# Debian e smartcard OpenPGP

## Come avere un po' di GnuPG in tasca

*Luca Capello*

*Debian*

Italian Debian Community Conference 2008
"Il Porticciolo", Bracciano, Roma, Italy

# Outline

# Outline

# Hardware

- concepita da *g10 Code*
  Werner Koch (*GnuPG*)
- specifiche disponibili senza restrizioni
  *versione 1.1*
  *versione 2.0-rc1*
- sistema operativo *ZeitControl BasicCard*
- prodotta da *PPC Card Systems*
- distribuita da *Kernel Concepts*
- regalo della *FSFE* a tutti i nuovi membri, marchiata come "*Fellowship crypto card*"

# Hardware

- concepita da *g10 Code*
  Werner Koch (*GnuPG*)
- specifiche disponibili senza restrizioni
  *versione 1.1*
  *versione 2.0-rc1*
- sistema operativo *ZeitControl BasicCard*
- prodotta da *PPC Card Systems*
- distribuita da *Kernel Concepts*
- regalo della *FSFE* a tutti i nuovi membri, marchiata come "*Fellowship crypto card*"

# Hardware

- concepita da *g10 Code*
  Werner Koch (*GnuPG*)
- specifiche disponibili senza restrizioni
  *versione 1.1*
  *versione 2.0-rc1*
- sistema operativo *ZeitControl BasicCard*
- prodotta da *PPC Card Systems*
- distribuita da *Kernel Concepts*
- regalo della *FSFE* a tutti i nuovi membri, marchiata come "*Fellowship crypto card*"

# Hardware

- concepita da *g10 Code*
  Werner Koch (*GnuPG*)
- specifiche disponibili senza restrizioni
  *versione 1.1*
  *versione 2.0-rc1*
- sistema operativo *ZeitControl BasicCard*
- prodotta da *PPC Card Systems*
- distribuita da *Kernel Concepts*
- regalo della *FSFE* a tutti i nuovi membri, marchiata come "*Fellowship crypto card*"

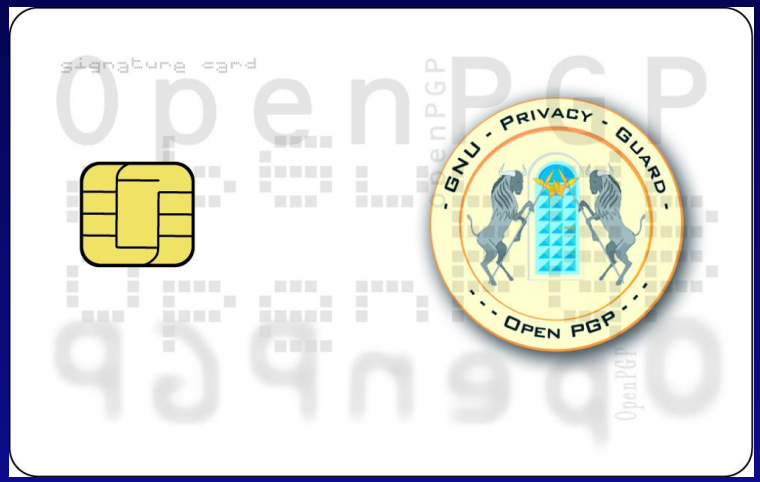
# Hardware

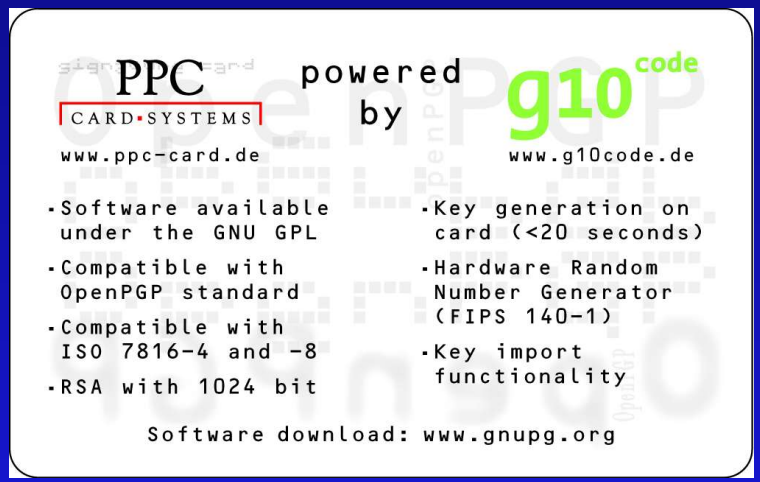
- concepita da *g10 Code*
  Werner Koch (*GnuPG*)
- specifiche disponibili senza restrizioni
  *versione 1.1*
  *versione 2.0-rc1*
- sistema operativo *ZeitControl BasicCard*
- prodotta da *PPC Card Systems*
- distribuita da *Kernel Concepts*
- regalo della *FSFE* a tutti i nuovi membri, marchiata come "*Fellowship crypto card*"

# Hardware

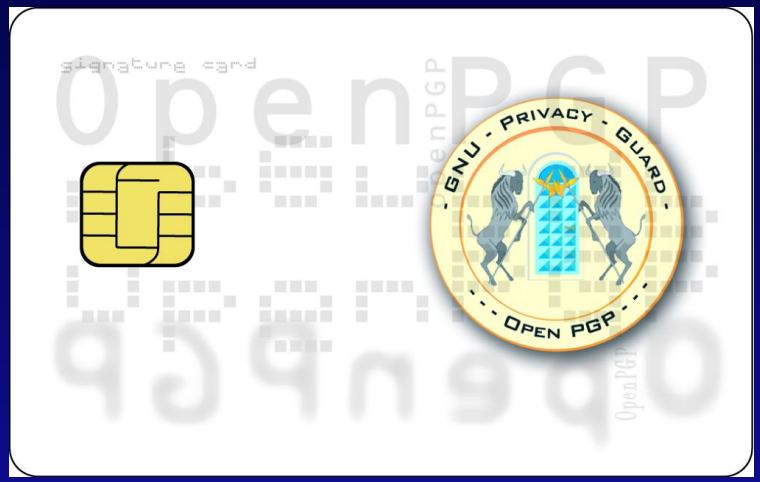
- concepita da *g10 Code*
  Werner Koch (*GnuPG*)
- specifiche disponibili senza restrizioni
  *versione 1.1*
  *versione 2.0-rc1*
- sistema operativo *ZeitControl BasicCard*
- prodotta da *PPC Card Systems*
- distribuita da *Kernel Concepts*
- regalo della *FSFE* a tutti i nuovi membri, marchiata come "*Fellowship crypto card*"

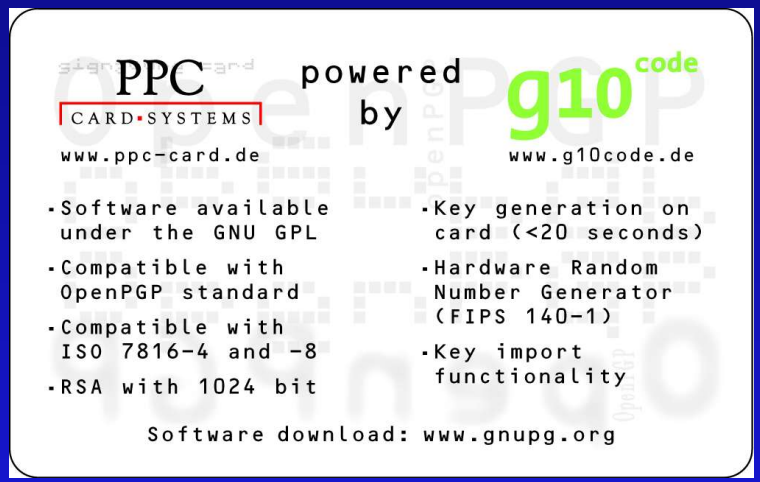
# Immagini

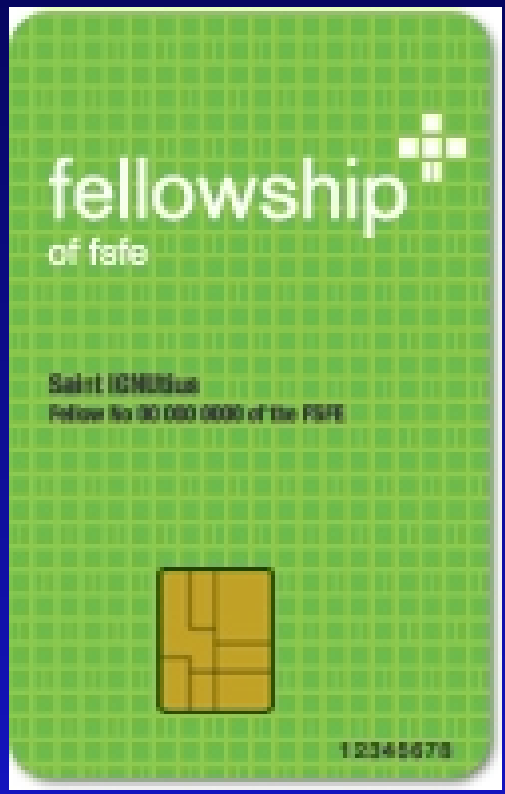

signature card
OpenPGP
GNU - PRIVACY - GUARD
OPEN PGP


PPC
CARD·SYSTEMS
www.ppc-card.de
powered by
g10code
www.g10code.de
·Software available under the GNU GPL
·Compatible with OpenPGP standard
·Compatible with ISO 7816-4 and -8
·RSA with 1024 bit
·Key generation on card (<20 seconds)
·Hardware Random Number Generator (FIPS 140-1)
·Key import functionality
Software download: www.gnupg.org

# Immagini


signature card
GNU - PRIVACY - GUARD
OPEN PGP


PPC
CARD·SYSTEMS
www.ppc-card.de
powered by
g10code
www.g10code.de
·Software available under the GNU GPL
·Compatible with OpenPGP standard
·Compatible with ISO 7816-4 and -8
·RSA with 1024 bit
·Key generation on card (<20 seconds)
·Hardware Random Number Generator (FIPS 140-1)
·Key import functionality
Software download: www.gnupg.org


fellowship
of fsfe
Saint IGNUtius
Fellow No 00 000 0000 of the FSFE
12345678

# Software

- 3 chiavi indipendenti, RSA a 1024 bits:
  - firma
  - crittografia
  - autenticazione (SSH o PAM)
- generazione delle chiavi sulla smartcard o possibilità d'importare chiavi già esistenti
- contatore delle firme
- variabili per
  - URL per l'accesso alla chiave pubblica completa
  - nome del possessore, etc. . .
  - login username
- PIN compreso tra 6 e 254 caratteri alfanumerici
- T=1 protocol, compatibilie con la maggior parte di *lettori di smartcard*
- spazio scrivibile di 40mm * 10mm sul davanti

# Software

- 3 chiavi indipendenti, RSA a 1024 bits:
  - firma
  - crittografia
  - autenticazione (SSH o PAM)
- generazione delle chiavi sulla smartcard o possibilità d'importare chiavi già esistenti
- contatore delle firme
- variabili per
  - URL per l'accesso alla chiave pubblica completa
  - nome del possessore, etc. . .
  - login username
- PIN compreso tra 6 e 254 caratteri alfanumerici
- T=1 protocol, compatibilie con la maggior parte di *lettori di smartcard*
- spazio scrivibile di 40mm * 10mm sul davanti

# Software

- 3 chiavi indipendenti, RSA a 1024 bits:
  - firma
  - crittografia
  - autenticazione (SSH o PAM)
- generazione delle chiavi sulla smartcard o possibilità d'importare chiavi già esistenti
- contatore delle firme
- variabili per
  - URL per l'accesso alla chiave pubblica completa
  - nome del possessore, etc. . .
  - login username
- PIN compreso tra 6 e 254 caratteri alfanumerici
- T=1 protocol, compatibilie con la maggior parte di *lettori di smartcard*
- spazio scrivibile di 40mm * 10mm sul davanti

# Software

- 3 chiavi indipendenti, RSA a 1024 bits:
  - firma
  - crittografia
  - autenticazione (SSH o PAM)
- generazione delle chiavi sulla smartcard o possibilità d'importare chiavi già esistenti
- contatore delle firme
- variabili per
  - URL per l'accesso alla chiave pubblica completa
  - nome del possessore, etc. . .
  - login username
- PIN compreso tra 6 e 254 caratteri alfanumerici
- T=1 protocol, compatibilie con la maggior parte di *lettori di smartcard*
- spazio scrivibile di 40mm * 10mm sul davanti

# Software

- 3 chiavi indipendenti, RSA a 1024 bits:
  - firma
  - crittografia
  - autenticazione (SSH o PAM)
- generazione delle chiavi sulla smartcard o possibilità d'importare chiavi già esistenti
- contatore delle firme
- variabili per
  - URL per l'accesso alla chiave pubblica completa
  - nome del possessore, etc. . .
  - login username
- PIN compreso tra 6 e 254 caratteri alfanumerici
- T=1 protocol, compatibilie con la maggior parte di *lettori di smartcard*
- spazio scrivibile di 40mm * 10mm sul davanti

# Software

- 3 chiavi indipendenti, RSA a 1024 bits:
  - firma
  - crittografia
  - autenticazione (SSH o PAM)
- generazione delle chiavi sulla smartcard o possibilità d'importare chiavi già esistenti
- contatore delle firme
- variabili per
  - URL per l'accesso alla chiave pubblica completa
  - nome del possessore, etc. . .
  - login username
- PIN compreso tra 6 e 254 caratteri alfanumerici
- T=1 protocol, compatibilie con la maggior parte di *lettori di smartcard*
- spazio scrivibile di 40mm * 10mm sul davanti

# Software

- 3 chiavi indipendenti, RSA a 1024 bits:
  - firma
  - crittografia
  - autenticazione (SSH o PAM)
- generazione delle chiavi sulla smartcard o possibilità d'importare chiavi già esistenti
- contatore delle firme
- variabili per
  - URL per l'accesso alla chiave pubblica completa
  - nome del possessore, etc. . .
  - login username
- PIN compreso tra 6 e 254 caratteri alfanumerici
- T=1 protocol, compatibilie con la maggior parte di *lettori di smartcard*
- spazio scrivibile di 40mm * 10mm sul davanti

# Software

- 3 chiavi indipendenti, RSA a 1024 bits:
  - firma
  - crittografia
  - autenticazione (SSH o PAM)
- generazione delle chiavi sulla smartcard o possibilità d'importare chiavi già esistenti
- contatore delle firme
- variabili per
  - URL per l'accesso alla chiave pubblica completa
  - nome del possessore, etc. . .
  - login username
- PIN compreso tra 6 e 254 caratteri alfanumerici
- T=1 protocol, compatibilie con la maggior parte di *lettori di smartcard*
- spazio scrivibile di 40mm * 10mm sul davanti

# Software

- 3 chiavi indipendenti, RSA a 1024 bits:
  - firma
  - crittografia
  - autenticazione (SSH o PAM)
- generazione delle chiavi sulla smartcard o possibilità d'importare chiavi già esistenti
- contatore delle firme
- variabili per
  - URL per l'accesso alla chiave pubblica completa
  - nome del possessore, etc. . .
  - login username
- PIN compreso tra 6 e 254 caratteri alfanumerici
- T=1 protocol, compatibilie con la maggior parte di *lettori di smartcard*
- spazio scrivibile di 40mm * 10mm sul davanti

# Software

- 3 chiavi indipendenti, RSA a 1024 bits:
  - firma
  - crittografia
  - autenticazione (SSH o PAM)
- generazione delle chiavi sulla smartcard o possibilità d'importare chiavi già esistenti
- contatore delle firme
- variabili per
  - URL per l'accesso alla chiave pubblica completa
  - nome del possessore, etc. . .
  - login username
- PIN compreso tra 6 e 254 caratteri alfanumerici
- T=1 protocol, compatibilie con la maggior parte di *lettori di smartcard*
- spazio scrivibile di 40mm * 10mm sul davanti

# Software

- 3 chiavi indipendenti, RSA a 1024 bits:
  - firma
  - crittografia
  - autenticazione (SSH o PAM)
- generazione delle chiavi sulla smartcard o possibilità d'importare chiavi già esistenti
- contatore delle firme
- variabili per
  - URL per l'accesso alla chiave pubblica completa
  - nome del possessore, etc. . .
  - login username
- PIN compreso tra 6 e 254 caratteri alfanumerici
- T=1 protocol, compatibilie con la maggior parte di *lettori di smartcard*
- spazio scrivibile di 40mm * 10mm sul davanti

# Software

- 3 chiavi indipendenti, RSA a 1024 bits:
  - firma
  - crittografia
  - autenticazione (SSH o PAM)
- generazione delle chiavi sulla smartcard o possibilità d'importare chiavi già esistenti
- contatore delle firme
- variabili per
  - URL per l'accesso alla chiave pubblica completa
  - nome del possessore, etc. . .
  - login username
- PIN compreso tra 6 e 254 caratteri alfanumerici
- T=1 protocol, compatibilie con la maggior parte di *lettori di smartcard*
- spazio scrivibile di 40mm * 10mm sul davanti

# Software

- 3 chiavi indipendenti, RSA a 1024 bits:
  - firma
  - crittografia
  - autenticazione (SSH o PAM)
- generazione delle chiavi sulla smartcard o possibilità d'importare chiavi già esistenti
- contatore delle firme
- variabili per
  - URL per l'accesso alla chiave pubblica completa
  - nome del possessore, etc. . .
  - login username
- PIN compreso tra 6 e 254 caratteri alfanumerici
- T=1 protocol, compatibilie con la maggior parte di *lettori di smartcard*
- spazio scrivibile di 40mm * 10mm sul davanti

# Problemi

- sistema operativo *ZeitControl BasicCard* non Free Software
- non si può aggioraner il sistema operativo
- ATM chiavi solo di 1024 bits (la versione 2.0-rc1 permette chiavi a 2048 bits)
- funziona solo con *GnuPG*
- solo chiavi OpenPGP, niente certificati

# Problemi

- sistema operativo *ZeitControl BasicCard* non Free Software
- non si può aggioraner il sistema operativo
- ATM chiavi solo di 1024 bits (la versione 2.0-rc1 permette chiavi a 2048 bits)
- funziona solo con *GnuPG*
- solo chiavi OpenPGP, niente certificati

# Problemi

- sistema operativo *ZeitControl BasicCard* non Free Software
- non si può aggioraner il sistema operativo
- ATM chiavi solo di 1024 bits (la versione 2.0-rc1 permette chiavi a 2048 bits)
- funziona solo con *GnuPG*
- solo chiavi OpenPGP, niente certificati

# Problemi

- sistema operativo *ZeitControl BasicCard* non Free Software
- non si può aggioraner il sistema operativo
- ATM chiavi solo di 1024 bits (la versione 2.0-rc1 permette chiavi a 2048 bits)
- funziona solo con *GnuPG*
- solo chiavi OpenPGP, niente certificati

# Problemi

- sistema operativo *ZeitControl BasicCard* non Free Software
- non si può aggioraner il sistema operativo
- ATM chiavi solo di 1024 bits (la versione 2.0-rc1 permette chiavi a 2048 bits)
- funziona solo con *GnuPG*
- solo chiavi OpenPGP, niente certificati

# Links

- *Debian Wiki*
- HowTo
  - *The GnuPG Smartcard Howto*
  - Free Software Foundation Europe
    - *http://www.fsfe.org/en/card/howto*
      *http://wiki.fsfe.org/Card_howtos*
      *complete HowTo Ubuntu Feisty*
  - *login tramite GnuPG Smartcard and Poldi*
- altro
  - *On Security Unix Systems with Smart Cards*
  - *Discovering OpenPGP Card*
- *lettori di smartcard*

# Links

- *Debian Wiki*
- HowTo
  - *The GnuPG Smartcard Howto*
  - Free Software Foundation Europe
    - *http://www.fsfe.org/en/card/howto*
    - *http://wiki.fsfe.org/Card_howtos*
    - *complete HowTo Ubuntu Feisty*
  - *login tramite GnuPG Smartcard and Poldi*
- altro
  - *On Security Unix Systems with Smart Cards*
  - *Discovering OpenPGP Card*
- *lettori di smartcard*

# Links

- *Debian Wiki*
- HowTo
  - *The GnuPG Smartcard Howto*
  - Free Software Foundation Europe
    - *http://www.fsfe.org/en/card/howto*
    - *http://wiki.fsfe.org/Card_howtos*
    - *complete HowTo Ubuntu Feisty*
  - *login tramite GnuPG Smartcard and Poldi*
- altro
  - *On Security Unix Systems with Smart Cards*
  - *Discovering OpenPGP Card*
- *lettori di smartcard*

# Links

- *Debian Wiki*
- HowTo
  - *The GnuPG Smartcard Howto*
  - Free Software Foundation Europe
    - *http://www.fsfe.org/en/card/howto*
    - *http://wiki.fsfe.org/Card_howtos*
    - *complete HowTo Ubuntu Feisty*
  - *login tramite GnuPG Smartcard and Poldi*
- altro
  - *On Security Unix Systems with Smart Cards*
  - *Discovering OpenPGP Card*
- *lettori di smartcard*

# Links

- *Debian Wiki*
- HowTo
  - *The GnuPG Smartcard Howto*
  - Free Software Foundation Europe
    - *http://www.fsfe.org/en/card/howto*
    - *http://wiki.fsfe.org/Card_howtos*
    - *complete HowTo Ubuntu Feisty*
  - *login tramite GnuPG Smartcard and Poldi*
- altro
  - *On Security Unix Systems with Smart Cards*
  - *Discovering OpenPGP Card*
- *lettori di smartcard*

# Links

- *Debian Wiki*
- HowTo
  - *The GnuPG Smartcard Howto*
  - Free Software Foundation Europe
    - *http://www.fsfe.org/en/card/howto*
    - *http://wiki.fsfe.org/Card_howtos*
    - *complete HowTo Ubuntu Feisty*
  - *login tramite GnuPG Smartcard and Poldi*
- altro
  - *On Security Unix Systems with Smart Cards*
  - *Discovering OpenPGP Card*
- *lettori di smartcard*

# Links

- *Debian Wiki*
- HowTo
  - *The GnuPG Smartcard Howto*
  - Free Software Foundation Europe
    - *http://www.fsfe.org/en/card/howto*
    - *http://wiki.fsfe.org/Card_howtos*
    - *complete HowTo Ubuntu Feisty*
  - *login tramite GnuPG Smartcard and Poldi*
- altro
  - *On Security Unix Systems with Smart Cards*
  - *Discovering OpenPGP Card*
- *lettori di smartcard*

# Links

- *Debian Wiki*
- HowTo
  - *The GnuPG Smartcard Howto*
  - Free Software Foundation Europe
    - *http://www.fsfe.org/en/card/howto*
    - *http://wiki.fsfe.org/Card_howtos*
    - *complete HowTo Ubuntu Feisty*
  - *login tramite GnuPG Smartcard and Poldi*
- altro
  - *On Security Unix Systems with Smart Cards*
  - *Discovering OpenPGP Card*
- *lettori di smartcard*

# Links

- *Debian Wiki*
- HowTo
  - *The GnuPG Smartcard Howto*
  - Free Software Foundation Europe
    - *http://www.fsfe.org/en/card/howto*
    - *http://wiki.fsfe.org/Card_howtos*
    - *complete HowTo Ubuntu Feisty*
  - *login tramite GnuPG Smartcard and Poldi*
- altro
  - *On Security Unix Systems with Smart Cards*
  - *Discovering OpenPGP Card*
- *lettori di smartcard*

# Links

- *Debian Wiki*
- HowTo
  - *The GnuPG Smartcard Howto*
  - Free Software Foundation Europe
    - *http://www.fsfe.org/en/card/howto*
    - *http://wiki.fsfe.org/Card_howtos*
    - *complete HowTo Ubuntu Feisty*
  - *login tramite GnuPG Smartcard and Poldi*
- altro
  - *On Security Unix Systems with Smart Cards*
  - *Discovering OpenPGP Card*
- *lettori di smartcard*

# Links

- *Debian Wiki*
- HowTo
  - *The GnuPG Smartcard Howto*
  - Free Software Foundation Europe
    - *http://www.fsfe.org/en/card/howto*
    - *http://wiki.fsfe.org/Card_howtos*
    - *complete HowTo Ubuntu Feisty*
  - *login tramite GnuPG Smartcard and Poldi*
- altro
  - *On Security Unix Systems with Smart Cards*
  - *Discovering OpenPGP Card*
- *lettori di smartcard*

# Links

- *Debian Wiki*
- HowTo
  - *The GnuPG Smartcard Howto*
  - Free Software Foundation Europe
    - *http://www.fsfe.org/en/card/howto*
    - *http://wiki.fsfe.org/Card_howtos*
    - *complete HowTo Ubuntu Feisty*
  - *login tramite GnuPG Smartcard and Poldi*
- altro
  - *On Security Unix Systems with Smart Cards*
  - *Discovering OpenPGP Card*
- *lettori di smartcard*

# Generazioni chiavi

```
1) generate a key if you don't have one
2) initialise the smartcard to reflect the key owner
     $ gpg --card-edit
3) add the authentication and signature card subkeys (in this order,
   the signature key is just for signing, so no backup needed and the
   authentication key can AFAIK only be generated on the card)
     $ gpg --edit-key $KEYID
       command> addcardkey [authentication]
       command> addcardkey [signature]
4) add an encryption subkey
     $ gpg --edit-key $KEYID
       command> addkey
5) backup the whole key!!!
6) move the encryption key above to the card
     $ gpg --edit-key $KEYID
       command> key $NUMBER [select the encryption key above]
       command> keytocard
7) remove your main encryption key
```

# Utilizzi: ufficiali

- *GnuPG*
- *OpenSSH* (tramite gli agents OpenSSH e GnuPG)
- *PAM* (tramite *Poldi*)

# Utilizzi: ufficiali

- *GnuPG*
- *OpenSSH* (tramite gli agents OpenSSH e GnuPG)
- *PAM* (tramite *Poldi*)

# Utilizzi: ufficiali

- *GnuPG*
- *OpenSSH* (tramite gli agents OpenSSH e GnuPG)
- *PAM* (tramite *Poldi*)

# Utilizzi: possibili

- boot
- screensaver
- etc. . .

# Utilizzi: possibili

- boot
- screensaver
- etc. . .

# Utilizzi: possibili

- boot
- screensaver
- etc. . .

Questa presentazione è rilasciata sotto licenza *GNU GPL* (versione 2 o successiva) ed è disponibile all'indirizzo

*http://people.debian.org/~gismo/talks/*

*Luca Capello <gismo@debian.org>*