Korea IT Security Evaluation and Certification Scheme

2005. 9. 28

Korea Certification Body

Dae Ho, Lee
Agenda

I  KECS Introduction

II  Role and Responsibility of CB

III  Evaluation and Certification Procedure

IV  Product and Protection Profile
Korea IT Security Evaluation and Certification Scheme (KECS)

- Overview
- History
- Organization
- Publication
- Quality System
- Approval policy of EF
**Objective**
- Gain global trust and reliability of IT security system
- Improve international competitiveness of IT product
- Improve IT security level of national communication Network
- Contribute to the realization of a sound information society

**Legal Status**
- Article 15 of the *Framework Act on Information Promotion*
- Article 16 of the Enforcement Decree of the Framework Act on Information Promotion
KECS History

1995
- Aug: Framework Act on IP and its Enforcement Decree

1998
- Feb: Firewall Evaluation

2000
- Jul: IDS evaluation
- Aug: Established Evaluation · Certification Scheme

2002
- Aug: Adopted CC, ISO/IEC 15408 as IT security evaluation criteria
- VPN evaluation

2003
- Nov: Access Control System, Fingerprint Recognition System, Smartcard evaluation

2004
- Sep: Submitted Application to join CCRA

2005
- Jan: CC became the only evaluation criteria
KECS Organization

Certification Body
(National Intelligence Service)
- EWP
- Work Package
- Observation Report
- Evaluation Report
- Certificate
- Certification Report

User
- Certified Products List
- Publish Certification Report

Evaluation Facility
(Korea Info. Security Agency)
- Evaluation and Certification Scheme
- Evaluation Methodology
- Evaluation Management and Oversight
- Consultation on evaluation

Sponsor
- Application for evaluation

Developer
- IT Product
- Protection Profile
- Deliverables
KECS Organization – CB(1/2)

Senior Executive

Certification committee

ITSCC

Director, ITSCC (Certification manager)

Certification Mgmt Team (Quality manager)
- Oversee evaluation
- Site visit
- Operate Certification Committee
- Issue certificates
- Maintenance of Assurance

Support Mgmt Team
- Prepare to Join CCRA
- Operate scheme
- Develop Roadmap for PP development
- Publish CPL
- Audit
- Provide training course

ITSCC : IT Security Certification Center
KECS Organizations – CB(2/2)

**Senior Executive/Certification/Quality Manager**

- Approves scheme
- Approves quality manual
- Approves issuance of certificate

**Certification Manager**

- Supervises operation of certification body
- Approves internal audit
- Operates Certification Committee

**Quality Manager**

- Operates and Maintains the quality system
- Develops plan and executes internal audit
- Operates education and training course
KECS Organizations - EF

IT Security Evaluation Center

Vice president (Quality manager)

Evaluation Planning Team (Quality assistant manager)
- Operate EF quality system
- Develop PP
- Research & support related to evaluation service

Evaluation Team 1 (Technical manager)
- Firewall
- Fingerprint
- Smartcard
- Etc

Evaluation Team 2 (Technical manager)
- IDS
- VPN
- Access control
- Etc
Overview of scheme: Principle of evaluation, Scope, Organizational structure, Legal status, Operating resource, Etc.

Role and Responsibility of the Sponsor/EF/CB

Evaluation and Certification procedure

Maintenance of certified products

ISO/IEC Guide 65

Quality system management
  - Qualification of personnel, Training & education
  - Data/Record management, Protecting and sharing of information
  - Oversee Evaluation, Management of evaluation lab/equipment
  - Appeal or Conciliation, Internal audits, Etc.
Quality Manual

- Management of Deliverables
- Sampling
- Reparation
- Protection of Confidential Information
- Corrective and Preventive Measure
- Handling of Dispute
- Training and Education
- Certification
- Certification Committee
- Written Pledge
- Management of Certification Regulation
- Guaranteeing of Independence
- Internal Audit
- Record Management
- Certification Management
- Management of Assurance
- Document Management
- Operation of Certification lab
- Management Review
- Handling of Dispute Management
- Management of Deliverables
Approval policy of EF

KECS
- Framework Act on Information Promotion
  
  KISA (EF)

CCRA B.3
- Evaluation Facility
  accredited
  approved
  AB
  CB

 or

Evaluation Facility
  established
  Law/statutory instrument
Role and Responsibility of Certification Body

- Qualification Assignment
- Basic/Advanced Training
- Certification Activity
- Certification Committee
- Certification Report and Certificate
Qualification of Evaluator and Certifier

Trainee Certifier (evaluator)
- Basic/Advanced Training

Certifier (evaluator)
- Experience of C/E (more than 2 product)
- Capability of EAL3 C/E

Senior Certifier (evaluator)
- Experience of C/E (more than 3 years)
- Capability of EAL4 C/E

* C/E: Certification and Evaluation
Role and Responsibility of CB

Basic/Advanced Training

Basic (5days)
- ISO/IEC Guide 65
- ISO/IEC 17025
- CC/CEM
- KECS
- CCRA Requirements

Advanced (10days)
- How to write and evaluate
  - PP, ST and deliverables
  - EWP
  - Evaluate deliverables
  - write Evaluation Technical Report
  - Site visit
Role and Responsibility of CB

Certification Activity

**Review and Record**
- Review the following document and record result of certification in the “CB Review Comment”
  - EWP, ST, WP, OR, ETR(PP, TOE)

**Attend**
- The review meeting of EWP and OR
- Evaluation of Testing and Vulnerability
  - Review the plan for testing of EF
  - Independent evaluator testing and vulnerability testing
- Evaluation of the on site security environment
  - Review the plan for on site evaluation
Role and Responsibility of CB Certification Committee

- Composed of 12 professionals from industry, academia, research institutes and the government
- Check for validity and impartiality of the evaluation results
- Review any major changes made to scheme
- Mediate dispute between sponsor, EF and CB
Evaluation · Certification Procedure

- Preparation Phase
- Evaluation Phase
- Certification Phase
**Sponsor**
- Inquiry about Evaluation
- Preparation of Deliverables
- Apply for evaluation(deliverables)

**EF**
- Consultation of Evaluation
- Sign Contract
- Develop EWP
- Evaluate TOE
- Develop ETR

**CB**
- Accept deliverables
- Monitor Evaluation
- Review ETR

---

**Evaluation Phase**

- Kick off Meeting with EF and CB

**Certification Phase**

- Certification Committee
- Produce the Certification Report
- Issue the certificate

---

**Preparation Phase**

- Apply for evaluation(deliverables)
- Sign Contract

---

- Publish the certification report on the website
- Register the certificate to the CPL
- Receive the certificate
Evaluation • Certification Procedure

Preparation Phase

<table>
<thead>
<tr>
<th>Sponsor</th>
<th>EF</th>
<th>CB</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inquiry about Evaluation</td>
<td>Consultation of Evaluation</td>
<td>Accept deliverables</td>
</tr>
<tr>
<td>Preparation of Deliverables</td>
<td>Separate evaluator with consultant for impartiality and independency of evaluation</td>
<td>- Assign a certifier</td>
</tr>
<tr>
<td>Apply for evaluation With deliverables</td>
<td>Sign Contract</td>
<td>- Review deliverables</td>
</tr>
<tr>
<td></td>
<td>- Review deliverables for completeness</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Review Contract</td>
<td></td>
</tr>
</tbody>
</table>

- Review deliverables
## Evaluation Phase (1/2)

<table>
<thead>
<tr>
<th>Sponsor</th>
<th>EF</th>
<th>CB</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Develop EWP</td>
<td>Approve EWP</td>
</tr>
</tbody>
</table>
|  | Consider complexity of security functions, scope of evaluation | Review the EWP  
- Appropriateness of the formation of the evaluation team  
- Appropriateness of the method of calculating the duration of the evaluation  
- Appropriateness of the claimed PP and TOE scope |
|  | Kick off Meeting With Sponsor and CB |  |
Evaluation Phase (2/2)

**Sponsor**

- Development ETR

**EF**

- Evaluation TOE
  - Compliance with CC, CEM
  - Produce OR, WP for each work unit
  - Site visit

- Develop ETR

**CB**

- Review ETR
  - Impartiality of evaluation
  - Conformance of CC/CEM
  - Compliance with scheme

- Monitor Evaluation
  - Review OR, WP
  - Testing and vulnerability
  - Site visit
  - Compliance with scheme
### Evaluation - Certification Procedure

#### Certification Phase

<table>
<thead>
<tr>
<th>Sponsor</th>
<th>EF</th>
<th>CB</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Certification Committee</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Review all documents of evaluation and certification (EWP, OR, WP, ETR, etc)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Produce the Certification Report</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Issue the certificate</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Receive the certificate</td>
</tr>
</tbody>
</table>

- Receive the certificate
- Publish the Certification Report on the website
- Register the certificate to the CPL
Certification Maintenance

Sponsor

CB

Approve Change?

Yes

Sponsor

Yes

Application for change approval (deliverables)

No

Sponsor

EF

· Consult
· Contract
· Evaluation

No

Notify result

Yes

Sponsor

EF

deliverables

Test and analysis result

Re-evaluation
Product and Protection Profile

- Certified product
- Protection Profile
## Product and Protection Profile

### Certified Product

<As of July 18, 2005>

<table>
<thead>
<tr>
<th>Category</th>
<th>'98</th>
<th>'99</th>
<th>'00</th>
<th>'01</th>
<th>'02</th>
<th>'03</th>
<th>'04</th>
<th>'05</th>
<th>sum</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domestic Criteria</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FW</td>
<td>1</td>
<td>2</td>
<td>5</td>
<td>7</td>
<td>10</td>
<td>8</td>
<td>7</td>
<td>-</td>
<td>40</td>
</tr>
<tr>
<td>IDS</td>
<td>3</td>
<td>11</td>
<td>9</td>
<td>2</td>
<td>1</td>
<td>26</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Common Criteria</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FW</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>FW, VPN</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>3</td>
<td>10</td>
<td>1</td>
<td>14</td>
</tr>
<tr>
<td>IDS</td>
<td>1</td>
<td>4</td>
<td>5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Access Control System</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>8</td>
<td>8</td>
</tr>
<tr>
<td>Total</td>
<td>1</td>
<td>2</td>
<td>5</td>
<td>10</td>
<td>21</td>
<td>20</td>
<td>20</td>
<td>16</td>
<td><strong>95</strong></td>
</tr>
</tbody>
</table>

### Industry Standards

- Common Criteria: **95**
- Domestic Criteria: 40
- Total: 95

---

**Certification Badges:**
- Firewall
- IDS
- VPN
- Biometric
- Access Control
- Smart Card
- IPS
## Protection Profile

<table>
<thead>
<tr>
<th>Publication</th>
<th>Title</th>
<th>EAL</th>
</tr>
</thead>
<tbody>
<tr>
<td>2003. 4</td>
<td>Firewall protection profile V1.1</td>
<td>EAL3+</td>
</tr>
<tr>
<td>2003. 4</td>
<td>VPN protection profile V1.1</td>
<td>EAL3+</td>
</tr>
<tr>
<td>2003. 4</td>
<td>Intrusion detection system protection profile V1.1</td>
<td>EAL3+</td>
</tr>
<tr>
<td>2003. 4</td>
<td>VPN gateway protection profile V1.1</td>
<td>EAL3+</td>
</tr>
<tr>
<td>2004. 2</td>
<td>Firewall-VPN composite protection profile V1.0</td>
<td>EAL2</td>
</tr>
<tr>
<td>2004. 2</td>
<td>Label-based access control system protection profile V1.0</td>
<td>EAL3+</td>
</tr>
<tr>
<td>2004. 2</td>
<td>Fingerprint recognition system protection profile V1.0</td>
<td>EAL2+</td>
</tr>
<tr>
<td>2004. 12</td>
<td>Smartcard open platform protection profile V1.0</td>
<td>EAL4+</td>
</tr>
<tr>
<td>2005. 5</td>
<td>Network Intrusion Prevention System Protection Profile V1.0</td>
<td>EAL4</td>
</tr>
</tbody>
</table>
ITSCC of NIS (Certification Body)
- Homepage: http://www.kecs.go.kr
- E-mail: kecs@ncsc.go.kr

KISA (Evaluation Body)
- Homepage: http://www.kisa.or.kr
- E-mail: kecs@kisa.or.kr