

Evaluation over a composite TOE in conformity  
with Java Card Protection Profile version 1.0 and  
Global Platform specifications

Ismael Kane

23<sup>rd</sup> September 2010

IT Security / Applus+

# Outline

- 1 Scope
- 2 Planning and Scheduling
- 3 Evaluation
- 4 Experiences

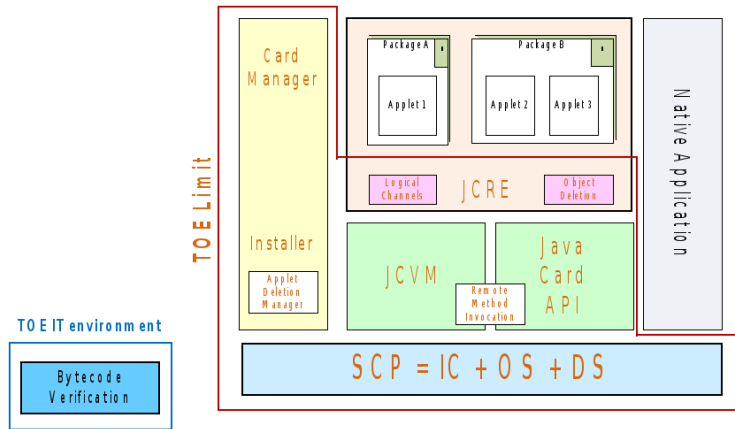
## Scope I

Initially, the TOE claimed conformity with JavaCard Protection profile version 1.0. After the analysis of the specifications and the source code the final scope was:

The TOE provides conformity against JavaCard Protection profile version 1.0 specifications 2.2.1 with an assurance level of EAL4 + augmented with ALC\_DVS.2 and AVA\_VAN.5 and it also fulfils the Global Platform Specifications version 2.1.1.

## Scope II

The TOE is a composition of an IC hardware and an embedded software that controls the IC.



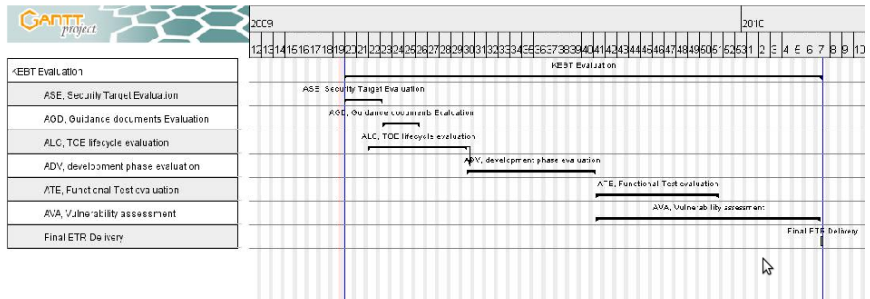
## Planning and Scheduling I

During the commercial stage of the process, Applus and KEBT agreed on the following schedule:

- ⊕ Agreement and contracts
- ⊕ Preparation phase
- ⊕ Evaluation

# Agreement and contracts I

The project plan phase concluded with the following project schedule:



## Preparative phase I

During that phase, Applus performed the following activities, emphasising:

- ⊕ Source code review, identification of some security problems (Overflows, timing, bad authentication mechanism, leakage, etc). All was solved and fixed by the KEBT.
- ⊕ Site Visit preparation, facilities alignment with the security requirements.
- ⊕ IC guidance review, confirmation of IC libraries (Crypto and RNG).
- ⊕ Specification review, identification of protection profiles and guidance for global platform specification.

# Evaluation I

During the evaluation stage the following EAL4+ assurance level was tackled:

- ⊕ ASE class
- ⊕ ADV class
- ⊕ ALC class, augmented with ALC\_DVS.2 component
- ⊕ AGD class
- ⊕ ATE class
- ⊕ AVA class, augmented with AVA\_VAN.5 component

## Evaluation II

The evaluation stage covers the ASE class with a security target available in <http://www.oc.ccn.cni.es/pdf/2009-9/2009-09-DS.pdf>.

It suffered different changes as a result of the observation reports found during the evaluation process, emphasizing:

- ⊕ Updating SPD for aligning the JavaCard Protection profile and Global Platform specification.
- ⊕ Modification of cryptographic algorithm key size due to Certification Body requirements.

## Evaluation III

The ADV evidences fulfil the requirements for EAL4+ common Criteria assurance level and give assurance of that describing the product with:

- ⊕ TSFIs are split in: Physical Boundary and I/O Pads with its logical and physical behaviour.
- ⊕ Subsystems and modules are provided and fulfil the requirements of composition, using the IC as an enforcing module.
- ⊕ The security architecture used the document ( JIL-Security Architecture requirements (ADV\_ARC.1) 1.0 for trial use) as a base.

## Evaluation IV

The developer adapts its work flow to Common Criteria, defining effective procedure that covers the whole life cycle:

- ⊕ Usage of a Configuration Management tool for centralizing all the configuration items
- ⊕ Automating all the generation process and providing integrity assurance of all the process steps
- ⊕ Facilities are re-structured for ensuring Site Development.
- ⊕ Adapt the JIL Protection Profile life cycle, aligning it with the underlying Platform (PP0035B) and Java Card Platform (JCSPPC)

## Evaluation V

The guidance covers all the product configuration and provides security recommendations and requirements for TOE users (Java Card application developers).

The preparative guidance describes the initialization process to put the product in the user phase, covering the ISD management.

The guidance documentation is aligned with the Global Platform Specification 2.1.1 and Java Card Specification 2.2.1.

## Evaluation VI

The testing approach defined by the developer tackled the TOE as a whole, using the standard tools provided by the specification developers to perform the testing:

- ⊕ Java Card subsystems, tested through I/O TSFI logical interface are done with Java Card Testing test suite.
- ⊕ Global Platform subsystems, tested through I/O TSFI logical interface are done with GlobalPlatform Test Plan using a commercial test suite.
- ⊕ IC subsystem, tested the pseudo random number generator using AIS20 probabilistic test suite and IC certificate.
- ⊕ TOE integration tests were created to check the security mechanism defined by the Operative System

## Evaluation VII

The evaluator considered the Attack method for performing the vulnerability assessment over the TOE and checked the confirmation attacks that were supposed to be protected by the underlying platform,

- 1 Physical analysis for confirming the strength of active and passive layers
- 2 Semi-invasive attacks using laser, Vcc, clock glitch
- 3 Side-channel for cryptographic operations (RSA and DES)
- 4 Software attacks covering ill-formed types, buffer transaction, RMI and shareable interface poisoning

## Experiences I

The CC evaluation process followed the correct flow. However some issues are going to be taken into consideration for further evaluation:

- 1 The protection profile is an aid for the generation of the Security Target but it should be aligned between different schemes, and notification of certificate misuse should be public in the common criteria portal.
- 2 The protection profile and the security target established an assumption that the Offcard Verifier validates the code loaded in the card. However there is not a clear and complete specification of the Offcard verifier so as a result, the TOE guidance should take this specification exception role.

## Experiences II

- 3 The GlobalPlatform security target guidance is a "mess" and there are a lot of inconsistencies with the Java Card protection profile.
- 4 The JIL-Security Architecture description (ADV\_ARC.1) v1.0 (for trial use) is focused on IC platform. However composite TOE should be included in this document because most of self-protection and none-bypassing security functions come from the IC underlying platform.
- 5 Get profit from the improvements in the CC specification. A clear example is that in the new release CC 3.1 R3, the testing is focused at subsystem level avoiding breaking down at very low level.

## Experiences III

- 6 Non-availability of the Java Card PP certified against CC 3.1 during the evaluation process and this issue produces the generation of further compatibility documentation.
- 7 For a composite TOE developers should use a the current versioned of the IC libraries.

# Questions and requests



Thanks for your attention

Applus<sup>+</sup>

LGAI

Ismael Kane