KECS-CR-08-21

RedCastle v3.0 for Asianux Server 3 Certification Report

Certification No.: KECS-CISS-0104-2008

April 2008

IT Security Certification Center
National Intelligence Service

This document is the certification report on RedCastle v3.0 for Asianux Server 3 of RedGate Co., Ltd.

Certification Committee Members

ETRI-J. W. Park
Kwangwoon University-H. B. Yoo
Sungkyunkwan University-H. K. Choi
Chungnam University-J. C. Ryu
Hanyang University-J. H. Song

Certification Institute

National Intelligence Service IT Security Certification Center

Evaluation Facility

Korea System Assurance, Inc.

Table of Contents

1. Summary

This report describes the certification result drawn by the certification body on the results of the EAL4 evaluation of RedCastle v3.0 for Asianux Server 3 with reference to the Common Criteria for Information Technology Security Evaluation (notified 21 May 2005, "CC" hereinafter). It describes the evaluation result and its soundness and confirmity.

The evaluation of RedCastle v3.0 for Asianux Server 3 has been carried out by Korea System Assurance Inc. and completed on 16 April 2008. This report grounds on the evaluation technical report (ETR) KOSYAS had submitted, in which the evaluation has confirmed that the product had satisfied the CC Part 2 and EAL4 of the CC Part 3 and had been "suitable" according to the CC Part 1, paragraph 191.

RedCastle v3.0 for Asianux Server 3 is an Secure Operating System developed by RedGate Inc., which is installed on Asianux Server 3 and comprises RedCastle Agent, which performs access control at the request for information about the assets to be protected, and RedCastle Manager, which manages multiple RedCastle Agents and performs establishment of security policy. This certified product provides security functions listed below:

- Access Control
  - Reference monitor
  - LBAC
  - RBAC
  - Allow/deny list based DAC
- Identification and Authentication
  - Identification and Authentication of administrator/user of RedCastle Manager
  - Identification and Authentication of the Security Manager of RedCastle Agent
- Security management
  - Management of Administrator and user
  - Configuration of security function
  - Management of access control policy
  - Audit data reference and configuration
  - Management of service control policy
  - Integrity check and management
- Security audit
  - Audit data collection and storage
  - Potential violation analysis and action
  - Audit storage trail check

- Protection of the TSF
  - Abstract machine and TSF operation testing
  - Integrity check and management
- TOE access
  - Service/session control
  - Manager screen saver

The CB has examined the evaluation activities and test procedures, provided the guidance for the technical problems and evaluation procedures, and reviewed each evaluation work package report and evaluation technical report. Consequently, the CB has confirmed that the certified product had satisfied all security functional requirements and assurance requirements specified in the ST, thus the observations and evaluation results made by the evaluator had been correct and reasonable, and the verdicts assigned by the evaluator on the product had been correct.

Certification validity Range: Information in this certification report does not guarantee that RedCastle v3.0 for Asianux Server 3 is permitted use or that its quality is assured by the government of Republic of Korea.

2. Identification

[Table 1] identifies the certified product.

[Table 1] Evaluation Identifiers

Evaluation Guidance	Korea IT Security Evaluation and Certification Guidance (2007. 8.) Korea IT Security Evaluation and Certification Scheme (2007. 12.)
TOE	RedCastle v3.0 for Asianux Server 3
Protection Profile	N/A
Security Target	RedCastle v3.0 for Asianux Server 3 Security Target V1.4 (2008. 1. 30)
Evaluation Report	RedCastle v3.0 for Asianux Server 3 ETR V1.0 (2008. 4. 16)
Evaluation Result	CC Part 2 – Valid CC Part 3 – Valid
Evaluation Criteria	Common criteria for information technology security evaluation V2.3 (2005. 8.)
Evaluation Methodology	Common methodology for information technology security evaluation V2.3 (2005. 8.)
Sponsor	RedGate Co., Ltd.
Developer	RedGate Co., Ltd.
Evaluator	Korea System Assurance Inc., Evaluation Team, Yeowung Yun, Yongjoon Choi, Jungdae Kim
Certified by	National Intelligence Service

The certified product comprises RedCastle Agent, which covers the functions of access control, identification and authentication, generation and reference of audit data, and service control, and RedCastle Manager, which manages security functions. [Table 2] shows the specification required for the operation of the product.

[Table 2] Specification required of the certified product

Item	RedCastle Agent	RedCastle Manager
CPU	Intel Xeon 64 bit 2.4 GHz and above	Pentium IV 1.0 GHz and above
RAM	1,024 MB and above	512 MB and above
HDD	500 MB and above	100 MB and above
Network	10/100 BaseT	10/100 BaseT
OS	Asianux Server 3 (Kernel 2.6.18-8.10AX)	Windows XP Professional SP2

3. Security policy

The certified product operates in conformance with the security polices below:

P.Audit All security-relevant events shall be recorded and maintained and the data be reviewed to secure accountability of all security-relevant actions.

P.IA An access to information shall be identified and authenticated before it is permitted.

P.Management The authorized administrator shall manage the TOE in a secure manner.

P.Securitylevel The TOE shall be able to assign a subject and object an appropriate security level or annul it in accordance with the access control policy and procedures of the organization.

P.Securityrole The authorized administrator shall be able to manage and review the roles to establish and execute the role-based access control policy.

P.DAC The TOE shall be able to control the access to information based on the identity of users or group to which they belong.

P.MAC The TOE shall be able to control the access to information based on the security level of information and users.

P.RBAC The TOE shall be able to control the access to an object based on the user's roles.

4. Assumptions and Scope

4.1 Assumptions

The certified product shall be installed and operated with the following assumptions:

A.Locate The server on which the TOE is installed is located in a physically secure environment and protected from unauthorized physical modification.

A.Administrator The administrator of the TOE is not malicious, is adequately trained, and correctly performs duties according to the administrator's guide.

A.OSpatch The administrator of the TOE is not malicious, is adequately trained, and correctly performs duties according to the administrator's guide.

A.Installation The TOE is delivered, installed, generated, and operated in accordance with an appropriate procedure and ensured by the trusted administrator not to have an error in its security functions.

A.SSLprotocol The SSL protocol, which RedCastle Manager implemented using openssl for the secure communication with RedCaste Agent, is secure.

A.Timestamp Asianux Server 3 OS provides the TSF a reliable timestamp.

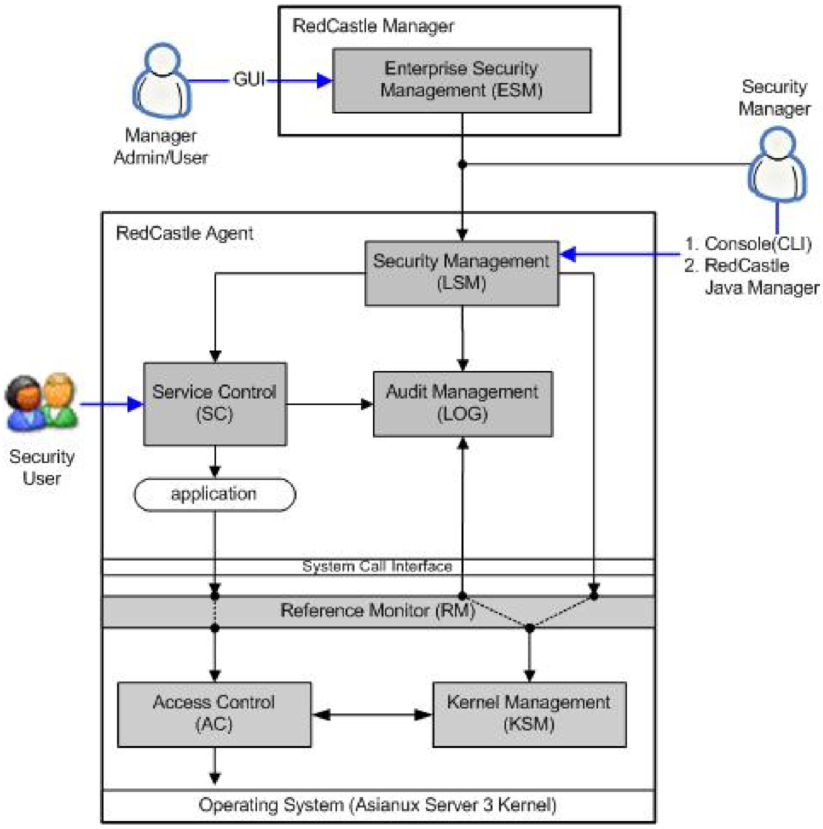
4.2 Threat Reaction Scope

The certified product provides a means to counter threats such as bypassing TSF data or user data that is to be protected by the TOE and tampering with data. It also provides a means to counter the logical attack launched by a threat agent possessing low-level expertise, resources, and motivation, though not a means to counter the direct physical attack such as disabling or bypassing security functions.

For a means to counter identified threats be provided, all security objectives and policies are described.

5. Product Information

The certified product is a Secure Operating System installed and operated on Asianux Server 3. It comprises RedCastle Agent, which processes security functions, and RedCastle Manager, which manages the security.



[Figure 1] TOE Architecture

RedCastle Agent performs LBAC, RBAC, and DAC in the domain of kernel of the OS and security management, service control, and audit data management in the application domain.

RedCastle Manager operates in the Windows XP Professional SP2 system and provides the Manager administrator and user with Windows based GUI for an integrated management of RedCastle Agent. It provides the Manager administrator and user acting as the security officer with a function to remotely manage the RedCastle Agent security functions; and the Manager administrator with the function to manage the Manager user.

The security officer can control RedCastle Agent remotely after accessing RedCastle Manager as the role of Manager administrator or user. The SO can also perform security management functions by accessing RedCastle Agent through console login and security management functions of RedCastle Agent by accessing X Windows and executing RedCastle Java

Manager.

The certified product comprises 7 subsystems as depicted in [Figure 1], main functions of which are described below:

■ Enterprise Security Management (ESM) Subsystem

ESM is a subsystem to manage the security functions of RedCastle Manager and Agent, provided with the Windows-based GUI.

ESM comprises functions stated below:

- Security functions of RedCastle Manager
  - Identification & authentication of the Manager administrator and user
  - Management of the Manager administrator and user
  - Management of the integrity of Manager
  - Management of audit log
  - Screen saver
- Management of the security of RedCastle Agent
  - Security functions configuration
  - Security function initiation and stop
  - Management of access control policy
  - Management of the operation of Agent
  - Management of service control
  - Reference and search of audit data
  - Document a report
  - Management of the integrity of Agent

ESM maintains secure communication session using SSL protocol that is provided in the IT environment during communication with LSM, which performs security management functions. Command given through ESM by the Manager administrator or user that has the authority of the security officer will be transmitted to the LSM for processing, the result of which will be transmitted to ESM to be checked through the GUI.

ESM provides a function to manage multiple RedCastle Agents including the security management functions. To perform the security management functions of RedCastle Agent, the identification and authentication of the security officer of Agent should be followed by the identification and authentication of the Manager administrator and user.

■ Local Security Management (LSM) Subsystem

For the management of security functions of RedCastle Agent, LSM provides command that is executable on the console and RedCastle Java Manager that can be operated on the X Windows.

LSM comprises functions stated below:

- Identification & authentication of the security officer
- Establishment of security functions
  - Security function initiation and stop
  - Security function configuration
- Management of access control policy
  - Management of security group and user
  - Management of user roles
  - Management of the security attributes of subject/object
  - Management of LBAC policy
  - Management of RBAC policy
  - Management of allow/deny list-based DAC policy
- Management of security audit
  - Audit configuration
  - Reference and search of audit data
  - Management of the state of system

LSM processes the command on security management transmitted from ESM and sends the result to ESM. Communication between LSM and ESM is supported by the SSL protocol provided in the IT environment.

The functions of LSM that interact with AC, such as security function initiation and stop, management of the data associated with access control policy, etc., invoke system call controlled under RM, which will be reflected to AC through KSM.

■ Audit Management (LOG) Subsystem

LOG is operated in the domain of application of RedCastle Agent, comprising the following functions:

- Audit log collection/storing
- Potential violation analysis and action
- Audit storage trail check

LOG collects regularly the security violation logs created in the kernel module of RedCastle Agent and stores them in the security log file. It analyzes the security violation logs of AC and, if the number of violation exceeds the limit set by the security officer, considers it potential violation to kill the process and terminate the session. It also checks regularly the audit storage space; if 80% of the storage is occupied, warns the security officer by e-mail at every other increase by 5%; when the storage reaches 100%, deletes the oldest audit data.

■ Service Control (SC) Subsystem

SC provides functions to control the login service of a user in accordance with the access control policy (e.g. the login period, access IP, user identity, group identity, number of login sessions, etc.).

- Service control and session control
- Management of the policies for service control and session control

■ Reference Monitor (RM) Subsystem

RM provides the following functions to enforce the TOE security policy when a system call is made within the TOE scope.

- Add control system call at the start-up of security functions
- Delete control system call at the stop of security functions
- Replace the OS system call at the start-up of access control function
- Recover the OS system call at the stop of access control function
- Intercept the system call within the TSF scope of control
- Intercept control system call

To intercept system call, the TOE replaces the system call table in the OS with a new system call that is included in the TSF scope of control at the start-up of security functions. In this process, the system call table is backed up so that it can be re-operated when the security function is stopped.

The control system call is only used within the TOE for the security policy and security function configuration and audit data collection.

RM processes the input/output of data of AC, input/output between LOG and AC, and control of AC.

■ Access Control (AC) Subsystem

When a system call intercept is occurred in RM, the request for system call is sent to AC, which will perform a function of security attribute establishment, LBAC, RBAC, and DAC in that order. AC provides the following functions:

- Identify subject and assign security attribute to subject
- Manage LBAC policy
- Manage RBAC policy
- Manage allow/deny list-based DAC

If a system call is occurred within the TSF scope of control by a user or process, RM intercepts and transmits it to AC. Then AC identifies the subject and performs LBAC function according to the security attributes of the subject and object. If it is denied by LBAC policy, AC transmits the audit data to KSM and generates a security violation log to store in the kernel memory; if it is allowed, AC enforces RBAC policy and compares the subject's role and object's use access to determine either to allow or deny. Finally, if DAC policy of the OS is allowed as well, the use access of the subject on the object will be approved.

■ Kernel Management (KSM) Subsystem

KSM performs, in connection with the LSM, security functions for the application of access control policies that the security officer defined to the AC. KSM provides the following functions:

- Start-up and stop of an access control security function
- Management of security function configuration
- Management of security group/user
- Management of the user role list
- Management of the security attribute of object
- Management of the security attribute of subject
- Management of LBAC policy
- Management of RBAC policy
- Management of allow/deny list-based DAC policy
- Storage and reference of kernel log

KSM manages the initiation and stop of AC and access control policy of kernel memory. It is started by the control system call invoked in LSM.

LSM invokes control system call and sends the security officer's command on security management to KSM.

Access control policies are stored in the kernel memory and referred to by AC. At the start-up of the TOE, however, the policy is not provided, so LSM should send the access control policy to KSM using the control system call. KSM stores the access control policy transmitted in the kernel memory. LSM notifies KSM of the modification of policy and stores it in a file. The operational environment value required for the enforcement of AC will be processed in the same manner as the access control policy.

6. Administrator Guidance

The certified product provides the following as a guidance document.

- RedCastle v3.0 for Asianux Server 3 Administration Manual v1.2, 2008. 3. 4

7. Product Testing

7.1 Developer Testing

- Test method

The developer devised the test considering the security function of the product. Each test described in the test documents includes the details below:

- Test No.: Test identifier
- Purpose: Purpose of the test, including the security function to be tested
- Test configuration: Detailed test configuration for testing
- Detailed test procedures: Detailed procedures for testing the security function
- Expected result: The result expected from carrying out the test procedures
- Actual result: The result given by carrying out the test procedures
- Comparison between the expected result and actual result: The result of comparing the expected result and actual result

The evaluator has assessed the suitability of test regarding the configuration, procedures, scope analysis, and low-level design test and verified that the developer's test and its result had been appropriate for the test configuration.

- Test configuration

The test configuration in the test documents describes the configuration details including network configuration for testing, product to be evaluated, and arrangement procedures, and the test configuration details including test tools required for each test.

- Test scope analysis / Low-level design test

Detailed evaluation results are described in the evaluation results of ATE_COV and ATE_DPT.

- Test results

The test documents describe expected test result and actual test result for each test. The actual test result can be confirmed by the audit records as well as by the screen of the product.

7.2 Evaluator Testing

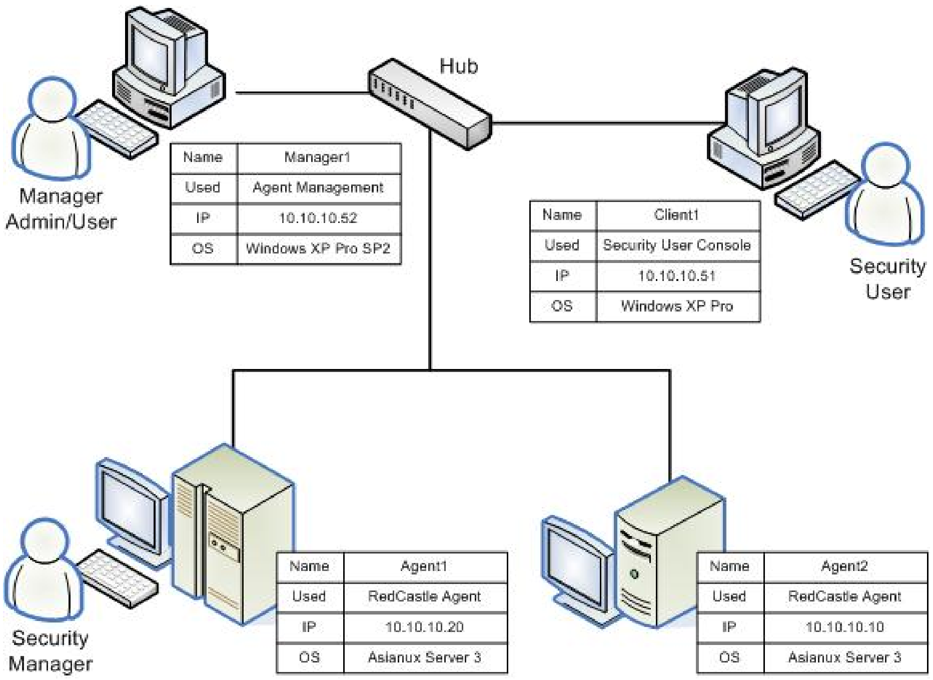
The evaluator has installed the product using the same evaluation configuration and tools as the developer's test and performed all tests provided by the developer. The evaluator has confirmed that, for all tests, the expected results had been consistent with the actual results.

The evaluator has confirmed this consistency by performing additional tests based on the developer's test. The evaluator has also confirmed that, after performing vulnerability test, no vulnerability had been exploitable in the evaluation configuration.

The evaluator's test result has ensured that the product had normally operated as described in the design documents.

8. Evaluated Configuration

The evaluator has configured the environment for test as consistent with that specified in the ST as [Figure 2] below.



Name	Manager1
Used	Agent Management
IP	10.10.10.52
OS	Windows XP Pro SP2

Name	Client1
Used	Security User Console
IP	10.10.10.51
OS	Windows XP Pro

Name	Agent1
Used	RedCastle Agent
IP	10.10.10.20
OS	Asianux Server 3

Name	Agent2
Used	RedCastle Agent
IP	10.10.10.10
OS	Asianux Server 3

[Figure 2] Evaluator Test Configuration

All security functions provided by the product are considered in the scope of evaluation. The evaluation is configured regarding the security attributes and method of configuration of each security function.

9. Results of the Evaluation

The evaluation is performed with reference to the CC V2.3 and CEM V2.3. The result claims that the evaluated product satisfies the requirements from the CC Part 2 and EAL4 in the CC Part 3. Refer to the evaluation technical report for more details.

- ST evaluation (ASE)

The evaluator has performed ST evaluation with the ASE work units in CEM.

The TOE description in the ST is coherent, internally consistent, and consistent with all other parts of the ST. The security environment in the ST provides a clear and consistent definition of the security problem that is induced in the TOE and its environment. The security objectives in the ST are described completely and consistently. They counter the identified threats, achieve the identified organizational security policies, and are consistent with the stated assumptions. The TOE security requirements and the security requirements for the IT environment in the ST are described completely and consistently, and provide an adequate basis for development of a TOE that will achieve its security objectives. The TOE summary specification in the ST provides a clear and consistent high-level definition of the security functions and assurance measures, and satisfies the specified TOE security requirements. The ST states that no PP claim is made for the TOE.

- Configuration management evaluation (ACM)

The evaluator has performed configuration management evaluation with the ACM work units in CEM.

The configuration management specifies configuration item, how to identify configuration, how to give a version, and how to control configuration change. It is confirmed that all development documents and source files were developed applying configuration management system and that generation and modification of configuration item are performed by the organization and configuration management system.

- Delivery and operation evaluation (ADO)

The evaluator has performed delivery and operation evaluation with the ADO work units in CEM.

The delivery and operation describes the measures and procedures for secure delivery, installation, and operational use of the TOE, ensuring that the security protection offered by the TOE is not compromised during transfer, installation, start-up, and operation. The site visit carried out by the evaluator has confirmed that what is described in the document had actually been enforced in the development site.

- Development evaluation (ADV)

The evaluator has performed development evaluation with the ADV work units in CEM.

The development defines the TOE security functional requirements from the TOE summary specification down to the actual implementation, using the functional specification, high-level design, low-level design, and implementation representation. It describes clearly that the requirements are correctly and completely implemented using the relationship between all adjacent pairs of development representations. The security policy model clearly and consistently describes the rules and characteristics of the security policies and the description corresponds with the description of security functions in the functional specification.

- Guidance documents evaluation (AGD)

The evaluator has performed guidance documents evaluation with the AGD work units in CEM.

The guidance documents describe the GUI provided when a user accesses the evaluated product and its way of operation with appropriate examples. The administration manual gives examples about the method of the administrator's accessing a security management interface and the description and notes for each menu provided by the interface. The evaluator has confirmed that what is specified in the administration manual had been correctly performed.

- Life cycle support evaluation (ALC)

The evaluator has performed life cycle support evaluation with the ALC work units in CEM.

The life cycle support describes that the development environment is protected using security measures such as the procedures, policies, tools and techniques for each and every step of the development of the TOE. The site visit carried out by the evaluator has confirmed that what is described in the document had actually been enforced in the development site.

- Tests evaluation (ATE)

The evaluator has performed tests evaluation with the ATE work units in CEM.

The test documents describe the test purpose, procedures for each step, and test results, and give proper examples. By repetitive performance of the service test and integrated test for the provided development steps, the evaluator has confirmed the correctness of the test description in the test documents and the consistency of the operation of security functions implemented during development. The evaluator's independent testing has confirmed the correctness of the developer's test.

- Vulnerability assessment evaluation (AVA)

The evaluator has performed vulnerability assessment evaluation with the AVA work units in CEM.

The vulnerability analysis properly and correctly describes the analysis of and action to the known vulnerabilities and chance of misuse. The evaluator's penetration testing has confirmed that the developer's vulnerability analysis had been correct. The strength of function (SOF) analysis describes that the SOF of the TOE meets the SOF metric defined in the ST.

10. Recommendations

- The security officer shall have knowledge of the property of access control of the TOE, where the LBAC, RBAC, and DAC are applied in that order, and apply them with deliberation.
- Since the security officer can manage audit data generated by more than one RedCastle Agent, the security officer should set correct time of the system on which each RedCastle Agent is installed; otherwise the time of audit data of one RedCastle Agent may differ from that of the other to bring about difficulty having confidence in the audit data.
- Understanding that the TOE overwrites the oldest audit data in the case that the audit storage is full, the security officer shall check the storage of RedCastle Manager and e-mail regularly and backup before exhaustion to maintain the audit data.

11. Terminology

The following abbreviations are used in this report:

EAL	Evaluation Assurance Level
TOE	Target of Evaluation
TSF	TOE Security Functions

The following terms are used in this report:

TOE
An IT product or system and its associated guidance documentation that is the subject of an evaluation

Audit record
Audit data that stores events associated with the security of the TOE

LBAC
Label−based access control; a kind of MAC where the security attributes of a subject and object have a label by the protection level and category; the label gives ground to mandatorily control the access of that subject to that object. BLP model is an example. An abbreviated form of label−based mandatory access control

Security attribute
Characteristics of subjects and objects that are used for the enforcement of the LBAC, RBAC, and DAC policies

Security level
Categorizes into Top Secret, Secret, Confidential, Restricted, and Unclassified in a hierarchical order

Security category
Security group; the security officer, the highest category, is assigned an ID 1; the system administrator 2; and the security user 3 − 127.

RBAC
Role−based access control; A means to control the access of a user to an object with the roles that are dependent on the property of an organization as a mediator, thus based on the 'user−role relationship' and 'access permission−role relationship' rather than a direct relationship between the user and access permission

Threat agent
An unauthorized user or external IT entity that causes threats for assets such as illicit access, modification, or deletion

DAC
Discretionary access control; a means to control access to objects based on the identity of a user or group to which the user belongs

Assets
Information or resources to be protected by the countermeasures of a TOE

12. Reference

The CB has referred to the following documents to produce this report:

[1] Common Criteria for Information Technology Security Evaluation V2.3 (2005. 8.)

[2] Common Methodology for Information Technology Security Evaluation V2.3 (2005. 8.)

[3] Korea IT Security Evaluation and Certification Guidance (2007. 8. 22)

[4] Korea IT Security Evaluation and Certification Scheme (2007. 12.)

[5] RedCastle v3.0 for Asianux Server 3 ETR V1.0 (2008. 4. 16)