SSH Authentication Using GPG Smart Cards

UNIVERSITY OF
SOUTHERN
INDIANA®

Information Technology

Introduction

- Nick Bebout
- Senior Systems Administrator at the University of Southern Indiana
- nb@usi.edu
- https://nb.usi.edu

Benefits of using Smart Cards

- Your GPG key does not reside on your hard drive
- Key cannot be extracted from smart card
  - Keys can be generated on the smart card itself, however, I recommend generating the key on your machine (while not connected to internet), so you can make a backup in case your smart card malfunctions in the future and you need to reset or replace it
- Protection against brute-force of your passphrase
  - 3 incorrect PINs will lock the card until Admin PIN is used
  - 3 incorrect Admin PINs will permanently lock the card, until/unless the card is completely wiped, which will remove any keys stored on that card
- Requires no additional configuration on servers, other than placing your public key in the authorized_keys file on that server, same as a traditional SSH key

Types of Smart Cards

- YubiKey 4
  - Support up to 4096 bit RSA keys
  - Also can do Yubico auth, HOTP, U2F
  - Also available in Nano size, USB-C and USB-C Nano
  - YK4 $40 USD, YK4 Nano or USB-C $50 USD, YK4 USB-C Nano $60
  - Can order from Yubico directly or “Fulfilled by Amazon”
  - Ships from USA (or Europe)

- YubiKey NEO
  - Support up to **2048** bit RSA keys
  - Also can do Yubico auth, HTOP, U2F, and NFC
  - $50 USD
  - Can order from Yubico directly or “Fulfilled by Amazon”
  - Ships from USA (or Europe)

- SIM sized GPG smart cards with Gemalto readers
  - Support up to 4096 bit RSA keys
  - Support NIST P-256,384,521
  - 18.50 EUR for smart cards
  - 19.00 EUR for Gemalto reader
- Must order from Germany https://www.floss-shop.de/en and takes a while to arrive

- Full size GPG smart cards with various types of readers
  - Support up to 4096 bit RSA keys
  - Support NIST P-256,384,521
  - 17.90 EUR for smart cards
  - Must order from Germany https://www.floss-shop.de/en and takes a while to arrive

GnuPG
0005
0000
2E2A
V2.1 0005 00002E2A
g10 code
Works with GnuPG
www.gnupg.org
- Compatible to OpenPGP-Standard
- RSA with up to 4096 bit
- Key generation on card
- Hardware Random Number Generator
- Software download: www.gnupg.org
BasicCard
ZeitControl

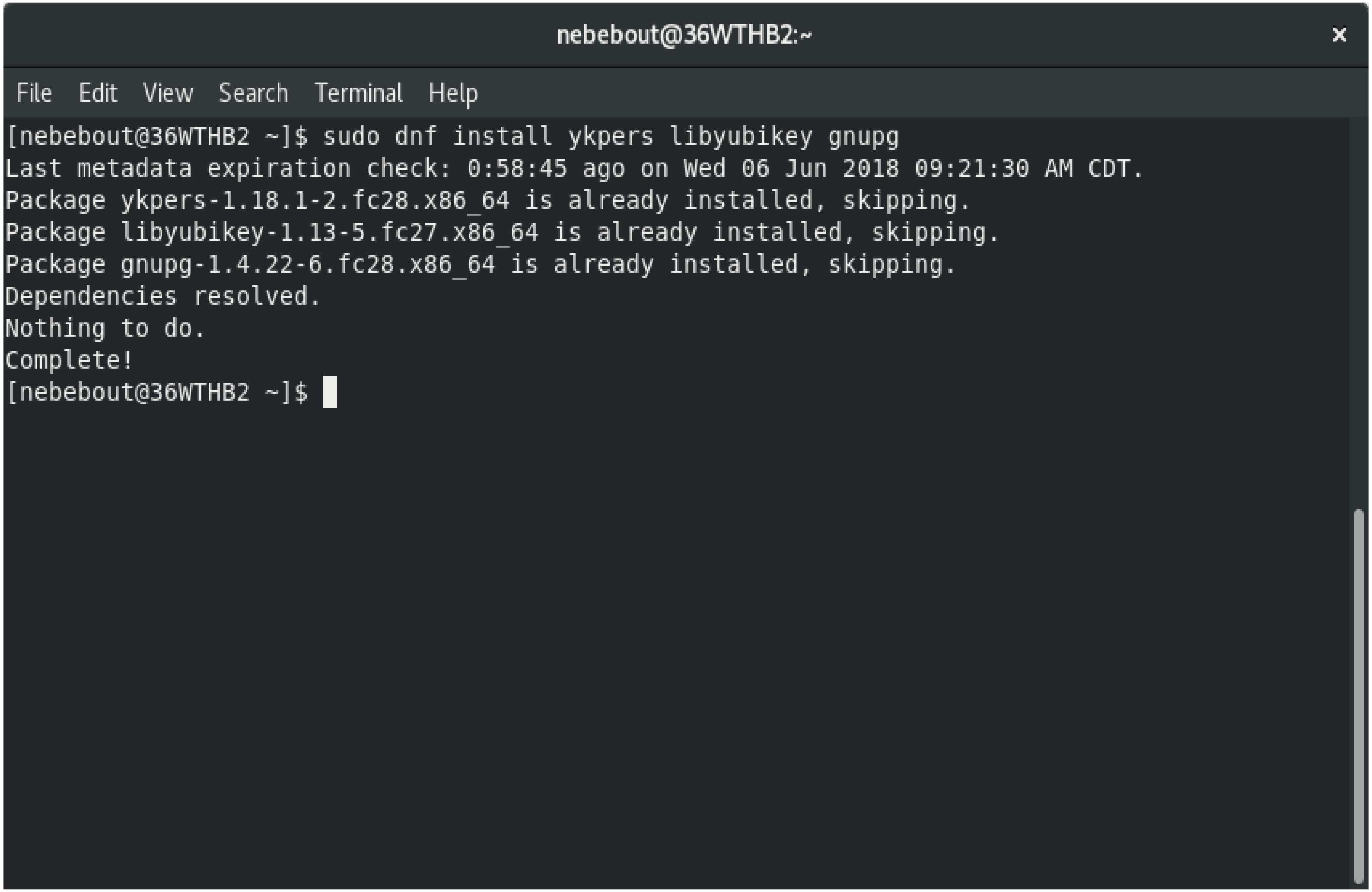
How to use GPG smart cards

https://git.nb.zone/nb/ssh-gpg-smartcard-config
or
https://da.gd/smartcards

This repository has instructions for Linux, macOS, and Windows

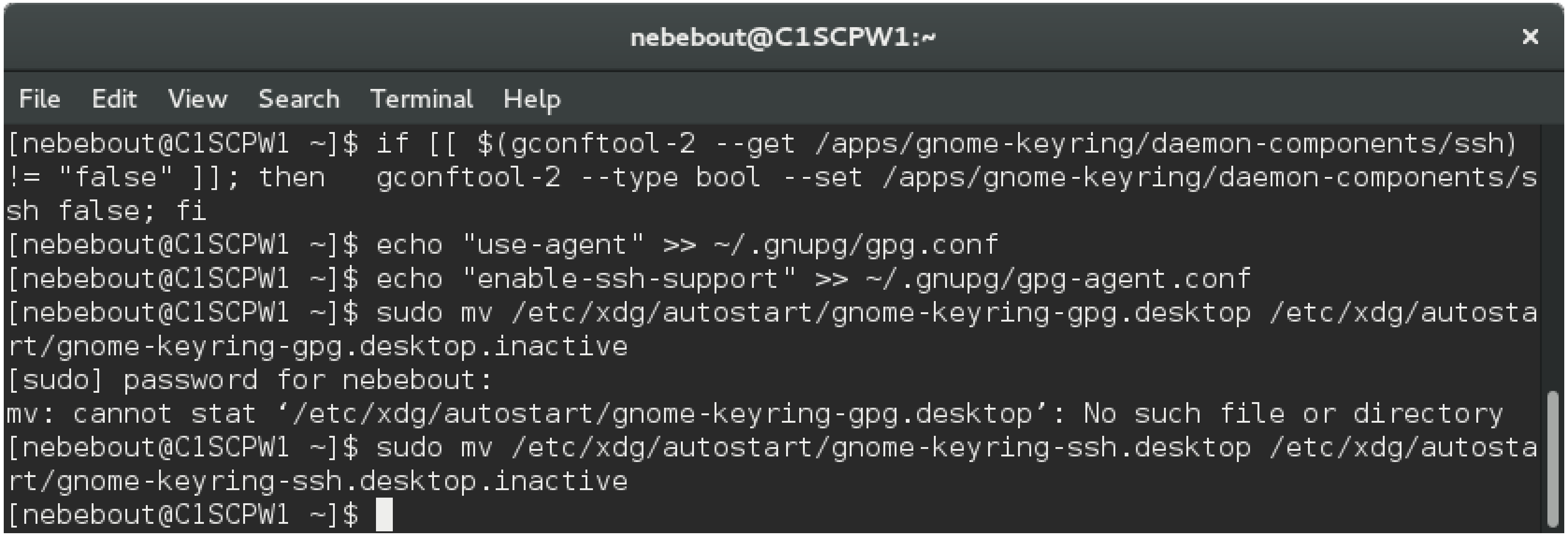
Enabling Smart Card Support

Installing Required Packages



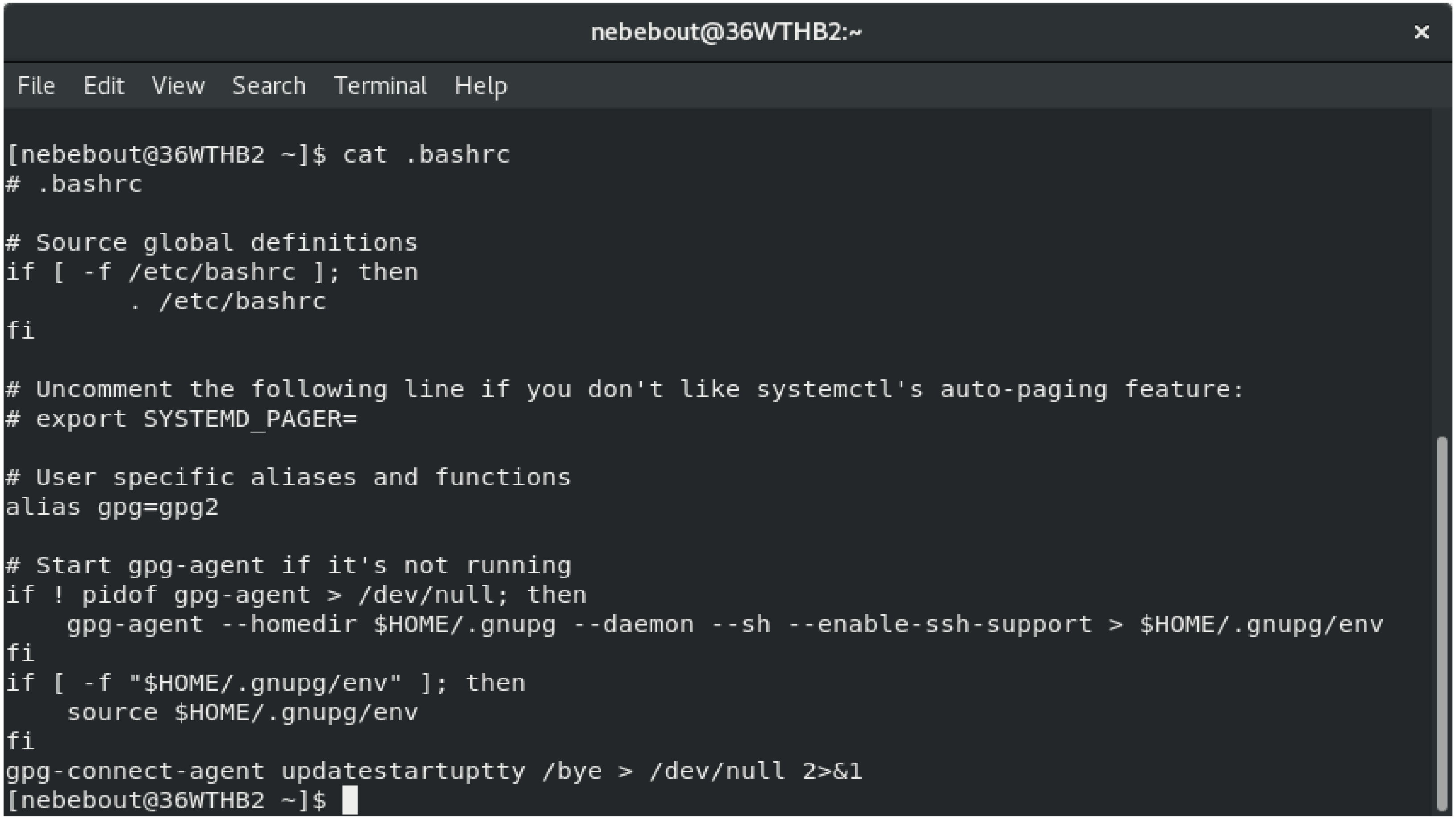
```
[nebebout@36WTHB2 ~]$ sudo dnf install ykpers libyubikey gnupg
Last metadata expiration check: 0:58:45 ago on Wed 06 Jun 2018 09:21:30 AM CDT.
Package ykpers-1.18.1-2.fc28.x86_64 is already installed, skipping.
Package libyubikey-1.13-5.fc27.x86_64 is already installed, skipping.
Package gnupg-1.4.22-6.fc28.x86_64 is already installed, skipping.
Dependencies resolved.
Nothing to do.
Complete!
[nebebout@36WTHB2 ~]$ 
```

Disable gnome-keyring and enable gpg-agent to replace ssh-agent



```
[nebebout@C1SCPW1 ~]$ if [[ $(gconftool-2 --get /apps/gnome-keyring/daemon-components/ssh)
!= "false" ]]; then   gconftool-2 --type bool --set /apps/gnome-keyring/daemon-components/s
sh false; fi
[nebebout@C1SCPW1 ~]$ echo "use-agent" >> ~/.gnupg/gpg.conf
[nebebout@C1SCPW1 ~]$ echo "enable-ssh-support" >> ~/.gnupg/gpg-agent.conf
[nebebout@C1SCPW1 ~]$ sudo mv /etc/xdg/autostart/gnome-keyring-gpg.desktop /etc/xdg/autosta
rt/gnome-keyring-gpg.desktop.inactive
[sudo] password for nebebout:
mv: cannot stat ‘/etc/xdg/autostart/gnome-keyring-gpg.desktop’: No such file or directory
[nebebout@C1SCPW1 ~]$ sudo mv /etc/xdg/autostart/gnome-keyring-ssh.desktop /etc/xdg/autosta
rt/gnome-keyring-ssh.desktop.inactive
[nebebout@C1SCPW1 ~]$ 
```

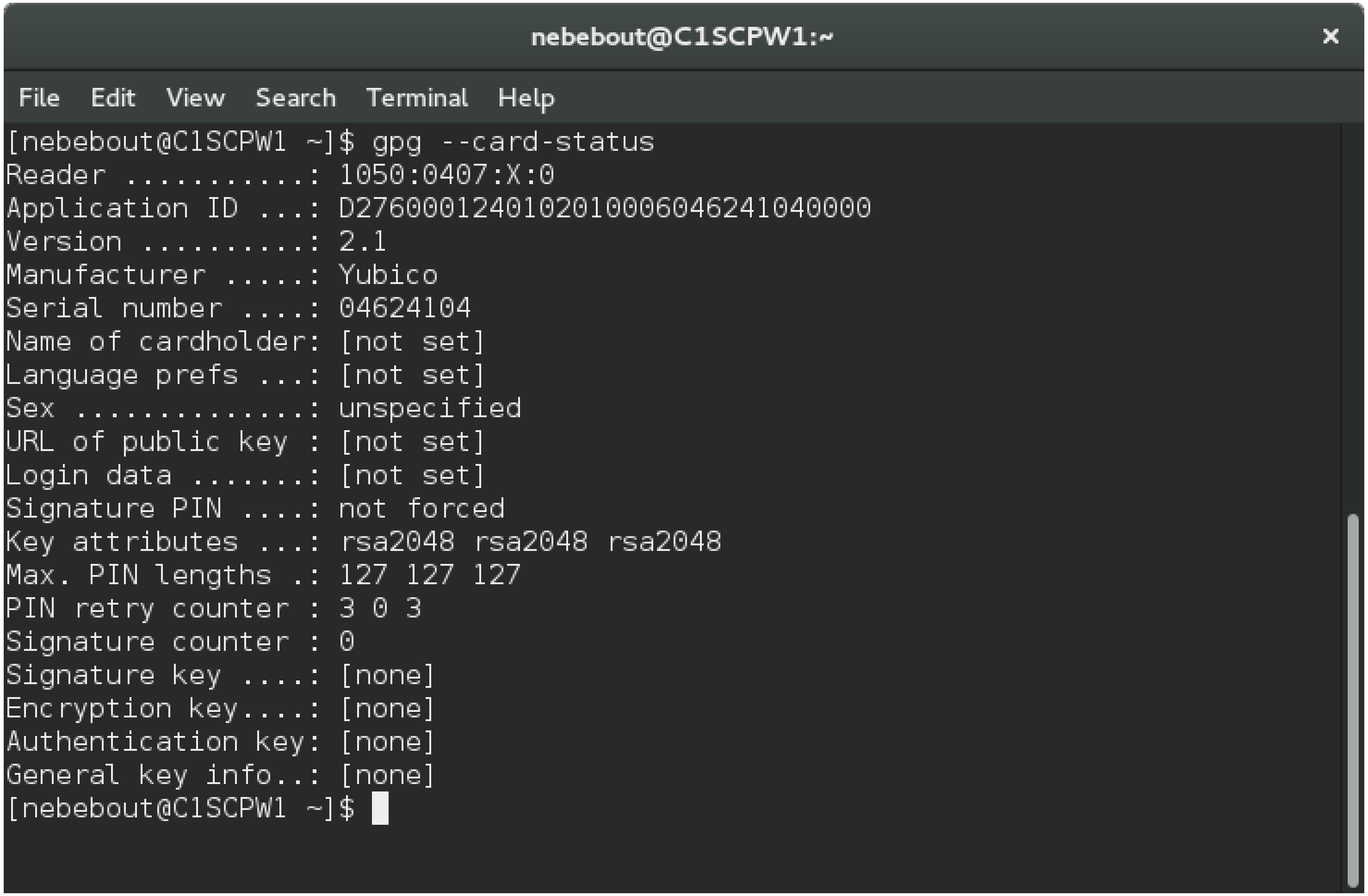
Set ~/.bashrc to automatically start gpg-agent



```
[nebebout@36WTHB2 ~]$ cat .bashrc
# .bashrc

# Source global definitions
if [ -f /etc/bashrc ]; then
        . /etc/bashrc
fi

# Uncomment the following line if you don't like systemctl's auto-paging feature:
# export SYSTEMD_PAGER=

# User specific aliases and functions
alias gpg=gpg2

# Start gpg-agent if it's not running
if ! pidof gpg-agent > /dev/null; then
    gpg-agent --homedir $HOME/.gnupg --daemon --sh --enable-ssh-support > $HOME/.gnupg/env
fi
if [ -f "$HOME/.gnupg/env" ]; then
    source $HOME/.gnupg/env
fi
gpg-connect-agent updatestartuptty /bye > /dev/null 2>&1
[nebebout@36WTHB2 ~]$ 
```

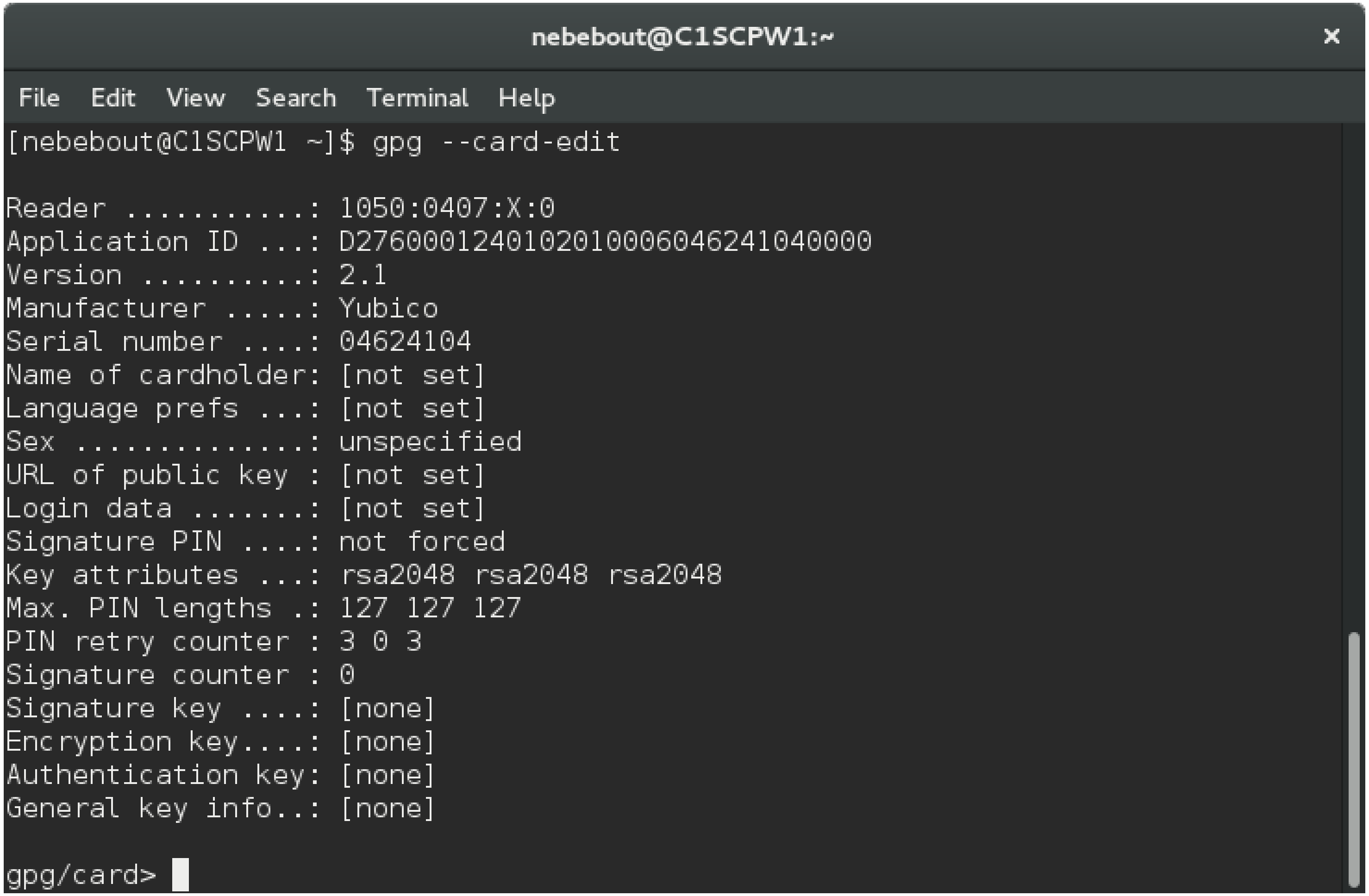
Configuring Your Smart Card

Verify if your smart card is working properly with GPG



```
[nebebout@C1SCPW1 ~]$ gpg --card-status
Reader ...........: 1050:0407:X:0
Application ID ...: D2760001240102010006046241040000
Version ..........: 2.1
Manufacturer .....: Yubico
Serial number ....: 04624104
Name of cardholder: [not set]
Language prefs ...: [not set]
Sex ..............: unspecified
URL of public key : [not set]
Login data .......: [not set]
Signature PIN ....: not forced
Key attributes ...: rsa2048 rsa2048 rsa2048
Max. PIN lengths .: 127 127 127
PIN retry counter : 3 0 3
Signature counter : 0
Signature key ....: [none]
Encryption key....: [none]
Authentication key: [none]
General key info..: [none]
[nebebout@C1SCPW1 ~]$ 
```

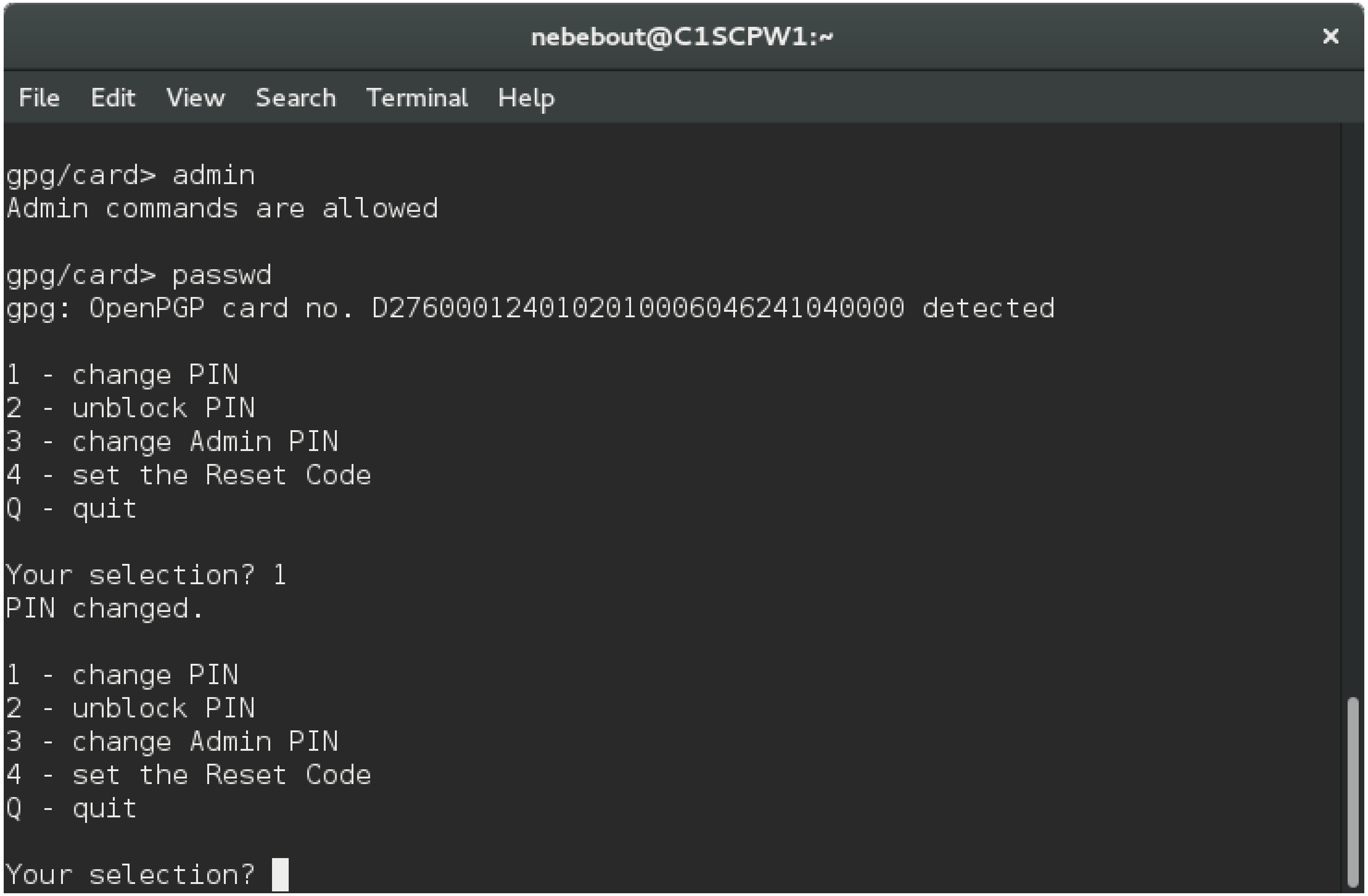
Enter “card edit” mode



```
[nebebout@C1SCPW1 ~]$ gpg --card-edit

Reader ...........: 1050:0407:X:0
Application ID ...: D2760001240102010006046241040000
Version ..........: 2.1
Manufacturer .....: Yubico
Serial number ....: 04624104
Name of cardholder: [not set]
Language prefs ...: [not set]
Sex ..............: unspecified
URL of public key : [not set]
Login data .......: [not set]
Signature PIN ....: not forced
Key attributes ...: rsa2048 rsa2048 rsa2048
Max. PIN lengths .: 127 127 127
PIN retry counter : 3 0 3
Signature counter : 0
Signature key ....: [none]
Encryption key....: [none]
Authentication key: [none]
General key info..: [none]

gpg/card> 
```

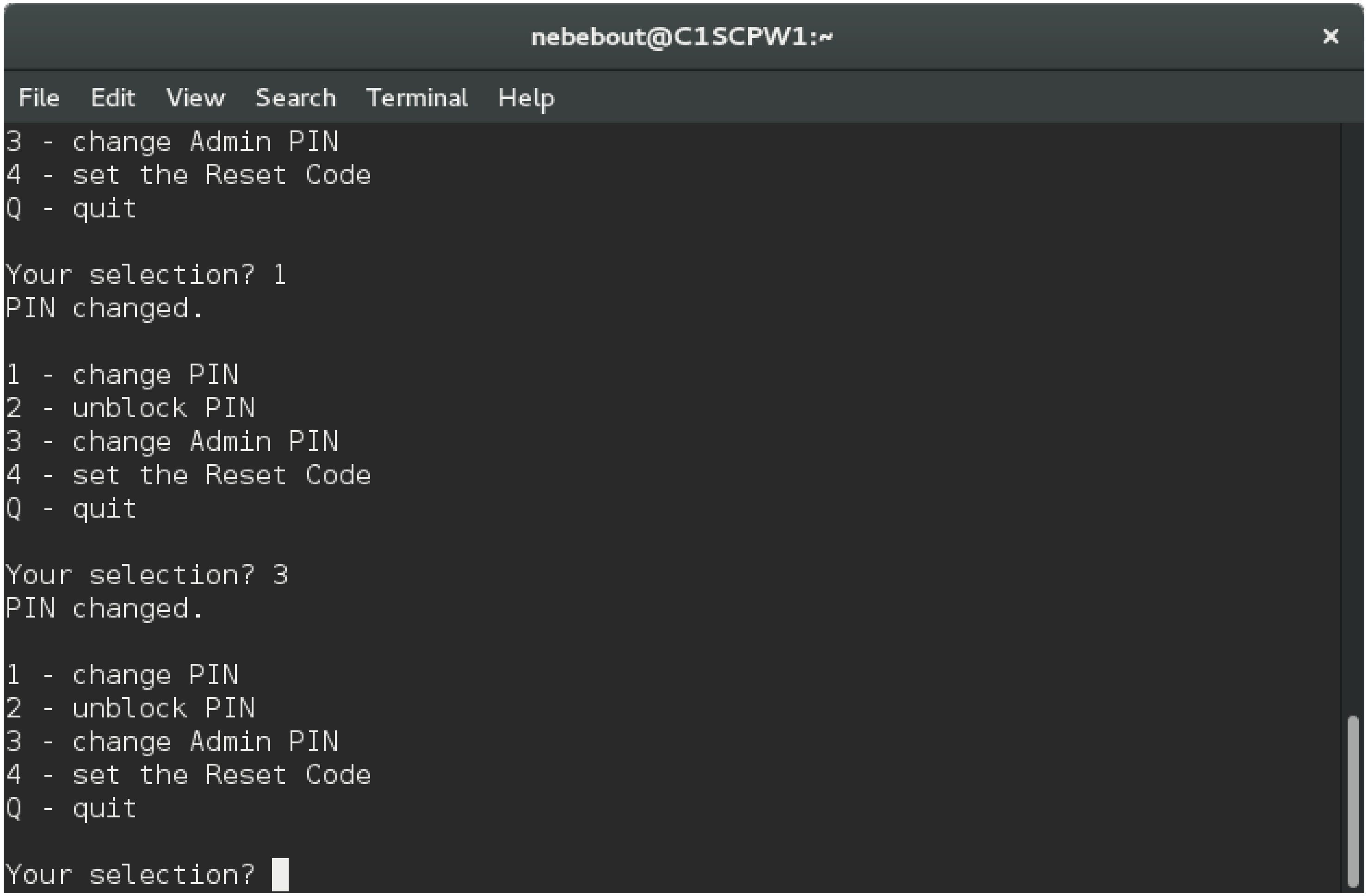
UNIVERSITY OF SOUTHERN INDIANA®
Information Technology

Set your PIN



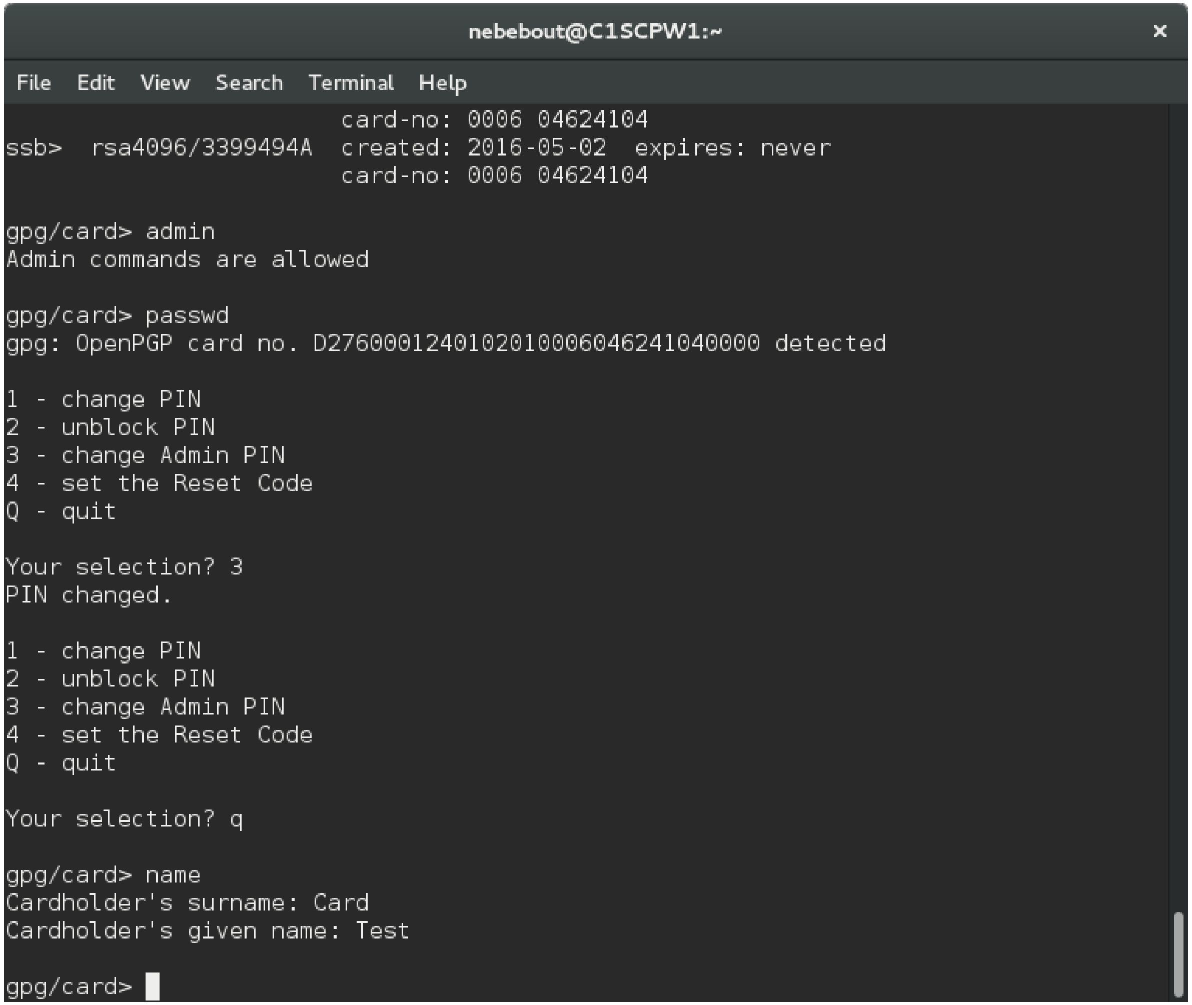
```
gpg/card> admin
Admin commands are allowed

gpg/card> passwd
gpg: OpenPGP card no. D2760001240102010006046241040000 detected

1 - change PIN
2 - unblock PIN
3 - change Admin PIN
4 - set the Reset Code
Q - quit

Your selection? 1
PIN changed.

1 - change PIN
2 - unblock PIN
3 - change Admin PIN
4 - set the Reset Code
Q - quit

Your selection? 
```

Set your Admin PIN



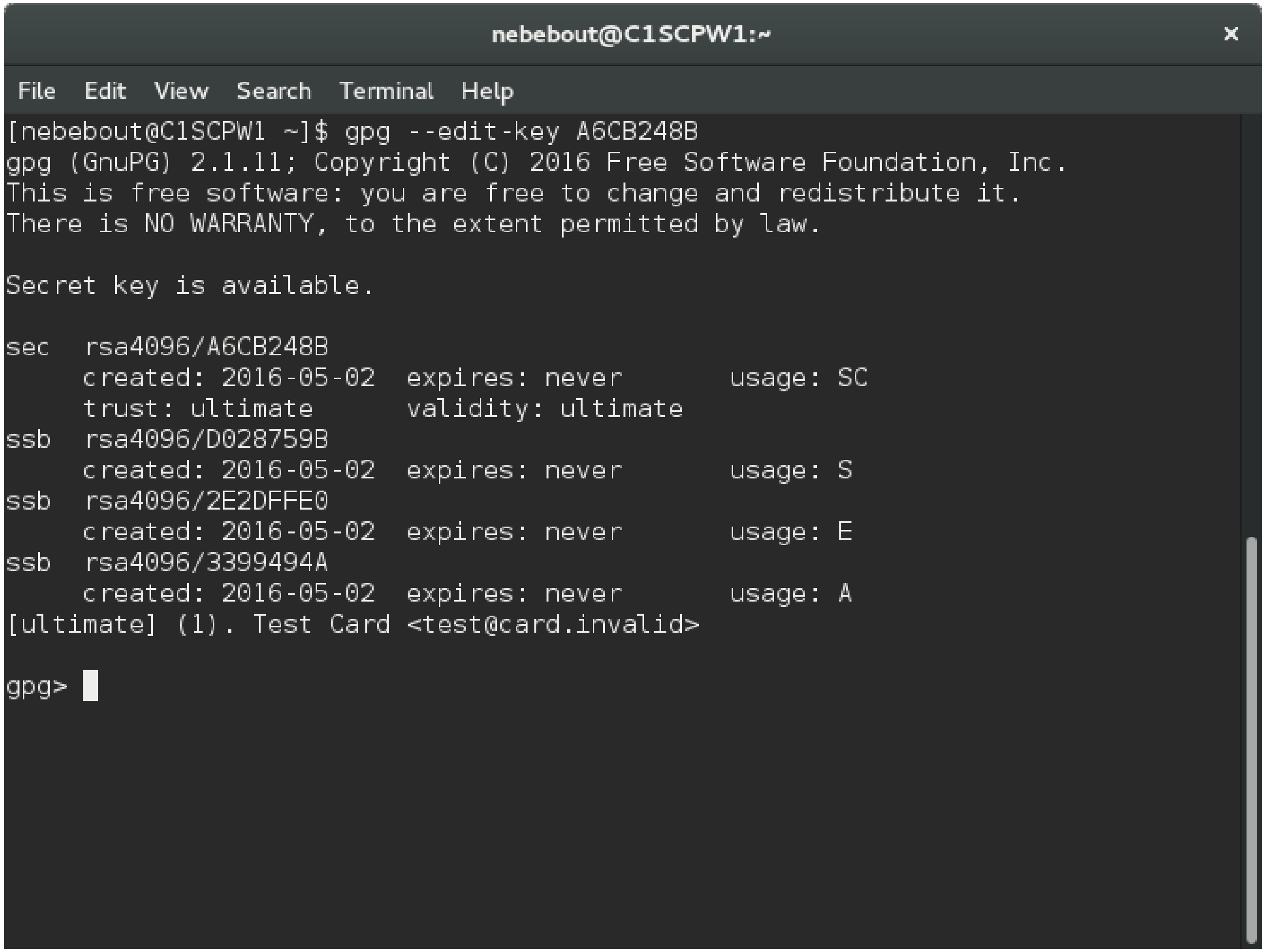
```
3 - change Admin PIN
4 - set the Reset Code
Q - quit

Your selection? 1
PIN changed.

1 - change PIN
2 - unblock PIN
3 - change Admin PIN
4 - set the Reset Code
Q - quit

Your selection? 3
PIN changed.

1 - change PIN
2 - unblock PIN
3 - change Admin PIN
4 - set the Reset Code
Q - quit

Your selection? 
```

Set your name (optional)



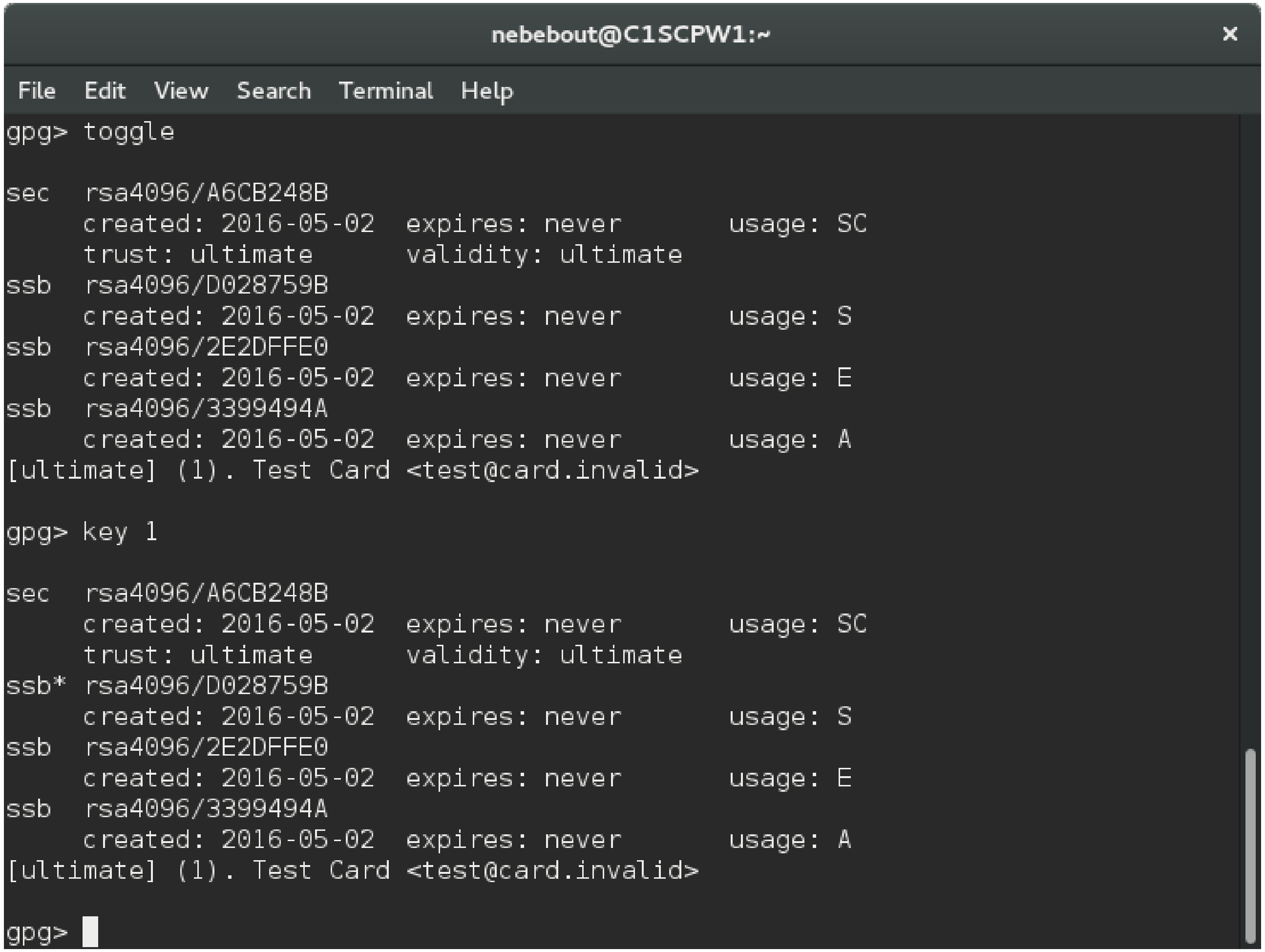
```
                        card-no: 0006 04624104
ssb>  rsa4096/3399494A  created: 2016-05-02  expires: never
                        card-no: 0006 04624104

gpg/card> admin
Admin commands are allowed

gpg/card> passwd
gpg: OpenPGP card no. D2760001240102010006046241040000 detected

1 - change PIN
2 - unblock PIN
3 - change Admin PIN
4 - set the Reset Code
Q - quit

Your selection? 3
PIN changed.

1 - change PIN
2 - unblock PIN
3 - change Admin PIN
4 - set the Reset Code
Q - quit

Your selection? q

gpg/card> name
Cardholder's surname: Card
Cardholder's given name: Test

gpg/card> 
```

Enter “edit key” mode



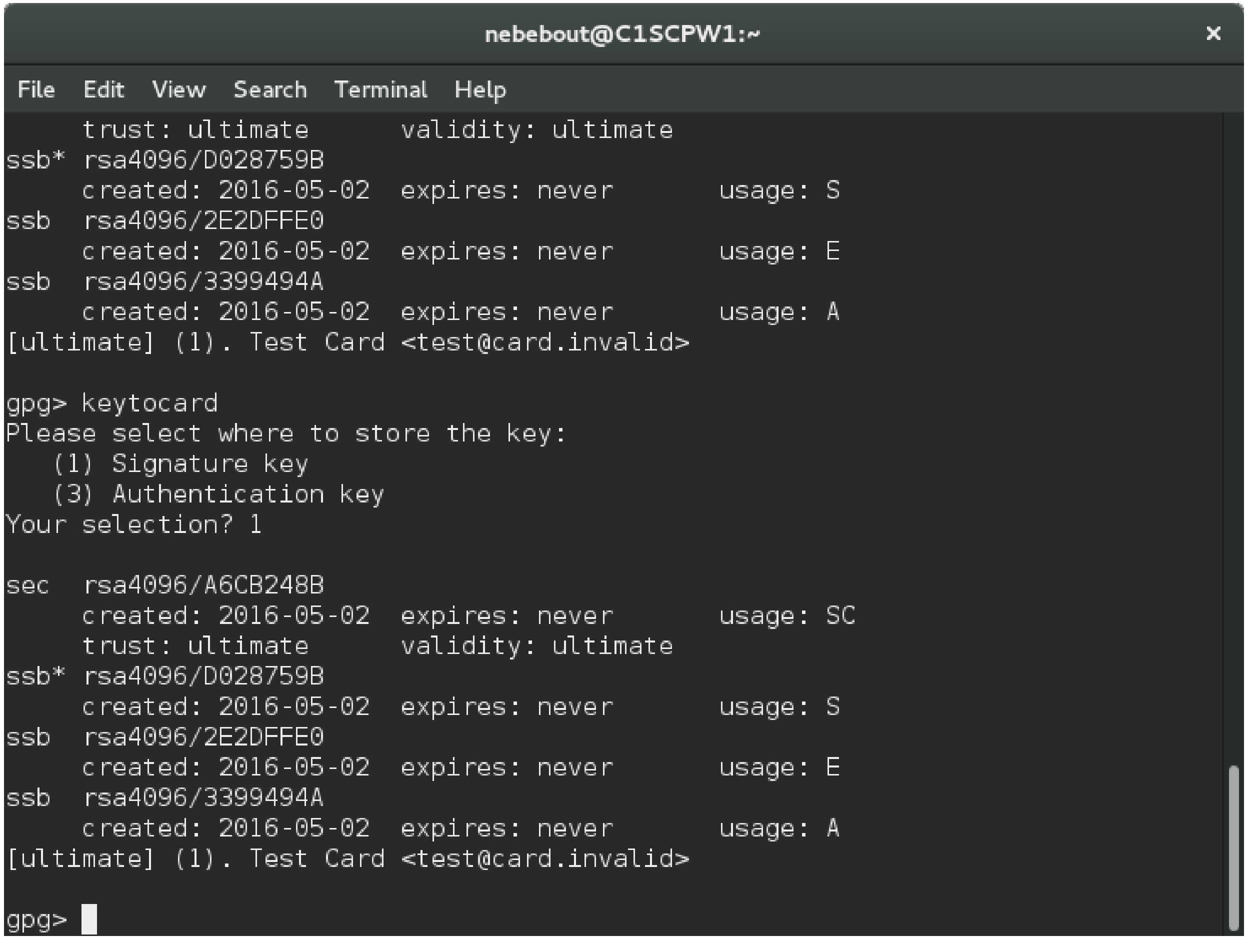
```
[nebebout@C1SCPW1 ~]$ gpg --edit-key A6CB248B
gpg (GnuPG) 2.1.11; Copyright (C) 2016 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Secret key is available.

sec  rsa4096/A6CB248B
     created: 2016-05-02  expires: never       usage: SC
     trust: ultimate      validity: ultimate
ssb  rsa4096/D028759B
     created: 2016-05-02  expires: never       usage: S
ssb  rsa4096/2E2DFFE0
     created: 2016-05-02  expires: never       usage: E
ssb  rsa4096/3399494A
     created: 2016-05-02  expires: never       usage: A
[ultimate] (1). Test Card <test@card.invalid>

gpg> 
```

Toggle (to change to private keys)
& Select 1st subkey (In this case, is the signature subkey)



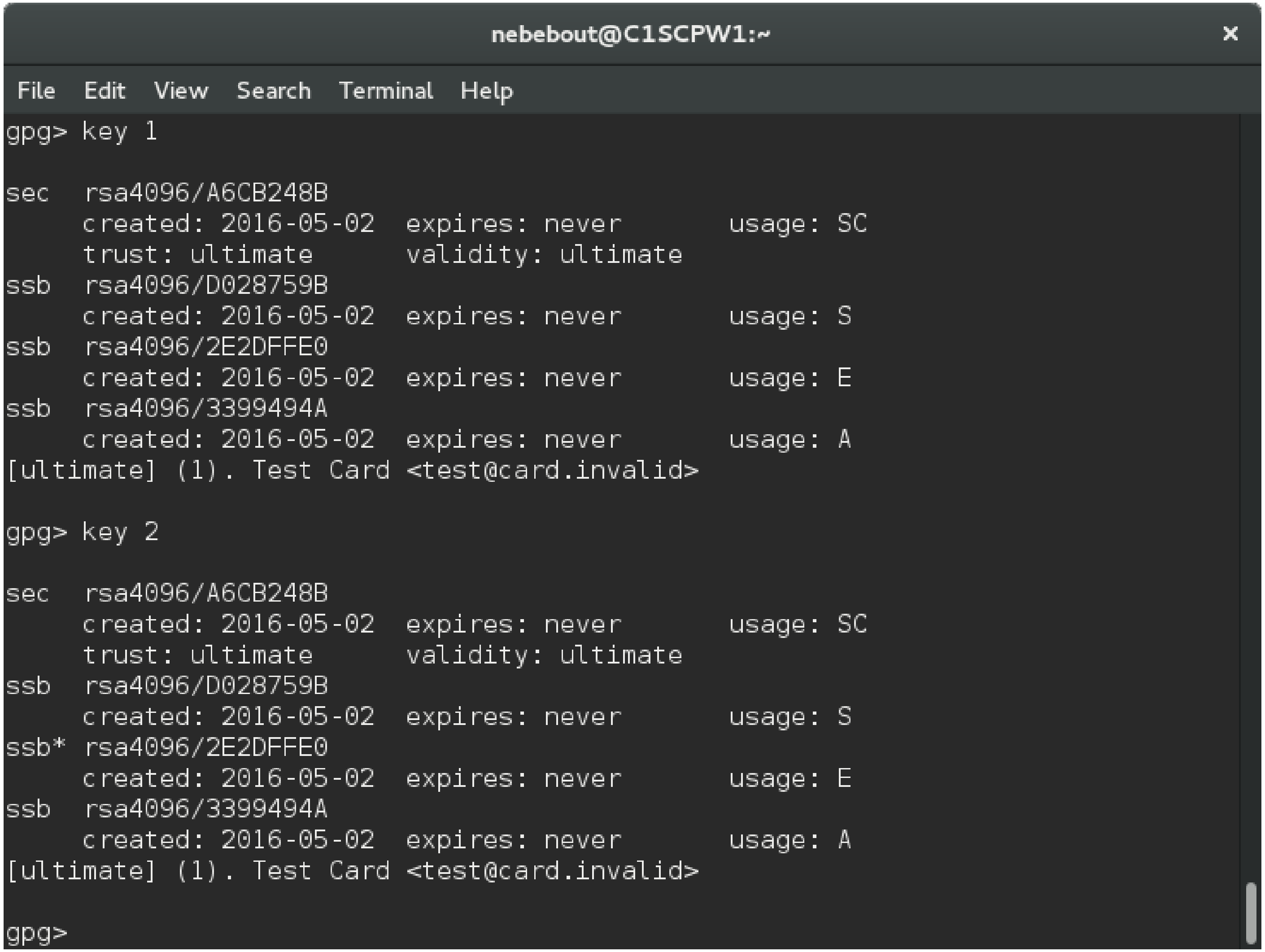
```
gpg> toggle

sec   rsa4096/A6CB248B
      created: 2016-05-02  expires: never       usage: SC
      trust: ultimate      validity: ultimate
ssb   rsa4096/D028759B
      created: 2016-05-02  expires: never       usage: S
ssb   rsa4096/2E2DFFE0
      created: 2016-05-02  expires: never       usage: E
ssb   rsa4096/3399494A
      created: 2016-05-02  expires: never       usage: A
[ultimate] (1). Test Card <test@card.invalid>

gpg> key 1

sec   rsa4096/A6CB248B
      created: 2016-05-02  expires: never       usage: SC
      trust: ultimate      validity: ultimate
ssb*  rsa4096/D028759B
      created: 2016-05-02  expires: never       usage: S
ssb   rsa4096/2E2DFFE0
      created: 2016-05-02  expires: never       usage: E
ssb   rsa4096/3399494A
      created: 2016-05-02  expires: never       usage: A
[ultimate] (1). Test Card <test@card.invalid>

gpg> 
```

Move 1st subkey to smart card



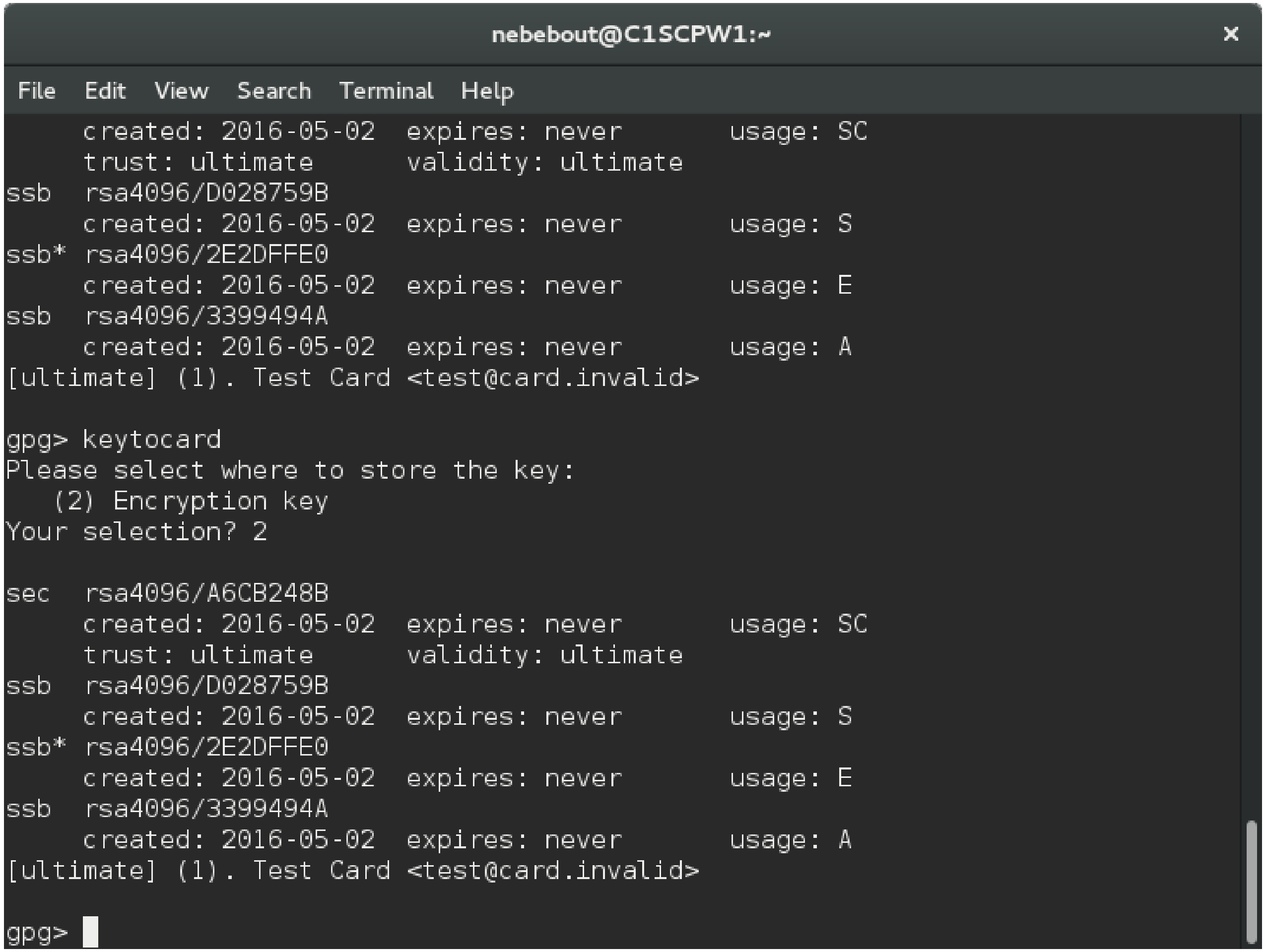
```
     trust: ultimate      validity: ultimate
ssb* rsa4096/D028759B
     created: 2016-05-02  expires: never       usage: S
ssb  rsa4096/2E2DFFE0
     created: 2016-05-02  expires: never       usage: E
ssb  rsa4096/3399494A
     created: 2016-05-02  expires: never       usage: A
[ultimate] (1). Test Card <test@card.invalid>

gpg> keytocard
Please select where to store the key:
   (1) Signature key
   (3) Authentication key
Your selection? 1

sec  rsa4096/A6CB248B
     created: 2016-05-02  expires: never       usage: SC
     trust: ultimate      validity: ultimate
ssb* rsa4096/D028759B
     created: 2016-05-02  expires: never       usage: S
ssb  rsa4096/2E2DFFE0
     created: 2016-05-02  expires: never       usage: E
ssb  rsa4096/3399494A
     created: 2016-05-02  expires: never       usage: A
[ultimate] (1). Test Card <test@card.invalid>

gpg> 
```

Deselect subkey 1, select subkey 2



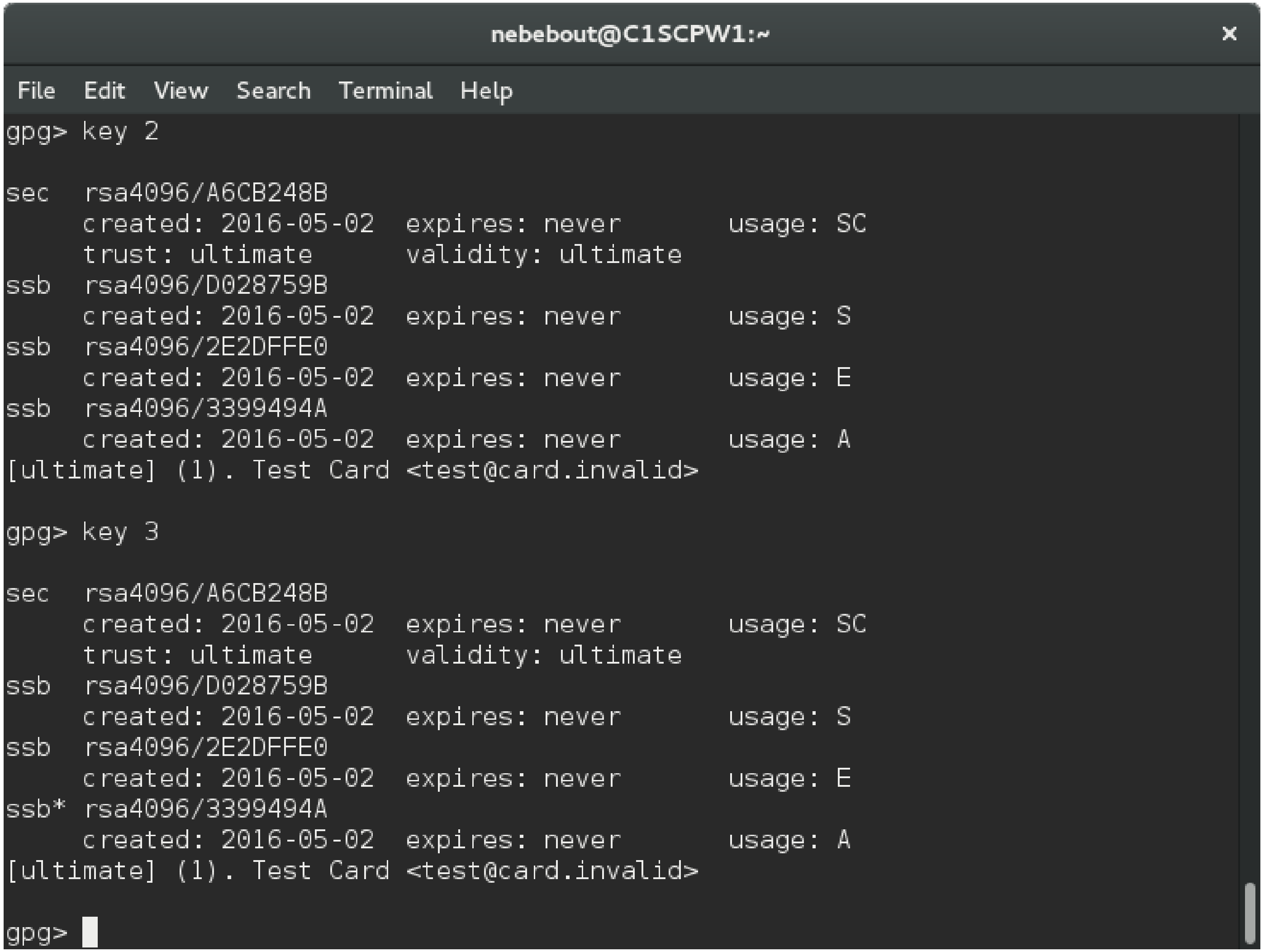
```
gpg> key 1

sec   rsa4096/A6CB248B
      created: 2016-05-02  expires: never       usage: SC
      trust: ultimate      validity: ultimate
ssb   rsa4096/D028759B
      created: 2016-05-02  expires: never       usage: S
ssb   rsa4096/2E2DFFE0
      created: 2016-05-02  expires: never       usage: E
ssb   rsa4096/3399494A
      created: 2016-05-02  expires: never       usage: A
[ultimate] (1). Test Card <test@card.invalid>

gpg> key 2

sec   rsa4096/A6CB248B
      created: 2016-05-02  expires: never       usage: SC
      trust: ultimate      validity: ultimate
ssb   rsa4096/D028759B
      created: 2016-05-02  expires: never       usage: S
ssb*  rsa4096/2E2DFFE0
      created: 2016-05-02  expires: never       usage: E
ssb   rsa4096/3399494A
      created: 2016-05-02  expires: never       usage: A
[ultimate] (1). Test Card <test@card.invalid>

gpg>
```

Move 2nd subkey to smart card



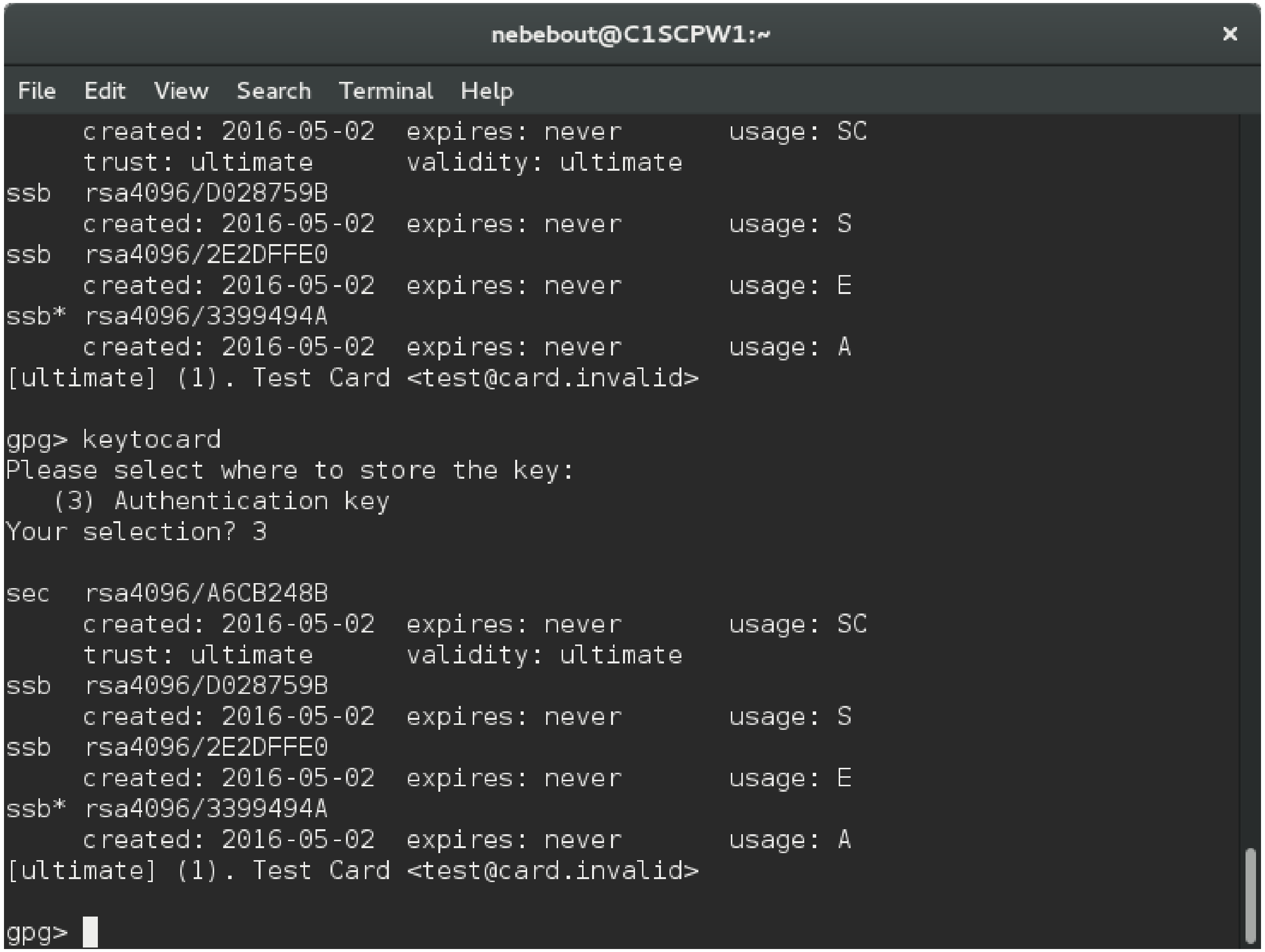
```
     created: 2016-05-02  expires: never       usage: SC
     trust: ultimate      validity: ultimate
ssb  rsa4096/D028759B
     created: 2016-05-02  expires: never       usage: S
ssb* rsa4096/2E2DFFE0
     created: 2016-05-02  expires: never       usage: E
ssb  rsa4096/3399494A
     created: 2016-05-02  expires: never       usage: A
[ultimate] (1). Test Card <test@card.invalid>

gpg> keytocard
Please select where to store the key:
   (2) Encryption key
Your selection? 2

sec  rsa4096/A6CB248B
     created: 2016-05-02  expires: never       usage: SC
     trust: ultimate      validity: ultimate
ssb  rsa4096/D028759B
     created: 2016-05-02  expires: never       usage: S
ssb* rsa4096/2E2DFFE0
     created: 2016-05-02  expires: never       usage: E
ssb  rsa4096/3399494A
     created: 2016-05-02  expires: never       usage: A
[ultimate] (1). Test Card <test@card.invalid>

gpg> 
```

Deselect subkey 2, select subkey 3



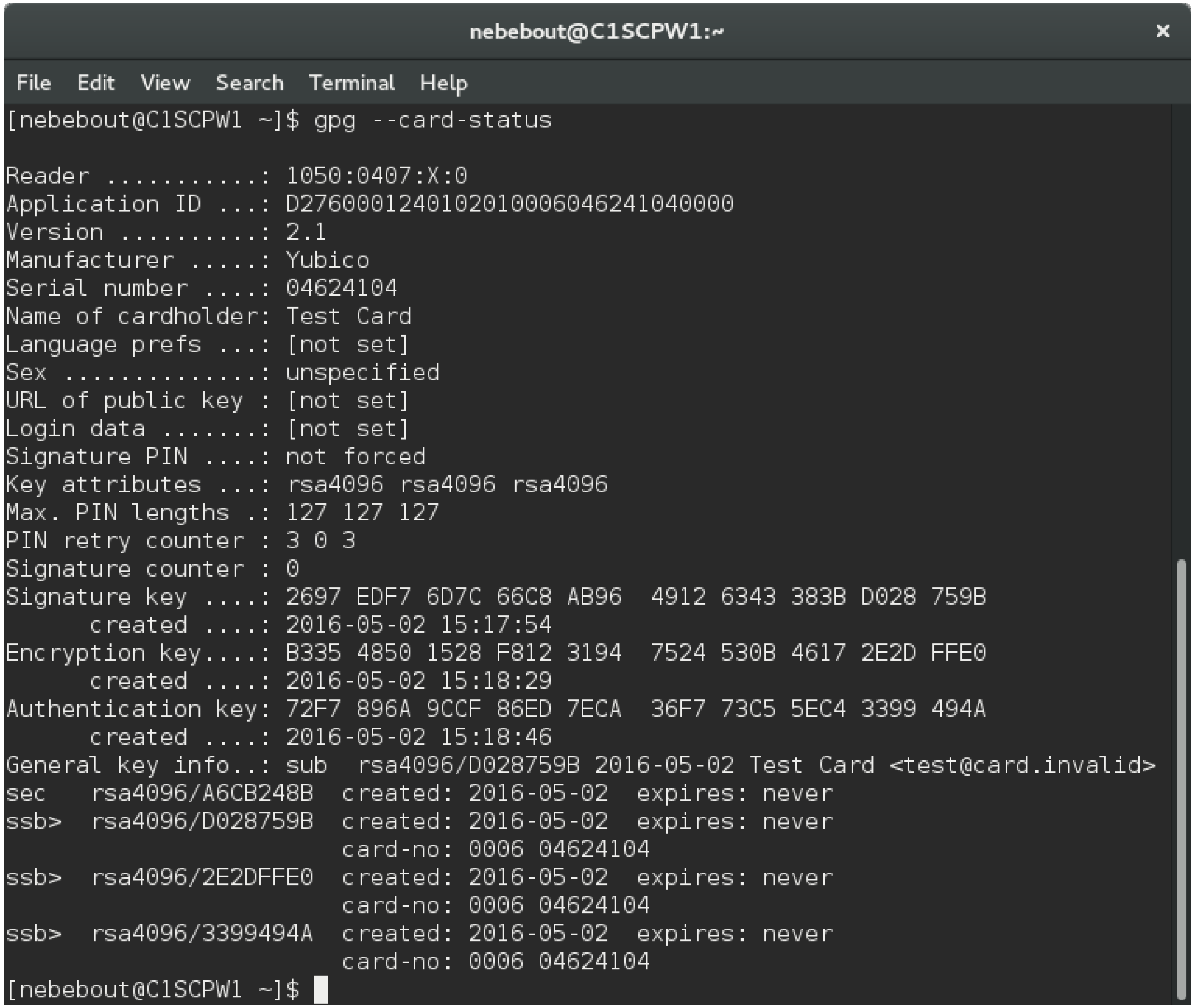
```
gpg> key 2

sec   rsa4096/A6CB248B
      created: 2016-05-02  expires: never       usage: SC
      trust: ultimate      validity: ultimate
ssb   rsa4096/D028759B
      created: 2016-05-02  expires: never       usage: S
ssb   rsa4096/2E2DFFE0
      created: 2016-05-02  expires: never       usage: E
ssb   rsa4096/3399494A
      created: 2016-05-02  expires: never       usage: A
[ultimate] (1). Test Card <test@card.invalid>

gpg> key 3

sec   rsa4096/A6CB248B
      created: 2016-05-02  expires: never       usage: SC
      trust: ultimate      validity: ultimate
ssb   rsa4096/D028759B
      created: 2016-05-02  expires: never       usage: S
ssb   rsa4096/2E2DFFE0
      created: 2016-05-02  expires: never       usage: E
ssb*  rsa4096/3399494A
      created: 2016-05-02  expires: never       usage: A
[ultimate] (1). Test Card <test@card.invalid>

gpg> 
```

Move 3rd subkey to smart card



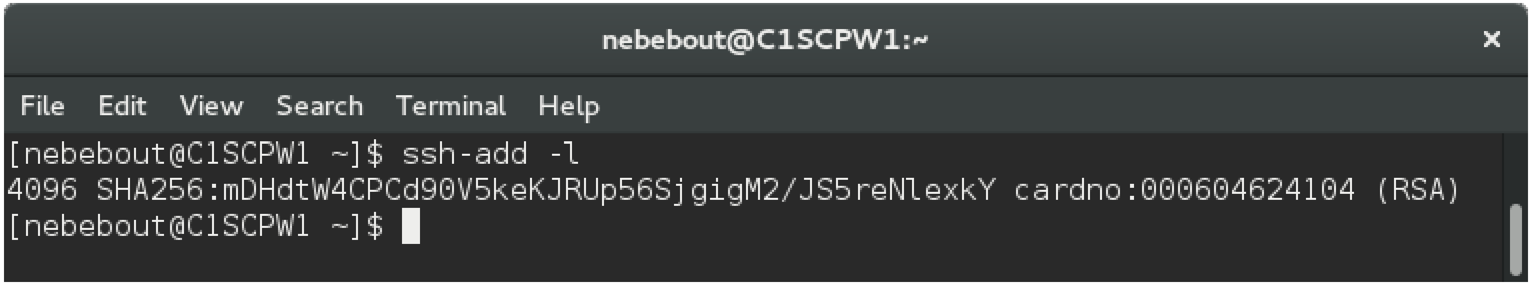
```
     created: 2016-05-02  expires: never       usage: SC
     trust: ultimate      validity: ultimate
ssb  rsa4096/D028759B
     created: 2016-05-02  expires: never       usage: S
ssb  rsa4096/2E2DFFE0
     created: 2016-05-02  expires: never       usage: E
ssb* rsa4096/3399494A
     created: 2016-05-02  expires: never       usage: A
[ultimate] (1). Test Card <test@card.invalid>

gpg> keytocard
Please select where to store the key:
   (3) Authentication key
Your selection? 3

sec  rsa4096/A6CB248B
     created: 2016-05-02  expires: never       usage: SC
     trust: ultimate      validity: ultimate
ssb  rsa4096/D028759B
     created: 2016-05-02  expires: never       usage: S
ssb  rsa4096/2E2DFFE0
     created: 2016-05-02  expires: never       usage: E
ssb* rsa4096/3399494A
     created: 2016-05-02  expires: never       usage: A
[ultimate] (1). Test Card <test@card.invalid>

gpg>
```

Verify that keys show up on smart card



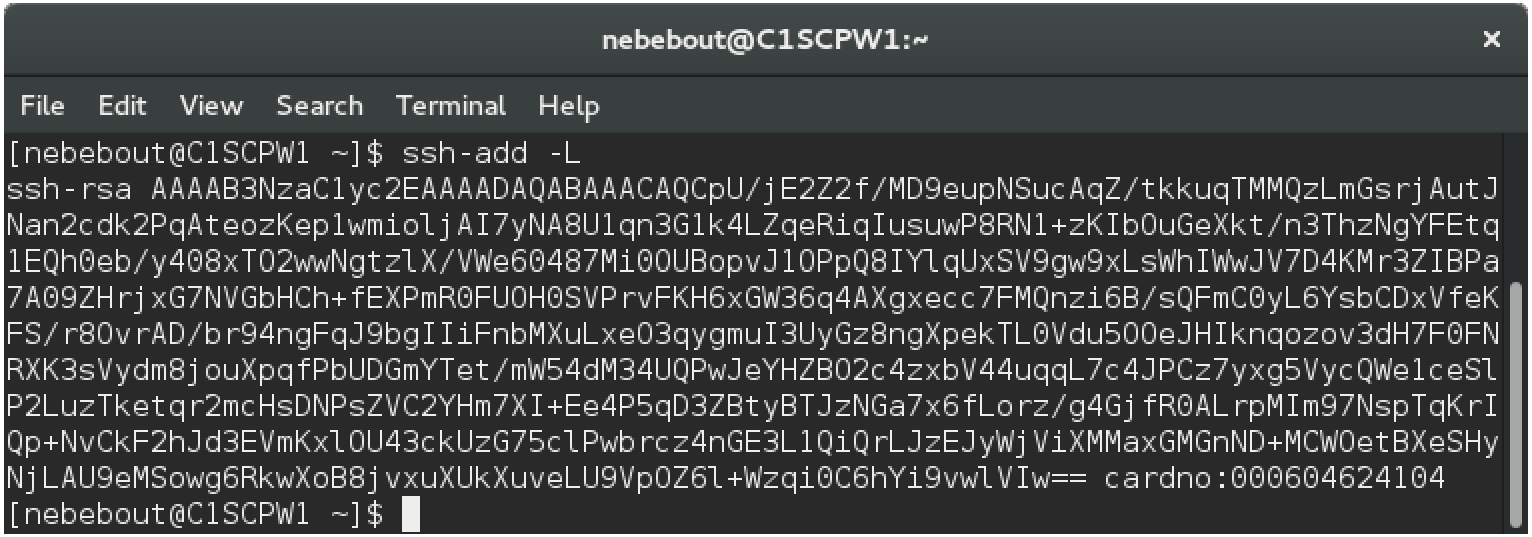
```
[nebebout@C1SCPW1 ~]$ gpg --card-status

Reader ...........: 1050:0407:X:0
Application ID ...: D2760001240102010006046241040000
Version ..........: 2.1
Manufacturer .....: Yubico
Serial number ....: 04624104
Name of cardholder: Test Card
Language prefs ...: [not set]
Sex ..............: unspecified
URL of public key : [not set]
Login data .......: [not set]
Signature PIN ....: not forced
Key attributes ...: rsa4096 rsa4096 rsa4096
Max. PIN lengths .: 127 127 127
PIN retry counter : 3 0 3
Signature counter : 0
Signature key ....: 2697 EDF7 6D7C 66C8 AB96  4912 6343 383B D028 759B
      created ....: 2016-05-02 15:17:54
Encryption key....: B335 4850 1528 F812 3194  7524 530B 4617 2E2D FFE0
      created ....: 2016-05-02 15:18:29
Authentication key: 72F7 896A 9CCF 86ED 7ECA  36F7 73C5 5EC4 3399 494A
      created ....: 2016-05-02 15:18:46
General key info..: sub  rsa4096/D028759B 2016-05-02 Test Card <test@card.invalid>
sec   rsa4096/A6CB248B  created: 2016-05-02  expires: never
ssb>  rsa4096/D028759B  created: 2016-05-02  expires: never
                        card-no: 0006 04624104
ssb>  rsa4096/2E2DFFE0  created: 2016-05-02  expires: never
                        card-no: 0006 04624104
ssb>  rsa4096/3399494A  created: 2016-05-02  expires: never
                        card-no: 0006 04624104
[nebebout@C1SCPW1 ~]$ 
```

Make sure gpg-agent will use your key for SSH



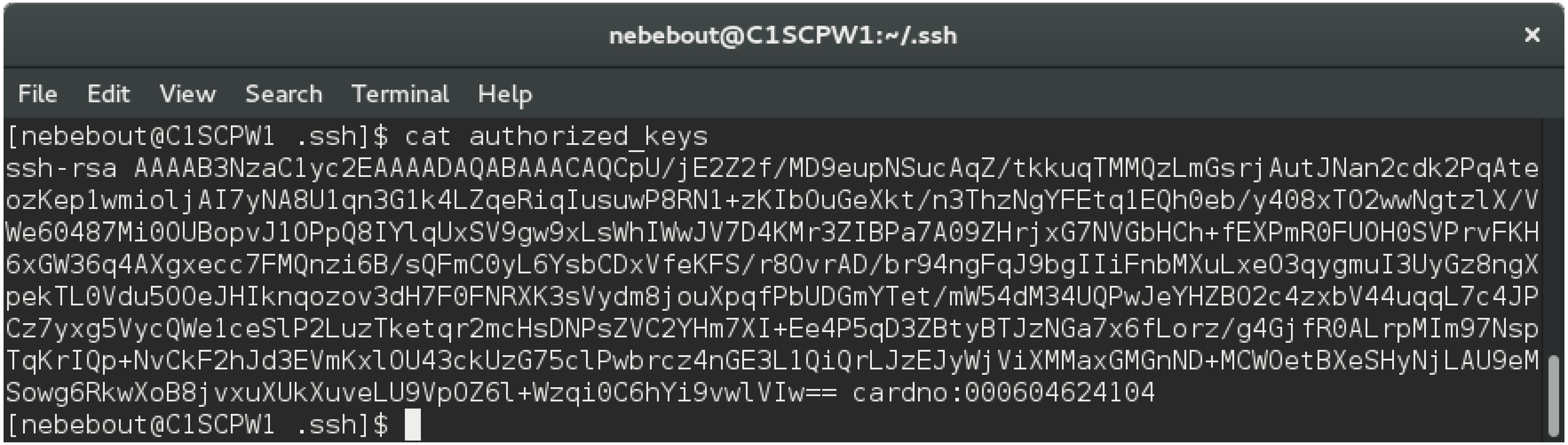
```
[nebebout@C1SCPW1 ~]$ ssh-add -l
4096 SHA256:mDHdtW4CPCd90V5keKJRUp56SjgigM2/JS5reNlexkY cardno:000604624104 (RSA)
[nebebout@C1SCPW1 ~]$ 
```

Output public key in SSH format to put in ~/.ssh/authorized_keys



```
[nebebout@C1SCPW1 ~]$ ssh-add -L
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAACAQCpU/jE2Z2f/MD9eupNSucAqZ/tkkuqTMMQzLmGsrjAutJ
Nan2cdk2PqAteozKep1wmioljAI7yNA8U1qn3G1k4LZqeRiqIusuwP8RN1+zKIbOuGeXkt/n3ThzNgYFEtq
1EQh0eb/y408xTO2wwNgtzlX/VWe60487Mi0OUBopvJ1OPpQ8IYlqUxSV9gw9xLsWhIWwJV7D4KMr3ZIBPa
7A09ZHrjxG7NVGbHCh+fEXPmR0FUOH0SVPrvFKH6xGW36q4AXgxecc7FMQnzi6B/sQFmC0yL6YsbCDxVfeK
FS/r8OvrAD/br94ngFqJ9bgIIiFnbMXuLxeO3qygmuI3UyGz8ngXpekTL0Vdu5OOeJHIknqozov3dH7F0FN
RXK3sVydm8jouXpqfPbUDGmYTet/mW54dM34UQPwJeYHZBO2c4zxbV44uqqL7c4JPCz7yxg5VycQWe1ceSl
P2LuzTketqr2mcHsDNPsZVC2YHm7XI+Ee4P5qD3ZBtyBTJzNGa7x6fLorz/g4GjfR0ALrpMIm97NspTqKrI
Qp+NvCkF2hJd3EVmKxl0U43ckUzG75clPwbrcz4nGE3L1QiQrLJzEJyWjViXMMaxGMGnND+MCWOetBXeSHy
NjLAU9eMSowg6RkwXoB8jvxuXUkXuveLU9VpOZ6l+Wzqi0C6hYi9vwlVIw== cardno:000604624104
[nebebout@C1SCPW1 ~]$ 
```

Put public key in ~/.ssh/authorized_keys



```
[nebebout@C1SCPW1 .ssh]$ cat authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAACAQCpU/jE2Z2f/MD9eupNSucAqZ/tkkuqTMMQzLmGsrjAutJNan2cdk2PqAte
ozKep1wmioljAI7yNA8U1qn3G1k4LZqeRiqIusuwP8RN1+zKIbOuGeXkt/n3ThzNgYFEtq1EQh0eb/y408xTO2wwNgtzlX/V
We60487Mi0OUBopvJ1OPpQ8IYlqUxSV9gw9xLsWhIWwJV7D4KMr3ZIBPa7A09ZHrjxG7NVGbHCh+fEXPmR0FUOH0SVPrvFKH
6xGW36q4AXgxecc7FMQnzi6B/sQFmC0yL6YsbCDxVfeKFS/r8OvrAD/br94ngFqJ9bgIIiFnbMXuLxeO3qygmuI3UyGz8ngX
pekTL0Vdu5OOeJHIknqozov3dH7F0FNRXK3sVydm8jouXpqfPbUDGmYTet/mW54dM34UQPwJeYHZBO2c4zxbV44uqqL7c4JP
Cz7yxg5VycQWe1ceSlP2LuzTketqr2mcHsDNPsZVC2YHm7XI+Ee4P5qD3ZBtyBTJzNGa7x6fLorz/g4GjfR0ALrpMIm97Nsp
TqKrIQp+NvCkF2hJd3EVmKxlOU43ckUzG75clPwbrcz4nGE3L1QiQrLJzEJyWjViXMMaxGMGnND+MCWOetBXeSHyNjLAU9eM
Sowg6RkwXoB8jvxuXUkXuveLU9VpOZ6l+Wzqi0C6hYi9vwlVIw== cardno:000604624104
[nebebout@C1SCPW1 .ssh]$
```

Questions?