KECS-CR-06-19

INFOSEC Technologies Co., Ltd.
TESS TMS v4.5
Certification Report

Certification No.: KECS-NISS-0059-2006

December 2006

National Intelligence Service
IT Security Certification Center

This document is the certification report on TESS TMS v4.5 of the INFOSEC Technologies Co., Ltd.

Certification Body

National Intelligence Service IT Security Certification Center

Evaluation Body

Korea Information Security Agency (KISA)

Table of Contents

1 SUMMARY 1

2 TOE IDENTIFICATION 3

3 SECURITY POLICY 5

4 ASSUMPTIONS & SCOPE 6

4.1 ASSUMPTIONS 6

4.2 SCOPE TO COUNTER A THREAT 7

5 TOE INFORMATION 9

6 GUIDANCE 12

7 TOE TEST 13

7.1 DEVELOPER'S TEST 13

7.2 EVALUATOR'S TEST 14

8 EVALUATION CONFIGURATION 15

9 EVALUATION RESULT 15

10 RECOMMENDATIONS 19

11 ACRONYMS AND GLOSSARY 20

12 REFERENCE 22

1 Summary

This report is for the certification body to describe the certification result, which inspects the result and the conformance fo the EAL4 evaluation of TESS TMS v4.5 with regard to the Common Criteria for Information Technology Security Evaluation(hereinafter CC).

The evaluation on TESS TMS v4.5 was performed by KISA and was completed on December 7, 2006. The contents of this report were written based on the contents of the report submitted by KISA. In the evaluation, the product satisfies the demand of the CC part 2 and the EAL 4 of the CC part 3 assurance requirements as well as was evaluated to be "suitable" in accordance with Article 191 of the CC part 1. Also, the evaluated product meets V1.1 (Dec. 21, 2005), the PP of the network intrusion prevention system.

TESS TMS v4.5 is the software to provide the function of the intrusion prevention through the functions of the intrusion detection & interception and was developed by INFOSEC Technologies. The evaluation product can be installed as the in-line mode in the network section that should be protected while be managed by GUI (Graphic User Interface) of the dedicated console.

TESS TMS v4.5, the evaluation product, broadly consists of TESS TAS v4.5 that is the evaluation scope and TESS TMS Web v4.5 & TESS TMS Report v4.5 that are out of the scope. TESS TAS v4.5 consists of TESS TAS Sensor v4.5 (hereinafter TESS TAS Sensor), TESS TAS Manager v4.5 (hereinafter TESS TAS Manager), and TESS TAS Console v4.5 (hereinafter TESS TAS Console). While TOE is TESS TAS v4.5, the evaluation scope is restricted to TESS TAS Sensor, TESS TAS Manager, and TESS TAS Console consisting of TESS TAS v4.5.

Of security functions provided by the evaluation product, the security function below is included in the evaluation scope.

- Counter to the creation/inquiry/retrieval of the audit data & type of

audit data

- Judgment on the possible harmful data through the intrusion detection & packet filtering and protection of the network by properly countering to the packet judged as the harmful traffic
- Performance of identifying & certifying an administrator
- Security management function of querying or setting the attribute and information of each function provided by TOE
- Performance of the health check or integrity check to make TOE function normally
- Locking of the security management screen when deactivating the security management over a certain period of time
- Performance of safe communication through SSL between ingredients of TOE

Of security functions provided by the evaluation product, something that is outside the evaluation scope is like those below, refer to the security target for more details.

- Comprehensive Diagram
- Comprehensive Correlation Analysis
- Prediction/Alarm System

The certification body should check the evaluation activity of the evaluator & test procedure, provide guides for technical problems & evaluation procedure, and review each evaluation unit & contents of the evaluation report. The body confirmed that the evaluation product meets the requirements for all security functions and certification described in the security target through the evaluation result. Thus, the body certified that the observed items and the evaluation results were accurate and reasonable while the result on the possible conformance was correct.

Certification Effective Scope: The information that is included in this certification report doesn't mean that TESS TMS v4.5 (TOE: TESS TAS v4.5) is approved to use by the government body of Korea or the quality for TESS TMS v4.5 is guaranteed.

2 TOE Identification

[Table 1] is the information for the identification of the evaluation product & TOE.

[Table 1] TOE Identification

Evaluation Guide	Korea IT Security Evaluation and Certification Guidance (May 21, 2005) Korea IT Security Evaluation and Certification Scheme (Dec. 26, 2005)
Evaluation Product	TESS TMS v4.5
TOE	TESS TAS v4.5
Protection Profile	Network Intrusion Prevention System Protection Profile V1.1 (Dec. 21, 2005)
Security Target	TESS TMS v4.5 Security Target V6 (July 28, 2006)
ETR	TESS TMS v4.5 ETR, V1.0 (Dec. 7, 2006)
Evaluation Results	Satisfies the CC part 2 Satisfies the EAL4 of the CC part 3 assurance requirements
Evaluation Criteria	Common Criteria for Information Technology Security Evaluation V2.3(Aug. 2005)
Evaluation Methodology	Common Methodology for Information Technology Security Evaluation V2.3(Aug. 2005)
Sponser	INFOSEC Technologies Co., Ltd
Developer	INFOSEC Technologies Co., Ltd
Evaluataion Team	KISA Evaluation Center, Evaluation Team 1 Jae Young Ahn, Gyu Chul Song, Tae Seung Lee
Certification Body	National Intelligence Service

Underlying hardware specification of the TOE is stated in the [Table 2].

[Table 2] TESS TAS v4.5 Specification

Item			Specification
TESS TAS Sensor	Hardware	CPU	Intel Xeon 3.0G stepping 3 Dual
		Memory	DDR 2G or more
		Interface	Security Management: 1 Intel pro 10/100 Fast Ethernet Packet Collection: 2 Fast Ethernets
		HDD	64G or more
	Software	OS	InfosecOS V1.0 (Dedicated OS)
TESS TAS Manager	Hardware	CPU	Intel Xeon 3.0G stepping 3 Dual
		Memory	DDR 2G or more
		Interface	1 10/100 Fast Ethernet or more
		HDD	36G or more
	Software	OS	Windows Server 2003
TESS TAS Console	Hardware	CPU	Pentium4 2.4G
		Memory	DDR 1G or more
		Interface	1 10/100 Fast Ethernet or more
		HDD	36G or more
	Software	OS	Windows Server 2003

3 Security Policy

TOE is operated by observing the security policies below.

Name	Description
Audit	Security-related events should be written & maintained to trace the responsibility for the security-related activities while recorded data must be reviewed.
Security Manage	Authorized administrator should manage TOE safely
SSL Certificate Management	SSL certificate should be generated at the time of the installation, stored, and managed in a safe manner.

4 Assumptions & Scope

4.1 Assumptions

TOE should be installed and operated by observing the assumptions below.

Name	Description
A. Physical Security	TOE is located in physically secure environment where only authorized administrators are allowed the access.
A. Security Maintenance	When the internal network environment is changed due to network configuration changes, an increase or decrease of hosts, or an increase or decrease of services, the new changes are immediately noted and security policies are configured in accordance with the TOE operational policy to maintain the same level of security as before.
A. Trusted Administrator	Authorized person of TOE has no evil intention, is well educated about the TOE management function and performs the duty according to the administrator guide.
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. Single Connection Point	The TOE is installed and operated on a network and separates the network into external and internal network. Information cannot flow between the two without passing through the TOE.
A. Secure TOE External Server	The network time protocol (NPT) server which maintains a trusted time outside the TOE for security functions of the TOE and the update server which

	provides the latest attack pattern rules are secure. NTP is used to get the trustable visual information while the live update server is used to update the recent intrusion pattern rule.
A. SSL Certificate	For the safe communication, the certificate used in the SSL protocol is generated at the time of installation, and safely 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.
A DBMS	Intrusion detection & traffic data generated in TOE is stored in DBMS. The stored data can be safely managed by identification & certification method defined in DBMS itself. DBMS provides functions of the retrieval and inquiry of the stored intrusion detection & traffic data at the request of the administrator. DBMS is safely managed and operated by applying the advanced security & vulnerability-related patch.

4.2 Scope to Counter a Threat

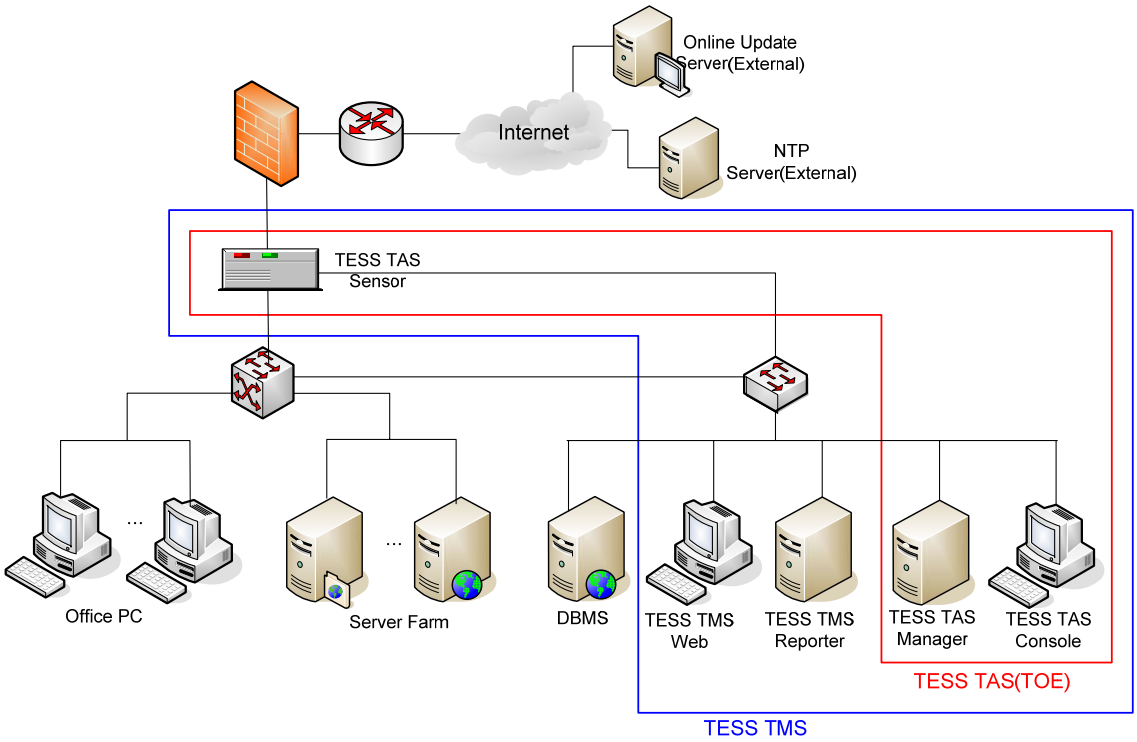
TOE provides the right method of countering to the security threats occurring in the IT environment requiring the thorough control as well as the attempt to intrude the main server which is the subject to be protected. TOE doesn't provide a way of countering to the direct physical attack that incapacitates or makes a detour around the security function. It gives the way of countering to the logical attack that is happened by the source of threats with a low level of technical knowledge and resource. Also, it provides the way of countering to such attacks as an access to TOE by mocking an authorized person, exhausting the storage capacity, service or anomalous packet attacks. It can't not bypass the counter to a series of attempts to certify and offered security functions while providing a way of

countering to the change in the TSF data without notice.

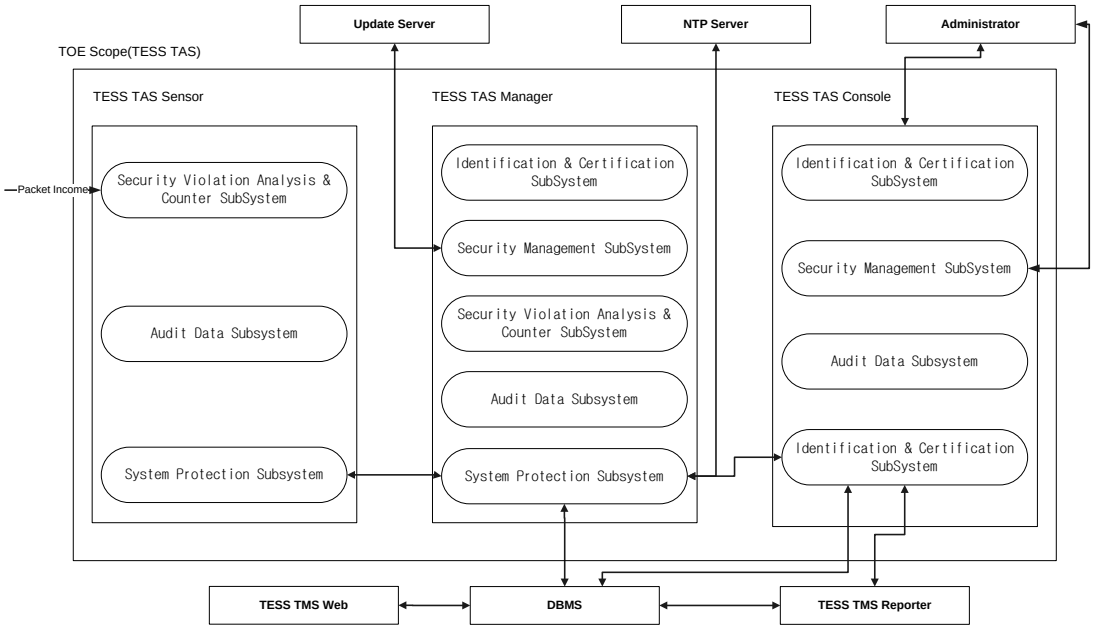
All security goals and security policies are described to respond to the identified security threats.

5 TOE Information

The evaluation product provides the intrusion prevention function. The product's operating environment is like [Figure 1] while its structure is like [Figure 2]



[Figure 1] TOE Operating Environment



[Figure 2] Basic Structure of TOE

The evaluation product consists of five subsystems, and main roles of each subsystem are as follows.

- Audit Data (S_AT)

The audit data subsystem is to generate the audit data, provide the retrieval function for the audit data, and perform the function of countering to the audit data.

- Security Violation Analysis & Counter (S_DP)

The security violation analysis & counter subsystem is to collect & condense the network packet and perform the protocol vulnerability analysis, session management, intrusion detection according to signature, intrusion detection in accordance with the statistical analysis while countering to every violation in a proper manner. The system also analyzes the traffic data and generates the statistics.

- Identification & Certification (S_IA)

The identification & certification subsystem is to provide the function of the identification and certification when the administrator logs in and to respond to a series of fails of the log-in in a good way. The system is

allowed to lock the console for a certain period of time when the administrator is not active, and to ask the recertification for the activation of the screen.

- Security Management (S_SM)

The security management subsystem is to manage the security functions provided by TOE and performs the function of managing the TSF data. The administrator is using the security management subsystem to manage the administrator account, security audit counter, signature list, packet filtering policy, integrity, administrator environment, sensor, host, and anomalous symptom policy.

- System Protection (S_PT)

The system protection subsystem is to check whether TOE is operating well and the possibility of damage of the integrity in the TSF data & executable code. The system also guarantees the safe communication by forming the safe channel between segments of TOS that is physically separated.

6 Guidance

The guidance document provided by the evaluation product is as follows.

- TESS TMS v4.5 Administrator Guidance V5, November 9, 2006
- TESS TMS v4.5 Delivery Documentation V5, November 8, 2006
- TESS TMS v4.5 Installation Manual V5, November 2, 2006

7 TOE Test

7.1 Developer's Test

- Test Method

The developer derived the test items given the security function of the product. Each item is well described in the test description. Each item also includes the detailed items below.

- Test No./Tester: Identifier of the test items & developer participating in the test
- Test Objective: Describe the test objective including the security function & security module for the test
- Test Configuration: Test environment for performing the test.
- Detailed Test Procedure: Detailed procedure for the security function test
- Expected Result: Test result that is expected when performing the test procedure
- Real Result: Test result when performing the test procedure
- Comparison of Expected Result & Real Result: Results gained by comparing the expected result with the real result

The evaluator evaluated the validity of the test like the test configuration, test procedure, test scope analysis, low-level design test, etc. The evaluator verified that the developer's test or test result is right for the evaluation configuration.

- Test Configuration

The test configuration described in the test description is including such detailed environment as test formation, TOE products, and internal & external networks. Other details are described like test tools so as to test each test item.

- Test Scope Analysis/Low-Level Design Test

The detailed evaluation result is described the evaluation result of ATE_COV & ATE_DPT.

- Test Result

The test description describes the expected result and real result of each item. The real result can be confirmed through not only the working screen but also audit records.

7.2 Evaluator's Test

The evaluator installed the evaluation product using the same evaluation configuration & evaluation tool as those of the developer's test, and tested the entire test items provided by the developer.

Also, the evaluator could confirm that the real result coincided with the expected result as a result of planning the extra evaluator's test items based on the developer's test.

As a result of the test on the vulnerability, the evaluator could confirm that any vulnerability could not be used in a malicious way in the evaluation configuration.

The test result of the evaluator guaranteed that the evaluation product was normally operated in accordance with what was described in the design document.

8 Evaluation Configuration

It was configured by separating the internal from the external network for the evaluation. The hardware below was used to configure the evaluation configuration.

- Computer: 8 Units (6PCs & 2Servers)
- CPU: Intel Xeon 3.0G stepping 3 Dual (Server), Pentium IV 1.5GHz or more (PC)
- RAM: Over 512MB
- HDD: Over 36GB

The Software blow was used to configure the evaluation configuration.

- Hancomm Linux 2.2
- Windows Server 2003
- Windows 2000 Server
- Windows XP Professional
- Oracle 9i

The test was progressed for all security functions provided by TOE, the evaluation configuration was configured in accordance with the detailed security attribute and environment setting method of each security function.

9 Evaluation Result

The evaluation applied CC and common evaluation methodology. The evaluation evaluated that the evaluated product satisfied the CC part 2 and the EAL 4 of the CC part 3 assurance requirements. More detailed evaluation results are described in the evaluation report.

- ST Evaluation (ASE)

The evaluator progressed the evaluation by applying the work unit of the ASE common evaluation methodology. ST (Security Target) described TOE in a

logical and consistent way matching well with other parts of the ST. The security environment provided the clear, exact definition of the security problems that were induced in TOE & TOE security environment, the security objective was well narrated in a complete, consistent way while satisfying the described assumptions. The security requirements for TOE security requirement & IT environment were completely, consistently described, providing the right base for the TOE development to meet the security objective. In the TOE summary specification, the security function and guarantee scale were well defined in a consistent way while meeting the narrated TOE security requirements. Also, the PP that was taken by the ST was exactly substantiated.

- Configuration Management Evaluation (ACM)

The evaluator progressed the evaluation by applying the work unit of the ACM common evaluation methodology. The configuration management indicated the configuration list, configuration identification method, version method, & configuration change control method, was developed by applying the configuration management system to all developed documents & source files while confirming that the configuration items were created and changed through the configuration management structure & configuration management system.

- Delivery & Operating Evaluation (ADO)

The evaluator progressed the evaluation by applying the work unit of the ADO common evaluation methodology. In the delivery & operating evaluation, the measure and procedure for the TOE's safe delivery, installation, and operation were described, the security was guaranteed not to be damaged during the transmission, installation, start and operation of TOE while the contents of the document were confirmed to be applied as a result of the actual company inspection.

- Development Evaluation (ADV)

The evaluator progressed the evaluation by applying the work unit of the ADV common evaluation methodology. In the development, the requirement for the TSF was well defined in a systematic and detailed way ranging from the TOE

summary specification of ST to the real implementation using function specification, basic design description, detail chart, representation of the implementation. Also, the security policy model was describing the rules and traits of the security policy to coincide with the description on the security function of the function specification.

- Guidance Document Evaluation (AGD)

The evaluator progressed the evaluation by applying the work unit of the AGD common evaluation methodology. The administrator guidance document describes the method for the administrator to access to the interface of the security management, and descriptions & notices for each menu provided by the interface by making good examples. In the guidance document, all described contents were confirmed to perform well. As a requirement for guarantee, at the same time, TOE was not demand the user guidance document so that the evaluation on it is impossible.

- Life Cycle Support Evaluation (ALC)

The evaluator progressed the evaluation by applying the work unit of the AGD common evaluation methodology. The life cycle support document described that security measures like the procedure & policy, tool & technique at the stage of the TOE development were used to protect the developing environment in a reasonable way while the contents of the document were confirmed to apply as a result of the actual company inspection.

- Test Evaluation (ATE)

The evaluator progressed the evaluation by applying the work unit of the ATE common evaluation methodology. The test description described the test objective, test procedure by state and test result for the security function indicated well in ST while foreshadowing the result. It could confirm that the test contents described in the test description was correct by repeating the test procedures like function test by process and interface test of the subsystem and that the operation of implemented security function in the course of the development was coincided. By performing the independent test of the evaluator, the developer's test turned out to be correct.

- Vulnerability Analysis (AVA)

The evaluator progressed the evaluation by applying the work unit of the AVA common evaluation methodology. The analysis and counter measures for the known vulnerability and possible misuse were described in the analysis report in a reasonable and correct way. By performing the independent test of the evaluator for the vulnerability, the developer's analysis turned out to be correct. In the strength analysis of the security function, the strength of the TSF met the level of the strength of function defined in the PP/ST.

10 Recommendations

- As time lapses until the counter rule is applied, allowing the attack packet to inflow into the internal network, the intrusion detection policy which detects things according to the setting of threshold should set the proper threshold through the tuning process considering the traits of the traffic in the protection network.

- TOE allows one administrator to implement the security management after he or she gains the security management control during the operation in order to prevent the asynchronous problem from occurring when administrators access at the same time. Thus, the administrator gains the control to use if necessary and should return it to others after using it.

- TOE provides the live update function to update the intrusion detection pattern when new vulnerability occurs, the administrator must keep the latest intrusion detection pattern through the periodic update.

- When TOE reaches the threshold as the storage for the audit records is depleted, it provides the administrator-notification function but the administrator should not depend on the function and has to continuously check the usage of the storage while securing it for the audit records.

11 Acronyms and Glossary

Abbreviations & terms below were used in the report.

(1) Abbreviation

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) Terms

TOE
IT products that are the targets of evaluation or system & related guidance document

Audit Record
The audit data to store the event records which are related to the security of TOE

User
All entities, users, external IT entities, etc. which are operating with TOE outside TOE

Authorized Administrator
The authorized user who safely manages TOE according to the TSP

Authorized User

The user who can perform the function in accordance with the TSP

Identity

The only expression to identify the authorized user

Certification Data

The information used to prove the identity of the user

External IT Entity

All safe or unsafe IT products or systems that are operating with TOE outside TOE

Assets

The information & resources that are protected by the security measures of TOE

Intrusion Protection System

The information protection product designed to keep the protection target network (or, internal network) away from the attack by detecting and intercepting the attack from outside

NTP

The protocol used to synchronize the clocks among computers that are connected to the network.

12 Reference

Certification body wrote the certification report by using the documents below.

[1] Common Criteria for Information Technology Security Evaluation V2.3

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

[3] Network Intrusion Prevention System Protection Profile V1.1 (Dec. 21, 2005)

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

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

[6] TESS TMS v4.5 Security Target V6 (July 28, 2006)

[7] TESS TMS v4.5 Evaluation Technical Report V1.0 (Dec. 7, 2006)