KECS-CR-06-17

RedCastle v2.0 for RedHat
Certification Report

Certification No. : KECS-CISS-57-2006

2006. 12.

National Intelligence Service

IT Security Certification Center

Document History

Version	Date	Page	Summary
00	2006.12.22	-	Initial Version

The document is the certification report on

RedCastle v2.0 for RedHat

Certification Body

National Intelligence Service

Evaluation Body

Korea Information Security Agency

Table of Contents

1. Overview

This report documents the evaluation agency's assessment of the EAL3+ evaluation of the RedCastle v2.0 for RedHat ('RedCastle' hereinafter) with regard to the Common Criteria for Information Technology Security Evaluation(Notification No. 2005-25 of the Ministry of Information and Communication; 'CC' hereinafter). It presents the evaluation results, their justifications, and the conformance results.

The evaluation was performed by the Korea Information Security Agency(KISA), and was completed on December 7, 2006. This report is largely driven from the Evaluation Technical Report (ETR) written by the KISA. The evaluation determined that the product satisfies the CC part 2 and the EAL3 assurance requirements of the CC part 3 which is augmented by ADV_IMP.2, ADV_LLD, ALC_TAT.1, ATE_DPT.2, and AVA_VLA.2. Thus, it resulted in a 'pass' statement on the basis of the paragraph 175 of the CC part 1. In addition, the TOE was shown to satisfy the requirements of the Label-based Access Control System Protection Profile for Government (LACSPP) V1.1 (May 17, 2006).

RedCastle is installed in a specific system shall be protected, and it is the label-based access control system, which provides the security function of mandatory access control, discretionary access control, etc. RedCastle provides the security functions such as the mandatory access control, the discretionary access control, the identification and authentication, and the security audit, and other functions to protect the system. The evaluation covers the following security functions provided by the TOE :

- Reference Monitor Function
  - Reference monitor function is provided to ensure that the TSP enforcement functions are invoked and succeed before each function within the TSC(TSF Scope of Control) is allowed to proceed.
- Security Audit Function
- User Data Protection Function
- Security Management Function
- Identification and Authentication Function
- TSF Protection Function

- Mandatory Access Control
- Discretionary Access Control

The certification team monitored the activities of the evaluation team and reviewed test plans, provided guidance on technical issues and evaluation processes, reviewed intermediate evaluation results and reviewed successive versions of the evaluation technical report.

The certification team determined that the evaluation results showed that the product satisfies all of the functional requirements and assurance requirements defined in the Security Target.

Therefore, the certification team concludes that the evaluator's findings are accurate, and the conclusion is justified.

Certification Validity : This report not the usage endorsement or the qualification guaranteed by any agency of the Korea Government.

2. Identification

The [Table 1] describes the information about the TOE identification.

[Table 1] TOE identification

Evaluation Scheme	Information Security System Evaluation & Certification Guidance (2005. 5. 21) Information Security System Evaluation & Certification Regulations (2005. 12. 26)
TOE	RedCastle v2.0 for RedHat
Protection Profile	Label-based Access Control System Protection Profile for Government V1.1 (2006. 5. 17)
Security Target	RedCastle v2.0 for RedHat Security Target V1.7 (2006. 9. 26)
Evaluation Technical Report	RedCastle v2.0 for RedHat Evaluation Technical Report V1.00
Conformance Result	Common Criteria v2.3, part 2 conformant Part 3 conformant, EAL3 augmented by ADV_IMP.2, ADV_LLD, ALC_TAT.1, ATE_DPT.2, and AVA_VLA.2
Evaluation Criteria	Common Criteria for Information Technology Security Evaluation (2005. 5. 21) Final Interpretation (2005. 4. 4)
Evaluation Methodology	Common Evaluation Methodology for Information Technology Security V2.3 Final Interpretation (2005. 4. 4)
Sponsor	RedGate Co., Ltd.
Developer	RedGate Co., Ltd.
Evaluation Team	KISA IT Security Evaluation Division Evaluation Team II Kim Min-Kyoung, Choi Yong-Joon
Certification Body	National Intelligence Service

The [Table 2] describes the operating environment about the TOE.

[Table 2] Operating Environment for RedCastle

Items		Secification
RedCastle SecureOS (RedHat)	CPU	AMD Opteron(tm) Processor 244 (dual)
	RAM	2G
	HDD	73 GB Ultra 320 SCSI
	Operating System	RedHat Enterprise Linux ES release 4 (Nahnt Update 4) Kernel 2.6.9-42.ELsmp on an x86_64
RedCastle ESM	CPU	Pentium 4 1.8GHz
	Memory	512M
	HDD	60Gbyte
	Operating system	Windows 2000 Professional

3. Security Policy

The TOE is operated according to the following security policy.

Identification and Authentication The administrator must be identified and authenticated before using the security function of the TOE.

Security Management It is only possible for the administrator with authorized secure connection to use the security management function.

4. Assumptions and Scope

4.1 Assumptions

The TOE must be installed and operated according to the following assumptions.

A. LOCATE It is assumed that the processing resources of the TOE will be located within controlled access facilities and will be protected from unauthorized physical modification.

A. ADMINS It is assumed that there are one or more competent individuals who are assigned to manage the TOE and the security of the information it contains. Such personnel are assumed not to be careless, willfully negligent or hostile.

A. PATCH It is assumed that the operating system, where TOE is installed, is secured and reliable. Before installing the TOE, the operating system will be patched the vulnerabilities and removed the useless services.

A. SSL The SSL (Secure Socket Layer) protocol, which is used for the secure communication between RedCastle Agent and Manager, is secured.

A. TIME It is reliable for the timestamp of Operating System to be used by the TSF of this TOE.

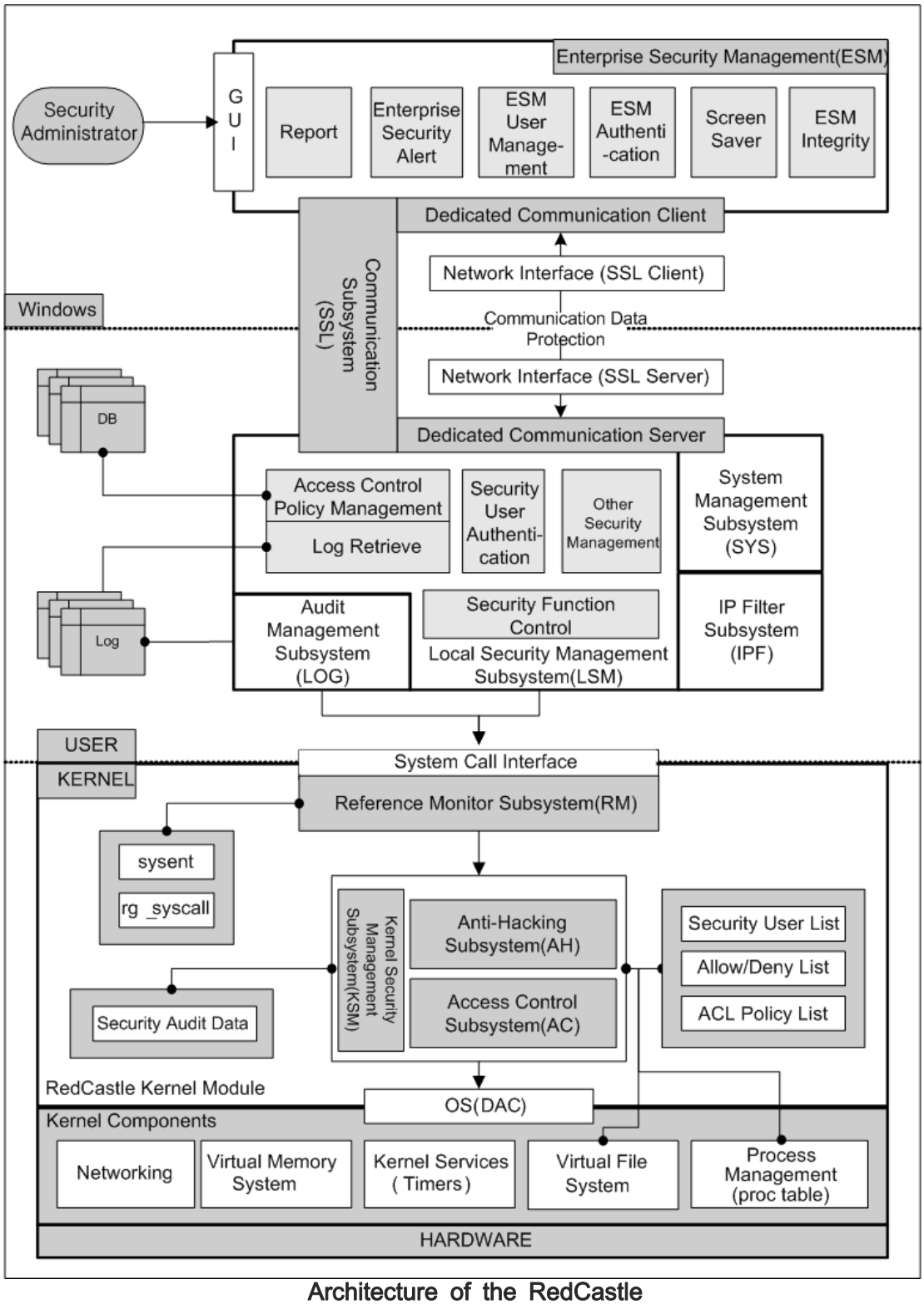
4.2 Threats countered by TOE

The TOE provides a countermeasure against the security threats, such as attempts to infringe the asset of main server. The TOE does not provide a countermeasure against direct physical attacks that makes the SFP ineffective or bypasses. But The TOE provides a countermeasure against logical attacks from threat sources of low-level expertise, resources, and motivation.

All security objectives and security policies are described to provide a countermeasure against the identified security threats.

5. TOE Information

The TOE provides the function including label-based access control. And the simplified architecture of the TOE is as follows.



Architecture of the RedCastle

RedCastle is divided into 10 subsystems laying stress on security function, and primary function of each subsystem is as follows.

Enterprise Security Management Subsystem (ESM)

The enterprise security management subsystem (ESM) provides GUI to manage the RedCastle ESM such as identification and authentication function (SEED encryption algorithm) about security administrator who uses RedCastle ESM, ESM screen saver functions that provide administrator session locking function, ESM integrity management function that uses SHA-1 Hash algorithm, report function, integrated security alert function, etc. and security function of the RedCastle SecureOS. Also, the enterprise security management subsystem (ESM) offers function that security administrator can manage many integrated RedCastle SecureOS.

The enterprise security management subsystem (ESM) provides the function that transmits the security administrator's commands to the communication subsystem (SSL) of secure communication session, and process commands transmitted the security management subsystem (LSM) again, and transmits processing result to the enterprise security management subsystem (ESM) through the communication subsystem (SSL) again.

Communication Subsystem (SSL)

The communication subsystem (SSL) provides the function that ensure a secure communication session through a network interface between the security management subsystem (LSM) in the RedCastle SecureOS and in the enterprise management subsystem (ESM), the RedCastle ESM. It offers safe communication function because SSL client is installed in RedCastle ESM, and SSL server is installed in RedCastle SecureOS.

Communication subsystem (SSL) uses SSL v3 protocol, and by key exchange method Diffie-Hellman, encryption algorithm is AES (bit), and Hash algorithm is SHA-1(160 bit) use.

Security Management Subsystem (LSM)

The security management subsystem (LSM) is a part that processes receiving security management command of the enterprise security management subsystem (ESM), and the processed results will be transmitted to the integrated management subsystem (ESM) through the communication subsystem (SSL). Also, the interoperable functions with the access control subsystem (AC) such as the security function initiating and terminating processing function, and access control policy related data management function of the security

management subsystem (LSM)'s function transmit commands to the kernel management subsystem (KSM) through the reference monitor subsystem (RM).

The security management subsystem (LSM) enables the authorized security administrator to operate RedCastle SecureOS through the GUI of the enterprise security management subsystem (ESM) and the commands interface of system console by providing the following functions.

- RedCastle ESM Connection Control Function, Identification and Authentication Function, Authentication Function for Authority Acquisition, Security Function Beginning and Discontinuance Processing Function, Management Function of Security Group/Security User/File Security Attribute/ACL Policy/Commend Allowed·Denied/Security Password, Retrieve Function of Process Security Attribute/Security Log/System Log, Configuration Function of Security Function Environment/Audit Environment, RedCastle SecureOS Integrity Checking Function that use SHA-1 Hash Algorithm, Commend Interface Function.

Audit Management Subsystem (LOG)

The audit management subsystem (LOG) provides collecting and storing function for security log (kernel log, IP Filter log, system log) that generated in RedCastle SecureOS, audit storage traces management function, and potential violation analysis and response function. Also, the audit management subsystem (LOG) transmits generated security log by real-time to the enterprise security management subsystem (ESM) through the security management subsystem (LSM) or conduct this job upon a request of security administrator.

Reference Monitor Subsystem (RM)

The reference monitor subsystem (RM) provides function that adds control system call on operating system's system call to control the access control subsystem (AC) when RedCastle's kernel module load, and erases control system call when RedCastle's kernel module is separated.

If the system call occurs so that it performs security policy and security function environment configuration in the security management subsystem (LSM), and condition retrieve of the access control subsystem(AC), operating environment configuration, retrieve and configuration of DB about access control policy, etc., the reference monitor subsystem (RM) provides function that transfers control to kernel management subsystem (KSM) after intercept existing system call in list after compare with control system call list. Also, when access control security function begins, operating system's system call is replaced by TSF's system call and when access control security function is discontinued, it return operating system's system call table and intercept

operating system's system call in TOE control scope calling in discretionary application, and it provides function that transfers control to the access control subsystem (AC).

The reference monitor subsystem (RM) provides security module hiding function to prevent that RedCastle SecureOS kernel module is separated from operating system without permission by unauthorized user.

Kernel Management Subsystem (KSM)

The kernel management subsystem (KSM) delivers command to kernel management subsystem (KSM) through control system call if security management subsystem (LSM) that is located in kernel of operating system and is located in application does beginning and discontinuance command of security function. Kernel management subsystem (KSM) does a role which executing beginning and discontinuance actually of security function.

Functions that kernel management subsystem (KSM) offers are as follows.

- Access Control Security Function initiating and terminating, Security Function Environment Configuration Management, Security Group Data Management, Security User Data Management, Object Security Attribute Data Management, Subject Security Attribute Retrieve and Configure, ACL Policy Data Management, Allowed/Denied List Data Management, Kernel Log Save and Retrieve.

Access Control Subsystem (AC)

If a system call intercept in reference monitor subsystem (RM) occurred, system call request is delivered to access control subsystem (AC). It performs subject security attributes setting (identifying the subject and assigning attribute when a process is created), label-based mandatory access control, object security attribute inheritance and recovery, ACL (Access Control List) based discretionary access control, and allowed/denied list based access control upon the delivered system call requests to the Subsystem (AC).

Anti-Hacking Subsystem (AH)

If a system call occurred which is suspected as hacking attempt, the anti-hacking subsystem (AH) intercepts this in the reference monitor subsystem (RM). And it performs tmp directory misuse prevention (Symbolic Link vulnerability prevention, FIFO iniquity access prevention), hard link misuse prevention, CHROOT vulnerability prevention, network mode misuse prevention

functions according to the system call request delivered to the anti-hacking subsystem (AH).

System Management Subsystem (SYS)

The System management subsystem (SYS) provides system account management function, system information retrieve function, system performance retrieve function, process start-up monitoring function, process performance monitoring function, and disk usage monitoring function through GUI of the enterprise security management (ESM).

IP Filtering Subsystem (IPF)

The IP filtering subsystem (IPF) provides IP filter's policy file storing and querying function through the GUI of the integrated management subsystem (ESM) to enable server's intrusion detection function by using the IP filter product that is supported separately from TOE. It is separated physically from the above 5 subsystems. A VPN client subsystem is installed to outside network for VPN communication with the core engine subsystem installed site. The VPN client subsystem (VPNC) has its own windows management console.

6. Guidance Documents

The TOE provides the following guidances:

- RedCastle v2.0 Administrator Guidance Version 1.13, Oct. 12. 2006
- RedCastle v2.0 User Guidance Version 1.6 Feb. 25. 2006

7. TOE Testing

7.1 Developer testing

- **Test Method**

The developer produced the test item by considering the security function of the TOE. Each test item is described in test documentation. Each test item described in the test documentation includes the following items in detail:

- Test No./Tester : The identifier of the test and the developer who participated in testing
- Test purpose : Description of the purpose of the test including security function of test subject and security module
- Test configuration : Detailed test configuration to carry out the testing
- Detailed test procedure : Detailed procedure to test security functions
- Expected result : The expected test result when implementing test procedure
- Actual result : The test result when implementing actual test procedure
- Comparison of the expected result and the actual result :

The result of comparison of the expected result and the actual result

The evaluator assessed the suitability of the testing such as the test configuration, test procedure, analysis of test scope and the test of low-level design. The developer assured that the developer's test and test results were adequate for the evaluation configuration.

- **Test configuration**

The test configuration described in the test document includes the detailed configuration such as the network configuration, the TOE, PC, and server. In addition, it describes detailed test configuration such as the application server (web server, mail server, etc.) and evaluation tools required for the test.

- **Test scope analysis/Low-level design test**

The detailed evaluation results are described in the evaluation result in ATE_COV and ATE_DPT.

- **Test Result**

The test document describes the expected result and the actual result of each test. The actual result is confirmed through not only responses including APDU of the TOE but also the audit record.

7.2 Evaluator testing

The evaluator configured the TOE by using the evaluation configuration and evaluation tools identical to the developer test, and examined the overall tests provided by the developer. The evaluator assured that the actual test result is consistent with the expected result in all test items.

In addition, the evaluator devised evaluator tests additionally on the basis of developer test, and confirmed that the actual test result is consistent with the expected test result.

The evaluator carried out the vulnerability test, and there was no vulnerability for malicious use in the evaluation configuration.

The evaluator's test result assured that the TOE works normally as described in the design documentation.

8. Evaluated Configuration

The network was configured as inside and outside separately for evaluation. The following hardwares were used to configure the evaluation environment:

- PC : 3 ea. (for inside & outside PC 3 ea.)
- CPU : AMD 64
- Memory : 2 Gbyte

The following software products were used to configure the evaluation environment:

- RedHat Enterprise Linux ES release 4
- Windows 2000 Professional

All security functions provided by the TOE are included in the scope of the evaluation, and we configure the evaluation environments according to the specified security attribute and environment setting method of each security function.

9. Evaluation Results

The evaluation applied the Common Criteria and the Common Methodology for Information Technology Security Evaluation V2.3, and Final Interpretation(2005. 7. 4). It concludes that the TOE satisfies the CC V2.3 part 2 and EAL3+ of the CC V2.3 part 3. The detailed information regarding the evaluation is described in the ETR.

- **Security Target Evaluation (ASE)**

The evaluator applied the ASE work unit of the Common Methodology for Information Technology Security Evaluation(CEM).

The executive summary of the Security Target Specification is complete, consistent with other parts of the Security Target Specification and accurately describes the Security Target Specification. TOE description explains TOE objective and its functions for easy understanding, is logical, complete, internally consistent and consistent with other parts of the Security Target Specification.

Security environment presents security issues that are derived from TOE and its security environment is clear and consistent manner in terms of assumptions, threats and organizational security policy. The description is complete and consistent. Security goals satisfy identified threats, perform identified organizational security policy and satisfy stated assumptions.

IT security requirements are described in complete and consistent manner, and provide suitable basis for TOE development to achieve security goals. TOE Summary defines security functions and assurance measures in accurate and consistent manner, and satisfy stated TOE security requirements. Security Target Specification accurately substantiates protection profiles to accommodate.

Accordingly, Security Target Specification is complete and consistent manner, and provide suitable basis for TOE development to achieve security goals. In result, it is suitable to be used as the basic data to perform TOE evaluation.

- **Configuration Management (ACM)**

The evaluator applied the ACM work unit of the Common Methodology for Information Technology Security Evaluation(CEM) for evaluation. The evaluator verified through the configuration management document that the developer uses automated tools to control changes of deployed expressions. Through the configuration

management document, it was verified that the developer clearly identifies TOE and its related configuration items and those changes of such items are appropriately controlled. It was also verified that the developer performs configuration management on the minimum TOE descriptions, evaluation proofs required by the ST warranty component and security defects.

Accordingly, the configuration management document does that a customer identifies the TOE which is evaluated, ensure that configuration items are uniquely identified, and that the procedure which the developer uses to control and track change of the TOE is appropriate.

- Delivery and Operation (ADO)

The evaluator applied the ADO work unit of the Common Methodology for Information Technology Security Evaluation(CEM) for evaluation. Distributed documents describe all procedures for maintaining TOE security and detecting any changes and replacements of TOE when TOE is distributed to users. Procedures and steps for safe installation and initiation of TOE have been documented properly. Thus, it has been confirmed that TOE is safely configured.

Accordingly, distribution and operating documents are suitable to ensure that the TOE is installed, created and initiated in the way intended by the developer and that the TOE is distributed without being modified.

- Development (ADV)

The evaluator applied the ADV work unit of the Common Methodology for Information Technology Security Evaluation(CEM) for evaluation. The functional specification describes TOE security functions appropriately and explains that they are sufficient to satisfy the security functional requirements of the Security Target Specification. It also describes TOE external interfaces appropriately. The security policy model is clear and consistent in describing the security policy rules and characteristics corresponding to the security functions specified in the functional specification.

The high-level design describes TSF as a major component subsystem, appropriately describes subsystem interfaces and accurately implements functional specifications. The low-level design describes the internal operations of TOE security functions as the interactions between modules and their interdependencies. The low-level design is sufficient to satisfy the security

functional requirements and reflects the high-level design accurately and effectively.

The implementation description is sufficient to satisfy the security functional requirements of the Security Target Specification and accurately implements the low-level design. The consistency in expression shows that the requirements of the Security Target Specification have been accurately and completely implemented in terms of functional specification, high-level design, low-level design and implementation.

Accordingly, documents including the functional specification, which describes the development requirements and TOE external interfaces; the high-level design, which describes the TOE architecture in terms of interior subsystems; the low-level design, which describes the TOE architecture in terms of internal modules; the implementation document, which describes the source code level implementation; and the consistency in expression document, which ensures consistency of TOE expressions; all facilitate quite effectively understanding of the ways of how the TOE security functions are provided.

- Guidance Documents (AGD)

The evaluator applied the AGD work unit of the Common Methodology for Information Technology Security Evaluation(CEM) for evaluation. The administrator guidance documentation is describing method of taking care of the TOE in a way which is safe. Accordingly, guidance documentation is properly describing method used for operating the TOE.

- Life Cycle Support (ALC)

The evaluator applied the ALC work unit of the Common Methodology for Information Technology Security Evaluation(CEM) for evaluation. It was verified that the security control on development environment suitably provides confidentiality and fault-free requirement of the TOE design and implementation. The evaluator verified that the developer used a documented TOE life cycle model. The evaluator also confirmed that the developer used a well defined development tool for producing consistent and predictable results.

Accordingly, the ALC section describes appropriately the procedures used by the developer during TOE development and maintenance periods including security procedures and tools used during the entire TOE development process.

- Test (ATE)

The evaluator applied the ATE work unit of the Common Methodology for Information Technology Security Evaluation(CEM) for evaluation. The test was enough to establish that the TOE security function was tested systematically about function specification. The Developer confirmed that performed TOE security function test about high-level design. The developer's functional test was enough to prove as security function is specified. The evaluator performs independent test of TSF by selecting some part of it and confirmed operation as TOE is specified, and the evaluator got trust about the test that developer conducted.

Accordingly, the evaluator confirmed that the TOE security function operates according to the TOE's security functional requirements that is specified in design documentation and ST by testing some of TOE's security functions independently.

- Vulnerability Assessment (AVA)

The evaluator applied the AVA work unit of the Common Methodology for Information Technology Security Evaluation(CEM) for evaluation. The misuse analysis verified that the Users' Manual is not misunderstood, irrational or conflicting; that all safety procedures of operating modes are well prepared; and that the Users' Manual can be used effectively to prevent and detect abnormalities of TOE. The functional strength declaration mentioned all probabilistic and permutation mechanisms in the Security Target Specification and the analysis of the developer's functional strength declaration was verified its accuracy.

Vulnerability Analysis document describes clearly known vulnerabilities of TOE and their countermeasures in terms of their functional implementation and specification of operating environment in guidelines or Users' Manual. The evaluator conducted an independent vulnerability test and confirmed that TOE does not have any vulnerabilities that can be misused by intruders of low level attack capability within the intended environment.

Accordingly, the evaluator confirms that TOE does not have any defect or weakness that can be misused within the intended environment based on the vulnerability analysis and the evaluator's infiltration testing.

10. Recommendations

- The label-based mandatory access control system must be in operation condition after TOE is installed. However, if a company can not apply the mandatory access control policy to a job such as maintenance due to its special policy, this job can be done in 'Warning' mode which only generates audit records and should be converted into the actual access control policy applying mode after completion of that specific job.
- The user who wants to connect to this certified product, must conduct identification and authentication process by execution of 'rclogin' command to have access authority to the object which has security attributes. However, a connected user through FTP can not execute the 'rclogin' command and the access to the object which has security attributes is impossible. And this should be notified to the users.
- The IP filter function provided into operating system was set to 'Deny' in default for all ports except the port needed for product operation (for communication between RedCastle ESM and RedCastle SecureOS : 5002 [TCP]) only. For this reason, the administrator must set the port to allow properly according to the organization's policy.

11. Abbreviations and Terminologies

The following abbreviations were used in the report.

CR	Certification Report
EAL	Evaluation Assurance Level
IT	Information Technology
KECS	Korea IT security Evaluation and Certification Scheme
TOE	Target of Evaluation

The following terminologies were used in the report.

TOE	An IT product or system and its associated guidance documentation that is the subject of an evaluation.
Audit record	Audit data that is kept to record TOE security related events.
User	Any entity(human user or external IT entity) outside the TOE that interacts with the TOE.
Authorized administrator	An authorized user who may, in accordance with the TSP, manage safely the TOE.
Authorized user	A user who may, in accordance with the TSP, perform an operation.
Identity	A representation(e.g. a string) uniquely identifying an authorized user.
Authentication data	Information used to verify the claimed identity of a user.
External IT entity	Any IT product or system, untrusted or trusted, outside of the TOE that interacts with the TOE.
Assets	Information or resources to be protected by the countermeasures of a TOE.
Daemon	A program which is continuously executed to manage periodic service request.

12. References

The certification body has used the following documents to produce the certification report:

[1] Common Criteria for Information Technology Security Evaluation (2005. 5. 21)

[2] Common Evaluation Methodology for Information Technology Security V2.3

[3] Label-based Access Control System Protection Profile for Government V1.1 (2006. 5. 17)

[4] Information Security System Evaluation & Certification Guidance (2005. 5. 21)

[5] Information Security System Evaluation & Certification Regulations (2005. 12. 26)

[6] RedCastle v2.0 for RedHat Security Target V1.7 (2006. 9. 26)

[7] RedCastle v2.0 for RedHat Evaluation Report, V1.00 (2006. 12. 7)