Common Criteria methodology for Smart Cards and Similar Devices

an overview of ISCI achievements

ISCI-WG1 - Eurosmart

Speaker: Alain Boudou

alain.boudou@gemalto.com
SOG-IS Mutual Recognition Agreement

Joint Interpretation Working Group (JIWG)

Supporting Documents

Smart Card & Similar Devices Technical Domain

ISCI - WG1 Methodology
(ISCI-WG2) JHAS Attacks

Common Criteria Recognition Arrangement

CCDB
ISCI is a Eurosmart initiative

Sharing a common objective with JIWG:
Consistent application of the criteria and methods between national schemes
Continuous improvement of the efficiency and cost effectiveness of the process
ISCI WG1 Contributors

IC manufacturers

Smart card manufacturers and issuers

Evaluation laboratories

Certification Authorities

2012 September 18th
ICCC 2012 PARIS
ISCI WG1: one common way of working

• A common objective: efficiency improvement, consistent application
• A consensus on the needs: which direction?
• A consensus on the methods: how to interpret CC?
• An implementation keeping the process applicable
• A common understanding and agreement expressed in supporting documents
• An environment promoting the emergence of useful and applicable PPs
Smart Cards & Similar Devices Technical Domain

Which is the direction of the technology evolution?

- Introduction of new actors and new roles
- Increased complexity of the lifecycle, i.e. of the supply chain
- Multiplication of the on-the-field configurations mixing secure and non-secure applications
- Fast renewal of products (versioning, customization, porting)

Modification of the trust model

Optimization
Modification of the trust model

- Distributed responsibility in the Smart Cards & SD supply chain:
  - Trust model is a chain of trust.
  - CC certificates are guarantees along this chain
Modification of the trust model

From …
Modification of the trust model

TO ...

Secure Appli Provider

Card Issuer

Certifier

Lab

Developer

Other appli providers

Developers

TSM

Usage phase

Suitable protocols

Respect of guidance for card administration

Trust chain

Supply chain

Other appli providers
Modification of the trust model

1. A certificate applies to a TOE in a given configuration of the product
2. Application domain separation may suffer exceptions
3. Application may be loaded after the product delivery
4. Application may be unknown at evaluation time

How to manage addition of applications to a certified product without certificate invalidation?

Objectives for the TOE
- Domain Separation
- Load protection

Objectives for the environment
- Verification
- Secure loading

with known
pre-issuance
applis
Addition of other types of applications

<table>
<thead>
<tr>
<th>Domain Separation</th>
<th>Load protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verification</td>
<td>Secure loading</td>
</tr>
<tr>
<td></td>
<td>Guidance</td>
</tr>
</tbody>
</table>

*Certificate usage restrictions*
*Risk manager’s responsibility*

with
unknown
applis

with
known
post-issuance
applis

<table>
<thead>
<tr>
<th>Domain Separation</th>
<th>Load protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verification</td>
<td>Secure loading</td>
</tr>
<tr>
<td></td>
<td>Guidance</td>
</tr>
</tbody>
</table>

*Certificate usage restrictions*
*Risk manager’s responsibility*
Modification of the trust model

- ANSSI Application Note to be JIWG supporting documents
  - Certification of « open » smart card products
    Requirements for a platform or an application on a platform to be certified with various types of applications
    - Known / Unknown
    - Pre-issuance / Post-issuance
    Define the responsibilities of the product risk manager
  - Independent certificate
    For the specific case where all applications are considered as unknown
Optimization: mutualization of appli evaluation

At this conference: Reuse of evidences and evaluation results by Carolina Lavatelli
Optimization: mutualization of ALC evaluation

Same Developer
- different products
- different Labs / Schemes
- different development sites

But some processes are common between sites and between products

Site A
- Product 2

Site B
- Product 1

Mutualization of ALC evaluation
Mutualization of ALC evaluation

Work units (from CEM) are classified (from AIS38)
  – Generic: reusable
  – Specific: evidences must be checked for each product

**Principle**

- **Site visit**
  – Generic ALC docs: processes & supporting activities of the site
  – Mutualization Report able to be transferred to other Labs
- **Product evaluation**
  – Specific ALC docs reference the used processes / sites
  – Evidences for specific work units
  – ALC report consolidation from the Mutualization Reports

**Benefit**

- Avoid redundancy between products and labs
- Different schedules for products and sites
- Homogenization of the ALC treatment between Labs / Schemes
Harmonization: security of development environment

- ALC_DVS Objectives:
  - Security measures shall be adequate to provide the integrity and confidentiality of the TOE design & implementation
  - Integrity & confidentiality that is necessary to ensure that secure operation of the TOE is not compromised

- Site security measures
  - Physical
  - Logical
  - Procedural
  - Personnel

- Interpretations by Labs
  - Product security policy
    - Info to be kept confidential
    - Material to be protected against unauthorized modification
    - People allowed to access

- Minimum requirements
- Based on standard practices

At this conference: Minimum Site Requirements for the smart secure device supply chain by J.Noller & W Gutau
The End

Questions?