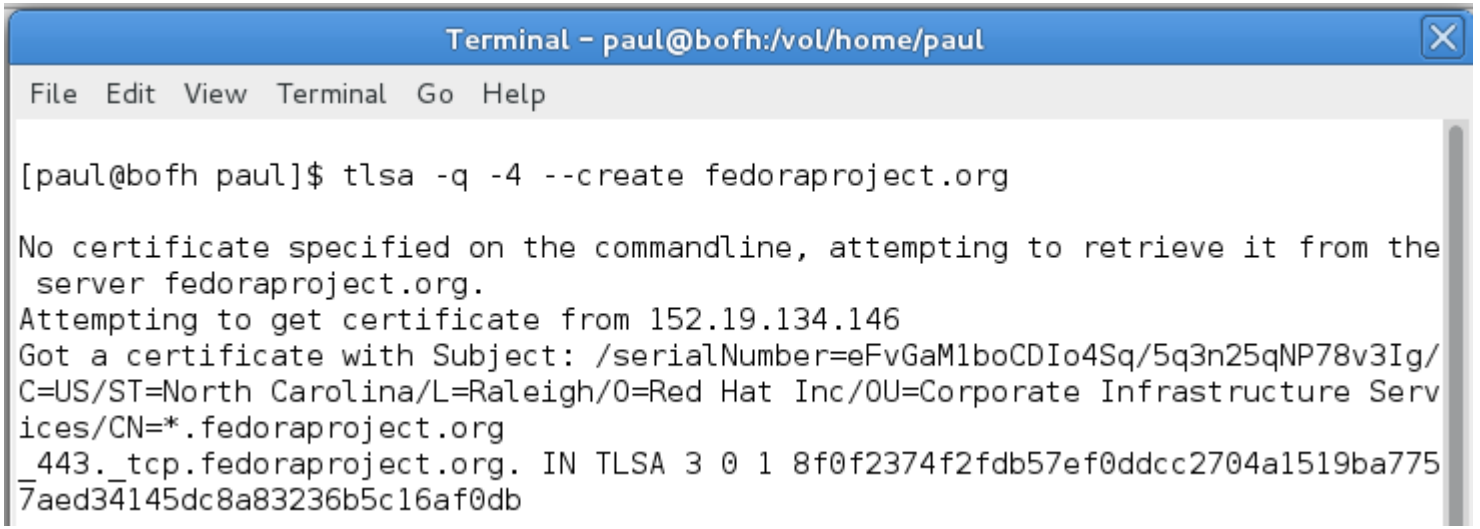
DNSSEC / DANE demo

Paul Wouters
Senior software engineer,
Red Hat
October 17, 2015

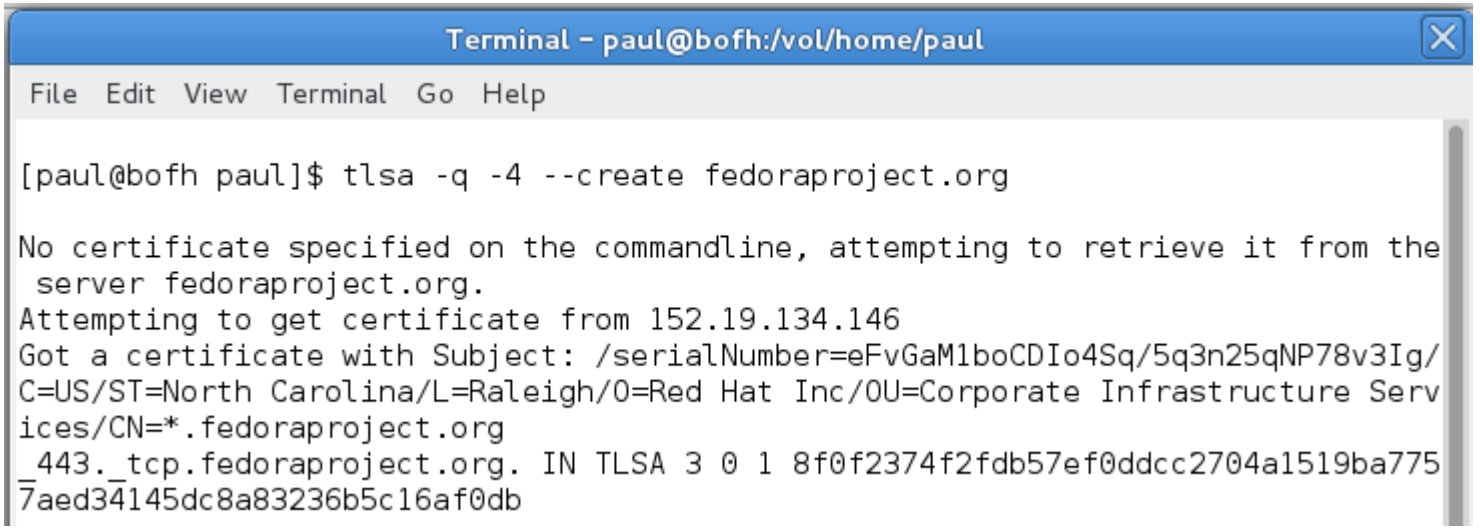
Generating TLSA, SSHFP and OPENPGPKEY records

- yum install hash-slinger
- tlsa --create www.example.com (for https)
- sshfp -a (known_hosts)
- sshfp -a -d -d nohats.ca -n ns0.nohats.ca (axfr+scan)
- openpgpkey --create pwouters@fedoraproject.org



Verifying TLSA, SSHFP and OPENPGPKEY records

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



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

Paul Wouters <pwouters@redhat.com>

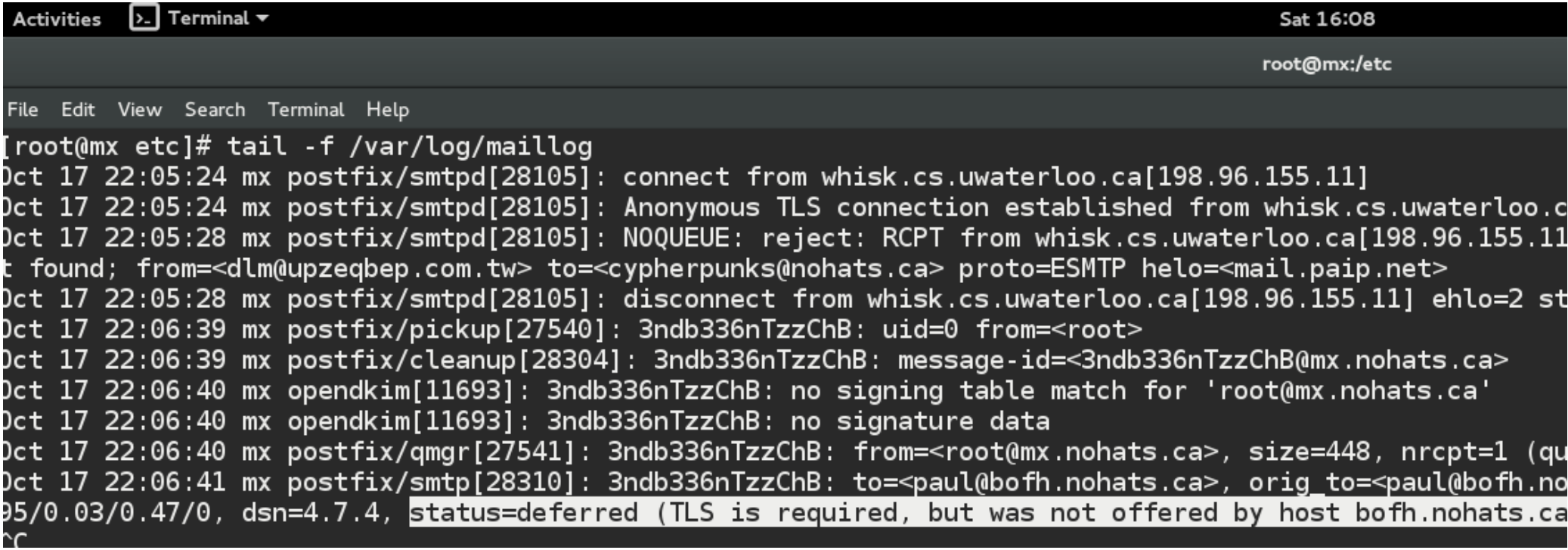

Configure postfix to use DNSSEC and DANE

- postconf -e "smtp_dns_support_level = dnssec"
- postconf -e "smtp_tls_security_level = dane"

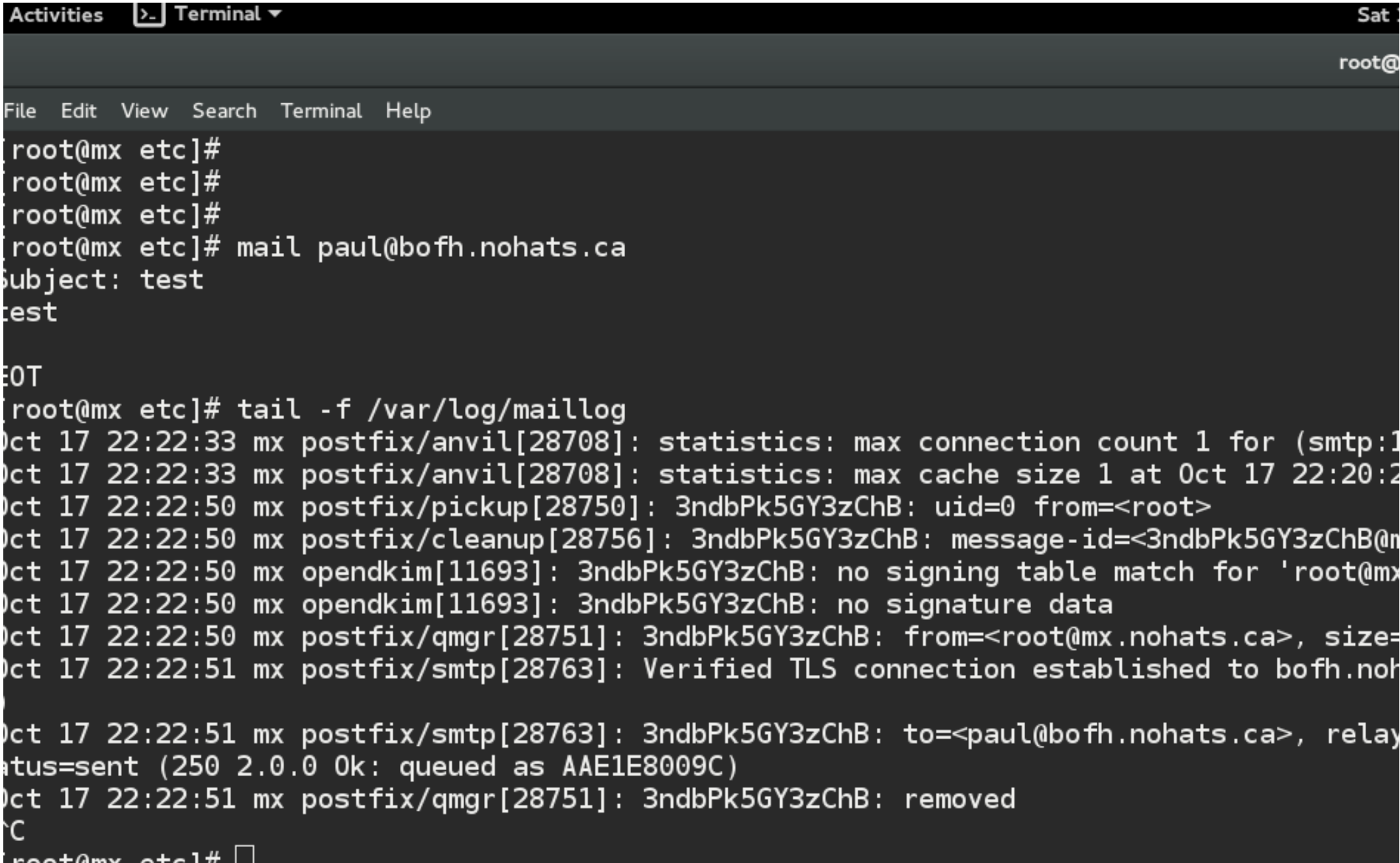
- Ensure the server postfix runs on is configured to use a DNSSEC capable server specified in /etc/resolv.conf
  (you can point to 8.8.8.8 or 193.110.157.123)

Paul Wouters <pwouters@redhat.com>


Postfix now requires TLS when a TLSA record is present



Postfix validates the TLSA record before sending email



Publishing an OPENPGPKEY:

- Generate a new gpg key, for example using gnupg

```
[demo@thinkpad ~]$ ls -a
.  ..  .bash_logout  .bash_profile  .bashrc  .lesshst  .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>"
```

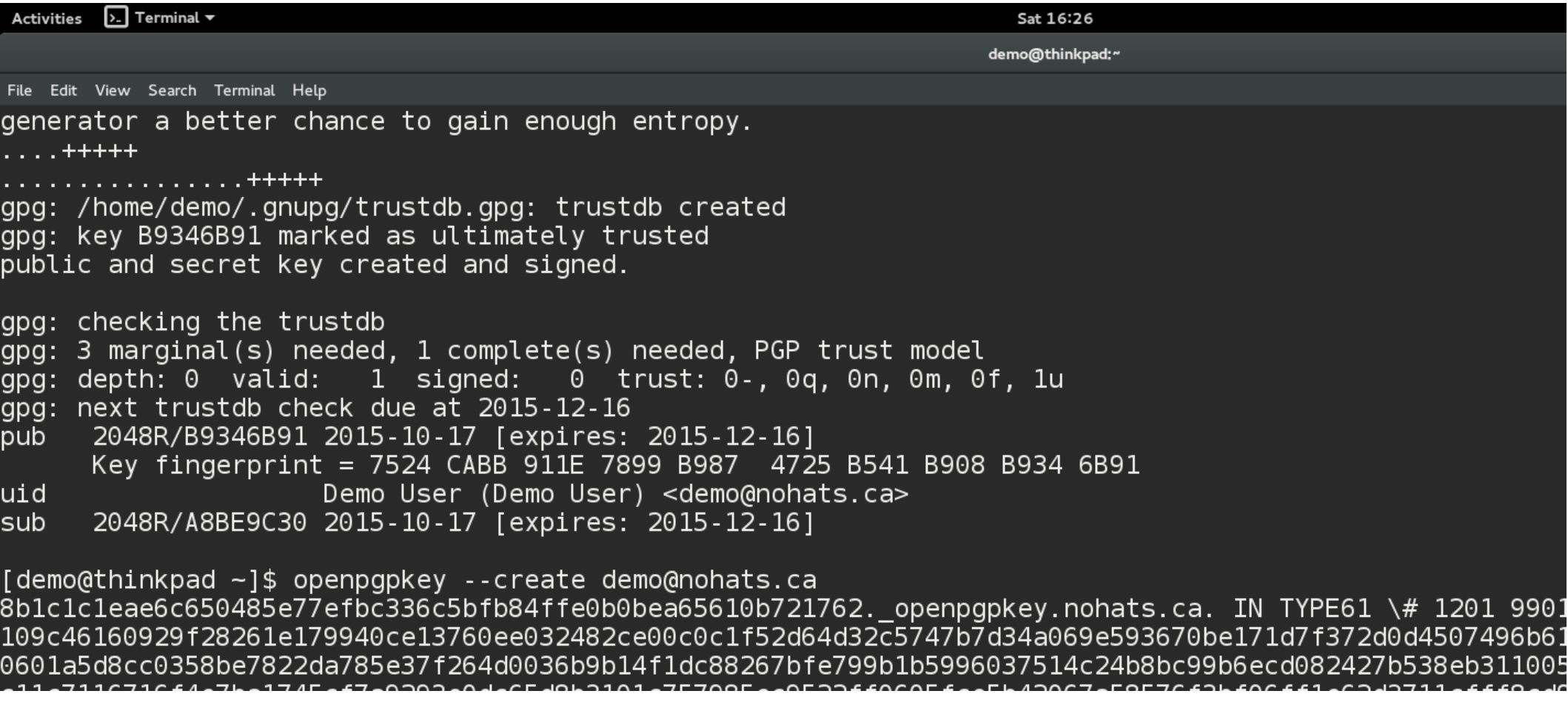

Publishing an OPENPGPKEY:

- 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? O
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]
```

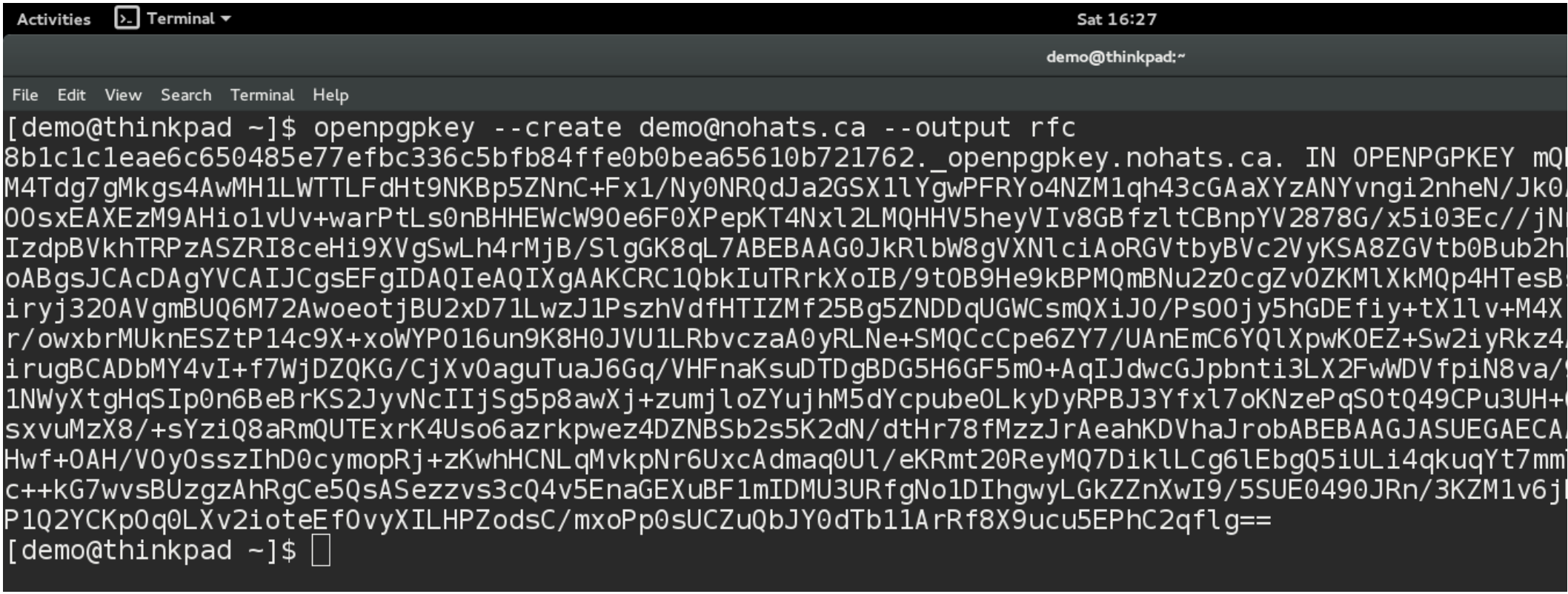

Publishing an OPENPGPKEY:

- Create an OPENPGPKEY record (in generic format)



Publishing an OPENPGPKEY:

- Create an OPENPGPKEY record (in rfc format)



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

mQENBFYirugBCADqh1lNam3SgQnEYWCSnygmHheZQM4Tdg7gMkgs4AwMH1LWTTLF
dHt9NKBp5ZNnC+Fx1/Ny0NRQdJa2GSX1lYgwPFRYo4NZM1qh43cGAaXYzANYvngi
azrkpwez4DZNBSb2s5K2dN/dtHr78fMzzJrAeahKDVhaJrobABEBAAGJASUEGAEC
AA8FAlYirugCGwwFCQBPGgAACgkQtUG5CLk0a5HBHwf+OAH/V0y0sszIhD0cymop
Rj+zKwhHCNLqMvkpNr6UxcAdmaq0Ul/eKRmt20ReyMQ7DiklLCg6lEbgQ5iULi4q
kuqYt7mmTwPMlOqSY6zk+ZM4DEyx+OKcTyOBvsHDX02kcknc++kG7wvsBUzgzAhR
gCe5QsASezzvs3cQ4v5EnaGEXuBF1mIDMU3URfgNo1DIhgwyLGkZZnXwI9/5SUE0
490JRn/3KZM1v6jLfBvNElXRNrphjB8/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/2hrtp4YrNMcOAAF8YbM8ryWl8uH/dTFzV2plMt+CVh7V5EG
N7icm8n+aXUJeY+pvftjiXj0kvEJmcOllfbvG+4Bus4cn2NtM7Yy0kZLSE050bkn
OE+WX9/ffbnXQcnk/E6DBnosIaxPCxnmL2SV6UtGNkbeC3tDcUWfrMtQaqkUhhqN
gfD1p47HIrbPGnr4EX+Ck52HPe7/neo9WZ6XR4pWNQ50clJXJfBpwZVpedx9f0ys
ARbH6uk4BQbxDGVUBj5S2n2oopnz4L+GvDW7ltcfZLjmaCoZUoH9eWMW35fJ4phr
a4k3CINDF8pquC+66kLEabffvEHW5xgGprXMJ+EABRG0HVBhdWwgV291dGVycyA8
cGF1bEB4dGRuZXQubmw+iQEVAwUTP3tGiucYBqa1zCfhAQHBowf/Qd57/Ag1Sf4S
J1W9wyzm4KxeQs8ds318FDvrdXixLhBGdUz6ErFIMMkT5wYag2lrBjP4fO6fg4H6
90Pj+TSjN6DULnVtJRGYYASC53m9DTYbnNIKVBr/VmyrCtGzEyhZm11LllxLx0PB
UlQ4+K9z1/SIFqcfm8e6lZQ2y7zADD+K7w7bG0xE8tfrOBXZSRpDpi/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/WBtaZjQsc7EKIEtwhy7ox5tr1OizCIsXCGvmbiV1Q+M1
mZIKVF8lDAGVSUo5PMuU1GrTAtwaItY5C5OCYgEFcFgFCy8LRtOLPoT5OWkDb0df
QbCbYbuB3RFenZHGAVxRRoUSHI99EZDq72HzfaUVJkFofoC1cBCYM6er7ImwYAg6
Ua7YXouR7qRlMCshfDF48MWhJeapnMfl71p7C+wGPo3xefzrBvT5G47rVwXDvnN5
0S/1tFTHwEe6r1UI9xTieYENlNZV8V1UvckBA7Fq6lCg73GAwcBGwpnED8L9V1+R
cPBGqNcZs7mLo1w0ppp3ZT3gWl2TuNaObZqoy+cPa8nAXfBiRoa/JcQRBrQR+mCy
hq+rzyUu+FUQVnEoCcVl9AR3UDcWOT+rxfXMuPGfITEXvXs8+mJb5OwqRLnpsNuq
Rwpx3FGyG3ItqRBC+211DqwnzjKsgSp7QYHB2wDx7Ryb+t60756MxGhiP3gfnKIj
PTuxCDtF9BOTNaXXD0WkzquYOrQ7lk7Btiv+svFdmUpgAT6ovJlxkftZ5ZIVhwqY
gCmqdzp0Y+lpJeBuJk9M4gGIbWo6m/itLA8fw2X8WZlWrcYGKsKOSlyPxNaulQtz
OdKqmWdgqHSewEN2I0WS/iyXRk7qqLffnn8rxZX44EUKeCZXbsegAWo/TYy7c1qW
79X1qHqhlsL2mImNOwib6TyYogw5q6q99lwR1kQviA==
=fFWC
-----END PGP MESSAGE-----




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


Paul Wouters <pwouters@redhat.com>

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

Paul Wouters <pwouters@redhat.com>

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)?
```


Paul Wouters <pwouters@redhat.com>

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 0000000000000000000000000000000000000000
rogue.nohats.ca.        3575    IN      SSHFP   2 1 0000000000000000000000000000000000000000

;; 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)?
```


Paul Wouters <pwouters@redhat.com>