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

Cf. Masahiro Yoshizawa, Hideyuki Unno, Toshinori Fukunaga and Hiroshi Ban, "ELWISE - A Super Multi-purpose Smart Card", NTT REVIEW, Vol. 14,No. 1, pp. 23--27 (2002).

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)

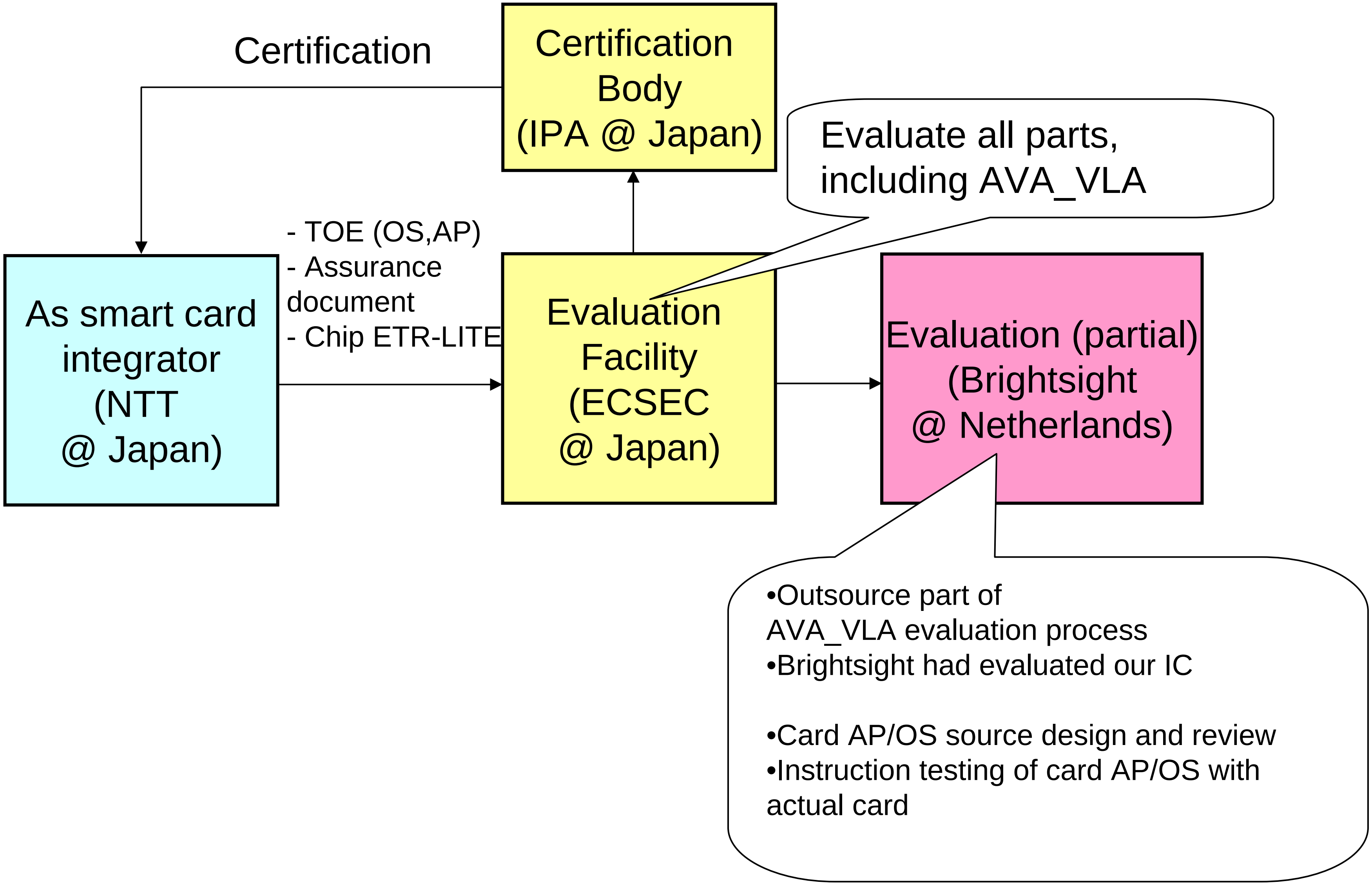
- Note: ECSEC outsources parts of evaluation (ex. penetration test, vulnerability analysis) to another evaluation facility - Brightsight (Netherlands).

- 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)

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

Evaluation Facility
(ECSEC
@ Japan)

Evaluation (partial)
(Brightsight
@ Netherlands)

Evaluate all parts, including AVA_VLA

•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

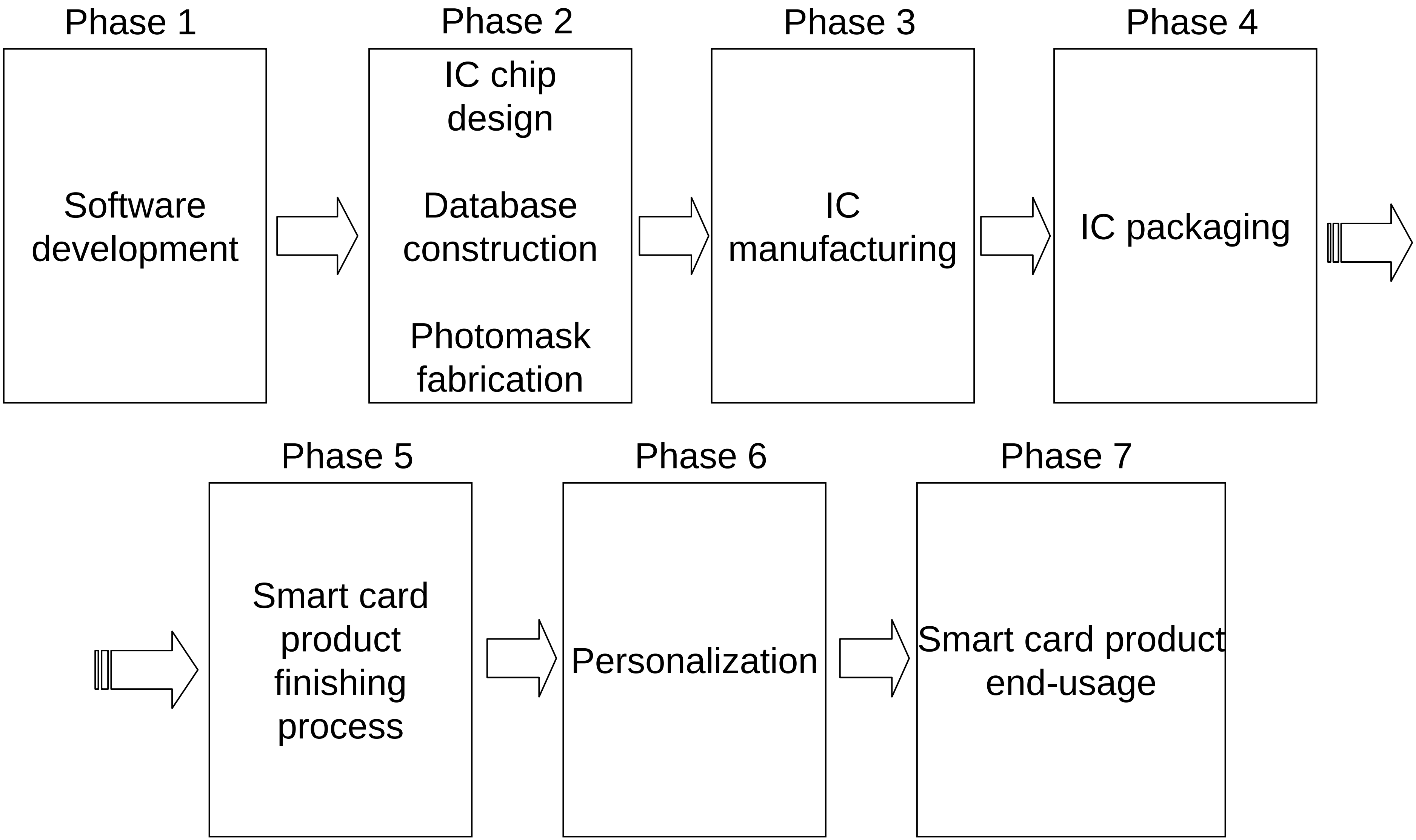
- Before starting the CC evaluation, we need to decide on what should be evaluated.
  - Scope of TOE
  - Scope of the smart card product lifecycle

Viewpoint of evaluation

	Scope of TOE	Scope of smart card product lifecycle (PP9806)
IC chip vendor (IC development, IC manufacture)	IC chip	Phase 2〜Phase 3
Smart card vendor (IC OS development, card manufacture)	•Smart card software (IC OS)＋IC chip or •IC OS	Phase 1〜Phase 5
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)



Phase 1

Software development

Phase 2

IC chip design

Database construction

Photomask fabrication

Phase 3

IC manufacturing

Phase 4

IC packaging

Phase 5

Smart card product finishing process

Phase 6

Personalization

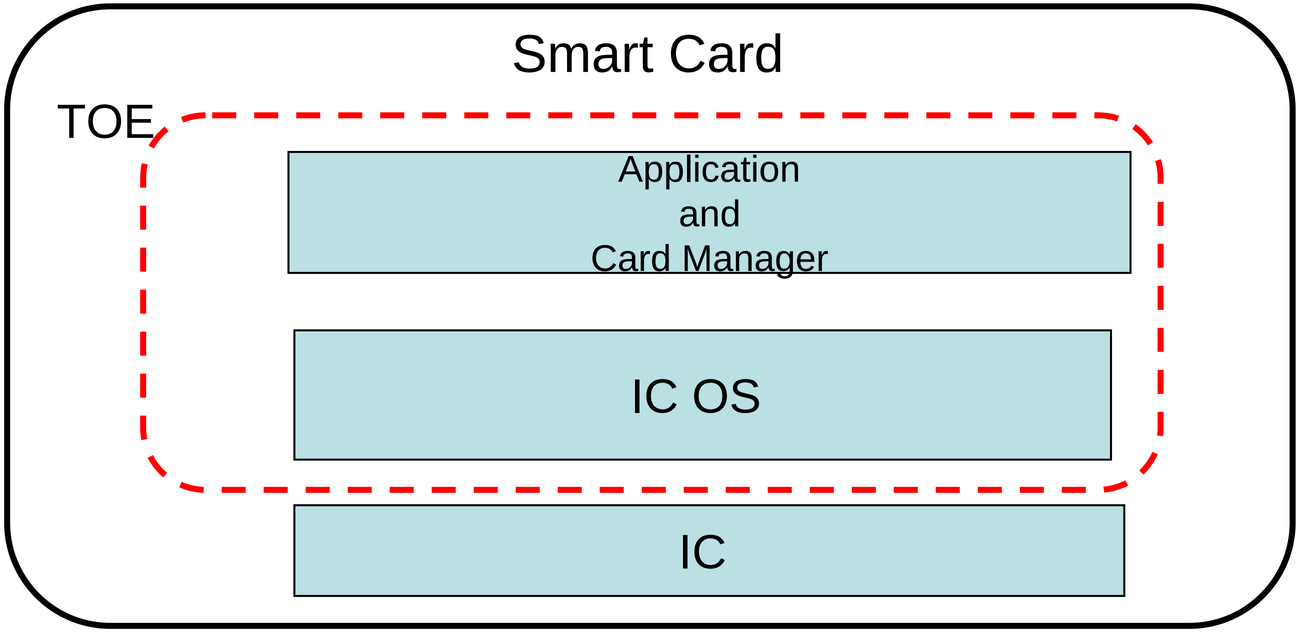
Phase 7

Smart card product end-usage

4-1. Scope of TOE

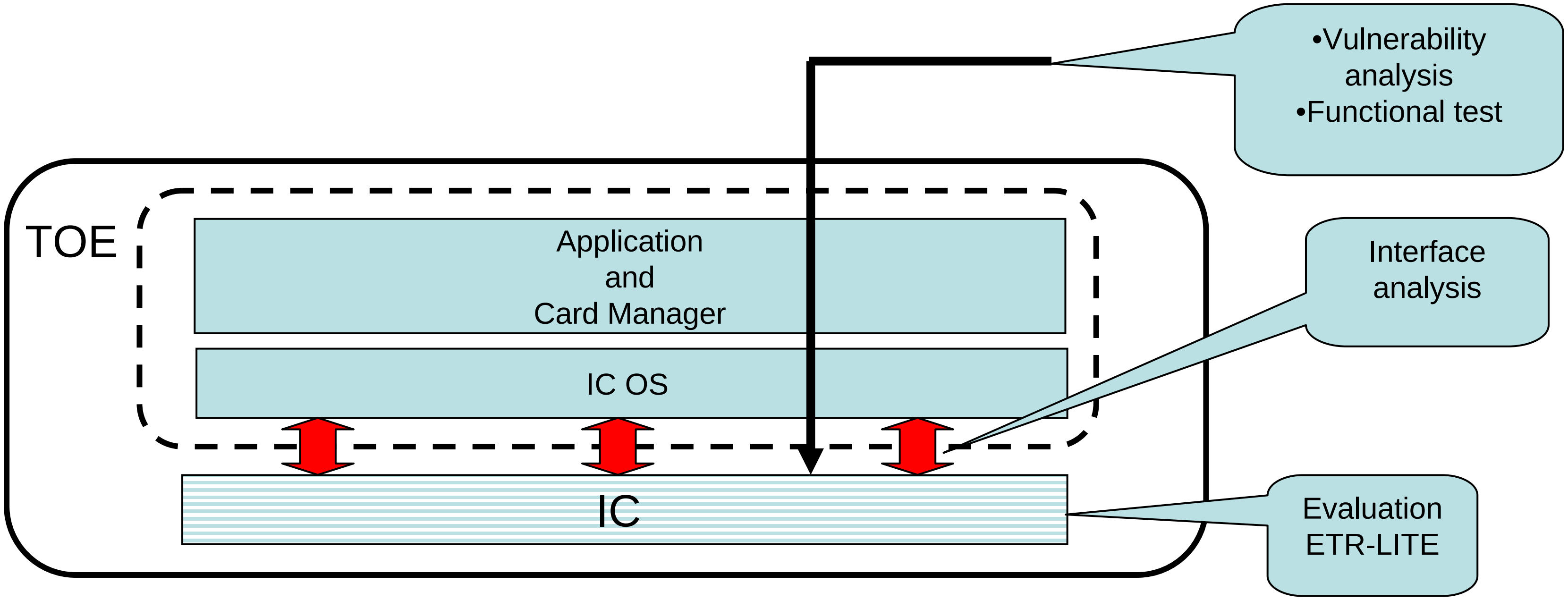
- Japanese CC scheme was careful about smart card composite evaluation (under CC v2.3).
  - Note: CC v3 is now OK.

- Thus, smart card software (IC OS, card manager, and application) are defined as scope of TOE.



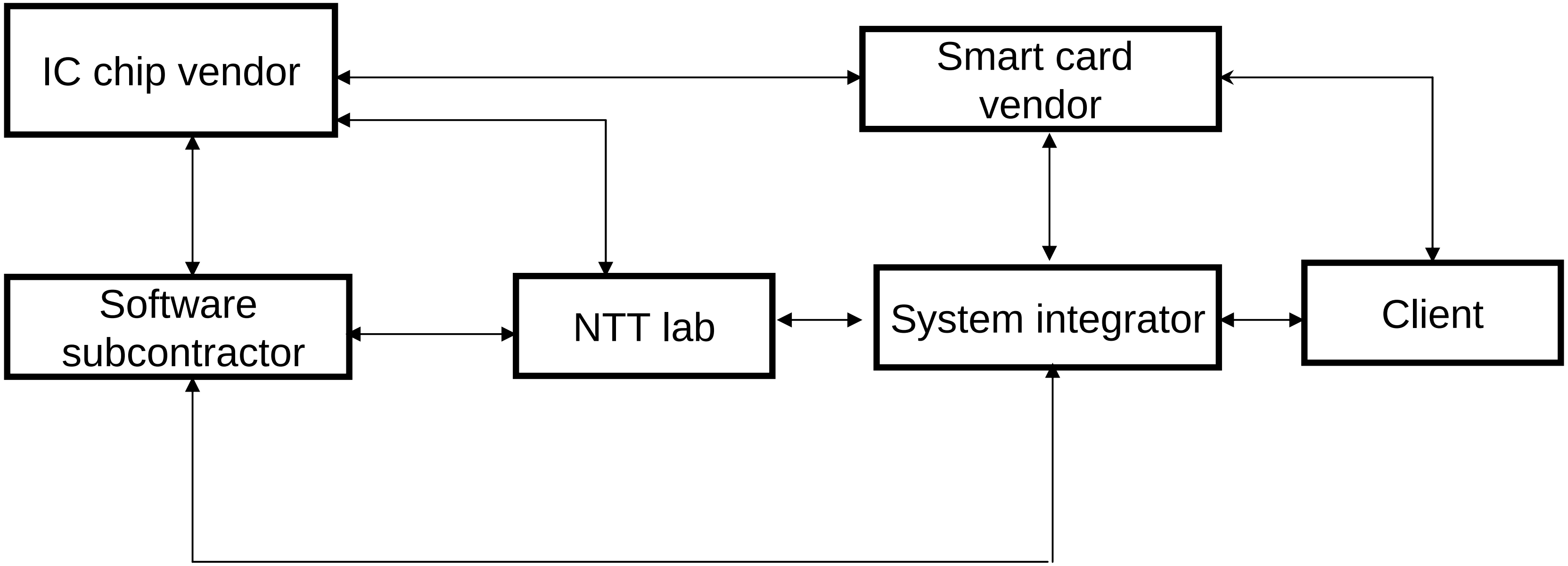
Smart Card Evaluation
TOE: smartcard software

- 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)

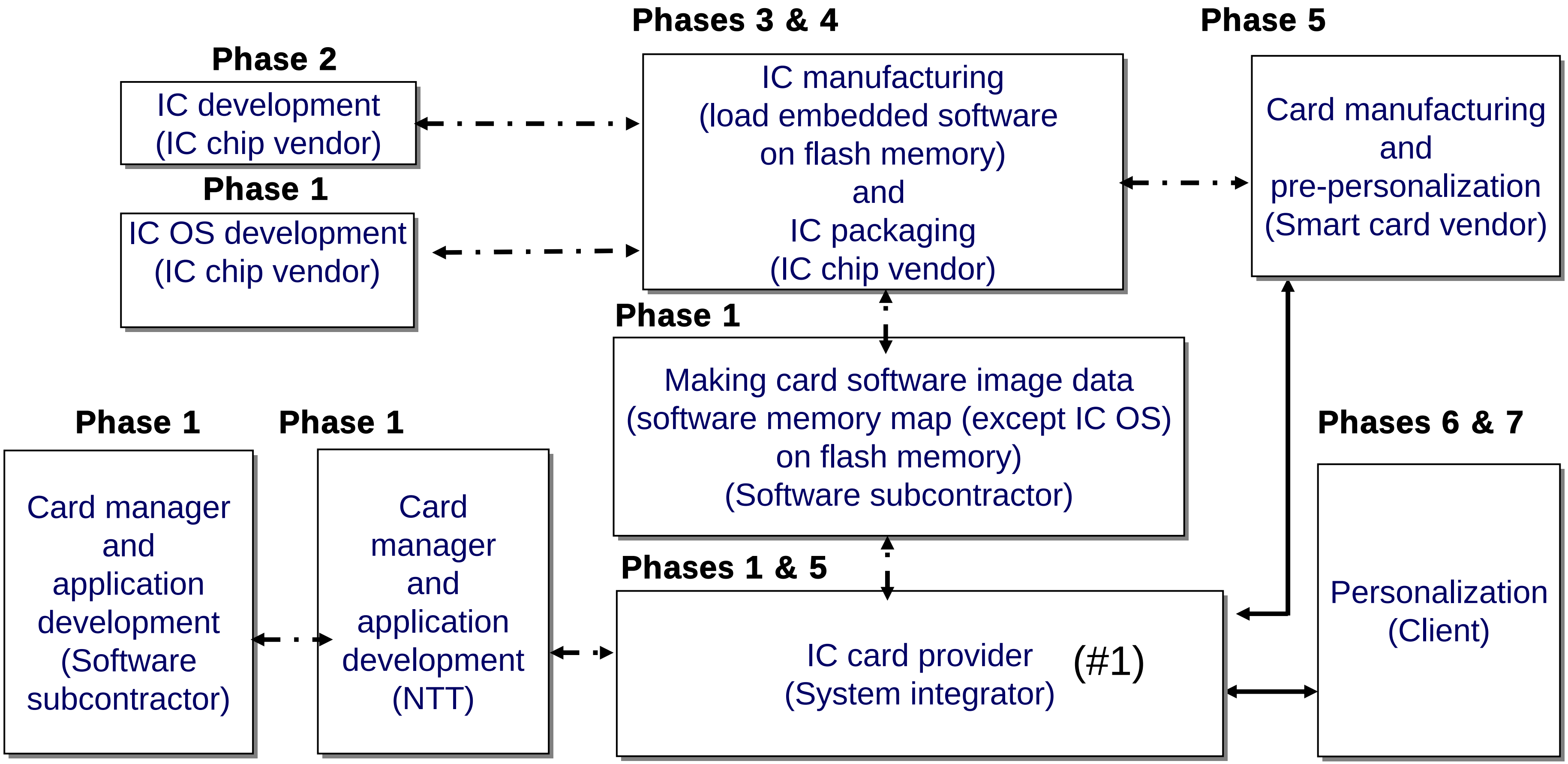
The following parties participated in evaluation activities.



Copyright (C) 2008 NTT Corporation

Scope of smart card product lifecycle (2)

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



Phase 2

IC development (IC chip vendor)

Phase 1

IC OS development (IC chip vendor)

Phases 3 & 4

IC manufacturing (load embedded software on flash memory) and IC packaging (IC chip vendor)

Phase 5

Card manufacturing and pre-personalization (Smart card vendor)

Phase 1

Making card software image data (software memory map (except IC OS) on flash memory) (Software subcontractor)

Phase 1

Card manager and application development (Software subcontractor)

Phase 1

Card manager and application development (NTT)

Phases 1 & 5

IC card provider (System integrator) (#1)

Phases 6 & 7

Personalization (Client)

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

Define roles and responsibilities for all parties (1)

- **Smart Card Software Development (Software subcontractor)**
  - Card manager and application implementation
  - Preparation of deliverables (ST, ADV, ADO, ALC, ACM, AGD, AVA)
  - Site audit

- **Smart Card Software Development (NTT Lab)**
  - CC project management
  - Card manager and application design
  - Preparation of deliverables (ADO, ALC, ACM)
  - Site audit

- **IC OS Development (IC chip vendor)**
  - Preparation of deliverables (ADV, ADO, ALC, ACM, AGD, AVA)
  - Site audit

Define roles and responsibilities for all parties (2)

- **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