

Smart Cards Integration in Distributed Information Systems : the Interactive Execution Model



Sébastien JEAN, **USTL/LIFL/RD2P**,
Didier DONSEZ, **UVHC/LAMIHIROI**,
Sylvain LECOMTE, **UVHC/LAMIHIROI**,

Email : jean@ifl.fr
{donsez,lecomte}@univ-valenciennes.fr



Summary



- Smart cards technology
 - Overview, Architecture, Communication protocols, OS and applications
- Smart cards and information systems
 - Execution models
- The Interactive Execution Model
 - Motivations, use cases and requirements
- Perspectives

Smart Card Overview



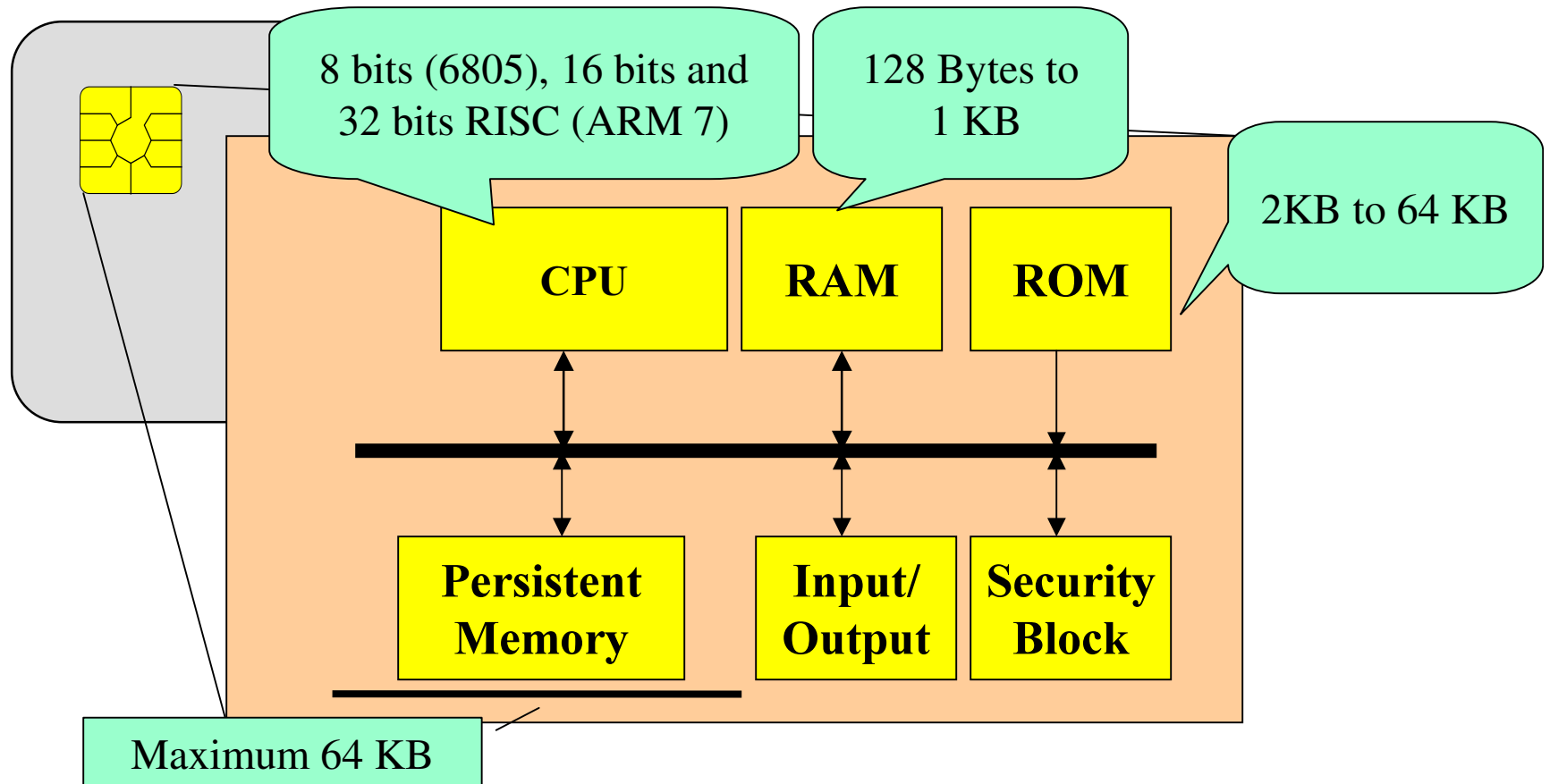
■ History

- | 1974 : Moreno ' patent
- | 1987-1999 : ISO normalization
- | 1997 : JavaCard, OCF
- | 1999 : Smart Card for Windows

■ A smart card is a computer but ...

- | communication rate is 500 times slower
- | memory amount is 100 000 times smaller
- | CPU is 100 times less powerful

Smart Card Architecture



- Power supply and clock signal are external

Smart Card Applications

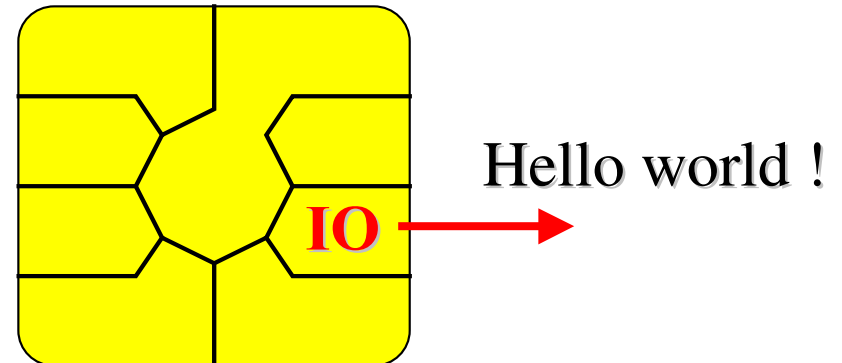
- Various smart card kinds :
 - payment cards, access cards, portable data files
- Various application domains
 - Phone : Prepaid cards, SIM/WIM cards
 - **requires wide service range, cost does not matter**
 - Bank : Electronic Purse, Bank card
 - **requires security but low cost**
 - Healthcare : Patient card,
 - **requires data security**
 - Gambling, Loyalty, Computer Secure Login, ...



Smart Card communication facility

- Serial link, half-duplex, asynchronous

- 1 wire comm. Link
- commonly 19200 bit/s



- 2 communication protocols

- "T=0" : bytes oriented
- "T=1" : byte-blocks oriented

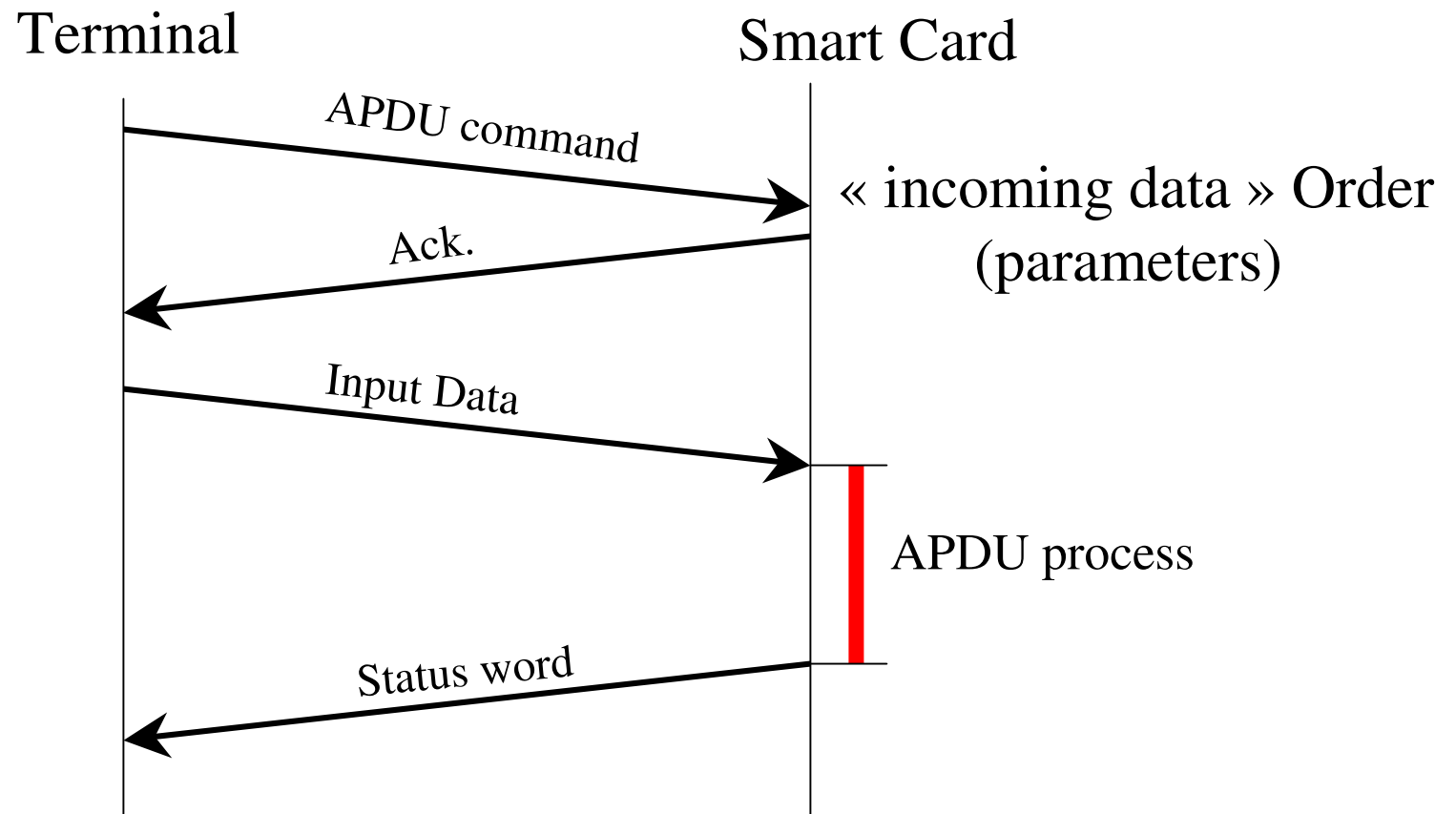
Smart Card communication facility



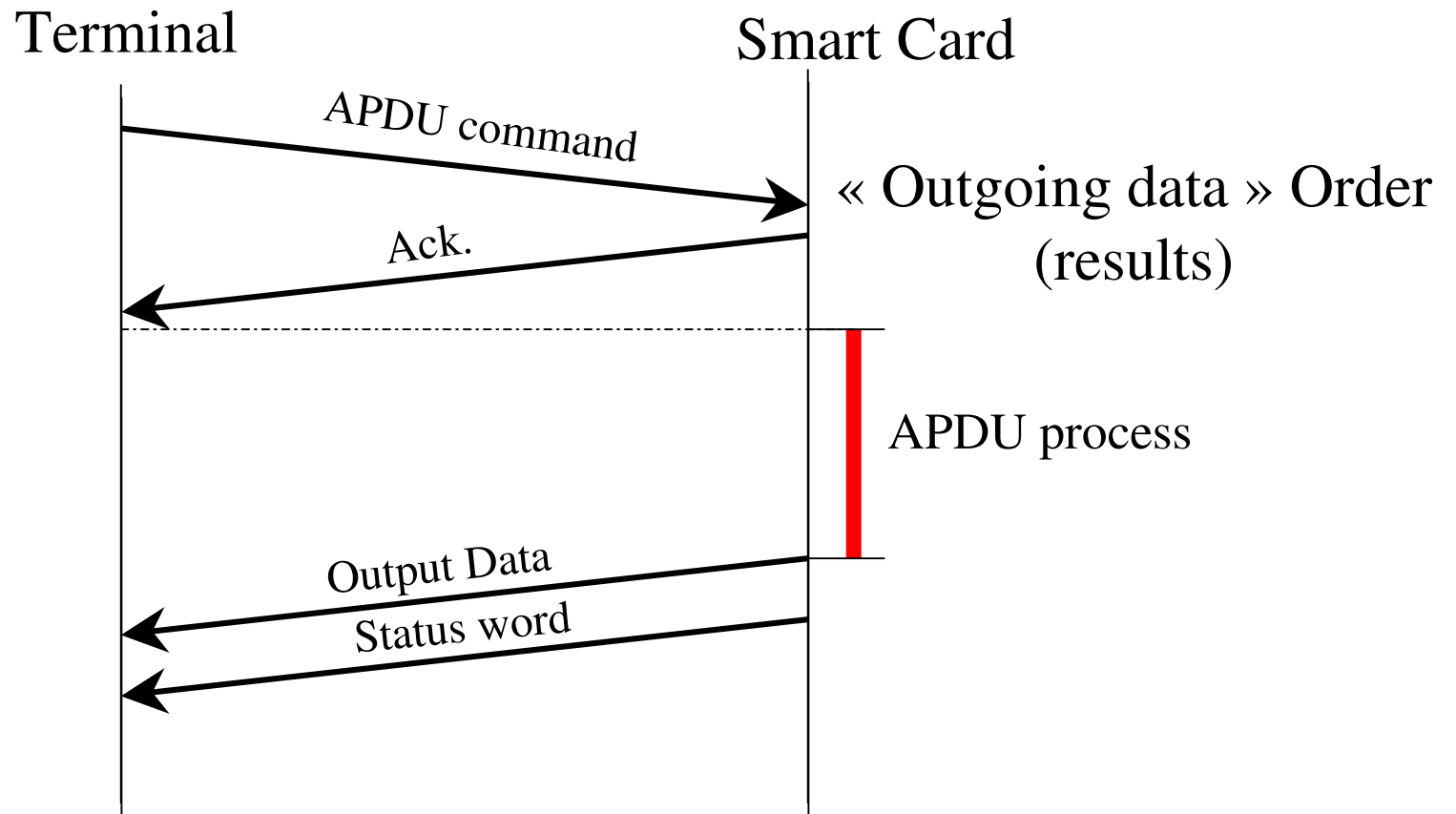
- OSI communication stack based model
 - TPDU
 - | Transport Protocol Data Unit
 - APDU
 - | Application Protocol Data Unit

- APDU are not encapsulated
but mapped on TPDU

APDU exchanges : communication protocol



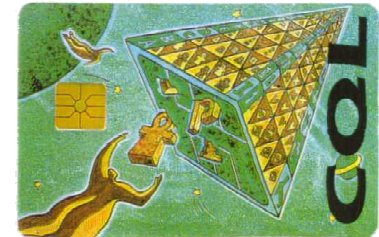
APDU exchanges : communication protocol



Smart Card Operating Systems

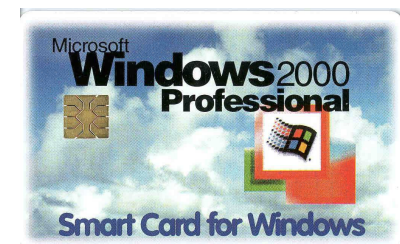
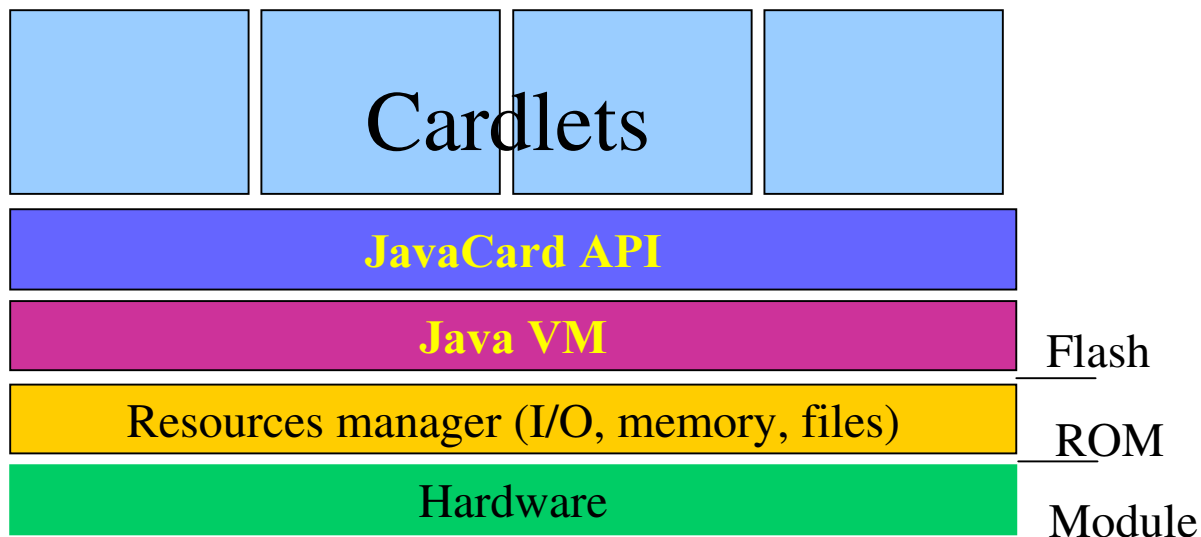
■ Data-oriented smart cards

- **7816-4** : FileSystem
- **7816-7/SCQL** : RDBMS in a smart card



■ Application-oriented smart cards


- provide an execution platform for multiple applications (cardlets)
- **Java Card, Smart Card for Windows, ...**



Smart Card Operating Systems

- **Smart Card OS are operating system**
- **because**
 - manage resources
 - memory, storage
 - organise resources (file systems, ...)
 - manage communication with terminal (card reader)
 - execution support for multiple applications (cardlets)
 - communication between cardlets
 - security (authentication, privileges, ...)
- **But**
 - no multi-threading (time-sharing)
 - no communication from a cardlet to an external server

Smart Cards in Information Systems : Realisations



■ CQL

- element of a distributed database
 - Portable relational database accessed via ODBC/JDBC drivers

■ Corba

- card services as « corba objects »
 - COA (Card Object Adapter) as proxy

■ WebCard

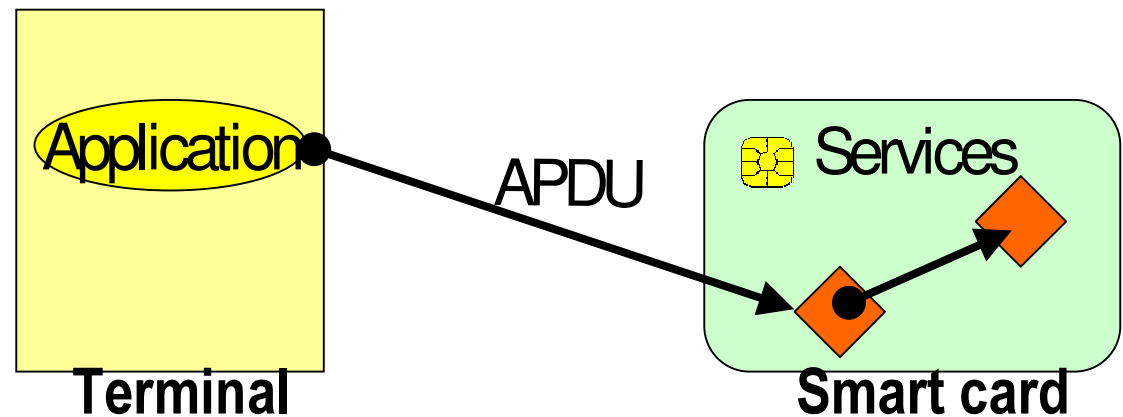
- Web server Cardlet, IP/HTTP stack

■ PNDS Card

- contains a directory accessed with a JNDI SPI

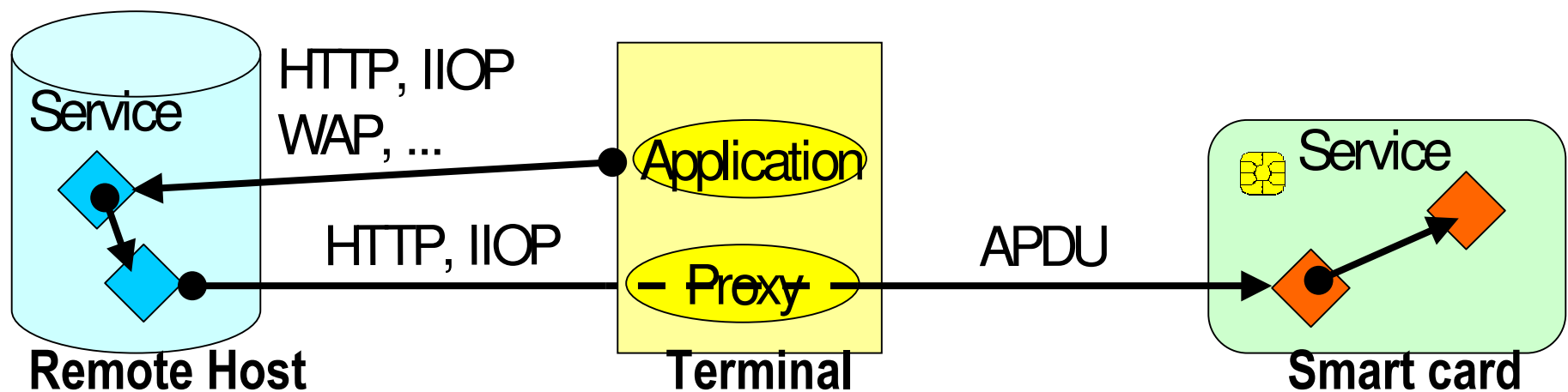
Smart Card & I. Systems: Server Execution Model

- Client / Server architecture
- Smart Card is always seen as a server
 - for local client
 - for remote clients



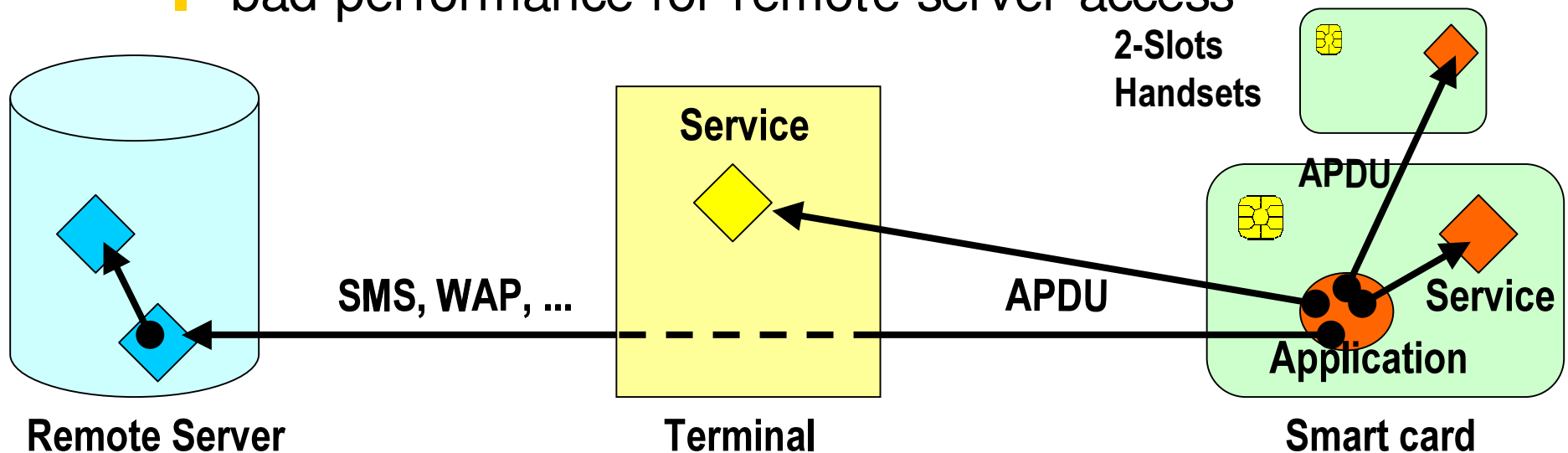
Smart Card & I. Systems: Server Execution Model

- Client / Server architecture
- Smart Card is always seen as a server
 - for local client
 - for remote clients



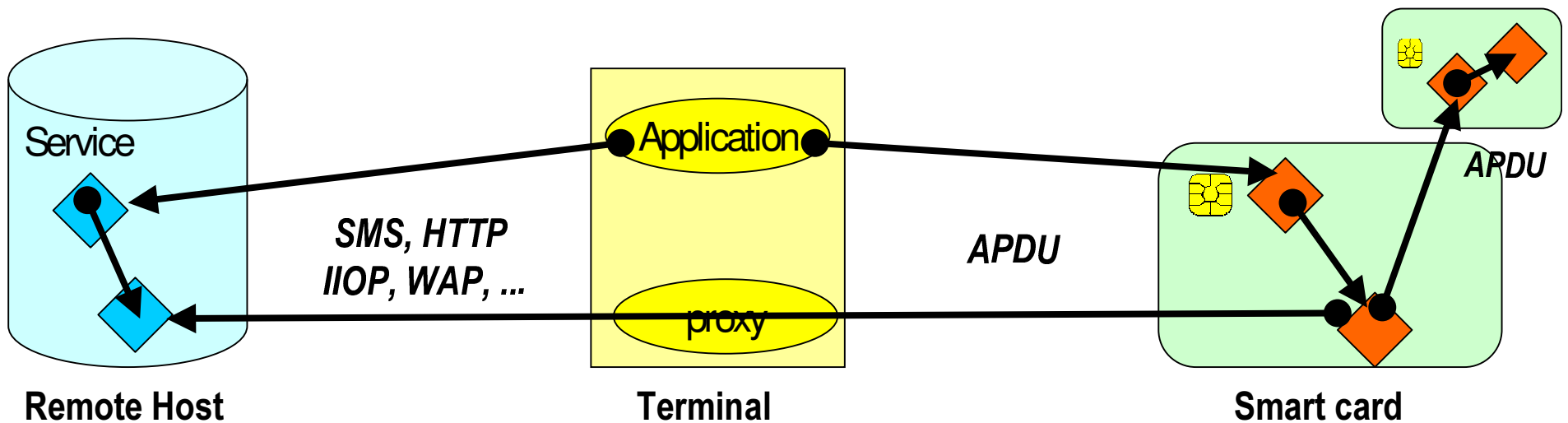
The SIM-Toolkit Case : ProActive Execution Model

- Smart Card is client only
 - It drives the mobile phone GUI
- Limits :
 - application logic fully predefined in the card
 - bad performance for remote server access



The Interactive Model

- The Smart Card is both
- Server and Client (*other SC, other remote service*)
 - looks like a Corba service



Why an interactive card



- What smart card is :
 - an intrinsic secure component
 - a mediator between its holder and Information Systems
 - Smart card is the only device that its holder accept to trust

- With the interactive model, external applications take benefits of smart card security

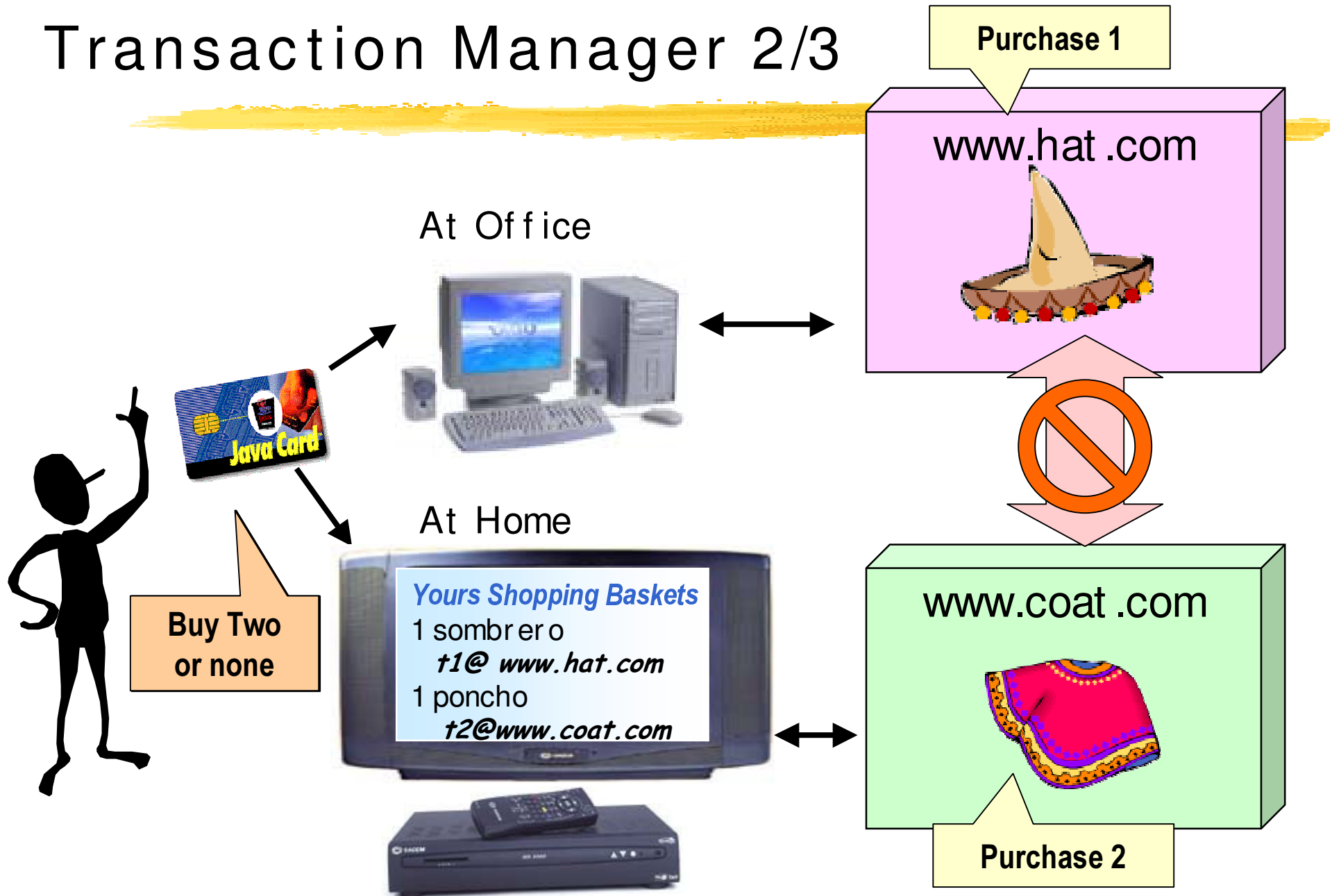
Use Case :

Transaction Manager 1/3

- MultiPurpose Internet Shopping Basket
 - Multiple purchases in several Web stores
 - 1 sombrero @ www.hat.com
 - 1 poncho @ www.coat.com
- Purchase rules
 - All baskets are managed by a client application
 - No shared baskets between
www.hat.com and www.coat.com
 - All or None items are purchased



Use Case : Transaction Manager 2/3



Use Case :

Transaction Manager 3/3

- Multi-Basket application is embedded in the SC
 - Requires secure transactional completion
 - | avoid repudiation
 - | Need of trust (holder point of view)
- 👉 Transactional Monitor embedded in SC
 - Commit if all products are available
 - abort and rollback else
- Pro-activemodel is enough for Multi-Basket application
- but interactive model is required for Transactional Monitor

Use Case :

Component Deployment (CESURE Project)

- Adaptable Component-Based large scale applications for mobile users
 - The smart card acts as a « bootstrap » for application deployment on heterogeneous platforms
 - Some components algorithms have to be kept secret
 - Some components are executed inside the smart card
 - These components can be both client and servers
- So smart card has to be both Client and Server

Toward authentication flexibility

- **Static server-oriented approach**
 - 1- An external application authenticates itself
 - 2- It asks the card for a service
 - 3- The card gives the results
- **Dynamic interactive-oriented approach**
 - 1- An ext. application asks for a service
 - 2- The card requests it for authentication
 - 3- If done, the smart card gives the results

Requirements 1/2

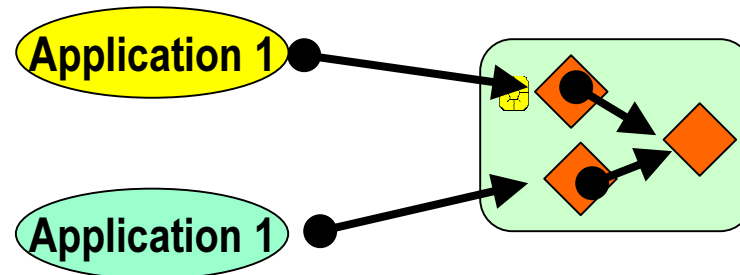


- A Full-duplex protocol is required...
 - Because interactive model needs 2-way requests emission
- But it might be "virtual full duplex"
 - Real full duplex on 1 wire has to fight with collisions (Ethernet)
 - "natural" handshaking

Requirements 2/2

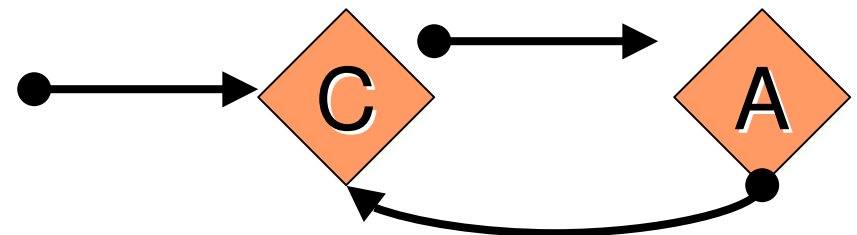
Multi execution context

- 1 smart card / N remote hosts
 - Several request (that are not related) have to be managed by the smart card simultaneously



Loop Back

- Card C calls a remote service A
- and service A calls C



Perspectives



- Communication Protocol required by the interactive model is specified
- Prototype and experimentation are in progress
- Part of the PhD Thesis of Sébastien JEAN
- Related work :
 - CESURE project
 - Hybrid smart card model