A smart card evaluation experience under a Japanese scheme

Masashi Tanaka
NTT Service Integration Laboratories
NTT Corporation
Contents

1. Outline of our smart card
2. Background
3. Selection of evaluation facility and CB
4. Experience - viewpoint of evaluation
   4-1 Scope of TOE
   4-2 Scope of smart card product lifecycle
5. Conclusion
1. Outline of our smart card

ELWISE card

- Features
  - 1M bytes flash memory
  - Contact and contactless interface
  - Multi application (application firewall)
  - Post issuance application download
  - Main client: government agency and municipality

2. Background

- Procurement policy guidance of IT products in government agencies of Japan was made public around 2005-2006.

- Guidance recommended that each IT product receive CC certification.

- CC-certificated IT products are increasing in government agencies of Japan.

CC-certificated ELWISE card is necessary. Objective of Evaluation Assurance Level: EAL4 + CC version: 2.3
3. Selection of evaluation facility and certification body (CB)

• Our selection
  – Evaluation facility: ECSEC (Japan)
  – CB: IPA (Japan)

• Note: ECSEC outsources parts of evaluation (ex. penetration test, vulnerability analysis) to another evaluation facility - Brightsight (Netherlands).

• Why did we select both an evaluation facility and CB in Japan?

To avoid difficulties due to differences of cultural background
  – Evaluation/certificate processes in foreign facilities are difficult.
    • Language problems (documentation, communication)
    • Differences in security concept (site audit etc.)
  
  Cf. “East meets west” SHARP, TNO-ITSEF BV ICCC2005
CC certification flow in our case

Certification

Certification Body (IPA @ Japan)

As smart card integrator (NTT @ Japan)

Evaluation Facility (ECSEC @ Japan)

Evaluation (partial) (Brightsight @ Netherlands)

Evaluate all parts, including AVA_VLA

- TOE (OS,AP)
- Assurance document
- Chip ETR-LITE

- Outsource part of AVA_VLA evaluation process
- Brightsight had evaluated our IC
- Card AP/OS source design and review
- Instruction testing of card AP/OS with actual card
4. Viewpoint of evaluation

• Before starting the CC evaluation, we need to decide on what should be evaluated.
  – Scope of TOE
  – Scope of the smart card product lifecycle
## Viewpoint of evaluation

<table>
<thead>
<tr>
<th>IC chip vendor (IC development, IC manufacture)</th>
<th>Scope of TOE</th>
<th>Scope of smart card product lifecycle (PP9806)</th>
</tr>
</thead>
<tbody>
<tr>
<td>IC chip</td>
<td>Phase 2〜Phase 3</td>
<td></td>
</tr>
<tr>
<td>Smart card vendor (IC OS development, card manufacture)</td>
<td>•Smart card software (IC OS) + IC chip or •IC OS</td>
<td>Phase 1〜Phase 5</td>
</tr>
</tbody>
</table>
| System integrator (Smart card integration, Application development) | •Smart card software (IC OS, Application) + IC chip or •Smart card software (IC OS, Application) | Phase 1〜Phase 7
  #Due to business requirement |

Our case:
Smartcard product lifecycle (PP9806)
4-1. Scope of TOE

• Japanese CC scheme was careful about smart card composite evaluation (under CC v2.3).
  • Note: CC v3 is now OK.

• Thus, smart card software (IC OS, card manager, and application) are defined as scope of TOE.
Smart Card Evaluation
TOE: smartcard software

- TOE is smart card software, but IC also needs to be evaluated.
- IC was evaluated from the following viewpoints
  - ETR-LITE
  - Interface analysis between IC and embedded software
    - Confirm the security guidance
- IC OS and application embedded on IC is evaluated from the following viewpoint
  - by vulnerability analysis
  - by functional testing
4-2. Scope of smart card product lifecycle (1)

The following parties participated in evaluation activities.

IC chip vendor → Smart card vendor

Software subcontractor → NTT lab → System integrator → Client

NTT lab
Scope of smart card product lifecycle (2)

Mapping “PP/9806 Phase 1 - Phase 7” to our smartcard product lifecycle is as follows:

(#1) System integrator only directs execution of Phase 1 and Phase 5. It does not actually develop and manufacture.

Copyright (C) 2008 NTT Corporation
Define roles and responsibilities for all parties (1)

<table>
<thead>
<tr>
<th><strong>Smart Card Software Development (Software subcontractor)</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>• Card manager and application implementation</td>
</tr>
<tr>
<td>• Preparation of deliverables (ST, ADV, ADO, ALC, ACM, AGD, AVA)</td>
</tr>
<tr>
<td>• Site audit</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Smart Card Software Development (NTT Lab)</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>• CC project management</td>
</tr>
<tr>
<td>• Card manager and application design</td>
</tr>
<tr>
<td>• Preparation of deliverables (ADO, ALC, ACM)</td>
</tr>
<tr>
<td>• Site audit</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>IC OS Development (IC chip vendor)</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>• Preparation of deliverables (ADV, ADO, ALC, ACM, AGD, AVA)</td>
</tr>
<tr>
<td>• Site audit</td>
</tr>
</tbody>
</table>
Define roles and responsibilities for all parties (2)

<table>
<thead>
<tr>
<th>Role</th>
<th>Responsibilities</th>
</tr>
</thead>
</table>
| **IC Development, IC Manufacturing, and IC Packaging (IC chip vendor)** | - Preparation of ETR-LITE  
- Setting IC OS configuration  
- Site audit                                                                |
| **Card Manufacture and Pre-personalization (Smart card vendor)**       | - Preparation of deliverables (ALC, ADO)  
- Site audit                                                                |
| **IC Card Provider (System integrator)**                               | - Preparation of deliverables (ALC, ADO, AGD)  
- Arrangement of smart card vendor and client  
- CC project sponsor                                                        |
| **Personalization (Client)**                                           | - Preparation of deliverable (AGD)                                                |
Define roles and responsibilities for all parties (3)

The most serious matter is:
Which party should set IC OS to “locked?”
“Locked” means that no-one can execute IC OS external API directly.

Up to now (before evaluation):
• IC developer loads application to chip but does not set OS to “locked”.
• To prevent accidental addition/deletion of applications, smart card manufacturer must set OS to “locked”.

Issue:
• Evaluation facility points out security risk in delivery (IC developer => smart card manufacturer)

Our solution:
• Options:
  – Maximize security of delivery
  – Change party who sets OS

We chose the 2nd option: IC developer sets OS to “locked” (by considering total cost of certification processes).
Conclusion

- ECSEC (Japan) cooperates with Brightsight (Netherlands) to evaluate efficiently.

- TOE is smart card software, but it was evaluated in the form of the smart card including IC. Security for the smart card has been confirmed.

- It is very important to clearly share information about the product architecture and product lifecycle with the evaluation facilities in order to decide the viewpoint of the evaluation.

- In the product lifecycle, the roles and responsibility of each party should be decided considering security and cost.
Thank you
Masashi Tanaka
tanaka.ma@lab.ntt.co.jp

NTT Service Integration Laboratories