

GPG keys and the Web of Trust

Christian Perrier

Thailand MiniDebconf 2010, Khon Kaen, Thailand



1 GPG keys



1 GPG keys



Purpose of GPG keys

Cipher data

Authenticate data (by signing it)

All important actions in Debian are signed by GPG keys

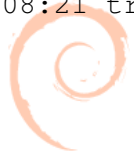


Key handling

```
bubulle@mykerinos:~/.gnupg$ LC_ALL=C ls -la
```

```
total 8232
```

```
drwx----- 6 bubulle bubulle 4096 Mar 16 08:42 .
drwxr-xr-x 137 bubulle bubulle 8192 Mar 16 07:55 ..
-rw-r--r-- 1 bubulle bubulle 267 Aug 23 2009 gn
-rw----- 1 bubulle bubulle 8187258 Mar 16 08:21 pu
-rw----- 1 bubulle bubulle 600 Mar 16 08:15 ra
-rw-rw-r-- 1 bubulle bubulle 283 Sep 12 2005 re
-rw----- 1 bubulle bubulle 10970 Mar 16 08:21 se
-rw-rw-r-- 1 bubulle bubulle 150960 Mar 16 08:21 tr
```



Key handling: good practices

Create a revocations certificate

Store it SECURELY

Take care of secring.gpg (encrypted removable media)



What does signing a key mean?

I have verified this person's identity as best as I could

I verified this identity with a government-issued ID or anything else I have trust into

I know that this person controls the mail address in the key ID



What does signing a key NOT mean?

I put my trust in this person

This person is my friend

(debated) I trust this person's ability to handle his—her key properly



Typical signature process: signee

Alice gives to Bob a printed or handwritten copy of her fingerprint

This copy carries her name AND e-mail address

She confirms Bob that she verified that the fingerprint she's giving out in hers and was not tampered

She gives Bob a government-issued ID, preferably checking with him that he has trust in that kind of ID

Typical signature process: signer

Bob reads Alice's name on the fingerprint copy

He COMPARES this to the name on the ID

He checks the validity of the ID to the best of his abilities (exp. date, logos, holograms)

He records somewhere (eventually his mind) whether he decides to sign the key or not

Signing the collected keys

apt-get install signing-party

Use caff

REALLY CHECK fingerprints

I mean, REALLY



Sending the signed keys

NEVER reupload signed keys to keyservers

Send the key to the signee in an encrypted mail

Use caff



Be serious in keysigning parties

Your trust is believed

Really carefully check identities

Accept other people's policies



Be serious in keysigning parties

Welcome to the Web of Trust

