Smart Card Operating Systems Overview and Trends

Pierre.Paradinas@gemplus.com
Gemplus Labs

GEMPLUS

Smart card...

- A piece of plastic...
- with a chip that contains: CPU, memories and programs...
- SC is your personal information system, your wallet, your e-key, your cell phone subscriber identification (GSM)...

GEMPLUS

9-Apr-01

Labs

Agenda

- Smart card industry and application
- Smart card embeds computing power
- Smart card OS & Software
- Issue in SC software
- Q/A

GEMPLUS

9-Apr-01

Labs

Smart card industry and application

- First SC were produced 2O years ago
- After a French industry, it becomes a more European industry (80% of the market share)
- Large worldwide business with revenues of 2,2 billion $:
  - GSM
  - Payment/e-purse (Blue Card, EMV,...)
  - E-security (logical access, Pay-TV,...)

GEMPLUS

9-Apr-01

SC industry and application (Cont'd)

- From analysts:
  - 2000
    - 628 Mu are shipped [chip cards = 1 700 Mu] (Gartner Inc)
  - 2006
    - 2 300 Mu [chip cards = 4 100Mu] (Datamonitor)
- New applications will appear:
  - WAP, UMTS, 3G-Network,...
  - Deployment of payment card (Visa, Amex,...)
  - M-commerce
  - Access control based on SC: part of Wins and Solaris distribution

GEMPLUS

9-Apr-01

SC industry and application (Cont'd)

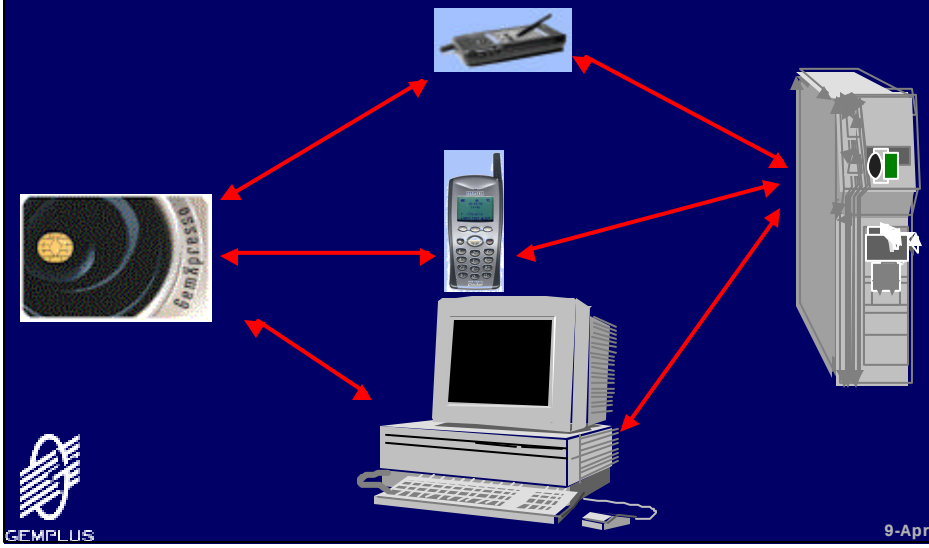
- Our industry is based on :
  - Plastic and secure printing
  - Silicon and packaging
  - Software and application
- Software is part of our expertise but its role is more and more crucial

GEMPLUS

9-Apr-01

Labs

SC Application Architecture



GEMPLUS

9-Apr-01

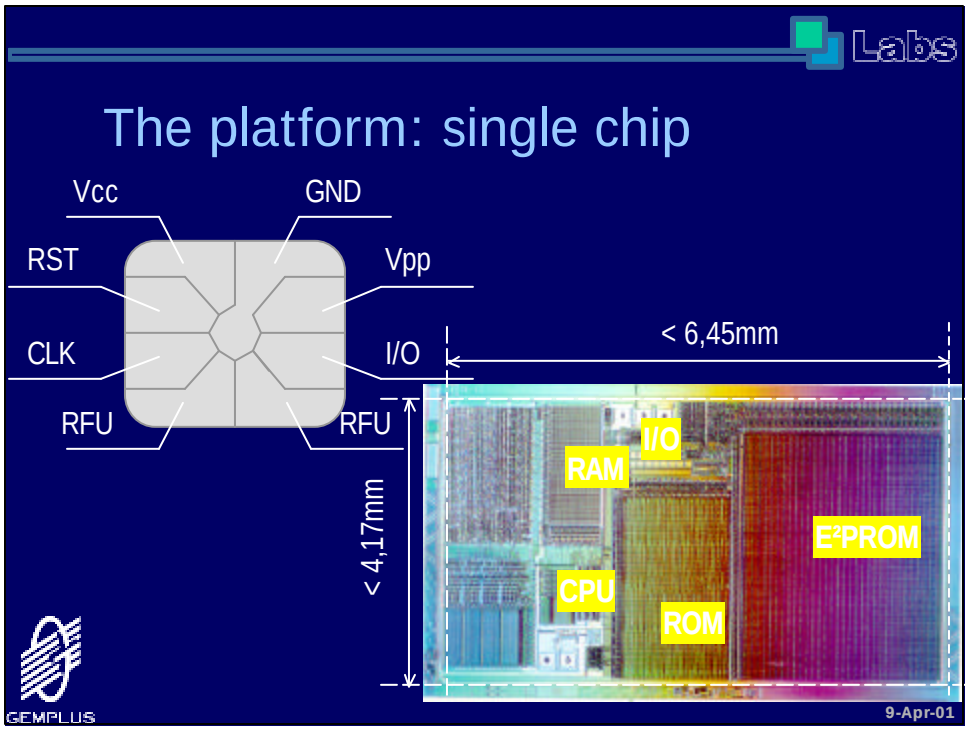
Labs

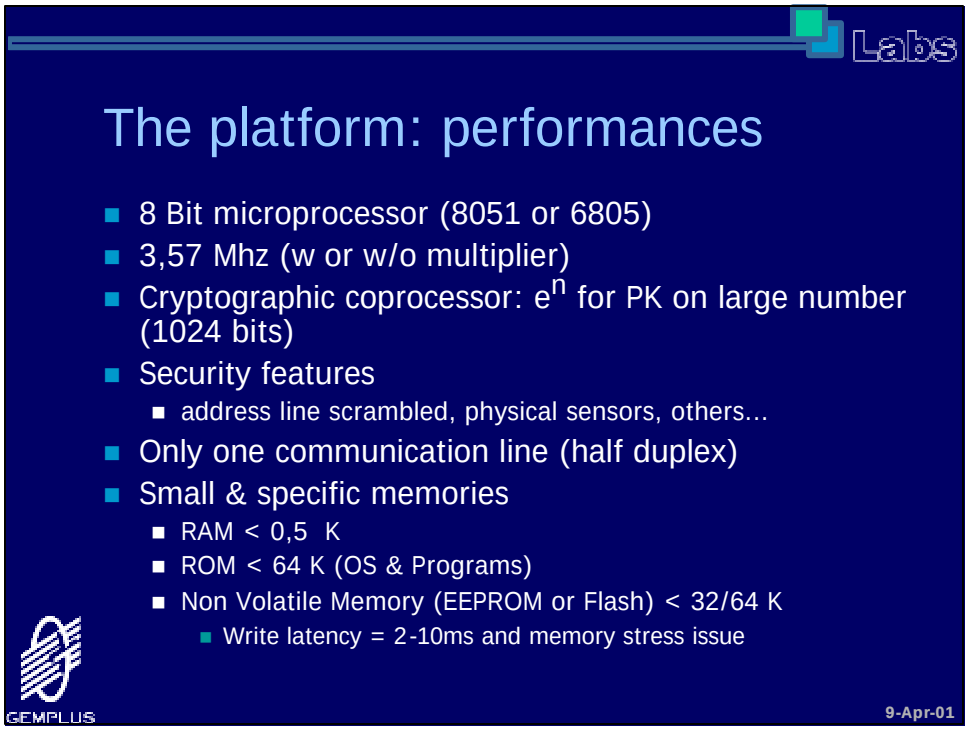
Durable smart card benefits

- Card software is part of the application
- Processing and data will be shared along the chain
- Security will be shared by each part of the chain
- Personal repository of data & services
- The “supervisor” of your services
- Provides and controls a personalized view of the system

GEMPLUS

9-Apr-01


Labs
The platform: single chip
Vcc
GND
RST
Vpp
CLK
I/O
RFU
RFU
< 6,45mm
< 4,17mm
I/O
RAM
E²PROM
CPU
ROM
GEMPLUS
9-Apr-01


Labs
The platform: performances
8 Bit microprocessor (8051 or 6805)
3,57 Mhz (w or w/o multiplier)
Cryptographic coprocessor: e^n for PK on large number (1024 bits)
Security features
address line scrambled, physical sensors, others…
Only one communication line (half duplex)
Small & specific memories
RAM < 0,5 K
ROM < 64 K (OS & Programs)
Non Volatile Memory (EEPROM or Flash) < 32/64 K
Write latency = 2-10ms and memory stress issue
GEMPLUS
9-Apr-01

Platform constraints

- No internal clock and power supply
- But
  - Tamper responsive
  - Size of the chip: the card is in your pocket
  - Chip cost is directly related to the size
  - Consumption
    - Handset, small SC reader,...
    - Heat of the CPU
    - Some cards are contactless

GEMPLUS

9-Apr-01

New platforms

- 32 bit arrives
- More memory:
  - Ram: 1 to 4 (8)
  - Rom: ~128K
  - NVM: ~64k (128k)
- Always co-processor

GEMPLUS

9-Apr-01

Card Software: Agenda

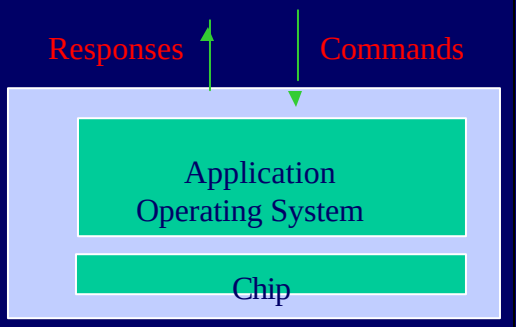
- First software generation
- Open OS
  - Java Card
- Research issues in SC-OS
  - Security, Portability, Sharing, ...
  - Integration in IT

GEMPLUS

9-Apr-01

First generation software

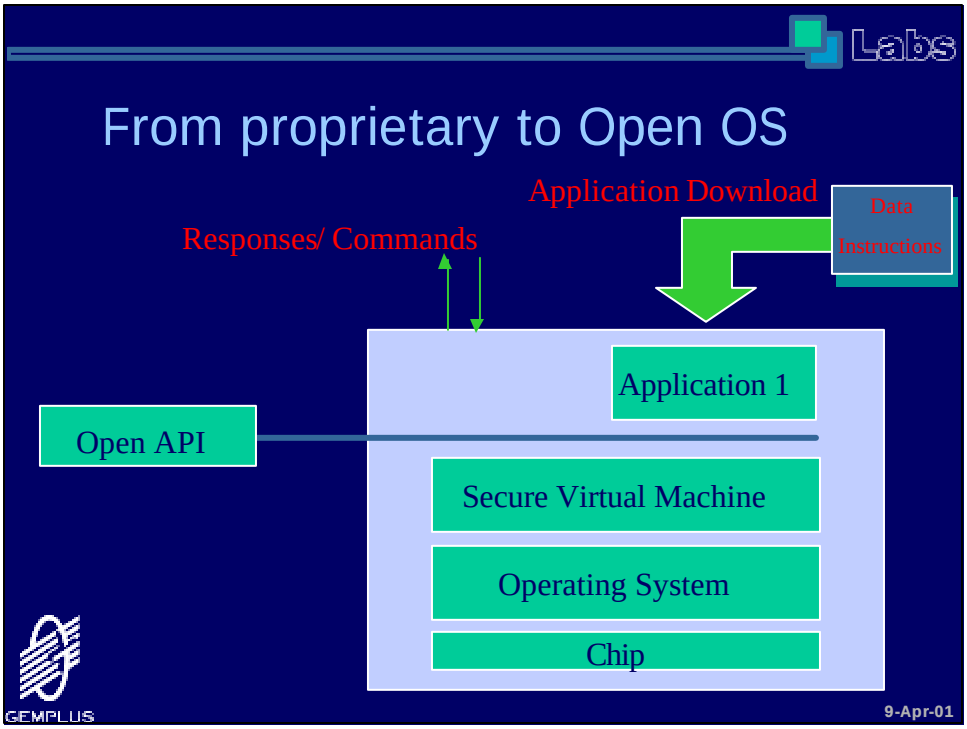
- Applications are developed by the card provider in a secure environment with assembler or C
- Drawbacks:
  - costly
  - poor flexibility
  - time to market



GEMPLUS

9-Apr-01

From proprietary to Open OS



GEMPLUS 9-Apr-01

Open Card...

- Applications developed by:
  - the customer
  - any application provider
- Dynamically downloaded through a network
- The card life cycle is changed...

GEMPLUS 9-Apr-01

Smart Card Lifetime (1/2)

- Manufacturing
- Application masked in the ROM
  - OS libraries and command dispatcher,
  - Application routines.
  - Card serial number and issuer references
- Initialization
  - Writing in EEPROM application data
  - Secret key and object attributes (r,w,rw,…)
- Personalization
  - Writing in EEPROM card holder data
  - Graphical (picture, logo, hologram…)

GEMPLUS

9-Apr-01

Smart Card Lifetime (2/2)

- Usage
  - Process APDU command from a reader
  - Send back a response APDU or an error APDU
  - For open card only: application downloading
- End
  - Deactivation (unauthorized action), memory overhead, loss, theft, ...

GEMPLUS

9-Apr-01

Candidate Platforms

- Multos (from Mastercard)
- W4SC (Microsoft)
- Java Card 2.1 (Sun)

GEMPLUS

9-Apr-01

Introduction to the Java card

- The Java Card
- The JCVM architecture
- The security procedures

GEMPLUS

9-Apr-01

What is a Java Card ?

- The Java Card
  - a smart card dedicated to Java applications
  - a platform with highly limited resources
  - a dedicated Java language
  - a multi-application device
  - a specific Java Card Virtual Machine (JCVM) architecture.

GEMPLUS

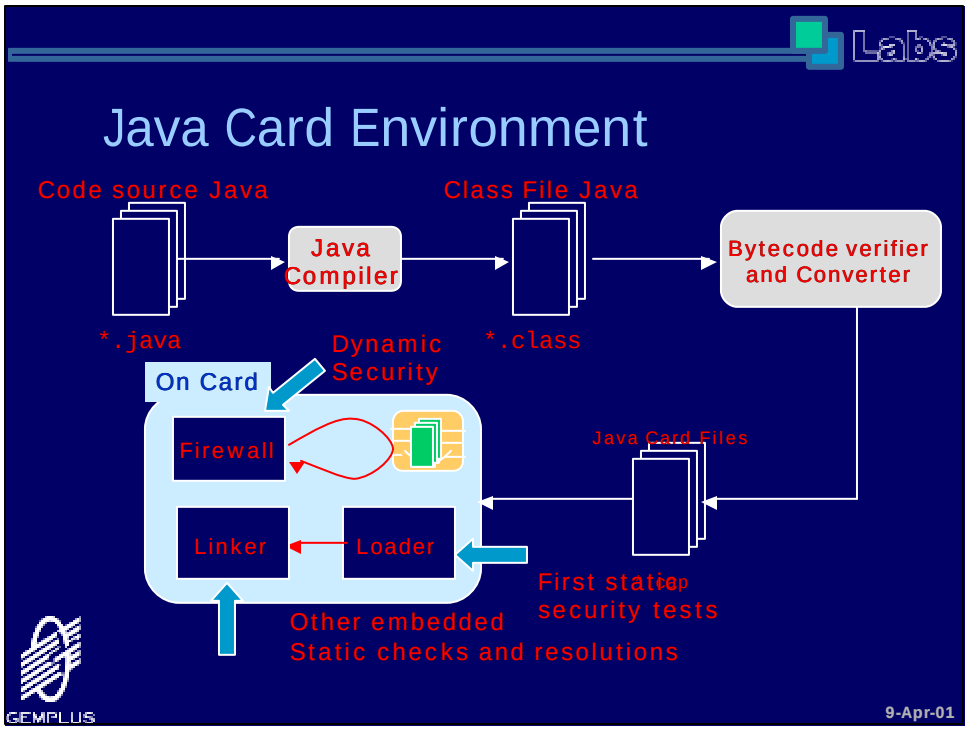
9-Apr-01

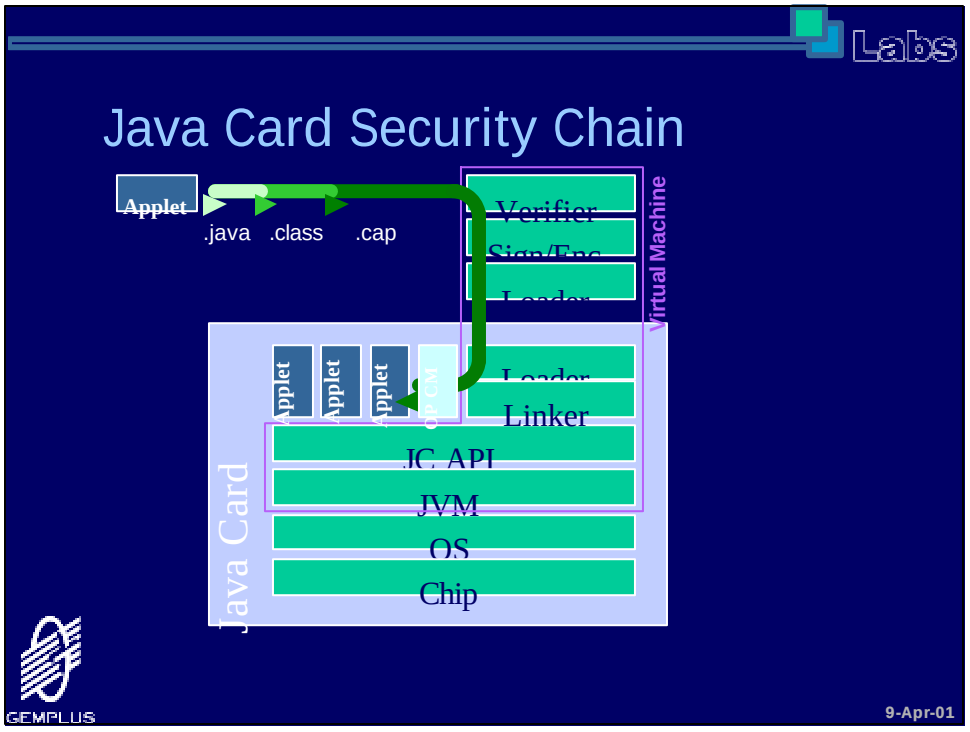
A subset of Java

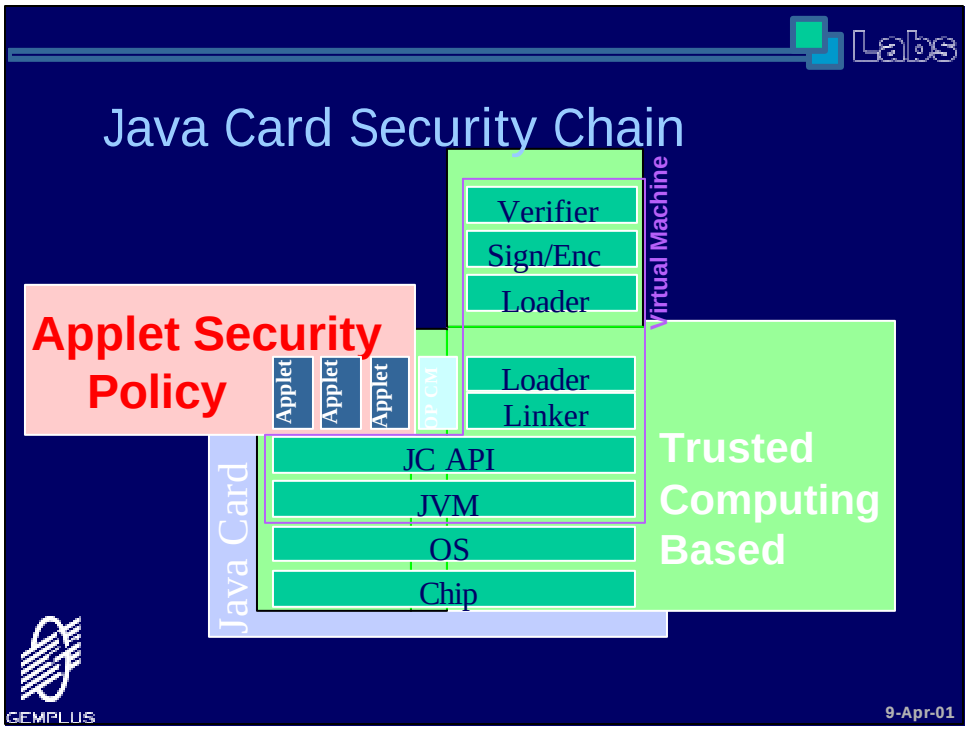
- A single thread virtual machine
- Unsupported features
  - Dynamic class loading
  - String and Thread classes
  - Double, float, char types
  - Multiple dimension arrays
  - Java.lang.System class
  - Garbage collection
  - Security manager
- The Applet Firewall
- Programming limitations

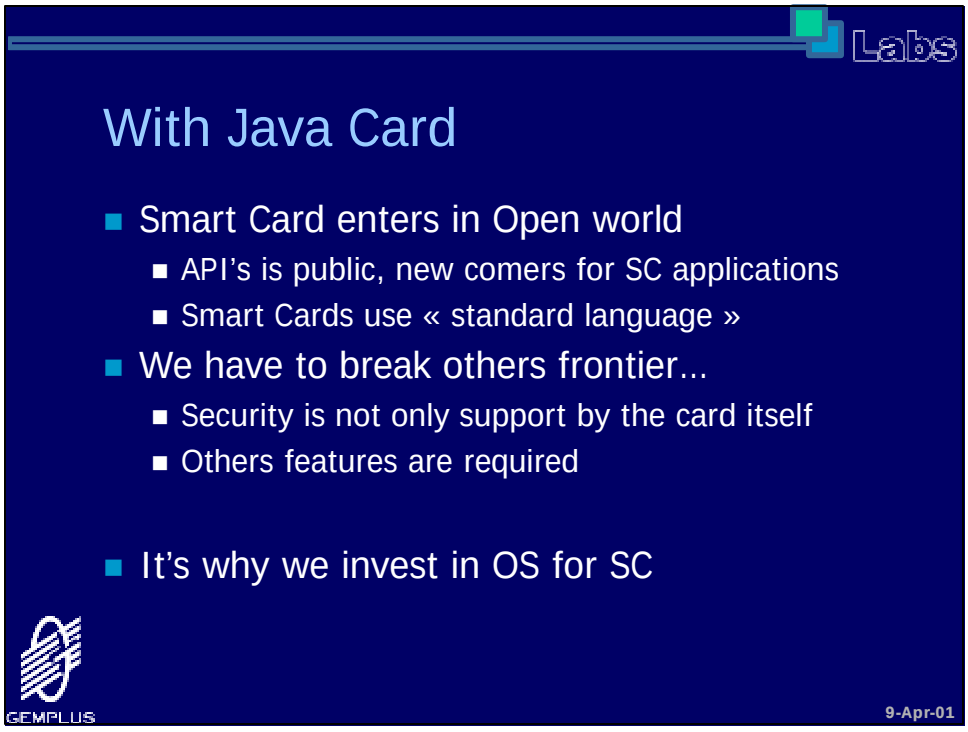
GEMPLUS

9-Apr-01


Labs
Java Card Environment
Code source Java
Class File Java
Java Compiler
Bytecode verifier and Converter
*.java
*.class
Dynamic Security
On Card
Firewall
Java Card Files
Linker
Loader
First static security tests
Other embedded Static checks and resolutions
GEMPLUS
9-Apr-01


Labs
Java Card Security Chain
Applet
.java
.class
.cap
Verifier
Loader
Virtual Machine
Applet
Applet
Applet
Linker
JC API
JVM
OS
Chip
Java Card
GEMPLUS
9-Apr-01


Labs
Java Card Security Chain
Verifier
Sign/Enc
Loader
Virtual Machine
Applet Security Policy
Applet
Applet
Applet
OP CM
Loader
Linker
JC API
JVM
OS
Chip
Java Card
Trusted Computing Based
GEMPLUS
9-Apr-01


Labs
With Java Card
Smart Card enters in Open world
API's is public, new comers for SC applications
Smart Cards use « standard language »
We have to break others frontier…
Security is not only support by the card itself
Others features are required
It's why we invest in OS for SC
GEMPLUS
9-Apr-01

Research issues in SC-OS

- How to secure the code down loading
- Portability
- Extensibility
- Object sharing

GEMPLUS

9-Apr-01

Two security levels

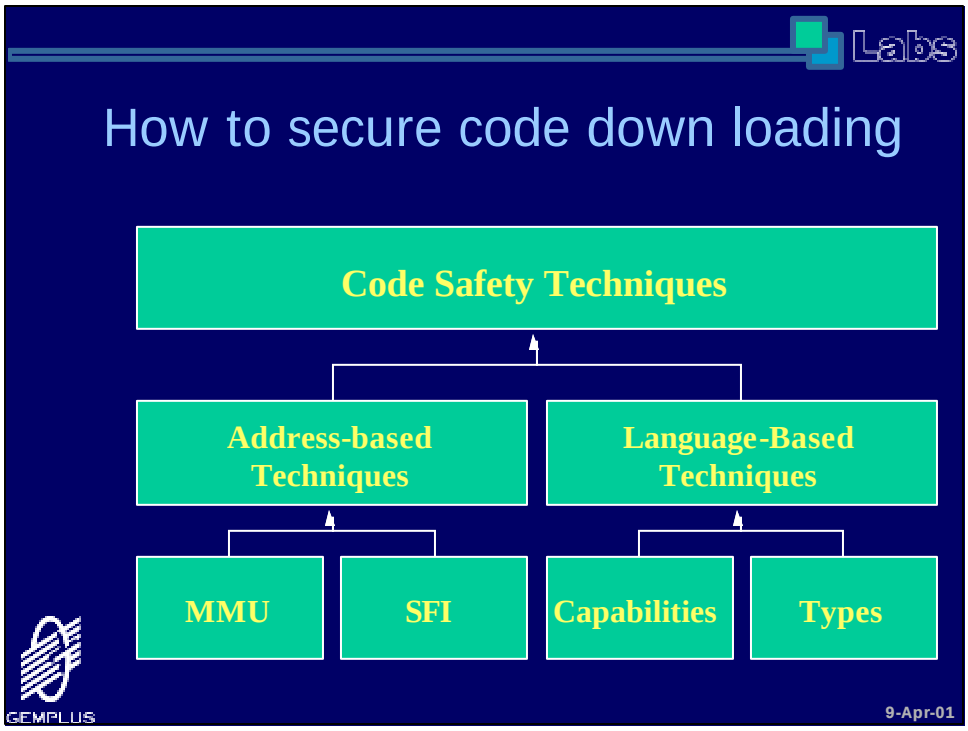
- Applications are no more developed under card issuer control
- Platform security
  - Traditional means
  - Use of formal methods

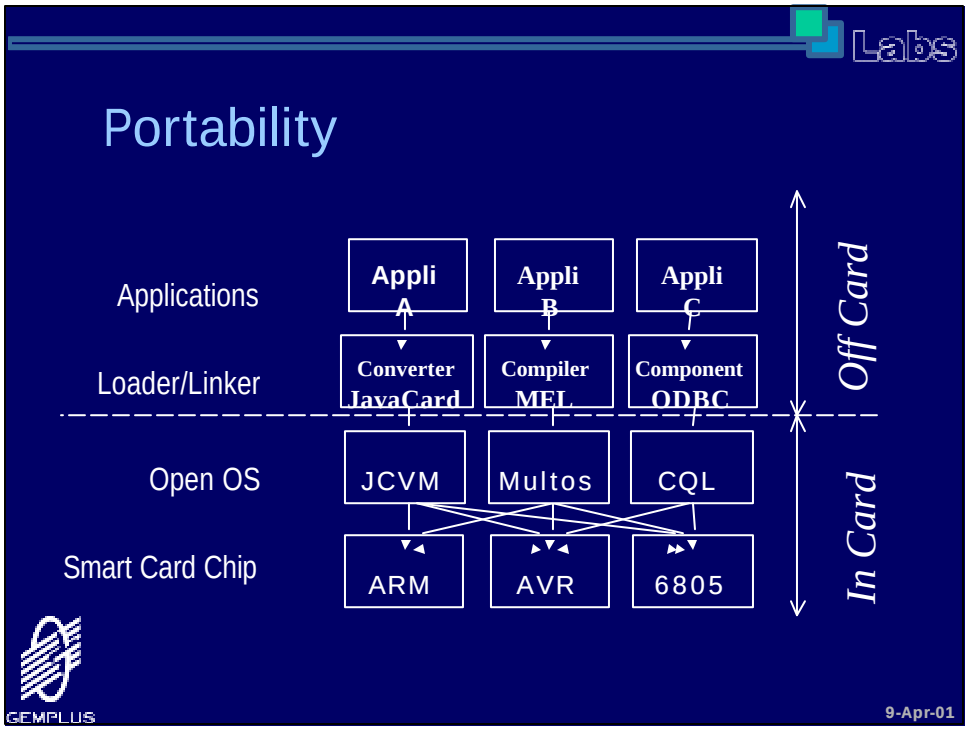
    => Models of the platform security modules
- Application security
  - There is a need for a global security policy
  - Flow control (data and/or code sharing)
  - Resources consumption (memory, CPU, method calls…)

  => Static & dynamic analysis of applet configurations (part of the CMS)

GEMPLUS

9-Apr-01


Labs
How to secure code down loading
Code Safety Techniques
Address-based Techniques
Language-Based Techniques
MMU
SFI
Capabilities
Types
GEMPLUS
9-Apr-01

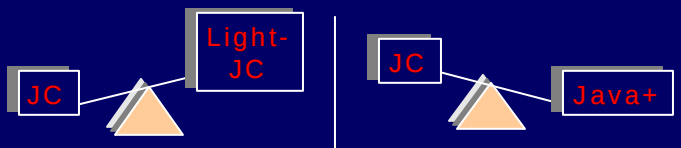

Labs
Portability
Applications
Loader/Linker
Open OS
Smart Card Chip
Appli A
Appli B
Appli C
Converter JavaCard
Compiler MEL
Component ODBC
JCVM
Multos
CQL
ARM
AVR
6805
Off Card
In Card
GEMPLUS
9-Apr-01

Labs

Extensibility

- No dynamic class loading
- Changing applications requirements various and growing

  E.g: the Java Card dilemma



Optimize the most crucial parts

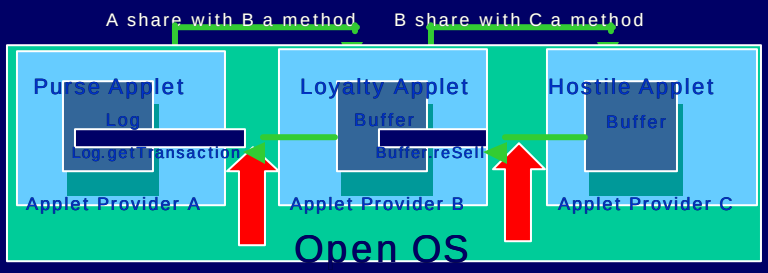
Increase functionality

GEMPLUS

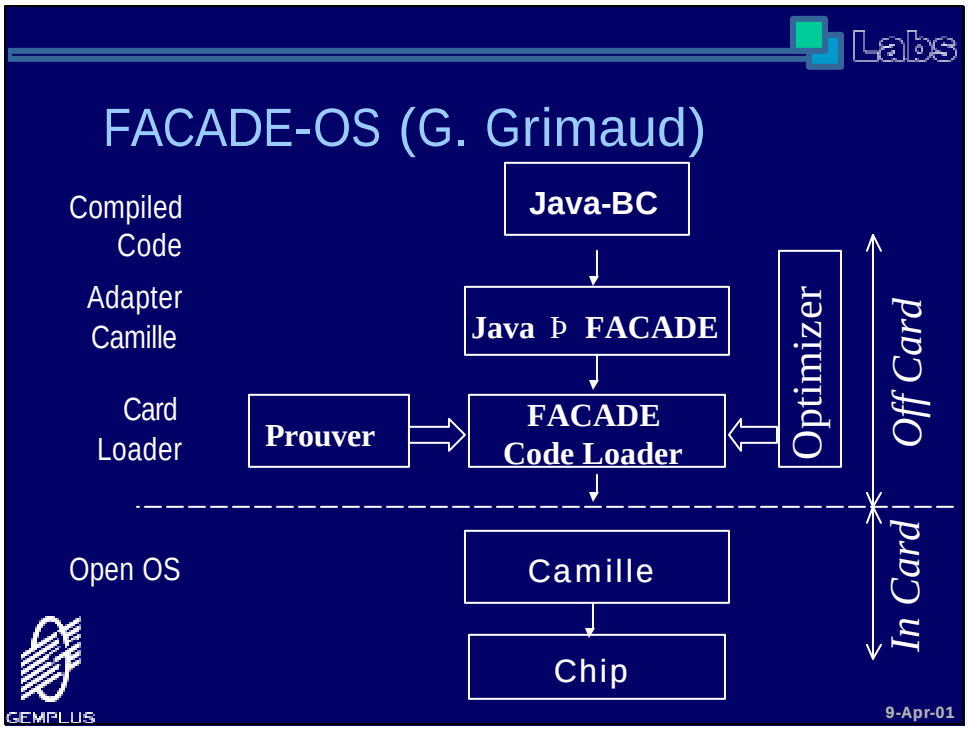
Labs

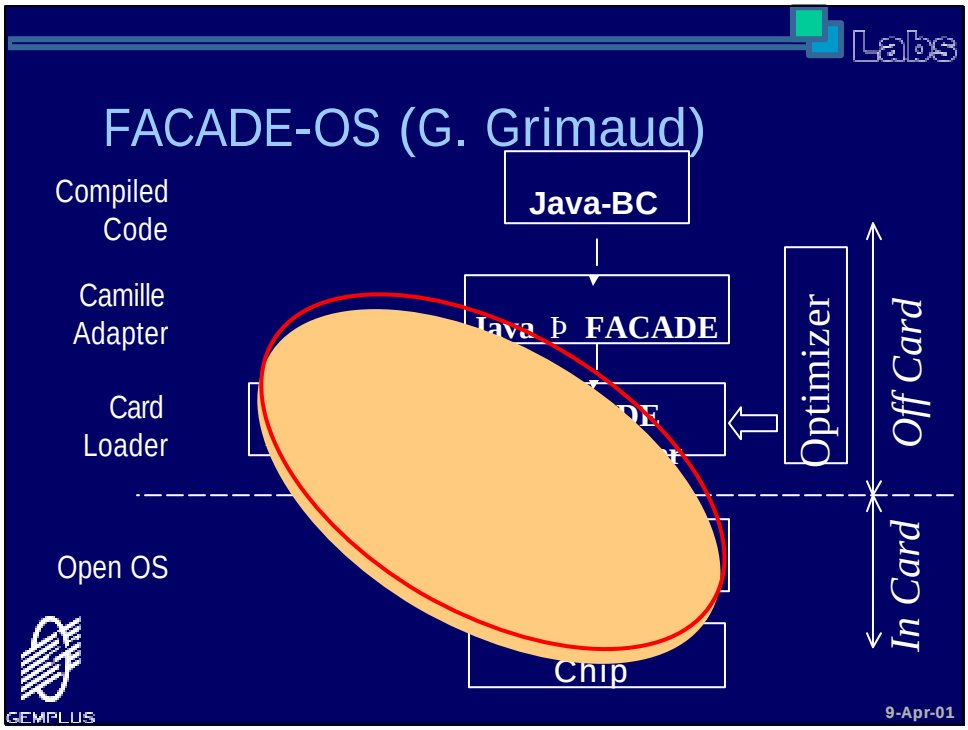
Objects Sharing

- For example: a purse and a loyalty applet can share methods and/or objects,



GEMPLUS


Labs
FACADE-OS (G. Grimaud)
Compiled Code
Adapter Camille
Card Loader
Open OS
Java-BC
Java Þ FACADE
Prouver
FACADE Code Loader
Optimizer
Off Card
In Card
Camille
Chip
GEMPLUS
9-Apr-01


Labs
FACADE-OS (G. Grimaud)
Compiled Code
Camille Adapter
Card Loader
Open OS
Java-BC
Optimizer
Off Card
In Card
Chip
GEMPLUS
9-Apr-01

Facade figures

- Based on AVR (8 bits RISC, RAM 1536 Octets, ROM 32 Ko and Flash 64 Ko)

Classes	Type Inference	Code Generation	Total
CardKernel			2670
CardByte	540	900	1460
CardShort	70	46	116
CardBool	70	62	132
CardBxxx	300	800	1100
I/O, MM,...			3900
Total	**3690**	**9074**	**17748**

GEMPLUS

9-Apr-01

Integration/Interoperability

- J-J Vandewalle defines a Corba Object Adaptor in his PhD (1997)
- In the new Java Card version RMI mechanism will be integrated
- SC have to deal with high level objects or services

GEMPLUS

9-Apr-01

Trends....

- Communication model (TCP/IP,...)
  - Card as a Web Server !
- Multi-tasking
  - Payment and Telecom services at the same time
- Security model with criteria on the availability of resources
- Sharing and managing of resources (CPU, I/O, memories)

GEMPLUS

9-Apr-01

Q/A

http://www.gemplus.com

Pierre.Paradinas@gemplus.com

GEMPLUS

Labs

Historical account

- 1967: First idea on the use of electronic component in credit card (Europe, US, Japan).
- 1974: Roland Morenos patents
- 1979: First Bull CP8 card prototype
- 1982-1984: First experimentation in France
- 1987-1989: ISO standard
- 1990-1999: Applications
  - French “Carte Bleue” for banking
  - European mobile phone with GSM/SIM cards
  - Health insurance, e-purse,...
- 1997: First Java based open card

GEMPLUS

9-Apr-01

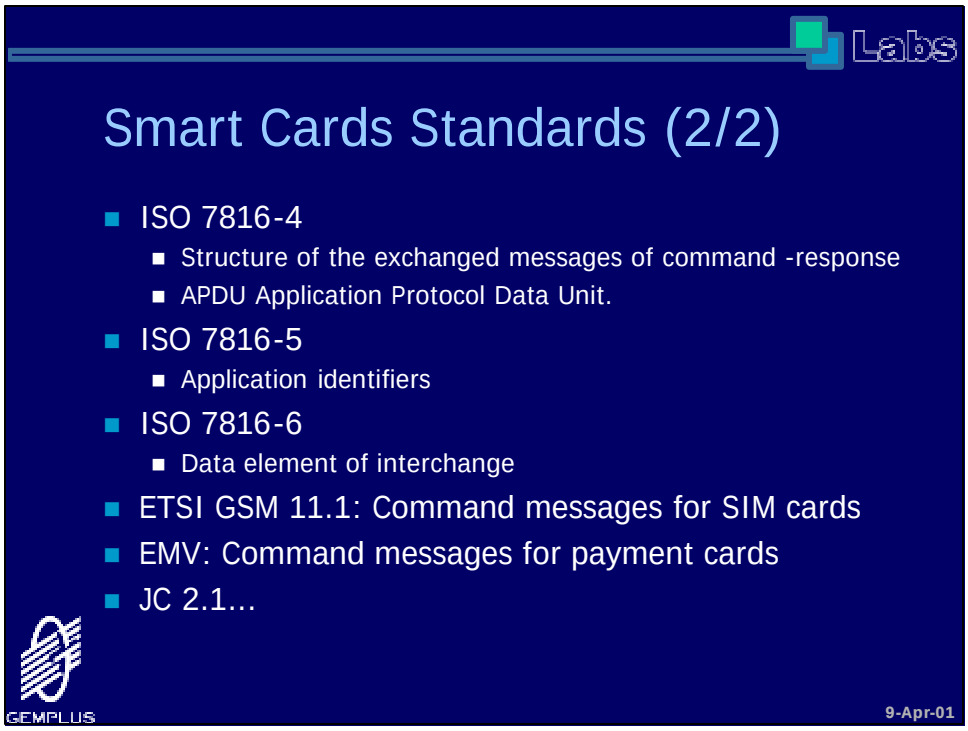
Labs

Smart Cards Standards (1/2)

- ISO 7816-1
  - Physical characteristic, constraints, size
- ISO 7816-2
  - Dimension and location of the contacts
- ISO 7816-3
  - Electric signal and transmission protocols
  - Card Answer to Reset: information about card characteristic
  - T=0; T=1

GEMPLUS

9-Apr-01


Labs
Smart Cards Standards (2/2)
ISO 7816-4
Structure of the exchanged messages of command -response
APDU Application Protocol Data Unit.
ISO 7816-5
Application identifiers
ISO 7816-6
Data element of interchange
ETSI GSM 11.1: Command messages for SIM cards
EMV: Command messages for payment cards
JC 2.1…
GEMPLUS
9-Apr-01