

Installer un lecteur de carte à puce USB sous Linux

Référence : pki_interne_tutoriel_carte_puce_v1.0

Paris, le mardi 10 juillet 2007

HISTORIQUE DES RÉVISIONS

VERSION	DATE	OBJET DE LA RÉVISION
V1	10/07/07	version initiale

	RÉDACTION	VÉRIFICATION	APPROBATION
NOM	YANNICK QUENECHDU		
FONCTION			
VISA			

DOCUMENTS DE RÉFÉRENCE

ORDRE	INTITULÉ DU DOCUMENT	AUTEUR

SOMMAIRE

1. Introduction	5
1.1. <i>Présentation des cartes à puces</i>	5
2. PS/SC LITE	5
2.1. <i>Présentation</i>	5
2.2. <i>Installation de PC/SC LITE</i>	6
2.2.1. <i>Installation de la librairie libsub</i>	6
2.2.2. <i>Installation de pcsc-lite</i>	6
2.3. <i>Installation des drivers du lecteur</i>	6
2.3.1. <i>Vérification préliminaires</i>	6
2.3.2. <i>Installation des drivers Omnikey</i>	7
2.4. <i>Test de l'installation de PC/SC Lite</i>	7
3. Installation d'outils et d'applications compatibles PC/SC	7
3.1. <i>Installation de pcsc-tools</i>	7
3.2. <i>Installation de OpenSC</i>	8

CONVENTIONS DE NOTATION

Les contenus de fichiers sont retranscrits ainsi :

```
# Ceci est un fichier  
parametre="valeur"
```

Les commandes sont indiquées sous la forme suivante et précédées d'un caractère '\$' (commande à taper avec des droits utilisateurs) ou '#' (commande à taper avec des droits root) qui n'est pas à saisir dans la ligne de commande :

```
$ commande1  
# commande2
```

Les remarques ou autres éléments particuliers sont notés dans les cadres suivants :

Style des remarques

1. INTRODUCTION

Ce tutoriel aborde l'installation d'un lecteur de cartes à puces sous Linux. Le lecteur utilisé pour réaliser ce tutoriel est le lecteur USB Omnikey Cardman 6121 mais notre propos peut facilement s'étendre aux autres lecteurs, notamment ceux sur port série ou parallèle. L'objectif de cette installation est de gérer l'authentification des utilisateurs via une carte à puce. La réalisation de cet objectif (notamment la configuration des modules PAM etc... Voir aussi [4]) fera l'objet d'un document ultérieur. Ce tutoriel se contente de détailler la phase d'installation et de configuration du lecteur, tout en proposant l'installation d'outils complémentaires permettant de manipuler le contenu de la carte à puce. Enfin, bien que la distribution utilisée soit une Ubuntu festy.

1.1. Présentation des cartes à puces

cf les documents suivants :

- http://www.jalix.org/ressources/miscellaneous/security/_IFT6271/Chap_14.pdf (FR)
- <http://people.cs.uchicago.edu/~dinoj/smartcard/javacardarch.html> (EN)

Dans la suite, les commandes shell nécessitant les droits utilisateurs (root) seront préfixées par user% (root#).

2. PS/SC LITE

2.1. Présentation

La gestion standard de la communication entre un ordinateur et une carte à puce a été définie par le groupe de travail PC/SC¹. PC/SC est donc une API qui fournit aux développeurs un ensemble de primitives standard permettant de gérer les lecteurs de cartes à puces et de communiquer avec le lecteur et les cartes à puces qu'il contient. Ainsi, les opérations standards effectuées sur les cartes à puces sont gérées par cette API de façon homogène. Chaque fournisseur de lecteur doit simplement fournir un driver spécifique à son lecteur implémentant chaque fonctions de cette API.

¹ <http://www.pcscworkgroup.com/>

2.2. Installation de PC/SC LITE

2.2.1. Installation de la librairie libusb

PC/SC-lite utilise la librairie libusb pour accéder à un lecteur USB. Pour l'installer (sous Debian) :

```
apt-get install libusb-dev libusb-0.1-4
```

La librairie est installée dans `/usr/lib/libusb.so`

Sinon, il suffit de récupérer les sources sur le site <http://libusb.sourceforge.net/> et procéder à l'installation manuellement.

2.2.2. Installation de pcsc-lite

```
apt-get install pcscd
```

En complément, il installe la librairie libccid qui contient les drivers de carte à puce. Dans le cas où l'installation de libccid n'est pas réalisée en relation avec pcsc, ajouter la commande suivante :

```
apt-get install libccid
```

2.3. Installation des drivers du lecteur

2.3.1. Vérification préliminaires

Comme le lecteur fonctionne sur le port USB, les modules `usbcore` et `usb-uhci` doivent être chargés. On le vérifie par les commandes :

```
root# lsmod | grep usbcore
root# lsmod | grep usb-uhci
```

Résultat :

```
usbcore      134280 4 usbhid, ehci_hcd, uhci_hcd
```

Si ce n'est pas le cas, les insérer avec la commande `modprobe <module>`. Le port USB doit être monté dans le système de fichier.

2.3.2. Installation des drivers Omnikey

Les drivers linux du lecteur Omnikey Cardman 6121 peuvent être récupérés sur le site <http://omnikey.aaitg.com/index.php?id=69> sous la référence « CardMan Dongle USB 6121 (CCID) ». Au moment où ce tutoriel est écrit, l'archive récupérée ainsi est ifdokccid_lnx-3.0.0.tar.gz

L'installation s'effectue à l'aide des commandes suivantes :

```
user% tar xvzf ifdokccid_lnx-3.0.0.tar.gz
user% cd ifdokccid_lnx-3.0.0
root# ./install -d /usr/lib/pcsc/drivers
```

2.4. Test de l'installation de PC/SC Lite

La commande lsusb liste les périphériques attachés aux ports USB. Par exemple, pour le lecteur omnikey :

```
lsusb | grep -i omnikey
```

Résultat :

```
Bus 005 Device 006: ID 076b:6622: OmniKey AG
```

Sur cet exemple,

- 076b est le "Vendor ID";
- 6622 est le "Product ID"

3. INSTALLATION D'OUTILS ET D'APPLICATIONS COMPATIBLES PC/SC

3.1. Installation de pcsc-tools

Pcsc-tool est un ensemble d'outils pour manipuler les cartes `a puce `a travers PC/SC. Ces outils permettent notamment de tester un driver PC/SC, une carte ou un lecteur, d'envoyer des commandes dans un environnement en ligne de commande ou graphique etc. Les outils fournis par *pcsc-tools* sont détaillés dans la liste suivante :

- `pcsc_scan` qui scanne chaque lecteur PC/SC connecté et fournit des informations sur les cartes insérées. Cet exécutable utilise un script Perl – `ATR_analysis` - qui permet de récupérer et d'interpréter l'ATR₆ de la carte insérée.
- `scriptor` (et sa version graphique par interface GTK `gscriptor`) est un script perl permettant

d'envoyer des commandes à la carte insérée.

L'installation est réalisée par la commande suivante :

```
apt-get install pcsc-tools
```

3.2. Installation de OpenSC

Un 'card format' est une description détaillée de la façon dont sont représentés sur une carte des objets cryptographiques comme une clé ou un certificat. PKCS#15 [3] est un standard pour le card format supportant tous les objets définis dans la norme PKCS#11. OpenSC est une bibliothèque (libopensc) permettant notamment de gérer les cartes compatible avec le standard PKCS#15.

L'utilisateur pourra ainsi initialiser, personnaliser et manipuler des cartes PKCS#15, signer et déchiffrer des données à partir de clés privées stockées sur la carte. La procédure d'installation de OpenSC est la suivante :

```
apt-get install opensc
```