



Inspired Training Workshop

“The future of Smart Cards”

ENST Paris, Wednesday - December 13th



The Mobile Java Card™ Grid Project

Serge Chaumette, Konstantinos Markantonakis,
Keith Mayes, and **Damien Sauveron**

damien.sauveron@xlim.fr

<http://damien.sauveron.free.fr/>

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.



AGENDA

- Members of the project
 - The Mobile Java Card Grid
 - Overview
 - Framework
 - Challenges
 - Future applications
 - Conclusions & Perspectives
 - Thanks
-
-

MEMBERS



Smart Card Centre
Royal Holloway



Royal Holloway
University of London



- Konstantinos Markantonakis
- Keith Mayes



- Serge Chaumette

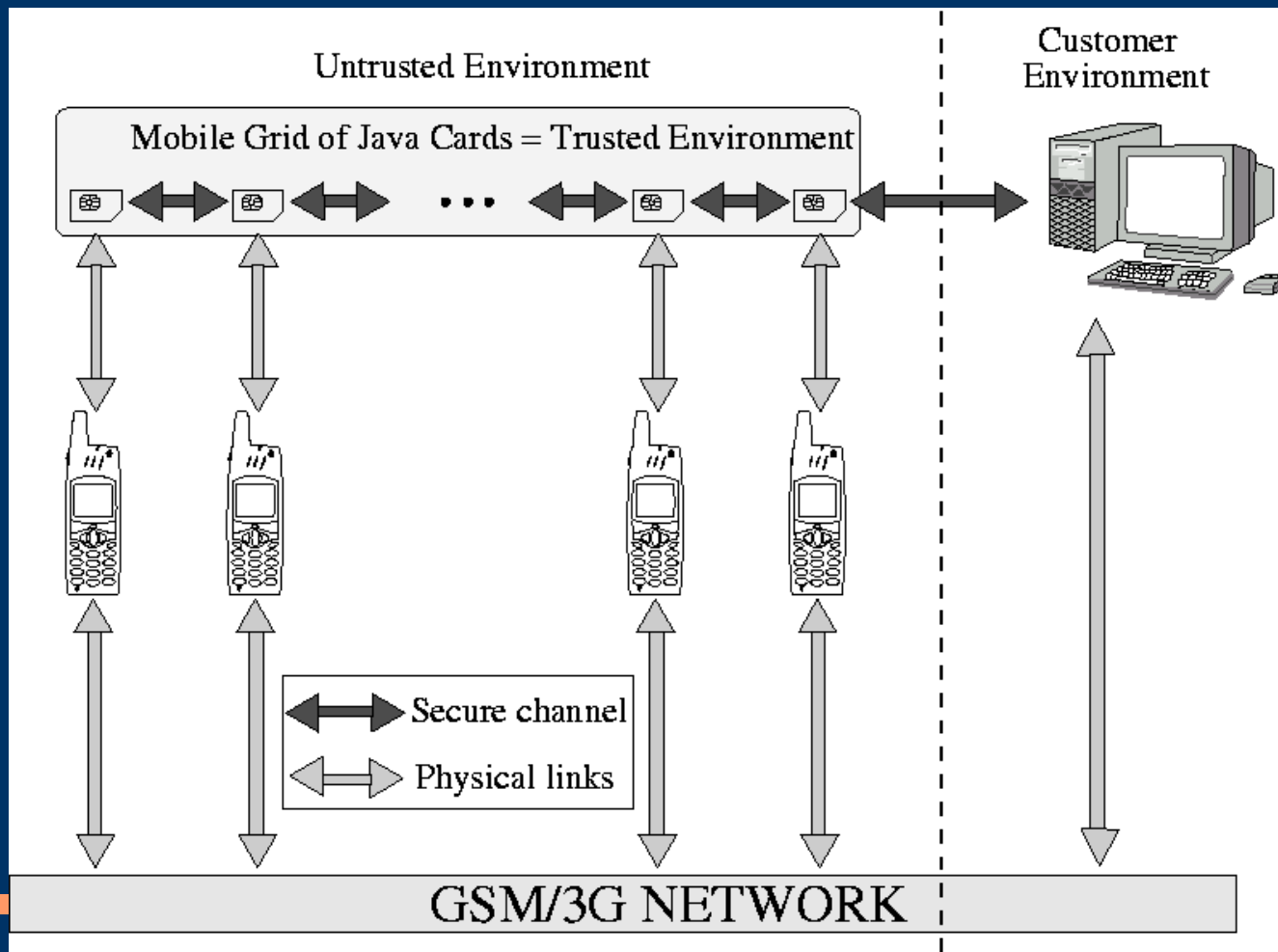


- Damien Sauveron

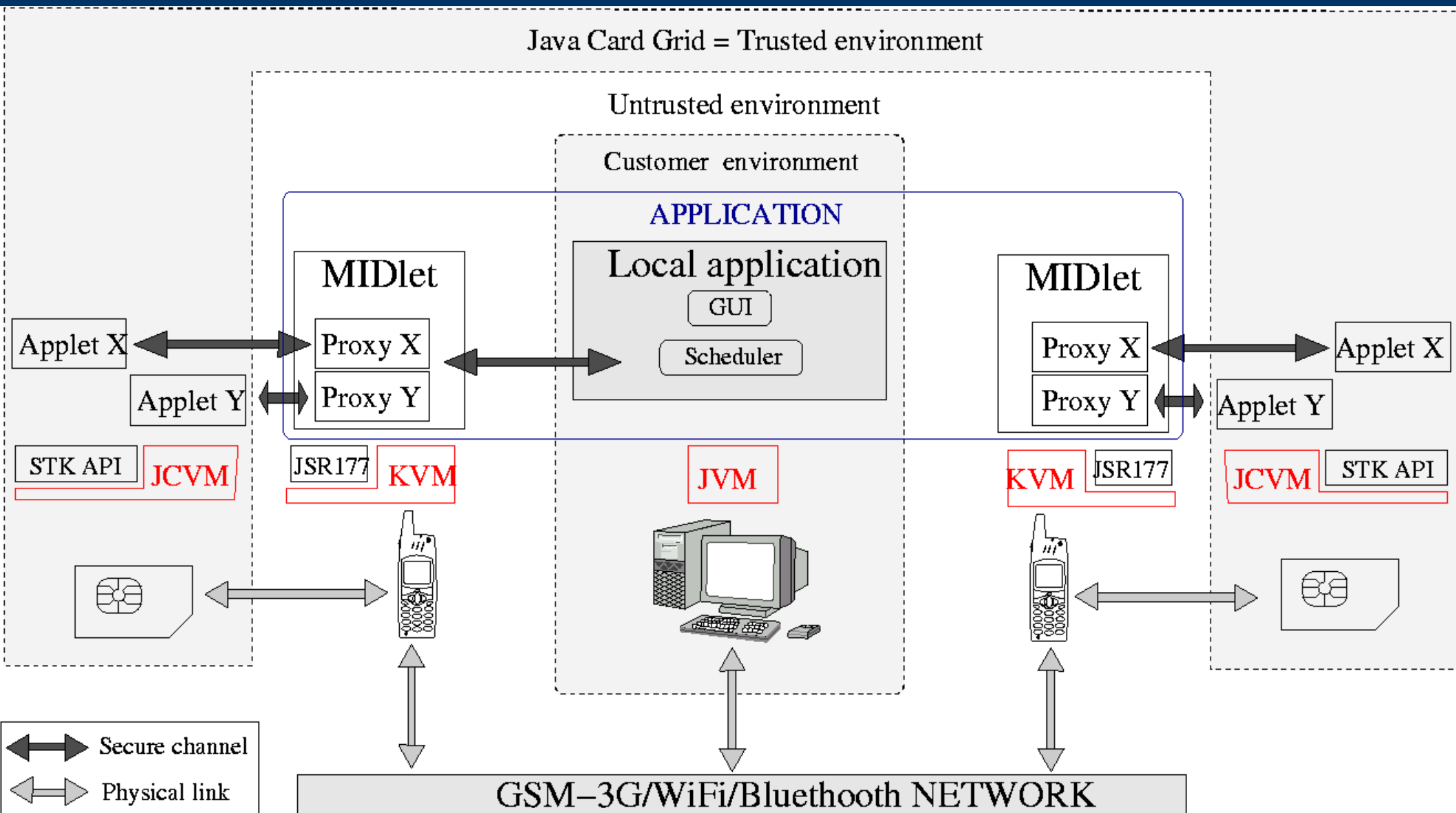


THE MOBILE JAVA CARD GRID

- GOAL: explore new application domains, by extending to a mobile context **based on mobile phones** the possibilities offered by the original Java Card Grid



FRAMEWORK OVERVIEW



Assume that Java is used everywhere: JVM, KVM, JCVM

CHALLENGES

- Applications deployment
- Pro-activity
- Communication
- Memory constraints

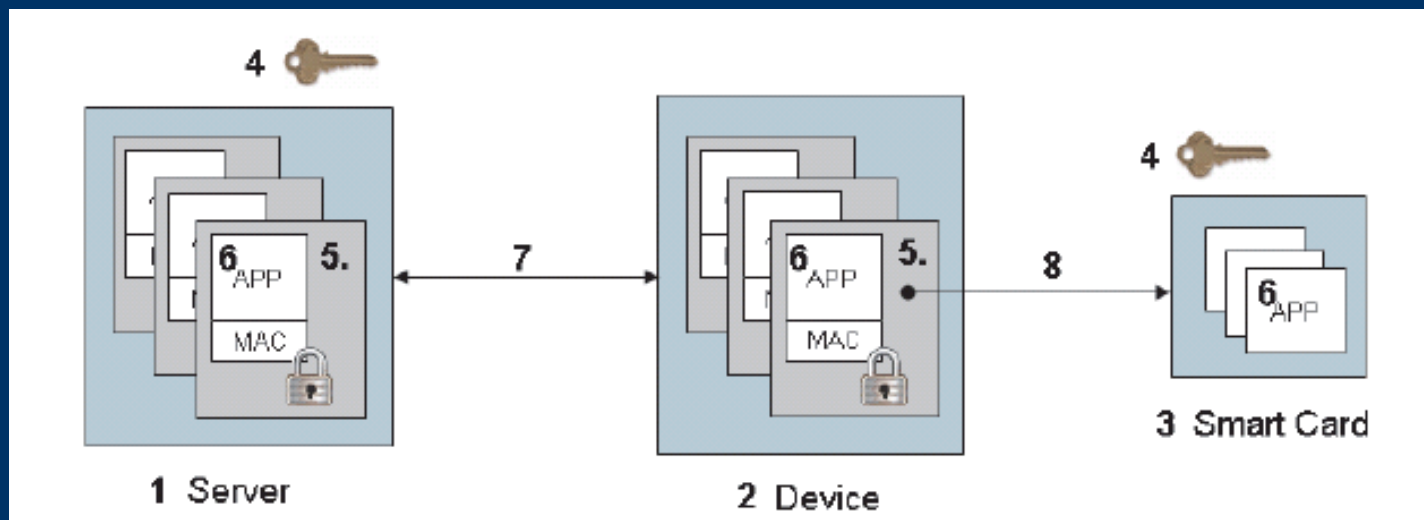


NEXT SLIDES



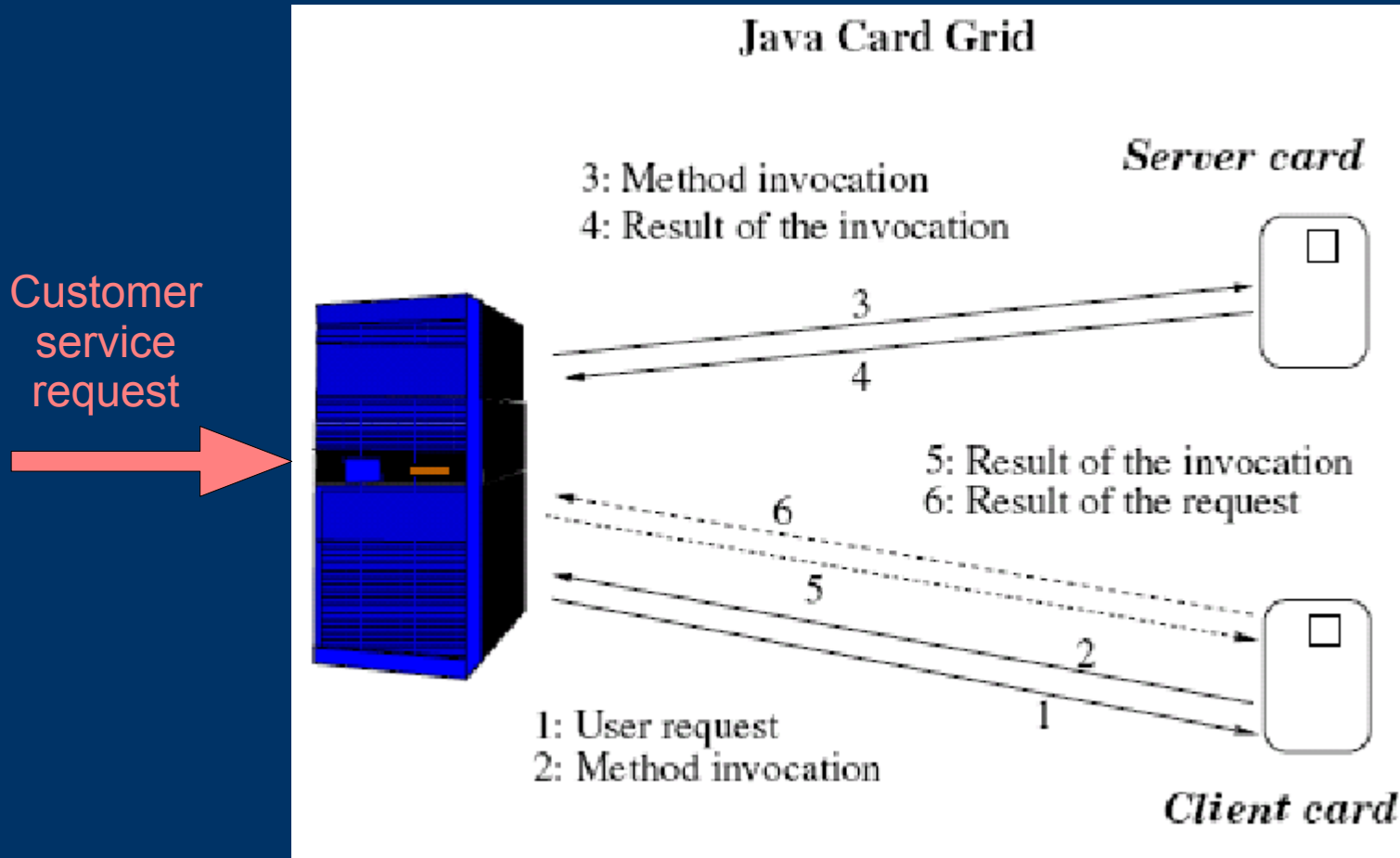
APPLICATIONS DEPLOYMENT

- Problem with OTA deployment: **limited bandwidth**
- Solved using the solutions developed by the RHUL ISG-SCC:
 - Uses high bandwidth channels (GSM, ...) and **security agents** (MIDlet + ciphered card applet) for the deployment
 - GlobalPlatform compliant solution



PRO-ACTIVITY

- Enables the card to act as a client
 - In the original Java Card Grid



- Already built in (U)SIM cards

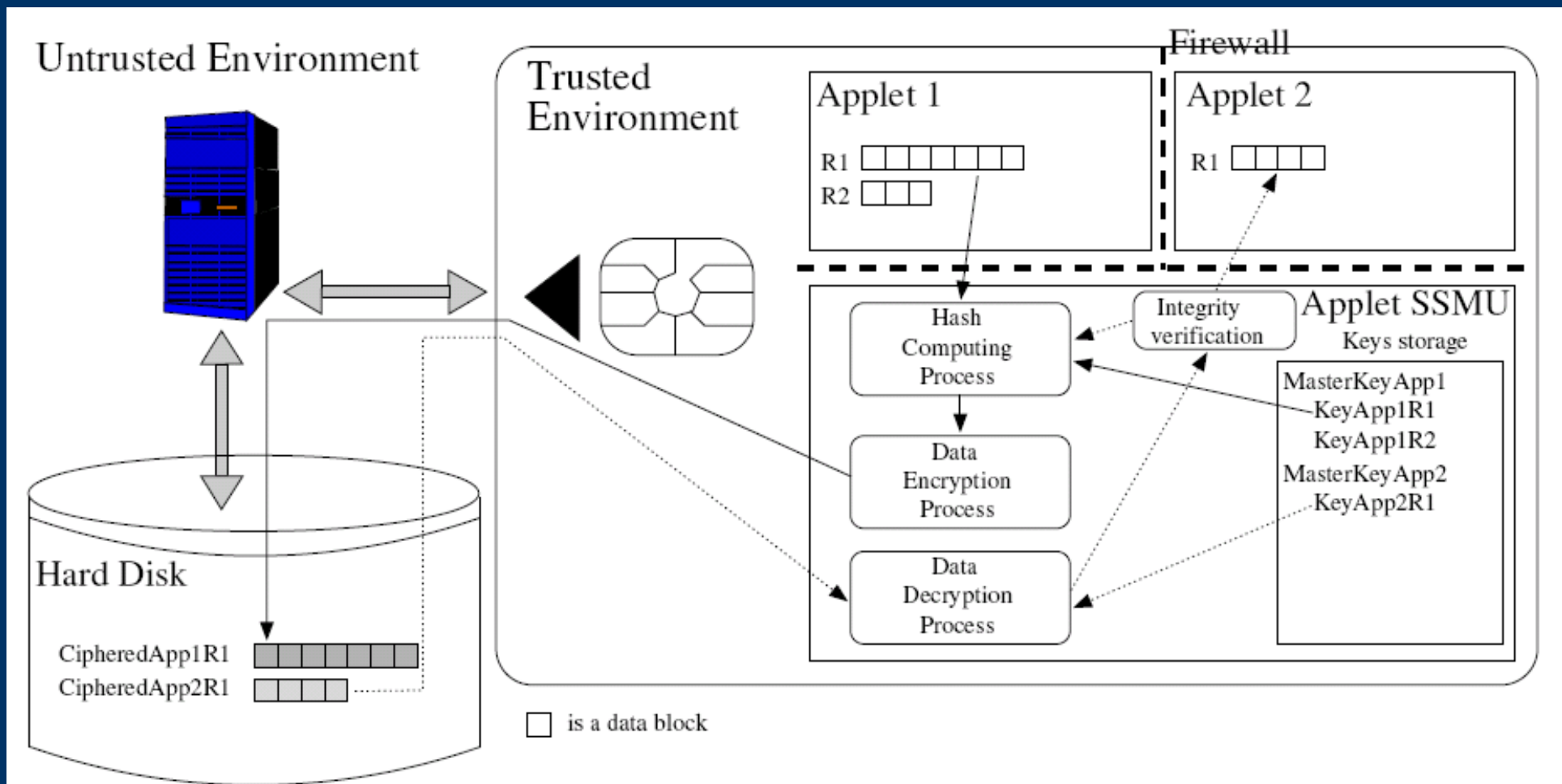
COMMUNICATION

- Between the mobile and the smart card
 - JSR177
- Between the mobiles
 - through Bluetooth: JSR-82
 - through WiFi
 - GSM/UMTS
- Between the smart cards (in client/server mode)
 - STK (SIM ToolKit) API



MEMORY CONSTRAINTS

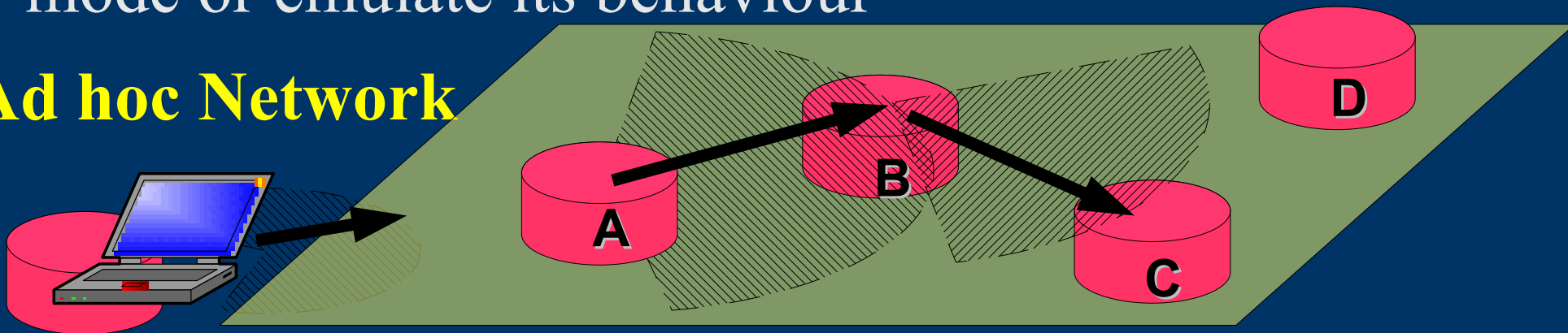
- 2 solutions:
 - Waiting the next generation cards (1Gb)
 - Using secure extended memory developed at LaBRI



FUTURE APPLICATIONS

- Credential sharing between a group of users
- Distributed datamining
 - In phonebook of the employees
 - ...
- Set up a multilevel ad hoc network in a peer to peer mode or emulate its behaviour

Ad hoc Network



CFP: Who has a killer application?

CONCLUSIONS & PERSPECTIVES

- To gather all the developed solutions to build a prototype
- To imagine a killer application
- Will be a joint project between:
 - The ISG-SCC
 - The LaBRI
 - The XLIM



THANKS

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

