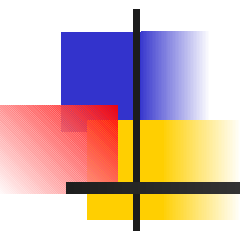


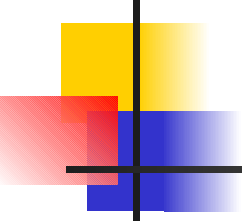
The Software Infrastructure of a Java Card based Security Platform for Distributed Applications



Serge Chaumette, Achraf Karray, **Damien Sauveron**

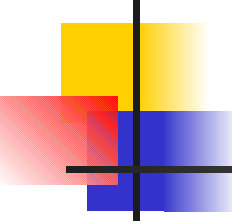
Contact: damien.sauveron@labri.fr

LaBRI, UMR CNRS 5800
Université Bordeaux 1
FRANCE



Copyright

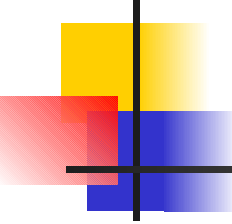
Java and all Java-based marks are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries. The authors are independent of Sun Microsystems, Inc.



How things are evolving

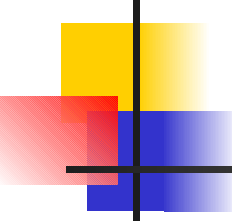


- The network is every where
 - Internet, GPRS, UMTS, IRDA, BlueTooth, 802.11, WUSB.
- The resources are every where
 - Workstations, PCs, embedded systems, next generation Smart/Java Cards
- Make these resources usable in a secure way
- We believe that Java Cards are a good platform to experiment with



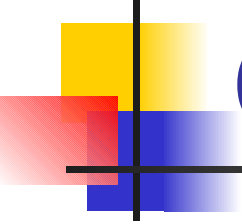
Our vision and approach

- Goal
 - Securisation of resources (including applications)
- How
 - Use smart (Java) cards
- Two main phases
 - Prototype as a Java Card Grid
 - Map this approach to real, possibly mobile, grids
 - bigger processors
 - underlying infrastructure to support a higher level grid



Examples

- Seti@home like applications
 - Search for ExtraTerrestrial Intelligence at Home
- Decryphon by IBM
- Applications that require code/data confidentiality
 - data mining
 - medical information
 - ...



Outline of the presentation

- Rational for a Java Card Grid
 - see previous slides
- Smart (Java) Card Technology
- The Java Card Grid Platform
- Services in the Java Card Grid
- Conclusion and Future Work

Smart Card Technology



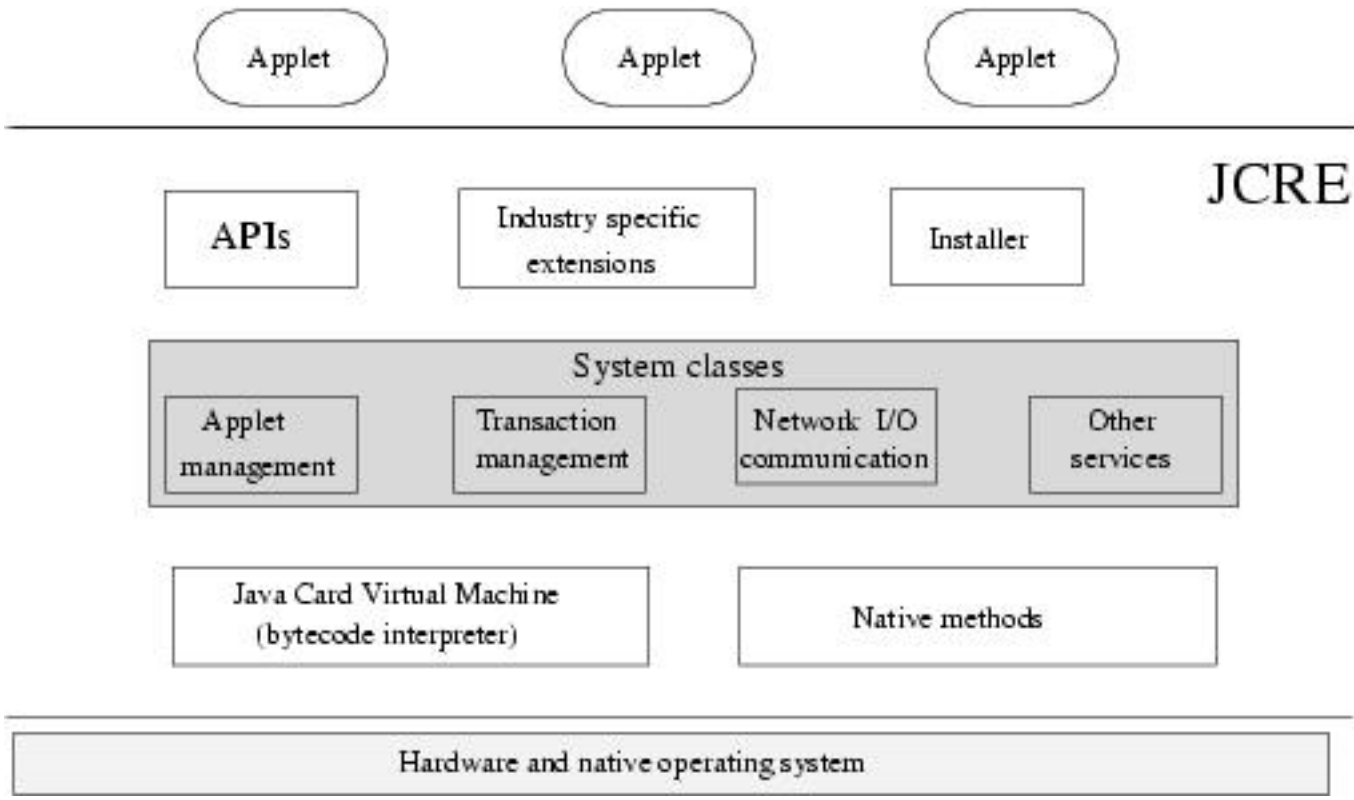
- Security
 - Software level
 - Hardware level
- Certification procedures
 - Common Criteria
ISO15408
 - ITSEC

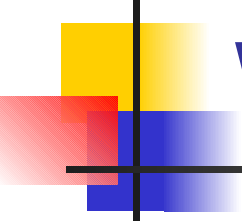
Java Card Technology



- Java Card Forum
- Embedded *jcv*
- Multiple *applets*
- Dynamic

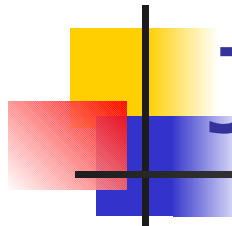
Overview of the Java Card Architecture





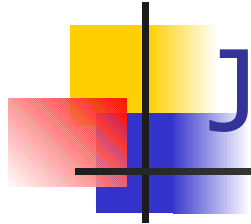
Why Java Cards ?

- Pull security
- Push security
- Java



Java Cards provide Pull Security

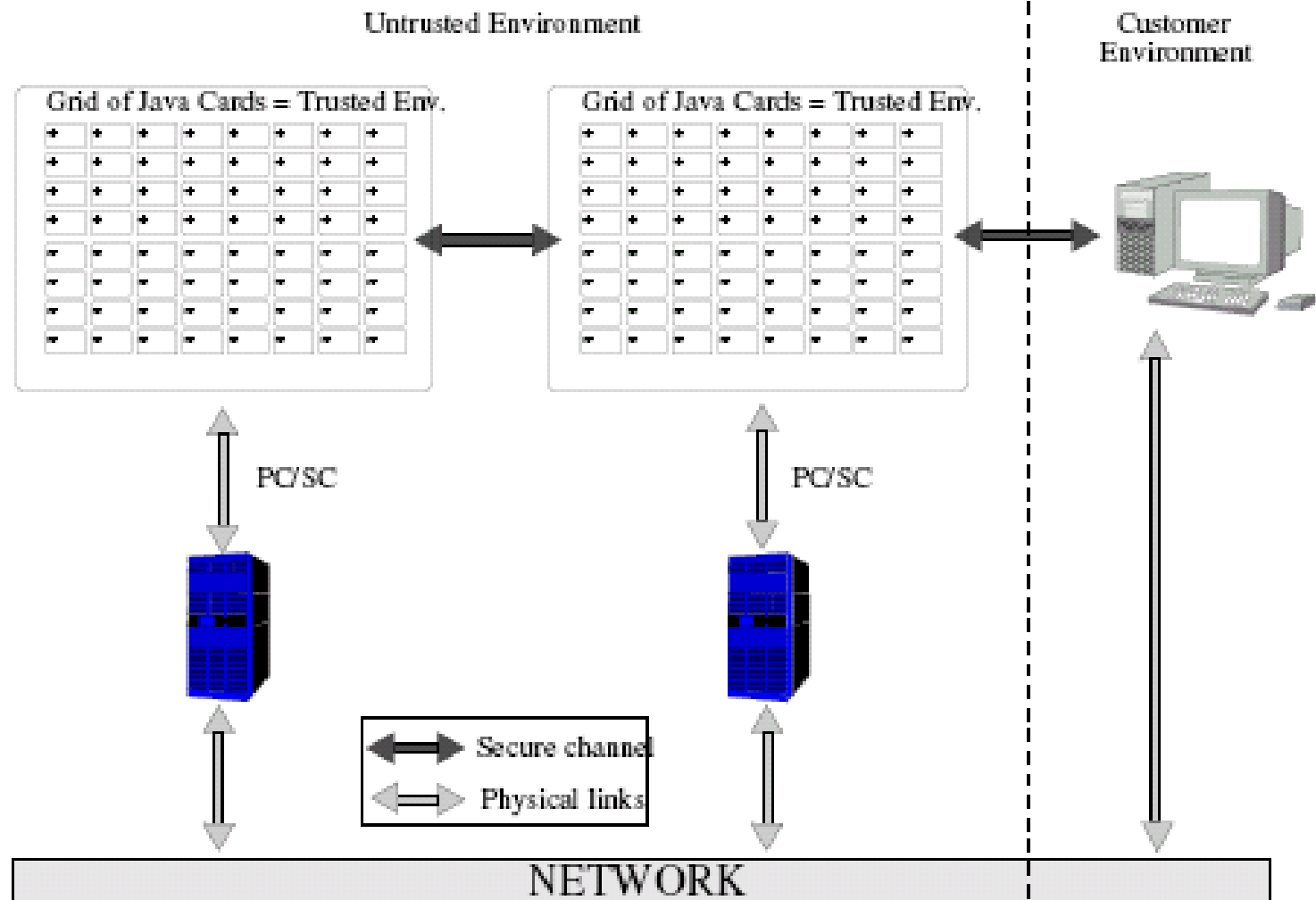
- The fact that when you download a code from the network, you are sure that it cannot be harmful neither for your processing element nor for the other codes that it is running
- Sand box approach
 - *Using Memory Errors to Attack Virtual Machine*



Java Cards provide Push Security

- The fact that when you upload a code to a computing resource of the network you are sure that your code remains confidential and cannot be spied by anyone
- JCRE firewall

The Java Card Grid Platform



The initial platform that we have set up (2003 ?)

- Readers
 - Contact
 - 2 Gemplus, 10 Omnikey, 6 SCM Microsystems,
 - Contactless
 - 1 SCM Microsystems
 - 1 Philips
 - 1 Gemplus
- Cards
 - Contact
 - 24 Gemplus, 4 DataCard, 2 Giesecke & Devrient
 - Hybrid (contact and contactless)
 - 12 IBM

[The Java Card Grid Platform]



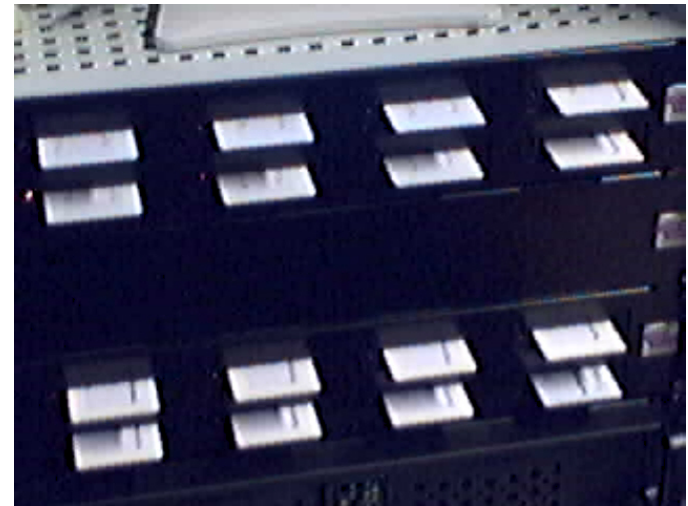
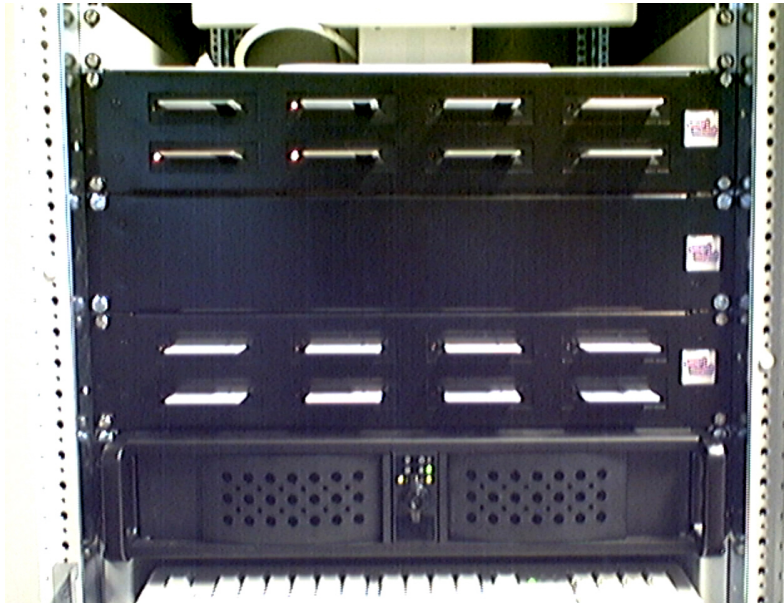
[The Java Card Grid Platform]



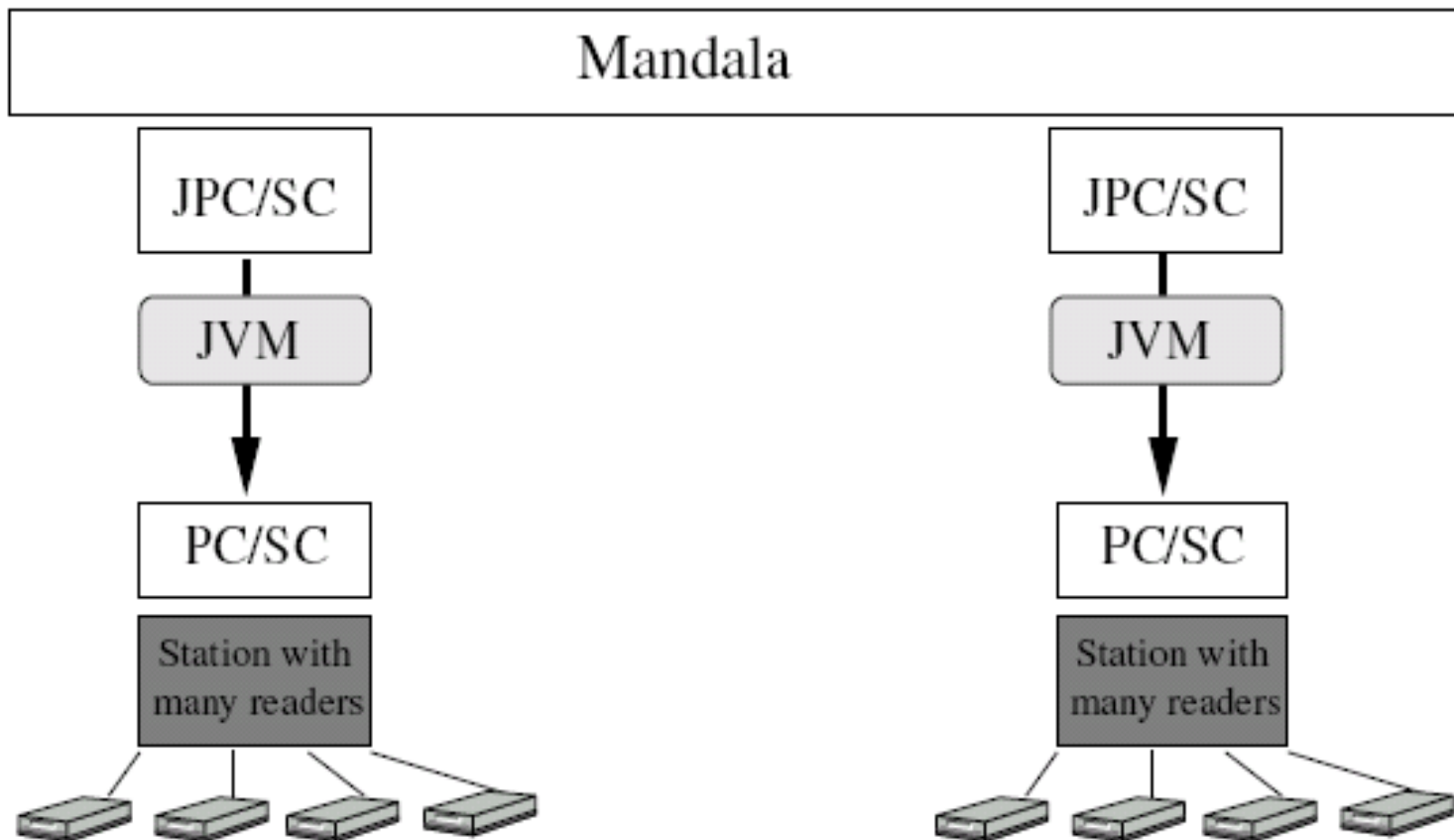
The current platform

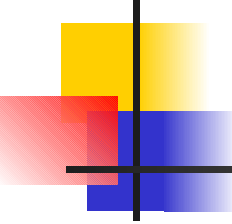


- 2 times
 - 1 PC
 - 16 USB card readers
 - WiFi access point
- The two computers are connected together (wire)



The software framework

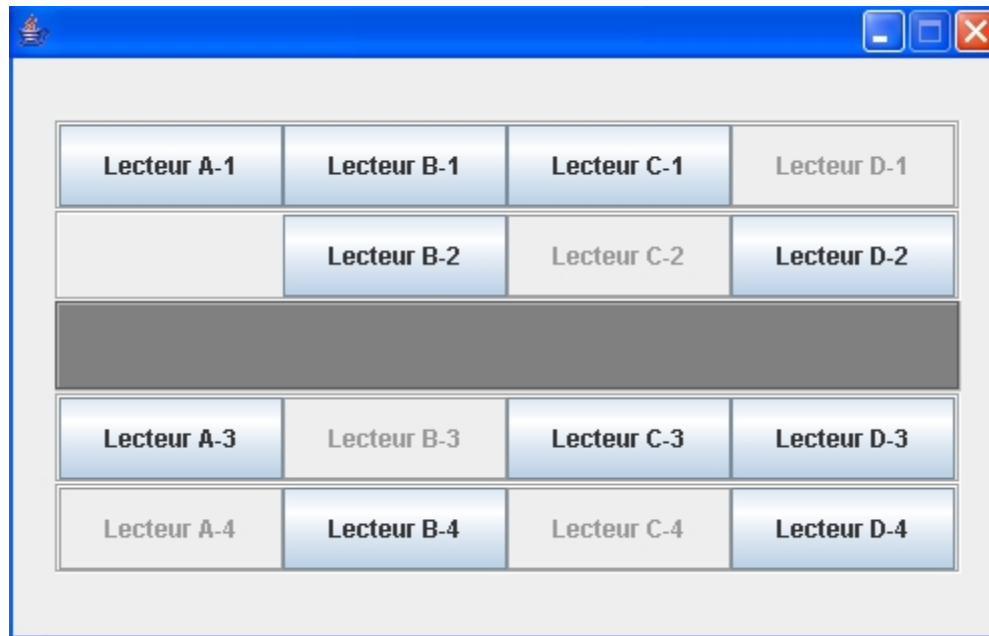




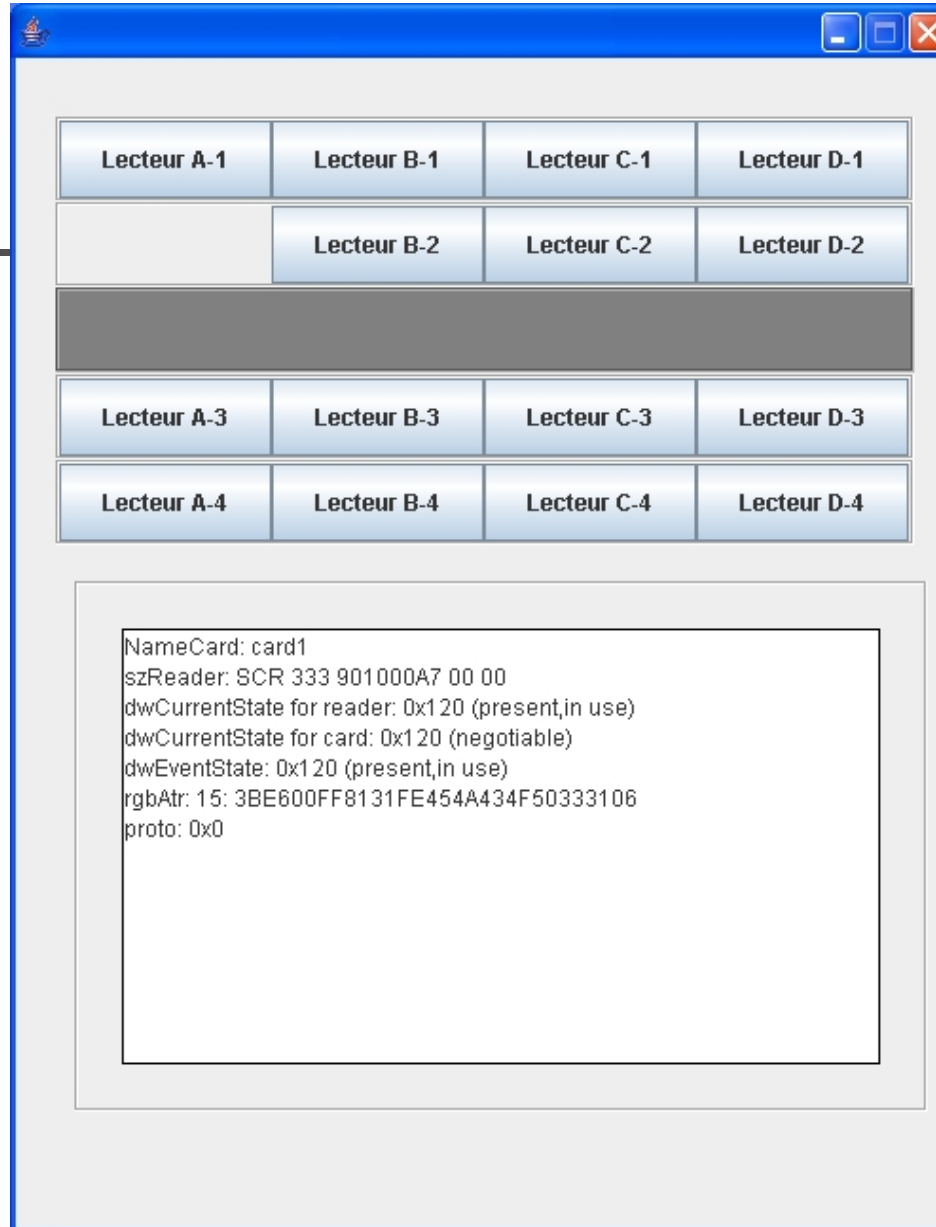
Advantages of the platform

- Low cost
 - 3000 \$ for the whole platform
- Built-in security (at least inside cards)
- Common programming language and runtime
- Features easy to test (on/off, breaking connections, ...)

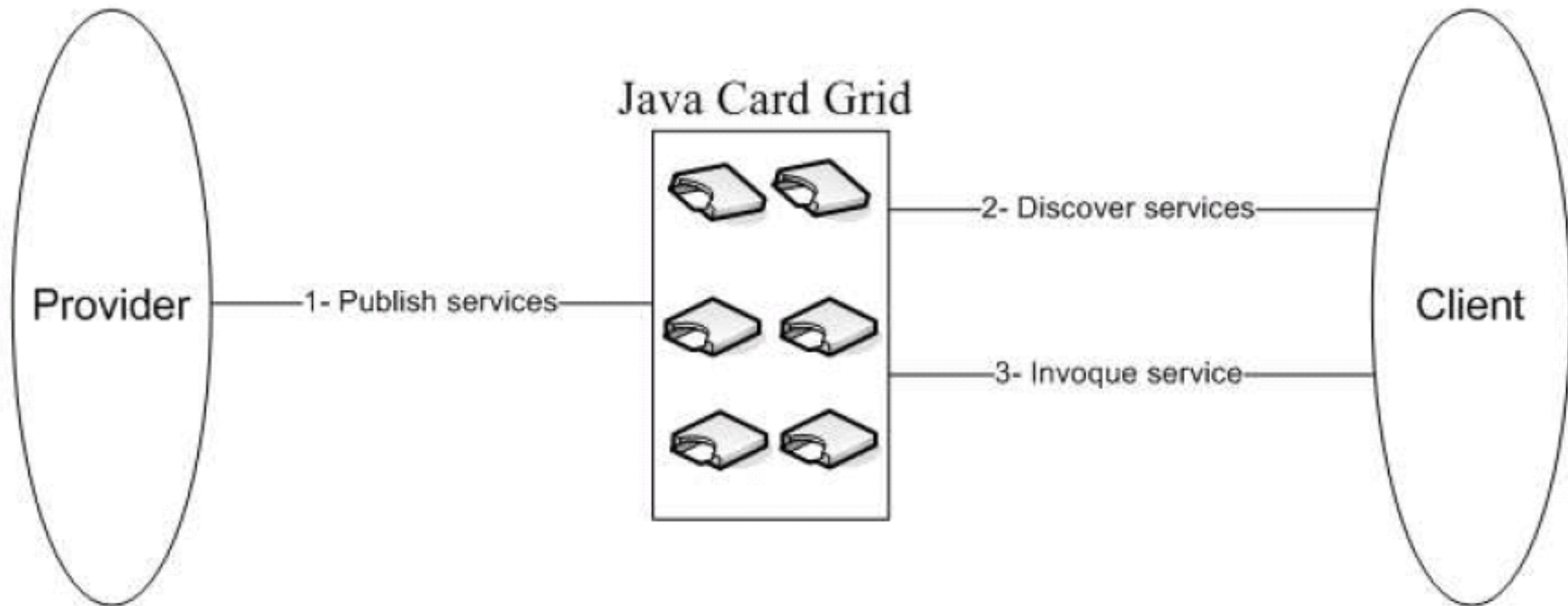
Administration environment



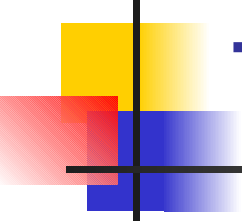
[The Java Card Grid Platform]



Services in the Java Card Grid



- A service is represented by a XML description
- A catalog of services is maintained in each card
- ➔ a global catalog is built/maintained that is passed to client applications



Two kinds of services

- Stand alone services or services that are composed outside of the Grid

- Distributed inter card services
 - services that use other services
 - this is basically a distributed application that uses collaboration of services

Service collaboration: Proactivity

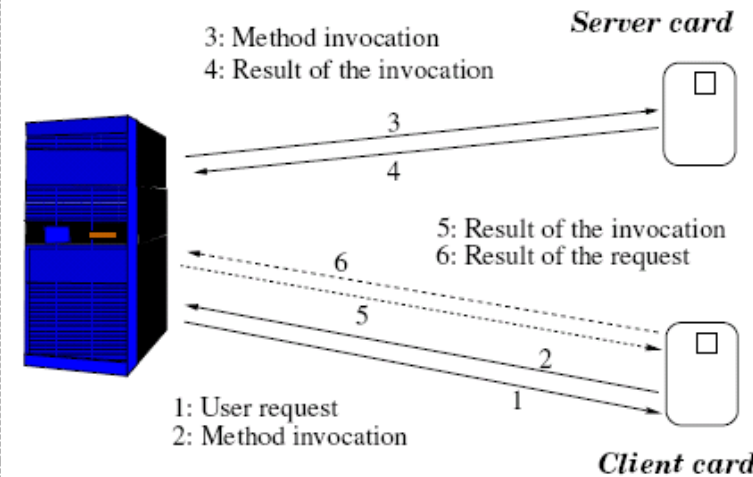
Client Environment



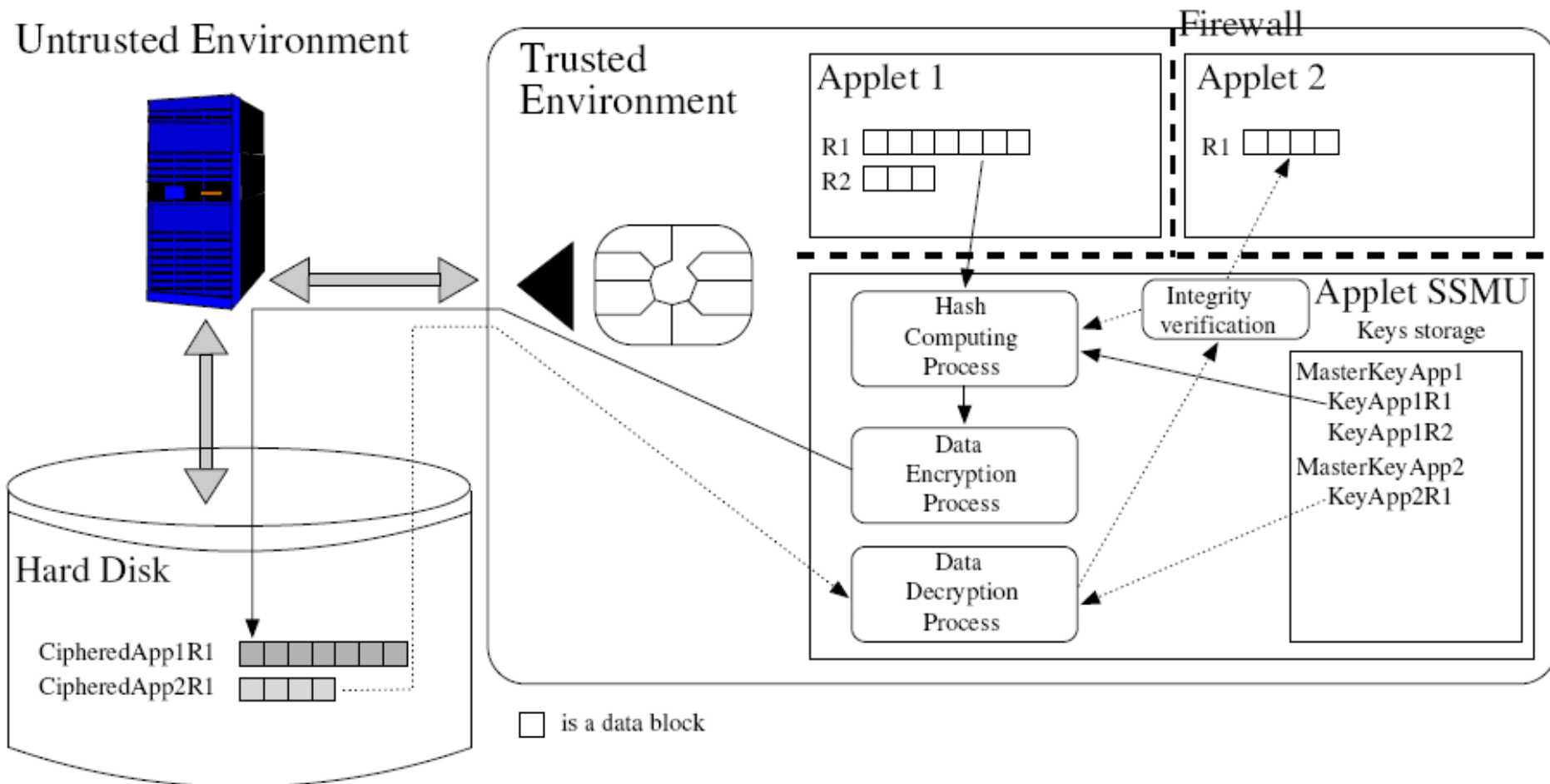
Untrusted Network



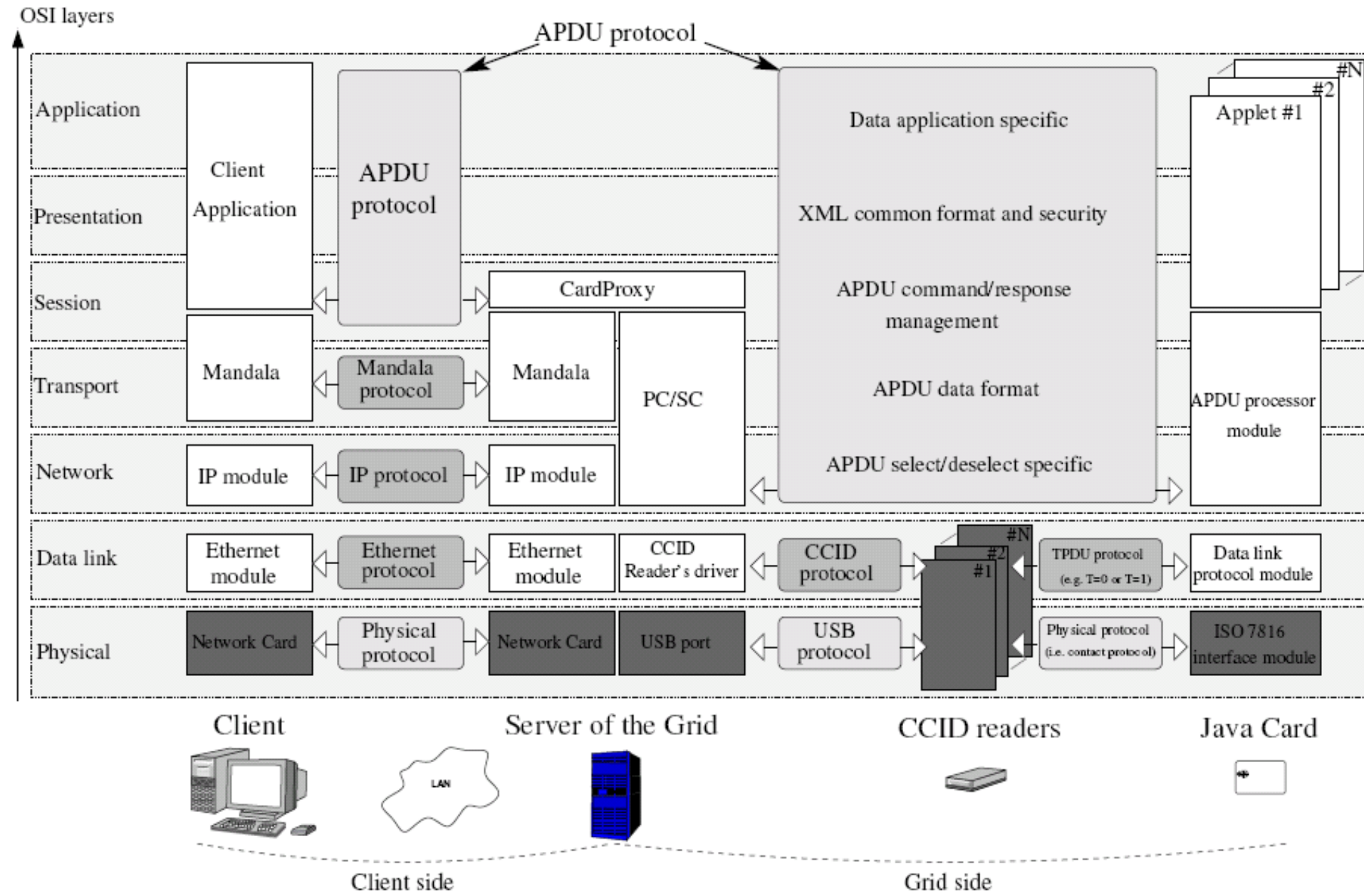
Java Card Grid

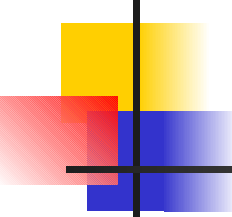


Extended Memory in the JCG



Communication stack (OSI)

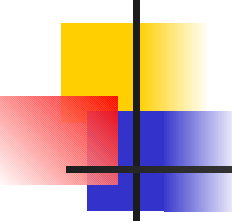




Current Status

- The platform is working
- « Best innovative technology » award at e-smart 2005
- Invited paper at HPC&S 2006

- Under development
 - Failure management
 - Composition of services



Perspectives

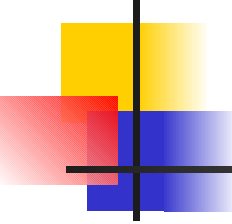
- Scaling
 - With 1000 cards/readers (supported by a private company)
- With real processors
 - e.g. Trusted Computing Group
- With real grids
 - Using the ProActive framework
(INRIA, Nice)
 - Using a mobile grid
(Smart Card Centre, ISG @ Royal Holloway, Univ. Of London)

Support

- National Research Agency
- University Bordeaux 1
- French Cooperation Institute
- XLIM, University of Limoges

- Sun Microsystems
- IBM
- Oberthur
- Gemplus
- Axalto
- Smartmount
- SCM microsystems
- Giesecke & Devrient GmbH
- Fujitsu





The Java Card Grid

Questions ?

