 ~]# tail -10 /etc/ssh/ssh_config
# mode correctly we set this to yes.
    ForwardX11Trusted yes
# Send locale-related environment variables
    SendEnv LANG LC_CTYPE LC_NUMERIC LC_TIME LC_COLLATE LC_MONETARY LC_MESSAGES
    SendEnv LC_PAPER LC_NAME LC_ADDRESS LC_TELEPHONE LC_MEASUREMENT
    SendEnv LC_IDENTIFICATION LC_ALL LANGUAGE
    SendEnv XMODIFIERS

#VerifyHostKeyDNS ask
VerifyHostKeyDNS yes
[root@ns0 ~]# grep bofh .ssh/authorized_keys
[root@ns0 ~]# ssh root@bofh.nohats.ca
root@bofh.nohats.ca's password: 
```



# ssh client detecting Man-in-the-middle attack

```
[root@ns0 ~]# dig sshfp rogue.nohats.ca.

; <<>> DiG 9.8.2rc1-RedHat-9.8.2-0.37.rc1.el6_7.4 <<>> sshfp rogue.nohats.ca.
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 61386
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;rogue.nohats.ca.            IN      SSHFP

;; ANSWER SECTION:
rogue.nohats.ca.           3575    IN      SSHFP   1 1 0000000000000000000000000000000000000000000000000000000000000000
rogue.nohats.ca.           3575    IN      SSHFP   2 1 0000000000000000000000000000000000000000000000000000000000000000

;; Query time: 0 msec
;; SERVER: 193.110.157.123#53(193.110.157.123)
;; WHEN: Sat Oct 17 15:59:57 2015
;; MSG SIZE  rcvd: 101

[root@ns0 ~]# ssh rogue.nohats.ca.
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@   WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!   @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle attack)!
It is also possible that the RSA host key has just been changed.
The fingerprint for the RSA key sent by the remote host is
82:24:c1:40:b4:2f:fa:c3:8e:18:71:cc:ba:25:8b:87.
Please contact your system administrator.
Update the SSHFP RR in DNS with the new host key to get rid of this message.
The authenticity of host 'rogue.nohats.ca. (193.110.157.104)' can't be established.
RSA key fingerprint is 82:24:c1:40:b4:2f:fa:c3:8e:18:71:cc:ba:25:8b:87.
No matching host key fingerprint found in DNS.
Are you sure you want to continue connecting (yes/no)? 
```

