

## Note per l'installazione di DiKe 4.2.2 L

### 1 Prerequisiti

- Distribuzione Linux:
  - Ubuntu 7.10/8.04/8.10
  - Fedora 10
- Driver del lettore di smart card in uso.

#### 1.1 *Installazione pcsc-tools*

L'installazione di questo pacchetto non è tecnicamente necessaria: si rivela però assai utile per verificare che il sistema veda correttamente sia i lettori che le smart card. Nell'*allegato A* è possibile trovare alcune note di utilizzo.

##### 1.1.1 Ubuntu

Il pacchetto **pcsc-tools** si trova nel repository *Universe*. Questo pacchetto installa anche i seguenti pacchetti:

- **libpcsc-perl**, interfaccia perl alle funzioni di libreria di pcsc
- **libcairo-perl**
- **libglib-perl**
- **libgtk2-perl**

##### 1.1.2 Fedora

Il pacchetto **pcsc-tools** installa i seguenti pacchetti:

- **pcsc-perl**, interfaccia perl alle funzioni di libreria di pcsc,
- **perl-cairo**,
- **perl-Glib**,
- **perl-Gtk2**.

### 2 Lettore di smart card

Come lettore di smart card si consiglia di utilizzare il modello ACR38U, solitamente marchiato Bit4Id 38U o ACS 38U: si tratta di un HW affidabile, in generale ben supportato su GNU/Linux.

E' possibile, comunque, utilizzare anche altri lettori; preconditione è che questi siano supportati dai pacchetti **pcsc**.

**ATTENZIONE:** i driver per il lettore ACR38U sono stati aggiornati per correggere alcune malfunzioni. I driver corretti sono presenti sul sito

[http://www.firma.infocert.it/installazione/installazione\\_DiKe.php](http://www.firma.infocert.it/installazione/installazione_DiKe.php)

**Tale aggiornamento driver non è ancora presente nei repository ufficiali delle distribuzioni Linux.**

### **3 Installazione del programma Dike per Linux**

Scaricare il programma dal sito <http://www.firma.infocert.it>; scaricare il pacchetto nel formato della propria distribuzione e procedere all'installazione.

Il pacchetto ha installa (per dipendenza) tutto il software necessario al funzionamento.

Esecuzione del programma:

- da riga di comando sarà disponibile il comando “dike”
- dal menu “Other” (oppure “Altro”, dipende dalla lingua di installazione) cliccare sull'icona Dike.

## 4 Allegato A

I lettori necessitano di un driver SW in grado di gestirli; una serie di driver per lettori USB sono installati con il pacchetto *ccid*, presente nelle distribuzioni considerate.

Per le proprietà e modello del lettore è possibile utilizzare il comando *lsusb*. Si veda il seguente esempio:

```
mario@mambo:~$ lsusb
Bus 002 Device 001: ID 0000:0000
Bus 001 Device 003: ID 072f:9000 Advanced Card Systems, Ltd ACR38 AC1038-based Smart Card Reader
Bus 001 Device 002: ID 0e0f:0002
Bus 001 Device 001: ID 0000:0000
```

Il comando *pcsc\_scan*, incluso nel pacchetto *pcsc-tools*, è molto utile sia per verificare che il lettore sia visto dal resource manager pcsc che per leggere l'ATR della carta. La successiva figura mostra l'output che si ottiene, inserendo una smart card tipo CNS modello 1204.

Se l'ATR della carta che si sta testando (nel nostro caso la stringa 3B FF 18 00 FF 81 31 FE 55 00 6B 02 09 02 00 01 11 01 43 4E 53 11 31 80 8E ) non è associato a una carta nota, si può provare a scaricare la versione più recente del file *smartcard\_list.txt*, utilizzando l'URL: [http://ludovic.rousseau.free.fr/software/pcsc-tools/smartcard\\_list.txt](http://ludovic.rousseau.free.fr/software/pcsc-tools/smartcard_list.txt)

All'indirizzo <http://ludovic.rousseau.free.fr/software/pcsc-tools/index.html> sono presenti maggiori informazioni sull'utilizzo di questo ed altri tool correlati.

```
mario@mambo:~$ pcsc_scan
PC/SC device scanner
V 1.4.9 (c) 2001-2006, Ludovic Rousseau <ludovic.rousseau@free.fr>
Compiled with PC/SC lite version: 1.4.2
Scanning present readers
0: ACS ACR38U 00 00
Sat Nov 3 20:46:51 2007
Reader 0: ACS ACR38U 00 00
Card state: Card inserted,
ATR: 3B FF 18 00 FF 81 31 FE 55 00 6B 02 09 02 00 01 11 01 43 4E 53 11 31 80 8E
ATR: 3B FF 18 00 FF 81 31 FE 55 00 6B 02 09 02 00 01 11 01 43 4E 53 11 31 80 8E
+ TS = 3B --> Direct Convention
+ T0 = FF, Y(1): 1111, K: 15 (historical bytes)
TA(1) = 18 --> Fi=372, Di=12, 31 cycles/ETU (115200 bits/s at 3.57 MHz)
TB(1) = 00 --> VPP is not electrically connected
TC(1) = FF --> Extra guard time: 255 (special value)
TD(1) = 81 --> Y(i+1) = 1000, Protocol T = 1
-----
TD(2) = 31 --> Y(i+1) = 0011, Protocol T = 1
-----
TA(3) = FE --> IFSC: 254
TB(3) = 55 --> Block Waiting Integer: 5 - Character Waiting Integer: 5
+ Historical bytes: 00 6B 02 09 02 00 01 11 01 43 4E 53 11 31 80
Category indicator byte: 00 (compact TLV data object)
Tag: 6, len: B (pre-issuing data)
Data: 02 09 02 00 01 11 01 43 4E 53
Mandatory status indicator (3 last bytes)
LCS (life card cycle): 11 (Proprietary)
```

SW: 3180 (Error not defined by ISO 7816)  
+ TCK = 8E (correct checksum)  
Possibly identified card (using /usr/share/pcsc/smartcard\_list.txt):  
3B FF 18 00 FF 81 31 FE 55 00 6B 02 09 02 00 01 11 01 43 4E 53 11 31 80 8E  
Infocamere CNS