Advantages and drawbacks to use CC for private schemes

Francois GUERIN
Security Program Manager
francois.guerin@gemalto.com
Gemalto delivers secure personal devices, platforms and services, enabling its clients to offer trusted and convenient digital services to billions of individuals.
Gemalto experience in security evaluations

- Mastering Standard schemes for smart cards
  - More than 25 CC certificates (From EAL1+ to EAL5+)
  - More than 10 FIPS 140-X and FIPS 201 certificates
  - More than 20 ITSEC certificates
  - 7 sites certified ISO 27001 (some in progress)

- Leader to provide products in private schemes in markets:
  (Banking, MobileCom, PayTV, ID, Transportation, Health, IT,…)

> We spend near 10 M€ per year for product and site evaluations
Setting the problem

✦ As developer, some private schemes with divergent requirements.

✦ We have to manage an adaptative process for product development and site security in order to be compliant with new set of requirements. It is not effective and not security relevant.

✦ Customer would like more security proofs to be confident in product & site security but keeping flexibility and lost costs for evaluation.

✦ So we would like to promote reuse of best items of CC to integrate in private schemes in order to make more effective evaluations and to obtain more easily customer confidence.
## Sponsor requests for security evaluations

<table>
<thead>
<tr>
<th>Sponsors</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Government agencies for Public sector (ID, Health, Transport)</td>
<td>CC with dedicated PP</td>
</tr>
<tr>
<td>Private organizations for banking or Pay-TV market</td>
<td></td>
</tr>
<tr>
<td>Organization representatives for IT and ID market</td>
<td>FIPS</td>
</tr>
<tr>
<td>Organization representatives for banking market</td>
<td>Well defined private schemes including product and site evaluations</td>
</tr>
<tr>
<td>“The Target” Customers (Mobile com, Pay-TV, IT)</td>
<td>Simple private schemes with black box or grey box testing and optional production site evaluation</td>
</tr>
</tbody>
</table>
Why customers are reluctant in use of CC?

- Complex to manage (evaluation, certification, acceptance)
- Complex language to understand
- Not enough specific to answer to their needs
- Not enough flexible (standard EAL package)

=> CC: a tool made by expert for experts

- Costly
- Long duration
- Less efficient than black box or grey box testing approach

We often miss the target: obtaining customer confidence

- Lack of knowledge of context (real product usage, hacker profiles),
- Attack paths used by labs are complex versus real hacking scenarios,
- No shared risk analysis between actors.
Reuse of results: CC vs Private scheme

- A CC evaluation is performed for one product to address one or several customers.
  - The product certificate is reusable for composition in some cases.
  - CC results for a product evaluation:
    - A security target (ST lite is public for recognition)
    - Evaluation technical report (not public)
    - Certification report and a certificate (public on demand)
    - Mutual recognition (applicable between CB)

- A private scheme evaluation is performed for one product to address one customer.
  - Usually there is a testing report (not public), no public requirements, no public certificate.

=> In Private scheme, there is no way to reuse evaluation result.
Common « New » customer request

« We would like you perform testing of your product to convince me that our product is secure ».

That means select a lab, perform a 2-month testing campaign on a specific set of requirements to obtain my confidence.

Then, this is the beginning of a long story.

- How to convince ?
- How to obtain confidence ?
- What kind of confidence ?
- What is the security problem ?
- What is the context?
- What is the customer acceptance of risk ?
- Who pays for that?
Confidence = Effectiveness* Objectivity * Independence

✦ Effectiveness

(scope * requirements* consistency * correctness * robustness * expertise * evolutive)

- Clear **terminology** and definition of **requirements** with work packages and tasks
- Identified **scope** with coverage rationale
- **Correctness** with selection of scope, depth, rigor
  - work definition, application, evidences and rationale, checks
- **Robustness** with shared methodology and attack quotation
  - Context analysis and attacker profile definition
  - Vulnerability search, Product analysis, attack quotation table
- **Evolution** of CC covers changing environmental and technical factors
- **Re-usability** Appropriateness including previous evaluation results

✦ Laboratory competency requirement

- Laboratory accreditation scheme (competency check)
- Sharing of Knowledge Attack through CB control

✦ Objectivity and Independence

- External labs and Certification body control
- Definition of State of the art managed by CB
CC evaluation process / Principles

- **Objectivity**
  - Evaluation results are deduced from factual evidence, independent of a personal opinion

- **Impartiality**
  - When subjective judgment is required, the evaluation results are unbiased

- **Reproducibility**
  - An evaluator action carried out on a given set of evaluation deliverables, should always yield the same result.

- **Correctness**
  - The evaluation actions provide an accurate technical assessment.

- **Sufficiency**
  - The evaluation activities carried out meet all of the requirements for confidence

- **Appropriateness**
  - Each evaluator action provides assurance benefits at least proportional to the expended effort.

- **Clear definition of evaluation requirements for developer and evaluator**
- **Clear definition of evaluation methodology for evaluator minimizing interpretations & issues**
Evaluation methodology

- **Scope of evaluation** (what part of product is evaluated)

- **Functional requirements** (which functions are evaluated)
  - Security by construction (defined security function)
  - Security by design (consistency between SF)

- **Assurance requirements** (what evidences are evaluated)
  - by documentation inspection
  - by product testing
  - by product vulnerability assessment
  - by usage environment analysis
  - by development and production environment analysis

- **Evaluation Methodology** (how evidences are checked)
CC scheme: Roles & Responsibilities

**Sponsor**
- funds the evaluation
- receives the Evaluation Technical Report
- receives the Certificate / Certification Report

**Developer**
- supplies product & deliverables

**Laboratory**
- performs the evaluation
- write ETR

**Certification body**
- manages scheme and Labs
- accredits Lab (challenges)
- follows evaluation work
- harmonizes assurance tasks and environment audits
- mitigates attack path quotation
- validates ETR
- issues certificate

**Observers**
Represent final customers & organisms
- validates product usage (acceptance)

After certification, observers performs risk assessment and acceptance
Private Scheme: Roles & Responsibilities

**Sponsor**
- funds the evaluation & acceptance
- receives the Evaluation Technical Report
- receives product acceptance

**Developer**
- supplies product & deliverables
- performs the evaluation
- write ETR

**Laboratory**
- performs the evaluation
- write ETR

**Actor as Certification body**
- manages scheme and labs
- selects labs
- follows evaluation work
- harmonizes assurance tasks and environment audits (if any)
- mitigates attack quotation
- validates ETR
- issues acceptance list (not public)

After evaluation, ACB performs risk assessment and acceptance
3 common kinds of issues

- Product acceptance (for developer & sponsor)
  - Spend money for development & evaluation and miss the market
  - Perform a weak risk assessment leading to issues with customer after deployment

- Product evaluation (for laboratory)
  - Perform more work than planned in evaluation contract
  - Miss a weakness in product or environment leading to lost of image

- Product acceptance (for Customer)
  - Perform a weak risk assessment leading to issues on FIELD
Risk Analysis: Balance risks vs Benefits

Risks:
- Money
- Image
- Durability of company
- Employee & Customer security

Benefits:
- Money
- Market share
- Competitors
- Business opportunity
Issue in attack quotation according to expertise profile

Hacker profiles defining reference lab profile

Accredited & specialized Lab profiles vs reference lab profile

Even if same attack quotation table is used, different attack quotations may appear according to lab expertise. CB are able to leverage quotation better than customers.
Cost of product security

- Cost of definition including business case study
- Cost of development
- Cost of manufacturing
- Cost of transportation
- Cost of deployment
- Cost of administration (update, renewal,…)
- Cost of revocation

- Cost of fraud

- Cost of Product & Process evaluation
Cost of confidence with Common Criteria

CC evaluation is costly if you want a complete confidence:

- Product / Process / Environment / Delivery => (EAL4)

- It is possible to use specific packages to use CC items aligned to Private Scheme scope:
  - Level 1: Functional testing, Black box testing, VLA.2
  - Level 2: Functional testing, Grey box testing
What activities for customer confidence?

- Confidence in Product Security may be obtained through:
  - Risk Management
  - Shared Evaluation Methodology
  - Checks on Product security
  - Checks on Process (Dev, Manufacturing, Perso, Installation, Admin, usage)
  - Checks on Environment (Dev, Manu, Perso, IT)
  - Checks on delivery (roles, procedures, Logical & Physical)

- Confidence increases with the scope of evaluation (balance for confidence increase and cost & delay)
CC assurance classes & risk coverage

<table>
<thead>
<tr>
<th>Assurance on</th>
<th>APE</th>
<th>ASE</th>
<th>ADV</th>
<th>AGD</th>
<th>ALC</th>
<th>ATE</th>
<th>AHA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product resistance</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Product correctness</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Product Devt Process</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Manufacturing Process</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Personalization Process</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Final Delivery</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Guidance for operation</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Environment Development</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Environment Manufacturing</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Environment Personalization</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Private schemes cover only parts of assurance for product correctness and robustness (optionally environment manufacturing)
Assurance classes and Life cycle coverage

The CC EAL4 assurance components supply requirements for all the phases in TOE life cycle and all activities.

<table>
<thead>
<tr>
<th>Life cycle</th>
<th>Activities</th>
<th>Assurance class</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requirements</td>
<td>Need definition</td>
<td>APE&amp;ASE</td>
</tr>
<tr>
<td>Construction</td>
<td>Development</td>
<td>ADV&amp;ALC_LCD</td>
</tr>
<tr>
<td></td>
<td>Test</td>
<td>ATE</td>
</tr>
<tr>
<td></td>
<td>Vulnerability analysis</td>
<td>AVA</td>
</tr>
<tr>
<td></td>
<td>Development environment</td>
<td>ALC_CMx, ALC_TAT&amp; ALC_DVS</td>
</tr>
<tr>
<td>Delivery to user</td>
<td>Development environment</td>
<td>ALC_DEL</td>
</tr>
<tr>
<td>Installation and start up</td>
<td>Exploitation environment</td>
<td>ADO_IGS</td>
</tr>
<tr>
<td>Operation</td>
<td>Exploitation environment</td>
<td>AGD</td>
</tr>
<tr>
<td>End of Life</td>
<td>Exploitation environment</td>
<td>AGD</td>
</tr>
</tbody>
</table>

Private scheme requirements focuses only on operational phase
## Private scheme contents and CC proposal (1)

<table>
<thead>
<tr>
<th></th>
<th>Level 1 (Black Box)</th>
<th>CC Items &amp; Methodology</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Objectives</strong></td>
<td>Focused on major customer issues</td>
<td>Aligned but including CC terminology added value</td>
</tr>
<tr>
<td></td>
<td>Service availability, Key confidentiality</td>
<td></td>
</tr>
<tr>
<td></td>
<td>No theft of valued services</td>
<td></td>
</tr>
<tr>
<td><strong>Risk Management</strong></td>
<td>Not shared</td>
<td>Context shared (threat, attacker profile, asset, objectives) &amp; SF &amp; vulnerabilities</td>
</tr>
<tr>
<td><strong>Evaluation Methodology</strong></td>
<td>Poorly described and no sharing of attack paths and quotation</td>
<td>Described and shared</td>
</tr>
<tr>
<td><strong>Product dependant scope</strong></td>
<td>Weak definition of scope and requirements</td>
<td>Simple security target reading (Reuse) + CC Terminology</td>
</tr>
<tr>
<td><strong>Product dependant Correctness</strong></td>
<td>Functional specification reading (subset) Independent Functional Testing</td>
<td>ADV_FSP + Functional spec reading ATE_IND + Functional Testing</td>
</tr>
<tr>
<td><strong>Product dependant Robustness</strong></td>
<td>Penetration testing &amp; Potential Basic on a limited scope &amp; Customer acceptance</td>
<td>AVA_VAN.1* on a ST scope Customer acceptance</td>
</tr>
<tr>
<td><strong>Process</strong></td>
<td>No checks</td>
<td>Few checks</td>
</tr>
<tr>
<td><strong>Environment</strong></td>
<td>No checks</td>
<td>No checks</td>
</tr>
<tr>
<td><strong>Duration</strong></td>
<td>1 + 2 months</td>
<td># 1 + 2 Months</td>
</tr>
</tbody>
</table>
### Private scheme contents and CC proposal (2)

<table>
<thead>
<tr>
<th>Level 2 (Grey Box)</th>
<th>CC Items &amp; Methodology</th>
</tr>
</thead>
</table>
| **Objectives**     | Focused on major customer issues  
                     | Service availability, asset protection  
                     | No theft of valued services |
| **Risk Management**| Idem level 1             |
| **Eval Methodology**| Idem level 1             |
| **Product dependant scope** | Weak definition of scope and requirements |
| **Product dependant Correctness** | Functional specification, design reading  
                                       | Developer & Independent functional Testing |
| **Product dependant Robustness** | Penetration testing & Potential enhanced Basic on a limited scope & Customer acceptance |
| **Process**        | No checks               |
| **Environment**    | Visit                   |
| **Duration**       | 1+ 3 months             |

**Aligned but including CC added value**

**Simple security target reading (Reuse) + CC Terminology**

**ADV_FSP.1 + Functional spec reading**

**ADV_TDS.1, ADV_ARC.1, ADV_IMP.1 ATE_IND + Functional Testing**

**AVA_VAN.3* on a ST scope CB certificate & Customer acceptance**

**ALC_CMS, ALC_LCD**

**ATE_IND + Functional Testing**

**#2+ 4 months**
Proposal objectives & assumptions

Alignment of CC requirements on actual work items:
1. To introduce CC terminology and rigor
2. To decrease effort on correctness and process consistency
3. To focus effort on Robustness testing and Functional testing

These proposals are based on assumptions:
1. Developers have repeatable development & manufacturing process (ISO 9001)
2. Developers manage security environment (ISO 27001)
My proposal

- Explain customer interest of using CC
- Train Customer to CC terminology
- Share Risk methodology with Customer to leverage cost of evaluation vs cost of security

- Define assurance package aligned with risk assessment with a narrow scope than standard EAL.

- Write customer oriented packages of security objectives to include in security targets
Questions

Thank you for your attention