

Relations entre
XLIM
Université de Limoges
et
ISG-SCC
Royal Holloway, University of London

Damien Sauveron

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

GT SeFSI – 3 octobre 2006

Le Campus du Royal Holloway



L'ISG et le SCC

- The ISG is one of the largest academic security groups in the world.
- Cryptographic algorithms and protocols, smart cards, electronic commerce, security management, mobile telecommunications security, and the integration of security techniques into specific applications.
- 40 permanents
- 10 postdocs
- 80 thésards
- The ISG also includes the Smart Card Centre of Excellence which it founded with Vodafone and Giesecke & Devrient.



Programme :

- Publications communes
 - Activités diverses
 - The Mobile Java Card Grid
 - Members of the project
 - The Original Java Card Grid
 - Overview
 - Framework
 - Challenges
 - Future applications
 - Thanks
-
-

Publications communes

- 1 chapitre de livre (40 pages), Springer SCI
- 1 chapitre soumis, Wiley
- 1 chapitre à soumettre
- 1 poster (SCC-LaBRI-XLIM)
- 1 publication internationale (SCC-LaBRI-XLIM) à e-Smart 2006



Activités diverses

- Relecture d'articles en interne (une dizaine + thèse)
 - Relecture d'articles en externe
 - Soutien/guide de doctorants
 - Public relationship (Career days, Conférences, ...)
 - Début de projet européen
 - Brainstorming pour un sponsor
 - Rédaction d'un projet EPSRC (à finaliser)
 - Préparation du dossier pour Cardis 2008
 - Beaucoup d'autres choses ...
 - Participation à quelques séminaires, à des cours, ...
-
-

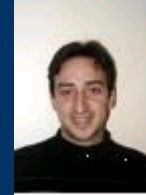
MEMBERS



Smart Card Centre
Royal Holloway

Royal Holloway
University of London

- Konstantinos Markantonakis
- Keith Mayes



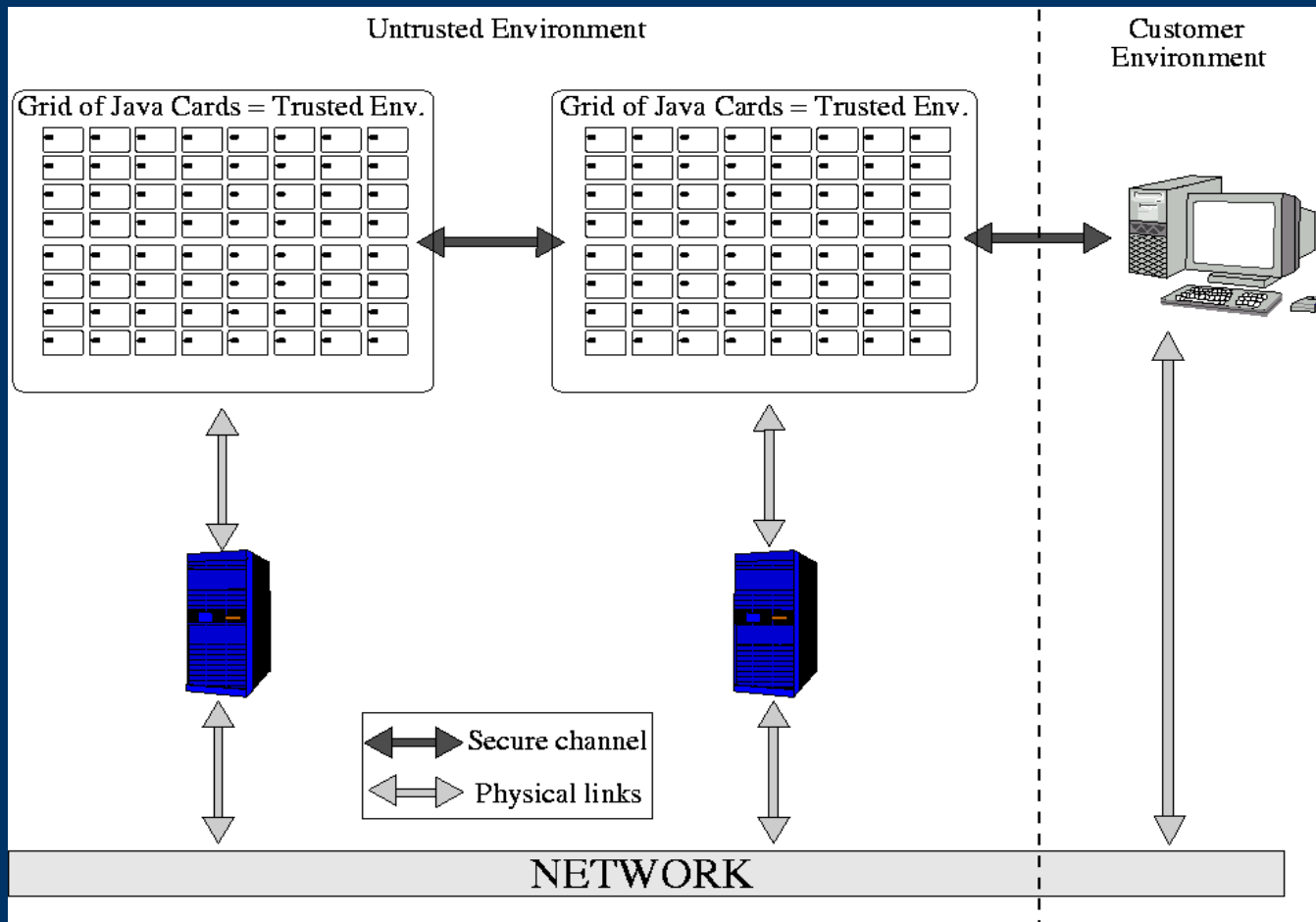
- Serge Chaumette



- Damien Sauveron



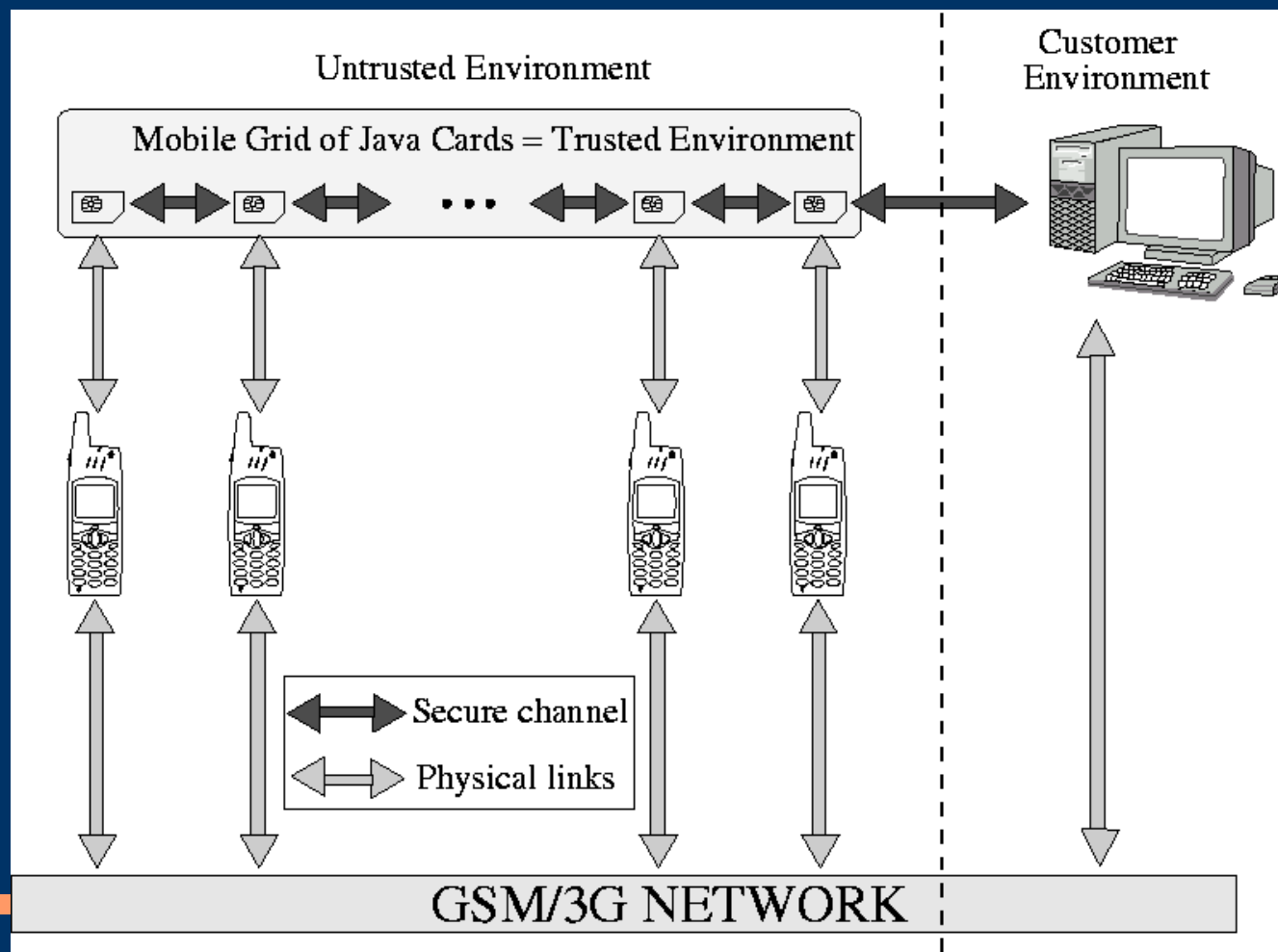
THE ORIGINAL JAVA CARD GRID (LaBRI)



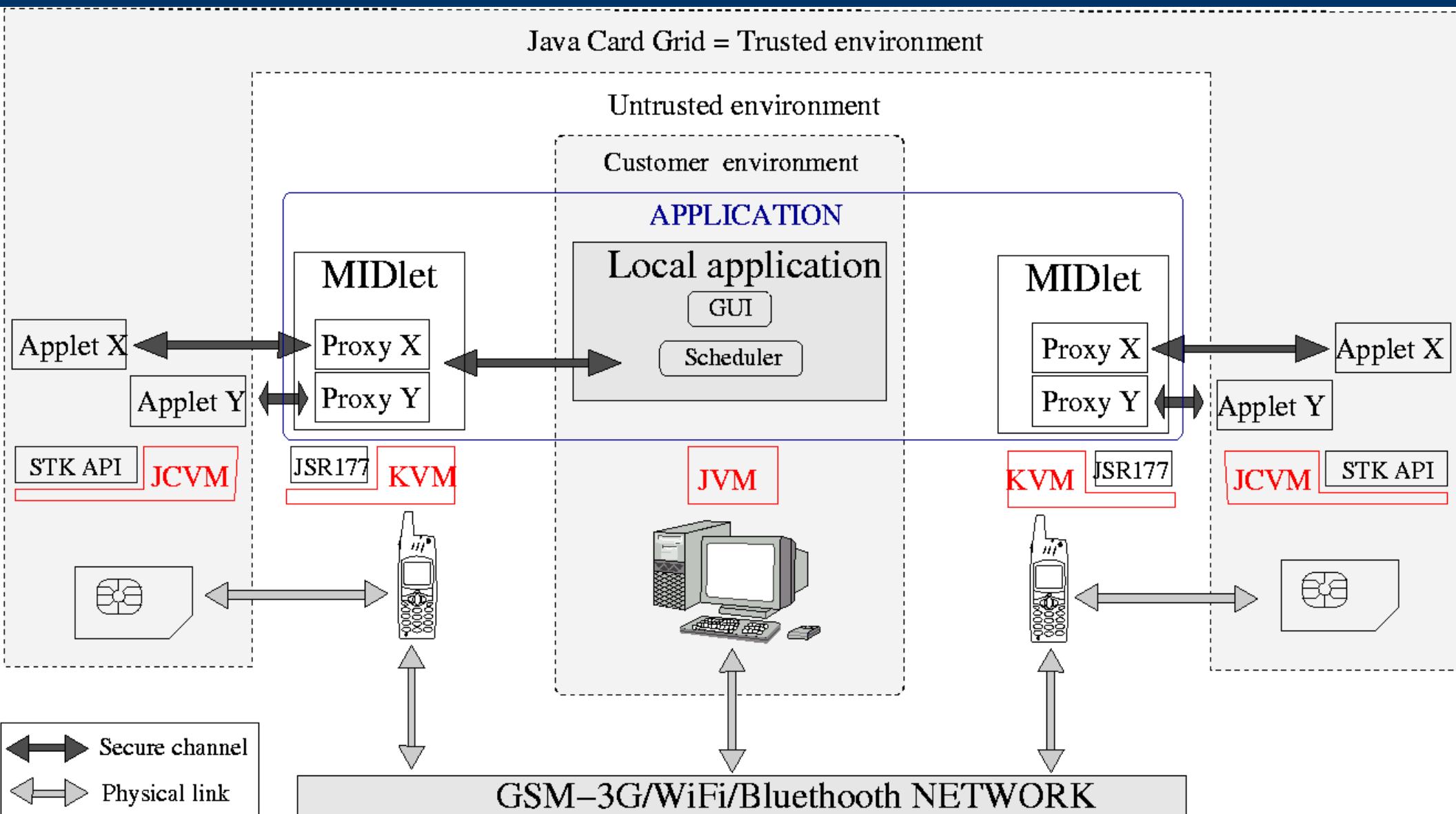
- GOAL: build a cluster of smart cards and to provide a software framework for developing and managing secure applications on it.
- e-Smart 2005 Isabelle Attali Award for the best innovative technology (France)
- Invited paper at the 2006 HPC&S Conference (Germany)

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

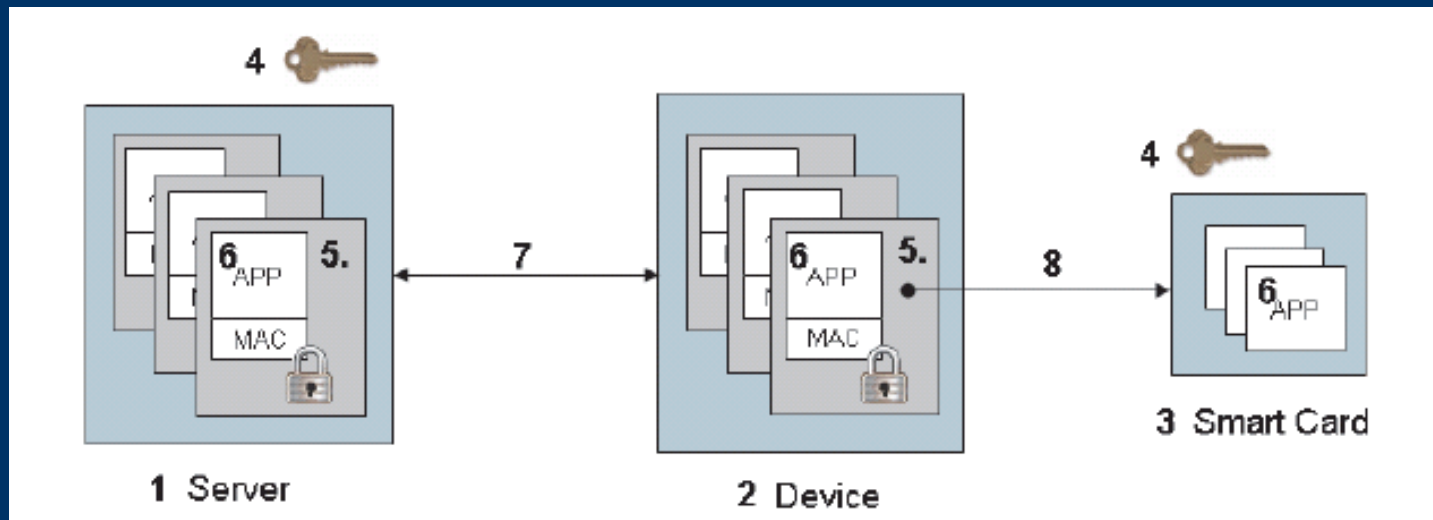
- Applications deployment
- Pro-activity
- Communication
- Memory constraints



NEXT SLIDES

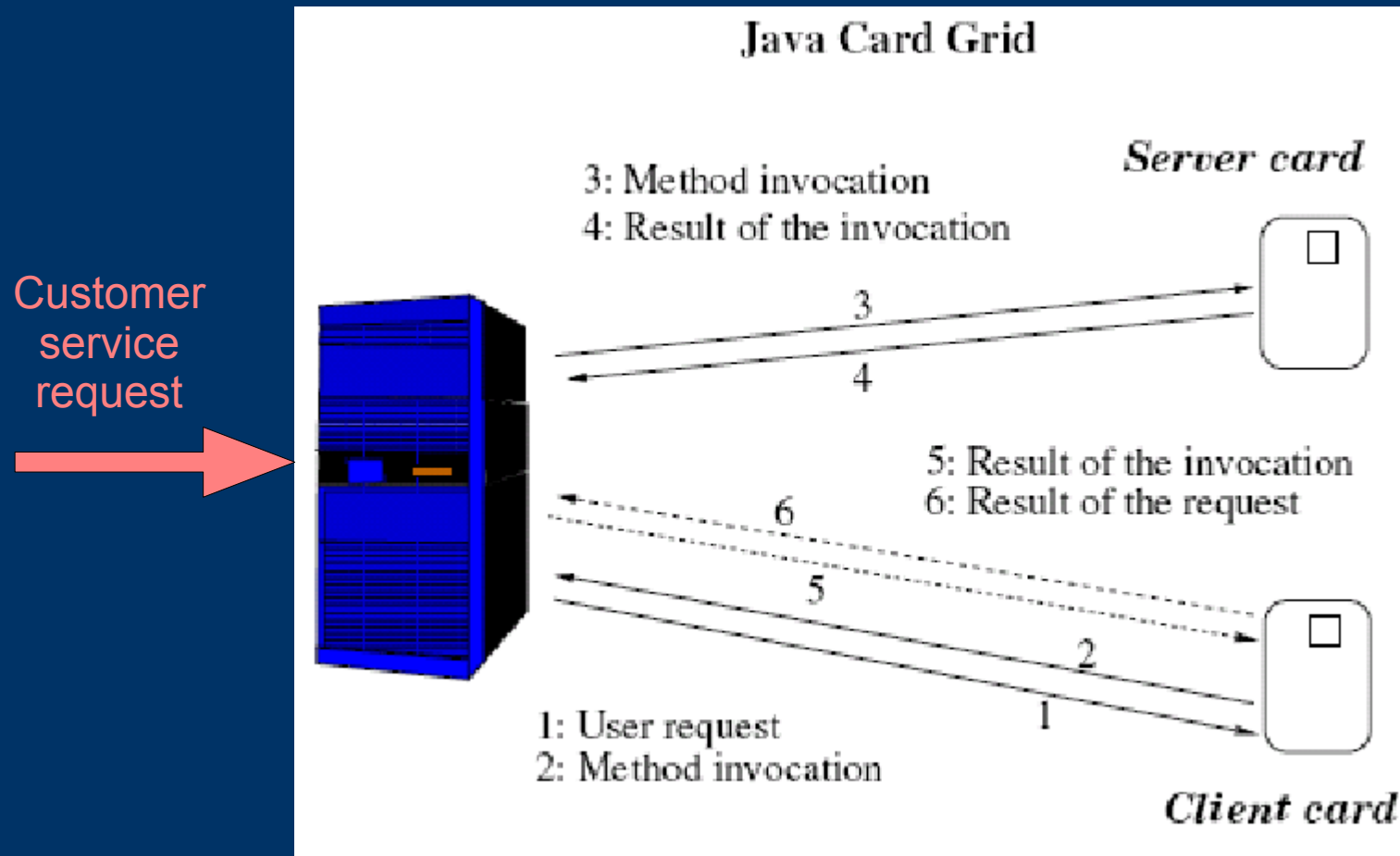
APPLICATIONS DEPLOYMENT

- 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

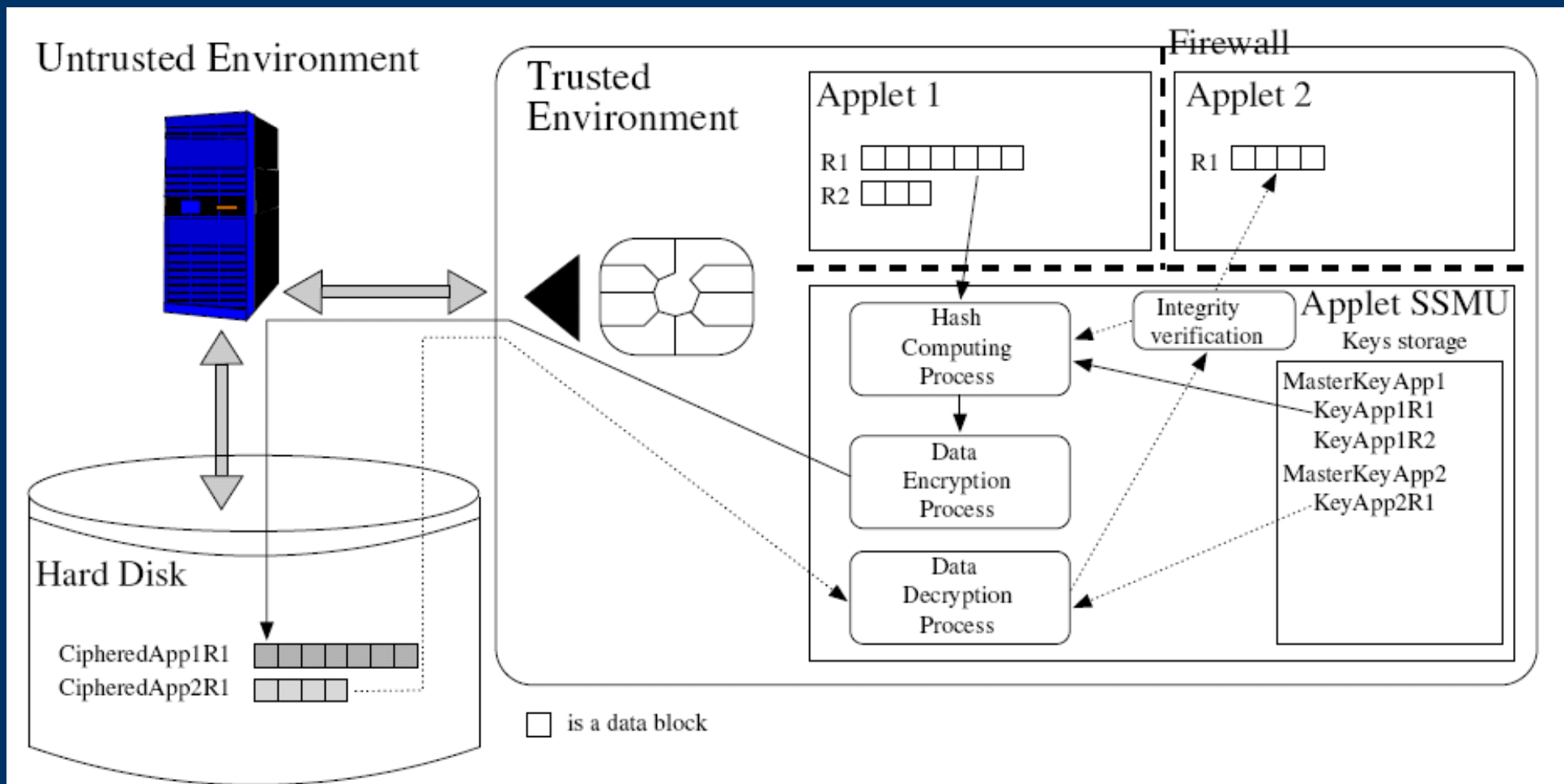
COMMUNICATION

- 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

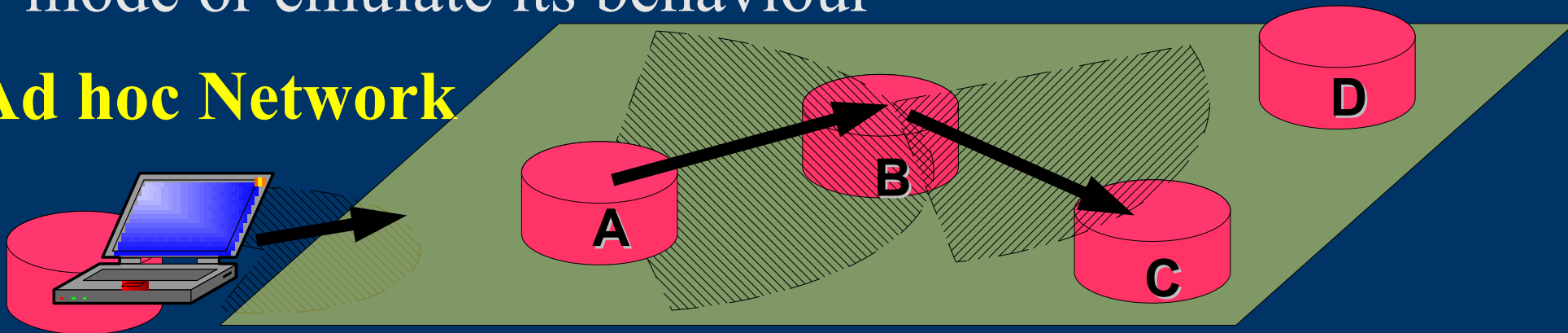
- 2 solutions:
 - Waiting the next generation cards (1Gb)
 - Using secure extended memory developed at LaBRI



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?

THANKS

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

Bibliography

- (1) Secure storage for the Java Card Grid.
 - (2) A High Level Security Framework for the Grid: the Java Card Grid Testbed.
 - (3) The Software Infrastructure of a Java Card Based Security Platform for Distributed Applications.
 - (4) Secure Collaborative and Distributed Services in the Java Card Grid Platform.
 - (5) A Grid of Java Cards to Deal with Security Demanding Application Domains.
 - (6) Secure distributed computing on a Java Card grid.
 - (7) Will Sirret, PhD thesis
-
-

