KECS-CR-07-12

V3Pro2004 and AhnLab Policy Center 3.0 Certification Report

Certificate Number: KECS-ISIS-0073-2007

August 2007

National Intelligence Service
IT Security Certification Center

Revision History

No.	Date	Page	Contents
00	09.17.2007	-	First Draft

This document is the certification report on V3Pro2004 and AhnLab Policy Center 3.0 of AhnLab, Inc.

Certification Body

National Intelligence Service IT Security Certification Center

Evaluation Body

Korea Information Security Agency

Table of Contents

1. Executive Summary ····· 4
2. TOE Identification ····· 6
3. Security Policy ····· 7
4. TOE Assumptions and Scope ····· 8
4.1 Assumptions ····· 8
4.2 Threats ····· 10
5. TOE Information ····· 13
6. Guidance ····· 15
7. TOE Test ····· 16
7.1 Developer Testing ····· 16
7.2 Evaluator Testing ····· 17
8. Evaluated Configuration ····· 18
9. Evaluation Result ····· 18
10. Recommendations ····· 23
11. Acronyms and Glossary ····· 25
12. References ····· 26

1. Executive Summary

This report documents the certification result of the EAL4 evaluation of V3Pro2004 and AhnLab Policy Center 3.0 with regard to the Common Criteria for Information Technology Security Evaluation (Announcement No. 2005-25 by Ministry of Information and Communication; CC hereinafter). It presents the evaluation results, their validation, and the conformance results.

The Korea Information Security Agency (KISA) has finished the evaluation of V3Pro2004 on the 17th of Aug. 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 the EAL4 of the part 3 assurance requirements; thus, it is assigned the verdict 'pass' on the basis of the paragraph 175 of the CC part 1.

The TOE consists of V3Pro2004 (Hereinafter referred to as V3), the anti-virus program that performs virus scan/repair function, and the V3 management server program, AhnLab Policy Center (Hereinafter referred to as APC). The APC consists of Policy Center Admin, Policy Server, and Policy Agent which is installed on the V3 installed system and transfers administrator's commands from the server to V3. V3, Policy Center Admin and Policy Agent are software installed and operated on the Windows XP, and Policy Server is installed and operated on the Windows 2003 Server.

The management server, APC, provides centralized management for V3. APC transmits and enforces configurations for the scan/repair function to each V3.

The centralized management software, APC, manages V3 in 3-tiered architecture transmitting encrypted administrator's commands to V3.

Policy Center Admin is installed on the administrator's PC transmitting V3 scan/repair policies and Agent security management policies to Policy Server in a secure manner.

Policy Server stores V3 and Agent management polices in the LDAP, audit data from V3, APC, and administrator command history in DBMS. Policy Server forwards administrator's commands to Policy Agent, and handle requests from Policy Agent to send the polices to V3.

Policy Agent is installed on the V3 installed system and runs in active mode or passive mode. In active mode, Policy Agent requests V3 and Agent policies to Policy Server periodically, applies Agent policies to itself, and forwards V3 policies to V3. According to the audit data forwarding policy, Policy Agent forwards V3 audit data to Policy Server. In passive mode, Policy Agent operates only the administrator's commands from Policy Server.

The certification body has examined the evaluation activities and testing procedures of the evaluator; provided the guidance regarding the technical problems and evaluation procedures; reviewed each evaluation work package and the evaluation technical report.

The certification body has confirmed that the evaluation results assure that the TOE meets all of the security function requirements and assurance requirements described in the ST.

As a result, the certification body has certified that the observations and evaluation results by the evaluator are accurate and reasonable; and that each verdict on each work package of the evaluator is correct.

Certification Validity: The information in this report guarantees that V3Pro2004 obtained neither approval for use nor quality assurance from the Government Agency of the Republic of Korea.

2. TOE Identification

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

[Table 1] TOE Identification

Evaluation Guidance	Korea IT Security Evaluation and Certification Guidance (2005. 5. 21) Korea IT Security Evaluation and Certification Scheme (2007. 4. 15)
TOE	V3Pro2004 and AhnLab Policy Center 3.0
Protection Profile	None
Security Target	V3Pro2004 and AhnLab Policy Center 3.0 ST V1.7
ETR	V3Pro2004 and AhnLab Policy Center 3.0 ETR, V1.00
Conformance Result of the Evaluation	Conformance to the CC V2.3 part 2 Conformance to the CC V2.3 part 3
Evaluation Criteria	Common Criteria for Information Technology Security Evaluation (2006. 5. 21)
Evaluation Methodology	Common Methodology for Informations Technology Security Evaluation V2.3 (2005. 8)
Sponsor	AhnLab, Inc.
Developer	AhnLab, Inc.
Evaluators	KISA IT Security Evaluation Center, Evaluation Team 2 Kwonhyun Cho, Eunkyeong Yi, Sungjae Lee
Certification Body	National Intelligence Service

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

[Table 2] V3 Net Operating Environment

TOE		Software	Hardware (Recommended)
V3		Microsoft Windows XP Internet Explorer 6.0 or higher Winsock 2.0 or higher	CPU: Intel Pentium III or higher RAM: 256MB HDD: 200MB or more NIC: 10/100 Ethernet Card
APC	Policy Agent	Microsoft Windows XP Winsock 2.0 or higher Internet Explorer 6.0 or higher	CPU: Intel Pentium III or higher RAM: 256MB HDD: 200MB or more NIC: 10/100 Ethernet Card
	Policy Server	Microsoft Windows 2003 Server MS SQL SERVER 2003 SP3 or higher OpenLDAP 2.0 or higher Winsock 2.0 or higher	CPU: Intel Pentium 1GHz or higher RAM: 1GB or more HDD: 5GB or more NIC: 10/100 Ethernet Card
	Policy Center Admin	Microsoft Windows XP Winsock 2.0 or higher Internet Explorer 6.0 or higher	CPU: Intel Pentium 1GHz or higher RAM: 256MB or more HDD: 200MB or more NIC: 10/100 Ethernet Card

3. Security Policy

The TOE operation conforms to the security policies as follows:

P.ROLES The TOE provides authorized security management roles to manage the TOE in a secure manner: server administrator, policy administrator, monitor center, authorized general user, and restricted general user. These roles shall be separated clearly from other users.

P.AUDIT To Trace responsibilities of all security-related behaviors, all security-related events shall be stored, maintained, and the record data shall be reviewed in a variety ways.

P.MANAGEUTIL Management tools are provided for authorized general users (V3) or authorized administrator (APC) to manage the TOE in a secure manner, and V3 policies set by authorized administrators has higher priority than by authorized general user.

P.ANTIHARMFULL The TOE shall scan key logger programs defined as harmful program by AhnLab, Inc.

P.STRENGTHENOS Authorized general users or authorized administrators shall review the vulnerabilities to guarantee the normal operation and stability by reinforcement of vulnerabilities of the operating system and applications which are necessary to run the TOE.

4. TOE Assumptions and Scope

4.1 Assumptions

The TOE installation and operation shall be conformance to the assumptions as follows:

A.NO_EVIL	The authorized general users (V3) and authorized administrators (APC) of the TOE shall not have any malicious intention, receive proper training on TOE management, and follow the user (V3)/administrator (APC) guidelines.
A.PHYSICAL	The policy server is installed in physically safe environment, and protected by un-authorized access.
A.SAFEITENTITY	The update server for the TOE, administrator's computers for security management functions, and the NTP server are secure.
A.TIMESTAMP	The time stamp referred to the NTP server or operating system is reliable.
A.CERT	The certificate being used to verify engine/patch files from the update server are issued in a secure manner and stored/managed by AhnLab, Inc. To verify engine/patch files signed by the certificate, the reliable authentication agency of the Internet Explorer on the V3 or policy server installed system must be up-to-date.

A.GUARD	The TOE is installed on the trusted network where is protected by network security devices (firewall). The trusted network is protected by the security policies of network security devices.
A.INTERNALENTITY	IT entities connected to the trusted network and interoperate with the TOE are run with the same security level according to the security policies of network security devices.
A.AVCONFILICT	The V3 installed system does not have any other anti-virus software, and software with POP3 real-time scan (monitoring), and spam mail filtering.

4.2 Threats

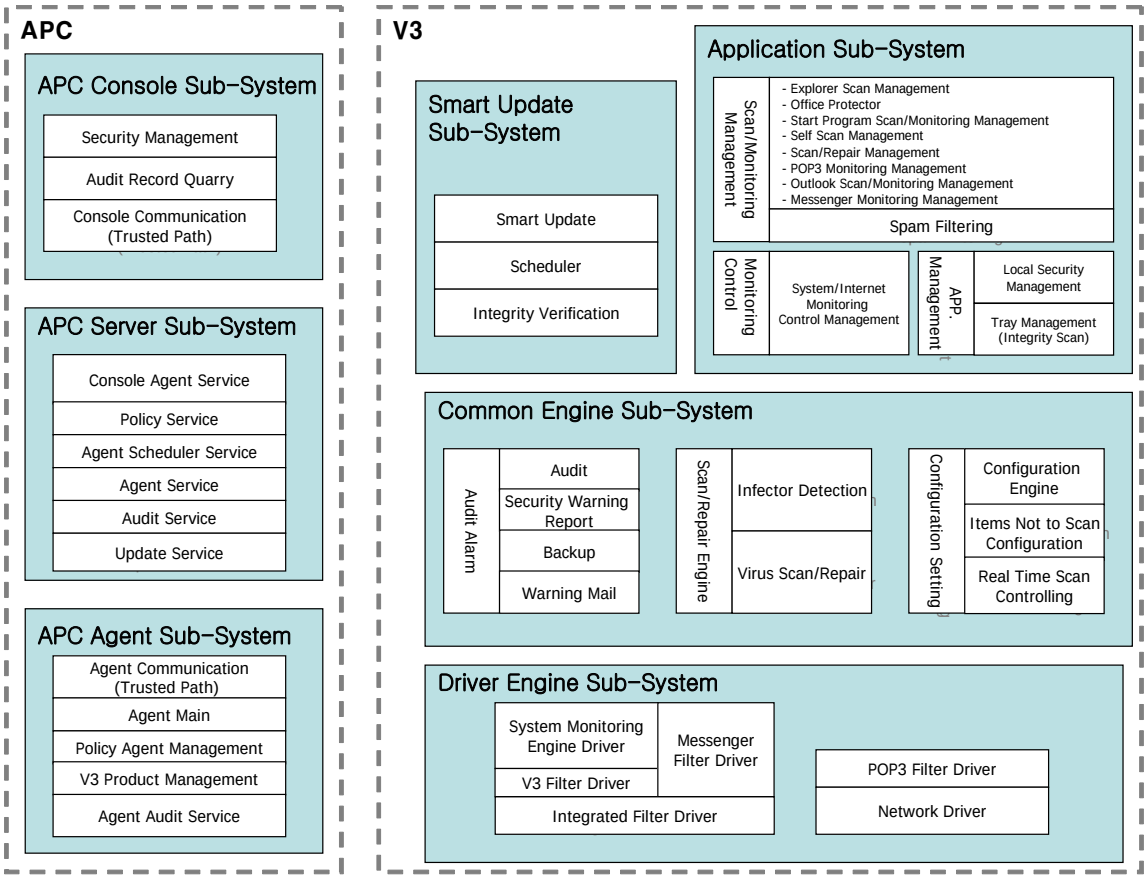
All security objectives and security policies are described to provide means to counter identified security threats.

Objective	Description
O.ADMIN_ROLE	The TOE shall provide security management roles to separate management behaviors.
O.MANAGE	The TOE shall provides secure means and management functions for authorized general users (V3) or authorized administrators (APC) to efficiently manage the TOE.
O.SELF_PROTECTION	The TOE shall provide protect TSF and TSF resource from unauthorized modification via TSFI.
O.VIRUS	The TOE shall identify and response for well-known viruses that come from removable media or network traffic.
O.AUDIT	The TOE shall provide store and maintain security-related events to trace responsibilities of security-related behaviors, and provide means for the authorized users to review the audit data.
O.ALARM	The TOE shall provide methods to alert authorized general users and authorized administrators for security threats.
O.TSFDATA_PROTECT	The TOE shall protect TSF data transmitted between separated TOEs from the exposure and modification.
O.INA	The TOE shall identify and authenticate authorized administrators (APC).
O.SECURE_UPDATE	The TOE shall store engine/patch files from the update server, check their integrity, and verify whether they are developed by AhnLab, Inc.
O.STRENGTHENOS	The TOE shall provides means to review if vulnerabilities to guarantee the normal operation and stability, and the reinforcement of vulnerabilities of the operating system and applications which are necessary to run the TOE.
OE.AUDIT_STORAGE	The IT environment shall provide means to store audit files of the TOE in a secure manner.
OE.NO_EVIL	The authorized general users (V3) and authorized administrators (APC) of the TOE shall not have any malicious intentions, receive proper training on the TOE management, and follow the user (V3)/administrator (APC) guidance.
OE.PHYSICAL	The TOE shall be located in a physically safe environment, and protected from the unauthorized access.

Objective	Description
OE.CERT	The certificate being used to verify engine/patch files from the update server is issued in a secure manner and stored/managed by AhnLab, Inc. To verify engine/patch files signed by the certificate, the reliable authentication agency of the Internet Explorer on the V3 or policy server installed system must be up-to-date.
OE.SAFEITENTITY	The update server for the TOE, administrator's computers for security management functions, and NTP server (or operating system providing the time stamp) shall secure.
OE.TIMESTAMP	The IT environment shall provide reliable time stamps from the NTP server or the operating system.
OE.TOE_ACCESS	The IT environment shall provide means to control logical access of users to the TOE.
OE.GUARD	The TOE is installed on the trusted network where is protected by network security devices (firewall). The trusted network is protected by the security policies of network security devices.
OE.INTERNALENTITY	IT entities connected to the trusted network and interoperate with the TOE are run with the same security level according to the security policies of network security devices.
OE.AVCONFLICT	The V3 installed system does not have any other anti-virus software, and software with POP3 real-time scan (monitoring), and spam mail filtering.
OE.AUDIT_SEARCH	The IT environment shall provide the search function for the audit records.
OE.RESIDUAL_INFO	The IT environment shall protect resources in the scope of control of the TOE from exposing them to users when re-allocating the memory.
OE.DOM_SEPARATION	The IT environment shall provide separated areas for executing of the TOE.
OE.NO_BYPASS	The IT environment shall not allow the bypass of the security mechanisms since the access authority to the TOE resource can be taken.

5. TOE Information

The TOE provides security functions such as virus scan/repair with the following subsystems.



[Figure 2] Subsystems of the TOE

The Application subsystem provides the authorized user interface (security management screen) to perform security functions of V3, and operates management function to scan/monitor viruses on the system with configuration by general users. The application subsystem requests scan/repair viruses to the common engine subsystem with the request by the plug-in scan on each application (Office Protector, Outlook) or the manual can request by authorized users. The application subsystem also requests to scan/repair its own execution files, and checks the integrity of executable files or configuration files of itself at startup. The subsystem provides not only the scan/repair function but also the port block function.

The common engine subsystem applies configurations from users and the APC Server subsystem and security management command (from APC Agent subsystem) to the system. It also scans and repairs viruses, backs the original infection files up, generates audit records, and scans system vulnerability.

The Driver Engine subsystem monitors the file systm on the V3 installed system,

and when an I/O event occurs on a file, the subsystem scans the file in real-time. V3 registers the information of the monitoring target to the filter driver to support system/Internet/ instant messenger monitoring. After register, the subsystem hooks the data up in case that the transmitting data is scan target. The hooked data by system/Internet monitoring is scanned/repaired. Besides, the subsystem performs the port block function filtering traffic based on the port information.

The Smart Update subsystem applies the smart update configurations from authorized general users to the system, and handles update requests. Depending on the update configuration, update files are downloaded from the Internet or network shared folders. Once completing download, integrity scan operates, signatures and patch files are updated. At startup of the operating system, the subsystem requests the operating system to execute real-time scans. The scheduler function runs scheduled scan, screen saver scan, and real-time system scan according to their scheduled time, checking for their scheduled time periodically.

The APC Console subsystem transmits policies from authorized administrators to the APC server subsystem, and displays the result. To provide the secure channel for the communication, transmitting data are encrypted (except audit data) with embedding the integrity value. Authorized administrators are allowed to queries audit records of APC and V3.

The APC Server subsystem handles commands or policies from authorized administrators. The subsystem exchanges a key for the secure channel with the APC Console subsystem, identifies and authenticates administrators. Direct-commands from the APC Console subsystem are stored in DB and forwarded to the APC Agent subsystem. The results of commands from the APC Agent subsystem are forwarded to the APC Console subsystem. The subsystem stores policies of V3 and the policy agent in LDAP, and sends the command to the APC Agent subsystem to apply the policies. The subsystem stores audit data from APC to DBMS. If V3 requests updates, the subsystem sends the patch/engine files of V3 from the update server.

The APC Agent subsystem forwards new or urgent policies from APC server subsystem to V3. By scheduler, the APC Agent subsystem get policies or update information from APC Server subsystem, updates its status on a specific time. If policy Agent installation program or V3 is installed, the APC Agent subsystem registers its own status to APC Server subsystem. Data encryption (except audit records) integrity is provided for the secure channel with the APC Server subsystem. The APC Agent subsystem transmits audit records of V3 which are filtered by log filtering rules to the APC Server subsystem.

6. Guidance

The TOE provides the following guidances:

- V3Pro2004 User Guide V6.0.10
- AhnLab Policy Center 3.0 User Guide V3.0 3.0.11

7. TOE Test

7.1 Developer Testing

- **Test Method**

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

- Test No./Tester : The identifier of the test and the developer who participated in testing

- Test Purpose : Describe the purpose of the test including security function or modules of the test

- Test Configuration : Detailed test configuration to carry out the testing

- Test Procedure : Detailed procedure to test the security function

- Expected Result : The expected test result when carrying out the test procedure

- Actual Result : The test result when carrying out the test procedure

- Comparison: The result of comparison between the expected and the actual result

The evaluator evaluated the validity of the test reviewing the test configuration, test procedure, test scope analysis of the test documentation and testing low-level design. The evaluator also assured that the developer's test and test results are 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, PCs, application servers (web server and mail server), and evaluation tools.

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

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

- **Test Result**

The test documentation describes the expected and actual result of each test. The actual result can be verified using not only GUI of the TOE but also the audit record.

7.2 Evaluator Testing

The evaluator installed the TOE by using the evaluation configuration and tools identical to the developer testing, and tested all of test cases provided by the developer. The evaluator assured that the actual test result was identical to the expected result.

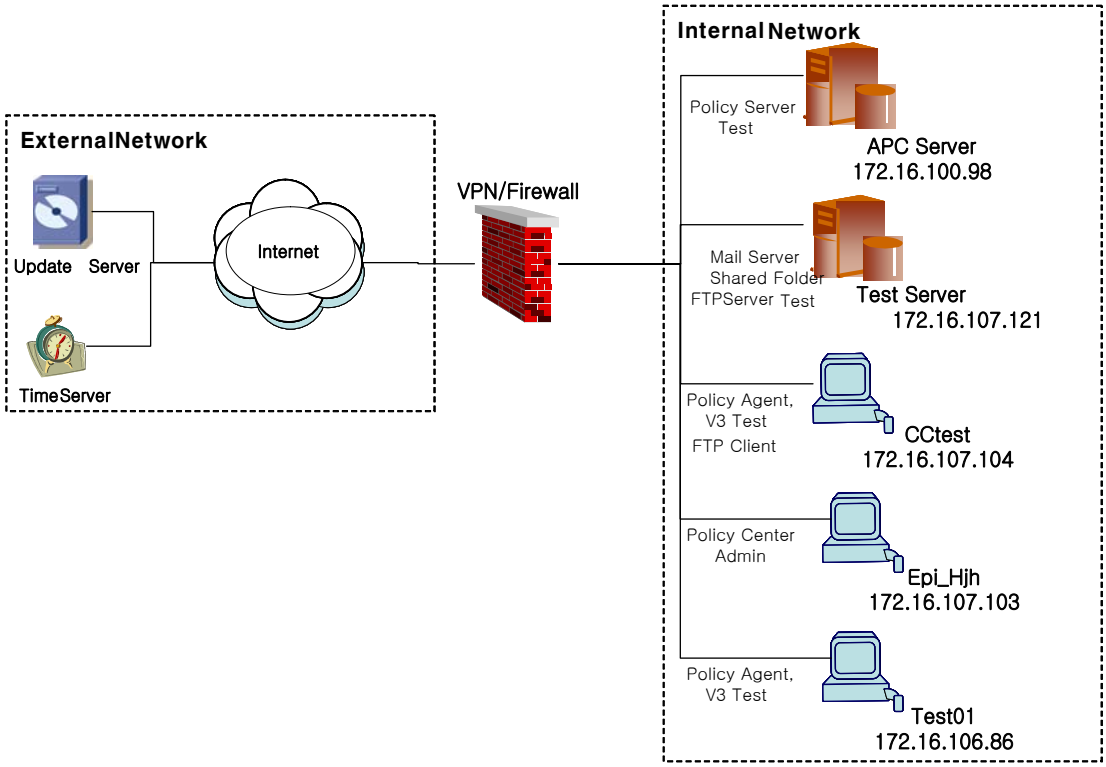
In addition, the evaluator created additional evaluator test cases on the basis of developer test, and verified that the actual test result was identical to the expected one.

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

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

8. Evaluated Configuration

The network configuration for the evaluation is separated into the external and internal network. The following hardware is used for the evaluation configuration;



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

9. Evaluation Result

The latest the Common Criteria for Information Technology Security Evaluation and Common Methodology for Informations Technology Security Evaluation are applied to the evaluation (June 2006). It concludes that the TOE satisfies the CC V2.2 part 2 and EAL4 of the CC V2.2 part3 assurance requirements. The detailed information regarding the evaluation result is described in the ETR.

- ST Evaluation (ASE)

The evaluator applied the ASE sub-activities described in the CC to the ST evaluation.

The introduction of the ST is completed, consistent with other parts of the ST, and identified the ST accurately. The TOE description is coherent and consistent internally and with the other parts of the ST.

The statement of TOE security environment provides a clear and consistent definition of the security problem as assumptions, threats, and organizational security policies and describes them completely and consistently. The security objectives counter the identified threats, achieve the identified organizational security policies and are consistent with the stated assumptions.

The security requirements for the IT environment are described completely and consistently, and they provide an adequate basis for 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 that these satisfy the specified TOE security requirements. The ST is a correct insanitation of PPs for which compliance is being claimed.

The ST is completed, consistent and appropriate in a technical way. Consequently, it is adequate for TOE evaluation to use the ST as the fundamental material.

- Configuration Management Evaluation (ACM)

The evaluator applied the ACM sub-activities described in the CC to configuration management evaluation of the TOE. It is confirmed that developers use an automated tool for controlling the modification of the implementation representation in the configuration management documentation. Developers identified the TOE and configuration list for the TOE accurately, and the ability to modify them was controlled adequately in the configuration management documentation. The configuration management documentation described that configuration management was performed for TOE implementation representations, evaluation evidences which are requested by assurance components of the ST, and security faults.

Consequently, the configuration management documentation allows consumers to identify the evaluated TOE, guarantees that the configurations are identified uniquely, and the procedure used to control and trace the TOE modification is appropriate.

- Delivery and Operation Evaluation (ADO)

The evaluator applied the ADO sub-activities described in the CC to the delivery and operation evaluation. The delivery documentation describes all procedures used to maintain security and detect modification or substitution of the TOE when distributing the TOE to the user's site. The documentation included secure installation, initialization, generation, and start-up procedures of the TOE, and as a result, the TOE confirmed the establishment of the secure environment.

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

- Development Evaluation (ADV)

The evaluator applied the ADV sub-activities described in the CC to the development evaluation. The functional specification provides an adequate description of TOE security functions which are sufficient to satisfy the security functional requirements of the ST. This also provides an adequate description of the TOE external interfaces. The security policy model describes the rules and characteristics of the security policies clearly, and consistently, mapping them into security functions in the functional specification.

High-level design provides a description of the TSF in terms of major structure units, subsystems, and of the interfaces to these structural units, and correct realization of the functional specification. Low-level design provides a description of the internal operation of the TOE security functions with interrelationships and dependencies on the other modules. The low-level design is sufficient to satisfy the functional requirement of the ST, and is a correct and effective refinement of the high-level design.

The implementation representation is sufficient to satisfy the functional requirements of 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 of the ST, functional specification, high-level design, and low-level design in the implementation representation.

Consequently, functional specification describing TOE external interfaces, high-level design describing TOE in terms of subsystems, low-level design describing the TOE structure in terms of internal modules, implementation representation which is the description of the source code level, and the

representation correspondence ensuring the consistency of these TOE representation methods are adequate to understand how the TOE security functions are provided.

- Guidance Evaluation (AGD)

The evaluator applied the AGD sub-activities described in the CC to the guidance evaluation. The administrator guidance provides a description of management of the TOE in a secure manner. Consequently, the user guidance describe how to use the TOE which is managed by the administrator.

- Life Cycle Support Evaluation (ALC)

The evaluator applied the ALC sub-activities described in the CC to the life cycle support evaluation. It was ensured that the developer's security controls on the development environment were adequate to provide the confidentiality and integrity of the TOE design and implementation. The developer used the documented TOE life cycle model and well-defined development tools to yield consistent and predictable results.

Consequently, documentations related to life cycle support describe procedures the developer uses during the development and maintenance of the TOE adequately including the security procedures and tools used throughout TOE development.

- Tests Evaluation (ATE)

The evaluator applied the ATE sub-activities described in the CC to the test evaluation. Tests were sufficient to demonstrate that TOE security functions are performed as specified in the functional specification on the tests. It was confirmed that the developer performed TOE security function tests for the high-level design. The test documentation of the developer was sufficient to ensure that the security functions were performed as specified. The evaluator confirmed that the TOE operated as specified by performing independent tests, and gained reasonable confidence from the developer testing by performing routine tests.

Consequently, independent testing of parts of TOE security functions verified TOE security functions run as specified in the design documentations and TOE security functional requirements in the ST.

- Vulnerability Evaluation (AVA)

The evaluator applied the AVA sub-activities described in the CC to the vulnerability evaluation. The misuse analysis of the guidance verified that the guidance is not misleading, unreasonable or conflicting, whether secure procedures for all modes of operation have been addressed, whether use of the guidance will facilitate prevention and detection of insecure TOE states. Strength of function claimed for all probabilistic or permutational mechanism in the ST, and developer's SOF claim made in the ST is supported by an analysis that is correct.

The vulnerability analysis documentation describes the measures appropriately by implementing the measures of the obvious vulnerabilities of the TOE or specifying the operating environment in the guidances. The evaluator verified the correctness of the vulnerability analysis by independent vulnerability analysis. The vulnerability analysis verified that the TOE, in its intended environment, has no vulnerabilities exploitable by attackers possessing low attack potential.

Consequently, the vulnerability analysis by the developer or evaluator or penetration testing by the evaluator verified that vulnerabilities exploitable by attackers possessing low attack potential do not exist.

10. Recommendations

① The authorized general users (V3Pro2004) and authorized administrators (APC Server) of the TOE shall not have any malicious intention, receive proper training on TOE management, and follow the user (V3Pro2004)/administrator (APC) guidelines.

② The policy server is installed in physically safe environment, and protected by un-authorized access.

③ The update server for the TOE, administrator's computers for security management functions, and the NTP server are secure.

④ The time stamp referred to the NTP server or operating system is reliable.

⑤ The TOE is installed on the trusted network where is protected by network security devices (firewall). The trusted network is protected by the security policies of network security devices.

⑥ IT entities connected to the trusted network and interoperate with the TOE are run with the same security level according to the security policies of network security devices.

⑦ The certificate being used to verify engine/patch files from the update server are issued in a secure manner and stored/managed by AhnLab, Inc. To verify engine/patch files signed by the certificate, the reliable authentication agency of the Internet Explorer on the V3 or policy server installed system must be up-to-date.

⑧ The V3Pro2004 installed system should not have any other anti-virus software, and software with port filtering to run the TOE normally.

⑨ Policy Agent runs in active or passive mode. In active mode, Policy Agent requests V3 and Agent policies to Policy Server periodically, applies Agent policies to itself, and forwards V3 policies to V3. According to the audit data forwarding policy, Policy Agent forwards V3 audit data to Policy Server. In passive mode, Policy Agent operates only the administrator's commands from Policy Server. If the administrator does not set the V3 security lock with Policy Agent in passive mode, it is out of scope of the evaluation because it is not enterprise environment, the TOE operating environment. Therefore, the administrator must run Policy Agent in active mode or passive mode with setting V3Pro2004 security lock.

⑩ The operating system provides identification and authentication because the general user of V3Pro2004 is a system account user. Therefore, the user on the V3 installed Windows system must use the secure password and manage it in a secure way.

11. Acronyms and Glossary

The following acronyms are used in the 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 glossary are used in the certification report.

TOE	An IT product or system and its associated guidance documentation that is the subject of an evaluation
Audit Record	Audit data to save an auditable event relevant to the TOE security
User	Any entity (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
Authentication Data	Information used to verify the claimed identity of a user
External IT Entity	Any IT product or system, untrusted or trusted, outside of the TOE that interacts with the TOE
Asset	Information and resources to be protected by the countermeasures of a TOE
Daemon	A process that runs in the background and respond periodical service requests

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] Korea IT Security Evaluation and Certification Guidance (May. 21, 2005)
[4] Korea IT Security Evaluation and Certification Scheme (April. 15, 2007)