National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme

Validation Report

Promia Incorporated

Promia Intelligent Agent Security Manager, Version 1.2 (IASM)

Report Number: CCEVS-VR-06-0025

Dated: 9 June 2006

Version: 1.0

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6740
Fort George G. Meade, MD 20755-6740

ACKNOWLEDGEMENTS

Validation Team

Jean Hung

The MITRE Corporation

Jandria Alexander

The Aerospace Corporation

Common Criteria Testing Laboratory

Computer Sciences Corporation

Annapolis Junction, Maryland

Table of Contents

1. EXECUTIVE SUMMARY

This report documents the NIAP validators' assessment of the evaluation of Promia Incorporated Intelligent Agent Security Manager, Version 1.2 (IASM). It presents the evaluation results, their justifications, and the conformance results. This validation report is not an endorsement of the IT product by any agency of the U.S. Government and no warranty of the IT product is either expressed or implied.

The evaluation was performed by Computer Sciences Corporation (CSC), and was completed during May 2006. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test report, both written by CSC. The evaluation determined the product to be **Part 2 extended and Part 3 augmented,** and to meet the requirements of **EAL3 augmented with ALC_FLR.2 and ALC_LCD.1**. The product is not conformant with any published Protection Profiles.

The IASM TOE (Target Of Evaluation) is a Security Incident Management Platform that provides a subset of IASM Suite functions that both are needed in an enterprise-specific security incident management system (SIMS). Consideration for defining the IASM TOE was determining which IASM Suite functions could be specified and tested without reference to detailed knowledge of a specific network. The IASM TOE consists of the following functions:

- Dedicated, commodity, IASM TOE hardware running a security-hardened OS, the Java Runtime Environment with Secure Socket Extensions, and CORBA middleware;
- A security incident management (SIM) repository that implements the abstractions needed for a SIMS – specifically: events, assets, incidents, and responses;
- Interfaces that devices on the monitored network can use to submit potentially security relevant operational and security events to the IASM TOE for normalization and storage into the SIM repository and redistribution to analytic engines;
- Interfaces for managing IASM TOE and site-specific SIMS software components;
- An identified set of SIMS roles and interfaces for managing those roles;
- Interfaces for managing and identifying and authenticating authorized SIMS users.

The TOE includes security functions implemented at the TOE interfaces, as follows:

- Protected External Communications (TSF_PEC)
- Protection of Security Functions (TSF_PSF)
- Security Function Management (TSF_SFM)
- Security Information Consolidation (TSF_SIC)
- Security Incident Management (TSF_SIM)
- User Identification & Authentication (TSF_UIA)

A Strength of Function claim of SOF-basic is made for Version 1.2 IASM.

The cryptography used in this product has not been FIPS certified, nor has it been analyzed or tested to conform to cryptographic standards during this evaluation. All cryptography has only been asserted as tested by the vendor.

The Security Target (ST) for Promia Intelligent Agent Security Manager, Version 1.2 (IASM) is contained within the document *Promia Intelligent Agent Security Manager, Version 1.2 (IASM) Security Target, Revision 3.3d, 28 April 2006*.

2. IDENTIFICATION

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) for Evaluation Assurance Level (EAL) 1 through EAL4 in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Validated Products List.

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated;
- The Security Target (ST), describing the security features, claims, and assurances of the product;
- The conformance result of the evaluation;
- Any Protection Profile to which the product is conformant;
- The organizations participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
Target of Evaluation	Promia Intelligent Agent Security Manager, Version 1.2 (IASM)
Protection Profile	None
Security Target	*Promia Intelligent Agent Security Manager, Version 1.2 (IASM) Security Target, Revision 3.3d, 28 April 2006*
Evaluation Technical Report	*Promia Intelligent Agent Security Manager, Version 1.2 (IASM) Security Target Version 1.0, Version 1.0, 5 May 2006*
Conformance Result	Part 2 extended, Part 3 conformant, EAL 3 Augmented with ALC_FLR.2 and ALC_LCD.1
Sponsor	Promia Incorporated 160 Spear St., Suite 320 San Francisco, CA 94105
Developer	Promia Incorporated
Evaluators	Computer Sciences Corporation
Validators	Jean Hung of The MITRE Corporation and Jandria Alexander of The Aerospace Corporation

3. SECURITY POLICY

The Promia Intelligent Agent Security Manager, Version 1.2 (IASM) enforces the following security policies:

3.1 Protected External Communications

All information that is transmitted between the TOE and an Authorized External Entity – i.e., an entity accessing the TOE through the network connection to the monitored network and with which the TOE intends and expects to communicate securely – is protected from both disclosure and modification by using SSL version 3.0 as implemented in the standard Java Secure Sockets Extension implementation provided with the Java Runtime Environment version 1.5. The disclosure protection is accomplished by the symmetric encryption of the data being transferred using either the DESede (aka, Triple DES – defined in US FIPS-46-3) or AES (defined in US FIPS-197) ciphers and a per connection key generated as part of the Secure Socket Layer Version 3 (SSLv3) protocol. The modification protection is accomplished by the use of the HMAC (Hashed Message Authentication Code – defined by IETF RFC2104) that is incorporated into the SSLv3 record transfer protocol.

3.2 Protection of Security Functions

Protection of Security Functions provides the common self-protection capabilities upon which the implementations of the other security functions rely.

3.3 Security Functions Management

Security Functions Management provides the interface through which an IASM Administrator establishes, monitors, and manages the security and operational configuration of the IASM.

3.4 User Identification & Authentication

User Identification & Authentication provides the identification, authentication, and authentication secret (i.e., password) generation capabilities that provide a substantial proportion of the technical and operational assurance in the security of the TOE.

3.5 Security Information Consolidation

Security Information Consolidation, which both accepts, normalizes, stores, and redistributes (to analytic software components) operational and security events from devices on the monitored network and allows analytic software components to create, modify, and store security incidents in the IASM TOE SIM repository.

3.6 Security Incident Management

Security Incident Management, which provides the operational interface by which IASM Operators are alerted to newly detected or changed security incidents and provided with the tools to review and react to the incidents. The IASM_SIM subsystem also provides the related interfaces with which the IASM Analysts and IASM Reporters can accomplish their jobs.

4. ASSUMPTIONS

The Security Targets [7] identifies the assumptions regarding the security environment and the intended usage of the TOE.

4.1 Intended Usage Assumptions

- A.DYNMIC - The TOE will be actively managed in a manner that allows it to appropriately address changes in the IT System.

- A.EVENTS - The devices on the IT System that supply events to the TOE are protected from attacks on their integrity and availability and are designed and operated to correctly use the standard SSL/TLS technologies for protecting the in-transit confidentiality of the events they supply to the TOE.

- A.ASCOPE - The average quantity and rate of events generated by the IT System being monitored fall within the specified capacity of the TOE.

- A.COMMS - Adequate communications exist among the TOE components and between the TOE components and the IT System components.

- A. NETSEP - The internal communications path between TOE components is separated from the external communications path between the TOE components and the IT System components using either physical (separate network switches) or logical (VLANs within a single network switch) techniques.

4.2 Physical Assumptions

- A.PROTCT - The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.

- A.LOCATE - The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.

4.3 Personnel Assumptions

- A.MANAGE - There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.

- A.NOEVIL - The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.

- A.NOTRST - The TOE can only be accessed by authorized user.

5. ARCHITECTURAL INFORMATION

The Intelligent Agent Security Manager (IASM) Suite developed by Promia, which provides security countermeasures for security incident detection, management, and response. The IASM Suite is an example of Security Incident Management System (SIMS) products that automatically collect, normalize, and analyze the operational and security event logs of diverse kinds of security relevant devices on monitored networks in order to detect security incidents that are only visible when data available from multiple devices is considered. Having detected the incidents, the IASM Suite then identifies candidate responses based on site-specific policies and provides a unified operator interface for managing the incidents and responses.

The IASM TOE consists of the following functions:

- Dedicated, commodity, IASM TOE hardware running a security-hardened OS, the Java Runtime Environment with Secure Socket Extensions, and CORBA middleware;
- A security incident management (SIM) repository that implements the abstractions needed for a SIMS – specifically: events, assets, incidents, and responses;
- Interfaces that devices on the monitored network can use to submit potentially security relevant operational and security events to the IASM TOE for normalization and storage into the SIM repository and redistribution to analytic engines;
- Interfaces for managing IASM TOE and site-specific SIMS software components;
- An identified set of SIMS roles and interfaces for managing those roles;
- Interfaces for managing and identifying and authenticating authorized SIMS users.

The relative scopes of a complete SIMS and the IASM TOE are shown in the Figure below. The scope of the full SIMS is circumscribed by the large dashed box labeled Intelligent Agent Security Manager Suite, while the IASM TOE is shown as the subset of IASM Suite components denoted by double solid lined boxes.

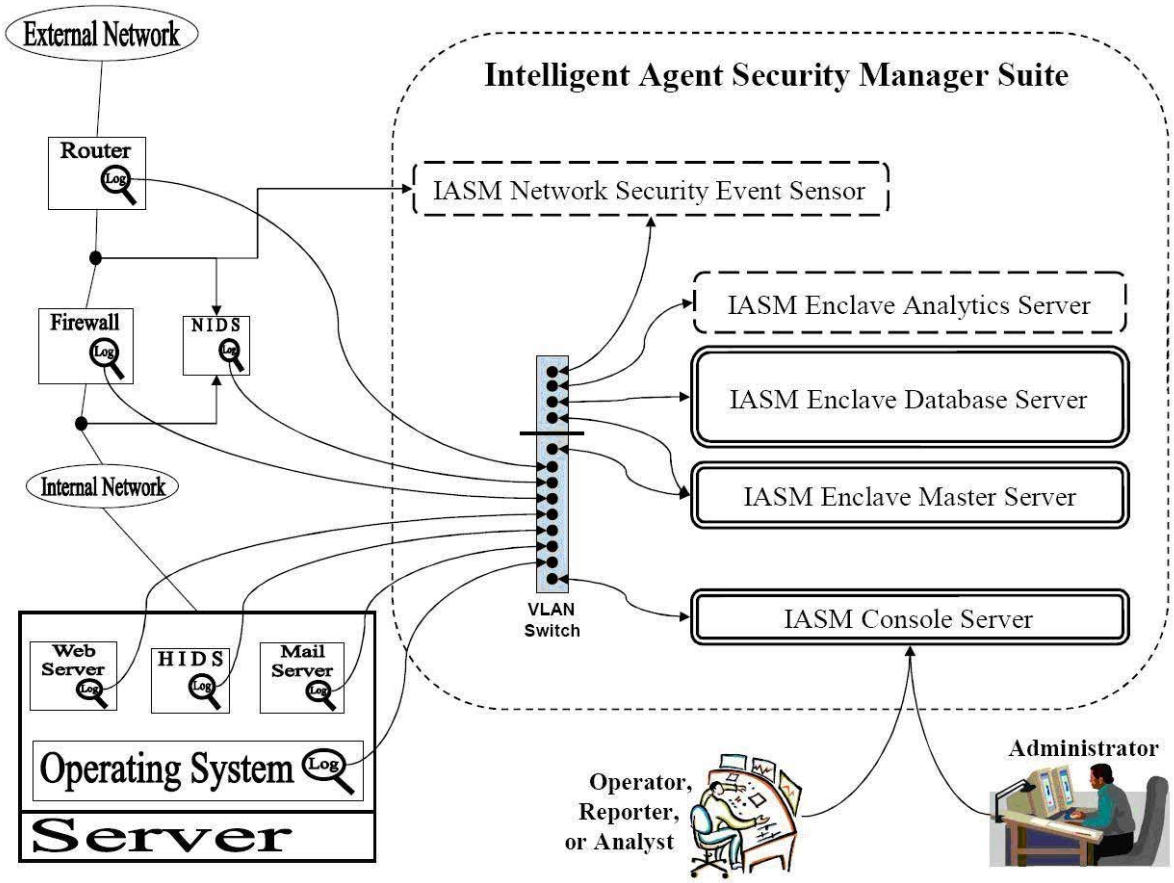

Figure 1. IASM Conceptual Approach

The TOE logical boundary composed of the following logical security functions:

- Protected External Communications, which provides the core capability for ensuring that the IASM TOE only communicates with the external entities that it intends and expects to communicate with;

- Protection of Security Functions, which provides the common self-protection capabilities upon which the implementations of the other security functions rely;

- Security Functions Management, which provides the interface through which an IASM Administrator establishes, monitors, and manages the security and operational configuration of the IASM;

- User Identification & Authentication, which provides the identification, authentication, and authentication secret (i.e., password) generation capabilities that provide a substantial proportion of the technical and operational assurance in the security of the TOE;

- Security Information Consolidation, which both accepts, normalizes, stores, and redistributes (to analytic software components) operational and security events from devices on the monitored network and allows analytic software components to create, modify, and store security incidents in the IASM TOE SIM repository;

- Security Incident Management, which provides the operational interface by which IASM Operators are alerted to newly detected or changed security incidents and provided with the tools to review and react to the incidents. The IASM_SIM subsystem also provides the related interfaces with which the IASM Analysts and IASM Reporters can accomplish their jobs.

6. DOCUMENTATION

During the course of the evaluation, the CCTL had access to documentation and evidence[1], covering:

- Configuration Management Documentation,
- Functional Specification,
- High-level Design,
- Correspondence Evidence,
- Installation, Generation, and Startup Procedures,
- Delivery Procedures, Secure Installation and Operation Guidelines,
- Strength of Function Analysis,
- Test Coverage Analysis Evidence,
- Vulnerability Analysis Report,
- Administrator Guide,
- User Guide,
- Test Documentation to include Test Plans, Procedures, and Test Results,
- Security Target.

Specific references necessary to install, configure and minister the TOE include:

- IASM v1.2 Operations Manual v2.1, dated 23 March 2006,
- IASM v1.2 Quick Start Guide: IASM 6100 Installation, Configuration and Operation (rev 1.1), dated June 2, 2005,
- Intelligent Agent Security Manager (IASM V1.2) USER CONSOLE MANUAL, Revision 2.1, dated 2 December 2005.

[1] A complete list of the documentation used during the evaluation is included in Section 3.5 of the *Evaluation Technical Report for a Target of Evaluation*, Version 1.0, May 05, 2006.

7. IT PRODUCT TESTING

7.1 Evaluation Tools

To perform functional and vulnerability testing activities, the evaluation team used the following equipment:

IASM_master

IASM_master provides the core services needed for IASM v1.2 to function. This unit was configured during the installation process by Promia technicians, as documented in the IASM v1.2 Quick Start Guide: IASM 6100 Installation, Configuration and Operation. This unit was assigned the IP address 10.4.0.99 for the external network and 10.100.0.50 for the internal network. The following accounts were assigned on this machine:

Account	Password	Role
root	pgfhr-41	system administrator
iasm	pgfhr-41	IASM administrator

IASM_dbserver

IASM_dbserver is a repository of information for security incident recording and management. It's primary function is to store a security incident management data model. This unit was configured during the installation process by Promia technicians, as documented in the IASM v1.2 Quick Start Guide: IASM 6100 Installation, Configuration and Operation. This unit's IP address is not visible on the external network. Its internal network IP address is 10.100.0.53. All communications are through the IASM master unit. The following accounts were assigned on this machine:

Account	Password	Role
Root	pgfhr-41	System Administrator
Iasm	pgfhr-41	IASM administrator

IASM_Console

IASM_Console is used to provide human users with an interface to the TOE. The applications run are the user console login dialog and the Promia IASM v1.2 Taskbar (GUI). Its network IP address is 10.4.0.100. The following accounts were assigned on this machine:

Account	Password	Role
Root	pgfhr-41	System Administrator

Account	Password	Role
Iasm	pgfhr-41	IASM Administrator

IASM_ids

This unit does not form a part of the TOE (see Promia ST, Section 2.1, Figure 2.1), though IASM_ids is a part of the IASM product. This unit maps to the IASM Network Security Event Sensor shown in ST figure 2.1. This unit's IP address is not visible on the external network. Its internal network IP address is 10.100.0.52. The following accounts were assigned on this machine:

Account	Password	Role
Root	pgfhr-41	System Administrator
Iasm	pgfhr-41	IASM Administrator

IASM_aes

The IASM_aes is a part of the IASM Suite (see Promia ST, Section 2.1, Figure 2.1); this unit maps to the IASM Enclave Analytics Server shown in ST figure 2.1. The IASM_aes server derives a significant amount of its behavior from the monitored network. To allow the TOE to remain general in scope of application the AES was excluded from the evaluation and consequently this testing effort. The AES uses artificial intelligence to do data mining and classification for the information collected from the environment. Data mining and classification algorithms are not deterministic like most computer programs. Because the AES has interfaces to the TOE, the Targethost machine was created to replicate the interfaces. The difference between the Targethost and AES is that the Targethost is deterministic and therefore has well known and predictable behavior that is appropriate for testing since the values presented over the interface(s) can be reproduced. NOTE: The IASM_aes was an element included as part of the IASM Suite for completeness (ref. ADO_IGS.1 and ADO_DEL.1) and was not utilized for any portion of this testing effort. This unit's IP address is not visible on the external network. Its internal network IP address is 10.100.0.51. The following accounts were assigned on this machine:

Account	Password	Role
Root	pgfhr-41	System Administrator
Iasm	pgfhr-41	IASM Administrator

Cat_1

Cat_1 is not a part of the TOE, but is shipped with the IASM suite (see Promia ST, Section 2.1, Figure 2.1). Cat_1 is a Cisco Catalyst 2970 switch, with a Promia-installed configuration. This configuration partitions the Ethernet ports on the switch into two logically disjointed networks through use of the Virtual LAN (VLAN) feature of the switch. This enables the interconnections of the various TOE and non-TOE items into logically isolated TOE-internal and TOE-external networks.

RSSSP

RSSSP is a PC running Microsoft Windows XP. Its IP address is 10.4.0.101. Its purpose is to host the Test Sensor Agent (TSA). This means that the RSSSP acts as an event generator. The Sensor Agent is a normal part of the working environment for the IASM v1.2 unit. It doesn't form part of the TOE but is needed to generate data for testing.

TARGETHOST

TARGETHOST is a PC running Microsoft Windows 2K. Its IP address is 10.100.0.55. Its purpose is to host the JessSim, a test Analytic Engine, which logs the alerts it receives to a local trace file. The Analytic Engine is a normal part of the working environment for the IASM v1.2 unit. It doesn't form part of the TOE but is needed to verify correct behavior of the IASM_master unit. A test analytic engine is used to allow the tests to be explicitly repeatable. The standard analytic engines use AI which is not explicitly repeatable.

Kitfox Laptop

The Kitfox is an IBM thinkpad running Fedora core 4.

7.2 Evaluator Testing

Testing of the Promia Intelligent Agent Security Manager, Version 1.2 (IASM) TOE took place at Promia Incorporated facility in Linthicum, MD during March 2006.

The Promia evaluation team's analysis of the developer's test plans, test scripts, and test results demonstrate accurate correspondence between the tests identified and the functional specification, and that the developer's testing is adequate to satisfy the requirements of EAL3 augmented with ALC_FLR.2 and ALC_LCD.1.

In addition, the evaluation team executed a subset of the developer tests, as well as tests they devised. Testing covered each security functional component claimed for the TOE, and demonstrated the validity of each component.

The Promia evaluation team also performed penetration testing as required at EAL3. The evaluation team devised penetration tests, building on the developer vulnerability analysis. The penetration tests were documented in sufficient detail to enable the tests to be repeatable. The evaluator considered all evaluation evidence as the basis for the penetration testing effort. Of particular interest were the vendor supplied vulnerability assessment, development evidence, and the security target.

The evaluation team used the following documents to form the test basis for the penetration testing effort:

- ST
- FSP
- User guidance
- Administrator guidance
- Test documentation
- Test coverage and depth analyses.

The evaluation team defined tests based on TOE functionality and its IT environment. The process, activities, and results are described in the test report. The evaluator followed up on any unexpected behavior found while executing the test plan. The vulnerability test plan/report notes both process and findings.

The evaluator performed an analysis of the vendor-supplied vulnerability analysis, and researched public domain vulnerabilities; the vulnerabilities listed were network related. Due to the nature of the TOE and the intended environment, the focus of the vulnerability analysis effort was on attacks against the network interfaces it provides.

The attacks that were selected by the evaluation team were based upon the sophistication level of the attack and the time necessary to develop the attack. The claim of SOF-Basic excludes most intricate and specially crafted attacks, leaving common and easily executed attacks for testing. The following test areas attempted to stay within the scope of SOF-Basic while still representing a thorough testing effort: network scan, low-level network attacks, and database access attacks. The separation between the TOE internal and external networks was also tested.

The attacks were performed from a single platform. This platform hosted numerous publicly available test/attack tools and one commercially available tool. These tools helped the tester to observe the TOE behavior, and attempt to manipulate the TOE. The free public availability of most of these tools makes them a viable threat mechanism. The commercial tool was used to run a general scan that checks for a wide range of vulnerabilities.

Although the evaluation team limited the scope of penetration testing to the environment and threats described in the ST, the evaluation team investigated techniques, and attack methods, in excess of those anticipated in the ST. The constraints listed in the ST made most attacks impossible for SOF-basic. Therefore, in order to perform a thorough testing effort, tests were run despite the mitigating policies. The vulnerabilities found during testing that were mitigated by the ST, were noted as residual vulnerabilities and the final disposition of the vulnerability were addressed in the Evaluation Technical Report and the Vulnerability Assessment Work Package.

8. EVALUATED CONFIGURATION

Evaluated TOE: Promia Intelligent Agent Security Manager, Version 1.2 (IASM).

The following table summarizes the categories of configuration items that comprise the evaluated TOE. Since the IASM TOE is defined as a collection of appliances, the table includes both software and hardware configuration items. The table also shows the IASM components that are included in each category of configuration item.

Table 2: TOE Software and Hardware Configuration Items

CI Category	IASM Component(s)
IASM Master Server	Hardware Components: • A dual Opteron (2-2.4GHz) Motherboard, with 8-16 Gigabytes RAM, a single channel 10/100MB Ethernet NIC, and a dual-channel GigE NIC Software Components • SuSE Linux Enterprise Server 9.0 Operating System • IASM Version 1.2 Core Services
IASM Database Server	Hardware Components: • A dual Opteron (2-2.4GHz) Motherboard, with 8-16 Gigabytes RAM, a single channel 10/100MB Ethernet NIC, and a dual-channel GigE NIC • 5 x 250Gb drives in RAID configuration Software Components • SuSE Linux Enterprise Server 9.0 Operating System • IASM Multi-collector Agents
IASM Console Server	A Dell 1750 workstation with Windows XP Professional installed in the CC evaluated configuration IASM User Console SW (1 per Enclave Server)

The items listed below are specifically excluded from the TOE evaluation:

- IASM SensorAgents that supply the events from various third party devices on the monitored network that are received normalized, and stored by IASM;
- Sensor Agent filters – both raw and normalized;

- Analytic software components that monitor and mine the stream of monitored network events to detect potential security incidents;

- The Promia Network Security Event Sensor (NSES) that performs Anomaly- and Signature-based analysis of monitored network traffic to detect and send potentially security-relevant events to the IASM and the additional forensic tools on the NSES that allow an Analyst to conduct more extensive in-place analysis of the traffic surrounding an NSES anomalous event.

9. RESULTS OF THE EVALUATION[2]

The TOE was found to provide the capabilities defined by the Security Target, and to satisfy all the requirements of EAL3 augmented with ALC_FLR.2 and ALC_LCD.1.

10. VALIDATOR COMMENTS

The Validator offers the following comments:

- The Validator did not attend testing for this product, but did carefully review all of the documentation provided by Promia Corporation and Computer Sciences Corporation, in support of the evaluation.
- The cryptography used in this product has not been FIPS certified, nor has it been analyzed or tested to conform to cryptographic standards during this evaluation. All cryptography has only been asserted as tested by the vendor.

11. SECURITY TARGET

The ST, *Promia Intelligent Agent Security Manager, Version 1.2 (IASM) Security Target, Revision 3.3d, 28 April 2006* is included here by reference.

[2] The terminology in this section is defined in CC Interpretation 008, specifying new language for CC Part 1, section/Clause 5.4.

12. GLOSSARY

CC	Common Criteria
CCEL	Common Evaluation Laboratory
CCEVS	Common Criteria Evaluation and Validation Scheme
CCTL	Common Evaluation Testing Laboratory
CEM	Common Evaluation Methodology
CSC	Computer Sciences Corporation
EAL	Evaluation Assurance Level
EDR	Evaluation Discovery Report
ETR	Evaluation Technical Report
HMAC	Hashed Message Authentication Code
IASM	Intelligent Agent Security Manager
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards & Technology
NSA	National Security Agency
NSES	Network Security Event Sensor
NVLAP	National Voluntary laboratory Assessment Program
SIM	Security Incident Management
SIMS	Security Incident Management System
SOF	Strength of Function
SSLv3	Secure Socket Layer Version 3
ST	Security Target
TOE	Target of Evaluation
TSA	Test Sensor Agent
TSF	TOE Security Function
VLAN	Virtual LAN

13. BIBLIOGRAPHY

[1] Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, dated January 2004, Version 2.2.

[2] Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, dated January 2004, Version 2.2.

[3] Common Criteria for Information Technology Security Evaluation – Part 2: Annexes, dated January 2004, Version 2.2.

[4] Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, dated January 2004, Version 2.2.

[5] Common Evaluation Methodology for Information Technology Security: Introduction and general model, dated January 2004, version 2.2.

[6] Security Target, Promia Intelligent Agent Security Manager Version 1.2 (IASM) Security Target, Revision 3.3d, April 28, 2006.

[7] Common Criteria Testing Laboratory Penetration Test Plan and Report for Promia Intelligent Agent Security Manager Version 1.2 (IASM), April 27, 2006.

[8] CSC Common Criteria Laboratory Independent Test Plan and Report for Promia Intelligent Agent Security Manager Version 1.2 (IASM), March 27, 2006.

[9] Evaluation Technical Report for a Target of Evaluation, Promia Intelligent Agent Security Manager Version 1.2 (IASM), Security Target Version 1.0, Version 1.0, May 05, 2006