KECS-CR-06-16

Oullim Information Technology. ActiveTSM V3.0

Certification Report

Certification No. : KECS-ISIS-0056-2006

October 2006

National Intelligence Service

IT Security Certification Center

This document is a certification report on ActiveTSM V3.0 of Oullim Information Technology Inc.

Certification Body

National Intelligence Service IT Security Certification Center

Evaluation Facility

Korea Information Security Agency

Table of Contents

1. Executive Summary

This report describes the EAL4 evaluation results by certification body on Common Criteria for Information Technology Security Evaluation (published on This report describes the evaluation results, their appropriateness and suitability.

Evaluation of ActiveTSM V3.0 was performed by Korea Information Security Agency (KISA), which completed the evaluation on September 28, 2006. This report has been prepared based on the evaluation report of KISA. The evaluation confirms that the product satisfies the EAL4 evaluation guarantee grades of Part 2 and Part 3 of the Common Criteria and is assessed as 'satisfactory' based on Article 191 of Part I of the Common Criteria.

ActiveTSM V3.0 is an integrated Enterprise Security Management Agent System that provides overall control, operation and management based on a coherent enterprise security policy through collection and analysis of user activity data. Enterprise Security Management Agent Systems(hereinafter referred as 'Agent System') that are subject to security management of ActiveTSM V3.0 are server level systems that provide general security functions including IDS, F/W, IPS, general servers and network equipment.

TOEs of ActiveTSM V3.0 consist of Master, Slave, Monitor and Agents. TOE Agents collect data of Agent Systems using either SNMP or Syslog and delivers the data to the Slave. The Slave analyzes the collected data based on established policy and delivers the result to the Master. Admin performs security admin activities via the Monitor.

TOE provides the following major security functions:

- Security admin function where only authorized administrator is allowed to manage and operate the access control policy.

- Security audit function where the audit records are accessible only by authorized admin.

- Data protection function performed through access control policy and data receive security policy of Agent Systems.

- Identification and authentication function to ensure only trusted external IT entities and authorized admin have access to TOE.

- TSF protection function where security functions of TOE are checked periodically and any abnormal function is re-executed.

Security functions of the product that are not included in the evaluation scope are as follows. For further details, please refer to the Security Target Specification.

- Data management via Oracle 9i DBMS(Database Management System)
- Java RMI communication

The certification body verified the evaluation activities and test procedures of the evaluator, presented technical issues and the guideline for evaluation procedure, and reviewed contents of each evaluation unit and the evaluation report. The certification body affirm that the evaluation results confirmed that the subject product satisfies all security functional requirements and guarantee requirements described in the Security Target Specification. Therefore, the certification body certifies that the observations of the evaluator and the evaluation results are accurate and appropriate and the product assessment is accurate.

Scope of certification: The information contained in this certification report does not imply any authorization of use for ActiveTSM V3.0 by the Republic of Korea Government or its quality guarantee.

2. Identification

[Table 1] includes information for the subject product identification.

[Table 1] Identification Information

Evaluation Scheme	Guideline for evaluation & certification of information protection systems (2005. 5. 21) Regulations for evaluation & certification of information protection systems (2005. 12. 26)
TOE	ActiveTSM V3.0
Protection Profile Claims	N/A
Security Target	ActiveTSM V3.0 Security Target Version 1.8 (July 3, 2006), Oullim Information Technology Inc.
Evaluation Technical Report	ActiveTSM V3.0 Evaluation Technical Report, Version 1.1 (September 28, 2006)
Conformance Result	CC Part 2 Conformance CC Part 3 Conformance
Version of CC	CC V2.3, August 2005
Version of CEM	CEM V2.3, August 2005
Sponsor	Oullim Information Technology Inc.
Developer	Oullim Information Technology Inc.
Evaluation Facility	KISA Korea IT Security Evaluation Center (KISEC) Evaluation Team I Oh Yong-Seok, Lee Jae-Ro, Park Hyun-Mi
Certification Body	National Intelligence Service Republic of Korea (NIS)

ActiveTSM V3.0 scope for evaluation is only the software installed on the operating system. Master and Slave are installed and operated on SUN Solaris 9 OS and can be installed for operation on a system. Monitor is installed for operation on Windows 2000 Server (SP4) or Windows XP (SP2). Security admin activities are performed through the Monitor. Agent can be installed for operation on the Slave system but may be installed for operation on a Agent System in case the Agent System does not support either SNMP or Syslog.

Specifications for lower level hardware are as in [Table 2].

[Table 2] ActiveTSM V3.0 H/W & Lower Level Hardware Specification

Items			Specification
Distributed System	Master	CPU	1Ghz or higher
		Memory	1GByte or higher
		Interface	10/100 Ethernet Card 1 ea or more
		HDD	20GB or higher
		Operating Environment	SUN Solaris 9 for SPARC Java(v 1.4) VM DBMS - Oracle 9i
	Slave	CPU	1Ghz or higher
		Memory	1GByte or higher
		Interface	10/100 Ethernet Card 1 ea or more
		HDD	40GB or higher
		Operating Environment	SUN Solaris 9 for SPARC Java(v 1.4) VM Syslog, SNMP support DBMS - Oracle 9i
Integrated System	Master/Slave	CPU	1.5Ghz * 2 ea or more
		Memory	4GByte or higher
		Interface	10/100 Ethernet Card 1 ea or more
		HDD	73GB * 4 ea or more
		Operating Environment	SUN Solaris 9 for SPARC Java(v 1.4) VM Syslog, SNMP support DBMS - Oracle 9i
Monitor		CPU	1Ghz or higher
		Memory	1GByte or higher
		Interface	10/100 Ethernet Card 1 ea or more
		HDD	100MB or higher
		OS	Windows 2000(SP4) or Windows XP(SP2) Java(v 1.4) VM
Agent		CPU	300Mhz or higher
		Memory	128Mbyte or higher
		Interface	10/100 Ethernet Card 1 ea or more
		HDD	100MB or higher
		Operating Environment	SUN Solaris 9 for SPARC or Agent System OS Java(v 1.4) VM

3. Security Policy

The subject product shall comply with the following security policy:

Audit All security related events shall be logged and maintained to enable tracking accountability of security related actions and the log data shall be reviewed.

Safe management

Authorized admin shall manage TOE in safe methods.

Statistics The system shall allow authorized admin to conduct statistical processing of audit data and data generated from integrated security control activities.

4. Assumptions and Scope

4.1 Assumptions

The subject product shall be installed and operated in compliance of the following assumptions.

A. Dynamic Management

TOE shall be managed to enable appropriate handling of dynamic variations in Agent Systems.

A. Physical Security TOE shall be located in a physically safe environment where only authorized personnel can access.

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

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

A. Operating Environment Augmentation

Weaknesses of Java VM environment shall be augmented to ensure its reliability and safety.

A. Access Slave and Agent, components of TOE, shall have access to all Agent Systems for security control purposes.

A. Limitation of DB Installation

DBMS for TOE data management shall be installed in the same system where TOE is installed to ensure reliability and safety of the DB access.

A. Safe External Servers

Reliability and safety of the following servers, which reside outside of TOE in support of TOE functions, shall be ensured.
- SMTP server for sending mails to admin.
- SMS server for sending character messages to admin.

4.2 Scope of Threats to Counter

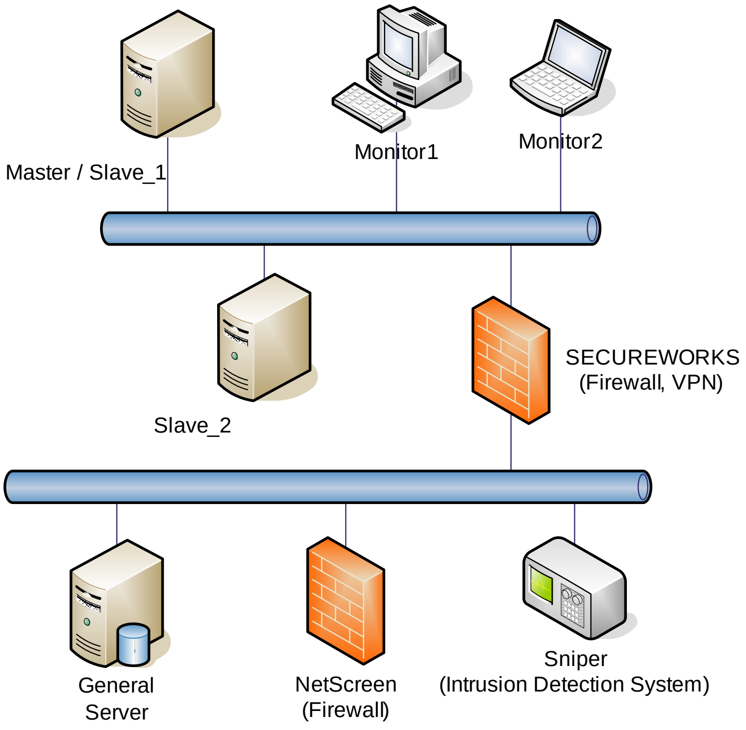
The subject product provides appropriate level of countermeasures against security threats in the IT environment required of TOE. However, it does not provide measures against direct physical attacks, which target abnormal operation of Agent Systems.

However, the subject product provides countermeasures against logical attacks from threat sources of low level knowledge, resources or motives from networks connected to the subject product. In addition, it provides countermeasures against attempts including admin disguised TOE access, depletion of storage capacity, attacks on services and abnormal packet attacks. It cannot handle repeated authentication attempts; does not circumvent security functions provided; but provides a measure against unauthorized editing of TSF data.

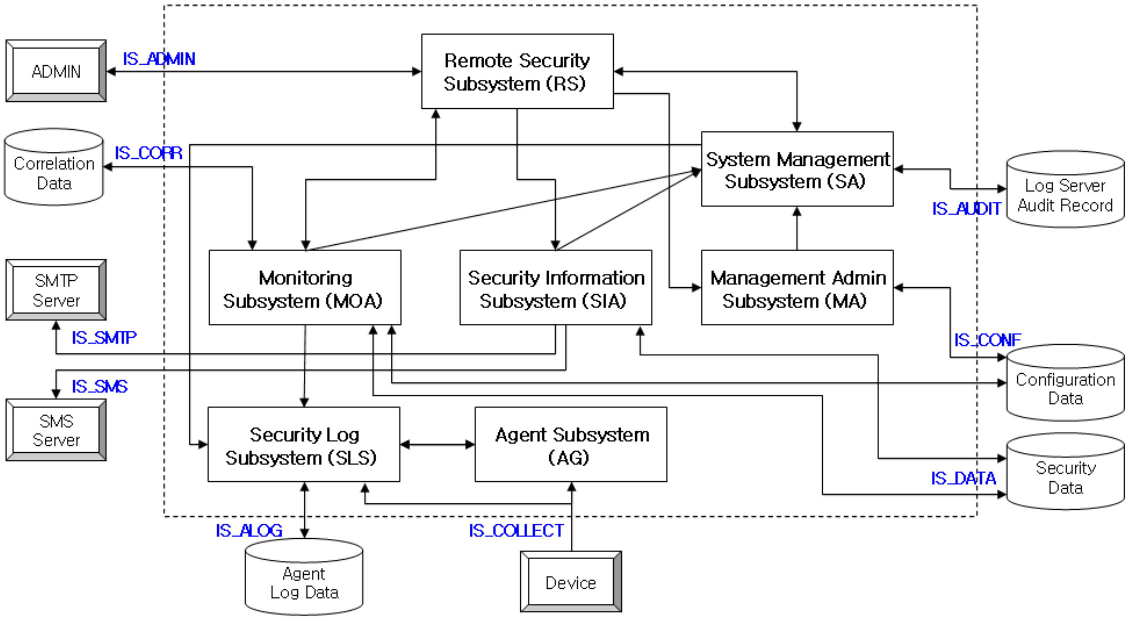
All security goals and policies are described to present countermeasures against identified security threats.

5. TOE Architecture

The subject product shall be installed at the point connected to Agent Systems within the internal network. Its operating environment is as in Figure 1 and the basic architecture as in Figure 2.



[Figure 1] ActiveTSM V3.0 Operating Environment



[Figure 2] ActiveTSM V3.0 Basic Architecture

The subject product consists of the following subsystems.

- Management Admin Subsystem (MA)

MA provides admin related information and functions. MA functions include Create, Edit and Delete of admin information as well as admin log-in and log-out. Admin information function includes automatic access freeze when the admin fails to succeed in admin authentication within three log-in attempts.

- Monitoring Subsystem (MOA)

MOA periodically collects and processes various security related information from Security Log Subsystem (SLS), then delivers this information to the admin via Remote Security Subsystem (RS), which provides various real-time monitoring functions. Also, the admin configures rules or configuration information for filtering, leveling and compression of SLS information within RS, where the MOA receives such information and stores it in a relevant DB and transmits to SLS for real-time application. In addition, MOA delivers admin requests for search results, which are delivered to RS via MOA.

- Security Information Subsystem (SIA)

SIA functions include analysis of collected security information and security control measures. SIA manages security related knowledge using information on attacks and viruses collected from control history data and external data. In addition, SIA processes admin requests for security performance and event trend reporting.

- System Management Subsystem (SA)

SA stores in DB audit records that are generated from creation, editing and deletion of security configuration information and TOE security log and error data; and processes admin requests for audit log data. SA selectively processes alarms based on importance levels of audit records. Other major functions include session management, fault-free test, system test, DB capacity test, system time setting and code management.

- Security Log Subsystem (SLS)

SLS is a Slave subsystem of TOE. It receives security related information from AG. SLS does not deliver this information directly to MOA, which is a part of TOE Master. Rather, MOA takes periodic information collected by SLS; stores it in the log DB; performs selective filtering, leveling and compression; and delivers the information to RS via MOA. When the admin requests search for security log data, the request is sent to SLS via MOA and the search result is delivered in the reverse order to RS.

- Agent Subsystem (AG)

AG functions include periodic collection of information from security related devices and their log information, which are delivered to SLS.

- Remote Security Subsystem (RS)

RS is a client subsystem, which does not directly perform most of the TOE functions but either requests security assignments to another subsystem or generates security processing output data. RS performs own fault-free test at initialization.

6. Guidance documents

Guidance documents provided by the subject product are as follows:

- ActiveTSM V3.0 Administrator guidance V1.4, June 18, 2006
- ActiveTSM V3.0 Installation guidance V1.6, July 24, 2006

7. IT Product Testing

7.1 Developer Test

- Test Method

The developer derived test items in consideration of the product's security functions. Test items are described in the test document and include the following:

- Test no. & tester: Test item ID number and the developer who participated in testing.
- Test objective: Describes test objective including security functions and modules for testing.
- Test environment: Detailed test environment for testing.
- Detailed test procedure: Procedures of security function testing.
- Expected results: Test results anticipated when test procedures are followed.
- Actual results: Test results from following specified test procedures.
- Comparison of results: Comparison between expected results and actual results.

The evaluator evaluated the suitability of tests including test environment, test procedures, test scope analysis and detailed design test. The evaluator verified that the developer's test and test results were satisfactory for the evaluation environment.

- Test environment

Test environment described in the test document includes details of test architecture, evaluation product, servers of TOE installation or Agent Systems. Also, it describes detailed test environment including test equipment required for testing of each test item.

- Test scope analysis/ detailed design test

Detailed evaluation results are described in ATE_COV & ATE_DPT Evaluation Results.

- Test results

The test document describes expected result and actual result of each test item. Actual results could be verified not only through the product's actual screen displays but also through audit log data.

7.2 Evaluator Test

The evaluator installed the subject product using the same evaluation environment and tools as those used in the developer tests and tested all of the test items provided by the developer. The evaluator confirmed that the actual results coincided with the expected results in all test items.

In addition, the evaluator devised separate evaluator test items based on the developer tests and confirmed that their actual results coincided with expected results.

The evaluator conducted vulnerability testing of the subject product and confirmed that no vulnerability of the subject product can be wrongfully misused under the evaluation environment.

The evaluator's test results guarantee that the subject product operates normally as described in its design documents.

8. Evaluation Configuration

The evaluator configured the following test environment consistent with the environment configuration specified in [ST].

- Servers: 2 ea. (For distributed system environment)
  - CPU: 1Ghz or higher
  - RAM: 1GByte or higher
  - Hard Disk: 40GB or higher
- Computers: 2 ea. (Monitoring PC 2 ea.)
  - CPU: 1Ghz or higher
  - RAM: 1GByte or higher
  - Hard Disk: 100MB or higher

The following software products were used to configure the evaluation environment:

- SUN Solaris 9 for SPARC
- Windows 2000, XP
- Java(v 1.4) VM
- Oracle 9i

The Agent consisted of SecureWorks and NetScreen, which are firewall systems, and Sniper IDS, which is an intrusion detection system. Master/Slave 1 and Slave 2 were installed on two servers to configure a distributed system environment and an integrated system environment. Two monitors were also used for testing. Router and general server testing was jointly conducted by the evaluator and the developer under the developer environment.

9. Evaluation Results

CC V2.3 and CEM V2.3 were applied for evaluation. The evaluation result confirmed that the subject product satisfies requirements of EAL4 evaluation guarantee grade of CC Part 2 and CC Part 3. Details of evaluation results are included in the evaluation report.

- Security target evaluation activity (ASE)

The evaluator applied the ASE work unit of the Common Evaluation Methodology for evaluation.

The executive summary of the Security Target Specification is complete, consistent with other parts of the Security Target Specification and accurately describes the Security Target Specification. TOE description explains TOE objective and its functions for easy understanding, is logical, complete, internally consistent and consistent with other parts of the Security Target Specification.

Security environment presents security issues that are derived from TOE and its security environment in clear and consistent manner in terms of assumptions, threats and organizational security policy. The description is complete and consistent. Security goals satisfy identified threats, achieve identified organizational security policy and satisfy stated assumptions.

IT security requirements are described in complete and consistent manner; and provide suitable basis for TOE development to achieve security goals. TOE Summary defines security functions and assurance measures in accurate and consistent manner; and satisfy stated TOE security requirements. Security Target Specification accurately substantiates protection profiles to accommodate.

- Configuration management activity (ACM)

The evaluator applied the ACM unit of Common Evaluation Methodology for evaluation. The evaluator verified from the configuration management documents that the developer uses automated tools to control changes to implementation expressions. From the configuration management documents it was verified that the developer clearly identifies TOE and its related configuration items and that changes to such items are appropriately controlled. It was also verified that the developer performs configuration management on the minimum TOE descriptions, evaluation proofs required by the ST warranty component and security defects.

- Delivery and operation activity (ADO)

The evaluator applied the ADO work unit of Common Evaluation Methodology for evaluation. Distributed documents describe all procedures for maintaining TOE security and detecting any changes and replacements of TOE when TOE is distributed to users. Procedures and steps for safe installation and creation of TOE have been documented. Thus, it has been confirmed that TOE is safely configured.

Accordingly, distribution and operating documents are suitable to ensure that the TOE is installed, created and initiated in the way intended by the developer and that the TOE is distributed without being modified.

- Development activity (ADV)

The evaluator applied the ADV work unit of the Common Methodology for evaluation. The functional specification describes TOE security functions appropriately and explains that they are sufficient to satisfy the security functional requirements of the Security Target Specification. It also describes TOE external interfaces appropriately. The security policy model is clear and consistent in describing the security policy rules and characteristics corresponding to the security functions specified in the functional specification.

The basic design describes TSF as a major component subsystem, appropriately describes subsystem interfaces and accurately implements functional specifications. The detailed design describes the internal operations of TOE security functions as the interactions between modules and their interdependencies. The detailed design is sufficient to satisfy the security functional requirements and details the basic design accurately and effectively.

The implementation description is sufficient to satisfy the security functional requirements of the Security Target Specification and accurately implements the detailed design. 'The consistency in expression' description shows that the requirements of the Security Target Specification have been accurately and completely implemented in terms of functional specification, basic design, detailed design and implementation.

Thus, documents including the functional specification, which describes the development requirements and TOE external interfaces; the basic design, which describes the TOE architecture in terms of interior subsystems; the detailed design, which describes the TOE architecture in terms of internal modules; the implementation document, which describes the source code level implementation; and the consistency in expression document, which ensures consistency of TOE expressions; all facilitate quite effectively understanding of the ways of how the TOE security functions are provided.

- Guidance documentation activity (AGD)

The evaluator applied the AGD work unit of the Common Evaluation Methodology for evaluation. Users' Manual describes user interfaces and operating methods for accessing the subject product through example illustrations. The Admin Manual describes how to access the security admin interface and menu items of the security admin interface using explanations and cautions through example illustrations. The evaluator confirmed that the menu descriptions in the Admin Manual are accurately stated.

- Life cycle support activity (ALC)

The evaluator applied the ALC work unit of the Common Evaluation Methodology for evaluation of ALC. It was verified that the security control on development environment suitably provides confidentiality and fault-free requirement of the TOE design and implementation. The evaluator verified that the developer used a documented TOE life cycle model. The evaluator also confirmed that the developer used a well defined development tool for producing consistent and predictable results.

Thus, the ALC section describes appropriately the procedures used by the developer during TOE development and maintenance periods including security procedures and tools used during the entire TOE development process.

- Test activity (ATE)

The evaluator applied the ATE work unit of the Common Evaluation Methodology for evaluation. The test document describes the test purpose, test procedure by stage and test results for security functions specified in the Security Target Specification, as well as prediction of the test results. Test processes including functional tests and module tests for each development process were replicated to verify that the test details of the test document are accurate and that the security functions' operations implemented through development are consistent with their designs. In addition, the evaluator conducted independent tests and confirmed the accuracy of the developer tests.

- Vulnerability assessment activity (AVA)

The evaluator applied the AVA work unit of the Common Evaluation Methodology for evaluation. The misuse analysis verified that the Users' Manual is not misunderstood, irrational or conflicting; that all safety procedures of operating modes are well prepared; and that the Users' Manual can be used effectively to prevent and detect abnormalities of TOE. The functional strength declaration declares on all probabilistic and permutation mechanisms in the Security Target Specification and the analysis of the developer's functional strength declaration confirmed its accuracy.

Vulnerability Analysis document describes clearly known vulnerabilities of TOE and their countermeasures in terms of their functional implementation and specification of operating environment in guidelines or Users' Manual. The evaluator conducted an independent vulnerability test and confirmed that TOE does not have any vulnerabilities that can be misused by intruders of low level attack capability within the intended environment.

Thus, the evaluator confirms that TOE does not have any defect or weakness that can be misused within the intended environment based on the vulnerability analysis and the evaluator's infiltration testing.

10. Recommendations

- The subject product conducts RMI communication of SSL base that is provided by Java for all communication between TOEs (Master-Monitor, Master-Slave and Slave-Agent). RMI communication is categorized as a non-evaluation item. However, since it is used in all inter-TOE communication, attention should be focused on detection and dissemination of recent RMI weaknesses. Also, the same type of interest should be focused on Oracle 9i used by TOE. Thus, TOE shall be safely operated by applying appropriate patches when a vulnerable area is discovered.

- TOE Agents are diverse based on OS and install environment, unlike Master, Slave or Monitor. That is, the Agent Systems are diverse products including firewall, intruder detection system, network devices and general servers. Therefore, evaluation and certification cannot be done on all products. Therefore, although product safety and reliability validation can be done on the environment implemented during evaluation testing, validation would not be feasible on other environments. Accordingly, in case of implementing a product in an environment different from the evaluation environment, inquiry shall be addressed to a certification body

- This product is an Enterprise Security Management system that collects and analyzes data from Management Targets and implements control and operation at enterprise level through consistent security policies. Therefore, this product collects diverse types of data from numerous Management Targets. However, since the timing of Management Targets are not synchronized, it may pose difficulty to properly analyze and utilize collected data for security management purposes. Therefore, time synchronization of Management Targets should be considered.

- To receive valid control and analysis event data, event validation should be performed over a sufficient length of time through customizing in consideration of network environment and characteristics of each site where TOE is installed and is in operation.

- Communication between TOE and Oracle 9i is not encoded. However, there is TSF sensitive data communicated between these two. Therefore, Oracle 9i should be installed in the same server as the TOE to ensure safety against external attacks.

- Data communicated from Agent Systems to TOE for communication with SNMP, Syslog and Agents may contain security sensitive data. Therefore, TOE and Agent Systems should be installed protected with firewalls in locations separated from external Internet network to ensure safe operation.

11. Acronyms & Terminology

The following acronyms and terms were used in this report.

(1) Common abbreviations

CC	Common Criteria
EAL	Evaluation Assurance Level
ESM	Enterprise Security Management
PP	Protection Profile
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control

(2) Glossary

Target of Evaluation (TOE)

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

Audit record

Audit data that is kept to record TOE security related events.

User

Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.

Authorized Admin

Authorized user that safely manages the TOE in accordance with TOE Security Policy.

Authorized user

A user who may, in accordance with the TSP, perform an operation.

Identity

A representation (e.g. a string) uniquely identifying an authorized user, which can either be the full or abbreviated name of that user or a pseudonym.

Authorized data

Information used to verify the claimed identify of a user.

External IT entity

Any IT product or system, untrusted or trusted, outside of the TOE that interacts with the TOE.

Assets

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

Enterprise Security Management Agent System

System that is subject of TOE security control activities

Authorized Administrator

TOE Administrators include the top level admin, control admin and monitoring admin by their level of authority. Unless specified otherwise, the 'authorized admin' refers to the top level admin only. Lower level admin users are configured by the top level admin. An authorized admin cannot perform control functions outside of permitted privileges.

12. References

The certification body prepared this certification report based on the following references:

[1] Information Protection System Common Criteria (2005. 5. 21)
[2] Information Protection System Common Evaluation Methodology V2.3
[3] Guidelines for Evaluation & Certification of Information Protection Systems (2005. 5. 21)
[4] Regulations for Evaluation & Certification of Information Protection Systems (2005. 12. 26)
[5] ActiveTSM V3.0 Security Target V1.8 (July 3, 2006)
[6] ActiveTSM V3.0 Evaluation Report, V1.1 (2006. 9. 28)