Accessing the Cambride University Card under Linux

Rich Wareham, <richwareham@users.sourceforge.net> v0.3alpha, 2001 September 21

This mini-HOWTO outlines the steps required to install and configure the PC/SC smartcard resource manager middleware under Linux.

Contents

1 Introduction

This document has been written to provide Systems Administrators and privileged users with information on how to access the Cambride University Card under the Linux operating system. Although untested on other platforms, there is nothing particularly Linux specific about the software described here and it should be poossible to install it under many flavours of Unix.

1.1 New versions of this document

New versions of this document can be obtained from *http://www.srcf.ucam.org/~rjw57/sc/pcsc_lite* .

1.2 Feedback

All comments, error reports, additional information and criticism of all sorts should be directed to:

```
richwareham@users.sourceforge.net
```

1.3 Disclaimer

No liability for the contents of this documents can be accepted. Use the concepts, examples and other content at your own risk. Additionally, this is an early version, with many possibilities for inaccuracies and errors.

One of many possible setups will be described. In the Linux world, there is usually a number of ways in which to accomplish things.

As far as I know, all of the programs mentioned here are released under the GNU General Public License or the Lesser GNU Public License.

1.4 Copyright information

1.5 How do I submit changes or additions to the HOWTO?

The preferred method is to edit the file `howto.sgml` to incorporate the changes, create a diff file by typing something like

```
diff -uw original-file new-file
```

and send it to `richwareham@users.sourceforge.net`. If you do not know SGML, that's ok. Changes or new information in any form will be accepted. Creating the diff file just makes it easier on the HOWTO maintainer. `:-)`

2 About the University of Cambridge Card

The University card is described in detail on *http://www.admin.cam.ac.uk/offices/misd/univcard/* . This document will only deal with the use of the smart chip on the card rather than the TDSi Infrared strip or the barcode.

From the above site:

> The smart chip is a microprocessor embedded in the card. The chip is able to store a small amount of information and to control the conditions under which the information can be accessed or modified. The chip is also able to perform some cryptographic functions such as creating or checking a digital signature. The primary purpose of the chip is to authenticate the identity of the cardholder. For this purpose, the chip holds a public/private key pair together with a digital certificate. The certificate asserts that the public key on the card belongs to the person associated with a particular identifier; this assertion is made by a Certificate Authority run by the University Card Services. The corresponding private key remains on the card: it cannot normally be extracted, but is used by the card's own cryptographic functions.
>
> The private key on the card is protected by a PIN (personal identification number). PINs are assigned at random when the cards are issued; it may also be possible for individuals to change their PINs at a later date. Cardholders must never reveal their PIN to anyone else, even to members of staff at the card office. If the PIN is entered incorrectly three times in succession, the card becomes 'blocked' and cannot then be used for authentication. The card must then be returned to the card office where it can be 'unblocked' if staff are assured that it is in the hands of the rightful owner.

The University Card uses an IBM MFC 4.22 chip. Technical details on this chip are available at *http://vertebra.cbcu.cam.ac.uk/* .

3 Programming Interfaces to Smartcards

There exists a widely used Application Programmers Interface (API) called PC/SC which abstracts the various Smartcard readers available. In this document, the *GemPlus* GemPC410 reader will be used as an example, although there are many other readers which may work (see the Resources at the end of this document).

Under Linux, this API is implemented as a two tier system; your application uses the PC/SC API to talk to a middleware resource manager. The resource manager then talks to one or more readers using reader specific drivers. In this way the middleware need be set up only once for each reader and all applications are reader agnostic.

Linux implements a subset of PC/SC called PC/SC lite. Details of this API may be obtained from the MUSCLE web-site (see Resources). For most uses, existing PC/SC programs may be ported simply to the PC/SC lite API.

It is outside the scope of this document to provide a tutorial on PC/SC lite programming although many such documents can be found on the Internet.

4 Obtaining and Installing the Software

4.1 Obtaining the software

The main source of software is the *MUSCLE web-site* . The PC/SC lite middleware should be downloaded from *http://www.linuxnet.com/middle.html* and drivers from *http://www.linuxnet.com/sourcedrivers.html* .

Note: The GemPlus reader driver available from the above sites does not work well with the University Card. Instead, you should use the modified version available from *http://www.srcf.ucam.org/˜rjw57/sc* .

4.2 Installing the software

4.2.1 PC/SC lite middleware

Download the `pcsc-lite-x.x.x.tar.gz` file to a convenient location. The `x.x.x` denotes the version number of the software. The latest version at the time of writing is 0.9.3.

Open a terminal and change to the directory the file was downloaded to. Enter the following commands:

```
$ gunzip -c pcsc-lite-*.tar.gz | tar xv
$ cd pcsc-lite-x.x.x     # Replace x.x.x with version
$ ./configure --prefix=/usr/local/pcsc
$ make
$ su
Password: (enter root password)
# make install
# exit
$
```

The PC/SC lite software will then be installed to `/usr/local/pcsc`. Note: Under Solaris, you may have to modify the Makefile to add the following linker flags:

```
-lsocket -lnsl -lrt
```

4.2.2 Reader drivers

Download the reader drivers and install as per instructed by files which came with the driver. If you have the GemPlus serial reader driver note that the GemPlus readers have problems understanding the Answer to Reset (ATR) response of the card. To use the card with GemPlus readers, you must download the correct driver from this site and perform the following steps.

Open a terminal and change to the directory you downloaded the `libgemcore-hacked.tar.gz` file to and enter the following commands:

```
$ gunzip -c libcamgemcore-x.x.x.tar.gz | tar xv
$ cd libcamgem*
$ ./configure
$ make
$ su
Password: (enter root password)
# make install
# exit
$
```

Then edit `/etc/reader.conf` to point to the `libcamgemcore.so.0.0.0` file which has been created as per the next section.

Configuration The main configuration file is `/etc/reader.conf`. This file should contain an entry for each driver of the following form:

```
FRIENDLYNAME     "FooBar Inc. FB100 reader"
DEVICENAME       FOOBAR_FB100
```

```
LIBPATH          /usr/lib/libfoobar.so.1.0.0
CHANNELID        0x0102F8
```

Where the fields have the following meanings:

- `FRIENDLYNAME` – Any descriptive name for the reader.
- `DEVICENAME` – Any shorter name.
- `LIBPATH` – **Full** path to the driver library.
- `CHENNELID` – The serial port the reader is connected to, taken from the following table:
  - `0x0103F8` – COM1 or `/dev/ttyS0`
  - `0x0102F8` – COM2 or `/dev/ttyS1`
  - `0x0103E8` – COM3 or `/dev/ttyS2`
  - `0x0102E8` – COM4 or `/dev/ttyS3`

Invocation To launch the PC/SC middleware, you may need to set some environment variables. If you are using the Bash shell then the following commands should launch the PC/SC middleware:

```
$ su
Password: (enter root password)
# export PATH=$PATH:/usr/local/pcsc/bin
# export LD_LIBRARY_PATH=$LD_LIBRARY_PATH:/usr/local/pcsc/lib
# pcscd
```

5 Testing

A simple program to test the card reader with a University Card is available at *http://www.srcf.ucam.org/˜rjw57/sc/software/kcardtest.html*

6 Using the Cambridge Smartcard with Netscape/Mozilla

The University SmartCard has the ability to securely authenticate itself to a remote server by use of a suitable ‘plugin’ for the Netscape/Mozilla browsers. The plugin conforms to the PKCS#11 Cryptoki interface standard so may also be used by other software which can make use of such plugins.

The plugin is available from *http://www.srcf.ucam.org/˜rjw57/sc* . To use it, one must download both the `libcamcard` and `campkcs` tar-balls. Also the PCSC-lite middleware must be correctly set-up as in the above sections.

Both `libcamcard` and `campkcs` must be unpacked and installed in the usual manner (`libcamcard` is required for `campkcs` and so must be built first).

When you have built `campkcs`, a new library will be installed on your system, `libcampkcs11.so.x.x.x`. It is this file which is the PKCS#11 module. Full installation instructions are available at *http://vertebra.cbcu.cam.ac.uk/pkcs-install.html* (except replace the Windows DLL available there for the `libcampkcs11.so.x.x.x` file).

`campkcs` adds some extra functionality to the one available from the above site. Firstly, it supports the newer (layout) Version 1 Univeristy Smartcard. Also Logout and Change PIN functions are supported. Finally, the module also adds support for multiple certificates on one card.

7 Resources

7.1 General resources

- MUSCLE homepage – *http://www.linuxnet.com*