KECS-CR-07-23

Certification Report
RedCastle v2.0 for Windows

Certification Number : KECS-CISS-0082-2007

Dec. 2007

National Intelligence Service

IT Security Certification Center

The document is the certification report on

RedCastle v2.0 for Windows

Certification Body

National Intelligence Service

Evaluation Body

Korea Information Security Agency

Table of Contents

1. Overview

This report is for the certification body to describe the certification result, which inspects the results of the EAL3+ evaluation of RedCastle v2.0 for Windows with regard to the Common Criteria for Information Technology Security Evaluation (Announcement on May 21, 2005)('CC' hereinafter). The report describes evaluation results, and its appropriateness and adequacy.

The Korea Information Security Agency(KISA) has evaluated RedCastle, and finished the evaluation on November 30, 2007. This report is written based on the Evaluation Technical Report produced and provided by the KISA. The evaluation concludes that the TOE satisfies the CC part 2 and EAL3+ of the CC part 3 assurance requirements. Thus, it is assigned the verdict 'suitability' on the basis of the paragraph 191 of the CC part 1.

The TOE consists of RedCastle SecureOS which is security function processing part and RedCastle ESM (Enterprise Security Management) which is security management part.

RedCastle SecureOS will be installed on each operating system and this can be divided into kernel part - commits MAC and DAC and application part which commits other security functions. The management part of TOE, RedCastle ESM will be operated on Windows 2000 Professional (Service Pack 4).

The TOE provides security functions which is included in the scope of the evaluation as follows :

. Reference Monitor

. Mandatory Access Control (MAC)

. Discretionary Access Control (DAC)

. Identification and Authentication

. Security Audit

. Security Administration

. TSF Protection

The certification body verified the evaluation activities and test procedures of the evaluator, presented technical issues and the guidelines for evaluation procedure, and reviewed contents of each evaluation unit and the evaluation report.

The certification body affirms that the evaluation results confirmed that the subject product satisfies all security functional requirements and guarantees

requirements described in the Security Target Specification.

Therefore, the certification body certifies that the observations of the evaluator and the evaluation results are accurate and appropriate, and also the product assessment is accurate.

Certification Validity : The information contained in the certification report means neither the use of RedCastle v2.0 for Windows is approved nor its qualification is assured by any Government Agency of the Republic of Korea.

2. Identification

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

[Table 1] TOE identification

Evaluation Guidance	Information Protection System Evaluation & Certification Guidance (2007.8.22) Information Protection System Evaluation & Certification Regulations (2007.4.15)
TOE	RedCastle v2.0 for Windows
Protection Profile	Label-based Access Control System Protection Profile for Government V1.1 (2006. 5. 17)
Security Target	RedCastle v2.0 for Windows V1.6(2007. 6. 14)
Evaluation Technical Report	RedCastle v2.0 for Windows Evaluation Technical Report V1.0
Evaluation Result	Suitability in the Common Criteria part 2 Suitability in the EAL3 of the Common Criteria part 3 assurance requirements
Evaluation Criteria	Common Criteria for Information Technology Security Evaluation (2005. 5. 21), Final Interpretation (2005. 4. 4)
Evaluation Methodology	Common Methodology for Information Technology Security Evaluation V2.3 (2005. 8)
Sponsor	Kim Ki-Hyun, CEO of REDGATE Co., Ltd.
Developer	REDGATE Co., Ltd.
Evaluation Team	KISA IT Security Evaluation Division Evaluation Team Cho Kyu-Min, Kim Min-Kyung, Part Jeong-Hwan
Certification Body	National Intelligence Service

The TOE is divided into SecureOS and ESM system physically. The SecureOS system will be operated by installing on Windows 2003 Server. The ESM system provides user with GUI(Graphic User Interface) for more convenient usage and it will be operated on Windows 2000 professional operating system.

The following [Table 2] describes the operating environment of the TOE.

[Table 2] Software / Hardware Platform

Classification	Hardware Specifications / Operating System	
RedCastle SecureOS (Windows)	CPU	Pentium III 600 MHz and higher
	RAM	256MB and higher
	HDD	200MB and higher
	Interface	10/100Base T
	OS	Windows 2003 Server
RedCastle ESM	CPU	Pentium III 600 MHz and higher
	RAM	128 MB and higher
	HDD	10 MB and higher
	Interface	10/100BaseT
	OS	Windows 2000 Professional SP4

3. Security Policy

The TOE is operated according to the following security policy.

P. Security Audit

To trace accountability for all practices related to security, security relevant events should be recorded and maintained with through review.

P. Mandatory Access Control

The TOE must control all access trials to the object according to the security level of the subject.

P. Security Level Allocation

The TOE must be able to assign adequate security level to the subject and object or cancel it according to the organization's access control policy and regulations.

P. Identification and Authentication

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

P. Secure Management

The authorized administrator should manage the TOE with secured methods.

P. Encryption

The encryption algorithm and module for the TOE should be authorized by the chief of National Intelligence Service.

P. Discretionary Access Control

The TOE must be able to control access trials to the information according to the identity of user or group the user belongs.

4. Assumptions and Scope

4.1 Assumptions

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

A. Physical Security

The TOE shall be located in a physically safe environment where only authorized personnel can access, and is protected from the physical change which is not authorized.

A. Trusted Admin

TOE's authorized admin shall have no malice, be trained on TOE admin functions, and perform his/her duties in accordance with the admin guideline.

A. OS Augmentation

OS services and tools that are not needed by TOE shall be removed and OS weaknesses shall be augmented to ensure reliability and safety of OS.

The following are additional assumptions described in the Security Target document.

A. SSL Protocol

A SSL version 3 protocol implemented by using openssl (openssl-0.9.8e) for the secure communication between RedCastle SecureOS and RedCastle ESM is secure.

A. TIME

The reliable time stamp that TSF uses is provided by the commercial operating system.

4.2 Threats Response Scope

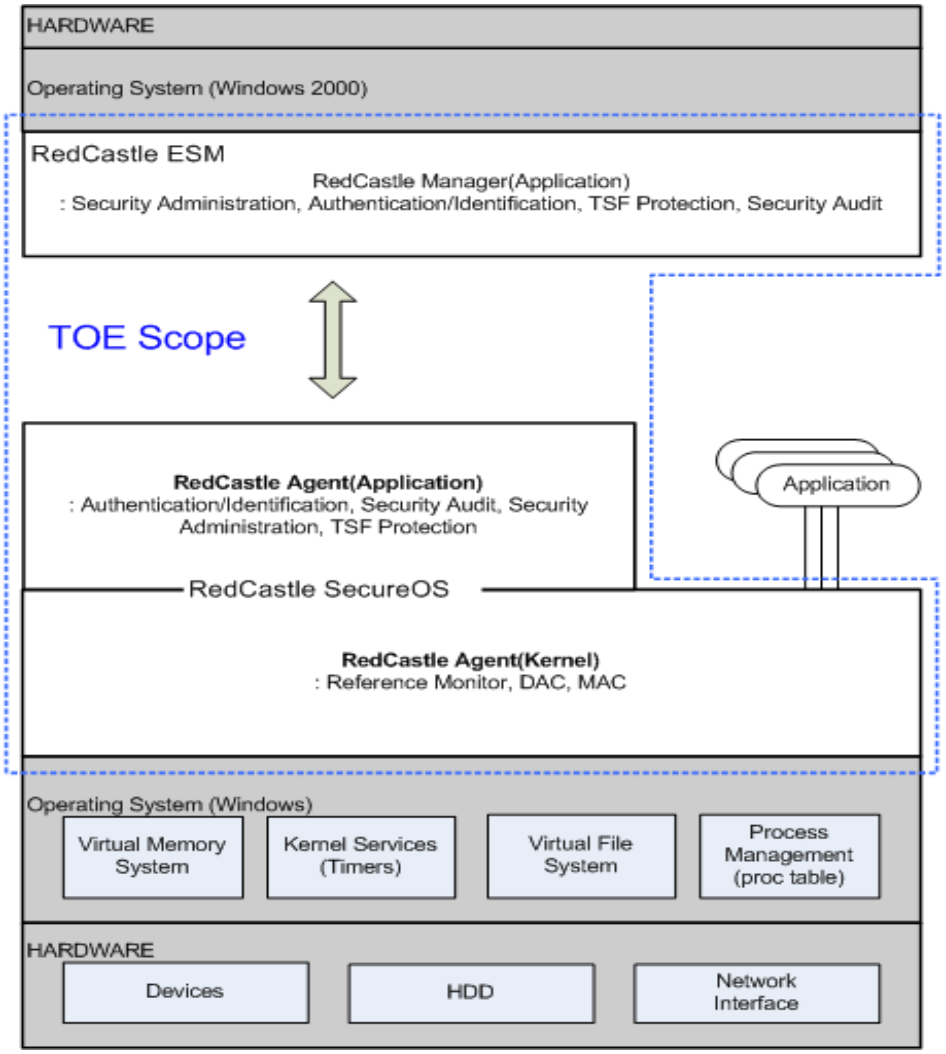
The TOE provides a countermeasure against the security threats, such as attempts to infringe the asset of main server. The TOE does not provide a countermeasure against direct physical attacks that makes the SFP ineffective or bypasses. But The TOE provides a countermeasure against logical attacks from 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, RedCastle v2.0 is consisting of RedCastle SecureOS which is security function processing part and RedCastle ESM (Enterprise Security Management) which is security management part.

RedCastle SecureOS will be installed on each operating system and this can be divided into kernel part - commits MAC and DAC and application part which commits other security functions. The management part of TOE, RedCastle ESM will be operated on Windows 2000 Professional (Service Pack 4). RedCastle SecureOS and RedCastle ESM is connected by 10/100BaseT Ethernet environment.



[Figure 1] Physical TOE Scope

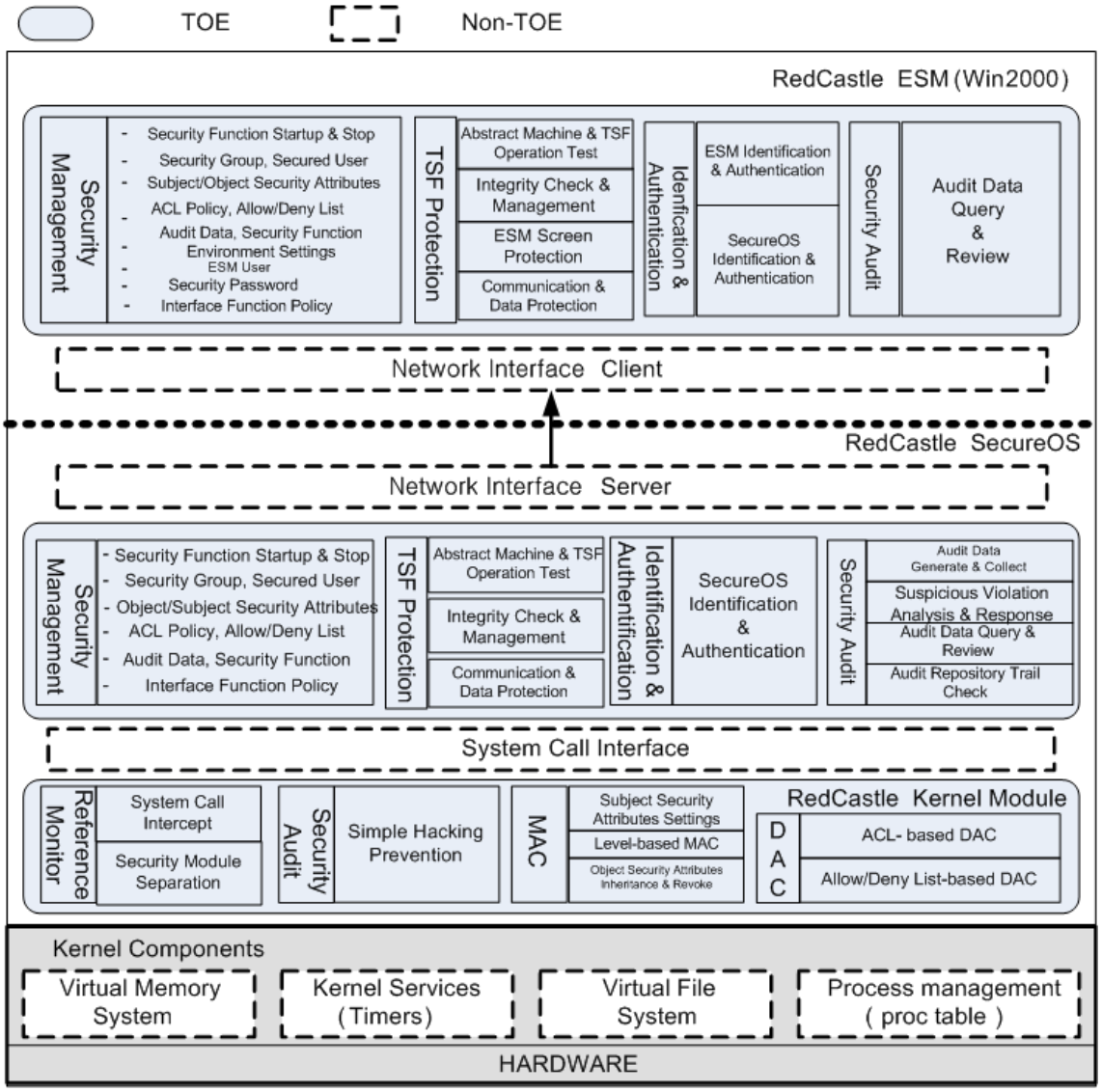
The detailed physical scope of TOE including hardware and software configurations in [Figure 1] is as follows.

[Table 3] Physical Environment of TOE

Class.	Security Fuction Processing	Security Management
Software	RedCastle SecureOS - Windows 2003 Server	RedCastle ESM - Windows 2000 Professional SP4
Hardware	CPU: Pentium III 600 MHz or higher RAM: 256MB or higher HDD: 200MB or higher Network: 10/100BaseT	CPU: Pentium III 600 MHz or higher RAM: 128 MB or higher HDD: 10 MB or higher Network: 10/100BaseT

Logical Scope and Boundary

The TOE, RedCastle v2.0 is divided into RedCastle SecureOS and RedCastle ESM. RedCastle SecureOS consists of application and kernel parts. The following [figure 2] shows logical TOE scope of RedCastle v2.0.



[Figure 2] Logical TOE Scope

As you can see in [Figure 2], the logical TOE scope of RedCastle includes TSF protection functions (reference monitor function, MAC and DAC function, security audit function, identification and authentication function, integrity check function and others), IP Filter (conducting intrusion prevention function on Network), and security management functions (system account management, interfacing for system monitoring to check system status).

6. Guidance Documents

The TOE provides the following guidance:

- RedCastle v2.0 Administrator Guidance Version 1.15, Aug. 27. 2007

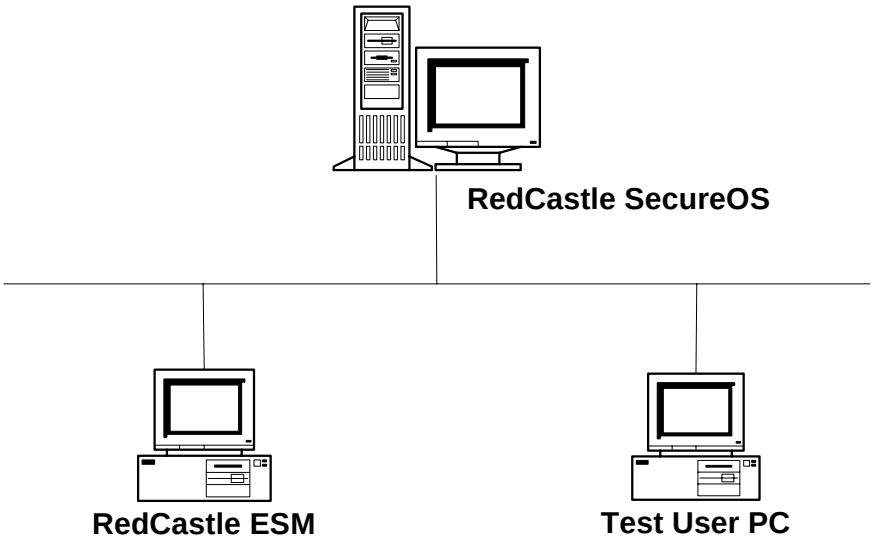
7. TOE Test

7.1 Developer Test

The developer produced the test item by considering the security function of the TOE. Each test item is described in test document. The detailed contents for developer testing efforts required by ATE_FUN.1-12 Working Unit Evaluation Activity are summarized and recorded as follows.

- **TOE Test Configuration**

The evaluator configured testing environment according to the testing environment described in the [ST] as follows.



[Figure 3] Developer Testing Environment

Class.	RedCastle SecureOS	RedCastle ESM	Test User PC
OS	Windows 2003 Server	Windows 2000 Professional	Windows 2000 Professional
Hardware	i386 RAM : 512MB HDD : 36GB Network : 10/100BaseT	Pentium IV 1.8GHz RAM : 512MB HDD : 3.5GB Network : 10/100BaseT	Pentium IV 1.8GHz RAM : 512MB HDD : 15GB Network : 10/100BaseT
Software	RedCastle v2.0 (RedCastle SecureOS)	RedCastle v2.0 (RedCastle ESM)	Remote Desktop (Terminal)

- **Testing Method**

The developer produced the test item by considering the security function of the TOE. Each test item is described in test documentation. The test item will include 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

- **Testing Results**

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

7.2 Evaluator Test

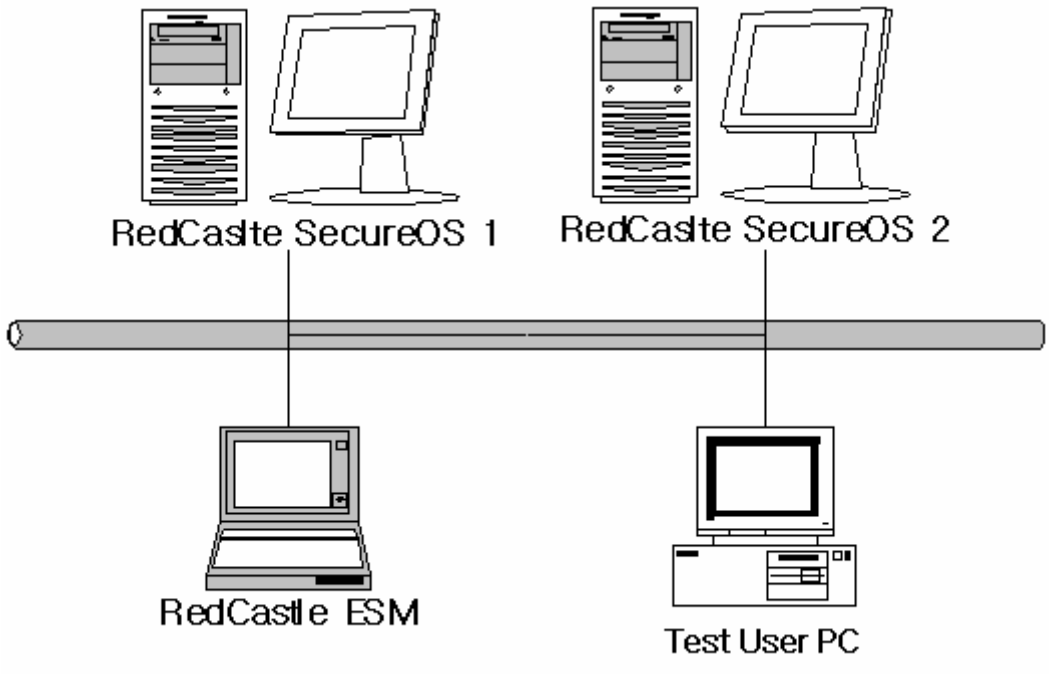
The evaluator configured the TOE by using the evaluation configuration and evaluation tools identical to the developer test, and examined the overall tests provided by the developer. The evaluator assured that the actual test results are consistent with the expected results in all test items.

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

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. Evaluation Configuration



All security functions provided by the TOE are included in evaluation scope and test environment is configured based on each security function's detailed security attributes and configuration methods.

o Security Function

TSF	Description
System Call Intercept (Refer.1)	TSF provides the reference monitor function to ensure the calling and succeeding of TSP enforcing functions before each function in TSC (TSF Scope of Control) to be allowed its conduct. For the security policy and security function environment settings of RedCastle Secure OS, system call will be added for use in the TOE. The newly added system call will be used to collect audit record also in the audit recording subsystem. This reference monitor function is deployed by changing the system call table of OS to the system call table used in RedCastle.
Security Module Separation	This function is provided to protect security function from external interference and tampering by unauthorized subject

(Refer.2)	through RedCastle kernel module deletion from operating system's module list when RedCastle kernel module is loaded into kernel. That is a function to prevent any removal trial by a unauthorized user by checking the installation of the TOE. Through this function, the unauthorized user can't remove the TOE since the one can't realize the installation of security module and the information of it. The Security Officer can check installation and running status of RedCastle kernel module.
Subject Security Attributes Settings (Ac_mac.1)	In the TOE, the subject will be identified and assigned its security attributes before it conducts access control function. In general UNIX system, if the subject's attributes is searched based on the subject information at the point of time MAC policy applied, the consistency can't be kept since the subject information is changed by 'su' and 'setuid' program. For this reason, the subject information has to keep its consistency for applying MAC policy. In the TOE, since TSF should realize subject and object identification information and security attributes before applying access control rule, subject security attributes setting function identifies subject/object system information and security attributes and if the security attributes can't be identified, it assigns security attributes and modify the security attributes based on subject or object's own properties. If a user login or a new process is created, the subject security attributes setting function will identify the subject and do connecting process of user security attributes to the subject before allowing all the TSF handling practices. When the subject security attributes is assigned, it will accord security level and category based on the security role.
Level based MAC (Ac_mac.2)	If all processes are identified and assigned its security attributes in the subject security attributes setting function, the multi-level based MAC functions will be performed. The TOE enforces level-based MAC policy based on the subject or object security attributes such as its sensitivity label (category, security level, etc.). The TOE applied modified B&L(Bell & La Padula) model for level-based Mandatory Access Control policy. If a user want

	to 'read' a file, the user has to satisfy the following condition : Subject (security level, security category) ≥ object (security level, security category). And if a user want to 'write' a file, the user has to satisfy the following condition : subject (security level, security category) = object (security level, security category). In 'read' rule, write and execute operation will be conducted. And in 'write' rule, write, create, and delete operation will be conducted.
Object Security Attributes Inheritance and revocation (Ac_mac.3)	When an object is created, the object will inherit the subject's security attributes automatically and when it is deleted, the security attributes and information of object will be deleted through the function of object security attributes inheritance and revocation. This function assures the prevention of previous information abuse.
ACL based DAC (Ac_dac.1)	System call which allowed in MAC is transmitted to DAC. DAC forces access control rules on the basis of ACL(Access Control List) according to identity of subject in DAC. This TOE provides DAC on the basis of ACL(Access Control List) separately with DAC by permission bit supporting in OS. The subject information identified in the ACL-based DAC policy are user identity(user ID, user name), subject belonged group identity(security category, security role), and user execution program(process name). ACL-based DAC controls read, write, execute, create, delete, rename, change mode ('chmod'), and change owner ('chown') operations.
Allow/Deny List based DAC (Ac_dac.2)	Allowed/Denied list based DAC is control according to allowed/denied list for operation to manage specially or for operation that is not applied to ACL. Policy based allowed list : If an act performed that is not in the allowed list, it will be denied. Policy based denied list : If a user performs an act which is in the denied list, it will be denied unless a user is SO The subject's user identity is used for security attributes and to decide whether an operation between controlled subject and object, the rule will be enforced based on Controlled Command List, Kill Prevention Process List, setuid List, and su control List.
ESM Identification & Authentication (Auth.1)	RedCastle ESM user can be classified into System Admin who can manage SecureOS, and a user who can query security log by connecting into SecureOS.

	In the RedCastle ESM's identification and authentication function, the access right to ESM will be decided through the authentication data verification by decryption of encrypted authentication data which is generated when an ESM user was registered based on the authentication information provided by an ESM user. The encrypted authentication data is configured based on the selected ID when a user registered. If five unsuccessful authentication attempts were occurred, repetition will be prohibited because the RedCastle ESM is killed compulsory.
SecureOS Identification & Authentication (Auth.2)	The Secure OS Authentication provides the following security function; SecureOS identification and authentication of SO by ESM, Identification and authentication of SecureOS user(Security Officer - SO, System Admin - SA, and Secured User - MU). (1) SecureOS Identification & Authentication for ESM User ESM user can connect by each server that RedCastle SecureOS is installed if succeed in login to console for administration in RedCastle ESM. SO must identify and authenticate about relevant SecureOS in case of connect to each server. Before perform SecureOS identification and authentication through ESM, it provides the identifying functions whether administrator account and ESM IP can connect to the Secure OS. The communication between RedCastle SecureOS and RedCastle ESM uses the SSL(Secure Socket Layer) version 3 protocol. The SSL protocol encodes data to secure the authentication information. (2) Secure OS identification and authentication of user for login All users identifiedin Secure OS will be permitted the access to the object which has its own security attributes after the completion of authentication process by security password.
	The following audit data will be generated in the TOE and log daemon will collect and store this data. ● The generated security log in security management

Audit Data Generation & Collection (Audit.1)	● The generated kernel log in RedCastle kernel ● The generated log in system monitoring Log daemon provides a function to collect and save log generated from IP Filter product as well as system log (login status log-wtmpx), login fail log (loginlog), ‘su’ succeeded and failed log (sulog), and 'syslog' (messages). In security management function and kernel module security function, security log are generated for thirty three kinds of classified audit targeting events include responding actions description against suspicious security violation detected (subject process compulsory termination, e-mail alert to system admin, etc), audit function's start-up and shut-down, and modified status of security audit environment settings. Each security log will configure audit data includes audit occurred time, audit occurred location (communication daemon, log daemon, kernel module), alert level(Information, Notice, Warning, Notice, Critical, Error).
Suspicious Violation Analysis and Response (Audit.2)	The SO can define unit time and the accumulation frequency limit for potential violation analysis in collected audit data in the TOE. In collected audit data, if a reviewed security violation exceeds accumulation frequency per unit time, TSF detects and warns this.
Audit Repository Trail Inspection (Audit.3)	Audit storage provides 50MB of file size and 5 files count in default value, and if thislimit is exceeded, it will warn the administrator by registry e-mail, and perform audit data loss prevention function.
Audit Data Query and Review (Audit.4)	In this TOE, the audit record will be stored in the directory to which SO can access only and provided in the format of which SO is able to read. The audit data which can query and review in this TOE is as follows. ● Security Log ● System Log ● System Monitoring Log ● IP Filter Log SO queries and reviews a selective audit data through GUI provided in RedCastle ESM and CLI provided in RedCastle SecureOS. The SO can develop the following reports about the stored audit data by using GUI(Graphical User Interface) and CLI(Command Line Interface). ● Security violation statistics/specification report ● User/IP login analysis report ● System information report

Simple Hacking Prevention (Audit.5)	The Simple attack prevention security function is to deny specific abuse actions detected as a violation conducted by a user over resources such as files and has the following detailed functions. ● Prevent the vulnerability of symbolic-link ● Prevent an illegal access to FIFO special file ● Prevent an illegal creation of Hard-link file ● Prevent the vulnerability of CHROOT ● Prevent attempts to switch the promiscuous mode ●
Security Function Start up and Stop (Admin.1)	When OS is booting and shutdown, or for SO to perform exceptional operations, the TOE provides the functions as follows. Collection and storage of audit log Security kernel module IP Filter which provides system services SO manages security functions through GUI provided in RedCastle ESM and CLI provided in RedCastle SecureOS. To start-up and stop security functions through GUI, communication function of RedCastle SecureOS must be in operation and should be keep its operation state even though the security functions are stopped. Administrator is not possible to perform any security management functions such as security policy-making unless he starts security function. But identification and authentication processes are possible to perform.
Security Group Management (Admin.2)	The security category corresponds to non-hierarchical attribute among security label of subject or object and SO is able to set this according to the character of organization. The security category means category of subject or object that defined in MAC and will be configured reflecting organization's system area or department usually.
Secured User Management (Admin.3)	The function of secured user management is able to set security label, and retrieve, change, and delete security attributes of labeled users. The security attributes of secured user will be configured based on user identity, user belonged group identity, authentication data, and sensitivity label (security group, security level, security role).
Object Security Attributes Management (Admin.4)	The attributes of object will be configured as file name, sensitivity label (security group, security level, security role). When a new file is created, the TOE is designed to inherit the security attributes of subject automatically andthis

	function will be used also when it assigns specificsecurity attribute by security officer (SO). The SO can assign sensitivity label to the object (file, directory) and also can refer, change, and cancel the security attributes of the file by using RedCastle ESm and CLI..
Subject Security Attributes Management (Admin.5)	The security attributes of process as a subject is consisted of process ID, owner identity, and sensitivity label (security group, security level, and security role status). When a new process is created, the TOE is designed to assign the security attributes of subject automatically and this function will be used when security officer (SO) want to query the security attributes of process.
ACL Policy Management (Admin.6)	In the TOE, the security officer (SO) is able to configure following rule of discretionary access control by file or file group for ACL policies management. ● Subject information : Default value - Any - The owner of subject - The security category of subject - The security role status of subject ● Subject program name ● Operation : Default value – Allow access - read - write - execute - create - delete - rename - mode change (chmod) - owner change (chown) The subject information will be selected as one of among subject owner, subject security group, and subject security role. If it is not selected, it would be all subjects. The subject program name can be selected with subject information and if it is not selected, it would be all programs. The Subject's operation on the object is selected by default value and allowed. The operation not selected will deny the access to it.
Allow/Deny List Management (Admin.7)	The security officer(SO) is able to add, search, and delete the following rules by GUI(Graphical User Interface) and CLI(Command Line Interface) for managing the policy that will allow or deny explicitly the access of subjects to objects based on the security attribute.

	● The denied rule of the restricting command execution ● The denied rule of the controlling kill signal ● The allowed rule for setuid operation ● The allowed rule for su operation ● The allowed rule for bypass of execution
Audit Data Environment Settings (Admin.8)	A security officer(SO) in the TOE is provided functions that are able to configure path, file, and alarm of audit storage.
ESM User Management (Admin.9)	By using the GUI(Graphical User Interface) provided in RedCastle ESM, it is possible to add/delete ESM administrator and user, and to change own ESM password. The password to be used for an ESM user registration or its changes must satisfy the following conditions. ● Password length: between 8 and 15 characters ● Acceptable password characters - 52 alphabetic letters (lowercase or uppercase) - 10 numeric digits (0-9) - 16 special characters (!,@,#,$,%,^,&,*,(,),+,=,<,>,:,;) ● A password must contain at least one character of alphabetic, numeric, and special characters ● Allow to use the consecutive alphabetic or numeric ● Allow to use the repetition of characters
Security Password Management (Admin.10)	This TOE provides function that can register and change authentication data, namely security password. A registration and a change of security password are possible only related user. A security officer (SO) is possible to change a security password by GUI and CLI. A system administrator except SO and a multi-label security user (MU) are possible to change a security password of self. An authentication data is generated mixing ID and password and this is encrypted using SEED algorithm and SHA-2 Hash algorithm. When security password registered or changed, a password must satisfy following conditions. ● Password length: between 8 and 15 characters ● Acceptable password characters - 52 alphabetic letters (lowercase or uppercase) - 10 numeric digits (0-9) - 16 special characters (!,@,#,$,%,^,&,*,(,),+,=,<,>,:,;) ● A password must contain at least one character of

	alphabetic, numeric, and special characters ● Allow to use the consecutive alphabetic or numeric ● Allow to use the repetition of characters
Security Function Environment Settings (Admin.11)	After the security function activated, the TOE provides the following functions to the security Officer to configure the security operating environment by GUI and CLI. ● Level-based MAC function : On, Warning ● ACL-based DAC function : On, Warning, Off ● Allow/Deny based DAC: On, Warning, Off ● Simple hacking prevention function : On, Warning, Off ● Security module hiding : On, Off ● Restriction of process attribute monitoring : On, Off
Interface Function Policy Management (Admin.12)	These functions provide the system service management's GUI(Graphical User Interface) and these are as follows. ● IP Filter function : Network connection control ● System monitoring function : System performance monitoring, process operation monitoring, process CPU occupation restrict, disk usage monitoring ● System account management function
Abstract Machine and TSF Operation Test (Protect.1)	The TOE provides abstract machine and TSF operation testing function to check operating system state and operation state of the TOE on the system. ● System status query : CPU usage, memory usage, booting over-lapsed time ● SecureOS status query : ESM connection time, security module version, security module operation status, log daemon operation status, IP Filter operation status, security log real time query
Integrity Check and Management (Protect.2)	For TSF's secure operation, the TOE provides integrity checking functions over TSF's execute file, TSF's data file, and files which administrator select. Execution files of RedCastle ESM and RedCastle SecureOS is registered as a default file for integrity checking target and will not be deleted from the list. In the case of a first integrity checking, the integrity checking value will bestored, and afterward created integrity value and stored integrity checking value will be compared. The TOE will use SHA-2 (256 bit) for integrity checking.
ESM Screen Protection (Protect.3)	The TSF can lock an interactive of security officer (SO) inactivity and can unlock by identification and authentication of administrator. This TOE is provided a session locking of administrator inactivity by the ESM Screen Saving.

Communication & Data Protection (Protect.4)	The TOE is installed the communication Server in the RedCastle SecureOS and the communication Client in the RedCastle ESM. The communication between RedCastle SecureOS and RedCastle ESM uses the SSL(Secure Socket Layer) version 3 protocol. The SSL protocol encodes data, and therefore authentication information is secured by SSL protocol. The key exchange method uses Diffie-Hellman mechanism. For cipher-suite, AES encryption algorithm (256 bit) and SHA-1 Hash algorithm were selected. The secure communication server provides control function of the RedCastle ESM connection that identify by security officer's account and ESM IP address when connect by RedCastle ESM for security officer manages RedCastle SecureOS.

9. Evaluation Results

· Security Target Evaluation

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. And it is logical, complete, internally consistent and coherent 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 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 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 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 Documentation 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 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 Life Cycle 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 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 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 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 allowed port properly according to the organization's policy.
- Even though the TOE provides admin alert function when its audit record repository space is reach to the threshold, the admin has to check its audit record repository space regularly and keep enough space always.

- The TOE is designed for security officer to use and manage only. Accordingly, the security officer must change its security password periodically and conduct special cares for not to be exposed.

11. Abbreviations and Terminologies

The following abbreviations were used in the report.

(1) Common Abbreviations

CC Common Criteria

EAL Evaluation Assurance Level

PP Protection Profile

SOF Strength of Function

ST Security Target

TOE Target of Evaluation

TSC TSF Scope of Control

TSF TOE Security Functions

TSP TOE Security Policy

(2) Terminologies

MAC (Mandatory Access Control)

Access control method based on an object's sensitivity label and subject's access right. In Common Criteria, B&L(Bell and La Padula) security model is presented as an example.

Object

Entity in the TSC (TSF Scope of Control) targeted for subject operation and includes or receives information.

Attack Potential

Success possibility of specific attack trial recognized in the light of attacker's expertise, resource, and motive.

Security Level

Combination of hierarchical Classification and non-hierarchical Category to present the importance of user or information.

DAC (Discretionary Access Control)

Access control method based on a user identity or group identity.

Sensitivity Label

Security attributes presenting security level of a subject or object

OS System Call

Callable interface by user program for kernel to conduct specific function (ex. file open)

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 Methodology for Information Technology Security Evaluation V2.3
[3] Information Security System Evaluation & Certification Guidance (2005. 5. 21)
[4] Information Security System Evaluation & Certification Regulations (2007.04.01)
[5] RedCastle v2.0 for Windows Security Target V1.6 (2007. 6. 14)
[6] RedCastle v2.0 for Windows Evaluation Report, V1.0 (2007. 11. 30)