Ways to CC evaluation cost reduction - beyond CC V3

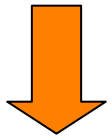
7th ICCC – Lanzarote 19-21 September 2006

Speaker : Françoise Forge
Security Management System- Evaluation schemes

Presentation overview

- Introducing gemalto
- What is gained from CC evaluation?
- Learning from 6 years of CC evaluations
- What are the next steps?
- Conclusion

gemalto = Gem(plus)+ (Ax)alto



- € 1.7 billions in combined pro-forma 2005 revenue
- 11,000 employees, 1500 R&D engineers
- 21 production sites, 32 personalization centers , 9 R&D centers

- Our business is smart cards
  - Telecommunication, Banking, e-passport, Heath Cards, Identity, Transportation, Pay-TV...
- Our concern is security
  - ITSEC, Common Criteria, FIPS, and other private schemes
- Our expectation is convergence of evaluation schemes
  - Actively contribute to the definition of methodology and security levels

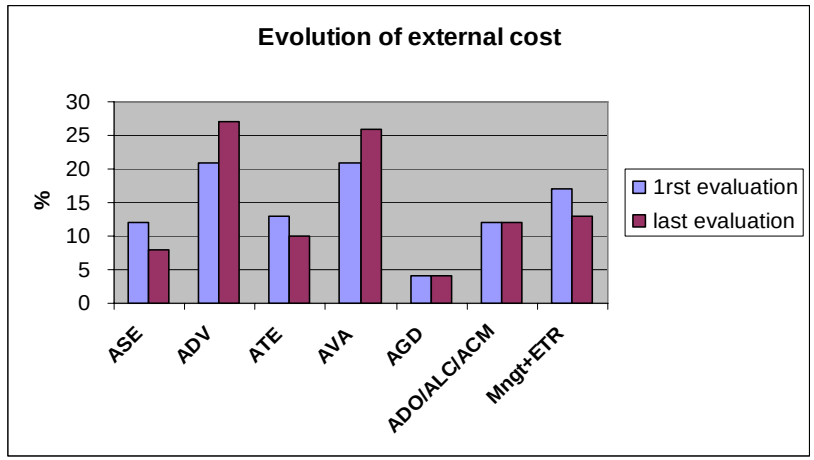
What is gained from CC evaluation?

- CC provides a standard for security evaluation
  - Common language for security description
  - Well defined level of security assessment
  - Well defined frame allowing reusability of evaluation work
  - Mutual recognition for international business
  - High level of confidence by efficient analysis and testing
- Still facing issues
  - Long and expensive process
  - Too much conformity checking and paper work
  - Time to market issue

Learning from 6 years of CC evaluations (1)

- Starting was tough !
  - Smart card industry put efforts in CC evaluation
  - Development and manufacturing process organized to fit CC requirements
  - Work with evaluation labs and evaluation authorities for interpretation and supporting documents

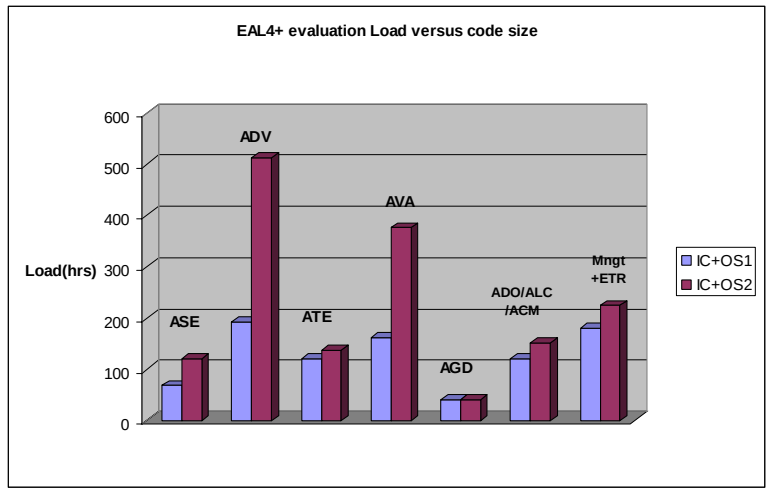
- Looking at some figures
  - Evolution on same product type at EAL4+ (AVA_VLA)



- Learning curve allows
  - Reducing conformity check (ASE, ATE)
  - Putting more efforts on ADV and AVA
- Management and reporting still represents a big part!

Learning from 6 years of CC evaluations (2)

- Looking at some other figures
  - Same product type EAL4+ (AVA_VLA4)
  - IC+OS1 = OS with 2 applications
  - IC+OS2 = OS with 5 applications



- When TOE complexity increases
  - High impact on ADV,AVA
  - Less impact on other classes due to
    - Knowledge of product type
    - Knowledge of developers' methods
    - Reuse of previous documentation (updates)
    - Tools shared with evaluators

Learning from 6 years of CC evaluations (3)

- Evaluation work load is reduced through
  - Learning curve of CC
  - Learning curve on product and application type
  - Reusing of previous evaluation results (developers environment)
  - Sharing tools with evaluators
- Continuous effort is made on smart cards evaluation process
  - Formalization of reusability
    - Smart cards composite evaluation methodology
    - Site CC evaluation project
  - Sharing information and techniques
    - Smart cards attack method & potential table definition

What are the next steps ?

- First of all ……..need some stability in CC !
- Continue the actions started for the improvement of CC process
  - impact of CC V3 (expected from clarification and simplification)
  - Site certification process
  - Improvement of supporting documents (composite evaluation, interpretation)

Go further ….

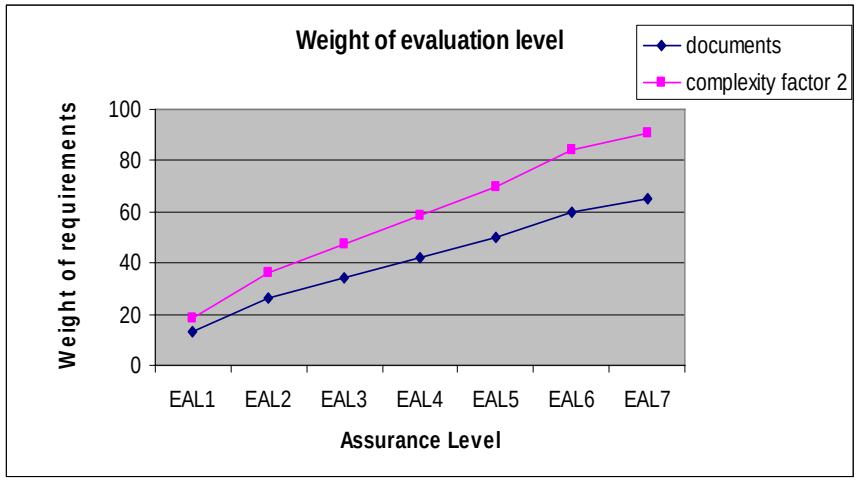
- Considering risk analysis
  - Defining the right level for the right TOE
- Reducing conformity check
  - Auditing a smoothly running process …

Benefits expected from current actions

- Benefits expected from CC V3
  - Considering EAL4+
    - ADV_SPM removed but ADV_ARC added
    - ADV_HLD/LLD merged in ADV_TDS
    - ADV_RCR removed but split inside documents
    - AVA class task removed for developers
  - Theoretically less documentation conformity check
  - But ….let's start first CC V3 evaluation
- Benefits expected from site certification process
  - Structured documents facilitate updating and change tracking
  - Removed travel expenses for distributed development sites
- Benefits expected from supporting documents
  - Save days of discussion and rework of documents
  - Save management expenses

Consider risk analysis - what security is needed?

- Evaluation load increases with
  - Assurance level
  - Size and scope of the TOE
  - Number of assets and attack paths



- Asking the good questions
  - What are the assets, the values I want to protect?
  - Is the evaluation scope appropriate?
  - Is targeted level of security appropriate?
  - Are security requirements pertinent considering product usage?

Consider risk analysis - defining the right TOE

- Risk analysis should be considered in PP/ST
  - Taking into account the application and the impact of loss
  - Usage environment (protected/open),
  - Assets to consider (value / accepted loss)
  - Achievable attack paths on the field (access conditions)
  - What the attackers gain from the attack (just for fun!)

Define the right security requirements and the right level, to optimize evaluation scope and load

Reducing conformity check

- Management represents more than 10% of the evaluation load
  - Systematic checking of documentation with detailed reporting,
  - Meeting, reviews, reports review and approval …..
- Looking for process simplification but keeping confidence
  - Concentrate evaluator task to acquisition of product knowledge, vulnerability analysis and penetration testing,
  - Limit conformity check work load (mainly developer documentation)
    - Documentation inspection by sampling
    - Tools for automatic generation and checking of documentation

Define standard frame of developer documentation
Define common tools to share between developers and evaluators

Conclusion

- The work started in smart cards industries shall continue
  - Migrate to CC V3 as soon as possible
  - Implement site certification process
  - Continue to supply supporting documents in collaboration with evaluators
- New ways shall be considered
  - Educate CC consumers on security level & risk management
  - Beyond CC V3, propose a methodology for simplification of documentation checking.

gemalto

Thank you for your attention !

Françoise Forge : Security Management System -Evaluation schemes
francoise.forge@gemalto.com