gemalto

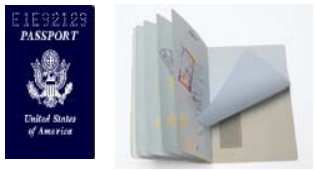
About the world-first smart card certificate with EAL7 formal assurances

Boutheina Chetali, Quang-Huy Nguyen
Security Labs
Technology & Innovation
Meudon, France

9thICCC, Jeju, September 2008

Why ?

e-passport **ID cards** **Health**



Mobile Payment

Transport

Loyalty

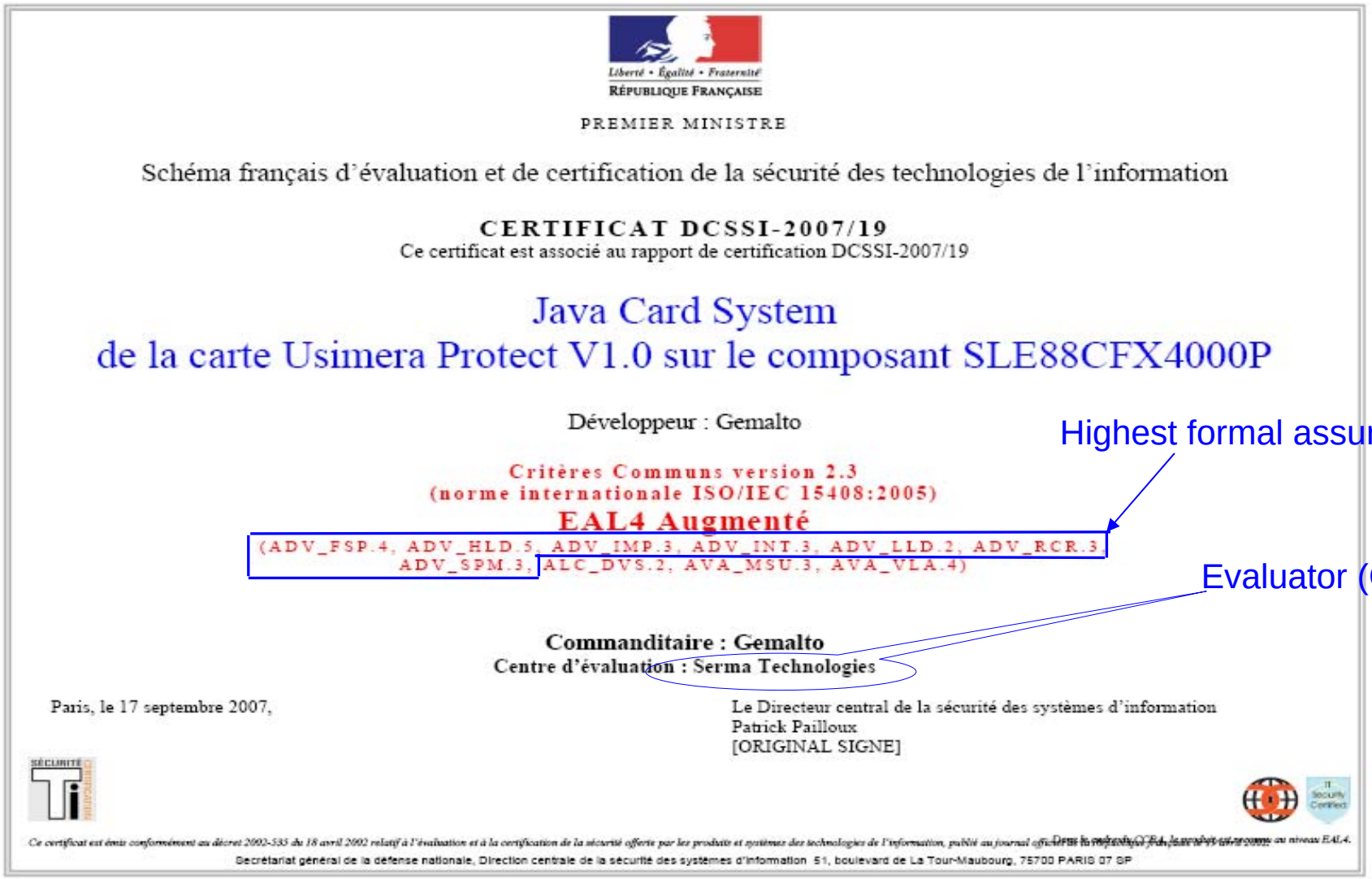
Credit/Debit

Ticketing

Smart Poster

- New threats
  - Privacy and Identity theft
  - Data disclosure between applications e.g., the bank do not want to be spied by the mobile operator
- New requirements on security and trust:
  - strong need of certification by independent authority
  - Both robustness (against physical attacks) and correctness (against software attacks) shall be ensured
- Robustness is ensured by penetration test: fault-injection, side-channel attacks, etc
- Correctness is ensured by evidence elements on the product development process (from specification to code)

The certificate



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Schéma français d'évaluation et de certification de la sécurité des technologies de l'information

CERTIFICAT DCSSI-2007/19
Ce certificat est associé au rapport de certification DCSSI-2007/19

Java Card System
de la carte Usimera Protect V1.0 sur le composant SLE88CFX4000P

Développeur : Gemalto

Critères Communs version 2.3
(norme internationale ISO/IEC 15408:2005)
EAL4 Augmenté
(ADV_FSP.4, ADV_HLD.5, ADV_IMP.3, ADV_INT.3, ADV_LLD.2, ADV_RCR.3, ADV_SPM.3, ALC_DVS.2, AVA_MSU.3, AVA_VLA.4)

Commanditaire : Gemalto
Centre d'évaluation : Serma Technologies

Paris, le 17 septembre 2007,

Le Directeur central de la sécurité des systèmes d'information
Patrick Pailloux
[ORIGINAL SIGNE]

Ce certificat est émis conformément au décret 2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerts par les produits et systèmes des technologies de l'information, publié au journal officiel [illegible] au niveau EAL4.

Secrétariat général de la défense nationale, Direction centrale de la sécurité des systèmes d'information 51, boulevard de La Tour-Maubourg, 75700 PARIS 07 SP

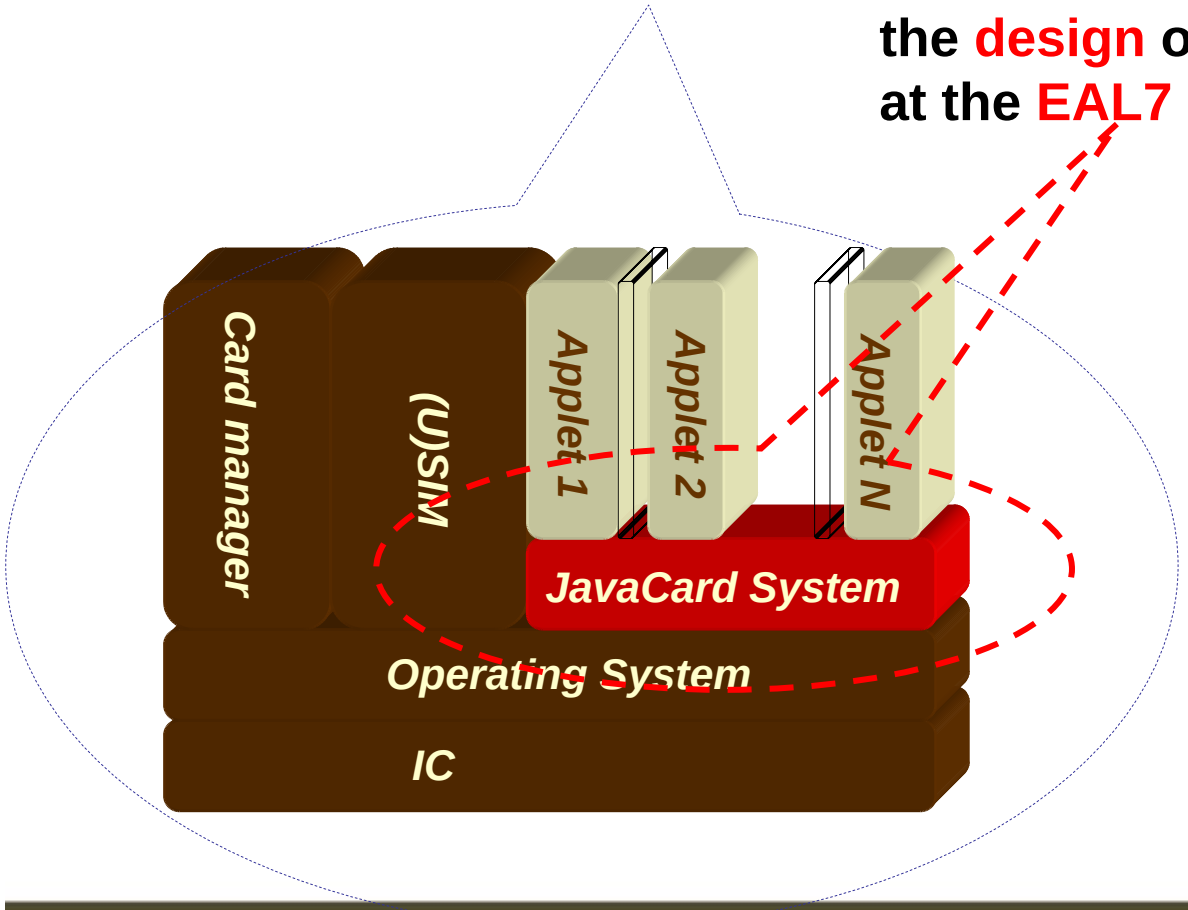
Highest formal assurances

Evaluator (CESTI)

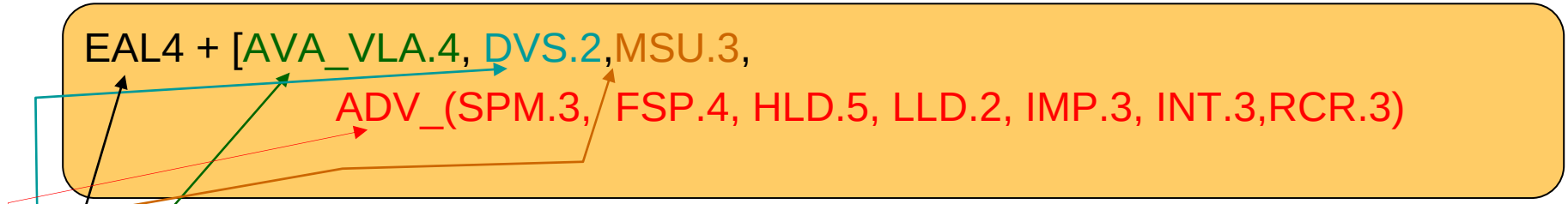
What it is ?

A SIM card embedding a Java Card System,
evaluated at the EAL4+ level , and where
the design of its JCS has been evaluated
at the EAL7 level

- ADV_SPM.3,
- ADV_FSP.4,
- ADV_HLD.5,
- ADV_LLD.2,
- ADV_IMP.3,
- ADV_INT.3,
- ADV_RCR.3



What does it mean ?



Testifies that the product…

- has been methodically designed, tested and reviewed, but also
- it is highly resistant,
- its security measures are sufficient for its confidentiality and integrity,
- its insecure states have been analysed and tested,
- its Virtual Machine has been formally proved correct :
  - The design and the development of the JVM security functions have been formally proved correct
  - The « C code » correctly implements the security functions
  - **And** the Firewall, as specified by Sun, is correct

How does it work ?

Goal : prove formally the correctness of the (security) design of the JVM, w.r.t. its specification

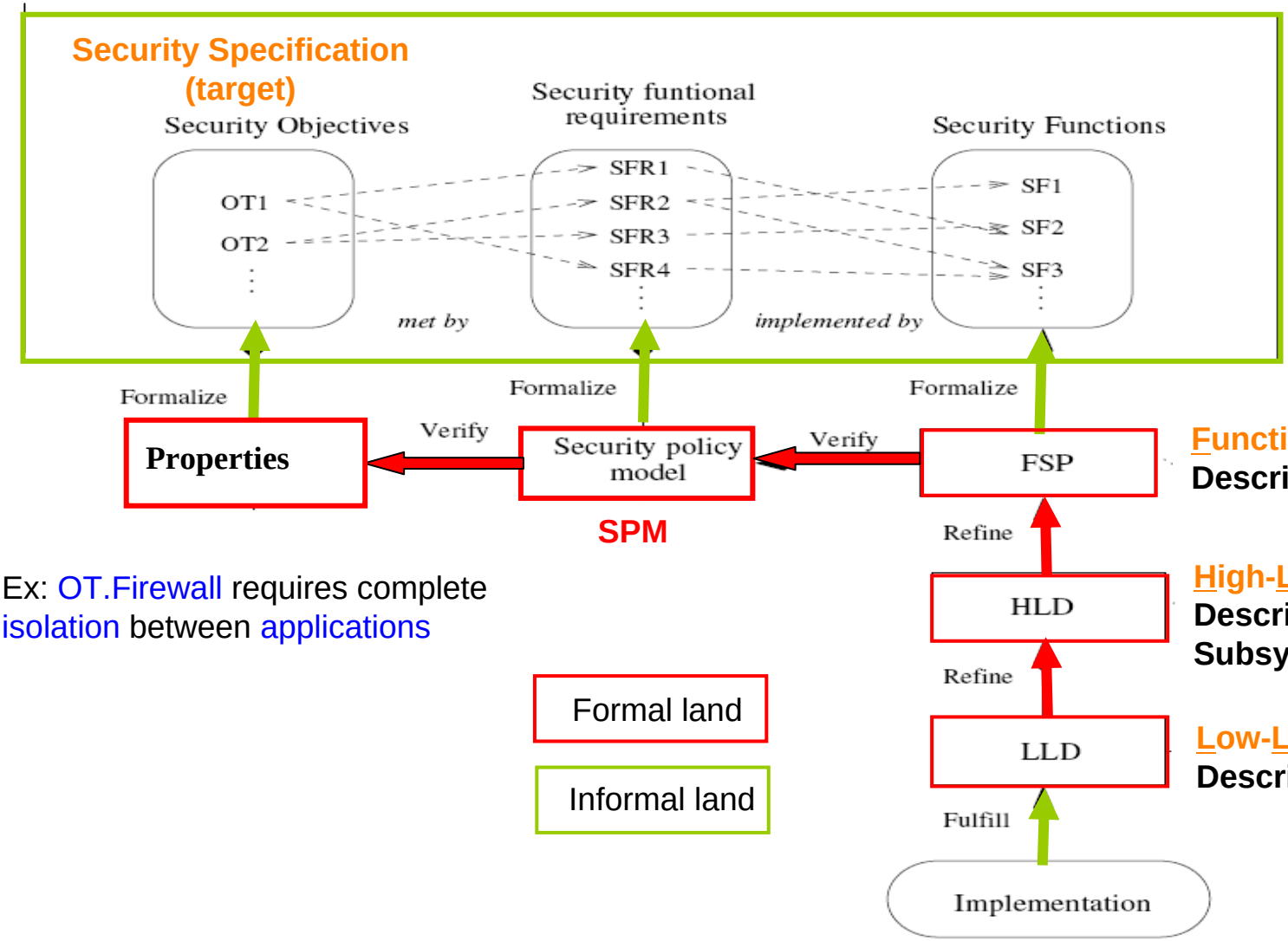
- Functional specification : Sun's JC2.2.1
- Security specification : security target
  - Security objectives
    - **O.Firewall** : The *JC Platform* shall ensure controlled sharing of data containers owned by applets of different packages, and between applets and the system.
  - Security functional requirements
    - **FDP_ACF.1.1/FIREWALL** The *JC platform* shall enforce the Firewall access control to objects based on their security attributes: the currently active context, the SELECTed applet Context, and the attribute ActiveApplets.
  - Security functions
    - **SF.Firewall** The JCRE firewall enforces applet isolation. The *JCRE* shall allocate and manage a context for each *applet* or *package* installed, respectively loaded, on the card and its own JCRE context. *Applet*s cannot access each other's objects unless they share the same context or they use the object sharing mechanism supported by *JCRE*.

ensure

Correctly implements

C implementation of the JVM

The global refinement from the ST



Ex: OT.Firewall requires complete isolation between applications

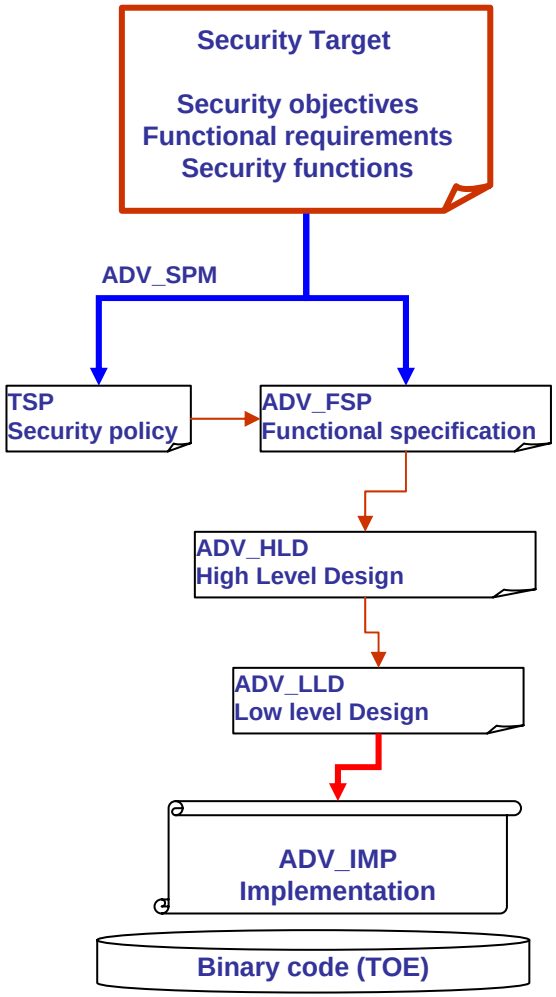
Functional Specification
Description of Interface

High-Level Design
Description of Subsystems

Low-Level Design
Description of Modules

Formalisation of the Security Target

- security target and the formal security policy ?
  - Each security objective is formalized as a (set of) property that the security policy model must ensure
  - The security policy formalizes (the behaviour) functional requirements
    - Firewall objective is translated into confidentiality and integrity theorems
- Security target and the formal functional specification ?
  - a mapping between the security functions and their formal specification.
  - this correspondence must show that the FSP is a complete and consistent representation of the security functions.



From Low Level Design to Implementation : bridging the gap between models and code

- Top-down: C code is generated from formal specification (e.g. [Bert *et al*.-FME-03]) but in smart cards industry
  - Certification of existing codes
  - performance and size issues of generated code
- Bottom-up: formal model is generated from C code (e.g. [Andronick *et al*.-FM-05])
  - It does not cover all C features and the model is complex
- Semi-formal link : the LLD has been built as a mapping between the model (HLD) and the code using a precise and complete code-to-spec review
- ADV_INT to minimize the complexity of the code-to-spec review task
- Note : no CC requirement on this correpondence

Some Figures

- The initial work started in 2002 (with Trusted Logic and INRIA)
- Evaluation, by Serma Technologies, lasted 1 year (June 2006-June 2007) including the training of the evaluator
- ~= 20K lines of C
- Most important formal development in Coq
  - > 117,000 lines (5 state machines of the JC Virtual Machine)
  - > 1600 proved theorems
- 30 elements have been delivered for evaluation (models and proofs)
- The most complex tasks have been the informal ones !

Summary

- A breakthrough in java Card security but also in CC methodology
  - **Feasibility** : first complete formal ADV chain (EAL7)
  - **Security** : the security properties of the specification are fulfilled by the code
- An implementation of the augmentation methodology providing the highest level of confidence:
  - the state of the art level for the whole product but with
  - The highest level of robustness for the whole product
  - The highest level of correctness for sensitive parts (security functions) of the product
- A contribution to the state of the art of the certifications
  - French certification body takes into account the achievement of this evaluation
    - Correspondence between informal and formal components
    - Formal modeling and tool

Challenges

- **Cost-effective reuse :**
  - Same VM is embedded on several (JC) products
    - each certificate includes the same augmentation
  - Enhanced/other VM implementations (code)
    - only the last step, between the most detailed description and the code, has to be developed
  - Other sensitive function
    - Global methodology is reused but models and proofs are rebuild

Questions ?

Boutheina Chetali
FM Group Manager
Security Labs
Technology & Innovation
Tel: +331 55015924

Boutheina.chetali@gemalto.com

References

- Chetali (B.) and Nguyen (Q.H.).—***Industrial Use of Formal Methods for a High-level Security Evaluation***, Proceedings **FM08**, LNCS 5014, 15TH International symposium on Formal Methods (FM08).—Turku, Finland, May 08.
- J. Andronick, Q-H. Nguyen. ***Certifying an Embedded Remote Method Invocation Protocol***. The 23rd ACM Symposium on Applied Computing (**SAC08**), Brazil,2008.
- Chetali (B.). ***How the Common Criteria requirements could be used for the development of secure software***, **ICCC'06**.Lanzarote, Spain, September 06.
- Chetali (B.) and Nguyen (Q.H.), ***Certifying Native Java Card API by Formal Refinement e***, In J. Domingo-Ferrer, J. Posegga, and D. Schreckling, editors, **CARDIS'06**, volume 3928 of LNCS, pages 313–328. Springer-Verlag, 2006.
- Chetali (B.) and Nguyen (Q.H.).—***Towards the CC Certification of a Java Card Virtual Machine*** Proceedings 5th International Conference on Common Criteria (**ICCC**'04).—Berlin, September 04.
- Chetali (B.), Gimenez (E.), Loiseaux (C.), and Ly (O.) .—***An Interpretation of the Common Criteria EAL7 level***, Proceedings 2th International Conference on Common Criteria (**ICCC**'02).—Ottawa, Mai 02.
- Certificate **http://www.ssi.gouv.fr/fr/confiance/certificats/certificat2007_19.html**