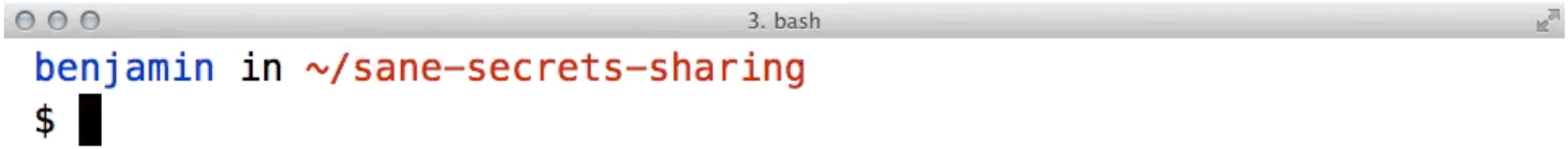
Sane Secrets Sharing



Deal with it

3. bash

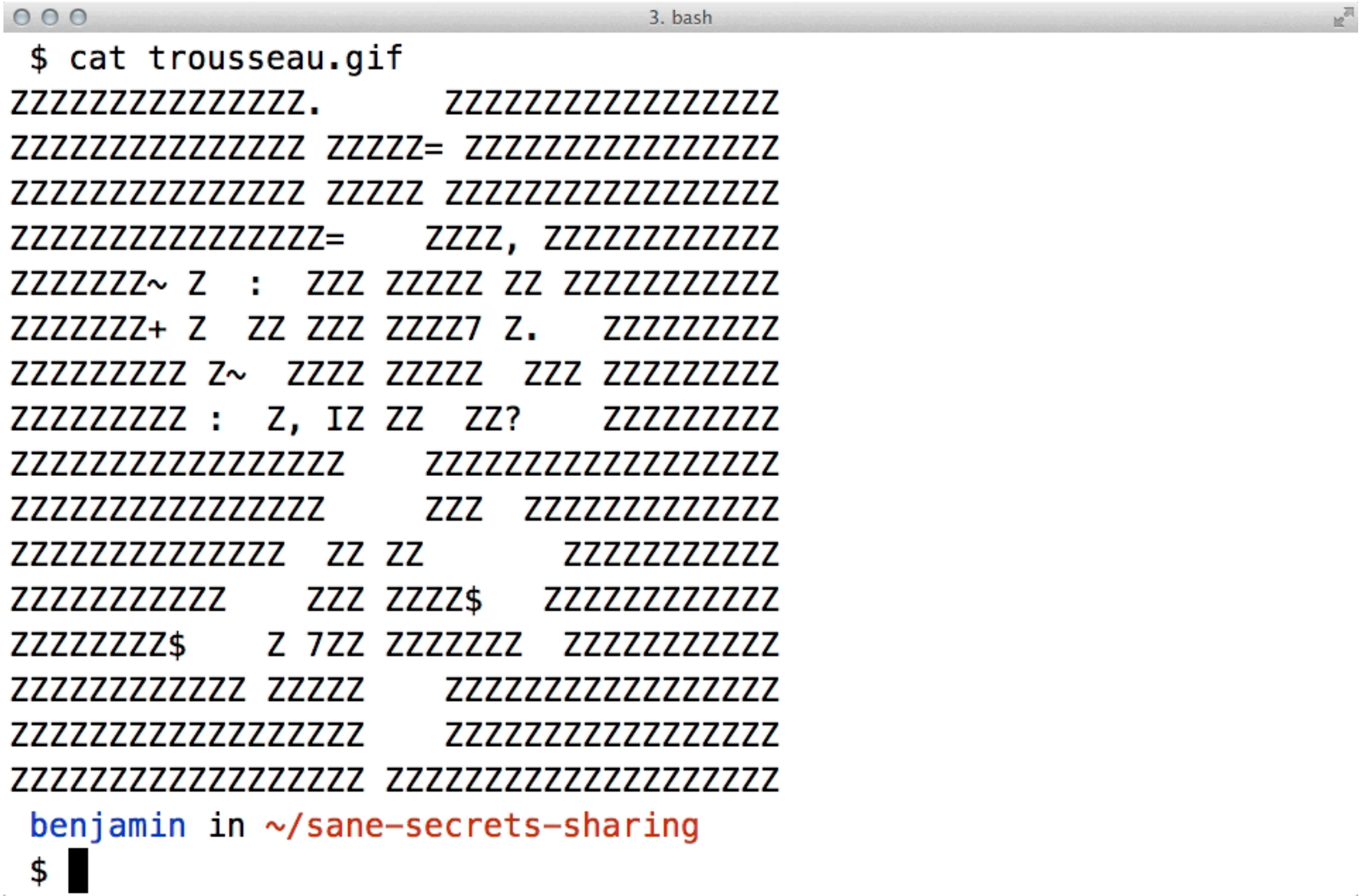
```
benjamin in ~/sane-secrets-sharing
$ cat who-is-benjamin

Hi,

J.B. Rainsberger said about me:
"Benjamin Reitzammer is a pretty smart guy.
You owe it to yourself to see what he has to say.
He lives in Frankfurt."


Who am I to dispute that?


So I only add: I'm @benjamin on Twitter.

benjamin in ~/sane-secrets-sharing
$
```

`trousseau`

3. bash

```
benjamin in ~/sane-secrets-sharing
$ cowsay vaamo
 ________
< vaamo >
 --------
        \   ^__^
         \  (oo)\_______
            (__)\       )\/\
                ||----w |
                ||     ||
benjamin in ~/sane-secrets-sharing
$
```

`trousseau`?



Interacting w/ stores

3. bash

```
 $ trousseau create benjamin.reitzammer@vaamo.de
Trousseau data store succesfully created
 benjamin in ~/sane-secrets-sharing/example
 $ gpg --decrypt trousseau.asc

Sie benötigen eine Passphrase, um den geheimen Schlüssel zu entsperr
en.
Benutzer: "Benjamin Reitzammer <benjamin.reitzammer@vaamo.de>"
2048-Bit RSA Schlüssel, ID F938CCAA, erzeugt 2014-04-22 (Hauptschlüs
sel-ID BD2B61EE)

gpg: verschlüsselt mit 2048-Bit RSA Schlüssel, ID F938CCAA, erzeugt
2014-04-22
      "Benjamin Reitzammer <benjamin.reitzammer@vaamo.de>"
{"KVStore":null,"_meta":{"created_at":"2014-10-20 15:36:57.93878046
+0200 CEST","last_modified_at":"2014-10-20 15:36:57.939730878 +0200
CEST","recipients":["benjamin.reitzammer@vaamo.de"],"version":"0.3.0
"},"data":{}} benjamin in ~/sane-secrets-sharing/example
 $
```

Teams

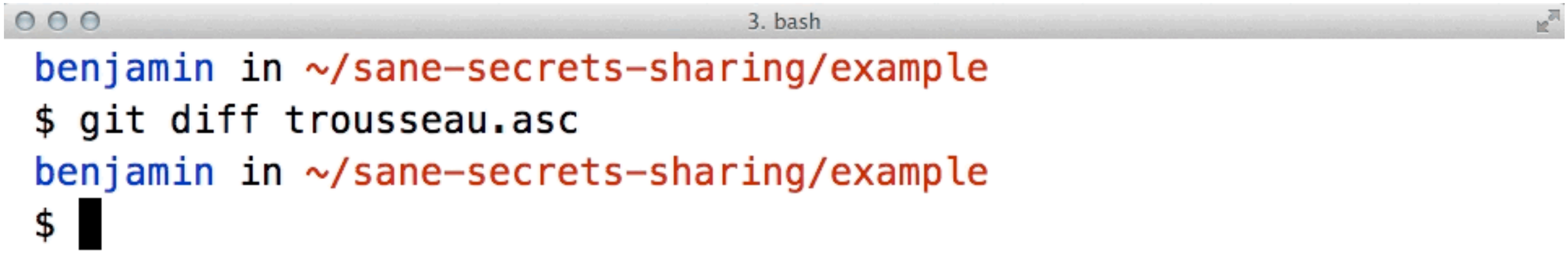
3. bash

```
2048-Bit RSA Schlüssel, ID F938CCAA, erzeugt 2014-04-22 (Hauptschlüs
sel-ID BD2B61EE)

gpg: verschlüsselt mit 2048-Bit RSA Schlüssel, ID F938CCAA, erzeugt
2014-04-22
      "Benjamin Reitzammer <benjamin.reitzammer@vaamo.de>"
{"KVStore":null,"_meta":{"created_at":"2014-10-20 15:42:31.496880834
 +0200 CEST","last_modified_at":"2014-10-20 15:42:31.497270341 +0200
 CEST","recipients":["benjamin.reitzammer@vaamo.de"],"version":"0.3.
0"},"data":{}} benjamin in ~/sane-secrets-sharing/example
 $ trousseau set id_rsa/pass somesecret
 benjamin in ~/sane-secrets-sharing/example
 $ trousseau get id_rsa/pass
somesecret
 benjamin in ~/sane-secrets-sharing/example
 $ trousseau keys
id_rsa/pass
 benjamin in ~/sane-secrets-sharing/example
 $
```

Teams - VCS

```
3. bash
 benjamin in ~/sane-secrets-sharing/example
 $ trousseau meta
CreatedAt : 2014-10-20 15:42:31.496880834 +0200 CEST
LastModifiedAt : 2014-10-20 15:42:31.497270341 +0200 CEST
Recipients : [benjamin.reitzammer@vaamo.de]
TrousseauVersion : 0.3.0
 benjamin in ~/sane-secrets-sharing/example
 $ trousseau add-recipient timo.hirt@vaamo.de
 benjamin in ~/sane-secrets-sharing/example
 $ trousseau meta
CreatedAt : 2014-10-20 15:42:31.496880834 +0200 CEST
LastModifiedAt : 2014-10-20 15:42:31.497270341 +0200 CEST
Recipients : [benjamin.reitzammer@vaamo.de timo.hirt@vaamo.de]
TrousseauVersion : 0.3.0
 benjamin in ~/sane-secrets-sharing/example
 $
```

Teams - Split stores



Teams - Split stores

3. bash

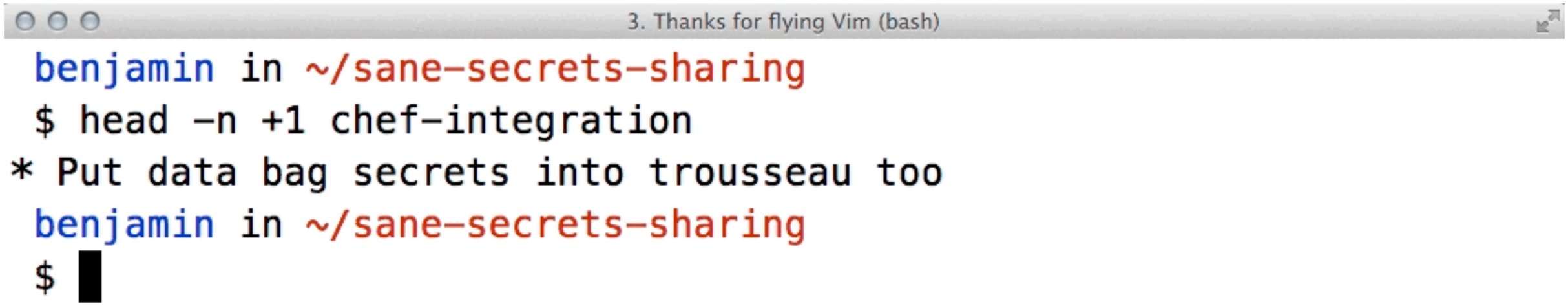
```
benjamin in ~/sane-secrets-sharing/example
$ git diff trousseau.asc
benjamin in ~/sane-secrets-sharing/example
$ cd ..
benjamin in ~/sane-secrets-sharing
$ mkdir weblogins
benjamin in ~/sane-secrets-sharing
$ cd weblogins
benjamin in ~/sane-secrets-sharing/weblogins
$ trousseau create benjamin.reitzammer@vaamo.de
Trousseau data store succesfully created
benjamin in ~/sane-secrets-sharing/weblogins
$ trousseau set squirrel.vaamo.de supersecret
benjamin in ~/sane-secrets-sharing/weblogins
$ trousseau keys
squirrel.vaamo.de
benjamin in ~/sane-secrets-sharing/weblogins
$
```

Integrate w/ Chef

3. bash

```
 $ cd weblogins
 benjamin in ~/sane-secrets-sharing/weblogins
 $ trousseau create benjamin.reitzammer@vaamo.de
Trousseau data store succesfully created
 benjamin in ~/sane-secrets-sharing/weblogins
 $ trousseau set squirrel.vaamo.de supersecret
 benjamin in ~/sane-secrets-sharing/weblogins
 $ trousseau keys
squirrel.vaamo.de
 benjamin in ~/sane-secrets-sharing/weblogins
 $ cd ..
 benjamin in ~/sane-secrets-sharing
 $ (cd example/ && trousseau keys)
id_rsa/pass
 benjamin in ~/sane-secrets-sharing
 $ (cd weblogins/ && trousseau keys)
squirrel.vaamo.de
 benjamin in ~/sane-secrets-sharing
 $
```

Integrate w/ Chef



Integrate w/ Chef

3. Thanks for flying Vim (bash)

```
 benjamin in ~/sane-secrets-sharing
 $ head -n +5 chef-integration
* Put data bag secrets into trousseau too
* deploy encrypted data bag to Chef server
    & data bag secret to target server
* there's no step 3
```

```
benjamin in ~/sane-secrets-sharing
$
```

Integrate w/ Chef

3. Thanks for flying Vim (bash)

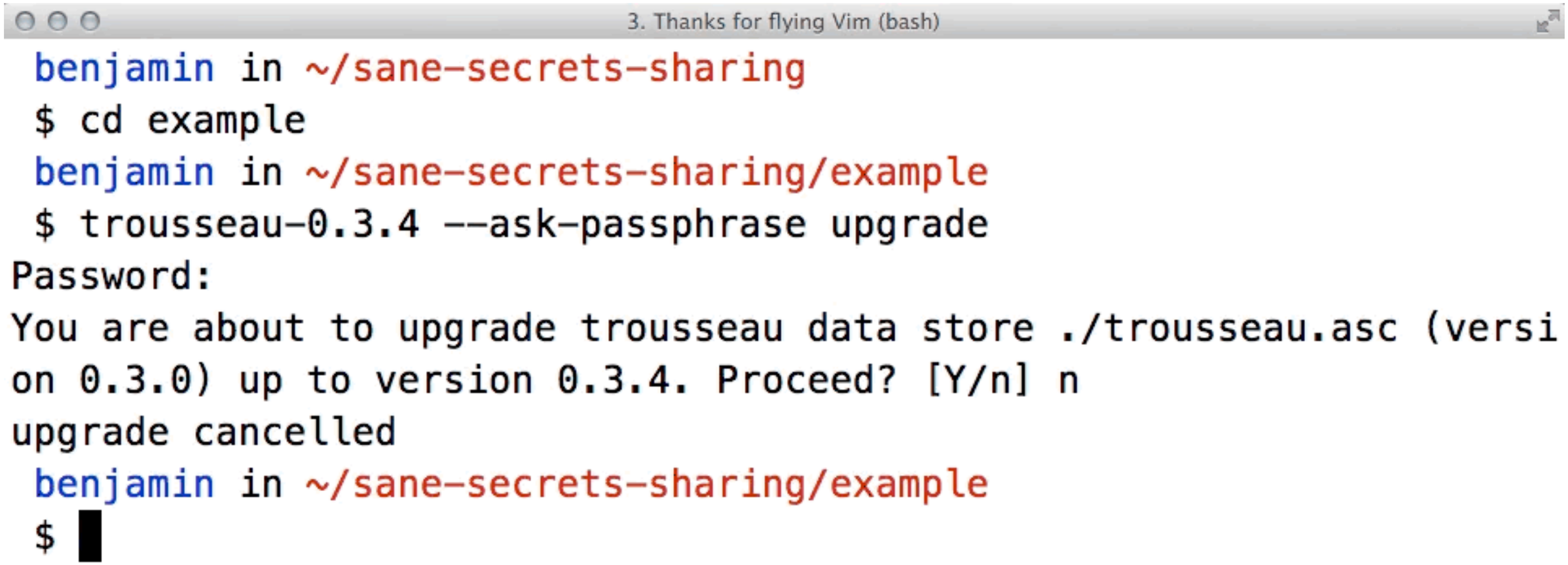
```
benjamin in ~/sane-secrets-sharing
$ tail -n 10 chef-integration

But here are the pros and cons
* pro
    * individual secrets per databag item
    * easy to automate
* con
    * updates to secrets need to be triggered manually
    * principle of least privilege only achievable
      by segregating stores by privilege ... kind of hacky

benjamin in ~/sane-secrets-sharing
$
```

Tips - upgrades

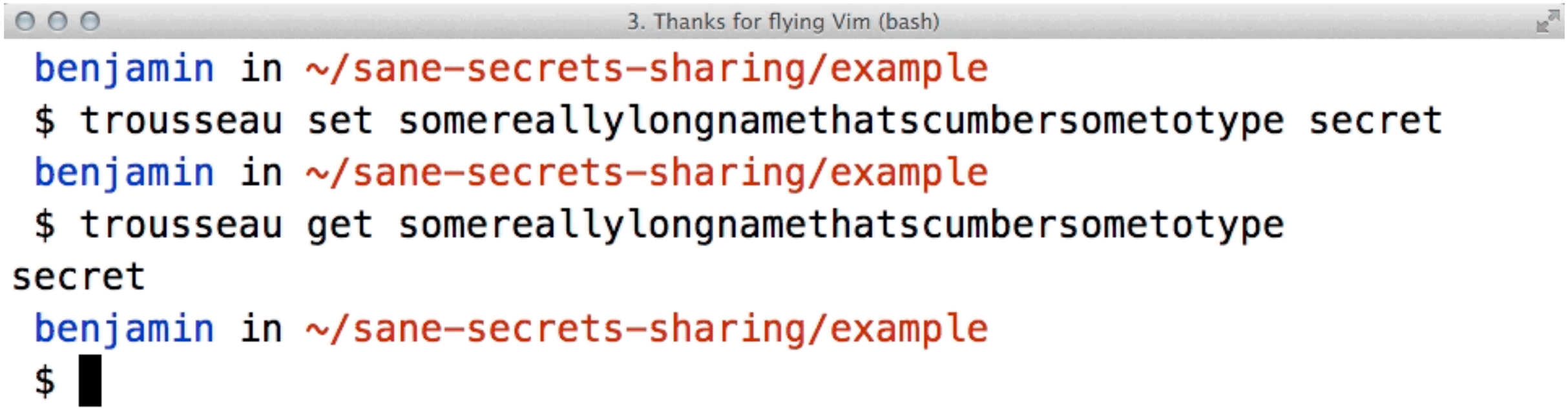
3. Thanks for flying Vim (bash)

```
Available commands:
  certificate      Create/Update encrypted data bag with the corresp
onding certificate for "fqdn".
  dkim             Create/Upload encrypted data bag with DKIM key
  duplicity        Create/Upload encrypted data bag with duplicity p
assphrases
  help             Displays help for a command
  keystore         Create/Upload encrypted data bag with base64 enco
ded binary keystore
  postgresql_user  Create/Upload encrypted data bag with postgresql
user passphrases
  ssh_keypairs     Create/Upload encrypted data bag with ssh public/
private keypairs
  ssh_public_keys  Upload ssh pubkeys to Chef server (unencrypted)

Options:
  -h, --help  Displays this help message
 benjamin in ~/sane-secrets-sharing
 $
```

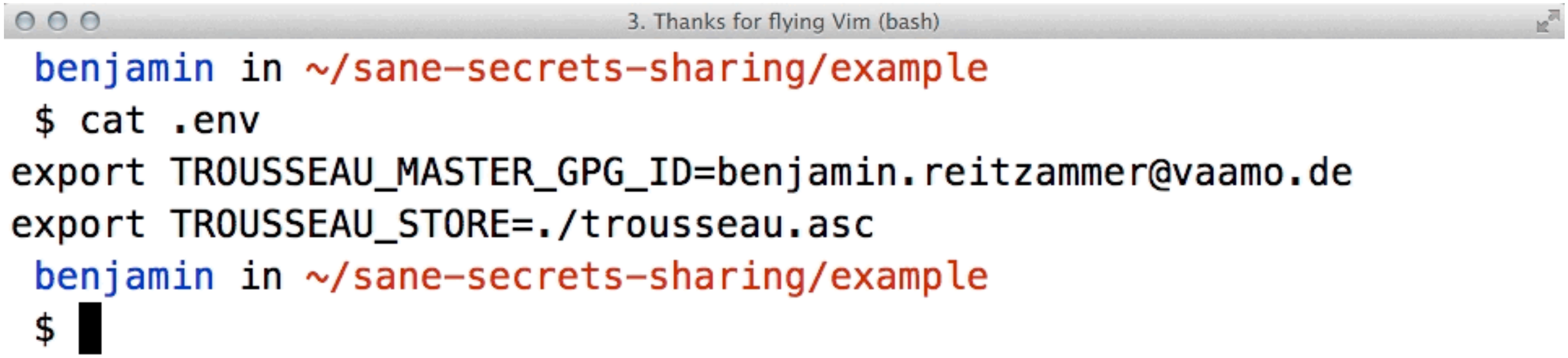
Tips - key completion



Tips - autoenv & Co



Tips - process subst.



Pros & Cons

3. Thanks for flying Vim (bash)

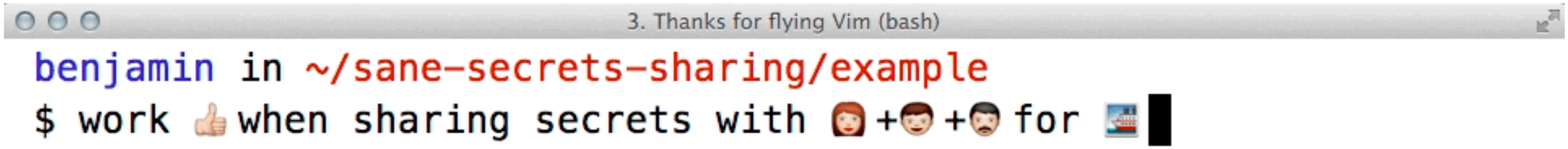
```
 $ ls
id_rsa          id_rsa.pub    trousseau.asc
 benjamin in ~/sane-secrets-sharing/example
 $ trousseau set id_rsa/head --file <(head id_rsa)
 benjamin in ~/sane-secrets-sharing/example
 $ trousseau get id_rsa/head
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,BB2FBE9FFCDFEBA9BCBA752D540C9378

fV35Ga5FSxMofOV/mJtqRPI5A0gDPY2MmuqeTqnmHjHdlUdjXJRj8pUd3IhbckXd
blEYuyatESXmsBieAOsST4oZ5sZqGhGB/IALxT3w9ZpnQIO+S16+czO6nrIItMIR
hzTcuLyupktr2F/o2pqWEznhTU2wgzlENOw1xqkt6GnwTRvUtxtF6VZFdCFcJeai
v4y0v2sW/etd5uXiRwU8pHditf7gomnfy+D5d2RMBACi3PBE921YVSn0lm82ALHp
iRcvfUXxHNZKtap8xSC/HZ3CUEw8oEm5DTw+XiZcMfGO9stTHOFJlhBJb4XCfgGN
MCx12UdgSM7HHmLjevoJf3I0CIuCK6a1v2bVmF8/2mXQeEP1V9mE7PJqpqESSiQ2

 benjamin in ~/sane-secrets-sharing/example
 $
```

TL;DR

3. Thanks for flying Vim (bash)

```
 benjamin in ~/sane-secrets-sharing/example
 $ vi pros-and-cons
 benjamin in ~/sane-secrets-sharing/example
 $ cat pros-and-cons

PROS
* simplicity
* just works
* secure foundation with GPG

CONS
* requires discipline and some tailoring
* trousseau as a tool is still quite young
 benjamin in ~/sane-secrets-sharing/example
 $
```

Thanks!


3. Thanks for flying Vim (bash)
benjamin in ~/sane-secrets-sharing/example
$ work 👍 when sharing secrets with 👩 +👦 +👨 for 🚢