

Open Benchmark for Java Card Technology

J-M. Douin, P. Paradinas & C. Pradel

Cnam / Cedric

Mobile and Embedded Systems Group

Motivations

- There is no benchmark to day in smart card industry,
- What means “no” :
 - It is not public,
 - It is not accepted,
 - It is not opened.
- Benchmarks exist in :
 - R&D department of smart card manufacturer,
 - Some smart cards users organization.

Benchmark in others areas

- CPU
 - SPEC CPU2004 (<http://www.spec.org/>)
- Data base
 - The Open Source Database Benchmark (<http://osdb.sourceforge.net/>)

Benchmark in others area (cont'd)

- Transaction Processing
 - <http://www.tpc.org/>,
 - Top Ten TPC-C Results by Performance or
Top Ten TPC-C Results by Price/
Performance.
- Evolution from transactional to web services ...

What we may learn from IT

- Maturity of technology,
- Interoperable systems,
- Complexity of systems,

- ==>> Require elements of measure.

- We will not replace the technology choice by a simple ranking.

What is necessary to benchmark

- In Java Card Technology :
 - Performance,
 - Compatibility in term of interoperability.
 -
- Our goals and project is to provide open benchmark on these points.

Our approach in the project

- Inventory of measurable performances,
- Applet reference design and development,
- Performance evaluation in term of time, memory consumption and power,
- Comparison with existing in house benchmark,
- Benchmark tools packaging as an open software,
- Publishing on the web.

Our approach in the project

- Inventory of measurable performances,
- Applet reference design and development,
- Performance evaluation in term of time, memory consumption and power (in progress 1st step of card collection),
- Comparison with existing in house benchmark :
 - Volunteers ?
- Benchmark tools packaging as an open software,
- Publishing on the web.

Not an easy task

- Hardware configuration :
 - EEPROM/FLASH/FeRAM.
- OS, memory model and VM implementation.
- Garbage collector.

- But this is the challenge.

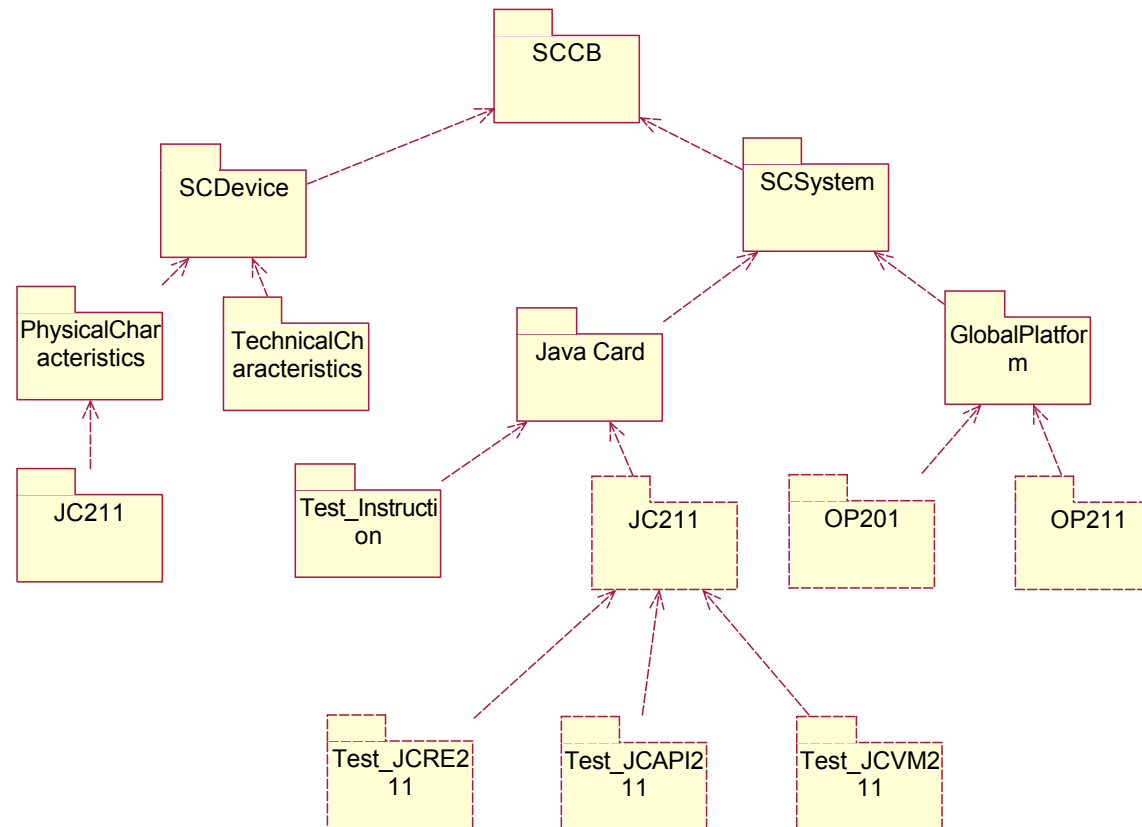
Others points

- We collect Java Card from different source :
 - 1st step with small number of card,
 - 2d step with large number of card from large manufacturer but also now with Java Technology provider.

What we will not perform...

- Java Card Technology specification conformance testing,
- Security evaluation,
- Measure and publication on product results.

Smart Card Cnam Benchmark



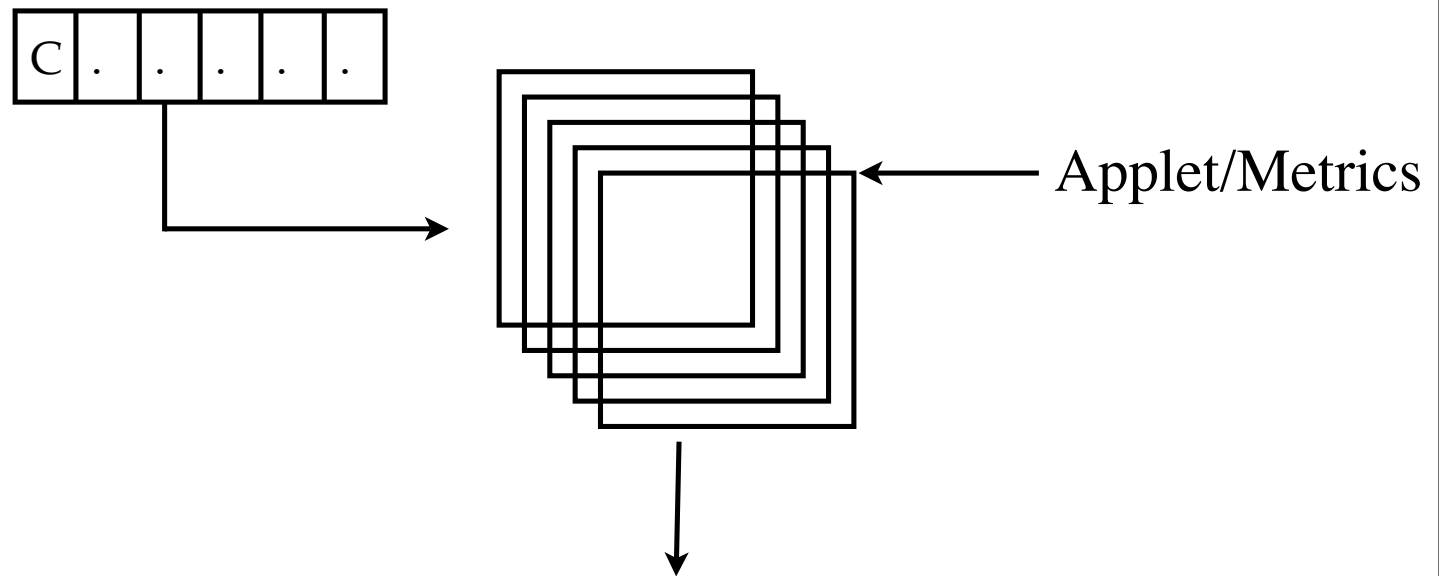
SCCB

- SCDevice checks hardware function like : memories, stack size and physical features,
- SCSystem evaluates performance of JC and OP :
 - Each packages performances are measured,
 - Others instructions (for, while,...) are also implemented.

Evaluation context

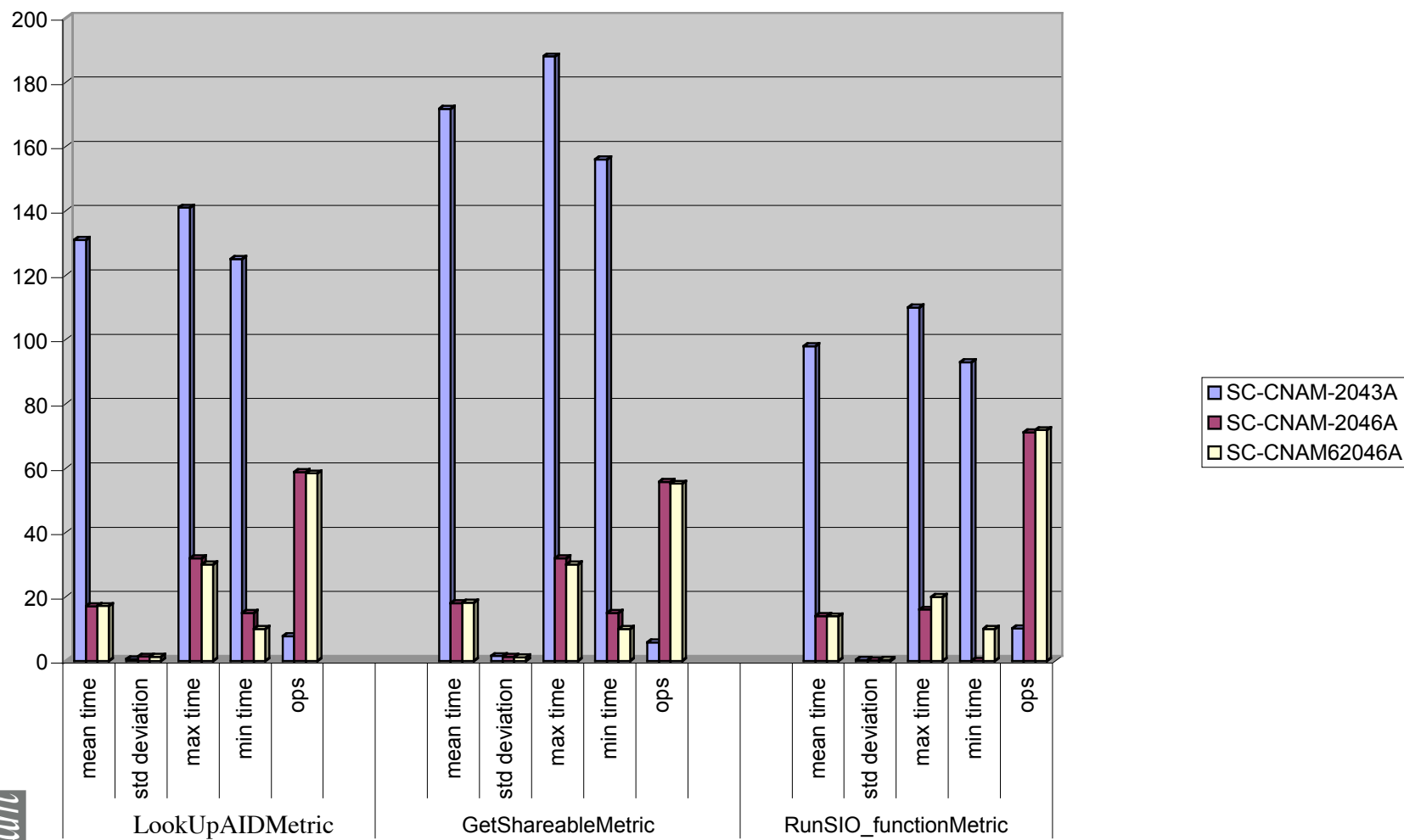
- Based on Windows platform and XP :
- Windows XP used with action :
 - To reduce and avoid constraints due to the Windows OS latency, PCs are not connected (autonomous),
- Variance on commands (command are repeated and an average calculated),
- Different PC platforms and readers will be used.

SCCB references : proposal

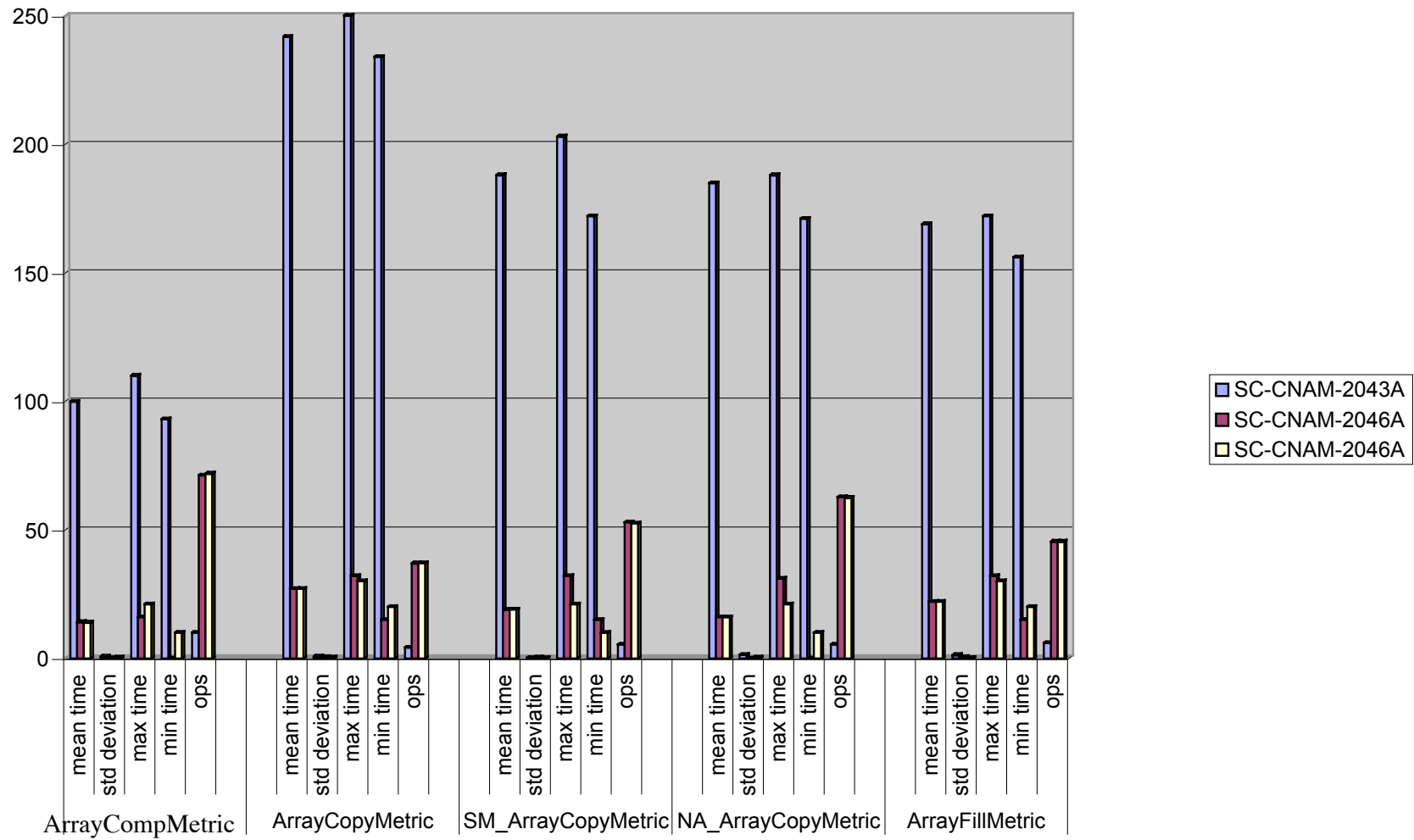


- * $\Sigma (\alpha.\text{metrics}) / \text{nbcards} = 100$
- * A card will be ranked after a complete test of Applet/Metrics compare to base 100.

ShareableMetric



UtilMetric



SCCBenchmark

File Edit View ?



List of Readers

Update list

GEMPLUS GCR410P 0
Gemplus USB SmartCard Reader 0
OMNIKEY CardMan 2020 0

Evaluation

Benchmark files

BasisInstruction-Arithmetic.rcb

List of results

ArithmeticSubtrac

Benchmark

Run single

Run all

- Benchmark
 - physical features evaluation
 - LTU (Latency Time)
 - NONVMMY (Non Volatile Memory)
 - STACK
 - VMMY (Volatile Memory)
 - javacard.framework package evaluation
 - JCSYS (JCSYSTEM Package)
 - OWNPIN (OwnerPIN Package)
 - SHARE (Shareable Interface)
 - UTIL (Util Package)
 - basis instructions evaluation
 - ARITHMETICS (Basis arithmetics)

Label	Value
ops	34.3997
min	15
max	32
std_deviation	0.293
mean	29.07

Rank Card

1.35



Ready

NUM

SCCBenchmark

File Edit View ?



List of Readers

Update list

GEMPLUS GCR410P 0
Gemplus USB SmartCard Reader 0
OMNIKEY CardMan 2020 0

Benchmark

Run single

Run all

- [-] Benchmark
 - [-] physical features evaluation
 - LTU (Latency Time)
 - NONVMMY (Non Volatile Memory)
 - STACK
 - VMMY (Volatile Memory)
 - [-] javacard.framework package evaluation
 - JCSYS (JCSYSTEM Package)
 - OWNPIN (OwnerPIN Package)
 - SHARE (Shareable Interface)
 - UTIL (Util Package)
 - [-] basis instructions evaluation
 - ARITHMETICS (Basis arithmetics)**
 - LOGIC

Evaluation

Benchmark files

BasisInstruction-Arithmetic.rcb

List of results

ArithmeticSubtrac

Label	Value
ops	34.3997
min	15
max	32
std_deviation	0.293
mean	29.07

Rank Card

1.35

Ready

NUM

Benchmark value added

- Generation differentiation,
- Plan improvement on new implementation,
- Provide a user point of view.

Benchmark value added

- Product performances comparison and evaluation,
- May help on QoS,
- May help on consumption with a better understanding of performance (local and global),
- Open question is how “security may be measured and ranked”.

Conclusion

- Open Benchmark (SCCB) for Java Technology is launched,
- We will collect a new collection of card :
 - From volunteers,
 - and from direct purchasing.
- We will present more results directly to card providers or users organization and complete SCCB in e-smart 2005.

Thank you.