JAPAN SECURITY CONFERENCE

USING COMMON CRITERIA FOR SITE EVALUATION

TOKYO, 29-30 March 2001
PLAN OF PRESENTATION

1- REASONS AND GOALS

2- DIFFICULTIES & SOLUTIONS

3- METHODS

4- SECURITY TARGET

5- RESULTS & CONCLUSIONS
1- REASONS & GOALS

1.1- IMPLEMENT “ON-SITE SECURITY”.

- “Physical Environmental” Security.
  -> Access control, Secure storage, ...

  -> Configuration, Firewall, Access control, ...


- Training & Education.
1- REASONS & GOALS

1.2- OFFICIALLY RECOGNIZED SECURITY.

- Compliance to recognized Standards.

  -> Common Criteria (CC).

- Compliance to “Recommendations” used by the Industry.

  -> Protection Profile (PP/9806).

- Conducted under Official Certification Scheme.

- Possibly Certified Activity after Evaluation.
1. REASONS & GOALS

1.3- KNOWLEDGE & EDUCATION ON COMMON CRITERIA.

- Deploy the aim and scope of the CC Standard to employees.

- Training to the security requirements and measures.

- Learning processes during the evaluation phase.
1.4- CHALLENGING THE SECURITY & CONTINUOUS IMPROVEMENT.

- Identification of what need to be secured & of the Threats.

- Implementation of a “Security System”.

- Maintenance Program.
1- REASONS & GOALS

1.5- RECOGNITION OF EMPLOYEES WORK.

- Reporting during evaluation process.

- Audits.

- Certification.

- Recognition from Management.

- Recognition from CUSTOMERS.
2.1- TOE SELECTION & SECURITY TARGET

- TOE is a “physical” feature: “Development Environment”.

- Common Criteria are applicable to Information Technology.

- Environment of the TOE is the Environment of the “Development Environment”.

SOLUTIONS:

- TOE is the “Development Flow”: Production Flow,...

- “Development Flow” is using Information Technology.
2.1- TOE SELECTION & SECURITY TARGET

SOLUTIONS (Ct’ d):

- TOE Environment is the environment in which the “Development Flow” is taking place.
2.2- CC & INFORMATION TECHNOLOGY

- Common Criteria are applicable to Information Technology.

- Security Requirements dependencies.

**SOLUTIONS:**

- Keep focus on the evaluation goals: “Development Environment”.

- Clearly identify the IT of the TOE and its boundaries.

- Limit the list of selected Security Requirements only to those mandatory for the security.
2.3- INFORMATION SYSTEM & NETWORKING

- Usually, the “IS” of “Development Environment” is huge.

- Usually, links to other networks exist.

SOLUTIONS:

- Clearly identify the IT of the TOE and its boundaries.

- Limit the application of CC to this part of the “IS”.

- Move other part of “IS” into the TOE Environment: Can be covered with Security Procedures.
2.4- CC & ASSURANCE MEASURES

- Some Assurance Measures may be difficult to apply to a TOE that is of a “System” type (“Development Environment”). Ex: ACM_CAP.1 Version Numbers.

SOLUTIONS:

- Partnership with Certification Body and with Evaluation Laboratory.

- Use the “concept” and methodology of the CC and not the “basic requests” from the CC wording.
2- DIFFICULTIES & SOLUTIONS

2.5- SUSTAINING A PRODUCT EVALUATION

- Evaluation of a product issued from this “Development Environment” may be needed.

- Product Evaluation have security requirements to the Environment.

**SOLUTIONS:**

- Use existing Protection Profile, that product evaluation may claim for: PP/9806,…

- Validate and introduce the requirements on the Environment into the Security Target of the “Development Environment”. 
3. METHODS

3.1- Implement Working Groups.

3.2- Train Working Groups:
   - To Common Criteria.
   - To Security.

3.3 Write Security Target and Documentation:
   - CC documentation.
   - “Company Documentation”.
3.4 Implement Procedures:
- Policies.
- Specifications.
- Security Measures.

3.5 Evaluate as per CC.
4- SECURITY TARGET

4.1- TOE & TOE ENVIRONMENT DESCRIPTION.

4.2- ASSETS:
   - From the TOE.
   - Used by the TOE.

4.3- ASSUMPTIONS:
   + Assumptions for conformance to “Product PP”.

4.4- THREATS:
   + Threats for conformance to “Product PP”.
4.5- ORGANIZATIONAL SECURITY POLICIES.
  + OSP’s for conformance to “Product PP”.

4.6- SECURITY OBJECTIVES:
  - IT Security Objectives for the TOE.
  - Non-IT Security Objectives for the TOE.
  - Security Objectives for the TOE Environment.
  + Security Objectives for conformance to “Product PP”.

4.7- SECURITY REQUIREMENTS:
  - TOE IT Security Functional Requirements.
4. SECURITY TARGET

4.7- SECURITY REQUIREMENTS (Ct’ d):
   - TOE NON-IT Security Requirements.
   - TOE Environment Security Requirements.

4.8- TOE IT ASSURANCE REQUIREMENTS:
   + Augmentation (if claimed).

4.9- SUMMARY SPECIFICATION:
   - TOE Security Functions.
   - TOE Assurance Measures.
   - Non-IT Security Measures for the TOE.
   - Security Measures for the TOE Environment.
4- SECURITY TARGET

4.10- PP CLAIMS.

4.11- RATIONALE.
5- RESULTS & CONCLUSIONS

5.1- IT IS POSSIBLE TO USE CC FOR SITE OR ENVIRONMENT EVALUATION.

5.2- AT THE CONDITION THAT “IT” IS AVAILABLE INSIDE THE TOE.

5.3- NEED TO CAREFULLY SELECT THE TOE.

5.4- KEEP FOCUS ON THE GOALS OF THE PROCESS » SITE, ENVIRONMENT.

5.5- GOOD PROCESS FOR IMPLEMENTING & CHALLENGING SECURITY.
5- RESULTS & CONCLUSIONS

5.6- IS BETTER IF MAINTENANCE PROGRAM IS FORESEEN.

5.7- LIGHTENING ANY FUTURE EVALUATION ON PRODUCT.
5- RESULTS & CONCLUSIONS

SUCH PROJECT HAS BEEN PERFORMED FOR THE NEC SMARTCARD WAFER MANUFACTURING SITE - YAMAGUCHI JAPAN, IN COLLABORATION WITH FRENCH EVALUATION LABORATORY & FRENCH CERTIFICATION BODY!