Short/Medium Term Technological
Challenges for Smartcards 1

- **Impact on Chip technology**

Java card standard evolution (à V 2.2)
Stronger interoperability Silicon independent card O/S
Use of RMI (remote methods invocation) Comm. I/Os / CPU performances
Logical channels to access memories NVM technology
Garage collection MPU / MMU
New cryptographic API (RSA 2048, AES, Elliptic Curves) Dedicated H/W or ISA

- **Biometric API**

Embedding card manager (for install / uninstall of Applets) MMU or MPU
Java card O/S will reach 200 / 300 KB Memory size
Improved security levels (EAL 5+, 6, 7**)**
Resistance to fault attacks Chip architecture or design methods
Tamper resistance H/W sensors

- **Applets verifiers**

New algorithms and appropriate countermeasures Specific ISA
Memory protection and partitioning MMU / MPU

Short/Medium Term Technological
Challenges for Smartcards 2

- **Impact on Chip technology**

Card interface with external networks and systems
High-speed communications protocols Comm. I/Os
Distributed applications architectures Comm. I/Os, CPU speed
Client / server architectures
Increasing need for computing power CPU architecture
Contact less / contact communication capability Multiple I/Os / UART
Multiple browsers on board Memory size / NVM technology.
Dynamic memory management MMU / MPU
Low power compliance (GSM / 3G / Contactless) Chip architecture / PM
Card manufacturing Process
Smallest dies size as possible IC process technology
Low cost assembly process Reduced test flow / quality
Personalization Specific I/Os / Fast writing NVM

Medium/Long Term Technological
Challenges for Smartcards 1

- **Impact on Chip technology**

Java card standard evolution (à V 3.0)
Evolution toward J2ME Size of ROM / RAM
Java card O/S may reach 512 KB Size of ROM

Migration of Toolkit (STK) toward Java card Applet
Distributed Java card applications becoming
a de facto model

- **I/O communication speed /MMU**

Card will run in a client / server environment MMU / MPU
Addressable memory size will reach 1 Mbytes CPU architecture / memory technology.
Average size of applets will be above 32 KB NVM memory technology.
Enhanced interoperability Open architectures for CPU
Enhanced garbage collector / No persistent heap MMU
Multithreading / Multitasking operations Logical memory access
Performances will request all Java Object in RAM RAM size or technology
O/S will be optimised for 32 bit chip architectures 32 bit CPU – ISA

Medium/Long Term Technological
Challenges for Smartcards 2

- **Impact on Chip technology**

Improved Security level (Above EAL 7)
On Card applet verifiers dedicated hardware
Embedded Security audit systems
Improved tamper resistance
Improved fault tolerant architectures Chip architecture / design methodology.
New algorithms Specific H/W or ISA

- **Card interface with external world**

Distributed Java card applications Firewall / comm. I/Os/ MMU/CPU
Integration of cards in frameworks for back offices, handsets, terminals Comm. I/Os/ chip architecture/CPU
Operated services NVM technology and MM
High-speed communications protocols Comm. I/Os
Low power compliance Chip architecture / PM / Chip technology.

- **Card manufacturing/ management requirements**

Low cost manufacturing Chip size / Auto test features
Performing personalisation process NVM technology / Comm. I/Os
OTA management NVM technology / MM / Communication I/Os

Two Contactless Technological Challenges from many :

- *Non Volatile Memory* :

– Cost
– Size
– Power Consumption
– Speed

- *High Speed Communications*

– Speed
– Interoperability
•Note: IST FP6 (European Technology Funding Recommendations)
•Short/medium term priorities
•High-speed protocols implementation

Must be Standardised !
Frequency choice needs to be made!
Use of existing standards may be possible
– WiFi
– Bluetooth
BUT POWER CONSUMPTION IS AN ISSUE!

Contactless Smart Card NVM

Requirements for Contactless Smart Cards :

- Fast program/erase
- Low power
- Granularity

Conclusion

- The Smart Card itself has to meet a number of Short/Mid/Long term challenges without the luxury of being a driving technology
- The Contactless Smart Card has to (in many applications) remain compatible with contact cards despite its technological differences

The main short term/medium term contactless issues that need to be addressed are:
– Non Volatile Memory choices
– How to obtain true high speed communications
- International Cooperation is needed if the smart card and its contactless interface are to succeed !