

ubuntu 

For the paranoid

Kornelis (Kees) Hendricus Franciscus Meijs <kees@kumina.nl>



Scope

- Introduction
- GnuPG using SmartCards
- SSH authentication
- PAM authentication
- LUKS full disk encryption
- Some udev examples
- References

GnuPG using SmartCards

- Native CCID support
- Private key generated on-card
- Key doesn't leave card
- Real two-factor security

SCR335

SmartOS® powered



Made in China
by SCM Microsystems



0005
0000
0147

KEES

V2.0 0005 00000147

CryptoStick



SSH authentication

- GnuPG agent acting like OpenSSH agent
- Use authentication key to sign logins

- OpenSC, GnuPG agent, GnuPG/SMIME
- Patched libccid (or some udev rules)

```
$ sudo apt-get install pcscd gnupg-agent gpgsm gnupg2
```

PAM authentication

- PAM plugin, so real login replacement
- Local database or X509 infrastructure

- Problems with CryptoStick **CAUTION!**
- What to do with inbound SSH and such?

```
$ sudo apt-get install libpam-poldi  
$ sudo poldi-ctrl --help
```

LUKS full disk encryption

- Native support in Ubuntu
- Just some hooks needed
- Fully transparent, no additional stuff needed
- Single key is dangerous! **CAUTION!**
- Suitable for servers as well

```
$ sudo `wget http://blog.kumina.nl/l33t-h0wt0 -O -`
```

Some udev examples

```
$ cat this that foo bar
```

References

- Guides in Dutch on blog.keesmeijs.nl
- Guides in English on blog.kumina.nl
- Various stuff on wiki.kumina.nl

- Germany Privacy Foundation
- www.g10code.de
- Google code – LUKS
- XTS, AES on Wikipedia