New DNSSEC Technologies

Paul Wouters
Senior software engineer,
Red Hat

February 9, 2015

*.fedoraproject.org PGP keys now in DNSSEC

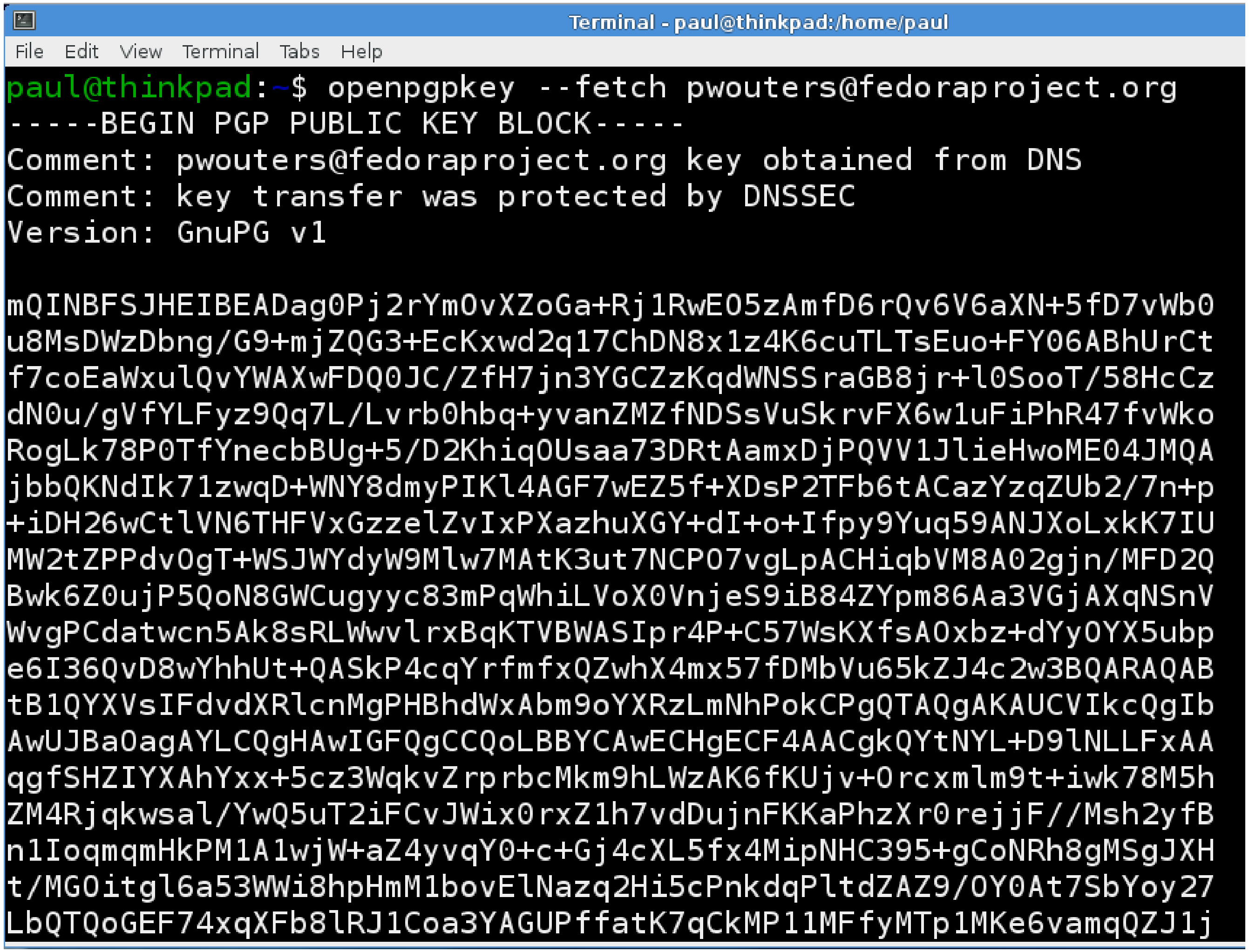
- All Fedora Account System users have a user@fedoraproject.org email
  - FAS web interface allows uploading PGP keyid (soon public keys itself)
- Publish PGP keys using DNSSEC
  - draft-ietf-openpgpkey
- Retrieve from DNSSEC using dig

```
dig +short +vc type61 `printf paul|sha224sum|cut -f1
-d\ `._openpgpkey.nohats.ca|sed 's/ [^ ]*//;s/\W//g'|xxd
-r -p|gpg --import -n
```

Managing PGP keys in DNS for humans

- openpgpkey command from the hash-slinger package
- create, verify and download keys
- missing features:
  - punycode support missing :)
  - DNSSEC root key location confusion
  - wrap long lines using (braces) syntax

openpgpkey –fetch to download a PGP key

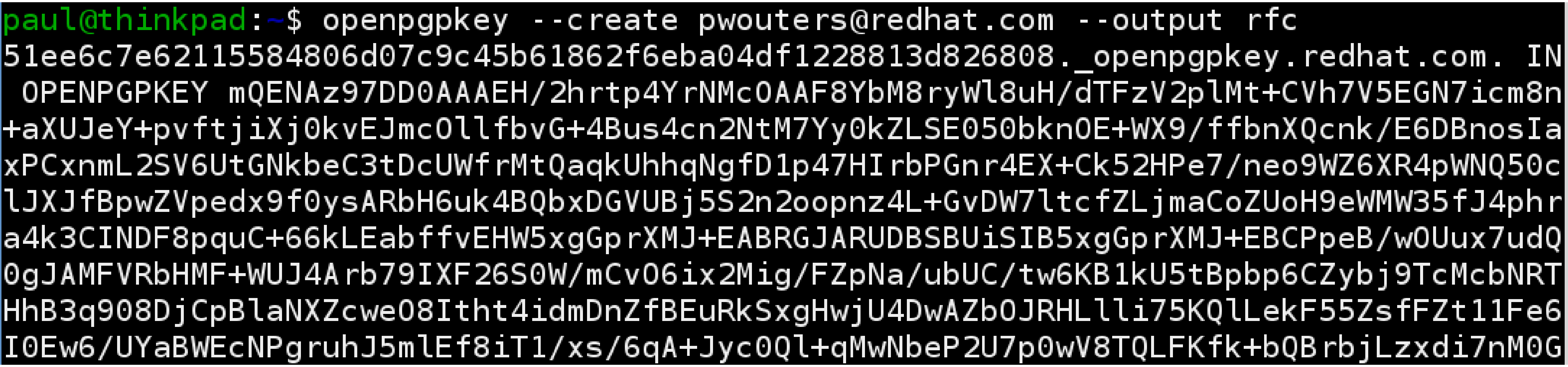


Terminal - paul@thinkpad:/home/paul
File Edit View Terminal Tabs Help

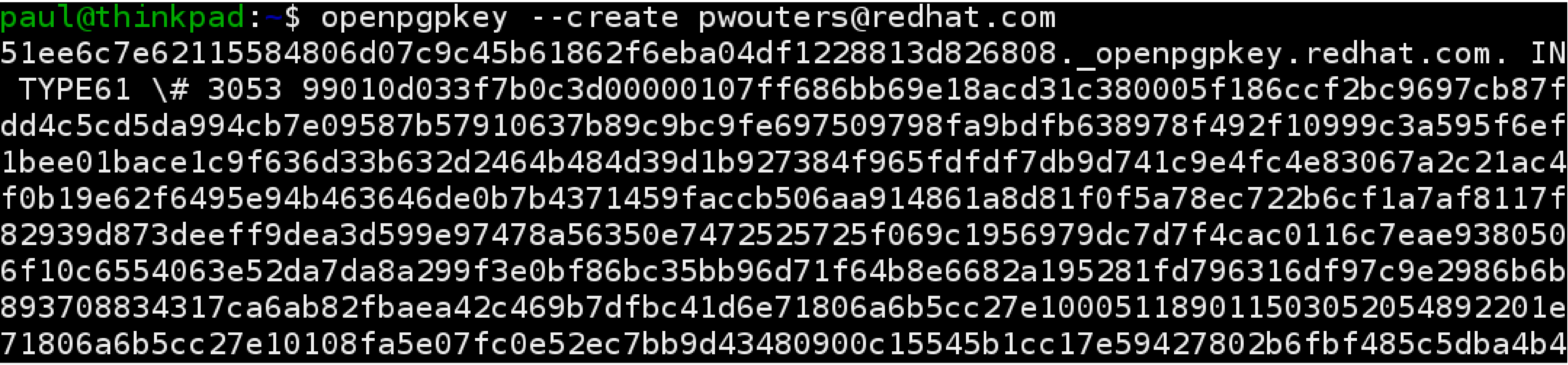
```
paul@thinkpad:~$ openpgpkey --fetch pwouters@fedoraproject.org
-----BEGIN PGP PUBLIC KEY BLOCK-----
Comment: pwouters@fedoraproject.org key obtained from DNS
Comment: key transfer was protected by DNSSEC
Version: GnuPG v1

mQINBFSJHEIBEADag0Pj2rYm0vXZoGa+Rj1RwE05zAmfD6rQv6V6aXN+5fD7vWb0
u8MsDWzDbng/G9+mjZQG3+EcKxwd2q17ChDN8x1z4K6cuTLTsEuo+FY06ABhUrCt
f7coEaWxulQvYWAXwFDQ0JC/ZfH7jn3YGCZzKqdWNSSraGB8jr+l0SooT/58HcCz
dN0u/gVfYLFyz9Qq7L/Lvrb0hbq+yvanZMZfNDSsVuSkrvFX6w1uFiPhR47fvWko
RogLk78P0TfYnecbBUg+5/D2KhiqOUsaa73DRtAamxDjPQVV1JlieHwoME04JMQA
jbbQKNdIk71zwqD+WNY8dmyPIKl4AGF7wEZ5f+XDsP2TFb6tACazYzqZUb2/7n+p
+iDH26wCtlVN6THFVxGzzelZvIxPXazhuXGY+dI+o+Ifpy9Yuq59ANJXoLxkK7IU
MW2tZPPdvOgT+WSJWYdyW9Mlw7MAtK3ut7NCPO7vgLpACHiqbVM8A02gjn/MFD2Q
Bwk6Z0ujP5QoN8GWCugyyc83mPqWhiLVoX0VnjeS9iB84ZYpm86Aa3VGjAXqNSnV
WvgPCdatwcn5Ak8sRLWwvlrxBqKTVBWASIpr4P+C57WsKXfsA0xbz+dYyOYX5ubp
e6I36QvD8wYhhUt+QASkP4cqYrfmfxQZwhX4mx57fDMbVu65kZJ4c2w3BQARAQAB
tB1QYXVsIFdvdXRlcnMgPHBhdWxAbm9oYXRzLmNhPokCPgQTAQgAKAUCVIkcQgIb
AwUJBa0agAYLCQgHAwIGFQgCCQoLBBYCAwECHgECF4AACgkQYtNYL+D9lNLLFxAA
qgfSHZIYXAhYxx+5cz3WqkvZrprbcMkm9hLWzAK6fKUjv+Orcxmlm9t+iwk78M5h
ZM4Rjqkwsal/YwQ5uT2iFCvJWix0rxZ1h7vdDujnFKKaPhzXr0rejjF//Msh2yfB
n1IoqmqmHkPM1A1wjW+aZ4yvqY0+c+Gj4cXL5fx4MipNHC395+gCoNRh8gMSgJXH
t/MGOitgl6a53WWi8hpHmM1bovElNazq2Hi5cPnkdqPltdZAZ9/OY0At7SbYoy27
LbQTQoGEF74xqXFb8lRJ1Coa3YAGUPffatK7qCkMP11MFfyMTp1MKe6vamqQZJ1j
```

openpgpkey –create to create DNS record

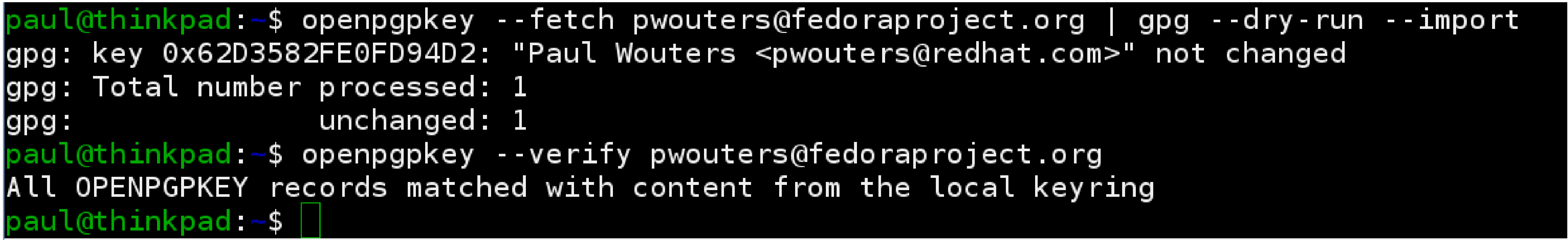


```
paul@thinkpad:~$ openpgpkey --create pwouters@redhat.com --output rfc
51ee6c7e62115584806d07c9c45b61862f6eba04df1228813d826808._openpgpkey.redhat.com. IN
 OPENPGPKEY mQENAz97DD0AAAEH/2hrtp4YrNMcOAAF8YbM8ryWl8uH/dTFzV2plMt+CVh7V5EGN7icm8n
+aXUJeY+pvftjiXj0kvEJmcOllfbvG+4Bus4cn2NtM7Yy0kZLSE050bknOE+WX9/ffbnXQcnk/E6DBnosIa
xPCxnmL2SV6UtGNkbeC3tDcUWfrMtQaqkUhhqNgfD1p47HIrbPGnr4EX+Ck52HPe7/neo9WZ6XR4pWNQ50c
lJXJfBpwZVpedx9f0ysARbH6uk4BQbxDGVUBj5S2n2oopnz4L+GvDW7ltcfZLjmaCoZUoH9eWMW35fJ4phr
a4k3CINDF8pquC+66kLEabffvEHW5xgGprXMJ+EABRGJARUDBSBUiSIB5xgGprXMJ+EBCPpeB/wOUux7udQ
0gJAMFVRbHMF+WUJ4Arb79IXF26S0W/mCvO6ix2Mig/FZpNa/ubUC/tw6KB1kU5tBpbp6CZybj9TcMcbNRT
HhB3q908DjCpBlaNXZcwe08Itht4idmDnZfBEuRkSxgHwjU4DwAZbOJRHLlli75KQlLekF55ZsfFZt11Fe6
I0Ew6/UYaBWEcNPgruhJ5mlEf8iT1/xs/6qA+Jyc0Ql+qMwNbeP2U7p0wV8TQLFKfk+bQBrbjLzxdi7nM0G
```



```
paul@thinkpad:~$ openpgpkey --create pwouters@redhat.com
51ee6c7e62115584806d07c9c45b61862f6eba04df1228813d826808._openpgpkey.redhat.com. IN
 TYPE61 \# 3053 99010d033f7b0c3d00000107ff686bb69e18acd31c380005f186ccf2bc9697cb87f
dd4c5cd5da994cb7e09587b57910637b89c9bc9fe697509798fa9bdfb638978f492f10999c3a595f6ef
1bee01bace1c9f636d33b632d2464b484d39d1b927384f965fdfdf7db9d741c9e4fc4e83067a2c21ac4
f0b19e62f6495e94b463646de0b7b4371459faccb506aa914861a8d81f0f5a78ec722b6cf1a7af8117f
82939d873deeff9dea3d599e97478a56350e747252572 5f069c1956979dc7d7f4cac0116c7eae938050
6f10c6554063e52da7da8a299f3e0bf86bc35bb96d71f64b8e6682a195281fd796316df97c9e2986b6b
893708834317ca6ab82fbaea42c469b7dfbc41d6e71806a6b5cc27e10005118901150305205489220le
71806a6b5cc27e10108fa5e07fc0e52ec7bb9d43480900c15545b1cc17e59427802b6fbf485c5dba4b4
```

openpgpkey –verify to compare DNS with keyring



```
paul@thinkpad:~$ openpgpkey --fetch pwouters@fedoraproject.org | gpg --dry-run --import
gpg: key 0x62D3582FE0FD94D2: "Paul Wouters <pwouters@redhat.com>" not changed
gpg: Total number processed: 1
gpg:              unchanged: 1
paul@thinkpad:~$ openpgpkey --verify pwouters@fedoraproject.org
All OPENPGPKEY records matched with content from the local keyring
paul@thinkpad:~$
```

TODO: publishing Fedora distribution key

- Use DNSSEC to publish the PGP used to sign all packages
- Problem:
  - Each version uses a different key
  - But using fedora@fedoraproject.org

The hash-slinger package

- openpgpkey: create, verify and download PGP keys using OPENPGPKEY records
- sshfp: create and verify SSH host keys using SSHFP records
- tlsa: create and verify SSL certificates using TLSA records (missing STARTTLS support)
- ipseckey: create IPSECKEY records for Libreswan IPsec (Opportunistic Encryption)

openpgpkey-milter – A reference implementation

- A sendmail and postfix plugin to auto-encrypt email
- Uses OPENPGPKEY to find encryption key
- yum install openpgpkey-milter
- service openpgpkey-milter start
- add to /etc/postfix/main.cf:
  smtpd_milters = inet:127.0.0.1:8890
- service postfix restart

- Biggest problem: it works (my email is routed from mx.nohats.ca to my own local mail server)

DNSSEC experience on laptops / phones

- dnssec-trigger + unbound per default in Fedora 22
- Still need better integration with Network-Manager
- Roaming / switching networks, split-DNS and TTL
- Cache management (Should I stay or should I flush)
- More than 1 domain in split-DNS cannot be conveyed with DHCP or VPN (XAUTH)
- Touch “search domains” in /etc/resolv.org or not ?
- DNS over port 80/443 needs to maintain TCP connction (i.e via draft-ietf-dnsop-ens-chain-query)
- When do we trust the AD bit ?

DNSSEC design for servers, virtual machines and containers

- Very much a work in progress

- Avoid using a single caching resolver per container
- Avoid DNSSEC validation inside every application ?
- Problems with trusting the hypervisor/host for AD bit ?

- Root KSK rollover

Current project: IPsec with DNSSEC

Opportunistic IPsec to protect against pervasive monitoring

- Anonymous IPsec (march 2015) (draft-ietf-ipsecme-authnull)
- Single side DNSSEC authenticated IPsec using DNS triggers (april 2015)
- Cloud encryption using reverse-DNS (may 2015)
- Mutual authenticated IPsec (june 2015)

- End result: draft-opportunistic-ipsec