

Le projet “Java CardTM Grid”



Damien SAUVERON
sauveron@labri.fr

<http://www.labri.fr/~sauveron/>

Présentation des grilles de calculs

Grille : ensemble de machines interconnectées.

Principe :

Partager de GROS calculs entre plusieurs machines.

Utilisateurs :

Organismes de la défense, CEA, laboratoires de recherche et universités, ...

Domaine d'utilisation :

Cryptographie, physique des particules, bio-informatique, observation de la terre, ...

Un des problèmes important : ***La sécurité !***

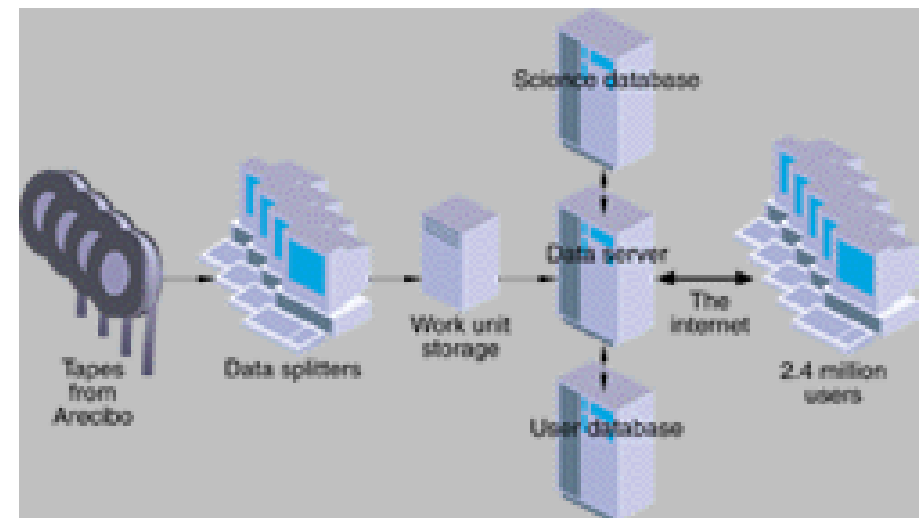
Quelques projets utilisant la grille



Décrypton

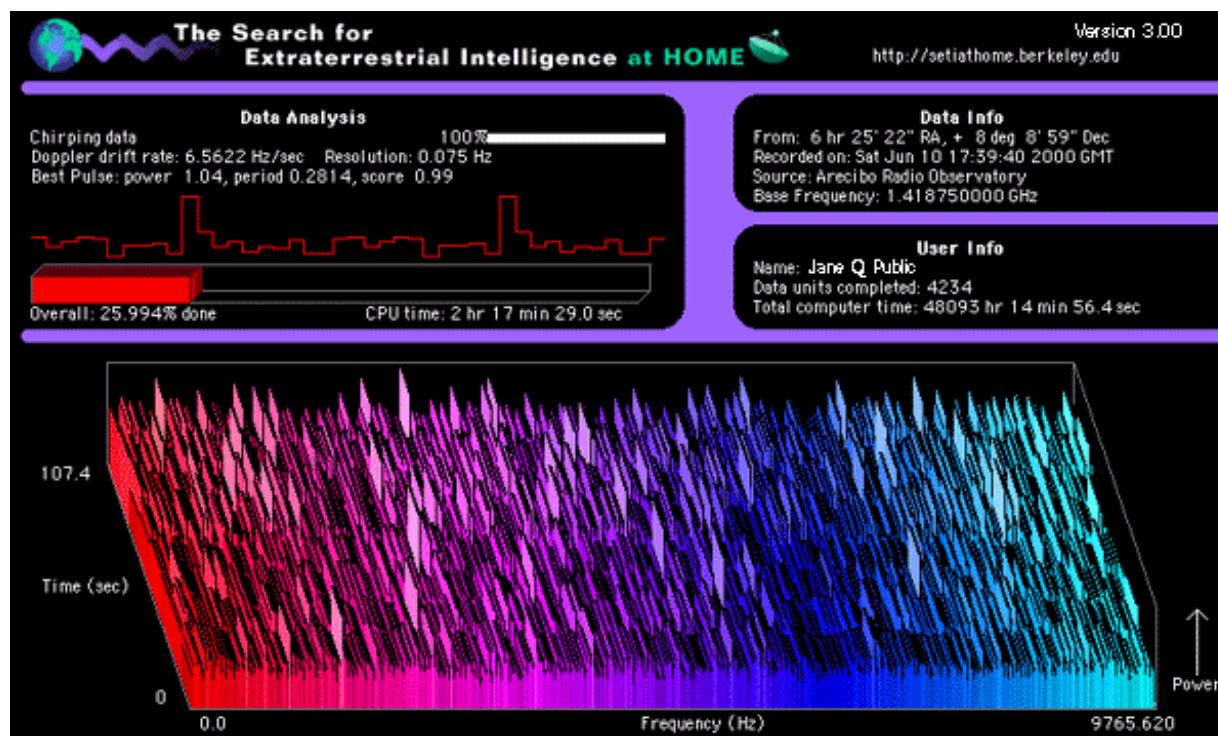
Seti@home

But : Recherche de signaux extra-terrestres.

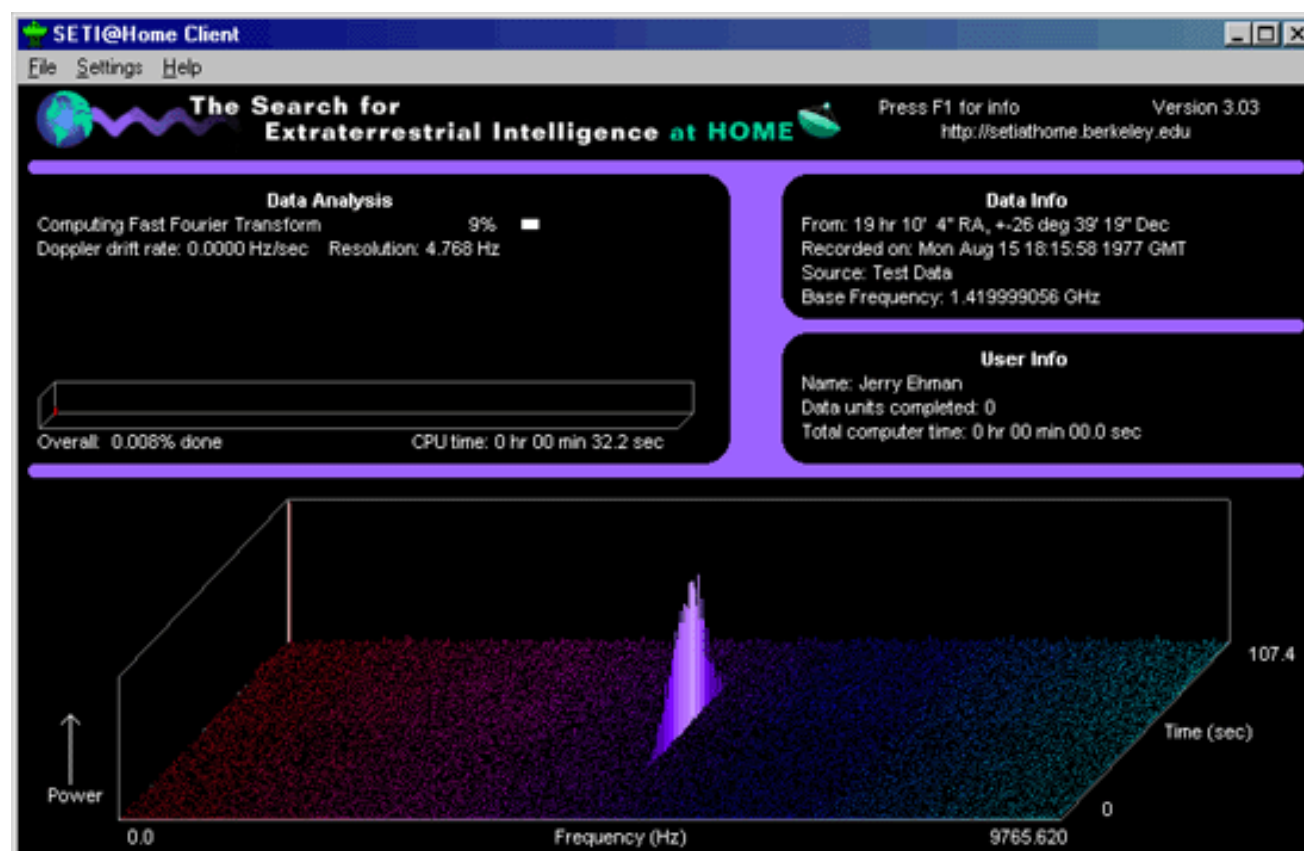


Les calculs

L'utilisateur télécharge un screensaver puis les données.



Les résultats



Nous ne
sommes PAS
SEULS dans
l'univers ?

SI! $\implies$ Il s'agit de résultats truqués! :-)

Les problèmes

Côté Seti@home :

- ☞ Les résultats positifs ou négatifs ne sont pas sûr.
 ⇒ *solution* : Faire calculer les mêmes données plusieurs fois par différents utilisateurs

Côté utilisateur final :

- ☞ Code source non disponible.
 ⇒ éviter les faux résultats.
- ☞ Que fait le code sur la machine de l'utilisateur ?

Le projet “Java Cards Grid”

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, ...

Le projet “Java Cards Grid”

Java Card fournit la Pull Security

Pull Security (resource provider) : le fait d’être sûr que quand vous téléchargez un programme sur le réseau, il ne sera pas dangereux ni pour votre machine ni pour les autres codes qui tournent dessus

➡ Approche Sand box : Firewall (JCRE) + verifier Java Card (JCVM)

Le projet “Java Cards Grid”

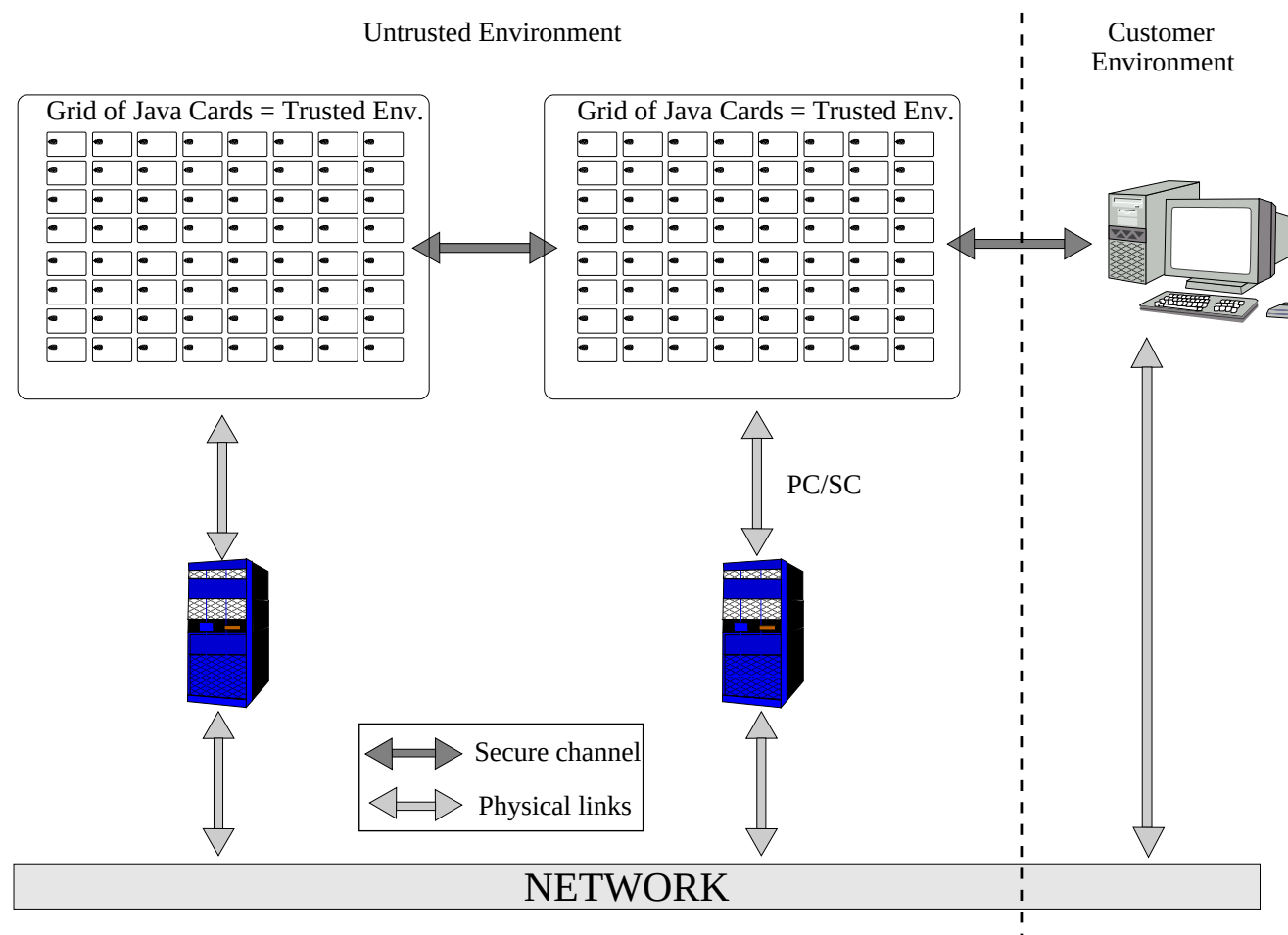
Java Card fournit la Push Security

Push Security (grid user) : le fait d’être sûr que quand vous installez un programme sur une ressource de calcul du réseau, le code restera confidentiel et ne sera espionné par personne.

☞ Firewall (JCRE)

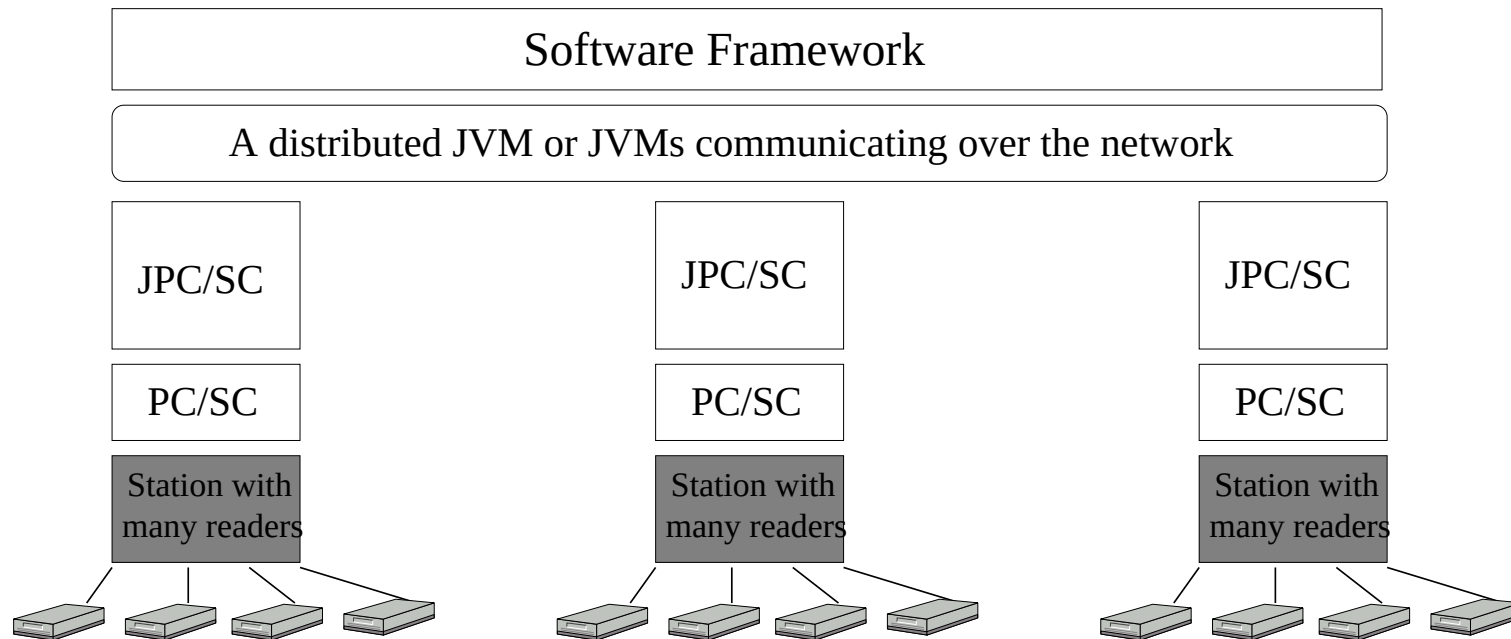
Le projet “Java Cards Grid”

Notre proposition



Le projet “Java Cards Grid”

La plate-forme logicielle



Le projet “Java Cards Grid”

PC/SC

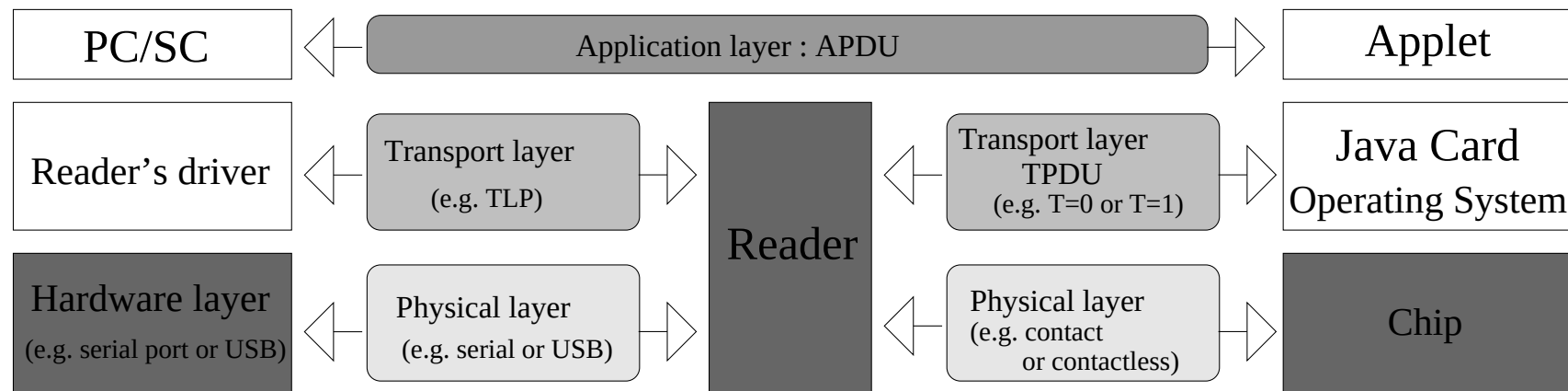


FIG. 1 – The PC/SC solution

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.

Le projet “Java Cards Grid”

La réalisation



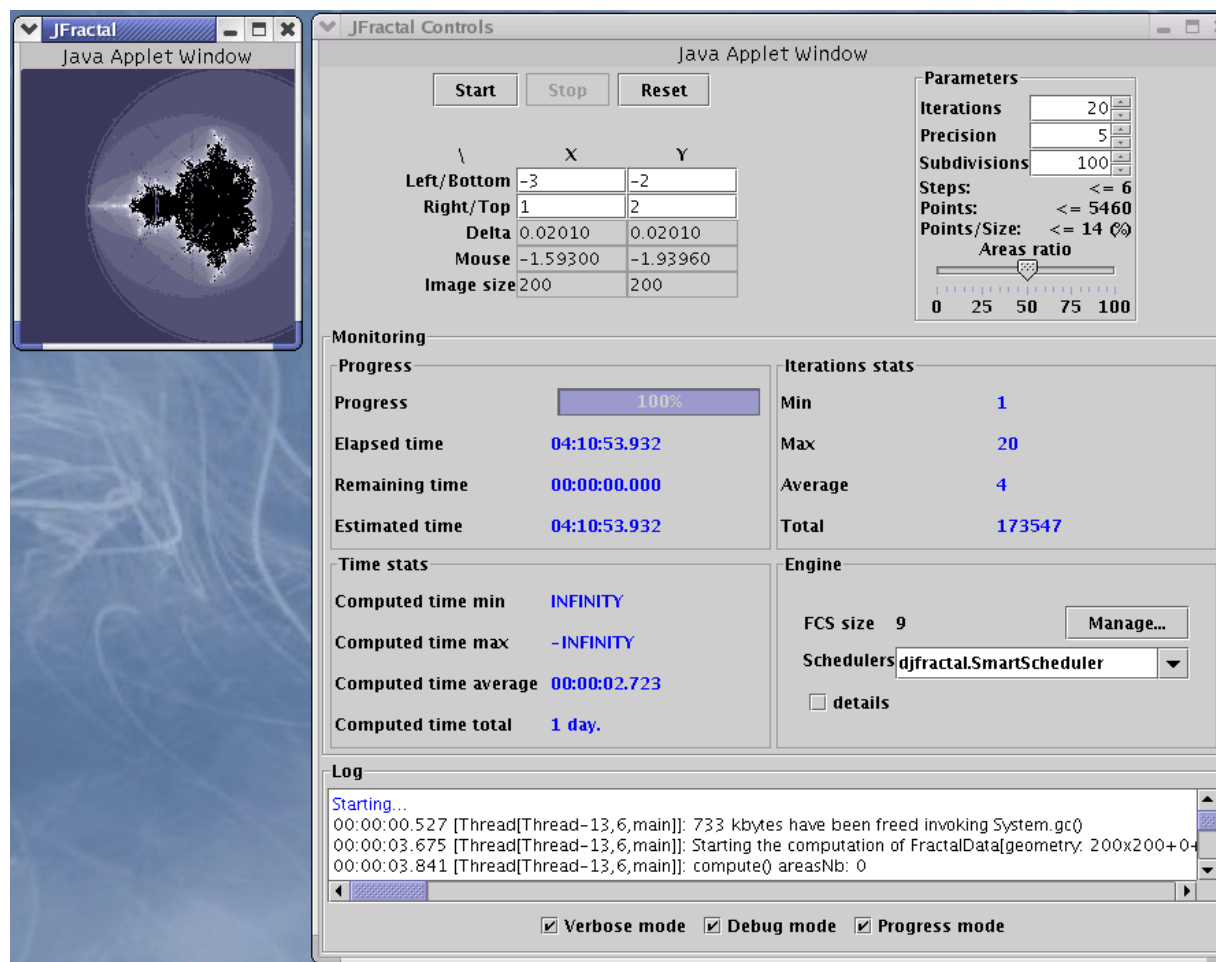
Le projet “Java Cards Grid”

Avantages de la plate-forme

- ➡ Peu coûteux : 1500 euros pour toute la plate-forme.
- ➡ Sécurité intégrée.
- ➡ Langage de programmation et runtime identiques sur toute la plate-forme : Java.
- ➡ Tests faciles de certaines caractéristiques (*e.g.* mobilité).

Le projet “Java Cards Grid”

Première démonstration



Le projet “Java Cards Grid”

Quelques benchmarks

9 Java Card onto Fujitsu mb94r215b (FRAM)	122 min
9 GemXpresso Pro R3 E32PK	202 min
9 JCOP31bio	253 min
9 GemXpresso Pro R3 64PK	376 min
9 SmartC@fé Expert	389 min

TAB. 1 – Benchmarks sans secure channel

Scalabilité en cours d’expérimentation.

1 Java Card onto Fujitsu mb94r215b (FRAM) $\implies 18heures = 9 * 120min$

Le projet “Java Cards Grid”

Les partenaires

Sponsors



IBM BlueZ Secure Systems



Supports



Giesecke & Devrient



Le projet “Java Cards Grid”

Résultats et perspectives

- ➡ 1 papier élu meilleur article de la session *Computer and Systems Security* CCCT'03.
- ➡ 1 poster présenté à Cartes 2003.
- ➡ 2 applications de démo.
- ➡ 1 papier en cours.
- ➡ 2 thèses en préparation (début septembre 2004).