



# Computing with Java Cards<sup>TM</sup>



Damien SAUVERON

sauveron@labri.u-bordeaux.fr

<http://dept-info.labri.u-bordeaux.fr/~sauveron>

# Plan

---

## Présentation

- La plate-forme
- Le framework logiciel
- PC/SC

## Mise en place de la plate-forme

- Matériels
- Utilisation de JCAT Emulator
- De la théorie à la pratique

## Perspectives

# Présentation

---

## Objectifs :

- ➡ Garantir la sécurité du code et des calculs sur la grille.
- ➡ Proposer un framework logiciel exploitant du matériel sécurisé pour assurer la confiance des utilisateurs.

## Avantages pour :

- les utilisateurs du *distributed computing* : une plus grande confiance dans le fournisseur des ressources de calculs ;
- les fournisseurs des ressources de calculs : accroître son marché avec des nouveaux clients comme le CEA, ...

## La plate-forme

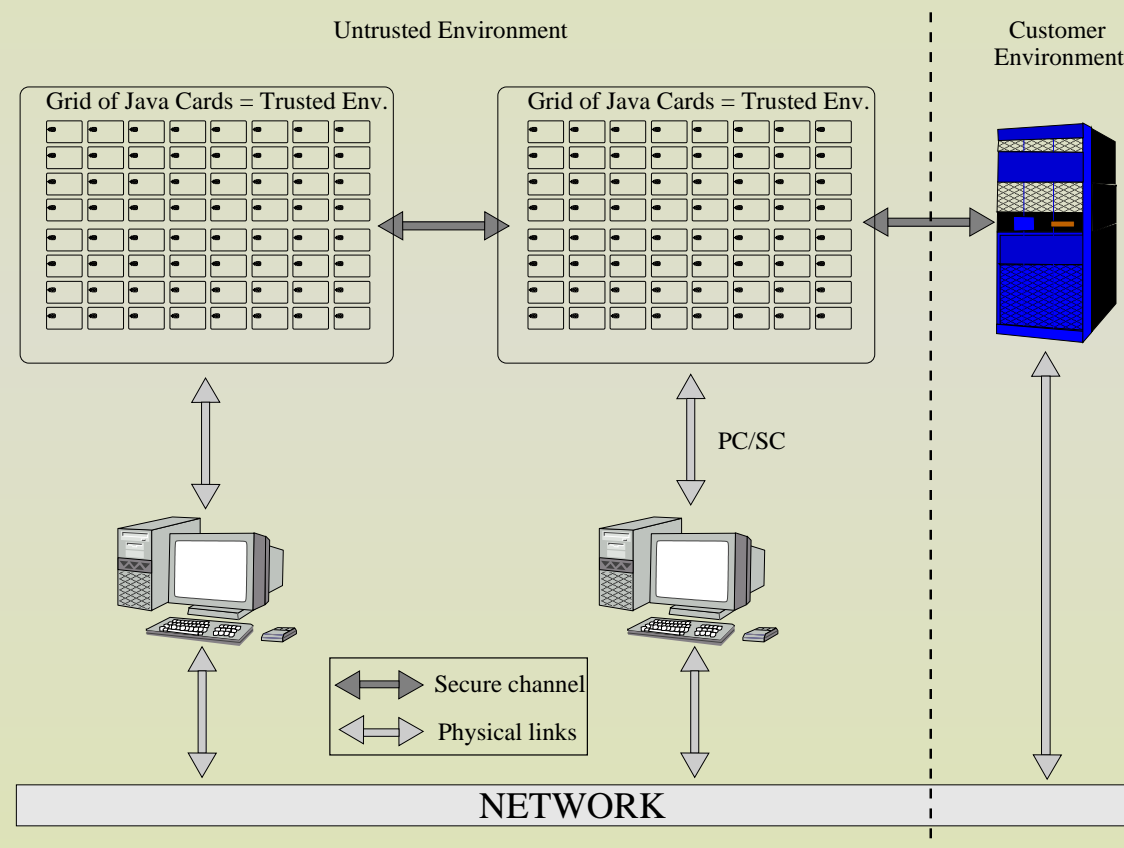


FIG. 1 – A solution for computing with Java Cards

## Le framework logiciel

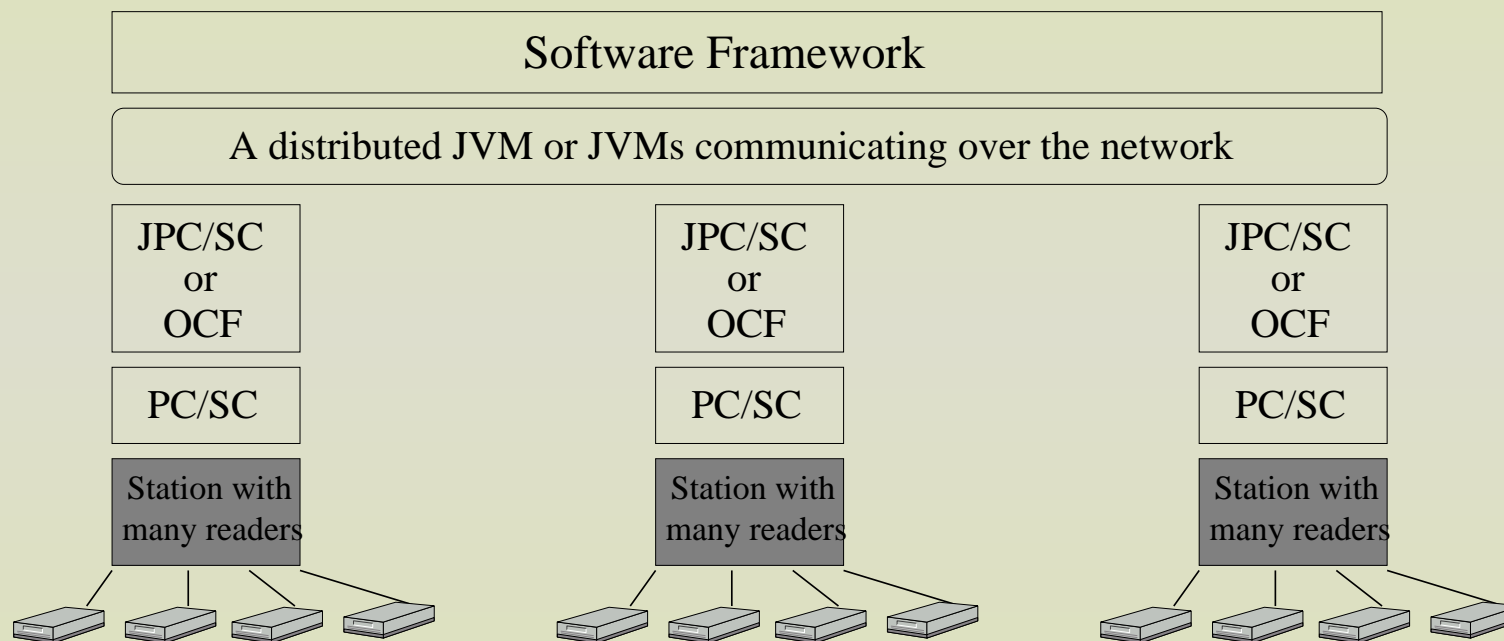


FIG. 2 – The software framework

## PC/SC

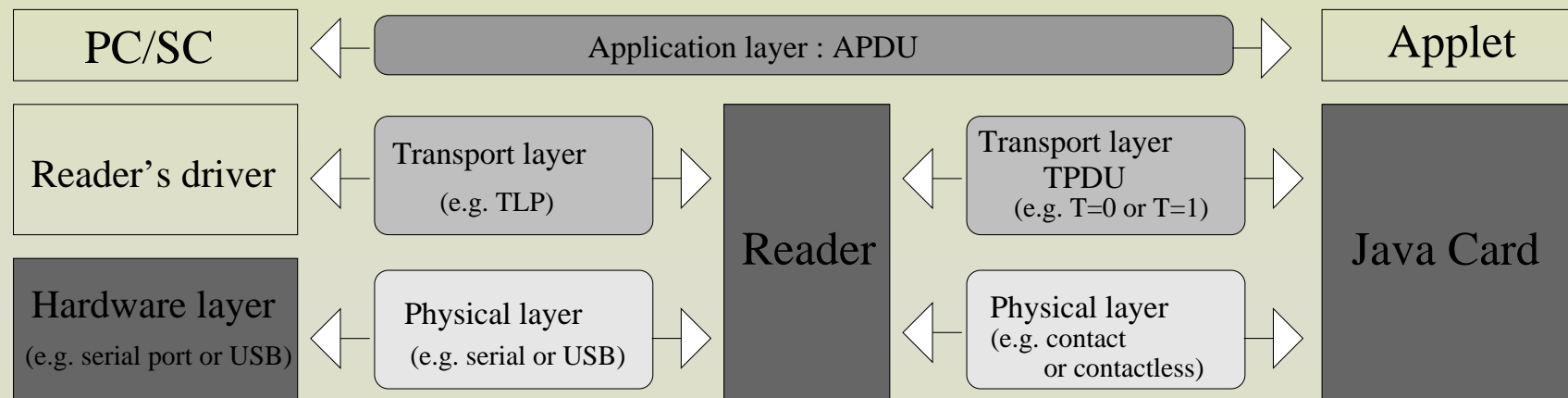


FIG. 3 – The PC/SC solution

PC/SC est un standard qui fournit :

- ☞ coté utilisateur une API de haut niveau pour dialoguer avec les lecteurs de carte à puce ;
- ☞ coté lecteur une interface à implémenter.

# La mise en place de la plate-forme

## Besoins :

- ☞ de bonnes connaissances des technologies Java, Java Card, OCF (OpenCard Framework), JPC/SC (JNI-wrapper for PC/SC) et PC/SC (Personal Computer/Smart Card) ;
- ☞ matériel :
  - lecteurs,
  - cartes,
  - connectiques ;

## Objectifs :

- utiliser les grands standards (Java, PC/SC) ;
- utiliser des systèmes ouverts au niveau du standard et du code (Java Card, PC/SC Lite – implémentation open source sous Linux).

## Le matériel (1/2)

### *Lecteurs :*

☞ avec contact :

- 10 Cardman2020 USB (Omnikey) ;

☞ sans contact :

- 1 pégoda MFEV 700 USB (Philips),
- 1 GemEasy Link 680SP série (Gemplus).

En cours de négociation avec SCM Microsystems pour du matériel (lecteur avec et sans contact).

## Le matériel (2/2)

---

### *Cartes :*

☞ avec contact :

- 19 GemXpresso PRO ;

☞ avec et sans contact :

- 10 JCOP31bio.

### *Connectiques et divers :*

☞ 2 hub USB 7 ports ;

☞ 4 clés USB 256 Mo.

## Utilisation de JCAT Emulator

JCAT Emulator est la machine virtuelle Java Card développée au sein de l'équipe SOD.

### **Idée :**

Lancer  $X$  instances de JCAT Emulator et établir notre framework dessus.  
 $\implies$  réduire les coûts matériels.

Nous avons développé un driver PC/SC permettant de se connecter à JCAT Emulator.

Le *middleware* PC/SC peut ainsi dialoguer avec notre émulateur.

# La mise en place de la plate-forme

## De la théorie à la pratique

---

### Problèmes :

- ➡ Nombreux bugs au niveau des drivers des lecteurs de beaucoup de constructeurs  $\implies$  Soumission de patch.
- ➡ Problème de verrou dans PC/SC Lite ;
- ➡ ...

# Perspectives

---

- ➡ Utilisation de la grille sur un cas réel.
- ➡ Application de notre expérience à tout périphérique connecté au réseau et possédant un haut niveau de sécurité.

Acceptation d'un article à CCCT'03 Orlando Floride et présentation en août.