Installation du lecteur de cartes

Emmanuel Mocquet

22 février 2013

1 Installation

L'installation des librairies et outils nécessaires à la reconnaissance et à l'utilisation de la carte se fait via le script "install" situé dans le répertoire `/lib`.

Il est ensuite possible de vérifier que le système est bien configuré et prêt à utiliser la carte en utilisant l'outil "pcsc_scan". Si la carte est détectée, diverses informations seront affichées ; sinon, le système entrera dans une boucle infinie de tentative de détection.

2 Développement d'applets

2.1 Note

La plupart des fichiers mentionnés dans cette partie sont disponibles dans le répertoire `/lib`.

2.2 Environnement

Une façon relativement simple de développer des applets pour des cartes Javacard est d'utiliser l'IDE Eclipse, disponible dans les dépôts.

Le plugin Eclipse JCDE permet de faciliter le développement de ces applets. Son installation se fait en copiant tous les fichiers JAR du répertoire `lib/JCDE` dans le répertoire "plugins" d'Eclipse (par défaut : */usr/lib/eclipse/plugins*)

2.3 Le JDK

Oracle fournit un SDK Javacard téléchargeable sur son site. La dernière version du SDK Javacard pour GNU/Linux est la 2.2.2. Cette version utilisant le JDK 1.5, il sera nécessaire de configurer le projet sous Eclipse en conséquence.

2.4 Création et configuration d'un projet

Sur Eclipse, le projet est créé en choisissant le type "Javacard". Cependant, à ce stage, le chemin vers le dossier du SDK Javacard n'a pas encore été donné à Eclipse et une erreur sera déclenchée. Elle est corrigeable en entrant ce chemin dans Window → Preferences → Java Card.

De plus, il peut être nécessaire de spécifier quel JDK doit utiliser Eclipse pour compiler le projet : Project → Properties → Java Compiler puis choisir "Compiler compilance level : 1.5".

Des exemples d'applets commentées sont disponibles dans le répertoire `lib/samples` et devraient permettre de se faire une idée de la structure générale d'une applet.

2.5 Préparation de l'installation sur carte

2.5.1 Etablissement d'AID

Avant de déployer l'applet sur sa carte, il faut donner une identifiant unique au package et à ses applets (un AID), en faisant en sorte que l'AID de chaque applet corresponde à celui du package (de 5 octets) complété par au minimum octet. Par exemple si l'AID du package est

```
0x01 0x02 0x03 0x04 0x05 0x06 0x07 0x08 0x09 0x00
```

un AID d'applet pourra être :

```
0x01 0x02 0x03 0x04 0x05 0x06 0x07 0x08 0x09 0x00 0x01
```

Ces AIDs sont modifiables en cliquant droit sur le package ou l'applet en question puis en choisissant Java Card Tools → Set Package AID/Set Applet AID.

2.5.2 Conversion du package

Avant toute utilisation d'applet, il faut bien évidemment passer par une phase d'installation. Le SDK Java Card met à disposition un outil permettant de convertir le package à installer en un fichier `.cap`.

Avec Eclipse/JCDE, cet outil est disponible en cliquant droit sur le package, en ouvrant le sous-menu "Java Card Tools" puis en sélectionnant "Convert".

2.6 Application cliente

Concernant l'application cliente, et contrairement aux applets installés sur carte, il est possible d'utiliser une version de Java en version supérieure à 1.5.

Comme pour les applets, des exemples de clients sont disponibles dans le répertoire `lib/samples`.

3 Installation des applets sur la carte

Prérequis : librairies GlobalPlatform, PCSC, et gpshell fonctionnels

Pour tester l'interrogation de la carte (installation, suppression, listing), il existe des scripts fournis par GPShell, situés dans `lib/gpshell-1.4.4`. Etant donné que les cartes sont compatibles avec la norme GlobalPlatform 2.1.1, les scripts à utiliser sont ceux dont le nom finit par "GP211.txt". L'utilisation de ces scripts se fait en entrant la commande :

```
gpshell fichier.txt
```

Pour installer une applet, il faut fournir plusieurs directives dans le fichier passé à GPshell :

```
// Protocole utilisé pour la norme GlobalPlatform 2.1.1
mode_211

// Commande nécessaire avant toute communication avec la carte :
// établissement d'un contexte
establish_context

// Connexion à la carte
// Si le lecteur n'est pas explicité, le premier branché est
// sélectionné
card_connect

// Sélection du "Security Domain". Cette valeur est la même pour
// toutes les cartes suivant la norme GlobalPlatform 2.1.1.
// Le security domain est une applet de confiance qui va donner un
// jeton de session à l'utilisateur qui sera, par la suite, correctement
// authentifié auprès de la carte.
select -AID a000000003000000

// Authentification et établissement d'un tunnel avec la carte
// security 1 : tunnel avec code MAC
// keyind 0 : numéro d'index de la clef
// keyver 0 : version de la clef (à laisser inchangé)
```

```
// Les clefs spécifiées correspondent à celles stockées par défaut
open_sc -security 1 -keyind 0 -keyver 0 -mac_key \
404142434445464748494a4b4c4d4e4f -enc_key 404142434445464748494a4b4c4d4e4f

// Suppression de notre applet (utile seulement pour une
// réinstallation)
delete -AID 0102030405060708090000

// Suppression de son package
delete -AID 010203040506070809 00

// Installation en fournissant le package compilé et les
// droits sur ce package (-priv)
install -file pack.cap -priv 2

// Déconnexion de la carte et "libération du contexte"
card_disconnect
release_context
```

L'applet pourra alors être utilisée avec une application Java cliente associée.