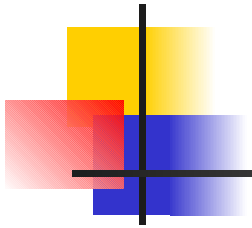
Extended Secure Memory for a Java Card in the context of the Java Card Grid project

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

damien.sauveron@xlim.fr
serge.chaumette@labri.fr

LaBRI, UMR CNRS 5800
Université Bordeaux 1
FRANCE



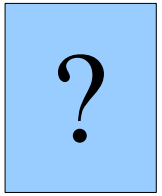
Copyright

Partners of the project

LaBRI

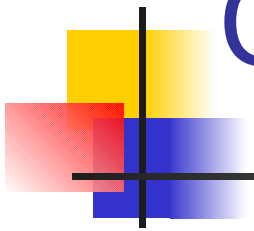
Pr. Serge Chaumette

PhD Student: Achraf Karray



XLIM

Dr. Damien Sauveron



Outline

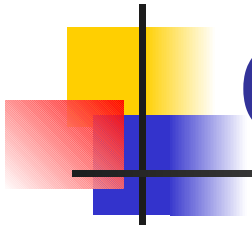
- The Java Card Grid
  - Rational for the Java Card Grid
  - Static Java Card Grid
  - Mobile Java Card Grid
- Java Card Memory Extension
  - Java Card Usage Justification
  - Objectives & Constraints
  - Technical Details
- Applications
- Conclusions & Future Work

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

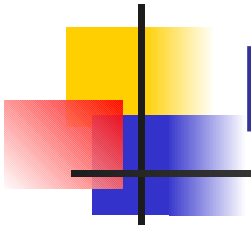
➔ Make these resources usable in a secure way

- 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

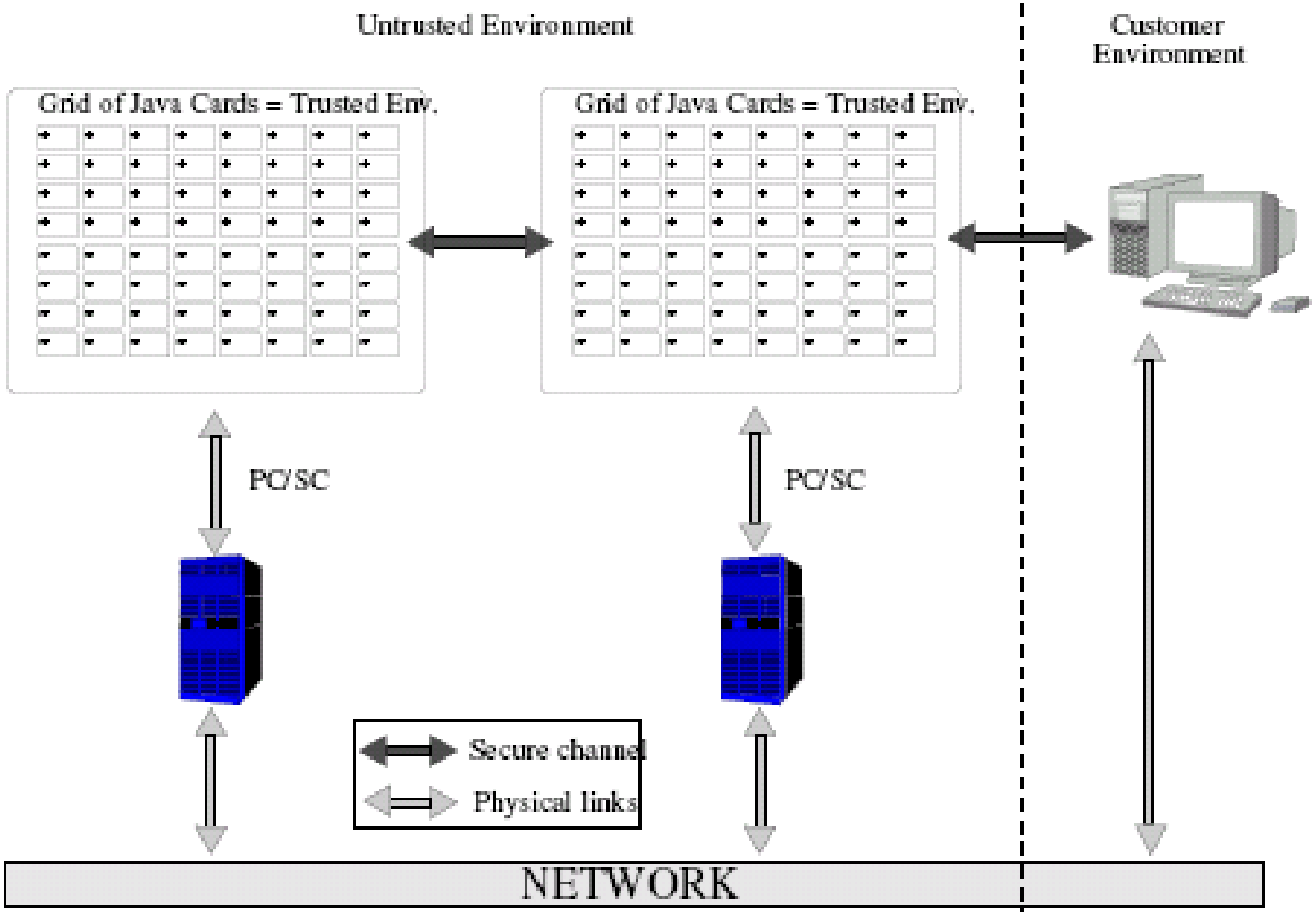


Examples of Grids

- Seti@home-like applications
  - Search for ExtraTerrestrial Intelligence at Home
- Decrypthon by IBM

- Applications that require code/data confidentiality
  - data mining confidential data
  - medical information management
  - …

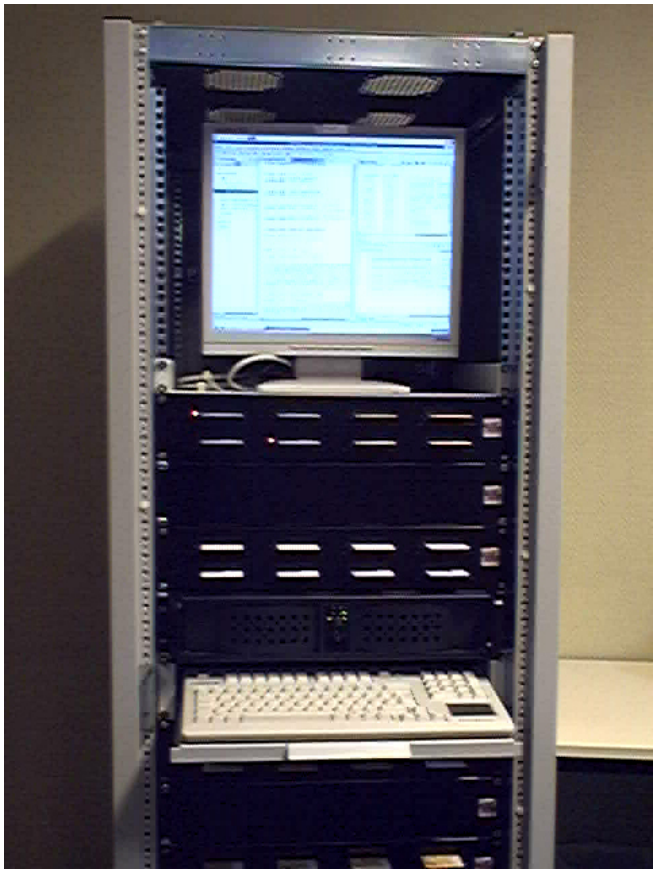
The Java Card Grid Platform




2003
CHIPDRIVE extern
SCM

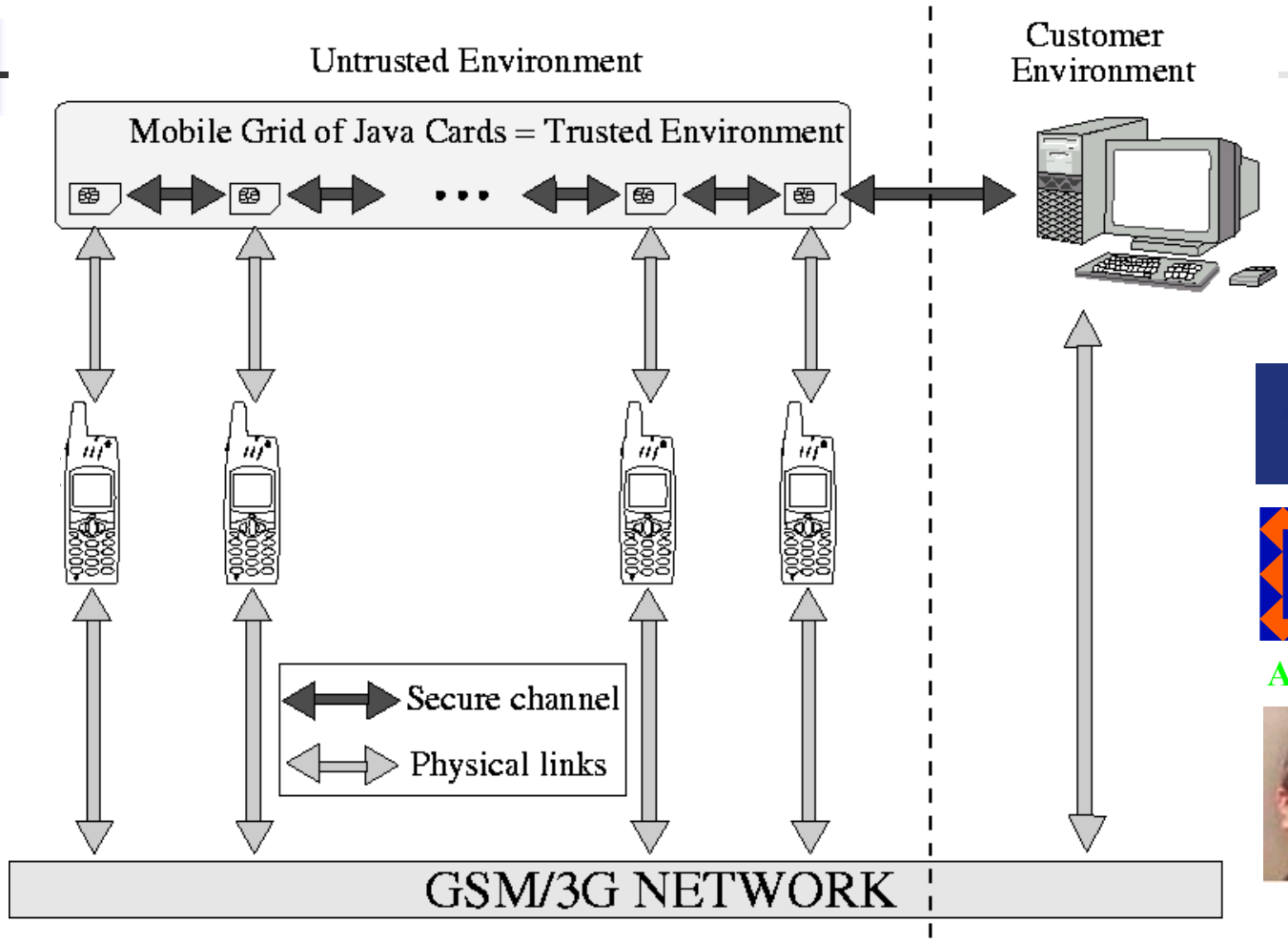
The current static platform

- 2 times
  - 1 PC
  - 16 USB card readers
  - WiFi access point
- The two computers are connected together (wire)
- Awards:
  - « Best innovative technology » at e-Smart 2005 (France)
  - Invited paper at HPC&S 2006 (Germany)



- The platform is working

The Mobile Java Card Grid



Smart Card Centre
Royal Holloway

Royal Holloway
University of London

Additional partners

Keith Mayes

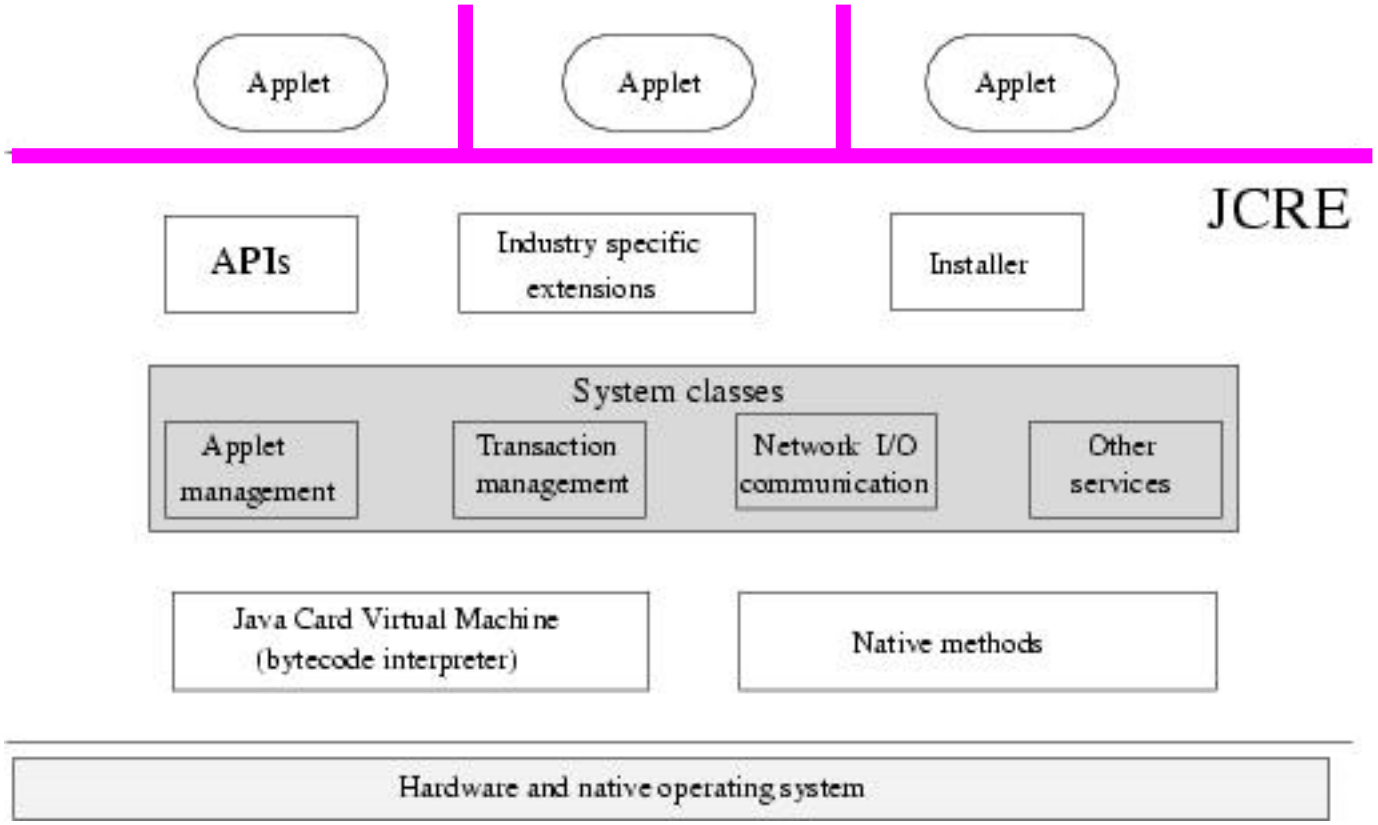
Kostas Markantonakis

Prospective project in development with ISG-SCC of the Royal Holloway, University of London

Smart Card Technology

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

Overview of the Java Card Architecture

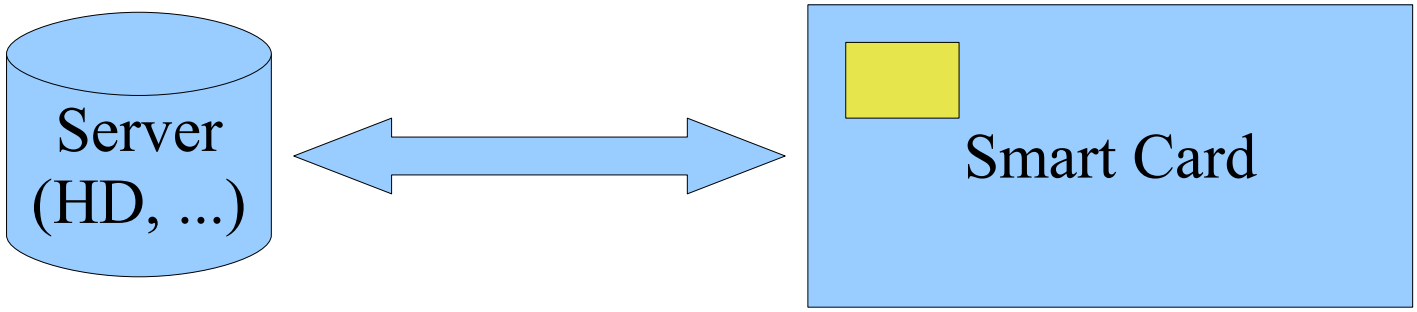


- Embedded *jcvm*
- Multiple *applets*
- Dynamic
- **Firewall**

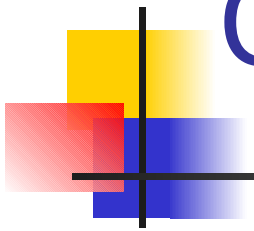
Our main problem

- Memory constraints
  - For the working memory (a few KB): RAM
  - For the storage memory (a few hundreds of KB): EEPROM
  - Difficulties to support real size applications in our grid
- Solutions
  - 1) Wait for the next generation of card with 1GB
  - 2) Develop a new solution

Extended Secure Memory



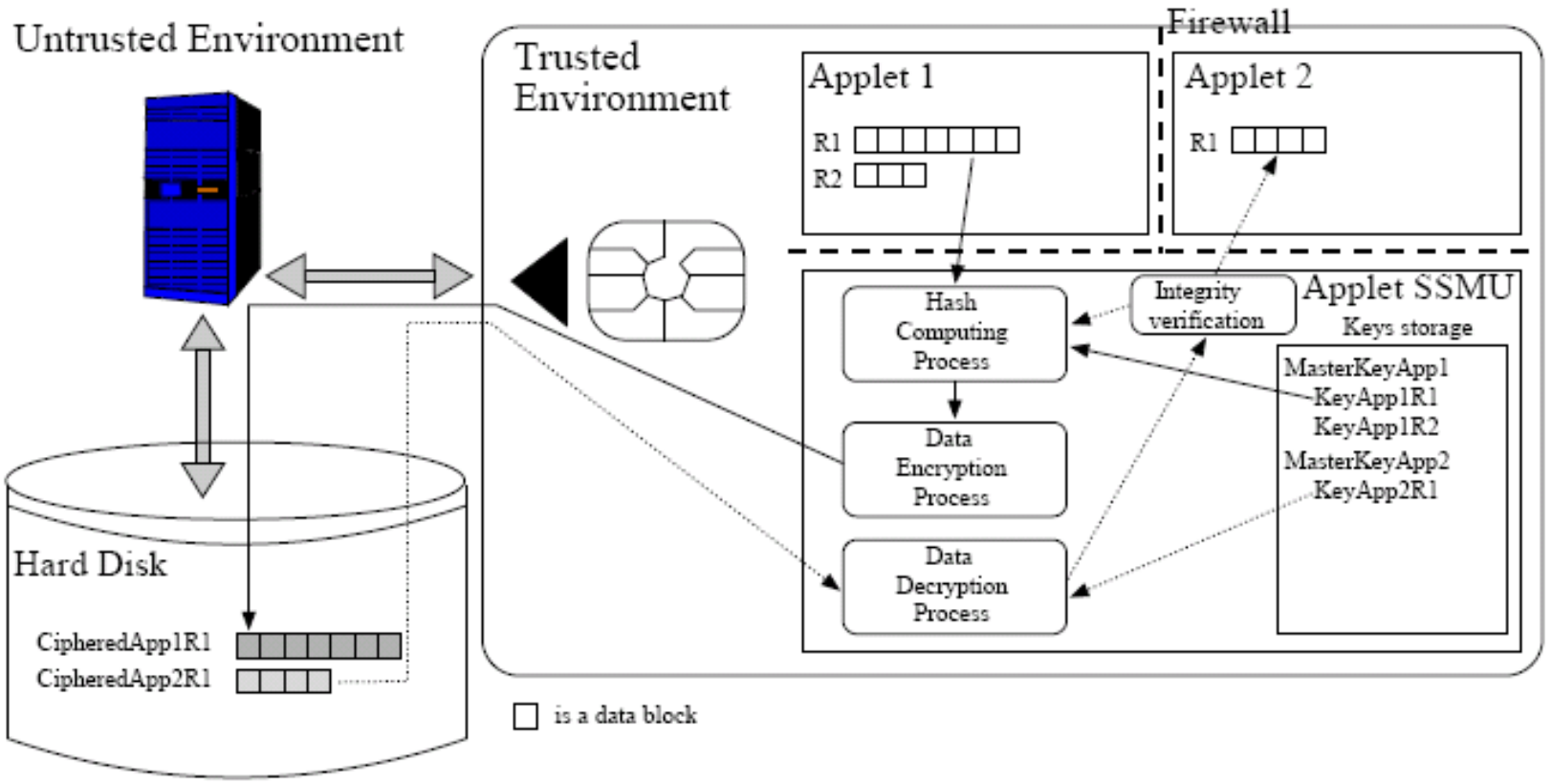
- Considered as a major application for the future smart cards in the course of D. Donsez, Gilles Grimaud, Sylvain Lecomte, Pierre Paradinas and Jean-Jacques Vandewalle.



Objectives & Constraints

- Extend the memory
  - In a secure way according to
    - The smart card security models:
      - Integrity (tamper resistant hardware/software mechanisms)
      - Confidentiality (tamper resistant hardware/software mechanisms)
    - The Java Card Policies:
      - Firewall between the applications
  - In a flexible and transparent way (in Java Card philosophy)
  - For short and long term
  - Minimize the memory space used by information needed for the extension

Details of the solution



- One dedicated Applet (Applet SSMU) called through the firewall (SIO) to transparently extend the memory
- One master key/Applet
- One subkey/record of each applet

Integrity Process

- Ensuring integrity
  - Compute SHA-1 with plaintext data
  - Store the value on the card
  - Next step is confidentiality
- Verification
  - Get the deciphered data and compute SHA-1
  - Compare it with the saved value
    - Valid or Invalid

Confidentiality Process

- We want to ensure PFS/PBS
  - Generate a random MasterKey / applet
  - Derive subkeys for Applet records from the MasterKey and 2 random bytes (V1, V2)

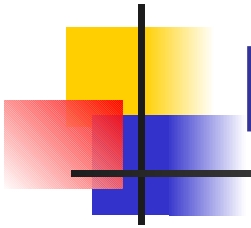
$$KeyAppxRy = SHA_{1-16}(MasterKeyAppx \oplus \{V1V2V1V2V1V2V1V2V1V2V1V2V1V2V1V2\})$$

- Records are ciphered with AES in CBC mode using subkeys and an IV derived from the MasterKey too:

$$IV = SHA_{1-16}(MasterKeyAppx \oplus \{\neg V1\neg V2\neg V1\neg V2\neg V1\neg V2\neg V1\neg V2\neg V1\neg V2\neg V1\neg V2\neg V1\neg V2\})$$

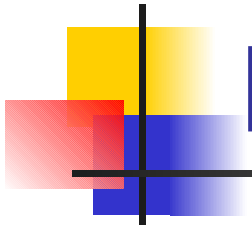
Applications in the grid that can take advantage from the memory extension

- Datamining of confidential data
  - e.g. FBI/European airway companies
    - Distributed database on the Java Card grid with data owned by the airway companies and code (running in the cards) owned by the FBI
- Secure storage
  - Dedicated ciphering/deciphering systems
- …



Perspectives (1/2)

- Privacy problems?
  - (work in progress)
- Detailled study of our cryptographic choices with cryptographs and cryptanalists
  - Relationship between the keys
  - Relationship between keys and IV
  - Choice of cryptographic primitives
  - (work in progress)
- Find new applications



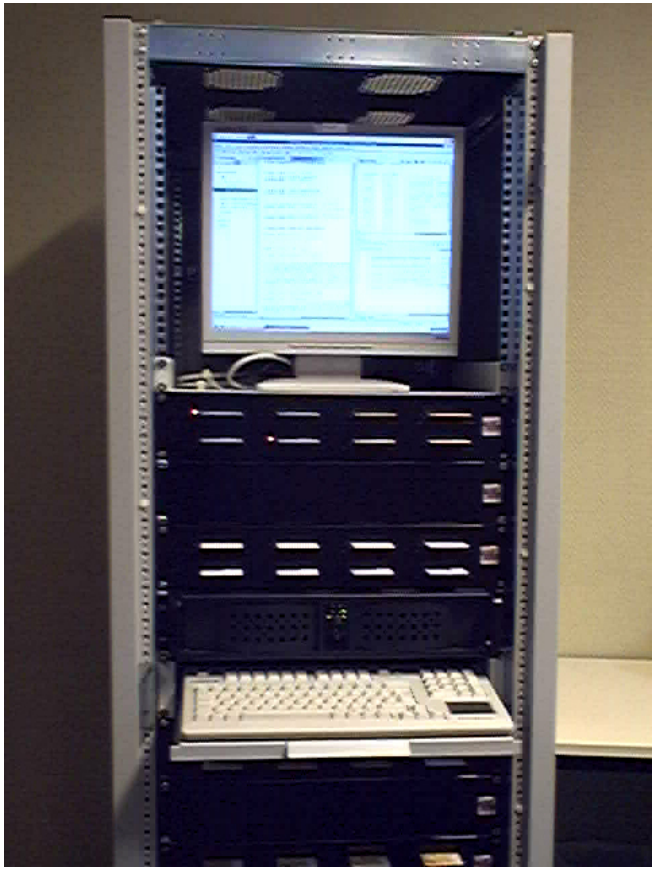
Perspectives (2/2)

- 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
- LaBRI, University Bordeaux 1
- French Cooperation Institute
- XLIM, University of Limoges

- Sun microsystems
- IBM
- Oberthur
- Gemalto (Gemplus + Axalto)
- Smartmount
- SCM Microsystems
- Giesecke & Devrient GmbH
- Fujitsu



The Java Card Grid

Questions ?