National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme
Validation Report

Sun Java™ System Identity Manager v5.0

Report Number: **CCEVS-VR-05-0117**
Dated: **6 September 2005**
Version: **1.1**

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

Richard Murphy
Mitretek Systems
Falls Church, Virginia

Common Criteria Testing Laboratory

Jean Petty
Peter Kukura
Dragua Zenelaj
CygnaCom Solutions
McLean, Virginia

Table of Contents

I. Executive Summary

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the Sun Microsystems Sun Java™ System Identity Manager V5.0. It presents the evaluation results, their justifications, and the conformance results. This Validation Report is not an endorsement of the Target of Evaluation (TOE) by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied.

The evaluation of the Sun Java System Identity Manager V5.0 was performed by CygnaCom Solutions Common Criteria Testing Laboratory in the United States and was completed during August 2005. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test report, both written by CygnaCom.

The evaluation was carried out in accordance to the Common Criteria Evaluation and Validation Scheme (CCEVS) processes and procedures. Sun Java™ System Identity Manager (IDM) was evaluated against the criteria contained in the Common Criteria for Information Technology Security Evaluation, Version 2.2. The evaluation methodology used by the evaluation team to conduct the evaluation is the Common Methodology for Information Technology Security Evaluation, Version 2.2. CygnaCom Solutions determined that the product meets the security criteria in the Security Target, which specifies an assurance level of EAL2. The evaluation team determined the product to be Part 2 conformant and Part 3 conformant, and concluded that the Common Criteria requirements for Evaluation Assurance Level (EAL) 2 have been met.

The TOE is a software-only server application that provides a consistent interface for system administrators to update user account and other configuration information in many target systems of various kinds such as applications, mainframes, databases, directory services (LDAP), operating systems, ERP systems, and messaging platforms. With role and rule based provisioning, this solution automates the routine, yet often complex, activities associated with granting, managing, and revoking user access privileges.

The evaluation considered only the IDM software and the associated IDM administrative user interface, running on a Windows 2000 platform. There are several components provided by the underlying system that the TOE depends upon but which are outside the evaluation boundary. These components include the operating system, the database system and its interface, third-party encryption software, and a Web Services engine. This evaluation does not demonstrate assurance for these components.

The TOE was not evaluated for self-protection features. This means that it may be possible for the IDM to be bypassed or to be tampered with by an attacker.

The validation team monitored the activities of the evaluation team, participated in team meetings, provided guidance on technical issues and evaluation processes, reviewed successive versions of the Security Target, reviewed selected evaluation evidence, reviewed test plans, reviewed intermediate evaluation results (i.e., the CEM work units), and reviewed successive versions of the ETR and test report. The validation team determined that the evaluation team showed that the product satisfies all of the functional and assurance requirements defined in the Security Target for an EAL 2 evaluation. Therefore the validation team concludes that the CygnaCom CCTL findings are accurate, and the conclusions justified.

II. 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 EAL 1 through EAL 4 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~~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;
- The Protection Profile to which the product is conformant (not applicable for this product);
- The organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme

Item	Identifier
Target of Evaluation	Sun Java™ System Identity Manager – Version 5.0. Part number 817-7804-05
Protection Profile	Not applicable
Security Target	*Sun Java™ System Identity Manger – Version 5.0, Security Target, version 2.4*
Evaluation Technical Report	*Sun Java™ System Identity Manager Evaluation Technical Report Volume 1, Version 1.8* *Sun Java™ System Identity Manager Evaluation Technical Report Volume 2, Version 1.8*
Conformance Result	CC Part 2 conformant, CC Part 3 conformant, EAL 2
Sponsor	Sun Microsystems, Inc. 4150 Network Circle Santa Clara, CA 95054 USA
Common Criteria Testing Lab (CCTL)	CygnaCom Solutions 7925 Jones Branch Drive, Suite 5200 McLean, VA 22102
CCEVS Validator(s)	Richard H. Murphy Mitretek Systems, Inc. 3150 Fairview Park South Falls Church, VA 22042-4519

III.Security Policy

The TOE assists in the enforcement of an Access Control Policy by managing a set of user identities. The TOE maintains information on users including their identification, their password policies, the roles associated with the user, and other security attributes. The TOE validates user identities using their passwords and uses that information to make access control decisions. User passwords can be user selected or automatically generated. A defined set of rules can constrain valid passwords. The TOE provides a consistent interface for managing user accounts that can then be used by various kinds of applications such as databases, directory services such as LDAP, ERP systems, and messaging platforms. Both role and rule based enforcement polices can be enforced.

IV. Assumptions and Clarification of Scope

Personnel Assumptions

- It is assumed that there will be no untrusted users or software on the IDM host.

- It is assumed that the administrator will follow administrator guidance for installing and maintaining the TOE, including ensuring that there will be no untrusted users and no untrusted software on the IDM Server host.

Physical Assumptions

- None.

IT Environment Assumptions

.

- It is assumed that the underlying operating system provides reliable time stamps.

V. Evaluated Configuration

The TOE Physical Boundary and the evaluated configuration include the following:

- Sun Java™ System Identity Manager V5.0 running on Microsoft Windows 2000;
- Sun Java™ System Identity Manager Administrator/User Interface running on the same machine.

The TOE includes the IDM Server and the IDM Administrator/User Interface and the physical boundary consists of these software components. The TOE does not include the underlying operating system (OS) software and hardware of the system hosting the TOE. The third party relational database is not included in the TOE. The interface of the third party database is not included as part of the TOE. The TOE also does not include the third-party encryption software that is used to provide a trusted communication path between users and the TOE. The Web Services Engine is not part of the TOE. Note that in the evaluated configuration, all TOE components run on the same machine running Microsoft Windows 2000.

It is assumed that there will be no untrusted users or software on the IDM host. IDM relies upon the underlying operating system platform to provide reliable time stamps. The evaluated configuration of IDM was tested on the following platform with the IT environment resources listed:

OS: Microsoft Windows 2000 Server SP4
Application Server: Apache Tomcat Version 4.1.27 (with JDK 1.4.2)
Database: MySQL™ 4.0.16.
System: Dell OptiPlex GX270 P4 2.4 GHz., 1GB RAM, 40 GB HD

TOE Logical Boundaries and Functionality

The TOE encompasses the following components of the Sun Java™ System Identity Manager product:

- IDM Server,
- Administrator/User Interface.

The main security service provided by Sun Java™ System Identity Manager is to manage user identities. The IDM server maintains information on users and the resources they can access. It provides a single interface for authorized administrators to grant, manage, and revoke user access privileges.

Sun Java™ System Identity Manager provides the following security functions:

- **Security Audit –**IDM provides the ability to audit the following events: generated accounts, approved requests, failed access attempts, password changes and resets, self provisioning activities, and administration of configuration data. IDM provides a utility for searching, sorting, ordering, and viewing audit records.
- **User Data Protection/Access Control –**IDM provides access control through the enforcement of the Sun Java™ System Identity Manager Access Control Policy. The IDM Access Control Policy is based on user roles also described as user capabilities in the Administrator's Guide. This functionality is specified using security attributes in user records in the IDM Data Store.
- **User Identification and Authentication –** The Sun Java™ System Identity Manager provides user identification and authentication through the use of user accounts and the enforcement of password policies. In addition, IDM provides the capability to automatically generate passwords that meet the rules of the password policy.
- **Security Management –**IDM provides security management through the use of the Administrator Interface and User Interface.

VI. Evaluation Process and Conclusions

The evaluation team performed the applicable Common Evaluation Methodology activities according to a CygnaCom proprietary methodology. As issues were raised during the evaluation process, observations were documented and provided to the sponsor for correction. Incremental ETRs were released to document the progress of the ST and TOE evaluations. The evaluation team provided rationale for each verdict as part of their final ETR, describing the steps that were executed for each work unit, including the source of information used to make an evaluation conclusion. The ETR provided detailed rationale for each evaluation decision.

VII. Validation Process and Conclusions

The Validation team used vendor-supplied documentation to familiarize themselves with the TOE usage and environment. The Validator used a combination of communications with the evaluation team (largely via electronic mail), records review, and review of the final ETR results to verify the results of the evaluation team's analysis. The evaluation team responded to Validator queries in a timely manner. No deficiencies were found in the execution of the CEM work units.

VIII. Validator Comments/Recommendations

No significant issues were found during the validation. The evaluation team responded quickly to all validation team requests and observations.

The TOE functional requirements do not include Reference Mediation (FPT_RVM) or Domain Separation (FPT_SEP). The consequence of this is that the TOE is not known to be self-protecting. FPT_RVM requires that the TOE be tamperproof (protect itself from tampering by untrusted subjects), that it always be invoked, and that it be self-contained and simple enough to analyze. FPT_SEP requires that TOE data be isolated so that TOE data cannot be observed or modified by untrusted subjects. This separation is enforced by operating the TOE security functions in an isolated, controlled execution environment that untrusted subjects cannot access without invoking the TSF. The fact that the TOE was not evaluated to meet these requirements means that there is no assurance provided that the TOE protects itself against bypass or tampering attacks. The TOE is designed to be used in a benign environment; the evaluation did not consider threats which attempt to bypass TOE enforcement. These threats are somewhat limited by the assumption that all users on the system running the TOE software are trusted users (A.NoUntrusted). The requirement that all TOE components execute on a single system also mitigates this threat.

IX. Annexes

Annex A: Architectural Description of the TOE

See section V above.

Annex B: Assurance Requirements Results

The Security Target demonstrates that the TOE meets the assurance requirements at EAL 2. There is no protection profile and therefore no extended assurance requirements met by the TOE.

Annex C: Security Functional Requirements Results

The evaluation demonstrated that the TOE met the functional requirements of the Security Target. There is no protection profile and therefore no extended functional requirements met by the TOE.

Annex D: Security Policy Details

See section III above.

Annex E: Assumptions and Clarification of Scope

See section IV above.

Annex F: IT Product Testing

Developer Testing

The TOE was installed using the vendor-supplied documentation. Vendor test cases were performed and verified. These covered audit generation and review, user identity, and access control. Both permission and denial cases were verified during access control tests. Management functions and password generation were verified, also using positive and negative cases.

The evaluation team determined that the developer's actual test results matched the vendor's expected results.

Evaluation Team Independent Testing

The evaluation team ensured that the TOE performed as described in the design documentation and demonstrated that the TOE enforces the TOE security functional requirements. Specifically, the evaluation team ensured that the developer test documentation sufficiently addresses the security functions as described in the functional specification and high level design. The evaluation team performed a sample of the developer's test suite and devised an independent set of team tests and penetration tests. Although the evaluation team performed a sample of the developer's test suite, the selected tests were representative of the TOE Security Functions.

Team testing was performed to verify details of the audit selection, reporting, and audit record protection mechanisms. Access control rules were verified as well as user account management restrictions.

Penetration testing was performed using probes of the user interface using a web browser. A port query tool was used to explore services provided by the IDM system.

Annex G: Security Target

Sun Java™ System Identity Manger – Version 5.0, Security Target, version 2.4

The document identifies the security functional requirements necessary to implement Access Control security policies. Additionally, the Security Target specifies the security assurance requirements necessary for EAL 2.

Annex H: Documentation

The following documentation was used during the evaluation.

IDM_Administration_5_0.pdf	Sun Java™ System Identity Manager Administration 5.0 Part No: 817-7804-05
IDM_Installation_5_0.pdf	Sun Java™ System Identity Manager Installation 5.0 Part No: 817-7803-05
IDM Release_Notes_5_0.pdf	Sun Java™ System Identity Manager Release Notes 5.0 Part No: 817-7988-01
IDM_Technical_Deployment_5_0.pdf	Sun Java™ System Identity Manager Technical Deployment Part No: 817-7805-05
IDM_Technical_Reference_5_0.pdf	Sun Java™ System Identity Manager Technical Reference - Part No: 817-7806-05

Annex I: Glossary

CC	Common Criteria
EAL	Evaluation Assurance Level
ID	Identifier
IDM	Sun Java™ System Identity Manager
IT	Information Technology
NIAP	National Information Assurance Partnership
PP	Protection Profile
SF	Security Function
SFP	Security Function Policy
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSFI	TSF Interface
TSP	TOE Security Policy

Annex J: Bibliography

The Validation Team used the following documents to produce this Validation Report:

- *Common Criteria for Information Technology Security Evaluation*, CCIMB-2004-01-002, Version 2.2, January 2004.

- Common Criteria, Evaluation and Validation Scheme for Information Technology Security, *Guidance to Validators of IT Security Evaluations*, Scheme Publication #3, Version 1.0, January 2002.

- *Common Evaluation Methodology for Information Technology Security* – Part 1: Introduction and general model, version 0.6, 11 January 1997.

- *Common Evaluation Methodology for Information Technology Security* – Part 2: Evaluation Methodology, CCIMB-2004-01-004, Version 2.2, January 2004

- *Sun Java™ System Identity Manger – Version 5.0, Security Target, version 2.4.*

- *Sun Java™ System Identity Manager Evaluation Technical Report Volume 1*, Version 1.8.

- *Sun Java™ System Identity Manager Evaluation Technical Report Volume 2*, Version 1.8.