

# PGP Introduction and Keysigning

Joel Jaeggli  
For  
SSE AFNOG 2011

# Rational

- We've talked about public key crypt in the context of web server certs.
- We talking about it in the context of encryption systems.
- Now it's time to do something with it.
- We're going to generate identities, validate and sign them.
- You can take them home with you, they can allow you communicate securily with your friends and colleagues.
- You'll form part of a web of trust with your AFNOG colleagues which you can further extend by signing the keys of your friends and colleagues.

# Get software (some useful examples)

- Windows
  - <http://www.gpg4win.org/download.html>
    - Install, run kleopatra, create new openpgp keypair
  - Enigmail (thunderbird)
- Ubuntu
  - <https://help.ubuntu.com/community/GnuPrivacyGuardHowto>
- Mac
  - <http://www.gpgtools.org/installer/index.html>
- Generic
  - <http://www.gnupg.org/download/index.en.html>

# Create a key (example is command-line GPG)

- `gpg --gen-key`
- Select DSA and el gamal ( you can read some rather long screens on the internet about which is better)
- 2048 bit key size
- Does not expire or 20y are reasonable depending on whether you want a safety net for expiration or not.
- Real name
- Email address
- Comment
- Password

# Uploading the key for the key-signing

- `gpg -list`
- Once you find the key-id
- Do `gpg -export -a keyid` to generate the ascii armor version of your public key.
- Go to <http://biglumber.com/x/web?keyring=1203>
- Paste in your ascii armored key

# How a PGP-signing party works

- Everyone uploads their public keys...
- Keyfile is downloaded and distributed.
- A participant presents an identity document satisfactory to the other participants (government issued photo-id for example)
- And reads out-loud their keyfingerprint
- Other participants sign the validated key having verified the key fingerprint.

## View Keyring


- Event: [afnog ws sse keysigning event](#)
- Date: **June 2 - 05, 2011**
- Keyring name: **afnog ws sse keysigning event keyring**
- You may add keys to this keyring.

[Download this keyring](#)

**Total entries: 2**

You are the owner of this keyring. [\[Edit keyring settings\]](#)

[View keyring as others see it](#)

Visible?	Date uploaded	Fingerprint Key type / Key size Creation date / Expiration date	UIDs	Image
<input checked="" type="checkbox"/>	20110601 08:00 EDT <a href="#">[remove from keyring]</a>	<a href="#">5C6E0104BAF040B05BD3C38BF00035ABB67F56B2</a> DSA / 1024 2003-08-11 / None	<ul style="list-style-type: none"> <li>• Joel Jaeggli (08112003-alternate to pgp 5 keypair) &lt;joelja "at" twin DOT uoregon.edu&gt;</li> </ul>	
<input checked="" type="checkbox"/>	20110601 07:54 EDT <a href="#">[remove from keyring]</a>	BEDA1F529F0769A2B1CF336781BDD3C40E1F9B79 DSA / 1024 1999-09-23 / None	<ul style="list-style-type: none"> <li>• Phil Regnaud (private) &lt;pr "at" eu DOT org&gt;</li> <li>• Phil Regnaud (home address) &lt;regnaud "at" starBSD DOT org&gt;</li> </ul>	

[Make changes](#)

Paste an ascii-armored file below containing the key(s) you wish to add to the keyring.

- MAILBOXES
  - Inbox
  - MobileMe
  - nagasaki 924
  - Gmail 2893
  - Drafts
    - MobileMe
    - nagasaki 227
    - Gmail
  - Sent
    - MobileMe
    - nagasaki
    - Gmail
  - Trash
  - RSS
    - Apple Hot News
  - ON MY MAC
    - Recovered Messag...
  - MOBILEME
    - Junk
  - NAGASAKI
    - Archives
    - duplicates 1934
- MAIL ACTIVITY

To	Subject	Date Sent
Patrick J Okui	Re: did v4 transit get particularly crappy?	Yesterday 3:04 AM
teemu.savolainen@nokia.com	fyi... the ietf mailman seems to be getting bounces ...	Yesterday 4:30 AM
<teemu.savolainen@nokia.com> <teemu.savolainen@no...	Re: fyi... the ietf mailman seems to be getting boun...	Yesterday 5:44 AM
Livingood, Jason	Re: very private: whitelisting-implications	Yesterday 6:40 AM
Phil Regnaud	Re: Evening session proposal for tonight: virtualiza...	Yesterday 6:40 AM
eric clark	Re: Deploying IPv6 globally	Yesterday 8:54 AM
Jens Kuehlers	Re: nokia/microsoft	Yesterday 10:45 AM
Alexa Morris	Re: NANOG transition update	Yesterday 11:10 AM
John Kemp	test	Today 2:11 AM

The message has been encrypted with OpenPGP. Decrypt

**Subject:** test  
**From:** Joel Jaeggli  
**Date:** June 1, 2011 2:11:37 AM PDT  
**To:** John Kemp

-----BEGIN PGP MESSAGE-----  
 Version: GnuPG v1.4.11 (Darwin)

```

hQIOA6uaU7C8mGypEaf+0zM2mFHCwu1S8wE8df8khhbDEKtjVc/V9IvKJbVchKTgw
fDyxSJE15KkApbxEC006XAXhC5xyeRoUX8HN4ox2eSjQkv0p0AXHeH2W3oY8hf8S
0+8IETlBhshfAhi0oHIoCXRDM8XHkys2HmDQX7ZixFcx6rk11xMyXzVRWAzo1VsD
AHX0QfzqyUi0VLS3BRkZ3M2RiyWIKLDWLF39Uzuh/o853zcmwsvygz20ucZm2bY
bqMBT0grw+mPq5w9IfKkhdGEwIox5v6wHpDxo6mr3NL8C58R/yYwfh6JtGp4+rOP
3h0jttf0ime4asd0hS9op8K+JhUjcwEYKZsynNLPgJAF/Y1pZPmELJcgIV1NhHVLJ
g27ZE4ZAc/16VtM2ExZiK8X09JU5v1FgLOl+5nfiw6ID2njPqDocIgc0mzaapxyx
EPaDPCEsuaav7UFFw8Q7TNjFPp1ARSyrjEiItl/+E/Gol07QIwwx8uSyqlzeow9Ln
Ha2Z0IVPJ+Dehu0x1VGa/wPV7jAscXGgHx+T6w80hE0wxdZXPmLv6mf88vX8mQ2D
S2Uz93bwV0Bx8wIagGpFx906YnKZaZ0cRnD/jAhxAKASvw8c8b7w99N82Bowhhu2
4Uw80UR0Gex/Komzww025zJmrIR4n8rFyZCG+gjkQHR2Dr1Zw1+pze0Zoe7E1vt+
pIUEDgN6HX/mKUB/khAP/3FUKbCX0qoQpbu8trzqb6x/3Sv2GhfuQkIAxf+BwFwy
yLpoKhZJy/3wC6Er3G3zgS3yIbtX7mU29HrcAwqIiWVoPcgKZSt34/3KZw/IeNrh
sGniJYbdD5L0PGeK0/6wbZCz/CrA3cXcFuWawf+IpWcx0v6KVS0VEtgBXIaeAS0v
W2LYck0V5fFoUuVTV8QTSpaExw5ni/trQiMKVxL+qYSXVvSYCrJg0xeX0xr8DwPh
kePTux/Vqt04qaza+Jz2BhhtSxSvJ4HGv0fEXor64jec7vemz0Mfzg6Jc41+tjbj
E05Jny/sN3ckdJTi/OTPaUQKhjLEDVR9D/K/dnkwT3b/EGNDRhoKhE02diMlai5+
  
```



