Chipkartenleser unter Linux

Bernhard Walle
<bernhard.walle@gmx.de>
19. Januar 2005

Chipkartenleser sind immer weiter verbreitet: Als Telefon- oder Krankenversicherungskarte, als *Geld-Karte* oder für digitale Signierverfahren. Es gibt preisgünstige Chipkartenleser für den PC – warum also nicht einen solchen auch unter Linux nutzen? Im Internet gibt es eine Vielzahl von Programmen und Informationsseiten, ich habe hiermit einmal versucht, die wichtigsten zusammenzutragen. Falls Sie weitere Informationen haben oder den einen oder anderen Fehler entdecken (wenn es auch nur ein „toter Link“ ist), bitte ich um eine E-Mail.

1 Hardware

Chipkartenleser werden entweder über USB oder über die serielle Schnittstelle an den PC angeschlossen. Vereinzelt gibt es auch Geräte, die über die PS/2-Schnittstelle verbunden werden; dies ist v. a. dann sinnvoll, wenn der Leser in die Tastatur integriert ist. Ansonsten wird die Tastatur einfach durchgeschleift. Während die Leser mit serieller Schnittstelle preisgünstiger sind, verfügen die USB-Geräte über eine größere Zukunftssicherheit, da die serielle Schnittstelle wohl in absehbarer Zeit verschwinden wird.

Unter Linux gibt es Treiber für die Geräte der Hersteller *Towitoko* (http://www.towitoko.de) und *Kobil* (http://www.kobil.de). Möglicherweise existieren auch noch Treiber für andere Geräte, mir sind jedenfalls keine bekannt. Es wird sowohl die serielle als auch die USB-Schnittstelle unterstützt.

Einen sehr günstigen Kartenleser gibt es mit dem *Towitoko Chipdrive fun*, bei Conrad Electronic (http://www.conrad.de) für rund 18 Euro. Es handelt sich hierbei um das *Towitoko Chipdrive micro 120*, das normalerweise knapp 40 Euro kostet. Das gleiche Gerät gibt es auch als „Linux Pack“, dem neben der Treibersoftware für Linux noch zwei programmierbare Karten beiliegen. Letzteres gibt es direkt beim Towitoko-Onlineshop unter http://www.chipdrive.de für rund 25 Euro.

Viele Banken bieten die Towitoko-Geräte im Rahmen von HBCI-Onlinebanking auch vergünstigt oder teilweise sogar umsonst an. Eine Nachfrage bei Ihrem Kreditinstitut lohnt sich also auf jeden Fall, selbst wenn Sie danach Onlinebanking nur sporadisch oder gar nicht betreiben!

Gemäß der Sicherheitsstufe werden Chipkarten vom *ZKA*[1] in drei Klassen eingeteilt, siehe auch [1]:

Klasse 1 Diese Geräte sind die billigste Variante. Sie eignen sich für alle „normalen“ Anwendungen und verfügen weder über ein Display noch über eine Tastatur.

Klasse 2 Solche Geräte verfügen über eine eigene Tastatur, aber über kein Display. Somit ist es nicht möglich, dass Trojaner auf dem PC eine PIN ausspähen können. Somit bieten diese Geräte eine erhöhte Sicherheit beim HBCI-Homebanking.

[1] Zentraler Kreditausschuss: Gremium, in dem sich die Spitzenvertreter des deutschen Kreditgewerbes zusammengeschlossen haben. Homepage: http://www.zka.de..

Klasse 3 Sie verfügen über ein eigenes Display und eine eigene Tastatur. Damit ist es nicht möglich, dass die Daten zwischen PC und Kartenleser verfälscht werden. Klasse-3-Geräte eignen sich von der Sicherheitsstufe auch, um die *GeldKarte* am heimischen PC aufzuladen. Solche Anwendungen existieren aber meines Wissens noch nicht.

2 Treiber

Für Chipkarten gibt es eine feste Programmierschnittstelle, die sog. *CT-API*. Die hier vorgestellten Treiber implementieren diese Schnittstelle. Somit können Anwendungsprogramme unabhängig von der tatsächlich verwendeten Hardware über einen solchen Treiber auf den Kartenleser zugreifen.

Da ich nur das Chipdrive micro 120 besitze, kann ich hier nur auf die Geräte von Towitoko eingehen. Mit diesem Treiber sollen folgende Kartenleser unterstützt werden:

- Towitoko Chipdrive Micro
- Towitoko Chipdrive Extern (II)
- Towitoko Chipdrive Intern
- Towitoko Chipdrive Twin
- Kartenzwerg

Der Treiber kann jeweils in der neuesten Version unter http://www.geocities.com/cprados/ heruntergeladen werden.

Die Installation erfolgt – wie unter Linux üblich – folgendermaßen:

1. Nach dem Download der Quellcode-Archivdatei („Tarball“), muss diese zunächst ausgepackt werden. Dies geschieht mit dem Befehl `tar xvfz towitoko-2.0.6.tar.gz`.
2. Danach wird mit `cd towkitoko-2.0.6` in das entsprechende Verzeichnis gewechselt.
3. Mit dem Kommando `./configure` wird der Treiber auf die Kompilation vorbereitet. Wenn Sie die USB-Version verwenden, und USB nicht funktioniert, können Sie die Unterstützung mit dem Parameter `--enable-usb` explizit aktivieren. Es wurde aber auch berichtet, dass USB ohne diesen Parameter funktioniert und es *mit* dem Parameter Probleme gibt.
   Damit der Treiber auch mit *Moneyplex* (einer Homebanking-Software für Linux) funktioniert, sind zusätzlich die beiden Parameter `--enable-win32-com` und `--disable-atr-check` erforderlich. Beachten Sie dazu auch die Hinweise unter 3.1.
4. Durch den `make`-Befehl wird der Treiber kompiliert, d. h. aus dem Quellcode werden ausführbare Dateien erstellt.
5. Zum Schluss muss der Treiber installiert werden. Dazu muss als Administrator („root“) der Befehl `make install` ausgeführt werden.

Nun ist der Treiber unter /usr/local/towitoko installiert und kann verwendet werden. Zum Testen der Installation eignet sich das Programm *tester*, das im Verzeichnis /usr/local/towitoko/bin installiert wurde. Starten Sie dazu einfach das Programm, geben Sie `in` *`Nummer`* ein, wobei *`Nummer`* für die serielle Schnittstelle steht. Nachdem eine Meldung wie `Status: Memory smartcard present` ausgegeben wurde, können Sie das Programm mit `q` beenden.

3 Programme

3.1 Moneyplex

Moneyplex ist das einzige Homebankingprogramm für Linux[2]. Es handelt sich hinbei nicht um freie Software; das Programm kann stattdessen (ohne Quellcode) gekauft werden – entweder direkt beim Hersteller *matrica* (http://www.matrica.de) oder bei sonstigen Softwareverkäufern, beispielsweise bei *LinuxLand* (http://www.linuxland.de).

Neben PIN/TAN-Banking für die Postbank wird v. a. HBCI-Internetbanking angeboten, und zwar sowohl mit Sicherheitsdiskette als auch mit Chipkarte. Letzteres ist die deutlich sicherere Lösung, da die Verschlüsselung in der Karte stattfindet und die Karte nach dreimaliger Eingabe einer falschen PIN ungültig wird. Bei einer Diskette ist zum einen eine einfache Kopie mit jedem PC möglich, zum anderen können beliebig viele Versuche angewandt werden, um die PIN zu „knacken".

Um das oben erwähnte Towitoko-Gerät mit dem installierten Treiber und Moneyplex zu verwenden, muss unter *Einstellungen*, *Chipkartenleser*, *CTAPI-Treiber* der vollständige Pfad des Treibers, in diesem Fall also /usr/local/towitoko/lib/libtowitoko.so eingetragen werden. Mit dem Online-Update vom 14.07.2002 liefert Matrica auch Treiber für die Towitoko-Kartenlesegeräte mit. Der Treiber heißt libct_towitoko.so und befindet sich im Unterverzeichnis ctapi der Moneyplex-Installation. Dieser Treiber funktioniert natürlich ebenfalls. Wenn man also das Kartenlesegerät ausschließlich für Homebanking verwendet, kann man sich die Kompilation und Installation des CTAPI-Treibers sparen. Allerdings wird dieser Treiber aufgrund von Lizenzproblemen nicht mehr mit dem Online-Update installiert. Ich kann ihn leider auch nicht auf Anfrage verschicken, da ich damit vermutlich ebenfalls gegen Lizenzen verstoßen würde.

Hinweis: In letzer Zeit habe ich mehrere Mails bekommen mit dem Problem, dass das USB-Gerät nicht mit Moneyplex funktioniert. Ich kann dazu leider auch keine Auskunft geben, da ich dieses Gerät nicht besitze. Auf jeden Fall wäre ich für Hinweise dankbar, wenn jemand diese Version zum Laufen bekommen hat. Ggf. sollten Sie sich bei der Neuanschaffung eines Towitoko-Chipkartenlesers lieber für die ohnehin billigere Version für die serielle Schnittstelle entscheiden.

Nachdem unter *Schnittstelle* der richtige Anschluss gewählt wurde, kann mit der Funktion *Testen* die Funktion überprüft werden. Dazu ist eine HBCI-Karte oder eine einfache *GeldKarte* erforderlich. Nachdem der Test abgeschlossen wurde, muss der Dialog nur noch mit *OK* bestätigt werden, woraufhin der Kartenleser problemlos verwendet werden kann.

3.2 Libchipcard

Unter http://www.libchipcard.de findet man eine umfangreiche Sammlung von Programmen und Bibliotheken für Chipkartenlesegeräte unter Linux.

[2] Neben Moneyplex gibt es auch noch GNU-Cash (http://www.gnucash.org), ein freies Finanzverwaltungsprogramm, das seit kurzem über die OpenHBCI-Bibliothek auch HBCI-Homebanking unterstützt. Eine Auflistung aller HBCI-Homebankingprogramme findet man unter [2] (HBCI-Produkte, Übersicht öffnen, Kundenprodukte, Offline). Zu anderen Programmen kann ich nichts sagen, da ich Moneyplex verwende (es war die erste HBCI-Lösung für Linux), ich damit zufrieden bin und ich nicht das Risiko eingehe, ein Konto mit zwei Programmen gleichzeitig zu verwalten.

Nach der erfolgreichen Installation findet man in *K-Menü*, *Dienstprogramme*, *Chipkarten Dienstprogramme* das Programm *kMedialCard*, mit dem ganz einfach deutsche Krankenversicherungskarten ausgelesen werden können. Bevor Sie dieses Programm nutzen können, muss jedoch die Programmsammlung mit dem Programm *kLCSetup* konfiguriert werden. Alternativ kann auch die im Quellcode-Archiv enthaltene Datei libchipcard.conf in das Systemkonfigurationsverzeichnis /etc/ kopiert und an die eigenen Bedürfnisse angepasst werden.

Für Programmierer dürfte das Programm *kCardDebugger* interessanter sein, da hiermit die auf der Karte enthaltenen Daten genauer betrachtet werden können.

Zum Betrieb dieser Programmsammlung ist ein CTAPI-Chipkartentreiber erforderlich. Somit eignen sich die Programme zum Betrieb einer Vielzahl von Kartenlesern.

3.3 Scez

Im Gegensatz zu den anderen vorgestellten Programmen kommt dieses Paket ohne einen CTAPI-Treiber aus, kann also Geräte direkt ansprechen. Zusätzlich kann aber auch ein CTAPI-Treiber verwendet werden. Die Geräte von Towitoko werden direkt unterstützt.

Die Homepage des Projektes befindet sich unter http://www.franken.de/crypt/scez.html. Dort befindet sich auch der Link zum FTP-Server ftp://ftp.franken.de/pub/crypt/chipcards/scez/, wo die aktuelle Version heruntergeladen werden kann. Zusätzlich befindet sich *scez* aber auch im Lieferumfang vieler aktuellen Linux-Distributionen, u. a. SuSE 7.2, so dass auf die Installation nicht näher eingegangen werden soll.

Auch dieses Paket besteht aus einer Vielzahl von kleineren Programmen. Ein Problem ist, dass diese relativ schlecht dokumentiert sind, was die Anwendungsprogramme angeht.

Bevor diese benutzt werden können, muss die Umgebungsvariable `SCEZ_READER` gesetzt werden. Der Wert einer solchen Variable besteht aus drei Teilen, die jeweils durch ein Komma (aber ohne Leerzeichen) getrennt sind. Der erste Teil gibt den Namen des Treibers an. Gültige Belegungen sind `TOWITOKO` (für die Towitoko-Geräte) oder `CTAPI` (Geräte anderer Hersteller mit CTAPI-Treiber). Danach folgt eine Zahl, die die Schnittstelle bezeichnet, z. B. `1` für *COM1*. Schließlich folgt ein Parameter, der die Schnittstellendatei angeben kann. Eine Dokumentation dieser Variable finden Sie in der Info-Datei zu dem Programm. Beispiele für gültige Werte sind `CTAPI,1,/dev/ttyS1` oder `TOWITOKO,1,0`. Ich verwende beispielsweise den Befehl `export SCEZ_READER="TOWITOKO,1,0"`, um meinen Kartenleser zu verwenden. Es empfiehlt sich, diesen Befehl in eine Startdatei, z. B. ~/.profile oder /etc/profile bzw. /etc/profile.local (empfohlen für SuSE) einzutragen.

Im folgenden sollen zwei nützliche Programme aus dem Paket vorgestellt werden:

scdir

Das Programm *scdir* dient dazu, die Daten auf einer Chipkarte auszulesen. Unterstützt wird an „normalen“ Karten die *GeldKarte*. Es lässt sich damit der Wert anzeigen oder auch die letzten Buchungen nachvollziehen.

Eine Dokumentation zur Ausgabe bei der *GeldKarte* befindet sich innerhalb des Quellcodearchivs im Unterverzeichnis txt, und zwar in der Datei geldkarte.txt.

simman

Dieses Programm unterstützt GSM-Handykarten. Normalerweise benötigt man dazu einen Adapter, damit die Handykarte auf die Größe einer normalen Scheckkarte „wächst“. Ein solcher wird bei vielen Kartenlesern mitgeliefert, kann aber auch extra erworben werden.

Mit *simman* lassen sich nicht nur – nach Eingabe der PIN – die auf der Karte gespeicherten Telefonbucheinträge und SMS auslesen, es lässt sich auch eine vorhandene Datei zurückschreiben, und zwar mit dem Befehl `simman -r <data.txt`. Damit lässt sich das Programm ideal als Backup benutzen.

Die Dokumentation zu dem Programm befindet sich in der Datei simman.txt, wieder im Unterverzeichnis txt.

Literatur

[1] *Chipkartenleser*, Einteilung in Sicherheitsklassen, Sparkasse Memmingen-Lindau-Mindelheim
http://home.s-planet.de/schulze.eb/hbci/leser.htm

[2] *Home Banking Computer Interface*, Informationen zu HBCI vom Zentralen Kreditausschuss
http://www.hbci.de

[3] *M. U. S. C. L. E. – Movement For The Use Of Smart Cards In A Linux Environment*
http://www.linuxnet.com

[4] „Chip, Chip, Hurra“, *Chipkarten unter Linux*, Martin Brüstle, iX 2/2000, S. 152
http://www.heise.de/ix/artikel/2000/12/152/

[5] „Kohle, Kies und Konten“, *Internet-Banking mit Linux*, Ulrich Wolf, Linux-Magazin 12/1999
http://www.linux-magazin.de/ausgabe/1999/12/Banking/banking.html

[6] *Chipdrive – Chipkarten auslesen*, Matthias Kranz, Linux NetMag
http://www.linuxnetmag.com/de/issue7/m7chipdrive1.html

[7] *Geld-Transport*, Das HBCI-Protokoll und seine Sicherheitsqualitäten, Michael Pramateftakis, Linux-Magazin 8/2003