KECS-CR-07-01

Certification Report on REDOWL SecuOS V4.0 for RHEL4 of TSonNet Co., Ltd.

Certification No. : KECS-CISS-0060-2007

Jan. 2007

National Intelligence Service

IT Security Certification Center

This document is the certification report on REDOWL SecuOS V4.0 for RHEL4 of TSonNet.

Certification Body

National Intelligence Service IT Security Certification Center

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 REDOWL SecuOS V4.0 for RHEL4 with regard to the Common Criteria for Information Technology Security Evaluation (Notification No. 2005-25 of the Ministry of Information and Communication; "CC" hereinafter).

The Korea Information Security Agency (KISA) has finished the evaluation of the REDOWL SecuOS V4.0 for RHEL4 on the 19th of Dec. 2006. 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 the EAL3 of the part 3 assurance requirements with augmenting ADV_IMP.2, ADV_LLD.1, ALC_TAT.1, ATE_DPT.2, AVA_VLA.2; thus, it is assigned the verdict 'pass' on the basis of the paragraph 191 of the CC part 1. In addition, the TOE satisfies the Label-based Access Control System Protection Profile for Government V1.1(May. 17. 2006).

REDOWL 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. REDOWL 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 :

- Security Audit
- User Date Protection
- Security Management
- Identification and Authentication
- TSF Protection
- Trusted Path/Channels
  - TOE uses the Open SSL V0.9.8a to connect trusted channels
- TOE Access
  - TOE controls access to the administrators and users session

The certification body has examined the evaluation activities and testing procedures, provided the guidance regarding the technical problems and evaluation procedures, and reviewed each evaluation work package and evaluation technical report. In conclusion, the certification body has confirmed that the evaluation results gave assurance that the TOE meets all security functional requirements and assurance requirements described in the Security Target(ST). As a result, the certification body has certified that the evaluator's observations and evaluation results were accurate and reasonable, and his verdict on each work package was correct.

Certification Validity: The information contained in this certification report does not mean that the use of REDOWL SecuOS V4.0 for RHEL4 is approved or its quality is guaranteed by governmental agency of the Republic of Korea.

2. TOE Identification

The [Table 1] summarizes the information of the TOE identification.

[Table 1] TOE Identification

Evaluation Guidance	Korea IT Security Evaluation and Certification Guidance (May. 21, 2005) Korea IT Security Evaluation and Certification Scheme (Dec. 26, 2005)
TOE	REDOWL SecuOS V4.0 for RHEL4
Protection Profile	Label-based Access Control System Protection Profile for Government V1.1(May. 17. 2006)
Security Target	REDOWL SecuOS V4.0 for RHEL4 ST V1.1 (May. 5, 2006)
ETR	REDOWL SecuOS V4.0 for RHEL4 ETR V1.00
Evaluation Result	Conformance to the CC V2.3 part 2 Conformance to the augmented part 3 (ADV_IMP.2, ADV_LLD.1, ALC_TAT.1, ATE_DPT.2, AVA_VLA.2)
Evaluation Criteria	Common Criteria for Information Technology Security Evaluation (May. 21, 2005) Final Interpretation (Sept. 30, 2006)
Evaluation Methodology	Common Methodology for Informations Technology Security Evaluation V2.3
Sponsor	TSonNet Co., Ltd.
Developer	TSonNet Co., Ltd.
Evaluation Team	KISA IT Security Evaluation Center, Evaluation Team 2 Chan Il Kim
Certification Body	National Intelligence Service

[Table 2] describes the system specification of the TOE.

[Table 2] REDOWL SecuOS V4.0 for RHEL4 Operating Environment

Category		Specification
REDOWL Enterprise	CPU	Intel Xeon64(Nocona) 1.7GHz, AMD64(Opteron) 1.7GHz, IA64 900MHz
	Memory	2Gbyte
	Interface	10/100base Ethernet card 1
	HDD	36Gbyte
	Operating System	RHEL4
REDOWL Agent	CPU	Intel Xeon64(Nocona) 1.7GHz, AMD64(Opteron) 1.7GHz, IA64 900MHz
	Memory	512Mbyte
	Interface	10/100base Ethernet card 1
	HDD	18Gbyt
	Operating System	RHEL4
REDOWL Manager	CPU	Pentium III(500MHz)
	Memory	256Mbyte
	Interface	10/100base Ethernet card 1
	HDD	10Gbyte
	Operating System	MS Windows 2000 Professional(SP4)

3. Security Policy

The TOE operation conforms to the security policies stated below:

Audit Record

Every security-relevant event should be recorded and saved to make it possible to trace the responsibility of every action; the recorded data should be reviewed.

Mandatory Access Control

TOE should have capability of controlling accesses toward objects by the basis of subject's security labeling.

Allowance of security labels

TOE should have capability of allowing or canceling of security labels in accordance with the organization's access control policies and procedures.

Identification & Authentication

The administrator should pass through the process of identification and authentication before using the security functions of the TOE.

Security Management

Only an authorized administrator who accesses through trusted communication can use the security management function.

Cryptographic

The cryptographic algorithm and module used in the TOE must be approved by the Director of National Intelligence Service.

Discretionary Access Control

TOE should have capability of controlling accesses toward information by identities of users or user-belonged groups.

SSL Certificate management

TOE should generate and manage SSL certificates in secure way.

4. TOE Assumptions and Scope

4.1 Assumptions

The TOE installation and operation should conform to the assumptions stated below:

A.Physical Security

The TOE is located in physically secure environment where only authorized administrators are allowed the access.

A.Trusted Administrator

An authorized administrator of the TOE possesses no malicious intention, is adequately educated, and performs his/her duties in accordance with the administrative guideline.

A.Hardened OS

The underlying OS of the TOE ensures the reliability and stability by both eliminating the unnecessary services or means not required by the TOE and installing the OS patches.

A. SSL certificate of TOE

TOE stores the certificate, which is to be used in case of SSL authentication, when it is installed. TOE's SSL certificate is securely generated and managed.

A.TIME

The IT environment of the TOE is provided with a reliable Timestamp from the NTP server which conforms to RFC 1305 or from the OS.

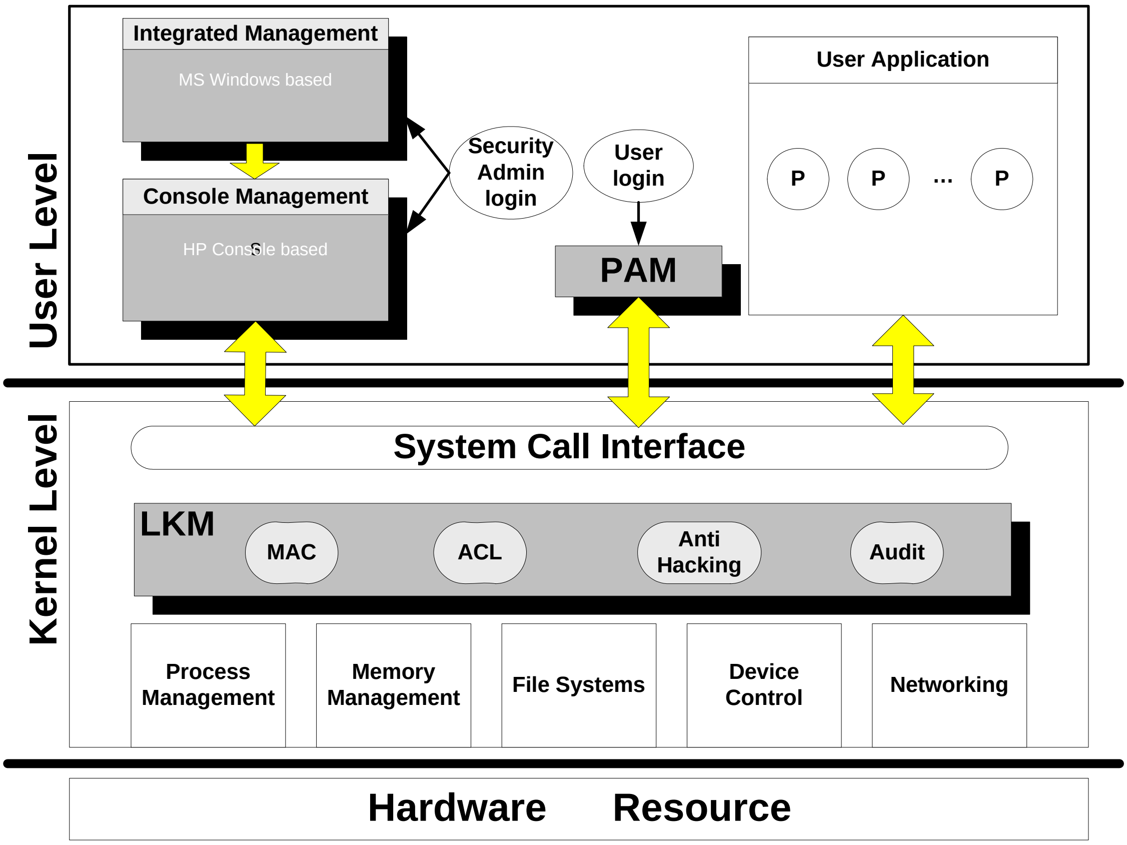
4.2 Scope to Counter a Threat

The TOE provides a means to counter security threat such as intrusion attempts on server assets, etc. Although the TOE does not have a countermeasure for a direct physical attack which disables or bypasses security functions, it provides a countermeasure for a logical attack occurred by threat agents possessing low-level expertise, resources, and motivation.

All security objectives and security policies are described to provide a means to counter an identified security threat.

5. TOE Information

The TOE provides an label based access control function. The figure below shows the structure of the TOE.



(Figure 1) REDOWL basic structure

The main components of TOE include LKM, PAM, CUI and GUI. As the core component, LKM performs MAC (Mandatory Access Control), detecting hacking attacks by tracing 'root' privileged daemon processes, prevention mechanism of resource reuse and controls executions of system commands by users or IP addresses by managing extra access control lists. And LKM also collects and generates audit data for every security events.

PAM, which provides user authentication function, is loadable authentication module presented by OS. PAM presents the capability and flexibility of various authentication services for system administrator to choose and perform them. By using PAM, various functions, such as, user password combination rule, password expiration period set-up, prohibition of identical password reuse, user log-in time zone set-up and log gathering of various authentications, are provided.

CUI(Character User Interface) is the interface between security administrator, GUI(Graphic User Interface) and LKM. By using CUI, it is able to operate the activation and termination of REDOWL system, setting up and inquiry of security information or audit data. For the secure channel formation, CUI use security protocol of SSL.

GUI(Graphic User Interface) provides graphical interface to REDOWL administrator. GUI performs the same functions as CUI component, and those commands called by GUI are conducted through CUI subsystem. And separately from CUI, GUI presents statistics and analysis for audit data. For the secure channel formation, GUI use security protocol of SSL.

6. Guidance

The TOE provides the following guidances:

- REDOWL SecuOS V4.0 for RHEL4 Administrator Guidance V1.0, Dec. 30, 2005
- REDOWL SecuOS V4.0 for RHEL4 Delivery and Operation V1.0, Dec. 30, 2005

7. TOE Test

7.1 Developer's Test

- Test Method

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

- Test No./Tester : The identifier of the test and the developer who participated in testing
- Purpose of the test : Describes the purpose of the test including security function and security module to be tested
- Test configuration : Detailed environment where the test is carried out
- Detailed test procedure : Detailed procedure to test security functions
- Expected result : Test result expected when performing the test procedure
- Actual result : Test result acquired when the test is performed

The evaluator performed an evaluation of the validity such as the test configuration, test procedure, test scope analysis, and the low-level design test.

The evaluator verified that the developer's test and its results were adequate for the evaluation configuration.

- **Test configuration**

The test configuration described in the test documentation includes the detailed configuration such as the organization of network for the test, the TOE, PC and the server. In addition, it describes detailed test configuration such as the application sever(e.g. web server, mail server, etc.) and test tools required to perform each test.

- **Test Scope Analysis/Low-Level Design Test**

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

- **Test Result**

The test documentation describes the expected result and actual result of each test. The actual result is confirmed through the audit record as well as the GUI of the TOE.

7.2 Evaluator's Test

The evaluator installed the TOE using the evaluation configuration and evaluation tools identical to those of the developer test and performed testing for the overall tests provided by the developer. The evaluator confirmed that the actual result of every test was consistent with the expected result.

Moreover, the evaluator devised and performed additional evaluator's tests on the basis of the developer's test, and confirmed that the actual test result was consistent with the expected test result.

The evaluator carried out the vulnerability test and confirmed that there was no exploitable vulnerability in the evaluation configuration.

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

8. Evaluation Configuration

The network configuration for the evaluation is only internal network. The following information is about the hardware used for the evaluation configuration:

[Table 3] Hardware used for the evaluation configuration

Category	REDOWL Server			REDOWL Manger
CPU	Xeon 2.4MHz	AMD64 Opteron 1.7Ghz	IA64 9000MhZ 2CPU	Pentium Ⅳ 1.8GHz
Memory	2 Gbyte	2 Gbyte	3 Gbyte	512 Mbyte
Total	4			

The following information is about the software used for the evaluation configuration:

- RedHat Enterprise Linux AS release 4 : Kernel 2.6.9
- Windows 2000 Professional

All security functions provided by the TOE are included in the scope of evaluation. The evaluation configuration is based on the detailed security attributes and configuration of each security function.

9. Evaluation Result

The evaluation is on the basis of the Common Criteria for Information Technology Security Evaluation, Common Methodology for Information Technology Security Evaluation V2.3, and the Final Interpretation (Sept. 2006). It concludes that the TOE satisfies the CC V2.3 part 2 and EAL3+ of the CC V2.3 part 3 assurance requirements. The detailed information regarding the evaluation is described in the ETR

- ST Evaluation (ASE)

The evaluator applied the ASE sub-activities described in the CEM V2.2 to the evaluation of the ST of the TOE.

The ST introduction is complete and consistent with other parts of the ST, and correctly identifies the ST. The TOE description contains relevant information to aid the understanding of the purpose of the TOE and its functionality, and is complete, internally consistent, and consistent with other parts of the ST.

The TOE security environment in the ST clearly and consistently defines the assumptions, threats, and organizational security policies related to the security problem that the TOE and its environment are intended to address, and is described completely and consistently. The security objectives counter the identified threats, achieve the organizational security policies, and satisfy the stated assumptions.

The IT security requirements (both the TOE security functional requirements and the TOE security assurance requirements) and the security requirements for the IT environment are described completely and consistently and provide an adequate basis for the development of a TOE that will achieve its security objectives. The TOE summary specification provides a clear and consistent definition of the security functions and assurance measures and satisfies the specified TOE security requirements. The ST is a correct instantiation of any PP for which compliance is being claimed.

Thus, the ST is complete, consistent, technically sound, and hence suitable for use as the basis for the corresponding TOE evaluation.

- Configuration Management Evaluation (ACM)

The evaluator applied the ACM sub-activities described in the CEM V2.3 to the evaluation of the configuration management of the TOE.

The evaluator confirmed the following through an examination of the configuration management documentation:

- The developer controls changes of the implementation representation with the support of automated tools.

- The developer has clearly identified the TOE and its associated configuration items; the ability to modify these items is properly controlled.

- The developer performs configuration management on, at a minimum, the TOE implementation representation, the evaluation evidence required by the assurance components in the ST, and security flaws.

Thus, the configuration management documentation assists the consumer in identifying the evaluated TOE, and ensures that the configuration items are uniquely identified and that the procedures used by the developer to control and track changes of the TOE are adequate.

- Delivery and Operation Evaluation (ADO)

The evaluator applied the ADO sub-activities described in the CEM V2.3 to the evaluation of the delivery and operation of the TOE.

The delivery documentation describes all procedures used to maintain the security of the TOE and detect modification or substitution of the TOE when distributing the TOE to the user's site.

The procedures and steps for the secure installation, generation, and start-up of the TOE have been documented, which ensures a secure configuration of the TOE.

Thus, the delivery and operation documentation is adequate to ensure that the TOE is installed, generated, and started in the same way the developer intended it and that it is delivered without modification.

- Development Evaluation (ADV)

The evaluator applied the ADV sub-activities described in the CEM V2.3 to the evaluation of the development of the TOE.

The functional specification adequately describes all security functions of the TOE and explains that the security functions of the TOE are sufficient to satisfy the security functional requirements in the ST.

The security policy modeling clearly and consistently describes the rules and characteristics of the security policies; this description corresponds with the security functions described in the functional specification.

The high-level design describes the TSF in terms of subsystems, major TOE structural units, and adequately explains the interfaces to the subsystems. It is a correct realization of the functional specification.

The low-level design describes the internal workings of the TSF in terms of modules and their interrelationships and dependencies. It is sufficient to satisfy the functional requirements in the ST and is a correct and effective refinement of the high-level design.

The implementation representation is sufficient to satisfy the functional requirements in the ST and is a correct realization of the low-level design.

The representation correspondence shows that the developer has correctly and completely implemented the requirements in the ST into the functional specification, high-level design, low-level design, and implementation representation.

Thus, the following design documentations are adequate to aid understanding how the TSFs are provided: the functional specification which describes the external interfaces to the TOE; the high-level design which describes the architecture of the TOE in terms of internal subsystems; the low-level design which describes the architecture of the TOE in terms of internal modules; the implementation representation in the form of source code-level description; and the representation correspondence which maps representations of the TOE to one another in order to ensure consistency.

- Guidance Evaluation (AGD)

The evaluator applied the AGD sub-activities described in the CEM V2.3 to the evaluation of the guidance of the TOE.

The administrator guidance describes how to administer the TOE in a secure manner.

Thus, the guidance documentation adequately describes how to use the TOE in a secure manner.

- Life Cycle Support Evaluation (ALC)

The evaluator applied the ALC sub-activities described in the CEM V2.3 to the evaluation of the life cycle support of the TOE.

The evaluator confirmed that the developer's control on the security of the development environment was adequate to provide the confidentiality and integrity of the TOE design and implementation that are necessary to ensure secure operation of the TOE; that the developer had used a documented life-cycle model of the TOE; and that the developer had used well-defined development tools that yield consistent and predictable results.

Thus, the life cycle support adequately describes the procedures which the developer uses during the development and maintenance of the TOE, including the security procedures and tools used in the development of the TOE.

- Tests Evaluation (ATE)

The evaluator applied the ATE sub-activities described in the CEM V2.3 to the evaluation of the test of the TOE.

The testing is sufficient to establish that the TSF has been systematically tested against the functional specification.

The evaluator confirmed that the developer had tested the TSF against its high-level design.

The developer's functional test documentation is sufficient to demonstrate that the security functions perform as specified.

The evaluator confirmed that the TOE behaved as specified by performing independent testing of a subset of the TSF and gained confidence in the developer's test results by performing entire developer's tests.

Thus, by performing independent testing of a subset of the TSF, the evaluator confirmed that the TSF behaved in accordance with the TOE security functional requirements stated in the ST and the design documentation.

- Vulnerability Assessment Evaluation (AVA)

The evaluator applied the AVA sub-activities described in the CEM V2.3 to the evaluation of the vulnerability assessment of the TOE.

From the misuse analysis, it is confirmed that the guidance is not misleading, unreasonable, or conflicting; that secure procedures for all modes of operation have been addressed; and that the use of the guidance will facilitate prevention and detection of insecure TOE state.

It is confirmed that the SOF claims are made for all probabilistic or permutational mechanisms in the ST and that the analysis of the developer's SOF claims is correct.

The vulnerability analysis document describes the identified vulnerabilities of the TOE and appropriate countermeasures, for example, by specifying operational environment in the functional specification or guidance documents. The evaluator confirmed the accuracy of the vulnerability analysis by conducting independent vulnerability analysis.

From the vulnerability analysis, it is confirmed that the TOE, in its intended environment, has no vulnerability exploitable by attackers possessing low attack potential.

Thus, based upon the developer/evaluator's vulnerability analysis and the evaluator's penetration testing, it is confirmed that there are no flaws or weaknesses of the TOE that are exploitable in its intended environment.

10. Recommendations

- The user who accesses the TOE using the security code shall have it securely. If he loses it, he must report the fact to the security administrator and get the new security code. The security administrator shall change the security code in terms of the security policies of organization by periods and then distribute it securely.

- The product registers the system administrator and ordinary users in same security level, so whenever the security administrator registers them, must be careful and grants the security level correctly according to their adequate security level. Therefore, before granting the security level, the security administrator should determine the standard of security policies, then permit the user's clearance and category.
- The port control function in this product provides the default policy as all port being 'disable' except some necessary port(11102(TCP), 4001(UDP) port for communicating between REDOWL Enterprise and Manager) to operate the product. Therefore, the security administrator should re-configure the port policy for the organization.
- The product provides the function sending mail to the security administrator whenever the storage space is arrived in the limit space. So, the security administrator must check the storage media and make more space.

11. Acronyms and Glossary

The following acronyms are used in this certification 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 terms are used in this certification report.

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

Audit record
Audit data to save an auditable event relevant to the security of the TOE

User
Any entity (either human or external IT entity) outside the TOE that interacts with the TOE

Authorized administrator
Authorized user that can manage the TOE in accordance with the TSP

Authorized user
User that can run functions of the TOE in accordance with the TSP

Identity
A representation uniquely identifying an authorized user

External IT entity
Any IT product or system, either trusted or untrusted, outside the TOE that interacts with the TOE

Assets
Information and resources to be protected by the security measures of the TOE

Daemon
A process that runs in the background and respond periodical service requests

NTP
An internet standard protocol that assures accurate synchronization to the millisecond of computer clock times in a network of computers

12. References

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

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

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

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

[4] Korea IT Security Evaluation and Certification Guidance (May. 21, 2005)

[5] Korea IT Security Evaluation and Certification Scheme (Dec. 26, 2005)

[6] REDOWL SecuOS V4.0 for RHEL4 Security Target V1.1 (May. 20, 2006)

[7] REDOWL SecuOS V4.0 for RHEL4 Evaluation Technical Report, V1.00 (Dec. 14, 2006)