Certification Report

EAL 4+ Evaluation of

Solaris 10 Release 11/06 Trusted Extensions

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number:	383-4-57-CR
Version:	1.0
Date:	11 June 2008
Pagination:	i to iv, 1 to 15

DISCLAIMER

The Information Technology (IT) product identified in this certification report, and its associated certificate, have been evaluated at an approved evaluation facility – established under the Canadian Common Criteria Evaluation and Certification Scheme (CCS) – using the *Common Methodology for Information Technology Security Evaluation, Version 2.3*, for conformance to the *Common Criteria for IT Security Evaluation, Version 2.3*. This certification report, and its associated certificate, apply only to the identified version and release of the product in its evaluated configuration. The evaluation has been conducted in accordance with the provisions of the CCS, and the conclusions of the evaluation facility in the evaluation report are consistent with the evidence adduced. This report, and its associated certificate, are not an endorsement of the IT product by the Communications Security Establishment Canada, or any other organization that recognizes or gives effect to this report, and its associated certificate, and no warranty for the IT product by the Communications Security Establishment Canada, or any other organization that recognizes or gives effect to this report, and its associated certificate, is either expressed or implied.

FOREWORD

The Canadian Common Criteria Evaluation and Certification Scheme (CCS) provides a third-party evaluation service for determining the trustworthiness of Information Technology (IT) security products. Evaluations are performed by a commercial Common Criteria Evaluation Facility (CCEF) under the oversight of the CCS Certification Body, which is managed by the Communications Security Establishment Canada.

A CCEF is a commercial facility that has been approved by the CCS Certification Body to perform Common Criteria evaluations; a significant requirement for such approval is accreditation to the requirements of *ISO Standard 17025, General requirements for the accreditation of calibration and testing laboratories*. Accreditation is performed under the Program for the Accreditation of Laboratories Canada (PALCAN), administered by the Standards Council of Canada.

The CCEF that carried out this evaluation is CGI Information Systems and Management Consultants Incorporated, located in Ottawa, Ontario.

By awarding a Common Criteria certificate, the CCS Certification Body asserts that the product complies with the security requirements specified in the associated security target. A security target is a requirements specification document that defines the scope of the evaluation activities. The consumer of certified IT products should review the security target, in addition to this certification report, in order to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the product satisfies the security requirements.

This certification report is associated with the certificate of product evaluation dated 11 June 2008, and the security target identified in Section 4 of this report.

The certification report, certificate of product evaluation and security target are posted on the CCS Certified Products list at: http://www.cse-cst.gc.ca/services/common-criteria/trusted-products-e.html and http://www.commoncriteriaportal.es .

This certification report makes reference to the following trademarked names:

- Solaris and Java, which are registered trademarks of Sun Microsystems Inc.;
- UNIX, which is a registered trademark of The Open Group in the United States and other countries; and
- SPARC, which is a registered trademark of SPARC International, Inc.

Reproduction of this report is authorized provided the report is reproduced in its entirety.

TABLE OF CONTENTS

Executive Summary

The Solaris 10 Release 11/06 Trusted Extensions (hereafter referred to as Solaris Trusted Extensions), from Sun Microsystems Inc., is the Target of Evaluation for this Evaluation Assurance Level (EAL) 4 augmented evaluation.

Solaris is a highly-configurable UNIX-based operating system. Originally developed to meet the requirements of the C2 class of the U.S. Department of Defence (DoD) Trusted Computer System Evaluation Criteria (TCSEC), it now meets specific equivalent Protection Profiles developed within the Common Criteria Project. These broad requirements are described for the Common Criteria scheme in the Controlled Access Protection Profile (CAPP) and the Role Based Access Control Protection Profile (RBAC).

Solaris Trusted Extensions has been developed to meet the requirements of the B1 class of the TCSEC, and now meets the equivalent Labeled Security Protection Profile (LSPP) in addition to the CAPP and RBAC by virtue of the underlying Solaris 10 Release 11/06 operating system. Solaris Trusted Extensions extends Solaris 10 Release 11/06 security by enforcing a mandatory access control policy. Sensitivity labels are automatically applied to all sources of data (networks, file systems, windows) and consumers of data (user and processes). Access to all data is restricted based on the relationship between the label of the data (object) and the consumer (subject).

A Solaris Trusted Extensions system consists of a number of workstations and/or servers linked together to form a single distributed system. Users share the resources of multiple workstations and/or servers connected together in a single, distributed Trusted Computing Base.

CGI Information Systems and Management Consultants Inc. is the CCEF that conducted the evaluation. This evaluation was completed on 10 June 2008, and was carried out in accordance with the rules of the Canadian Common Criteria Evaluation and Certification Scheme (CCS).

The scope of the evaluation is defined by the security target, which identifies assumptions made during the evaluation, the intended environment for Solaris Trusted Extensions, the security requirements, and the level of confidence (evaluation assurance level) at which the product is intended to satisfy the security requirements. Consumers are advised to verify that their operating environment is consistent with that specified in the security target, and to give due consideration to the comments, observations and recommendations in this certification report.

The results documented in the Evaluation Technical Report[1] for this product provide sufficient evidence that it meets the EAL 4 augmented assurance requirements for the evaluated security functionality. The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 2.3* (with applicable final interpretations), for conformance to the *Common Criteria for Information Technology Security Evaluation, version 2.3*. The following augmentations is claimed: ALC_FLR.3 – Systematic Flaw Remediation.

Communications Security Establishment Canada, as the CCS Certification Body, declares that the Solaris Trusted Extensions evaluation meets all the conditions of the *Arrangement on the Recognition of Common Criteria Certificates* and that the product will be listed on the CCS Certified Products list (CPL) and the Common Criteria portal (the official website of the Common Criteria Project).

[1] The evaluation technical report is a CCS document that contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 4 augmented evaluation is Solaris 10 Release 11/06 Trusted Extensions (hereafter referred to as Solaris Trusted Extensions), from Sun Microsystems Inc.

2 TOE Description

Solaris is a highly-configurable UNIX-based operating system. Originally developed to meet the requirements of the C2 class of the U.S. Department of Defence (DoD) Trusted Computer System Evaluation Criteria (TCSEC), it now meets specific equivalent Protection Profiles developed within the Common Criteria Project. These broad requirements are described for the Common Criteria scheme in the Controlled Access Protection Profile (CAPP) and the Role Based Access Control Protection Profile (RBAC).

Solaris Trusted Extensions has been developed to meet the requirements of the B1 class of the TCSEC, and now meets the equivalent Labeled Security Protection Profile (LSPP) in addition to the CAPP and RBAC by virtue of the underlying Solaris 10 Release 11/06 operating system. Solaris Trusted Extensions extends Solaris 10 Release 11/06 security by enforcing a mandatory access control policy. Sensitivity labels are automatically applied to all sources of data (networks, file systems, windows) and consumers of data (user and processes). Access to all data is restricted based on the relationship between the label of the data (object) and the consumer (subject).

A Solaris Trusted Extensions system consists of a number of workstations and/or servers linked together to form a single distributed system. Users share the resources of multiple workstations and/or servers connected together in a single, distributed Trusted Computing Base.

3 Evaluated Security Functionality

The complete list of evaluated security functionality for Solaris Trusted Extensions is identified in Section 6 of the Security Target.

4 Security Target

The ST associated with this Certification Report (CR) is identified by the following nomenclature:

Title: Solaris 10 11/06 Trusted Extensions Security Target
Version: 1.21
Date: 04 June 2008

5 Common Criteria Conformance

The evaluation was conducted using the *Common Methodology for IT Security Evaluation, Version 2.3,* for conformance to the *Common Criteria for IT Security Evaluation, Version 2.3.*

Solaris Trusted Extensions is:

a) Common Criteria Part 2 conformant, with security functional requirements based only upon functional components in Part 2;

b) Common Criteria Part 3 conformant, with security assurance requirements based only upon assurance components in Part 3; and

c) Common Criteria EAL 4 augmented, containing all security assurance requirements in the EAL 4 package, as well as the following: ALC_FLR.3 – Systematic Flaw Remediation.

Solaris Trusted Extensions is conformant to the following Protection Profiles:

a) Controlled Access Protection Profile Version 1.d, October 8, 1999;

b) Role Based Access Control Protection Profile, Version 1.0, July 30, 1998; and

c) Labeled Security Protection Profile, Version 1.b, 8 October 1999.

6 Security Policies

Solaris Trusted Extensions implements discretionary access control and mandatory access control security policies as specified in Controlled Access Protection Profile, Version 1.d, 8 October 1999, Role Based Access Control Protection Profile, Version 1.0, 30 July 1998, and Labeled Security Protection Profile, Version 1.b, 8 October 1999. Details on the Solaris Trusted Extensions access control policies are found in Section 5 of the ST.

In addition, Solaris Trusted Extension implements policies pertaining to audit, user data protection, identification and authentication, security management, protection of the TSF, trusted path/channels, trusted recovery, specification of management functions, and TOE access. Details on these security policies are found in Section 5 of the ST.

7 Assumptions and Clarification of Scope

Consumers of Solaris Trusted Extensions should consider assumptions about usage and environmental settings as requirements for the product's installation and its operating environment. This will help to ensure the proper and secure operation of Solaris Trusted Extensions.

7.1 Secure Usage Assumptions

The following secure usage assumptions are listed in the ST:

a. Each individual user is assumed to have a unique user ID.
b. Those responsible for the TOE must configure minimum password length for normal users to be at least 8 characters.
c. Rights for users to gain access and perform operations on information are based on their membership in one or more roles (and the profiles that accompany these roles). These roles are granted to the users by the TOE Administrator. These roles accurately reflect the users job function, responsibilities, qualifications, and/or competencies within the enterprise.
d. There will be one or more competent and trustworthy individuals assigned to manage TOE security. These individuals will have sole responsibility for the following functions: create and maintain roles; establish and maintain relationships among roles; and assignment and revocation of users to roles. In addition these individuals (as 'owners of the entire corporate data') along with object owners will have the ability to assign and revoke object access rights to roles.
e. A limited set of users is given the rights to "create new data objects" and they become owners for those data objects. The organization is the owner of the rest of the information under the control of TOE.
f. The system administrative personnel are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the administrator documentation.
g. Authorized users possess the necessary authorization to access at least some of the information managed by the TOE and are expected to act in a cooperating manner in a benign environment.
h. It is assumed that, if the product comprises more than one platform, all platforms are administered from a central point within each LDAP directory domain.

7.2 Environmental Assumptions

The following environmental assumptions are listed in the ST:

a. The TOE hardware and software critical to security policy enforcement will be physically protected from unauthorized modification by potentially hostile outsiders. It is assumed that all software and hardware, including network and peripheral cabling is approved for the transmittal of the most sensitive data held by the system. Such items are assumed to be physically protected against threats to the confidentiality and integrity of the data transmitted.
b. The processing resources of the TOE will be located within controlled access facilities which will prevent unauthorized physical access.
c. It is also assumed that the value of the stored assets merits moderately intensive penetration or masquerading attacks. It is also assumed that physical controls in place

would alert the system authorities to the physical presence of attackers within the controlled space.

d. Procedures exist for granting users authorization for access to specific security levels.
e. Procedures exist for establishing the security level of all information imported into the system, for establishing the security level for all peripheral devices (e.g., printers, tape drives, disk drives) attached to the TOE, and marking a sensitivity label on all output generated.
f. All bridges and routers are assumed to correctly pass data without modification.
g. All connections to peripheral devices reside within the controlled access facilities. CAPP/LSPP/RBAC-conformant TOEs address security concerns related to the manipulation of the TOE through its legitimate interfaces. Internal communication paths to interfaces points such as terminals are assumed to be adequately protected.
h. Any other systems with which the TOE communicates are assumed to be under the same management control and operate under the same security policy constraints. CAPP and LSPP-conformant TOEs are applicable to networked or distributed environments only if the entire network operates under the same constraints and resides within a single management domain. There are no security requirements which address the need to trust external systems or the communications links to such systems.

For more information about the TOE security environment, refer to Section 3 of the ST.

7.3 Clarification of Scope

As described in the ST, the following threats are not countered by the TOE and are assumed to be countered by the measures within the TOE environment:

a. Where specific threats to distributed systems need to be countered, data transferred between platforms may be disclosed to, or modified by, unauthorized users or processes either directly or indirectly (e.g. through spoofing of workstation/server identity).
b. Compromise of the IT assets may occur because of improper administration and operation of the TOE. Users or external threat agents may, through accidental discovery or directed search, discover inadequacies in the security administration of the TOE which permit them to gain logical access to and perform operations on its resources in breach of any permissions they may have. Potential attackers may seek to develop methods whereby the improperly administered security functions of the TOE may be circumvented during normal operation.
c. The development and assignment of user roles may be done in a manner that undermines security. In general, roles could be developed which have an incorrect or improper combination of authorizations to perform operations on objects. In addition, users could be assigned to roles that are incommensurate with their duties, giving them either too much or too little scope of authorization. A particular concern arises in that users could be assigned conflicting roles with respect to ‘separation of duties’. An individual user could be authorized to perform multiple operations on data objects

that represent the parts of a transaction that should be separated among different individuals.

8 Architectural Information

The Solaris Trusted Extensions is an operating system that comprises the following main subsystems:

Kernel Processes. The Kernel Processes subsystem supports the security functionality of the product. Detail on security functionality can be found in Section 2.4 of the ST.

Kernel V Inter-Process Communications (SVIPC). Solaris Trusted Extensions implements System V IPC (Inter Process Communication) that allows single-level communication between processes. Three mechanisms are provided: Semaphores; Message Queues; and Shared Memory. The Semaphore mechanism allows processes to synchronize their execution using mutually exclusive access to critical sections. The Message Queue mechanism allows cooperating processes to send and receive formatted data between themselves. The Shared Memory mechanism allows processes to attach (map) system memory spaces to their virtual address spaces and share these attached system spaces.

File Systems. The File System component provides a system call interface used to access the variety of file system types supported by Solaris Trusted Extensions. The system call interface provides a consistent set of operations which can be performed on all the file system types.

Audit. The Audit subsystem collects extensive auditing information about security related actions taken or attempted by users, ensuring that users are accountable for their actions. For each such action or event an audit record is generated containing: date and time of the event, user, security attributes and success or failure. Detail on Audit can be found in Section 2.4.7 of the ST.

Identification and Authentication (I&A). The I&A subsystem provides identification and authentication as a built-in feature using the Pluggable Authentication Module (PAM) based on user ID and passwords. As part of the login process session clearance and sensitivity labels are processed and obtained. Detail on I&A can be found in Section 2.4.4 of the ST.

Lightweight Directory Access Protocol (LDAP). The LDAP subsystem maintains a central database of name services information for workstations and servers within a Domain.

Trusted Startup. The Trusted Startup subsystem ensures a secure transition from run level 0 (the power-down state) to the system run level.

Trusted Windowing. The Trusted Windowing subsystem provides the user with a choice of desktop environments. Solaris Trusted Extensions includes both the Common Desktop Environment (CDE) windowing environment and the Sun Trusted Java Desktop System

(TJDS) Operating Environment. Individual windows are labelled and must be within the range of sensitivity labels allowed to the corresponding user. Data transfer operations among windows is controlled in accordance with the MAC policy rules.

Trusted Admin Tools. The Trusted Admin Tools includes File Manager, which is a desktop application that enables users to create, locate, organize and work with files and directories on the desktop, and Solaris Management Console (SMC), that provides the user a Graphical User Interface (GUI) and a set of tools to help in administering a distributed configuration.

Devices. The Devices subsystem requires that a device (file system, terminal, disk drive, printer, network, etc.) be allocated for use and that the user is authorized to use the device.

Trusted Networking. The trusted networking subsystem allows data to be transmitted between workstations via the network while upholding applicable security policies.

Trusted Printing. The Trusted Printing subsystem provides labelling of printed output based on the sensitivity label of the data being printed.

Profile Shells. The Profile Shell subsystem provides a way to control the capabilities of users and roles assigned by an administrator. A profile defines commands, CDE or TJDS actions and authorizations that are permitted to the user.

9 Evaluated Configurations

The evaluated configurations for Solaris Trusted Extensions comprise the following:

Platform 1: Entry Level workstations and servers utilizing an UltraSPARC II, UltraSPARC IIe, UltraSPARC IIi, UltraSPARCIII, UltraSPARCIIIi, or UltraSPARC T1 processor in a single or multiple configuration.

Platform 2: The Netra 1280 and SunFire mid-frame and high-end family offering Dynamic Reconfiguration and Multiple Domaining and utilizing an UltraSPARC III Cu (copper based) or UltraSPARC IV processor.

Platform 3: AMD based processor systems: AMD Opteron 800, 1200, and 8000 series; AMD-64 100, 200, and 2000 series; AMD dual-core 1200 and 2000 series; AMD Opteron 285; and, Intel Xeon.

Detailed configuration information concerning the above mentioned platforms can be found in the ST, Appendix A.

10 Documentation

The documentation for Solaris Trusted Extensions consists of the following:

a. The Release Notes: Solaris 10 Operating System 11/06 SPARC, Part No. 708-0204-10, November 2006, Revision A; and Solaris 10 Operating System 11/06 x64/x86, Part No. 708-0205-10, November 2006, Revision A.
b. The Security Release Notes: v0.9, 28 May 2008.
c. The Delivery & Configuration Procedures: v0.5, 27 November 2006.
d. The System Administration Guide – Basic Administration: Part No. 817-1985-17, April 2008.
e. The System Administration Guide – Advanced Administration: Part No. 817-0403-15, 2008.
f. The System Administration Guide: Security Services; Part No: 816-4557-15, April 2008.
g. The Common Desktop Environment: User's Guide; Part No: 806-4743-10, May 2002.
h. The Common Desktop Environment: Advanced User's and System Administrator's Guide: Part No. 806-7492-10, May 2002.
i. The Man pages: Part No. 816-5165-13, April 2008.

Note: A comprehensive library of Solaris 10 11/06 documentation is available online at http://docs.sun.com/app/docs/coll/40.10?l=en

11 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of Solaris Trusted Extensions, including the following areas:

Configuration management: An analysis of the Solaris Trusted Extensions configuration management system and associated documentation was performed. The evaluators found that the Solaris Trusted Extensions configuration items were clearly marked, and could be modified and controlled, and that the configuration management system supported generation of the TOE. The developer's configuration management system was observed during a site visit, and it was found to be mature and well developed.

Secure delivery and operation: The evaluators examined the delivery documentation and determined that it described all of the procedures required to maintain the integrity of Solaris Trusted Extensions during distribution to the consumer. The evaluators examined and tested the installation, generation and start-up procedures, and determined that they were complete and sufficiently detailed to result in a secure configuration.

Design documentation: The evaluators analysed the Solaris Trusted Extensions functional specification, high-level design, low-level design, security policy model, and a subset of the implementation representation; they determined that the documents were internally consistent, and completely and accurately instantiated all interfaces and security functions. The evaluators also independently verified that the correspondence mappings between the design documents were correct.

Guidance documents: The evaluators examined the Solaris Trusted Extensions administrator and user guidance documentation and determined that it sufficiently and unambiguously described how to securely use and administer the product, and that it was consistent with the other documents supplied for evaluation.

Life-cycle support: The evaluators examined the development security procedures during a site visit and determined that they detailed sufficient security measures for the development environment to protect the confidentiality and integrity of the Solaris Trusted Extensions design and implementation. The evaluators determined that the developer has used a documented model of the TOE life-cycle and well-defined development tools that yield consistent and predictable results.

The evaluators reviewed the flaw remediation procedures used by Sun Microsystems Inc for Solaris Trusted Extensions. During a site visit, the evaluators also examined the evidence generated by adherence to the procedures. The evaluators concluded that the procedures that sufficiently describe the tracking of security flaws, the identification of corrective actions, and the distribution of corrective action information to TOE users.

Vulnerability assessment: The Solaris Trusted Extensions ST's strength of function claims were validated through independent evaluator analysis. The evaluators examined the developer's vulnerability analysis for the Solaris Trusted Extensions and found that it sufficiently described each of the potential vulnerabilities along with a sound rationale as to why it was not exploitable in the intended environment. Additionally, the evaluators conducted an independent review of public domain vulnerability databases, and all evaluation deliverables to provide assurance that the developer has considered all potential vulnerabilities.

All these evaluation activities resulted in **PASS** verdicts.

12 ITS Product Testing

Testing at EAL 4 consists of the following three steps: assessing the developer's tests, performing independent functional tests, and performing independent penetration tests.

12.1 Assessing Developer Tests

The evaluators verified that the developer has met their testing responsibilities by examining their test evidence, and reviewing their test results, as documented in the ETR[2].

[2] The ETR is a CCS document that contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

The developer’s tests comprise a Test Suite, that contains both automated and manual tests. The automated tests are used to cover most security functions and do not require manual input from the user. Throughout the automated tests, a details commentary is echoed to the active shell window and written to a log file. These log files comprise a large part of the Test Report and are written in an intuitive enough way for the evaluators to understand.

Supplementary *ad hoc* manual tests are also used to ensure complete security functions coverage in conjunction with the automated test suite. The developer’s Manual Tests and the Installation Procedures documents provide considerable test cases including test procedure descriptions and expected test results.

The evaluators analyzed the developer’s test coverage and depth analysis and found them to be complete and accurate. The correspondence between the tests identified in the developer’s test documentation and the functional specification was complete.

12.2 Independent Functional Testing

During this evaluation, the evaluator developed independent functional tests by examining design and guidance documentation, examining the developer's test documentation, executing a sample of the developer's test cases, and creating test cases that augmented the developer tests.

All testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and results. Resulting from this test coverage approach was the following list of CGI Information Systems and Management Consultants Incorporated test goals:

a. Repeat of Developer's Tests: The objective of this test goal is to repeat a subset of the developer's tests and compare with the developers results;
b. Mandatory Access Control (MAC): The objective of this test goal is to determine that a subject may only access labelled objects that are at or below their specific clearance level;
c. Discretionary Access Control (DAC): The objective of this test goal is to determine that a subject may only access objects based on UserID and GroupID and that DAC is not affected by MAC;
d. Trusted Path: The objective of this test goal is to determine the TOE's ability to provide a subject with a limited conduit between objects of different clearance levels;
e. Identification and Authentication: The objective of this test goal is to determine the TOE's ability to ensure the Identification and Authentication requirements have been met; and
f. Audit: The objective of this test goal is to determine the TOE's ability to ensure audit data is recorded, stored and can be viewed.

12.3 Independent Penetration Testing

Subsequent to the examination of the developer's vulnerability analysis, independent vulnerability analysis, and the independent review of public domain vulnerability databases and all evaluation deliverables, limited independent evaluator penetration testing was conducted. The penetration tests focused on:

a. Verification that the certification patch set was effective in mitigating vulnerabilities known to exist in Solaris Trusted Extensions;
b. Attempts to disprove the developer’s vulnerability analysis;
c. Regression testing, involving re-running penetration tests from the previous Solaris 10 Release 11/06 evaluation; and
d. Testing based on vulnerability analysis conducted by the evaluator.

The independent penetration testing did not uncover any exploitable vulnerabilities in the anticipated operating environment.

12.4 Conduct of Testing

Solaris Trusted Extensions was subjected to a comprehensive suite of formally documented, independent, functional and penetration tests. The testing took place at the ITSET facility at CGI Information Systems and Management Consultants Incorporated. The CCS Certification Body witnessed a portion of the independent testing. The detailed testing activities, including configurations, procedures, test cases, expected results and observed results are documented in a separate Test Results document.

12.5 Testing Results

The developer’s tests and the independent functional tests yielded the expected results, giving assurance that Solaris Trusted Extensions behaves as specified in its ST and functional specification. The penetration testing resulted in a **PASS** verdict, as the evaluators were unable to exploit any of the identified potential vulnerabilities in Solaris Trusted Extensions in its intended operating environment

13 Results of the Evaluation

This evaluation has provided the basis for an EAL 4 + level of assurance. The overall verdict for the evaluation is PASS. These results are supported by evidence in the ETR.

14 Evaluator Comments, Observations and Recommendations

As described in the ST and previous sections of this document, where specific threats to distributed systems need to be countered, data transferred between platforms may be disclosed to or modified by unauthorized users or processes either directly or indirectly (e.g.

through spoofing of workstation/server identity). This threat is not countered by the TOE and is assumed to be countered by the measures within the TOE environment. Consumers are advised to review the ST and ensure that their deployment environment is consistent with the defined intended environment.

15 Acronym/Abbreviation/Initialization

Acronym/Abbreviation/Initialization	Description
CAPP	Controlled Access Protection Profile
CB	Certification Body
CC	Common Criteria for Information Technology Security Evaluation
CCEF	Common Criteria Evaluation Facility
CCRA	Common Criteria Recognition Arrangement
CCS	Common Criteria Evaluation and Certification Scheme
CDE	Common Desktop Environment
CEM	Common Methodology for Information Technology Security Evaluation
CPL	Certified Products List
CR	Certification Report
DAC	Discretionary Access Control
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
GUI	Graphical User Interface
I&A	Identification and Authentication
ISO	International Organisation for Standardisation
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
LDAP	Lightweight Directory Access Protocol
SMC	Solaris Management Console
SVIPC	Kernel V Inter-Process Communications
LDAP	Lightweight Directory Access Protocol
LSPP	Labelled Security Protection Profile
OS	Operating System
MAC	Mandatory Access Control
PALCAN	Program for the Accreditation of Laboratories Canada
PAM	Pluggable Authentication Module
PP	Protection Profile
RBAC	Role Based Access Control
ST	Security Target
TCSEC	Trusted Computer System Evaluation Criteria
TJDS	Trusted Java Desktop System
TOE	Target of Evaluation
TSF	TOE security functions

16 References

This section lists all documentation used as source material for this report:

a) Canadian Common Criteria Evaluation and Certification Scheme (CCS) Publication #4, Technical Oversight, Version 1.0.

b) Common Criteria for Information Technology Security Evaluation, version 2.3, August 2005.

c) Common Methodology for Information Technology Security Evaluation, CEM, version 2.3, August 2005.

d) Solaris 10 11/06 Trusted Extensions Security Target, Version 1.21, 04 June 2008.

e) Evaluation Technical Report of Solaris Trusted Extensions, Version 1.2, 10 June 2008.

f) Controlled Access Protection Profile (CAPP), Version 1.d, 8 October 1999.

g) Role Based Access Control Protection Profile (RBAC), Version 1.0, 30 July 1998.

h) Labeled Security Protection Profile (LSPP), Version 1.b, 8 October 1999.