



# Installation d'une carte à puce sous Linux

## PKI et certificats numériques

API PC/SC, librairie OpenSC, Omnikey

Version 1.1

Le 23/10/2009

Identifiant : -

Fichier original : 9999-02\_DOC\_PKI\_Installation-Carte-a-puce-Linux\_1.1.odt



## Historique des évolutions et visas

### Visas

	RÉDACTION	APPROBATION	VALIDATION
<b>NOM</b>	Yannick QUENEC'H DU		
<b>FONCTION</b>	Responsable Pôle Sécurité		
<b>DATE</b>	10/07/2007		
<b>VISA</b>			

### Historique des évolutions

L'ajout de son nom par tout nouvel **acteur contributeur** exprime son consentement exprès et non vicié à une distribution du document conforme à la licence indiquée en pied de page.

VERSION	DATE	ACTEUR CONTRIBUTEUR	OBJET DE L'ÉVOLUTION
1.0	10/07/2007	Yannick QUENEC'H DU	Création
1.1	23/10/2009	David CARELLA	Relecture et adaptation

Statut du document : **60 – En application**

### Diffusion du document

Mention de diffusion : **Publique**

NOM	ORGANISME	POUR	MÉDIA

### Liste des contributeurs

Yannick QUENEC'H DU, David CARELLA.



## Table des matières

<b>1</b>	<b>Introduction.....</b>	<b>4</b>
1.1	Présentation des cartes à puce.....	4
<b>2</b>	<b>PS/SC Lite.....</b>	<b>5</b>
2.1	Présentation.....	5
2.2	Installation de PC/SC LITE.....	5
2.2.1	Installation de la librairie libsub.....	5
2.2.2	Installation de pcsc-lite.....	5
2.3	Installation des drivers du lecteur.....	5
2.3.1	Vérification préliminaire.....	5
2.3.2	Installation des drivers Omnikey.....	6
2.4	Test de l'installation de PC/SC Lite.....	6
<b>3</b>	<b>Installation d'outils compatibles PC/SC.....</b>	<b>7</b>
3.1	Installation de pcsc-tools.....	7
3.2	Installation de OpenSC.....	7
<b>4</b>	<b>Références.....</b>	<b>8</b>



## 1 Introduction

Ce tutoriel aborde l'installation d'un lecteur de cartes à puces cryptographiques 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.) 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 puce

---

Veillez vous référer aux documents suivants :

[fr] [http://www.jalix.org/ressources/miscellaneous/security/\\_IFT6271/Chap\\_14.pdf](http://www.jalix.org/ressources/miscellaneous/security/_IFT6271/Chap_14.pdf)

[en] <http://people.cs.uchicago.edu/~dinoj/smartcard/javacardarch.html>

Dans la suite, les commandes shell nécessitant les droits utilisateurs (ou `root`) seront préfixées par « `user%` » (ou « `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/SC<sup>1</sup>. 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 standard 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 fonction de cette API.

### 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), lancer la commande suivante :

```
# 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

Commande :

```
# 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 préliminaire

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
```

<sup>1</sup> <http://www.pcscworkgroup.com/>



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 web du fabricant <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 le fichier `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 :

- la valeur « 076b » est le « Vendor ID »;
- la valeur « 6622 » est le « Product ID ».



## 3 Installation d'outils compatibles PC/SC

### 3.1 Installation de pcsc-tools

**Pcsc-tool** est un ensemble d'outils pour manipuler les cartes à puce à 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'ATR 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 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 compatibles 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
```



## 4 Références

### Références Linagora

RÉFÉRENCE	VER.	PROJET	TITRE OU IDENTIFIANT

### Références externes

RÉFÉRENCE	VER.	ÉDITEUR	TITRE OU IDENTIFIANT

### Références web

RÉFÉRENCE	TITRE	LANG	ADRESSE WEB